

# Differential Algebra and Algebraic Groups

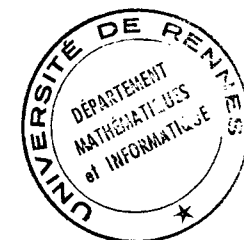
**E. R. Kolchin**

*Department of Mathematics  
Columbia University, New York*

This is Volume 54 in  
PURE AND APPLIED MATHEMATICS  
A series of Monographs and Textbooks  
Editors: PAUL A. SMITH AND SAMUEL EILENBERG  
A complete list of titles in this series appears at the end of this volume



ACADEMIC PRESS 1973 New York and London



12 H 05  
14 L 107

To Kate

COPYRIGHT © 1973, BY ACADEMIC PRESS, INC.  
ALL RIGHTS RESERVED.  
NO PART OF THIS PUBLICATION MAY BE REPRODUCED OR  
TRANSMITTED IN ANY FORM OR BY ANY MEANS, ELECTRONIC  
OR MECHANICAL, INCLUDING PHOTOCOPY, RECORDING, OR ANY  
INFORMATION STORAGE AND RETRIEVAL SYSTEM, WITHOUT  
PERMISSION IN WRITING FROM THE PUBLISHER.

ACADEMIC PRESS, INC.  
111 Fifth Avenue, New York, New York 10003

*United Kingdom Edition published by*  
ACADEMIC PRESS, INC. (LONDON) LTD.  
24/28 Oval Road, London NW1

LIBRARY OF CONGRESS CATALOG CARD NUMBER: 72-77346

AMS (MOS) 1970 Subject Classifications: 12H05, 14L10

PRINTED IN THE UNITED STATES OF AMERICA

## Contents

<i>Preface</i>	xi
<i>Acknowledgments</i>	xvii

### Chapter 0 Algebraic Preliminaries

1	Conventions	1
2	Separable dependence	2
3	Quasi-separable field extensions	4
4	Quotients	7
5	Perfect ideals	7
6	Separable, quasi-separable, and regular ideals	8
7	Conservative systems	10
8	Perfect conservative systems	12
9	Noetherian conservative systems	13
10	Morphisms and birational equivalence of ideals	16
11	Polynomial ideals and generic zeros	19
12	Polynomial ideals and ground field extension	20
13	Power series	29
14	Specializations	33
15	Algebraic function fields of one variable	41
16	Dimension of components	43
17	Lattice points	49
18	Shapiro's lemma	53
19	$t$ -Values	56

**Chapter I Basic Notions of Differential Algebra**

1	Differential rings	58
2	Homomorphisms and differential ideals	61
3	Differential rings of quotients	63
4	Transformation and restriction of the set of derivation operators	65
5	Differential modules; differential algebras	66
6	Differential polynomial algebras	69
7	Permissible gradings	72
8	Rank	75
9	Autoreduced sets	77
10	Characteristic sets	81
11	Pseudo-leaders	83
12	Differential algebras of power series	84

**Chapter II Differential Fields**

1	Linear dependence over constants	86
2	Separable extensions	89
3	Differentially perfect and differentially quasi-perfect differential fields	92
4	Separable dependence over constants	93
5	Differential polynomial functions	95
6	Dependence of derivative operators	95
7	Differentially separable dependence	99
8	Differentially separable extensions	100
9	Differential inseparability bases	104
10	Differential transcendence bases	108
11	Finitely generated extensions	109
12	Differential inseparability polynomials	115
13	Differential type; typical differential inseparability degree	118

**Chapter III The Basis Theorem and Some Related Topics**

1	Differential conservative systems	121
2	Quasi-separable differential ideals	123
3	Differential fields of definition	125
4	The basis theorem	126
5	Differential dimension polynomials	129
6	Extension of the differential field of coefficients	130
7	Universal extensions	133
8	$\mathfrak{f}$ -Coherent autoreduced sets	135
9	Differential specializations	138
10	Constrained families	142

**Chapter IV Algebraic Differential Equations****PART A. CHARACTERISTIC  $p$  ARBITRARY**

1	Differential affine space. The differential Zariski topology	145
2	Generic zeros. The theorem of zeros	146
3	Closed sets and $\mathcal{A}$ -separable differential ideals	147
4	The relative topologies; differential fields of definition	148
5	Linear differential ideals	150
6	General components	155
7	General components and differential dimension polynomials	160
8	Multiplicity of zeros	164

**PART B. CHARACTERISTIC  $p = 0$** 

9	Finite sets of differential polynomials	166
10	The leading coefficient theorem	171
11	Levi's lemma	176
12	The domination lemma	178
13	Preparations	183
14	The component theorem	185
15	The low power theorem	187
16	The Ritt problem	190
17	Systems of bounded order	194
18	Substitution of powers	202

<b>Bibliography for Chapters I-IV</b>	<b>206</b>
---------------------------------------	------------

**Chapter V Algebraic Groups**

1	Introduction	212
2	Pre- $K$ -sets	215
3	$K$ -Groups and homogeneous $K$ -spaces. $K$ -Sets	218
4	Extending the universal field	227
5	Extending the basic field	230
6	Zariski topology; $K$ -topology	236
7	Closed sets	240
8	$K$ -Subgroups	247
9	$K$ -Homomorphisms	249
10	Direct products	257
11	Quotients	267
12	Galois cohomology	273
13	Principal homogeneous $K$ -spaces	281
14	Holomorphicity at a specialization	287
15	$K$ -Mappings	294
16	$K$ -Functions	306
17	$K$ -Cohomology	318
18	Invariant derivations and differentials. The Lie algebra	322



19	Local rings	331
20	Tangent spaces	334
21	Crossed $K$ -homomorphisms	341
22	Logarithmic derivatives	349
23	Linear $K$ -groups	354
24	Abelian $K$ -groups	376
	<b>Bibliography for Chapter V</b>	383
	<b>Chapter VI Galois Theory of Differential Fields</b>	
1	Specializations of isomorphisms	385
2	Strong isomorphisms	388
3	Strongly normal extensions. Galois groups	393
4	The fundamental theorems	398
5	Examples	404
6	Picard–Vessiot extensions	409
7	$G$ -Primitives	418
8	Differential Galois cohomology	421
9	Applications	426
10	$V$ -Primitives	427
	<b>Bibliography for Chapter VI</b>	431
	<i>Glossary of Notation</i>	435
	<i>Index of Definitions</i>	441

## Preface

It is common knowledge that algebra, including algebraic geometry, historically grew out of the study of algebraic equations with numerical coefficients. In much the same way, differential algebra sprang from the classical study of algebraic differential equations with coefficients that are meromorphic functions in a region of some complex space  $C^m$ . As a consequence, differential algebra bears a considerable resemblance to the elementary parts of algebraic geometry. Indeed, since an algebraic equation can be considered as a differential equation in which derivatives do not occur, it is possible to consider algebraic geometry as a special case of differential algebra.<sup>1</sup>

It is noteworthy that a subject so substantial as differential algebra owes its existence to one person. J. F. Ritt (1893–1951) was not only its founding father, but also its principal prophet and practitioner. Today, 22 years after his death, the majority of the main results, and the deepest ones, are due to him, and despite a new look, the main lines of the subject today are the same as in 1951. It had already become clear then that differential algebra is pure algebra, and although Ritt's life blood was classical analysis, in his second book<sup>2</sup> on the subject [95]<sub>1</sub> he made a great effort to meet the algebraist half way.

<sup>1</sup> This can be done in two ways: (1) by thinking of an algebraic equation as a differential equation of order 0; (2) by allowing the number  $m$  to be 0.

<sup>2</sup> There are three bibliographies in the present book, the first (and main) one for Chapters I–IV, the second one for Chapter V, and the third one for Chapter VI. The notation [95]<sub>1</sub> refers to the work numbered 95 in the first bibliography. Within Chapters I–IV the same work is referred to simply by [95].

My main goal in this book is to provide a unified exposition of present-day differential algebra, in a purely algebraic setting and subject to the constraint that everything be accessible to the reader who has mastered a standard first year graduate course in algebra (the material in Lang's "Algebra" [22]<sub>2</sub>, for example, being more than enough). This constraint has necessitated a preliminary Chapter 0 containing some algebraic results not likely to be met in such a course. Differential algebra itself begins in Chapter I, which introduces the basic concepts (differential rings, differential fields, differential polynomials, ...) and develops some of the basic techniques. Chapter II deals with differential fields and their extensions, not including the Galois theory. Chapter III is concerned mainly with differential polynomials; among other things it contains the basis theorem and some results about differential specializations. Chapter IV applies the preceding chapters to the study of algebraic differential equations; systems of equations and, in greater detail, single equations are treated. These four chapters make up the Ritt theory, present version.

The concluding Chapter VI is devoted to the Galois theory of differential fields. Although it makes use of the Ritt theory, its roots lie elsewhere, namely, in the late 19th century work of Picard [33, 34]<sub>3</sub> and his follower Vessiot [40, 41]<sub>3</sub>. This pioneering work suffered somewhat from an incompleteness and a certain lack of clarity and rigor, imposed in part by the absence of a well-developed theory of algebraic differential equations and of a theory of algebraic groups. During the ensuing half century the field lay largely fallow. In addition to expository articles by Schlesinger [38]<sub>3</sub>, Picard [37]<sub>3</sub>, and Vessiot [42]<sub>3</sub>, and a critical appraisal by Baer [1]<sub>3</sub>, there were only a few papers published that shed new light on the subject (Beke [2, 3]<sub>3</sub>, Picard [35, 36]<sub>3</sub>, Marotte [30]<sub>3</sub>, Fano [9]<sub>3</sub>, Loewy [27–29]<sub>3</sub>). Their chief concern was clarifying the nature of the group of a homogeneous linear ordinary differential equation, working out the connection between reducibility of the equation and reducibility of the group, and studying the case in which a fundamental system of solutions is algebraically dependent over constants.

In the Galois theory as presented here, the emphasis is on extensions as opposed to equations. The first order of business is to identify the "right" class of extensions of a differential field  $\mathcal{F}$ , namely, the "strongly normal" ones. After these have been defined and the group  $G$  of such an extension has been defined, it is possible to proceed by either of two routes: (1) to make use of the existing theory of algebraic groups and to prove that  $G$  is isomorphic, in a certain way, to an algebraic group defined over the field of constants of  $\mathcal{F}$ ; (2) to develop anew the theory of algebraic groups along axiomatic lines and then to show that  $G$  satisfies the axioms. My papers [18, 19]<sub>3</sub> on the Galois theory followed (1); the present book follows (2). This has the advantage that now  $G$  is not merely isomorphic to an algebraic group, but actually is one.

The axiomatic development of algebraic groups is carried out in the huge Chapter V (which unfortunately has grown in size far beyond my original expectations). More precisely, for any field  $K$  the axioms define the notion of " $K$ -group." These  $K$ -groups are the objects of a category (this word is not mentioned in the exposition), the morphisms of which are called " $K$ -homomorphisms." Every algebraic group defined over  $K$  has a natural structure of  $K$ -group, and (see Chapter V, Section 16, Corollary to Theorem 11 and the comment immediately following) every  $K$ -group is  $K$ -isomorphic to an algebraic group defined over  $K$ . A  $K$ -homomorphism between algebraic groups defined over  $K$  is a rational homomorphism defined over  $K$ . In keeping with the constraint imposed above, Chapter V does not demand of the reader any prior knowledge of the theory of algebraic groups; for all but a few exercises and the concluding Section 24, devoted to Abelian varieties, external references are not needed. In Section 24, I did not, unfortunately, find it possible to meet the constraint; in this section repeated use of external references is made.

Two features of the development of differential algebra in this book may be worth noting. The first is that there is no special distinction made between ordinary and partial differential equations. The governing philosophy is that I is merely a special case of  $m$ , a case neither requiring nor greatly benefitting from special treatment.

The second feature is that I try to do as much as possible for differential fields of arbitrary characteristic  $p$ . This is at the cost of tougher going at a number of places, and it is not clear that the results justify the cost. When the chips are down (namely, in Part B of Chapter IV and in Chapter VI), I am forced to retreat to the safe ground where  $p = 0$ . Perhaps the justification is that one should try, at least once, to learn just how much can be pushed through for arbitrary  $p$ . That a considerable amount can be was first shown by Seidenberg [108–110, 112]<sub>1</sub> (see also Okugawa [67]<sub>1</sub>). Ritt himself had no use for fields of nonzero characteristic and referred to them as "monkey fields."

There is a different approach possible to the case  $p \neq 0$ , namely, to change the definition of differential ring by replacing the notion of a derivation  $\delta$  by the notion of a "differentiation"  $(\delta^{(k)})_{k \in \mathbb{N}}$  in the sense of Helmut Hasse and F. K. Schmidt. When the underlying ring is an algebra over a field of characteristic 0, then  $\delta^{(k)} = (1/k!) \delta^k$  and the two definitions are equivalent, but in general neither subsumes the other. This different approach, which has been explored by Okugawa [68]<sub>1</sub> (see also Nishimura [57]<sub>1</sub>, Jaeger [23–29]<sub>1</sub>, Kasch [34]<sub>1</sub>), is not included in this book.

Among other significant and interesting results or theories not included are the following:

(a) Some analytic results of Ritt [95]<sub>1</sub>, Chapter VI, Strodt [116]<sub>1</sub>, and Seidenberg [111, 115]<sub>1</sub>. Among Ritt's results are an approximation theorem and a theorem on the components of an ordinary differential polynomial of order 1 over a differential field  $\mathcal{F}$  of meromorphic functions; the latter theorem makes sense when  $\mathcal{F}$  is any abstract ordinary differential field of characteristic 0, but a direct proof in this general setting is not known. Seidenberg's result is that an abstract finitely generated differential field of characteristic 0 is isomorphic to a differential field of meromorphic functions, and hence there is a "differential Lefschetz principle" whereby theorems true in the analytic case must be true in abstracto. This gives an indirect proof of the result of Ritt referred to above.

(b) Results of Goldman [10]<sub>3</sub> relating the Galois group of a homogeneous linear ordinary differential equation to the Galois group of the equation obtained by differentially specializing differential parameters appearing in the coefficients of the equation.

(c) Results of Johnson [30–32]<sub>1</sub>, on filtered differential modules and their applications to questions of dimension.

(d) Results of Kovacic [24, 25]<sub>3</sub> on the inverse problem of the Galois theory of differential fields. Given a differential field  $\mathcal{F}$  of characteristic 0 with field of constants  $\mathcal{C}$ , and given an algebraic group  $G$  defined over  $\mathcal{C}$ , the problem is to describe the set of strongly normal extensions of  $\mathcal{F}$  with Galois groups isomorphic to  $G$  over  $\mathcal{C}$  (in particular, to tell whether the set is empty or not). When  $\mathcal{F}$  is ordinary and  $G$  is either a connected solvable linear group or an Abelian variety, Kovacic's results are definitive. (For an earlier result see Białynicki-Birula [6]<sub>3</sub>.)

(e) Kovacic's generalization [26]<sub>3</sub> of the Galois theory in which a strongly normal extension need not be finitely generated and its Galois group has a natural structure of pro-algebraic group.

(f) Cassidy's launching [10]<sub>1</sub> of a theory of differential algebraic groups.

(g) Recent and current work by Blum [5]<sub>1</sub>, by Cassidy, and by Johnson on generalizing the concept of "differential algebraic set" (which is a subset of differential affine space closed in the differential Zariski topology), much as abstract algebraic varieties and schemes generalize the concept of affine algebraic variety.

The items on this list, especially the last three, are in areas ready for further development. To this list should be added a final item, not quite in the mainstream of differential algebra:

(h) The theory of integration in finite terms, created by Joseph Liouville in a series of papers between 1833 and 1841. Ritt's book [94]<sub>3</sub> summarizes the theory as of 1948, and contains a bibliography of the important contributions up to then. The subject has witnessed renewed activity more recently in


the work of Rosenlicht [106, 107]<sub>1</sub> (containing simple purely algebraic proofs of Liouville's theorem on functions with elementary integrals and related results), and Risch [76, 77]<sub>1</sub> (containing an algorithm for Liouville's theorem.) The paper by Ax [2]<sub>1</sub> has points of contact with the Liouville theory, especially with the results of Rosenlicht [107]<sub>1</sub>.

A word is in order about the bibliographies. In principle, every work on algebraic differential equations belongs to differential algebra, but obviously it would be both impractical and counterproductive to list all such works. The criterion I have used for selecting a work in the first or third bibliography is highly subjective: if it looks, sounds, feels, tastes, or smells like differential algebra it is included, otherwise not. Subject to this vague test, I have tried to be complete. As a consequence these two bibliographies include some unimportant or trivial or only marginally relevant papers. Excluded are works dealing with analogous or more general theories (difference algebra, fields with various kinds of operators, ...) unless they contribute something new to differential algebra. Various borderline cases were settled more or less at random.

By contrast, the criterion used for the second bibliography is fairly precise: a work is included if it is referred to in the text of Chapter V or was useful in its preparation.

## Acknowledgments

It is impossible for me to list all the people who helped or encouraged me during the various phases of the writing of this book. Foremost among these are my students and ex-students; countless hours of our continuing differential algebra seminar have been spent in thrashing out one point or another. Professors Cassidy and Kovacic, especially, have played important roles in this respect; they have read the text in many of its stages, have made numerous valuable suggestions, and have read the final draft with hawk-like vigilance. I take this opportunity to thank them both. The staff of Academic Press were cooperative and helpful; they have my sincere appreciation. Finally, I am grateful to the National Science Foundation, which subsidized my mathematical activities for many summers and two winters during the preparation of this book, and to the John Simon Guggenheim Memorial Foundation, which did the same throughout the year 1961–1962.



**Differential Algebra  
and Algebraic Groups**

## Algebraic Preliminaries

In this chapter, we describe the conventions that are in force throughout this book, and develop various algebraic notions for use in subsequent chapters. Most of these notions, and the results concerning them, are well known; they are included for the convenience of the reader and to set the terminology and notation, and in only a few cases is there some novelty in the development. A few of these notions and results, while known “in principle,” do not seem to be available in the form used here.

The reader is urged not to try to read this chapter as a whole, but rather to read appropriate parts of it when necessary for the later chapters. For almost all of Chapter I, Sections 1 and 4 of the present chapter will suffice; for most of Chapter II, only Sections 2 and 3 need be added, and near the end, Section 17. For Chapter III, the reader should be familiar with Sections 1–12 and 14. Of the remaining parts, Sections 18 and 19 are not used until Part B of Chapter IV, and Sections 13, 15, 16 play a serious role in only a few places in Chapter V.

### 1 Conventions

The term *ring* is used exclusively, and without further notice, for *commutative ring with unity element*. In particular, every field is commutative, every integral domain has a unity element different from 0, and a prime ideal of a ring is always different from the ring itself. Correspondingly, every ring homomorphism is unitary (maps unity onto unity), every subring of a

ring is unitary (contains the unity of the ring), every module or algebra over a ring is unitary (multiplication by the unity of the ring is the identity mapping of the module or algebra), and every algebra has a unity element. It is left to the reader to determine, if he or she wishes, which results extend to the noncommutative or nonunitary cases.

A mapping  $f$  of a set  $A$  into a set  $A'$  is *injective* if  $f(x) \neq f(y)$  whenever  $x$  and  $y$  are distinct elements of  $A$ , and is *surjective* if the image  $f(A)$  is  $A'$ ;  $f$  is *bijective* if it is both injective and surjective.

If  $R$  and  $R'$  are rings, we permit ourselves, when there is no danger of confusion, to denote a family of indeterminates over  $R$  and a family of indeterminates over  $R'$  by the same symbol, for example  $(X_i)_{i \in I}$  or  $X$ . If  $f: R \rightarrow R'$  is a mapping such that  $f(0) = 0$ , then  $f$  extends in a canonical way to a mapping  $R[X] \rightarrow R'[X]$  between the polynomial algebras, the image of a polynomial  $P$  in  $R[X]$  being the polynomial in  $R'[X]$  obtained by applying  $f$  to each coefficient in  $P$ ; we denote this image by  $P^f$ , and for any subset  $\Sigma$  of  $R[X]$  we let  $\Sigma^f$  denote the set of all polynomials  $P^f$  with  $P \in \Sigma$ . When  $f$  is injective (or surjective), then so is its canonical extension  $R[X] \rightarrow R'[X]$ .

We use the following notation of Bourbaki:  $\mathbf{N}$  is the set of natural numbers (including 0);  $\mathbf{Z}$  is the ring of rational integers;  $\mathbf{Q}$  is the field of rational numbers;  $\mathbf{R}$  is the field of real numbers;  $\mathbf{C}$  is the field of complex numbers;  $\mathbf{F}_q$  is the finite field of  $q$  elements ( $q$  being a power of a prime).

If  $K$  is a field, then  $K_a$  denotes the (or an) algebraic closure of  $K$ ,  $K_s$  denotes the separable closure of  $K$  (that is, the set of all elements of  $K_a$  that are separably algebraic over  $K$ ), and  $K_i$  denotes the purely inseparable closure of  $K$  (that is, denotes  $K$  when the characteristic of  $K$  is 0 and denotes  $K^{p^\infty}$  when the characteristic of  $K$  is  $p \neq 0$ ).

If  $R$  is a ring and  $\mathfrak{f}$  is an ideal of  $R$  and  $\Sigma$  is a subset of  $R$ , then  $\mathfrak{f}:\Sigma$  denotes the set of all elements  $x \in R$  such that  $xs \in \mathfrak{f}$  for every  $s \in \Sigma$ ;  $\mathfrak{f}:\Sigma$  is an ideal of  $R$ . When  $\Sigma$  consists of a single element  $s$ , we write  $\mathfrak{f}:s$  for  $\mathfrak{f}:\Sigma$ . The union  $\bigcup_{n \in \mathbf{N}} \mathfrak{f}:s^n$  is denoted by  $\mathfrak{f}:s^\infty$ ; it is an ideal of  $R$ .

## 2 Separable dependence

Let  $K$  be a subfield of a field  $L$  of arbitrary characteristic  $p$ . A family  $(x_i)_{i \in I}$  of elements of  $L$  is *separably dependent* over  $K$  if there exists a polynomial  $f \in K[(X_i)_{i \in I}]$  vanishing at  $(x_i)_{i \in I}$  such that at least one of the partial derivatives  $\partial f / \partial X_i$  does not vanish there, and the family is *separably independent* over  $K$  in the contrary case. To say that  $(x_i)_{i \in I}$  is separably dependent over  $K$  is the same as to say that, for some  $j \in I$ ,  $x_j$  is separably algebraic over  $K((x_i)_{i \in J})$ ,  $J$  denoting the set of elements of  $I$  different from  $j$ . When  $p = 0$ , then separable dependence is the same as algebraic dependence.

It is apparent that if  $(x_1, \dots, x_n)$  is separably dependent over  $K$  and  $x'_j = \sum_{1 \leq i \leq n} c_{ij} x_i$  ( $1 \leq j \leq n$ ), where  $(c_{ij})$  is an invertible matrix over  $K$ , then  $(x'_1, \dots, x'_n)$  is separably dependent over  $K$ .

**Lemma 1** Let  $u_1, \dots, u_r, v_1, \dots, v_s$  be elements of a field extension of  $K$ , and suppose that  $r < s$  and that each  $v_i$  is separably algebraic over  $K(u_1, \dots, u_r)$ . Then  $(v_1, \dots, v_s)$  is separably dependent over  $K$ .

*Proof* We may suppose that  $p \neq 0$ . First let  $r = 1$ , and denote by  $n_j$  the degree of  $v_j$  over  $K(u_1)$ . For each  $j$  there exists a polynomial  $f_j \in K[X_1, Y_j]$  such that  $\deg_{Y_j} f_j = n_j$ ,  $f_j(u_1, v_j) = 0$ , and  $(\partial f_j / \partial Y_j)(u_1, v_j) \neq 0$ . We may suppose that either  $u_1$  is transcendental over  $K$  or else  $u_1$  is algebraic over  $K$  of some degree  $m$  and  $\deg_{X_1} f_j < m$  and the coefficient of  $Y_j^{n_j}$  in  $f_j$  as a polynomial in  $Y_j$  is 1. We may suppose, too, that no  $v_j$  is separably algebraic over  $K$ . Let  $v$  be the biggest natural number such that  $f_j \in K[X_1^v, Y_j]$  for every  $j$ , let  $\varphi_j$  be the polynomial in  $K[X_1, Y_j]$  defined by  $\varphi_j(X_1^v, Y_j) = f_j(X_1, Y_j)$ , and let  $t = u_1^v$ . For some  $j$  then  $\varphi_j \notin K[X_1^v, Y_j]$ ; suppose this happens for  $j = 1$ , so that  $\partial \varphi_1 / \partial X_1 \neq 0$ . Either  $t = u_1^v$  is transcendental over  $K$ , or  $u_1$  is of degree  $m$  over  $K$  and  $\deg_{X_1}(\partial \varphi_1 / \partial X_1)(X_1^v, Y_1) < m$ ; in either case  $(\partial \varphi_1 / \partial X_1)(t, Y_1) \neq 0$ . In the former case  $(\partial \varphi_1 / \partial X_1)(t, Y_1)$  fails to be divisible by  $\varphi_1(t, Y_1)$  in  $K[t, Y_1]$  and therefore also in  $K(t)[Y_1]$ ; in the latter case the coefficient of  $Y_1^{n_1}$  in  $\varphi_1$  is 1 so that  $\deg_{Y_1} \partial \varphi_1 / \partial X_1 < n_1$ , and again  $(\partial \varphi_1 / \partial X_1)(t, Y_1)$  fails to be divisible by  $\varphi_1(t, Y_1)$  in  $K(t)[Y_1]$ . Hence  $(\partial \varphi_1 / \partial X_1)(t, v_1) \neq 0$ , so that  $t$  is separably algebraic over  $K(v_1)$ . As  $v_2$  is separably algebraic over  $K(t)$ , and therefore over  $K(t, v_1)$ , it follows that  $v_2$  is separably algebraic over  $K(v_1)$ , so that  $(v_1, \dots, v_s)$  is separably dependent over  $K$ .

Now let  $r > 1$  and suppose the lemma proved for lower values of  $r$ . Then  $(v_1, \dots, v_s)$  is separably dependent over  $K(u_1)$  so that, say,  $v_s$  is separably algebraic over  $K(u_1, v_1, \dots, v_{s-1})$ ; also,  $(v_1, \dots, v_{s-1})$  is separably dependent over  $K(u_1)$  so that, say,  $v_{s-1}$  is separably algebraic over  $K(u_1, v_1, \dots, v_{s-2})$ . Therefore  $v_{s-1}$  and  $v_s$  are both separably algebraic over  $K(v_1, \dots, v_{s-2})(u_1)$ , so that  $(v_{s-1}, v_s)$  is separably dependent over  $K(v_1, \dots, v_{s-2})$ , whence  $(v_1, \dots, v_s)$  is separably dependent over  $K$ .

It is easy to see that for a subset  $B$  of  $L$  the following two conditions are equivalent:

- (i)  $B$  is a minimal element of the set of all subsets  $\Sigma$  of  $L$  such that  $L$  is separably algebraic over  $K(\Sigma)$ ;
- (ii)  $B$  is separably independent over  $K$  and  $L$  is separably algebraic over  $K(B)$ .

We shall call a subset  $B$  of  $L$  having these properties an *inseparability basis* of  $L$  over  $K$ . It is immediate from Lemma 1 that if there exists a finite inseparability basis of  $L$  over  $K$ , then all inseparability bases of  $L$  over  $K$  are finite with the same cardinal number. We shall say in this case that  $L$  has *finite inseparability degree* over  $K$  and shall call this cardinal number the *inseparability degree* of  $L$  over  $K$ .

Every finitely generated field extension has finite inseparability degree.

Every family of elements of  $L$  that is separably dependent over  $K$  is algebraically dependent over  $K$ , and, if  $L$  is separable over  $K$ , conversely. It is not difficult to see that this is actually a criterion for separability, that is: *a necessary and sufficient condition that  $L$  be separable over  $K$  is that every family of elements of  $L$  that is algebraically dependent over  $K$  be separably dependent over  $K$* . In particular, for finitely generated separable field extensions the inseparability degree coincides with the transcendence degree.

### EXERCISES

- Let  $M \supset L \supset K$  be a tower of finitely generated field extensions. Prove that the inseparability degree of  $M$  over  $K$  is less than or equal to the sum of the inseparability degrees of  $L$  over  $K$  and  $M$  over  $L$ . Give an example in which the inequality is strict.
- Prove the above criterion for separability (*Hints*: (a) A field extension is separable if and only if every finitely generated subextension is. (b) A finitely generated extension is separable if and only if it has a separating transcendence basis.)
- Let  $L$  be a finitely generated field extension of a field  $K$ . Show that if  $L$  is separable over  $K$ , then every inseparability basis of  $L$  over  $K$  is a separating transcendence basis of  $L/K$ . Derive from this the criterion that  $L$  is separable over  $K$  if and only if the inseparability degree and the transcendence degree of  $L$  over  $K$  are equal.

### 3 Quasi-separable field extensions

We are going to introduce a condition on field extensions that is weaker than that of separability. To this end we observe, for a family of elements  $(x_i)_{i \in I}$  of  $L$ , that if some subset  $J$  of  $I$  for which  $(x_i)_{i \in J}$  is a transcendence basis of  $K((x_i)_{i \in I})$  over  $K$  has the property that  $I - J$  is finite, then every such  $J$  has this property, and the cardinal number  $r$  of  $I - J$  is independent of  $J$ . We say, in this case, that the family  $(x_i)_{i \in I}$  has *finite algebraic codimension* over  $K$ , and that  $r$  is its *algebraic codimension* over  $K$ .

With this terminology the criterion for separability given in Section 2

can be stated as follows:  $L$  is separable over  $K$  if and only if every family of elements of  $L$  that is separably independent over  $K$  has algebraic codimension 0 over  $K$ . We now define  $L$  as *quasi-separable* over  $K$  if every family of elements of  $L$  that is separably independent over  $K$  has finite algebraic codimension over  $K$ .

Every separable field extension is quasi-separable; but so is every finitely generated field extension, since by Lemma 1 in such an extension a separably independent family must be finite.

It is natural to call a field *quasi-perfect* if every field extension of it is quasi-separable. The following two technical lemmas lead to an internal characterization of quasi-perfect fields, and are used in an analogous situation in Chapter II.

**Lemma 2** *Let  $a_1, \dots, a_n$  be elements of a field  $K$  of characteristic  $p \neq 0$ . In the polynomial algebra  $K[X_1, \dots, X_n]$  the ideal  $(X_1^p - a_1, \dots, X_n^p - a_n)$  is prime if and only if  $a_j \notin K^p(a_1, \dots, a_{j-1})$  ( $1 \leq j \leq n$ ).*

*Proof*  $K$  is isomorphic to  $K^p$ , and therefore the ideal in question is prime if and only if in the ring  $K^p[X_1, \dots, X_n]$  the ideal  $\mathfrak{a} = (X_1^p - a_1^p, \dots, X_n^p - a_n^p)$  is prime. The substitution mapping  $f(X_1, \dots, X_n) \mapsto f(a_1, \dots, a_n)$  is a  $K^p$ -homomorphism of  $K^p[X_1, \dots, X_n]$  onto  $K^p[a_1, \dots, a_n] = K^p(a_1, \dots, a_n)$  with prime kernel, say  $\mathfrak{p}$ , and obviously  $\mathfrak{a} \subset \mathfrak{p}$ . If  $f \in \mathfrak{p}$ , then  $f$  is in the ideal  $(X_1 - a_1, \dots, X_n - a_n)$  of  $K[X_1, \dots, X_n]$ , so that  $f^p \in \mathfrak{a}$ . Therefore  $\mathfrak{a}$  is prime if and only if  $\mathfrak{a} = \mathfrak{p}$ , which happens if and only if  $K^p[X_1, \dots, X_n]/\mathfrak{a}$  has, as a vector space over  $K^p$ , the same dimension as  $K^p[X_1, \dots, X_n]/\mathfrak{p} \approx K^p(a_1, \dots, a_n)$ . Now,  $\mathfrak{a}$  is contained in the ideal  $((X_1 - a_1)^p, \dots, (X_n - a_n)^p)$  of  $K[X_1, \dots, X_n]$  and therefore cannot contain a nonzero polynomial of degree less than  $p$  in each  $X_j$ . Hence the dimension of  $K^p[X_1, \dots, X_n]/\mathfrak{a}$  is  $p^n$ . However  $[K^p(a_1, \dots, a_n):K^p] = \prod_{1 \leq j \leq n} [K^p(a_1, \dots, a_j):K^p(a_1, \dots, a_{j-1})]$ , and this equals  $p^n$  if and only if  $a_j \notin K^p(a_1, \dots, a_{j-1})$  ( $1 \leq j \leq n$ ).

**Lemma 3** *Let  $E, K, L$  be fields of characteristic  $p \neq 0$  with  $K^p \subset E \subset K \subset L$  and  $[E:K^p] < \infty$  such that  $L^p E$  and  $K$  are linearly disjoint over  $E$ ; let  $(x_i)_{i \in I}$  be a family of elements of  $L$  that is separably independent over  $K$ . Then  $(x_i)_{i \in I}$  has finite algebraic codimension over  $K$ .*

*Proof* Assume the contrary. Then there is a subset  $J$  of  $I$  for which  $(x_j)_{j \in J}$  is algebraically independent over  $K$ , and an infinite sequence  $(i_n)_{n \in \mathbb{N}}$  of distinct elements of  $I - J$ , such that  $x_{i_n}$  is algebraic over  $K((x_j)_{j \in J}, x_{i_0}, \dots, x_{i_{n-1}})$  of degree, say  $d_n$  ( $n \in \mathbb{N}$ ). There does not exist a nonzero polynomial in  $K[(X_j)_{j \in J}, X_{i_0}, \dots, X_{i_n}]$  vanishing at  $((x_j)_{j \in J}, x_{i_0}, \dots, x_{i_n})$  with the property that its degree in  $X_{i_v}$  is less than  $d_v$  ( $0 \leq v \leq n$ ), but there does exist such a polynomial with the property that its degree in  $X_{i_n}$  equals  $d_n$  and its degree



in  $X_{i_v}$  is less than  $d_v$  ( $0 \leq v < n$ ). Of these polynomials, let  $f_n$  denote one of minimal degree. Because  $(x_i)_{i \in I}$  is separably independent over  $K$ , for each  $i \in I$  the partial derivative  $\partial f_n / \partial X_i$  vanishes at  $((x_j)_{j \in J}, x_{i_0}, \dots, x_n)$ , and because of the minimality of the degree of  $f_n$  this implies that  $\partial f_n / \partial X_i = 0$ ; therefore  $f_n \in K[(X_j)_{j \in J}, X_{i_0}^p, \dots, X_{i_n}^p]$ . Because  $L^p E$  and  $K$  are linearly disjoint over  $E$ , this shows that we may suppose that the coefficients in  $f_n$  are all in  $E$ . Setting  $m = [E:K^p]$ , we know that there exists a basis  $(e_1, \dots, e_m)$  of  $E$  over  $K^p$ . Therefore we may write  $f_n = e_1 f_{1n}^p + \dots + e_m f_{mn}^p$ , where  $f_{\mu n} \in K[(X_j)_{j \in J}, X_{i_0}, \dots, X_{i_n}]$  and the degree of  $f_{\mu n}$  in  $X_{i_v}$  is less than or equal to  $d_v/p$  ( $1 \leq \mu \leq m, 0 \leq v \leq n$ ). Since  $\sum_{1 \leq \mu \leq m} e_\mu f_{\mu n}^p$  vanishes at  $((x_j)_{j \in J}, x_{i_0}, \dots, x_n)$ , or as an element of  $E[(X_i)_{i \in I}]$  vanishes at  $(x_i)_{i \in I}$ , we see that the matrix  $(f_{\mu n}((x_i)_{i \in I})^p)_{1 \leq \mu \leq m, 0 \leq n < \infty}$  has a rank  $r < m$ , and obviously  $r$  is also the rank of the matrix  $(f_{\mu n}((x_i)_{i \in I}))_{1 \leq \mu \leq m, 0 \leq n < \infty}$ . Therefore there exist  $r$  distinct natural numbers  $n(1), \dots, n(r)$  such that the  $r$  rows

$$(f_{1, n(k)}((x_i)_{i \in I}), \dots, f_{m, n(k)}((x_i)_{i \in I})), \quad 1 \leq k \leq r,$$

are linearly independent, and for every  $n \in \mathbb{N}$  the row  $(f_{1, n}((x_i)_{i \in I}), \dots, f_{m, n}((x_i)_{i \in I}))$  is a linear combination of these  $r$  rows. Fixing  $n$  bigger than each  $n(k)$  we may therefore write

$$f_{\mu, n}((x_i)_{i \in I}) = \sum_{1 \leq k \leq r} h((x_i)_{i \in I})^{-1} g_k((x_i)_{i \in I}) f_{\mu, n(k)}((x_i)_{i \in I}) \quad (1 \leq \mu \leq m),$$

where  $h \in K[(X_j)_{j \in J}]$ ,  $g_k \in K[(X_j)_{j \in J}, X_{i_0}, \dots, X_{i_n}]$ , and the degree of  $g_k$  in  $X_{i_v}$  is less than  $d_v$  ( $0 \leq v \leq n$ ). Thus  $h f_{\mu n} - \sum_{1 \leq k \leq r} g_k f_{\mu, n(k)}$  is a polynomial in  $K[(X_j)_{j \in J}, X_{i_0}, \dots, X_{i_n}]$  that vanishes at  $((x_j)_{j \in J}, x_{i_0}, \dots, x_n)$  and that has degree less than  $d_n$  in  $X_{i_n}$ . It follows that it has the property that if we regard it as a polynomial in  $X_{i_n}$ , then its coefficients, which are elements of  $K[(X_j)_{j \in J}, X_{i_0}, \dots, X_{i_{n-1}}]$ , all vanish at  $((x_j)_{j \in J}, x_{i_0}, \dots, x_{i_{n-1}})$ . The same must be true for the polynomial  $h^p f_{\mu n}^p - \sum_{1 \leq k \leq r} g_k^p f_{\mu, n(k)}^p$ , and therefore for the polynomial

$$\sum_{1 \leq \mu \leq m} e_\mu \left( h^p f_{\mu n}^p - \sum_{1 \leq k \leq r} g_k^p f_{\mu, n(k)}^p \right) = h^p f_n - \sum g_k^p f_{n(k)}.$$

Since  $f_{n(k)}$  is free of  $X_{i_n}$  and vanishes at  $((x_j)_{j \in J}, x_{i_0}, \dots, x_{i_{n(k)}})$  ( $1 \leq k \leq r$ ), we see that  $h^p f_n$  has this property too. However, each of its coefficients is in  $K[(X_j)_{j \in J}, X_{i_0}, \dots, X_{i_{n-1}}]$ , and in  $X_{i_v}$  it is of degree less than  $d_v$  ( $0 \leq v < n$ ). This contradiction completes the proof.

**Corollary** *A field  $K$  of characteristic  $p \neq 0$  is quasi-perfect if and only if  $[K:K^p] < \infty$ .*

*Proof* If the condition is satisfied and  $L$  is any field extension of  $K$ , then, by Lemma 3 with  $E = K$ ,  $L$  is quasi-separable over  $K$ ; thus,  $K$  is

quasi-perfect. Suppose the condition is not satisfied. Then there exists an infinite sequence  $a_0, a_1, \dots, a_n, \dots$  of elements of  $K$  such that  $a_n \notin K^p$  ( $a_0, \dots, a_{n-1}$ ). It is an easy consequence of Lemma 2 that the ideal  $(X_0^p - a_0, \dots, X_n^p - a_n, \dots)$  of the polynomial algebra  $K[X_0, \dots, X_n, \dots]$  is prime. Therefore if  $\alpha_0, \dots, \alpha_n, \dots$  are the respective  $p$ th roots of  $a_0, \dots, a_n, \dots$  in a field extension of  $K$ , then  $(\alpha_n)_{n \in \mathbb{N}}$  is separably independent over  $K$  but not of finite algebraic codimension. Thus  $K((\alpha_n)_{n \in \mathbb{N}})$  is not quasi-separable over  $K$ , so that  $K$  is not quasi-perfect.

#### 4 Quotients

Let  $R$  be a ring. If  $\Sigma$  is any multiplicatively stable subset of  $R$ , then  $1 \in \Sigma$ , and we can form in the usual way the ring of quotients of  $R$  over  $\Sigma$ ; this ring, often denoted by  $\Sigma^{-1}R$ , consists of the quotients (or fractions)  $a/s$  with  $a \in R$  and  $s \in \Sigma$ , two such fractions  $a_1/s_1$  and  $a_2/s_2$  being equal when there exists an  $s \in \Sigma$  such that  $a_1 s_2 s = a_2 s_1 s$ . The mapping  $\varphi: R \rightarrow \Sigma^{-1}R$  given by the formula  $\varphi(a) = a/1$  is a homomorphism (called "canonical") of  $R$  into  $\Sigma^{-1}R$  with kernel consisting of all  $a \in R$  such that  $as = 0$  for some  $s \in \Sigma$ .

An ideal  $\mathfrak{f}$  of  $R$  is  $\Sigma$ -prime if  $\mathfrak{f}:s = \mathfrak{f}$  for every  $s \in \Sigma$ . For any ideal  $\mathfrak{f}$  of  $R$ ,  $\bigcup_{s \in \Sigma} \mathfrak{f}:s$  is the smallest  $\Sigma$ -prime ideal of  $R$  that contains  $\mathfrak{f}$ . It is easy to see that the formula  $\mathfrak{f} \mapsto \Sigma^{-1}R \cdot \varphi(\mathfrak{f})$  defines a bijection of the set of  $\Sigma$ -prime ideals of  $R$  onto the set of all ideals of  $\Sigma^{-1}R$ , the inverse of this bijection being given by the formula  $\mathfrak{f}' \mapsto \varphi^{-1}(\mathfrak{f}')$ . We usually denote the ideal  $\Sigma^{-1}R \cdot \varphi(\mathfrak{f})$  by  $\Sigma^{-1}\mathfrak{f}$ .

The canonical homomorphism  $\varphi: R \rightarrow \Sigma^{-1}R$  is injective if and only if  $\Sigma$  contains no divisor of 0. When such is the case,  $\varphi$  is generally used to identify  $R$  with a subring of  $\Sigma^{-1}R$ . A special case in which this happens is that in which  $\Sigma$  is the set of all nondivisors of 0 in  $R$ ; in this case  $\Sigma^{-1}R$  is called the *complete ring of quotients* of  $R$  and is denoted by  $Q(R)$ . When  $R$  is an integral domain, then  $Q(R)$  is the field of quotients of  $R$ .

Another case that has its own terminology is that in which  $\Sigma = R - \mathfrak{p}$ , where  $\mathfrak{p}$  is a prime ideal in  $R$ ; in this case  $\Sigma^{-1}R$  is called the *localization of  $R$  at  $\mathfrak{p}$*  and is denoted by  $R_{\mathfrak{p}}$ . In  $R_{\mathfrak{p}}$  there is a unique maximal ideal, namely  $R_{\mathfrak{p}}\mathfrak{p}$ , so that  $R_{\mathfrak{p}}$  is a local ring.

#### 5 Perfect ideals

An ideal  $\mathfrak{f}$  of a ring  $R$  is said to be *perfect* if  $\mathfrak{f}$  contains an element  $x \in R$  whenever  $x^n \in \mathfrak{f}$  for some  $n \in \mathbb{N}$ ; in other words,  $\mathfrak{f}$  is perfect if the residue ring  $R/\mathfrak{f}$  has no nonzero nilpotent element. A prime ideal is always perfect.

If  $x^n \in \mathfrak{f}$ , then  $x^{2^v} \in \mathfrak{f}$  for some  $v \in \mathbb{N}$ ; it follows that to show that  $\mathfrak{f}$  is perfect it suffices to verify that  $x^2 \in \mathfrak{f} \Rightarrow x \in \mathfrak{f}$ .

Let  $\mathfrak{f}$  be a perfect ideal of  $R$ , and consider the ideal  $R[X]\mathfrak{f}$  generated by  $\mathfrak{f}$  in the polynomial algebra over  $R$  in a single indeterminate  $X$ . If  $f = \sum a_i X^i$  is not in  $R[X]\mathfrak{f}$ , then there is a smallest  $h \in \mathbb{N}$  such that  $a_h \notin \mathfrak{f}$ ; the coefficient of  $X^{2h}$  in  $f^2$  is  $\sum_{i+j=2h} a_i a_j \equiv a_h^2 \not\equiv 0 \pmod{\mathfrak{f}}$ , so that  $f^2 \notin R[X]\mathfrak{f}$ . Thus,  $R[X]\mathfrak{f}$  is a perfect ideal of  $R[X]$ . An induction argument yields the same result for any finitely generated polynomial algebra  $R[X_1, \dots, X_n]$ . It is now easy to see that if  $S = R[(X_i)_{i \in I}]$  is any polynomial algebra over  $R$  and  $\mathfrak{f}$  is a perfect ideal of  $R$ , then  $S\mathfrak{f}$  is a perfect ideal of  $S$ .

- Lemma 4** (a) <sup>1</sup>The intersection of any set of perfect ideals of  $R$  is perfect.  
 (b) The union of any nonempty set, totally ordered by inclusion, of perfect ideals of  $R$  is perfect.  
 (c) If  $\mathfrak{f}$  is a perfect ideal of  $R$  and  $s \in R$ , then  $\mathfrak{f}:s$  is perfect.

The proof is routine.

It follows that if  $\Sigma$  is a subset of  $R$ , then the intersection of all the perfect ideals of  $R$  containing  $\Sigma$  is the smallest perfect ideal of  $R$  containing  $\Sigma$ . We call it the *perfect ideal of  $R$  generated by  $\Sigma$* . It consists, as is easy to see, of all elements  $x \in R$  such that  $x^n$  is in the ideal  $(\Sigma)$  of  $R$  for some  $n \in \mathbb{N}$ .

## 6 Separable, quasi-separable, and regular ideals

Let  $R_0$  be a subring of  $R$ . If  $R$  is an integral domain, it is natural to call  $R$  *separable* (respectively *quasi-separable*, respectively *regular*) over  $R_0$  if  $Q(R)$  is a separable (respectively quasi-separable, respectively regular) field extension of  $Q(R_0)$ . (We recall that a field extension  $L$  of a field  $K$  is called regular if  $L$  is separable over  $K$  and  $K$  is algebraically closed in  $L$ .) For our purposes it is useful to extend the notion "separable" to a more general situation in the following way. No longer assuming that  $R$  is an integral domain, we define  $R$  to be *separable* over  $R_0$  either if  $R$  is the zero ring, or else if  $R$  is not the zero ring and the following three conditions are satisfied.

- S1** The ring  $R$  has no nonzero nilpotent element.  
**S2** Whenever  $a_0 \in R_0$ ,  $a_0 \neq 0$ ,  $b \in R$ ,  $b \neq 0$ , then  $a_0 b \neq 0$  (so that, in particular,  $R_0$  is an integral domain).  
**S3** Either the characteristic  $p$  of  $R_0$  is 0, or else  $p \neq 0$  and  $R^p$  and  $R_0$  are linearly disjoint over  $R_0^p$ .

(*Attention:* This definition is not equivalent to one commonly used<sup>1</sup> even in the cases in which both are applicable. For example, any algebra over a field  $K$  of characteristic 0 is separable over  $K$  in our sense if it is an integral domain, but if it is also a local ring, then its radical coincides with its maximal ideal which in general is not (0).)

It is easy to see that if  $R_0, R_1, R_2$  are rings with  $R_0 \subset R_1 \subset R_2$ ,  $R_1$  separable over  $R_0$ , and  $R_2$  separable over  $R_1$ , then  $R_2$  is separable over  $R_0$ .

Consider an ideal  $\mathfrak{f}$  of  $R$ , and the canonical homomorphism  $f: R \rightarrow R/\mathfrak{f}$ . We define the ideal  $\mathfrak{f}$  to be *separable* (respectively *quasi-separable*, respectively *regular*) over  $R_0$  if  $f(R)$  is separable (respectively quasi-separable, respectively regular) over  $f(R_0)$ , it being understood in the quasi-separable and regular cases that  $\mathfrak{f}$  is prime so that  $f(R)$  is an integral domain. Every ideal that is separable over  $R_0$  is perfect (see condition S1 above). We frequently say " $R_0$ -separable" instead of "separable over  $R_0$ ," and " $R_0$ -regular" instead of "regular over  $R_0$ ."

It is easy to see that if  $R_0, R_1, R_2$  are rings with  $R_0 \subset R_1 \subset R_2$ , and  $\mathfrak{f}$  is an  $R_1$ -separable ideal of  $R_2$  such that  $\mathfrak{f} \cap R_1$  is an  $R_0$ -separable ideal of  $R_1$ , then  $\mathfrak{f}$  is an  $R_0$ -separable ideal of  $R_2$ .

We remark that if  $g: R \rightarrow R'$  is a ring homomorphism with kernel contained in  $\mathfrak{f}$ , then  $\mathfrak{f}$  is separable (respectively quasi-separable, respectively regular) over  $R_0$  if and only if  $g(\mathfrak{f})$  is separable (respectively quasi-separable, respectively regular) over  $g(R_0)$ . This is a consequence of the fact that if  $f'$  denotes the canonical homomorphism  $g(R) \rightarrow g(R)/g(\mathfrak{f})$ , then  $g$  induces an isomorphism  $f(R) \approx f'(g(R))$  mapping  $f(R_0)$  onto  $f'(g(R_0))$ .

**Lemma 5** (a) The intersection of any set of  $R_0$ -separable ideals of  $R$ , all of which have the same intersection with  $R_0$ , is  $R_0$ -separable.

(b) The union of any nonempty set, totally ordered by inclusion, of  $R_0$ -separable ideals of  $R$ , all of which have the same intersection with  $R_0$ , is  $R_0$ -separable.

(c) If  $\mathfrak{f}$  is an  $R_0$ -separable ideal of  $R$  and  $s \in R$ , then  $\mathfrak{f}:s$  is  $R_0$ -separable, and  $(\mathfrak{f}:s) \cap R_0 = \mathfrak{f} \cap R_0$  provided  $\mathfrak{f}:s \neq R$ .

*Proof* (a) Let  $I = \bigcap \mathfrak{f}$ , with all the  $\mathfrak{f}$   $R_0$ -separable and intersecting  $R_0$  in  $\mathfrak{h}_0$ , so that  $I \cap R_0 = \mathfrak{h}_0$ . We may suppose that  $\mathfrak{h}_0 \neq R_0$ . By Lemma 4(a),  $R/I$  has no nonzero nilpotent element. If  $a_0 \in R_0$ ,  $a_0 \notin I$ ,  $b \in R$ ,  $b \notin I$ , then (for some  $\mathfrak{f}$ )  $b \notin \mathfrak{f}$ , and  $a_0 \notin \mathfrak{h}_0 = \mathfrak{f} \cap R_0$ , whence  $a_0 \notin \mathfrak{f}$ , so that (because  $\mathfrak{f}$  is  $R_0$ -separable)  $a_0 b \notin \mathfrak{f}$  whence  $a_0 b \notin I$ . Finally, supposing that  $R_0/\mathfrak{h}_0$  has characteristic  $p \neq 0$ , let  $(c_i)$  be a family of elements of  $R_0$  linearly independent over  $R_0^p \pmod{I}$ ; since  $I \cap R_0 = \mathfrak{f} \cap R_0$  for every  $\mathfrak{f}$ ,  $(c_i)$  is also linearly independent over  $R_0^p \pmod{\mathfrak{f}}$ . If  $\sum \alpha_i^p c_i \equiv 0 \pmod{I}$ , where each  $\alpha_i \in R$ ,

<sup>1</sup> See, e.g., N. Bourbaki, "Algèbre," Chap. 8, §7. Hermann, Paris, 1958.

then  $\sum \alpha_i^p c_i \equiv 0 \pmod{\mathfrak{f}}$  for every  $\mathfrak{f}$ . Because each  $\mathfrak{f}$  is  $R_0$ -separable, this implies that each  $\alpha_i \equiv 0 \pmod{\mathfrak{f}}$  for every  $\mathfrak{f}$ ; that is, each  $\alpha_i \equiv 0 \pmod{I}$ . Thus,  $(c_i)$  is linearly independent over  $R^p \pmod{I}$ . This shows that  $I$  is  $R_0$ -separable.

(b) Let  $I = \bigcup \mathfrak{f}$  be the union of a totally ordered set of  $R_0$ -separable ideals all having intersection  $\mathfrak{h}_0$  with  $R_0$ . We suppose that  $\mathfrak{h}_0 \neq R_0$ . By Lemma 4(b),  $R/I$  has no nonzero nilpotent element. If  $a_0 \in R_0$ ,  $a_0 \notin I$ ,  $b \in R$ ,  $b \notin I$ , then (for every  $\mathfrak{f}$ )  $a_0 \notin \mathfrak{f}$ ,  $b \notin \mathfrak{f}$  so that  $a_0 b \notin \mathfrak{f}$ , whence  $a_0 b \notin I$ . Supposing that  $R_0/\mathfrak{h}_0$  has characteristic  $p \neq 0$ , let  $(c_i)$  be a family of elements of  $R_0$  linearly independent over  $R_0^p \pmod{I}$ . Since  $I \cap R_0 = \mathfrak{f} \cap R_0$  for every  $\mathfrak{f}$ ,  $(c_i)$  is also linearly independent over  $R_0^p \pmod{\mathfrak{f}}$ ; if  $\sum \alpha_i^p c_i \equiv 0 \pmod{I}$ , where each  $\alpha_i \in R$ , then  $\sum \alpha_i^p c_i \equiv 0 \pmod{\mathfrak{f}}$  for some  $\mathfrak{f}$ , so that each  $\alpha_i \equiv 0 \pmod{\mathfrak{f}}$  for this  $\mathfrak{f}$ , and therefore each  $\alpha_i \equiv 0 \pmod{I}$ . Thus,  $(c_i)$  is linearly independent over  $R^p \pmod{I}$ . This shows that  $I$  is  $R_0$ -separable.

(c) We may suppose that  $\mathfrak{f}:s \neq R$ . By Lemma 4(c),  $R/(\mathfrak{f}:s)$  has no nonzero nilpotent element. If  $a_0 \in R_0$ ,  $a_0 \notin \mathfrak{f}$ ,  $b \in R$ ,  $b \notin \mathfrak{f}:s$ , then  $s \notin \mathfrak{f}$  so that (because  $\mathfrak{f}$  is  $R_0$ -separable)  $a_0 s \notin \mathfrak{f}$ , that is  $a_0 \notin \mathfrak{f}:s$ . It follows on the one hand that  $(\mathfrak{f}:s) \cap R_0 = \mathfrak{f} \cap R_0$ , and on the other hand that  $a_0 b s \notin \mathfrak{f}$ , that is,  $a_0 b \notin \mathfrak{f}:s$ . Supposing that  $R_0/(\mathfrak{f} \cap R_0)$  has characteristic  $p \neq 0$ , let  $(c_i)$  be a family of elements of  $R_0$  linearly independent over  $R_0^p \pmod{\mathfrak{f}:s}$ , that is, since  $(\mathfrak{f}:s) \cap R_0 = \mathfrak{f} \cap R_0$ , linearly independent over  $R_0^p \pmod{\mathfrak{f}}$ ; since  $\mathfrak{f}$  is  $R_0$ -separable,  $(c_i)$  is linearly independent over  $R^p \pmod{\mathfrak{f}}$ . If  $\sum \alpha_i^p c_i \equiv 0 \pmod{\mathfrak{f}:s}$ , where each  $\alpha_i \in R$ , then  $\sum (s\alpha_i)^p c_i \equiv 0 \pmod{\mathfrak{f}}$ , each  $s\alpha_i \equiv 0 \pmod{\mathfrak{f}}$ , whence each  $\alpha_i \equiv 0 \pmod{\mathfrak{f}:s}$ . Therefore  $(c_i)$  is linearly independent over  $R^p \pmod{\mathfrak{f}:s}$ . This shows that  $\mathfrak{f}:s$  is  $R_0$ -separable.

## 7 Conservative systems

Let  $M$  be a module over a ring  $R$ . A set  $\mathfrak{C}$  of submodules of  $M$  will be called a *conservative system* of  $M$  if the following two conditions are satisfied.

**CS1** *The intersection of any set of elements of  $\mathfrak{C}$  is an element of  $\mathfrak{C}$ .*

**CS2** *The union of any nonempty set, totally ordered by inclusion, of elements of  $\mathfrak{C}$  is an element of  $\mathfrak{C}$ .*

We shall be interested primarily in the case in which  $M = R$ ; in this case the elements of  $\mathfrak{C}$  are ideals of  $R$ , which we call  *$\mathfrak{C}$ -ideals*.

By CS1, applied to the empty set of submodules of  $M$ ,  $M$  itself is an element of every conservative system of  $M$ . The set of all submodules of  $M$  is a conservative system of  $M$ ; so is, at the other extreme, the set consisting of the single element  $M$ . By Section 5, Lemma 4, the set of all perfect ideals of  $R$

is a conservative system of  $R$ , and by Section 6, Lemma 5, so is the set consisting of  $R$  and of all the  $R_0$ -separable ideals of  $R$  having a given intersection with  $R_0$  ( $R_0$  being a subring of  $R$ ).

The intersection of a nonempty set of conservative systems of  $M$  is itself a conservative system of  $M$ . Therefore if  $\mathfrak{M}$  is any set of submodules of  $M$ , there is a unique smallest conservative system of  $M$  containing  $\mathfrak{M}$ .

If  $\mathfrak{C}$  is a conservative system of  $M$  and  $\Sigma$  is a subset of  $M$ , the intersection of all the elements of  $\mathfrak{C}$  that contain  $\Sigma$  is, by CS1, the smallest element of  $\mathfrak{C}$  containing  $\Sigma$ ; we call it the submodule of  $M$   *$\mathfrak{C}$ -generated* by  $\Sigma$  and denote it by  $(\Sigma)_{\mathfrak{C}}$ . An element of  $\mathfrak{C}$  that is  $\mathfrak{C}$ -generated by a finite set is said to be *finitely  $\mathfrak{C}$ -generated*, and any such finite set is called a  *$\mathfrak{C}$ -basis* of that element of  $\mathfrak{C}$ .

**Lemma 6** *Let  $\mathfrak{C}$  be a conservative system of an  $R$ -module  $M$ , and let  $\Sigma$  be a subset of  $M$ . If  $x \in (\Sigma)_{\mathfrak{C}}$ , then there exists a finite set  $\Phi \subset \Sigma$  such that  $x \in (\Phi)_{\mathfrak{C}}$ .*

*Proof* We may suppose that  $\Sigma$  is infinite. Then there exists a set  $\mathfrak{T}$  of subsets of  $\Sigma$  such that  $\mathfrak{T}$  is totally ordered by inclusion, each element of  $\mathfrak{T}$  has cardinal number strictly smaller than that of  $\Sigma$ , and  $\bigcup_{T \in \mathfrak{T}} T = \Sigma$ . By CS2,  $\bigcup_{T \in \mathfrak{T}} (T)_{\mathfrak{C}}$  is an element of  $\mathfrak{C}$ , and obviously  $\Sigma \subset \bigcup_{T \in \mathfrak{T}} (T)_{\mathfrak{C}} \subset (\Sigma)_{\mathfrak{C}}$ , so that  $(\Sigma)_{\mathfrak{C}} = \bigcup_{T \in \mathfrak{T}} (T)_{\mathfrak{C}}$ . The lemma now follows by induction on the cardinal number of  $\Sigma$ .

Now consider a mapping  $F$  of the conservative system  $\mathfrak{C}$  of  $M$  into a conservative system  $\mathfrak{C}'$  of a module  $M'$  over a ring  $R'$ , and suppose that  $F$  is intersection preserving in the sense that  $F(\bigcap_{c \in \mathfrak{M}} c) = \bigcap_{c \in \mathfrak{M}} F(c)$  for every subset  $\mathfrak{M}$  of  $\mathfrak{C}$ . If  $a, b \in \mathfrak{C}$  and  $a \subset b$ , then  $F(a) = F(a \cap b) = F(a) \cap F(b)$ , so that  $F(a) \subset F(b)$ ; that is,  $F$  is inclusion preserving. If  $F$  has the further property that  $F(\bigcup_{c \in \mathfrak{T}} c) = \bigcup_{c \in \mathfrak{T}} F(c)$  for every nonempty totally ordered subset  $\mathfrak{T}$  of  $\mathfrak{C}$ , then we call  $F$  a *conservative mapping*, or *homomorphism*, of  $\mathfrak{C}$  into  $\mathfrak{C}'$ . It is easy to see that if  $F$  is bijective, then the inverse mapping  $F^{-1}$  is also conservative; we say in this case that  $F$  is an *isomorphism* of  $\mathfrak{C}$  onto  $\mathfrak{C}'$ , and that the two conservative systems are *isomorphic*.

For a conservative mapping  $F: \mathfrak{C} \rightarrow \mathfrak{C}'$  an element  $c' \in F(\mathfrak{C})$  may be the image of several elements of  $\mathfrak{C}$ ; the intersection of all of them is the smallest element  $c$  of  $\mathfrak{C}$  with  $F(c) = c'$ . If  $a', b' \in F(\mathfrak{C})$  and  $a' \subset b'$ , and if  $a$ , respectively  $b$ , denotes the smallest element of  $\mathfrak{C}$  mapped onto  $a'$ , respectively  $b'$ , then  $F(a \cap b) = F(a) \cap F(b) = a' \cap b' = a'$  so that  $a \cap b = a$ ; in other words, if  $a' \subset b'$ , then  $a \subset b$ . Using this fact it is easy to see that  $F(\mathfrak{C})$  satisfies CS2. Since  $F(\mathfrak{C})$  obviously satisfies CS1, we see that  $F(\mathfrak{C})$  is a conservative system of  $M'$ .

As an example of a conservative mapping, let  $\mathfrak{C}$  be a conservative system

of  $R$ , let  $\mathfrak{r}$  be either a subring or an ideal of  $R$ , and consider the mapping  $\mathfrak{c} \mapsto \mathfrak{c} \cap \mathfrak{r}$  ( $\mathfrak{c} \in \mathfrak{C}$ ). It is easy to see that this is a homomorphism (called canonical) of  $\mathfrak{C}$  onto a conservative system of  $\mathfrak{r}$ . We denote this conservative system of  $\mathfrak{r}$  by  $\mathfrak{C}|\mathfrak{r}$ .

To obtain a second example, consider a ring epimorphism  $f: R \rightarrow R'$ , and denote the kernel of  $f$  by  $\mathfrak{f}$ . The set of all elements of the conservative system  $\mathfrak{C}$  of  $R$  that contain  $\mathfrak{f}$  is a conservative system of  $R$ , and  $\mathfrak{c} \mapsto f(\mathfrak{c})$  defines an isomorphism of this conservative system onto a conservative system, which we permit ourselves to denote by  $f(\mathfrak{C})$ , of  $R'$ . When  $f$  is the canonical ring homomorphism  $R \rightarrow R/\mathfrak{f}$ , we denote the conservative system  $f(\mathfrak{C})$  of  $R/\mathfrak{f}$  by  $\mathfrak{C}/\mathfrak{f}$  (and call the isomorphism canonical).

For a third example let  $\Sigma$  be a multiplicatively stable subset of  $R$  and consider the canonical homomorphism  $\varphi: R \rightarrow \Sigma^{-1}R$  of  $R$  into the ring of quotients  $\Sigma^{-1}R$  (see Section 4). The set of all  $\Sigma$ -prime elements of the conservative system  $\mathfrak{C}$  of  $R$  is a conservative system of  $R$  and  $\mathfrak{c} \mapsto \Sigma^{-1}\mathfrak{c}$  defines an isomorphism (called canonical) of this conservative system onto a conservative system, which we denote by  $\Sigma^{-1}\mathfrak{C}$ , of  $\Sigma^{-1}R$ . The inverse of this isomorphism is defined by  $\mathfrak{b} \mapsto \varphi^{-1}(\mathfrak{b})$ .

These three examples can be subsumed under a single construction. Let  $f: M' \rightarrow M$  be a homomorphism of  $R$ -modules. The set  $\mathcal{S}(M)$  of all submodules of  $M$  is a conservative system of  $M$ , and the set  $\mathcal{S}_{\mathfrak{f}}(M')$  of all submodules of  $M'$  containing the kernel  $\mathfrak{f}'$  of  $f$  is a conservative system of  $M'$ . The mapping  $f^*: \mathcal{S}(M) \rightarrow \mathcal{S}_{\mathfrak{f}}(M')$  defined by  $f^*(\mathfrak{f}) = f^{-1}(\mathfrak{f})$  is then a conservative one.

## 8 Perfect conservative systems

A conservative system  $\mathfrak{C}$  of a module over a ring  $R$  will be called *divisible* if  $\mathfrak{c}:s \in \mathfrak{C}$  whenever  $\mathfrak{c} \in \mathfrak{C}$  and  $s \in R$ . When this is the case, then  $\mathfrak{c}:\Sigma \in \mathfrak{C}$  whenever  $\mathfrak{c} \in \mathfrak{C}$  and  $\Sigma$  is a subset of  $R$ , for  $\mathfrak{c}:\Sigma = \bigcap_{s \in \Sigma} (\mathfrak{c}:s)$ .

A conservative system of the ring  $R$  will be called *perfect* if it is divisible and every element of it is a perfect ideal of  $R$ .

**Lemma 7** *Let  $\mathfrak{C}$  be a divisible conservative system of the ring  $R$ . Let  $\Sigma$  and  $\mathfrak{T}$  be subsets of  $R$  and let  $\Sigma\mathfrak{T}$  denote the set of all products  $st$  with  $s \in \Sigma$  and  $t \in \mathfrak{T}$ . Then  $(\Sigma)_{\mathfrak{C}}(\mathfrak{T})_{\mathfrak{C}} \subset (\Sigma\mathfrak{T})_{\mathfrak{C}}$ . If  $\mathfrak{C}$  is perfect, then  $(\Sigma\mathfrak{T})_{\mathfrak{C}} = (\Sigma)_{\mathfrak{C}} \cap (\mathfrak{T})_{\mathfrak{C}}$ .*

*Proof* Since  $(\Sigma\mathfrak{T})_{\mathfrak{C}}:\Sigma$  is a  $\mathfrak{C}$ -ideal containing  $\mathfrak{T}$ , it also contains  $(\mathfrak{T})_{\mathfrak{C}}$ . Therefore  $(\Sigma\mathfrak{T})_{\mathfrak{C}}:(\mathfrak{T})_{\mathfrak{C}}$  is a  $\mathfrak{C}$ -ideal containing  $\Sigma$ , hence containing  $(\Sigma)_{\mathfrak{C}}$ , so that  $(\Sigma)_{\mathfrak{C}}(\mathfrak{T})_{\mathfrak{C}} \subset (\Sigma\mathfrak{T})_{\mathfrak{C}}$ . Consequently  $((\Sigma)_{\mathfrak{C}} \cap (\mathfrak{T})_{\mathfrak{C}})^2 \subset (\Sigma\mathfrak{T})_{\mathfrak{C}}$ , so that if  $(\Sigma\mathfrak{T})_{\mathfrak{C}}$  is perfect, then  $(\Sigma)_{\mathfrak{C}} \cap (\mathfrak{T})_{\mathfrak{C}} \subset (\Sigma\mathfrak{T})_{\mathfrak{C}}$ ; the inclusion in the opposite direction is obvious.

Let  $\mathfrak{C}$  be any conservative system of the ring  $R$ . Let  $\mathfrak{c}$  be a perfect ideal of  $R$  with  $\mathfrak{c} \in \mathfrak{C}$ . By a  $\mathfrak{C}$ -component of  $\mathfrak{c}$  we shall mean any minimal element of the set, ordered by inclusion, of prime ideals that are elements of  $\mathfrak{C}$  and contain  $\mathfrak{c}$ . It is an easy consequence of Zorn's lemma and CS1 that every prime  $\mathfrak{C}$ -ideal containing  $\mathfrak{c}$  contains a  $\mathfrak{C}$ -component of  $\mathfrak{c}$ . The following proposition is, in the case in which  $\mathfrak{C}$  is the set of all perfect ideals of  $R$ , a remark due to Krull.

**Proposition 1** *Let  $\mathfrak{C}$  be a perfect conservative system of a ring  $R$ . Every  $\mathfrak{C}$ -ideal is the intersection of its  $\mathfrak{C}$ -components.*

*Proof* Let  $\mathfrak{c} \in \mathfrak{C}$ . If  $x \in R$  and  $x \notin \mathfrak{c}$ , there exists a  $\mathfrak{C}$ -ideal containing  $\mathfrak{c}$ , but not  $x$  (for example  $\mathfrak{c}$ ). By CS2 and Zorn's lemma there is a maximal such  $\mathfrak{C}$ -ideal, say  $\mathfrak{p}$ . If  $a, b \in R$  and  $a, b \notin \mathfrak{p}$ , then  $x \in (\mathfrak{p}, a)_{\mathfrak{C}}$ ,  $x \in (\mathfrak{p}, b)_{\mathfrak{C}}$ , whence (by Lemma 7)  $x \in (\mathfrak{p}, ab)_{\mathfrak{C}}$ , so that  $ab \notin \mathfrak{p}$ . Thus  $\mathfrak{p}$  is prime and hence contains a  $\mathfrak{C}$ -component of  $\mathfrak{c}$ . Therefore the intersection of all the  $\mathfrak{C}$ -components of  $\mathfrak{c}$  does not contain  $x$ . Since  $x$  is an arbitrary element of  $R$  not in  $\mathfrak{c}$ , this intersection is  $\mathfrak{c}$ .

## EXERCISE

- Let  $\mathfrak{C}$  be a divisible conservative system of a ring  $R$ , and let  $\mathfrak{c} \in \mathfrak{C}$ .
  - Show that the perfect ideal  $\mathfrak{c}^\dagger$  of  $R$  generated by  $\mathfrak{c}$  is a  $\mathfrak{C}$ -ideal. (*Hint*: For every  $x \in R$  with  $x^n \notin \mathfrak{c}$  ( $n \in \mathbb{N}$ ) there exists a maximal  $\mathfrak{C}$ -ideal containing  $\mathfrak{c}$  but not containing any  $x^n$ ; such a maximal  $\mathfrak{C}$ -ideal is prime.)
  - Show that if  $\mathfrak{c}^\dagger$  of part (a) is the intersection of finitely many prime ideals of  $R$  none of which contains any other, then each of these prime ideals is a  $\mathfrak{C}$ -ideal. (*Hint*: If  $\mathfrak{p}$  is one of these prime ideals and  $s$  is an element in the intersection of the others but not in  $\mathfrak{p}$ , then  $\mathfrak{c}^\dagger:s = \mathfrak{p}$ .)

## 9 Noetherian conservative systems

If  $\mathfrak{C}$  is a conservative system of an  $R$ -module  $M$ , the following three conditions are evidently equivalent.

- Every element of  $\mathfrak{C}$  has a  $\mathfrak{C}$ -basis.
- Every strictly increasing sequence of elements of  $\mathfrak{C}$  is finite.
- Every nonempty set of elements of  $\mathfrak{C}$  has a maximal element.

If these conditions are satisfied, we say that  $\mathfrak{C}$  is *Noetherian*, or that  $M$  is  *$\mathfrak{C}$ -Noetherian*.

For perfect conservative systems that are Noetherian, Proposition 1 can be greatly sharpened.

**Theorem 1** Let  $\mathfrak{C}$  be a Noetherian perfect conservative system of a ring  $R$ . Every  $\mathfrak{C}$ -ideal  $c$  is the intersection of a finite set of prime  $\mathfrak{C}$ -ideals none of which contains another. This finite set is unique, being the set of  $\mathfrak{C}$ -components of  $c$ .

*Proof* If the set of  $\mathfrak{C}$ -ideals that are not finite intersections of prime  $\mathfrak{C}$ -ideals were not empty, this set would have a maximal element  $a$ ; obviously  $a$  could not be prime or be  $R$ . There would then exist elements  $b, c \in R$  such that  $b, c \notin a$  and  $bc \in a$ . By Section 8, Lemma 7 we could write  $a = (a, b)_{\mathfrak{C}} \cap (a, c)_{\mathfrak{C}}$ , and by the maximality of  $a$  each of  $(a, b)_{\mathfrak{C}}$  and  $(a, c)_{\mathfrak{C}}$  would be a finite intersection of prime  $\mathfrak{C}$ -ideals, so that  $a$  would, too. This shows that every  $\mathfrak{C}$ -ideal is a finite intersection of prime  $\mathfrak{C}$ -ideals. Let  $c \in \mathfrak{C}$ . Discarding every superfluous prime ideals, we may express  $c$  as the intersection of a finite set  $\mathfrak{M}$  of prime  $\mathfrak{C}$ -ideals none of which contains another. If  $p'$  is any  $\mathfrak{C}$ -component of  $c$ , then, because  $\bigcap_{p \in \mathfrak{M}} p = c \subset p'$ , we have  $p \subset p'$  for some  $p \in \mathfrak{M}$ , whence  $p = p'$ . Thus, every  $\mathfrak{C}$ -component of  $c$  is an element of  $\mathfrak{M}$ . Conversely, if  $p \in \mathfrak{M}$ , then  $p$  contains a  $\mathfrak{C}$ -component of  $c$ , and by what we have just shown must be that  $\mathfrak{C}$ -component of  $c$ . This proves the theorem.

**REMARK** If a perfect ideal  $c$  of  $R$  is the intersection of finitely many prime ideals none of which contains any other, then every divisible conservative system  $\mathfrak{C}$  containing  $c$  also contains these prime ideals (see Section 8, Exercise 1) and they are the  $\mathfrak{C}$ -components of  $c$ . For such a perfect ideal  $c$  we may therefore refer to the *components* of  $c$ , without specifying the conservative system.

**Proposition 2** Let  $\mathfrak{C}$  be a Noetherian conservative system.

- (a) Every conservative system contained in  $\mathfrak{C}$  is Noetherian.
- (b) Every homomorphic image of  $\mathfrak{C}$  is Noetherian.

*Proof* The first part is obvious. If  $F: \mathfrak{C} \rightarrow \mathfrak{C}'$  is a surjective homomorphism of conservative systems, then (see Section 7) for each  $c' \in \mathfrak{C}'$  there exists a smallest  $c \in \mathfrak{C}$  with  $F(c) = c'$ , and the mapping  $c' \mapsto c$  of  $\mathfrak{C}'$  into  $\mathfrak{C}$  is a strictly increasing one. Therefore if  $\mathfrak{C}'$  contains an infinitely strictly increasing sequence, then so does  $\mathfrak{C}$ .

**Corollary 1** Let  $\mathfrak{C}$  be a conservative system of a ring  $R$ , let  $R_0$  be a subring of  $R$ ,  $\mathfrak{f}$  be an ideal of  $R$ , and  $\Sigma$  be a multiplicatively stable subset of  $R$ . If  $\mathfrak{C}$  is Noetherian, then so are  $\mathfrak{C}|R_0$ ,  $\mathfrak{C}|\mathfrak{f}$ ,  $\mathfrak{C}|\Sigma$ , and  $\Sigma^{-1}\mathfrak{C}$ .

**Corollary 2** Let  $\mathfrak{C}$  be a perfect conservative system of a ring  $R$ , and let  $\mathfrak{f}$  be an ideal of  $R$ . A necessary and sufficient condition that  $\mathfrak{C}$  be Noetherian is that  $\mathfrak{C}|\mathfrak{f}$  and  $\mathfrak{C}/\mathfrak{f}$  both be Noetherian.

*Proof* The necessity is contained in Corollary 1. If  $a, b$  are  $\mathfrak{C}$ -ideals with  $b \cap \mathfrak{f} \subset a \cap \mathfrak{f}$  and  $(b + \mathfrak{f})_{\mathfrak{C}} \subset (a + \mathfrak{f})_{\mathfrak{C}}$ , then  $b \subset b \cap (a + \mathfrak{f})_{\mathfrak{C}}$  so that (by Section 8, Lemma 7)  $b \subset (ab + b\mathfrak{f})_{\mathfrak{C}} \subset (a + a \cap \mathfrak{f})_{\mathfrak{C}} = a$ . Therefore if an inclusion  $a \subset b$  of  $\mathfrak{C}$ -ideals is strict, then either the inclusion  $a \cap \mathfrak{f} \subset b \cap \mathfrak{f}$  of elements of  $\mathfrak{C}|\mathfrak{f}$  is strict or the inclusion  $(a + \mathfrak{f})_{\mathfrak{C}}/\mathfrak{f} \subset (b + \mathfrak{f})_{\mathfrak{C}}/\mathfrak{f}$  of  $\mathfrak{C}/\mathfrak{f}$ -ideals is strict. It follows that if  $\mathfrak{C}$  is not Noetherian, then either  $\mathfrak{C}|\mathfrak{f}$  or  $\mathfrak{C}/\mathfrak{f}$  is not Noetherian.

**Lemma 8** Let  $\mathfrak{C}$  be a perfect conservative system of a ring  $R$ . If  $\mathfrak{C}$  is not Noetherian, then the set of  $\mathfrak{C}$ -ideals that are not finitely  $\mathfrak{C}$ -generated has a maximal element, and every such maximal element is prime.

*Proof* If  $\mathfrak{T}$  is a nonempty subset of  $\mathfrak{C}$ , totally ordered by inclusion, and if every element of  $\mathfrak{T}$  fails to be finitely  $\mathfrak{C}$ -generated, then  $\bigcup_{c \in \mathfrak{T}} c$  is not finitely  $\mathfrak{C}$ -generated. The existence of a maximal element is therefore a consequence of Zorn's lemma. Let  $m$  be any such maximal element; clearly  $m \neq R$ . If  $a, b \in R$  and  $a, b \notin m$ , then  $(m, a)_{\mathfrak{C}}$  and  $(m, b)_{\mathfrak{C}}$  are finitely  $\mathfrak{C}$ -generated, so that we may write  $(m, a)_{\mathfrak{C}} = (\Phi)_{\mathfrak{C}}$ ,  $(m, b)_{\mathfrak{C}} = (\Psi)_{\mathfrak{C}}$  with  $\Phi, \Psi$  finite; by Section 8, Lemma 7 then  $(m, ab)_{\mathfrak{C}} = (m, a)_{\mathfrak{C}} \cap (m, b)_{\mathfrak{C}} = (\Phi)_{\mathfrak{C}} \cap (\Psi)_{\mathfrak{C}} = (\Phi\Psi)_{\mathfrak{C}}$ , so that  $(m, ab)_{\mathfrak{C}}$  is finitely  $\mathfrak{C}$ -generated; since  $m$  is not,  $ab \notin m$ . Thus,  $m$  is prime.

**Proposition 3** Let  $R$  be a finitely generated overring of a ring  $R_0$ , and let  $\mathfrak{C}$  be a perfect conservative system of  $R$ . If  $\mathfrak{C}|R_0$  is Noetherian, then so is  $\mathfrak{C}$ .

**REMARK** The converse is part of Corollary 1 to Proposition 2.

*Proof* An obvious induction argument shows that it suffices to consider the case in which  $R = R_0[v]$  for some element  $v \in R$ . Assume the proposition false. By Lemma 8 there is a maximal  $\mathfrak{C}$ -ideal  $m$  that is not finitely  $\mathfrak{C}$ -generated, and  $m$  is prime. Since  $\mathfrak{C}|R_0$  is Noetherian,  $m \cap R_0$  has a  $\mathfrak{C}|R_0$ -basis  $\Psi$ . Evidently  $(m \cap R_0)_{\mathfrak{C}} = (\Psi)_{\mathfrak{C}}$ , so that  $m \neq (m \cap R_0)_{\mathfrak{C}}$ . Therefore there exists a polynomial  $f = a_0 + a_1 X + \dots + a_n X^n \in R_0[X]$  such that  $f(v) \in m$  and  $f(v) \notin (m \cap R_0)_{\mathfrak{C}}$ ; obviously  $n \neq 0$ . We suppose  $f$  chosen with  $n$  as small as possible, so that  $a_n \notin m$ . By the maximality of  $m$ ,  $(a_n, m)_{\mathfrak{C}}$  is finitely  $\mathfrak{C}$ -generated; it follows by Section 7, Lemma 6, that there exists a finite set  $\Phi \subset m$  such that  $(a_n, m)_{\mathfrak{C}} = (a_n, \Phi)_{\mathfrak{C}}$ . Now, for any  $w \in m$  there exists a polynomial  $g \in R_0[X]$  such that  $w = g(v)$ . Dividing  $g$  by  $f$  we obtain an equation  $a_n^k g = qf + r$  with  $q, r \in R_0[X]$  and  $\text{degr } r < n$ , so that  $a_n^k w = q(v)f(v) + r(v)$ , whence  $r(v) \in m$ . By the minimality of  $n$ , then  $r(v) \in (m \cap R_0)_{\mathfrak{C}} = (\Psi)_{\mathfrak{C}}$ , from which we conclude that  $a_n^k w \in (f(v), \Psi)_{\mathfrak{C}}$ . Thus  $a_n m \subset (f(v), \Psi)_{\mathfrak{C}}$ . Using Section 8, Lemma 7, we therefore find that

$$m = m \cap (a_n, m)_{\mathfrak{C}} = m \cap (a_n, \Phi)_{\mathfrak{C}} = (a_n m, \Phi)_{\mathfrak{C}} = (f(v), \Psi, \Phi)_{\mathfrak{C}},$$

contradicting the fact that  $m$  is not finitely generated.

**Corollary** *If the set of all perfect ideals of a ring  $R_0$  is a Noetherian conservative system, then so is the set of all perfect ideals of the polynomial algebra  $R_0[X]$ .*

EXERCISES

- Let  $\mathfrak{C}$  be a perfect conservative system of a ring. Show that  $\mathfrak{C}$  is Noetherian if and only if: (i) every strictly increasing sequence of prime  $\mathfrak{C}$ -ideals is finite; (ii) every  $\mathfrak{C}$ -ideal has only finitely many components. (*Hint: Prove the following lemma about ordered sets: Let  $C$  be an ordered set and assume there exists an infinite sequence  $(C_n)_{n \in \mathbb{N}}$  of distinct finite subsets of  $C$  such that distinct elements of  $C_n$  are never comparable and each element of  $C_{n+1}$  is greater than an element of  $C_n$ ; then there exists an infinite strictly increasing sequence of elements of  $C$ .*)
- Let  $\mathfrak{C}$  be a Noetherian conservative system of a ring  $R$ . Say that a  $\mathfrak{C}$ -ideal  $c$  is  $\mathfrak{C}$ -irreducible if  $c$  is not the intersection of a finite set of  $\mathfrak{C}$ -ideals different from  $c$ .
  - Show that every  $\mathfrak{C}$ -ideal is the intersection of a finite set of  $\mathfrak{C}$ -irreducible  $\mathfrak{C}$ -ideals.
  - Show that if  $\mathfrak{C}$  is divisible and has the property that  $u \in (v, \Sigma)_{\mathfrak{C}} \Rightarrow u \in ((u, \Sigma)_{\mathfrak{C}} : v^{\infty})_{\mathfrak{C}}$  for all elements  $u, v$  of  $R$  and all subsets  $\Sigma$  of  $R$ , then every  $\mathfrak{C}$ -irreducible  $\mathfrak{C}$ -ideal is primary.

10 Morphisms and birational equivalence of ideals

Let  $A$  be an algebra over a ring  $R$ . For any prime ideal  $p$  of  $A$ , the complete ring of quotients  $Q(A/p)$  is a field. If  $p'$  is a prime ideal of an  $R$ -algebra  $A'$ , it is natural to call any  $R$ -algebra isomorphism  $Q(A/p) \approx Q(A'/p')$  a "birational correspondence" between  $p$  and  $p'$  over  $R$ . The purpose of the present section is to generalize this notion. The generalization will be used in Section 12 to derive certain known results in a form suitable for use in later chapters.

Consider any ideal  $\mathfrak{f}$  of  $A$ . If  $s \in A$ , the element  $s + \mathfrak{f}$  of  $A/\mathfrak{f}$  is a nondivisor of zero precisely when  $\mathfrak{f}:s = \mathfrak{f}$ . We denote by  $\mathfrak{I}(\mathfrak{f})$  the set of all ideals  $I$  of  $A$  with  $I \supset \mathfrak{f}$  such that

$$s \in A, \quad \mathfrak{f}:s = \mathfrak{f} \quad \Rightarrow \quad I:s = I.$$

For any  $I \in \mathfrak{I}(\mathfrak{f})$  the canonical  $R$ -algebra homomorphism  $A/\mathfrak{f} \rightarrow A/I$  extends to a unique homomorphism  $Q(A/\mathfrak{f}) \rightarrow Q(A/I)$ , which we also call canonical.

Obviously  $\mathfrak{f} \in \mathfrak{I}(\mathfrak{f})$ . It is easy to verify that the intersection of any set of ideals in  $\mathfrak{I}(\mathfrak{f})$  is in  $\mathfrak{I}(\mathfrak{f})$ , that the union of any nonempty totally ordered set of ideals in  $\mathfrak{I}(\mathfrak{f})$  is in  $\mathfrak{I}(\mathfrak{f})$ , and that  $I:s \in \mathfrak{I}(\mathfrak{f})$  whenever  $I \in \mathfrak{I}(\mathfrak{f})$  and  $s \in A$ .

Thus,  $\mathfrak{I}(\mathfrak{f})$  is a divisible conservative system of  $A$ .

If  $I \in \mathfrak{I}(\mathfrak{f})$ , then  $\mathfrak{I}(I) \subset \mathfrak{I}(\mathfrak{f})$ .

If  $\mathfrak{f} = q_1 \cap \dots \cap q_r$ , where the ideals  $q_i$  are primary, belong to distinct prime ideals (i.e., the perfect ideals they generate are distinct), and are irredundant (i.e., no one of them contains the intersection of the others), then each  $q_i \in \mathfrak{I}(\mathfrak{f})$ . This is an easy consequence of the fact that  $\mathfrak{f}:s = \mathfrak{f}$  if and only if  $s \notin p_1 \cup \dots \cup p_r$ ,  $p_i$  denoting the prime ideal to which  $q_i$  belongs. It follows that each  $p_i \in \mathfrak{I}(\mathfrak{f})$ , too.

By way of example, we see that if  $p$  is a prime ideal of  $A$ , then  $\mathfrak{I}(p)$  consists of the two elements  $p$  and  $A$ . If  $A$  happens to be a factorial ring (i.e., a unique factorization domain) and  $f \in A, f \neq 0$ , then  $\mathfrak{I}(Af)$  consists of all the ideals  $Ag$  with  $g \in Af$ . (We leave the proof as an exercise.)

Let  $\mathfrak{f}, \mathfrak{f}'$  be ideals of the  $R$ -algebras  $A, A'$ , respectively. By an  $R$ -morphism of  $\mathfrak{f}$  into  $\mathfrak{f}'$  we shall mean a pair  $\Psi = (\psi, (\psi_I)_{I \in \mathfrak{I}(\mathfrak{f})})$  such that  $\psi$  is a conservative mapping of  $\mathfrak{I}(\mathfrak{f})$  into  $\mathfrak{I}(\mathfrak{f}')$  with  $\psi(\mathfrak{f}) = \mathfrak{f}'$ ,  $(\psi_I)_{I \in \mathfrak{I}(\mathfrak{f})}$  is a family such that, for each  $I \in \mathfrak{I}(\mathfrak{f})$ ,  $\psi_I$  is an  $R$ -algebra homomorphism of  $Q(A'/\psi(I))$  into  $Q(A/I)$ , and the diagram

$$\begin{array}{ccc} Q(A/\mathfrak{m}) & \xleftarrow{\psi_{\mathfrak{m}}} & Q(A'/\psi(\mathfrak{m})) \\ \uparrow & & \uparrow \\ Q(A/I) & \xleftarrow{\psi_I} & Q(A'/\psi(I)) \end{array} \quad (1)$$

is commutative for all  $I \in \mathfrak{I}(\mathfrak{f})$  and  $\mathfrak{m} \in \mathfrak{I}(I)$ , the vertical arrows denoting the canonical homomorphisms. We often write  $\Psi : \mathfrak{f} \rightarrow \mathfrak{f}'$ .

Let  $\Psi = (\psi, (\psi_I)_{I \in \mathfrak{I}(\mathfrak{f})})$  be an  $R$ -morphism of  $\mathfrak{f}$  into  $\mathfrak{f}'$ . If  $\Psi' = (\psi', (\psi'_I)_{I' \in \mathfrak{I}(\mathfrak{f}')})$  is an  $R$ -morphism of  $\mathfrak{f}'$  into an ideal  $\mathfrak{f}''$  of an  $R$ -algebra  $A''$ , then  $(\psi' \circ \psi, (\psi'_I \circ \psi_{\psi(I)})_{I \in \mathfrak{I}(\mathfrak{f})})$  is an  $R$ -morphism of  $\mathfrak{f}$  into  $\mathfrak{f}''$ ; we call it the composite of  $\Psi$  and  $\Psi'$ , and denote it by  $\Psi' \circ \Psi$ . Composition is obviously associative. The identity mapping of  $\mathfrak{I}(\mathfrak{f})$  into itself together with the identity homomorphisms  $Q(A/I) \rightarrow Q(A/I)$  define an  $R$ -morphism of  $\mathfrak{f}$  into  $\mathfrak{f}$ , which we call the identity  $R$ -morphism of  $\mathfrak{f}$  and denote by  $I^{\mathfrak{f}}$  or  $I$ . If the conservative mapping  $\psi : \mathfrak{I}(\mathfrak{f}) \rightarrow \mathfrak{I}(\mathfrak{f}')$  is a bijective one, and  $\psi_I : Q(A'/\psi(I)) \rightarrow Q(A/I)$  is an isomorphism for each  $I \in \mathfrak{I}(\mathfrak{f})$ , then we call the  $R$ -morphism  $\Psi = (\psi, (\psi_I)_{I \in \mathfrak{I}(\mathfrak{f})})$  a birational correspondence between  $\mathfrak{f}$  and  $\mathfrak{f}'$  over  $R$ . A necessary and sufficient condition for this to be the case is that there exist an  $R$ -morphism  $\Psi' : \mathfrak{f}' \rightarrow \mathfrak{f}$  such that  $\Psi' \circ \Psi = I^{\mathfrak{f}}$  and  $\Psi \circ \Psi' = I^{\mathfrak{f}'}$ . If such a  $\Psi'$  exists it is unique; we then call it the inverse of  $\Psi$  and denote it by  $\Psi^{-1}$ . If there exists a birational correspondence between  $\mathfrak{f}$  and  $\mathfrak{f}'$  over  $R$ , we say that these ideals are birationally equivalent over  $R$ . This notion of birational equivalence defines an equivalence relation on any set of ideals of  $R$ -algebras.

If  $I \in \mathfrak{I}(\mathfrak{f})$  and we set  $I' = \psi(I)$ , it is easy to see that  $\psi$  maps  $\mathfrak{I}(I)$  into  $\mathfrak{I}(I')$ .

It follows that if we denote the restriction of  $\psi$  to  $\mathfrak{I}(I)$  by  $\lambda$ , then  $(\lambda, (\psi_m)_{m \in \mathfrak{I}(I)})$  is an  $R$ -morphism of  $I$  into  $I'$ ; we call it the  $R$ -morphism induced by  $\Psi$  on  $I$ .

It is easy to see that if  $\Psi: \mathfrak{f} \rightarrow \mathfrak{f}'$  is a birational correspondence over  $R$  and if  $\mathfrak{f}$  has one of the properties of being prime, being perfect, being primary, being  $R$ -regular, or being  $R$ -separable, then  $\mathfrak{f}'$  has the same property. In particular, if  $\mathfrak{f} = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_r$ , with the  $\mathfrak{q}_i$  primary, belonging to distinct prime ideals  $\mathfrak{p}_i$ , and irredundant, then  $\psi(\mathfrak{f}) = \psi(\mathfrak{q}_1) \cap \cdots \cap \psi(\mathfrak{q}_r)$  and the ideals  $\psi(\mathfrak{q}_i)$  are primary, belong to the distinct prime ideals  $\psi(\mathfrak{p}_i)$ , and are irredundant.

Before continuing with the matter at hand, we prove the following lemma which is sometimes useful in passing from an ideal in a subring of  $R$  to an ideal of  $R$ .

**Lemma 9** *Let  $R_0$  be a subring of a ring  $R$  such that  $R$  is a free  $R_0$ -module; let  $\mathfrak{f}_0$  be an ideal of  $R_0$ .*

(a) *If  $(u_i)$  is a basis of the  $R_0$ -module  $R$  and  $x = \sum a_i u_i$  with each  $a_i \in R_0$ , then  $x$  is in the ideal  $R\mathfrak{f}_0$  of  $R$  if and only if each  $a_i \in \mathfrak{f}_0$ .*

(b)  $(R\mathfrak{f}_0) \cap R_0 = \mathfrak{f}_0$ .

*Proof* If  $x \in R\mathfrak{f}_0$ , we may write  $x = \sum x_j k_j$  with  $x_j \in R$  and  $k_j \in \mathfrak{f}_0$  for every  $j$ , and then we may write  $x_j = \sum_i b_{ij} u_i$  with  $b_{ij} \in R_0$ ; hence  $\sum a_i u_i = x = \sum_i (\sum_j b_{ij} k_j) u_i$ , so that  $a_i = \sum_j b_{ij} k_j \in \mathfrak{f}_0$ . Since the converse is obvious, part (a) is proved. If  $a \in (R\mathfrak{f}_0) \cap R_0$ , then, for any fixed index  $i$ ,  $au_i \in R\mathfrak{f}_0$  so that by part (a)  $a \in \mathfrak{f}_0$ . Since the converse is obvious, part (b) is proved.

We return to  $R$ -morphisms with the following lemma, which is the source of most of the applications in Section 12.

**Lemma 10** (a) *If  $f: A' \rightarrow A$  is a surjective homomorphism of  $R$ -algebras and  $\mathfrak{f}, \mathfrak{f}'$  are ideals of  $A, A'$ , respectively, with  $\mathfrak{f}' = f^{-1}(\mathfrak{f})$ , then the formula  $l \mapsto f^{-1}(l)$  defines a bijective conservative mapping  $f^l: \mathfrak{I}(\mathfrak{f}) \rightarrow \mathfrak{I}(\mathfrak{f}')$ ; for each  $l \in \mathfrak{I}(\mathfrak{f})$   $f$  induces an  $R$ -algebra isomorphism  $f_l: Q(A'/f^{-1}(l)) \approx Q(A/l)$ , and  $(f^l, (f_l)_{l \in \mathfrak{I}(\mathfrak{f})})$  is a birational correspondence between  $\mathfrak{f}$  and  $\mathfrak{f}'$  over  $R$ .*

(b) *If  $f: A' \rightarrow A$  is a homomorphism of  $R$ -algebras such that  $A$  is a free  $f(A')$ -module, and  $\mathfrak{p}'$  is a prime ideal of  $A'$  containing the kernel of  $f$ , then the formula  $l \mapsto f^{-1}(l)$  defines a conservative mapping  $f^{A f(\mathfrak{p}')}: \mathfrak{I}(A f(\mathfrak{p}')) \rightarrow \mathfrak{I}(\mathfrak{p}')$ ; for each  $l \in \mathfrak{I}(A f(\mathfrak{p}'))$   $f$  induces an  $R$ -algebra homomorphism  $f_l: Q(A'/f^{-1}(l)) \rightarrow Q(A/l)$ , and  $(f^{A f(\mathfrak{p}')}, (f_l)_{l \in \mathfrak{I}(A f(\mathfrak{p}')})$  is an  $R$ -morphism of  $A f(\mathfrak{p}')$  into  $\mathfrak{p}'$ .*

(c) *If  $\Sigma$  is a multiplicatively stable subset of an  $R$ -algebra  $A$ , and  $\varphi: A \rightarrow \Sigma^{-1}A$  denotes the canonical homomorphism, and  $\mathfrak{f}$  is a  $\Sigma$ -prime ideal of  $A$  (see Section 4), then the formula  $\Sigma^{-1}l \mapsto l$  defines a bijective conservative mapping  $\varphi^{\Sigma^{-1}l}: \mathfrak{I}(\Sigma^{-1}\mathfrak{f}) \rightarrow \mathfrak{I}(\mathfrak{f})$ ; for each  $\Sigma^{-1}l \in \mathfrak{I}(\Sigma^{-1}\mathfrak{f})$ ,  $\varphi$*

*induces an  $R$ -algebra isomorphism  $\varphi_{\Sigma^{-1}l}: Q(A/l) \approx Q(\Sigma^{-1}A/\Sigma^{-1}l)$ , and  $(\varphi^{\Sigma^{-1}l}, (\varphi_{\Sigma^{-1}l})_{\Sigma^{-1}l \in \mathfrak{I}(\Sigma^{-1}\mathfrak{f})})$  is a birational correspondence between  $\Sigma^{-1}\mathfrak{f}$  and  $\mathfrak{f}$  over  $R$ .*

*Proof* (a) Because  $f$  is a surjective,  $l \mapsto f^{-1}(l)$  defines a bijective conservative mapping of the set of all ideals of  $A$  onto the set of all ideals of  $A'$  containing the kernel of  $f$ ; the relation  $f^{-1}(l): s' = f^{-1}(l)$  is evidently equivalent to the relation  $l: f(s') = l$ , so that  $\mathfrak{I}(\mathfrak{f})$  is mapped bijectively onto  $\mathfrak{I}(\mathfrak{f}')$ . Moreover,  $f$  induces an isomorphism  $A'/f^{-1}(l) \approx A/l$ , which extends to a unique isomorphism  $f_l: Q(A'/f^{-1}(l)) \approx Q(A/l)$ . The fact that the diagrams analogous to (1) are all commutative is easy to see.

(b) By Lemma 9 we observe first that if  $s' \in A'$  and  $\mathfrak{p}': s' = \mathfrak{p}'$ , then  $(A f(\mathfrak{p}')): f(s') = A f(\mathfrak{p}')$ . We observe next that if  $l \in \mathfrak{I}(A f(\mathfrak{p}'))$ , then  $f^{-1}(l) \in \mathfrak{I}(\mathfrak{p}')$  (and therefore, since  $\mathfrak{p}'$  is prime, then either  $f^{-1}(l) = \mathfrak{p}'$  or  $f^{-1}(l) = A'$ ); indeed, if  $\mathfrak{p}': s' = \mathfrak{p}'$ , then by our first observation  $l: f(s') = l$ , whence  $f^{-1}(l): s' = l$ , so that  $f^{-1}(l) \in \mathfrak{I}(\mathfrak{p}')$ . We therefore have our mapping  $f^{A f(\mathfrak{p}')}: \mathfrak{I}(A f(\mathfrak{p}')) \rightarrow \mathfrak{I}(\mathfrak{p}')$  defined by  $l \mapsto f^{-1}(l)$ , and  $f^{-1}(l) = \mathfrak{p}'$  whenever  $l \in \mathfrak{I}(A f(\mathfrak{p}'))$  and  $l \neq A$ ;  $f^{A f(\mathfrak{p}'})$  is clearly conservative, and  $f$  induces a homomorphism  $f_l: Q(A'/f^{-1}(l)) \rightarrow Q(A/l)$  for each  $l \in \mathfrak{I}(A f(\mathfrak{p}'))$ . The commutativity of the diagrams analogous to (1) is obvious.

(c) The formula  $l \mapsto \Sigma^{-1}l$  defines a bijective conservative mapping of the set of all  $\Sigma$ -prime ideals of  $A$  onto the set of all ideals of  $\Sigma^{-1}A$ , the inverse of this mapping being defined by  $\Sigma^{-1}l \mapsto \varphi^{-1}(\Sigma^{-1}l) = l$ . If  $\mathfrak{f}$  is  $\Sigma$ -prime, then so is every  $l \in \mathfrak{I}(\mathfrak{f})$ . For any  $\Sigma$ -prime  $l$  and any  $s \in A$  the relation  $l: s = l$  is equivalent to the relation  $(\Sigma^{-1}l): \varphi(s) = \Sigma^{-1}l$ , and  $\varphi$  induces an injective homomorphism  $A/l \rightarrow \Sigma^{-1}A/\Sigma^{-1}l$ , the image of which has the same complete ring of quotients as  $\Sigma^{-1}A/\Sigma^{-1}l$ . Part (c) of the lemma follows easily from these facts.

## EXERCISE

- Let  $\mathfrak{f}, \mathfrak{f}'$  be ideals of a Noetherian ring  $R$  with  $\mathfrak{f} \subset \mathfrak{f}'$ ; let  $\Pi, \Pi'$ , respectively  $\Pi', \Pi$ , denote the set of prime ideals associated with  $\mathfrak{f}$ , respectively  $\mathfrak{f}'$ . Show that  $\mathfrak{f}' \in \mathfrak{I}(\mathfrak{f})$  if and only if every element of  $\Pi'$  is a subset of an element of  $\Pi$ , and that when this is the case then every element of  $\Pi'$  contains an element of  $\Pi$ . (*Hint*: See Section 16, footnote in proof of Corollary 2 to Proposition 11.)

## 11 Polynomial ideals and generic zeros

Consider a prime ideal  $\mathfrak{p}$  of a polynomial algebra  $K[X] = K[(X_i)_{i \in I}]$  over a field  $K$ . A *generic zero* of  $\mathfrak{p}$  is a family  $x = (x_i)_{i \in I}$  of elements of a field extension of  $K$  such that a polynomial in  $K[X]$  is an element of  $\mathfrak{p}$  if and only

if the polynomial vanishes at  $x$ , that is, such that  $\mathfrak{p}$  is the kernel of the substitution homomorphism  $K[X] \rightarrow K[x]$ . It follows that  $x$  is a generic zero of  $\mathfrak{p}$  precisely when there exists a  $K$ -algebra isomorphism  $K[x] \approx K[X]/\mathfrak{p}$  that maps  $x_i$  onto  $X_i + \mathfrak{p}$  for every  $i$ . This shows that every prime ideal of  $K[X]$  has a generic zero, and it is unique up to  $K$ -isomorphism.

Let  $x = (x_i)_{i \in I}$  be a generic zero of  $\mathfrak{p}$ . By the definitions in Section 6,  $\mathfrak{p}$  is a separable (respectively quasi-separable, respectively regular) ideal over  $K$  if and only if  $K(x)$  is a separable (respectively quasi-separable, respectively regular) field extension of  $K$ .

The dimension of  $\mathfrak{p}$ , denoted by  $\dim \mathfrak{p}$ , is by definition the transcendence degree of  $K(x)$  over  $K$ . It is easy to see that if  $f$  is an irreducible polynomial in a finitely generated polynomial algebra  $K[X_1, \dots, X_n]$ , then the principal ideal  $(f)$  is prime and of dimension  $n-1$ . The following proposition implies that if, conversely,  $\mathfrak{p}$  is a prime ideal of  $K[X_1, \dots, X_n]$  of dimension  $n-1$ , then  $\mathfrak{p}$  is principal.

**Proposition 4** *If  $\mathfrak{p}$  and  $\mathfrak{p}'$  are prime ideals of  $K[X_1, \dots, X_n]$  with  $\mathfrak{p} \subset \mathfrak{p}'$ , then  $\dim \mathfrak{p} \geq \dim \mathfrak{p}'$ ; if moreover  $\dim \mathfrak{p} = \dim \mathfrak{p}'$ , then  $\mathfrak{p} = \mathfrak{p}'$ .*

*Proof* Let  $(x_1, \dots, x_n), (x'_1, \dots, x'_n)$  be generic zeros of  $\mathfrak{p}, \mathfrak{p}'$ , respectively, with say  $(x'_1, \dots, x'_d)$  a transcendence basis of  $K(x'_1, \dots, x'_n)$  over  $K$ . Then  $(x_1, \dots, x_d)$  is algebraically independent over  $K$ , for otherwise  $\mathfrak{p}$  would contain a nonzero element of  $K[X_1, \dots, X_d]$  so that  $\mathfrak{p}'$  would too, and  $(x'_1, \dots, x'_d)$  would not be algebraically independent over  $K$ . Therefore  $\dim \mathfrak{p} \geq d = \dim \mathfrak{p}'$ . If  $f, g \in K[X_1, \dots, X_n]$  and  $f(x_1, \dots, x_n) = g(x_1, \dots, x_n)$ , then  $f - g \in \mathfrak{p}$ , whence  $f - g \in \mathfrak{p}'$ , so that  $f(x'_1, \dots, x'_n) = g(x'_1, \dots, x'_n)$ . Therefore there exists a mapping  $\varphi: K[x_1, \dots, x_n] \rightarrow K[x'_1, \dots, x'_n]$  such that  $\varphi(f(x_1, \dots, x_n)) = f(x'_1, \dots, x'_n)$  for every  $f \in K[X_1, \dots, X_n]$ , and  $\varphi$  is easily seen to be an algebra homomorphism. Of course,  $\varphi$  is surjective. Suppose  $\dim \mathfrak{p} = d$ . Then any nonzero  $y \in K[x_1, \dots, x_n]$  is algebraic of some degree  $m$  over  $K(x_1, \dots, x_d)$ , so that there exists a polynomial  $h \in K[X_1, \dots, X_d, Y]$  of degree  $m$  in  $Y$  such that  $h(x_1, \dots, x_d, Y)$  is an irreducible polynomial in  $K(x_1, \dots, x_d)[Y]$  vanishing at  $y$ . Clearly  $h(x_1, \dots, x_d, 0) \neq 0$ . Writing  $y = f(x_1, \dots, x_n)$  with  $f \in K[X_1, \dots, X_n]$ , we see that  $h(X_1, \dots, X_d, f(X_1, \dots, X_n))$  vanishes at  $(x_1, \dots, x_n)$ , hence is in  $\mathfrak{p}$ , hence in  $\mathfrak{p}'$ , and therefore vanishes at  $(x'_1, \dots, x'_n)$ . However,  $h(x'_1, \dots, x'_d, 0) \neq 0$ , so that  $\varphi(y) = f(x'_1, \dots, x'_n) \neq 0$ . Thus,  $\varphi$  is injective, hence an isomorphism, so that  $\mathfrak{p} = \mathfrak{p}'$ .

**12 Polynomial ideals and ground field extension**

If  $\mathfrak{f}$  is an ideal of a polynomial algebra  $K[X] = K[(X_i)_{i \in I}]$  over a field  $K$  and  $L$  is a field extension, then  $\mathfrak{f}$  generates an ideal of the polynomial algebra

$L[X]$  over  $L$ ; we generally denote this ideal by  $L\mathfrak{f}$ . The purpose of this section is to obtain certain information about  $L\mathfrak{f}$  under various assumptions on  $\mathfrak{f}$ .

**Lemma 11** *Let  $\mathfrak{p}$  be a prime ideal of a polynomial algebra  $K[X] = K[(X_i)_{i \in I}]$  over a field  $K$ , let  $\mathfrak{f}'$  be an ideal of a polynomial algebra  $K[X'] = K[(X'_i)_{i \in I'}]$  over  $K$ , let  $\mathfrak{r}$  be the ideal of  $K[X, X']$  generated by  $\mathfrak{p} \cup \mathfrak{f}'$ , and let  $x$  be a generic zero of  $\mathfrak{p}$ . Then there exists a birational correspondence between  $K(x)\mathfrak{f}'$  and  $\mathfrak{r}$  over  $K$ . If  $\mathfrak{v}$  and  $\mathfrak{s}$  are corresponding elements of  $\mathfrak{S}(K(x)\mathfrak{f}')$  and  $\mathfrak{S}(\mathfrak{r})$ , respectively, then (for any  $f \in K[X, X']$ )  $f(x, X') \in \mathfrak{v}$  if and only if  $f(X, X') \in \mathfrak{s}$ , and the  $K$ -isomorphism  $Q(K[X, X']/\mathfrak{s}) \approx Q(K(x)[X']/\mathfrak{v})$  is given by*

$$(g(X, X') + \mathfrak{s}) / (h(X, X') + \mathfrak{s}) \mapsto (g(x, X') + \mathfrak{v}) / (h(x, X') + \mathfrak{v}).$$

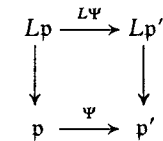
*Proof* The substitution homomorphism  $K[X, X'] \rightarrow K[x, X']$  is surjective, has kernel  $K[X, X']\mathfrak{p} \subset \mathfrak{r}$ , and maps  $\mathfrak{r}$  onto  $K[x, X']\mathfrak{f}'$ . Also,  $K(x)[X']$  is the ring of quotients of  $K[x, X']$  over the set  $\Sigma$  of nonzero elements of  $K[x, X']$ ,  $K[x, X']\mathfrak{f}'$  is a  $\Sigma$ -prime ideal of  $K[x, X']$  (easy consequence of Section 10, Lemma 9(a)), and  $\Sigma^{-1}K[x, X']\mathfrak{f}' = K(x)[X']\mathfrak{f}' = K(x)\mathfrak{f}'$ . The result now follows from Section 10, Lemma 10(a) and (c).

**Proposition 5** *Let  $\mathfrak{p}$  and  $\mathfrak{p}'$  be prime ideals of polynomial algebras over a field  $K$ , and let them have generic zeros  $x$  and  $x'$ , respectively. Then there exists a birational correspondence between  $K(x)\mathfrak{p}'$  and  $K(x')\mathfrak{p}$  over  $K$ . If  $\mathfrak{v}'$  and  $\mathfrak{v}$  are corresponding elements of  $\mathfrak{S}(K(x)\mathfrak{p}')$  and  $\mathfrak{S}(K(x')\mathfrak{p})$ , respectively, then (for any  $f \in K[X, X']$ )  $f(x, X') \in \mathfrak{v}'$  if and only if  $f(X, x') \in \mathfrak{v}$ , and the  $K$ -isomorphism  $Q(K(x')[X']/\mathfrak{v}) \approx Q(K(x)[X']/\mathfrak{v}')$  is given by*

$$(g(X, x') + \mathfrak{v}) / (h(X, x') + \mathfrak{v}) \mapsto (g(x, X') + \mathfrak{v}') / (h(x, X') + \mathfrak{v}').$$

*Proof* By Lemma 11 there are birational correspondences  $K(x)\mathfrak{p}' \rightarrow \mathfrak{r}$  and  $K(x')\mathfrak{p} \rightarrow \mathfrak{r}$ , where  $\mathfrak{r}$  is the ideal of  $K[X, X']$  generated by  $\mathfrak{p} \cup \mathfrak{p}'$ . Composing the former with the inverse of the latter we obtain the desired result.

**Proposition 6** *Let  $\mathfrak{p}$  and  $\mathfrak{p}'$  be prime ideals of polynomial algebras over a field  $K$ , let  $\Psi: \mathfrak{p} \rightarrow \mathfrak{p}'$  be a  $K$ -morphism and let  $L$  be a field extension of  $K$ . Then there exists a unique  $L$ -morphism  $L\Psi: L\mathfrak{p} \rightarrow L\mathfrak{p}'$  (which is therefore a  $K$ -morphism) such that the diagram*



*is commutative, the vertical arrows denoting the  $K$ -morphisms induced (according to Section 10, Lemma 10(b)) by the inclusions  $K[X] \rightarrow L[X]$  and  $K[X'] \rightarrow L[X']$ . If  $\Psi$  is a birational correspondence, then so is  $L\Psi$ .*



*Proof* To give a  $K$ -morphism  $\Psi: \mathfrak{p} \rightarrow \mathfrak{p}'$  is to give a  $K$ -homomorphism  $\psi: Q(K[X']/\mathfrak{p}') \rightarrow Q(K[X]/\mathfrak{p})$ . Denote the image of  $X$  under the canonical homomorphism  $K[X] \rightarrow Q(K[X]/\mathfrak{p})$  by  $x$  and the image of  $X'$  under the composite homomorphism  $K[X'] \rightarrow Q(K[X']/\mathfrak{p}') \xrightarrow{\psi} Q(K[X]/\mathfrak{p})$  by  $x'$ ; then  $x$  and  $x'$  are generic zeros of  $\mathfrak{p}$  and  $\mathfrak{p}'$ , respectively, and  $K(x') \subset K(x)$ . Therefore we may write  $x' = C(x)/D(x) = (C_{i'}(x)/D_{i'}(x))_{i' \in I'}$ , where  $C_{i'}, D_{i'} \in K[X]$  and  $D_{i'} \notin \mathfrak{p}$ . Let  $x''$  be a family of generators of the field extension  $L$  of  $K$ , let  $X''$  be a corresponding family of indeterminates, and let  $\mathfrak{p}''$  be the defining ideal of  $x''$  in  $K[X'']$ . We have the three  $K$ -morphisms  $L\mathfrak{p} = K(x'')\mathfrak{p} \rightarrow K(x)\mathfrak{p}$  (according to Proposition 5),  $K(x)\mathfrak{p} \rightarrow K(x')\mathfrak{p}$  (induced by the inclusion  $K(x') \rightarrow K(x)$  according to Section 10, Lemma 10(b)), and  $K(x')\mathfrak{p} \rightarrow K(x'')\mathfrak{p}' = L\mathfrak{p}'$  (according to Proposition 5). Their composite is a  $K$ -morphism  $L\mathfrak{p} \rightarrow L\mathfrak{p}'$  which we denote by  $L\Psi$ .

To facilitate the description of  $L\Psi$  let us agree, for any polynomial  $f$  in  $L[X'] = L[(X_{i'})_{i' \in I'}]$  or in  $K[X, X']$  with  $\deg_{X_{i'}} f = d_{i'}$  ( $i' \in I'$ ) and for any family  $P = (P_{i'})_{i' \in I'}$  of elements of a ring, to denote the product  $\prod_{i' \in I'} P_{i'}^{d_{i'}}$  by  $P^{\deg f}$ . Let  $I \in \mathfrak{Z}(L\mathfrak{p})$ , and denote the image of  $I$  under the conservative mapping  $\mathfrak{Z}(L\mathfrak{p}) = \mathfrak{Z}(K(x'')\mathfrak{p}) \rightarrow \mathfrak{Z}(K(x)\mathfrak{p})$  by  $I''$ ; the image of  $I''$  under  $\mathfrak{Z}(K(x)\mathfrak{p}) \rightarrow \mathfrak{Z}(K(x')\mathfrak{p})$  is then  $I'' \cap K(x')[X'']$ . Denote the image of  $I'' \cap K(x')[X'']$  under  $\mathfrak{Z}(K(x')\mathfrak{p}) \rightarrow \mathfrak{Z}(K(x'')\mathfrak{p}') = \mathfrak{Z}(L\mathfrak{p}')$  by  $I'$ . Then the conservative mapping  $\mathfrak{Z}(L\mathfrak{p}) \rightarrow \mathfrak{Z}(L\mathfrak{p}')$  maps  $I$  onto  $I'$ . For any nonzero  $f \in K[X', X'']$ ,  $f(X', x'') \in I'$  if and only if  $f(x', X'') \in I'' \cap K(x')[X'']$ , that is, if and only if  $f(x', X'') \in I''$ , or even  $f(C(x)/D(x), X'') D(x)^{\deg f} \in I$ . Similar reasoning then happens if and only if  $f(C(X)/D(X), x'') D(X)^{\deg f} \in I$ . Similar reasoning then shows that the  $K$ -homomorphism  $Q(L[X']/I') \rightarrow Q(L[X]/I)$  is given by

$$(g(X', x'') + I') / (h(X', x'') + I') \mapsto (g(C(X)/D(X), x'') D(X)^{\deg gh} + I) / (h(C(X)/D(X), x'') D(X)^{\deg gh} + I),$$

where  $g, h$  are arbitrary polynomials in  $K[X', X'']$  with  $h(X', x'') \notin I'$ , that is, is given by

$$(g(X') + I') / (h(X') + I') \mapsto (g(C(X)/D(X)) D(X)^{\deg gh} + I) / (h(C(X)/D(X)) D(X)^{\deg gh} + I), \quad (2)$$

where now  $g, h$  are arbitrary polynomials in  $L[X']$  with  $h \notin I'$ . In particular, this is a homomorphism over  $L$ , so that  $L\Psi$  is an  $L$ -morphism.

To prove the commutativity of the diagram in the statement of the proposition, we must show that the diagram

$$\begin{array}{ccc} \mathfrak{Z}(L\mathfrak{p}) & \longrightarrow & \mathfrak{Z}(L\mathfrak{p}') \\ \downarrow & & \downarrow \\ \mathfrak{Z}(\mathfrak{p}) & \longrightarrow & \mathfrak{Z}(\mathfrak{p}') \end{array}$$

of conservative mappings and, for each  $I \in \mathfrak{Z}(L\mathfrak{p})$  with  $I \neq L[X]$  and with corresponding  $I' \in \mathfrak{Z}(L\mathfrak{p}')$ , the diagram

$$\begin{array}{ccc} Q(L[X]/I) & \longleftarrow & Q(L[X']/I') \\ \uparrow & & \uparrow \\ Q(K[X]/\mathfrak{p}) & \longleftarrow & Q(K[X']/\mathfrak{p}') \end{array}$$

of homomorphisms are commutative. That the diagram of conservative mappings is commutative is obvious, since  $\mathfrak{Z}(\mathfrak{p})$  consists solely of  $\mathfrak{p}$  and  $K[X]$  and similarly for  $\mathfrak{Z}(\mathfrak{p}')$ . In the diagram of homomorphisms, the lower horizontal arrow is given by

$$(g(X') + \mathfrak{p}') / (h(X') + \mathfrak{p}') \mapsto (g(C(X)/D(X)) D(X)^{\deg gh} + \mathfrak{p}) / (h(C(X)/D(X)) D(X)^{\deg gh} + \mathfrak{p}),$$

where now  $g, h$  are arbitrary polynomials in  $K[X']$  with  $h \notin \mathfrak{p}'$ ; the vertical arrow on the right is given by

$$(g(X') + \mathfrak{p}') / (h(X') + \mathfrak{p}') \mapsto (g(X') + I') / (h(X') + I'),$$

and the vertical arrow on the left is given similarly. Together with what we already know about the upper horizontal arrow, this shows that the diagram is commutative.

To prove the uniqueness as stated in the proposition, let  $\Phi = (\varphi, (\varphi_{i'})_{i' \in \mathfrak{Z}(L\mathfrak{p})})$  be an  $L$ -morphism  $L\mathfrak{p} \rightarrow L\mathfrak{p}'$  that makes a commutative diagram. The element  $(X_{i'} + \mathfrak{p}') / (1 + \mathfrak{p}')$  of  $Q(K[X']/\mathfrak{p}')$  is mapped onto the element  $(C_{i'}(X) + \mathfrak{p}) / (D_{i'}(X) + \mathfrak{p})$  of  $Q(K[X]/\mathfrak{p})$ , which in turn is mapped onto the element  $(C_{i'}(X) + I) / (D_{i'}(X) + I)$  of  $Q(L[X]/I)$ . On the other hand,  $(X_{i'} + \mathfrak{p}') / (1 + \mathfrak{p}')$  is mapped onto the element  $(X_{i'} + I') / (1 + I')$  of  $Q(L[X']/I')$ . It follows that

$$\varphi_{i'}((X_{i'} + I') / (1 + I')) = (C_{i'}(X) + I) / (D_{i'}(X) + I).$$

Therefore if  $f \in L[X']$ , then

$$\begin{aligned} f(X') \in I' &\Leftrightarrow f((X' + I') / (1 + I')) = 0 \\ &\Leftrightarrow f((C(X) + I) / (D(X) + I)) = 0 \\ &\Leftrightarrow (f(C(X)/D(X)) D(X)^{\deg f} + I) / (D(X)^{\deg f} + I) = 0 \\ &\Leftrightarrow f(C(X)/D(X)) D(X)^{\deg f} \in I, \end{aligned}$$

so that  $\varphi$  coincides with the conservative mapping of  $L\Psi$ , and  $\varphi_{i'}$  is given by Eq. (2). Thus,  $\Phi = L\Psi$  and the uniqueness is proved.

Finally, suppose that  $\Psi$  is a birational correspondence, i.e., has an inverse

$\Psi^{-1}$ . Then there exists a  $K$ -morphism  $L\Psi^{-1}: L\mathfrak{p}' \rightarrow L\mathfrak{p}$  such that the diagram

$$\begin{array}{ccc} L\mathfrak{p}' & \xrightarrow{L\Psi^{-1}} & L\mathfrak{p} \\ \downarrow & & \downarrow \\ \mathfrak{p}' & \xrightarrow{\Psi^{-1}} & \mathfrak{p} \end{array}$$

is commutative. Combining this diagram with the one in the statement of the proposition we find the commutative diagram

$$\begin{array}{ccc} L\mathfrak{p} & \xrightarrow{L\Psi^{-1} \circ L\Psi} & L\mathfrak{p} \\ \downarrow & & \downarrow \\ \mathfrak{p} & \xrightarrow{I^{\mathfrak{p}}} & \mathfrak{p} \end{array}$$

However, if we replace the upper horizontal arrow here by  $I^{L\mathfrak{p}}$ , we also obtain a commutative diagram so that, by the properties and uniqueness of  $L I^{\mathfrak{p}}$ ,  $L\Psi^{-1} \circ L\Psi = L I^{\mathfrak{p}} = I^{L\mathfrak{p}}$ . Similarly,  $L\Psi \circ L\Psi^{-1} = I^{L\mathfrak{p}'}$ . Therefore  $L\Psi$  is a birational correspondence (with inverse  $L\Psi^{-1}$ ). This completes the proof of Proposition 6.

Before we use Propositions 5 and 6 to study the behavior of a prime ideal under the influence of an extension of the coefficient field, we need a lemma which is really a very special case.

**Lemma 12** Let  $K$  be a subfield of a field  $L$ , with  $K$  algebraically (respectively separably) closed in  $L$ . Let  $(X_i)_{i \in I}$  be a family of indeterminates.

(a) The field  $K((X_i)_{i \in I})$  is algebraically (respectively separably) closed in  $L((X_i)_{i \in I})$ .

(b) If  $f$  is a polynomial (respectively polynomial having a nonzero partial derivative) in  $K[[X_i]_{i \in I}]$  and  $f$  is irreducible over  $K$ , then  $f$  is irreducible over  $L$ .

*Proof* (a) It clearly suffices to consider the case in which  $I$  is finite; an induction argument shows we may suppose that  $I$  consists of a single element. Consider first the hypothesis that  $K$  be algebraically closed in  $L$ . If  $\varphi \in L(X)$  is nonzero and algebraic over  $K(X)$ , and we write  $\varphi = \lambda g/h$ , with  $\lambda \in L$  and with  $g, h \in L[X]$  relatively prime and unitary, then  $f_0 \lambda^n g^n + f_1 \lambda^{n-1} g^{n-1} h + \dots + f_n h^n = 0$  for suitable  $f_0, f_1, \dots, f_n \in K[X]$  with  $f_0 f_n \neq 0$ . Every root of  $h$  is a root of  $f_0$ , hence is algebraic over  $K$ ; the coefficients in  $h$  are in  $L$  and are plus or minus the elementary symmetric functions of these roots, hence are algebraic over  $K$ , hence are in  $K$ , so that  $h \in K[X]$ ; similarly  $g \in K[X]$ . Therefore  $\lambda$  is algebraic over  $K(X)$ , from which it easily follows that  $\lambda$  is

algebraic over  $K$ , so that  $\lambda \in K$ . Thus  $\varphi \in K(X)$ . Now consider the hypothesis that  $K$  be separably closed in  $L$ , and let  $\varphi \in L(X)$  be separably algebraic over  $K(X)$ . Setting  $K'$  equal to the algebraic closure of  $K$  in  $L$ , so that  $K' \subset K_i$ , we see by the case already treated that  $\varphi \in K'(X)$ , whence  $\varphi \in K_i(X) \subset K(X)_i$ . Therefore  $\varphi \in K(X)$ .

(b) Let  $i$  be a fixed element of  $I$  such that  $X_i$  is present in  $f$  (respectively such that  $\partial f / \partial X_i \neq 0$ ), let  $Y$  denote the family  $(X_j)_{j \in I, j \neq i}$ , and consider  $f$  as a polynomial in  $X_i$ . The coefficients in  $f$  are elements of  $K[Y]$  and do not have a common divisor in  $K[Y]$  (for  $f$  is irreducible in  $K[(X_j)_{j \in I}]$ ), hence do not have a common divisor in  $L[Y]$ . Therefore, if  $f$  is reducible in  $L[(X_j)_{j \in I}]$ , then  $f$  is reducible in  $L(Y)[X_i]$ , and we can write  $f = f_0 \prod g_k$ , where  $f_0 \in K[Y]$ , and each  $g_k \in L(Y)[X_i]$  is irreducible in  $L(Y)[X_i]$  and unitary. The roots of  $g_k$  are roots of  $f$ , hence algebraic over  $K(Y)$ . Therefore the coefficients in  $g$  are algebraic over  $K(Y)$  and are in  $L(Y)$ . It is easy to see in the separably closed case that  $\partial g_k / \partial X_i \neq 0$ . Hence, in either case, the coefficients in  $g_k$  are elements of  $K(Y)$ , so that  $f$  is reducible in  $K(Y)[X_i]$ , and therefore in  $K[Y, X_i] = K[(X_j)_{j \in I}]$ , contrary to hypothesis. This completes the proof of the lemma.

**Proposition 7** Let  $\mathfrak{p}$  be a prime ideal of a polynomial algebra  $K[(X_i)_{i \in I}]$  over a field  $K$ ; let  $x = (x_i)_{i \in I}$  be a generic zero of  $\mathfrak{p}$ .

(a) If  $I$  is finite,  $L$  is any field extension of  $K$ , and  $\mathfrak{q}$  is a component of the perfect ideal generated by  $L\mathfrak{p}$  in  $L[(X_i)_{i \in I}]$ , then  $\mathfrak{q} \cap K[(X_i)_{i \in I}] = \mathfrak{p}$  and  $\dim \mathfrak{q} = \dim \mathfrak{p}$ .

(b) A necessary and sufficient condition that  $L\mathfrak{p}$  be perfect for every field extension  $L$  of  $K$  is that  $\mathfrak{p}$  be separable over  $K$ . When this is the case then  $L\mathfrak{p}$  is separable over  $L$  for every  $L$ . If, in addition,  $I$  is finite and  $d = \dim \mathfrak{p}$ , then  $\mathfrak{p}$  is birationally equivalent over  $K$  to a principal ideal  $K[X_0, X_1, \dots, X_d]f$  with  $f$  an irreducible element of  $K[X_0, X_1, \dots, X_d]$  such that  $\partial f / \partial X_0 \neq 0$ , and there exists a polynomial  $g \in K[(X_i)_{i \in I}]$  with  $g \notin \mathfrak{p}$  such that, for any  $L$ ,  $g$  is contained in the sum of any two distinct components of  $L\mathfrak{p}$ .

(c) If  $\mathfrak{p}$  is separable over  $K$ , then a necessary and sufficient condition that  $L\mathfrak{p}$  be prime for a given  $L$  is that, for every element  $u \in L$  that is separably algebraic over  $K$ , the minimal polynomial of  $u$  over  $K$  be irreducible over  $K(x)$ .

(d) A necessary and sufficient condition that  $L\mathfrak{p}$  be prime for every  $L$  is that  $\mathfrak{p}$  be regular over  $K$ . When this is the case then  $L\mathfrak{p}$  is regular over  $L$  for every  $L$ .

*Proof* (a) Let  $J$  be a subset of  $I$  such that  $(x_j)_{j \in J}$  is a transcendence basis of  $K(x)$  over  $K$ , and let  $0_J$  denote the zero ideal of  $K[(X_j)_{j \in J}]$ . Because  $\mathfrak{I}(\mathfrak{p})$  consists of  $\mathfrak{p}$  and the unity ideal, and similarly for  $\mathfrak{I}(0_J)$ , we see that the inclusion homomorphism  $K[(X_j)_{j \in J}] \rightarrow K[(X_i)_{i \in I}]$  induces a  $K$ -morphism

$\Psi: \mathfrak{p} \rightarrow 0_J$ . In accordance with Proposition 6 this yields a commutative diagram

$$\begin{array}{ccc} L\mathfrak{p} & \xrightarrow{L\Psi} & L0_J \\ \Pi \downarrow & & \downarrow \\ \mathfrak{p} & \xrightarrow{\Psi} & 0_J \end{array}$$

The conservative mapping  $\mathfrak{Z}(L\mathfrak{p}) \rightarrow \mathfrak{Z}(\mathfrak{p})$  of  $\Pi$  maps any  $I$  onto  $I \cap K[(X_{i \in I})]$ . If the perfect ideal generated by  $L\mathfrak{p}$  has only finitely many components (in particular, if  $I$  is finite), each such component  $q$  is in  $\mathfrak{Z}(L\mathfrak{p})$ , and therefore  $q \cap K[(X_{i \in I})] = \mathfrak{p}$ . Similarly, the conservative mapping  $\mathfrak{Z}(L\mathfrak{p}) \rightarrow \mathfrak{Z}(L0_J)$  of  $L\Psi$  maps any  $I$  onto  $I \cap L[(X_{j \in J})]$  and therefore, under the same circumstances,  $q \cap L[(X_{j \in J})] = L0_J$ . If  $y = (y_{i \in I})$  is a generic zero of  $q$ , so that certainly  $L(y)$  is algebraic over  $L((y_{j \in J}))$ ; the latter conclusion shows that  $(y_{j \in J})$  is algebraically independent over  $L$ . Therefore  $\dim q = \text{Card } J = \dim \mathfrak{p}$ .

(b) Let  $\mathfrak{p}$  not be separable over  $K$ . Then  $K$  has characteristic  $p \neq 0$ , and there exist elements  $a_1, \dots, a_r \in K$  and polynomials  $f_1, \dots, f_r \in K[(X_{i \in I})]$  not all in  $\mathfrak{p}$  such that  $a_1, \dots, a_r$  are linearly independent over  $K^p$  and  $\sum f_j^p a_j \in \mathfrak{p}$ . Then the elements  $a_1^{1/p}, \dots, a_r^{1/p} \in K^{1/p}$  are linearly independent over  $K$ , so that by Section 10, Lemma 9, the polynomial  $\sum f_j a_j^{1/p} \in K^{1/p}[(X_{i \in I})]$  is not in  $K^{1/p} \mathfrak{p}$ . However,  $(\sum f_j a_j^{1/p})^p = \sum f_j^p a_j \in K^{1/p} \mathfrak{p}$ , so that  $K^{1/p} \mathfrak{p}$  is not perfect.

Now let  $\mathfrak{p}$  be separable over  $K$ . It is easy to see that for any  $J \subset I$  the prime ideal  $\mathfrak{p} \cap K[(X_{j \in J})]$  is separable over  $K$ ; also, if  $L\mathfrak{p}$  is not separable over  $L$ , then we may choose a finite  $J$  such that  $L(\mathfrak{p} \cap K[(X_{j \in J})])$  is not separable over  $L$ . Thus, in the present part of the proof it suffices to consider the case in which  $I$  is finite, say consists of  $1, 2, \dots, n$ . As  $\mathfrak{p}$  is separable over  $K$ , some of the  $x_i$ , say  $x_1, \dots, x_d$ , form a separating transcendence basis of  $K(x)$  over  $K$ . Then there exists a single element  $x_0 \in K(x)$  such that  $K(x_0, x_1, \dots, x_d) = K(x_1, \dots, x_n)$ . The defining ideal  $\bar{f}$  of  $(x_0, x_1, \dots, x_d)$  in  $K[X_0, X_1, \dots, X_d]$  has dimension  $d$  and is principal, say  $\bar{f} = K[X_0, X_1, \dots, X_d] f$ . Then  $f$  is an irreducible polynomial in  $K[X_0, X_1, \dots, X_d]$  and, because  $x_0$  is separably algebraic over  $K(x_1, \dots, x_d)$ ,  $\partial f / \partial X_0 \neq 0$ . Because  $K(x_1, \dots, x_n) = K(x_0, x_1, \dots, x_d)$ , there is a birational correspondence  $\Psi: \mathfrak{p} \rightarrow \bar{f}$  over  $K$ , which, in accordance with Proposition 6, yields the birational correspondence  $L\Psi: L\mathfrak{p} \rightarrow L\bar{f}$  over  $L$ . Writing  $f = f_1 \cdots f_r$  with each  $f_i$  an irreducible polynomial in  $L[X_0, X_1, \dots, X_d]$  we see that the  $f_j$  are distinct and  $\partial f_j / \partial X_0 \neq 0$ , so that  $L\bar{f}$  is the intersection of the  $L$ -separable prime ideals  $L[X_0, X_1, \dots, X_d] f_j$ . Thus,  $L\bar{f}$  is separable over  $L$  and has these ideals as components. Therefore the birationally equivalent ideal  $L\mathfrak{p}$  is separable over  $L$  and has corresponding components  $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ . The isomorphism

$Q(K[X_0, X_1, \dots, X_d]/\bar{f}) \approx Q(K[X_1, \dots, X_n]/\mathfrak{p})$  connected with the birational correspondence  $\Psi$  carries the element  $(X_0 + \bar{f})/(1 + \bar{f})$  onto some element  $(C + \mathfrak{p})/(D + \mathfrak{p})$ , where  $C, D \in K[X_1, \dots, X_n]$  and  $D \notin \mathfrak{p}$ , and carries  $(X_i + \bar{f})/(1 + \bar{f})$  onto  $(X_i + \mathfrak{p})/(1 + \mathfrak{p})$  ( $1 \leq i \leq d$ ). Starting with the equation

$$\partial f / \partial X_0 = \sum_{0 \leq j \leq r} f_1 \cdots (\partial f_j / \partial X_0) \cdots f_r,$$

if we substitute  $C/D$  for  $X_0$  and then multiply by  $D^e$ , where  $e = \deg_{X_0} f - 1$ , we find an equation

$$g = \sum_{0 \leq j \leq r} p_1 \cdots g_j \cdots p_r,$$

where  $g \in K[X_1, \dots, X_n]$ ,  $p_j \in \mathfrak{p}_j$ ,  $p_j \notin \mathfrak{p}_{j'}$  ( $j \neq j'$ ),  $g_j \in L[X_1, \dots, X_n]$ ,  $g_j \notin \mathfrak{p}_j$ . Therefore  $g \notin \mathfrak{p}$  and  $g \in \mathfrak{p}_j + \mathfrak{p}_{j'}$  whenever  $j \neq j'$ .

(c) For each  $u \in L$  that is separably algebraic over  $K$  let  $f_u$  be the minimal polynomial of  $u$  in  $K[U]$ . Suppose some  $f_u$  is reducible over  $K(x)$ , that is, the ideal  $K(x)[U] f_u$  is not prime. This ideal is, by Proposition 5, birationally equivalent over  $K$  to  $K(u) \mathfrak{p}$ , which must therefore also not be prime, so that  $L\mathfrak{p}$  is not prime, too. Conversely, suppose  $L\mathfrak{p}$  is not prime. Then there exists a finite set  $J \subset I$  such that the  $K$ -separable prime ideal  $\mathfrak{p}_J = \mathfrak{p} \cap K[(X_{j \in J})]$  has the property that  $L\mathfrak{p}_J$  is not prime;  $x_J = (x_{j \in J})$  is a generic zero of  $\mathfrak{p}_J$ . By (b),  $\mathfrak{p}_J$  is birationally equivalent over  $K$  to some  $\bar{f} = K[(X_{j \in J})] f$ , and, by Proposition 6,  $L\mathfrak{p}_J$  is birationally equivalent over  $L$  to  $L\bar{f}$ , so that  $L\bar{f}$  is not prime, that is,  $f$  is reducible over  $L$ . By Lemma 12,  $f$  is reducible over the separable closure of  $K$  in  $L$ , hence over a separable extension of  $K$  in  $L$  of finite degree, hence over  $K(u)$  for some  $u \in L$  that is separably algebraic over  $K$ . Thus,  $K(u)\bar{f}$  is not prime, hence  $K(u)\mathfrak{p}_J$  is not prime, so that, by Proposition 5,  $f_u$  is reducible over  $K(x_J)$ , and therefore over  $K(x)$ .

(d) If  $\mathfrak{p}$  is not  $K$ -separable, then  $\mathfrak{p}$  is not regular over  $K$  and (by (b))  $L\mathfrak{p}$  is not prime for some  $L$ . Therefore we may suppose that  $\mathfrak{p}$  is  $K$ -separable. By part (c),  $L\mathfrak{p}$  is prime for every  $L$  if and only if every separable irreducible polynomial in  $K[U]$  remains irreducible over  $K(x)$ , which, by Lemma 12, happens if and only if  $K$  is separably closed in  $K(x)$ , that is, if and only if  $\mathfrak{p}$  is regular over  $K$ .

**Corollary 1** *If  $\mathfrak{a}$  is a  $K$ -separable ideal of  $K[(X_{i \in I})]$ , then, for every extension  $L$  of  $K$ ,  $L\mathfrak{a}$  is an  $L$ -separable ideal of  $L[(X_{i \in I})]$ . When, in addition, the extension  $L$  of  $K$  is separable, then  $L\mathfrak{a}$  is  $K$ -separable.*

*Proof* We may write  $\mathfrak{a} = \bigcap \mathfrak{p}_j$ , where each  $\mathfrak{p}_j$  is a  $K$ -separable prime ideal. Using Section 10, Lemma 9 we can see that  $L\mathfrak{a} = \bigcap L\mathfrak{p}_j$ . By the Proposition, part (b), each  $L\mathfrak{p}_j$  is  $L$ -separable, so that  $L\mathfrak{a}$  is, too. Now suppose that  $L$  is a separable extension of  $K$ . Then the ideal  $L\mathfrak{a} \cap L = (0)$  of  $L$  is  $K$ -separable. It follows (see Section 6) that  $L\mathfrak{a}$  is  $K$ -separable.

**Corollary 2** Let  $K$  be a field,  $(X_i)_{i \in I}$  be a family of indeterminates,  $(I_\lambda)_{\lambda \in \Lambda}$  be a partition of the set of indices  $I$ , and (for each  $\lambda \in \Lambda$ )  $\mathfrak{p}_\lambda$  be a  $K$ -regular ideal of  $K[(X_i)_{i \in I_\lambda}]$ ; let  $\mathfrak{r}$  denote the ideal of  $K[(X_i)_{i \in I}]$  generated by  $\bigcup_{\lambda \in \Lambda} \mathfrak{p}_\lambda$ . Then  $\mathfrak{r}$  is  $K$ -regular,  $\mathfrak{r} \cap K[(X_i)_{i \in I_\lambda}] = \mathfrak{p}_\lambda$  ( $\lambda \in \Lambda$ ), and  $\dim \mathfrak{r} = \sum_{\lambda \in \Lambda} \dim \mathfrak{p}_\lambda$ .

*Proof* It is easy to see that it suffices to consider the case in which  $\Lambda$  is finite, and it follows by induction that we may suppose that  $\Lambda$  consists of two elements, say the numbers 1 and 2. Let  $x^1$  be a generic zero of  $\mathfrak{p}_1$ . By Lemma 11,  $\mathfrak{r}$  is birationally equivalent to  $K(x^1)\mathfrak{p}_2$  over  $K$ ; by Proposition 7, the latter ideal is  $K(x^1)$ -regular, so that if  $x^2$  is a generic zero of it, then  $K(x^1, x^2)$  is regular over  $K(x^1)$ . As  $K(x^1)$  is regular over  $K$  it follows that  $K(x^1, x^2)$  is regular over  $K$ . Also by Lemma 11, if  $f \in K[X^1, X^2]$ , then

$$f(X^1, X^2) \in \mathfrak{r} \Leftrightarrow f(x^1, X^2) \in K(x^1)\mathfrak{p}_2 \Leftrightarrow f(x^1, x^2) = 0,$$

so that  $(x^1, x^2)$  is a generic zero of  $\mathfrak{r}$ . Therefore  $\mathfrak{r}$  is  $K$ -regular,  $\mathfrak{r} \cap K[X^1] = \mathfrak{p}_1$ , and

$$\begin{aligned} \dim \mathfrak{r} &= \text{tr deg } K(x^1, x^2)/K \\ &= \text{tr deg } K(x^1)/K + \text{tr deg } K(x^1, x^2)/K(x^1) \\ &= \dim \mathfrak{p}_1 + \dim K(x^1)\mathfrak{p}_2 = \dim \mathfrak{p}_1 + \dim \mathfrak{p}_2. \end{aligned}$$

**Corollary 3** Let  $K$  be a field, let  $R_1, \dots, R_m$  be integral domains that are finitely generated algebras over  $K$ , let  $L$  be an extension of  $K$ , and let  $U$  be an algebraically closed extension of  $L$  of infinite transcendence degree. For each index  $i$  there exist finitely many isomorphisms  $f_{ij} : R_i \approx R_{ij}$  over  $K$  ( $1 \leq j \leq n_i$ ), each  $R_{ij}$  being a subring of  $U$  containing  $K$ , with the following properties.

- Whenever  $f'_i : R_i \rightarrow U$  is a homomorphism over  $K$  ( $1 \leq i \leq m$ ), then there exist indices  $j_1, \dots, j_m$  such that the  $m$  homomorphisms  $f'_i \circ f_{ij_i}^{-1}$  ( $1 \leq i \leq m$ ) extend to a single homomorphism  $L[R_{1j_1} \cup \dots \cup R_{mj_m}] \rightarrow U$  over  $L$ .
- $\text{tr deg } L(\bigcup_{1 \leq i \leq m} \bigcup_{1 \leq j \leq n_i} R_{ij})/L = \sum_{1 \leq i \leq m} n_i \text{tr deg } K(R_i)/K$ .
- If  $K(R_i)$  is separable over  $K$ , then  $L(R_{ij})$  is separable over  $L$  ( $1 \leq j \leq n_i$ ).
- If  $K(R_i)$  is regular over  $K$ , then  $n_i = 1$  and  $L(R_{i1})$  is regular over  $L$ .

*Proof* There exists a family  $x^i = (x_1^i, \dots, x_{n_i}^i)$  of elements of  $R_i$  such that  $R_i = K[x^i]$ . Let  $\mathfrak{p}_i$  denote the defining ideal of  $x^i$  over  $K$ , and let  $L_{\mathfrak{a}}$  denote the algebraic closure of  $L$ . By the proposition, the perfect ideal  $\bar{\mathfrak{p}}_i$  generated by  $\mathfrak{p}_i$  over  $L_{\mathfrak{a}}$  has finitely many components  $\mathfrak{p}_{i1}, \dots, \mathfrak{p}_{in_i}$ , the set of elements of  $\mathfrak{p}_{ij}$  that have all their coefficients in  $K$  is  $\mathfrak{p}_i$ , and  $\dim \mathfrak{p}_{ij} = \dim \mathfrak{p}_i$ . Each ideal  $\mathfrak{p}_{ij}$  ( $1 \leq i \leq m, 1 \leq j \leq n_i$ ) is  $L_{\mathfrak{a}}$ -regular. We now treat these  $\sum_{1 \leq i \leq m} n_i$  ideals as the ideals  $\mathfrak{p}_\lambda$  of Corollary 2 (with  $L_{\mathfrak{a}}$  instead of  $K$ ), and form the

ideal  $\mathfrak{r}$  as in that corollary. Then  $\mathfrak{r}$  is  $L_{\mathfrak{a}}$ -regular, hence has a generic zero  $(x^{ij})_{1 \leq i \leq m, 1 \leq j \leq n_i}$ . Now,  $x^{ij}$  is a generic zero of  $\mathfrak{p}_{ij}$ , hence also of  $\mathfrak{p}_i$ , so that there is a unique isomorphism  $f_{ij}$  over  $K$  of the ring  $R_i = K[x^i]$  onto the ring  $R_{ij} = K[x^{ij}]$  carrying  $x^i$  onto  $x^{ij}$ , and

$$\begin{aligned} \text{tr deg } L\left(\bigcup_{1 \leq i \leq m} \bigcup_{1 \leq j \leq n_i} R_{ij}\right)/L &= \text{tr deg } L_{\mathfrak{a}}((x^{ij})_{1 \leq i \leq m, 1 \leq j \leq n_i})/L_{\mathfrak{a}} \\ &= \dim \mathfrak{r} = \sum_{1 \leq i \leq m} \sum_{1 \leq j \leq n_i} \dim \mathfrak{p}_{ij} \\ &= \sum_{1 \leq i \leq m} n_i \dim \mathfrak{p}_i. \end{aligned}$$

If  $f'_i : R_i \rightarrow U$  is a homomorphism over  $K$  ( $1 \leq i \leq m$ ), then  $f'_i(x^i)$  is a zero of  $\mathfrak{p}_i$ , hence of  $\bar{\mathfrak{p}}_i$ , and therefore of  $\mathfrak{p}_{ij}$  for some index  $j$ , say for  $j = j_i$ . Writing the ideals  $\mathfrak{p}_{1j_1}, \dots, \mathfrak{p}_{mj_m}$  in different sets of indeterminates, and letting  $\mathfrak{r}'$  denote the ideal generated by  $\mathfrak{p}_{1j_1} \cup \dots \cup \mathfrak{p}_{mj_m}$  in the polynomial algebra over  $L_{\mathfrak{a}}$  in all these indeterminates, we see that  $(f'_1(x^1), \dots, f'_m(x^m))$  is a zero of  $\mathfrak{r}'$  and, by Corollary 2, that the point  $(x^{1j_1}, \dots, x^{mj_m}) = (f_{1j_1}(x^1), \dots, f_{mj_m}(x^m))$  is a generic zero of  $\mathfrak{r}'$ . Therefore there exists a homomorphism  $L_{\mathfrak{a}}[f_{1j_1}(x^1), \dots, f_{mj_m}(x^m)] \rightarrow L_{\mathfrak{a}}[f'_1(x^1), \dots, f'_m(x^m)]$  over  $L_{\mathfrak{a}}$  mapping  $f_{ij_i}(x^i)$  onto  $f'_i(x^i)$  ( $1 \leq i \leq m$ ), and this yields by restriction a homomorphism  $L[f_{1j_1}(R_1) \cup \dots \cup f_{mj_m}(R_m)] \rightarrow L[f'_1(R_1) \cup \dots \cup f'_m(R_m)]$  over  $L$  extending  $f'_i \circ f_{ij_i}^{-1}$  ( $1 \leq i \leq m$ ). By Corollary 1, if  $K(R_i)$  is separable over  $K$ , so that  $\mathfrak{p}_i$  is  $K$ -separable, then  $L\mathfrak{p}_i$  is  $L$ -separable, hence has  $L$ -separable components. However, it is easy to see that each  $x^{ij}$  is a generic zero of a component of  $L\mathfrak{p}_i$ , so that  $L(R_{ij}) = L(x^{ij})$  is separable over  $L$ . Similarly, by the proposition, part (d), if  $K(R_i)$  is regular over  $K$ , then  $n_i = 1$  and  $L(R_{i1})$  is regular over  $L$ .

**REMARK** When  $K(R_i)$  is separable over  $K$ , we have the following converse to part (d) of Corollary 3: If  $n_i = 1$  for every extension  $L$  of  $K$ , then  $K(R_i)$  is regular over  $K$ . This follows easily from Proposition 7.

### 13 Power series

We recall certain well-known facts about power series. Let  $R$  be a ring and let  $X = (X_i)_{i \in I}$  be a family of indeterminates. Then we may construct the *power series algebra* in  $X$  over  $R$ , which we denote by  $R[[X]]$ . The elements of  $R[[X]]$  are the infinite sequences  $A = (A_k)_{k \in \mathbb{N}}$ , in which  $A_k$  is an arbitrary homogeneous polynomial in  $X$  over  $R$  of degree  $k$  (including the possibility  $A_k = 0$ );  $A$  is called a *power series* in  $X$  over  $R$ ,  $A_k$  is the *homogeneous part* of  $A$  of degree  $k$ , and we sometimes denote it by  $h_k(A)$ .

Addition and multiplication of two power series  $A, B \in R[[X]]$  are defined by the formulae

$$h_k(A+B) = h_k(A) + h_k(B), \quad h_k(AB) = \sum_{k'+k''=k} h_{k'}(A)h_{k''}(B) \quad (k \in \mathbb{N}).$$

The *series-order* of  $A$ , denoted by  $v(A)$ , is defined to be the smallest  $k$  for which  $h_k(A) \neq 0$  if  $A \neq 0$  (i.e., if  $A \neq (0)_{k \in \mathbb{N}}$ ) and to be  $\infty$  if  $A = 0$ . Clearly  $v(A+B) \geq \min(v(A), v(B))$  and  $v(AB) \geq v(A) + v(B)$ . The former inequality is an equality whenever  $v(A) \neq v(B)$ , and the latter inequality is an equality whenever  $R$  is an integral domain.

Certain infinite sums in  $R[[X]]$  are meaningful. Namely, if  $(A^{(\lambda)})_{\lambda \in \Lambda}$  is a family of elements of  $R[[X]]$  such that for each  $k \in \mathbb{N}$  there exist only finitely many indices  $\lambda \in \Lambda$  with  $v(A^{(\lambda)}) \leq k$ , then  $\sum_{\lambda \in \Lambda} A^{(\lambda)}$  is defined as the element of  $R[[X]]$  of which the homogeneous part of degree  $k$  is  $\sum_{\lambda \in \Lambda} h_k(A^{(\lambda)})$  (this being, in effect, a finite sum). Such infinite sums enjoy various obvious formal properties, among which we mention the following:

$$\begin{aligned} \sum_{\lambda \in \Lambda} A^{(\lambda)} + \sum_{\lambda \in \Lambda} B^{(\lambda)} &= \sum_{\lambda \in \Lambda} (A^{(\lambda)} + B^{(\lambda)}), \\ \left( \sum_{\lambda \in \Lambda} A^{(\lambda)} \right) \left( \sum_{\mu \in \mathbb{M}} B^{(\mu)} \right) &= \sum_{(\lambda, \mu) \in \Lambda \times \mathbb{M}} A^{(\lambda)} B^{(\mu)}, \\ \sum_{\lambda \in \Lambda} A^{(\lambda)} &= \sum_{\lambda \in \Lambda'} A^{(\lambda)} \end{aligned}$$

for any set  $\Lambda' \subset \Lambda$  such that  $A^{(\lambda)} = 0$  whenever  $\lambda \in \Lambda - \Lambda'$ . If, for each polynomial  $f \in R[X]$ , we let  $f_k$  denote the sum of the terms of  $f$  of degree  $k$ , then the mapping  $R[X] \rightarrow R[[X]]$  that maps each polynomial  $f \in R[X]$  onto the power series  $(f_k)_{k \in \mathbb{N}}$  is an injective algebra homomorphism; it is used to identify  $R[X]$  with a subalgebra of  $R[[X]]$ . With this identification, any power series  $A = (A_k)_{k \in \mathbb{N}}$  may be expressed as the infinite sum  $\sum_{k \in \mathbb{N}} A_k$ , and it is this notation that is generally used.

It is easy to see that  $A$  is an invertible element of  $R[[X]]$  if and only if  $h_0(A)$  is an invertible element of  $R$ . When this is the case, and we write  $A = h_0(A)(1-B)$ , so that  $v(B) \geq 1$ , then  $A^{-1} = h_0(A)^{-1} \sum_{k \in \mathbb{N}} B^k$ , the infinite sum obviously being meaningful.

If  $I = I_1 \cup I_2$  and  $I_1 \cap I_2 = \emptyset$ , there is an obvious  $R$ -algebra isomorphism  $R[[X_i]_{i \in I}] \approx R[[X_i]_{i \in I_1}] [[X_i]_{i \in I_2}]$ , by means of which the two algebras are usually identified.

Let  $R[[X']] = R[[X'_i]_{i \in I'}]$  also be a power series algebra over  $R$ , and let  $P = (P_i)_{i \in I}$  be a family, with set of indices  $I$ , of power series in  $R[[X']]$  such that  $v(P_i) \geq 1$  for each  $i$ . If  $A = (A_k)_{k \in \mathbb{N}}$  is any element of  $R[[X]]$ , then  $A_k(P)$  is an element of  $R[[X']]$  of series order greater than or equal to  $k$ , so that the infinite sum  $\sum_{k \in \mathbb{N}} A_k(P)$ , which we denote by  $A(P)$ , is meaningful.

It is easy to see that the mapping that to each  $A \in R[[X]]$  associates the element  $A(P) \in R[[X']]$  is an algebra homomorphism  $R[[X]] \rightarrow R[[X']]$ ; we call it the *substitution of  $P$  for  $X$* . When each  $P_i$  is a polynomial, this homomorphism extends the ordinary substitution homomorphism  $R[X] \rightarrow R[P] \subset R[X']$  of polynomial algebras.

If  $D$  is any derivation of the polynomial ring  $R[X]$ , then, for any homogeneous polynomial  $H \in R[X]$ ,  $v(DH) \geq v(H) - 1$ . It follows that, for any  $A \in R[[X]]$ , the infinite sum  $\sum_{k \in \mathbb{N}} Dh_k(A)$  is meaningful. Therefore  $D$  can be extended to a mapping of  $R[[X]]$  into itself, that we still denote by  $D$ , by the formula  $DA = \sum_{k \in \mathbb{N}} Dh_k(A)$ . This extension is a derivation of  $R[[X]]$  (called the *canonical extension* of the given derivation). If  $D_1, D_2$  are two derivations of  $R[X]$  and if they commute, then so do their canonical extensions to  $R[[X]]$ .

These remarks apply, in particular, to the partial derivations  $\partial/\partial X_i$  ( $i \in I$ ). Consider a power series  $A \in R[[X]]$ , and let  $P = (P_i)_{i \in I}$  and  $Q = (Q_i)_{i \in I}$  be two families of elements of  $R[[X']]$  such that  $v(P_i) \geq 1$ ,  $v(Q_i) \geq 1$  ( $i \in I$ ) and such that  $Q_i = 0$  for all but finitely many indices  $i$ . Let  $\mathfrak{q}$  denote the ideal of  $R[[X']]$  generated by all the power series  $Q_i$ . Then, substituting  $P+Q$  for  $X$ , we obtain the congruence

$$A(P+Q) \equiv A(P) + \sum_{i \in I} \frac{\partial A}{\partial X_i}(P) Q_i \pmod{\mathfrak{q}^2}.$$

Indeed, since this congruence holds when  $A$  is a polynomial in  $R[X]$ , the general case may be proved by considering separately each of the homogeneous parts of  $A$ .

We now describe an implicit function theorem for power series. To facilitate the description let  $J$  be a finite subset of  $I$ , say the set consisting of the  $q$  indices  $i_1, \dots, i_q$ , put  $Y_j = X_{i_j}$  ( $1 \leq j \leq q$ ), and let  $K = I - J$ , so that we may use the self-explanatory notation  $R[[X, Y_1, \dots, Y_q]] = R[[X_i]_{i \in K}, Y_1, \dots, Y_q]$  for what we have heretofore been denoting by  $R[[X]]$ . The result can now be stated as follows.

**Proposition 8** (Implicit function theorem) *If  $F_1, \dots, F_q \in R[[X, Y_1, \dots, Y_q]]$  and  $F_j((0), 0, \dots, 0) = 0$  ( $1 \leq j \leq q$ ), and if*

$$\det((\partial F_j / \partial Y_{j'})((0), 0, \dots, 0))_{1 \leq j \leq q, 1 \leq j' \leq q}$$

*is an invertible element of  $R$ , then there exist unique power series  $P_1, \dots, P_q \in R[[X]] = R[[X_i]_{i \in K}]$  such that:*

- (a)  $P_j((0)) = 0$  ( $1 \leq j \leq q$ );
- (b)  $F_j(X, P_1, \dots, P_q) = 0$  ( $1 \leq j \leq q$ ).

*These power series have the further property that the ideals  $(F_1, \dots, F_q)$  and  $(Y_1 - P_1, \dots, Y_q - P_q)$  of  $R[[X, Y_1, \dots, Y_q]]$  coincide.*

*Proof* The power series are obtained by an inductive construction. Suppose that for each  $j$  with  $1 \leq j \leq q$  we have polynomials  $P_{j,0}, \dots, P_{j,k-1} \in R[[X]]$ , with  $P_{j,0} = 0$  and  $P_{j,\kappa}$  homogeneous of degree  $\kappa$  ( $1 \leq \kappa \leq k-1$ ), such that  $v(F_j(X, \sum_{0 \leq \kappa < k} P_{1,\kappa}, \dots, \sum_{0 \leq \kappa < k} P_{q,\kappa})) \geq k$  ( $1 \leq j \leq q$ ). If  $P_{j,k}$  ( $1 \leq j \leq q$ ) are any  $q$  homogeneous polynomials in  $R[[X]]$  of degree  $k$ , then

$$F_j \left( X, \sum_{0 \leq \kappa \leq k} P_{1,\kappa}, \dots, \sum_{0 \leq \kappa \leq k} P_{q,\kappa} \right) \equiv F_j \left( X, \sum_{0 \leq \kappa < k} P_{1,\kappa}, \dots, \sum_{0 \leq \kappa < k} P_{q,\kappa} \right) + \sum_{1 \leq j' \leq q} \partial F_j / \partial Y_{j'} \left( X, \sum_{0 \leq \kappa < k} P_{1,\kappa}, \dots, \sum_{0 \leq \kappa < k} P_{q,\kappa} \right) P_{j',k} \pmod{\mathfrak{p}_k^2},$$

where  $\mathfrak{p}_k$  denotes the ideal  $(P_{1,k}, \dots, P_{q,k})$  of  $R[[X]]$ , so that

$$v \left( F_j \left( X, \sum_{0 \leq \kappa \leq k} P_{1,\kappa}, \dots, \sum_{0 \leq \kappa \leq k} P_{q,\kappa} \right) \right) \geq k$$

and

$$F_j \left( X, \sum_{0 \leq \kappa \leq k} P_{1,\kappa}, \dots, \sum_{0 \leq \kappa \leq k} P_{q,\kappa} \right) \equiv h_k \left( F_j \left( X, \sum_{0 \leq \kappa \leq k} P_{1,\kappa}, \dots, \sum_{0 \leq \kappa \leq k} P_{q,\kappa} \right) \right) + \sum_{1 \leq j' \leq q} \partial F_j / \partial Y_{j'}((0, 0, \dots, 0)) P_{j',k} \pmod{\mathfrak{m}^{k+1}},$$

where  $\mathfrak{m}$  is the ideal of  $R[[X]]$  generated by all the  $X_i$  with  $i \in K$ . It follows that if we let  $(\varphi_{j,j'})_{1 \leq j \leq q, 1 \leq j' \leq q}$  denote the inverse of the invertible matrix  $((\partial F_j / \partial Y_{j'})((0, 0, \dots, 0)))_{1 \leq j \leq q, 1 \leq j' \leq q}$ , and if we take

$$P_{j,k} = - \sum_{1 \leq j' \leq q} \varphi_{j,j'} h_k \left( F_{j'} \left( X, \sum_{0 \leq \kappa < k} P_{1,\kappa}, \dots, \sum_{0 \leq \kappa < k} P_{q,\kappa} \right) \right),$$

then

$$v \left( F_j \left( X, \sum_{0 \leq \kappa \leq k} P_{1,\kappa}, \dots, \sum_{0 \leq \kappa \leq k} P_{q,\kappa} \right) \right) \geq k + 1 \quad (1 \leq j \leq q).$$

Thus, starting with  $P_{j,0} = 0$  ( $1 \leq j \leq q$ ), we can define all the  $P_{j,k}$  ( $1 \leq j \leq q$ ,  $k \in \mathbb{N}$ ) by induction on  $k$ , and it is clear that if we set  $P_j = \sum_{k \in \mathbb{N}} P_{j,k}$  ( $1 \leq j \leq q$ ), then conditions (a) and (b) are satisfied.

It remains to verify the last statement of the proposition (which implies the uniqueness of  $P_1, \dots, P_q$ ). Working in the ring  $R[[X, Y_1, \dots, Y_q]]$  we have

$$\begin{aligned} 0 &= F_j(X, P_1, \dots, P_q) \\ &= F_j(X, Y_1 + P_1 - Y_1, \dots, Y_q + P_q - Y_q) \\ &\equiv F_j + \sum_{1 \leq j' \leq q} \partial F_j / \partial Y_{j'} \cdot (P_{j'} - Y_{j'}) \pmod{(Y_1 - P_1, \dots, Y_q - P_q)^2}, \end{aligned}$$

whence

$$F_j = \sum_{1 \leq j' \leq q} ((\partial F_j / \partial Y_{j'})((0, 0, \dots, 0) + M_{j,j'})(Y_{j'} - P_{j'}) \quad (1 \leq j \leq q),$$

where  $M_{j,j'} \in R[[X, Y_1, \dots, Y_q]]$  and  $v(M_{j,j'}) \geq 1$ . Therefore it suffices to show that the matrix  $((\partial F_j / \partial Y_{j'})((0, 0, \dots, 0) + M_{j,j'}))$  is invertible over  $R[[X, Y_1, \dots, Y_q]]$ . However, this is immediate since the homogeneous part of degree 0 of the determinant of this matrix is the invertible element

$$\det((\partial F_j / \partial Y_{j'})((0, 0, \dots, 0))).$$

We conclude this review with some remarks about power series algebras  $R[[X]]$  in a single indeterminate. In this case  $R[[X]]$  can be embedded in an algebra  $R((X))$  consisting of all power series  $\sum_{k \in \mathbb{Z}} a_k X^k$  in  $X$  over  $R$  for which there are only finitely many negative indices  $k$  with  $a_k \neq 0$ . Then  $R((X))$  can be considered as the ring of quotients of  $R[[X]]$  over the multiplicatively stable set consisting of all the powers  $X^k$  ( $k \in \mathbb{N}$ ). The series-order function on  $R[[X]]$  extends in an obvious way to a function, still denoted by  $v$  and still called "series-order," on  $R((X))$ . For any series  $A = \sum_{k \in \mathbb{Z}} a_k X^k$  the elements  $a_k \in R$  are called the *coefficients* in  $A$ ; if  $A \neq 0$ , then we call  $a_{v(A)}$  the *leading coefficient* in  $A$ . We shall often denote the leading coefficient of a nonzero power series  $A$  by  $J_A$ . Thus,  $A = J_A X^{v(A)} + \dots$  where the dots stand for a power series of series-order greater than  $v(A)$ . It is evident that  $A$  is invertible in  $R((X))$  if and only if  $J_A$  is invertible in  $R$ . In particular, if  $R$  is a field, then so is  $R((X))$ .

## 14 Specializations

Let  $R$  be an integral domain. A homomorphism of  $R$  into a field is called a *specialization* of  $R$ . If a subring  $R_0$  of  $R$  is a subring of the field, too, and if the homomorphism maps each element of  $R_0$  onto itself, the specialization is said to be *over*  $R_0$ . If  $x = (x_i)_{i \in I}$  and  $x' = (x'_i)_{i \in I}$  are families of elements of  $R$  and of the field, respectively, and the homomorphism maps  $x_i$  onto  $x'_i$  for each  $i \in I$ , then  $x$  is said to *specialize* to  $x'$  (under the specialization in question). If  $x$  and  $x'$  are families of elements of  $R$  and of a field  $L$ , respectively, such that  $x$  specializes to  $x'$  under some specialization of  $R_0[x]$  into  $L$  over  $R_0$ , then we also say that  $x'$  is a *specialization of  $x$  over  $R_0$* . If  $x'$  is a specialization of  $x$  over  $R_0$  such that  $x$  is a specialization of  $x'$  over  $R_0$ , we say that  $x'$  is a *generic specialization of  $x$  over  $R_0$* . A necessary and sufficient condition that  $x'$  be a specialization (respectively a generic specialization) of  $x$  over  $R_0$  is that the defining ideal of  $x$  in a polynomial algebra  $R_0[[X_i]_{i \in I}]$  be contained in (respectively be equal to) the defining ideal of

$x'$  in this algebra. When this is the case then the specialization  $R_0[x] \rightarrow L$  over  $R_0$  under which  $x$  specializes to  $x'$  is unique, and induces a surjective  $R_0$ -homomorphism (respectively  $R_0$ -isomorphism)  $R_0[x] \rightarrow R_0[x']$ .

If  $R \rightarrow L$  is a specialization of  $R$  into a field  $L$ , the kernel  $\mathfrak{p}$  is prime so that the subset  $R - \mathfrak{p}$  of  $R$  is multiplicatively stable. The local ring  $R_{\mathfrak{p}} = (R - \mathfrak{p})^{-1}R$  is also an integral domain, and may be considered to be an overring of  $R$ . The specialization  $R \rightarrow L$  can be extended to a unique specialization  $R_{\mathfrak{p}} \rightarrow L$ ; its kernel is the maximal ideal of  $R_{\mathfrak{p}}$ , so that the specialization maps  $R_{\mathfrak{p}}$  onto a subfield of  $L$ .

A specialization of a ring into  $L$  followed by the inclusion mapping of  $L$  into some overfield  $L'$  is a specialization of the ring into  $L'$ . We sometimes do not distinguish between these two specializations of the ring (when this does not lead to difficulty). If  $R \rightarrow L$  is a specialization of  $R$  with kernel  $\mathfrak{p}$ , then restriction to a subring  $R_0$  gives a specialization of  $R_0$  with kernel  $\mathfrak{p} \cap R_0$ . Conversely, if we are given a specialization of  $R_0$  with kernel  $\mathfrak{p}_0$  and if there exists a prime ideal  $\mathfrak{p}$  of  $R$  with  $\mathfrak{p} \cap R_0 = \mathfrak{p}_0$ , then the given specialization of  $R_0$  can be extended to a specialization of  $R$  with kernel  $\mathfrak{p}$ .

The key to the problem of when a specialization can be extended is the following observation (known as *Nakayama's lemma*): *If an ideal  $\mathfrak{a}$  is contained in every maximal ideal of the ring  $R$ , and  $M$  is a finitely generated  $R$ -module such that  $\mathfrak{a}M = M$ , then  $M = 0$ .* Indeed, if  $M$  is generated by  $x_1, \dots, x_n$  with  $n > 0$ , then we may write  $x_n = \sum_{1 \leq j \leq n} c_j x_j$ , where each  $c_j \in \mathfrak{a}$ , so that  $(1 - c_n)x_n \in \sum_{1 \leq j \leq n-1} R x_j$ . However,  $1 - c_n$ , like every element of  $R$  not in any maximal ideal, is invertible in  $R$ , so that  $x_n \in \sum_{1 \leq j \leq n-1} R x_j$  and  $M$  is generated by  $x_1, \dots, x_{n-1}$ . Thus, the result follows by induction on  $n$ .

**Proposition 9** *Let  $R_0$  and  $R$  be subrings of a field, with  $R_0 \subset R$ .*

(a) *If  $R$  is integral over  $R_0$ , then every specialization of  $R_0$  into an algebraically closed field  $L$  can be extended to a specialization of  $R$  into  $L$ .*

(b) *Let  $x \in R$ . If a specialization  $f_0: R_0 \rightarrow L$  into an algebraically closed field  $L$  cannot be extended to a specialization  $R_0[x] \rightarrow L$ , then  $f_0$  can be extended to a unique specialization  $f: R_0[x^{-1}] \rightarrow L$ , and  $f(x^{-1}) = 0$ .*

(c) *If  $R$  is finitely generated (respectively finitely generated and separable) over  $R_0$  and  $u$  is a nonzero element of  $R$ , then there exists a nonzero element  $u_0 \in R_0$  with the following property: Every specialization  $f_0: R_0 \rightarrow L$  into an algebraically closed (respectively a separably closed) field  $L$  such that  $f_0(u_0) \neq 0$  can be extended to a specialization  $f: R \rightarrow L$  such that  $f(u) \neq 0$  (respectively such that  $f(u) \neq 0$  and  $f(R)$  is separable over  $f(R_0)$ ).*

*Proof* (a) Let  $\mathfrak{p}_0$  be the kernel of a specialization  $f_0: R_0 \rightarrow L$ , and suppose first that  $R = R_0[x]$  for some element  $x \in R$ . Replacing  $R_0$  by the local ring  $(R_0)_{\mathfrak{p}_0}$ , we may suppose that  $R_0$  itself is a local ring and that  $\mathfrak{p}_0$

is its maximal ideal. Since  $x$  is integral over  $R_0$ ,  $R$  is a finitely generated  $R_0$ -module, and by Nakayama's lemma,  $R\mathfrak{p}_0 \neq R$ ; hence the ideal  $R\mathfrak{p}_0$  of  $R$  is contained in a maximal ideal  $\mathfrak{p}$ . By the maximality of  $\mathfrak{p}_0$  we have  $\mathfrak{p} \cap R_0 = \mathfrak{p}_0$ . Therefore  $f_0$  can be extended to a specialization of  $R = R_0[x]$  into  $L$ . This case settled, we no longer suppose that  $R$  is generated over  $R_0$  by a single element. The set  $\mathfrak{M}$  of all pairs  $(R', f')$ , where  $R'$  is a ring with  $R_0 \subset R' \subset R$  and  $f'$  is a specialization of  $R'$  into  $L$  extending  $f_0$ , can be ordered by defining  $(R', f') \leq (R'', f'')$  to mean that  $R' \subset R''$  and  $f''$  is an extension of  $f'$ . Zorn's lemma then shows that there exists a maximal element  $(R', f')$  of  $\mathfrak{M}$ . If  $R'$  were not  $R$ , there would exist an element  $x \in R - R'$ , and of course  $R'[x]$  would be integral over  $R'$ . By the case already treated,  $f'$  could be extended to a specialization  $f'': R'[x] \rightarrow L$ , contradicting the maximality of  $(R', f')$ ; hence  $R' = R$ .

(b) Let  $\mathfrak{q}$  denote the defining ideal of  $x$  in the polynomial algebra  $R_0[X]$ . The mapping  $F \mapsto F^{f_0}$  of  $R_0[X]$  into  $f_0(R_0)[X]$  is a surjective homomorphism  $g: R_0[X] \rightarrow f_0(R_0)[X]$ , and therefore maps  $\mathfrak{q}$  into an ideal  $g(\mathfrak{q}) = \mathfrak{q}^{f_0}$  of  $f_0(R_0)[X]$ . If  $\mathfrak{q}^{f_0} \cap f_0(R_0) = (0)$ , then  $\mathfrak{q}^{f_0}$  has a zero  $x'$  in  $L$ . The homomorphism  $g$  followed by the substitution of  $x'$  for  $X$  is a homomorphism  $R_0[X] \rightarrow L$  with kernel containing  $\mathfrak{q}$ , and therefore induces a homomorphism  $R_0[x] \rightarrow L$ , that is, a specialization which evidently extends  $f_0$ . Thus, if  $f_0$  cannot be extended to a specialization  $R_0[x] \rightarrow L$ , then  $\mathfrak{q}^{f_0} \cap f_0(R_0) \neq (0)$ . Letting  $\mathfrak{p}_0$  denote the kernel of  $f_0$ , we see in this case that  $f_0(a) = \sum f_0(b_j) X^j$  for some  $a \in R_0 - \mathfrak{p}_0$  and some  $\sum b_j X^j \in \mathfrak{q}$ , so that  $a = \sum b_j X^j + \sum p_j X^j$ , where each  $p_j$  is in  $\mathfrak{p}_0$ . Substituting  $x$  for  $X$  we find that  $a = \sum p_j x^j$ , so that  $(p_0 - a)x^{-n} + p_1 x^{-n+1} + \dots + p_n = 0$ . It follows from this equation that  $x^{-1}$  is integral over the local ring  $(R_0)_{\mathfrak{p}_0}$ . Since  $f_0$  can be extended to a specialization  $f': (R_0)_{\mathfrak{p}_0} \rightarrow L$ , and, by part (a),  $f'$  can be extended to a specialization  $(R_0)_{\mathfrak{p}_0}[x^{-1}] \rightarrow L$ , we conclude that  $f_0$  can be extended to a specialization  $f: R_0[x^{-1}] \rightarrow L$ . It also follows from the same equation that, for any such  $f$ ,  $f(x^{-1}) = 0$ , so that  $f$  is unique.

(c) It follows from the hypothesis that there exist finitely many elements  $x_1, \dots, x_n \in R$  such that  $R = R_0[x_1, \dots, x_n]$  (respectively such that  $R = R_0[x_1, \dots, x_n]$  and  $R_0[x_1, \dots, x_j]$  is separable over  $R_0[x_1, \dots, x_{j-1}]$  ( $1 \leq j \leq n$ )). Hence a simple induction argument allows us to assume that  $n = 1$ , so that we may write  $R = R_0[x]$ . Then there exists a polynomial  $G \in R_0[X]$  with  $u = G(x)$ . If  $x$  is transcendental over  $R_0$ , it is easy to see that we may take for  $u_0$  any one of the nonzero coefficients in  $G$ . Therefore we may suppose that  $x$  is algebraic over  $R_0$  of degree, say  $m$ , and may let  $F = a_0 X^m + \dots$  denote an element of  $R_0[X]$  of degree  $m$  vanishing at  $x$ . The ideal  $(F, G)$  (respectively the ideal  $(F, (dF/dX)G)$ ) of  $R_0[X]$  contains a nonzero element  $b_0 \in R_0$ . Let  $u_0 = a_0 b_0$ . If  $f_0: R_0 \rightarrow L$  is any specialization with  $f_0(u_0) \neq 0$  and  $L$  algebraically closed (respectively  $L$  separably closed),

then  $f_0$  can be extended to a specialization  $f_0' : R_0[a_0^{-1}] \rightarrow L$ . As  $x$  is integral over  $R_0[a_0^{-1}]$ , part (a) shows that  $f_0'$  can be extended to a specialization  $f'$  of  $R_0[a_0^{-1}, x]$  into  $L$  (respectively into the algebraic closure  $L_a$  of  $L$ ). Since  $f'(u_0) \neq 0$  and  $F'$  vanishes at  $f'(x)$ , it is clear that  $G^{f'}$  (respectively  $((dF/dX)G)^{f'}$ ) does not vanish at  $f'(x)$ , so that  $f'(u) \neq 0$  (respectively  $f'(u) \neq 0$  and  $f'(R_0[x])$  is separable over  $f'(R_0)$ , whence  $f'(R_0[x]) \subset L$ ).

The following lemma is used in the proof of the succeeding one concerning the behavior of a prime ideal under specialization.

**Lemma 13** *Let  $R$  be an integral domain, let  $(X_1, \dots, X_n)$  be a finite family of indeterminates over  $R$ , and let  $A_j$  be a polynomial in  $R[X_1, \dots, X_j]$  not in  $R[X_1, \dots, X_{j-1}]$  ( $1 \leq j \leq n$ ). Let  $m_j = \deg_{X_j} A_j$  and let  $I_j$  denote the coefficient of  $X_j^{m_j}$  in  $A_j$  (when  $A_j$  is considered as a polynomial in  $X_j$ ). Assume that  $\deg_{X_i} A_j < m_i$  ( $1 \leq i < j \leq n$ ), that  $(A_1, \dots, A_{j-1}, I_j) \cap R \neq (0)$  ( $1 \leq j \leq n$ ), and that  $(A_1, \dots, A_j, \partial A_j / \partial X_j) \cap R \neq (0)$  ( $1 \leq j \leq n$ ). Then the ideal  $\mathfrak{a} = (A_1, \dots, A_n) : (I_1 \cdots I_n)^\infty$  of  $R[X_1, \dots, X_n]$  is separable over  $R$  and does not contain a nonzero element  $F$  such that  $\deg_{X_j} F < m_j$  for every index  $j$ .*

*Proof* We first prove the contention that  $\mathfrak{a}$  does not contain an element  $F \neq 0$  with  $\deg_{X_j} F < m_j$  ( $1 \leq j \leq n$ ). Indeed, suppose that  $F \in \mathfrak{a}$  and  $\deg_{X_j} F < m_j$  ( $1 \leq j \leq n$ ). For some  $h \in \mathbb{N}$  we may write  $(I_1 \cdots I_n)^h F = \sum_{1 \leq j \leq n} C_j A_j$ , where  $C_j \in R[X_1, \dots, X_n]$ . Dividing each  $C_j$  by  $A_n$  we obtain equations  $I_n^k C_j = D_j + E_j A_n$  ( $1 \leq j \leq n-1$ ), where  $D_j, E_j \in R[X_1, \dots, X_n]$  and  $\deg_{X_n} D_j < m_n$ , so that the polynomial  $(I_1 \cdots I_n)^h I_n^k F - \sum_{1 \leq j \leq n-1} D_j A_j$  is divisible by  $A_n$ . As the degree of this polynomial in  $X_n$  is less than  $m_n$ , it must vanish, so that  $I_n^{h+k} F \in (A_1, \dots, A_{n-1}) : (I_1 \cdots I_{n-1})^\infty$ . Since the ideal  $(A_1, \dots, A_{n-1}, I_n)$  contains a nonzero element  $a \in R$ , we may write  $a^{h+k} F \in (A_1, \dots, A_{n-1}) : (I_1 \cdots I_{n-1})^\infty$ . If either  $n = 1$ , or  $n > 1$  and we suppose the contention true for  $n-1$  instead of  $n$  (and  $R[X_n]$  instead of  $R$ ), this relation shows that  $F = 0$ . This proves the contention in general.

It remains to show the ideal  $\mathfrak{a}$  is separable over  $R$ . We denote the field of quotients of  $R$  by  $K$ . For any  $F \in K[X_1, \dots, X_n]$ , we may divide  $F$  in succession by  $A_n, \dots, A_1$  to obtain a relation  $I_1^{q_1} \cdots I_n^{q_n} F = F_0 + \sum_{1 \leq j \leq n} C_j A_j$ , where  $F_0, C_1, \dots, C_n \in K[X_1, \dots, X_n]$  and  $\deg_{X_j} F_0 < m_j$  ( $1 \leq j \leq n$ ); furthermore, if  $F$  has all its coefficients in  $R$ , then so do  $F_0, C_1, \dots, C_n$ , and  $F \in \mathfrak{a} \Leftrightarrow F_0 \in \mathfrak{a}$ . It follows that an element of  $R[X_1, \dots, X_n]$  is in  $\mathfrak{a}$  if and only if it is in the ideal  $(A_1, \dots, A_n) : (I_1 \cdots I_n)^\infty$  of the ring  $K[X_1, \dots, X_n]$ . It follows from this that in the rest of the proof we may replace  $R$  by  $K$ , that is, we may suppose that  $R$  is a field.

This being done, we next show that we may assume that  $A_1$  is irreducible over  $R$ . Indeed, suppose that  $A_1 = A_{11} A_{21}$ , where  $A_{11}$  and  $A_{21}$  are in

$R[X_1]$  but not in  $R$ . Writing  $m_{h1} = \deg_{X_1} A_{h1}$  ( $h = 1, 2$ ), and letting  $I_{h1}$  denote the coefficient of  $X_1^{m_{h1}}$  in  $A_{h1}$  ( $h = 1, 2$ ), we see that  $I_1 = I_{11} I_{21}$ . Now, if  $x_1, \dots, x_{i-1}$  are elements of a field extension of  $R$  such that  $A_i(x_1) = 0, \dots, A_{i-1}(x_1, \dots, x_{i-1}) = 0$ , then, because  $(A_1, \dots, A_{i-1}, I_i) \cap R \neq (0)$ , we have  $I_i(x_1, \dots, x_{i-1}) \neq 0$ , so that there exists an element  $x_i$  of a larger field extension such that  $A_i(x_1, \dots, x_i) = 0$ ; it follows that for any root  $x_1$  of  $A_1$  and any  $A_j$  with  $j > 1$  we have  $I_j(x_1, X_2, \dots, X_{j-1}) \neq 0$ . In particular,  $I_j$  is not divisible by  $A_{h1}$  ( $2 \leq j \leq n$ ), and a similar argument shows that  $\partial A_j / \partial X_j$  is not divisible by  $A_{h1}$  ( $2 \leq j \leq n$ ). Dividing  $A_j$  by  $A_{h1}$  we therefore find a congruence  $A_j \equiv A_{hj} \pmod{A_{h1}}$ , where  $A_{hj} \neq 0$ ,  $\deg_{X_1} A_{hj} < m_{h1}$ ,  $\deg_{X_i} A_{hj} < m_i$  ( $1 < i < j$ ), and  $\deg_{X_j} A_{hj} = m_j$ ; furthermore, if we denote the coefficient of  $X_j^{m_j}$  in  $A_{hj}$  (considered as a polynomial in  $X_j$ ) by  $I_{hj}$ , then  $I_j \equiv I_{hj} \pmod{A_{h1}}$ , and also  $\partial A_j / \partial X_j \equiv \partial A_{hj} / \partial X_j \pmod{A_{h1}}$ . It follows that  $A_{h1}, \dots, A_{nn}$  and the ideal  $\mathfrak{a}_h = (A_{h1}, \dots, A_{nn}) : (I_{h1} \cdots I_{nn})^\infty$  satisfy the hypothesis of the lemma. However, the condition  $(A_1, \partial A_1 / \partial X_1) \cap R \neq (0)$  implies, since  $R$  is now a field, the condition  $1 \in (A_{11}, A_{21})$ , and therefore

$$\begin{aligned} (A_1, \dots, A_n) &= (A_{11}, A_2, \dots, A_n) \cap (A_{21}, A_2, \dots, A_n) \\ &= (A_{11}, A_{12}, \dots, A_{1n}) \cap (A_{21}, A_{22}, \dots, A_{2n}); \end{aligned}$$

since evidently  $(A_{h1}, \dots, A_{nn}) : (I_1 \cdots I_n)^\infty = (A_{h1}, \dots, A_{nn}) : (I_{h1} \cdots I_{nn})^\infty$ , this implies that  $\mathfrak{a} = \mathfrak{a}_1 \cap \mathfrak{a}_2$ . Thus, to prove that  $\mathfrak{a}$  is separable it suffices to prove that  $\mathfrak{a}_1$  and  $\mathfrak{a}_2$  are separable. It follows from this that in proving a separable we may assume that  $A_1$  is irreducible over  $R$ .

Let  $x_1$  be a root of  $A_1$  in some field extension of  $R$ . The substitution of  $x_1$  for  $X_1$  is a surjective homomorphism  $R[X_1, X_2, \dots, X_n] \rightarrow R[x_1, X_2, \dots, X_n]$  over  $R[X_2, \dots, X_n]$  (and therefore over  $R$ ), with prime kernel  $(A_1)$  which is contained in  $\mathfrak{a}$ ; it maps  $A_j$  onto the polynomial  $B_j = A_j(x_1, X_2, \dots, X_j)$  of the polynomial algebra  $R(x_1)[X_2, \dots, X_n]$  over  $R(x_1)$ , and maps  $\mathfrak{a}$  onto the ideal  $\mathfrak{b} = (B_2, \dots, B_n) : (J_2 \cdots J_n)^\infty$  of  $R(x_1)[X_2, \dots, X_n]$ ,  $J_j$  here denoting  $I_j(x_1, X_2, \dots, X_{j-1})$ . If  $n = 1$ , then  $\mathfrak{b} = (0)$ , which is separable over  $R(x_1)$  and therefore over  $R$ , since  $R(x_1)$  is separable over  $R$ . It follows in this case (for example by Section 10, Lemma 10(a)) that  $\mathfrak{a}$  is separable over  $R$ . If  $n > 1$ , we verify without difficulty that  $B_2, \dots, B_n$  and  $\mathfrak{b}$  satisfy the hypothesis of the present lemma, so that if we assume the lemma proved for  $n-1$  instead of  $n$  (and  $R(x_1)$  instead of  $R$ ), then  $\mathfrak{b}$  is separable over  $R(x_1)$  and therefore over  $R$ . Again it follows that  $\mathfrak{a}$  is separable over  $R$ . This completes the proof.

**Lemma 14** *Let  $R$  be an integral domain, let  $R[X_1, \dots, X_n]$  be a finitely generated polynomial algebra over  $R$ , let  $\mathfrak{p}$  be an  $R$ -separable prime ideal of  $R[X_1, \dots, X_n]$  with  $\mathfrak{p} \cap R = (0)$ , and let  $U \in R[X_1, \dots, X_n]$ ,  $U \notin \mathfrak{p}$ . Then there exist a nonzero element  $u \in R$  and a polynomial  $D \in R[X_1, \dots, X_n]$  with the*



following property: For every specialization  $f$  of  $R$  with  $f(u) \neq 0$ , the ideal  $p^f : (D^f)^\infty$  of the polynomial algebra  $f(R)[X_1, \dots, X_n]$  is  $f(R)$ -separable and does not contain  $a' U^f D^f$  for any nonzero element  $a' \in f(R)$ .

*Proof* Let  $K$  be the field of quotients of  $R$ . Then  $Kp$  is a  $K$ -separable prime ideal of  $K[X_1, \dots, X_n]$ , and  $(Kp) \cap R[X_1, \dots, X_n] = p$ . Let  $(x_1, \dots, x_n)$  be a generic zero of  $Kp$ . Then  $U(x_1, \dots, x_n) \neq 0$ . Also,  $K(x_1, \dots, x_n)$  is separable over  $K$ . Permuting the indices, we may suppose that  $(x_1, \dots, x_d)$  is a separating transcendence basis of  $K(x_1, \dots, x_n)$  over  $K$  ( $d$  denoting the dimension of  $Kp$ ). For each  $x_j$  with  $d < j \leq n$  let  $m_j = [K(x_1, \dots, x_j) : K(x_1, \dots, x_{j-1})]$ . Then  $p$  contains nonzero polynomials  $A_j \in R[X_1, \dots, X_j]$  ( $d < j \leq n$ ) such that  $\deg_{X_j} A_j = m_j$  ( $d < j \leq n$ ) and  $\deg_{X_i} A_j < m_i$  ( $d < i < j \leq n$ ), and  $Kp$  does not contain a nonzero element  $F$  with  $\deg_{X_j} F < m_j$  ( $d < j \leq n$ ). If we let  $I_j$  denote the coefficient of  $X_j^{m_j}$  in  $A_j$  (considered as a polynomial in  $X_j$ ), then it is not difficult to see that

$$\begin{aligned} p &= (A_{d+1}, \dots, A_n) : (I_{d+1} \cdots I_n)^\infty && \text{in } R[X_1, \dots, X_n], \\ Kp &= (A_{d+1}, \dots, A_n) : (I_{d+1} \cdots I_n)^\infty && \text{in } K[X_1, \dots, X_n]. \end{aligned}$$

We shall now show that if  $C \in R[X_1, \dots, X_j]$  and  $C \notin p$ , then the ideal  $(A_{d+1}, \dots, A_j, C)$  of  $R[X_1, \dots, X_j]$  contains a polynomial in  $R[X_1, \dots, X_{j-1}]$  not in  $p$ . It follows by induction that  $(A_{d+1}, \dots, A_j, C)$  contains a nonzero element of  $R[X_1, \dots, X_d]$ . In the first place, the ideal  $(A_{d+1}, \dots, A_j) : (I_{d+1} \cdots I_j)^\infty$  of  $K[X_1, \dots, X_j]$  coincides with  $Kp \cap K[X_1, \dots, X_j]$  and hence is prime, and evidently has dimension  $d$ . Each component of the perfect ideal generated by this prime ideal and  $C$  is a strictly larger prime ideal, therefore (by Section 11, Proposition 4) has dimension less than  $d$ , and hence contains a nonzero polynomial in  $K[X_1, \dots, X_d]$ . The product of all these polynomials (one for each component), is in the perfect ideal. Raising to a sufficiently high power, and then multiplying by a suitable element of  $R$ , we obtain a nonzero element of  $R[X_1, \dots, X_d]$  that is in the ideal  $(A_{d+1}, \dots, A_j) : (I_1 \cdots I_j)^\infty + (C)$  of  $R[X_1, \dots, X_j]$ . Multiplying by a high power of  $I_1 \cdots I_j$ , we obtain, finally, an element of the ideal  $(A_{d+1}, \dots, A_j, C)$  that is in  $R[X_1, \dots, X_{j-1}]$  but not in  $p$ .

It follows that the product of the  $2(n-d)$  ideals  $(A_{d+1}, \dots, A_{j-1}, I_j)$  ( $d < j \leq n$ ) and  $(A_{d+1}, \dots, A_j, \partial A_j / \partial X_j)$  ( $d < j \leq n$ ) of  $R[X_1, \dots, X_n]$  contains a nonzero polynomial  $D \in R[X_1, \dots, X_d]$ . Of course,  $D(x_1, \dots, x_d) \neq 0$ .

By Proposition 9(c), there exists a nonzero  $u \in R$  such that every specialization  $f: R \rightarrow L$  with  $f(u) \neq 0$  can be extended to a specialization  $f': R[x_1, \dots, x_n] \rightarrow L_s$  ( $L_s$  denoting the separable closure of  $L$ ) with  $f'(D(x_1, \dots, x_d) U(x_1, \dots, x_n)) \neq 0$ , that is, with  $D^f(f'(x_1), \dots, f'(x_d)) \neq 0$  and  $U^f(f'(x_1), \dots, f'(x_n)) \neq 0$ . For every such  $f$  we see from Lemma 13 (applied to  $f(R)[X_1, \dots, X_d]$ ,  $A_{d+1}^f, \dots, A_n^f$  instead of  $R, A_1, \dots, A_n$ ) that the ideal

$b = (A_{d+1}^f, \dots, A_n^f) : (I_{d+1}^f \cdots I_n^f)^\infty$  of  $f(R)[X_1, \dots, X_n]$  is  $f(R)[X_1, \dots, X_d]$ -separable and contains no nonzero polynomial  $F$  with  $\deg_{X_j} F < m_j$  ( $d < j \leq n$ ). In particular,  $b \cap f(R)[X_1, \dots, X_d] = (0)$ , so that  $b$  is  $f(R)$ -separable. Now,  $D \in (A_{d+1}^f, \dots, A_n^f, I_{d+1}^f \cdots I_n^f)$ ; since  $(f'(x_1), \dots, f'(x_n))$  is obviously a zero of  $(A_{d+1}^f, \dots, A_n^f)$ , we see that it is not a zero of  $I_{d+1}^f \cdots I_n^f$ , and therefore is a zero of  $b$ . Hence  $a' U^f D^f \notin b$  for every nonzero  $a' \in f(R)$ .

We complete the proof by showing that  $b = p^f : (D^f)^\infty$ . It is evident that  $p^f \subset b \subset p^f : (I_{d+1}^f \cdots I_n^f)^\infty \subset p^f : (D^f)^\infty$ , whence  $p^f : (D^f)^\infty = b : (D^f)^\infty$ . However, for any  $F' \in b : (D^f)^\infty$  we can write a congruence  $(I_{d+1}^f)^{i_{d+1}} \cdots (I_n^f)^{i_n} F' \equiv G' \pmod{(A_{d+1}^f, \dots, A_n^f)}$ , where  $G' \in f(R)[X_1, \dots, X_n]$  and  $\deg_{X_j} G' < m_j$  ( $d < j \leq n$ ). For some  $k \in \mathbb{N}$  then  $(D^f)^k G'$  is an element of  $b$  of degree less than  $m_j$  in  $X_j$  ( $d < j \leq n$ ) and therefore vanishes, and from this we readily see that  $F' \in b$ . Hence  $b = b : (D^f)^\infty = p^f : (D^f)^\infty$ .

We conclude this section with a sequence of remarks related to Nakayama's lemma (see discussion leading up to Proposition 9) that will be used in Section 16.

**REMARK 1** (Artin-Rees lemma) *If  $R$  is a Noetherian ring,  $\mathfrak{a}$  is an ideal of  $R$ ,  $M$  is a finitely generated  $R$ -module, and  $N$  is a submodule of  $M$ , then there exists an  $m \in \mathbb{N}$  such that  $(\mathfrak{a}^{m+n}M) \cap N = \mathfrak{a}^n((\mathfrak{a}^mM) \cap N)$  for every  $n \in \mathbb{N}$ . To show this, let  $R'$  denote the set of all polynomials  $\sum a_i T^i \in R[T]$  with  $a_i \in \mathfrak{a}^i$  for every  $i$ . Then  $R'$  is a subring of  $R[T]$ , and if  $x_1, \dots, x_r$  form a set of generators of  $\mathfrak{a}$ , then  $R' = R[x_1 T, \dots, x_r T]$ , so that  $R'$  is Noetherian. Let  $M[T] = \sum_{i \in \mathbb{N}} M T^i$  have the obvious structure of the  $R[T]$ -module, and likewise for  $N[T]$ , and let  $M'$  denote the set of all "polynomials"  $\sum e_i T^i \in M[T]$  with  $e_i \in \mathfrak{a}^i M$  for every  $i$ . Thus  $M'$  is an  $R'$ -module, and if  $f_1, \dots, f_s$  form a set of generators of  $M$ , then  $M' = R'f_1 + \cdots + R'f_s$ , so that the  $R'$ -module  $M'$  is Noetherian. Hence its submodule  $M' \cap N[T]$  is finitely generated, so that for some  $m \in \mathbb{N}$ ,*

$$\begin{aligned} \sum_{i \in \mathbb{N}} ((\mathfrak{a}^i M) \cap N) T^i &= M' \cap N[T] \\ &= R' \cdot \sum_{0 \leq i \leq m} ((\mathfrak{a}^i M) \cap N) T^i \\ &= \sum_{i \in \mathbb{N}} \mathfrak{a}^i T^i \cdot \sum_{0 \leq i \leq m} ((\mathfrak{a}^i M) \cap N) T^i \\ &= \sum_{0 \leq i < m} ((\mathfrak{a}^i M) \cap N) T^i + \sum_{m \leq i < \infty} \mathfrak{a}^{i-m} ((\mathfrak{a}^m M) \cap N) T^i, \end{aligned}$$

whence  $(\mathfrak{a}^{m+n}M) \cap N = \mathfrak{a}^n((\mathfrak{a}^mM) \cap N)$  for every  $n$ .

**REMARK 2** (Krull's theorem) *If the ideal  $\mathfrak{a}$  of the Noetherian ring  $R$  is contained in every maximal ideal, and  $M$  is a finitely generated  $R$ -module,*

then  $\bigcap_{n \in \mathbb{N}} (\mathfrak{a}^n M) = 0$ . Indeed, if we set  $N = \bigcap (\mathfrak{a}^n M)$ , then by the Artin-Rees lemma  $N = (\mathfrak{a}^{m+1} M) \cap N = \mathfrak{a}(\mathfrak{a}^m M) \cap N = \mathfrak{a}N$  for some  $m$ , whence  $N = 0$  by Nakayama's lemma.

We recall that if  $\mathfrak{o}$  is any local ring and  $\mathfrak{m}$  is its maximal ideal, then  $\mathfrak{o}/\mathfrak{m}$  is a field and, for each  $d \in \mathbb{N}$ ,  $\mathfrak{m}^d/\mathfrak{m}^{d+1}$  is a vector space over  $\mathfrak{o}/\mathfrak{m}$ . If  $x_1, \dots, x_m$  form a set of generators of the ideal  $\mathfrak{m}$ , then the cosets of the elements  $x_1^{i_1} \dots x_m^{i_m}$  ( $i_1 + \dots + i_m = d$ ) form a set of generators of the vector space  $\mathfrak{m}^d/\mathfrak{m}^{d+1}$ , so that this vector space has dimension less than or equal to  $\binom{m+d-1}{m-1}$ .

**REMARK 3** If  $\mathfrak{o}$  is a Noetherian local ring,  $\mathfrak{m}$  is its maximal ideal, and  $\mathfrak{m}/\mathfrak{m}^2$  has finite dimension  $m$ , then  $\mathfrak{m}$  has a set of  $m$  generators. Indeed, if  $\mathfrak{m} = \mathfrak{o}x_1 + \dots + \mathfrak{o}x_m + \mathfrak{m}^2$ , then the quotient module  $M = \mathfrak{m}/(\mathfrak{o}x_1 + \dots + \mathfrak{o}x_m)$  satisfies the condition  $\mathfrak{m}M = M$  so that, by Nakayama's lemma,  $M = 0$ , whence  $\mathfrak{m} = \mathfrak{o}x_1 + \dots + \mathfrak{o}x_m$ .

**REMARK 4** If  $\mathfrak{o}$  is a Noetherian local integral domain for which the maximal ideal  $\mathfrak{m}$  has a finite number  $m$  of generators and if  $\mathfrak{o}$  is not integrally closed, then, for some  $d \in \mathbb{N}$ , the vector space  $\mathfrak{m}^d/\mathfrak{m}^{d+1}$  has dimension less than  $\binom{m+d-1}{m-1}$ . Indeed, by hypothesis there exist  $x, y \in \mathfrak{o}$  with  $y \neq 0$  such that  $x/y$  is integral over  $\mathfrak{o}$  and  $x \notin \mathfrak{o}y$ . By Krull's theorem (applied to the local ring  $\mathfrak{o}/\mathfrak{o}y$ , its maximal ideal  $\mathfrak{m}/\mathfrak{o}y$  and the  $\mathfrak{o}/\mathfrak{o}y$ -module  $\mathfrak{o}/\mathfrak{o}y$ ), the element  $x + \mathfrak{o}y \in \mathfrak{o}/\mathfrak{o}y$  is not in the intersection  $\bigcap (\mathfrak{m}/\mathfrak{o}y)^n$ , that is,  $x \notin \bigcap (\mathfrak{m}^n + \mathfrak{o}y)$ , and therefore there is an  $n \in \mathbb{N}$  such that  $x \in \mathfrak{m}^n + \mathfrak{o}y$  and  $x \notin \mathfrak{m}^{n+1} + \mathfrak{o}y$ . Fixing  $w \in \mathfrak{m}^n$  and  $z \in \mathfrak{o}$  such that  $x = w + zy$ , we see that  $w \notin \mathfrak{o}y + \mathfrak{m}^{n+1}$  and  $w/y$  is integral over  $\mathfrak{o}$ . Therefore there exists an  $h \in \mathbb{N}$  such that  $\mathfrak{o}[w/y] = \sum_{0 \leq i \leq h} \mathfrak{o}w^i/y^i$ , whence  $\mathfrak{o}[w/y]y^h \subset \mathfrak{o}$ ; hence for each  $k \in \mathbb{N}$ , there exists an element  $v_k \in \mathfrak{o}$  such that  $w^{h+k} = v_k y^k$ , and by Krull's theorem again, there exist  $r, s_k \in \mathbb{N}$  such that  $y \in \mathfrak{m}^r$ ,  $y \notin \mathfrak{m}^{r+1}$ ,  $v_k \in \mathfrak{m}^{s_k}$ ,  $v_k \notin \mathfrak{m}^{s_k+1}$ . Fixing generators  $x_1, \dots, x_m$  of  $\mathfrak{m}$ , we see that there exist homogeneous polynomials  $R, N, S_k \in \mathfrak{o}[X_1, \dots, X_m]$  of respective degrees  $r, n, s_k$ , none congruent to 0 modulo  $\mathfrak{m}$ , such that  $y = R(x_1, \dots, x_m)$ ,  $w = N(x_1, \dots, x_m)$ ,  $v_k = S_k(x_1, \dots, x_m)$ , and obviously  $N^{h+k} - S_k R^k$  vanishes at  $(x_1, \dots, x_m)$ . If we had  $N^{h+k} \equiv S_k R^k \pmod{\mathfrak{m}}$  for every  $k$ , then  $N$  would be divisible by  $R$  modulo  $\mathfrak{m}$ , that is, for some homogeneous  $Q \in \mathfrak{o}[X_1, \dots, X_m]$  of degree  $n-r$  we would have  $N \equiv QR \pmod{\mathfrak{m}}$  and hence also

$$w = Q(x_1, \dots, x_m)y + N(x_1, \dots, x_m) - Q(x_1, \dots, x_m)R(x_1, \dots, x_m) \in \mathfrak{o}y + \mathfrak{m}^{n+1},$$

which is false. Therefore  $N^{h+k} \not\equiv S_k R^k \pmod{\mathfrak{m}}$  for some  $k$ , so that if we set  $d = \min(nh + hk, s_k + rk)$  for that  $k$ , then the vanishing of  $N^{h+k} - S_k R^k$  at  $(x_1, \dots, x_m)$  provides a nontrivial linear relation over  $\mathfrak{o}/\mathfrak{m}$  of the elements  $x_1^{i_1} \dots x_m^{i_m} + \mathfrak{m}^{d+1}$  ( $i_1 + \dots + i_m = d$ ) of the vector space  $\mathfrak{m}^d/\mathfrak{m}^{d+1}$ . Hence  $\dim \mathfrak{m}^d/\mathfrak{m}^{d+1} < \binom{d+m-1}{m-1}$ .

## 15 Algebraic function fields of one variable

The purpose of this section is to prove the following well-known result on power series representation of algebraic function fields of one variable.

**Proposition 10** Let  $K$  be an algebraically closed field, let  $L$  be a finitely generated field extension of  $K$  of transcendence degree 1, let  $R$  be a ring with  $K \subset R \subset L$ , and let  $f: R \rightarrow K$  be a specialization over  $K$ . There exists a homomorphism  $\varphi: L \rightarrow K[[t]]$  over  $K$  into a power series field in one indeterminate over  $K$  such that  $\varphi(R) \subset K[[t]]$  and, for every  $x \in R$ ,  $(\varphi(x))(0) = f(x)$ .

*Proof* Consider the set of all pairs  $(R', f')$  such that  $R'$  is a ring with  $R \subset R' \subset L$  and  $f': R' \rightarrow K$  is a specialization extending  $f$ . We can introduce an order on this set by defining  $(R', f') \leq (R'', f'')$  to mean that  $R' \subset R''$  and  $f''$  extends  $f'$ . By Zorn's lemma this ordered set has a maximal element; fixing one, we denote it by  $(R', f')$ . By Section 14, Proposition 9(b), we see that if  $x \in L$  and  $x \notin R'$ , then  $x^{-1} \in R'$  and  $f'(x^{-1}) = 0$ . It follows that the multiplicative group  $U$  of invertible elements of  $R'$  consists of the elements  $x \in R'$  with  $f'(x) \neq 0$ . An easy induction argument shows that if  $\Phi$  is any nonempty finite set of elements of  $L$  not all of which are 0, then  $\Phi$  contains an element  $x_0$  such that  $x/x_0 \in R'$  for every  $x \in \Phi$ . If none of the  $x/x_0$  ( $x \in \Phi$ ,  $x \neq x_0$ ) is in  $U$ , then  $f'(\sum_{x \in \Phi} x/x_0) = \sum_{x \in \Phi, x \neq x_0} f'(x/x_0) + f'(1) = 1$ , so that  $\sum_{x \in \Phi} x \neq 0$ . Putting it the other way around, if  $\sum_{x \in \Phi} x = 0$ , then there exist distinct nonzero elements  $x_1, x_2 \in \Phi$  with  $x_2/x_1 \in U$ .

By hypothesis there exists an element  $v \in L$  with  $v$  transcendental over  $K$  and  $L$  algebraic over  $K(v)$  of finite degree, say  $n$ . Since  $R'$  contains  $v$  or  $v^{-1}$  we may suppose that  $v \in R'$ . Setting  $R_0 = K(v) \cap R'$ , we see that  $K[v] \subset R_0$ , so that  $R'$  is algebraic over  $R_0$ . Hence, for any nonzero element  $z \in R'$  there exist elements  $a_0, \dots, a_n \in R_0$  not all 0 such that  $\sum a_j z^j = 0$ . By what we have proved above, there exist integers  $i, j$  with  $0 \leq i < j \leq n$  and  $a_i a_j \neq 0$  such that  $a_j z^j/a_i z^i \in U$ . Since  $a_i/a_j \in K(v)$  and  $a_i/a_j = (a_j z^j/a_i z^i)^{-1} z^{j-i} \in R'$ , we have  $a_i/a_j \in R_0$ . This permits us to record the following observation: For each nonzero  $z \in R'$  there exist a  $u \in U$  and a nonzero  $a \in R_0$  such that  $z^n = au$ .

Now the element  $w = v - f'(v)$  is transcendental over  $K$ , and  $K[v] = K[w]$ ; also,  $f'(w) = 0$ . Since every nonzero element of  $K(v)$  can be expressed as an integral power of  $w$  multiplied by a quotient of two polynomials in  $w$  neither of which is divisible by  $w$ , we conclude that  $R_0$  consists of 0 and all elements of  $K(v)$  of the form  $w^k P(w)/Q(w)$  with  $k \in \mathbb{N}$ ,  $P, Q \in K[X]$ , and  $P(0)Q(0) \neq 0$ . We infer from this that  $R_0$  cannot contain an infinite sequence of nonzero elements  $x_0, x_1, \dots, x_k, \dots$  such that  $x_k/x_{k+1} \in R'$  and  $x_{k+1}/x_k \notin R'$  for every  $k$ . By the observation recorded above,  $R'$  cannot contain such a sequence, either. It follows that there exists a nonzero element  $t \in R'$  with

$f'(t) = 0$  such that every element  $x \in R'$  with  $f'(x) = 0$  is a multiple of  $t$  in  $R'$ . That is, the kernel of  $f'$  is the principal ideal  $R't$ .

Since  $f'(a) = a$  for every  $a \in K$  and  $f'(R') \subset K$ , for each  $x \in R'$  we have  $f'(x - f'(x)) = 0$ , so that there exists a unique  $x' \in R'$  such that  $x = f'(x) + x't$ . The mapping  $x \mapsto x'$  of  $R'$  into itself has the following properties, all easy to verify:

$$\begin{aligned}(x_1 + x_2)' &= x_1' + x_2' & (x_1, x_2 \in R'), \\ (x_1 x_2)' &= x_1' x_2 + x_1 x_2' - x_1' x_2' t & (x_1, x_2 \in R'), \\ a' &= 0 & (a \in K), \\ \mathbf{1}' &= 1, \\ (xt)' &= x & (x \in R').\end{aligned}$$

We now define by induction a sequence of mappings  $x \mapsto x^{(k)}$  of  $R'$  into itself by the formulae

$$x^{(0)} = x, \quad x^{(k+1)} = (x^{(k)})' \quad (k \in \mathbf{N}).$$

These mappings have the following properties:

$$\begin{aligned}(x_1 + x_2)^{(k)} &= x_1^{(k)} + x_2^{(k)} & (x_1, x_2 \in R'), \\ (x_1 x_2)^{(k)} &= \sum_{i+j=k} x_1^{(i)} x_2^{(j)} - \sum_{i+j=k-1} x_1^{(i+1)} x_2^{(j+1)} t & (x_1, x_2 \in R'), \\ a^{(k)} &= \begin{cases} a & \text{if } k = 0 \\ 0 & \text{if } k > 0 \end{cases} & (a \in K).\end{aligned}$$

The first and third of these are obvious. The second reduces for  $k = 0$  to the identity  $x_1 x_2 = x_1 x_2$  and for  $k = 1$  to the identity  $(x_1 x_2)' = x_1' x_2 + x_1 x_2' - x_1' x_2' t$  established above, and for  $k > 1$  it follows by a straightforward induction argument using the properties of the mapping  $x \mapsto x'$ . Now, if  $x \in R'$  and  $f'(x) = 0$ , then  $x = x't$ . By induction we infer that if  $f'(x^{(j)}) = 0$  ( $0 \leq j < k$ ), then  $x = x^{(k)} t^k$ . It follows from this that if  $f'(x^{(k)}) = 0$  for every  $k \in \mathbf{N}$ , then  $x = 0$  (for otherwise  $x, x/t, \dots, x/t^k, \dots$  would be an infinite sequence of nonzero elements of  $R'$  each term of which is divisible by the succeeding term but not vice versa, contrary to a property of  $R'$  proved above).

We now define a mapping  $\varphi' : R' \rightarrow K[[t]]$  by the formula

$$\varphi'(x) = \sum_{k \in \mathbf{N}} f'(x^{(k)}) t^k.$$

By what we have just shown,  $\varphi'$  is a homomorphism, leaves invariant each element of  $K$ , is injective, and has the property that  $(\varphi'(x))(0) = f'(x)$ . Since  $L$  is the field of quotients of  $R'$  and  $K((t))$  is that of  $K[[t]]$ ,  $\varphi'$  can be extended to a unique homomorphism  $\varphi : L \rightarrow K((t))$ .

## 16 Dimension of components

The following proposition is the ideal-theoretic counterpart of a well-known theorem of algebraic geometry concerning hypersurface sections of algebraic varieties. The present beautiful proof is due to J. Tate.<sup>2</sup>

**Proposition 11** *Let  $\mathfrak{p}$  be a prime ideal of a finitely generated polynomial algebra  $K[X_1, \dots, X_n]$  over a field  $K$ , and let  $d = \dim \mathfrak{p}$ . Let  $f \in K[X_1, \dots, X_n]$ ,  $f \notin \mathfrak{p}$ , and let  $\mathfrak{r}$  be the perfect ideal generated by  $(\mathfrak{p}, f)$  in  $K[X_1, \dots, X_n]$ . Then every component of  $\mathfrak{r}$  has dimension  $d-1$ .*

*Proof* If  $\mathfrak{r}$  has no component (that is, if  $\mathfrak{r} = K[X_1, \dots, X_n]$ ), the result is trivial. Suppose  $\mathfrak{r}$  has precisely one component (that is,  $\mathfrak{r}$  is prime), and let  $x = (x_1, \dots, x_n)$  and  $x' = (x_1', \dots, x_n')$  be generic zeros of  $\mathfrak{p}$  and  $\mathfrak{r}$ , respectively.

We first establish the fact (Noether's *normalization lemma*) that there exists a family  $y = (y_1, \dots, y_d)$  of  $d$  elements  $y_i = g_i(x) \in K[x]$ , such that  $K[x]$  is integral over  $K[y]$ . If  $d = n$ , this is obvious, for we may then use  $x$  for  $y$ ; hence we may suppose in this connection that  $\mathfrak{p}$  contains a nonzero polynomial  $g$ . Let  $cX_1^{i_1} \dots X_n^{i_n}$  be the highest nonzero term of  $g$  when we order these terms lexicographically<sup>3</sup> with respect to  $(i_n, i_{n-1}, \dots, i_1)$ , let  $m_j = (1 + \deg g)^{j-1}$  ( $2 \leq j \leq n$ ), and let  $x_{1j} = x_j - x_1^{m_j}$  ( $2 \leq j \leq n$ ). Then

$$g(x_1, x_{12} + x_1^{m_2}, \dots, x_{1n} + x_1^{m_n}) = cx_1^{i_1 + i_2 m_2 + \dots + i_n m_n} + g'(x_1, x_{12}, \dots, x_{1n}),$$

where  $g'$  is a polynomial in  $K[X_1, X_2, \dots, X_n]$  with  $\deg_{X_1} g' < i_1 + i_2 m_2 + \dots + i_n m_n$ . Since  $g(x_1, x_{12} + x_1^{m_2}, \dots, x_{1n} + x_1^{m_n}) = g(x_1, x_2, \dots, x_n) = 0$ , this shows that  $K[x_1, x_2, \dots, x_n]$  is integral over  $K[x_{12}, \dots, x_{1n}]$ . The proof of the normalization lemma now can be completed by induction.

This being so,  $f(x)$  is integral over  $K[y]$ . Since  $y = (y_1, \dots, y_d)$  is obviously algebraically independent over  $K$ ,  $K[y]$  is integrally closed in  $K(y)$ , so that the minimal equation

$$f(x)^r + f_{r-1}(y)f(x)^{r-1} + \dots + f_0(y) = 0 \quad (3)$$

of  $f(x)$  over  $K(y)$  has its coefficients  $f_0(y), \dots, f_{r-1}(y)$  in  $K[y]$ . Computing the norm of  $f(x)$  from  $K(x)$  to  $K(y)$  we therefore find:

$$\begin{aligned}N_{K(x)/K(y)} f(x) &= N_{K(f(x), y)/K(y)} N_{K(x)/K(f(x), y)} f(x) \\ &= N_{K(f(x), y)/K(y)} f(x)^{[K(x):K(f(x), y)]} \\ &= ((-1)^r f_0(y))^{[K(x):K(f(x), y)]} = \pm f_0(y)^a.\end{aligned}$$

<sup>2</sup> See S. Lang, "Introduction to Algebraic Geometry," Chap. II, §7. Interscience, New York, 1958.

<sup>3</sup> See Section 17 for the definition of the lexicographic order on  $\mathbf{N}^n$ .

A similar result holds for any  $k(x) \in K[x]$ . Setting  $y' = (y'_1, \dots, y'_d)$ , where  $y'_i = g_i(x')$ , we see that  $K[x']$  is integral over  $K[y']$ , so that  $\dim \mathfrak{r} = \text{tr deg } K(x')/K = \text{tr deg } K(y')/K$ . By (3) we see that  $f_0(y') = 0$ , so that there exists an irreducible factor  $f'$  of  $f_0$  in  $K[Y_1, \dots, Y_d]$  that vanishes at  $y'$ . If  $h$  is any polynomial in  $K[Y_1, \dots, Y_d]$  vanishing at  $y'$ , then the polynomial  $h(g_1, \dots, g_d) \in K[X_1, \dots, X_n]$  vanishes at  $x'$ , hence is in  $\mathfrak{r}$ , and hence has a power that is in the ideal  $(\mathfrak{p}, f)$ . Substituting  $x$  for  $(X_1, \dots, X_n)$ , we therefore find an equation  $h(y)^b = k(x)f(x)$ , whence

$$h(y)^c = N_{K(x)/K(y)} h(y)^b = N_{K(x)/K(y)} k(x)f(x) = \pm k_0(y)^d f_0(y)^a,$$

so that  $h$  is divisible by  $f'$ . Thus, the defining ideal of  $y'$  in  $K[Y_1, \dots, Y_d]$  is the principal ideal  $(f')$ , so that  $\dim \mathfrak{r} = \text{tr deg } K(y')/K = \dim(f') = d-1$ . This proves the proposition in the case in which  $\mathfrak{r}$  has just one component.

Now let  $\mathfrak{r}$  have  $s > 1$  components  $\mathfrak{p}_1, \dots, \mathfrak{p}_s$ . Let  $x = (x_1, \dots, x_n)$  and  $x' = (x'_1, \dots, x'_n)$  be generic zeros of  $\mathfrak{p}$  and say  $\mathfrak{p}_1$ , respectively. There exists an  $h \in K[X_1, \dots, X_n]$  with  $h \in \bigcap_{2 \leq j \leq s} \mathfrak{p}_j$  and  $h \notin \mathfrak{p}_1$ . Let  $\mathfrak{p}'$  be the defining ideal of  $(x_1, \dots, x_n, 1/h(x))$  in  $K[X_1, \dots, X_n, X_{n+1}]$ , and let  $\mathfrak{r}'$  be the perfect ideal generated by  $(\mathfrak{p}', f)$  in  $K[X_1, \dots, X_n, X_{n+1}]$ . It is clear that  $(x'_1, \dots, x'_n, 1/h(x'))$  is a zero of  $\mathfrak{r}'$ . On the other hand,  $X_{n+1}h - 1 \in \mathfrak{p}' \subset \mathfrak{r}'$ , so that if  $(a_1, \dots, a_n, a_{n+1})$  is any zero of  $\mathfrak{r}'$ , then  $h(a_1, \dots, a_n) \neq 0$ . Hence  $(a_1, \dots, a_n)$  is a zero of  $\mathfrak{p}_1$  and therefore is a specialization of  $(x'_1, \dots, x'_n)$  over  $K$ , whence  $(a_1, \dots, a_n, a_{n+1})$  is a specialization of  $(x'_1, \dots, x'_n, 1/h(x'))$  over  $K$ . Thus,  $\mathfrak{r}'$  is prime and has generic zero  $(x'_1, \dots, x'_n, 1/h(x'))$ . By the case of the proposition already treated,

$$\begin{aligned} \dim \mathfrak{r}' &= \dim \mathfrak{p}' - 1 = \text{tr deg } K(x_1, \dots, x_n, 1/h(x))/K - 1 \\ &= \text{tr deg } K(x)/K - 1 = d - 1. \end{aligned}$$

Therefore

$$\dim \mathfrak{p}_1 = \text{tr deg } K(x')/K = \text{tr deg } K(x'_1, \dots, x'_n, 1/h(x'))/K = \dim \mathfrak{r}' = d - 1.$$

This completes the proof.

**Corollary 1** *Let  $\mathfrak{p}$  and  $\mathfrak{q}$  be prime ideals of  $K[X_1, \dots, X_n]$ , and let  $\mathfrak{r}$  denote the perfect ideal of  $K[X_1, \dots, X_n]$  generated by  $\mathfrak{p} + \mathfrak{q}$ . Every component of  $\mathfrak{r}$  has dimension greater than or equal to  $\dim \mathfrak{p} + \dim \mathfrak{q} - n$ .*

*Proof* If  $K_a$  is the algebraic closure of  $K$  and if we denote the components of the perfect ideal generated by  $K_a \mathfrak{p}$ , respectively  $K_a \mathfrak{q}$ , by  $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ , respectively  $\mathfrak{q}_1, \dots, \mathfrak{q}_s$ , then, as is easy to see, the perfect ideal  $\bar{\mathfrak{r}}$  generated by  $K_a \mathfrak{r}$  coincides with the intersection of the  $rs$  perfect ideals  $\mathfrak{r}_{ij}$  generated by various  $\mathfrak{p}_i + \mathfrak{q}_j$  in  $K_a[X_1, \dots, X_n]$ . By Section 12, Proposition 7(a), each component of  $\bar{\mathfrak{r}}$  has the same dimension as a component of  $\mathfrak{r}$ , and also as a component of some  $\mathfrak{r}_{ij}$ , and each  $\mathfrak{p}_i$ , respectively  $\mathfrak{q}_j$ , has the same dimension

as  $\mathfrak{p}$ , respectively  $\mathfrak{q}$ . Therefore it suffices to prove the corollary under the additional hypothesis that  $K$  be algebraically closed, in which case  $\mathfrak{p}$  and  $\mathfrak{q}$  are regular over  $K$ . This being the case, let  $X'_1, \dots, X'_n$  be  $n$  more indeterminates and let  $\mathfrak{q}'$  denote the ideal of  $K[X'_1, \dots, X'_n]$  corresponding to the ideal  $\mathfrak{q}$  of  $K[X_1, \dots, X_n]$ . The substitution of  $(X_1, \dots, X_n, X'_1, \dots, X'_n)$  for  $(X_1, \dots, X_n, X_1, \dots, X_n)$  is a surjective homomorphism  $K[X_1, \dots, X_n, X'_1, \dots, X'_n] \rightarrow K[X_1, \dots, X_n]$  with kernel  $(X_1 - X'_1, \dots, X_n - X'_n)$ ; the ideal  $\mathfrak{a}' = (\mathfrak{p} + \mathfrak{q}', X_1 - X'_1, \dots, X_n - X'_n)$  is mapped onto  $\mathfrak{p} + \mathfrak{q}$ . Hence by Section 10, Lemma 10(a),  $\mathfrak{p} + \mathfrak{q}$  is birationally equivalent to  $\mathfrak{a}'$  over  $K$ . By Section 12, Corollary 2 to Proposition 7,  $\mathfrak{p} + \mathfrak{q}'$  is prime of dimension equal to  $\dim \mathfrak{p} + \dim \mathfrak{q}$ . By  $n$ -fold application of Proposition 11 we therefore find that each component of the perfect ideal generated by  $\mathfrak{a}'$  has dimension greater than or equal to  $\dim \mathfrak{p} + \dim \mathfrak{q} - n$ .

**Corollary 2** *Let  $\mathfrak{p}$  and  $\mathfrak{q}$  be prime ideals of  $K[X_1, \dots, X_n]$  with  $\mathfrak{p} \subset \mathfrak{q}$ , let  $s = \dim \mathfrak{p} - \dim \mathfrak{q}$ , and let  $f \in K[X_1, \dots, X_n]$ ,  $f \notin \mathfrak{p}$ . Then there exists a strictly increasing sequence of  $s+1$  prime ideals  $\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \dots \subset \mathfrak{p}_s$  with  $\mathfrak{p}_0 = \mathfrak{p}$ ,  $\mathfrak{p}_s = \mathfrak{q}$ , and  $f \notin \mathfrak{p}_i$  ( $0 \leq i < s$ ).*

*Proof* By Section 11, Proposition 4,  $s \geq 0$  and if  $s = 0$ , then  $\mathfrak{p} = \mathfrak{q}$ , in which case the result is trivial; it is also trivial if  $s = 1$ . Letting  $s \geq 2$  we see that it suffices to prove the existence of a prime ideal  $\mathfrak{p}_1$  between  $\mathfrak{p}$  and  $\mathfrak{q}$  with  $\dim \mathfrak{p}_1 = \dim \mathfrak{p} - 1$  and  $f \notin \mathfrak{p}_1$ . Let  $f_1$  be an element of  $\mathfrak{q}$  not in  $\mathfrak{p}$  (if  $f \in \mathfrak{q}$ , we take  $f_1 = f$ ). Each component of the perfect ideal generated by  $(\mathfrak{p}, f_1)$  has dimension equal to  $\dim \mathfrak{p} - 1$  and therefore does not contain  $\mathfrak{q}$ , and at least one of these components is contained in  $\mathfrak{q}$ . It is easy to see that  $\mathfrak{q}$  contains an element  $f_2$  not contained in any of these components.<sup>4</sup> Each component of the perfect ideal generated by  $(\mathfrak{p}, f_1, f_2)$  has dimension equal to  $\dim \mathfrak{p} - 2$ . At least one component  $\mathfrak{p}_1$  of the perfect ideal generated by  $(\mathfrak{p}, f_2)$  is contained in  $\mathfrak{q}$ ; by Proposition 11,  $\dim \mathfrak{p}_1 = \dim \mathfrak{p} - 1$ . If  $\mathfrak{p}_1$  contained  $f_1$ , then  $\mathfrak{p}_1$  would be a component of the perfect ideal generated by  $(\mathfrak{p}, f_1, f_2)$  and therefore would be of dimension equal to  $\dim \mathfrak{p} - 2$ .

**Corollary 3** *Let  $\mathfrak{p}$  be a prime ideal of  $K[X_1, \dots, X_n]$ , let  $f \in K[X_1, \dots, X_n]$ ,  $f \notin \mathfrak{p}$ , let  $K'$  be an algebraically closed field extension of  $K$ , and let  $(a_1, \dots, a_n)$*

<sup>4</sup> This is an immediate consequence of the following well-known fact: *If the union of a finite set of prime ideals contains a given ideal, then one of the prime ideals does.* Indeed, let  $\mathfrak{a}$  be an ideal and  $\mathfrak{p}_1, \dots, \mathfrak{p}_m$  be prime ideals with  $\mathfrak{a} \subset \bigcup \mathfrak{p}_i$ . We may suppose that  $\mathfrak{a}$  is not contained in the union of any  $m-1$  of these prime ideals. Assume  $m > 1$ . For each  $i$  there exists an  $x_i \in \mathfrak{a}$  with  $x_i \notin \bigcup_{j \neq i} \mathfrak{p}_j$ , and obviously  $x_i \in \mathfrak{p}_i$ . Setting  $y_i = \prod_{j \neq i} x_j$  we see that  $y_i \notin \mathfrak{p}_i$ ,  $y_i \in \mathfrak{a}$ ,  $y_i \in \bigcap_{j \neq i} \mathfrak{p}_j$ . Therefore the element  $z = \sum y_i$  is in  $\mathfrak{a}$ , and hence is in some  $\mathfrak{p}_i$ , say  $z \in \mathfrak{p}_{i_0}$ . However, then  $y_{i_0} = z - \sum_{i \neq i_0} y_i \in \mathfrak{p}_{i_0}$ . This contradiction shows that  $m = 1$ .

be a zero of  $\mathfrak{p}$  with each  $a_j \in K'$ . Then there exist power series  $Q_1, \dots, Q_n$  in a power series algebra  $K'[[t]]$  in one indeterminate over  $K'$  such that  $(Q_1, \dots, Q_n)$  is a zero of  $\mathfrak{p}$  but not of  $f$ , and  $Q_j(0) = a_j$  ( $1 \leq j \leq n$ ).

*Proof* It is obvious that  $(a_1, \dots, a_n)$  is a zero of some component  $\mathfrak{p}'$  of the perfect ideal generated by  $K'\mathfrak{p}$  in  $K'[X_1, \dots, X_n]$ ; by Section 12, Proposition 7(a),  $f \notin \mathfrak{p}'$ . Of course  $\mathfrak{p}'$  is contained in the prime ideal  $\mathfrak{a}' = (X_1 - a_1, \dots, X_n - a_n)$  of dimension 0. If  $\mathfrak{p}' = \mathfrak{a}'$ , we may take  $Q_j = a_j$  ( $1 \leq j \leq n$ ). If  $\mathfrak{p}' \neq \mathfrak{a}'$ , then by Corollary 2 there exists a prime ideal  $\mathfrak{p}_1'$  of  $K'[X_1, \dots, X_n]$  of dimension 1 with  $\mathfrak{p}' \subset \mathfrak{p}_1' \subset \mathfrak{a}'$  and  $f \notin \mathfrak{p}_1'$ . Let  $(x_1, \dots, x_n)$  be a generic zero of  $\mathfrak{p}_1'$ . By Section 15, Proposition 10, there is a homomorphism  $K'(x_1, \dots, x_n) \rightarrow K'((t))$  over  $K'$  mapping  $x_j$  onto an element  $Q_j \in K'[[t]]$  such that  $Q_j(0) = a_j$  ( $1 \leq j \leq n$ ).

**Corollary 4** Let  $f_1, \dots, f_m$  be polynomials in  $K[X_1, \dots, X_n]$  with  $m \leq n$  and let  $(a_1, \dots, a_n)$  be a zero of the ideal  $\bar{f} = (f_1, \dots, f_m)$  of  $K[X_1, \dots, X_n]$  that is not a zero of the polynomial  $J = \det(\partial f_i / \partial X_i)_{1 \leq i \leq m, 1 \leq i' \leq m}$ . Then  $(a_1, \dots, a_n)$  is a zero of precisely one component of the perfect ideal of  $K[X_1, \dots, X_n]$  generated by  $\bar{f}$ ; that component has dimension  $n - m$  and is separable over  $K$ .

*Proof* Let  $\mathfrak{p}_1, \dots, \mathfrak{p}_r$  denote the components of the perfect ideal generated by  $\bar{f}$ . It is clear that  $(a_1, \dots, a_n)$  is a zero of at least one  $\mathfrak{p}_k$ . By  $m$ -fold application of Proposition 11,  $\dim \mathfrak{p}_k \geq n - m$ . Let  $(x_1, \dots, x_n)$  be a generic zero of  $\mathfrak{p}_k$ ; then  $J(x_1, \dots, x_n) \neq 0$ . If  $D$  is any derivation of  $K(x_1, \dots, x_n)$  over  $K(x_{m+1}, \dots, x_n)$ , then

$$0 = Df_i(x_1, \dots, x_n) = \sum_{1 \leq i' \leq m} (\partial f_i / \partial X_{i'})(x_1, \dots, x_n) D x_{i'} \quad (1 \leq i \leq m),$$

hence  $D x_{i'} = 0$  ( $1 \leq i' \leq m$ ), so that  $D = 0$ . Thus, there does not exist a nonzero derivation of  $K(x_1, \dots, x_n)$  over  $K(x_{m+1}, \dots, x_n)$ . By a well-known criterion,<sup>5</sup> it follows that  $K(x_1, \dots, x_n)$  is a separable algebraic field extension of  $K(x_{m+1}, \dots, x_n)$ . Therefore  $\dim \mathfrak{p}_k = n - m$  and  $\mathfrak{p}_k$  is separable over  $K$ . It remains to prove the uniqueness of  $\mathfrak{p}_k$ . It is easy to see by Section 12, Proposition 7(a), that we may replace  $K$  by any larger field; in particular, we may assume that  $K$  contains each  $a_j$  and that  $K$  is algebraically closed. Because of the former assumption we may even suppose that  $a_j = 0$  ( $1 \leq j \leq n$ ). This being the case, we see that, in the power series algebra  $\mathfrak{o} = K[[X_1, \dots, X_n]]$ ,  $\mathfrak{o}\bar{f} \subset \mathfrak{o}\mathfrak{p}_1 \cap \dots \cap \mathfrak{o}\mathfrak{p}_r \subset$  the perfect ideal of  $\mathfrak{o}$  generated by  $\mathfrak{o}\bar{f}$ . However, by the implicit function theorem (Section 13, Proposition 8), there exist power series  $P_1, \dots, P_m \in K[[X_{m+1}, \dots, X_n]]$  vanishing at  $(0, \dots, 0)$  such that  $\mathfrak{o}\bar{f} = (X_1 - P_1, \dots, X_m - P_m)$ , so that  $\mathfrak{o}\bar{f}$  is prime and  $\mathfrak{o}\bar{f} = \mathfrak{o}\mathfrak{p}_1 \cap \dots \cap \mathfrak{o}\mathfrak{p}_r$ . It follows

<sup>5</sup> See, e.g., N. Bourbaki, "Algèbre," Chap. V, §9 p. 140. Hermann, Paris, 1950 or 1959.

that  $\mathfrak{o}\bar{f}$  coincides with some  $\mathfrak{o}\mathfrak{p}_k$ , say with  $\mathfrak{o}\mathfrak{p}_1$ , and  $\mathfrak{o}\mathfrak{p}_1 \subset \mathfrak{o}\mathfrak{p}_k$  ( $2 \leq k \leq r$ ). In particular,  $(0, \dots, 0)$  is a zero of  $\mathfrak{p}_1$ . Consider any  $\mathfrak{p}_k$  with  $k \neq 1$ . There exists an  $f \in \mathfrak{p}_1$  with  $f \notin \mathfrak{p}_k$ . If  $(0, \dots, 0)$  were a zero of  $\mathfrak{p}_k$ , then, by Corollary 3 above, there would exist power series  $Q_1, \dots, Q_n \in K[[t]]$  with  $Q_j(0) = 0$  ( $1 \leq j \leq n$ ) such that  $(Q_1, \dots, Q_n)$  is a zero of  $\mathfrak{p}_k$  but not of  $f$ , hence a zero of  $\mathfrak{o}\mathfrak{p}_k$  but not of  $\mathfrak{o}\mathfrak{p}_1$ , contrary to the inclusion  $\mathfrak{o}\mathfrak{p}_1 \subset \mathfrak{o}\mathfrak{p}_k$ .

**Corollary 5** Let  $\mathfrak{p}$  and  $\mathfrak{q}$  be prime ideals of  $K[X_1, \dots, X_n]$  with  $\mathfrak{p} \supset \mathfrak{q}$ , let  $x = (x_1, \dots, x_n)$  and  $y = (y_1, \dots, y_n)$  be generic zeros of  $\mathfrak{p}$  and  $\mathfrak{q}$  respectively, and set  $r = \dim \mathfrak{p}$  and  $s = \dim \mathfrak{q}$ . Consider the local ring  $\mathfrak{o} = K[X_1, \dots, X_n]_{\mathfrak{p}}$ , its maximal ideal  $\mathfrak{m} = \mathfrak{o}\mathfrak{p}$ , and the prime ideal  $\mathfrak{n} = \mathfrak{o}\mathfrak{q}$ . Let  $J_q$  denote the matrix  $(\partial Q_i / \partial X_j)_{Q_i \in \mathfrak{q}, 1 \leq i \leq n}$  having coordinates in  $K[X_1, \dots, X_n]$ .

- The rank of  $J_q(x)$  is at most  $n - s$ .
- Every set of generators of the maximal ideal  $\mathfrak{m}/\mathfrak{n}$  of the local ring  $\mathfrak{o}/\mathfrak{n}$  has at least  $s - r$  elements.
- If the rank of  $J_q(x)$  is  $n - s$ , then  $\mathfrak{m}/\mathfrak{n}$  has a set of generators with precisely  $s - r$  elements.
- If  $\mathfrak{m}/\mathfrak{n}$  has a set of generators with precisely  $s - r$  elements, then  $\mathfrak{o}/\mathfrak{n}$  is integrally closed.

*Proof* (a) If say  $\det(\partial Q_i / \partial X_j)_{s \leq i \leq n, s \leq j \leq n}$  did not vanish at  $y$  for some  $Q_s, \dots, Q_n \in \mathfrak{q}$ , then by Corollary 4 there would exist a prime ideal  $\mathfrak{q}'$  of dimension  $s - 1$  containing  $Q_s, \dots, Q_n$  and having  $y$  as zero, and this would imply that  $\mathfrak{q}' \subset \mathfrak{q}$  and  $s - 1 = \dim \mathfrak{q}' \geq \dim \mathfrak{q} = s$ . Thus, every  $(n - s + 1)$ -rowed minor of  $J_q$  vanishes at  $y$  and hence also at  $x$ , so that the rank of  $J_q(x)$  is less than or equal to  $n - s$ .

(b) Let  $F_1, \dots, F_m$  be elements of  $\mathfrak{m}$  such that  $F_1 + \mathfrak{n}, \dots, F_m + \mathfrak{n}$  generate  $\mathfrak{m}/\mathfrak{n}$ ; the denominator of each  $F_i$  is a unit of  $\mathfrak{o}$ , and hence we may suppose that  $F_1, \dots, F_m \in \mathfrak{p}$ . Then  $\mathfrak{p}$  contains the perfect ideal of  $K[X_1, \dots, X_n]$  generated by  $\mathfrak{q} + (F_1, \dots, F_m)$ , and hence contains a component  $\mathfrak{p}'$  of that perfect ideal. By Proposition 11,  $\dim \mathfrak{p}' \geq s - m$ . Since  $\mathfrak{p} \subset \mathfrak{m}$ , for any  $P \in \mathfrak{p}$  we have  $P \in \sum_{1 \leq i \leq m} \mathfrak{o}F_i + \mathfrak{n}$ , and therefore there exists an  $H \in K[X_1, \dots, X_n]$  with  $H \notin \mathfrak{p}$  (and hence with  $H \notin \mathfrak{p}'$ ) such that  $HP \in \mathfrak{p}'$ , so that  $P \in \mathfrak{p}'$ . Thus,  $\mathfrak{p} = \mathfrak{p}'$  and  $r = \dim \mathfrak{p} \geq s - m$ , whence  $m \geq s - r$ .

(c) By Section 14, Remark 3, in order to show that  $\mathfrak{m}/\mathfrak{n}$  has a set of  $s - r$  generators it suffices to show that the vector space  $(\mathfrak{m}/\mathfrak{n})/(\mathfrak{m}/\mathfrak{n})^2 = (\mathfrak{m}/\mathfrak{n})/((\mathfrak{m}^2 + \mathfrak{n})/\mathfrak{n})$  over  $(\mathfrak{o}/\mathfrak{n})/(\mathfrak{m}/\mathfrak{n})$  has dimension less than or equal to  $s - r$ , that is, that the vector space  $\mathfrak{m}/(\mathfrak{m}^2 + \mathfrak{n})$  over  $\mathfrak{o}/\mathfrak{m}$  has dimension less than or equal to  $s - r$ . To do this it suffices to show that  $(\mathfrak{m}^2 + \mathfrak{n})/\mathfrak{m}^2$  has dimension greater than or equal to  $n - s$  and  $\mathfrak{m}/\mathfrak{m}^2$  has dimension less than or equal to  $n - r$ .

To settle the first point, observe that if  $Q_{s+1}, \dots, Q_n \in \mathfrak{q}$  and  $\sum \alpha_i Q_i \in \mathfrak{m}^2$

where  $\alpha_{s+1}, \dots, \alpha_n \in \mathfrak{o}$  and  $\alpha_i \notin \mathfrak{m}$  for some  $i$ , then

$$\sum_i \alpha_i \partial Q_i / \partial X_j = \partial \left( \sum_i \alpha_i Q_i \right) / \partial X_j - \sum_i (\partial \alpha_i / \partial X_j) Q_i \in \mathfrak{m}$$

for every  $j$ , so that every  $(n-s)$ -rowed minor of the matrix  $(\partial Q_i / \partial X_j)_{s < i \leq n, 1 \leq j \leq n}$  must be in  $\mathfrak{m}$  and hence must vanish at  $x$ . Since the rank of  $J_q(x)$  is  $n-s$ , this shows that  $\mathfrak{q}$  (and hence also  $\mathfrak{m}$ ) contains  $n-s$  elements that modulo  $\mathfrak{m}^2$  are linearly independent over  $\mathfrak{o}/\mathfrak{m}$ . Therefore the dimension of  $(\mathfrak{n} + \mathfrak{m}^2)/\mathfrak{m}^2$  is greater than or equal to  $n-s$ .

To settle the second point, suppose that, say  $x_1, \dots, x_r$  form a transcendence basis of  $K(x)$  over  $K$ , and let  $d_j$  denote the degree of  $x_j$  over  $K(x_1, \dots, x_{j-1})$  ( $r < j \leq n$ ). For each  $j$  with  $r < j \leq n$ ,  $\mathfrak{p}$  contains a nonzero polynomial  $P_j \in K[X_1, \dots, X_j]$  with  $\deg_{X_j} P_j = d_j$  and  $\deg_{X_i} P_j < d_i$  ( $r < i < j$ ), and  $\mathfrak{p}$  does not contain a nonzero polynomial  $P$  with  $\deg_{X_i} P < d_i$  ( $r < i \leq n$ ). Writing  $P_j = I_j X_j^{d_j} + \dots$ , where  $I_j, \dots$  are polynomials in  $K[X_1, \dots, X_{j-1}]$  with  $I_j \notin \mathfrak{p}$ , we see that for any  $P \in \mathfrak{p}$  there is a congruence

$$I_{r+1}^{e_{r+1}} \dots I_n^{e_n} P \equiv P' \pmod{(P_{r+1}, \dots, P_n)}$$

with  $\deg_{X_i} P' < d_i$  ( $r < i \leq n$ ) and hence with  $P' = 0$ . Since each  $I_i$  is a unit of  $\mathfrak{o}$ , it follows that  $\mathfrak{m} = \mathfrak{o}\mathfrak{p} = \mathfrak{o}P_{r+1} + \dots + \mathfrak{o}P_n$  and hence that  $\mathfrak{m}/\mathfrak{m}^2$  has dimension less than or equal to  $n-r$ .

(d) To prove that  $\mathfrak{o}/\mathfrak{n}$  is integrally closed, it suffices by Section 14, Remark 4, to show for each  $d \in \mathbb{N}$  that the vector space  $(\mathfrak{m}/\mathfrak{n})^d / (\mathfrak{m}/\mathfrak{n})^{d+1}$  over  $(\mathfrak{o}/\mathfrak{n}) / (\mathfrak{m}/\mathfrak{n})$  has dimension  $\binom{s-r+d-1}{s-r-1}$ , that is, that the vector space  $(\mathfrak{m}^d + \mathfrak{n}) / (\mathfrak{m}^{d+1} + \mathfrak{n})$  over  $\mathfrak{o}/\mathfrak{m}$  does. By hypothesis, there exist polynomials  $F_{r+1}, \dots, F_s \in \mathfrak{p}$  such that their residue classes modulo  $\mathfrak{n}$  generate the ideal  $\mathfrak{m}/\mathfrak{n}$  of  $\mathfrak{o}/\mathfrak{n}$ . To complete the proof it evidently suffices to show that whenever

$$P = \sum_{\sum e_i = d} A_{e_{r+1}, \dots, e_s} Y_{r+1}^{e_{r+1}} \dots Y_s^{e_s}$$

is a homogeneous polynomial of degree  $d$  with coefficients in  $\mathfrak{o}$  such that  $P(F_{r+1}, \dots, F_s) \in \mathfrak{m}^{d+1} + \mathfrak{n}$ , then every coefficient in  $P$  is an element of  $\mathfrak{m}$ , and to do this it is enough to show that when the coefficients in  $P$  all are in  $K[X_1, \dots, X_n]$  and  $P$  has the property that  $P(F_{r+1}, \dots, F_s) \in \mathfrak{p}^{d+1} + \mathfrak{q}$ , then the coefficients all are in  $\mathfrak{p}$ . Now, because of this property,  $P(F_{r+1}, \dots, F_s)$  can be expressed modulo  $\mathfrak{q}$  as a homogeneous polynomial in  $F_{r+1}, \dots, F_s$  of degree  $d+1$  with coefficients in  $K[X_1, \dots, X_n]$ , or if we prefer, as a homogeneous polynomial  $\sum_{\sum e_i = d} B_{e_{r+1}, \dots, e_s} F_{r+1}^{e_{r+1}} \dots F_s^{e_s}$  in  $F_{r+1}, \dots, F_s$  of degree  $d$  with coefficients in  $\mathfrak{p}$ ; then

$$\sum_{\sum e_i = d} (A_{e_{r+1}, \dots, e_s} - B_{e_{r+1}, \dots, e_s}) F_{r+1}^{e_{r+1}} \dots F_s^{e_s} \in \mathfrak{q}. \quad (4)$$

Assume that  $A_{e_{r+1}, \dots, e_s} \notin \mathfrak{p}$  for some  $(e_{r+1}, \dots, e_s)$ . Fixing elements  $t_{r+1}, \dots, t_{s-1}$  of an extension of  $K$  that are algebraically independent over  $K$ , and setting  $L = K(t_{r+1}, \dots, t_{s-1})$ , we see that  $L\mathfrak{p}$  and  $L\mathfrak{q}$  are prime ideals of  $L[X_1, \dots, X_n]$  of respective dimensions  $r$  and  $s$  with  $L\mathfrak{p} \supset L\mathfrak{q}$  and that

$$\sum_{\sum e_i = d} (A_{e_{r+1}, \dots, e_s} - B_{e_{r+1}, \dots, e_s}) t_{r+1}^{e_{r+1}} \dots t_{s-1}^{e_{s-1}} \notin L\mathfrak{p}.$$

Therefore if we set  $G_i = F_i - t_i F_s \in L\mathfrak{p}$  ( $r < i < s$ ) and in (4) replace  $F_i$  by  $G_i + t_i F_s$  ( $r < i < s$ ), we find a relation

$$C_0 F_s^d + C_1 F_s^{d-1} + \dots + C_d \in L\mathfrak{q}, \quad (5)$$

where  $C_j$  is a homogeneous polynomial in  $G_{r+1}, \dots, G_{s-1}$  of degree  $j$  with coefficients in  $L[X_1, \dots, X_n]$  ( $0 \leq j \leq d$ ) and  $C_0 \notin L\mathfrak{p}$ . Now,  $L\mathfrak{p}$  contains the perfect ideal of  $L[X_1, \dots, X_n]$  generated by  $L\mathfrak{q} + (G_{r+1}, \dots, G_{s-1})$ , and hence contains a component  $\mathfrak{p}'$  of that perfect ideal. By Proposition 11,  $\dim \mathfrak{p}' \geq s - (s-1-r) = r+1$ . By the above,  $C_0 \notin \mathfrak{p}'$  and  $C_j \in \mathfrak{p}'$  ( $1 \leq j \leq d$ ); therefore  $F_s \in \mathfrak{p}'$  by (5), and hence also  $F_i = G_i + t_i F_s \in \mathfrak{p}'$  ( $r < i < s$ ), so that  $\mathfrak{p}'$  is a component of the perfect ideal of  $L[X_1, \dots, X_n]$  generated by  $L\mathfrak{q} + (F_{r+1}, \dots, F_s)$ . As we saw in the proof of part (b), then  $L\mathfrak{p} = \mathfrak{p}'$ , whence  $r = \dim L\mathfrak{p} = \dim \mathfrak{p}' \geq r+1$ . This contradiction completes the proof.

## 17 Lattice points

Let  $W_1, \dots, W_m$  be a finite sequence of ordered sets, and consider the product set  $P = \prod_{1 \leq i \leq m} W_i$ . We shall use various orders on  $P$ . The *product* order on  $P$  is defined by the condition that  $(a_1, \dots, a_m) \leq (b_1, \dots, b_m)$  in  $P$  if and only if  $a_i \leq b_i$  in  $W_i$  ( $1 \leq i \leq m$ ). The *lexicographic* order on  $P$  is defined by the condition that  $(a_1, \dots, a_m) < (b_1, \dots, b_m)$  in  $P$  if and only if there exists an index  $h$  such that  $a_i = b_i$  ( $1 \leq i < h$ ) and  $a_h < b_h$  in  $W_h$ .

If each  $W_i$  is totally ordered, then  $P$  is totally ordered relative to the lexicographic order but not, in general, relative to the product order. If each  $W_i$  is well-ordered, then  $P$  is well-ordered relative to the lexicographic order;  $P$  is not, in general, well-ordered relative to the product order, but it is true that then every infinite sequence of elements of  $P$  has an infinite subsequence that is increasing (not necessarily strictly); in particular, every nonempty subset of  $P$  then has a minimal element.

The set  $\mathbb{N}$  is well-ordered relative to its usual order, as is the finite set  $\mathbb{N}_n$  consisting of the  $n$  numbers  $1, 2, \dots, n$ .

**Lemma 15** (a) *Every infinite sequence of elements of  $\mathbb{N}^m \times \mathbb{N}_n$  has an infinite subsequence, increasing relative to the product order, in which every term has the same projection on  $\mathbb{N}_n$ .*

(b)  $\mathbb{N}^m \times \mathbb{N}_n$  can be totally ordered so as to satisfy (for all  $i_1, \dots, i_m, e_1, \dots, e_m, i_1', \dots, i_m' \in \mathbb{N}$  and all  $j, j' \in \mathbb{N}_n$ ) the two conditions

$$(i_1, \dots, i_m, j) \leq (i_1 + e_1, \dots, i_m + e_m, j),$$

$$(i_1, \dots, i_m, j) \leq (i_1', \dots, i_m', j') \Rightarrow (i_1 + e_1, \dots, i_m + e_m, j) \leq (i_1' + e_1, \dots, i_m' + e_m, j').$$

(c) Relative to any total order satisfying the first of these conditions,  $\mathbb{N}^m \times \mathbb{N}_n$  is well-ordered.

*Proof* (a) As remarked above, some infinite subsequence is increasing relative to the product order. Since  $\mathbb{N}_n$  is finite, infinitely many terms of this subsequence have the same projection on  $\mathbb{N}_n$ .

(b) The lexicographic order satisfies the two conditions as does the lexicographic order with respect to  $(\sum i_\mu, j, i_1, \dots, i_m)$ , that is, the order on  $\mathbb{N}^m \times \mathbb{N}_n$  induced by the lexicographic order on  $\mathbb{N} \times \mathbb{N}_n \times \mathbb{N}^m$  via the injective mapping  $(i_1, \dots, i_m, j) \mapsto (\sum i_\mu, j, i_1, \dots, i_m)$  of  $\mathbb{N}^m \times \mathbb{N}_n$  into  $\mathbb{N} \times \mathbb{N}_n \times \mathbb{N}^m$ .

(c) By (a) an infinite sequence in  $\mathbb{N}^m \times \mathbb{N}_n$  has an infinite subsequence, increasing relative to the product order, in which all terms have the same projection on  $\mathbb{N}_n$ . This subsequence obviously is increasing relative to any order satisfying the first condition in (b). Thus, relative to any such order, every strictly decreasing sequence is finite, so that if the order is total, then  $\mathbb{N}^m \times \mathbb{N}_n$  is well-ordered.

We shall have occasion to consider polynomials in one indeterminate  $X$  over  $\mathbb{R}$ . The degree of such a polynomial is defined in the usual way with the proviso that the polynomial 0 have degree  $-1$ . If  $f \in \mathbb{R}[X]$  and  $\deg f \leq m$ , then there exist unique  $a_0, a_1, \dots, a_m \in \mathbb{R}$  such that  $f = \sum_{0 \leq i \leq m} a_i \binom{X+i}{i}$ , where  $\binom{X}{i}$  denotes the "binomial coefficient" polynomial  $X(X-1)\dots(X-i+1)/i! \in \mathbb{Q}[X]$  of degree  $i$ . We can introduce a total order on  $\mathbb{R}[X]$  by defining  $f \leq g$  to mean that  $f(s) \leq g(s)$  for all sufficiently big  $s \in \mathbb{N}$ . If  $f = \sum_{0 \leq i \leq m} a_i \binom{X+i}{i}$  and  $g = \sum_{0 \leq i \leq m} b_i \binom{X+i}{i}$ , then  $f \leq g$  if and only if  $(a_m, \dots, a_1, a_0) \leq (b_m, \dots, b_1, b_0)$  relative to the lexicographic order on  $\mathbb{R}^{m+1}$ .

By a numerical polynomial we shall mean a polynomial  $f \in \mathbb{R}[X]$  such that  $f(s) \in \mathbb{Z}$  for all sufficiently big  $s \in \mathbb{N}$ . The polynomials  $\binom{X}{i}$  are numerical, and therefore so is every  $\sum_{0 \leq i \leq m} a_i \binom{X+i}{i}$  with  $a_0, a_1, \dots, a_m \in \mathbb{Z}$ . Conversely, if  $f = \sum_{0 \leq i \leq m} a_i \binom{X+i}{i}$  is numerical, then  $a_0, a_1, \dots, a_m \in \mathbb{Z}$ . Indeed, if  $\deg f = m \geq 0$ , then

$$\Delta f = f(X+1) - f(X) = \sum_{0 \leq i \leq m-1} a_{i+1} \binom{X+1+i}{i}$$

as we see from the relation  $\Delta \binom{X}{i} = \binom{X}{i-1}$ , so that  $\deg \Delta f = m-1$ . Since  $\Delta f$  is obviously numerical whenever  $f$  is, the result follows from this formula by induction. From this result and this formula it also follows that  $f$  is

numerical whenever  $\Delta f$  is numerical and  $f(s) \in \mathbb{Z}$  for some  $s \in \mathbb{Z}$ ; also, if  $f$  is numerical, then  $f(s) \in \mathbb{Z}$  for all  $s \in \mathbb{Z}$ .

**Lemma 16** Let  $\mathbf{E}$  be a subset of  $\mathbb{N}^m$ , considered as an ordered set relative to the product order. Let  $\mathbf{V}$  denote the set of all points of  $\mathbb{N}^m$  that are not greater than or equal to any point of  $\mathbf{E}$ . Let  $\mathbf{W}$  denote the set of all points of  $\mathbf{V}$  that are less than or equal to only finitely many points of  $\mathbf{V}$ .

(a)  $\mathbf{W}$  is a finite set.

(b) There exists a numerical polynomial  $\omega_{\mathbf{E}}$  such that, for every sufficiently big  $s \in \mathbb{N}$ , the number of points  $(v_1, \dots, v_m) \in \mathbf{V}$  with  $\sum v_i \leq s$  is equal to  $\omega_{\mathbf{E}}(s)$ .

(c)  $\deg \omega_{\mathbf{E}} \leq m$ ; equality occurs if and only if  $\mathbf{E}$  is empty, in which case  $\omega_{\mathbf{E}} = \binom{X+m}{m}$ .

(d)  $\omega_{\mathbf{E}} = 0$  if and only if  $(0, \dots, 0) \in \mathbf{E}$ .

(e) If  $\mathbf{E} \cup \mathbf{W}$  contains a smallest point  $(e_1, \dots, e_m)$ , then

$$\omega_{\mathbf{E}} = \binom{X+m}{m} - \binom{X - \sum e_i + m}{m} + \text{Card } \mathbf{W}.$$

Conversely, if

$$\omega_{\mathbf{E}} = \binom{X+m}{m} - \binom{X-e+m}{m} + a$$

with  $a, e \in \mathbb{R}$ , then  $\mathbf{E} \cup \mathbf{W}$  has a smallest point.

*Proof* It is clear that if we replace  $\mathbf{E}$  by the set of its minimal points, then  $\mathbf{V}$  and  $\mathbf{W}$  will remain the same. Since every infinite sequence in  $\mathbb{N}^m$  has an infinite increasing subsequence, this set of minimal points is finite. Therefore we may suppose that  $\mathbf{E}$  is finite. Then we may set  $\bar{e}_i = \max_{(e_1, \dots, e_m) \in \mathbf{E}} e_i$  ( $1 \leq i \leq m$ ) and  $|\mathbf{E}| = \sum_{(e_1, \dots, e_m) \in \mathbf{E}} \sum_{1 \leq i \leq m} e_i$ .

If  $(v_1, \dots, v_m) \in \mathbf{V}$  and  $v_1 \geq \bar{e}_1$ , then  $(v_1 + j, v_2, \dots, v_m) \in \mathbf{V}$  for every  $j \in \mathbb{N}$ , so that  $(v_1, \dots, v_m) \notin \mathbf{W}$ . Therefore if  $(v_1, \dots, v_m) \in \mathbf{W}$ , then  $v_1 < \bar{e}_1$  and, similarly,  $v_i < \bar{e}_i$  for every  $i$ . Hence  $\text{Card } \mathbf{W} \leq \bar{e}_1 \dots \bar{e}_m$ . This proves (a).

Let  $N_{\mathbf{E}}(s)$  denote the number of points  $(v_1, \dots, v_m) \in \mathbf{V}$  with  $\sum_{1 \leq i \leq m} v_i \leq s$ . For each such point either  $v_m = 0$  and  $\sum_{1 \leq i \leq m-1} v_i \leq s$  or else  $v_m = v_m' + 1$  with  $v_m' \in \mathbb{N}$  and  $\sum_{1 \leq i \leq m-1} v_i + v_m' \leq s-1$ . Therefore if  $\mathbf{E}_0$  denotes the set of points  $(e_1, \dots, e_{m-1}) \in \mathbb{N}^{m-1}$  such that  $(e_1, \dots, e_{m-1}, 0) \in \mathbf{E}$ , and  $\mathbf{E}_1$  denotes the set of points  $(e_1, \dots, e_{m-1}, e_m') \in \mathbb{N}^m$  such that either  $(e_1, \dots, e_{m-1}, e_m' + 1) \in \mathbf{E}$ , or  $e_m' = 0$  and  $(e_1, \dots, e_{m-1}, 0) \in \mathbf{E}$ , then  $N_{\mathbf{E}}(s) = N_{\mathbf{E}_0}(s) + N_{\mathbf{E}_1}(s-1)$ .

We prove the existence of the polynomial  $\omega_{\mathbf{E}}$  with the property described in (b) by induction on  $|\mathbf{E}|$ . If  $|\mathbf{E}| = 0$ , then either  $\mathbf{E}$  is empty or  $\mathbf{E}$  consists solely of the point  $(0, \dots, 0)$ . In the former case  $N_{\mathbf{E}}(s)$  equals the number  $N_m(s)$  of points  $(v_1, \dots, v_m) \in \mathbb{N}^m$  with  $\sum_{1 \leq i \leq m} v_i \leq s$ , and the above equation becomes  $N_m(s) = N_{m-1}(s) + N_m(s-1)$ . We find by induction on  $m+s$  that

$N_m(s) = \binom{s+m}{m}$ , so that we may take  $\omega_E = \binom{X+m}{m}$ . In the latter case  $V$  is empty so that  $N_E(s) = 0$ , and we may take  $\omega_E = 0$ . Now let  $|E| > 0$  and suppose the existence of  $\omega_E$  established for lower values of  $|E|$ . Then  $E$  contains a point different from  $(0, \dots, 0)$ ; permuting the indices, we may suppose that  $E$  contains a point with nonzero  $m$ th coordinate. Then  $|E_0| < |E|$  and  $|E_1| < |E|$ , so that  $\omega_{E_0}$  and  $\omega_{E_1}$  exist. It is now clear that we may take

$$\omega_E(X) = \omega_{E_0}(X) + \omega_{E_1}(X-1). \quad (6)$$

This proves (b).

We have already seen that if  $E$  is empty, then  $\omega_E = \binom{X+m}{m}$ . If  $E$  contains a point  $(e_1, \dots, e_m)$ , then no point of  $V$  is of the form  $(e_1 + u_1, \dots, e_m + u_m)$  with  $(u_1, \dots, u_m) \in \mathbb{N}^m$  and  $\sum_{1 \leq i \leq m} u_i \leq s - \sum_{1 \leq i \leq m} e_i$ , so that for big values of  $s \in \mathbb{N}$ ,

$$\omega_E(s) \leq N_m(s) - N_m\left(s - \sum_{1 \leq i \leq m} e_i\right) = \binom{s+m}{m} - \binom{s - \sum e_i + m}{m},$$

whence  $\deg \omega_E < m$ . This proves (c). The proof of (d) is obvious.

Before proving (e) we observe that an easy induction argument making use of (6) shows that if, for each  $i$ ,  $E$  contains a point with vanishing  $i$ th coordinate, then  $\deg \omega_E \leq m-2$ .

It is evident that replacing  $E$  by  $E \cup W$  has the effect of replacing  $V$  and  $W$  by  $V-W$  and  $\emptyset$ , respectively; therefore  $\omega_E = \omega_{E \cup W} + \text{Card } W$ . If  $E \cup W$  has a smallest point  $(e_1, \dots, e_m)$ , then a point is in  $V-W$  if and only if it is not of the form  $(e_1 + u_1, \dots, e_m + u_m)$ , so that  $\omega_{E \cup W} = \binom{X+m}{m} - \binom{X - \sum e_i + m}{m}$ , and therefore  $\omega_E = \binom{X+m}{m} - \binom{X - \sum e_i + m}{m} + \text{Card } W$ .

Conversely, let  $\omega_E = \binom{X+m}{m} - \binom{X-e+m}{m} + a$ . If  $\deg \omega_E \leq 0$ , then  $N_E(s)$  is bounded, and  $V$  is finite; in this case  $V = W$ , so that  $(0, \dots, 0) \in E \cup W$ . Suppose then that  $\deg \omega_E \geq 1$ . Then  $m \geq 2$  and  $e \neq 0$  whence  $\deg \omega_E = m-1$ , so that by our observation above there is an index  $i$  such that every point of  $E$  has nonvanishing  $i$ th coordinate. Permuting the indices, we may suppose that  $m$  is such an index. Then the set  $E_0$  in (6) is empty, so that by (c)  $\omega_{E_0} = \binom{X+m-1}{m-1}$ , and therefore

$$\begin{aligned} \omega_{E_1}(X) &= \omega_E(X+1) - \omega_{E_0}(X+1) \\ &= \binom{X+1+m}{m} - \binom{X+1-e+m}{m} + a - \binom{X+m}{m-1} \\ &= \binom{X+m}{m} - \binom{X+1-e+m}{m} + a. \end{aligned}$$

Thus, if we replace  $E, e, a$  by  $E_1, e-1, a$ , respectively, the hypothesis remains satisfied. Furthermore, as every point of  $E$  has nonvanishing  $m$ th coordinate,  $W$  is replaced by the set  $W_1$  consisting of all points  $(v_1, \dots, v_m)$  such that

$(v_1, \dots, v_{m-1}, v_m+1) \in W$  and obviously  $\text{Card } W_1 = \text{Card } W$ . However,  $|E_1| < |E|$ , so that we may assume, inductively, that  $E_1 \cup W_1$  contains a smallest point  $(e_1', \dots, e_m')$ ,  $e-1 = \sum e_i'$ , and  $a = \text{Card } W_1$ . Then  $E \cup W$  contains a smallest point  $(e_1, \dots, e_m) = (e_1', \dots, e_{m-1}', e_m'+1)$ ,  $e = \sum e_i$ , and  $a = \text{Card } W$ . This completes the proof of the lemma.

## EXERCISES

- Let  $(a_{ik})_{1 \leq i \leq m, 1 \leq k \leq s}$  be a matrix over  $\mathbf{R}$  with the following two properties: the rank of the matrix is  $m$ ; for each index  $i$  if  $k(i)$  denotes the smallest  $k$  with  $a_{ik} \neq 0$ , then  $a_{i, k(i)} > 0$ . Show that the order on  $\mathbf{N}^m$ , induced by the lexicographic order on  $\mathbf{R}^s$  via the injective mapping  $(v_1, \dots, v_m) \mapsto (\sum a_{i1} v_i, \dots, \sum a_{is} v_i)$  of  $\mathbf{N}^m$  into  $\mathbf{R}^s$ , satisfies the two conditions of Lemma 15(b).
- (more difficult) Prove that every total order on  $\mathbf{N}^m$  satisfying the two conditions of Lemma 15(b) can be obtained as in Exercise 1.

## 18 Shapiro's lemma

The following lemma, which will not be needed until Chapter IV, Part B, was proved by Arnold Shapiro in 1961. For any set  $K$  we denote the set of all nonempty subsets of  $K$  by  $\mathfrak{P}'(K)$ .

**Lemma 17** *Let  $K$  be a nonempty finite set, let  $(a_k)_{k \in K}$  be a family with  $a_k \in \mathbf{R}$  and  $a_k \geq 0$  ( $k \in K$ ), let  $(x_J)_{J \in \mathfrak{P}'(K)}$  be a family with  $x_J \in \mathbf{R}$  and  $x_J \geq 0$  ( $J \in \mathfrak{P}'(K)$ ), and suppose that*

$$\sum_{J \in \mathfrak{P}'(K) - \mathfrak{P}'(K-I)} x_J > \sum_{i \in I} a_i \quad (I \in \mathfrak{P}'(K)). \quad (7)$$

*Then there exist numbers  $x_{J,j} \in \mathbf{R}$  with  $x_{J,j} \geq 0$  ( $J \in \mathfrak{P}'(K), j \in J$ ) such that*

$$\sum_{j \in J} x_{J,j} = x_J \quad (J \in \mathfrak{P}'(K))$$

*and*

$$\sum_{j \in J} x_{J,j} > a_j \quad (j \in K).$$

**REMARK 1** We may think of the elements of  $K$  as representing the vertices of a simplex, the nonempty subsets of  $K$  as representing the faces of that simplex, the numbers  $a_j$  as forming a system of masses located at the vertices, and the numbers  $x_J$  as forming a system of masses located on the faces. The lemma then asserts that if, for each face  $I$ , the sum of the masses of the second system located on the faces touching  $I$  exceeds the sum of the masses of the first system located at the vertices of  $I$ , then the mass on each face can be



redistributed among the vertices of that face in such a way that, for each vertex, the redistributed mass of the second system at that vertex exceeds the mass of the first system there.

**REMARK 2** The proof shows that the numbers  $x_{J,j}$  may be taken in the field  $\mathbf{Q}((a_k)_{k \in K}, (x_j)_{J \in \mathfrak{P}(K)})$ .

*Proof* Let  $s = \text{Card } K$ . There exists a  $J \in \mathfrak{P}(K)$  with  $x_J > 0$ , and therefore there exists a unique  $r \in \mathbf{N}$  such that  $x_J \neq 0$  for some  $J$  with  $\text{Card } J = r$  but  $x_J = 0$  for all  $J$  with  $\text{Card } J > r$ ; of course  $1 \leq r \leq s$ . Let  $t$  denote the number of elements  $J \in \mathfrak{P}(K)$  with  $\text{Card } J = r$  and  $x_J \neq 0$ ; then  $t > 0$ . If  $r = 1$ , then the nonzero masses of the second system are already all at the vertices, so that the result is trivial. Therefore we may assume that  $r > 1$ . We assume, too, that the result has been proved for lower values of  $(s, r, t)$  in the lexicographically well-ordered set  $\mathbf{N}^3$ .

Fix some  $I_0 \in \mathfrak{P}(K)$  with  $\text{Card } I_0 = r$  and  $x_{I_0} \neq 0$ , and fix some  $k \in I_0$ . Let  $J_1$  denote the set of elements of  $I_0$  other than  $k$ . Then  $K - I_0 \subset K - I_1 \subset K$ , so that the system of inequalities (7) can be written as three subsystems:

(7a) corresponding to  $I \in \mathfrak{P}(K - I_0)$ ,

(7b) corresponding to  $I \in \mathfrak{P}(K - I_1) - \mathfrak{P}(K - I_0)$ ,

(7c) corresponding to  $I \in \mathfrak{P}(K) - \mathfrak{P}(K - I_1)$ .

The left members in (7a) contain neither of the terms  $x_{I_0}, x_{J_1}$ , and the left members in (7c) contain both these terms; the left members in (7b) contain  $x_{I_0}$  but not  $x_{J_1}$ . It follows that if  $\zeta \in \mathbf{R}$ ,  $\zeta > 0$ , and if we replace  $x_{I_0}$  by  $x_{I_0} - \zeta$  and  $x_{J_1}$  by  $x_{J_1} + \zeta$ , then (7a) and (7c) remain valid. The system (7b) remains valid provided  $\zeta$  is sufficiently small. If (7b) remains valid for  $\zeta = x_{I_0}$ , then the replacement transforms the original system (7) into a similar system with a lower value for  $(s, r, t)$ . We may therefore suppose that at least one of the inequalities (7b) fails after the replacement using  $\zeta = x_{I_0}$ . Then there is a smallest value for  $\zeta$ , and we denote it simply by  $\zeta$ , such that after the replacement (7b) fails to hold. Using this  $\zeta$  we see that (7b) becomes a system (7b') of *weak* inequalities in the same direction. Obviously  $0 < \zeta \leq x_{I_0}$ , and at least one of the weak inequalities (7b') is an equality.

From among all the  $I \in \mathfrak{P}(K - I_1) - \mathfrak{P}(K - I_0)$  for which the corresponding inequality (7b') is an equality, choose a maximal one, say  $K'$ , and set  $K'' = K - K'$ . Then

$$\sum_{J \in \mathfrak{P}(K) - \mathfrak{P}(K'')} x_J = \sum_{i \in K'} a_i. \quad (8)$$

Consider any  $I'' \in \mathfrak{P}(K'')$ . Writing  $I = K' \cup I''$ , we see that either  $I \notin \mathfrak{P}(K - I_1)$  and  $I$  corresponds to an inequality (7c) or else  $I \in \mathfrak{P}(K - I_1) - \mathfrak{P}(K - I_0)$  and  $I$  corresponds to an inequality (7b'). In either case the

inequality is strict. Subtracting from it Eq. (8) we obtain

$$\sum_{J \in \mathfrak{P}(K'') - \mathfrak{P}(K' - I'')} x_J > \sum_{i \in I''} a_i \quad (I'' \in \mathfrak{P}(K'')). \quad (9)$$

On the other hand, if we start with some  $I \in \mathfrak{P}(K')$ , then either  $I \in \mathfrak{P}(K - I_0)$  and we have a strict inequality (7a) or else  $I \in \mathfrak{P}(K - I_1) - \mathfrak{P}(K - I_0)$  and we have a weak inequality (7b'). If we now reduce  $\zeta$  slightly, still keeping it positive, then the inequalities (7a) remain valid, and the inequalities (7b') all become strict, that is, we regain (7b). Furthermore, if the amount by which we reduce  $\zeta$  is sufficiently small, then (9) remains valid, too. Then, in addition to (9) we obtain (denoting  $I$  by  $I'$ )

$$\sum_{J \in \mathfrak{P}(K') - \mathfrak{P}(K - I')} x_J > \sum_{i \in I'} a_i \quad (I' \in \mathfrak{P}(K')). \quad (10)$$

If  $J \in \mathfrak{P}(K) - \mathfrak{P}(K - I')$ , then  $J \in \mathfrak{P}(K) - \mathfrak{P}(K - K')$  and therefore this  $J$  does not occur in the left side of (9). For each  $J \in \mathfrak{P}(K) - \mathfrak{P}(K - K')$  we now decrease  $x_J$  and increase  $x_{J \cap K'}$  by the same amount  $x_J$  (that is, we shift the entire mass  $x_J$  from the face  $J$  to the face  $J \cap K'$ ). This does not affect the inequalities (9), and replaces the inequalities (10) by

$$\sum_{J \in \mathfrak{P}(K') - \mathfrak{P}(K' - I')} x_J > \sum_{i \in I'} a_i \quad (I' \in \mathfrak{P}(K')). \quad (11)$$

Since  $\text{Card } K' < s$  and  $\text{Card } K'' < s$ , the lemma holds for each of the two systems (9) and (11). It is now a simple matter to see that the lemma holds for the original system (7).

**Corollary** Let  $K$  be a finite set, let  $a_k \in \mathbf{N}$  ( $k \in K$ ), let  $x_j \in \mathbf{N}$  ( $J \in \mathfrak{P}(K)$ ), and suppose that

$$\sum_{J \in \mathfrak{P}(K) - \mathfrak{P}(K - I)} x_J > \sum_{i \in I} a_i \quad (I \in \mathfrak{P}(K)).$$

Then, for each sufficiently big  $h \in \mathbf{N}$ , there exist  $y_{J,j} \in \mathbf{N}$  ( $J \in \mathfrak{P}(K)$ ,  $j \in J$ ) such that

$$\sum_{j \in J} y_{J,j} = hx_J \quad (J \in \mathfrak{P}(K))$$

and

$$\sum_{j \in J} y_{J,j} > ha_j \quad (j \in K).$$

*Proof* There exist (see Remark 2 after Lemma 17) *rational* numbers  $x_{J,j}$  satisfying the conclusion of the lemma. There obviously exists a  $\zeta > 0$ , smaller than every nonzero  $x_{J,j}$ , such that if we set

$$x'_{J,j} = \begin{cases} x_{J,j} - \zeta & (x_{J,j} \neq 0), \\ 0 & (x_{J,j} = 0), \end{cases}$$

then  $\sum_{j \in J} x'_{j,j} > a_j$  ( $j \in K$ ); of course  $\sum_{j \in J} x'_{j,j} \leq x_j$ . For any  $h \in \mathbf{N}$  with  $h \geq \xi^{-1}$  there exist  $x''_{j,j} \in h^{-1}\mathbf{N}$  such that  $x'_{j,j} \leq x''_{j,j} \leq x_{j,j}$ , and for such  $x''_{j,j}$  obviously

$$\sum_{j \in J} x''_{j,j} \leq x_j \quad (J \in \mathfrak{P}'(K)) \quad \text{and} \quad \sum_{j \in J} x''_{j,j} > a_j \quad (j \in K).$$

For each  $J \in \mathfrak{P}'(K)$  fix an element  $i(J) \in J$  and set

$$y_{J,j} = hx''_{j,j} \quad (j \in J, j \neq i(J)) \quad \text{and} \quad y_{J,i(J)} = hx''_{j,i(J)} + hx_J - \sum_{j \in J} hx''_{j,j}.$$

It is easy to see that the numbers  $y_{J,j}$  have the required properties.

## 19 $\mathfrak{f}$ -Values

Let  $R$  be a ring and let  $\mathfrak{f}$  be an ideal of  $R$ . For any  $x \in R$  let  $\mu_{\mathfrak{f}}(x)$  denote the biggest integer  $m$  with  $x \in \mathfrak{f}^m$  if the set of such integers  $m$  is bounded, and denote the symbol  $\infty$  otherwise. It is clear that if  $\mathfrak{f} \neq R$ , then  $\mu_{\mathfrak{f}}(\pm 1) = 0$ , whereas  $\mu_R(x) = \infty$  ( $x \in R$ ).

We adopt the convention that

$$\begin{aligned} \infty > \alpha, \quad \infty + \alpha = \alpha + \infty = \infty + \infty = \infty \quad (\alpha \in \mathbf{R}), \\ \alpha \infty = \infty \alpha = \infty \infty = \infty \quad (\alpha \in \mathbf{R}, \alpha > 0). \end{aligned}$$

It is then apparent that

$$\begin{aligned} \mu_{\mathfrak{f}}(x_1 \pm x_2) &\geq \min(\mu_{\mathfrak{f}}(x_1), \mu_{\mathfrak{f}}(x_2)) \quad (x_1, x_2 \in R), \\ \mu_{\mathfrak{f}}(x_1 x_2) &\geq \mu_{\mathfrak{f}}(x_1) + \mu_{\mathfrak{f}}(x_2) \quad (x_1, x_2 \in R), \\ \mu_{\mathfrak{f}}(x^n) &\geq n\mu_{\mathfrak{f}}(x) \quad (x \in R, n \in \mathbf{N}, n \neq 0). \end{aligned}$$

We also show that

$$\lim_{n \rightarrow \infty} n^{-1} \mu_{\mathfrak{f}}(x^n) = \sup_{n > 0} n^{-1} \mu_{\mathfrak{f}}(x^n) \quad (x \in R).$$

For this it suffices to show that whenever  $\alpha \in \mathbf{R}$ ,  $\alpha > 0$ , and  $\alpha < \sup_{n > 0} n^{-1} \mu_{\mathfrak{f}}(x^n)$ , then  $n^{-1} \mu_{\mathfrak{f}}(x^n) > \alpha$  for all big  $n \in \mathbf{N}$ . Now, for any such  $\alpha$ , we may fix  $m \in \mathbf{N}$  with  $m > 0$  and  $m^{-1} \mu_{\mathfrak{f}}(x^m) > \alpha$ ; for any  $n \in \mathbf{N}$  with  $n > m$ , we may write  $n = qm + r$  with  $q, r \in \mathbf{N}$ ,  $q > 0$ , and  $r < m$ , so that

$$\begin{aligned} n^{-1} \mu_{\mathfrak{f}}(x^n) &= n^{-1} \mu_{\mathfrak{f}}(x^{qm} x^r) \\ &\geq n^{-1} \mu_{\mathfrak{f}}(x^{qm}) \\ &\geq n^{-1} \cdot (qm)(qm)^{-1} \cdot q \mu_{\mathfrak{f}}(x^m) \geq n^{-1} (n-m) \cdot m^{-1} \mu_{\mathfrak{f}}(x^m) \end{aligned}$$

which is greater than  $\alpha$  for all big values of  $n$ .

This being the case, we define  $v_{\mathfrak{f}}(x)$  by the equations

$$v_{\mathfrak{f}}(x) = \lim_{n \rightarrow \infty} n^{-1} \mu_{\mathfrak{f}}(x^n) = \sup_{n > 0} n^{-1} \mu_{\mathfrak{f}}(x^n),$$

and call  $v_{\mathfrak{f}}(x)$  the  $\mathfrak{f}$ -value of  $x$ . Thus,  $v_{\mathfrak{f}}(x)$  is either a real number greater than or equal to 0 or is the symbol  $\infty$ . If  $\mathfrak{f} \neq R$ , then  $v_{\mathfrak{f}}(\pm 1) = 0$ , whereas  $v_R(x) = \infty$  ( $x \in R$ ).

For any  $\alpha \in \mathbf{R}$ , to say that  $v_{\mathfrak{f}}(x) > \alpha$  is to say that there exist  $m, n \in \mathbf{N}$  with  $m > n\alpha$  such that  $x^m \in \mathfrak{f}^n$ .

**Proposition 12** Let  $\mathfrak{f}$  be an ideal of a ring  $R$ .

- (a)  $v_{\mathfrak{f}}(x_1 + x_2) \geq \min(v_{\mathfrak{f}}(x_1), v_{\mathfrak{f}}(x_2))$  ( $x_1, x_2 \in R$ ).
- (b)  $v_{\mathfrak{f}}(x_1 x_2) \geq v_{\mathfrak{f}}(x_1) + v_{\mathfrak{f}}(x_2)$  ( $x_1, x_2 \in R$ ).
- (c)  $v_{\mathfrak{f}}(x^n) = n v_{\mathfrak{f}}(x)$  ( $x \in R, n \in \mathbf{N}, n > 0$ ).

*Proof* (a) It suffices to show that for any  $\alpha \in \mathbf{R}$  with  $0 \leq \alpha < \min(v_{\mathfrak{f}}(x_1), v_{\mathfrak{f}}(x_2))$  there exists an  $n \in \mathbf{N}$  with  $n \neq 0$  such that  $\mu_{\mathfrak{f}}((x_1 + x_2)^n) > n\alpha$ . To this end, fix  $\beta \in \mathbf{R}$  such that  $\alpha < \beta < \min(v_{\mathfrak{f}}(x_1), v_{\mathfrak{f}}(x_2))$ . There exists an  $m \in \mathbf{N}$  so big that  $n^{-1} \mu_{\mathfrak{f}}(x_i^n) > \beta$  ( $i = 1, 2$ ) for all  $n \in \mathbf{N}$  with  $n > m$ . Now, for any  $n \in \mathbf{N}$ ,

$$\mu_{\mathfrak{f}}((x_1 + x_2)^n) = \mu_{\mathfrak{f}}\left(\sum_{i=0}^n \binom{n}{i} x_1^{n-i} x_2^i\right) \geq \min_{0 \leq i \leq n} (\mu_{\mathfrak{f}}(x_1^{n-i}) + \mu_{\mathfrak{f}}(x_2^i)).$$

Taking  $n > 2m\beta/(\beta - \alpha)$ , we see that we cannot have  $n - i \leq m$  and  $i \leq m$ , and that if  $n - i > m$  and  $i \leq m$ , then

$$\mu_{\mathfrak{f}}(x_1^{n-i}) + \mu_{\mathfrak{f}}(x_2^i) > (n-i)\beta \geq (n-m)\beta > n\alpha,$$

if  $n - i \leq m$  and  $i > m$ , then

$$\mu_{\mathfrak{f}}(x_1^{n-i}) + \mu_{\mathfrak{f}}(x_2^i) > i\beta \geq (n-m)\beta > n\alpha,$$

and if  $n - i > m$  and  $i > m$ , then

$$\mu_{\mathfrak{f}}(x_1^{n-i}) + \mu_{\mathfrak{f}}(x_2^i) > (n-i)\beta + i\beta = n\beta > n\alpha.$$

(b)  $v_{\mathfrak{f}}(x_1 x_2) = \lim_{n \rightarrow \infty} n^{-1} \mu_{\mathfrak{f}}(x_1^n x_2^n) \geq \lim_{n \rightarrow \infty} n^{-1} (\mu_{\mathfrak{f}}(x_1^n) + \mu_{\mathfrak{f}}(x_2^n)) = v_{\mathfrak{f}}(x_1) + v_{\mathfrak{f}}(x_2)$ .

(c)  $v_{\mathfrak{f}}(x^n) = \lim_{r \rightarrow \infty} r^{-1} \mu_{\mathfrak{f}}(x^{nr}) = n \lim_{r \rightarrow \infty} (nr)^{-1} \mu_{\mathfrak{f}}(x^{nr}) = n v_{\mathfrak{f}}(x)$ .

## Basic Notions of Differential Algebra

In this chapter we introduce the notions that are basic to all of differential algebra, and we go through some technical considerations that will facilitate the study of these notions in the subsequent chapters.

### 1 Differential rings

An operator  $\delta$  on a ring is called a *derivation operator* if  $\delta(a+b) = \delta a + \delta b$  and  $\delta(ab) = (\delta a)b + a\delta b$  for all elements  $a, b$  of the ring.

A *differential ring* is defined as a ring  $\mathcal{R}$  with a finite set  $\Delta$  of derivation operators on  $\mathcal{R}$  such that  $\delta\delta'a = \delta'\delta a$  ( $a \in \mathcal{R}$ ,  $\delta \in \Delta$ ,  $\delta' \in \Delta$ ). If the ring  $\mathcal{R}$  is an integral domain, or a field, we speak of a *differential integral domain*, or a *differential field*. If the number  $m = \text{Card}\Delta$  is 1, the differential ring is *ordinary*, and if  $m > 1$ , it is *partial*.<sup>1</sup>

**EXAMPLE 1** Any ring  $\mathcal{R}$  on which the elements of a finite set  $\Delta$  operate trivially ( $\delta a = 0$  for every  $a \in \mathcal{R}$  and every  $\delta \in \Delta$ ) is a differential ring.

**EXAMPLE 2** The ring of all real-valued functions defined and infinitely differentiable at every point of a given region in the space of  $m$  real variables  $x_1, \dots, x_m$ , with the set of operators  $\partial/\partial x_1, \dots, \partial/\partial x_m$ , is a differential ring.

<sup>1</sup> In the case  $m = 0$  the notion of differential ring reduces to that of ring. In this book we shall always suppose that  $m \geq 1$ , except in a few proofs in which we use induction on  $m$  and start with  $m = 0$ .

**EXAMPLE 3** The ring of all complex-valued functions defined and analytic at every point of a given region in the space of  $m$  complex variables  $x_1, \dots, x_m$ , with the set of operators  $\partial/\partial x_1, \dots, \partial/\partial x_m$ , is a differential integral domain.

**EXAMPLE 4** The field of all complex meromorphic functions on a given region in the space of  $m$  complex variables  $x_1, \dots, x_m$ , together with the set of operators  $\partial/\partial x_1, \dots, \partial/\partial x_m$ , is a differential field.

Let  $\mathcal{R}$  be a differential ring with set  $\Delta$  of derivation operators. Let  $\Theta$  denote the free commutative semigroup (written multiplicatively) generated by the elements of  $\Delta$ . Every element of  $\Theta$  can be expressed uniquely in the form of a product  $\prod_{\delta \in \Delta} \delta^{e(\delta)}$ , where each exponent  $e(\delta)$  is a natural number, and every such product is an element of  $\Theta$ . There is a unique way of making  $\Theta$  into a set of operators on  $\mathcal{R}$  consistent with the way in which the elements of  $\Delta$  already operate on  $\mathcal{R}$  and subject to the two conditions that  $1a = a$  and  $(\theta\theta')a = \theta(\theta'a)$  for all  $a \in \mathcal{R}$ ,  $\theta \in \Theta$ ,  $\theta' \in \Theta$  (1 here denoting the unity element of  $\Theta$ ). We call the elements of  $\Theta$  the *derivative operators* of the differential ring  $\mathcal{R}$ . If  $\theta = \prod_{\delta \in \Delta} \delta^{e(\delta)}$ , then the number  $s = \sum_{\delta \in \Delta} e(\delta)$  is called the *order* of  $\theta$ , and is denoted by  $\text{ord } \theta$ ; for any  $a \in \mathcal{R}$ ,  $\theta a$  is said to be a *derivative of a* of order  $s$ . In particular,  $a$  is its own derivative of order 0. A derivative of  $a$  of order greater than 0 is called a *proper derivative* of  $a$ . In the special case of an ordinary differential ring,  $\Delta$  consists of a single element  $\delta$ ; the derivatives  $\delta a, \delta^2 a, \delta^3 a, \delta^s a$ , are then frequently denoted by  $a', a'', a''', a^{(s)}$ , respectively.

If  $\mathcal{R}_0$  is a subring of the ring  $\mathcal{R}$  and is stable under  $\Delta$ , that is, has the property that  $\Delta\mathcal{R}_0 \subset \mathcal{R}_0$ , then the elements of  $\Delta$  become, on restriction, derivation operators of  $\mathcal{R}_0$ , and  $\mathcal{R}_0$  is then a differential ring with the same set of derivation operators  $\Delta$ ; we say in this case that  $\mathcal{R}_0$  is a *differential subring* of  $\mathcal{R}$ , and that  $\mathcal{R}$  is a *differential overring* of  $\mathcal{R}_0$ . The intersection of any set of differential subrings of  $\mathcal{R}$  is itself a differential subring of  $\mathcal{R}$ . Therefore if  $\Sigma$  is any set (or family) of elements of  $\mathcal{R}$ , there exists a smallest differential subring of  $\mathcal{R}$  containing all the elements of  $\mathcal{R}_0$  and of  $\Sigma$ ; it is called the *differential ring generated by  $\Sigma$  over  $\mathcal{R}_0$* , and is denoted by  $\mathcal{R}_0\{\Sigma\}$ , and  $\Sigma$  is said to be a set (or family) of generators of the differential ring  $\mathcal{R}_0\{\Sigma\}$  over  $\mathcal{R}_0$ . If  $\Sigma$  is a subset of  $\mathcal{R}$  and  $\Theta\Sigma$  denotes the set of all elements  $\theta a$  with  $\theta \in \Theta$  and  $a \in \Sigma$  (or if  $\Sigma$  is a family  $(a_i)_{i \in I}$  of elements of  $\mathcal{R}$  and  $\Theta\Sigma$  denotes the family  $(\theta a_i)_{\theta \in \Theta, i \in I}$ ), then  $\mathcal{R}_0\{\Sigma\}$  coincides, as a ring, with the ring  $\mathcal{R}_0[\Theta\Sigma]$  generated by  $\Theta\Sigma$  over  $\mathcal{R}_0$ . A differential overring of a differential ring  $\mathcal{R}_0$  is said to be *finitely generated over  $\mathcal{R}_0$*  if it has a finite set of generators over  $\mathcal{R}_0$ .

If  $\mathcal{F}_0$  and  $\mathcal{F}$  are differential fields such that  $\mathcal{F}_0$  is a differential subring of  $\mathcal{F}$ , then  $\mathcal{F}_0$  is said to be a *differential subfield* of  $\mathcal{F}$ , and  $\mathcal{F}$  is said to be a

differential overfield, or a differential field extension or simply an extension, of  $\mathcal{F}_0$ .<sup>2</sup>

The intersection of a set of differential subfields of  $\mathcal{F}$  is itself a differential subfield of  $\mathcal{F}$ . Therefore if  $\Sigma$  is a set (or family) of elements of  $\mathcal{F}$ , there exists a smallest differential subfield of  $\mathcal{F}$  containing all the elements of  $\mathcal{F}_0$  and of  $\Sigma$ ; we denote it by  $\mathcal{F}_0\langle\Sigma\rangle$ , call it the differential field obtained by adjoining the elements of  $\Sigma$  to  $\mathcal{F}_0$ , or the extension of  $\mathcal{F}_0$  generated by  $\Sigma$ , and say that  $\Sigma$  is a set (or family) of generators of the extension  $\mathcal{F}_0\langle\Sigma\rangle$  of  $\mathcal{F}_0$ . Then  $\mathcal{F}_0\langle\Sigma\rangle$  coincides, as a field, with the overfield  $\mathcal{F}_0(\Theta\Sigma)$  of  $\mathcal{F}_0$  generated by  $\Theta\Sigma$ .

An extension is said to be *finitely generated* if it has a finite set of generators, and is said to be *simply generated* if it has a set of generators consisting of a single element.† If  $\mathcal{F}_1$  and  $\mathcal{F}_2$  are both differential subfields of  $\mathcal{F}$ , then  $\Theta\mathcal{F}_1 = \mathcal{F}_1$  and  $\Theta\mathcal{F}_2 = \mathcal{F}_2$ , so that  $\mathcal{F}_1\langle\mathcal{F}_2\rangle = \mathcal{F}_1(\mathcal{F}_2) = \mathcal{F}_2(\mathcal{F}_1) = \mathcal{F}_2\langle\mathcal{F}_1\rangle$ ; this differential field is called the *compositum* of  $\mathcal{F}_1$  and  $\mathcal{F}_2$ , and is often denoted by  $\mathcal{F}_1\mathcal{F}_2$ .

An element  $c$  of a differential ring  $\mathcal{R}$  with set  $\Delta$  of derivation operators is said to be a *constant* if  $\delta c = 0$  for every  $\delta \in \Delta$ . The set of all constants of  $\mathcal{R}$  is a differential subring of  $\mathcal{R}$ , called the *ring of constants* of  $\mathcal{R}$ . The ring of constants of a differential field  $\mathcal{F}$  is a differential subfield of  $\mathcal{F}$ , called the *field of constants* of  $\mathcal{F}$ . The field of constants of  $\mathcal{F}$  always contains the prime field of  $\mathcal{F}$  and, if  $\mathcal{F}$  is of characteristic  $p \neq 0$ , contains the field  $\mathcal{F}^p$  of  $p$ th powers of elements of  $\mathcal{F}$ .

## EXERCISES

- Let  $\mathcal{R}$  be a differential ring with set of derivation operators  $\Delta$  and set of derivative operators  $\Theta$ . For all  $\theta = \prod_{\delta \in \Delta} \delta^{e(\delta)} \in \Theta$  and  $\theta' = \prod_{\delta \in \Delta} \delta^{e'(\delta)} \in \Theta$  with  $\theta' | \theta$  (i.e., with  $\theta'$  dividing  $\theta$  in  $\Theta$ ), define the natural number  $\binom{\theta}{\theta'} = \prod_{\delta \in \Delta} \binom{e(\delta)}{e'(\delta)}$ , product of binomial coefficients. Show that  $\theta(uv) = \sum_{\theta_1 | \theta} \binom{\theta}{\theta_1} (\theta/\theta_1) u \cdot \theta_1 v$  for all  $u, v \in \mathcal{R}$ . Prove that if  $\mathcal{R}$  has prime characteristic  $p$  then  $\delta^{p^e}$  is a derivation operator ( $\delta \in \Delta, e \in \mathbb{N}$ ).
- Prove that a finite differential field is its own field of constants.
- (Baer [4]) Let  $\mathcal{F}$  be an ordinary differential field of characteristic  $p \neq 0$  with field of constants  $\mathcal{C}$ , let  $a \in \mathcal{F}$ , and suppose that  $a$  is not the derivative of any element of  $\mathcal{F}$ .
  - Prove that if  $t$  is an element of an extension of  $\mathcal{F}$  with  $t \notin \mathcal{F}$ ,  $t^p \in \mathcal{F}$ ,  $t' \in \mathcal{F}$ , then  $a/t$  is not the derivative of any element of  $\mathcal{F}\langle t \rangle$ .
  - Prove that if  $t$  is an element of a field extension of  $\mathcal{F}$  with  $t \notin \mathcal{F}$

<sup>2</sup> In this book (except for Chapter V) the field theoretic notion generally associated with this word will always be called *field extension*, and the word "extension" unqualified by the word "field" will denote "differential field extension."

and  $t^p \in \mathcal{C}$ , then there is a unique way of extending the differential field structure on  $\mathcal{F}$  to  $\mathcal{F}\langle t \rangle$  so that  $t' = a$ ; show that the field of constants of the differential field  $\mathcal{F}\langle t \rangle$  is  $\mathcal{C}$ .

- (Baer [4]) Let  $C$  be a subfield of a field  $K$  of characteristic  $p \neq 0$  with  $K^p \subset C$ . Prove that there exists an ordinary differential field structure on  $K$  for which the field of constants is  $C$ . (*Hint*: Let  $T$  be a maximal subset of  $K$  that is separably independent (see Chapter 0, Section 2) over  $C$ , and show that  $C(T) = K$ . If  $T$  is empty, all is clear. If  $T$  is non-empty and finite, then adjoin its elements one by one using Exercise 3 to extend the differential field structure at each step. If  $T$  is infinite, use Zorn's lemma.)

## 2 Homomorphisms and differential ideals

Let  $\mathcal{R}$  and  $\mathcal{R}'$  be differential rings with the same set  $\Delta$  of derivation operators. A *differential ring homomorphism*, or simply a *homomorphism*, of  $\mathcal{R}$  into  $\mathcal{R}'$  is a ring homomorphism  $f: \mathcal{R} \rightarrow \mathcal{R}'$  such that  $f(\delta a) = \delta f(a)$  for all  $a \in \mathcal{R}$  and  $\delta \in \Delta$ . This definition carries with it, of course, corresponding definitions of *isomorphism*, *automorphism*, etc. If  $\mathcal{R}$  and  $\mathcal{R}'$  are differential overrings of a common differential ring  $\mathcal{R}_0$ ,  $f$  is called a *homomorphism over  $\mathcal{R}_0$* , or an  *$\mathcal{R}_0$ -homomorphism*, provided  $f(a) = a$  for every  $a \in \mathcal{R}_0$ .

The image  $f(\mathcal{R})$  of a homomorphism  $f: \mathcal{R} \rightarrow \mathcal{R}'$  is a differential subring of  $\mathcal{R}'$ . The kernel of  $f$  is an ideal of  $\mathcal{R}$  stable under  $\Delta$ . Any ideal of  $\mathcal{R}$  stable under  $\Delta$  is called a *differential ideal* of  $\mathcal{R}$ .

Let  $g$  be a surjective ring homomorphism of  $\mathcal{R}$  onto some ring  $\mathcal{S}$ . If the kernel of  $g$  happens to be a differential ideal, it is easy to see that there exists on  $\mathcal{S}$  a unique differential ring structure with set  $\Delta$  of derivation operators such that  $g$  is a differential ring homomorphism of  $\mathcal{R}$  into  $\mathcal{S}$ . If we apply this remark to the canonical ring homomorphism of  $\mathcal{R}$  onto the residue ring  $\mathcal{R}/\mathfrak{f}$  of  $\mathcal{R}$  modulo a differential ideal  $\mathfrak{f}$ , then  $\mathcal{R}/\mathfrak{f}$  becomes a differential ring, called the *differential residue ring* of  $\mathcal{R}$  modulo  $\mathfrak{f}$ .

The intersection of any family of differential ideals of  $\mathcal{R}$  is itself a differential ideal; similarly for the sum and, provided the family is finite, for the product. Also, if  $\mathfrak{f}$  is a differential ideal of  $\mathcal{R}$ , and  $\Sigma$  is any subset of  $\mathcal{R}$  stable under  $\Delta$ , then the quotient  $\mathfrak{f}:\Sigma$  is a differential ideal of  $\mathcal{R}$ .

Let  $\Sigma$  be any set (or family) of elements of  $\mathcal{R}$ . The intersection of all the differential ideals containing the elements of  $\Sigma$ , which obviously is the smallest differential ideal containing the elements of  $\Sigma$ , is called the *differential ideal of  $\mathcal{R}$  generated by  $\Sigma$* , and is denoted by  $[\Sigma]_{\mathcal{R}}$  or, when there is no danger of ambiguity concerning the differential ring  $\mathcal{R}$ , simply by  $[\Sigma]$ . Set-theoretically,  $[\Sigma]$  coincides with the ideal  $(\Theta\Sigma)$  of  $\mathcal{R}$  generated by  $\Theta\Sigma$ .

**Lemma 1** Let  $a$  and  $b$  be elements of a differential ring, let  $h \in \mathbb{N}$ , and let  $\theta$  be a derivative operator of order  $h$ . Then  $a^{h+1}\theta b \in [ab]$ . More precisely,  $a^{h+1}\theta b$  is in the ideal generated by all the derivatives  $\theta_1(ab)$  with  $\theta_1$  dividing  $\theta$ .

*Proof* If  $h > 0$ , we may write  $\theta = \delta\theta'$  with  $\delta$  a derivation operator and  $\theta'$  a derivative operator of order  $h-1$ . Computing  $\delta(a^h\theta'b)$  and multiplying by  $a$ , we find that  $a^{h+1}\theta b \in (a^h\theta'b, \delta(a^h\theta'b))$ . Since the case  $h = 0$  is obvious, the general result follows by induction.

**Corollary** Let  $a$  be an element and  $\mathfrak{f}$  be a differential ideal of a differential ring. Then  $\mathfrak{f}:a^\infty$  is a differential ideal.

*Proof* If  $b \in \mathfrak{f}:a^\infty$ , then  $a^n b \in \mathfrak{f}$  for some  $n \in \mathbb{N}$ . By the lemma (case  $h = 1$ ), for every derivation operator  $\delta$ ,  $a^{n+1}\delta b \in [a^n b] \subset \mathfrak{f}$ , so that  $\delta b \in \mathfrak{f}:a^\infty$ .

**Lemma 2** Let  $a$  be an element of a differential ring, let  $h \in \mathbb{N}$ , and let  $\delta_1, \dots, \delta_{2h-1}$  be derivation operators (not necessarily distinct). Then  $h! \prod_{1 \leq \lambda \leq 2h-1} (\delta_\lambda a) \in [a^h]$ .

*Proof* We may suppose that  $h > 0$ . The desired result is the case  $i = h$  of the more general result

$$h(h-1)\cdots(h-i+1)a^{h-i} \prod_{1 \leq \lambda \leq 2i-1} (\delta_\lambda a) \in [a^h] \quad (1 \leq i \leq h).$$

The case  $i = 1$  is obvious since  $ha^{h-1}\delta_1 a = \delta_1(a^h)$ . Assuming the case  $i = r$  (for a particular  $r < h$ ), apply  $\delta_{2r}$  and then multiply by  $\delta_{2r+1} a$ . The case  $i = r+1$  then follows.

**Corollary** Let  $a$  be an element of a differential ring with  $m$  derivation operators, let  $h, k \in \mathbb{N}$ ,  $h > 0$ , let

$$c = c(k, h) = \prod_{0 \leq i < k} (2^i(h-1) + 1)!,$$

$$d = d(k, h, m) = \begin{cases} h & (k = 0), \\ 2(h-1)(2m)^{k-1} + 1 & (k > 0), \end{cases}$$

and let  $\theta_1, \dots, \theta_d$  be derivative operators of order  $k$ . Then

$$c \prod_{1 \leq \lambda \leq d} (\theta_\lambda a) \in [a^h].$$

*Proof* For  $k = 0$  the result is obvious, and for  $k = 1$  it reduces to Lemma 2. Let  $k > 1$  and suppose the result proved for lower values of  $k$  (and all values of  $h$ ). Setting  $c' = c(k-1, 2h-1)$  and  $d' = d(k-1, 2h-1, m)$ , we see that  $c = h!c'$  and  $d = m(d'-1) + 1$ . If, for every one of the  $m$  derivation

operators  $\delta$ , no more than  $d'-1$  of the derivative operators  $\theta_1, \dots, \theta_d$  were divisible by  $\delta$  we should have  $d \leq m(d'-1)$ . Therefore some  $\delta$  divides at least  $d'$  of the operators  $\theta_1, \dots, \theta_d$ , so that  $c \prod_{1 \leq \lambda \leq d} (\theta_\lambda a)$  is a multiple of  $h!c' \prod_{1 \leq \lambda' \leq d'} (\theta_{\lambda'} \delta a)$ , where  $\theta_{\lambda'}, \dots, \theta_{d'}$  are derivative operators of order  $k-1$ . Hence, by the inductive hypothesis and Lemma 2,

$$c \prod_{1 \leq \lambda \leq d} (\theta_\lambda a) \in [h!(\delta a)^{2h-1}] \subset [a^h].$$

### EXERCISES

- (See Ritt [95, pp. 14–16]) Let  $\mathfrak{f}$  be a differential ideal of a differential ring  $\mathcal{R}$ .
  - Show that if  $a_1, a_2 \in \mathcal{R}$ ,  $a_1 + a_2 = 1$ , and  $a_1, a_2 \in \mathfrak{f}$ , then  $[a_i] \subset (a_i) + \mathfrak{f}$  ( $i = 1, 2$ ),  $(a_i) + \mathfrak{f}$  is a differential ideal of  $\mathcal{R}$  ( $i = 1, 2$ ), and  $\mathfrak{f} = [(a_1) + \mathfrak{f}] \cap [(a_2) + \mathfrak{f}] = [(a_1) + \mathfrak{f}] \cdot [(a_2) + \mathfrak{f}]$ .
  - Let  $I$  be an ideal of  $\mathcal{R}$  with  $I \supset \mathfrak{f}$  such that every element of  $I$  has a power contained in  $\mathfrak{f}$ , and let  $I_1, I_2$  be ideals of  $\mathcal{R}$  such that  $I_1 + I_2 = \mathcal{R}$  and  $I_1 \cap I_2 = I$ . Show that there exist unique differential ideals  $\mathfrak{f}_1, \mathfrak{f}_2$  of  $\mathcal{R}$  such that every element of  $I_i$  has a power contained in  $\mathfrak{f}_i$  ( $i = 1, 2$ ),  $\mathfrak{f}_1 + \mathfrak{f}_2 = \mathcal{R}$ , and  $\mathfrak{f}_1 \cap \mathfrak{f}_2 = \mathfrak{f}$ . Show that  $\mathfrak{f}_i \subset I_i$  ( $i = 1, 2$ ).
- (See Kolchin [36, Sections 2, 3]) Let the hypothesis and notation be as in Exercise 1(b).
  - For any two ideals  $\mathfrak{a}, \mathfrak{b}$  of  $\mathcal{R}$  define  $l_{\mathfrak{a}} \mathfrak{b}$  to be the smallest natural number  $n$  such that  $\mathfrak{b}^n \subset \mathfrak{a}$  if such an  $n$  exists and to be  $\infty$  otherwise. Show that  $l_i \mathfrak{f} = \max_{i=1,2} l_i \mathfrak{f}_i$ .
  - For any differential ideal  $\mathfrak{a}$  of  $\mathcal{R}$  set  $b(\mathfrak{a}) = \min_{\Phi} l_{\mathfrak{a}}[\Phi]$ , where  $\Phi$  runs over the set of all finite subsets of  $\mathfrak{a}$ . Show that  $b(\mathfrak{f}) = \max_{i=1,2} b(\mathfrak{f}_i)$ .
- Let  $S$  be a multiplicatively stable subset of the differential ring  $\mathcal{R}$ , and let  $\mathfrak{q}$  be a maximal differential ideal of  $\mathcal{R}$  disjoint from  $S$ . Prove that  $\mathfrak{q}$  is primary, and that if  $\mathcal{R}$  is an overring of  $\mathbf{Q}$ , then  $\mathfrak{q}$  is prime. (*Hint:* Let  $a, b \in \mathcal{R}$ ,  $a \notin \mathfrak{q}$ ,  $b^n \notin \mathfrak{q}$  ( $n \in \mathbb{N}$ ). Show there exist an  $s \in S \cap (\sum_{\text{ord } \theta \leq h} \mathcal{R}\theta a + \mathfrak{q})$  for some  $h \in \mathbb{N}$  and a  $t \in S \cap (\sum_{\text{ord } \theta \leq k} \mathcal{R}\theta(b^{h+1}) + \mathfrak{q})$  for some  $k \in \mathbb{N}$ , and infer by Lemma 1 that  $s't \in [ab] + \mathfrak{q}$  for some  $l \in \mathbb{N}$ . Conclude that  $ab \notin \mathfrak{q}$ , so that  $\mathfrak{q}$  is primary. The set  $\mathfrak{p}$  of all elements  $c \in \mathcal{R}$  such that  $c^n \in \mathfrak{q}$  for some  $n \in \mathbb{N}$  is a prime ideal disjoint from  $S$ . Use Lemma 2 to show that when  $\mathcal{R} \supset \mathbf{Q}$ , then  $\mathfrak{p}$  is a differential ideal, and conclude that  $\mathfrak{q} = \mathfrak{p}$ .)

### 3 Differential rings of quotients

Let  $\mathcal{R}$  be a differential ring, and let  $\Sigma$  be a multiplicatively stable subset of  $\mathcal{R}$ . Then we may form the ring of quotients  $\Sigma^{-1}\mathcal{R}$  of  $\mathcal{R}$  over  $\Sigma$  (see Chapter

0, Section 4). If  $a_1/s_1 = a_2/s_2$  in  $\Sigma^{-1}\mathcal{R}$ , that is, if there exists an  $s \in \Sigma$  such that  $a_1 s_2 s = a_2 s_1 s$ , and if  $\delta$  is any one of the derivation operators of  $\mathcal{R}$ , then

$$\begin{aligned} & (\delta a_1 \cdot s_1 - a_1 \delta s_1) s_2^2 s^2 - (\delta a_2 \cdot s_2 - a_2 \delta s_2) s_1^2 s^2 \\ &= (\delta a_1 \cdot s_1 s_2^2 + a_2 \delta s_2 \cdot s_1^2 - \delta a_2 \cdot s_1^2 s_2 - a_1 \delta s_1 \cdot s_2^2) s^2 \\ &= (\delta a_1 \cdot s_1 s_2^2 + a_1 \delta s_2 \cdot s_1 s_2 - \delta a_2 \cdot s_1^2 s_2 - a_2 \delta s_1 \cdot s_1 s_2) s^2 \\ &= (\delta a_1 \cdot s_2 + a_1 \delta s_2 - \delta a_2 \cdot s_1 - a_2 \delta s_1) s_1 s_2 s^2 \\ &= \delta(a_1 s_2 - a_2 s_1) \cdot s^2 s_1 s_2; \end{aligned}$$

but by Section 2, Lemma 1, this is an element of  $[(a_1 s_2 - a_2 s_1) s] = [0]$ , that is, is 0. This shows that

$$(\delta a_1 \cdot s_1 - a_1 \delta s_1) / s_1^2 = (\delta a_2 \cdot s_2 - a_2 \delta s_2) / s_2^2.$$

Hence we may define an operation of  $\delta$  on  $\Sigma^{-1}\mathcal{R}$  by the formula

$$\delta(a/s) = (\delta a \cdot s - a \delta s) / s^2.$$

It is easy to verify that  $\Sigma^{-1}\mathcal{R}$  then becomes a differential ring (with the same set of derivation operators as  $\mathcal{R}$ ). We call it the *differential ring of quotients* of  $\mathcal{R}$  over  $\Sigma$ ; in the special case of  $Q(\mathcal{R})$ , we call it the *complete differential ring of quotients* of  $\mathcal{R}$  or, when  $\mathcal{R}$  is a differential integral domain, the *differential field of quotients* of  $\mathcal{R}$ .

The canonical ring homomorphism  $\varphi: \mathcal{R} \rightarrow \Sigma^{-1}\mathcal{R}$  is easily seen to be a differential ring homomorphism. If  $f$  is a homomorphism of  $\mathcal{R}$  into a differential ring  $\mathcal{R}'$ , and if we set  $\Sigma' = f(\Sigma)$  and write  $\varphi': \mathcal{R}' \rightarrow \Sigma'^{-1}\mathcal{R}'$  to denote the canonical homomorphism, then there exists a unique homomorphism  $g: \Sigma^{-1}\mathcal{R} \rightarrow \Sigma'^{-1}\mathcal{R}'$  such that  $g \circ \varphi = \varphi' \circ f$ . The kernel of  $g$  is the set of all fractions  $a/s \in \Sigma^{-1}\mathcal{R}$  such that the numerator  $a$  has the property that  $as \in \text{Ker } f$  for some  $s \in \Sigma$  (i.e., such that  $a$  is in the smallest  $\Sigma$ -prime ideal of  $\mathcal{R}$  containing the kernel of  $f$ ). In particular, if  $f$  is injective, then so is  $g$ ; if  $f$  is surjective, then  $g$  is too.

#### EXERCISE

- Let  $\mathfrak{a}$  be a perfect (see Chapter 0, Section 5) differential ideal of the differential ring  $\mathcal{R}$ , let  $\mathfrak{p}$  be a minimal element of the set of all prime ideals that contain  $\mathfrak{a}$ . Show that  $\mathfrak{p}$  is a differential ideal and that, in the local ring  $\mathcal{R}_{\mathfrak{p}}$ ,  $\mathcal{R}_{\mathfrak{p}} \mathfrak{a} = \mathcal{R}_{\mathfrak{p}} \mathfrak{p}$ . (Hint: Show that  $\mathcal{R}_{\mathfrak{p}} \mathfrak{a}$  is a perfect differential ideal, that  $\mathcal{R}_{\mathfrak{p}} \mathfrak{p}$  is a minimal element of the set of all prime ideals of  $\mathcal{R}_{\mathfrak{p}}$  that contain  $\mathcal{R}_{\mathfrak{p}} \mathfrak{a}$ , and hence that  $\mathcal{R}_{\mathfrak{p}} \mathfrak{p}$  is the only prime ideal of  $\mathcal{R}_{\mathfrak{p}}$  that contains  $\mathcal{R}_{\mathfrak{p}} \mathfrak{a}$ . Conclude that  $\mathcal{R}_{\mathfrak{p}} \mathfrak{a} = \mathcal{R}_{\mathfrak{p}} \mathfrak{p}$  and that the ideal  $\mathfrak{p}$  is a differential one.)

#### 4 Transformation and restriction of the set of derivation operators

A ring  $\mathcal{R}$  may have several different differential ring structures, that is,  $\mathcal{R}$  may be a differential ring relative to several different sets of derivation operators  $\Delta$ ,  $\Delta'$ , etc. When we are considering more than one differential ring structure on  $\mathcal{R}$ , we use the term  $\Delta$ -ring to denote the differential ring for which  $\Delta$  is the set of derivation operators. We then also use, in an obvious way, such terms as  $\Delta$ -field,  $\Delta$ -ideal,  $\Delta$ -ring of quotients,  $\Delta$ -constant, etc. If  $\mathcal{R}$  is a  $\Delta$ -subring of a  $\Delta$ -ring  $\mathcal{S}$  and  $\Sigma$  is a subset of  $\mathcal{S}$ , we denote the  $\Delta$ -ring generated by  $\Sigma$  over  $\mathcal{R}$  by  $\mathcal{R}\langle\Sigma\rangle_{\Delta}$ . Similarly, if  $\mathcal{F}$  is a  $\Delta$ -subfield of a  $\Delta$ -field  $\mathcal{G}$  and  $\Sigma$  is a subset of  $\mathcal{G}$ , we denote the  $\Delta$ -field extension of  $\mathcal{F}$  generated by  $\Sigma$  by  $\mathcal{F}\langle\Sigma\rangle_{\Delta}$ .

We shall describe two ways of associating with a given differential ring structure certain other differential ring structures.

Let  $\mathcal{A}$  be any differential ring in which every element is a constant, and let  $\Delta$  denote the set of derivation operators of  $\mathcal{A}$ . Denote the free  $\mathcal{A}$ -module with basis  $\Delta$  by  $\mathfrak{D}$ . Every element  $\delta' \in \mathfrak{D}$  can be expressed uniquely in the form  $\delta' = \sum_{\delta \in \Delta} c_{\delta} \delta$ , where each  $c_{\delta} \in \mathcal{A}$ . We make  $\delta'$  into a derivation operator on any differential overring  $\mathcal{R}$  of  $\mathcal{A}$  by defining  $\delta' \alpha = \sum_{\delta \in \Delta} c_{\delta} \delta \alpha$  for every element  $\alpha$  of  $\mathcal{R}$ . If  $\Delta'$  is another basis of  $\mathfrak{D}$ , there exist matrices  $c = (c_{\delta \delta'})_{\delta \in \Delta, \delta' \in \Delta'}$  and  $c' = (c'_{\delta' \delta})_{\delta' \in \Delta', \delta \in \Delta}$  over  $\mathcal{A}$  inverse to each other, such that  $\delta = \sum_{\delta' \in \Delta'} c_{\delta \delta'} \delta'$  ( $\delta \in \Delta$ ) and  $\delta' = \sum_{\delta \in \Delta} c'_{\delta' \delta} \delta$  ( $\delta' \in \Delta'$ ). The differential overrings of  $\mathcal{A}$  can all be considered as differential rings with set of derivation operators  $\Delta'$ . We say that  $\Delta'$  results from transformation of  $\Delta$  by  $c$ , and call the  $\Delta'$ -ring  $\mathcal{R}$  the differential ring obtained from the  $\Delta$ -ring  $\mathcal{R}$  by *transformation of  $\Delta$  by  $c$* .

It is clear that if  $\Delta'$  results from transformation of  $\Delta$  as above, so that every  $\Delta$ -overring  $\mathcal{R}$  of  $\mathcal{A}$  is also a  $\Delta'$ -overring of  $\mathcal{A}$ , then an ideal of such an  $\mathcal{R}$  is a  $\Delta$ -ideal if and only if it is a  $\Delta'$ -ideal; an element of  $\mathcal{R}$  is a  $\Delta$ -constant if and only if it is a  $\Delta'$ -constant; and a ring homomorphism over  $\mathcal{A}$  of  $\mathcal{R}$  into a  $\Delta$ -overring of  $\mathcal{A}$  is a  $\Delta$ -ring homomorphism if and only if it is a  $\Delta'$ -ring homomorphism. Also, if  $\mathcal{S}$  is a  $\Delta$ -overring of  $\mathcal{R}$  and  $\Sigma$  is a subset of  $\mathcal{S}$ , then  $\mathcal{R}\langle\Sigma\rangle_{\Delta} = \mathcal{R}\langle\Sigma\rangle_{\Delta'}$ , and (if  $\mathcal{R}$  and  $\mathcal{S}$  happen to be fields)  $\mathcal{R}\langle\Sigma\rangle_{\Delta} = \mathcal{R}\langle\Sigma\rangle_{\Delta'}$ .

Starting afresh, let  $\mathcal{R}$  be any differential ring and denote the set of derivation operators of  $\mathcal{R}$  by  $\Delta$ . If  $\Delta_1$  is any subset of  $\Delta$ , we may regard  $\mathcal{R}$  as a  $\Delta_1$ -ring. We call the  $\Delta_1$ -ring  $\mathcal{R}$  the differential ring obtained from the  $\Delta$ -ring  $\mathcal{R}$  by *restriction of  $\Delta$  to  $\Delta_1$* .

It is clear that every  $\Delta$ -overring of  $\mathcal{R}$  is also a  $\Delta_1$ -overring of  $\mathcal{R}$ , that every  $\Delta$ -ideal of  $\mathcal{R}$  is also a  $\Delta_1$ -ideal of  $\mathcal{R}$ , that every  $\Delta$ -constant is also a  $\Delta_1$ -constant, and that every  $\Delta$ -ring homomorphism of  $\mathcal{R}$  into a  $\Delta$ -ring is also a  $\Delta_1$ -ring homomorphism. The converses to these statements are in general false.

Let  $\Delta_2$  denote the complement of  $\Delta_1$  in  $\Delta$ , let  $\Theta$  denote the set of derivative operators of the  $\Delta$ -ring  $\mathcal{R}$ , and let  $\Theta_1$  and  $\Theta_2$  denote the respective semi-groups in  $\Theta$  generated by  $\Delta_1$  and  $\Delta_2$  (so that  $\Theta = \Theta_1 \Theta_2$ ). If  $\mathcal{S}$  is a  $\Delta$ -overring of  $\mathcal{R}$  and  $\Sigma$  is a subset of  $\mathcal{S}$ , then  $\mathcal{R}\langle\Sigma\rangle_\Delta = \mathcal{R}\langle\Theta_2\Sigma\rangle_{\Delta_1}$ , and (if  $\mathcal{R}$  and  $\mathcal{S}$  happen to be fields)  $\mathcal{R}\langle\Sigma\rangle_\Delta = \mathcal{R}\langle\Theta_2\Sigma\rangle_{\Delta_1}$ .

### 5 Differential modules; differential algebras

Let  $\mathcal{R}$  be a differential ring with a set of derivation operators  $\Delta$ . By a *differential module over  $\mathcal{R}$* , or *differential  $\mathcal{R}$ -module*, we mean an  $\mathcal{R}$ -module  $\mathcal{M}$  on which  $\Delta$  operates subject to the conditions

$$\begin{aligned} \delta(u+v) &= \delta u + \delta v, & \delta(au) &= (\delta a)u + a\delta u \\ (\delta \in \Delta, u \in \mathcal{M}, v \in \mathcal{M}, a \in \mathcal{R}). \end{aligned}$$

A differential module over a differential field  $\mathcal{F}$  is called a *differential vector space over  $\mathcal{F}$* . The terms *differential submodule* and *differential subspace* are defined in the obvious way, as is the notion of homomorphism of one differential  $\mathcal{R}$ -module into another. If  $f: \mathcal{M} \rightarrow \mathcal{N}$  is such a homomorphism, its kernel and image are differential submodules of  $\mathcal{M}$  and  $\mathcal{N}$ , respectively. In particular, when  $\mathcal{M}$  and  $\mathcal{N}$  are differential vector spaces, the kernel and image are differential subspaces of  $\mathcal{M}$  and  $\mathcal{N}$ , respectively. On the other hand, if  $f: \mathcal{M} \rightarrow \mathcal{N}$  is a surjective module homomorphism of a differential  $\mathcal{R}$ -module  $\mathcal{M}$  onto an  $\mathcal{R}$ -module  $\mathcal{N}$ , and if the kernel is a differential submodule of  $\mathcal{M}$ , then  $\mathcal{N}$  has a unique differential  $\mathcal{R}$ -module structure such that  $f$  is a differential  $\mathcal{R}$ -module homomorphism. In particular, if  $\mathcal{M}_0$  is any differential submodule of  $\mathcal{M}$ , there is a unique differential  $\mathcal{R}$ -module structure on the quotient module  $\mathcal{M}/\mathcal{M}_0$  such that the canonical module homomorphism  $\mathcal{M} \rightarrow \mathcal{M}/\mathcal{M}_0$  is a differential module homomorphism. We call  $\mathcal{M}/\mathcal{M}_0$ , with this structure, the *differential quotient module* of  $\mathcal{M}$  by  $\mathcal{M}_0$ .

An element  $u$  of a differential  $\mathcal{R}$ -module  $\mathcal{M}$  is said to be a *constant* if  $\delta u = 0$  ( $\delta \in \Delta$ ). The set of constants of  $\mathcal{M}$  is a subgroup of the additive group  $\mathcal{M}$ , and has a natural structure of module over the ring of constants of  $\mathcal{R}$ .

Let  $V$  be a vector space over a field  $K$  with basis  $e = (e_i)_{i \in I}$ . If  $\sigma$  is any automorphism of  $K$ , the mapping  $\sigma_e: V \rightarrow V$  defined by the formula  $\sigma_e(\sum c_i e_i) = \sum (\sigma c_i) e_i$  is obviously an automorphism of the additive group  $V$ , and  $\sigma_e(cu) = (\sigma c)\sigma_e u$  ( $c \in K, u \in V$ ). If  $f = (f_j)_{j \in J}$  is a family of vectors in  $V$ , we let  $P_e(f)$  denote the field generated by all the coefficients  $a_{ji}$  in the equations

$$f_j = \sum_{i \in I} a_{ji} e_i \quad (j \in J).$$

Let  $W$  be a subspace of  $V$ . For a subfield  $K_0$  of  $K$ , the condition

$$K \cdot \left( W \cap \sum_{i \in I} K_0 e_i \right) = W$$

is evidently equivalent to the condition that  $W$  have a basis  $f$  such that  $P_e(f) \subset K_0$ . A subfield  $K_0$  satisfying these conditions is called a *field of definition* of  $W$  with respect to  $e$ .

**Lemma 3** (a) *Let  $V$  be a vector space over a field  $K$ , let  $e$  be a basis of  $V$ , and let  $W$  be a subspace of  $V$ . There exists a smallest field of definition  $P_e(W)$  of  $W$  with respect to  $e$ . If an automorphism  $\sigma$  of  $K$  leaves invariant every element of  $P_e(W)$ , then  $\sigma_e(W) = W$ . Conversely, if  $\sigma_e(W) \subset W$ , then  $\sigma$  leaves invariant every element of  $P_e(W)$ .*

(b) *Let  $\mathcal{V}$  be a differential vector space over a differential field  $\mathcal{F}$  with set of derivation operators  $\Delta$ , let  $e = (e_i)_{i \in I}$  be a basis of the vector space  $\mathcal{V}$ , and let  $\mathcal{W}$  be a differential subspace of  $\mathcal{V}$ . If the family  $\Delta e = (\delta e_i)_{\delta \in \Delta, i \in I}$  has the property that  $P_e(\Delta e) \subset P_e(\mathcal{W})$ , then  $P_e(\mathcal{W})$  is a differential subfield of  $\mathcal{F}$ .*

**REMARK** This lemma is useful when there is a canonically given basis  $e$ . Examples for part (a) are the vector spaces  $K^n$  and the polynomial algebras  $K[(X_j)_{j \in J}]$ ; in the former case we have the basis vectors  $(1, 0, \dots, 0)$ , etc., and in the latter case we have the basis formed by all the monomials in  $(X_j)_{j \in J}$ . Examples for part (b) are the differential vector spaces  $\mathcal{F}^n$  and the differential polynomial algebras over  $\mathcal{F}$  defined in the next section.

*Proof* (a) The canonical homomorphism  $V \rightarrow V/W$  maps the basis  $e = (e_i)_{i \in I}$  of  $V$  onto a family  $\bar{e} = (\bar{e}_i)_{i \in I}$  of generators of  $V/W$ . Let  $J'$  be a subset of  $I$  such that  $(\bar{e}_i)_{i \in J'}$  is a basis of  $V/W$ , let  $J = I - J'$ , and let  $W' = \sum_{i \in J'} K e_i$ . Clearly  $V = W + W'$  (direct sum), so that we may write

$$e_j = f_j + \sum_{j' \in J'} a_{jj'} e_{j'} \quad (j \in J),$$

where  $f_j \in W$  and  $a_{jj'} \in K$ . It is clear that the family  $f = (f_j)_{j \in J}$  is a basis of  $W$  and that  $P_e(f)$  is the field generated by  $(a_{jj'})_{j \in J, j' \in J'}$ , so that  $P_e(f)$  is a field of definition of  $W$  with respect to  $e$ . If  $g = (g_j)_{j \in J}$  is any other basis of  $W$  and we write

$$g_j = \sum_{i \in I} b_{ji} e_i \quad (j \in J),$$

then

$$\begin{aligned} g_j &= \sum_{i \in J} b_{ji} e_i + \sum_{i \in J'} b_{ji} e_i \\ &= \sum_{i \in J} b_{ji} \left( f_i + \sum_{j' \in J'} a_{ij'} e_{j'} \right) + \sum_{j' \in J'} b_{jj'} e_{j'} \\ &= \sum_{i \in J} b_{ji} f_i + \sum_{j' \in J'} \left( \sum_{i \in J} b_{ji} a_{ij'} + b_{jj'} \right) e_{j'}. \end{aligned}$$

Since the sum  $W + W'$  is direct this means that

$$g_j = \sum_{i \in J} b_{ji} f_i \quad (j \in J),$$

$$\sum_{i \in J} b_{ji} a_{ij'} + b_{jj'} = 0 \quad (j \in J, j' \in J').$$

The first set of these equations shows that the matrix  $(b_{ji})_{j \in J, i \in J}$  is invertible, and the second set therefore shows that  $P_e(f) \subset P_e(g)$ . This proves that  $P_e(f)$  is the smallest field of definition of  $W$  with respect to  $e$  and thus is our field  $P_e(W)$ . If the automorphism  $\sigma$  of  $K$  leaves invariant each element of  $P_e(W)$ , and in particular each  $a_{jj'}$ , then  $\sigma_e f_j = \sigma_e(e_j - \sum_{j' \in J'} a_{jj'} e_{j'}) = e_j - \sum_{j' \in J'} a_{jj'} e_{j'} = f_j$  for each  $j \in J$ , so that  $\sigma_e(W) = \sigma_e(\sum K f_j) = \sum K f_j = W$ . Conversely, if  $\sigma_e(W) \subset W$ , then the computation

$$\begin{aligned} \sigma_e f_j + \sum_{j' \in J'} (\sigma a_{jj'}) e_{j'} &= \sigma_e \left( f_j + \sum_{j' \in J'} a_{jj'} e_{j'} \right) \\ &= \sigma_e e_j \\ &= e_j = f_j + \sum_{j' \in J'} a_{jj'} e_{j'} \end{aligned}$$

shows that  $\sigma a_{jj'} = a_{jj'}$  ( $j \in J, j' \in J'$ ) and therefore that  $\sigma$  leaves invariant every element of  $P_e(W)$ .

(b) Keeping the same notation, but now supposing that  $K$  is the differential field  $\mathcal{F}$ ,  $V$  is the differential vector space  $\mathcal{V}$ , and  $W$  is the differential subspace  $\mathcal{W}$ , we may write  $\delta e_i = \sum_{k \in I} c_{\delta ik} e_k$  ( $\delta \in \Delta, i \in I$ ), where, by hypothesis,  $c_{\delta ik} \in P_e(\mathcal{W})$ . Then

$$\begin{aligned} \delta f_j &= \delta \left( e_j - \sum_{j' \in J'} a_{jj'} e_{j'} \right) \\ &= \delta e_j - \sum_{j' \in J'} (\delta a_{jj'}) e_{j'} - \sum_{j' \in J'} a_{jj'} \delta e_{j'} \\ &= \sum_{k \in I} c_{\delta jk} e_k - \sum_{j' \in J'} (\delta a_{jj'}) e_{j'} - \sum_{k \in I} \sum_{j' \in J'} a_{jj'} c_{\delta j'k} e_k \\ &= \sum_{k \in J} b_{\delta jk} e_k + \sum_{k' \in J'} (-\delta a_{jk'} + b_{\delta jk'}) e_{k'} \end{aligned}$$

(where  $b_{\delta jk}, b_{\delta jk'} \in P_e(\mathcal{W})$ )

$$\begin{aligned} &= \sum_{k \in J} b_{\delta jk} \left( f_k + \sum_{k' \in J'} a_{kk'} e_{k'} \right) + \sum_{k' \in J'} (-\delta a_{jk'} + b_{\delta jk'}) e_{k'} \\ &= \sum_{k \in J} b_{\delta jk} f_k + \sum_{k' \in J'} \left( \sum_{k \in J} b_{\delta jk} a_{kk'} - \delta a_{jk'} + b_{\delta jk'} \right) e_{k'}, \end{aligned}$$

so that (by the directness of the sum  $\mathcal{W} + \mathcal{W}'$  and the linear independence of the  $e_k$ )

$$\delta a_{jk'} = \sum_{k \in J} b_{\delta jk} a_{kk'} + b_{\delta jk'} \in P_e(\mathcal{W}) \quad (\delta \in \Delta, j \in J, k' \in J').$$

Since  $P_e(\mathcal{W})$  is the field generated by the elements  $a_{jk'}$ , we conclude that  $P_e(\mathcal{W})$  is a differential field.

By a *differential algebra* over  $\mathcal{R}$ , or *differential  $\mathcal{R}$ -algebra*, we mean a ring  $\mathcal{A}$ , on which  $\mathcal{R}$  operates in such a way as to make  $\mathcal{A}$  an algebra over the ring  $\mathcal{R}$ , and on which  $\Delta$  operates in such a way as to make  $\mathcal{A}$  a differential ring, which satisfies the condition

$$\delta(au) = (\delta a)u + a\delta u \quad (\delta \in \Delta, a \in \mathcal{R}, u \in \mathcal{A}).$$

Then  $\mathcal{A}$  has an obvious structure of differential  $\mathcal{R}$ -module.

If  $\mathcal{R}$  is a differential subring of a differential ring  $\mathcal{R}'$ , then  $\mathcal{R}'$  has a natural structure of differential  $\mathcal{R}$ -algebra. More generally, if we have a homomorphism  $f: \mathcal{R} \rightarrow \mathcal{R}'$  of  $\mathcal{R}$  into a differential ring  $\mathcal{R}'$ , and we define an operation of  $\mathcal{R}$  on  $\mathcal{R}'$  by the formula  $aa' = f(a)a'$  ( $a \in \mathcal{R}, a' \in \mathcal{R}'$ ), then  $\mathcal{R}'$  becomes a differential  $\mathcal{R}$ -algebra.

## 6 Differential polynomial algebras

Let  $\mathcal{R}$  be a nonzero differential ring. Denote the set of derivation operators of  $\mathcal{R}$  by  $\Delta$ , and the set of derivative operators of  $\mathcal{R}$  by  $\Theta$ .

A family  $(\alpha_i)_{i \in I}$  of elements of a differential overring of  $\mathcal{R}$  is said to be *differentially algebraically dependent over  $\mathcal{R}$*  if the family  $(\partial \alpha_i)_{i \in I, \theta \in \Theta}$  is algebraically dependent over  $\mathcal{R}$ , and is said to be *differentially algebraically independent over  $\mathcal{R}$* , or to be a *family of differential indeterminates over  $\mathcal{R}$* , in the contrary case. A *subset  $\Sigma$  of a differential overring of  $\mathcal{R}$*  is said to be differentially algebraically dependent or differentially algebraically independent, over  $\mathcal{R}$ , according as the family  $(\alpha)_{\alpha \in \Sigma}$  is. In the special case in which  $\Sigma$  consists of a single element  $\alpha$ ,  $\alpha$  is said to be, correspondingly, *differentially algebraic* or *differentially transcendental*, over  $\mathcal{R}$ .

It is clear that if  $\Delta'$  is a set of derivation operators that results from transformation of  $\Delta$  by an invertible matrix over the ring of constants of  $\mathcal{R}$ , then  $(\alpha_i)_{i \in I}$  is  $\Delta$ -algebraically dependent over  $\mathcal{R}$  if and only if it is  $\Delta'$ -algebraically dependent over  $\mathcal{R}$ . Also, if we restrict  $\Delta$  to a subset  $\Delta_1$ , and let  $\Theta_2$  denote the semigroup in  $\Theta$  generated by the complement of  $\Delta_1$  in  $\Delta$ , then  $(\alpha_i)_{i \in I}$  is  $\Delta$ -algebraically dependent over  $\mathcal{R}$  if and only if  $(\partial \alpha_i)_{\theta \in \Theta_2, i \in I}$  is  $\Delta_1$ -algebraically dependent over  $\mathcal{R}$ .



Let  $J$  be any set. We claim that *there always exists a family of differential indeterminates over  $\mathcal{R}$  with set of indices  $J$* . Indeed, let  $\mathcal{R}[(y_{j\theta})_{j \in J, \theta \in \Theta}]$  be the polynomial algebra over  $\mathcal{R}$  in a family of indeterminates  $(y_{j\theta})_{j \in J, \theta \in \Theta}$  with set of indices  $J \times \Theta$ . For each  $\delta \in \Delta$ , the derivation  $a \mapsto \delta a$  ( $a \in \mathcal{R}$ ) of  $\mathcal{R}$  can be extended<sup>3</sup> to a unique derivation of  $\mathcal{R}[(y_{j\theta})_{j \in J, \theta \in \Theta}]$  mapping  $y_{j\theta}$  onto  $y_{j, \delta\theta}$  ( $j \in J, \theta \in \Theta$ ). Correspondingly,  $\Delta$  becomes a set of derivation operators on  $\mathcal{R}[(y_{j\theta})_{j \in J, \theta \in \Theta}]$ , and this algebra thereby becomes a differential algebra over  $\mathcal{R}$ . If we set  $y_j = y_{j1}$  (1 here denoting the derivative operator of order 0), then  $\theta y_j = y_{j\theta}$ , so that  $\mathcal{R}\{(y_j)_{j \in J}\} = \mathcal{R}[(y_{j\theta})_{j \in J, \theta \in \Theta}]$ , and  $(y_j)_{j \in J}$  is differentially algebraically independent over  $\mathcal{R}$ . This establishes our claim.

Let  $(y_j)_{j \in J}$  be any family of differential indeterminates over  $\mathcal{R}$ . The elements of  $\mathcal{R}\{(y_j)_{j \in J}\}$  are called *differential polynomials over  $\mathcal{R}$*  (or with *coefficients in  $\mathcal{R}$* )<sup>\*</sup> in  $(y_j)_{j \in J}$ , and  $\mathcal{R}\{(y_j)_{j \in J}\}$  itself is called the *differential polynomial algebra over  $\mathcal{R}$  in  $(y_j)_{j \in J}$* .

Since the family of derivatives  $(\theta y_j)_{j \in J, \theta \in \Theta}$  is algebraically independent over  $\mathcal{R}$ , the differential polynomial algebra  $\mathcal{R}\{(y_j)_{j \in J}\}$  may be regarded as the polynomial algebra over  $\mathcal{R}$  in the family of indeterminates  $(\theta y_j)_{j \in J, \theta \in \Theta}$ . Therefore, if  $G \in \mathcal{R}\{(y_j)_{j \in J}\}$ , it is clear what we mean by the *degree of  $G$*  (which we denote by  $\deg G$ ), or more generally (if  $\Lambda$  is any subfamily of  $(\theta y_j)_{j \in J, \theta \in \Theta}$ ) the *degree of  $G$  in  $\Lambda$*  (which we denote by  $\deg_\Lambda G$ ), the corresponding notions of *homogeneity*, the *terms of  $G$* , and the *coefficients in  $G$* . Similarly, for any  $j \in J$  and  $\theta \in \Theta$ , it is meaningful to say that  $G$  *involves  $\theta y_j$*  (or  $\theta y_j$  is *present* in  $G$ ) and, in the contrary case, that  $G$  is *free* of  $\theta y_j$ . If  $G$  involves a derivative  $\theta y_j$  of order  $r$  but does not involve any derivative of order greater than  $r$ , then  $r$  is called the *order of  $G$*  and is denoted by  $\text{ord } G$ . If  $G$  is free of every derivative  $\theta y_j$ , that is, if  $G \in \mathcal{R}$ , we define the order of  $G$  to be  $-1$ . For a given  $j \in J$ , if there exists a  $\theta \in \Theta$  such that  $G$  involves  $\theta y_j$  we shall say that  $G$  *involves  $y_j$  differentially* (or that  $y_j$  is *differentially present* in  $G$ ) and, in the contrary case, that  $G$  is *differentially free* of  $y_j$ .

By a *differential monomial* in  $(y_j)_{j \in J}$ , we shall mean a differential polynomial in  $(y_j)_{j \in J}$  having precisely one nonzero term, *the coefficient in that term being 1*. By a *prime factor* of such a differential monomial  $M$ , we shall mean any derivative  $\theta y_j$  that divides  $M$ .

Let  $(\eta_j)_{j \in J}$  be any family, with the same set of indices  $J$ , of elements of a differential overring of  $\mathcal{R}$ . Because  $(\theta y_j)_{j \in J, \theta \in \Theta}$  is algebraically independent over  $\mathcal{R}$ , there exists a unique ring homomorphism

$$\sigma : \mathcal{R}[(\theta y_j)_{j \in J, \theta \in \Theta}] \rightarrow \mathcal{R}[(\theta \eta_j)_{j \in J, \theta \in \Theta}]$$

over  $\mathcal{R}$  mapping  $\theta y_j$  onto  $\theta \eta_j$  ( $j \in J, \theta \in \Theta$ ). The equations  $\sigma \delta u = \delta \sigma u$  ( $\delta \in \Delta$ ) obviously hold when  $u$  is one of the derivatives  $\theta y_j$  and also when  $u \in \mathcal{R}$ .

<sup>3</sup> See e.g., N. Bourbaki "Algèbre," Chap. V, §9, Prop. 4, p. 139. Hermann, Paris, 1950 or 1959.

These equations therefore hold for every  $u \in \mathcal{R}[(\theta y_j)_{j \in J, \theta \in \Theta}]$ , so that  $\sigma$  is a differential ring homomorphism

$$\mathcal{R}\{(y_j)_{j \in J}\} \rightarrow \mathcal{R}\{(\eta_j)_{j \in J}\}.$$

We call this homomorphism the *substitution of  $(\eta_j)_{j \in J}$  for  $(y_j)_{j \in J}$* . It is obvious that if  $(\eta_j)_{j \in J}$  is differentially algebraically independent over  $\mathcal{R}$  (and only then), the substitution of  $(\eta_j)_{j \in J}$  for  $(y_j)_{j \in J}$  is an  $\mathcal{R}$ -isomorphism.

Let  $G \in \mathcal{R}\{(y_j)_{j \in J}\}$ . The substitution of  $(\eta_j)_{j \in J}$  for  $(y_j)_{j \in J}$  maps  $G$  onto an element of  $\mathcal{R}\{(\eta_j)_{j \in J}\}$ . This element is called the *value of  $G$  at  $(\eta_j)_{j \in J}$*  and is denoted by  $G((\eta_j)_{j \in J})$ . In particular,  $G((y_j)_{j \in J}) = G$ . If the value of  $G$  at  $(\eta_j)_{j \in J}$  is 0, that is, if  $G$  belongs to the kernel of the substitution, then we say that  $G$  *vanishes* at  $(\eta_j)_{j \in J}$ . The set of differential polynomials that vanish at  $(\eta_j)_{j \in J}$ , being the kernel of the substitution homomorphism, is a differential ideal of  $\mathcal{R}\{(y_j)_{j \in J}\}$ . We call it the *defining differential ideal* of  $(\eta_j)_{j \in J}$  in  $\mathcal{R}\{(y_j)_{j \in J}\}$  (or over  $\mathcal{R}$ ).

If  $\mathcal{R}$  happens to be a differential field  $\mathcal{F}$ , then  $\mathcal{F}\{(y_j)_{j \in J}\}$  is a differential integral domain. Its differential field of quotients is denoted by  $\mathcal{F}\langle\langle(y_j)_{j \in J}\rangle\rangle$ , in conformity with the notation introduced in Section 1, and its elements are called *differential rational fractions over  $\mathcal{F}$*  (or with *coefficients in  $\mathcal{F}$* ) in  $(y_j)_{j \in J}$ .

## EXERCISES

In the following exercises  $\mathcal{R}$  denotes a differential ring, with set of derivation operators  $\Delta$  consisting of  $\delta_1, \dots, \delta_m$ , and with set of derivative operators  $\Theta$ .

1. Call a differential polynomial  $B \in \mathcal{R}\{y_0, y_1, \dots, y_n\}$  *differentially homogeneous* if there exists an  $r \in \mathbb{N}$  such that  $B(ty_0, ty_1, \dots, ty_n) = t^r B(y_0, y_1, \dots, y_n)$  for a differential indeterminate  $t$  over  $\mathcal{R}\{y_0, y_1, \dots, y_n\}$ .
  - (a) Show that if  $B$  is differentially homogeneous and  $B \neq 0$ , then  $B$  is homogeneous and the number  $r$  above equals  $\deg B$ .
  - (b) Show that  $B$  is differentially homogeneous and of degree  $r$  if and only if there exists a differential polynomial  $A \in \mathcal{R}\{y_1, \dots, y_n\}$  such that  $B(y_0, y_1, \dots, y_n) = y_0^r A(y_1/y_0, \dots, y_n/y_0)$  in  $\mathcal{Q}(\mathcal{R}\{y_0, y_1, \dots, y_n\})$ .
  - (c) Using the notation  $\binom{\theta'}{\theta}$  of Exercise 1 of Section 1, show that a necessary condition that  $B$  be differentially homogeneous and of degree  $r$  is that  $B$  satisfy the system of differential equations

$$\sum_{\substack{\theta' \in \Theta \\ 0 \leq j \leq n}} \binom{\theta'}{\theta} \theta' y_j \cdot \frac{\partial B}{\partial (\theta' y_j)} = \begin{cases} rB & (\theta = 1), \\ 0 & (\theta \in \Theta, \theta \neq 1). \end{cases}$$

- (d) Show that if  $\mathcal{R}$  is a differential field of characteristic 0, then the condition in (c) is sufficient.

2. Show that the ordinary differential polynomial

$$W = \det(y_j^{i-1})_{1 \leq i \leq n, 1 \leq j \leq n}$$

(Wronskian determinant) is differentially homogeneous.

3. Let  $(z_1, \dots, z_m)$  be a family of differential indeterminates over  $\mathcal{R}$ , and set  $\mathcal{S} = \mathcal{R}\{z_1, \dots, z_m\}$ . Let  $D$  denote the derivation operator on  $\mathcal{S}$  defined by  $D = \sum_{1 \leq i \leq m} z_i \delta_i$ . Let  $W_D$  denote the differential polynomial in  $(y_1, \dots, y_n)$  over  $\mathcal{S}$  defined by  $W_D = \det(D^{i-1} y_j)_{1 \leq i \leq n, 1 \leq j \leq n}$ .
- (a) Show that  $W_D$  can be written as a linear combination over  $\mathcal{S}$  of determinants of the form  $\det(\theta_i y_j)_{1 \leq i \leq n, 1 \leq j \leq n}$ , where  $\theta_i \in \Theta$  and  $\text{ord } \theta_i < i$  ( $1 \leq i \leq n$ ).
- (b) Show that when  $W_D$  is written as a linear combination over  $\mathcal{R}\{y_1, \dots, y_n\}$  of differential monomials in  $(z_1, \dots, z_m)$ , then the coefficients in this linear combination are differentially homogeneous. (Hint: Use the result of Exercise 2.)
4. (a) Show that for each  $A \in \mathcal{R}\{y_1, \dots, y_n\}$  there exists a  $d \in \mathbb{N}$  such that if we embed  $\mathcal{R}\{y_0, y_1, \dots, y_n\}$  in  $Q(\mathcal{R}\{y_0, y_1, \dots, y_n\})$ , then  $y_0^d A(y_1/y_0, \dots, y_n/y_0) \in \mathcal{R}\{y_0, y_1, \dots, y_n\}$ . The smallest such  $d$  is called the *denomination* of  $A$  and is denoted by  $\text{den } A$ .
- (b) Show that  $\text{den } \theta y_j \leq 1 + \text{ord } \theta$ ,  $\text{den}(A+B) \leq \max(\text{den } A, \text{den } B)$ , and  $\text{den } AB \leq \text{den } A + \text{den } B$ .
5. Let  $\alpha$  be a differential ideal of a differential polynomial algebra over a differential field. Show that if  $\alpha$  has a set of generators that are linear (i.e., of degree 1), then either  $1 \in \alpha$  or  $\alpha$  is prime. (Hint: The problem reduces to the analogous problem for polynomial ideals.)

## 7 Permissible gradings

The contents of this section are not used until the second half of Chapter IV.

Let  $\mathcal{R}$  be a differential ring with set of derivation operators  $\Delta$  and set of derivative operators  $\Theta$ ; denote the elements of  $\Delta$  by  $\delta_1, \dots, \delta_m$ . Let  $(y_j)_{j \in J}$  be a family of differential indeterminates over  $\mathcal{R}$ , and consider the differential polynomial algebra  $\mathcal{A} = \mathcal{R}\{(y_j)_{j \in J}\}$ .

If  $\mathcal{A}_k$  denotes the set of all elements of  $\mathcal{A}$  that are homogeneous of degree  $k$ , then  $\mathcal{A}_k$  is a submodule (indeed, a differential one) of the differential  $\mathcal{R}$ -module  $\mathcal{A}$ , we have a direct sum decomposition  $\mathcal{A} = \sum_{k \in \mathbb{Z}} \mathcal{A}_k$ , and  $\mathcal{A}_k \mathcal{A}_l \subset \mathcal{A}_{k+l}$  for all  $k$  and  $l$ . Thus,  $\mathcal{A}$  is a graded algebra with grading  $(\mathcal{A}_k)_{k \in \mathbb{Z}}$ . We call this the *usual* grading of  $\mathcal{A}$ .

It is sometimes useful to consider other gradings of  $\mathcal{A}$ . Let  $v_j$  ( $j \in J$ ),  $\mu_1, \dots, \mu_m$  be arbitrary elements of  $\mathbb{Z}$ . For each derivative  $u = \delta_1^{e_1} \cdots \delta_m^{e_m} y_j$  define  $g(u) = v_j + \mu_1 e_1 + \cdots + \mu_m e_m$ , and let  $\mathcal{A}_k$  denote the submodule of  $\mathcal{A}$  generated by all the differential monomials  $\prod_h u_h$  in  $(y_j)_{j \in J}$  with  $\sum_h g(u_h) = k$ .

It is clear that  $\mathcal{A} = \sum_{k \in \mathbb{Z}} \mathcal{A}_k$  (direct sum) and  $\mathcal{A}_k \mathcal{A}_l \subset \mathcal{A}_{k+l}$  ( $k, l \in \mathbb{Z}$ ), so that  $\mathcal{A}$  is a graded algebra with grading  $(\mathcal{A}_k)_{k \in \mathbb{Z}}$ . We call any grading obtained in this way a *permissible* grading of  $\mathcal{A}$ .

The special case in which  $v_j = 1$  ( $j \in J$ ) and  $\mu_i = 0$  ( $1 \leq i \leq m$ ) is the usual grading. The special case in which  $v_j = 0$  ( $j \in J$ ) and  $\mu_i = 1$  ( $1 \leq i \leq m$ ) carries its own terminology: The elements of  $\mathcal{A}$  that are homogeneous relative to this grading (i.e., that are in  $\bigcup_{k \in \mathbb{Z}} \mathcal{A}_k$ ) are called *isobaric*. An isobaric element  $F$  of  $\mathcal{A}$  is an element of  $\mathcal{A}_k$  for at least one  $k$  (for precisely one  $k$  if  $F \neq 0$ , for every  $k$  if  $F = 0$ ), and  $F$  is then said to have *weight*  $k$ . If  $F$  is nonzero and isobaric, we denote the weight of  $F$  by  $\text{wt } F$ .

A grading of  $\mathcal{A}$  is *positive* if  $\mathcal{A}_k = (0)$  whenever  $k < 0$ , and is *strictly positive* if it is positive and  $\mathcal{A}_0 = \mathcal{R}$ . A permissible grading is positive if and only if  $v_j \geq 0$  ( $j \in J$ ) and  $\mu_i \geq 0$  ( $1 \leq i \leq m$ ), and is strictly positive if and only if  $v_j > 0$  ( $j \in J$ ) and  $\mu_i \geq 0$  ( $1 \leq i \leq m$ ). Thus, the grading by weight is positive; the usual grading is strictly positive.

The usual grading has the property that  $\delta \mathcal{A}_k \subset \mathcal{A}_k$  ( $\delta \in \Delta$ ,  $k \in \mathbb{Z}$ ). We call any grading of  $\mathcal{A}$  enjoying this property a *differential* grading. A permissible grading is differential if and only if  $\mu_i = 0$  ( $1 \leq i \leq m$ ). Relative to a differential grading of  $\mathcal{A}$ , the differential ideal  $[\Sigma]$  generated by a set  $\Sigma$  of homogeneous elements of  $\mathcal{A}$  is homogeneous. (An ideal of a graded ring is homogeneous if, for every element of the ideal, the homogeneous parts of the element are all in the ideal.) Relative to a permissible grading that is not differential, a derivative of a homogeneous element  $F$  is in general not homogeneous. However, if  $F$  has constant coefficients, then every derivative of  $F$  is homogeneous. More precisely, if  $\mathcal{A}_k^0$  denotes the set of elements of  $\mathcal{A}_k$  that have constant coefficients, then  $\delta_i \mathcal{A}_k^0 \subset \mathcal{A}_{k+\mu_i}^0$  ( $1 \leq i \leq m$ ,  $k \in \mathbb{Z}$ ). It follows that if  $\Sigma \subset \bigcup \mathcal{A}_k^0$ , then  $[\Sigma]$  is homogeneous. In the absence of mention of other gradings, terms like “degree” and “homogeneous” will always refer to the usual grading.

The following somewhat technical lemma plays an important role in the second half of Chapter IV.

**Lemma 4** Let  $(y_1, \dots, y_n)$  be a finite family of differential indeterminates over  $\mathbb{Q}$  (considered as a differential field with  $m$  derivation operators), let  $h, k, l \in \mathbb{N}$ , and let

$$e = e(n, k, h, m) = n(h-1)(k+1) \left( 1 + 2 \frac{(2m)^k - 1}{2m-1} \right) + 1.$$

Then for each differential monomial  $M$  in  $(y_1, \dots, y_n)$  with  $\text{deg } M \geq e + lh$  and  $\text{wt } M \leq ke$ , there exist indices  $j_0, \dots, j_l$  such that  $M \in \prod_{0 \leq \lambda \leq l} [\mathcal{A}_{j_\lambda}^h]$  in  $\mathbb{Q}\{y_1, \dots, y_n\}$ .

*Proof* Let  $f = \deg M$  and suppose that  $f \geq e + lh$ . We may suppose that  $n > 0$ ,  $h > 0$ . First let  $l = 0$ , and write  $M = \prod_{1 \leq i \leq f} \theta_i y_{j(i)}$ , where each  $\theta_i$  is a derivative operator. If  $M \notin [y_j^h]$  ( $1 \leq j \leq n$ ), then (by Section 2, the Corollary to Lemma 2) for each  $y_j$  and each  $k' \in \mathbb{N}$ , the number of indices  $i$  with  $j(i) = j$  and  $\text{ord} \theta_i = k'$  is less than or equal to  $d(k', h, m) - 1$ , so that the number of indices  $i$  with  $\text{ord} \theta_i \leq k$  is less than or equal to  $\sum_{1 \leq j \leq n} \sum_{0 \leq k' \leq k} (d(k', h, m) - 1) = (k+1)^{-1}(e-1)$ . Therefore the number of indices  $i$  with  $\text{ord} \theta_i \geq k+1$  is greater than or equal to  $e - (k+1)^{-1}(e-1)$ , so that

$$\text{wt } M = \sum_{1 \leq i \leq f} \text{ord} \theta_i \geq [e - (k+1)^{-1}(e-1)](k+1) = ke + 1.$$

This proves the lemma when  $l = 0$ .

Now let  $l > 0$  and make the inductive hypothesis that the lemma holds for lower values of  $l$ . By the case  $l = 0$  we have  $M \in [y_j^h]$  for some  $j$ , say for  $j = n$ . Writing  $M = NP$  with  $N$  a differential monomial in  $(y_1, \dots, y_{n-1})$  and  $P$  a differential monomial in  $y_n$ , we see that  $P \in [y_n^h]$ , so that  $P = \sum_i a_i P_i \theta_i (y_n^h)$ , where  $a_i \in \mathbb{Q}$ ,  $\theta_i \in \Theta$ , and  $P_i$  is a differential monomial in  $y_n$  with  $\deg P_i = \deg P - h$  and  $\text{wt } P_i = \text{wt } P - \text{ord} \theta_i$ . For each index  $i$ ,  $NP_i$  is a differential monomial in  $(y_1, \dots, y_n)$  with  $\deg NP_i \geq e + (l-1)h$  and  $\text{wt } NP_i \leq ke$ . By the inductive hypothesis then  $NP_i \in [y_1^h]^{\lambda_{i1}} \dots [y_n^h]^{\lambda_{in}}$ , where  $\lambda_{i1}, \dots, \lambda_{in} \in \mathbb{N}$  and  $\lambda_{i1} + \dots + \lambda_{in} = l$ . Evidently  $N \in [y_1^h]^{\lambda_{11}} \dots [y_{n-1}^h]^{\lambda_{i, n-1}}$  and  $P_i \in [y_n^h]^{\lambda_{in}}$ . Fixing  $j$  so that  $\lambda_{jn} = \min_i \lambda_{in}$ , we see that  $P_i \in [y_n^h]^{\lambda_{jn}}$  for every  $i$ , so that

$$M = \sum_i a_i NP_i \theta_i (y_n^h) \in [y_1^h]^{\lambda_{j1}} \dots [y_{n-1}^h]^{\lambda_{j, n-1}} [y_n^h]^{\lambda_{jn}} [y_n^h].$$

This yields a corollary about  $\mathfrak{f}$ -values (see Chapter 0, Section 19).

**Corollary** Let  $\mathcal{R}$  be a differential overring of  $\mathbb{Q}$  with a set of derivation operators  $\Delta$  and let  $\mathfrak{f}$  be a differential ideal of  $\mathcal{R}$ . Then  $v_{\mathfrak{f}}(\delta x) \geq v_{\mathfrak{f}}(x)$  ( $x \in \mathcal{R}$ ,  $\delta \in \Delta$ ).

*Proof* It suffices to show that if  $\alpha$  is any real number with  $\alpha < v_{\mathfrak{f}}(x)$ , then  $\alpha < v_{\mathfrak{f}}(\delta x)$ , that is, then there exist  $n, r \in \mathbb{N}$  with  $r > n\alpha$  such that  $(\delta x)^n \in \mathfrak{f}^r$ . Now, there exists a rational number  $\rho$  with  $\alpha < \rho < v_{\mathfrak{f}}(x)$ , and there exists an  $h \in \mathbb{N}$  that is a multiple of the denominator of  $\rho$  and is so big that  $\rho h / (h+1) > \alpha$  and  $x^h \in \mathfrak{f}^{\rho h}$ . Set  $e = e(1, h+1, h, m)$  in the notation of Lemma 4. Then  $(\delta y)^{(h+1)e}$  is a differential monomial in  $y$  of degree  $e + eh$  and weight  $(h+1)e$ , and therefore by the lemma (case  $l = e$ ) is an element of  $[y^h]^e$  in  $\mathbb{Q}\{y\}$ . Substituting  $x$  for  $y$ , we find that  $(\delta x)^{(h+1)e} \in [x^h]^e$  in  $\mathbb{Q}\{x\}$  and therefore also in  $\mathcal{R}$ , so that  $(\delta x)^{(h+1)e} \in \mathfrak{f}^{\rho h e}$ . Since  $\rho h e > (h+1)e \cdot \alpha$ , the proof is complete.

## 8 Rank

Again let  $\mathcal{R}$  be a nonzero differential ring. Denote the set of derivation operators of  $\mathcal{R}$  by  $\Delta$ , and the set of derivative operators of  $\mathcal{R}$  by  $\Theta$ .

Consider a finite family  $(y_1, \dots, y_n)$  of differential indeterminates over  $\mathcal{R}$ . By a *ranking* of  $(y_1, \dots, y_n)$  we shall mean a total ordering of the set of all derivatives  $\theta y_j$  ( $\theta \in \Theta$ ,  $1 \leq j \leq n$ ) that satisfies (for all such derivatives  $u$  and  $v$ , and for all  $\theta \in \Theta$ ) the two conditions

$$u \leq \theta u, \quad u \leq v \Rightarrow \theta u \leq \theta v.$$

If we denote the elements of  $\Delta$  by  $\delta_1, \dots, \delta_m$ , then the derivatives  $\theta y_j$  can all be expressed in the form  $\delta_1^{i_1} \dots \delta_m^{i_m} y_j$ . It follows from Chapter 0, Section 17, Lemma 15, that a ranking exists and every ranking is a well ordering of the set of derivatives  $\theta y_j$ .

Let there be given a ranking of  $(y_1, \dots, y_n)$ . We indicate the relation  $u < v$  of the ranking by saying that  $u$  has lower rank than  $v$ , or the rank of  $u$  is lower than the rank of  $v$ , or  $v$  has higher rank than  $u$ , or something similar (or when there is no danger of confusion, by saying simply that  $u$  is lower than  $v$ , or  $v$  is higher than  $u$ ).

A ranking will be said to be *integrated* if for each pair of derivatives  $\theta_1 y_{j_1}, \theta_2 y_{j_2}$  there exists a  $\theta \in \Theta$  such that  $\theta \theta_1 y_{j_1}$  has higher rank than  $\theta_2 y_{j_2}$ . To show that this is the case, it suffices to show that each  $y_j$  has a derivative of higher rank than every other  $y_j$ .

A ranking will be said to be *sequential* if its order type is that of  $\mathbb{N}$ , that is, if every derivative  $\theta y_j$  is of higher rank than only finitely many other derivatives. Every sequential ranking is integrated.

A ranking will be said to be *orderly* if the rank of  $\theta y_j$  is less than that of  $\theta' y_j$  whenever  $\text{ord} \theta < \text{ord} \theta'$ . Every orderly ranking is sequential. An example of an orderly ranking is obtained by ordering the set of derivatives  $\delta_1^{i_1} \dots \delta_m^{i_m} y_j$  lexicographically with respect to  $(\sum i_u, j, i_1, \dots, i_m)$ .

Let  $A \in \mathcal{R}\{y_1, \dots, y_n\}$ ,  $A \notin \mathcal{R}$ . The highest ranking derivative  $\theta y_j$  present in  $A$  is called the *leader* of  $A$ . We shall frequently, without further notice, denote the leader of  $A$  by  $u_A$ . If  $d = \deg_{u_A} A$ , we may write  $A = \sum_{0 \leq i \leq d} I_i u_A^i$ , where  $I_0, \dots, I_d$  are in  $\mathcal{R}\{y_1, \dots, y_n\}$  and are free of  $u_A$ . Then  $I_0, \dots, I_d$  are unique,  $I_d \neq 0$ , and every derivative  $\theta y_j$  present in an  $I_i$  is lower than  $u_A$ . The differential polynomial  $I_d$  is called the *initial* of  $A$ , and the differential polynomial  $\sum i I_i u_A^{i-1}$  ( $= \partial A / \partial u_A$ ) is called the *separant* of  $A$ . We shall frequently, without further notice, denote the initial of  $A$  by  $I_A$  and the separant of  $A$  by  $S_A$ . The notions of leader, initial, and separant are, of course, relative ones, depending on the particular ranking used.

It is useful to extend the notion of *comparative rank* to the whole differential polynomial algebra by the following convention:

- (i) Every element of  $\mathcal{R}$  has lower rank than every element of  $\mathcal{R}\{y_1, \dots, y_n\}$  not in  $\mathcal{R}$ .
- (ii) If  $A$  and  $B$  are in  $\mathcal{R}\{y_1, \dots, y_n\}$  but not in  $\mathcal{R}$ , and if either  $u_A$  is lower than  $u_B$  or  $u_A = u_B$  and  $\deg_{u_A} A < \deg_{u_A} B$ , then  $A$  has lower rank than  $B$ .
- (iii) Two elements of  $\mathcal{R}\{y_1, \dots, y_n\}$  that either are both in  $\mathcal{R}$  or have the same leader and the same degree in that leader, have the same rank.

Since distinct differential polynomials evidently may have the same rank, the relation "the rank of  $A$  is lower than or equal to the rank of  $B$ " does not define an order on  $\mathcal{R}\{y_1, \dots, y_n\}$ . However, it does define a *pre-order*, being reflexive and transitive.

If  $A \in \mathcal{R}\{y_1, \dots, y_n\}$ ,  $A \notin \mathcal{R}$ , then  $A$  has higher rank than  $I_A$  and  $S_A$ .

It is clear that in every nonempty subset of  $\mathcal{R}\{y_1, \dots, y_n\}$  there exists an element the rank of which is lower than or equal to the rank of every element of the subset. Any such element is called an *element of lowest rank*, or a *lowest element*, of the subset.

**Lemma 5** *Let  $A$  be an element of the differential polynomial algebra  $\mathcal{R}\{y_1, \dots, y_n\}$  not in  $\mathcal{R}$  and let  $\theta$  be a derivative operator of  $\mathcal{R}$  of order greater than 0. Then  $\theta A - S_A \theta u_A$  has lower rank than  $\theta u_A$ .*

*Proof* If we write  $A = \sum I_i u_A^i$  as before, and if  $\delta \in \Delta$ , then

$$\delta A = S_A \delta u_A + \sum \delta I_i \cdot u_A^i.$$

Since any derivative of a  $y_j$  present in any  $I_i$  is lower than  $u_A$ , any derivative present in any  $\delta I_i$  is lower than  $\delta u_A$ , and  $u_A$  is too. Thus  $\delta A - S_A \delta u_A$  is lower than  $\delta u_A$ , that is, the lemma holds when  $\text{ord } \theta = 1$ . The lemma for arbitrary  $\theta$  follows quickly by induction on  $\text{ord } \theta$ .

**Corollary** *If  $\mathcal{R}$  is a differential integral domain and if  $A \in \mathcal{R}\{y_1, \dots, y_n\}$  has the property that  $\delta A \in (A)$  for some derivation operator  $\delta \in \Delta$ , then  $A \in \mathcal{R}[(\theta y_j)^p]_{\theta \in \Theta, 1 \leq j \leq n}$ , where  $p$  denotes the characteristic of  $\mathcal{R}$ .*

*Proof* We may suppose that  $A \notin \mathcal{R}$ , as otherwise the lemma is obvious, and therefore we may argue by induction on the leader  $u_A$  (relative to some fixed ranking). Because of the obvious inequality  $\deg \delta A \leq \deg A$ , the relation  $\delta A \in (A)$  implies that  $\delta A = aA$ , where  $a \in \mathcal{R}$ ; in particular,  $\delta A$  is free of  $\delta u_A$ . Since by Lemma 5 we have  $\delta A = S_A \delta u_A + T$  with  $T$  free of  $\delta u_A$ , we conclude that  $S_A = 0$ , so that  $p \neq 0$  and  $A = \sum A_i u_A^{p_i}$ , where each  $A_i$  is lower than  $u_A$ . Then  $\sum (\delta A_i) u_A^{p_i} = \delta(\sum A_i u_A^{p_i}) = \delta A = aA = \sum a A_i u_A^{p_i}$ . As the degree in  $u_A$  of each  $\delta A_i$  is obviously less than or equal to 1, we conclude that each  $\delta A_i$  is free of  $u_A$ , so that  $\delta A_i = a A_i$  for every  $i$ . As  $A_i$  either is in  $\mathcal{R}$  or else has leader lower than  $u_A$  the result follows by induction.

## 9 Autoreduced sets

Let  $(y_1, \dots, y_n)$  be a finite family of differential indeterminates over a non-zero differential ring  $\mathcal{R}$ , and suppose we are given a ranking of  $(y_1, \dots, y_n)$ .

Let  $A$  be an element of  $\mathcal{R}\{y_1, \dots, y_n\}$  not in  $\mathcal{R}$ . A differential polynomial  $F \in \mathcal{R}\{y_1, \dots, y_n\}$  is called *partially reduced* with respect to  $A$  if  $F$  is free of every proper derivative of  $u_A$ . If  $F$  is partially reduced with respect to  $A$  and  $\deg_{u_A} F < \deg_{u_A} A$ , then  $F$  is said to be *reduced* with respect to  $A$  (it being understood that 0 is always reduced with respect to  $A$ ). More generally, if  $\Sigma$  is any set or family of elements of  $\mathcal{R}\{y_1, \dots, y_n\}$  none of which is in  $\mathcal{R}$ ,  $F$  is said to be *reduced* or *partially reduced with respect to  $\Sigma$*  if  $F$  is, respectively, reduced or partially reduced with respect to each element of  $\Sigma$ .

A subset of  $\mathcal{R}\{y_1, \dots, y_n\}$  will be called *autoreduced* if no element of the subset belongs to  $\mathcal{R}$  and each element of the subset is reduced with respect to all the others. In any autoreduced set distinct elements must obviously have distinct leaders. It is an easy consequence of Chapter 0, Section 17, Lemma 15(a), that *every autoreduced set is finite*. As examples of autoreduced sets we have the empty set, and any set consisting of a single element of  $\mathcal{R}\{y_1, \dots, y_n\}$  not in  $\mathcal{R}$ .

**REMARK** Autoreduced sets were introduced by Ritt (who called them "ascending sets" or "chains") as a tool in his process of reduction of differential polynomials. This process, which plays a role analogous to that of Euclidean division of polynomials, is described below in the discussion culminating with Propositions 1 and 2.

If  $A$  is any autoreduced set we shall frequently, without further comment, denote by  $H_A$  the product  $\prod_{A \in A} I_A S_A$ .

Let  $A$  be an autoreduced subset of  $\mathcal{R}\{y_1, \dots, y_n\}$ . We are going to define, for each  $F \in \mathcal{R}\{y_1, \dots, y_n\}$ , a differential polynomial  $\tilde{F} \in \mathcal{R}\{y_1, \dots, y_n\}$ , called the *partial remainder* of  $F$  with respect to  $A$ , and corresponding natural numbers  $s_A$  ( $A \in A$ ), such that  $\tilde{F}$  is partially reduced with respect to  $A$ , the rank of  $\tilde{F}$  is lower than or equal to that of  $F$ , and  $\prod_{A \in A} S_A^{s_A} \cdot F \equiv \tilde{F} \pmod{[A]}$ .

If  $F$  is partially reduced with respect to  $A$ , we define  $\tilde{F} = F$  and  $s_A = 0$  ( $A \in A$ ). It is then obvious that  $\tilde{F}$  and the numbers  $s_A$  have the desired properties. We suppose that  $F$  is not partially reduced with respect to  $A$ , that is, that  $F$  involves a proper derivative  $u$  of some  $u_A$ , and define  $\tilde{F}$  and the  $s_A$  by induction on the highest such  $u$ . Let  $v$ , then, denote the highest such  $u$  present in  $F$ , and assume the partial remainder and corresponding natural numbers have been defined, and have the desired properties, for every differential polynomial in  $\mathcal{R}\{y_1, \dots, y_n\}$  that does not involve a proper derivative of any  $u_A$  of rank higher than or equal to that of  $v$ . Let  $u_C$  denote the highest  $u_A$  of which  $v$  is a proper derivative, and write  $v = \theta u_C$ . By Section 8,

Lemma 5, we may write  $S_C v = T + \theta C$ , where  $T \in \mathcal{R}\{y_1, \dots, y_n\}$  and  $T$  is lower than  $v$ . Letting  $e = \deg_v F$ , we may write  $F = \sum_{0 \leq i \leq e} J_i v^i$ , where  $J_0, \dots, J_e \in \mathcal{R}\{y_1, \dots, y_n\}$  are lower than  $v$ . Then

$$S_C^e F = \sum_{0 \leq i \leq e} S_C^{e-i} J_i (S_C v)^i \equiv \sum_{0 \leq i \leq e} S_C^{e-i} J_i T^i \pmod{\theta C}.$$

Obviously, the differential polynomial  $G = \sum_{0 \leq i \leq e} S_C^{e-i} J_i T^i$  cannot involve a proper derivative of any  $u_A$  as high as  $v$ , and the rank of  $G$  is no higher than that of  $F$ . Therefore the partial remainder  $\tilde{G}$  of  $G$  with respect to  $A$  and the corresponding natural numbers  $t_A$  are defined and have the desired properties. We now define  $\tilde{F} = \tilde{G}$ ,  $s_C = t_C + e$ , and  $s_A = t_A$  ( $A \in A$ ,  $A \notin C$ ). It is obvious that  $\tilde{F}$  and the numbers  $s_A$  have the properties announced above.

What we have just proved is summarized in the following lemma.

**Lemma 6** *Let  $A$  be an autoreduced set (relative to some given ranking) in the differential polynomial algebra  $\mathcal{R}\{y_1, \dots, y_n\}$ , let  $F \in \mathcal{R}\{y_1, \dots, y_n\}$ , let  $\tilde{F}$  denote the partial remainder of  $F$  with respect to  $A$ , and let  $s_A$  ( $A \in A$ ) denote the corresponding family of natural numbers. Then  $\tilde{F}$  is partially reduced with respect to  $A$ , the rank of  $\tilde{F}$  is lower than or equal to that of  $F$ , and*

$$\prod_{A \in A} S_A^{s_A} \cdot F \equiv \tilde{F} \pmod{[A]}.$$

More precisely,  $\prod_{A \in A} S_A^{s_A} \cdot F - \tilde{F}$  can be written as a linear combination over  $\mathcal{R}\{y_1, \dots, y_n\}$  of derivatives  $\theta A$  such that  $A \in A$  and  $\theta u_A$  is lower than or equal to the leader of  $F$ .

**Corollary** *If  $F_1, \dots, F_q \in \mathcal{R}\{y_1, \dots, y_n\}$ , then there exist  $G_1, \dots, G_q \in \mathcal{R}\{y_1, \dots, y_n\}$ , partially reduced with respect to  $A$  and of rank no higher than the highest of the ranks of  $F_1, \dots, F_q$ , and there exist natural numbers  $t_A$  ( $A \in A$ ), such that*

$$\prod_{A \in A} S_A^{t_A} \cdot F_j \equiv G_j \pmod{[A]} \quad (1 \leq j \leq q).$$

*Proof* Let  $\tilde{F}_j$  be the partial remainder of  $F_j$  with respect to  $A$ , and let  $s_{jA}$  ( $A \in A$ ) be the corresponding natural numbers. If we define  $t_A = \max(s_{1A}, \dots, s_{qA})$  and  $G_j = \prod_{A \in A} S_A^{t_A - s_{jA}} \cdot \tilde{F}_j$ , the conditions are met.

Now consider finitely many differential polynomials  $H_1, \dots, H_q \in \mathcal{R}\{y_1, \dots, y_n\}$ , all partially reduced with respect to  $A$ . Let the elements of  $A$  be denoted by  $A_1, \dots, A_r$ , and set  $u_k = u_{A_k}$ ,  $I_k = I_{A_k}$ ,  $S_k = S_{A_k}$  ( $1 \leq k \leq r$ ). Furthermore, let the notation be arranged so that  $u_k$  is lower than  $u_{k'}$  whenever  $1 \leq k < k' \leq r$ . Then we may write

$$A_k = I_k u_k^{d_k} + I_{k1} u_k^{d_k-1} + \dots + I_{kd_k},$$

where  $d_k = \deg_{u_k} A_k$ , and each  $I_{kj}$ , like  $I_k$ , is an element of  $\mathcal{R}\{y_1, \dots, y_n\}$  free of every derivative of  $u_i$  ( $k \leq i \leq r$ ) and free of every proper derivative of  $u_i$  ( $1 \leq i < k$ ).

Let  $e_r = \max(\deg_{u_r} H_1, \dots, \deg_{u_r} H_q)$ , and define  $i_r = e_r - d_r + 1$  or  $i_r = 0$  according as  $e_r \geq d_r$  or  $e_r < d_r$ . In either case we may write

$$I_r^{i_r} H_j \equiv H_j^{(r)} \pmod{A_r} \quad (1 \leq j \leq q),$$

where each  $H_j^{(r)} \in \mathcal{R}\{y_1, \dots, y_n\}$  is, like  $H_j$ , partially reduced with respect to  $A$ , is reduced with respect to  $A_r$ , and has rank lower than or equal to the highest of the ranks of  $H_1, \dots, H_q$ .

Next, let  $e_{r-1} = \max(\deg_{u_{r-1}} H_1^{(r)}, \dots, \deg_{u_{r-1}} H_q^{(r)})$ , and define  $i_{r-1} = e_{r-1} - d_{r-1} + 1$  or  $i_{r-1} = 0$  according as  $e_{r-1} \geq d_{r-1}$  or  $e_{r-1} < d_{r-1}$ . In either case we may write

$$I_{r-1}^{i_{r-1}} H_j^{(r)} \equiv H_j^{(r-1)} \pmod{A_{r-1}} \quad (1 \leq j \leq q),$$

where each  $H_j^{(r-1)} \in \mathcal{R}\{y_1, \dots, y_n\}$  is, like  $H_j^{(r)}$ , partially reduced with respect to  $A$ , is reduced with respect to  $A_{r-1}$  and  $A_r$ , and has rank lower than or equal to the highest of the ranks of  $H_1^{(r)}, \dots, H_q^{(r)}$ .

Continuing in this way, we define successively  $i_r, (H_j^{(r)})_{1 \leq j \leq q}, i_{r-1}, (H_j^{(r-1)})_{1 \leq j \leq q}, \dots, i_1, (H_j^{(1)})_{1 \leq j \leq q}$ , where, for each  $k$ ,  $i_k$  is a natural number,  $H_j^{(k)} \in \mathcal{R}\{y_1, \dots, y_n\}$  is partially reduced with respect to  $A$ , is reduced with respect to  $A_k, \dots, A_r$ , and has rank lower than or equal to the highest of the ranks of  $H_1, \dots, H_r$ , and  $H_j^{(k)} \equiv I_k^{i_k} \dots I_r^{i_r} H_j \pmod{(A_k, \dots, A_r)}$ .

If we apply this process of successive division to the case in which  $q = 1$  and  $H_1$  is the partial remainder  $\tilde{F}$  of the differential polynomial  $F \in \mathcal{R}\{y_1, \dots, y_n\}$  with respect to  $A$ , the resulting differential polynomial  $H_1^{(1)}$  is called the *remainder* of  $F$  with respect to  $A$ . The resulting natural numbers  $i_1, \dots, i_r$ , which we now denote by  $i_{A_1}, \dots, i_{A_r}$ , together with the natural numbers  $s_{A_1}, \dots, s_{A_r}$  corresponding to the partial remainder  $\tilde{F}$ , we call the *exponents* corresponding to the remainder of  $F$  with respect to  $A$ . We thus have the following result.

**Proposition 1** *Let  $A$  be an autoreduced set (relative to some given ranking) in the differential polynomial algebra  $\mathcal{R}\{y_1, \dots, y_n\}$ , let  $F \in \mathcal{R}\{y_1, \dots, y_n\}$ , let  $F_0$  denote the remainder of  $F$  with respect to  $A$ , and let  $i_A, s_A$  ( $A \in A$ ) denote the corresponding exponents. Then  $F_0$  is reduced with respect to  $A$ , the rank of  $F_0$  is lower than or equal to that of  $F$ , and*

$$\prod_{A \in A} I_A^{i_A} S_A^{s_A} \cdot F \equiv F_0 \pmod{[A]}.$$

More precisely,  $\prod_{A \in A} I_A^{i_A} S_A^{s_A} \cdot F - F_0$  can be written as a linear combination over  $\mathcal{R}\{y_1, \dots, y_n\}$  of derivatives  $\theta A$  such that  $A \in A$  and  $\theta u_A$  is lower than or equal to the leader of  $F$ .

If we apply the same process of successive division to the case in which  $H_1, \dots, H_q$  are the differential polynomials  $G_1, \dots, G_q$  of the Corollary to Lemma 6, we obtain the following generalization of Proposition 1.

**Proposition 2** *With notation as in Proposition 1, if  $F_1, \dots, F_q \in \mathcal{R}\{y_1, \dots, y_n\}$ , then there exist differential polynomials  $E_1, \dots, E_q \in \mathcal{R}\{y_1, \dots, y_n\}$ , reduced with respect to  $A$  and of rank no higher than the highest of the ranks of  $F_1, \dots, F_q$ , and there exist natural numbers  $j_A, t_A$  ( $A \in A$ ), such that*

$$\prod_{A \in A} I_A^{j_A} S_A^{t_A} \cdot F_j \equiv E_j \pmod{[A]} \quad (1 \leq j \leq q).$$

The following lemma is recorded for use in the second part of Chapter IV.

**Lemma 7** *Let  $A$  be an autoreduced set in  $\mathcal{R}\{y_1, \dots, y_n\}$ , and denote the elements of  $A$  by  $A_1, \dots, A_r$ ; let  $F \in \mathcal{R}\{y_1, \dots, y_n\}$ , and let  $z_1, \dots, z_r$  denote  $r$  differential indeterminates over  $\mathcal{R}\{y_1, \dots, y_n\}$ . Then there exist natural numbers  $t_A, \sigma_A$  ( $A \in A$ ), and a finite family  $(M_\alpha)$  of distinct differential monomials in  $(z_1, \dots, z_r)$ , and a family  $(C_\alpha)$  of nonzero elements of  $\mathcal{R}\{y_1, \dots, y_n\}$ , with the following properties:*

(a) *Whenever  $\theta z_k, \theta' z_k$  are distinct derivatives, each one present in at least one  $M_\alpha$ , then*

$$\theta u_{A_k} \neq \theta' u_{A_k}.$$

(b) *Each  $C_\alpha$  is reduced with respect to  $A$ .*

(c)  $\prod_{A \in A} I_A^{t_A} S_A^{\sigma_A} \cdot F = \sum_\alpha C_\alpha \cdot M_\alpha(A_1, \dots, A_r).$

*Proof* For each derivative  $v$  of a leader of an element of  $A$  there exists a pair  $(\theta, k) \in \Theta \times \mathbb{N}$  with  $1 \leq k \leq r$  such that  $v = \theta u_{A_k}$ , but the pair need not be unique. From among the various possibilities for  $(\theta, k)$  choose one and denote it by  $(\theta_v, k(v))$ . If  $F$  is reduced with respect to  $A$ , the conclusion in the lemma is obvious, so we may suppose that  $F$  involves a highest ranking derivative  $v$  of a leader of an element of  $A$  such that either  $v$  is a proper derivative of  $u_{A_k(v)}$ , or  $v = u_{A_k(v)}$  and  $f \geq a$  where  $f = \deg_v F$  and  $a = \deg_v A_{k(v)}$ . In the former case  $\theta_v A_{k(v)} = S_{A_{k(v)}} v + T$  with  $T$ , like  $S_{A_{k(v)}}$ , of lower rank than  $v$  (see Section 8, Lemma 5), so that  $S_{A_{k(v)}}^e F$  can be expressed as a polynomial  $\Phi$  in  $\theta_v A_{k(v)}$  and in derivatives  $\theta y_j$  lower than  $v$ . In the latter case,  $A_{k(v)} = I_{A_{k(v)}} v^a + I_1 v^{a-1} + \dots + I_a$  with  $I_1, \dots, I_a$ , like  $I_{A_{k(v)}}$ , of lower rank than  $v$ ; an easy induction argument then shows that, for each integer  $e \geq a$ ,  $I_{A_{k(v)}}^{e-a+1} v^e$  can be expressed as a polynomial in  $A_{k(v)}$ , in derivatives  $\theta y_j$  lower than  $v$ , and in  $v$  itself, of degree in  $v$  less than  $a$ , so that  $I_{A_{k(v)}}^{e-a+1} F$  can be expressed as a polynomial  $\Phi$  in  $A_{k(v)}$ , in derivatives  $\theta y_j$  lower than  $v$ , and in  $v$  itself with  $\deg_v \Phi < a$ . In either case, if  $\Phi$  is free of every proper derivative of a leader of an element of  $A$  and if  $\deg_{u_A} \Phi < \deg_{u_A} A$  ( $A \in A$ ), then we

have finished, so we may suppose that  $\Phi$  involves a highest ranking derivative  $w$  of a leader of an element of  $A$  such that either  $w$  is a proper derivative of  $u_{A_k(w)}$ , or  $w = u_{A_k(w)}$  and  $\deg_w \Phi \geq \deg_w A_{k(w)}$ . Then we can give  $\Phi$  and  $w$  the same treatment we gave  $F$  and  $v$ , above. After a finite number of such treatments we obtain the desired conclusion.

## 10 Characteristic sets

Let  $\mathcal{R}$  be a nonzero differential ring, let  $(y_1, \dots, y_n)$  be a finite family of differential indeterminates over  $\mathcal{R}$ , and suppose given a ranking of  $(y_1, \dots, y_n)$ .

It is useful to introduce the notion of comparative rank into the set of all autoreduced subsets of  $\mathcal{R}\{y_1, \dots, y_n\}$ . This is done by the following convention, in the statement of which  $A_1, \dots, A_r$  denote the elements of an autoreduced set  $A$  and  $B_1, \dots, B_s$  denote those of an autoreduced set  $B$ , in each case arranged in order of increasing rank.

(1) If there exists a nonzero  $k \in \mathbb{N}$  with  $k \leq r$  and  $k \leq s$  such that

$$\text{rank } A_i = \text{rank } B_i \quad (1 \leq i < k), \quad \text{rank } A_k < \text{rank } B_k,$$

or if  $r > s$  and

$$\text{rank } A_i = \text{rank } B_i \quad (1 \leq i \leq s),$$

then  $A$  is said to have lower rank than  $B$ .

(2) If  $r = s$  and  $\text{rank } A_i = \text{rank } B_i$  ( $1 \leq i \leq r$ ), then  $A$  is said to have the same rank as  $B$ .

It is clear that this notion of comparative rank defines a pre-order on the set of all autoreduced sets in  $\mathcal{R}\{y_1, \dots, y_n\}$ .

**Proposition 3** *In every nonempty set of autoreduced subsets of  $\mathcal{R}\{y_1, \dots, y_n\}$  there exists an autoreduced subset of lowest rank.*

*Proof* Let  $\mathfrak{M}$  be any nonempty set of autoreduced subsets of  $\mathcal{R}\{y_1, \dots, y_n\}$ . Define by induction an infinite decreasing sequence of subsets of  $\mathfrak{M}$  by the conditions that  $\mathfrak{M}_0 = \mathfrak{M}$  and, for  $i > 0$ ,  $\mathfrak{M}_i$  is the set of all autoreduced sets  $A \in \mathfrak{M}_{i-1}$  with  $\text{Card } A \geq i$  such that the  $i$ th lowest element of  $A$  is of lowest possible rank. It is obvious that in all elements of  $\mathfrak{M}_i$  the  $i$ th lowest differential polynomials have the same leader  $v_i$ . If every  $\mathfrak{M}_i$  were nonempty, then the leaders  $v_i$  would form an infinite sequence of derivatives of the  $y_j$  such that no  $v_i$  is a derivative of any other, and this would contradict Chapter 0, Section 17, Lemma 15(a). Therefore there is a smallest  $i$  such that  $\mathfrak{M}_i = \emptyset$  and, since  $\mathfrak{M}_0 = \mathfrak{M} \neq \emptyset$ ,  $i > 0$ . Any element of  $\mathfrak{M}_{i-1}$  is clearly an autoreduced subset in  $\mathfrak{M}$  of lowest rank.

If  $\mathfrak{f}$  is any differential ideal of  $\mathcal{R}\{y_1, \dots, y_n\}$ , there exists an autoreduced subset  $A$  of  $\mathfrak{f}$  such that  $S_A \notin \mathfrak{f}$  ( $A \in A$ ); for example, the empty set. Such an autoreduced set of lowest rank is called a *characteristic set* of  $\mathfrak{f}$  (relative to the given ranking).

**Lemma 8** *Let  $A$  be a characteristic set of a differential ideal  $\mathfrak{f}$  of  $\mathcal{R}\{y_1, \dots, y_n\}$ . Then  $I_A \notin \mathfrak{f}$  ( $A \in A$ ) and, for every  $P \in \mathfrak{f}$  that is not in  $\mathcal{R}$  and is reduced with respect to  $A$ ,  $S_P \in \mathfrak{f}$ .*

*Proof* Let  $P \in \mathfrak{f}$ ,  $P \notin \mathcal{R}$ , and suppose that  $P$  is reduced with respect to  $A$ . Then  $P$  and the elements  $A \in A$  for which  $u_A$  is lower than  $u_P$  form an autoreduced set lower than  $A$ , so that  $S_P \in \mathfrak{f}$ . If for some  $A \in A$  we had  $I_A \in \mathfrak{f}$ , then  $A - I_A u_A^d$ , with  $d = \deg_{u_A} A$ , would be an element of  $\mathfrak{f}$  reduced with respect to  $A$  and either with leader  $u_A$  or else free of  $u_A$ . In either case the differential polynomial  $\partial(A - I_A u_A^d)/\partial u_A = S_A - dI_A u_A^{d-1}$  would be in  $\mathfrak{f}$ , so that  $S_A$  would too.

The following technical lemma, which makes special hypotheses on both the differential ideal and the ranking, is used several times in subsequent chapters.

**Lemma 9** *Let  $A$  be a characteristic set of a prime differential ideal  $\mathfrak{p}$  of  $\mathcal{R}\{y_1, \dots, y_n\}$ . Assume either that the ranking is sequential or that  $A$  is empty and the ranking is integrated. Denote by  $V$  the set of all derivatives  $\theta y_j$  that are not proper derivatives of any leader  $u_A$  ( $A \in A$ ), and denote by  $W$  the set of all elements  $w \in V$  such that only finitely many derivatives of  $w$  are in  $V$ . If  $P \in \mathfrak{p}$ , and if  $v \in V - W$  has the property that every derivative  $\theta y_j$  present in  $P$  and higher than  $v$  is in  $V - W$ , then  $\partial P/\partial v \in \mathfrak{p}$ .*

*Proof* Let  $r = \deg P$ . Let  $s$  denote the number of derivatives  $\theta y_j$  present in  $P$  and higher than  $v$ . Under either of the alternative assumptions in the hypothesis, there exists a derivative operator  $\bar{\theta}$  of minimal order  $t$  such that  $\bar{\theta}v \in V - W$  and  $\bar{\theta}v$  is higher than or equal to every derivative of any  $y_j$  present in  $P$ . Arguing by induction on the element  $(r, s, t)$  of the lexicographically well-ordered set  $\mathbb{N}^3$ , we make the appropriate inductive hypothesis.

If  $t = 0$ , we have  $P = \sum P_i v^i$ , where each  $P_i$  is lower than  $v$ . By Section 9, Proposition 2, we may write  $HP_i \equiv Q_i \pmod{[A]}$  for every  $i$ , where  $H$  is a product of the form  $\prod_{A \in A} I_A^{\alpha} S_A^{\beta}$  and  $Q_i$  is reduced with respect to  $A$  and is lower than  $v$ . By Lemma 8,  $\sum i Q_i v^{i-1} \in \mathfrak{p}$ , so that  $H \sum i P_i v^{i-1} = H \partial P/\partial v$  is in  $\mathfrak{p}$ , whence  $\partial P/\partial v$  is too.

Let  $t > 0$ . Then we may write  $\bar{\theta} = \bar{\theta}_1 \delta$ , with  $\delta$  a derivation operator and  $\bar{\theta}_1$  a derivative operator of order  $t-1$ . For any derivative  $v_1 = \theta y_j$  with  $v_1 > v$  our inductive hypothesis implies that  $\partial P/\partial v_1 \in \mathfrak{p}$ . Since  $\delta P =$

$P^\delta + \sum_{v_1} \partial P/\partial v_1 \cdot \delta v_1$ , we conclude that the differential polynomial  $P_1 = P^\delta + \sum_{v_1} \partial P/\partial v_1 \cdot \delta v_1$  is in  $\mathfrak{p}$ . Since  $\delta v > v$  we have  $\partial P/\partial(\delta v) \in \mathfrak{p}$ , and because  $\deg \partial P/\partial(\delta v) < r$ , our inductive hypothesis implies that  $\partial(\partial P/\partial(\delta v))/\partial v_1 \in \mathfrak{p}$  whenever  $v_1 \geq v$ . Therefore

$$\begin{aligned} \partial P_1/\partial(\delta v) &= \partial P^\delta/\partial(\delta v) + \sum_{v_1 \leq v} \partial^2 P/\partial v_1 \partial(\delta v) \cdot \delta v_1 + \partial P/\partial v \\ &\equiv (\partial P/\partial(\delta v))^\delta + \sum_{v_1} \partial(\partial P/\partial(\delta v))/\partial v_1 \cdot \delta v_1 + \partial P/\partial v \\ &\equiv \delta(\partial P/\partial(\delta v)) + \partial P/\partial v \\ &\equiv \partial P/\partial v \pmod{\mathfrak{p}}. \end{aligned}$$

However,  $\deg P_1 \leq r$ , and the derivatives  $\theta y_j$  present in  $P_1$  and higher than  $\delta v$  are all present in  $P$ , and hence are in  $V - W$ , and are at most  $s$  in number. Also  $\delta v \in V - W$ ,  $\bar{\theta}_1(\delta v) \in V - W$ , and  $\bar{\theta}_1(\delta v)$  is higher than or equal to every derivative of any  $y_j$  present in  $P_1$ . Since  $\text{ord } \bar{\theta}_1 = t-1$ , we see by our inductive hypothesis that  $\partial P_1/\partial(\delta v) \in \mathfrak{p}$ . It follows from the congruence above that  $\partial P/\partial v \in \mathfrak{p}$ .

## 11 Pseudo-leaders

Let  $\mathcal{R}$  be a nonzero differential ring, let  $(y_1, \dots, y_n)$  be a finite family of differential indeterminates, and suppose given a ranking.

Consider a differential polynomial  $A \in \mathcal{R}\{y_1, \dots, y_n\}$ , and suppose there exists a derivative  $u$  of one of the differential indeterminates  $y_j$  such that  $\partial A/\partial u \neq 0$ . Then there is such a derivative  $u$  of maximal order, and we call its order the *essential order* of  $A$ . There is also such a derivative  $u$  of highest rank; denote this derivative by  $v$ . If  $A$  is free of every proper derivative of  $v$ , we call  $v$  *pseudo-leader* of  $A$  (relative to the given ranking), and call  $\partial A/\partial v$  *pseudo-separant* of  $A$ . We say that a differential polynomial  $B \in \mathcal{R}\{y_1, \dots, y_n\}$  is *partially pseudo-reduced* with respect to  $A$  if  $B$  is free of every proper derivative of the pseudo-leader  $v$ . (When  $\mathcal{R}$  has the property that  $ka \neq 0$  for every nonzero  $k \in \mathbb{N}$  and every nonzero  $a \in \mathcal{R}$ , then the notions "pseudo-leader," "pseudo-separant," and "partially pseudo-reduced" coincide, respectively, with the notions "leader," "separant," and "partially reduced.") We say a differential polynomial is *pseudo-led* if there exists a ranking relative to which the differential polynomial has pseudo-leader.

The following lemma is similar to Section 8, Lemma 5.

**Lemma 10** *Let  $A \in \mathcal{R}\{y_1, \dots, y_n\}$ , let  $v$  be the highest ranking derivative of  $A$  such that  $\partial A/\partial v \neq 0$ , and let  $e$  be the essential order of  $A$ . For each derivative operator  $\theta$  of  $\mathcal{R}$  of order greater than 0,  $\theta v$  is the highest ranking derivative*

$u$  such that  $\partial(\theta A)/\partial u \neq 0$ ,  $\theta A$  has essential order  $e + \text{ord } \theta$ , and we may write  $\theta A = (\partial A/\partial v)\theta v + U_\theta$ , where  $U_\theta \in \mathcal{R}\{y_1, \dots, y_n\}$  and every derivative  $w$  present in  $U_\theta$  with  $w \geq \theta v$  is present in  $A$  and has the property that  $\partial U_\theta/\partial w = 0$ . In particular, if  $v$  is pseudo-leader of  $A$ , then  $\theta v$  is pseudo-leader of  $\theta A$  and  $U_\theta$  is free of every derivative of  $v$  that is higher than or equal to  $\theta v$ .

The proof, similar to that of Section 8, Lemma 5, is by induction on the order of  $\theta$ .

Using this lemma it is easy to deduce the following result.

**Corollary 1** Let  $A$  have pseudo-separant  $S$ , and let  $B \in \mathcal{R}\{y_1, \dots, y_n\}$ . Then there exist  $b \in \mathbf{N}$  and  $B_1 \in \mathcal{R}\{y_1, \dots, y_n\}$  such that  $B_1$  is partially pseudo-reduced with respect to  $A$  and  $S^b B \equiv B_1 \pmod{[A]}$ .

**Corollary 2** Assuming that  $\mathcal{R}$  is a differential field, let  $v$  be the highest ranking derivative with  $\partial A/\partial v \neq 0$ . If  $B \in [A]:(\partial A/\partial v)^\infty$  and  $v_0$  denotes the highest ranking derivative of  $v$  present in  $AB$ , then  $B \in (\Theta_0 A):(\partial A/\partial v)^\infty$ , where  $\Theta_0$  is the set of derivative operators  $\theta$  of  $\mathcal{R}$  such that  $\theta v \leq v_0$ . In particular, if  $v$  is pseudo-leader of  $A$ , then every element of  $[A]:(\partial A/\partial v)^\infty$  that is partially pseudo-reduced with respect to  $A$  is in  $(A):(\partial A/\partial v)^\infty$ .

*Proof* Suppose there exists a relation  $(\partial A/\partial v)^b B = \sum_{1 \leq i \leq t} C_i \theta_i A$ , where each  $C_i$  is in  $\mathcal{R}\{y_1, \dots, y_n\}$  and each  $\theta_i$  is derivative operator of  $\mathcal{R}$ . Of all such relations we use one with  $t$  as small as possible, and we suppose the notation arranged so that  $\theta_i v < \theta_t v$  ( $1 \leq i < t$ ). If  $t > 0$  and  $\theta_t v > v_0$ , then we may write  $\theta_t A = (\partial A/\partial v)\theta_t v + U_{\theta_t}$  as in Lemma 10, and  $\theta_t v$  is not present in any of  $\partial A/\partial v$ ,  $B$ ,  $\theta_1 A, \dots, \theta_{t-1} A$ . Therefore if, in the above relation we substitute  $-U_{\theta_t}/(\partial A/\partial v)$  for  $\theta_t v$  and then multiply both members by a high power of  $\partial A/\partial v$ , we obtain a similar relation with  $t$  replaced by a smaller number. Therefore either  $t = 0$ , or  $t > 0$  and  $\theta_t v \leq v_0$ ; in either case,  $B \in (\Theta_0 A):(\partial A/\partial v)^\infty$ .

## 12 Differential algebras of power series

Let  $\mathcal{R}$  be a nonzero differential ring. Denote the set of derivation operators of  $\mathcal{R}$  by  $\Delta$  and the set of derivative operators of  $\mathcal{R}$  by  $\Theta$ .

Suppose  $s = (s_i)_{i \in I}$  is a family of elements of a differential overring of  $\mathcal{R}$  such that

- (i)  $s$  is algebraically independent over  $\mathcal{R}$ ;
- (ii)  $\mathcal{R}[s] = \mathcal{R}\{s\}$  (i.e., for each  $i_0 \in I$  and each  $\delta \in \Delta$ ,  $\delta s_{i_0}$  equals a polynomial in  $(s_i)_{i \in I}$  over  $\mathcal{R}$ ).

Because of (i) we may form the power series algebra  $\mathcal{R}[[s]]$  in  $s$  over  $\mathcal{R}$ . Because of (ii) each  $\delta \in \Delta$  yields a derivation  $A \mapsto \delta A$  of the polynomial ring  $\mathcal{R}[s]$ . By Chapter 0, Section 13, these derivations extend canonically to derivations of  $\mathcal{R}[[s]]$  that commute with each other. Thus, the operation of  $\Delta$  on  $\mathcal{R}[s]$  extends to  $\mathcal{R}[[s]]$ , and  $\mathcal{R}[[s]]$  becomes a differential algebra over  $\mathcal{R}$  that is a differential overring of  $\mathcal{R}[s]$ .

It is easy to verify that if  $(A_\lambda)_{\lambda \in \Lambda}$  is a family of elements of  $\mathcal{R}[[s]]$  such that the sum  $\sum_{\lambda \in \Lambda} A_\lambda$  is meaningful, then, for each  $\delta \in \Delta$ , the sum  $\sum_{\lambda \in \Lambda} \delta A_\lambda$  is meaningful and equals  $\delta \sum_{\lambda \in \Lambda} A_\lambda$ . Also, if  $I = I_1 \cup I_2$ , with  $I_1$  and  $I_2$  disjoint and  $\mathcal{R}[(s_i)_{i \in I_1}] = \mathcal{R}\{(s_i)_{i \in I_1}\}$ , then the canonical ring isomorphism

$$\mathcal{R}[(s_i)_{i \in I}] \approx \mathcal{R}[(s_i)_{i \in I_1}] [[(s_i)_{i \in I_2}]]$$

is a differential ring isomorphism.

Let  $\mathcal{R}[[s']] = \mathcal{R}[(s'_i)_{i \in I'}]$  also be a differential algebra of power series over  $\mathcal{R}$ , like  $\mathcal{R}[[s]]$ , and let  $S = (S_i)_{i \in I}$  be a family, with set of indices  $I$ , of elements of  $\mathcal{R}[[s']]$  such that  $v(S_i) > 0$  for each  $i$ . Then the substitution of  $S$  for  $s$  is defined and is a ring homomorphism  $\mathcal{R}[[s]] \rightarrow \mathcal{R}[[s']]$ . A straightforward computation shows that if  $\delta S_i = (\delta s_i)(S)$  for each  $i \in I$  and each  $\delta \in \Delta$ , then (and only then) substitution of  $S$  for  $s$  is a differential ring homomorphism.

For an example, let  $(y_1, \dots, y_n)$  be a family of differential indeterminates over  $\mathcal{R}$ . Then we may form the differential algebra of power series  $\mathcal{R}[[\theta y_j]_{\theta \in \Theta, 1 \leq j \leq n}]$ . It is called the *differential power series algebra* in  $(y_1, \dots, y_n)$  over  $\mathcal{R}$ , and is denoted by  $\mathcal{R}\{\{y_1, \dots, y_n\}\}$ ; its elements are called *differential power series* in  $(y_1, \dots, y_n)$  over  $\mathcal{R}$ . If  $Y_1, \dots, Y_n$  are elements of the differential algebra of power series  $\mathcal{R}[[s']]$  such that  $v(\theta Y_j) > 0$  ( $\theta \in \Theta$ ,  $1 \leq j \leq n$ ), then the substitution of  $(\theta Y_j)_{\theta \in \Theta, 1 \leq j \leq n}$  for  $(\theta y_j)_{\theta \in \Theta, 1 \leq j \leq n}$  is defined and is a differential algebra homomorphism  $\mathcal{R}\{\{y_1, \dots, y_n\}\} \rightarrow \mathcal{R}[[s']]$ . When there is no danger of confusion, we call it the substitution of  $(Y_1, \dots, Y_n)$  for  $(y_1, \dots, y_n)$ , and denote its image by  $\mathcal{R}\{\{Y_1, \dots, Y_n\}\}$ .

For another example, let  $c$  be a constant that is transcendental over  $\mathcal{R}$ . Then  $\mathcal{R}[[c]]$  is a differential algebra over  $\mathcal{R}$ . The differential ring of quotients of  $\mathcal{R}[[c]]$  over the multiplicatively stable set consisting of the powers of  $c$  is then  $\mathcal{R}((c))$ . For any element  $C = \sum_{k \in \mathbf{Z}} a_k c^k$  of  $\mathcal{R}((c))$  we have  $\delta C = \sum_{k \in \mathbf{Z}} (\delta a_k) c^k$  ( $\delta \in \Delta$ ). Thus,  $C$  is a constant if and only if every coefficient in  $C$  is a constant. If this is the case, and if  $C \neq 0$ ,  $v(C) > 0$ , and the leading coefficient in  $C$  is invertible in  $\mathcal{R}$  (so that  $C$  is invertible in  $\mathcal{R}((c))$ ), then the substitution of  $C$  for  $c$ , which is an endomorphism of the differential algebra  $\mathcal{R}[[c]]$ , can be extended to a unique endomorphism of  $\mathcal{R}((c))$ ; this extended endomorphism, too, is called the *substitution of  $C$  for  $c$* .



for all choices of  $\theta_1, \dots, \theta_n \in \Theta$  and all choices of the indices  $k(1), \dots, k(n)$ . Conversely, if (1) holds for all choices of  $\theta_1, \dots, \theta_n$  with  $\theta_i \in \Theta(i-1)$  ( $1 \leq i \leq n$ ) and all choices of  $k(1), \dots, k(n)$ , then  $\eta_1, \dots, \eta_n$  are linearly dependent over  $\mathcal{C}$ .

*Proof* If  $\sum_{1 \leq j \leq n} c_j \eta_j = 0$  with  $c_1, \dots, c_n \in \mathcal{C}$  not all 0, then  $\sum_{1 \leq j \leq n} c_j \theta \eta_{jk} = 0$  for all  $\theta \in \Theta$  and all indices  $k$ , so that (1) holds. Conversely, suppose that (1) holds whenever  $\theta_i \in \Theta(i-1)$  and  $k(i)$  is arbitrary ( $1 \leq i \leq n$ ). We may suppose that  $n > 1$  and that the result is proved for lower values of  $n$ . Then we may further suppose that there exist  $\theta'_i \in \Theta(i-1)$  ( $1 \leq i \leq n-1$ ) and indices  $k'(1), \dots, k'(n-1)$  such that  $\det(\theta'_i \eta_{j, k'(i)})_{1 \leq i \leq n-1, 1 \leq j \leq n-1} \neq 0$ . Letting  $\Pi$  denote the Cartesian product of the set  $\Theta(n-1)$  and the set of indices  $1, \dots, r$ , we see that the matrix  $(\theta \eta_{jk})_{(\theta, k) \in \Pi, 1 \leq j \leq n}$  has the property that the  $n-1$  rows  $(\theta'_i \eta_{1, k'(i)}, \dots, \theta'_i \eta_{n, k'(i)})$  with  $1 \leq i \leq n-1$  are linearly independent and every other row is a linear combination of these; hence the rank of the matrix is  $n-1$ . Therefore there exists a nonzero vector  $(c_1, \dots, c_n) \in \mathcal{F}^n$  with the property that  $\sum_{1 \leq j \leq n} c_j \theta \eta_{jk} = 0$  for all  $\theta \in \Theta(n-1)$  and all indices  $k$ , and every vector with this property is a scalar multiple of this one. We may suppose, moreover, that  $c_j = 1$  for some  $j$ . For any  $\delta \in \Delta$  we have  $\sum_{1 \leq j \leq n} (\delta c_j) \theta \eta_{jk} + \sum_{1 \leq j \leq n} c_j (\delta \theta) \eta_{jk} = 0$ . However, if  $\theta \in \Theta(n-2)$ , then  $\delta \theta \in \Theta(n-1)$ , in which case,  $\sum_{1 \leq j \leq n} (\delta c_j) \theta \eta_{jk} = 0$ . Since this holds, in particular, for  $\theta = \theta'_i$  ( $1 \leq i \leq n-1$ ), and since every row  $(\theta \eta_{1k}, \dots, \theta \eta_{nk})$  is a linear combination of the rows  $(\theta'_i \eta_{1, k'(i)}, \dots, \theta'_i \eta_{n, k'(i)})$ , we see that

$$\sum_{1 \leq j \leq n} (\delta c_j) \theta \eta_{jk} = 0$$

for all  $\theta \in \Theta(n-1)$  and all indices  $k$ . Therefore  $(\delta c_1, \dots, \delta c_n)$  is a scalar multiple of  $(c_1, \dots, c_n)$ . Since  $c_j = 1$  and hence  $\delta c_j = 0$  for some  $j$ , the scalar factor must be 0, so that  $\delta c_j = 0$  for every  $j$ . Thus, each  $c_j \in \mathcal{C}$ .

The most important case of Theorem 1 is that in which  $r = 1$ .

**Corollary 1** Let  $\mathcal{A}$  be a differential algebra over  $\mathcal{F}$  with ring of constants  $\mathcal{A}_0$ . Then  $\mathcal{F}$  and  $\mathcal{A}_0$  are linearly disjoint over  $\mathcal{C}$ .

*Proof* If  $\eta_1, \dots, \eta_n \in \mathcal{F}$  are linearly dependent over  $\mathcal{A}_0$ , say

$$\sum_{1 \leq j \leq n} \gamma_j \eta_j = 0,$$

where  $\gamma_1, \dots, \gamma_n \in \mathcal{A}_0$  and some  $\gamma_j \neq 0$ , then  $\sum_{1 \leq j \leq n} \gamma_j \theta \eta_j = 0$  for all  $\theta \in \Theta$ , so that  $\det(\theta_i \eta_j)_{1 \leq i \leq n, 1 \leq j \leq n} = 0$  for all  $\theta_1, \dots, \theta_n \in \Theta$ . By Theorem 1 then  $\eta_1, \dots, \eta_n$  are linearly dependent over  $\mathcal{C}$ .

A consequence of Corollary 1 is that if elements of a differential field are linearly dependent (or independent) over the field of constants of some

CHAPTER II

Differential Fields

In this chapter we develop the elementary theory of differential fields and their extensions. Most (but not all) of the main results of Sections 1-10 were essentially obtained by Ritt in the case of differential fields of functions meromorphic in a region, and were extended to abstract differential fields of characteristic 0 by Ritt and his students (Raudenbush and the author). The generalization to arbitrary characteristic received its main initial impetus from Seidenberg.

Throughout the chapter  $\mathcal{F}$  denotes a differential field. We denote the set of derivation operators of  $\mathcal{F}$  by  $\Delta$ , the set of derivative operators of  $\mathcal{F}$  by  $\Theta$ , the set of elements of  $\Theta$  of order less than or equal to  $s$  by  $\Theta(s)$ , the characteristic of  $\mathcal{F}$  by  $p$ , and the field of constants of  $\mathcal{F}$  by  $\mathcal{C}$ ;  $(y, z, y_0, y_1, \dots, y_n, \dots)$  denotes a family of differential indeterminates.

1 Linear dependence over constants

The following theorem generalizes a well-known classical result on Wronskian determinants.

**Theorem 1** Let

$$\eta_j = (\eta_{j1}, \dots, \eta_{jr}), \quad 1 \leq j \leq n,$$

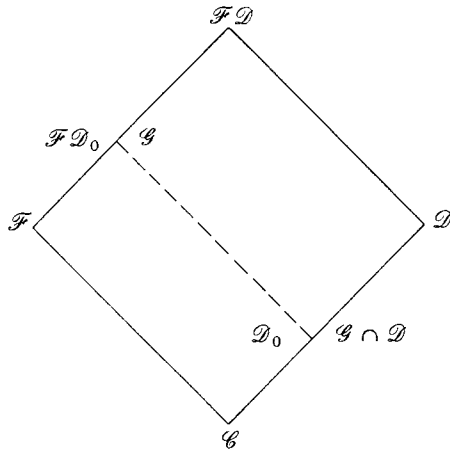
be  $n$  elements of  $\mathcal{F}^r$ . If they are linearly dependent over  $\mathcal{C}$ , then

$$\det(\theta_i \eta_{j, k(i)})_{1 \leq i \leq n, 1 \leq j \leq n} = 0 \tag{1}$$

differential field containing them, then they are linearly dependent (or independent) over the field of constants of any differential field containing them. Therefore we may speak simply of linear dependence (or independence) over constants.

**Corollary 2** Let  $\mathcal{D}$  be the field of constants of an extension of  $\mathcal{F}$ . The mapping that to each field  $\mathcal{D}_0$  between  $\mathcal{C}$  and  $\mathcal{D}$  associates the differential field  $\mathcal{F}\mathcal{D}_0$  between  $\mathcal{F}$  and  $\mathcal{F}\mathcal{D}$ , and the mapping that to each differential field  $\mathcal{G}$  between  $\mathcal{F}$  and  $\mathcal{F}\mathcal{D}$  associates the field  $\mathcal{G} \cap \mathcal{D}$ , are bijective and inverse to each other.

*Proof* We must prove that if  $\mathcal{D}_0$  is given, then  $(\mathcal{F}\mathcal{D}_0) \cap \mathcal{D} = \mathcal{D}_0$ , and that if  $\mathcal{G}$  is given then  $\mathcal{F}(\mathcal{G} \cap \mathcal{D}) = \mathcal{G}$  (see the accompanying diagram).



Now, by Corollary 1,  $\mathcal{F}$  and  $\mathcal{D}$  are linearly disjoint over  $\mathcal{C}$  and therefore, for any given  $\mathcal{D}_0$ ,  $\mathcal{F}\mathcal{D}_0$  and  $\mathcal{D}$  are linearly disjoint over  $\mathcal{D}_0$ , so that  $(\mathcal{F}\mathcal{D}_0) \cap \mathcal{D} = \mathcal{D}_0$ . To establish the second point let  $(\varphi_i)$  be a basis of  $\mathcal{F}$  over  $\mathcal{C}$ . Then  $(\varphi_i)$  is linearly independent over  $\mathcal{D}$ . For any  $\eta \in \mathcal{G}$  we may (since  $\eta \in \mathcal{F}\mathcal{D}$ ) write  $\eta = \sum \varphi_i \kappa_i / \sum \varphi_i \lambda_i$ , where  $\kappa_i, \lambda_i \in \mathcal{D}$  and  $\sum \varphi_i \lambda_i \neq 0$ . It follows that the various elements  $\eta \varphi_i$  and  $\varphi_i$  of  $\mathcal{G}$  are linearly dependent over constants, hence over the field of constants of  $\mathcal{G}$ , that is, over  $\mathcal{G} \cap \mathcal{D}$ . Thus, there exist elements  $\kappa'_i, \lambda'_i \in \mathcal{G} \cap \mathcal{D}$  not all 0 such that  $\sum \eta \varphi_i \lambda'_i - \sum \varphi_i \kappa'_i = 0$ . Because the elements  $\varphi_i$  are linearly independent over constants,  $\sum \varphi_i \lambda'_i \neq 0$  and we may write  $\eta = \sum \varphi_i \kappa'_i / \sum \varphi_i \lambda'_i \in \mathcal{F}(\mathcal{G} \cap \mathcal{D})$ . This shows that  $\mathcal{G} = \mathcal{F}(\mathcal{G} \cap \mathcal{D})$  and completes the proof.

EXERCISE

- Let  $\eta_1, \dots, \eta_n$  be nonzero elements of a differential field with  $m$  derivation operators  $\delta_1, \dots, \delta_m$ , suppose that each of the  $mn$  elements  $\eta_i^{-1} \delta_i \eta_j = k_{ij}$  is a constant, and that the  $n$  vectors  $(k_{1j}, \dots, k_{mj})$  are distinct. Prove that  $\eta_1, \dots, \eta_n$  are linearly independent over constants. (*Hint:* Refer to Chapter I, Section 1, Exercise 2, and show that constants  $c_1, \dots, c_m$  can be fixed so that the  $n$  constants  $k'_j = \sum_i c_i k_{ij}$  are distinct. Set  $\delta' = \sum c_i \delta_i$ , verify that  $\eta_j^{-1} \delta' \eta_j = k'_j$ , and show that  $\det(\delta'^{h-1} \eta_j)_{1 \leq h \leq n, 1 \leq j \leq n} \neq 0$ .)

2 Separable extensions

We recall (Chapter 0, Section 6) that a nonzero algebra  $A$  over a field  $K$  of characteristic  $p$  is separable (in the sense used in this book) if  $A$  has no nonzero nilpotent element and either  $p = 0$  or else  $p \neq 0$  and  $A^p$  and  $K$  are linearly disjoint over  $K^p$ . The following proposition shows that for differential algebras a seemingly weaker condition suffices.

**Proposition 1** Let  $\mathcal{A}$  be a nonzero differential algebra over  $\mathcal{F}$  with no nonzero nilpotent element, let  $p \neq 0$ , and suppose that  $\mathcal{A}^p$  and  $\mathcal{C}$  are linearly disjoint over  $\mathcal{F}^p$ . Then  $\mathcal{A}$  is separable over  $\mathcal{F}$ .

*Proof* By Section 1, Corollary 1 to Theorem 1,  $\mathcal{C}[\mathcal{A}^p]$  and  $\mathcal{F}$  are linearly disjoint over  $\mathcal{C}$ . By hypothesis,  $\mathcal{A}^p$  and  $\mathcal{C}$  are linearly disjoint over  $\mathcal{F}^p$ . Therefore  $\mathcal{A}^p$  and  $\mathcal{F}$  are linearly disjoint over  $\mathcal{F}^p$ .

A separable extension of a differential field need not be separable over an intermediate differential field. The following proposition describes precisely when it is.

**Proposition 2** Let  $\mathcal{H}$  be a separable extension of  $\mathcal{F}$ , let  $\mathcal{G}$  be a differential field with  $\mathcal{F} \subset \mathcal{G} \subset \mathcal{H}$ , and denote the field of constants of  $\mathcal{G}$  by  $\mathcal{D}$ . A necessary and sufficient condition that  $\mathcal{H}$  be separable over  $\mathcal{G}$  is that  $\mathcal{H}^p \mathcal{C}$  and  $\mathcal{D}$  be linearly disjoint over  $\mathcal{G}^p \mathcal{C}$ .

*Proof* We may suppose that  $p \neq 0$ . Then  $\mathcal{H}^p$  and  $\mathcal{C}$  are linearly disjoint over  $\mathcal{F}^p$ , so that  $\mathcal{H}^p$  and  $\mathcal{G}^p \mathcal{C}$  are linearly disjoint over  $\mathcal{G}^p$ . It follows that a necessary and sufficient condition that  $\mathcal{H}^p$  and  $\mathcal{D}$  be linearly disjoint over  $\mathcal{G}^p$  is that  $\mathcal{H}^p \mathcal{C}$  and  $\mathcal{D}$  be linearly disjoint over  $\mathcal{G}^p \mathcal{C}$ .

**Corollary** Let the hypothesis be as in Proposition 2. Each of the following conditions is sufficient for  $\mathcal{H}$  to be separable over  $\mathcal{G}$ .

- (a)  $\mathcal{G}$  is algebraic over  $\mathcal{F}$ .
- (b) The field of constants of  $\mathcal{G}$  is  $\mathcal{G}^p\mathcal{C}$ .
- (c)  $\mathcal{G} = \mathcal{F}\langle\gamma\rangle$ , where  $\gamma$  is a constant and  $\gamma \notin \mathcal{H}^p\mathcal{C}$ .

*Proof* The sufficiency of (a) is well known, not depending on the differential structure<sup>1</sup>; the sufficiency of (b) is an immediate consequence of Proposition 2. Let (c) be satisfied, with  $p \neq 0$ . Since  $\gamma \notin \mathcal{H}^p\mathcal{C}$  and  $\gamma^p \in \mathcal{H}^p\mathcal{C}$  we see that  $\gamma$  is not separably algebraic over  $\mathcal{H}^p\mathcal{C}$ , so that  $(1, \gamma, \dots, \gamma^{p-1})$  is linearly independent over  $\mathcal{H}^p\mathcal{C}$ . By Section 1, Corollary 2 to Theorem 1, the field of constants of  $\mathcal{G} = \mathcal{F}\mathcal{C}(\gamma)$  is  $\mathcal{C}(\gamma)$ , so that  $\mathcal{C}(\gamma) \supset \mathcal{H}^p\mathcal{C} \cap \mathcal{C}(\gamma) \supset \mathcal{G}^p\mathcal{C}$ . As the degrees of  $\mathcal{C}(\gamma)$  over  $\mathcal{H}^p\mathcal{C} \cap \mathcal{C}(\gamma)$  and  $\mathcal{G}^p\mathcal{C}$  are both evidently  $p$  we infer that  $\mathcal{H}^p\mathcal{C} \cap \mathcal{C}(\gamma) = \mathcal{G}^p\mathcal{C}$  and that  $(1, \gamma, \dots, \gamma^{p-1})$  is a basis of  $\mathcal{C}(\gamma)$  over  $\mathcal{G}^p\mathcal{C}$ . Hence  $\mathcal{H}^p\mathcal{C}$  and  $\mathcal{C}(\gamma)$  are linearly disjoint over  $\mathcal{G}^p\mathcal{C}$ , so that (by Proposition 2)  $\mathcal{H}$  is separable over  $\mathcal{G}$ .

If  $L$  is a separable algebraic field extension of a field  $K$ , then every derivation  $D$  of  $K$  can be extended to a unique derivation  $D_L$  of  $L$ .<sup>2</sup> If also  $D'$  is a derivation of  $K$ , then  $DD' - D'D$  is a derivation of  $K$ ,  $D_L D'_L - D'_L D_L$  is a derivation of  $L$  extending  $DD' - D'D$ , so that  $D_L D'_L - D'_L D_L = (DD' - D'D)_L$ . Since the zero derivation of  $K$  extends to the zero derivation of  $L$ , it follows that if  $D$  and  $D'$  commute, then so do  $D_L$  and  $D'_L$ .

**Lemma 1** *A separable algebraic field extension of  $\mathcal{F}$  has a unique structure of differential field extension of  $\mathcal{F}$ .*

*Proof* By the above there is a unique way of defining  $\delta\alpha$  for all elements  $\alpha$  of the field extension  $\mathcal{G}$  and all  $\delta \in \Delta$  so that the mappings  $\alpha \mapsto \delta\alpha$  ( $\alpha \in \mathcal{G}$ ) are derivations of  $\mathcal{G}$  extending the derivations  $\alpha \mapsto \delta\alpha$  ( $\alpha \in \mathcal{F}$ ) of  $\mathcal{F}$ , and these derivations of  $\mathcal{G}$  commute with each other.

**Proposition 3** *Let  $\mathcal{G}$  be a separable algebraic extension of  $\mathcal{F}$ , let  $\mathcal{G}'$  be an extension of a differential field  $\mathcal{F}'$ , and let  $f$  be a field isomorphism of  $\mathcal{G}$  onto  $\mathcal{G}'$  such that the restriction of  $f$  to  $\mathcal{F}$  is a differential field isomorphism of  $\mathcal{F}$  onto  $\mathcal{F}'$ . Then  $f$  is a differential field isomorphism.*

*Proof* For each  $\delta \in \Delta$  the mapping  $\alpha \mapsto f^{-1}(\delta f(\alpha))$  ( $\alpha \in \mathcal{G}$ ) is a derivation of  $\mathcal{G}$  extending the derivation  $\alpha \mapsto \delta\alpha$  ( $\alpha \in \mathcal{F}$ ) of  $\mathcal{F}$ , and so too is the mapping  $\alpha \mapsto \delta\alpha$  ( $\alpha \in \mathcal{G}$ ). These two mappings must coincide, so that  $\delta f(\alpha) = f(\delta\alpha)$  ( $\alpha \in \mathcal{G}$ ) for every  $\delta \in \Delta$ . That is,  $f$  is a differential field isomorphism.

<sup>1</sup> See, e.g., N. Bourbaki, "Algèbre," Chap. V, §8, Prop. 5, p. 130. Hermann, Paris, 1950 or 1959.

<sup>2</sup> See, e.g., N. Bourbaki, *op. cit.*, §9, Prop. 5, p. 139.

Now,  $\mathcal{F}$  has a separable algebraic field extension that is *separably closed*, that is, that has no proper separable algebraic field extension. This separably closed field extension is unique up to a field isomorphism over  $\mathcal{F}$ . By Lemma 1, there is a unique way of making this field extension into a differential field extension of  $\mathcal{F}$ . Thus,  $\mathcal{F}$  has a separably closed separable algebraic extension. We call such an extension a *separable closure* of  $\mathcal{F}$ . By Proposition 3, a separable closure of  $\mathcal{F}$  is unique up to a differential field isomorphism over  $\mathcal{F}$ .

A differential field may well have two extensions that are incompatible in the sense that they cannot both be embedded in a single extension (see Exercise 1 below). The following proposition shows that with separable extensions such incompatibility does not occur.

**Proposition 4** *Let  $(\mathcal{G}_\lambda)_{\lambda \in \Lambda}$  be a family of separable extensions of  $\mathcal{F}$ . There exist a separable extension  $\mathcal{G}$  of  $\mathcal{F}$  and, for each  $\lambda \in \Lambda$ , an  $\mathcal{F}$ -homomorphism  $f_\lambda: \mathcal{G}_\lambda \rightarrow \mathcal{G}$ , such that  $\mathcal{G}$  is the compositum of all the differential fields  $f_\lambda(\mathcal{G}_\lambda)$ .*

*Proof* Let  $\mathcal{F}'$  be a separable closure of  $\mathcal{F}$ , and let  $\mathcal{G}_{\lambda 0}$  be the separable closure of  $\mathcal{F}$  in  $\mathcal{G}_\lambda$ . There exists an  $\mathcal{F}$ -isomorphism of  $\mathcal{G}_{\lambda 0}$  onto an extension  $\mathcal{F}_\lambda$  of  $\mathcal{F}$  in  $\mathcal{F}'$ , and this can be extended to an isomorphism  $g_\lambda: \mathcal{G}_\lambda \approx \mathcal{H}_\lambda$ , where  $\mathcal{H}_\lambda$  is some extension of  $\mathcal{F}_\lambda$ . Now,  $\mathcal{G}_\lambda$  is separable over  $\mathcal{F}$  and therefore is regular over  $\mathcal{G}_{\lambda 0}$ ; hence  $\mathcal{H}_\lambda$  is regular over  $\mathcal{F}_\lambda$ . Let  $(\zeta_{\lambda j})_{j \in J_\lambda}$  be a family of elements such that  $\mathcal{H}_\lambda = \mathcal{F}_\lambda\langle(\zeta_{\lambda j})_{j \in J_\lambda}\rangle$ . Let  $(y_{\lambda j})_{\lambda \in \Lambda, j \in J_\lambda}$  be a family of differential indeterminates over  $\mathcal{F}'$ . For each  $\lambda \in \Lambda$  let  $\mathfrak{p}_\lambda$  be the defining differential ideal of  $(\zeta_{\lambda j})_{j \in J_\lambda}$  in  $\mathcal{F}_\lambda\langle(y_{\lambda j})_{j \in J_\lambda}\rangle$ . Then  $\mathfrak{p}_\lambda$  is a prime differential ideal and is regular over  $\mathcal{F}_\lambda$ , so that (by Chapter 0, Section 12, Proposition 7(d))  $\mathcal{F}'\mathfrak{p}_\lambda$  is a prime ideal of  $\mathcal{F}'\langle(y_{\lambda j})_{\lambda \in \Lambda, j \in J_\lambda}\rangle$ , regular over  $\mathcal{F}'$ , and obviously is differential. By Chapter 0, Section 12, Corollary 2 to Proposition 7, the ideal  $\mathfrak{r}$  of  $\mathcal{F}'\langle(y_{\lambda j})_{\lambda \in \Lambda, j \in J_\lambda}\rangle$  generated by  $\bigcup_{\lambda \in \Lambda} \mathcal{F}'\mathfrak{p}_\lambda$ , which obviously is differential, is prime and regular over  $\mathcal{F}'$ , and has the property that  $\mathfrak{r} \cap \mathcal{F}'\langle(y_{\lambda j})_{j \in J_\lambda}\rangle = \mathcal{F}'\mathfrak{p}_\lambda$ , so that (by Chapter 0, Section 10, Lemma 9)  $\mathfrak{r} \cap \mathcal{F}_\lambda\langle(y_{\lambda j})_{j \in J_\lambda}\rangle = \mathfrak{p}_\lambda$ . Now let  $\eta_{\lambda j}$  denote the image of  $y_{\lambda j}$  under the canonical homomorphism  $\mathcal{F}'\langle(y_{\lambda j})_{\lambda \in \Lambda, j \in J_\lambda}\rangle \rightarrow \mathcal{F}'\langle(y_{\lambda j})_{\lambda \in \Lambda, j \in J_\lambda}\rangle/\mathfrak{r}$ . The differential field  $\mathcal{G}' = \mathcal{F}'\langle(\eta_{\lambda j})_{\lambda \in \Lambda, j \in J_\lambda}\rangle$  is regular over  $\mathcal{F}'$  and therefore separable over  $\mathcal{F}$ . For each  $\lambda$ , the defining differential ideal of  $(\eta_{\lambda j})_{j \in J_\lambda}$  in  $\mathcal{F}_\lambda\langle(y_{\lambda j})_{j \in J_\lambda}\rangle$  is  $\mathfrak{p}_\lambda$ . It follows that there exists an  $\mathcal{F}_\lambda$ -isomorphism  $\mathcal{F}_\lambda\langle(\zeta_{\lambda j})_{j \in J_\lambda}\rangle \approx \mathcal{F}_\lambda\langle(\eta_{\lambda j})_{j \in J_\lambda}\rangle$ , and consequently an  $\mathcal{F}_\lambda$ -homomorphism  $h_\lambda: \mathcal{H}_\lambda \rightarrow \mathcal{G}'$ , where  $\mathcal{G}$  is the compositum in  $\mathcal{G}'$  of all the differential fields  $\mathcal{F}_\lambda\langle(\eta_{\lambda j})_{j \in J_\lambda}\rangle$ . Setting  $f_\lambda = h_\lambda \circ g_\lambda$ , we see that  $\mathcal{G}$  and the  $f_\lambda$  have the required properties.

It is now a simple matter to prove the existence of an extension of  $\mathcal{F}$  into which every finitely generated separable extension of  $\mathcal{F}$  may be embedded.

Because we shall find it useful to have still more inclusive extensions (which we shall introduce in Chapter III) we call such extensions *semiuniversal* (over  $\mathcal{F}$ ). Let  $\Lambda_n = \Lambda_n(\mathcal{F})$  denote the set of all  $\mathcal{F}$ -separable prime differential ideals of the differential polynomial algebra  $\mathcal{F}\{y_1, \dots, y_n\}$  ( $n = 1, 2, \dots$ ). It is apparent that an extension  $\mathcal{S}$  of  $\mathcal{F}$  is semiuniversal if and only if, for each  $n \in \mathbb{N}$  with  $n \neq 0$  and each  $\mathfrak{p} \in \Lambda_n$ , there exist elements  $\eta_1, \dots, \eta_n \in \mathcal{S}$  such that  $\mathfrak{p}$  is the defining differential ideal of  $(\eta_1, \dots, \eta_n)$  in  $\mathcal{F}\{y_1, \dots, y_n\}$ .

**Corollary** Every differential field has a separable semiuniversal extension.

*Proof* By Proposition 4 it suffices to exhibit a family  $(\mathcal{G}_\lambda)_{\lambda \in \Lambda}$  of separable extensions of  $\mathcal{F}$  such that every finitely generated separable extension of  $\mathcal{F}$  is  $\mathcal{F}$ -isomorphic to at least one  $\mathcal{G}_\lambda$ . Let  $\Lambda = \bigcup \Lambda_n$ . For each  $\mathfrak{p} \in \Lambda$  let  $\mathcal{R}_\mathfrak{p}$  denote the differential polynomial algebra  $\mathcal{F}\{y_1, \dots, y_n\}$  of which  $\mathfrak{p}$  is an ideal, and let  $\mathcal{G}_\mathfrak{p} = Q(\mathcal{R}_\mathfrak{p}/\mathfrak{p})$ . For every finitely generated separable extension  $\mathcal{F}\langle \eta_1, \dots, \eta_n \rangle$  of  $\mathcal{F}$  the defining differential ideal of  $(\eta_1, \dots, \eta_n)$  in  $\mathcal{F}\{y_1, \dots, y_n\}$  is an element  $\mathfrak{p} \in \Lambda$ , and  $\mathcal{F}\langle \eta_1, \dots, \eta_n \rangle$  is  $\mathcal{F}$ -isomorphic to  $\mathcal{G}_\mathfrak{p}$ .

EXERCISE

- Let  $\mathcal{F}$  be a differential field of nonzero characteristic  $p$  containing a constant  $c \notin \mathcal{F}^p$ , and let  $\delta \in \Delta$ . Show that for each  $\alpha \in \mathcal{F}$  the ideal  $\mathfrak{p}_\alpha = (y^p - c) + [\delta y - \alpha]$  of  $\mathcal{F}\{y\}$  is a prime differential one, so that  $\mathcal{E}_\alpha = Q(\mathcal{F}\{y\}/\mathfrak{p}_\alpha)$  is an extension of  $\mathcal{F}$ . Show that if  $\alpha, \beta \in \mathcal{F}$  and  $\alpha \neq \beta$ , then  $\mathcal{E}_\alpha$  and  $\mathcal{E}_\beta$  are incompatible extensions of  $\mathcal{F}$ .

3 Differentially perfect and differentially quasi-perfect differential fields

We shall call  $\mathcal{F}$  *differentially perfect* if every extension of  $\mathcal{F}$  is separable. Similarly, we shall call  $\mathcal{F}$  *differentially quasi-perfect* if every extension of  $\mathcal{F}$  is quasi-separable (see Chapter 0, Section 3). The following internal characterizations of these notions show that  $\mathcal{F}$  may be differentially perfect (respectively differentially quasi-perfect) without being perfect (respectively quasi-perfect).

**Proposition 5** (a) A necessary and sufficient condition that  $\mathcal{F}$  be differentially perfect is that either  $p = 0$  or else  $p \neq 0$  and  $\mathcal{C} = \mathcal{F}^p$ .  
 (b) A necessary and sufficient condition that  $\mathcal{F}$  be differentially quasi-perfect is that either  $p = 0$  or else  $p \neq 0$  and  $[\mathcal{C} : \mathcal{F}^p]$  be finite.

*Proof* We may suppose that  $p \neq 0$ .

(a) If  $\mathcal{C} \neq \mathcal{F}^p$ , there exists an element  $\gamma \in \mathcal{C}$  with  $\gamma \notin \mathcal{F}^p$ . In the differential polynomial algebra  $\mathcal{F}\{y\}$ , the ideal  $(y^p - \gamma)$  is a prime differential one, and  $Q(\mathcal{F}\{y\}/(y^p - \gamma))$  is an extension of  $\mathcal{F}$  that is not separable. On the other hand, if  $\mathcal{C} = \mathcal{F}^p$  and  $\mathcal{G}$  is any extension of  $\mathcal{F}$ , then  $\mathcal{G}$  is separable over  $\mathcal{F}$  by Section 2, Proposition 1.

(b) If  $[\mathcal{C} : \mathcal{F}^p]$  is not finite, there exists an infinite sequence  $(\gamma_n)_{n \in \mathbb{N}}$  of elements of  $\mathcal{C}$  such that  $\gamma_n \notin \mathcal{F}^p(\gamma_0, \dots, \gamma_{n-1})$  ( $n \in \mathbb{N}$ ). In the differential polynomial algebra  $\mathcal{F}\{(y_n)_{n \in \mathbb{N}}\}$ , the ideal  $\mathfrak{p} = (y_0^p - \gamma_0, y_1^p - \gamma_1, \dots, y_n^p - \gamma_n, \dots)$ , which clearly is a differential one, is prime (easy consequence of Chapter 0, Section 3, Lemma 2). Thus  $Q(\mathcal{F}\{(y_n)_{n \in \mathbb{N}}\}/\mathfrak{p})$  is an extension of  $\mathcal{F}$  that is not quasi-separable, since the image of  $(y_n)_{n \in \mathbb{N}}$  is separably independent and of infinite algebraic codimension over  $\mathcal{F}$ . On the other hand, if  $[\mathcal{C} : \mathcal{F}^p]$  is finite and  $\mathcal{G}$  is any extension of  $\mathcal{F}$ , then, by Chapter 0, Section 3, Lemma 3 (applied to  $E = \mathcal{C}$ ,  $K = \mathcal{F}$ ,  $L = \mathcal{G}$ ),  $\mathcal{G}$  is quasi-separable over  $\mathcal{F}$ .

4 Separable dependence over constants

Let  $\eta_1, \dots, \eta_n \in \mathcal{F}$ . These elements are algebraically dependent over  $\mathcal{C}$  if and only if the family  $(\eta_1^{j_1} \cdots \eta_n^{j_n})_{j_1 \in \mathbb{N}, \dots, j_n \in \mathbb{N}}$  is linearly dependent over  $\mathcal{C}$ , and this is the case if and only if this family is linearly dependent over the field of constants of any differential field containing  $\eta_1, \dots, \eta_n$ . Thus, we may say simply that  $(\eta_1, \dots, \eta_n)$  is algebraically dependent (or independent) *over constants*.

This notion is of interest only when  $p = 0$ , for when  $p \neq 0$ , then the  $p$ th power of every element is a constant, so that every nonempty family is algebraically dependent over constants. It is, accordingly, more appropriate to consider separable dependence, which when  $p = 0$  is equivalent to algebraic dependence. When  $p \neq 0$  then, since  $\eta_j^p \in \mathcal{C}$ ,  $(\eta_1, \dots, \eta_n)$  is separably dependent over  $\mathcal{C}$  if and only if the family  $(\eta_1^{j_1} \cdots \eta_n^{j_n})_{0 \leq j_1 < p, \dots, 0 \leq j_n < p}$  is linearly dependent over  $\mathcal{C}$ . Therefore we may say simply that  $(\eta_1, \dots, \eta_n)$  is separably dependent (or independent) *over constants*.

**Proposition 6** Let  $(\eta_1, \dots, \eta_n)$  be separably dependent over constants. If  $p = 0$  (respectively if  $p \neq 0$  and  $\Delta^{(p)}$  denotes the set of all operators  $\delta^{(i)}$  ( $\delta \in \Delta$ ,  $i \in \mathbb{N}$ )), then the matrix  $(\delta \eta_j)_{\delta \in \Delta, 1 \leq j \leq n}$  (respectively the matrix  $(\theta \eta_j)_{\theta \in \Delta^{(p)}, 1 \leq j \leq n}$ ) has rank less than  $n$ .

*Proof* If  $f \in \mathcal{C}[X_1, \dots, X_n]$  vanishes at  $(\eta_1, \dots, \eta_n)$ , but not every  $\partial f / \partial X_j$  vanishes there, then

$$\sum_{1 \leq j \leq n} (\partial f / \partial X_j)(\eta_1, \dots, \eta_n) \delta \eta_j = \delta f(\eta_1, \dots, \eta_n) = 0 \quad (\delta \in \Delta)$$

so that the rank of the matrix  $(\delta \eta_j)_{\delta \in \Delta, 1 \leq j \leq n}$  is less than  $n$ . Now, for any

derivation  $D$  of a field of characteristic  $p \neq 0$ ,  $D^p$  is also a derivation of that field. This is an immediate consequence of the formula  $D^p(ab) = \sum_{0 \leq j \leq p} \binom{p}{j} D^{p-j}a \cdot D^j b$  and the fact that  $\binom{p}{j}$  is a multiple of  $p$  whenever  $0 < j < p$ . It follows that when  $p \neq 0$ , then the elements of  $\Delta^{(p)}$  all are derivation operators, and a computation like the one above shows that the rank of the matrix  $(\theta\eta_j)_{\theta \in \Delta^{(p)}, 1 \leq j \leq n}$  is less than  $n$ .

*Corollary* If an element of a differential field is separably algebraic over constants, then the element is a constant.

This is the case  $n = 1$  of the proposition.

EXERCISES

1. Denote the elements of  $\Delta$  by  $\delta_1, \dots, \delta_m$ , let  $z_1, \dots, z_m$  be differential indeterminates, set  $\mathcal{G} = \mathcal{F}\langle z_1, \dots, z_m \rangle$ , and consider the derivation operator  $D = \sum z_i \delta_i$  on  $\mathcal{G}$ .
  - (a) Show that every  $D$ -constant in  $\mathcal{G}$  is a constant.
  - (b) Show that if  $p \neq 0$ , then  $D^p$  is a linear combination over  $\mathcal{F}\{z_1, \dots, z_m\}$  of the  $2m$  derivation operators  $\delta_1, \dots, \delta_m, \delta_1^p, \dots, \delta_m^p$ . (*Hint:* First show that  $D^p = \sum_{1 \leq i_1 + \dots + i_m \leq p} A_{i_1, \dots, i_m} \delta_1^{i_1} \dots \delta_m^{i_m}$  with  $A_{i_1, \dots, i_m} \in \mathcal{F}\{z_1, \dots, z_m\}$ ; observing that  $D^p$  is a derivation operator and letting  $u, v$  be new differential indeterminates, make use of Chapter I, Section 1, Exercise 1 to compare  $(D^p u)v + uD^p v$  with  $D^p(uv)$ , and conclude that  $A_{i_1, \dots, i_m} = 0$  whenever  $1 < i_1 + \dots + i_m \leq p$  and  $i_\mu < p$  ( $1 \leq \mu \leq m$ )).
  - (c) Show that if  $p \neq 0$  and  $r \in \mathbb{N}$  and  $\Delta_r^{(p)}$  denotes the set of all operators  $\delta^{(r)}$  ( $\delta \in \Delta, 0 \leq i \leq r$ ), then  $D^{pr}$  is a linear combination over  $\mathcal{F}\{z_1, \dots, z_m\}$  of the elements of  $\Delta_r^{(p)}$ .
2. Let  $p \neq 0$ , and let  $\Delta_r^{(p)}$  have the same meaning as in Exercise 1(c). Prove the following partial converse of Proposition 6: If  $\eta_1, \dots, \eta_n \in \mathcal{F}$  have the property that  $\det(\theta_i \eta_j)_{1 \leq i \leq n, 1 \leq j \leq n} = 0$  whenever  $\theta_i \in \Delta_{r-1}^{(p)}$  ( $1 \leq i \leq n$ ), then  $(\eta_1, \dots, \eta_n)$  is separably dependent over constants. (*Hint:* With the help of Exercise 1(a) show that  $(\eta_1, \dots, \eta_n)$  is separably dependent over constants if the family  $(\eta_1^{i_1} \dots \eta_n^{i_n})_{(j_1, \dots, j_n) \in P^n}$  is linearly dependent over  $D$ -constants,  $P$  here denoting the set of numbers  $0, 1, \dots, p-1$ . Apply Theorem 1 to show that this is the case if the Wronskian

$$\det(D^{i_1 + i_2 p + \dots + i_n p^{n-1}} \eta_1^{j_1} \dots \eta_n^{j_n})_{(i_1, \dots, i_n) \in P^n, (j_1, \dots, j_n) \in P^n}$$

vanishes. By a succession of elementary transformations show that this Wronskian is the product of  $\det(D^{p^{i-1}} \eta_j)_{1 \leq i \leq n, 1 \leq j \leq n}$  and the determinant of a certain square matrix of  $p^n - n - 1$  rows. Finally, apply Exercise 1(c).

5 Differential polynomial functions

Let  $n$  be a natural number different from 0, and let  $\Sigma$  be a nonempty subset of the Cartesian  $n$ th power of some extension of the differential field  $\mathcal{F}$ . If  $F$  is an element of the differential polynomial algebra  $\mathcal{F}\{y_1, \dots, y_n\}$ , the mapping  $(a_1, \dots, a_n) \mapsto F(a_1, \dots, a_n)$  ( $(a_1, \dots, a_n) \in \Sigma$ ), which we sometimes denote by  $F_\Sigma$ , is called a *differential polynomial function on  $\Sigma$  over  $\mathcal{F}$* , and is said to be the differential polynomial function on  $\Sigma$  induced by  $F$ . This  $F_\Sigma$  is the zero function on  $\Sigma$  precisely when  $F$  vanishes at every element of  $\Sigma$ , that is, when  $F$  is in the intersection  $\alpha_\Sigma$  of the defining differential ideals over  $\mathcal{F}$  of all the elements of  $\Sigma$ ; we say in this case that  $F$  vanishes on  $\Sigma$ .

Obviously,  $\alpha_\Sigma$  is a differential ideal of  $\mathcal{F}\{y_1, \dots, y_n\}$ . Furthermore, two differential polynomials  $F, G \in \mathcal{F}\{y_1, \dots, y_n\}$  induce equal differential polynomial functions  $F_\Sigma, G_\Sigma$  precisely when  $F - G \in \alpha_\Sigma$ . It follows that there is a unique differential ring structure on the set of differential polynomial functions on  $\Sigma$  over  $\mathcal{F}$  such that the mapping  $F \mapsto F_\Sigma$  ( $F \in \mathcal{F}\{y_1, \dots, y_n\}$ ) is a differential ring homomorphism (called "canonical") with kernel  $\alpha_\Sigma$ .  $\mathcal{F}$  is mapped isomorphically, and therefore can be identified with its image. The differential polynomial functions then form a differential algebra over  $\mathcal{F}$ .

Of course, if  $\Sigma$  is suitably chosen, then  $\alpha_\Sigma = (0)$ , that is, 0 is the only differential polynomial in  $\mathcal{F}\{y_1, \dots, y_n\}$  vanishing on  $\Sigma$ ; this certainly will be the case if  $\Sigma$  contains an element  $(t_1, \dots, t_n)$  that is differentially algebraically independent over  $\mathcal{F}$ . Suppose, however, that  $\Sigma$  is the Cartesian  $n$ th power of a nonempty subset  $\Sigma'$  of  $\mathcal{F}$ . We shall say, loosely, that an  $F \in \mathcal{F}\{y_1, \dots, y_n\}$  vanishes on  $\Sigma'$  when  $F$  vanishes on  $\Sigma$ . An easy induction argument shows that the condition that 0 be the only element of  $\mathcal{F}\{y_1, \dots, y_n\}$  vanishing on  $\Sigma'$  is independent of  $n$ . Furthermore, if  $\mathcal{G}$  is an arbitrary extension of  $\mathcal{F}$ , any differential polynomial  $G$  over  $\mathcal{G}$  may be written in the form  $G = \sum G_i \gamma_i$ , where the elements  $\gamma_i$  of  $\mathcal{G}$  are linearly independent over  $\mathcal{F}$  and each  $G_i$  is a differential polynomial over  $\mathcal{F}$ . It follows that if there does not exist a nonzero differential polynomial vanishing on  $\Sigma'$  with coefficients in  $\mathcal{F}$ , then there does not exist one with coefficients in  $\mathcal{G}$ , so that we may say, simply, that 0 is the only differential polynomial vanishing on  $\Sigma'$ .

6 Dependence of derivative operators

More generally, let  $\Omega$  be any subset of the set  $\Theta$  of derivative operators. The condition that 0 be the only element of  $\mathcal{F}\{y_1, \dots, y_n\}$  that vanishes on  $\Sigma'$  and involves only derivatives  $\theta y_j$  with  $\theta \in \Omega$ , is independent of  $n$  and is preserved when  $\mathcal{F}$  is replaced by any extension  $\mathcal{G}$ . We shall say, when this

condition is satisfied, that  $\Omega$  is algebraically independent on  $\Sigma'$ , and in the contrary case that  $\Omega$  is algebraically dependent on  $\Sigma'$ .

Also, we shall call  $\Omega$  linearly dependent on  $\Sigma'$  if there exist elements  $a_\theta \in \mathcal{F}$  ( $\theta \in \Omega$ ), at least one of which is, and at most a finite number of which are, different from 0, such that the differential polynomial  $\sum_{\theta \in \Omega} a_\theta \theta y$  vanishes on  $\Sigma'$ , and shall call  $\Omega$  linearly independent on  $\Sigma'$  otherwise. These notions do not depend on  $\mathcal{F}$ .

We remark that if  $\Omega$  is linearly dependent on  $\Sigma'$ , and if  $\Sigma'$  has the property that the vector space generated by  $\Sigma'$  over  $\mathcal{C}$  is a differential one, then there exist distinct elements  $\theta_1, \dots, \theta_h \in \Omega$  with  $h > 0$  and nonzero constants  $c_1, \dots, c_h \in \mathcal{C}$  such that  $\sum_{1 \leq i \leq h} c_i \theta_i y$  vanishes on  $\Sigma'$ . Indeed, if  $\theta_1, \dots, \theta_h$  form a minimal nonempty subset of  $\Omega$  linearly dependent on  $\Sigma'$ , and  $c_1, \dots, c_h$  are elements of  $\mathcal{F}$ , not all 0, such that  $\sum_{1 \leq i \leq h} c_i \theta_i y$  vanishes on  $\Sigma'$ , then  $c_h \neq 0$  so that we may even suppose that  $c_h = 1$ ; for any  $\delta \in \Delta$  then  $\sum_{1 \leq i \leq h-1} \delta c_i \cdot \theta_i y$  vanishes on  $\Sigma'$ . By the minimality of the set  $\theta_1, \dots, \theta_h$  then  $\delta c_i = 0$  for each  $i$ , so that  $c_1, \dots, c_h$  are constants.

**Theorem 2** Let  $V$  be a subspace of  $\mathcal{F}$  considered as a vector space over  $\mathcal{C}$ , let  $\Phi$  be a finite subset of  $\Theta$ , and suppose that  $\mathcal{F}$  is infinite. Then the following three conditions are equivalent:

- (a)  $\Phi$  is algebraically independent on  $V$ .
- (b)  $\Phi$  is linearly independent on  $V$ .
- (c)  $V$  contains elements  $v_\theta$  ( $\theta \in \Phi$ ) such that  $\det(\theta v_\theta)_{\theta \in \Phi, \theta' \in \Phi} \neq 0$ .

**REMARK** If  $\mathcal{F}$  is finite, then  $\mathcal{F} = \mathcal{C}$ , and it is easy to verify the following statements: When  $\Phi$  contains a derivative operator other than 1, none of the three conditions is satisfied; when  $\Phi = \emptyset$ , all are satisfied; when  $\Phi$  consists of the single derivative operator 1, (a) is not satisfied whereas (b) and (c) are satisfied or not according as  $V \neq 0$  or  $V = 0$ .

*Proof* We may clearly suppose that  $\Phi \neq \emptyset$ . It is obvious that (a) implies (b). Suppose (b) holds. For arbitrary elements  $v_\theta \in V$  and fixed  $\theta_0 \in \Phi$  we may write  $\det(\theta v_\theta) = \sum_{\theta \in \Phi} a_\theta \theta v_{\theta_0}$ , where  $a_\theta$  is plus or minus the minor of  $\theta v_{\theta_0}$  in the matrix  $(\theta v_\theta)_{\theta \in \Phi, \theta' \in \Phi}$ . Arguing by induction on the number of elements of  $\Phi$ , we may suppose the elements  $v_\theta$  ( $\theta \neq \theta_0$ ) chosen so that  $a_{\theta_0} \neq 0$ . Condition (b) implies that we can then choose  $v_{\theta_0}$  so that  $\sum a_\theta \theta v_{\theta_0} \neq 0$ . Thus (b) implies (c). Finally, suppose that (c) holds and let  $G$  be a nonzero differential polynomial in  $\mathcal{F}\{y\}$  involving no derivative  $\theta y$  with  $\theta \notin \Phi$ . Let  $(b_{\theta\theta'})$  denote the inverse of the matrix  $(\theta v_\theta)$ , and define  $z_\theta = \sum_{\theta'} b_{\theta\theta'} \theta' y$ , so that  $\theta y = \sum_{\theta'} \theta v_{\theta'} \cdot z_{\theta'}$ . Because the family  $(\theta y)_{\theta \in \Phi}$  is algebraically independent over  $\mathcal{F}$ , so is  $(z_\theta)_{\theta \in \Phi}$ . There exists a polynomial  $g$  over  $\mathcal{F}$  in a family of indeterminates  $(Z_\theta)_{\theta \in \Phi}$  such that  $G(y) = g((z_\theta)_{\theta \in \Phi})$ . If  $p = 0$ , then  $\mathcal{C} \supset \mathcal{Q}$ , and if  $p \neq 0$ , then  $\mathcal{C} \supset \mathcal{F}^p$ . Thus, regardless of the value of  $p$ ,  $\mathcal{C}$  is

infinite, so that  $\mathcal{C}$  contains elements  $c_\theta$  ( $\theta \in \Phi$ ) such that  $g((c_\theta)_{\theta \in \Phi}) \neq 0$ . Setting  $w = \sum c_\theta v_\theta$  we see that  $w \in V$  and  $G(w) \neq 0$ . Thus (c) implies (a).

Because of Theorem 2 and the Remark following it, a subset  $\Omega$  of  $\Theta$  may, when  $\mathcal{F}$  is infinite or  $\Omega$  does not consist solely of 1, be called independent on  $V$  (or dependent on  $V$ ) without reference to algebraic or to linear independence (or dependence). Thus  $\Theta$  itself is independent on  $V$  precisely when 0 is the only differential polynomial vanishing on  $V$ .

**Theorem 3** Let  $A$  be a subalgebra of  $\mathcal{F}$  considered as an algebra over  $\mathcal{C}$ . A necessary and sufficient condition that  $\Theta$  be independent on  $A$  is that either  $p = 0$  and  $\Delta$  be independent on  $A$ , or  $p \neq 0$  and the set  $\Delta^{(p)}$  of all derivative operators  $\delta^{(i)}$  ( $\delta \in \Delta$ ,  $i \in \mathbb{N}$ ) be independent on  $A$ .

*Proof* The necessity of the condition is obvious. To prove the sufficiency suppose first that  $p = 0$  and  $\Delta$  is independent on  $A$ , and denote the elements of  $\Delta$  by  $\delta_1, \dots, \delta_m$ . By Theorem 2 there exist elements  $u_1, \dots, u_m \in A$  such that the matrix  $(\delta_i u_j)$  has an inverse, which we denote by  $(a_{ij})$ . We define new derivation operators  $\delta'_i$  on  $\mathcal{F}$  by the formulae

$$\delta'_i = \sum_{1 \leq j \leq m} a_{ij} \delta_j \quad (1 \leq i \leq m), \quad (2)$$

so that

$$\delta_i = \sum_{1 \leq j \leq m} \delta_i u_j \cdot \delta'_j \quad (1 \leq i \leq m) \quad (3)$$

and

$$\delta'_i u_j = \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{if } i \neq j. \end{cases} \quad (4)$$

A simple computation shows that

$$\delta'_i \delta'_j = \delta'_j \delta'_i + \sum_{1 \leq k \leq m} e_{ijk} \delta'_k \quad (1 \leq i \leq m, 1 \leq j \leq m), \quad (5)$$

where each  $e_{ijk} \in \mathcal{F}$ . For each  $\theta = \delta_1^{h_1} \dots \delta_m^{h_m} \in \Theta$ , define  $\theta'$  by the formula  $\theta' = \delta_1^{h_1} \dots \delta_m^{h_m}$ . It is apparent from (2), (3), and (5) that  $\mathcal{F}$  contains elements  $a_{\theta\omega}$  ( $\theta \in \Theta$ ,  $\omega \in \Theta$ ) and elements  $b_{\theta\omega}$  ( $\theta \in \Theta$ ,  $\omega \in \Theta$ ) such that for each  $s \in \mathbb{N}$

$$\theta' = \sum_{\omega \in \Theta(s)} a_{\theta\omega} \omega \quad (\theta \in \Theta(s)) \quad (6)$$

and

$$\theta = \sum_{\omega \in \Theta(s)} b_{\theta\omega} \omega' \quad (\theta \in \Theta(s)). \quad (7)$$

The two matrices  $(a_{\theta\omega})_{\theta \in \Theta(s), \omega \in \Theta(s)}$  and  $(b_{\theta\omega})_{\theta \in \Theta(s), \omega \in \Theta(s)}$  are inverse to each other and therefore have nonvanishing determinants. Now, by Section 4, Proposition 6,  $u_1, \dots, u_m$  are algebraically independent over  $\mathcal{C}$ . For each

$\theta = \delta_1^{h_1} \cdots \delta_m^{h_m} \in \Theta$  set  $v_\theta = (1/(h_1! \cdots h_m!))u_1^{h_1} \cdots u_m^{h_m}$ . It follows from (4) that if we also have  $\omega = \delta_1^{k_1} \cdots \delta_m^{k_m}$ , then  $\theta'v_\omega = 0$  whenever  $h_i > k_i$  for some  $i$ , and  $\theta'v_\theta = 1$ . Ordering the set of all operators  $\delta_1^{i_1} \cdots \delta_m^{i_m}$  lexicographically with respect to  $(i_1, \dots, i_m)$ , we therefore have

$$\theta'v_\omega = \begin{cases} 0 & \text{if } \theta > \omega, \\ 1 & \text{if } \theta = \omega, \end{cases} \quad (8)$$

so that  $\det(\theta'v_\omega)_{\theta \in \Theta(s), \omega \in \Theta(s)} = 1$ . Therefore by (7)

$$\begin{aligned} \det(\theta v_\omega)_{\theta \in \Theta(s), \omega \in \Theta(s)} &= \det\left(\sum_{\tau \in \Theta(s)} b_{\theta\tau} \tau'v_\omega\right)_{\theta \in \Theta(s), \omega \in \Theta(s)} \\ &= \det(b_{\theta\omega})_{\theta \in \Theta(s), \omega \in \Theta(s)} \det(\theta'v_\omega)_{\theta \in \Theta(s), \omega \in \Theta(s)} \neq 0. \end{aligned}$$

Since  $s$  is arbitrary, it follows from Theorem 2 that  $\Theta$  is independent on  $A$ .

Suppose now that  $p \neq 0$ , and continue to suppose merely that  $\Delta$  is independent on  $A$ . We can define the elements  $u_i$  ( $1 \leq i \leq m$ ) and  $a_{ij}$  ( $1 \leq i \leq m$ ,  $1 \leq j \leq m$ ) of  $\mathcal{F}$  and derivation operators  $\delta_i'$  ( $1 \leq i \leq m$ ) as before, and therefore introduce the operators  $\theta'$  and elements  $a_{\theta\omega}$  and  $b_{\theta\omega}$  satisfying (2)–(7). However, we can define the elements  $v_\theta = (1/(h_1! \cdots h_m!))u_1^{h_1} \cdots u_m^{h_m} \in \mathcal{F}$  only for the derivative operators  $\theta = \delta_1^{h_1} \cdots \delta_m^{h_m}$  such that  $h_1 < p, \dots, h_m < p$ . For the duration of this proof we denote the set of all such operators  $\theta$  by  $\Lambda$ . Then (8) holds for all  $\theta \in \Lambda$ ,  $\omega \in \Lambda$ ; it follows that  $\det(\theta'v_\omega)_{\theta \in \Lambda, \omega \in \Lambda} \neq 0$ . For each natural number  $s$  let  $\mathfrak{D}_s$  be the vector space over  $\mathcal{F}$  with basis  $\Theta(s)$ . It is clear from (6) and (7) that the family  $(\theta')_{\theta \in \Theta(s)}$  is also a basis of  $\mathfrak{D}_s$ , and that the mapping  $\theta' \mapsto \theta$  ( $\theta \in \Theta(s)$ ) defines an automorphism  $f$  of  $\mathfrak{D}_s$  which, relative to the basis  $(\theta')_{\theta \in \Theta(s)}$ , has the matrix  $(b_{\theta\omega})_{\theta \in \Theta(s), \omega \in \Theta(s)}$ .

Now, if  $s \geq 1$ , then  $f(\mathfrak{D}_{s-1}) = \mathfrak{D}_{s-1}$ . Furthermore,  $\delta_i'^p = (\sum_j a_{ij} \delta_j)^p \equiv \sum_j a_{ij}^p \delta_j^p \pmod{\mathfrak{D}_{p-1}}$  and  $\delta_i'^p = (\sum_j \delta_j u_j \cdot \delta_j')^p \equiv \sum_j (\delta_j u_j)^p \delta_j'^p \pmod{\mathfrak{D}_{p-1}}$ . It easily follows that the subspace  $\mathfrak{E}_s$  of  $\mathfrak{D}_s$ , generated by the elements of  $\mathfrak{D}_{s-1}$  and the operators  $\theta = \delta_1^{h_1} \cdots \delta_m^{h_m} \in \Theta(s)$  for which at least one exponent  $h_i$  is greater than or equal to  $p$ , is also the subspace of  $\mathfrak{D}_s$  generated by the elements of  $\mathfrak{D}_{s-1}$  and the operators  $\theta' = \delta_1^{h_1} \cdots \delta_m^{h_m}$  with  $\theta \in \Theta(s)$  for which at least one  $h_i$  is greater than or equal to  $p$ , and that  $f(\mathfrak{E}_s) = \mathfrak{E}_s$ . (Of course, if  $s < p$ , then  $\mathfrak{E}_s = \mathfrak{D}_{s-1}$ , and if  $s > m(p-1)$ , then  $\mathfrak{E}_s = \mathfrak{D}_s$ .) Therefore  $f$  induces an automorphism of the space  $\mathfrak{D}_s/\mathfrak{E}_s$ . A basis of  $\mathfrak{D}_s/\mathfrak{E}_s$  is the image under the canonical homomorphism  $\mathfrak{D}_s \rightarrow \mathfrak{D}_s/\mathfrak{E}_s$  of the family  $(\theta')_{\theta \in \Lambda(s)}$ , where  $\Lambda(s)$  is the set of elements  $\theta = \delta_1^{h_1} \cdots \delta_m^{h_m}$  of  $\Theta(s)$  with  $h_1 + \cdots + h_m = s$  and each  $h_i < p$ . Relative to this basis, the induced automorphism of  $\mathfrak{D}_s/\mathfrak{E}_s$  has matrix  $(b_{\theta\omega})_{\theta \in \Lambda(s), \omega \in \Lambda(s)}$ , so that the determinant of this matrix is not 0. Also, because  $f(\mathfrak{D}_{s-1}) = \mathfrak{D}_{s-1}$ , we see that  $b_{\theta\omega} = 0$  whenever  $\theta \in \Theta(s-1)$ ,  $\omega \in \Theta(s) - \Theta(s-1)$  and therefore whenever  $\theta \in \Lambda(s_1)$  and  $\omega \in \Lambda(s_2)$  with

$s_1 < s_2$ . Since  $(\Lambda(s))_{0 \leq s \leq m(p-1)}$  is a partition of  $\Lambda$  we conclude that  $\det(b_{\theta\omega})_{\theta \in \Lambda, \omega \in \Lambda} = \prod_{0 \leq s \leq m(p-1)} \det(b_{\theta\omega})_{\theta \in \Lambda(s), \omega \in \Lambda(s)} \neq 0$ .

We have already remarked that  $\det(\theta'v_\omega)_{\theta \in \Lambda, \omega \in \Lambda} \neq 0$ . Also, if  $\theta \notin \Lambda$ , then  $\theta'v_\omega = 0$  ( $\omega \in \Lambda$ ). Therefore

$$\begin{aligned} \det(\theta v_\omega)_{\theta \in \Lambda, \omega \in \Lambda} &= \det\left(\sum_{\tau \in \Lambda} b_{\theta\tau} \tau'v_\omega\right)_{\theta \in \Lambda, \omega \in \Lambda} \\ &= \det(b_{\theta\omega})_{\theta \in \Lambda, \omega \in \Lambda} \det(\theta'v_\omega)_{\theta \in \Lambda, \omega \in \Lambda} \neq 0. \end{aligned}$$

Thus, by Theorem 2, the assumption that  $\Delta$  is independent on  $A$  leads to the conclusion that  $\Lambda$  is independent on  $A$ .

This being the case, for each natural number  $r$ , let  $\Delta_r^{(p)}$  denote the set of all derivative operators  $\delta^p$  with  $\delta \in \Delta$  and  $0 \leq i \leq r$ , and let  $\Lambda_r$  denote the set of all derivative operators of the form  $\prod_{\lambda \in \Delta_r^{(p)}} \lambda^{h_\lambda}$ , where  $h_\lambda < p$  for each  $\lambda$ . It is evident that a derivative operator  $\theta = \delta_1^{k_1} \cdots \delta_m^{k_m}$  belongs to  $\Lambda_r$  if and only if each  $k_i < p^{r+1}$ . However, the elements of  $\Delta_r^{(p)}$  all are derivation operators on  $\mathcal{F}$  (see Section 4, the proof of Proposition 6). Hence we may consider the differential field structure on  $\mathcal{F}$  for which  $\Delta_r^{(p)}$  is the set of derivation operators. If we apply the conclusion we just reached to this differential field, we see that if  $\Delta_r^{(p)}$  is independent on  $A$ , then so is  $\Lambda_r$ . Since  $(\Delta_r^{(p)})_{r \in \mathbb{N}}$  and  $(\Lambda_r)_{r \in \mathbb{N}}$  are increasing sequences with  $\bigcup \Delta_r^{(p)} = \Delta^{(p)}$  and  $\bigcup \Lambda_r = \Theta$ , we conclude that if  $\Delta^{(p)}$  is independent on  $A$ , then so is  $\Theta$ .

**Corollary** Let  $A$  be a subalgebra of  $\mathcal{F}$  (considered as an algebra over  $\mathcal{C}$ ). A necessary and sufficient condition that 0 be the only differential polynomial vanishing on  $A$  is that either  $p = 0$  and there exist elements  $v_\delta \in A$  ( $\delta \in \Delta$ ) such that the “Jacobian”  $\det(\delta v_\delta)_{\delta \in \Delta, \delta' \in \Delta}$  does not vanish, or else  $p \neq 0$  and for each  $r \in \mathbb{N}$  there exist elements  $v_\theta \in A$  ( $\theta \in \Delta_r^{(p)}$ ) such that the “hyper-Jacobian”  $\det(\theta v_{\theta'})_{\theta \in \Delta_r^{(p)}, \theta' \in \Delta_r^{(p)}}$  does not vanish ( $\Delta_r^{(p)}$  denoting the set of all operators  $\delta^p$  with  $\delta \in \Delta$  and  $0 \leq i \leq r$ ).

*Proof* This is immediate from Theorems 3 and 2.

## 7 Differentially separable dependence

We recall (Chapter I, Section 6) that a family  $(\alpha_i)_{i \in I}$  of elements of an extension of  $\mathcal{F}$  is said to be *differentially algebraically dependent* over  $\mathcal{F}$  if the family  $(\theta \alpha_i)_{\theta \in \Theta, i \in I}$  is algebraically dependent over  $\mathcal{F}$ . We shall say that  $(\alpha_i)_{i \in I}$  is *differentially separably dependent* over  $\mathcal{F}$  if  $(\theta \alpha_i)_{\theta \in \Theta, i \in I}$  is separably dependent over  $\mathcal{F}$ , and shall say that  $(\alpha_i)_{i \in I}$  is *differentially separably independent* over  $\mathcal{F}$  in the contrary case. As in the case of differentially algebraic dependence, we call a set  $\Sigma$  *differentially separably dependent* or *independent* over  $\mathcal{F}$  according as the family  $(\alpha_\sigma)_{\sigma \in \Sigma}$  is. In the special case in which  $\Sigma$

consists of a single element  $\alpha$ , we call  $\alpha$  *differentially separable* or *differentially inseparable* over  $\mathcal{F}$  in the respective cases. It is clear that a set  $\Sigma$  is differentially separably dependent over  $\mathcal{F}$  if and only if there exists an  $\alpha \in \Sigma$  such that  $\alpha$  is differentially separable over  $\mathcal{F}\langle\Sigma'\rangle$ ,  $\Sigma'$  denoting the set of elements of  $\Sigma$  other than  $\alpha$ .

If there exists a subset of  $J$  of  $I$  such that  $(\alpha_j)_{j \in J}$  is differentially separably dependent over  $\mathcal{F}$ , then  $(\alpha_i)_{i \in I}$  is, too. Conversely, if  $(\alpha_i)_{i \in I}$  is, then there exists such a  $J$  that is *finite*. If  $\alpha_j \in \mathcal{F}$  for some  $j \in I$ , then  $(\alpha_i)_{i \in I}$  is differentially separably dependent over  $\mathcal{F}$ . A family that is differentially separably dependent over  $\mathcal{F}$  also is differentially separably dependent over any extension of  $\mathcal{F}$ .

By the remark in Chapter 0, Section 2, following the definition of separable dependence, we see that if  $\Delta'$  is a set of derivation operators resulting from transformation of  $\Delta$  by an invertible matrix over  $\mathcal{U}$  (see Chapter I, Section 4), then  $(\alpha_i)_{i \in I}$  is  $\Delta'$ -separably dependent over  $\mathcal{F}$  if and only if it is  $\Delta$ -separably dependent over  $\mathcal{F}$ .

**Proposition 7** Let  $\eta = (\eta_1, \dots, \eta_n)$  be a finite family of elements of an extension of  $\mathcal{F}$ . Let there be given an integrated ranking of the family  $(y_1, \dots, y_n)$  of differential indeterminates. Then the following three conditions are equivalent.

- (a)  $\eta$  is differentially separably dependent over  $\mathcal{F}$ .
- (b) There exists an  $A \in \mathcal{F}\{y_1, \dots, y_n\}$  with  $A \notin \mathcal{F}$  such that  $A(\eta) = 0$  and  $S_A(\eta) \neq 0$ .
- (c) There exists a derivative  $v$  of a  $y_j$  such that  $v(\eta) \in \mathcal{F}((\theta\eta_j)_{\theta \in \Theta, 1 \leq j \leq n, \theta y_j < v})$

**REMARK** The hypothesis that the ranking be integrated is used only in proving the implication (a)  $\Rightarrow$  (b). It is easy to see that if  $p = 0$ , then this hypothesis can be dropped.

*Proof* Let  $\mathfrak{p}$  denote the defining differential ideal of  $\eta$  in  $\mathcal{F}\{y_1, \dots, y_n\}$ . If (b) is false, then the empty set is a characteristic set of  $\mathfrak{p}$  (see Chapter I, Section 10). By Chapter I, Section 10, Lemma 9, then  $\partial P/\partial v \in \mathfrak{p}$  for every  $P \in \mathfrak{p}$  and every derivative  $v$  of any  $y_j$ , so that  $\eta$  is differentially separably independent over  $\mathcal{F}$ . Thus, (a) implies (b). If  $A(\eta) = 0$  and  $S_A(\eta) \neq 0$  as in (b), and if  $\delta \in \Delta$ , then (Chapter I, Section 8, Lemma 5)  $\delta u_A(\eta) \in \mathcal{F}((\theta\eta_j)_{\theta \in \Theta, 1 \leq j \leq n, \theta y_j < \delta u_A})$ . Therefore (b) implies (c). The fact that (c) implies (a) is obvious.

## 8 Differentially separable extensions

Let  $\mathcal{G}$  be an extension of  $\mathcal{F}$ . Then  $\mathcal{G}$  is said to be *differentially algebraic* over  $\mathcal{F}$  if each element of  $\mathcal{G}$  is. Similarly, we shall say that  $\mathcal{G}$  is *differentially separable* over  $\mathcal{F}$  if each element of  $\mathcal{G}$  is.

**Proposition 8** Let  $\alpha$  and  $\beta$  be elements of an extension of  $\mathcal{F}$ .

(a) If  $\beta$  is differentially separable over  $\mathcal{F}\langle\alpha\rangle$  and  $\alpha$  is differentially separable over  $\mathcal{F}$ , then  $\beta$  is differentially separable over  $\mathcal{F}$ .

(b) If  $\beta$  is differentially separable over  $\mathcal{F}\langle\alpha\rangle$ , but  $\alpha$  is not differentially separable over  $\mathcal{F}\langle\beta\rangle$ , then  $\beta$  is differentially separable over  $\mathcal{F}$ .

*Proof* (a) Fix some orderly ranking of a differential indeterminate  $y$ . By Section 7, Proposition 7, there exists a  $\theta_1 \in \Theta$  such that  $\theta_1 \alpha \in \mathcal{F}((\theta\alpha)_{\theta y < \theta_1 y})$ ; clearly  $\theta' \theta_1 \alpha \in \mathcal{F}((\theta\alpha)_{\theta y < \theta' \theta_1 y})$  for every  $\theta' \in \Theta$ . Setting  $r_1 = \text{ord } \theta_1$  we easily conclude that for any  $r \geq r_1$

$$\mathcal{F}((\theta\alpha)_{\theta \in \Theta(r)}) = \mathcal{F}((\theta\alpha)_{\theta \in \Theta(r) - \Theta(r-r_1)\theta_1}). \quad (9)$$

Similarly, there exists a  $\theta_2 \in \Theta$  such that  $\theta_2 \beta \in \mathcal{F}\langle\alpha\rangle((\theta\beta)_{\theta y < \theta_2 y})$ , and therefore  $\theta_2 \beta \in \mathcal{F}((\theta\alpha)_{\theta \in \Theta(q)}, (\theta\beta)_{\theta y < \theta_2 y})$  for some  $q \in \mathbb{N}$ . Then  $\theta' \theta_2 \beta \in \mathcal{F}((\theta\alpha)_{\theta \in \Theta(q + \text{ord } \theta')}, (\theta\beta)_{\theta y < \theta' \theta_2 y})$  for every  $\theta' \in \Theta$ . Setting  $r_2 = \text{ord } \theta_2$  we conclude that for any  $s \geq r_2$

$$\mathcal{F}((\theta\beta)_{\theta \in \Theta(s)}) \subset \mathcal{F}((\theta\alpha)_{\theta \in \Theta(s+q)}, (\theta\beta)_{\theta \in \Theta(s) - \Theta(s-r_2)\theta_2}).$$

In the light of (9) this yields (provided  $s+q > r_1$ ) the relation

$$\mathcal{F}((\theta\beta)_{\theta \in \Theta(s)}) \subset \mathcal{F}((\theta\alpha)_{\theta \in \Theta(s+q) - \Theta(s+q-r_1)\theta_1}, (\theta\beta)_{\theta \in \Theta(s) - \Theta(s-r_2)\theta_2}).$$

The number of generators  $\theta\beta$  on the left here equals

$$\text{Card } \Theta(s) = \binom{s+m}{m} = \frac{1}{m!} s^m + \dots,$$

whereas the number of generators  $\theta\alpha$  and  $\theta\beta$  on the right is equal to

$$\binom{s+q+m}{m} - \binom{s+q-r_1+m}{m} + \binom{s+m}{m} - \binom{s-r_2+m}{m},$$

which can be expressed as a polynomial in  $s$  of degree less than  $m$ . For a large value of  $s$  the number of generators on the left therefore exceeds the number on the right, and then (by Chapter 0, Section 2, Lemma 1)  $(\theta\beta)_{\theta \in \Theta(s)}$  is separably dependent over  $\mathcal{F}$ . Thus,  $\beta$  is differentially separable over  $\mathcal{F}$ .

(b) By Proposition 7 we may write  $\theta_0 \beta = A(\alpha, \beta)/B(\alpha, \beta)$ , where  $\theta_0 \in \Theta$ ,  $A$  and  $B$  are in the differential polynomial algebra  $\mathcal{F}\{y, z\}$ , every derivative of  $z$  present in  $A$  or  $B$  is lower than  $\theta_0 z$  (relative to some orderly ranking), and  $B(\alpha, \beta) \neq 0$ . For any  $\delta \in \Delta$  the differential polynomial

$$\begin{aligned} \delta(B\theta_0 z - A) &= B\delta\theta_0 z + (B\theta_0 z - A)^\delta + \sum_{u \in \Theta_y} \partial(B\theta_0 z - A)/\partial u \cdot \delta u \\ &\quad + \sum_{\substack{v \in \Theta_z \\ v < \theta_0 z}} \partial(B\theta_0 z - A)/\partial v \cdot \delta v \end{aligned}$$

vanishes at  $(\alpha, \beta)$ . Since  $\alpha$  is not differentially separable over  $\mathcal{F}\langle\beta\rangle$ , each



$\partial(B\theta_0 z - A)/\partial u$  here must vanish at  $(\alpha, \beta)$ . Therefore the differential polynomial  $B\partial\theta_0 z - A_\delta$ , with  $A_\delta = -(B\theta_0 z - A)^\delta - \sum_{v \in \Theta, v < \theta_0 z} \partial(B\theta_0 z - A)/\partial v \cdot \delta v$ , also vanishes at  $(\alpha, \beta)$ . It is obvious that every derivative of  $z$  present in  $A_\delta$  is lower than  $\delta\theta_0 z$ , and that every derivative of  $y$  present in  $A_\delta$  is present in  $A$  or  $B$ . By induction we now see that for every  $\theta' \in \Theta$  there exists an  $A_{\theta'} \in \mathcal{F}\{y, z\}$ , not involving derivatives of  $z$  other than those lower than  $\theta'\theta_0 z$  and not involving derivatives of  $y$  other than those present in  $A$  or  $B$ , such that  $\theta'\theta_0 \beta = A_{\theta'}(\alpha, \beta)/B(\alpha, \beta)$ . It follows, for every natural number  $s \geq r_0 = \text{ord } \theta_0$ , that

$$\mathcal{F}((\theta\beta)_{\theta \in \Theta(s)}) \subset \mathcal{F}(\theta_1 \alpha, \dots, \theta_k \alpha, (\theta\beta)_{\theta \in \Theta(s) - \Theta(s-r_0)\theta_0}),$$

where  $\theta_1 y \dots \theta_k y$  denote the derivatives of  $y$  present in  $A$  or  $B$ . However, for sufficiently big values of  $s$ ,  $\text{Card } \Theta(s) > k + \text{Card } \Theta(s) - \text{Card } \Theta(s-r_0)$ . Therefore (by Chapter 0, Section 2, Lemma 1)  $(\theta\beta)_{\theta \in \Theta(s)}$  is separably dependent over  $\mathcal{F}$ , so that  $\beta$  is differentially separable over  $\mathcal{F}$ .

**Corollary** Let  $\mathcal{G}$  be an extension of  $\mathcal{F}$ .

(a) The set  $\mathcal{F}_0$  of all elements of  $\mathcal{G}$  that are differentially separable over  $\mathcal{F}$  is a differential field.

(b) If  $\Sigma$  is a subset of  $\mathcal{G}$  every element of which is differentially separable over  $\mathcal{F}$ , then  $\mathcal{F}\langle \Sigma \rangle$  is differentially separable over  $\mathcal{F}$ .

(c) Let  $\mathcal{H}$  be an extension of  $\mathcal{G}$ . Then  $\mathcal{H}$  is differentially separable over  $\mathcal{F}$  if and only if  $\mathcal{H}$  is differentially separable over  $\mathcal{G}$  and  $\mathcal{G}$  is differentially separable over  $\mathcal{F}$ .

*Proof* (a) Let  $\alpha, \beta \in \mathcal{F}_0$  and let  $\gamma$  denote any one of  $\alpha + \beta, \alpha - \beta, \alpha\beta, \alpha/\beta, \delta\alpha$  ( $\delta \in \Delta$ ). Then  $\gamma$  is differentially separable over  $\mathcal{F}\langle \alpha, \beta \rangle = \mathcal{F}\langle \alpha \rangle \langle \beta \rangle$ ,  $\beta$  is over  $\mathcal{F}\langle \alpha \rangle$ , and  $\alpha$  is over  $\mathcal{F}$ . By double application of Proposition 8(a), then  $\gamma \in \mathcal{F}_0$ .

(b) Since  $\Sigma \subset \mathcal{F}_0$  it follows from part (a) that  $\mathcal{F}\langle \Sigma \rangle \subset \mathcal{F}_0$ .

(c) Suppose  $\mathcal{H}$  is differentially separable over  $\mathcal{G}$  and  $\mathcal{G}$  is over  $\mathcal{F}$ . Let  $\beta \in \mathcal{H}$ . Then there exist finitely many elements  $\alpha_1, \dots, \alpha_n \in \mathcal{G}$  such that  $\beta$  is differentially separable over  $\mathcal{F}\langle \alpha_1, \dots, \alpha_n \rangle$ . By  $n$ -fold application of Proposition 8(a),  $\beta$  is differentially separable over  $\mathcal{F}$ . Therefore  $\mathcal{H}$  is differentially separable over  $\mathcal{F}$ . The proof in the opposite direction is trivial.

The differential field  $\mathcal{F}_0$  described in part (a) of the above corollary will be called the *differentially separable closure of  $\mathcal{F}$  in  $\mathcal{G}$* . In the case  $p = 0$ , where the notions "differentially separable" and "differentially algebraic" coincide,  $\mathcal{F}_0$  will also be called the *differentially algebraic closure of  $\mathcal{F}$  in  $\mathcal{G}$* . If  $\mathcal{F} = \mathcal{F}_0$  we shall say that  $\mathcal{F}$  is *differentially separably closed* (when  $p = 0$ , *differentially algebraically closed*) in  $\mathcal{G}$ .

**Proposition 9** Assume that  $\Theta$  is independent on  $\mathcal{F}$ . Then every finitely generated differentially separable extension of  $\mathcal{F}$  is generated by a single element.

*Proof* It suffices to show that if  $\alpha$  and  $\beta$  are differentially separable over  $\mathcal{F}$ , then there exists an  $e \in \mathcal{F}$  such that  $\mathcal{F}\langle \alpha, \beta \rangle = \mathcal{F}\langle \alpha + e\beta \rangle$ . Let  $t, y, z$  be differential indeterminates over  $\mathcal{F}\langle \alpha, \beta \rangle$  and fix some integrated ranking of  $y$ . By the Corollary to Proposition 8,  $\alpha + t\beta$  is differentially separable over  $\mathcal{F}\langle t \rangle$ . By Section 7, Proposition 7 there exists an  $A \in \mathcal{F}\langle t \rangle\{y\}$  such that  $A(\alpha + t\beta) = 0$  and  $S_4(\alpha + t\beta) \neq 0$ . Clearing denominators and writing  $u_4 = \theta_0 y$  we find a  $B \in \mathcal{F}\{y, z\}$ , not involving a derivative of  $y$  higher than  $\theta_0 y$ , such that

$$B(\alpha + t\beta, t) = 0$$

and  $(\partial B/\partial(\theta_0 y))(\alpha + t\beta, t) \neq 0$ . Now,  $\theta_0(\alpha + t\beta) = \theta_0 t \cdot \beta +$  terms free of  $\theta_0 t$ . Also, for every  $\theta y$  present in  $B$  with  $\theta \neq \theta_0$ ,  $\theta(\alpha + t\beta)$  is free of  $\theta_0 t$ . Computing the partial derivative with respect to  $\theta_0 t$  of both sides of the equation displayed above, we therefore find that

$$\frac{\partial B}{\partial(\theta_0 y)}(\alpha + t\beta, t) \cdot \beta + \frac{\partial B}{\partial(\theta_0 z)}(\alpha + t\beta, t) = 0.$$

Since  $\Theta$  is independent on  $\mathcal{F}$ , there exists an  $e \in \mathcal{F}$  such that

$$\frac{\partial B}{\partial(\theta_0 y)}(\alpha + e\beta, e) \neq 0.$$

Substituting  $e$  for  $t$  in the last equation, we find that  $\beta \in \mathcal{F}\langle \alpha + e\beta \rangle$ , whence  $\mathcal{F}\langle \alpha, \beta \rangle = \mathcal{F}\langle \alpha + e\beta \rangle$ .

## EXERCISES

- (This exercise should be done after Section 9 and the beginning of Section 10) Prove the following converse to Proposition 9: *If every finitely generated differentially separable extension of  $\mathcal{F}$  is generated by a single element, then  $\Theta$  is independent on  $\mathcal{F}$ .* (Hint: Assume  $\Theta$  dependent on  $\mathcal{F}$ . When  $p = 0$  show by the results of Section 6 that for some  $\delta_1 \in \Delta$  there exist constants  $c_\delta$  ( $\delta \in \Delta_1$ ),  $\Delta_1$  denoting the set of elements of  $\Delta$  different from  $\delta_1$ , such that  $\delta_1 a + \sum_{\delta \in \Delta_1} c_\delta \delta a = 0$  for every  $a \in \mathcal{F}$ . Let

$$\mathcal{G} = \mathcal{Q}\left(\mathcal{F}\{y, z\} \left/ \left[ \delta_1 y + \sum_{\delta \in \Delta_1} c_\delta \delta y, \delta_1 z + \sum_{\delta \in \Delta_1} c_\delta \delta z \right] \right.\right)$$

and let  $\eta$ , respectively  $\zeta$ , denote the canonical image of  $y$ , respectively  $z$ ,

in  $\mathcal{G}$ . Show that  $\mathcal{G}$  is a differentially separable extension of  $\mathcal{F}$  with  $\mathcal{G} = \mathcal{F}\langle\eta, \zeta\rangle = \mathcal{F}\langle\eta, \zeta\rangle_{\Delta_1}$  and that the  $\Delta_1$ -transcendence degree of  $\mathcal{G}$  over  $\mathcal{F}$  is 2. Then show that, for any  $\gamma \in \mathcal{G}$ ,  $\mathcal{F}\langle\gamma\rangle = \mathcal{F}\langle\gamma\rangle_{\Delta_1}$ , so that the  $\Delta_1$ -transcendence degree of  $\mathcal{F}\langle\gamma\rangle$  over  $\mathcal{F}$  is less than or equal to 1. When  $p \neq 0$  show how this proof can be suitably modified.)

In the next three exercises let  $\mathcal{V}$  be a differential vector space over  $\mathcal{F}$ , and let  $\mathcal{V}'$ ,  $\mathcal{V}''$  be differential vector subspaces of  $\mathcal{V}$  with  $\mathcal{V}'' \subset \mathcal{V}'$ . Call an element  $\alpha \in \mathcal{V}$  differentially linear over  $\mathcal{V}''$  if there exists a nonzero homogeneous linear  $L \in \mathcal{F}\{y\}$  such that  $L(x) \in \mathcal{V}''$  (the meaning attached to  $L(x)$  being the obvious one). For any set  $\Sigma \subset \mathcal{V}$ , let  $[\Sigma]$  denote the smallest differential vector subspace of  $\mathcal{V}$  that contains  $\Sigma$ .

2. Let  $\alpha, \beta \in \mathcal{V}$ . Prove the following two facts (analog of Proposition 8):
  - (a) If  $\beta$  is differentially linear over  $\mathcal{V}' + [\alpha]$  and  $\alpha$  is differentially linear over  $\mathcal{V}'$ , then  $\beta$  is differentially linear over  $\mathcal{V}'$ .
  - (b) If  $\beta$  is differentially linear over  $\mathcal{V}' + [\alpha]$  but  $\alpha$  is not differentially linear over  $\mathcal{V}' + [\beta]$ , then  $\beta$  is differentially linear over  $\mathcal{V}'$ .
3. Prove the following three facts (analog of the corollary to Proposition 8):
  - (a) The set of elements of  $\mathcal{V}$  that are differentially linear over  $\mathcal{V}'$  is a differential vector subspace of  $\mathcal{V}$  containing  $\mathcal{V}'$ .
  - (b) If every element of a set  $\Sigma \subset \mathcal{V}$  is differentially linear over  $\mathcal{V}'$ , then so is every element of  $\mathcal{V}' + [\Sigma]$ .
  - (c) A necessary and sufficient condition that every element of  $\mathcal{V}$  be differentially linear over  $\mathcal{V}''$  is that every element of  $\mathcal{V}$  be differentially linear over  $\mathcal{V}'$  and every element of  $\mathcal{V}'$  be differentially linear over  $\mathcal{V}''$ .
4. Prove the following analog of Proposition 9: *If every element of a finite set  $\Phi$  is differentially linear over  $\mathcal{V}'$  and  $\Theta$  is independent on  $\mathcal{F}$ , then there exists an element  $\gamma \in \mathcal{V}$  such that  $\mathcal{V}' + [\Phi] = \mathcal{V}' + [\gamma]$ .*

### 9 Differential inseparability bases

**Proposition 10** *Let  $\mathcal{G}$  be an extension of  $\mathcal{F}$  and  $B$  be a subset of  $\mathcal{G}$ . The following three conditions on  $B$  are equivalent.*

- (a)  $B$  is differentially separably independent over  $\mathcal{F}$  and  $\mathcal{G}$  is differentially separable over  $\mathcal{F}\langle B \rangle$ .
- (b)  $B$  is a minimal subset of  $\mathcal{G}$  such that  $\mathcal{G}$  is differentially separable over  $\mathcal{F}\langle B \rangle$ .
- (c)  $B$  is a maximal subset of  $\mathcal{G}$  that is differentially separably independent over  $\mathcal{F}$ .

*Proof* It is obvious that (a) implies (b). Suppose (b) holds. If  $B$  were differentially separably dependent over  $\mathcal{F}$ , there would exist an  $\alpha \in B$  with  $\alpha$  differentially separable over  $\mathcal{F}\langle B' \rangle$ ,  $B'$  denoting the set of elements of  $B$  other than  $\alpha$ . By Section 8, Proposition 8(a), every element of  $\mathcal{G}$  would be differentially separable over  $\mathcal{F}\langle B' \rangle$  contrary to the minimality of  $B$ . Therefore  $B$  is differentially separably independent over  $\mathcal{F}$ . Clearly no bigger subset of  $\mathcal{G}$  is, because every element of  $\mathcal{G}$  is differentially separable over  $\mathcal{F}\langle B \rangle$ . Thus, (b) implies (c). That (c) implies (a) is a special case of the following lemma.

**Lemma 2** *Let  $T$  be a subset of an extension of  $\mathcal{F}$ . If  $B$  is a maximal subset of  $T$  that is differentially separably independent over  $\mathcal{F}$ , then every element of  $T$  is differentially separable over  $\mathcal{F}\langle B \rangle$ .*

*Proof* Assume the lemma false. Then there exists an  $\alpha \in T$  differentially inseparable over  $\mathcal{F}\langle B \rangle$ ; of course  $\alpha \notin B$ . By the maximality of  $B$  the set consisting of  $\alpha$  and the elements of  $B$  is differentially separably dependent over  $\mathcal{F}$ , so that this set contains an element  $\beta$  differentially separable over the extension of  $\mathcal{F}$  generated by the other elements of this set, and obviously  $\beta \in B$ . Denoting by  $B'$  the set of elements of  $B$  other than  $\beta$ , we see that  $\beta$  is differentially separable over  $\mathcal{F}\langle B' \rangle\langle \alpha \rangle$  but not over  $\mathcal{F}\langle B' \rangle$ , so that by Section 8, Proposition 8(b),  $\alpha$  is differentially separable over  $\mathcal{F}\langle B' \rangle\langle \beta \rangle = \mathcal{F}\langle B \rangle$ . This contradiction proves the lemma and completes the proof of Proposition 10.

We shall call a set  $B$  satisfying the equivalent conditions in Proposition 10 a *differential inseparability basis* of  $\mathcal{G}$  over  $\mathcal{F}$ .

**Theorem 4** *Let  $\mathcal{G}$  be an extension of  $\mathcal{F}$ .*

(a) *If  $\Sigma \subset T \subset \mathcal{G}$ , and  $\Sigma$  is differentially separably independent over  $\mathcal{F}$ , and  $\mathcal{G}$  is differentially separable over  $\mathcal{F}\langle T \rangle$ , then there exists a differential inseparability basis  $B$  of  $\mathcal{G}$  over  $\mathcal{F}$  with  $\Sigma \subset B \subset T$ .*

(b) *There exists a differential inseparability basis of  $\mathcal{G}$  over  $\mathcal{F}$ .*

(c) *All differential inseparability bases of  $\mathcal{G}$  over  $\mathcal{F}$  have the same cardinal number.*

(d) *Let  $\mathcal{H}$  be an extension of  $\mathcal{G}$ . If  $B$  is a differential inseparability basis of  $\mathcal{G}$  over  $\mathcal{F}$  and  $\Gamma$  is a differential inseparability basis of  $\mathcal{H}$  over  $\mathcal{G}$ , then  $B \cap \Gamma$  is empty and  $B \cup \Gamma$  is a differential inseparability basis of  $\mathcal{H}$  over  $\mathcal{F}$ .*

*Proof* (a) Using Zorn's lemma we see that among all subsets of  $T$  that contain  $\Sigma$  and are differentially separably independent over  $\mathcal{F}$  there is a maximal one. If  $B$  is such a maximal one, then, by Lemma 2, every element

of  $T$  is differentially separable over  $\mathcal{F}\langle B \rangle$  so that, by Section 8, the Corollary to Proposition 8,  $\mathcal{G}$  is differentially separable over  $\mathcal{F}\langle B \rangle$ . Thus  $B$  is a differential inseparability basis of  $\mathcal{G}$  over  $\mathcal{F}$ .

(b) In part (a) take  $\Sigma = \emptyset$  and  $T = \mathcal{G}$ .

(c) Let  $B$  be a differential inseparability basis of  $\mathcal{G}$  over  $\mathcal{F}$  of minimal cardinal number  $n$ . It suffices to prove that if  $B_1$  is any differential inseparability basis of  $\mathcal{G}$  over  $\mathcal{F}$ , then  $\text{Card } B_1 \leq n$ . If  $n = 0$ , then  $\mathcal{G}$  is differentially separable over  $\mathcal{F}$  and obviously  $B_1$  has cardinal number 0. Let  $n$  be a finite number greater than 0, and suppose that for any extension having a differential inseparability basis of fewer than  $n$  elements all differential inseparability bases are equipotent. Since  $n > 0$ ,  $\mathcal{G}$  is not differentially separable over  $\mathcal{F}$ , so that  $B_1 \neq \emptyset$ . Let  $\alpha \in B_1$  and let  $B_1'$  be the set of elements of  $B_1$  other than  $\alpha$ . By part (a) there exists a set  $B' \subset B$  such that  $\alpha \notin B'$  and the set consisting of  $\alpha$  and the elements of  $B'$  is a differential inseparability basis of  $\mathcal{G}$  over  $\mathcal{F}$ . Since  $\alpha$  is differentially separable over  $\mathcal{F}\langle B \rangle$ ,  $B' \neq B$ , so that  $B'$  contains less than or equal to  $n-1$  elements. Obviously  $B'$  is a differential inseparability basis of  $\mathcal{G}$  over  $\mathcal{F}\langle \alpha \rangle$ , as is  $B_1'$ . By the inductive hypothesis  $B_1'$  and  $B'$  have the same cardinal number, so that the cardinal number of  $B_1$  is less than or equal to  $1 + (n-1) = n$ . Finally, let  $n$  be an infinite cardinal number. For each  $\beta \in B$  there exists a finite set  $\Phi_\beta \subset B_1$  such that  $\beta$  is differentially separable over  $\mathcal{F}\langle \Phi_\beta \rangle$ . Then every element of  $B$  is differentially separable over  $\mathcal{F}\langle \bigcup_{\beta \in B} \Phi_\beta \rangle$  so that, by Section 8, the Corollary to Proposition 8,  $\mathcal{G}$  is, too. Since  $B_1$  satisfies condition (b) in Proposition 10, it follows that  $B_1 = \bigcup_{\beta \in B} \Phi_\beta$ . Therefore

$$\text{Card } B_1 \leq \sum_{\beta \in B} \text{Card } \Phi_\beta \leq \sum_{\beta \in B} \aleph_0 = n \aleph_0 = n.$$

(d) No element of  $\Gamma$  is differentially separable over  $\mathcal{G}$ , so that no element of  $\Gamma$  belongs to  $\mathcal{G}$ , whence  $B \cap \Gamma$  is empty. Every element of  $\mathcal{G}$  is differentially separable over  $\mathcal{F}\langle B \rangle$  and therefore over  $\mathcal{F}\langle B \cup \Gamma \rangle$ , and  $\mathcal{H} \supset \mathcal{G}\langle \Gamma \rangle = \mathcal{F}\langle B \cup \Gamma \rangle \langle \mathcal{G} \rangle \supset \mathcal{F}\langle B \cup \Gamma \rangle$ . Therefore (by Section 8, Proposition 8)  $\mathcal{H}$  is differentially separable over  $\mathcal{F}\langle B \cup \Gamma \rangle$ . To complete the proof it suffices to show that  $B \cup \Gamma$  is differentially separably independent over  $\mathcal{F}$ , that is, that no element of  $B \cup \Gamma$  is differentially separable over the extension of  $\mathcal{F}$  generated by the other elements of  $B \cup \Gamma$ . No element of  $\Gamma$  can have this property because  $\Gamma$  is differentially separably independent over  $\mathcal{G}$  and therefore over  $\mathcal{F}\langle B \rangle$ . If some  $\beta \in B$  had this property, then there would exist a minimal set of distinct elements  $\gamma_1, \dots, \gamma_s$  of  $\Gamma$  such that  $\beta$  is differentially separable over  $\mathcal{F}\langle B', \gamma_1, \dots, \gamma_s \rangle$ ,  $B'$  denoting the set of elements of  $B$  other than  $\beta$ . Because  $B$  is differentially separably independent over  $\mathcal{F}$ ,  $s$  could not be 0, and  $\beta$  would not be differentially separable over  $\mathcal{F}\langle B', \gamma_1, \dots, \gamma_{s-1} \rangle$ . By Section 8, Proposition 8(b),  $\gamma_s$  would be differentially separable over

$\mathcal{F}\langle B', \gamma_1, \dots, \gamma_{s-1} \rangle \langle \beta \rangle = \mathcal{F}\langle B, \gamma_1, \dots, \gamma_{s-1} \rangle$ , which by the above is impossible.

In virtue of Theorem 4 (b) and (c), we may define the *differential inseparability degree* of  $\mathcal{G}$  over  $\mathcal{F}$  as the cardinal number of an inseparability basis of  $\mathcal{G}$  over  $\mathcal{F}$ .

**Corollary 1** Let  $\mathcal{G}$  be an extension of  $\mathcal{F}$  of differential inseparability degree  $n$ , and let  $\Sigma$  be a subset of  $\mathcal{G}$  of cardinal number  $s$ . If  $\mathcal{G}$  is differentially separable over  $\mathcal{F}\langle \Sigma \rangle$ , then  $s \geq n$ . If  $\Sigma$  is differentially separably independent over  $\mathcal{F}$ , then  $s \leq n$ .

*Proof* This follows from part (a) of the theorem.

**Corollary 2** Let  $\mathcal{G}$  be an extension of  $\mathcal{F}$  and  $\mathcal{H}$  be an extension of  $\mathcal{G}$ , and let the differential inseparability degrees of  $\mathcal{G}$  over  $\mathcal{F}$ ,  $\mathcal{H}$  over  $\mathcal{G}$ , and  $\mathcal{H}$  over  $\mathcal{F}$  be  $n$ ,  $r$ , and  $s$ , respectively. Then  $s = n + r$ .

*Proof* This follows from part (d) of the theorem.

**Corollary 3** Let  $\mathcal{G}$  be a differentially separable extension of  $\mathcal{F}$ , and let  $\Sigma$  be a subset of an extension of  $\mathcal{G}$ . If  $\Sigma$  is differentially separably dependent over  $\mathcal{G}$ , then  $\Sigma$  also is over  $\mathcal{F}$ .

*Proof* By part (a) of the theorem some subset  $\Sigma'$  of  $\Sigma$  is a differential inseparability basis of  $\mathcal{G}\langle \Sigma \rangle$  over  $\mathcal{G}$ , and obviously  $\Sigma' \neq \Sigma$ . Also, the empty set is a differential inseparability basis of  $\mathcal{G}$  over  $\mathcal{F}$ . By part (d) of the theorem, then  $\Sigma'$  is a differential inseparability basis of  $\mathcal{G}\langle \Sigma \rangle$  over  $\mathcal{F}$ , so that  $\Sigma$ , being strictly bigger than  $\Sigma'$ , is differentially separably dependent over  $\mathcal{F}$ .

**Corollary 4** Let  $\mathcal{G}$  be a differentially separable extension of  $\mathcal{F}$  and let  $\Sigma$  be a subset of an extension  $\mathcal{H}$  of  $\mathcal{G}$  with  $\Sigma$  differentially separably independent over  $\mathcal{F}$ . Then  $\mathcal{H}^p \mathcal{G}$  and  $\mathcal{H}^p \mathcal{F}\langle \Sigma \rangle$  are linearly disjoint over  $\mathcal{H}^p \mathcal{F}$ .

**REMARK** If  $p = 0$ , this means that  $\mathcal{G}$  and  $\mathcal{F}\langle \Sigma \rangle$  are linearly disjoint over  $\mathcal{F}$ .

*Proof* Let  $q$  denote  $\infty$  or  $p$  according as  $p = 0$  or  $p \neq 0$ . Each element of  $\mathcal{H}^p$  is a constant and therefore is differentially separable over  $\mathcal{F}$ . It follows from Corollary 3 that  $\Sigma$  is differentially separably independent over  $\mathcal{H}^p \mathcal{F}$  and also over  $\mathcal{H}^p \mathcal{G}$ . Therefore the set of all elements of the form  $\prod_{w \in \Theta \Sigma} w^{e(w)}$ , where each  $e(w)$  is a natural number less than  $q$  and  $e(w) \neq 0$  for only finitely many elements  $w \in \Theta \Sigma$ , is a basis of  $\mathcal{H}^p \mathcal{F}\langle \Sigma \rangle$  over  $\mathcal{H}^p \mathcal{F}$  and also of  $\mathcal{H}^p \mathcal{G}\langle \Sigma \rangle$  over  $\mathcal{H}^p \mathcal{G}$ . Therefore  $\mathcal{H}^p \mathcal{G}$  and  $\mathcal{H}^p \mathcal{F}\langle \Sigma \rangle$  are linearly disjoint over  $\mathcal{H}^p \mathcal{F}$ , and the desired result follows.

**Corollary 5** Let  $\Sigma$ , a subset of an extension of  $\mathcal{F}$ , be differentially separably independent over  $\mathcal{F}$ . Then the field of constants of  $\mathcal{F}\langle\Sigma\rangle$  is  $\mathcal{F}\langle\Sigma\rangle^p\mathcal{C}$ .

*Proof* Let  $\mathcal{D}$  denote the field of constants of  $\mathcal{F}\langle\Sigma\rangle$ . By Corollary 4 (with  $\mathcal{G} = \mathcal{D}\mathcal{F}$  and  $\mathcal{H} = \mathcal{F}\langle\Sigma\rangle$ ) we find that  $\mathcal{F}\langle\Sigma\rangle^p\mathcal{D}\mathcal{F} (= \mathcal{D}\mathcal{F})$  and  $\mathcal{F}\langle\Sigma\rangle^p\mathcal{F}\langle\Sigma\rangle (= \mathcal{F}\langle\Sigma\rangle)$  are linearly disjoint over  $\mathcal{F}\langle\Sigma\rangle^p\mathcal{F}$ , and therefore  $\mathcal{D}\mathcal{F} \cap \mathcal{F}\langle\Sigma\rangle = \mathcal{F}\langle\Sigma\rangle^p\mathcal{D}$ . Since  $\mathcal{D}\mathcal{F} \subset \mathcal{F}\langle\Sigma\rangle$  this means that  $\mathcal{D}\mathcal{F} = \mathcal{F}\langle\Sigma\rangle^p\mathcal{F}$ , so that  $\mathcal{D}\mathcal{F} = \mathcal{F}\langle\Sigma\rangle^p\mathcal{C}\mathcal{F}$ . By Section 1, Corollary 2 to Theorem 1, this implies that  $\mathcal{D} = \mathcal{F}\langle\Sigma\rangle^p\mathcal{C}$ .

### EXERCISES

Let  $\mathcal{V}$  be a differential vector space over  $\mathcal{F}$ , and use the terminology and notation of Exercises 2–4 of Section 8. Call any set  $\Sigma \subset \mathcal{V}$  *differentially linearly independent* if the family  $(\theta x)_{\theta \in \Theta, x \in \Sigma}$  is linearly independent, that is, if  $\Sigma$  is not differentially linear over  $[0]$ .

1. Prove that the following conditions on a set  $B \subset \mathcal{V}$  are equivalent:
  - (a)  $B$  is differentially linearly independent and every element of  $\mathcal{V}$  is differentially linear over  $[B]$ .
  - (b)  $B$  is a minimal subset of  $\mathcal{V}$  such that every element of  $\mathcal{V}$  is differentially linear over  $[B]$ .
  - (c)  $B$  is a maximal subset of  $\mathcal{V}$  that is differentially linearly independent.

Call any set  $B$  having these properties a *differential basis* of  $\mathcal{V}$ .

2. Prove the following facts:
  - (a) If  $\Sigma \subset T \subset \mathcal{V}$ ,  $\Sigma$  is differentially linearly independent, and every element of  $\mathcal{V}$  is differentially linear over  $[T]$ , then there exists a differential basis  $B$  of  $\mathcal{V}$  with  $\Sigma \subset B \subset T$ .
  - (b) There exists a differential basis of  $\mathcal{V}$ .
  - (c) All differential bases of  $\mathcal{V}$  have the same cardinal number (called the *differential dimension* of  $\mathcal{V}$ ).
3. Let  $\mathcal{W}$  be a differential vector subspace of  $\mathcal{V}$  and let  $d$  respectively  $e$  respectively  $d'$  denote the differential dimension of  $\mathcal{V}$  respectively  $\mathcal{W}$  respectively  $\mathcal{V}/\mathcal{W}$ . Prove that  $d = e + d'$ .

### 10 Differential transcendence bases

Let  $\mathcal{G}$  be an extension of  $\mathcal{F}$ . A differential inseparability basis of  $\mathcal{G}$  over  $\mathcal{F}$  that is differentially algebraically independent over  $\mathcal{F}$  will be called a *differential transcendence basis* of  $\mathcal{G}$  over  $\mathcal{F}$ . A differential transcendence

basis  $B$  of  $\mathcal{G}$  over  $\mathcal{F}$  will be called *separating* if  $\mathcal{G}$  is separable over  $\mathcal{F}\langle B \rangle$ . If there exists a differential transcendence basis of  $\mathcal{G}$  over  $\mathcal{F}$ , the differential inseparability degree of  $\mathcal{G}$  over  $\mathcal{F}$  will be called, also, the *differential transcendence degree* of  $\mathcal{G}$  over  $\mathcal{F}$ .

**Proposition 11** If  $\mathcal{G}$  is a quasi-separable extension of  $\mathcal{F}$ , then there exists a differential transcendence basis of  $\mathcal{G}$  over  $\mathcal{F}$ .

*Proof* Let  $B$  be a differential inseparability basis of  $\mathcal{G}$  over  $\mathcal{F}$ . The family  $(\theta\beta)_{\theta \in \Theta, \beta \in B}$  is then separably independent over  $\mathcal{F}$ , and therefore has finite algebraic codimension over  $\mathcal{F}$ . Thus there exists a finite set of elements  $(\theta_1, \beta_1), \dots, (\theta_r, \beta_r)$  of  $\Theta \times B$  such that the family  $(\theta\beta)_{\theta \in \Theta, \beta \in B, (\theta, \beta) \neq (\theta_i, \beta_i) (1 \leq i \leq r)}$  is algebraically independent over  $\mathcal{F}$ . Fixing  $\theta' \in \Theta$  with  $\text{ord } \theta' > \text{ord } \theta_i$  ( $1 \leq i \leq r$ ) and letting  $B'$  denote the set of all derivatives  $\theta'\beta$  with  $\beta \in B$ , we see that  $B'$  is a differential transcendence basis of  $\mathcal{G}$  over  $\mathcal{F}$ .

**Theorem 5** Let  $\mathcal{G}$  be an extension of  $\mathcal{F}$ . If there exists a separating differential transcendence basis of  $\mathcal{G}$  over  $\mathcal{F}$ , then  $\mathcal{G}$  is separable over  $\mathcal{F}$ . Conversely, if  $\mathcal{G}$  is separable over  $\mathcal{F}$ , then every differential inseparability basis of  $\mathcal{G}$  over  $\mathcal{F}$  is a separating differential transcendence basis of  $\mathcal{G}$  over  $\mathcal{F}$ .

*Proof* We may suppose that  $p \neq 0$ . The first assertion is obvious since a separable extension of a separable extension of  $\mathcal{F}$  is a separable extension of  $\mathcal{F}$ . Let  $\mathcal{G}$  be separable over  $\mathcal{F}$  and let  $B$  be a differential inseparability basis of  $\mathcal{G}$  over  $\mathcal{F}$ . The family  $(\theta\beta)_{\theta \in \Theta, \beta \in B}$  is separably independent over  $\mathcal{F}$  and therefore algebraically independent over  $\mathcal{F}$ , so that  $B$  is a differential transcendence basis. By Section 9, Corollary 5 to Theorem 4 the field of constants of  $\mathcal{F}\langle B \rangle$  is  $\mathcal{F}\langle B \rangle^p\mathcal{C}$ . By Section 2, the Corollary to Proposition 2, then  $\mathcal{G}$  is separable over  $\mathcal{F}\langle B \rangle$ .

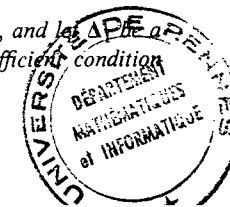
### EXERCISE

1. Prove that every finitely generated separable extension of  $\mathcal{F}$  of differential transcendence degree  $n > 0$  is generated by a set of  $n+1$  elements. (*Hint*: Use Theorem 5 and Proposition 9.)

### 11 Finitely generated extensions

The following two propositions sometimes make it possible to carry out proofs by induction on  $\text{Card } \Delta$ .

**Proposition 12** Let  $\mathcal{G}$  be a finitely generated extension of  $\mathcal{F}$ , and let  $\Delta$  be a subset of  $\Delta$  with  $\text{Card } \Delta = 1 + \text{Card } \Delta_1$ . A necessary and sufficient condition



that  $\mathcal{G}$  be  $\Delta$ -separable over  $\mathcal{F}$  is that  $\mathcal{G}$  have finite  $\Delta_1$ -inseparability degree over  $\mathcal{F}$ .

REMARK When  $\text{Card } \Delta = 1$  this is to mean that  $\mathcal{G}$  has finite inseparability degree over  $\mathcal{F}$  in the sense of Chapter 0, Section 2.

*Proof* By hypothesis we may write  $\mathcal{G} = \mathcal{F}\langle \alpha_1, \dots, \alpha_n \rangle_{\Delta}$ . Suppose the condition satisfied. Then there exist elements  $\beta_1, \dots, \beta_r \in \mathcal{G}$  such that  $\mathcal{G}$  is  $\Delta_1$ -separable over  $\mathcal{F}\langle \beta_1, \dots, \beta_r \rangle_{\Delta_1}$  (when  $\text{Card } \Delta = 1$  this means that  $\mathcal{G}$  is separably algebraic over  $\mathcal{F}\langle \beta_1, \dots, \beta_r \rangle$ ). Denoting by  $\delta$  the element of  $\Delta$  not in  $\Delta_1$ , we see that for some big  $h \in \mathbb{N}$  we have  $\beta_k \in \mathcal{F}\langle (\delta^i \alpha_j)_{0 \leq i < h, 1 \leq j \leq n} \rangle_{\Delta_1}$  ( $1 \leq k \leq r$ ). For any element  $\gamma \in \mathcal{G}$  each of the  $hn+1$  elements  $\gamma, \delta\gamma, \dots, \delta^{hn}\gamma$  is  $\Delta_1$ -separable over  $\mathcal{F}\langle (\delta^i \alpha_j)_{0 \leq i < h, 1 \leq j \leq n} \rangle_{\Delta_1}$ . By Section 9, Corollary 1 to Theorem 4, when  $\text{Card } \Delta > 1$ , and by Chapter 0, Section 2, Lemma 1, when  $\text{Card } \Delta = 1$ , we infer that  $\gamma, \delta\gamma, \dots, \delta^{hn}\gamma$  are  $\Delta_1$ -separably dependent over  $\mathcal{F}$ . It follows that each  $\gamma \in \mathcal{G}$  is  $\Delta$ -separable over  $\mathcal{F}$ , so that  $\mathcal{G}$  is  $\Delta$ -separable over  $\mathcal{F}$ .

Conversely, suppose that  $\mathcal{G}$  is  $\Delta$ -separable over  $\mathcal{F}$ . Letting  $\Theta_1$  denote the set of all elements of  $\Theta$  that are products of elements of  $\Delta_1$ , we see that every  $\theta \in \Theta$  has a unique expression of the form  $\theta = \delta^k \theta_1$  with  $k \in \mathbb{N}$  and  $\theta_1 \in \Theta_1$ . Fixing a ranking of  $y$  as a  $\Delta_1$ -indeterminate, and then ordering the set of all derivatives  $\delta^k \theta_1 y$  lexicographically with respect to  $(k, \theta_1 y)$ , we obtain a ranking of  $y$  as a  $\Delta$ -indeterminate. This ranking obviously is integrated. Hence by Section 7, Proposition 7, for any  $\alpha = \alpha_j$  there exists a  $\delta^k \theta_1 \in \Theta$  with

$$\delta^k \theta_1 \alpha \in \mathcal{F}\langle (\delta^k \theta_1 \alpha)_{(k', \theta_1' y) < (k, \theta_1 y)} \rangle,$$

that is, with

$$\theta_1 \delta^k \alpha \in \mathcal{F}\langle \alpha, \delta \alpha, \dots, \delta^{k-1} \alpha \rangle_{\Delta_1} \langle (\theta_1' \delta^k \alpha)_{\theta_1' y < \theta_1 y} \rangle. \quad (10)$$

It follows that for every  $l \geq k$

$$\theta_1 \delta^l \alpha \in \mathcal{F}\langle \alpha, \delta \alpha, \dots, \delta^{l-1} \alpha \rangle_{\Delta_1} \langle (\theta_1' \delta^l \alpha)_{\theta_1' y < \theta_1 y} \rangle.$$

Therefore for every  $l \geq k$ ,  $\delta^l \alpha$  is  $\Delta_1$ -separable over  $\mathcal{F}\langle \alpha, \delta \alpha, \dots, \delta^{l-1} \alpha \rangle_{\Delta_1}$ , hence is  $\Delta_1$ -separable over  $\mathcal{F}\langle \alpha, \delta \alpha, \dots, \delta^{k-1} \alpha \rangle_{\Delta_1}$ . Thus,  $\mathcal{F}\langle \alpha \rangle_{\Delta}$  is  $\Delta_1$ -separable over  $\mathcal{F}\langle \alpha, \delta \alpha, \dots, \delta^{k-1} \alpha \rangle_{\Delta_1}$ . Choosing  $k$  big enough for this to be the case for each  $\alpha = \alpha_j$ , we see that  $\mathcal{G} = \mathcal{F}\langle \alpha_1, \dots, \alpha_n \rangle_{\Delta}$  is  $\Delta_1$ -separable over  $\mathcal{F}\langle (\delta^i \alpha_j)_{0 \leq i < k, 1 \leq j \leq n} \rangle_{\Delta_1}$ . Hence  $\mathcal{G}$  has finite  $\Delta_1$ -inseparability degree over  $\mathcal{F}$ . ■

We observe that if, in the above proof of the necessity, we had found, instead of relation (10), the stronger relation

$$\delta^k \alpha \in \mathcal{F}\langle \alpha, \delta \alpha, \dots, \delta^{k-1} \alpha \rangle_{\Delta_1}, \quad (11)$$

then we could have concluded the stronger result that

$$\mathcal{G} = \mathcal{F}\langle (\delta^i \alpha)_{0 \leq i < k, 1 \leq j \leq n} \rangle_{\Delta_1},$$

that is, that  $\mathcal{G}$  is a finitely generated  $\Delta_1$ -field extension of  $\mathcal{F}$ . Such a relation (11) does not always exist, but we can avoid this obstacle in the following way.

Let the elements of  $\Delta$  be denoted by  $\delta_1, \dots, \delta_m$  and fix an orderly ranking of the  $\Delta$ -indeterminate  $y$ . By Section 7, Proposition 7, there exists a differential polynomial  $A \in \mathcal{F}\{y\}_{\Delta}$  with  $A \notin \mathcal{F}$  such that  $A(\alpha) = 0$  and  $S_A(\alpha) \neq 0$ . Let  $(c_{i'j'})_{1 \leq i \leq m, 1 \leq j' \leq m}$  be an invertible matrix over  $\mathcal{G}$ , let  $\Delta'$  denote the set of derivation operators  $\delta_1', \dots, \delta_m'$  defined by the equations  $\delta_i = \sum_{1 \leq i' \leq m} c_{i'i'} \delta_{i'}$  ( $1 \leq i \leq m$ ), and let  $\Delta_1'$  denote the set consisting of  $\delta_1', \dots, \delta_{m-1}'$ . For any derivative  $\delta_1^{e_1} \dots \delta_m^{e_m} y$  of order  $r = \sum e_i$ , we may write

$$\begin{aligned} \delta_1^{e_1} \dots \delta_m^{e_m} y &= \left( \sum_{1 \leq i_1 \leq m} c_{1i_1} \delta_{i_1}' \right)^{e_1} \dots \left( \sum_{1 \leq i_m \leq m} c_{mi_m} \delta_{i_m}' \right)^{e_m} y \\ &= c_{1m}^{e_1} \dots c_{mm}^{e_m} \delta_m^{e_m} y + \dots, \end{aligned}$$

so that if  $r$  is the order of  $A$  (as a  $\Delta$ -polynomial and hence also as a  $\Delta'$ -polynomial), then

$$\partial A / \partial (\delta_m^r y) = \sum_{e_1 + \dots + e_m = r} (\partial A / \partial (\delta_1^{e_1} \dots \delta_m^{e_m} y)) c_{1m}^{e_1} \dots c_{mm}^{e_m}.$$

However, one of the partial derivatives  $\partial A / \partial (\delta_1^{e_1} \dots \delta_m^{e_m} y)$  in the sum here is the separant  $S_A$ , which does not vanish at  $\alpha$ . Therefore if we substitute  $\alpha$  for  $y$  and then express each of these partial derivatives linearly in terms of a basis  $(\gamma_k)$  of  $\mathcal{G}$  over  $\mathcal{C}$ , we arrive at an equation

$$\partial A / \partial (\delta_m^r y)(\alpha) = \sum_k g_k(c_{1m}, \dots, c_{mm}) \gamma_k,$$

where each  $g_k$  is a homogeneous polynomial in  $\mathcal{C}[X_1, \dots, X_m]$  of degree  $r$ , and some  $g_k$  is not 0. Letting  $g$  denote some nonzero  $g_k$ , we see that if  $g(c_{1m}, \dots, c_{mm}) \neq 0$ , then  $\partial A / \partial (\delta_m^r y)$  does not vanish at  $\alpha$ . On expanding the left member of the equation  $\delta_m^r A(\alpha) = 0$  we then find that

$$\partial A / \partial (\delta_m^r y)(\alpha) \cdot \delta_m^{r+1} \alpha - T(\alpha) = 0,$$

where  $T$  is a  $\Delta'$ -polynomial over  $\mathcal{F}$  in  $y$  of order less than or equal to  $r+1$  and free of  $\delta_m^{r+1} y$ . Hence we have the following result.

**Proposition 13** *Let the element  $\alpha$  of an extension of  $\mathcal{F}$  be differentially separable over  $\mathcal{F}$ . Denote the elements of  $\Delta$  by  $\delta_1, \dots, \delta_m$ . Then there exist a number  $r \in \mathbb{N}$  and a nonzero homogeneous polynomial  $g \in \mathcal{C}[X_1, \dots, X_m]$  of degree  $r$  with the following property: If  $(c_{i'j'})_{1 \leq i \leq m, 1 \leq j' \leq m}$  is an invertible matrix over  $\mathcal{C}$  with  $g(c_{1m}, \dots, c_{mm}) \neq 0$ , and if  $\delta_1', \dots, \delta_m'$  are the derivation operators defined by the equations  $\delta_i = \sum_{1 \leq i' \leq m} c_{i'i'} \delta_{i'}$  ( $1 \leq i \leq m$ ), then*

$$\delta_m^{r+1} \alpha \in \mathcal{F}\langle (\delta_1^{i_1} \dots \delta_m^{i_m} \alpha)_{i_1 + \dots + i_m \leq r+1, i_m \leq r} \rangle. \quad (12)$$

If we denote by  $\Delta_1'$  the set consisting of  $\delta_1', \dots, \delta_{m-1}'$ , then evidently relation (12) implies

$$\delta_m^{r+1} \alpha \in \mathcal{F} \langle \alpha, \delta_m' \alpha, \dots, \delta_m^r \alpha \rangle_{\Delta_1'}. \tag{11'}$$

Comparing this with relation (11), and recalling the observation made in connection with (11), we see that if  $(c_{ii'})$  has the properties described in Proposition 13, then  $\mathcal{F} \langle \alpha \rangle_{\Delta}$  is a finitely generated  $\Delta_1'$ -field extension of  $\mathcal{F}$ . Now, there are two cases in which the existence of a matrix  $(c_{ii'})$  as above is guaranteed. (1) In the case of an ordinary differential field (that is,  $m = 1$ ),  $g$  is of the form  $aX_1'$  with  $a \neq 0$ , so that  $g(c) \neq 0$  for every nonzero  $c \in \mathcal{C}$ . (2) In the case of an infinite differential field  $\mathcal{F}$ ,  $\mathcal{C}$  too is infinite since  $\mathcal{C} \supset \mathcal{F}^p$ , and therefore there exist matrices  $(c_{ii'})$  over  $\mathcal{C}$  with  $g(c_{1m}, \dots, c_{mm}) \det(c_{ii'}) \neq 0$ . Thus we have the following two corollaries.

**Corollary 1** Every finitely generated differentially separable extension of an ordinary differential field is finitely generated as a field extension.

**Corollary 2** If  $\mathcal{G}$  is a finitely generated differentially separable extension of  $\mathcal{F}$  and  $\mathcal{F}$  is infinite, then, after transformation of  $\Delta$  by a suitable invertible matrix over  $\mathcal{C}$  and subsequent restriction of the resulting set of derivation operators to a set consisting of all but one of these operators,  $\mathcal{G}$  is a finitely generated extension of  $\mathcal{F}$ .

It is a well-known and easy to prove fact that a subextension of a finitely generated field extension is itself always finitely generated. The analog for differential fields is in general false (see Exercise 4 below), but starting with this fact and using Proposition 13 we can prove the following result which, under favorable conditions (certainly when  $p = 0$ ), yields the analog in question.

**Proposition 14** Let  $\mathcal{H}$  be a finitely generated extension of  $\mathcal{F}$  and let  $\mathcal{G}$  be a differential field with  $\mathcal{F} \subset \mathcal{G} \subset \mathcal{H}$ . Then  $\mathcal{H}^p \mathcal{G}$  is a finitely generated extension of  $\mathcal{H}^p \mathcal{F}$ . If  $\mathcal{H}$  is separable over  $\mathcal{F}$  and over  $\mathcal{G}$ , then  $\mathcal{G}$  is a finitely generated extension of  $\mathcal{F}$ .

*Proof* First suppose that  $\mathcal{F}$  is infinite. If  $B$  is a differential inseparability basis of  $\mathcal{G}$  over  $\mathcal{F}$ , then  $B$  is finite and  $\mathcal{H}$  is finitely generated over  $\mathcal{F} \langle B \rangle$  (and in the separable case  $\mathcal{H}$  is, by Section 10, Theorem 5, separable over  $\mathcal{F} \langle B \rangle$ ). Hence we may replace  $\mathcal{F}$  by  $\mathcal{F} \langle B \rangle$ , that is, we may suppose that  $\mathcal{G}$  is differentially separable over  $\mathcal{F}$ . This being done, let  $\Gamma$  be a differential inseparability basis of  $\mathcal{H}$  over  $\mathcal{F}$  and hence of  $\mathcal{H}$  over  $\mathcal{G}$ . Then  $\mathcal{H}$  is finitely generated over the differential field  $\mathcal{F}' = \mathcal{F} \langle \Gamma \rangle$  (and in the separable case

is, by Section 10, Theorem 5, separable over  $\mathcal{F}'$  and over the differential field  $\mathcal{G}' = \mathcal{G} \langle \Gamma \rangle$ ). Also,  $\mathcal{H}$  is differentially separable over  $\mathcal{F}'$ . By Corollary 2 to Proposition 13 we may transform  $\Delta$  to a set of derivation operators  $\Delta'$  and then restrict  $\Delta'$  to a proper subset  $\Delta_1'$  so that  $\mathcal{H}$  is finitely generated as a  $\Delta_1'$ -field extension of  $\mathcal{F}'$ . Arguing by induction on  $\text{Card } \Delta$ , we may suppose that  $\mathcal{H}^p \mathcal{G}'$  is finitely generated over  $\mathcal{H}^p \mathcal{F}'$  as a  $\Delta_1'$ -field extension, *a fortiori* as a  $\Delta'$ -field extension, and therefore as a  $\Delta$ -field extension (and in the separable case, similarly, we may suppose that  $\mathcal{G}'$  is finitely generated over  $\mathcal{F}'$ ). However, by Section 9, Corollary 4 to Theorem 4,  $\mathcal{H}^p \mathcal{G}$  and  $\mathcal{H}^p \mathcal{F}'$  are linearly disjoint over  $\mathcal{H}^p \mathcal{F}$  (and in the separable case, since by Section 10, Theorem 5,  $\Gamma$  is differentially algebraically independent over  $\mathcal{F}$  and over  $\mathcal{G}$ ,  $\mathcal{G}$  and  $\mathcal{F}'$  are linearly disjoint over  $\mathcal{F}$ ). Hence we conclude without difficulty that  $\mathcal{H}^p \mathcal{G}$  is finitely generated over  $\mathcal{H}^p \mathcal{F}$  (and in the separable case that  $\mathcal{G}$  is finitely generated over  $\mathcal{F}$ ).

Now suppose that  $\mathcal{F}$  is finite, so that  $p \neq 0$  and  $\mathcal{F} = \mathcal{C}$ . Let  $t$  be an element of an extension of  $\mathcal{H}$  with  $t$  differentially transcendental over  $\mathcal{H}$ . Clearly  $\mathcal{H}$  and  $\mathcal{F} \langle t \rangle$  are linearly disjoint over  $\mathcal{F}$ , as are  $\mathcal{H}$  and  $\mathcal{G} \langle t \rangle$  over  $\mathcal{G}$ , and also  $\mathcal{H}^p \mathcal{G}$  and  $\mathcal{H}^p \mathcal{F} \langle t \rangle$  over  $\mathcal{H}^p \mathcal{F}$ . Furthermore,  $\mathcal{F} \langle t \rangle$  is infinite. Now,  $\mathcal{H} \langle t \rangle$  is finitely generated over  $\mathcal{F} \langle t \rangle$  (and in the separable case, by the linear disjointness,  $\mathcal{H} \langle t \rangle$  is separable over  $\mathcal{F} \langle t \rangle$  and over  $\mathcal{G} \langle t \rangle$ ). Hence by what we have already proved  $\mathcal{H} \langle t \rangle^p \mathcal{G} \langle t \rangle = \mathcal{H}^p \mathcal{G} \langle t \rangle$  is finitely generated over  $\mathcal{H} \langle t \rangle^p \mathcal{F} \langle t \rangle = \mathcal{H}^p \mathcal{F} \langle t \rangle$  (and in the separable case  $\mathcal{G} \langle t \rangle$  is finitely generated over  $\mathcal{F} \langle t \rangle$ ). It follows by the linear disjointness that  $\mathcal{H}^p \mathcal{G}$  is finitely generated over  $\mathcal{H}^p \mathcal{F}$  (and in the separable case that  $\mathcal{G}$  is finitely generated over  $\mathcal{F}$ ).

**Corollary 1** Let  $\mathcal{G}$  be a finitely generated extension of  $\mathcal{F}$ , and let  $\mathcal{D}$  denote the field of constants of  $\mathcal{G}$ . Then  $\mathcal{D}$  is a finitely generated field extension of  $\mathcal{G}^p \mathcal{C}$ .

*Proof* We have  $\mathcal{F} \subset \mathcal{F} \mathcal{D} \subset \mathcal{G}$ , so that, by the proposition, the differential field  $\mathcal{G}^p \cdot \mathcal{F} \mathcal{D} = \mathcal{F} \mathcal{D}$  is a finitely generated extension of  $\mathcal{G}^p \mathcal{F}$ . Hence there exist finitely many constants  $d_1, \dots, d_n \in \mathcal{D}$  such that  $\mathcal{F} \mathcal{D} = \mathcal{G}^p \mathcal{F} \langle d_1, \dots, d_n \rangle = \mathcal{F} \cdot \mathcal{G}^p \mathcal{C} \langle d_1, \dots, d_n \rangle$ , so that by Section 1, Corollary 2 to Theorem 1,  $\mathcal{D} = \mathcal{G}^p \mathcal{C} \langle d_1, \dots, d_n \rangle$ .

**Corollary 2** Let  $\mathcal{G}$  be a finitely generated separable extension of  $\mathcal{F}$ , and let  $\mathcal{F}^\circ$  denote the algebraic (= separable) closure of  $\mathcal{F}$  in  $\mathcal{G}$ . Then  $\mathcal{G}$  is separable over  $\mathcal{F}^\circ$  and  $[\mathcal{F}^\circ : \mathcal{F}] < \infty$ .

*Proof*  $\mathcal{G}$  is separable over  $\mathcal{F}^\circ$  by Section 2, Corollary to Proposition 2, and therefore the second part of Proposition 14 applies.

## EXERCISES

1. Give an example of an extension  $\mathcal{G} = \mathcal{F}\langle\eta\rangle$ , generated by a single element, of an ordinary differential field  $\mathcal{F}$ , which has finite transcendence degree but which is not differentially separable. (*Hint*: Let  $p \neq 0$ , let  $\mathcal{C}$  contain elements  $c_k$  ( $k \in \mathbb{N}$ ) such that  $c_k \notin \mathcal{F}^p((c_i)_{0 \leq i < k})$ , and consider the ideal  $\mathfrak{p} = (y^p - c_0, y'^p - c_1, y''^p - c_2, \dots)$  of  $\mathcal{F}\{y\}$  (see Chapter 0, Section 3, Lemma 2).)
2. Let  $\Delta_1$  be a set consisting of all but one of the elements of  $\Delta$ . Show by example that  $\mathcal{G}$  can be a finitely generated differentially separable (i.e.,  $\Delta$ -separable) extension of  $\mathcal{F}$  without being finitely generated as a  $\Delta_1$ -field extension. (*Hint*: Let  $\Delta$  consist of  $\delta_1$  and  $\delta_2$ ,  $\Delta_1$  consist of  $\delta_2$  alone. The differential ideal  $[\delta_1 \delta_2 y]$  of  $\mathcal{F}\{y\}$  is prime (see Chapter I, Section 6, Exercise 5). Take  $\mathcal{G} = Q(\mathcal{F}\{y\}/[\delta_1 \delta_2 y])$ .)
3. Show by example that the condition that  $\mathcal{F}$  be infinite cannot be omitted from Corollary 2 of Proposition 13. (*Hint*: Let  $\Delta$  consist of  $\delta_1$  and  $\delta_2$  and let  $\mathcal{F}$  be the prime field of characteristic 2. Observe that the differential ideal  $\mathfrak{p} = [\delta_1 \delta_2 y_1, \delta_1^2 y_2 + \delta_1 \delta_2 y_2, \delta_1 \delta_2 y_3 + \delta_2^2 y_3]$  of  $\mathcal{F}\{y_1, y_2, y_3\}$  is prime, and take  $\mathcal{G} = Q(\mathcal{F}\{y_1, y_2, y_3\}/\mathfrak{p})$ .)
4. Let  $p \neq 0$ , and let  $\mathcal{H} = \mathcal{F}\langle\alpha\rangle$  with  $\alpha$  differentially transcendental over  $\mathcal{F}$ . Set  $\mathcal{G} = \mathcal{H}^p \mathcal{F}$ . Show that  $\mathcal{G}$  is not a finitely generated extension of  $\mathcal{F}$ .
5. Let  $t$  be differentially transcendental over  $\mathcal{F}$ .
  - (a) Let  $\mathcal{G}$  be an extension of  $\mathcal{F}$  with  $\mathcal{G} \subset \mathcal{F}\langle t \rangle$  such that  $\mathcal{F}\langle t \rangle$  is separable over  $\mathcal{G}$ . Show that  $\mathcal{G}$  is generated by a set of two elements. (*Hint*: Use Proposition 14 and Exercise 1 of Section 10.)
  - (b) Show that when  $\text{Card } \Delta > 1$  and  $\delta_1, \delta_2$  are distinct elements of  $\Delta$  then the extension  $\mathcal{F}\langle \delta_1 t, \delta_2 t \rangle$  of  $\mathcal{F}$  is not generated by one element, and therefore the result of part (a) can not be improved. (When  $\text{Card } \Delta = 1$  and  $p = 0$ , an improvement is given by Ritt's analog of Lüroth's theorem. See Chapter IV, Section 7, Exercise 2.)
6. Let  $\mathcal{V}$  be a differential vector space over  $\mathcal{F}$  that is finitely generated (as a differential vector space), and use the notation and terminology of the Exercises of Sections 8, 9. Let  $\Delta_1 \subset \Delta$ ,  $\text{Card } \Delta_1 = \text{Card } \Delta - 1$ .
  - (a) Prove the following analog of Proposition 12: *Every element of  $\mathcal{V}$  is differentially linear over  $[0]$  if and only if the  $\Delta_1$ -dimension of  $\mathcal{V}$  is finite.*
  - (b) State and prove the analogs of Proposition 13 and its two corollaries.
  - (c) Show that every differential vector subspace of  $\mathcal{V}$  is finitely generated.
  - (d) Let  $\mathcal{V}_0$  denote the set of all elements  $v \in \mathcal{V}$  with  $\delta v = 0$  ( $\delta \in \Delta$ ). Show that  $\mathcal{V}_0$  is a finitely generated vector space over  $\mathcal{G}$ .

## 12 Differential inseparability polynomials

For finitely generated extensions it is possible to refine the notion of differential inseparability degree. We shall do this in Section 13 by attaching an object to each finite family of generators, and then showing that the object is independent of the family. In the present section we attach to each finite family  $\eta = (\eta_1, \dots, \eta_n)$  of elements of an extension of  $\mathcal{F}$  a numerical polynomial (see Chapter 0, Section 17) that reflects some of the (differential) inseparability properties of  $\eta$ , and which is used to introduce the refinement mentioned above. This polynomial, which bears an analogy with Hilbert's "characteristic polynomial" in algebraic geometry,<sup>3</sup> is not an invariant of the extension; it depends on the family and not merely on the differential field  $\mathcal{F}\langle\eta\rangle$ . But it does, as indicated above, carry certain invariants with it.

**Theorem 6** Let  $\eta = (\eta_1, \dots, \eta_n)$  be a finite family of elements of an extension of  $\mathcal{F}$ . There exists a numerical polynomial  $\omega_{\eta/\mathcal{F}}$  with the following properties.

- (a) For every sufficiently big  $s \in \mathbb{N}$  the inseparability degree (see Chapter 0, Section 2) of  $\mathcal{F}((\theta\eta_j)_{\theta \in \Theta(s), 1 \leq j \leq n})$  over  $\mathcal{F}$  equals  $\omega_{\eta/\mathcal{F}}(s)$ .
- (b)  $\deg \omega_{\eta/\mathcal{F}} \leq m$  ( $= \text{Card } \Delta$ ).
- (c) If we write  $\omega_{\eta/\mathcal{F}} = \sum_{0 \leq i \leq m} a_i (X^+)^i$ , then  $a_m$  equals the differential inseparability degree of  $\mathcal{F}\langle\eta\rangle$  over  $\mathcal{F}$ .
- (d) If  $\mathfrak{p}$  is the defining differential ideal of  $\eta$  in  $\mathcal{F}\{y_1, \dots, y_n\}$ , if  $A$  is a characteristic set of  $\mathfrak{p}$  relative to an orderly ranking of  $(y_1, \dots, y_n)$ , and if for each  $y_j$  we let  $E_j$  denote the set of all points  $(e_1, \dots, e_m) \in \mathbb{N}^m$  for which  $\delta_1^{e_1} \dots \delta_m^{e_m} y_j$  is a leader of an element of  $A$ , then (see Chapter 0, Section 17, Lemma 16)  $\omega_{\eta/\mathcal{F}} = \sum_{1 \leq j \leq n} \omega_{E_j} - b$ , where  $b \in \mathbb{N}$ . If  $p = 0$ , then  $b = 0$ .

*Proof* For any  $A \in \mathcal{A}$  we have  $A(\eta) = 0$  and  $S_A(\eta) \neq 0$ . Therefore  $u_A(\eta)$  is separably algebraic over  $\mathcal{F}((\theta\eta_j)_{\theta \in \Theta, 1 \leq j \leq n, \theta y_j < u_A})$ . Repeated differentiation shows that if  $v$  is any derivative of a leader of an element of  $A$ , then  $v(\eta)$  is separably algebraic over  $\mathcal{F}((\theta\eta_j)_{\theta \in \Theta, 1 \leq j \leq n, \theta y_j < v})$ . Let  $V$  denote the set of all derivatives  $\theta y_j$  ( $\theta \in \Theta$ ,  $1 \leq j \leq n$ ) that are not derivatives of any  $u_A$  ( $A \in \mathcal{A}$ ), and let  $V(s)$  denote the set of all  $\theta y_j \in V$  with  $\text{ord } \theta \leq s$  ( $s$  being any natural number). It follows from the above that  $\mathcal{F}((\theta\eta_j)_{\theta \in \Theta(s), 1 \leq j \leq n})$  is separably algebraic over  $\mathcal{F}((v(\eta))_{v \in V(s)})$ .

Let  $W$  denote the set of all  $w \in V$  such that only finitely many derivatives of  $w$  are in  $V$ . By Chapter 0, Section 17, Lemma 16,  $W$  is finite. Therefore we may fix  $r \in \mathbb{N}$  so that  $W \subset V(r)$ . Then  $V(r)$  is finite and therefore has a minimal subset  $V'$  such that each  $w(\eta)$  with  $w \in V(r)$  is separably algebraic

<sup>3</sup> See, e.g., O. Zariski and P. Samuel, "Commutative Algebra," Vol. II, Chap. VII, §12. Van Nostrand, Princeton, New Jersey, 1960.

over  $\mathcal{F}((v(\eta))_{v \in (V-V(r)) \cup V'})$ . If  $P \in \mathfrak{p} \cap \mathcal{F}[(V-V(r)) \cup V']$ , then, by the minimality of  $V'$ ,  $\partial P/\partial v' \in \mathfrak{p}$  for every  $v' \in V'$ . However, if  $v \in V-V(r)$ , then  $v \in V-W$  and  $v$  is higher than every element of  $V'$ , and it follows from Chapter I, Section 10, Lemma 9, that  $\partial P/\partial v \in \mathfrak{p}$ . Thus,  $(v(\eta))_{v \in (V-V(r)) \cup V'}$  is separably independent over  $\mathcal{F}$ .

If  $\mathfrak{p}$  contains a nonzero element  $P$  reduced with respect to  $A$ , then  $S_p = \partial P/\partial u_p$  is an element of  $\mathfrak{p}$  (by Chapter I, Section 10, Lemma 8). Choosing  $P$  of minimal degree, we see that we must have  $\partial P/\partial u_p = 0$ , whence  $p \neq 0$ . Put the other way around: If  $p = 0$ , then  $\mathfrak{p}$  does not contain a nonzero element reduced with respect to  $A$ . In particular, if  $p = 0$ , then  $V' = V(r)$ .

By the above, there exists an  $s' \in \mathbb{N}$  with  $s' \geq r$  such that each  $w(\eta)$  with  $w \in V(r)$  is separably algebraic over  $\mathcal{F}((v(\eta))_{v \in (V(s')-V(r)) \cup V'})$ . It is clear now that, for any  $s \in \mathbb{N}$  with  $s \geq s'$ ,  $(v(\eta))_{v \in (V(s)-V(r)) \cup V'}$  is an inseparability basis of  $\mathcal{F}((\theta\eta_j)_{\theta \in \Theta(s), 1 \leq j \leq n})$  over  $\mathcal{F}$ .

For each  $y_j$  the number of derivatives  $\delta_1^{i_1} \dots \delta_m^{i_m} y_j$  that are in  $V(s)$  equals the number of points  $(i_1, \dots, i_m) \in \mathbb{N}^m$  with  $i_1 + \dots + i_m \leq s$  that, in the product order on  $\mathbb{N}^m$ , are not greater than or equal to any point of  $\mathbb{E}_j$ . Therefore (by Chapter 0, Section 17, Lemma 16) for all sufficiently big  $s \in \mathbb{N}$  the inseparability degree of  $\mathcal{F}((\theta\eta_j)_{\theta \in \Theta(s), 1 \leq j \leq n})$  over  $\mathcal{F}$  equals  $\text{Card}((V(s)-V(r)) \cup V') = \text{Card} V(s) - \text{Card}(V(r)-V') = \sum_{1 \leq j \leq n} \omega_{\mathbb{E}_j}(s) - \text{Card}(V(r)-V')$ . The polynomial

$$\omega_{\eta/\mathcal{F}} = \sum_{1 \leq j \leq n} \omega_{\mathbb{E}_j} - \text{Card}(V(r)-V')$$

obviously has the properties (a), (b), and (d) described in the theorem.

To establish (c), let  $d$  denote the differential inseparability degree of  $\mathcal{F}\langle \eta \rangle$  over  $\mathcal{F}$ . Permuting the indices, we may suppose that  $\eta_1, \dots, \eta_d$  form a differential inseparability basis of  $\mathcal{F}\langle \eta \rangle$  over  $\mathcal{F}$ . For each index  $j$  with  $d < j \leq n$ ,  $\eta_j$  is differentially separable over  $\mathcal{F}\langle \eta_1, \dots, \eta_d \rangle$ ; by Section 7, Proposition 7, there therefore exists a  $\theta_j \in \Theta$ , of order say  $r_j$ , such that

$$\theta_j \eta_j \in \mathcal{F}\langle \eta_1, \dots, \eta_d \rangle ((\theta\eta_i)_{\theta \in \Theta, \theta y_i < \theta_j y_j}).$$

Fixing  $h \in \mathbb{N}$  sufficiently large we then may write

$$\theta_j \eta_j \in \mathcal{F}((\theta\eta_i)_{\theta \in \Theta(h), 1 \leq i \leq d}, (\theta\eta_j)_{\theta \in \Theta, \theta y_j < \theta_j y_j}).$$

Repeated differentiation shows that if  $\theta' y_j$  is any derivative of  $\theta_j y_j$  with  $\text{ord } \theta' = r' \geq r_j$ , then

$$\theta' \eta_j \in \mathcal{F}((\theta\eta_i)_{\theta \in \Theta(r'-r_j+h), 1 \leq i \leq d}, (\theta\eta_j)_{\theta \in \Theta, \theta y_j < \theta' y_j}).$$

It follows that if  $s \in \mathbb{N}$  and  $s \geq \max(r_{d+1}, \dots, r_n)$ , then

$$\mathcal{F}((\theta\eta_j)_{\theta \in \Theta(s), 1 \leq j \leq n}) \subset \mathcal{F}((\theta\eta_i)_{\theta \in \Theta(s+h), 1 \leq i \leq d}, (\theta\eta_j)_{\theta \in \Theta(s) - \Theta(s-r_j), d < j \leq n}).$$

Therefore, for all sufficiently big  $s \in \mathbb{N}$ ,

$$\begin{aligned} \omega_{\eta/\mathcal{F}}(s) &\leq d \cdot \text{Card } \Theta(s+h) + \sum_{d < j \leq n} \text{Card}(\Theta(s) - \Theta(s-r_j)) \\ &= d \cdot \binom{s+h+m}{m} + \sum_{d < j \leq n} \left( \binom{s+m}{m} - \binom{s-r_j+m}{m} \right) \\ &= d \binom{s+m}{m} + \dots, \end{aligned}$$

so that  $a_m \leq d$ . On the other hand,  $(\theta\eta_i)_{\theta \in \Theta(s), 1 \leq i \leq d}$  is separably independent over  $\mathcal{F}$ , so that, for big  $s \in \mathbb{N}$ ,

$$\omega_{\eta/\mathcal{F}}(s) \geq d \cdot \text{Card } \Theta(s) = d \binom{s+m}{m},$$

whence  $a_m \geq d$ . This shows that  $a_m = d$ , and completes the proof of the theorem.

We shall call the polynomial  $\omega_{\eta/\mathcal{F}}$  the *differential inseparability polynomial* of  $\eta$  over  $\mathcal{F}$ . When  $\eta$  is separable over  $\mathcal{F}$  (i.e.,  $\mathcal{F}\langle \eta \rangle$  is separable over  $\mathcal{F}$ ), then for every  $s \in \mathbb{N}$  the inseparability degree of  $\mathcal{F}((\theta\eta_j)_{\theta \in \Theta(s), 1 \leq j \leq n})$  over  $\mathcal{F}$  coincides with its transcendence degree. In this case we shall call  $\omega_{\eta/\mathcal{F}}$  also the *differential transcendence polynomial* of  $\eta$  over  $\mathcal{F}$ .

If  $\Delta'$  is the set of derivation operators obtained by transformation of  $\Delta$  by an invertible matrix over  $\mathcal{C}$ , and if  $\Theta'(s)$  denotes the set of all derivative operators of order less than or equal to  $s$  formed with the derivation operators in  $\Delta'$ , then  $\mathcal{F}((\theta\eta_j)_{\theta \in \Theta(s), 1 \leq j \leq n}) = \mathcal{F}((\theta' \eta_j)_{\theta' \in \Theta'(s), 1 \leq j \leq n})$ . Therefore the  $\Delta$ - and  $\Delta'$ -inseparability polynomials of  $\eta$  over  $\mathcal{F}$  coincide. In other words, the notion of differential inseparability polynomial is invariant under transformation of  $\Delta$  by an invertible matrix over  $\mathcal{C}$ .

It is easy to see that if  $\mathcal{F}' \supset \mathcal{F}$  is a differential subfield of an extension of  $\mathcal{F}\langle \eta \rangle$  such that  $\mathcal{F}'$  and  $\mathcal{F}\langle \eta \rangle$  are linearly disjoint over  $\mathcal{F}$  (or even algebraically disjoint, provided  $\mathcal{F}\langle \eta \rangle$  is separable over  $\mathcal{F}$ ), then  $\omega_{\eta/\mathcal{F}'} = \omega_{\eta/\mathcal{F}}$ .

**Proposition 15** Let  $\eta = (\eta_1, \dots, \eta_n)$  and  $\zeta = (\zeta_1, \dots, \zeta_r)$  be finite families of elements of an extension of  $\mathcal{F}$ .

(a) If  $h \in \mathbb{N}$  and  $\eta_j \in \mathcal{F}((\theta\zeta_k)_{\theta \in \Theta(h), 1 \leq k \leq r})$  ( $1 \leq j \leq n$ ), then  $\omega_{\eta/\mathcal{F}}(X) \leq \omega_{\zeta/\mathcal{F}}(X+h)$ .

(b) If  $\mathcal{F}\langle \eta \rangle = \mathcal{F}\langle \zeta \rangle$ , then there exists an  $h \in \mathbb{N}$  such that  $\omega_{\zeta/\mathcal{F}}(X-h) \leq \omega_{\eta/\mathcal{F}}(X) \leq \omega_{\zeta/\mathcal{F}}(X+h)$ .

*Proof* Under the hypothesis of (a) we have

$$\mathcal{F}((\theta\eta_j)_{\theta \in \Theta(s), 1 \leq j \leq n}) \subset \mathcal{F}((\theta\zeta_k)_{\theta \in \Theta(s+h), 1 \leq k \leq r}),$$



whence  $\omega_{\eta/\mathcal{F}}(s) \leq \omega_{\zeta/\mathcal{F}}(s+h)$  for sufficiently big  $s$ ; this proves (a). Under the hypothesis of (b) there exists an  $h \in \mathbb{N}$  sufficiently big to ensure that  $\eta_j \in \mathcal{F}((\theta\zeta_k)_{\theta \in \Theta(h), 1 \leq k \leq r})$  ( $1 \leq j \leq n$ ) and  $\zeta_k \in \mathcal{F}((\theta\eta_j)_{\theta \in \Theta(h), 1 \leq j \leq n})$  ( $1 \leq k \leq r$ ); therefore (b) follows from (a).

In particular, we see that if  $\mathcal{F}(\eta) = \mathcal{F}(\zeta)$ , then  $\omega_{\eta/\mathcal{F}} = \omega_{\zeta/\mathcal{F}}$ .

EXERCISE

- Let  $\mathcal{V}$  be a differential vector space over  $\mathcal{F}$ , and use the notation and terminology of the Exercises of Sections 8 and 9 and Exercise 6 of Section 11. Let  $\Phi$  be a finite subset of  $\mathcal{V}$ . Prove the following analog of Theorem 6: *There exists a numerical polynomial  $\omega_\Phi$  with the following properties: (a) For every sufficiently big  $s \in \mathbb{N}$  the vector space over  $\mathcal{F}$  generated by  $\Theta(s)\Phi$  has dimension  $\omega_\Phi(s)$ . (b)  $\deg \omega_\Phi \leq m$ . (c) If we write  $\omega_\Phi = \sum_{0 \leq i \leq m} a_i (X_i^{+i})$ , then  $a_m$  is the differential dimension of  $[\Phi]$ . (d) If  $v_1, \dots, v_n$  denote the elements of  $\Phi$ , and  $l$  denotes the set of all homogeneous linear differential polynomials in  $\mathcal{F}\{y_1, \dots, y_n\}$  that vanish at  $(v_1, \dots, v_n)$ , and  $A$  is an autoreduced subset of  $l$  of minimal rank relative to an orderly ranking of  $(y_1, \dots, y_n)$ , and, for each  $y_j$ ,  $E_j$  denotes the set of all points  $(e_1, \dots, e_m) \in \mathbb{N}^m$  such that  $\delta_1^{e_1} \dots \delta_m^{e_m} y_j$  is a leader of an element of  $A$ , then  $\omega_\Phi = \sum_{1 \leq j \leq n} \omega_{E_j}$ .*

13 Differential type; typical differential inseparability degree

Let  $\mathcal{G}$  be a finitely generated extension of  $\mathcal{F}$ . Choose a finite family  $\eta = (\eta_1, \dots, \eta_n)$  of generators of  $\mathcal{G}$  over  $\mathcal{F}$ . It is an immediate consequence of Section 12, Proposition 15, that the quantity  $\tau = \deg \omega_{\eta/\mathcal{F}}$ , which is an integer greater than or equal to  $-1$ , is independent of the choice of  $\eta$ , that is, depends only on  $\mathcal{G}$  and  $\mathcal{F}$ . We shall call  $\tau$  the differential type of  $\mathcal{G}$  over  $\mathcal{F}$ .

We may write  $\omega_{\eta/\mathcal{F}} = \sum_{0 \leq i \leq \tau} a_i (X_i^{+i})$ , where each  $a_i \in \mathbb{Z}$ . If  $\tau \neq -1$ , then  $a_\tau > 0$ ; if  $\tau = -1$ , we adopt the convention that  $a_\tau = 0$ . Proposition 15 shows that  $a_\tau$  also is independent of the choice of  $\eta$ . We shall call  $a_\tau$  the typical differential inseparability degree of  $\mathcal{G}$  over  $\mathcal{F}$ . If  $\mathcal{G}$  is separable over  $\mathcal{F}$ , we also shall call  $a_\tau$  the typical differential transcendence degree of  $\mathcal{G}$  over  $\mathcal{F}$ .

By what we have seen at the end of Section 12, these two notions are invariant under transformation of  $\Delta$  by an invertible matrix over  $\mathcal{C}$ . Also, if  $\mathcal{F}'$  is an extension of  $\mathcal{F}$  contained in some extension of  $\mathcal{G}$ , and if  $\mathcal{F}'$  and  $\mathcal{G}$  are linearly disjoint over  $\mathcal{F}$  (or even algebraically disjoint, provided  $\mathcal{G}$  is separable over  $\mathcal{F}$ ), then the differential type and the typical differential inseparability degree of  $\mathcal{G}$  over  $\mathcal{F}$  equal those of  $\mathcal{F}'\mathcal{G}$  over  $\mathcal{F}'$ .

The following theorem justifies the terminology somewhat.

**Theorem 7** *Let  $\mathcal{F}$  be infinite, and let  $\mathcal{G}$  be a finitely generated extension of  $\mathcal{F}$  of differential type  $\tau$ .*

- If  $\tau = -1$ , then  $\mathcal{G}$  is a separable algebraic extension of  $\mathcal{F}$  of finite degree.
- If  $\tau \neq -1$  and  $d^*$  denotes the typical differential inseparability degree of  $\mathcal{G}$  over  $\mathcal{F}$ , then there exists a set  $\Delta^*$ , consisting of  $\tau$  linearly independent linear combinations over  $\mathcal{C}$  of the elements of  $\Delta$ , such that  $\mathcal{G}$  is a finitely generated  $\Delta^*$ -field extension of  $\mathcal{F}$  of  $\Delta^*$ -inseparability degree  $d^*$ .

REMARK 1 The hypothesis that  $\mathcal{F}$  be infinite is not needed for (a).

REMARK 2 The proof shows that the  $\tau \times m$  matrices over  $\mathcal{C}$  yielding sets  $\Delta^*$  as in the theorem, form a set that contains a nonempty open set, relative to the Zariski topology, in the space  $\mathcal{C}^{\tau m}$  of all  $\tau \times m$  matrices over  $\mathcal{C}$ .

*Proof* Let  $\eta = (\eta_1, \dots, \eta_n)$  be a family of generators of  $\mathcal{G}$  over  $\mathcal{F}$ . If  $\tau = -1$ , then  $\omega_{\eta/\mathcal{F}} = 0$ , so that for all sufficiently big  $s \in \mathbb{N}$  the inseparability degree of  $\mathcal{F}((\theta\eta_j)_{\theta \in \Theta(s), 1 \leq j \leq n})$  over  $\mathcal{F}$  is 0. In particular, each  $\eta_j$  is separably algebraic over  $\mathcal{F}$ . However, if  $\alpha$  is separably algebraic over  $\mathcal{F}$ , then  $\delta\alpha \in \mathcal{F}(\alpha)$  ( $\delta \in \Delta$ ). Therefore  $\mathcal{G} = \mathcal{F}\langle\eta\rangle = \mathcal{F}(\eta)$ , whence  $\mathcal{G}$  is separable, algebraic, and of finite degree over  $\mathcal{F}$ .

Suppose now that  $0 \leq \tau \leq m$ . If the differential inseparability degree  $d$  of  $\mathcal{G}$  over  $\mathcal{F}$  is greater than 0, then, by Section 12, Theorem 6,  $\tau = m$  and  $d^* = d$ . In that case, transformation of  $\Delta$  by any invertible  $m \times m$  matrix over  $\mathcal{C}$  yields a set  $\Delta'$  of  $m$  derivation operators such that  $\mathcal{G}$  is a finitely generated  $\Delta'$ -field extension of  $\mathcal{F}$  of  $\Delta'$ -inseparability degree  $d$ . Assume then that  $d = 0$ . Let  $(c_{i'})_{1 \leq i' \leq m, 1 \leq i' \leq m}$  be an invertible matrix over  $\mathcal{C}$ , let  $\delta'_1, \dots, \delta'_m$  be the linear combinations of the elements  $\delta_1, \dots, \delta_m$  of  $\Delta$  determined by the conditions  $\delta'_i = \sum_{1 \leq i' \leq m} c_{i'i} \delta_{i'}$  ( $1 \leq i \leq m$ ), and let  $\Delta'_1$  denote the set consisting of the  $m-1$  derivation operators  $\delta'_1, \dots, \delta'_{m-1}$ . We shall show that  $(c_{i'})$  may be chosen so that  $\mathcal{G}$  is a finitely generated  $\Delta'_1$ -field extension of  $\mathcal{F}$  having  $\Delta'_1$ -type  $\tau$  and typical  $\Delta'_1$ -inseparability degree  $d^*$ . This will, clearly, suffice to prove the theorem.

By Section 11, Proposition 13, there is a nonzero homogeneous polynomial  $g \in \mathcal{C}[X_1, \dots, X_m]$  such that if  $g(c_{1m}, \dots, c_{mm}) \neq 0$ , then for each  $\eta_j$

$$\delta_m^{r_j+1} \eta_j \in \mathcal{F}((\delta_1^{i_1} \dots \delta_m^{i_m} \eta_j)_{i_1+\dots+i_m \leq r_j+1, i_m \leq r_j}),$$

where  $r_j$  denotes a suitable natural number. It follows that then the finite family  $\zeta = (\delta_m^{i_j} \eta_j)_{0 \leq i_j \leq r_j, 1 \leq j \leq n}$  generates  $\mathcal{G}$  as a  $\Delta'_1$ -field extension of  $\mathcal{F}$ .

Denoting the set of all derivative operators  $\delta_1^{i_1} \cdots \delta_m^{i_m}$  with  $i_1 + \cdots + i_m \leq s$  by  $\Theta'(s)$  and the set of all derivative operators  $\delta_1^{i_1} \cdots \delta_{m-1}^{i_{m-1}}$  with  $i_1 + \cdots + i_{m-1} \leq s$  by  $\Theta_1'(s)$ , we readily conclude that whenever  $r > r_j$ , then

$$\delta_m^r \eta_j \in \mathcal{F}(\Theta_1'(r) \eta_j, \Theta_1'(r-1) \delta_m' \eta_j, \dots, \Theta_1'(r-r_j) \delta_m^{r_j} \eta_j).$$

Differentiating  $s-r$  times with derivation operators in  $\Delta_1'$  we find, for any  $s \geq r$ , that if  $\theta' \in \Theta'(s)$ , then

$$\theta' \eta_j \in \mathcal{F}(\Theta_1'(s) \eta_j, \Theta_1'(s-1) \delta_1' \eta_j, \dots, \Theta_1'(s-r_j) \delta_m^{r_j} \eta_j),$$

so that

$$\mathcal{F}((\theta' \eta_j)_{\theta' \in \Theta'(s), 1 \leq j \leq n}) \subset \mathcal{F}((\theta_1' \delta_m^i \eta_j)_{\theta_1' \in \Theta_1'(s), 0 \leq i \leq r_j, 1 \leq j \leq n})$$

for all sufficiently big  $s \in \mathbb{N}$ . Denoting the  $\Delta_1'$ -inseparability polynomial of  $\zeta$  over  $\mathcal{F}$  by  $\omega'_{\zeta/\mathcal{F}}$ , we therefore have  $\omega_{\eta/\mathcal{F}} \leq \omega'_{\zeta/\mathcal{F}}$ . On the other hand, it is clear that

$$\begin{aligned} \mathcal{F}((\theta_1' \delta_m^i \eta_j)_{\theta_1' \in \Theta_1'(s), 0 \leq i \leq r_j, 1 \leq j \leq m}) &\subset \mathcal{F}((\theta' \eta_j)_{\theta' \in \Theta'(s+r_j), 1 \leq j \leq m}) \\ &\subset \mathcal{F}((\theta' \eta_j)_{\theta' \in \Theta'(s+r_0), 1 \leq j \leq m}), \end{aligned}$$

where  $r_0 = \max(r_1, \dots, r_n)$ , so that  $\omega'_{\zeta/\mathcal{F}}(X) \leq \omega_{\eta/\mathcal{F}}(X+r_0)$ . It follows from these two inequalities that  $\mathcal{G}$  has  $\Delta_1'$ -type  $\tau$  and typical  $\Delta_1'$ -inseparability degree  $d^*$  over  $\mathcal{F}$ .

### EXERCISE

1. Let  $\mathcal{V}$  be a finitely generated differential vector space over  $\mathcal{F}$ , and use the notation of Exercise 1 of Section 12. For any choice  $\Phi$  of a finite set of generators of  $\mathcal{V}$ , let  $\tau = \deg \omega_\Phi$  and write  $\omega_\Phi = \sum_{0 \leq i \leq \tau} a_i (X^{i+1})$ .
  - (a) Show that  $\tau$  and  $a_\tau$  do not depend on the choice of  $\Phi$ .
  - (b) State and prove the analog of Theorem 7.

## CHAPTER III

### The Basis Theorem and Some Related Topics

There is no direct analog for differential polynomials of the Hilbert basis theorem for polynomials. There is, however, a weakened analog, the basis theorem of Ritt and Raudenbush. In this chapter we prove a very general version of this theorem. The Ritt–Raudenbush theorem and the known generalizations of it are corollaries of the present version.

The basis theorem and the lemma on which it is based are applied to the following varied topics: behavior of prime differential polynomial ideals under extension of the differential field of coefficients, differential fields of definition of differential polynomial ideals, universal extensions, and differential specializations.

Throughout the chapter  $\mathcal{R}$  denotes a differential ring, and  $\mathcal{F}$  denotes a differential field for the characteristic of which we write  $p$  and for the field of constants of which we write  $\mathcal{C}$ . For  $\mathcal{R}$  as well as for  $\mathcal{F}$  we denote the set of derivation operators by  $\Delta$ , the set of derivative operators by  $\Theta$ , and the set of derivative operators of order less than or equal to  $s$  by  $\Theta(s)$ . The letters  $y$  and  $z$ , with or without subscripts, stand for differential indeterminates.

#### 1 Differential conservative systems

Let  $\mathcal{M}$  be a differential module over the differential ring  $\mathcal{R}$ . By a *differential conservative system* of  $\mathcal{M}$  we shall mean a conservative system of  $\mathcal{M}$  (see Chapter 0, Section 7) every element of which is a differential submodule of  $\mathcal{M}$ .

We shall be interested exclusively in the case in which  $\mathcal{M} = \mathcal{R}$ . If  $\mathcal{C}$  is a

differential conservative system of  $\mathcal{R}$ , then the elements of  $\mathbb{C}$  are differential ideals of  $\mathcal{R}$ ; as in Chapter 0, Section 7, we call them  $\mathbb{C}$ -ideals.

The set of all differential ideals of  $\mathcal{R}$  is a differential conservative system of  $\mathcal{R}$ . So is the set consisting solely of the element  $\mathcal{R}$ .

Since the set of all perfect ideals of  $\mathcal{R}$  is a conservative system of  $\mathcal{R}$ , it follows that the set of all perfect differential ideals of  $\mathcal{R}$  is a conservative system of  $\mathcal{R}$ , and therefore a differential one. If  $\mathfrak{f}$  is a perfect differential ideal of  $\mathcal{R}$ , and  $s \in \mathcal{R}$ , then by Chapter I, Section 2, Corollary to Lemma 1,  $\mathfrak{f}:s$  is a perfect differential ideal of  $\mathcal{R}$ . Therefore the set of all perfect differential ideals of  $\mathcal{R}$  is a perfect differential conservative system of  $\mathcal{R}$  (see Chapter 0, Section 8).

Let  $\Sigma$  be a subset of  $\mathcal{R}$ . The smallest perfect differential ideal of  $\mathcal{R}$  containing  $\Sigma$  is called the perfect differential ideal of  $\mathcal{R}$  generated by  $\Sigma$ , and is denoted by  $\{\Sigma\}_{\mathcal{R}}$  or, when there is no ambiguity, by  $\{\Sigma\}$ . In other words, if we denote the set of all perfect differential ideals of  $\mathcal{R}$  by  $\mathbb{C}$ , then  $\{\Sigma\} = (\Sigma)_{\mathbb{C}}$ . The set  $\Sigma$  is said to be a set of perfect differential ideal generators of  $\{\Sigma\}$  or, if  $\Sigma$  is finite, a perfect differential ideal basis (or simply a basis) of  $\{\Sigma\}$ .

A description of  $\{\Sigma\}$  can be given by defining recursively:

$$\{\Sigma\}_1 \text{ is the set of all } x \in \mathcal{R} \text{ such that } x^n \in [\Sigma] \text{ for some } n \in \mathbb{N};$$

$$\{\Sigma\}_{k+1} = \{\{\Sigma\}_k\}_1.$$

Then it is easy to see that  $\{\Sigma\} = \bigcup \{\Sigma\}_k$ . When  $\mathcal{R}$  is an overring of  $\mathbb{Q}$ , the nature of  $\{\Sigma\}$  is especially transparent, namely,  $\{\Sigma\} = \{\Sigma\}_1$ . This is an immediate consequence of Chapter I, Section 2, Lemma 2.

Let  $\mathcal{A}$  be a differential algebra over  $\mathcal{F}$ . The set of all perfect differential ideals of  $\mathcal{A}$  and the set of all  $\mathcal{F}$ -separable ideals of  $\mathcal{A}$  are perfect conservative systems of  $\mathcal{A}$ , and therefore their intersection is. Thus, the set of all  $\mathcal{F}$ -separable differential ideals of  $\mathcal{A}$  is a perfect differential conservative system of  $\mathcal{A}$ .

Let  $\Sigma$  be a subset of  $\mathcal{A}$ . The smallest  $\mathcal{F}$ -separable differential ideal of  $\mathcal{A}$  containing  $\Sigma$  is called the  $\mathcal{F}$ -separable differential ideal of  $\mathcal{A}$  generated by  $\Sigma$ , and is denoted by  $\{\Sigma\}_{\mathcal{A}/\mathcal{F}}$  or, when there is no ambiguity, by  $\{\Sigma\}_{\mathcal{F}}$ . Of course, when  $p = 0$  then  $\{\Sigma\}_{\mathcal{F}} = \{\Sigma\}$ . When  $p \neq 0$  a description of  $\{\Sigma\}_{\mathcal{F}}$  can be given by defining recursively:

$\{\Sigma\}_{\mathcal{F}}^{(1)}$  is the set of all  $x \in \mathcal{A}$  for which there exists a relation  $\sum x_i^p c_i \in [\Sigma]$  with  $(c_i)$  a family of elements of  $\mathcal{C}$  linearly independent over  $\mathcal{F}^p$  and with  $(x_i)$  a family of elements of  $\mathcal{A}$  at least one of which equals  $x$ ;

$$\{\Sigma\}_{\mathcal{F}}^{(k+1)} = \{\{\Sigma\}_{\mathcal{F}}^{(k)}\}_{\mathcal{F}}^{(1)}.$$

Then  $\{\Sigma\}_{\mathcal{F}} = \bigcup \{\Sigma\}_{\mathcal{F}}^{(k)}$ . Indeed, consider any finite family  $(c_i)$  of elements of  $\mathcal{C}$  linearly independent over  $\mathcal{F}^p$ . Because  $\mathcal{A}/\{\Sigma\}_{\mathcal{F}}$  is separable over  $\mathcal{F}$ ,

$(c_i)$  is linearly independent over  $(\mathcal{A}/\{\Sigma\}_{\mathcal{F}})^p$ . Therefore if  $\sum x_i^p c_i \in \{\Sigma\}_{\mathcal{F}}$ , then each  $x_i \in \{\Sigma\}_{\mathcal{F}}$ . This shows that  $\{\Sigma\}_{\mathcal{F}}^{(1)} \subset \{\Sigma\}_{\mathcal{F}}$  and therefore, through an easy induction argument, that the union  $u = \bigcup \{\Sigma\}_{\mathcal{F}}^{(k)}$  has the property that  $u \subset \{\Sigma\}_{\mathcal{F}}$ . On the other hand, if  $\sum x_i^p c_i \in u$ , then  $\sum x_i^p c_i \in \{\Sigma\}_{\mathcal{F}}^{(k)}$  for some  $k$ , whence each  $x_i \in \{\Sigma\}_{\mathcal{F}}^{(k+1)} \subset u$ . Thus  $(\mathcal{A}/u)^p$  and  $\mathcal{C}$  are linearly disjoint over  $\mathcal{F}^p$ , so that by Chapter II, Section 2, Proposition 1, the differential algebra  $\mathcal{A}/u$  over  $\mathcal{F}$  is separable. This shows that the ideal  $u$  is  $\mathcal{F}$ -separable, so that  $u \supset \{\Sigma\}_{\mathcal{F}}$ .

EXERCISES

- Let  $\mathcal{A} = \mathcal{F}\{(y_i)_{i \in I}\}$  be a differential polynomial algebra over  $\mathcal{F}$ , and  $\Sigma$  be a subset of  $\mathcal{A}$ . Show that if each element of  $\Sigma$  is homogeneous then  $[\Sigma]$ ,  $\{\Sigma\}$ , and  $\{\Sigma\}_{\mathcal{F}}$  are homogeneous ideals.
- (Ritt [95, p. 146]) Let  $F_1, \dots, F_r \in \mathcal{F}\{y_1, \dots, y_n\}$  and suppose that  $\Theta$  is independent on  $\mathcal{F}$ . Show that there exist  $n+1$  linear combinations  $L_i = \zeta_{i1} F_1 + \dots + \zeta_{ir} F_r$  ( $1 \leq i \leq n+1$ ) of  $F_1, \dots, F_r$  over  $\mathcal{F}$  such that  $\{F_1, \dots, F_r\} = \{L_1, \dots, L_{n+1}\}$ . (Hint: Set  $e = \max_{1 \leq k \leq r} \text{ord } F_k$  and fix  $s \in \mathbb{N}$  so that  $(n+1) \binom{s+m}{m} > n \binom{s+e+m}{m}$ . Let  $(z_{ik})_{1 \leq i \leq n+1, 1 \leq k \leq r}$  be a family of differential indeterminates over  $\mathcal{F}\{y_1, \dots, y_n\}$ , let  $M_i = z_{i1} F_1 + \dots + z_{ir} F_r$  ( $1 \leq i \leq n+1$ ), and consider the ideal  $\mathfrak{a}$  generated by

$$\theta M_i \quad (\theta \in \Theta(s), 1 \leq i \leq n+1)$$

in the polynomial algebra

$$R = \mathcal{F}[(\theta y_j)_{\theta \in \Theta(s+e), 1 \leq j \leq n}, (\theta z_{ik})_{\theta \in \Theta(s), 1 \leq i \leq n+1, 1 \leq k \leq r}]$$

over  $\mathcal{F}$ . Show that if  $((\eta_{\theta, j}), (\zeta_{\theta, i, k}))$  is a generic zero of a prime ideal  $\mathfrak{p}$  of  $R$  with  $\mathfrak{a} \subset \mathfrak{p}$  and  $F_1 \notin \mathfrak{p}$ , then

$$\zeta_{\theta, i, 1} \in \mathcal{F}((\zeta_{\theta', i, k})_{\theta' \in \Theta(s), 2 \leq k \leq r}, ((\eta_{\theta', j})_{\theta' \in \Theta(s+e), 1 \leq j \leq n})$$

for all  $\theta \in \Theta(s)$ ,  $1 \leq i \leq n+1$ , and infer that  $\mathfrak{a}$  contains an element  $B_p F_1^{d_p}$ , where  $d_p \in \mathbb{N}$ ,  $B_p \in R$ ,  $B_p \neq 0$ , and  $B_p$  is free of every  $\theta y_j$ . Conclude that there exist a nonzero  $C \in \mathcal{F}((z_{ik})_{1 \leq i \leq n+1, 1 \leq k \leq r})$  and an  $f \in \mathbb{N}$  such that, for every  $k$ ,  $CF_k^f \in [M_1, \dots, M_{n+1}]$  in  $\mathcal{F}\{(y_j)_{1 \leq j \leq n}, (z_{ik})_{1 \leq i \leq n+1, 1 \leq k \leq r}\}$ , and then take elements  $\zeta_{ik} \in \mathcal{F}$  such that  $C((\zeta_{ik}) \neq 0)$ .

2 Quasi-separable differential ideals

The purpose of this section is to prove the following lemma and its corollary.

**Lemma 1** Let  $\mathcal{S} = \mathcal{R}\{y_1, \dots, y_n\}$  be a finitely generated differential polynomial algebra over  $\mathcal{R}$ , and suppose given a sequential ranking of  $(y_1, \dots, y_n)$ . Let  $\mathfrak{p}$  be a prime differential ideal of  $\mathcal{S}$  that is quasi-separable over  $\mathcal{R}$ , let  $\mathcal{A}$

be a characteristic set of  $\mathfrak{p}$ , and let  $V$  denote the set of derivatives  $\theta y_j$  that are not proper derivatives of any leader  $u_A$  with  $A \in A$ . Then there exists a finite set  $Y \subset V$  such that every element of  $\mathfrak{p}$  that is reduced with respect to  $A$  is in the ideal  $(\mathfrak{p} \cap \mathcal{R}[Y])$  of  $\mathcal{S}$ .

**REMARK** If  $\mathcal{S}/\mathfrak{p}$  is of characteristic 0, the lemma is trivial, even when it is strengthened by omitting the requirement that the ranking be sequential and by taking  $Y$  to be the empty set. Indeed, if there existed an element of  $\mathfrak{p}$  reduced with respect to  $A$  and not in  $(\mathfrak{p} \cap \mathcal{R})$ , then there would exist one, call it  $P$ , of minimal rank. The separant  $S_P = \partial P / \partial u_P$  would be in  $\mathfrak{p}$  by Chapter I, Section 10, Lemma 8. By the minimality of the rank of  $P$  then  $S_P$  would be in  $(\mathfrak{p} \cap \mathcal{R})$ , and by the hypothesis on the characteristic of  $\mathcal{S}/\mathfrak{p}$  this would force the contradiction that  $P \in (\mathfrak{p} \cap \mathcal{R})$ .

*Proof* Assume the conclusion false. For each  $s \in \mathbb{N}$  let  $V(s)$  denote the set of all elements  $\theta y_j \in V$  with  $\text{ord } \theta \leq s$ , and let  $q_s = \text{Card } V(s)$ . Because the conclusion is false, for each  $s \in \mathbb{N}$  there exists an  $s' \in \mathbb{N}$  with  $s' > s$  such that some element of  $\mathfrak{p} \cap \mathcal{R}[V(s')]$  is not an element of  $(\mathfrak{p} \cap \mathcal{R}[V(s)])$ . In other words, if  $f: \mathcal{S} \rightarrow \mathcal{S}/\mathfrak{p}$  denotes the canonical homomorphism, then the transcendence degree of  $f(\mathcal{R}[V(s')])$  over  $f(\mathcal{R}[V(s)])$  is less than  $q_{s'} - q_s$ . It follows that there exists an infinite strictly increasing sequence of natural numbers  $s, s', \dots, s^{(v)}, \dots$  such that the transcendence degree of  $f(\mathcal{R}[V(s^{(v+1)})])$  over  $f(\mathcal{R}[V(s^{(v)})])$  is less than or equal to  $q_{s^{(v+1)}} - q_{s^{(v)}} - 1$ . For any  $h \in \mathbb{N}$  the transcendence degree of  $f(\mathcal{R}[V(s^{(h)})])$  over  $f(\mathcal{R})$  is then less than or equal to  $q_s + \sum_{0 \leq v < h} (q_{s^{(v+1)}} - q_{s^{(v)}} - 1) = q_{s^{(h)}} - h$ , which is less than  $q_{s^{(h)}} - q_s$  provided  $h > q_s$ . Thus, for every  $s \in \mathbb{N}$  there exists a  $t \in \mathbb{N}$  with  $t > s$  such that the transcendence degree of  $f(\mathcal{R}[V(t)])$  over  $f(\mathcal{R})$  is less than  $q_t - q_s$ .

Let  $W$  denote the set of all  $w \in V$  such that only finitely many derivatives of  $w$  are in  $V$ . By Chapter 0, Section 17, Lemma 16,  $W$  is a finite set, so that if  $s(0)$  is a large enough natural number, then  $W \subset V(s(0))$ . Fixing  $s(0)$  large enough for this to be the case, we see from the final remark of the preceding paragraph that there exists an infinite strictly increasing sequence of natural numbers  $s(0), s(1), \dots, s(v), \dots$  such that the transcendence degree of  $f(\mathcal{R}[V(s(v+1))])$  over  $f(\mathcal{R})$  is less than  $q_{s(v+1)} - q_{s(v)}$ . Each family  $(f(v))_{v \in V(s(v+1)) - V(s(v))}$  is then algebraically dependent over  $f(\mathcal{R})$ . Since the sets  $V(s(v+1)) - V(s(v))$  are disjoint, and  $\bigcup_{v \in \mathbb{N}} (V(s(v+1)) - V(s(v))) = V - V(s(0))$ , we conclude that the family  $(f(v))_{v \in V - V(s(0))}$  has infinite algebraic codimension over  $Q(f(\mathcal{R}))$ . However, by Chapter I, Section 10, Lemma 9, this family is separably independent over  $Q(f(\mathcal{R}))$ . This shows that  $\mathfrak{p}$  is not quasi-separable over  $\mathcal{R}$ .

**Corollary** Let  $\mathcal{R}_0$  be a differential subring of  $\mathcal{R}$  over which  $\mathcal{R}$  is finitely generated (as a differential ring), and let  $\mathfrak{p}$  be a prime differential ideal of  $\mathcal{R}$

which is quasi-separable over  $\mathcal{R}_0$ . Then there exist a finite set  $\Phi \subset \mathcal{R}$ , a finite set  $\Psi \subset \mathfrak{p}$ , and an element  $u \in \mathcal{R}$  with  $u \notin \mathfrak{p}$ , such that  $\mathfrak{p} = ([\Psi] + (\mathfrak{p} \cap \mathcal{R}_0[\Phi])) : u^\infty$ .

*Proof* Since  $\mathcal{R}$  is finitely generated over  $\mathcal{R}_0$  there exist a finitely generated differential polynomial algebra  $\mathcal{S} = \mathcal{R}_0\{y_1, \dots, y_n\}$  over  $\mathcal{R}_0$  and a surjective  $\mathcal{R}_0$ -homomorphism  $g: \mathcal{S} \rightarrow \mathcal{R}$ . The inverse image  $\mathfrak{q} = g^{-1}(\mathfrak{p})$  is a prime differential ideal of  $\mathcal{S}$  containing the kernel of  $g$ , so that (see Chapter 0, Section 6, the Remark preceding Lemma 5)  $\mathfrak{q}$  is quasi-separable over  $\mathcal{R}_0$ . By Lemma 1 there exist an autoreduced set  $A \subset \mathfrak{q}$  with  $H_A \notin \mathfrak{q}$  and a finite set  $Y$  of derivatives  $\theta y_j$  such that every element of  $\mathfrak{q}$  that is reduced with respect to  $A$  is in  $(\mathfrak{q} \cap \mathcal{R}_0[Y])$ . Let  $x \in \mathfrak{p}$ . There exists an  $F \in \mathfrak{p}$  with  $g(F) = x$ . By Chapter I, Section 9, Proposition 1, the remainder  $F_0$  of  $F$  with respect to  $A$  is reduced with respect to  $A$ , and  $F \in ((F_0) + [A]) : H_A^\infty$ . By the above,  $F_0 \in (\mathfrak{q} \cap \mathcal{R}_0[Y])$ , so that  $F \in ([A] + (\mathfrak{q} \cap \mathcal{R}_0[Y])) : H_A^\infty$ . Applying  $g$  we obtain the relation  $x \in ([g(A)] + (\mathfrak{p} \cap \mathcal{R}_0[g(Y)])) : g(H_A)^\infty$ . Thus, the corollary holds with  $\Phi = g(Y)$ ,  $\Psi = g(A)$ , and  $u = g(H_A)$ .

### 3 Differential fields of definition

A polynomial algebra  $K[X] = K[(X_i)_{i \in I}]$  over a field  $K$  has, as a vector space over  $K$ , a basis consisting of the monomials in  $X$ ; an ideal is a subspace. By a *field of definition* of a polynomial ideal  $\mathfrak{f}$  is meant a subfield  $K_0$  of  $K$  that is a field of definition of the subspace  $\mathfrak{f}$  relative to the basis of monomials (see Chapter I, Section 5), that is, that has the property that  $K \cdot (\mathfrak{f} \cap K_0[X]) = \mathfrak{f}$ . It is apparent that if  $K_0$  is field of definition of  $\mathfrak{f}$ , then any field of definition of  $\mathfrak{f} \cap K_0[X]$  is a field of definition of  $\mathfrak{f}$ , and any field  $K_1$  between  $K_0$  and  $K$  is a field of definition of  $\mathfrak{f}$  such that  $K_0$  is a field of definition of  $\mathfrak{f} \cap K_1[X]$ .

If, furthermore, we denote the canonical homomorphism  $K[X] \rightarrow K[X]/\mathfrak{f}$  by  $f$ , then (by Chapter 0, Section 10, Lemma 9, applied to the ideal  $\mathfrak{f} \cap K_0[X]$ )  $f(K_0[X])$  and  $K$  are linearly disjoint over  $K_0$ . It easily follows from this that if the ideal  $\mathfrak{f}$  of  $K[X]$  with field of definition  $K_0$  is separable, respectively quasi-separable, respectively regular, over  $K$ , then  $\mathfrak{f} \cap K_0[X]$  is separable, respectively quasi-separable, respectively regular, over  $K_0$ .

A differential polynomial algebra  $\mathcal{F} \{(y_i)_{i \in I}\}$  in a family of differential indeterminates  $(y_i)_{i \in I}$  over a differential field  $\mathcal{F}$  is a polynomial algebra in the family of indeterminates  $(\theta y_i)_{\theta \in \Theta, i \in I}$  over the field  $\mathcal{F}$ , and a differential ideal is also an ideal. By a *differential field of definition* of a differential polynomial ideal  $\mathfrak{f}$  over  $\mathcal{F}$  we shall mean a differential subfield of  $\mathcal{F}$  that is a field of definition of  $\mathfrak{f}$ . It is an immediate consequence of Chapter I, Section 5, Lemma 3, that the smallest field of definition of a differential polynomial ideal over  $\mathcal{F}$  is a differential subfield of  $\mathcal{F}$ .

**Proposition 1** *Let  $\mathfrak{p}$  be a prime differential ideal of the finitely generated differential polynomial algebra  $\mathcal{F}\{y_1, \dots, y_n\}$  over  $\mathcal{F}$ , with  $\mathfrak{p}$  quasi-separable over  $\mathcal{F}$ . Then the smallest field of definition of  $\mathfrak{p}$  is a finitely generated differential field extension of the prime field.*

*Proof* By Section 2, the Corollary to Lemma 1, there exist an  $L \in \mathcal{F}\{y_1, \dots, y_n\}$  with  $L \notin \mathfrak{p}$  and an  $s \in \mathbb{N}$  such that

$$\mathfrak{p} = [\mathfrak{p} \cap \mathcal{F}[(\theta y_j)_{\theta \in \Theta(s), 1 \leq j \leq n}]] : L^\infty.$$

By Hilbert's basis theorem the polynomial ideal  $\mathfrak{p} \cap \mathcal{F}[(\theta y_j)_{\theta \in \Theta(s), 1 \leq j \leq n}]$  is finitely generated. Therefore  $\mathfrak{p}$  has a finite subset  $\Phi$  such that  $\mathfrak{p} = [\Phi] : L^\infty$ . Let  $\mathcal{F}_i$  be the differential field generated by the coefficients in  $L$  and in the elements of  $\Phi$ , and let  $(\varphi_i)$  be a vector space basis of  $\mathcal{F}$  over  $\mathcal{F}_i$ . For any  $G \in \mathfrak{p}$  we may write  $G = \sum G_i \varphi_i$  with each  $G_i \in \mathcal{F}_i\{y_1, \dots, y_n\}$ . By the above, there is an  $r \in \mathbb{N}$  such that  $L^r G \in \mathcal{F} \cdot (\mathfrak{p} \cap \mathcal{F}_i\{y_1, \dots, y_n\})$ , and by Chapter 0, Section 10, Lemma 9, this implies that  $L^r G_i \in \mathfrak{p} \cap \mathcal{F}_i\{y_1, \dots, y_n\}$ . Therefore each  $G_i \in \mathfrak{p} \cap \mathcal{F}_i\{y_1, \dots, y_n\}$ , so that  $G \in \mathcal{F} \cdot (\mathfrak{p} \cap \mathcal{F}_i\{y_1, \dots, y_n\})$ , and  $\mathcal{F}_i$  is a differential field of definition. Thus, we conclude that  $\mathfrak{p}$  has a finitely generated differential field of definition. Now let  $\mathcal{F}_0$  be the smallest field of definition of  $\mathfrak{p}$ . By our earlier remarks,  $\mathcal{F}_0$  is a differential field and  $\mathfrak{p} \cap \mathcal{F}_0\{y_1, \dots, y_n\}$  is a prime differential ideal quasiseparable over  $\mathcal{F}_0$ . Arguing for this ideal as we just did for  $\mathfrak{p}$ , we conclude that  $\mathfrak{p} \cap \mathcal{F}_0\{y_1, \dots, y_n\}$  has a finitely generated differential field of definition  $\mathcal{F}_{01}$ . However,  $\mathcal{F}_{01}$  is a field of definition of  $\mathfrak{p}$  and is contained in  $\mathcal{F}_0$ . Therefore  $\mathcal{F}_0 = \mathcal{F}_{01}$ .

#### 4 The basis theorem

We are now in a position to prove one of the main results of this chapter.

**Theorem 1** *Let  $\mathcal{R}_0$  be a differential subring of  $\mathcal{R}$  over which  $\mathcal{R}$  is finitely generated (as a differential ring). Let  $\mathbb{C}$  be a perfect differential conservative system of  $\mathcal{R}$ . If  $\mathbb{C}|\mathcal{R}_0$  is Noetherian, and if every prime  $\mathbb{C}$ -ideal is quasi-separable over  $\mathcal{R}_0$ , then  $\mathbb{C}$  is Noetherian.*

*Proof* Assume the conclusion false. By Chapter 0, Section 9, Lemma 8, there exists a maximal  $\mathbb{C}$ -ideal  $\mathfrak{m}$  that is not finitely  $\mathbb{C}$ -generated, and  $\mathfrak{m}$  is prime. By Section 2, Corollary to Lemma 1, there exist a finite  $\Phi \subset \mathcal{R}$ , a finite  $\Psi \subset \mathfrak{m}$ , and a  $u \in \mathcal{R}$  with  $u \notin \mathfrak{m}$ , such that  $u\mathfrak{m} \subset ([\Psi] + (\mathfrak{m} \cap \mathcal{R}_0[\Phi]))_{\mathbb{C}}$ . By Chapter 0, Section 9, Proposition 3 (applied to the perfect conservative system  $\mathbb{C}|\mathcal{R}_0[\Phi]$  of the ring  $\mathcal{R}_0[\Phi]$ ), there exists a finite set  $\Lambda \subset \mathfrak{m} \cap \mathcal{R}_0[\Phi]$  such that  $\mathfrak{m} \cap \mathcal{R}_0[\Phi] = (\Lambda)_{\mathbb{C}|\mathcal{R}_0[\Phi]}$ , whence  $\mathfrak{m} \cap \mathcal{R}_0[\Phi] \subset (\Lambda)_{\mathbb{C}}$ . Thus,  $u\mathfrak{m} \subset (\Psi \cup \Lambda)_{\mathbb{C}}$ . By the maximality of  $\mathfrak{m}$ ,  $(u, \mathfrak{m})_{\mathbb{C}}$  is finitely  $\mathbb{C}$ -generated. It

follows (by Chapter 0, Section 7, Lemma 6) that there exists a finite set  $M \subset \mathfrak{m}$  such that  $(u, \mathfrak{m})_{\mathbb{C}} = (u, M)_{\mathbb{C}}$ . By Chapter 0, Section 8, Lemma 7, then

$$\begin{aligned} \mathfrak{m} &= \mathfrak{m} \cap (u, \mathfrak{m})_{\mathbb{C}} = \mathfrak{m} \cap (u, M)_{\mathbb{C}} = (u\mathfrak{m}, M)_{\mathbb{C}} \subset ((\Psi \cup \Lambda)_{\mathbb{C}}, M)_{\mathbb{C}} \\ &= (\Psi \cup \Lambda \cup M)_{\mathbb{C}}, \end{aligned}$$

so that  $\mathfrak{m}$  is finitely  $\mathbb{C}$ -generated. This contradiction proves the theorem.

**Corollary 1** *Let  $n \in \mathbb{N}$ ,  $n \neq 0$ , and consider the differential polynomial algebra  $\mathcal{S} = \mathcal{R}\{y_1, \dots, y_n\}$  over  $\mathcal{R}$ . A necessary and sufficient condition that the set of all perfect differential ideals of  $\mathcal{S}$  be a Noetherian conservative system is that the set of all perfect differential ideals of  $\mathcal{R}$  be a Noetherian conservative system and, for every prime differential ideal  $\mathfrak{p}$  of  $\mathcal{R}$ ,  $Q(\mathcal{R}/\mathfrak{p})$  be differentially quasi-perfect.*

*Proof* If the condition is satisfied, then every prime differential ideal of  $\mathcal{S}$  is quasi-separable over  $\mathcal{R}$ , and the theorem therefore applies to the conservative system formed by all the perfect differential ideals of  $\mathcal{S}$ .

Let the condition not be satisfied. If  $\mathfrak{f}$  is a perfect differential ideal of  $\mathcal{R}$ , then  $\mathcal{S}\mathfrak{f}$  is a perfect differential ideal of  $\mathcal{S}$  (see Chapter 0, Section 5), and  $\mathcal{S}\mathfrak{f} \cap \mathcal{R} = \mathfrak{f}$ . It follows that if the set of all perfect differential ideals of  $\mathcal{R}$  is not Noetherian, then neither is the set of all perfect differential ideals of  $\mathcal{S}$ . Therefore we may suppose that there exists a prime differential ideal  $\mathfrak{p}$  of  $\mathcal{R}$  such that the differential field  $\mathcal{F}_0 = Q(\mathcal{R}/\mathfrak{p})$  is not differentially quasi-perfect. Now,  $\mathcal{F}_0\{y_1, \dots, y_n\}$  is the differential ring of quotients of  $(\mathcal{R}/\mathfrak{p})\{y_1, \dots, y_n\}$  over the multiplicatively stable set of nonzero elements of  $\mathcal{R}/\mathfrak{p}$ , and  $(\mathcal{R}/\mathfrak{p})\{y_1, \dots, y_n\}$  is a homomorphic image of  $\mathcal{S}$ . It follows from Chapter 0, Section 9, Proposition 2 and its first corollary, that to prove that the set of all perfect differential ideals of  $\mathcal{S}$  is not Noetherian, it suffices to prove the same thing for  $\mathcal{F}_0\{y_1, \dots, y_n\}$ . Since  $\mathcal{F}_0$  is not differentially quasi-perfect we see by Chapter II, Section 3, Proposition 5, that the characteristic  $p$  of  $\mathcal{F}_0$  is not 0 and there exists an infinite sequence  $c_0, c_1, \dots, c_k, \dots$  of constants in  $\mathcal{F}_0$  such that  $c_k \notin \mathcal{F}_0^p(c_0, \dots, c_{k-1})$  for every  $k$ . Fixing some  $\delta \in \Delta$  we see that the ideals  $\mathfrak{q}_k = (y_1^p - c_0, (\delta y_1)^p - c_1, \dots, (\delta^k y_1)^p - c_k)$  of  $\mathcal{F}_0\{y_1, \dots, y_n\}$  form an infinite strictly increasing sequence; each  $\mathfrak{q}_k$  is obviously a differential ideal, and by Chapter 0, Section 3, Lemma 2, is prime (hence perfect).

**Corollary 2** *Let  $n \in \mathbb{N}$ ,  $n \neq 0$ . A necessary and sufficient condition that the set of all perfect differential ideals of the differential polynomial algebra  $\mathcal{F}\{y_1, \dots, y_n\}$  be a Noetherian conservative system, is that  $\mathcal{F}$  be differentially quasi-perfect.*

*Proof* This is a special case of Corollary 1.

**Corollary 3** *A finitely generated extension of a differentially quasi-perfect differential field is itself differentially quasi-perfect.*

*Proof* Let  $\mathcal{F}$  be differentially quasi-perfect and  $\mathcal{G} = \mathcal{F}\langle\alpha_1, \dots, \alpha_n\rangle$ . Let  $y_1, \dots, y_{n+1}, y$  be differential indeterminates and  $\Sigma$  be the set of non-zero elements of  $\mathcal{F}\langle\alpha_1, \dots, \alpha_n\rangle$ . There exists a surjective homomorphism  $\mathcal{F}\langle y_1, \dots, y_{n+1}\rangle \rightarrow \mathcal{F}\langle\alpha_1, \dots, \alpha_n, y\rangle$  over  $\mathcal{F}$ , and if  $\mathfrak{k}$  is its kernel, then  $\mathcal{F}\langle y_1, \dots, y_{n+1}\rangle/\mathfrak{k} \approx \mathcal{F}\langle\alpha_1, \dots, \alpha_n, y\rangle$ . Also,  $\Sigma^{-1}\mathcal{F}\langle\alpha_1, \dots, \alpha_n, y\rangle = \mathcal{G}\langle y\rangle$ . By Corollary 2,  $\mathcal{F}\langle y_1, \dots, y_{n+1}\rangle$  has the property that the set of all its perfect differential ideals is a Noetherian conservative system. By the above and Chapter 0, Section 9, Corollary 1 to Proposition 2,  $\mathcal{G}\langle y\rangle$  has the same property. Hence, by Corollary 2,  $\mathcal{G}$  is differentially quasi-perfect.

**Corollary 4** *Let  $n \in \mathbb{N}$  and let  $\mathfrak{p}$  be a prime differential ideal of  $\mathcal{F}\langle y_1, \dots, y_n\rangle$ . If  $\mathfrak{p}$  is quasi-perfect over  $\mathcal{F}$ , then  $\mathfrak{p} = \{\Phi\}$  for some finite set  $\Phi \subset \mathfrak{p}$ .*

*Proof* By Section 3, Proposition 1, there is a finitely generated extension  $\mathcal{F}_0$  of the prime field such that if we set  $\mathfrak{p}_0 = \mathfrak{p} \cap \mathcal{F}_0\langle y_1, \dots, y_n\rangle$ , then  $\mathfrak{p} = \mathcal{F}\mathfrak{p}_0$ . By Corollary 3,  $\mathcal{F}_0$  is differentially quasi-perfect; hence by Corollary 2 there is a finite set  $\Phi \subset \mathfrak{p}_0$  such that  $\mathfrak{p}_0 = \{\Phi\}_{\mathcal{F}_0\langle y_1, \dots, y_n\rangle}$ . Then

$$\begin{aligned} \mathfrak{p} &= \{\Phi\}_{\mathcal{F}\langle y_1, \dots, y_n\rangle} \supset \mathcal{F} \cdot \{\{\Phi\}_{\mathcal{F}_0\langle y_1, \dots, y_n\rangle} \cap \mathcal{F}_0\langle y_1, \dots, y_n\rangle\} \\ &= \mathcal{F} \cdot \{\Phi\}_{\mathcal{F}_0\langle y_1, \dots, y_n\rangle} = \mathcal{F}\mathfrak{p}_0 = \mathfrak{p}, \end{aligned}$$

whence  $\mathfrak{p} = \{\Phi\}_{\mathcal{F}\langle y_1, \dots, y_n\rangle}$ .

**Corollary 5** *Let  $n \in \mathbb{N}$ . The set of all  $\mathcal{F}$ -separable differential ideals of  $\mathcal{F}\langle y_1, \dots, y_n\rangle$  is a Noetherian conservative system. If  $\mathfrak{a}$  is any  $\mathcal{F}$ -separable differential ideal of  $\mathcal{F}\langle y_1, \dots, y_n\rangle$ , then  $\mathfrak{a} = \{\Phi\}$  for some finite set  $\Phi \subset \mathfrak{a}$ .*

*Proof* Every prime  $\mathcal{F}$ -separable differential ideal is quasi-separable over  $\mathcal{F}$ , so the first assertion follows from the theorem. Therefore  $\mathfrak{a} = \mathfrak{p}_1 \cap \dots \cap \mathfrak{p}_r$ , where each  $\mathfrak{p}_k$  is an  $\mathcal{F}$ -separable prime differential ideal, and by Corollary 4,  $\mathfrak{p}_k = \{\Phi_k\}$  for a finite set  $\Phi_k \subset \mathfrak{p}_k$ . Hence by Chapter 0, Section 8, Lemma 7,  $\mathfrak{a} = \{\Phi_1\} \cap \dots \cap \{\Phi_r\} = \{\Phi_1 \cdots \Phi_r\}$ .

**REMARK** The first result in the direction of a basis theorem was obtained by Ritt [79, 81]. Working with a differential field  $\mathcal{F}$  of functions meromorphic in a region, and using the language of differential equations, he proved (a) that if  $\Sigma$  is a subset of  $\mathcal{F}\langle y_1, \dots, y_n\rangle$ , then the system of differential equations  $G = 0$  ( $G \in \Sigma$ ) is equivalent to (has the same solutions as) a finite subsystem, and (b) that if for an element  $F \in \mathcal{F}\langle y_1, \dots, y_n\rangle$  every solution of the above system is a solution of the differential equation  $F = 0$ , then some power of  $F$  is in  $[\Sigma]$ . (We shall take up this point of view in Chapter IV.) This led Raudenbush [73] to formalize the notion of perfect differential ideal

and to prove for an abstract differential field  $\mathcal{F}$  of characteristic 0 that every perfect differential ideal of  $\mathcal{F}\langle y_1, \dots, y_n\rangle$  has a basis. The same conclusion was obtained by Kolchin [37] for more general coefficient domains (including any perfect differential field, and also certain differential rings); in the same paper a counterexample was given for a nonperfect differential field  $\mathcal{F}$ . It was Seidenberg [108] who reestablished the Raudenbush result for an arbitrary differential field  $\mathcal{F}$  by requiring that the perfect differential ideals be separable over  $\mathcal{F}$ , that is, who first proved the first part of Corollary 5 above.

## EXERCISES

1. Let  $\Lambda_n$  denote the set of all  $\mathcal{F}$ -separable prime differential ideals of  $\mathcal{F}\langle y_1, \dots, y_n\rangle$ . Show that  $\text{Card } \Lambda_n = \max(\aleph_0, \text{Card } \mathcal{F})$ . Corollary: If  $\mathcal{S}$  is a semiuniversal extension of  $\mathcal{F}$  (see Chapter II, Section 2), then there exists a family  $(\mathcal{E}_\lambda)_{\lambda \in \Lambda}$  of differential subfields of  $\mathcal{S}$  such that each  $\mathcal{E}_\lambda$  is a finitely generated separable extension of  $\mathcal{F}$ , every finitely generated separable extension of  $\mathcal{F}$  is  $\mathcal{F}$ -isomorphic to some  $\mathcal{E}_\lambda$ , and  $\text{Card } \Lambda = \max(\aleph_0, \text{Card } \mathcal{F})$ .
2. Show that  $\mathcal{F}$  always has a separable semiuniversal extension  $\mathcal{S}$  such that  $\text{Card } \mathcal{S} = \max(\aleph_0, \text{Card } \mathcal{F})$ .

## 5 Differential dimension polynomials

Let  $\mathfrak{p}$  be a prime differential ideal of a finitely generated differential polynomial algebra  $\mathcal{F}\langle y_1, \dots, y_n\rangle$  over  $\mathcal{F}$ . The canonical homomorphism of  $\mathcal{F}\langle y_1, \dots, y_n\rangle$  into  $Q(\mathcal{F}\langle y_1, \dots, y_n\rangle/\mathfrak{p})$  maps  $(y_1, \dots, y_n)$  onto a family  $\bar{y} = (\bar{y}_1, \dots, \bar{y}_n)$ , and maps  $\mathcal{F}$  isomorphically onto a differential field that we may thus identify with  $\mathcal{F}$ . After this identification  $Q(\mathcal{F}\langle y_1, \dots, y_n\rangle/\mathfrak{p})$  may be written as  $\mathcal{F}\langle \bar{y}\rangle = \mathcal{F}\langle \bar{y}_1, \dots, \bar{y}_n\rangle$ , and the canonical homomorphism becomes the substitution of  $(\bar{y}_1, \dots, \bar{y}_n)$  for  $(y_1, \dots, y_n)$ . The differential inseparability polynomial  $\omega_{\bar{y}/\mathcal{F}}$  of  $\bar{y}$  over  $\mathcal{F}$  (see Chapter II, Section 12) we now call the *differential inseparability polynomial* of  $\mathfrak{p}$ , and we denote it by  $\omega_{\mathfrak{p}}$ . We have at our disposal in connection with  $\omega_{\mathfrak{p}}$  all the results of Chapter II, Sections 12 and 13. In particular,  $\omega_{\mathfrak{p}}$  is a numerical polynomial with  $\deg \omega_{\mathfrak{p}} \leq m$  (the cardinal number of the set  $\Delta$  of derivation operators), and if we write  $\omega_{\mathfrak{p}} = \sum_{0 \leq i \leq m} a_i (X_i^{+i})$ , then the coefficient  $a_m$  is the differential inseparability degree of  $\mathcal{F}\langle \bar{y}\rangle$  over  $\mathcal{F}$ ; we call this number the *differential inseparability degree* of  $\mathfrak{p}$ . The differential type  $\tau$  of  $\mathcal{F}\langle \bar{y}\rangle$  over  $\mathcal{F}$  (see Chapter II, Section 13), which is defined as  $\tau = \deg \omega_{\mathfrak{p}}$ , we now call the *differential type* of  $\mathfrak{p}$ . The typical differential inseparability degree  $a_i$  of

$\mathcal{F}\langle\bar{y}\rangle$  over  $\mathcal{F}$  we now call the *typical differential inseparability degree* of  $\mathfrak{p}$ .

If  $\mathfrak{p}$  is separable over  $\mathcal{F}$ , we also call  $\omega_{\mathfrak{p}}$  the *differential dimension polynomial* of  $\mathfrak{p}$ , call  $a_m$  the *differential dimension* of  $\mathfrak{p}$ , and call  $a_i$  the *typical differential dimension* of  $\mathfrak{p}$ . Since for a separable finitely generated field extension the notions of inseparability degree and transcendence degree coincide, we see by Chapter II, Section 12, Theorem 6, that if for each  $s \in \mathbb{N}$  we let  $\mathfrak{p}_s$  denote the polynomial ideal  $\mathfrak{p} \cap \mathcal{F}[(\theta y_j)_{\theta \in \Theta(s), 1 \leq j \leq n}]$ , then  $\omega_{\mathfrak{p}}(s) = \dim \mathfrak{p}_s$  for all sufficiently big  $s \in \mathbb{N}$ .

**Proposition 2** Let  $\mathfrak{p}$  and  $\mathfrak{p}'$  be  $\mathcal{F}$ -separable prime differential ideals of a finitely generated differential polynomial algebra  $\mathcal{F}\{y_1, \dots, y_n\}$  over  $\mathcal{F}$ , with  $\mathfrak{p} \subset \mathfrak{p}'$  and  $\mathfrak{p} \neq \mathfrak{p}'$ . Then  $\omega_{\mathfrak{p}} > \omega_{\mathfrak{p}'}$ .

*Proof* For each  $s \in \mathbb{N}$  let  $\mathfrak{p}_s$ , respectively  $\mathfrak{p}'_s$ , denote the prime polynomial ideal  $\mathfrak{p} \cap \mathcal{F}[(\theta y_j)_{\theta \in \Theta(s), 1 \leq j \leq n}]$ , respectively  $\mathfrak{p}' \cap \mathcal{F}[(\theta y_j)_{\theta \in \Theta(s), 1 \leq j \leq n}]$ . Since  $\mathfrak{p}$  and  $\mathfrak{p}'$  are separable, for all sufficiently big values of  $s$ ,  $\omega_{\mathfrak{p}}(s) = \dim \mathfrak{p}_s$  and  $\omega_{\mathfrak{p}'}(s) = \dim \mathfrak{p}'_s$ . However, for all big values of  $s$ ,  $\mathfrak{p}_s \subset \mathfrak{p}'_s$  and  $\mathfrak{p}_s \neq \mathfrak{p}'_s$ , so that (by Chapter 0, Section 11, Proposition 4)  $\omega_{\mathfrak{p}}(s) > \omega_{\mathfrak{p}'}(s)$ . Therefore  $\omega_{\mathfrak{p}} > \omega_{\mathfrak{p}'}$ .

The proposition becomes false if the hypothesis of separability is omitted (see Exercise 1 below).

### EXERCISE

- Let  $p \neq 0$ , let  $\Lambda$  be any subset of  $\Theta$ , let  $(c_{\theta})_{\theta \in \Lambda}$  be a family of constants in  $\mathcal{F}$  separably independent over  $\mathcal{F}^p$ , and let  $\mathfrak{p}(\Lambda)$  denote the ideal  $((\theta y)^p + c_{\theta})_{\theta \in \Lambda}$  of  $\mathcal{F}\{y\}$ . Show that  $\mathfrak{p}(\Lambda)$  is a prime differential ideal and that  $\omega_{\mathfrak{p}(\Lambda)} = \binom{x+m}{m}$ , where  $m = \text{Card } \Lambda$ .

### 6 Extension of the differential field of coefficients

Let  $\mathcal{G}$  be an extension of  $\mathcal{F}$  and let  $(y_i)_{i \in I}$  be a family of differential indeterminates over  $\mathcal{G}$ . We are interested in the behavior of a perfect differential ideal  $\mathfrak{a}$  of  $\mathcal{F}\{(y_i)_{i \in I}\}$  when  $\mathcal{F}$  is extended to  $\mathcal{G}$ , that is, we ask about the nature of the differential ideal  $\mathcal{G}\mathfrak{a}$  of  $\mathcal{G}\{(y_i)_{i \in I}\}$ . The question reduces, in a certain sense, to the case in which  $\mathfrak{a}$  is prime. Indeed, if  $\Pi$  is the set of components of  $\mathfrak{a}$ , then (by Chapter 0, Section 8, Proposition 1)  $\mathfrak{a} = \bigcap_{\mathfrak{p} \in \Pi} \mathfrak{p}$ ; if  $F \in \mathcal{G}\mathfrak{a}$  and we write  $F = \sum \gamma_k F_k$ , where each  $F_k \in \mathcal{F}\{(y_i)_{i \in I}\}$  and  $(\gamma_k)$  is a basis of  $\mathcal{G}$  over  $\mathcal{F}$ , then by Chapter 0, Section 10, Lemma 9,  $F \in \mathfrak{a}$  if and only if each  $F_k \in \mathfrak{a} = \bigcap_{\mathfrak{p} \in \Pi} \mathfrak{p}$ , that is, each  $F_k \in \mathfrak{p}$  ( $\mathfrak{p} \in \Pi$ ), that is,  $F \in \mathcal{G}\mathfrak{p}$  for every  $\mathfrak{p} \in \Pi$ ; thus,  $\mathcal{G}\mathfrak{a} = \bigcap_{\mathfrak{p} \in \Pi} \mathcal{G}\mathfrak{p}$ . The situation is especially good in this respect when  $I$  is finite and  $\mathfrak{a}$  is separable over  $\mathcal{F}$ , for then (by

Section 4, Corollary 5 to Theorem 1, and by Chapter 0, Section 9, Theorem 1)  $\Pi$  is finite and each  $\mathfrak{p} \in \Pi$  is separable over  $\mathcal{F}$ .

**Proposition 3** Let  $\mathfrak{p}$  be an  $\mathcal{F}$ -separable prime differential ideal of a finitely generated differential polynomial algebra  $\mathcal{F}\{y_1, \dots, y_n\}$  over  $\mathcal{F}$ , and let  $\mathcal{G}$  be an extension of  $\mathcal{F}$ .

(a)  $\mathcal{G}\mathfrak{p}$  is a  $\mathcal{G}$ -separable differential ideal of  $\mathcal{G}\{y_1, \dots, y_n\}$ . If  $\mathfrak{p}$  is regular over  $\mathcal{F}$ , then  $\mathcal{G}\mathfrak{p}$  is regular over  $\mathcal{G}$ .

(b)  $\mathcal{G}\mathfrak{p}$  has finitely many components, and each of them is a  $\mathcal{G}$ -separable prime differential ideal. If  $\mathfrak{p}'$  is any one of them, then  $\mathfrak{p}' \cap \mathcal{F}\{y_1, \dots, y_n\} = \mathfrak{p}$ , and  $\omega_{\mathfrak{p}'} = \omega_{\mathfrak{p}}$ .

(c) There exist, independent of  $\mathcal{G}$ , an irreducible polynomial  $P$  with coefficients in  $\mathcal{F}$  and with some partial derivative not equal to 0, and a differential polynomial  $H \in \mathcal{F}\{y_1, \dots, y_n\}$  with  $H \notin \mathfrak{p}$ , such that for each extension  $\mathcal{G}$  of  $\mathcal{F}$ , the number of components of  $\mathcal{G}\mathfrak{p}$  equals the number of irreducible factors into which  $P$  splits over  $\mathcal{G}$ , and the sum of any two distinct components of  $\mathcal{G}\mathfrak{p}$  contains  $H$ .

*Proof* For each  $s \in \mathbb{N}$  let

$$A_s = \mathcal{F}[(\theta y_j)_{\theta \in \Theta(s), 1 \leq j \leq n}], \quad B_s = \mathcal{G}[(\theta y_j)_{\theta \in \Theta(s), 1 \leq j \leq n}].$$

It is obvious that  $\mathcal{G}\mathfrak{p}$  is a differential ideal. Hence (a) follows from Chapter 0, Section 12, Proposition 7.

By Section 4, Corollary 5 to Theorem 1, and by Chapter 0, Section 9, Theorem 1,  $\mathcal{G}\mathfrak{p}$  has finitely many components  $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ , these are  $\mathcal{G}$ -separable prime differential ideals, and  $\mathcal{G}\mathfrak{p} = \mathfrak{p}_1 \cap \dots \cap \mathfrak{p}_r$ . It is an easy consequence of Chapter 0, Section 10, Lemma 9, that  $\mathcal{G} \cdot (\mathfrak{p} \cap A_s) = (\mathcal{G}\mathfrak{p}) \cap B_s$ , so that

$$\mathcal{G} \cdot (\mathfrak{p} \cap A_s) = (\mathfrak{p}_1 \cap B_s) \cap \dots \cap (\mathfrak{p}_r \cap B_s).$$

No one of the ideals  $\mathfrak{p}_1, \dots, \mathfrak{p}_r$  contains any other so that if  $s$  is sufficiently big, no one of the prime ideals  $\mathfrak{p}_1 \cap B_s, \dots, \mathfrak{p}_r \cap B_s$  contains another, and hence these must be the components of  $\mathcal{G} \cdot (\mathfrak{p} \cap A_s)$ . By Chapter 0, Section 12, Proposition 7, then  $(\mathfrak{p}_i \cap B_s) \cap A_s = \mathfrak{p} \cap A_s$ , whence  $\mathfrak{p}_i \cap \mathcal{F}\{y_1, \dots, y_n\} = \mathfrak{p}$ , and  $\dim(\mathfrak{p}_i \cap B_s) = \dim(\mathfrak{p} \cap A_s)$ . For sufficiently big values of  $s$  the last equation is equivalent to the equation  $\omega_{\mathfrak{p}_i}(s) = \omega_{\mathfrak{p}}(s)$ , so that  $\omega_{\mathfrak{p}_i} = \omega_{\mathfrak{p}}$ . This proves (b).

To prove (c) let  $s(\mathcal{G})$  denote the smallest natural number such that no one of the ideals  $\mathfrak{p}_1 \cap B_{s(\mathcal{G})}, \dots, \mathfrak{p}_r \cap B_{s(\mathcal{G})}$  contains any other. Then for every  $s \geq s(\mathcal{G})$ , the ideals  $\mathfrak{p}_1 \cap B_s, \dots, \mathfrak{p}_r \cap B_s$  are the components of  $\mathcal{G} \cdot (\mathfrak{p} \cap A_s)$ . We shall show below that  $s(\mathcal{G})$  is an increasing function of  $\mathcal{G}$ , that is, whenever  $\mathcal{G}$  and  $\mathcal{H}$  are extensions of  $\mathcal{F}$  with  $\mathcal{G} \subset \mathcal{H}$ , then  $s(\mathcal{G}) \leq s(\mathcal{H})$ . Assuming this result, let us see how we can prove (c). We may suppose that  $\mathfrak{p} \neq (0)$ ,

for otherwise (c) becomes trivial. By Chapter 0, Section 12, Proposition 7(b), for each  $s \in \mathbb{N}$  there exists an irreducible polynomial  $P_s$  with coefficients in  $\mathcal{F}$  and with some partial derivative not equal to 0, such that for any  $\mathcal{G}$  the number of components of  $\mathcal{G} \cdot (\mathfrak{p} \cap A_s)$  equals the number of irreducible factors into which  $P_s$  splits over  $\mathcal{G}$ . Let  $\mathcal{F}_0$  denote the separable closure of  $\mathcal{F}$  in  $\mathcal{G}$ , let  $\mathcal{F}'$  denote a separable closure of  $\mathcal{F}_0$  (and therefore of  $\mathcal{F}$ ), and set  $P = P_{s(\mathcal{F}')}.$  If  $\mathfrak{p}_{01}, \dots, \mathfrak{p}_{0q}$  denote the components of  $\mathcal{F}_0 \mathfrak{p}$ , then  $\mathcal{G}\mathfrak{p}_{01}, \dots, \mathcal{G}\mathfrak{p}_{0q}$  are prime (by Chapter 0, Section 12, Proposition 7(c)). As no  $\mathcal{G}\mathfrak{p}_{0i}$  contains any other (by Chapter 0, Section 10, Lemma 9), they are the components of  $\mathcal{G}\mathfrak{p}$ . Thus, the number of components of  $\mathcal{G}\mathfrak{p}$  equals that of  $\mathcal{F}_0 \mathfrak{p}$ . By the result we are assuming  $s(\mathcal{F}_0) \leq s(\mathcal{F}')$ , so that the number of components of  $\mathcal{F}_0 \mathfrak{p}$  equals that of  $\mathcal{F}_0 \cdot (\mathfrak{p} \cap A_{s(\mathcal{F}')}),$  which by the above equals the number of irreducible factors of  $P$  over  $\mathcal{F}_0$ . However, by Chapter 0, Section 12, Lemma 12, this last number equals the number of irreducible factors of  $P$  over  $\mathcal{G}$ . Finally, by Chapter 0, Section 12, Proposition 7(b), there exists an  $H \in A_{s(\mathcal{F}')}.$  with  $H \notin \mathfrak{p} \cap A_{s(\mathcal{F}')}.$  such that  $H$  is contained in the sum of any two distinct components of  $\mathcal{G} \cdot (\mathfrak{p} \cap A_{s(\mathcal{F}')}).$  However, the components of  $\mathcal{G} \cdot (\mathfrak{p} \cap A_{s(\mathcal{F}')}.)$  are the intersections with  $B_{s(\mathcal{F}')}.$  of the components of  $\mathcal{G}\mathfrak{p}.$  Thus,  $H \notin \mathfrak{p}$  and  $H$  is contained in the sum of any two distinct components of  $\mathcal{G}\mathfrak{p}.$

We now show that  $s(\mathcal{G})$  is an increasing function of  $\mathcal{G}.$  Let  $\mathcal{H}$  be an extension of  $\mathcal{G}$  and set  $C_s = \mathcal{H}[(\theta y_j)_{\theta \in \Theta(s), 1 \leq j \leq n}].$  Then  $\mathcal{H}\mathfrak{p} = \mathcal{H} \cdot \mathcal{G}\mathfrak{p} = \mathcal{H} \cdot (\mathfrak{p}_1 \cap \dots \cap \mathfrak{p}_r) = \mathcal{H}\mathfrak{p}_1 \cap \dots \cap \mathcal{H}\mathfrak{p}_r.$  If  $i \neq i',$  then a component  $\mathfrak{q}$  of  $\mathcal{H}\mathfrak{p}_i$  cannot be contained in a component  $\mathfrak{q}'$  of  $\mathcal{H}\mathfrak{p}_{i'},$  for otherwise we should have  $\mathfrak{p}_i = \mathfrak{q} \cap \mathcal{G}\{y_1, \dots, y_n\} \subset \mathfrak{q}' \cap \mathcal{G}\{y_1, \dots, y_n\} = \mathfrak{p}_{i'}$ . Therefore if  $\mathfrak{p}_{i1}, \dots, \mathfrak{p}_{iq_i}$  denote the components of  $\mathcal{H}\mathfrak{p}_i.$  ( $1 \leq i \leq r$ ), then the ideals  $\mathfrak{p}_{ij}$  ( $1 \leq i \leq r,$   $1 \leq j \leq q_i$ ) are the components of  $\mathcal{H}\mathfrak{p}.$  If  $s < s(\mathcal{G}),$  there exist indices  $i, i'$  with  $i \neq i'$  such that  $\mathfrak{p}_i \cap B_s \subset \mathfrak{p}_{i'} \cap B_s.$  For these  $i, i'$  we have

$$\begin{aligned} (\mathfrak{p}_{i1} \cap C_s) \cap \dots \cap (\mathfrak{p}_{iq_i} \cap C_s) &= \mathcal{H}\mathfrak{p}_i \cap C_s = \mathcal{H} \cdot (\mathfrak{p}_i \cap B_s) \subset \mathcal{H} \cdot (\mathfrak{p}_{i'} \cap B_s) \\ &= \mathcal{H}\mathfrak{p}_{i'} \cap C_s \subset \mathfrak{p}_{i'1} \cap C_s, \end{aligned}$$

so that, for some  $j,$   $\mathfrak{p}_{ij} \cap C_s \subset \mathfrak{p}_{i'1} \cap C_s$  whence  $s < s(\mathcal{H}).$  Thus, whenever  $s < s(\mathcal{G}),$  then  $s < s(\mathcal{H}),$  so that  $s(\mathcal{G}) \leq s(\mathcal{H}).$

**Corollary** Let  $(y_i)_{i \in I}$  be a family of differential indeterminates, let  $(I_\lambda)_{\lambda \in \Lambda}$  be a partition of  $I,$  for each  $\lambda \in \Lambda$  let  $\mathfrak{p}_\lambda$  be an  $\mathcal{F}$ -regular differential ideal of  $\mathcal{F}\{(y_i)_{i \in I_\lambda}\},$  and let  $\mathfrak{r}$  be the ideal of  $\mathcal{F}\{(y_i)_{i \in I}\}$  generated by  $\bigcup_{\lambda \in \Lambda} \mathfrak{p}_\lambda.$  Then  $\mathfrak{r}$  is an  $\mathcal{F}$ -regular differential ideal with  $\mathfrak{r} \cap \mathcal{F}\{(y_i)_{i \in I_\lambda}\} = \mathfrak{p}_\lambda$  ( $\lambda \in \Lambda$ ). If  $I$  is finite, then  $\omega_\mathfrak{r} = \sum_{\lambda \in \Lambda} \omega_{\mathfrak{p}_\lambda}.$

*Proof* It is obvious that  $\mathfrak{r}$  is a differential ideal. By Chapter 0, Section 12, Corollary 2 to Proposition 7,  $\mathfrak{r}$  is  $\mathcal{F}$ -regular and  $\mathfrak{r} \cap \mathcal{F}\{(y_i)_{i \in I_\lambda}\} = \mathfrak{p}_\lambda$  ( $\lambda \in \Lambda$ ). For the final part we may suppose that  $\Lambda$  consists of two elements,

say the numbers 1 and 2. Let  $\bar{y} = (\bar{y}_i)_{i \in I}$  denote the image of  $y = (y_i)_{i \in I}$  under the canonical homomorphism  $\mathcal{F}\{y\} \rightarrow \mathcal{F}\{y\}/\mathfrak{r},$  so that  $\bar{y}_i \in Q(\mathcal{F}\{y\}/\mathfrak{r})$  and  $\mathfrak{r}$  is the defining differential ideal of  $\bar{y}$  over  $\mathcal{F}.$  Setting  $\bar{y}' = (\bar{y}_i)_{i \in I_1}$  and  $\bar{y}'' = (\bar{y}_i)_{i \in I_2},$  we see that  $\mathfrak{r} \cap \mathcal{F}\{(y_i)_{i \in I_1}\} = \mathfrak{p}_1$  is the defining differential ideal of  $\bar{y}'$  over  $\mathcal{F}$  and  $\mathfrak{p}_2$  is that of  $\bar{y}''$  over  $\mathcal{F}.$  Also, the defining differential ideal of  $\bar{y}''$  over  $\mathcal{F}\langle \bar{y}' \rangle$  is the  $\mathcal{F}\langle \bar{y}' \rangle$ -regular ideal  $\mathcal{F}\langle \bar{y}' \rangle \mathfrak{p}_2.$  Now,

$$\begin{aligned} \text{tr deg } \mathcal{F}((\theta \bar{y}_i)_{\theta \in \Theta(s), i \in I})/\mathcal{F} &= \text{tr deg } \mathcal{F}((\theta \bar{y}_i)_{\theta \in \Theta(s), i \in I_1})/\mathcal{F} \\ &\quad + \text{tr deg } \mathcal{F}((\theta \bar{y}_i)_{\theta \in \Theta(s), i \in I_2})/\mathcal{F}((\theta \bar{y}_i)_{\theta \in \Theta(s), i \in I_1}). \end{aligned}$$

For big values of  $s \in \mathbb{N}$  the first term of the second member here equals  $\omega_{\mathfrak{p}_1}(s),$  whereas the second term is less than or equal to  $\text{tr deg } \mathcal{F}((\theta \bar{y}_i)_{\theta \in \Theta(s), i \in I_2})/\mathcal{F} = \omega_{\mathfrak{p}_2}(s)$  and is greater than or equal to  $\text{tr deg } \mathcal{F}\langle \bar{y}' \rangle((\theta \bar{y}_i)_{\theta \in \Theta(s), i \in I_2})/\mathcal{F}\langle \bar{y}' \rangle = \omega_{\mathcal{F}\langle \bar{y}' \rangle \mathfrak{p}_2}(s) = \omega_{\mathfrak{p}_2}(s).$  Hence  $\omega_\mathfrak{r}(s) = \omega_{\mathfrak{p}_1}(s) + \omega_{\mathfrak{p}_2}(s).$

## 7 Universal extensions

Let  $\mathcal{U}$  be an extension of  $\mathcal{F}.$  We shall say that  $\mathcal{U}$  is *universal* over  $\mathcal{F},$  or that  $\mathcal{U}$  is a *universal extension* of  $\mathcal{F},$  if  $\mathcal{U}$  is semiuniversal (see Chapter II, Section 2, especially the Corollary to Proposition 4) over every finitely generated extension of  $\mathcal{F}$  in  $\mathcal{U}.$  By a *universal differential field* we shall mean a differential field that is universal over its prime field.

Our results on universal extensions depend on the following lemma on semiuniversal extensions.

**Lemma 2** Let  $\mathcal{F}, \mathcal{F}', \mathcal{S}', \mathcal{S}$  be differential fields with  $\mathcal{F} \subset \mathcal{F}' \subset \mathcal{S}' \subset \mathcal{S}.$  If  $\mathcal{S}'$  is semiuniversal over  $\mathcal{F}',$  then  $\mathcal{S}$  is semiuniversal over  $\mathcal{F}.$

*Proof* Let  $\mathfrak{p}$  be any  $\mathcal{F}$ -separable prime differential ideal of  $\mathcal{F}\{y_1, \dots, y_n\}.$  By Section 6, Proposition 3,  $\mathcal{F}'\mathfrak{p}$  is an  $\mathcal{F}'$ -separable differential ideal, and has a component  $\mathfrak{p}'$  that is an  $\mathcal{F}'$ -separable prime differential ideal with  $\mathfrak{p}' \cap \mathcal{F}'\{y_1, \dots, y_n\} = \mathfrak{p}.$  Because  $\mathcal{S}'$  is semiuniversal over  $\mathcal{F}',$  there exist elements  $\eta_1, \dots, \eta_n \in \mathcal{S}' \subset \mathcal{S}$  such that  $\mathfrak{p}'$  is the defining differential ideal of  $(\eta_1, \dots, \eta_n)$  in  $\mathcal{F}'\{y_1, \dots, y_n\}.$  Then  $\mathfrak{p} = \mathfrak{p}' \cap \mathcal{F}\{y_1, \dots, y_n\}$  is the defining differential ideal of  $(\eta_1, \dots, \eta_n)$  in  $\mathcal{F}\{y_1, \dots, y_n\}.$  Thus,  $\mathcal{S}$  is semiuniversal over  $\mathcal{F}.$

**Proposition 4** Let  $\mathcal{F}, \mathcal{F}', \mathcal{U}$  be differential fields with  $\mathcal{F} \subset \mathcal{F}' \subset \mathcal{U}.$

- If  $\mathcal{U}$  is universal over  $\mathcal{F}',$  then  $\mathcal{U}$  is universal over  $\mathcal{F}.$
- If  $\mathcal{U}$  is universal over  $\mathcal{F},$  and  $\mathcal{F}'$  is finitely generated over  $\mathcal{F},$  then  $\mathcal{U}$  is universal over  $\mathcal{F}'.$



*Proof* (a) Let  $\mathcal{F}_1$  be a finitely generated extension of  $\mathcal{F}$  in  $\mathcal{U}$ . We must show that  $\mathcal{U}$  is semiuniversal over  $\mathcal{F}_1$ . Now,  $\mathcal{F}'\mathcal{F}_1$  is finitely generated over  $\mathcal{F}'$ . Since  $\mathcal{U}$  is universal over  $\mathcal{F}'$ , then  $\mathcal{U}$  is semiuniversal over  $\mathcal{F}'\mathcal{F}_1$ . By Lemma 2 then  $\mathcal{U}$  is semiuniversal over  $\mathcal{F}_1$ .

(b) If  $\mathcal{F}'_1$  is a finitely generated extension of  $\mathcal{F}'$  in  $\mathcal{U}$ , then  $\mathcal{F}'_1$  is also finitely generated over  $\mathcal{F}$ , so that  $\mathcal{U}$  is semiuniversal over  $\mathcal{F}'_1$ .

We have the following existence theorem for universal extensions.

**Theorem 2** Every differential field has a separable universal extension.

*Proof* Let  $\mathcal{F}$  be the differential field. By Chapter II, Section 2, Corollary to Proposition 4, there exists an infinite sequence  $(\mathcal{L}_k)_{k \in \mathbb{N}}$  of differential fields such that  $\mathcal{L}_0 = \mathcal{F}$  and  $\mathcal{L}_{k+1}$  is a separable semiuniversal extension of  $\mathcal{L}_k$  ( $k \in \mathbb{N}$ ). Then  $\mathcal{U} = \bigcup_{k \in \mathbb{N}} \mathcal{L}_k$  has a unique differential field structure for which  $\mathcal{U}$  is an extension of every  $\mathcal{L}_k$ . It is obvious that  $\mathcal{U}$  is separable over  $\mathcal{F}$ . Let  $\mathcal{F}_1$  be any finitely generated extension of  $\mathcal{F}$  in  $\mathcal{U}$ . There exists a  $k \in \mathbb{N}$  such that  $\mathcal{F}_1 \subset \mathcal{L}_k$ . Then  $\mathcal{F}_1 \subset \mathcal{L}_k \subset \mathcal{L}_{k+1} \subset \mathcal{U}$  and  $\mathcal{L}_{k+1}$  is semiuniversal over  $\mathcal{L}_k$ . By Lemma 2 it follows that  $\mathcal{U}$  is semiuniversal over  $\mathcal{F}_1$ . Thus,  $\mathcal{U}$  is a separable universal extension of  $\mathcal{F}$ .

### EXERCISES

- Let  $\mathcal{U}$  be a universal extension of  $\mathcal{F}$ .
  - Show that  $\mathcal{U}$  is separably closed.
  - Show that if  $\mathcal{F}'$  is an algebraic extension of  $\mathcal{F}$  in  $\mathcal{U}$ , then  $\mathcal{U}$  is universal over  $\mathcal{F}'$ .
- Let  $\mathcal{U}$  be a universal extension of  $\mathcal{F}$ . Let  $\mathcal{F}_n$  ( $n \in \mathbb{N}$ ) and  $\mathcal{G}$  be differential fields such that  $\mathcal{F}_0 = \mathcal{F}$ ,  $\mathcal{F}_{n+1}$  is a finitely generated separable extension of  $\mathcal{F}_n$  ( $n \in \mathbb{N}$ ), and  $\mathcal{G} = \bigcup_{n \in \mathbb{N}} \mathcal{F}_n$ . Prove that there exists an  $\mathcal{F}$ -homomorphism  $\mathcal{G} \rightarrow \mathcal{U}$ .
- Let  $\mathcal{U}$  be a universal extension of  $\mathcal{F}$ , let  $\mathcal{H}$  be a finitely generated extension of  $\mathcal{F}$  in  $\mathcal{U}$ , and let  $\mathcal{G}$  be a finitely generated separable extension of  $\mathcal{F}$ . Show that there exists in  $\mathcal{U}$  an extension  $\mathcal{G}'$  of  $\mathcal{F}$  that is  $\mathcal{F}$ -isomorphic to  $\mathcal{G}$  such that the compositum  $\mathcal{H}\mathcal{G}'$  is a finitely generated separable extension of  $\mathcal{H}$ . (*Hint*: Write  $\mathcal{G} = \mathcal{F}\langle \eta_1, \dots, \eta_n \rangle$ , let  $\mathfrak{p}$  be the defining differential ideal of  $(\eta_1, \dots, \eta_n)$  over  $\mathcal{F}$ , and consider  $\mathcal{H}\mathfrak{p}$ .)
- Let  $\mathcal{U}$  be a universal extension of  $\mathcal{F}$ , let  $\mathcal{F}_0, \mathcal{F}_1, \dots, \mathcal{F}_n$  be differential subfields of  $\mathcal{U}$  such that  $\mathcal{F}_0 = \mathcal{F}$  and  $\mathcal{F}_j$  is a finitely generated extension of  $\mathcal{F}_{j-1}$  ( $1 \leq j \leq n$ ), and let  $\mathcal{G}_j$  be a finitely generated separable extension of  $\mathcal{F}_j$  ( $0 \leq j \leq n$ ). Show that there exist differential subfields  $\mathcal{G}'_0, \mathcal{G}'_1, \dots, \mathcal{G}'_n$  of  $\mathcal{U}$  such that  $\mathcal{G}'_j$  is an extension of  $\mathcal{F}_j$  that is  $\mathcal{F}_j$ -isomorphic to  $\mathcal{G}_j$

( $0 \leq j \leq n$ ) and the compositum  $\mathcal{G}'_0\mathcal{G}'_1 \dots \mathcal{G}'_n$  is a finitely generated separable extension of  $\mathcal{F}_n$ . (*Hint*: Use induction and Exercise 3.)

- Prove: If  $\mathcal{F}$  is denumerable, then  $\mathcal{F}$  has a denumerable separable universal extension  $\mathcal{U}_*$  such that every universal extension of  $\mathcal{F}$  contains an  $\mathcal{F}$ -isomorphic image of  $\mathcal{U}_*$ . Outline of proof: (a) Let  $\mathcal{U}$  be a universal extension of  $\mathcal{F}$  (Theorem 2). Show that for every finitely generated separable extension  $\mathcal{G}$  of  $\mathcal{F}$  in  $\mathcal{U}$  there exists an infinite sequence  $(\mathcal{E}_n(\mathcal{G}))_{n \in \mathbb{N}}$  of differential subfields of  $\mathcal{U}$  such that each  $\mathcal{E}_n(\mathcal{G})$  is a finitely generated separable extension of  $\mathcal{G}$  and every finitely generated separable extension of  $\mathcal{G}$  is  $\mathcal{G}$ -isomorphic to some  $\mathcal{E}_n(\mathcal{G})$ . (*Hint*: Use Proposition 4(b), and see Section 4, Exercise 1.) (b) Show that there exists an infinite sequence  $(\mathcal{F}_n)_{n \in \mathbb{N}}$  of differential subfields of  $\mathcal{U}$  such that  $\mathcal{F}_0 = \mathcal{F}$ ,  $\mathcal{F}_{n+1}$  is a finitely generated separable extension of  $\mathcal{F}_n$ , and  $\mathcal{F}_{n+1}$  contains an  $\mathcal{F}_j$ -isomorphic image of  $\mathcal{E}_{n-j}(\mathcal{F}_j)$  ( $0 \leq j \leq n$ ). (*Hint*: Define the sequence inductively, using Exercise 3.) (c) Let  $\mathcal{U}_* = \bigcup_{n \in \mathbb{N}} \mathcal{F}_n$ , and show that  $\mathcal{U}_*$  is denumerable, and is separable and universal over  $\mathcal{F}$ . (d) Show that if  $\mathcal{U}'$  is any universal extension of  $\mathcal{F}$ , then there exists an  $\mathcal{F}$ -homomorphism  $\mathcal{U}_* \rightarrow \mathcal{U}'$ . (*Hint*: Use Exercise 2.)
- Let  $p$  be either 0 or a prime number. Show: There exists a denumerable universal differential field  $\mathcal{U}_p$  of characteristic  $p$  such every universal differential field of characteristic  $p$  contains an isomorphic image of  $\mathcal{U}_p$ . This is a special case of the result in Exercise 5.
- Prove: If  $\mathcal{F}$  has characteristic 0, then two universal extensions of  $\mathcal{F}$  always contain universal extensions of  $\mathcal{F}$  that are isomorphic to each other over  $\mathcal{F}$ . (*Hint*: Let  $\mathcal{U}$  and  $\mathcal{U}'$  be universal extensions of  $\mathcal{F}$ . The set of all mappings each of which is an  $\mathcal{F}$ -isomorphism of an extension of  $\mathcal{F}$  in  $\mathcal{U}$  onto an extension of  $\mathcal{F}$  in  $\mathcal{U}'$  can be ordered "by extension," and when so ordered has a maximal element  $f$  (Zorn's lemma). Let  $\mathcal{V}$  be the domain and  $\mathcal{V}'$  be the image of  $f$ , and show that  $\mathcal{V}$  and  $\mathcal{V}'$  are universal over  $\mathcal{F}$ .)

### 8 f-Coherent autoreduced sets

The purpose of the present section is to lay the groundwork for the proof in the following section of analogs for differential integral domains of some of the results on specializations described in Chapter 0, Section 14.

Throughout this section  $\mathcal{S} = \mathcal{A}\{y_1, \dots, y_n\}$  denotes a finitely generated differential polynomial algebra over  $\mathcal{A}$ .

Let  $A$  be an autoreduced set in  $\mathcal{S}$  relative to some fixed ranking, and let  $\mathfrak{f}$  be an ideal (not necessarily a differential one) of  $\mathcal{S}$ . We shall say that the autoreduced set  $A$  is *f-coherent* if the following three conditions are satisfied.

**C1** The ideal  $\mathfrak{k}$  has a set of generators that are partially reduced with respect to  $A$ .

**C2**  $[\mathfrak{k}] \subset ([A] + \mathfrak{k}): H_A^\infty$ .

**C3** Whenever  $A, A' \in A$  and  $v$  is a common derivative of  $u_A, u_{A'}$ , say  $v = \theta u_A = \theta' u_{A'}$ , then  $S_{A'} \theta A - S_A \theta' A' \in ((A_v) + \mathfrak{k}): H_A^\infty$ , where  $A_v$  denotes the set of all differential polynomials  $\tau B$  with  $B \in A$ ,  $\tau \in \Theta$ , and  $\text{rank } \tau B$  of lower rank than  $v$ .

**REMARK** This notion extends one previously introduced by Rosenfeld [105] for the same purpose. Limiting himself to the case in which  $\mathcal{R} = \mathcal{F}$  and  $p = 0$ , he called an autoreduced set *coherent* when it is (0)-coherent in the present sense. For this case this more special notion suffices.

**Lemma 3** Let  $\mathfrak{p}$  be a prime differential ideal of  $\mathcal{S}$  that is quasi-separable over  $\mathcal{R}$ , let there be given a sequential ranking of  $(y_1, \dots, y_n)$ , and let  $A$  be a characteristic set of  $\mathfrak{p}$ . Then there exists a finite set  $Y$  of derivatives of the  $y_j$ , each partially reduced with respect to  $A$ , such that if we set  $\mathfrak{p}_1 = \mathfrak{p} \cap \mathcal{R}[Y]$ , then  $A$  is  $\mathcal{S}_{\mathfrak{p}_1}$ -coherent and  $\mathfrak{p} = ([A] + \mathcal{S}_{\mathfrak{p}_1}): H_A^\infty$ . The set  $Y$  may be replaced by any larger finite set of derivatives of the  $y_j$  partially reduced with respect to  $A$ .

**REMARK** If  $\mathcal{S}/\mathfrak{p}$  is of characteristic 0, then the ranking need not be sequential, and we may take  $Y = \emptyset$ . This is evident from the proof and Section 2, the Remark following Lemma 1.

*Proof* For each  $A \in A$  we have  $S_A \notin \mathfrak{p}$  (by definition of characteristic set) and  $I_A \notin \mathfrak{p}$  (by Chapter I, Section 10, Lemma 8); therefore  $H_A \notin \mathfrak{p}$ . By Lemma 1 we may choose a finite set  $Y$  of derivatives of the  $y_j$ , all partially reduced with respect to  $A$ , so that every element of  $\mathfrak{p}$  that is reduced with respect to  $A$  is in  $\mathcal{S}_{\mathfrak{p}_1}$ , where  $\mathfrak{p}_1 = \mathfrak{p} \cap \mathcal{R}[Y]$ ; obviously any larger  $Y$  will do. Since the remainder with respect to  $A$  of any element of  $\mathfrak{p}$  is reduced with respect to  $A$  (see Chapter I, Section 9, Proposition 1), we conclude that  $\mathfrak{p} \subset ([A] + \mathcal{S}_{\mathfrak{p}_1}): H_A^\infty$  and that the condition C3 (with  $k = \mathcal{S}_{\mathfrak{p}_1}$ ) is satisfied. As the inclusion  $\mathfrak{p} \supset ([A] + \mathcal{S}_{\mathfrak{p}_1}): H_A^\infty$  is obvious, the lemma follows.

**Lemma 4** Let  $A$  be a  $\mathfrak{k}$ -coherent autoreduced set in  $\mathcal{S}$ , and let  $f: \mathcal{R} \rightarrow \mathcal{R}'$  be a differential ring homomorphism with  $H_A^f \neq 0$ . Then  $A^f$  is a  $\mathfrak{k}'$ -coherent autoreduced set in  $\mathcal{S}' = f(\mathcal{R})\{y_1, \dots, y_n\}$ .

*Proof* Since  $H_A^f \neq 0$ ,  $A^f$  is an autoreduced set in  $\mathcal{S}'$  with  $H_{A^f} = H_A^f$ ; as the homomorphism  $G \mapsto G^f$  of  $\mathcal{S}$  into  $\mathcal{S}'$  obviously preserves the conditions C1–C3,  $A^f$  is  $\mathfrak{k}'$ -coherent.

**Lemma 5** Let  $A$  be a  $\mathfrak{k}$ -coherent autoreduced set in  $\mathcal{S}$ , and suppose that for each  $A \in A$  the separant  $S_A$  is not a divisor of zero in  $\mathcal{S}$ . Then every element of  $([A] + \mathfrak{k}): H_A^\infty$  that is partially reduced with respect to  $A$  is in  $((A) + \mathfrak{k}): H_A^\infty$ .

*Proof* Let  $G \in ([A] + \mathfrak{k}): H_A^\infty$  be partially reduced with respect to  $A$ . We must show that  $G \in ((A) + \mathfrak{k}): H_A^\infty$ . We may write

$$H_A^h G = \sum_{1 \leq i \leq r} C_i \theta_i A_i + \sum_{1 \leq j \leq s} D_j K_j, \quad (1)$$

where  $C_i \in \mathcal{S}$ ,  $\theta_i \in \Theta$  and  $\text{ord } \theta_i > 0$ ,  $A_i \in A$ ,  $D_j \in \mathcal{S}$ ,  $K_j \in (A) + \mathfrak{k}$ , and  $K_j$  is partially reduced with respect to  $A$ . If there exists for  $G$  an equation (1) with  $r = 0$ , then certainly  $G \in ((A) + \mathfrak{k}): H_A^\infty$ . We assume that there does not exist for  $G$  an equation (1) with  $r = 0$ , and seek a contradiction.

Let  $v$  be the element of highest rank in the set consisting of  $\theta_1 u_{A_1}, \dots, \theta_r u_{A_r}$ , and suppose that among all possible equations (1) for  $G$  ours is one for which  $v$  has lowest rank. Choose the notation so that  $\theta_i u_{A_i}$  is lower than  $v$  for  $1 \leq i < q$  and  $\theta_i u_{A_i} = v$  for  $q \leq i \leq r$ . Multiplying both sides of (1) by  $S_{A_r}$  we may then write

$$S_{A_r} H_A^h G = \sum_{1 \leq i < q} S_{A_r} C_i \theta_i A_i + \sum_{1 \leq j \leq s} S_{A_r} D_j K_j \\ + \sum_{q \leq i \leq r} C_i (S_{A_r} \theta_i A_i - S_{A_i} \theta_r A_r) + \sum_{q \leq i \leq r} C_i S_{A_i} \theta_r A_r.$$

From this equation, condition C3, and the fact that  $H_A$  is a multiple of  $S_{A_r}$ , we obtain

$$H_A^h G = \sum_{1 \leq i \leq r'} C'_i \theta'_i A'_i + \sum_{1 \leq j \leq s'} D'_j K'_j + E \theta_r A_r, \quad (2)$$

where  $C'_i \in \mathcal{S}$ ,  $\theta'_i \in \Theta$  and  $\text{ord } \theta'_i > 0$ ,  $A'_i \in A$ ,  $\theta'_i u_{A'_i}$  is lower than  $v$ ,  $D'_j \in \mathcal{S}$ ,  $K'_j \in (A) + \mathfrak{k}$ ,  $K'_j$  is partially reduced with respect to  $A$ , and  $E \in \mathcal{S}$ . By Chapter I, Section 8, Lemma 5, we may write  $\theta_r A_r = S_{A_r} v + T$ , where  $T \in \mathcal{S}$  and  $T$  has lower rank than  $v$  (and therefore is free of  $v$ , as is  $S_{A_r}$ ). Since  $S_{A_r}$  is not a divisor of 0,  $\mathcal{S}$  may be isomorphically embedded in the ring of quotients  $\Sigma^{-1} \mathcal{S}$ , where  $\Sigma$  is the set of all powers  $S_{A_r}^l$  ( $l \in \mathbb{N}$ ). Substituting  $-T/S_{A_r}$  for  $v$  in (2), and then multiplying by a suitable power of  $H_A$ , we obtain an equation of the same form as (1) in which either  $r$  is replaced by 0 or else  $v$  is replaced by a derivative of a  $y_j$  of lower rank than  $v$ . This contradiction completes the proof.

**Lemma 6** Let  $A$  be a  $\mathfrak{k}$ -coherent autoreduced set in  $\mathcal{S}$ , and suppose that for each  $A \in A$  the separant  $S_A$  is not a divisor of zero in  $\mathcal{S}$ . Then  $([A] + \mathfrak{k}): H_A^\infty$  is a differential ideal of  $\mathcal{S}$ , and is prime, respectively perfect, respectively  $\mathcal{R}$ -separable if  $((A) + \mathfrak{k}): H_A^\infty$  is prime, respectively perfect, respectively  $\mathcal{R}$ -separable.

*Proof* Set  $\alpha = ([A] + \mathfrak{f}): H_A^\infty$  and  $\alpha_0 = ((A) + \mathfrak{f}): H_A^\infty$ . By C2,  $\alpha = ([A] + [\mathfrak{f}]): H_A^\infty$ . Hence (see Chapter I, Section 2, Corollary to Lemma 1)  $\alpha$  is a differential ideal, and  $\alpha: H_A^\infty = \alpha$ .

Let  $F, G \in \mathcal{S}$ ,  $FG \in \alpha$ . Denoting the remainder with respect to  $A$  of  $F$ , respectively  $G$ , by  $F_0$ , respectively  $G_0$ , we know that  $F_0 G_0 \in \alpha$  and  $F_0 G_0$  is partially reduced with respect to  $A$ , so that (by Lemma 5)  $F_0 G_0 \in \alpha_0$ . Hence, if  $\alpha_0$  is prime, then  $F_0$  or  $G_0$  is in  $\alpha_0$ , so that  $F$  or  $G$  is in  $\alpha$ , and therefore  $\alpha$  is prime (an even easier argument showing that  $1 \notin \alpha$ ). A similar proof (starting with  $F^2 \in \alpha$  instead of  $FG \in \alpha$ ) shows that if  $\alpha_0$  is perfect, then so is  $\alpha$ .

Suppose finally that  $\alpha_0$  is  $\mathcal{R}$ -separable. We must show that  $\alpha$  is  $\mathcal{R}$ -separable, and we may evidently suppose that  $\alpha \neq \mathcal{S}$ . By what we have already proved,  $\alpha$  is perfect. If  $a \in \mathcal{R}$ ,  $a \notin \alpha$ ,  $B \in \mathcal{S}$ ,  $B \notin \alpha$ , let  $B_0$  denote the remainder of  $B$  with respect to  $A$ , so that  $B_0$  is reduced with respect to  $A$  and  $B_0 \notin \alpha_0$ . Since  $\alpha_0$  is  $\mathcal{R}$ -separable we infer that  $aB_0 \notin \alpha_0$  and therefore (by Lemma 5) that  $aB_0 \notin \alpha$ , so that  $aB \notin \alpha$ . To complete the proof we may suppose that the characteristic of  $\mathcal{R}/(\alpha \cap \mathcal{R})$  is  $p \neq 0$ . We must then show that  $\mathcal{S}^p$  and  $\mathcal{R}$  are linearly disjoint (mod  $\alpha$ ) over  $\mathcal{R}^p$ . To this end let  $(c_i)$  be a family of elements of  $\mathcal{R}$  linearly dependent (mod  $\alpha$ ) over  $\mathcal{S}^p$ . Then there exist elements  $D_i \in \mathcal{S}$ , not all in  $\alpha$ , such that  $\sum D_i^p c_i \in \alpha$ . By Chapter I, Section 9, Corollary to Lemma 6, there are an exponent  $e$  and differential polynomials  $E_i \in \mathcal{S}$  partially reduced with respect to  $A$  such that  $H_A^e D_i \equiv E_i \pmod{[A]}$  for every  $i$ . Not every  $E_i$  is in  $\alpha$  and  $\sum E_i^p c_i \in \alpha$ , so that not every  $E_i$  is in  $\alpha_0$ ; by Lemma 5,  $\sum E_i^p c_i \in \alpha_0$ . Since  $\alpha_0$  is  $\mathcal{R}$ -separable this implies that there exist elements  $a_i \in \mathcal{R}$  not all in  $\alpha_0$  such that  $\sum a_i^p c_i \in \alpha_0$ . Hence (again by Lemma 5) the elements  $a_i$  are not all in  $\alpha$ , and  $\sum a_i^p c_i \in \alpha$ . This shows that  $\mathcal{S}^p$  and  $\mathcal{R}$  are linearly disjoint (mod  $\alpha$ ) over  $\mathcal{R}^p$ , and completes the proof.

EXERCISE

1. Let the hypothesis and notation be the same as in Lemmas 5 and 6. In addition, suppose that  $\mathfrak{f}$  has a set of generators that are reduced with respect to  $A$  and that each element of  $A$  is of degree 1 in its leader.
  - (a) Prove that every element of  $([A] + \mathfrak{f}): H_A^\infty$  that is reduced with respect to  $A$  is in  $\mathfrak{f}: H_A^\infty$ .
  - (b) Prove that  $([A] + \mathfrak{f}): H_A^\infty$  is prime, respectively perfect, respectively  $\mathcal{R}$ -separable if  $\mathfrak{f}: H_A^\infty$  is prime, respectively perfect, respectively  $\mathcal{R}$ -separable.

9 Differential specializations

We suppose in this section that  $\mathcal{R}$  is a differential integral domain. A homomorphism of  $\mathcal{R}$  into a differential field  $\mathcal{G}$  is called a differential

specialization of  $\mathcal{R}$  into  $\mathcal{G}$ . If  $\mathcal{R}$  and  $\mathcal{G}$  happen to have a common differential subring  $\mathcal{R}_0$  and the homomorphism leaves invariant each element of  $\mathcal{R}_0$ , the differential specialization is said to be over  $\mathcal{R}_0$ .

Let  $\xi = (\xi_i)_{i \in I}$  and  $\xi' = (\xi'_i)_{i \in I}$  be families of elements of  $\mathcal{R}$  and  $\mathcal{G}$ , respectively. If there exists a differential specialization  $f: \mathcal{R}_0 \{\xi\} \rightarrow \mathcal{G}$  over  $\mathcal{R}_0$  mapping  $\xi$  onto  $\xi'$  (that is, having the property that  $f(\xi_i) = \xi'_i$  for every  $i \in I$ ), we say that  $\xi'$  is a differential specialization of  $\xi$  over  $\mathcal{R}_0$ ; when such an  $f$  exists it is obviously unique. A necessary and sufficient condition that  $\xi'$  be a differential specialization of  $\xi$  over  $\mathcal{R}_0$  is that the defining differential ideal of  $\xi$  over  $\mathcal{R}_0$  be contained in the defining differential ideal of  $\xi'$  over  $\mathcal{R}_0$ . Another necessary and sufficient condition is that  $(\theta \xi'_i)_{\theta \in \mathfrak{o}, i \in I}$  be a specialization of  $(\theta \xi_i)_{\theta \in \mathfrak{o}, i \in I}$  over  $\mathcal{R}_0$ .

If  $\xi'$  is a differential specialization of  $\xi$  over  $\mathcal{R}_0$  such that  $\xi$  is a differential specialization of  $\xi'$  over  $\mathcal{R}_0$ , we say that  $\xi'$  is a generic differential specialization of  $\xi$  over  $\mathcal{R}_0$ . This is the case if and only if there exists an  $\mathcal{R}_0$ -isomorphism  $\mathcal{R}_0 \{\xi\} \approx \mathcal{R}_0 \{\xi'\}$  mapping  $\xi$  onto  $\xi'$ .

The following result is analogous to Chapter 0, Section 14, Lemma 14.

**Proposition 5** *Let  $\mathcal{R}$  be a differential integral domain, let  $\mathcal{S} = \mathcal{R}\{y_1, \dots, y_n\}$  be a finitely generated differential polynomial algebra over  $\mathcal{R}$ , let  $\mathfrak{p}$  be an  $\mathcal{R}$ -separable prime differential ideal of  $\mathcal{S}$  with  $\mathfrak{p} \cap \mathcal{R} = (0)$ , and let  $U \in \mathcal{S}$ ,  $U \notin \mathfrak{p}$ . Then there exist a nonzero element  $u \in \mathcal{R}$  and a differential polynomial  $E \in \mathcal{S}$  such that, for every differential specialization  $f: \mathcal{R} \rightarrow \mathcal{G}$  with  $f(u) \neq 0$ ,  $\mathfrak{p}^f: (E^f)^\infty$  is an  $f(\mathcal{R})$ -separable differential ideal of  $\mathcal{S}^f = f(\mathcal{R})\{y_1, \dots, y_n\}$  not containing  $\alpha U^f E^f$  for any nonzero element  $\alpha \in f(\mathcal{R})$ .*

*Proof* By Section 8, Lemma 3, there exist an autoreduced set  $A$  in  $\mathfrak{p}$ , and a finite set  $Y$  of derivatives of the  $y_j$  partially reduced with respect to  $A$ , such that if we set  $\mathfrak{p}_1 = \mathfrak{p} \cap \mathcal{R}[Y]$ , then  $\mathfrak{p} = ([A] + \mathcal{S} \mathfrak{p}_1): H_A^\infty$  and  $A$  is  $\mathcal{S} \mathfrak{p}_1$ -coherent;  $\mathfrak{p}_1$  is obviously an  $\mathcal{R}$ -separable prime ideal of  $\mathcal{R}[Y]$ . Denote the remainder of  $U$  with respect to  $A$  by  $U_0$ . By the last part of Lemma 3 we may suppose that  $A \subset \mathcal{R}[Y]$  and  $U_0 \in \mathcal{R}[Y]$ , so that  $H_A U_0 \in \mathcal{R}[Y]$  and  $H_A U_0 \notin \mathfrak{p}_1$ . By Chapter 0, Section 14, Lemma 14, there exist a nonzero  $u \in \mathcal{R}$  and a  $D \in \mathcal{R}[Y]$  such that, for every specialization  $f: \mathcal{R} \rightarrow L$  with  $f(u) \neq 0$ ,  $\mathfrak{p}_1^f: (D^f)^\infty$  is an  $f(\mathcal{R})$ -separable ideal of  $f(\mathcal{R})[Y]$  not containing  $\alpha H_A^f U_0^f D^f$  for any nonzero element  $\alpha \in f(\mathcal{R})$ .

Consider any differential specialization  $f: \mathcal{R} \rightarrow \mathcal{G}$  with  $f(u) \neq 0$ . From what we have just seen, it follows that  $\mathcal{S}^f \cdot (\mathfrak{p}_1^f: (D^f)^\infty)$  is an  $f(\mathcal{R})$ -separable ideal of  $\mathcal{S}^f$  not containing  $\alpha H_A^f U_0^f D^f$  for any nonzero element  $\alpha \in f(\mathcal{R})$ . By Section 8, Lemma 4,  $A^f$  is an  $\mathcal{S}^f \mathfrak{p}_1^f$ -coherent autoreduced set in  $\mathcal{S}^f$ . We now prove that  $A^f$  is  $\mathcal{S}^f \cdot (\mathfrak{p}_1^f: (D^f)^\infty)$ -coherent. All that we must show for this is that  $[\mathfrak{p}_1^f: (D^f)^\infty] \subset ([A^f] + \mathcal{S}^f \cdot (\mathfrak{p}_1^f: (D^f)^\infty)): (H_A^f)^\infty$ , that is, given

any  $G \in \mathcal{S}$  with  $G^f \in [p_1^f : (D^f)^\infty]$ , we must show that

$$G^f \in ([A^f] + \mathcal{S}^f \cdot (p_1^f : (D^f)^\infty)) : (H_A^f)^\infty.$$

Now,  $G^f$  is the sum of finitely many terms  $C^f \theta L^f$  with  $C \in \mathcal{S}$ ,  $\theta \in \Theta$ ,  $L \in \mathcal{R}[Y]$ , and  $L^f \in p_1^f : (D^f)^\infty$ ; the last relation here means that  $(D^f)^l L^f \in p_1^f$  for some  $l \in \mathbb{N}$  and this implies (by Chapter I, Section 2, Lemma 1) that  $(D^f)^k \theta L^f \in [p_1^f]$  for some  $k \in \mathbb{N}$ . Thus,  $(D^f)^k G^f \in [p_1^f]$ . Since  $A^f$  is  $\mathcal{S}^f p_1^f$ -coherent this implies that  $(D^f)^k G^f \in ([A^f] + \mathcal{S}^f p_1^f) : (H_A^f)^\infty$ . Denoting the remainder of  $G$  with respect to  $A$  by  $G_0$ , we easily infer that  $(D^f)^k G_0^f \in ([A^f] + \mathcal{S}^f p_1^f) : (H_A^f)^\infty$ , whence (by Section 8, Lemma 5)  $(D^f)^k G_0^f \in ((A^f) + \mathcal{S}^f p_1^f) : (H_A^f)^\infty = (\mathcal{S}^f p_1^f) : (H_A^f)^\infty$ . Hence

$$\begin{aligned} G_0^f &\in ((\mathcal{S}^f p_1^f) : (H_A^f)^\infty) : (D^f)^\infty = ((\mathcal{S}^f p_1^f) : (D^f)^\infty) : (H_A^f)^\infty \\ &= (\mathcal{S}^f \cdot (p_1^f : (D^f)^\infty)) : (H_A^f)^\infty, \end{aligned}$$

so that  $G^f \in ([A^f] + \mathcal{S}^f \cdot (p_1^f : (D^f)^\infty)) : (H_A^f)^\infty$ . This shows that  $A^f$  is  $\mathcal{S}^f \cdot (p_1^f : (D^f)^\infty)$ -coherent.

By Section 8, Lemma 6, then  $([A^f] + \mathcal{S}^f \cdot (p_1^f : (D^f)^\infty)) : (H_A^f)^\infty$  is an  $f(\mathcal{R})$ -separable differential ideal of  $\mathcal{S}^f$  that (by Lemma 5) does not contain  $\alpha H_A^f U_0^f D^f$  for any nonzero element  $\alpha \in f(\mathcal{R})$ . The same is evidently true of  $([A^f] + \mathcal{S}^f \cdot (p_1^f : (D^f)^\infty)) : (H_A^f D^f)^\infty$ . However,  $p \subset ([A] + \mathcal{S} p_1) : H_A^\infty$ , and therefore  $p^f \subset ([A^f] + \mathcal{S}^f p_1^f) : (H_A^f)^\infty$ , whence

$$p^f : (H_A^f D^f)^\infty \subset ([A^f] + \mathcal{S}^f \cdot (p_1^f : (D^f)^\infty)) : (H_A^f D^f)^\infty.$$

Since the last inclusion can evidently be reversed, we see that  $p^f : (H_A^f D^f)^\infty = ([A^f] + \mathcal{S}^f \cdot (p_1^f : (D^f)^\infty)) : (H_A^f D^f)^\infty$ . Setting  $E = H_A D$ , we thus see that  $p^f : (E^f)^\infty$  is an  $f(\mathcal{R})$ -separable differential ideal of  $\mathcal{S}^f$  not containing  $\alpha U_0^f E^f$  (hence not containing  $\alpha U^f E^f$ ) for any nonzero element  $\alpha \in f(\mathcal{R})$ .

From Proposition 5 we deduce the following theorem (analogous to Chapter 0, Section 14, Proposition 9(c)) on the possibility of extending differential specializations.

**Theorem 3** *Let  $\mathcal{R}$  be a differential integral domain, let  $\mathcal{R}_0$  be a differential subring of  $\mathcal{R}$  over which  $\mathcal{R}$  is finitely generated and separable, and let  $u$  be a nonzero element of  $\mathcal{R}$ . There exists a nonzero element  $u_0$  of  $\mathcal{R}_0$  such that every differential specialization  $f_0 : \mathcal{R}_0 \rightarrow \mathcal{U}$  with  $\mathcal{U}$  a semiuniversal extension of  $Q(f_0(\mathcal{R}_0))$  and  $f_0(u_0) \neq 0$  can be extended to a differential specialization  $f : \mathcal{R} \rightarrow \mathcal{U}$  with  $f(\mathcal{R})$  separable over  $f(\mathcal{R}_0)$  and  $f(u) \neq 0$ .*

*Proof* By hypothesis we may write  $\mathcal{R} = \mathcal{R}_0\langle \eta_1, \dots, \eta_n \rangle$ , and the defining differential ideal  $p$  of  $(\eta_1, \dots, \eta_n)$  in the differential polynomial algebra  $\mathcal{R}_0\{y_1, \dots, y_n\}$  is prime and  $\mathcal{R}_0$ -separable with  $p \cap \mathcal{R}_0 = (0)$ . Also, there

exists a differential polynomial  $U \in \mathcal{R}_0\{y_1, \dots, y_n\}$  with  $U(\eta_1, \dots, \eta_n) = u$ , and obviously  $U \notin p$ . By Proposition 5 there exist a nonzero element  $u_0 \in \mathcal{R}_0$  and a differential polynomial  $E \in \mathcal{R}_0\{y_1, \dots, y_n\}$  such that, for every differential specialization  $f_0 : \mathcal{R}_0 \rightarrow \mathcal{U}$  with  $f_0(u_0) \neq 0$ ,  $p^{f_0} : (E^{f_0})^\infty$  is an  $f_0(\mathcal{R}_0)$ -separable differential ideal of  $f_0(\mathcal{R}_0)\{y_1, \dots, y_n\}$  not containing  $\alpha U^{f_0}$  for any nonzero element  $\alpha \in f_0(\mathcal{R}_0)$ . The set  $\mathfrak{C}$ , consisting of the unit ideal and all  $f_0(\mathcal{R}_0)$ -separable differential ideals of  $f_0(\mathcal{R}_0)\{y_1, \dots, y_n\}$  not containing any nonzero element of  $f_0(\mathcal{R}_0)$ , is a perfect differential conservative system (see Chapter 0, Section 6, Lemma 5), and  $p^{f_0} : (E^{f_0})^\infty \in \mathfrak{C}$ . Therefore there exists a  $\mathfrak{C}$ -component  $p'$  of  $p^{f_0} : (E^{f_0})^\infty$  with  $U^{f_0} \notin p'$  (see Chapter 0, Section 8, Proposition 1). If  $\mathcal{U}$  is a semiuniversal extension of  $Q(f_0(\mathcal{R}_0))$ , then there exist elements  $\eta_1', \dots, \eta_n' \in \mathcal{U}$  such that  $p'$  is the kernel of the substitution homomorphism

$$\sigma : f_0(\mathcal{R}_0)\{y_1, \dots, y_n\} \rightarrow f_0(\mathcal{R}_0)\{\eta_1', \dots, \eta_n'\}.$$

Denoting the homomorphism  $G \mapsto G^{f_0}$  of  $\mathcal{R}_0\{y_1, \dots, y_n\}$  into  $f_0(\mathcal{R}_0)\{y_1, \dots, y_n\}$  by  $\varphi_0$ , we see that the composite homomorphism

$$\sigma \circ \varphi_0 : \mathcal{R}_0\{y_1, \dots, y_n\} \rightarrow f_0(\mathcal{R}_0)\{\eta_1', \dots, \eta_n'\}$$

has prime kernel containing  $p$  but not containing  $U$ . Since the kernel of the surjective substitution homomorphism

$$\tau : \mathcal{R}_0\{y_1, \dots, y_n\} \rightarrow \mathcal{R}_0\{\eta_1, \dots, \eta_n\} = \mathcal{R}$$

is  $p$ , there must exist a homomorphism  $f : \mathcal{R} \rightarrow f_0(\mathcal{R}_0)\{\eta_1', \dots, \eta_n'\}$  such that  $f \circ \tau = \sigma \circ \varphi_0$ . It is now a simple matter to see that  $f$  agrees with  $f_0$  on  $\mathcal{R}_0$ ,  $f(\mathcal{R})$  is separable over  $f(\mathcal{R}_0)$ , and  $f(u) \neq 0$ . This proves the theorem.

**REMARK** The earliest version of Theorem 3, proved by Ritt [91], dealt with the case in which  $\mathcal{R}_0$  is a finitely generated differential algebra over an ordinary differential field of functions meromorphic in a region of the complex plane. This was extended, independently and by different methods, by Seidenberg [110] and Rosenfeld [105], to the situation in which  $\mathcal{R}_0$  is a finitely generated differential algebra over an arbitrary differential field of characteristic zero. The above proof of the present general theorem entails a further development of Rosenfeld's methods.

It is noteworthy that the analog for differential specializations of Chapter 0, Section 14, Proposition 9(b), is false. There exist elements  $\eta, \zeta$  of a universal extension  $\mathcal{U}$  of  $\mathcal{F}$  having the following property: 0 is a differential specialization of  $\eta$  over  $\mathcal{F}$  but there does not exist an  $\alpha \in \mathcal{U}$  such that  $(0, \alpha)$  is a differential specialization over  $\mathcal{F}$  either of  $(\eta, \zeta)$  or of  $(\eta, \zeta^{-1})$ . This is more easily shown at a later stage (see Chapter IV, Section 6, Exercise 6(c)).

Another curious phenomenon is the existence of elements  $\eta, \zeta \in \mathcal{U}$  such that 0 is not a differential specialization of  $\eta$  or  $\zeta$  over  $\mathcal{F}$  but is a differential specialization of  $\eta\zeta$  over  $\mathcal{F}$  (see Chapter IV, Section 6, Exercise 7(d)).

### 10 Constrained families

A family  $\eta = (\eta_i)_{i \in I}$  of elements of an extension of  $\mathcal{F}$  will be said to be *constrained over  $\mathcal{F}$* , or to be  *$\mathcal{F}$ -constrained*, if  $\eta$  is separable over  $\mathcal{F}$  (that is,  $\mathcal{F}\langle\eta\rangle$  is separable over  $\mathcal{F}$ ) and there exists a differential polynomial  $B \in \mathcal{F}\{(y_i)_{i \in I}\}$  with  $B(\eta) \neq 0$  such that  $B(\eta') = 0$  for every *nongeneric* differential specialization  $\eta'$  of  $\eta$  over  $\mathcal{F}$  that is separable over  $\mathcal{F}$ . Any such  $B$  will be called a *constraint* of  $\eta$  over  $\mathcal{F}$ . (When  $\text{Card } I = 1$ , that is, when the constrained family  $\eta$  has just one coordinate  $\eta_i$ , we identify the family with its coordinate and call it a constrained *element*.)

If  $\eta = (\eta_i)_{i \in I}$  is separably algebraic over  $\mathcal{F}$  (that is,  $\mathcal{F}\langle\eta\rangle$  is a separable algebraic field extension of  $\mathcal{F}$ ), then  $\eta$  is constrained over  $\mathcal{F}$  with constraint 1. For a familiar transcendental example see Exercise 2 below.

**Proposition 6** *Let  $\eta = (\eta_i)_{i \in I}$  be a family of elements of an extension of  $\mathcal{F}$ , with  $\eta$  separable over  $\mathcal{F}$ , and let  $B \in \mathcal{F}\{(y_i)_{i \in I}\}$  be a differential polynomial such that  $B(\eta) \neq 0$ . There exists a differential specialization  $\eta'$  of  $\eta$  over  $\mathcal{F}$  such that  $\eta'$  is constrained over  $\mathcal{F}$  with constraint  $B$ .*

*Proof* By Zorn's lemma, in the set of all  $\mathcal{F}$ -separable prime differential ideals of  $\mathcal{F}\{(y_i)_{i \in I}\}$  that contain the defining differential ideal of  $\eta$  over  $\mathcal{F}$  but do not contain  $B$ , there is a maximal element, say  $\mathfrak{p}'$ . This  $\mathfrak{p}'$  is the defining differential ideal over  $\mathcal{F}$  of a family  $\eta'$  with coordinates in an extension of  $\mathcal{F}$ , and obviously  $\eta'$  is a differential specialization of  $\eta$  over  $\mathcal{F}$  and is  $\mathcal{F}$ -separable, and  $B(\eta') \neq 0$ . If  $\eta''$  is any nongeneric differential specialization of  $\eta'$  over  $\mathcal{F}$  and is  $\mathcal{F}$ -separable, then the defining differential ideal of  $\eta''$  in  $\mathcal{F}\{(y_i)_{i \in I}\}$  is  $\mathcal{F}$ -separable and properly contains  $\mathfrak{p}'$  and hence contains  $B$ , so that  $B(\eta'') = 0$ . Thus,  $\eta'$  is constrained over  $\mathcal{F}$  with constraint  $B$ .

**Proposition 7** *Let  $\eta = (\eta_i)_{i \in I}$  and  $\zeta = (\zeta_j)_{j \in J}$  be families of elements of an extension of  $\mathcal{F}$ .*

(a) *Let  $\mathcal{F}\langle\eta\rangle = \mathcal{F}\langle\zeta\rangle$  and  $I$  be finite. If  $\eta$  is constrained over  $\mathcal{F}$ , then so is  $\zeta$ .*

(b) *Let  $\mathcal{F}\langle\eta, \zeta\rangle$  be separable over  $\mathcal{F}\langle\eta\rangle$ . If  $(\eta, \zeta)$  is constrained over  $\mathcal{F}$ , then  $\zeta$  is constrained over  $\mathcal{F}\langle\eta\rangle$  and, provided  $J$  is finite,  $\eta$  is constrained over  $\mathcal{F}$ .*

(c) *Let the field of constants of  $\mathcal{F}\langle\eta\rangle$  be separable over  $\mathcal{F}\langle\eta\rangle^{\text{pc}}$ . If  $\zeta$  is constrained over  $\mathcal{F}\langle\eta\rangle$  and  $\eta$  is constrained over  $\mathcal{F}$ , then  $(\eta, \zeta)$  is constrained over  $\mathcal{F}$ .*

(d) *Let  $I$  be finite. If  $\eta$  is constrained over  $\mathcal{F}$ , then the field of constants of  $\mathcal{F}\langle\eta\rangle$  is separably algebraic over  $\mathcal{F}\langle\eta\rangle^{\text{pc}}$ .*

*Proof* (a) There exist differential polynomials  $M_i, N \in \mathcal{F}\{(z_j)_{j \in J}\}$  with  $N(\zeta) \neq 0$  such that  $\eta_i = M_i(\zeta)/N(\zeta)$ . Also,  $\eta$  has a constraint  $B \in \mathcal{F}\{(y_i)_{i \in I}\}$ . For a sufficiently big  $h \in \mathbb{N}$ ,  $N^h B(M/N)$  is a differential polynomial, which we denote by  $C$ ; clearly  $C(\zeta) = N(\zeta)^h B(\eta) \neq 0$ . Let  $\zeta'$  be a differential specialization of  $\zeta$  over  $\mathcal{F}$  with  $\zeta'$  separable over  $\mathcal{F}$  and  $N(\zeta')C(\zeta') \neq 0$ . Then we may set  $\eta' = (M_i(\zeta')/N(\zeta'))$ . It is clear that  $\eta'$  is a differential specialization of  $\eta$  over  $\mathcal{F}$  with  $\eta'$  separable over  $\mathcal{F}$  and  $B(\eta') \neq 0$ . Since  $B$  is a constraint of  $\eta$  it follows that  $\eta'$  is a generic differential specialization of  $\eta$  over  $\mathcal{F}$ , and hence that  $\zeta'$  is a generic differential specialization of  $\zeta$  over  $\mathcal{F}$ . Thus,  $NC$  is a constraint of  $\zeta$  over  $\mathcal{F}$ . Since  $\zeta$  is obviously separable over  $\mathcal{F}$ , this shows that  $\zeta$  is constrained over  $\mathcal{F}$ .

(b) Let  $B \in \mathcal{F}\{(y_i)_{i \in I}, (z_j)_{j \in J}\}$  be a constraint of  $(\eta, \zeta)$  over  $\mathcal{F}$ . If  $\zeta'$  is a differential specialization of  $\zeta$  over  $\mathcal{F}\langle\eta\rangle$  with  $\zeta'$  separable over  $\mathcal{F}\langle\eta\rangle$  and  $B(\eta, \zeta') \neq 0$ , then  $(\eta, \zeta')$  is a differential specialization of  $(\eta, \zeta)$  over  $\mathcal{F}$  with  $(\eta, \zeta')$  separable over  $\mathcal{F}$  and  $B(\eta, \zeta') \neq 0$ , so that  $(\eta, \zeta')$  is a generic differential specialization of  $(\eta, \zeta)$  over  $\mathcal{F}$ , and therefore  $\zeta'$  is a generic differential specialization of  $\zeta$  over  $\mathcal{F}\langle\eta\rangle$ . Thus,  $B(\eta, z)$  is a constraint of  $\zeta$  over  $\mathcal{F}\langle\eta\rangle$ , so that  $\zeta$  is constrained over  $\mathcal{F}\langle\eta\rangle$ .

Now suppose that  $J$  is finite. By Section 9, Theorem 3, there exists a  $U_0 \in \mathcal{F}\{(y_i)_{i \in I}\}$  with  $U_0(\eta) \neq 0$  such that for every differential specialization  $\eta'$  of  $\eta$  over  $\mathcal{F}$  with  $U_0(\eta') \neq 0$  there is a  $\zeta'$  separable over  $\mathcal{F}\langle\eta'\rangle$  for which  $(\eta', \zeta')$  is a differential specialization of  $(\eta, \zeta)$  over  $\mathcal{F}$  with  $B(\eta', \zeta') \neq 0$ . If  $\eta'$  is separable over  $\mathcal{F}$ , then  $(\eta', \zeta')$  is separable over  $\mathcal{F}$ , and therefore  $(\eta', \zeta')$  is a generic differential specialization of  $(\eta, \zeta)$  over  $\mathcal{F}$ . Thus,  $U_0$  is a constraint of  $\eta$  over  $\mathcal{F}$ , so that  $\eta$  is constrained over  $\mathcal{F}$ .

(c) It is obvious that  $(\eta, \zeta)$  is separable over  $\mathcal{F}$ . By hypothesis, there exists a constraint  $B \in \mathcal{F}\{(y_i)_{i \in I}\}$  of  $\eta$  over  $F$ , and there exists a  $C \in \mathcal{F}\{(y_i)_{i \in I}, (z_j)_{j \in J}\}$  such that  $C(\eta, (z_j)_{j \in J})$  is a constraint of  $\zeta$  over  $F\langle\eta\rangle$ . We shall show that  $BC$  is a constraint of  $(\eta, \zeta)$  over  $\mathcal{F}$ , thereby proving that  $(\eta, \zeta)$  is constrained over  $\mathcal{F}$ . Indeed, let  $(\eta', \zeta')$  be any differential specialization of  $(\eta, \zeta)$  over  $\mathcal{F}$  with  $\mathcal{F}\langle\eta', \zeta'\rangle$  separable over  $\mathcal{F}$  and  $B(\eta')C(\eta', \zeta') \neq 0$ . Then  $\eta'$  is a differential specialization of  $\eta$  over  $\mathcal{F}$  with  $\eta'$  separable over  $\mathcal{F}$  and  $B(\eta') \neq 0$ , so that  $\eta'$  is a generic differential specialization of  $\eta$  over  $\mathcal{F}$ . Hence, there exists an isomorphism  $\mathcal{F}\langle\eta'\rangle \approx \mathcal{F}\langle\eta\rangle$  over  $\mathcal{F}$  mapping  $\eta'$  onto  $\eta$ . This isomorphism can be extended to an isomorphism of  $\mathcal{F}\langle\eta', \zeta'\rangle$  onto an extension of  $\mathcal{F}\langle\eta\rangle$ . Denoting the image of  $\zeta'$  by  $\zeta''$ , we see that  $(\eta, \zeta'')$  is a generic differential specialization of  $(\eta', \zeta')$  over  $\mathcal{F}$  (so that  $(\eta, \zeta'')$  is separable over  $\mathcal{F}$ ), and is a differential specialization of  $(\eta, \zeta)$  over  $\mathcal{F}$ , so that  $\zeta''$  is a differential specialization of  $\zeta$  over  $\mathcal{F}\langle\eta\rangle$  with  $C(\eta, \zeta'') \neq 0$ .

If we can show that  $\mathcal{F}\langle\eta, \zeta''\rangle$  is separable over  $\mathcal{F}\langle\eta\rangle$ , this will therefore imply that  $\zeta''$  is a generic differential specialization of  $\zeta$  over  $\mathcal{F}\langle\eta\rangle$ , hence that  $(\eta, \zeta'')$  is a generic differential specialization of  $(\eta, \zeta)$  over  $\mathcal{F}$ , and therefore that  $(\eta', \zeta')$  is a generic differential specialization of  $(\eta, \zeta)$  over  $\mathcal{F}$ , establishing the fact that  $BC$  is a constraint of  $(\eta, \zeta)$  over  $\mathcal{F}$ .

If  $p = 0$ , there is nothing to prove, so we may suppose that  $p \neq 0$ . Since the field  $\mathcal{D}$  of constants of  $\mathcal{F}\langle\eta\rangle$  obviously has the property that  $\mathcal{D}^p \subset \mathcal{F}\langle\eta\rangle^p\mathcal{C}$ , and since by hypothesis  $\mathcal{D}$  is separable over  $\mathcal{F}\langle\eta\rangle^p\mathcal{C}$ , we must have  $\mathcal{D} = \mathcal{F}\langle\eta\rangle^p\mathcal{C}$ . By Chapter II, Section 2, part (b) of the corollary to Proposition 2, it follows that  $\mathcal{F}\langle\eta, \zeta''\rangle$  is separable over  $\mathcal{F}\langle\eta\rangle$ .

(d) Let  $\gamma$  be any constant in  $\mathcal{F}\langle\eta\rangle$ . By part (a) of the present proposition,  $(\gamma, \eta)$  is constrained over  $\mathcal{F}$ . If  $\gamma \in \mathcal{F}\langle\eta\rangle^p\mathcal{C}$ , then certainly  $\gamma$  is separably algebraic over  $\mathcal{F}\langle\eta\rangle^p\mathcal{C}$ . Suppose then that  $\gamma \notin \mathcal{F}\langle\eta\rangle^p\mathcal{C}$ . By Chapter II, part (c) of the Corollary to Proposition 2, the differential field  $\mathcal{F}\langle\eta\rangle = \mathcal{F}\langle\gamma, \eta\rangle$  is separable over  $\mathcal{F}\langle\gamma\rangle$ . By part (b) of the present proposition, then  $\gamma$  is constrained over  $\mathcal{F}$ . However, it is obvious that if a constant  $c$  is transcendental over  $\mathcal{F}$ , then every constant is a differential specialization of  $c$  over  $\mathcal{F}$  and therefore  $c$  cannot be constrained over  $\mathcal{F}$ . Hence  $\gamma$  is algebraic over  $\mathcal{F}$ . Because  $\mathcal{F}\langle\eta\rangle$  is separable over  $\mathcal{F}$  it follows that  $\gamma$  is separably algebraic over  $\mathcal{F}$ . Since  $\mathcal{F}$  and  $\mathcal{C}\langle\gamma\rangle$  are linearly disjoint over  $\mathcal{C}$  (see Chapter II, Section 1, Corollary 1 to Theorem 1) we conclude that  $\gamma$  is separably algebraic over  $\mathcal{C}$ , and *a fortiori* over  $\mathcal{F}\langle\eta\rangle^p\mathcal{C}$ .

### EXERCISES

- Let  $\eta = (\eta_i)_{i \in I}$  be a family of elements of an extension of  $\mathcal{F}$ , let  $\mathfrak{p}$  denote the defining differential ideal of  $\eta$  in  $\mathcal{F}\{(y_i)_{i \in I}\}$ , and let  $\mathfrak{a}$  be the intersection of all the  $\mathcal{F}$ -separable prime differential ideals of  $\mathcal{F}\{(y_i)_{i \in I}\}$  that properly contain  $\mathfrak{p}$ . Show that  $\eta$  is constrained over  $\mathcal{F}$  if and only if  $\mathfrak{p}$  is  $\mathcal{F}$ -separable and  $\mathfrak{a} \neq \mathfrak{p}$ , the set of constraints of  $\eta$  over  $\mathcal{F}$  being  $\mathfrak{a} - \mathfrak{p}$ .
- Prove that  $e^x$  is constrained, with constraint  $y$ , over the ordinary differential field of rational functions of a complex variable  $x$  (the derivation operator being  $d/dx$ ).
- Let  $\mathcal{G}$  be any separable extension of  $\mathcal{F}$ . Show that the family  $(\alpha)_{\alpha \in \mathcal{G}}$  is constrained over  $\mathcal{F}$  with constraint 1.
- Show that in Proposition 7(a), (b), and (d), the finiteness conditions cannot be omitted.
- Let  $\mathcal{F}_1$  be a separably algebraic extension of  $\mathcal{F}$ , let  $\eta$  be a finite family of elements of an extension of  $\mathcal{F}_1$ , and suppose that  $\eta$  is constrained over  $\mathcal{F}_1$ . Show that  $\eta$  is constrained over  $\mathcal{F}$ .

## CHAPTER IV

### Algebraic Differential Equations

Throughout this chapter  $\mathcal{U}$  stands for a universal differential field fixed once for all, and the characteristic of  $\mathcal{U}$  is denoted by  $p$ . The set of derivation operators of  $\mathcal{U}$  is denoted by  $\Delta$ , the cardinal number of  $\Delta$  by  $m$ , and the elements of  $\Delta$  by  $\delta_1, \dots, \delta_m$ . The set of derivative operators of  $\mathcal{U}$  is denoted by  $\Theta$  and the set of elements of  $\Theta$  of order less than or equal to  $s$  by  $\Theta(s)$ . The field of constants of  $\mathcal{U}$  is denoted by  $\mathcal{K}$ , and  $(y, z, (y_j)_{j \in \mathbb{N}}, (z_k)_{k \in \mathbb{N}}, (y_{jk})_{j \in \mathbb{N}, k \in \mathbb{N}})$  denotes a family of differential indeterminates over  $\mathcal{U}$ .

#### PART A. CHARACTERISTIC $p$ ARBITRARY

##### 1 Differential affine space. The differential Zariski topology

By a *differential affine space* we mean any one of the sets  $\mathcal{U}^n$  ( $n \in \mathbb{N}$ ). An element  $(\eta_1, \dots, \eta_n)$  of  $\mathcal{U}^n$  will be called a *point*.

If  $\Sigma$  is any subset of the differential polynomial algebra  $\mathcal{U}\{y_1, \dots, y_n\}$  over  $\mathcal{U}$ , by a *zero* of  $\Sigma$  we mean a point of  $\mathcal{U}^n$  at which every element of  $\Sigma$  vanishes. If  $\eta = (\eta_1, \dots, \eta_n)$  is a zero of  $\Sigma$ , we say also that  $\eta$  is a *solution* of the system of (algebraic) differential equations

$$P = 0 \quad (P \in \Sigma).$$

We denote the set of all zeros of  $\Sigma$  by  $\mathfrak{Z}(\Sigma)$ . If  $\Sigma$  consists of a single differential polynomial  $A$ , we write  $\mathfrak{Z}(A)$  instead of  $\mathfrak{Z}(\Sigma)$ .

It is apparent that if  $(\Sigma_i)_{i \in I}$  is a family of subsets of  $\mathcal{U}\{y_1, \dots, y_n\}$ , then  $\bigcap_{i \in I} \mathfrak{Z}(\Sigma_i) = \mathfrak{Z}(\bigcup_{i \in I} \Sigma_i)$ ; also,  $\emptyset = \mathfrak{Z}(1)$ . Finally, if  $\Sigma$  and  $T$  are subsets of  $\mathcal{U}\{y_1, \dots, y_n\}$ , then  $\mathfrak{Z}(\Sigma) \cup \mathfrak{Z}(T) = \mathfrak{Z}(\Sigma T)$ . Thus, the subsets  $\mathcal{V}$  of  $\mathcal{U}^n$  for which there exists a set  $\Sigma \subset \mathcal{U}\{y_1, \dots, y_n\}$  with  $\mathcal{V} = \mathfrak{Z}(\Sigma)$  are the closed sets for a topology on  $\mathcal{U}^n$ . We call it the differential Zariski topology on  $\mathcal{U}^n$ . When we use topological terms in connection with  $\mathcal{U}^n$  without specific qualification they will always refer to the differential Zariski topology.

If  $\mathcal{M}$  is any subset of  $\mathcal{U}^n$ , we denote by  $\bar{\mathcal{M}}$  the closure of  $\mathcal{M}$  (i.e., the smallest closed set containing  $\mathcal{M}$ ).

2 Generic zeros. The theorem of zeros

Let  $\mathcal{F}$  be a differential subfield of  $\mathcal{U}$  over which  $\mathcal{U}$  is semiuniversal (Chapter II, Section 2).

If  $\eta$  is a point of  $\mathcal{U}^n$ , the defining differential ideal of  $\eta$  in  $\mathcal{F}\{y_1, \dots, y_n\}$  is prime. If  $\mathfrak{p}$  is any prime differential ideal of  $\mathcal{F}\{y_1, \dots, y_n\}$ , a point of  $\mathcal{U}^n$  having  $\mathfrak{p}$  as its defining differential ideal in  $\mathcal{F}\{y_1, \dots, y_n\}$  is called a generic zero of  $\mathfrak{p}$ . If  $\eta$  is a generic zero of  $\mathfrak{p}$ , then every zero of  $\mathfrak{p}$  is a differential specialization of  $\eta$  over  $\mathcal{F}$ . In particular, two generic zeros of  $\mathfrak{p}$  are generic differential specializations over  $\mathcal{F}$  of each other. The following proposition is an immediate consequence of the definition of semiuniversal extension.

**Proposition 1** *If  $\mathcal{F}$  is a differential subfield of  $\mathcal{U}$  over which  $\mathcal{U}$  is semiuniversal, then every  $\mathcal{F}$ -separable prime differential ideal of  $\mathcal{F}\{y_1, \dots, y_n\}$  has a generic zero.*

Consider now the  $\mathcal{F}$ -separable differential ideal  $\{\Sigma\}_{\mathcal{F}\{y_1, \dots, y_n\}/\mathcal{F}} = \{\Sigma\}_{\mathcal{F}}$  of  $\mathcal{F}\{y_1, \dots, y_n\}$  generated by a set  $\Sigma \subset \mathcal{F}\{y_1, \dots, y_n\}$ , and let  $B$  be any differential polynomial in  $\mathcal{F}\{y_1, \dots, y_n\}$ . If  $B \notin \{\Sigma\}_{\mathcal{F}}$ , then  $B$  fails to be an element of some component  $\mathfrak{p}$  of  $\{\Sigma\}_{\mathcal{F}}$ ;  $\mathfrak{p}$  is an  $\mathcal{F}$ -separable prime differential ideal. Hence  $\mathfrak{p}$  has a generic zero  $\eta$ , and  $B(\eta) \neq 0$ . By Chapter III, Section 10, Proposition 7, there exists a differential specialization  $\eta'$  of  $\eta$  over  $\mathcal{F}$  such that  $\eta'$  is constrained over  $\mathcal{F}$  and  $B(\eta') \neq 0$ . Because  $\mathcal{U}$  is semiuniversal over  $\mathcal{F}$  we may suppose that  $\eta' \in \mathcal{U}^n$ . Thus,  $\eta'$  is a zero of  $\Sigma$  that is constrained over  $\mathcal{F}$  and that is not a zero of  $B$ . On the other hand, if  $\alpha$  is any zero of  $\Sigma$  that is separable over  $\mathcal{F}$ , then the defining differential ideal of  $\alpha$  in  $\mathcal{F}\{y_1, \dots, y_n\}$  is  $\mathcal{F}$ -separable and prime and contains  $\Sigma$ , and consequently contains  $\{\Sigma\}_{\mathcal{F}}$ . Thus, we have the following result.

**Theorem 1** *Let  $\mathcal{F}$  be a differential subfield of  $\mathcal{U}$  over which  $\mathcal{U}$  is semiuniversal, let  $\Sigma$  be a subset and let  $B$  be an element of the differential polynomial algebra*

$\mathcal{F}\{y_1, \dots, y_n\}$ . If  $B \in \{\Sigma\}_{\mathcal{F}}$ , then  $B$  vanishes at every  $\mathcal{F}$ -separable zero of  $\Sigma$ . Conversely, if  $B$  vanishes at every  $\mathcal{F}$ -constrained zero of  $\Sigma$ , then  $B \in \{\Sigma\}_{\mathcal{F}}$ .

3 Closed sets and  $\mathcal{U}$ -separable differential ideals

A topological space is said to be *irreducible* if it is not empty and is not a union of two closed proper subsets (or, equivalently, if it is not empty and the intersection of two nonempty open sets is always nonempty). A set of points in a topological space is called *irreducible* if it is an irreducible subspace. It is easy to see that an irreducible set must have an irreducible closure. By an *irreducible component* of a topological space is meant a maximal element of the set of irreducible sets in the space. By the preceding remark, an irreducible component is closed. Every point is contained in an irreducible set (e.g., the set consisting solely of the point). Also, a nonempty totally ordered set of irreducible sets is easily seen to have an irreducible union. Hence, by Zorn's lemma, every point is contained in an irreducible component, that is, *a topological space is the union of its irreducible components*.

A topological space is said to be *Noetherian* if every nonempty set of closed sets has a minimal element. A closed set that is not a finite union of irreducible closed sets is, in particular, not irreducible, and hence is the union of two closed proper subsets. As one of these must evidently fail to be a finite union of irreducible closed sets, we see that among the closed sets that are not finite unions of irreducible closed sets there cannot be a minimal one. It follows that in a Noetherian topological space every closed set  $V$  is a finite union of irreducible closed sets. If from such a union the superfluous irreducible closed sets are discarded, the remaining ones are, as is easy to see, the irreducible components of  $V$ . Thus, *in a Noetherian topological space every closed set has only a finite number of irreducible components*.

Let us return now to the differential affine space  $\mathcal{U}^n$ . For any subset  $\mathcal{M}$  of  $\mathcal{U}^n$  we denote by  $\mathfrak{A}(\mathcal{M})$  the set of all differential polynomials in  $\mathcal{U}\{y_1, \dots, y_n\}$  that vanish at every point of  $\mathcal{M}$ . In the special case in which  $\mathcal{M}$  consists of a single point  $\alpha = (\alpha_1, \dots, \alpha_n)$ , we see that the set  $\mathfrak{A}(\alpha) = \mathfrak{A}(\mathcal{M})$  coincides with the differential ideal  $[y_1 - \alpha_1, \dots, y_n - \alpha_n]$  of  $\mathcal{U}\{y_1, \dots, y_n\}$ , which is  $\mathcal{U}$ -separable and prime. In the general case evidently  $\mathfrak{A}(\mathcal{M}) = \bigcap_{\alpha \in \mathcal{M}} \mathfrak{A}(\alpha)$ , so that  $\mathfrak{A}(\mathcal{M})$  is a  $\mathcal{U}$ -separable differential ideal of  $\mathcal{U}\{y_1, \dots, y_n\}$ .

**Theorem 2** (a) *For any subset  $\mathcal{M}$  of  $\mathcal{U}^n$ ,  $\bar{\mathcal{M}} = \mathfrak{Z}(\mathfrak{A}(\mathcal{M}))$ .*

(b) *For any subset  $\Sigma$  of  $\mathcal{U}\{y_1, \dots, y_n\}$ ,  $\{\Sigma\}_{\mathcal{U}} = \mathfrak{A}(\mathfrak{Z}(\Sigma))$ .*

*Proof* (a) For some  $T$ ,  $\bar{\mathcal{M}} = \mathfrak{Z}(T)$ , and obviously  $T \subset \mathfrak{A}(\mathcal{M})$ . This implies that  $\bar{\mathcal{M}} = \mathfrak{Z}(T) \supset \mathfrak{Z}(\mathfrak{A}(\mathcal{M}))$ . However,  $\mathfrak{Z}(\mathfrak{A}(\mathcal{M}))$  is a closed set containing  $\mathcal{M}$ , and therefore contains  $\bar{\mathcal{M}}$ .

(b) By Chapter III, Section 3,  $\mathfrak{A}(\mathfrak{Z}(\Sigma))$  and  $\{\Sigma\}_{/\mathcal{U}}$  have a common differential field of definition  $\mathcal{F}$  that is a finitely generated extension of the prime field, and  $\{\Sigma\}_{/\mathcal{U}} \cap \mathcal{F}\{y_1, \dots, y_n\}$  is an  $\mathcal{F}$ -separable differential ideal of  $\mathcal{F}\{y_1, \dots, y_n\}$ . By Chapter III, Section 7, Proposition 4,  $\mathcal{U}$  is a universal extension of  $\mathcal{F}$ . Every zero of  $\{\Sigma\}_{/\mathcal{U}} \cap \mathcal{F}\{y_1, \dots, y_n\}$  is a zero of  $\mathcal{U} \cdot (\{\Sigma\}_{/\mathcal{U}} \cap \mathcal{F}\{y_1, \dots, y_n\}) = \{\Sigma\}_{/\mathcal{U}}$ , hence of  $\Sigma$ , hence of  $\mathfrak{A}(\mathfrak{Z}(\Sigma))$ , and hence of  $\mathfrak{A}(\mathfrak{Z}(\Sigma)) \cap \mathcal{F}\{y_1, \dots, y_n\}$ . It follows by Theorem 1 that  $\mathfrak{A}(\mathfrak{Z}(\Sigma)) \cap \mathcal{F}\{y_1, \dots, y_n\} \subset \{\Sigma\}_{/\mathcal{U}} \cap \mathcal{F}\{y_1, \dots, y_n\}$ , whence

$$\begin{aligned} \mathfrak{A}(\mathfrak{Z}(\Sigma)) &= \mathcal{U} \cdot (\mathfrak{A}(\mathfrak{Z}(\Sigma)) \cap \mathcal{F}\{y_1, \dots, y_n\}) \\ &\subset \mathcal{U} \cdot (\{\Sigma\}_{/\mathcal{U}} \cap \mathcal{F}\{y_1, \dots, y_n\}) = \{\Sigma\}_{/\mathcal{U}}. \end{aligned}$$

However,  $\mathfrak{A}(\mathfrak{Z}(\Sigma))$  is a  $\mathcal{U}$ -separable differential ideal containing  $\Sigma$ , and therefore contains  $\{\Sigma\}_{/\mathcal{U}}$ .

**Corollary 1** *The mapping  $\mathcal{V} \mapsto \mathfrak{A}(\mathcal{V})$  of the set of all closed sets in  $\mathcal{U}^n$  into the set of all  $\mathcal{U}$ -separable differential ideals of  $\mathcal{U}\{y_1, \dots, y_n\}$ , and the mapping  $\mathfrak{a} \mapsto \mathfrak{Z}(\mathfrak{a})$  of the set of all  $\mathcal{U}$ -separable differential ideals of  $\mathcal{U}\{y_1, \dots, y_n\}$  into the set of all closed sets in  $\mathcal{U}^n$ , are bijective and inverse to each other.*

This is immediate from the theorem.

Because  $\mathfrak{A}(\mathcal{V}_1 \cup \mathcal{V}_2) = \mathfrak{A}(\mathcal{V}_1) \cap \mathfrak{A}(\mathcal{V}_2)$ , a closed set  $\mathcal{V}$  in  $\mathcal{U}^n$  is irreducible if and only if the corresponding ideal  $\mathfrak{A}(\mathcal{V})$  of  $\mathcal{U}\{y_1, \dots, y_n\}$  is prime. Because of the obvious equivalence

$$\mathcal{V}_1 \subset \mathcal{V}_2 \Leftrightarrow \mathfrak{A}(\mathcal{V}_1) \supset \mathfrak{A}(\mathcal{V}_2),$$

$\mathcal{V}_1$  is an irreducible component of  $\mathcal{V}$  if and only if  $\mathfrak{A}(\mathcal{V}_1)$  is a component of  $\mathfrak{A}(\mathcal{V})$ . The same equivalence together with Chapter III, Section 4, Corollary 5 to Theorem 1, yields the following corollary.

**Corollary 2** *The differential affine space  $\mathcal{U}^n$  is Noetherian.*

For any irreducible closed set  $\mathcal{V}$ , we define the *differential dimension polynomial*  $\omega_{\mathcal{V}}$  of  $\mathcal{V}$  by the formula  $\omega_{\mathcal{V}} = \omega_{\mathfrak{A}(\mathcal{V})}$ . Similarly, we define the *differential dimension* of  $\mathcal{V}$ , the *differential type* of  $\mathcal{V}$ , and the *typical differential dimension* of  $\mathcal{V}$ , to be, respectively, the differential dimension of  $\mathfrak{A}(\mathcal{V})$ , the differential type of  $\mathfrak{A}(\mathcal{V})$ , and the typical differential dimension of  $\mathfrak{A}(\mathcal{V})$ . We shall not take the trouble of translating into the language of closed sets all the material of Chapter III, Section 5.

#### 4 The relative topologies; differential fields of definition

Let  $\mathcal{F}$  be a differential subfield of  $\mathcal{U}$ . We shall call a set  $\mathcal{V} \subset \mathcal{U}^n$   $\mathcal{F}$ -closed if there exists a set  $\Sigma \subset \mathcal{F}\{y_1, \dots, y_n\}$  such that  $\mathcal{V} = \mathfrak{Z}(\Sigma)$ . The same com-

putations that we used in the case of the differential Zariski topology in Section 1 show that the  $\mathcal{F}$ -closed sets are the closed sets for a topology on  $\mathcal{U}^n$ , which we call the differential Zariski topology *relative to  $\mathcal{F}$* , or simply the  $\mathcal{F}$ -topology, of  $\mathcal{U}^n$ . In the special case  $\mathcal{F} = \mathcal{U}$  we regain the "absolute" differential Zariski topology of Section 1.

If  $\mathcal{G}$  is another differential subfield of  $\mathcal{U}$ , and if  $\mathcal{F} \subset \mathcal{G}$ , then every  $\mathcal{F}$ -closed set is  $\mathcal{G}$ -closed. In particular, every  $\mathcal{F}$ -closed set is closed. It follows from this and Section 3, Corollary 1 to Theorem 2, that  $\mathcal{U}^n$  is *Noetherian with respect to the  $\mathcal{F}$ -topology*. We use the terms  $\mathcal{F}$ -irreducible and  $\mathcal{F}$ -irreducible component in the obvious sense.

If  $\mathcal{V}$  is  $\mathcal{F}$ -closed, then the intersection  $\mathfrak{a} = \mathfrak{A}(\mathcal{V}) \cap \mathcal{F}\{y_1, \dots, y_n\}$  is a perfect differential ideal of  $\mathcal{F}\{y_1, \dots, y_n\}$ . Since evidently  $\mathfrak{Z}(\mathfrak{a}) = \mathcal{V}$ , Section 3, Theorem 2, shows that  $\{\mathfrak{a}\}_{/\mathcal{U}} = \mathfrak{A}(\mathfrak{Z}(\mathfrak{a})) = \mathfrak{A}(\mathcal{V})$ , so that  $\mathfrak{a}$  has the property that

$$\{\mathfrak{a}\}_{/\mathcal{U}} \cap \mathcal{F}\{y_1, \dots, y_n\} = \mathfrak{a}. \tag{1}$$

Conversely, if  $\mathfrak{a}$  is any perfect differential ideal of  $\mathcal{F}\{y_1, \dots, y_n\}$  having this property, then  $\mathfrak{Z}(\mathfrak{a})$  is  $\mathcal{F}$ -closed and  $\mathfrak{A}(\mathfrak{Z}(\mathfrak{a})) \cap \mathcal{F}\{y_1, \dots, y_n\} = \{\mathfrak{a}\}_{/\mathcal{U}} \cap \mathcal{F}\{y_1, \dots, y_n\} = \mathfrak{a}$ . Thus, the mapping  $\mathcal{V} \mapsto \mathfrak{A}(\mathcal{V}) \cap \mathcal{F}\{y_1, \dots, y_n\}$  from the set of all  $\mathcal{F}$ -closed sets in  $\mathcal{U}^n$  into the set of all perfect differential ideals  $\mathfrak{a}$  of  $\mathcal{F}\{y_1, \dots, y_n\}$  satisfying (1), and the mapping  $\mathfrak{a} \mapsto \mathfrak{Z}(\mathfrak{a})$  in the opposite direction, are bijective and inverse to each other.

If  $\mathfrak{M}$  is any set of perfect differential ideals  $\mathfrak{a}$  of  $\mathcal{F}\{y_1, \dots, y_n\}$  satisfying (1), then

$$\begin{aligned} \bigcap_{\mathfrak{a} \in \mathfrak{M}} \mathfrak{a} &\subset \left\{ \bigcap_{\mathfrak{a} \in \mathfrak{M}} \mathfrak{a} \right\}_{/\mathcal{U}} \cap \mathcal{F}\{y_1, \dots, y_n\} \\ &= \bigcap_{\mathfrak{a} \in \mathfrak{M}} \{\mathfrak{a}\}_{/\mathcal{U}} \cap \mathcal{F}\{y_1, \dots, y_n\} = \bigcap_{\mathfrak{a} \in \mathfrak{M}} \mathfrak{a}, \end{aligned}$$

so that  $\bigcap_{\mathfrak{a} \in \mathfrak{M}} \mathfrak{a}$  satisfies condition (1). Similar computations show that if  $\mathfrak{M}$  is nonempty and totally ordered by inclusion, then  $\bigcup_{\mathfrak{a} \in \mathfrak{M}} \mathfrak{a}$  also satisfies (1), and that if  $S \in \mathcal{F}\{y_1, \dots, y_n\}$ , then  $\mathfrak{a} : S$  satisfies (1) whenever  $\mathfrak{a}$  does. Thus, the set of perfect differential ideals  $\mathfrak{a}$  of  $\mathcal{F}\{y_1, \dots, y_n\}$  that satisfy condition (1) is a perfect differential conservative system. Since the bijection  $\mathcal{V} \mapsto \mathfrak{A}(\mathcal{V}) \cap \mathcal{F}\{y_1, \dots, y_n\}$  of the set of  $\mathcal{F}$ -closed subsets of  $\mathcal{U}^n$  onto this conservative system reverses inclusions, and since  $\mathcal{U}^n$  is Noetherian relative to the  $\mathcal{F}$ -topology, we conclude that *this conservative system is a Noetherian one*.

We shall say that a closed set  $\mathcal{V}$  of  $\mathcal{U}^n$  is *defined over  $\mathcal{F}$*  (or that  $\mathcal{F}$  is a *differential field of definition of  $\mathcal{V}$* ) if  $\mathcal{F}$  is a differential field of definition of  $\mathfrak{A}(\mathcal{V})$ , that is (see Chapter III, Section 3), if  $\mathcal{U} \cdot (\mathfrak{A}(\mathcal{V}) \cap \mathcal{F}\{y_1, \dots, y_n\}) = \mathfrak{A}(\mathcal{V})$ . It is obvious that every closed set defined over  $\mathcal{F}$  is  $\mathcal{F}$ -closed. Further-



more, since  $\mathfrak{U}(\mathcal{V})$  is  $\mathcal{U}$ -separable, we see by a remark in Chapter III, Section 3, that if  $\mathcal{V}$  is defined over  $\mathcal{F}$ , then  $\mathfrak{U}(\mathcal{V}) \cap \mathcal{F}\{y_1, \dots, y_n\}$  is  $\mathcal{F}$ -separable. Conversely, if  $\mathfrak{a}$  is any  $\mathcal{F}$ -separable differential ideal of  $\mathcal{F}\{y_1, \dots, y_n\}$ , then by Chapter 0, Section 12, Corollary 1 to Proposition 7,  $\mathcal{U}\mathfrak{a}$  is  $\mathcal{U}$ -separable and hence coincides with  $\{\mathfrak{a}\}_{\mathcal{U}}$ , so that by Chapter 0, Section 10, Lemma 9,  $\mathfrak{a}$  satisfies condition (1). Furthermore  $\mathfrak{U}(\mathfrak{Z}(\mathfrak{a})) = \{\mathfrak{a}\}_{\mathcal{U}} = \mathcal{U}\mathfrak{a}$ , so that the closed set  $\mathfrak{Z}(\mathfrak{a})$  is defined over  $\mathcal{F}$ . Thus, the mapping  $\mathcal{V} \mapsto \mathfrak{U}(\mathcal{V}) \cap \mathcal{F}\{y_1, \dots, y_n\}$  from the set of all closed sets in  $\mathcal{U}^n$  that are defined over  $\mathcal{F}$  into the set of all  $\mathcal{F}$ -separable differential ideals of  $\mathcal{F}\{y_1, \dots, y_n\}$ , and the mapping  $\mathfrak{a} \mapsto \mathfrak{Z}(\mathfrak{a})$  in the opposite direction, are bijective and inverse to each other.

It follows easily from this that if  $\mathcal{V}$  is a closed set defined over  $\mathcal{F}$ , then so are all the  $\mathcal{F}$ -irreducible components of  $\mathcal{V}$ . Also, if  $\mathcal{V}$  and  $\mathcal{V}'$  are closed sets defined over  $\mathcal{F}$ , then so is  $\mathcal{V} \cup \mathcal{V}'$ .

Of course, if  $\mathcal{F}$  is differentially perfect (in particular, if  $p = 0$ ), then every  $\mathcal{F}$ -closed set is defined over  $\mathcal{F}$ .

If  $\mathcal{V}$  is an  $\mathcal{F}$ -closed set and  $\eta$  is a point of  $\mathcal{U}^n$ , we say that  $\eta$  is a *generic point of  $\mathcal{V}$  over  $\mathcal{F}$*  if  $\eta$  is a generic zero of  $\mathfrak{U}(\mathcal{V}) \cap \mathcal{F}\{y_1, \dots, y_n\}$ , or equivalently, if  $\mathcal{V}$  is the set of all points of  $\mathcal{U}^n$  that are differential specializations of  $\eta$  over  $\mathcal{F}$ , or again equivalently, if  $\mathcal{V}$  is the  $\mathcal{F}$ -closure (i.e., the closure relative to the  $\mathcal{F}$ -topology) of the set consisting solely of the point  $\eta$ . If  $\eta$  is a generic point of  $\mathcal{V}$  over  $\mathcal{F}$ , then  $\mathcal{V}$  must be  $\mathcal{F}$ -irreducible, and if  $\eta$  is  $\mathcal{F}$ -separable, then  $\mathcal{V}$  must be defined over  $\mathcal{F}$ . Section 2, Proposition 1 shows that, conversely, if  $\mathcal{V}$  is an  $\mathcal{F}$ -irreducible  $\mathcal{F}$ -closed set defined over  $\mathcal{F}$  and if  $\mathcal{U}$  is semiuniversal over  $\mathcal{F}$ , then  $\mathcal{V}$  has a generic point over  $\mathcal{F}$ .

It follows from Chapter III, Section 6, Proposition 3, that if  $\mathcal{V}$  is an irreducible closed set in  $\mathcal{U}^n$  and  $\mathcal{F}$  is any differential field of definition of  $\mathcal{V}$ , then  $\omega_{\mathcal{V}} = \omega_{\mathfrak{U}(\mathcal{V}) \cap \mathcal{F}\{y_1, \dots, y_n\}}$ .

### 5 Linear differential ideals

For any differential field  $\mathcal{F}$  we denote the set of all homogeneous linear elements of  $\mathcal{F}\{y_1, \dots, y_n\}$  by  $\mathcal{F}\{y_1, \dots, y_n\}_1$ .

If  $(X_i)_{i \in I}$  is a family of indeterminates over a field  $K$ , and  $\Lambda_0$  is a set of homogeneous linear polynomials in  $K[(X_i)_{i \in I}]$ , then the ideal  $(\Lambda_0)$  is regular over  $K$  (in particular, is prime) and is homogeneous. It follows that if  $\Lambda$  is any subset of  $\mathcal{U}\{y_1, \dots, y_n\}_1$ , and  $\mathcal{F}$  is any differential subfield of  $\mathcal{U}$  with  $\mathcal{F}\{y_1, \dots, y_n\} \supset \Lambda$ , then the differential ideal  $[\Lambda] = (\Theta\Lambda)$  of  $\mathcal{F}\{y_1, \dots, y_n\}$  is regular over  $\mathcal{F}$  and is homogeneous. In particular,

$$[\Lambda] \cap \mathcal{F}\{y_1, \dots, y_n\}_1 = \sum_{\theta \in \Theta, L \in \Lambda} \mathcal{F} \cdot \theta L.$$

We shall call a differential ideal of  $\mathcal{F}\{y_1, \dots, y_n\}$  *linear* if it is generated by a subset of  $\mathcal{F}\{y_1, \dots, y_n\}_1$ . By what we have just seen, every linear differential

ideal of  $\mathcal{F}\{y_1, \dots, y_n\}$  is homogeneous and  $\mathcal{F}$ -regular. Also, the mapping that to each linear differential ideal  $\mathfrak{p}$  of  $\mathcal{F}\{y_1, \dots, y_n\}$  associates the differential subspace  $\mathfrak{p} \cap \mathcal{F}\{y_1, \dots, y_n\}_1$  of the differential vector space  $\mathcal{F}\{y_1, \dots, y_n\}_1$  over  $\mathcal{F}$ , and the mapping that to each differential subspace  $\mathcal{L}$  of  $\mathcal{F}\{y_1, \dots, y_n\}_1$  associates the linear differential ideal  $[\mathcal{L}] = (\mathcal{L})$  of  $\mathcal{F}\{y_1, \dots, y_n\}$ , are bijective and inverse to each other.

If  $\mathcal{G}$  is any extension of  $\mathcal{F}$  in  $\mathcal{U}$ , then  $\mathcal{G}$  and  $\mathcal{F}\{y_1, \dots, y_n\}_1$  are linearly disjoint over  $\mathcal{F}$ . Hence the codimension of the subspace  $\sum_{\theta \in \Theta, L \in \Lambda} \mathcal{F} \cdot \theta L$  of  $\mathcal{F}\{y_1, \dots, y_n\}_1$  equals the codimension of  $\sum_{\theta \in \Theta, L \in \Lambda} \mathcal{G} \cdot \theta L$  in the vector space  $\mathcal{G}\{y_1, \dots, y_n\}_1$  over  $\mathcal{G}$ . In other words, for any set  $\Lambda \subset \mathcal{U}\{y_1, \dots, y_n\}_1$ , the codimension of  $\sum_{\theta \in \Theta, L \in \Lambda} \mathcal{F} \cdot \theta L$  in  $\mathcal{F}\{y_1, \dots, y_n\}_1$  does not depend on the choice of the differential field  $\mathcal{F}$  with  $\mathcal{F}\{y_1, \dots, y_n\} \supset \Lambda$ .

If  $\mathfrak{p}$  is any linear differential ideal of  $\mathcal{F}\{y_1, \dots, y_n\}$ , we call the codimension of  $\mathfrak{p} \cap \mathcal{F}\{y_1, \dots, y_n\}_1$  in  $\mathcal{F}\{y_1, \dots, y_n\}_1$  the *linear dimension* of  $\mathfrak{p}$ . This number need not be finite. By the above, for any extension  $\mathcal{G}$  of  $\mathcal{F}$ ,  $\mathcal{G}\mathfrak{p}$  is a linear differential ideal of  $\mathcal{G}\{y_1, \dots, y_n\}$  having the same linear dimension as  $\mathfrak{p}$ . Conversely, it is easy to see that if  $\mathfrak{q}$  is a linear differential ideal of  $\mathcal{G}\{y_1, \dots, y_n\}$  for which  $\mathcal{F}$  is a differential field of definition, then  $\mathfrak{q} \cap \mathcal{F}\{y_1, \dots, y_n\}$  is a linear differential ideal of  $\mathcal{F}\{y_1, \dots, y_n\}$  having the same linear dimension as  $\mathfrak{q}$ . It is obvious that  $\mathfrak{Z}(\Lambda)$  is a vector subspace of the vector space  $\mathcal{U}^n$  over  $\mathcal{K}$ . A basis of  $\mathfrak{Z}(\Lambda)$  is called a *fundamental system of zeros* of  $\Lambda$  (or of the linear differential ideal  $[\Lambda]$  of  $\mathcal{F}\{y_1, \dots, y_n\}$ ,  $\mathcal{F}$  denoting any differential subfield of  $\mathcal{U}$  with  $\mathcal{F}\{y_1, \dots, y_n\} \supset \Lambda$ ).

**Proposition 2** *Let  $l \in \mathbb{N}$ . If  $\mathcal{V}$  is any  $l$ -dimensional subspace of the vector space  $\mathcal{U}^n$  over  $\mathcal{K}$ , then  $\mathcal{V}$  is closed and  $\mathfrak{U}(\mathcal{V})$  is a linear differential ideal of  $\mathcal{U}\{y_1, \dots, y_n\}$  of linear dimension  $l$ . If  $\mathfrak{p}$  is any linear differential ideal of  $\mathcal{U}\{y_1, \dots, y_n\}$  of linear dimension  $l$ , then  $\mathfrak{Z}(\mathfrak{p})$  is an  $l$ -dimensional subspace of the vector space  $\mathcal{U}^n$  over  $\mathcal{K}$ .*

*Proof* Let  $\mathfrak{p}$  be a linear differential ideal of  $\mathcal{U}\{y_1, \dots, y_n\}$  of linear dimension  $l$ . Setting  $\mathcal{L} = \mathfrak{p} \cap \mathcal{U}\{y_1, \dots, y_n\}_1$ , we see that there exist  $l$  operators  $\theta_1, \dots, \theta_l \in \Theta$  and  $l$  indices  $k(1), \dots, k(l)$  such that the cosets  $\theta_1 y_{k(1)} + \mathcal{L}, \dots, \theta_l y_{k(l)} + \mathcal{L}$  form a basis of the vector space  $\mathcal{U}\{y_1, \dots, y_n\}_1 / \mathcal{L}$ . For every  $\theta \in \Theta$  and every index  $k$ , the derivative  $\theta y_k$  is congruent (mod  $\mathcal{L}$ ) to a linear combination of  $\theta_1 y_{k(1)}, \dots, \theta_l y_{k(l)}$  over  $\mathcal{U}$ . It follows that if  $(\eta_{11}, \dots, \eta_{1n}), \dots, (\eta_{l+1,1}, \dots, \eta_{l+1,n})$  are any  $l+1$  elements of  $\mathfrak{Z}(\mathcal{L}) = \mathfrak{Z}(\mathfrak{p})$ , and if we fix any operators  $\theta'_1, \dots, \theta'_{l+1} \in \Theta$  and indices  $k'(1), \dots, k'(l+1)$ , then each row of the matrix  $(\theta'_i \eta_{j, k'(i)})_{1 \leq i \leq l+1, 1 \leq j \leq l+1}$  is a linear combination of the  $l$  vectors  $(\theta_1 \eta_{1, k(1)}, \dots, \theta_1 \eta_{l+1, k(1)}), \dots, (\theta_l \eta_{1, k(l)}, \dots, \theta_l \eta_{l+1, k(l)})$ , so that the determinant of this matrix is 0. Then by Chapter II, Section 1, Theorem 1, the  $l+1$  elements of  $\mathfrak{Z}(\mathfrak{p})$  are linearly dependent over  $\mathcal{K}$ . Hence

$$\dim \mathfrak{Z}(\mathfrak{p}) \leq l. \tag{2}$$

Conversely, let  $\mathcal{V}$  be an  $l$ -dimensional subspace of the vector space  $\mathcal{U}^n$  over  $\mathcal{X}$ , and fix a basis  $(\eta_{11}, \dots, \eta_{1n}), \dots, (\eta_{l1}, \dots, \eta_{ln})$  of  $\mathcal{V}$ . By Chapter II, Section 1, Theorem 1, there exist  $\theta_1, \dots, \theta_l \in \Theta$  and indices  $k(1), \dots, k(l)$  such that  $\det(\theta_i \eta_{j, k(i)})_{1 \leq i \leq l, 1 \leq j \leq n} \neq 0$ . For any  $\theta \in \Theta$  and any index  $k$  the differential polynomial

$$\det \begin{pmatrix} \theta y_k & \theta \eta_{1k} & \cdots & \theta \eta_{lk} \\ \theta_1 y_{k(1)} & \theta_1 \eta_{1, k(1)} & \cdots & \theta_1 \eta_{l, k(1)} \\ \vdots & \vdots & \ddots & \vdots \\ \theta_l y_{k(l)} & \theta_l \eta_{1, k(l)} & \cdots & \theta_l \eta_{l, k(l)} \end{pmatrix}$$

in  $(y_1, \dots, y_n)$  is homogeneous and linear and vanishes at each  $(\eta_{j1}, \dots, \eta_{jn})$ , and hence is an element of  $\mathfrak{A}(\mathcal{V}) \cap \mathcal{U}\{y_1, \dots, y_n\}_1$ . Since the coefficient of  $\theta y_k$  is  $\det(\theta_i \eta_{j, k(i)})_{1 \leq i \leq l, 1 \leq j \leq n} \neq 0$ , we see that  $\theta y_k$  is congruent (mod  $\mathfrak{A}(\mathcal{V}) \cap \mathcal{U}\{y_1, \dots, y_n\}_1$ ) to a linear combination over  $\mathcal{U}$  of  $\theta_1 y_{k(1)}, \dots, \theta_l y_{k(l)}$ . This shows that  $\mathfrak{A}(\mathcal{V}) \cap \mathcal{U}\{y_1, \dots, y_n\}_1$  has a finite codimension  $l'$  in  $\mathcal{U}\{y_1, \dots, y_n\}_1$ . Applying (2) to the linear differential ideal  $[\mathfrak{A}(\mathcal{V}) \cap \mathcal{U}\{y_1, \dots, y_n\}_1]$  in place of  $\mathfrak{p}$ , we therefore find that

$$l = \dim \mathcal{V} \leq \dim \mathfrak{Z}(\mathfrak{A}(\mathcal{V}) \cap \mathcal{U}\{y_1, \dots, y_n\}_1) \leq l' \leq l,$$

so that  $\mathcal{V}$  is closed and  $\mathfrak{A}(\mathcal{V}) = \{\mathfrak{A}(\mathcal{V}) \cap \mathcal{U}\{y_1, \dots, y_n\}_1\}_{\mathfrak{A}} = [\mathfrak{A}(\mathcal{V}) \cap \mathcal{U}\{y_1, \dots, y_n\}_1]$ , and hence  $\mathfrak{A}(\mathcal{V})$  is linear and has linear dimension  $l$ . This proves the first part of the proposition. Applying this part to the vector space  $\mathfrak{Z}(\mathfrak{p})$ , we see that  $l$ , the linear dimension of  $\mathfrak{p} = \mathfrak{A}(\mathfrak{Z}(\mathfrak{p}))$ , equals  $\dim \mathfrak{Z}(\mathfrak{p})$ .

**Corollary 1** *The mapping that to each finite dimensional subspace  $\mathcal{V}$  of the vector space  $\mathcal{U}^n$  over  $\mathcal{X}$  associates  $\mathfrak{A}(\mathcal{V})$ , and the mapping that to each linear differential ideal  $\mathfrak{p}$  of  $\mathcal{U}\{y_1, \dots, y_n\}$  of finite linear dimension associates  $\mathfrak{Z}(\mathfrak{p})$ , are bijective and inverse to each other.*

**Corollary 2** *Let  $\mathfrak{p}$  be a linear differential ideal of  $\mathcal{F}\{y_1, \dots, y_n\}$  of finite linear dimension  $l$ . Then  $\mathfrak{p}$  has a fundamental system of zeros*

$$(\eta_{11}, \dots, \eta_{1n}), \dots, (\eta_{l1}, \dots, \eta_{ln})$$

such that the differential field  $\mathcal{G} = \mathcal{F}\langle(\eta_{ij})_{1 \leq i \leq l, 1 \leq j \leq n}\rangle$  is a separable extension of  $\mathcal{F}$  and the field of constants of  $\mathcal{G}$  is a separable algebraic field extension of  $\mathcal{C}^{\text{alg}}$  of finite degree,  $\mathcal{C}$  denoting the field of constants of  $\mathcal{F}$ .

*Proof* The substitution of  $(y_{i1}, \dots, y_{in})$  for  $(y_1, \dots, y_n)$  maps  $\mathfrak{p}$  onto a linear differential ideal  $\mathfrak{p}_i$  of  $\mathcal{F}\{y_{i1}, \dots, y_{in}\}$ . The ideal  $(\mathfrak{p}_1 \cup \dots \cup \mathfrak{p}_l)$  of  $\mathcal{F}\{(y_{ij})_{1 \leq i \leq l, 1 \leq j \leq n}\}$  is evidently a linear differential one, and therefore has a generic zero  $(\zeta_{ij})_{1 \leq i \leq l, 1 \leq j \leq n}$  that is  $\mathcal{F}$ -separable. By Proposition 2,

$\mathfrak{p}$  has a fundamental system of zeros  $(\zeta'_{11}, \dots, \zeta'_{1n}), \dots, (\zeta'_{l1}, \dots, \zeta'_{ln})$ , and we may fix operators  $\theta_1, \dots, \theta_l \in \Theta$  and indices  $k(1), \dots, k(l)$  such that  $\det(\theta_h \zeta'_{i, k(h)})_{1 \leq h \leq l, 1 \leq i \leq l} \neq 0$ . It is evident that  $(\zeta'_{ij})_{1 \leq i \leq l, 1 \leq j \leq n}$  is a zero of  $(\mathfrak{p}_1 \cup \dots \cup \mathfrak{p}_l)$  and hence is a differential specialization of  $(\zeta_{ij})_{1 \leq i \leq l, 1 \leq j \leq n}$  over  $\mathcal{F}$ . Therefore  $(\zeta_{ij})_{1 \leq i \leq l, 1 \leq j \leq n}$  is not a zero of the differential polynomial  $W = \det(\theta_h y_{i, k(h)})_{1 \leq h \leq l, 1 \leq i \leq l}$ . By Chapter III, Section 10, Proposition 6,  $(\zeta_{ij})_{1 \leq i \leq l, 1 \leq j \leq n}$  has a differential specialization  $(\eta_{ij})_{1 \leq i \leq l, 1 \leq j \leq n}$  over  $\mathcal{F}$  that is constrained over  $\mathcal{F}$  with constraint  $W$ , and by Chapter III, Section 10, Proposition 7(d), if we set  $\mathcal{G} = \mathcal{F}\langle(\eta_{ij})_{1 \leq i \leq l, 1 \leq j \leq n}\rangle$ , then the field of constants of  $\mathcal{G}$  is separably algebraic over  $\mathcal{C}^{\text{alg}}$ . Since  $W$  does not vanish at  $(\eta_{ij})_{1 \leq i \leq l, 1 \leq j \leq n}$ , the rows of this matrix are linearly independent over  $\mathcal{X}$  and therefore evidently form a basis of the  $l$ -dimensional vector space  $\mathfrak{Z}(\mathfrak{p})$  over  $\mathcal{X}$ .

**Corollary 3** *Let  $\eta_{ij} \in \mathcal{U}$  ( $1 \leq i \leq l, 1 \leq j \leq n$ ), let  $\theta_h' \in \Theta$  ( $1 \leq h \leq l$ ), let  $k'(1), \dots, k'(l)$  be integers between 1 and  $n$ , inclusive, and suppose that  $\det(\theta_h' \eta_{i, k'(h)})_{1 \leq h \leq l, 1 \leq i \leq l} \neq 0$ . If  $(\eta_{11}, \dots, \eta_{1n}), \dots, (\eta_{l1}, \dots, \eta_{ln})$  form a fundamental system of zeros of some linear differential ideal of  $\mathcal{F}\{y_1, \dots, y_n\}$ , then, for every choice of operators  $\theta_1, \dots, \theta_l \in \Theta$  and of indices  $k(1), \dots, k(l)$ , all the coordinates of the matrix*

$$(\theta_h \eta_{i, k(h)})_{1 \leq h \leq l, 1 \leq i \leq l} (\theta_h' \eta_{i, k'(h)})_{1 \leq h \leq l, 1 \leq i \leq l}^{-1}$$

are in  $\mathcal{F}$ . Conversely, if, for every choice of operators  $\theta_1, \dots, \theta_l \in \Theta$  with  $\theta_h \in \Theta(h)$  ( $1 \leq h \leq l$ ) and of indices  $k(1), \dots, k(l)$ , the determinant of this matrix is in  $\mathcal{F}$ , then  $(\eta_{11}, \dots, \eta_{1n}), \dots, (\eta_{l1}, \dots, \eta_{ln})$  form a fundamental system of zeros of a linear differential ideal of  $\mathcal{F}\{y_1, \dots, y_n\}$ .

*Proof* Suppose  $(\eta_{11}, \dots, \eta_{1n}), \dots, (\eta_{l1}, \dots, \eta_{ln})$  form a fundamental system of zeros of a linear differential ideal  $\mathfrak{p}$  of  $\mathcal{F}\{y_1, \dots, y_n\}$ , and therefore also of the linear differential ideal  $\mathcal{U}\mathfrak{p}$  of  $\mathcal{U}\{y_1, \dots, y_n\}$ . By the proposition,  $\mathcal{U}\mathfrak{p}$  has linear dimension  $l$ , hence  $\mathfrak{p}$  does too, so that we may fix operators  $\theta_1'', \dots, \theta_l''$  and indices  $k''(1), \dots, k''(l)$  such that  $\theta_1'' y_{k''(1)}, \dots, \theta_l'' y_{k''(l)}$  form a basis of  $\mathcal{F}\{y_1, \dots, y_n\}_1 \pmod{\mathfrak{p} \cap \mathcal{F}\{y_1, \dots, y_n\}_1}$ . For any  $\theta \in \Theta$  and any index  $k$ , there exist elements  $a_{\theta k 1}, \dots, a_{\theta k l} \in \mathcal{F}$  such that

$$\theta y_k \equiv \sum_{1 \leq \lambda \leq l} a_{\theta k \lambda} \theta_\lambda'' y_{k''(\lambda)} \pmod{\mathfrak{p} \cap \mathcal{F}\{y_1, \dots, y_n\}_1}.$$

Hence for any  $\theta_1, \dots, \theta_l \in \Theta$  and any indices  $k(1), \dots, k(l)$  we have

$$\begin{aligned} (\theta_h \eta_{i, k(h)})_{1 \leq h \leq l, 1 \leq i \leq l} &= \left( \sum_{1 \leq \lambda \leq l} a_{\theta_h k(h) \lambda} \theta_\lambda'' \eta_{i, k''(\lambda)} \right)_{1 \leq h \leq l, 1 \leq i \leq l} \\ &= (a_{\theta_h k(h) i})_{1 \leq h \leq l, 1 \leq i \leq l} (\theta_h'' \eta_{i, k''(h)})_{1 \leq h \leq l, 1 \leq i \leq l}, \end{aligned}$$

and from this we see that the matrix in the statement of the corollary has all its coordinates in  $\mathcal{F}$ .

Conversely, suppose the determinant of this matrix is in  $\mathcal{F}$  whenever  $\theta_h \in \Theta(h)$  for every  $h$ . Because  $\det(\theta_h' \eta_{i, k'(h)})_{1 \leq h \leq l, 1 \leq i \leq l} \neq 0$ , the  $l$  elements  $(\eta_{11}, \dots, \eta_{1n}), \dots, (\eta_{l1}, \dots, \eta_{ln})$  of  $\mathcal{U}^n$  form a basis of a vector space  $\mathcal{V}$  over  $\mathcal{K}$ . Also, we can fix operators  $\theta_h'' \in \Theta(h-1)$  ( $1 \leq h \leq l$ ) and indices  $k''(1), \dots, k''(l)$  such that  $\det(\theta_h'' \eta_{i, k''(h)})_{1 \leq h \leq l, 1 \leq i \leq l} \neq 0$ . For each  $\theta \in \Theta(l)$  and each index  $k$ , the differential polynomial

$$L_{\theta, k} = \det \begin{pmatrix} \theta y_k & \theta \eta_{1k} & \cdots & \theta \eta_{lk} \\ \theta_1'' y_{k''(1)} & \theta_1'' \eta_{1, k''(1)} & \cdots & \theta_1'' \eta_{l, k''(1)} \\ \vdots & \vdots & \ddots & \vdots \\ \theta_l'' y_{k''(l)} & \theta_l'' \eta_{1, k''(l)} & \cdots & \theta_l'' \eta_{l, k''(l)} \end{pmatrix} \det(\theta_h' \eta_{i, k'(h)})_{1 \leq h \leq l, 1 \leq i \leq l}^{-1}$$

is of the form  $\alpha \theta y_k + \alpha_1 \theta_1'' y_{k''(1)} + \cdots + \alpha_l \theta_l'' y_{k''(l)}$ , where  $\alpha, \alpha_1, \dots, \alpha_l \in \mathcal{F}$  and  $\alpha \neq 0$ . It easily follows that the linear differential ideal  $\mathfrak{p} = [(L_{\theta, k})_{\theta \in \Theta(l), 1 \leq k \leq n}]$  of  $\mathcal{F}\{y_1, \dots, y_n\}$  has the property that

$$\sum_{1 \leq i \leq l} \mathcal{F} \theta_i'' y_{k''(i)} + \mathfrak{p} \cap \mathcal{F}\{y_1, \dots, y_n\}_1 = \mathcal{F}\{y_1, \dots, y_n\}_1,$$

so that  $\mathfrak{p}$  (and therefore also  $\mathcal{U}\mathfrak{p}$ ) has linear dimension less than or equal to  $l$ . Since obviously  $\mathfrak{Z}(\mathfrak{p}) \supset \mathcal{V}$ , we see by the proposition that this linear dimension is equal to  $\dim \mathfrak{Z}(\mathcal{U}\mathfrak{p}) = \dim \mathfrak{Z}(\mathfrak{p}) \geq \dim \mathcal{V} = l$ . Hence the linear dimension of  $\mathfrak{p}$  is  $l$  and  $(\eta_{11}, \dots, \eta_{1n}), \dots, (\eta_{l1}, \dots, \eta_{ln})$  form a fundamental system of zeros of  $\mathfrak{p}$ .

**Proposition 3** Let  $a_i = (a_{ij'})_{1 \leq j' \leq n, 1 \leq i \leq m}$  be an  $n \times n$  matrix over  $\mathcal{F}$  ( $1 \leq i \leq m$ ), let  $A_{ij} = \delta_i y_j - \sum_{1 \leq j' \leq n} a_{ij'} y_{j'}$  ( $1 \leq i \leq m, 1 \leq j \leq n$ ), and let  $\mathfrak{p}$  denote the linear differential ideal  $[(A_{ij})_{1 \leq i \leq m, 1 \leq j \leq n}]$  of  $\mathcal{F}\{y_1, \dots, y_n\}$ . Then the linear dimension of  $\mathfrak{p}$  is less than or equal to  $n$ . A necessary and sufficient condition that it be equal to  $n$  is that  $a_1, \dots, a_m$  satisfy the integrability conditions

$$\delta_i a_{i'} + a_i a_{i'} = \delta_{i'} a_i + a_i a_{i'} \quad (1 \leq i \leq m, 1 \leq i' \leq m).$$

When this is the case then  $\mathfrak{p}$  does not contain a nonzero differential polynomial of order 0.

REMARK If  $a = (a_{ki})$  is a matrix over  $\mathcal{U}$  and  $\delta \in \Delta$ , then  $\delta a$  denotes the matrix  $(\delta a_{ki})$ .

Proof It is obvious that every  $\theta y_j$  ( $\theta \in \Theta, 1 \leq j \leq n$ ) is congruent (mod  $\mathfrak{p}$ )

to a linear combination of  $y_1, \dots, y_n$  over  $\mathcal{F}$ ; hence the linear dimension of  $\mathfrak{p}$  is less than or equal to  $n$ . A simple computation yields the equation

$$\delta_i A_{i'j} - \delta_{i'} A_{ij} = \sum_v \left( \delta_{i'} a_{ijv} + \sum_{j'} a_{ijj'} a_{i'j'v} \right) y_v + \sum_{j'} a_{ijj'} A_{i'j'} - \sum_v \left( \delta_i a_{i'jv} + \sum_{j'} a_{i'jj'} a_{ij'v} \right) y_v - \sum_{j'} a_{i'jj'} A_{ij'}.$$

It follows that if the integrability conditions are not satisfied, then  $y_1, \dots, y_n$  are linearly dependent over  $\mathcal{F} \pmod{\mathfrak{p}}$ , so that the linear dimension of  $\mathfrak{p}$  is less than  $n$ . Suppose that the integrability conditions are satisfied, that is, that

$$\delta_i A_{i'j} - \delta_{i'} A_{ij} = \sum_{j'} (a_{ijj'} A_{i'j'} - a_{i'jj'} A_{ij'}).$$

Fixing an orderly ranking, we see that the  $A_{ij}$  form an autoreduced set, and that this autoreduced set is (0)-coherent (see Chapter III, Section 8). It is an easy consequence of Chapter III, Section 8, Lemma 5, that  $\mathfrak{p}$  does not contain a nonzero differential polynomial of order 0. In particular,  $y_1, \dots, y_n$  are linearly independent (mod  $\mathfrak{p}$ ) over  $\mathcal{F}$ , so that the linear dimension of  $\mathfrak{p}$  is  $n$ .

EXERCISE

- Let  $\mathcal{F}$  be an ordinary differential field. Show that a differential ideal  $\mathfrak{p}$  of  $\mathcal{F}\{y\}$  is linear and of finite linear dimension  $l$  if and only if there exists a homogeneous linear differential polynomial  $L = y^{(l)} + a_1 y^{(l-1)} + \cdots + a_l y \in \mathcal{F}\{y\}$  of order  $l$  such that  $[L] = \mathfrak{p}$ .

6 General components

Let  $A \in \mathcal{U}\{y_1, \dots, y_n\}$ . A point  $\eta$  of  $\mathcal{U}^n$  is called a nonsingular zero of  $A$  (or a nonsingular solution of the differential equation  $A = 0$ ) if  $\eta$  is a zero of  $A$ , and there exists a ranking of  $(y_1, \dots, y_n)$  relative to which  $A$  is pseudo-led (see Chapter I, Section 11) and has pseudo-separant that does not vanish at  $\eta$ . A zero of  $A$  that is not nonsingular is called a singular zero of  $A$  (or a singular solution of the differential equation  $A = 0$ ).

**Theorem 3** Let  $\mathcal{F}$  be a differential subfield of  $\mathcal{U}$  and let  $A$  be an irreducible pseudo-led differential polynomial in  $\mathcal{F}\{y_1, \dots, y_n\}$ .

- Among the components of  $\{A\}_{\mathcal{F}}$  there is one, which we denote by  $\mathfrak{p}_{\mathcal{F}}(A)$ , that does not contain any pseudo-separant of  $A$ . Each of the other components of  $\{A\}_{\mathcal{F}}$  contains every pseudo-separant of  $A$ .

(b) If  $S$  is any pseudo-separant of  $A$ , then  $\mathfrak{p}_{\mathcal{F}}(A) = [A]:S^\infty = \{A\}:S = \{A\}_{/\mathcal{F}}:S$ . An element of  $\mathfrak{p}_{\mathcal{F}}(A)$  that is partially pseudo-reduced with respect to  $A$  must be divisible by  $A$ .

(c) If  $\mathcal{G}$  is an extension of  $\mathcal{F}$  in  $\mathcal{U}$  and  $A = A_1 \cdots A_r$  is the representation of  $A$  as a product of irreducible factors in  $\mathcal{G}\{y_1, \dots, y_n\}$ , then every pseudo-leader of  $A$  is a pseudo-leader of each  $A_i$ ,  $\mathfrak{p}_{\mathcal{G}}(A_i) \not\subset \mathfrak{p}_{\mathcal{G}}(A_{i'})$  whenever  $i \neq i'$ , and  $\mathfrak{G}_{\mathfrak{p}_{\mathcal{F}}}(A) = \mathfrak{p}_{\mathcal{G}}(A_1) \cap \cdots \cap \mathfrak{p}_{\mathcal{G}}(A_r)$ .

*Proof* Let  $S$  be a pseudo-separant of  $A$  relative to some ranking. Suppose  $B, C \in \mathcal{F}\{y_1, \dots, y_n\}$  and  $BC \in [A]:S^\infty$ . By Chapter I, Section 11, Corollary 1 to Lemma 10, we may write  $S^b B \equiv B_1$ ,  $S^c C \equiv C_1 \pmod{[A]}$ , where  $B_1, C_1$  are partially pseudo-reduced with respect to  $A$ , so that  $B_1 C_1$  is partially pseudo-reduced with respect to  $A$  and  $B_1 C_1 \in [A]:S^\infty$ . By Corollary 2 to the same lemma we conclude that, for some  $s$ ,  $S^s B_1 C_1$  is divisible by  $A$ . Since  $A$  is irreducible and  $\deg S < \deg A$  this implies that  $B_1$  or  $C_1$  is divisible by  $A$ , so that  $B$  or  $C$  is in  $[A]:S^\infty$ . The same reasoning shows that  $1 \notin [A]:S^\infty$ . Thus  $[A]:S^\infty$  is a prime differential ideal. If  $\Gamma$  denotes the set of all derivatives  $\theta y_j$  that are not derivatives of the pseudo-leader  $v$  of  $A$ , and if, for each  $\theta \in \Theta$ ,  $\Lambda(\theta)$  denotes the set of all derivatives of  $v$  that are of lower rank than  $\theta v$ , then we see by the same Corollary 2 that  $(\mathcal{F}[\Gamma]) \cap ([A]:S^\infty) = 0$ , and we see by the lemma referred to above that  $\theta A \in (\mathcal{F}[\Gamma, \Lambda(\theta), \theta v]) \cap ([A]:S^\infty)$  and  $\partial(\theta A)/\partial(\theta v) = S \notin [A]:S^\infty$ . It follows that the canonical homomorphism of  $\mathcal{F}\{y_1, \dots, y_n\}$  into  $Q(\mathcal{F}\{y_1, \dots, y_n\}/([A]:S^\infty))$  maps  $\Gamma$  onto a separating transcendence basis of that field over  $\mathcal{F}$ ; hence  $[A]:S^\infty$  is separable over  $\mathcal{F}$ . Therefore we may write  $\{A\}_{/\mathcal{F}} \subset [A]:S^\infty \subset \{A\}:S \subset \{A\}_{/\mathcal{F}}:S \subset ([A]:S^\infty):S = [A]:S^\infty$ , so that  $[A]:S^\infty = \{A\}:S = \{A\}_{/\mathcal{F}}:S$ . By Chapter 0, Section 8, Lemma 7,

$$\begin{aligned} \{A\}_{/\mathcal{F}} &\subset (\{A\}_{/\mathcal{F}}:S) \cap \{A, S\}_{/\mathcal{F}} \\ &\subset \{(\{A\}_{/\mathcal{F}}:S)A, (\{A\}_{/\mathcal{F}}:S)S\}_{/\mathcal{F}} \subset \{A, \{A\}_{/\mathcal{F}}\}_{/\mathcal{F}} = \{A\}_{/\mathcal{F}}, \end{aligned}$$

so that if we denote by  $\mathfrak{p}_1, \dots, \mathfrak{p}_r$  the components of  $\{A, S\}_{/\mathcal{F}}$  that do not contain  $[A]:S^\infty$ , then  $[A]:S^\infty, \mathfrak{p}_1, \dots, \mathfrak{p}_r$  are the components of  $\{A\}_{/\mathcal{F}}$ . Precisely one of these components, namely  $[A]:S^\infty$ , fails to contain the pseudo-separant  $S$ . If  $S'$  is a pseudo-separant of  $A$  relative to another ranking, then, of the  $r+1$  components of  $\{A\}_{/\mathcal{F}}$ , precisely one fails to contain  $S'$ . Since  $S'$  is partially pseudo-reduced with respect to  $A$  and is not divisible by  $A$ , we conclude by the Corollary 2 used above that  $S' \notin [A]:S^\infty$ . It is clear that (a) and (b) are proved.

Suppose now that  $A = A_1 \cdots A_r$ , with each  $A_i$  irreducible in  $\mathcal{G}\{y_1, \dots, y_n\}$ , and that  $v$  is a pseudo-leader of  $A$ . Obviously no proper derivative of  $v$  can be present in any  $A_i$ . As  $A$  is irreducible in  $\mathcal{F}\{y_1, \dots, y_n\}$  and  $\partial A/\partial v \neq 0$ ,  $A$  and  $\partial A/\partial v$  have no common factor, so that in the first place  $A_1, \dots, A_r$  are

distinct, and in the second place  $\partial A_i/\partial v \neq 0$  (for otherwise  $A_i$  would divide both  $A$  and  $\partial A/\partial v$ ). If  $w$  is a derivative  $\theta y_j$  of higher rank than  $v$ , then  $(\partial A_1/\partial w)A_2 \cdots A_r + A_1 \partial(A_2 \cdots A_r)/\partial w = \partial A/\partial w = 0$ ,  $A_1$  is irreducible in  $\mathcal{G}\{y_1, \dots, y_n\}$  and does not divide  $A_2, \dots, A_r$ , hence divides  $\partial A_1/\partial w$ , so that  $\partial A_1/\partial w = 0$ , and similarly every  $\partial A_i/\partial w = 0$ . Thus,  $v$  is a pseudo-leader of every  $A_i$ . As  $A_1, \dots, A_r$  are distinct and are obviously partially pseudo-reduced with respect to each other, we see by (b) that  $A_i \notin \mathfrak{p}_{\mathcal{G}}(A_{i'})$  whenever  $i \neq i'$ ; hence  $\mathfrak{p}_{\mathcal{G}}(A_i) \not\subset \mathfrak{p}_{\mathcal{G}}(A_{i'})$ , and also  $\partial A/\partial v \notin \mathfrak{p}_{\mathcal{G}}(A_i)$ , whence  $\mathfrak{p}_{\mathcal{G}}(A_i) = [A_i]_{\mathcal{G}\{y_1, \dots, y_n\}}:(\partial A/\partial v)^\infty = \{A_i\}_{\mathcal{G}\{y_1, \dots, y_n\}/\mathcal{G}}:\partial A/\partial v$ . Therefore

$$\begin{aligned} \bigcap \mathfrak{p}_{\mathcal{G}}(A_i) &= \bigcap \{A_i\}_{\mathcal{G}\{y_1, \dots, y_n\}/\mathcal{G}}:\partial A/\partial v \\ &= \{A\}_{\mathcal{G}\{y_1, \dots, y_n\}/\mathcal{G}}:\partial A/\partial v \subset \mathcal{G} \cdot \{A\}_{\mathcal{F}\{y_1, \dots, y_n\}/\mathcal{F}}:\partial A/\partial v \\ &= \mathfrak{G}_{\mathfrak{p}_{\mathcal{F}}}(A) = \mathcal{G} \cdot [A]_{\mathcal{F}\{y_1, \dots, y_n\}}:(\partial A/\partial v)^\infty \\ &= [A]_{\mathcal{G}\{y_1, \dots, y_n\}}:(\partial A/\partial v)^\infty \subset \bigcap [A_i]_{\mathcal{G}\{y_1, \dots, y_n\}}:(\partial A/\partial v)^\infty \\ &= \bigcap \mathfrak{p}_{\mathcal{G}}(A_i). \end{aligned}$$

This completes the proof.

The  $\mathcal{F}$ -separable prime differential ideal  $\mathfrak{p}_{\mathcal{F}}(A)$  is called the *general component* of  $A$  in  $\mathcal{F}\{y_1, \dots, y_n\}$ ; every other component of  $\{A\}_{/\mathcal{F}}$  is said to be a *singular component* of  $A$  in  $\mathcal{F}\{y_1, \dots, y_n\}$ .

If  $A$  is irreducible over the universal differential field  $\mathcal{U}$  or, what is the same thing, is absolutely irreducible, then, by Theorem 3 and the results of Section 3, the closed set  $\mathfrak{Z}(A)$  in  $\mathcal{U}^n$  has one irreducible component that contains all the nonsingular zeros of  $A$ , namely  $\mathfrak{Z}(\mathfrak{p}_{\mathcal{U}}(A))$ ; the other irreducible components consist solely of singular zeros of  $A$ . The irreducible component  $\mathfrak{Z}(\mathfrak{p}_{\mathcal{U}}(A))$  is called the *general irreducible component* of  $A$ , or the *general solution* of the differential equation  $A = 0$ , and the others are called the *singular irreducible components* of  $A$ . Of course, it may happen that there is no singular irreducible component. This will be the case, for example, if  $A$  is linear. On the other hand, the general irreducible component of  $A$  may contain some singular zeros of  $A$  (see Exercise 2(b) below). But since  $\mathfrak{p}_{\mathcal{U}}(A)$  does not contain any pseudo-separant of  $A$ , the nonsingular zeros of  $A$  form a nonempty open (and therefore dense) subset of the general irreducible component. The general irreducible component of  $A$  is defined over any differential field  $\mathcal{F}$  in  $\mathcal{U}$  containing all the coefficients in  $A$ , for  $\mathfrak{p}_{\mathcal{U}}(A) = \mathcal{U}\mathfrak{p}_{\mathcal{F}}(A)$  by Theorem 3(c).

## EXERCISES

In the following exercises  $\mathcal{F}$  denotes a differential subfield of  $\mathcal{U}$  and  $\mathcal{G}$  denotes the field of constants of  $\mathcal{F}$ .

1. (a) Show that if  $p=0$ , and  $A$  and  $B$  are irreducible elements of  $\mathcal{F}\{y_1, \dots, y_n\}$  with  $\mathfrak{p}_{\mathcal{F}}(A) = \mathfrak{p}_{\mathcal{F}}(B)$ , then  $B = aA$  for some nonzero  $a \in \mathcal{F}$ . (*Hint:* Use Theorem 3(b).)  
 (b) Show that if  $p \neq 0$ , and  $A = y_1 - y_2 + (\delta_1 y_2)^p$ ,  $B = y_1 - y_2 + (\delta_1 y_1)^p$ , then  $A$  and  $B$  are pseudo-led and absolutely irreducible, and  $\mathfrak{p}_{\mathcal{F}}(A) = [A] = [B] = \mathfrak{p}_{\mathcal{F}}(B)$ .
2. Let  $m = 1$  (that is, let  $\mathcal{U}$  be an ordinary differential field) and suppose that  $p \neq 2$ . Let  $x$  be an element of  $\mathcal{U}$  with  $x' = 1$ .  
 (a) Show that  $y^2 - 4y$  is pseudo-led and absolutely irreducible, has general component  $(y^2 - 4y) + [y'' - 2]$ , and has one singular component  $[y]$ . (*Hint:*  $(y^2 - 4y)' = 2(y'' - 2)y'$ .) Show that the general irreducible component consists of all  $(x + c)^2$  with  $c \in \mathcal{K}$ .  
 (b) Show that  $y^2 - 4y^3$  is pseudo-led and absolutely irreducible, and has no singular component. (*Hint:* Show that  $\{y^2 - 4y^3\} = (y^2 - 4y^3) + [y'' - 6y^2]$ .) Show that  $\mathfrak{Z}(y^2 - 4y^3)$  consists of all  $(x + c)^{-2}$  with  $c \in \mathcal{K}$ , and of 0.
3. Let  $m = 1$  and suppose that  $p \neq 0$ .  
 (a) Show that  $y^{p+1} + y^p$  is pseudo-led and absolutely irreducible, and has no singular component.  
 (b) Show that  $yy'^p + y''^p + y'^p y''^{p+1}$  is pseudo-led and absolutely irreducible, and has one singular component  $[y']$ .  
 (c) Show that  $z'^p + y^p z + y^p z'^{p+1}$  is pseudo-led and absolutely irreducible, has general component  $(z'^p + y^p z + y^p z'^{p+1}) + [1 + z'^{p-1} z'']$ , and has two singular components  $[z]$  and  $[y, z']$ .  
 (d) Show that  $y_1^p + y_2^{p+1} + y_2^p y_3$  is pseudo-led and absolutely irreducible, has general component  $(y_1^p + y_2^{p+1} + y_2^p y_3) + [y_3']$ , and has one singular component  $[y_1, y_2 + y_3]$ .
4. Show that if  $A$  is an irreducible pseudo-led element of  $\mathcal{F}\{y\}$  of order 0, then  $A$  has no singular component and  $\{A\}_{\mathcal{F}} = [A]$ .
5. Let  $x_1, \dots, x_m$  be elements of  $\mathcal{F}$  such that  $\delta_i x_i = 0$  or 1 according as  $i \neq i'$  or  $i = i'$  ( $1 \leq i \leq m$ ,  $1 \leq i' \leq m$ ). Set  $A = \sum_{1 \leq i \leq m} (\delta_i y)^2 - \sum_{1 \leq i \leq m} x_i \delta_i y + y$ .  
 (a) Show that  $A$  is pseudo-led and absolutely irreducible.  
 (b) Show that if  $p \neq 2$ , then  $A$  has general component

$$\{A, \det(\delta_i \delta_{i'} y)_{1 \leq i \leq m, 1 \leq i' \leq m}\}$$

and one singular component  $[y - \frac{1}{4} \sum_{1 \leq i \leq m} x_i^2]$ .

(c) Show that if  $p = 2$ , then  $A$  has no singular component.

6. Let  $m = 1$  and assume that  $\mathcal{U}$  is semiuniversal over  $\mathcal{F}$ . Let  $n \in \mathbb{N}$ ,  $n \geq 2$ ,  $p \nmid n$ . Let  $P \in \mathcal{C}[z]$ ,  $P \neq 0$ ,  $\deg P = 2n - 1$  or  $2n$ , and suppose that  $P, dP/dz$  are relatively prime. Set  $A = yz'^n + P$ .

- (a) Show that  $A$  is pseudo-led and absolutely irreducible.
- (b) Show that  $\mathfrak{p}_{\mathcal{F}}(A) = \{A, nyz'^{n-2}z'' + y'z'^{n-1} + dP/dz\}$  and that the singular components of  $A$  in  $\mathcal{F}\{y, z\}$  are the differential ideals  $[Q]$  generated by the irreducible factors  $Q$  of  $P$ .
- (c) Let  $(\eta, \zeta)$  be a generic zero of  $\mathfrak{p}_{\mathcal{F}}(A)$ . Show that 0 is a differential specialization of  $\eta$  over  $\mathcal{F}$  but there does not exist an  $\alpha \in \mathcal{U}$  such that  $(0, \alpha)$  is a differential specialization of  $(\eta, \zeta)$  or  $(\eta, \zeta^{-1})$  over  $\mathcal{F}$ . (*Hint:*  $(\eta, \zeta^{-1})$  is a zero of  $yz'^n + (-1)^n z^{2n} P(z^{-1})$ .)
7. (Example due to Ritt; see [91, Section 13]) Let  $m = 1$  and suppose that  $\mathcal{U}$  is semiuniversal over  $\mathcal{F}$ . Assume that  $p \neq 2, 3$ . Let  $A = 2yy'' - 3y'^2 + 2y$ ,  $B = 3y'y''' - 2(2y'' - 1)(y' + 1)$ .  
 (a) Show that  $A$  is pseudo-led and absolutely irreducible, and that  $(y' + 1)A' - y''A = y'B$ .  
 (b) Show that  $\mathfrak{p}_{\mathcal{F}}(A) = \{A, B\}$ , and that  $A$  has one singular component  $[y]$ .  
 (c) Show that the differential ideal  $\mathfrak{r} = \{A(y), B(y), A(z), B(z)\}$  of  $\mathcal{F}\{y, z\}$  is  $\mathcal{F}$ -separable and prime, and that if  $(\eta, \zeta)$  is a generic zero of  $\mathfrak{r}$ , then  $\eta$  and  $\zeta$  are generic zeros of  $\mathfrak{p}_{\mathcal{F}}(A)$ . (*Hint:* See Chapter 0, Section 12, Corollary 2 to Proposition 7.)  
 (d) Show that 0 is not a differential specialization of  $\eta$  or  $\zeta$  over  $\mathcal{F}$  but is a differential specialization of  $\eta\zeta$  over  $\mathcal{F}$ . (*Hint:* Prove that for any nonzero  $c \in \mathcal{K}$ , the differential polynomial  $E_c = y^2 - c^{-1}y^3 - y$  is pseudo-led and absolutely irreducible and  $yE_c' - 3y'E_c = Ay'$ ; conclude that  $\mathfrak{p}_{\mathcal{F}}(A) \subset \mathfrak{p}_{\mathcal{U}}(E_c)$ . Also,  $c^{-2}y^4 E_c(cy^{-1}) = E_c$ ; conclude that if  $\alpha$  is a zero of  $\mathfrak{p}_{\mathcal{U}}(E_c)$ , then so is  $\alpha\alpha^{-1}$ . Deduce from this that every nonzero  $c \in \mathcal{K}$  is a differential specialization of  $\eta\zeta$  over  $\mathcal{F}$ .)
8. Suppose that  $p = 0$ . Let  $t_1, \dots, t_n \in \mathcal{U}$  be differentially algebraically independent over  $\mathcal{F}$ , let  $P, Q \in \mathcal{F}\{y_1, \dots, y_n\}$ ,  $PQ \notin \mathcal{F}$ ,  $\gcd(P, Q) = 1$ , and set  $u = P(t_1, \dots, t_n)/Q(t_1, \dots, t_n)$ . Prove that  $u$  is differentially transcendental over  $\mathcal{F}$ ,  $P - uQ$  is irreducible in  $\mathcal{F}\langle u \rangle\{y_1, \dots, y_n\}$ , and  $(t_1, \dots, t_n)$  is a generic zero of  $\mathfrak{p}_{\mathcal{F}\langle u \rangle}(P - uQ)$ . (*Hint:* After establishing the first two points, fix a generic zero  $(t_1', \dots, t_n')$  of  $\mathfrak{p}_{\mathcal{F}\langle u \rangle}(P - uQ)$ , show that  $(t_1', \dots, t_n')$  is differentially algebraically independent over  $\mathcal{F}$ , and infer that there exists an isomorphism  $\mathcal{F}\langle t_1, \dots, t_n \rangle \approx \mathcal{F}\langle t_1', \dots, t_n' \rangle$  over  $\mathcal{F}$  with  $t_j \mapsto t_j'$  ( $1 \leq j \leq n$ ). Note that this is an isomorphism over  $\mathcal{F}\langle u \rangle$ , and conclude that  $(t_1, \dots, t_n)$  is a generic zero of  $\mathfrak{p}_{\mathcal{F}\langle u \rangle}(P - uQ)$ .)
9. (a) Suppose that  $p = 0$ . Prove that if  $u, t \in \mathcal{U}$  are differentially transcendental over  $\mathcal{F}$  and  $\mathcal{F}\langle u \rangle = \mathcal{F}\langle t \rangle$ , then there exist elements  $a, b, c, d \in \mathcal{F}$  with  $ad - bc \neq 0$  such that  $u = (at + b)/(ct + d)$ . (*Hint:* Write  $u = P(t)/Q(t)$  with  $P, Q \in \mathcal{F}\{y\}$  and  $\gcd(P, Q) = 1$ . Observe that  $t$  is a generic zero of  $\mathfrak{p}_{\mathcal{F}\langle u \rangle}(P - uQ)$  by the result in Exercise 8, and also of  $\mathfrak{p}_{\mathcal{F}\langle u \rangle}(y - t)$ , and then apply the result of Exercise 1(a).)

(b) Give an example to show that when  $p \neq 0$ , the result of part (a) is in general false. (*Hint:* See Exercise 1(b).)

**7 General components and differential dimension polynomials**

The following result characterizes general components in terms of their differential dimension polynomials. We recall (Chapter I, Section 11) that a differential polynomial  $A$  in  $(y_1, \dots, y_n)$  has *essential order*  $e$  if there exists a derivative  $u = \theta y_j$  of order  $e$  with  $\partial A/\partial u \neq 0$  but there does not exist such a derivative of order greater than  $e$ .

**Proposition 4** *Let  $\mathcal{F}$  be a differential subfield of  $\mathcal{U}$ , let  $\mathfrak{p}$  be an  $\mathcal{F}$ -separable prime differential ideal of  $\mathcal{F}\{y_1, \dots, y_n\}$ , and let  $e \in \mathbb{N}$ . A necessary and sufficient condition that  $\mathfrak{p} = \mathfrak{p}_{\mathcal{F}}(A)$  for some irreducible pseudo-led differential polynomial  $A \in \mathcal{F}\{y_1, \dots, y_n\}$  of essential order  $e$ , is that*

$$\omega_{\mathfrak{p}} = n \binom{X+m}{m} - \binom{X-e+m}{m}.$$

**REMARK** The proof shows that when the condition is satisfied then for any orderly ranking of  $(y_1, \dots, y_n)$  there exists an  $A$  with pseudo-leader of order  $e$  such that  $\mathfrak{p} = \mathfrak{p}_{\mathcal{F}}(A)$ . (When  $p \neq 0$  two essentially different polynomials may have identical general components, but when  $p = 0$  if two differential polynomials have the same general component, then one of them is a multiple of the other by a nonzero element of  $\mathcal{F}$ . See Section 6, Exercise 1.)

*Proof* We may, by Section 6, Theorem 3(c), and by Chapter III, Section 6, Proposition 3(b), replace  $\mathcal{F}$  by any smaller differential field of definition of  $\mathfrak{p}$ . By Chapter III, Sections 3 and 7, Propositions 1 and 4, we may therefore suppose that  $\mathcal{U}$  is a universal extension of  $\mathcal{F}$ . Then  $\mathfrak{p}$  has a generic zero  $\eta = (\eta_1, \dots, \eta_n)$ . For each  $s \in \mathbb{N}$  let  $A_s$  denote the polynomial algebra  $\mathcal{F}[(\theta y_j)_{\theta \in \Theta(s), 1 \leq j \leq n}]$ , let  $\mathfrak{p}_s = \mathfrak{p} \cap A_s$ , and let  $\eta^{(s)} = (\theta \eta_j)_{\theta \in \Theta(s), 1 \leq j \leq n}$ . Then  $\mathfrak{p}_s$  is an  $\mathcal{F}$ -separable prime ideal of  $A_s$  with generic zero  $\eta^{(s)}$ .

To prove the necessity of the condition, suppose that  $\mathfrak{p} = \mathfrak{p}_{\mathcal{F}}(A)$ , where  $A \in \mathcal{F}\{y_1, \dots, y_n\}$  is irreducible, has essential order  $e$ , and (relative to some ranking) has pseudo-leader  $v$ . Let  $s \geq \text{ord } A$ . For any  $\theta \in \Theta(s-e)$  then  $\theta A \in \mathfrak{p}_s$ . Also, by Chapter I, Section 11, Lemma 10,  $\theta A$  has pseudo-leader  $\theta v$  and pseudo-separant  $\partial A/\partial v$ , so that  $\partial(\theta A)/\partial(\theta' v) = 0$  whenever  $\theta' v > \theta v$ . Hence

$$\det(\partial(\theta A)/\partial(\theta' v))_{\theta \in \Theta(s-e), \theta' \in \Theta(s-e)} = (\partial A/\partial v)^q,$$

where  $q = \text{Card } \Theta(s-e) = \binom{s-e+m}{m}$ , so that this determinant is an element of  $A_s$  not vanishing at  $\eta^{(s)}$ . It follows (by Chapter 0, Section 16, Corollary 4 to

Proposition 11) that the perfect ideal of  $A_s$  generated by the polynomials  $\theta A \in A_s$  with  $\theta \in \Theta(s-e)$  has a unique component  $\mathfrak{p}^{(s)}$  that admits the zero  $\eta^{(s)}$ , and that  $\mathfrak{p}^{(s)}$  is  $\mathcal{F}$ -separable and of dimension  $n \binom{s+m}{m} - \binom{s-e+m}{m}$ . Since  $\eta^{(s)}$  is a generic zero of  $\mathfrak{p}_s$ , we have  $\mathfrak{p}^{(s)} \subset \mathfrak{p}_s$ . To prove the necessity of the condition in the proposition it suffices to show that  $\mathfrak{p}_s \subset \mathfrak{p}^{(s)}$ . Suppose then that  $B \in \mathfrak{p}_s$ . By Section 6, Theorem 3(b),  $(\partial A/\partial v)^b B \in [A]$  for some  $b \in \mathbb{N}$ . Introducing a new ranking that is orderly, let  $u$  be the derivative of a  $y_j$  with  $\partial A/\partial u \neq 0$  which is of highest rank relative to the new ranking. Evidently  $\text{ord } u = e$ , and (because  $\partial A/\partial u$  is obviously partially pseudo-reduced with respect to  $A$  relative to the old ranking)  $\partial A/\partial u \notin \mathfrak{p}$ . By Chapter I, Section 11, Corollary 2 to Lemma 10, we may write  $(\partial A/\partial v)^b B \in (\Theta_0 A) : (\partial A/\partial u)^\infty$ , where  $\Theta_0$  is the set of all  $\theta_0 \in \Theta$  such that  $\text{rank } \theta_0 u \leq \text{rank } A$   $(\partial A/\partial v)^b B$ . Evidently  $\Theta_0 \subset \Theta(s-e)$ , so that  $(\partial A/\partial v)^b B \in \mathfrak{p}^{(s)} : (\partial A/\partial u)^\infty = \mathfrak{p}^{(s)}$ , whence  $B \in \mathfrak{p}^{(s)}$ .

To prove the sufficiency of the condition, suppose that it is satisfied and fix any orderly ranking. Let  $A$  be a characteristic set of  $\mathfrak{p}$ , and let  $s \geq \max_{C \in A} \text{ord } C$ . For each  $y_j$  let  $E_j$  denote the set of lattice points  $(i_1, \dots, i_m) \in \mathbb{N}^m$  such that  $\delta_1^{i_1} \dots \delta_m^{i_m} y_j$  is a leader of an element of  $A$ . By Chapter II, Section 12, Theorem 6(d), then  $\omega_{\mathfrak{p}} = \sum \omega_{E_j} - b$  for some  $b \in \mathbb{N}$ . However, by Chapter 0, Section 17, Lemma 16(c), if  $E_j \neq \emptyset$ , then  $\deg \omega_{E_j} < m$  and if  $E_j = \emptyset$ , then  $\omega_{E_j} = \binom{X+m}{m}$ . Since by hypothesis

$$\omega_{\mathfrak{p}} = (n-1) \binom{X+m}{m} + \binom{X+m}{m} - \binom{X-e+m}{m},$$

we conclude that  $E_j \neq \emptyset$  for precisely one index  $j$ , say for  $j = k$ , so that

$$\omega_{\mathfrak{p}} = (n-1) \binom{X+m}{m} + \omega_{E_k} - b.$$

Thus, the leader of every element of  $A$  is a derivative of  $y_k$  and

$$\omega_{E_k} = \binom{X+m}{m} - \binom{X-e+m}{m} + b.$$

By double use of Chapter 0, Section 17, Lemma 16(e), we infer first that there exists a lowest derivative  $w = \delta_1^{e_1} \dots \delta_m^{e_m} y_k$  such that the leader of every element of  $A$  is a derivative of  $w$  and every derivative of  $w$  with only a finite number of exceptions is a derivative of a leader of an element of  $A$ , and second that if the number of these exceptions is denoted by  $a$ , then

$$\omega_{E_k} = \binom{X+m}{m} - \binom{X-\sum e_i+m}{m} + a.$$

By Chapter I, Section 10, Lemma 9, if  $P \in \mathfrak{p}$  is free of every derivative of

$w$ , then  $\partial P/\partial v \in \mathfrak{p}$  for every derivative  $v$  of any  $y_j$ . This means that the derivatives

$$\theta \eta_j \quad (\theta \in \Theta, \quad 1 \leq j \leq n, \quad \theta y_j \notin \Theta w)$$

are separably independent over  $\mathcal{F}$ . Since  $\mathcal{F}\langle \eta \rangle$  is separable over  $\mathcal{F}$ , they are even algebraically independent.

Now, if  $m > 1$ , then the two equations for  $\omega_{\mathbf{e}_k}$  above show that  $e = \sum e_i = \text{ord } w$ , so that the number of algebraically independent derivatives  $\theta \eta_j$  considered above with  $\text{ord } \theta \leq s$  is equal to

$$n \binom{s+m}{m} - \binom{s-e+m}{m} = \omega_{\mathfrak{p}}(s),$$

which for big  $s$  is the transcendence degree of  $\mathcal{F}((\theta \eta_j)_{\theta \in \Theta(s), 1 \leq j \leq n})$  over  $\mathcal{F}$ . Hence the element  $w(\eta) = \delta_1^{e_1} \cdots \delta_m^{e_m} \eta_k$  is algebraic over the field extension of  $\mathcal{F}$  generated by all the algebraically independent derivatives considered above. It follows that in this case there exists an irreducible  $A \in \mathfrak{p}$  that involves  $w$  but no proper derivative of  $w$ , and that each element of  $\mathfrak{p}$  free of every proper derivative of  $w$  is divisible by  $A$ .

On the other hand, if  $m = 1$ , then  $A$  contains just one differential polynomial (because  $y_k$  cannot have two derivatives neither of which is a derivative of the other) which we denote by  $C$ , and evidently  $w = y_k$  and  $a = \text{ord } C$ . This time the two equations for  $\omega_{\mathbf{e}_k}$  show merely that  $e + b = a$ , so that  $a \geq e$ . The algebraically independent derivatives considered above that are of order less than or equal to  $s$  are the derivatives  $\delta_1^i \eta_j$  ( $0 \leq i \leq s$ ,  $1 \leq j \leq n$ ,  $j \neq k$ ), and the number of these is  $(n-1)(s+1) = (n-1) \binom{s+1}{1}$ . Hence these together with the  $e+1$  derivatives  $\delta_1^i \eta_k$  ( $0 \leq i \leq e$ ) are in number equal to

$$n \binom{s+1}{1} - \binom{s-e+1}{1} + 1 = \omega_{\mathfrak{p}}(s) + 1,$$

and therefore are, for big  $s$ , algebraically dependent over  $\mathcal{F}$ . It follows in this case that there is a smallest number  $d \in \mathbb{N}$  such that  $\mathfrak{p}$  contains a non-zero differential polynomial free of every proper derivative of  $\delta_1^d y_k$ , and of course  $d \leq e \leq a$ , and there exists an irreducible  $A \in \mathfrak{p}$  that involves  $\delta_1^d y_k$  but no proper derivative of  $\delta_1^d y_k$ . Each element of  $\mathfrak{p}$  free of every proper derivative of  $\delta_1^d y_k$  is divisible by  $A$ .

We now treat both cases simultaneously, setting

$$\begin{aligned} e' = e, \quad w' = w = \delta_1^{e_1} \cdots \delta_m^{e_m} y_k & \quad \text{if } m > 1, \\ e' = d, \quad w' = \delta_1^d y_k & \quad \text{if } m = 1. \end{aligned}$$

We observe that if for a derivative  $v$  of some  $y_j$  we have  $\partial A/\partial v \in \mathfrak{p}$ , then  $\partial A/\partial v = 0$ , because  $\partial A/\partial v$  must be divisible by  $A$ . It follows by Chapter I,

Section 10, Lemma 9, that  $\partial A/\partial v = 0$  for every  $v$  of higher rank than  $w'$ . Among the derivatives  $\delta_1 y_k, \dots, \delta_m y_k$  let  $\delta_h y_k$  be the one of lowest rank. Then

$$\delta_h A = A^{\delta_h} + \sum_v (\partial A/\partial v) \delta_h v = A^{\delta_h} + \sum_{v \leq w'} (\partial A/\partial v) \delta_h v.$$

Now, it is easy to verify that the only  $v \leq w'$  for which  $\delta_h v$  is a proper derivative of  $w'$  is  $w'$ . Therefore we may write

$$\delta_h A = (\partial A/\partial w') \delta_h w' + B$$

with  $B$  free of every proper derivative of  $w'$ . If  $\partial A/\partial w' = 0$ , then  $\delta_h A$  would be free of every proper derivative of  $w'$  and hence would be divisible by  $A$ . By Chapter I, Section 8, Corollary to Lemma 5,  $A$  would then be in  $\mathcal{F}[\{(\theta y_j)^p\}_{\theta \in \Theta, 1 \leq j \leq n}]$ , but this is impossible because elements of  $\mathcal{F}\langle \eta \rangle$  that are algebraically dependent over  $\mathcal{F}$  must be separably dependent over  $\mathcal{F}$  so that some partial derivative  $\partial A/\partial v$  must be different from 0. Thus  $\partial A/\partial w' \notin \mathfrak{p}$ , and we see that  $w'$  is pseudo-leader of  $A$  and  $e'$  is the essential order of  $A$ . By the necessity of the condition (already proved),

$$\omega_{\mathfrak{p}_{\mathcal{F}}(A)} = n \binom{X+m}{m} - \binom{X-e'+m}{m}.$$

Since  $e' \leq e$  this implies that  $\omega_{\mathfrak{p}_{\mathcal{F}}(A)} \leq \omega_{\mathfrak{p}}$ . However,  $\mathfrak{p}_{\mathcal{F}}(A) = \{A : \partial A/\partial w' \in \mathfrak{p} : \partial A/\partial w' = \mathfrak{p}\}$ , so that by Chapter III, Section 5, Proposition 2,  $\mathfrak{p} = \mathfrak{p}_{\mathcal{F}}(A)$  and  $e = e'$ .

### EXERCISES

1. Suppose that  $m = 1$ .
  - (a) Let  $\mathfrak{p}$  be an  $\mathcal{F}$ -separable prime differential ideal of  $\mathcal{F}\{y_1, \dots, y_n\}$  of differential dimension  $n-1$ . Show that there exists an irreducible  $A \in \mathcal{F}\{y_1, \dots, y_n\}$  such that if we set  $e = \text{ord } A$ , then  $\partial A/\partial y_j^{(e)} \neq 0$  for some index  $j$  and  $\mathfrak{p} = \mathfrak{p}_{\mathcal{F}}(A)$ .
  - (b) Show that every  $\mathcal{F}$ -separable prime differential ideal of  $\mathcal{F}\{y\}$  other than (0) is the general component of some pseudo-led irreducible differential polynomial in  $\mathcal{F}\{y\}$ .
2. Suppose that  $\rho = 0$  and  $m = 1$ .
  - (a) (Ritt's analog of Lüroth's theorem. See Ritt [95], and also Kolchin [39, 40].) Let  $t \in \mathcal{U}$  be differentially transcendental over  $\mathcal{F}$ , and let  $\mathcal{G}$  be a differential field with  $\mathcal{F} \subset \mathcal{G} \subset \mathcal{F}\langle t \rangle$  and  $\mathcal{G} \neq \mathcal{F}$ . Show that there exists an element  $u \in \mathcal{G}$  such that  $\mathcal{F}\langle u \rangle = \mathcal{G}$ . (Hint: Use Exercise 1 to show that the defining differential ideal of  $t$  in  $\mathcal{G}\{y\}$  is  $\mathfrak{p}_{\mathcal{G}}(A)$  for some irreducible  $A \in \mathcal{G}\{y\}$ , of order say  $e$ , with some coefficient in  $A$  equal to 1 and not every coefficient in  $A$  an element of  $\mathcal{F}$ ; these coefficients

are quotients of elements of  $\mathcal{F}\langle t \rangle$ . Fix  $D \in \mathcal{F}\langle z \rangle$  so that  $D(t)$  is a lowest common denominator of the coefficients in  $A$ , and define  $B \in \mathcal{F}\langle y, z \rangle$  by the condition  $B(y, t) = D(t)A$ . Show that  $B \notin \mathcal{F}\langle y \rangle \cup \mathcal{F}\langle z \rangle$ ,  $\text{ord}_y B = e$ , and the irreducible factors of  $B$  in  $\mathcal{F}\langle y, z \rangle$  are distinct and of order  $e$  in  $y$  and involve  $z$  differentially. Set  $f = \text{ord}_z B$ . Let  $u$  be a coefficient in  $A$  with  $u \notin \mathcal{F}$ . Show that  $u = H(t)/K(t)$ , where  $H, K \in \mathcal{F}\langle z \rangle$ ,  $HK \neq 0$ ,  $\text{gcd}(H, K) = 1$ , the orders of  $H$  and  $K$  in  $z$  are less than or equal to  $f$ , and for each index  $i \leq f$  the degrees in  $(z^{(i)}, \dots, z^{(f)})$  of  $H$  and  $K$  are less than or equal to the corresponding degree of  $B$ . Show that  $uK(y) - H(y) \in \mathfrak{p}_{\mathcal{G}}(A)$ , and infer first that  $e \leq f$ , and second that  $H(z)K(y) - K(z)H(y) \in \mathfrak{p}_{\mathcal{G}}(C)$  for every irreducible factor  $C$  of  $B$ . Show in succession that  $H(z)K(y) - K(z)H(y)$  is divisible by every irreducible factor of  $B$  of order  $f$  in  $z$ , by every irreducible factor of  $B$  of order  $f-1$  in  $z$ , etc., and finally that  $H(z)K(y) - K(z)H(y) = aB$ , where  $a \in \mathcal{F}$ . Infer that  $e = f$  and  $uK(y) - H(y) = vA$ , where  $v \in \mathcal{G}$ , and therefore that  $A \in \mathcal{F}\langle u \rangle\langle y \rangle$ . Use this to show that  $\mathcal{F}\langle u \rangle\langle t \rangle$  and  $\mathcal{G}$  are linearly disjoint over  $\mathcal{F}\langle u \rangle$ , and conclude that  $\mathcal{G} = \mathcal{F}\langle u \rangle$ .

(b) Prove the following generalization of the result in part (a): *If  $t_1, \dots, t_n \in \mathcal{U}$  are differentially algebraically independent over  $\mathcal{F}$ , and  $\mathcal{G}$  is a differential field with  $\mathcal{F} \subset \mathcal{G} \subset \mathcal{F}\langle t_1, \dots, t_n \rangle$  such that the differential transcendence degree of  $\mathcal{G}$  over  $\mathcal{F}$  is 1, then there exists an element  $u \in \mathcal{G}$  such that  $\mathcal{F}\langle u \rangle = \mathcal{G}$ . (Hint: Copy the proof for part (a).)*

## 8 Multiplicity of zeros

Let  $A \in \mathcal{U}\langle y_1, \dots, y_n \rangle$  and  $\eta = (\eta_1, \dots, \eta_n) \in \mathcal{U}^n$ . If  $A \neq 0$ , then there is a smallest natural number  $\mu$  such that  $A(\eta_1 + y_1, \dots, \eta_n + y_n)$  has a nonzero term of degree  $\mu$ ; we call this smallest  $\mu$  the *multiplicity of  $A$  at  $\eta$* . The multiplicity of  $A$  at  $\eta$  can also be defined as the biggest  $\mu \in \mathbb{N}$  such that  $A \in [y_1 - \eta_1, \dots, y_n - \eta_n]^\mu$ . If  $A = 0$ , we define the multiplicity of  $A$  at  $\eta$  as  $\infty$ .

If  $A(\eta) = 0$ , then the multiplicity of  $A$  at  $\eta$  is some  $\mu > 0$ . We say in this case that  $\eta$  is a *zero of  $A$  of multiplicity  $\mu$* . Every zero of  $A$  has multiplicity greater than or equal to 1. If  $A$  is pseudo-led, the non-singular zeros of  $A$  evidently have multiplicity 1. At the other extreme, every zero of  $A$  has multiplicity less than or equal to  $\text{deg } A$ . If  $A$  is a power of a differential polynomial of degree 1, then every zero of  $A$  has multiplicity  $\text{deg } A$ . The following converse is used in Section 10.

**Lemma 1** *Let  $A$  be a pseudo-led element of  $\mathcal{F}\langle y_1, \dots, y_n \rangle$  of degree  $t$ , and suppose that every zero of  $A$  has multiplicity  $t$ . Then  $A = \varphi^L$  where  $\varphi \in \mathcal{F}$ ,  $L \in \mathcal{F}\langle y_1, \dots, y_n \rangle$ , and  $\text{deg } L = 1$ .*

*Proof* Replacing  $\mathcal{F}$  by a smaller differential field, we may suppose that  $\mathcal{U}$  is universal over  $\mathcal{F}$ . Let  $v$  be pseudo-leader of  $A$  relative to some ranking. Writing  $A = \varphi A_1^{a_1} \cdots A_r^{a_r}$ , where  $\varphi \in \mathcal{F}$  and  $A_1, \dots, A_r$  are the distinct irreducible factors of  $A$ , we see that  $\partial(A_k^{a_k})/\partial v \neq 0$  for at least one  $k$ , say for  $k = 1$ . Then  $a_1$  is not divisible by  $p$  and  $\partial A_1/\partial v \neq 0$ . If  $v'$  is any derivative of a  $y_j$  with  $v' > v$ , then  $\partial A/\partial v' = 0$ , and this implies that  $\partial A_1/\partial v'$  is divisible by  $A_1$ , so that  $\partial A_1/\partial v' = 0$ . Thus,  $v$  is pseudo-leader of  $A_1$ . Let  $\eta$  be a generic zero of  $\mathfrak{p}_{\mathcal{F}}(A_1)$ . Each  $A_k$  with  $k \neq 1$  is partially pseudo-reduced with respect to  $A_1$  and is not divisible by  $A_1$ . By Section 6, Theorem 3(b),  $A_k(\eta) \neq 0$ . As  $\eta$  is a zero of  $A_1$  of multiplicity 1,  $\eta$  must be a zero of  $A$  of multiplicity  $a_1$ , so that  $a_1 = t$ . However, obviously  $t = \sum_{1 \leq k \leq r} a_k \text{deg } A_k$ . Therefore  $r = 1$  and  $\text{deg } A_1 = 1$ .

## PART B. CHARACTERISTIC $p=0$

*Throughout this part of Chapter IV it is assumed that  $p = 0$ .*

We now turn to some of Ritt's deeper work, and for this we must assume that  $p = 0$ . The results that are most complete deal with the components of a differential polynomial. In his original treatment (Ritt [85, 86]) he dealt with algebraic differential equations with meromorphic coefficients, and his proofs were in part function-theoretic. The first step at algebraization in this connection was taken by Levi [49, 50] who proved a lemma obviating some of Ritt's dependence on analysis. The rest of the function theory was removed by Ritt himself ([93], see also [95]) by adapting his Newton polygon method to the abstract case. The whole complex of results was then studied anew by Hillman [19] and Hillman and Mead [20], who clarified their interdependence and simplified the exposition. It is this exposition that we follow here in the main lines, but with alterations and additions. After a preliminary section (Section 9) on finite sets of differential polynomials, containing a constructive result and a nonconstructive one due to Ritt and an improvement (Lemma 2) due to Rosenfeld, we turn to Ritt's main work on singular solutions. In the present development everything flows from two sources: Hillman's leading coefficient theorem (generalizing Ritt's lowest degree theorem, which played only a minor part in Ritt's treatment), and Levi's lemma. These are established first (Sections 10 and 11, respectively). With the view of improving some of Levi's improvements of some of Ritt's results, we formalize in Section 12 the notion of domination of differential monomials, and generalize a special case of Levi's lemma. Following a section devoted to the preparation of a differential polynomial with respect to a characteristic set, come Ritt's definitive results on the components of a differential polynomial: in Section 14 the component theorem, and in Section 15 the low power theorem. The remainder of the chapter is devoted to partial



results on the Ritt problem concerning the distribution of the singular zeros of an irreducible differential polynomial among its irreducible components, and to a few other topics.

9 Finite sets of differential polynomials

Let  $\mathcal{F}$  be a differential subfield of  $\mathcal{U}$ , and suppose given a ranking of  $(y_1, \dots, y_n)$ . As we shall see in Lemma 2, below, a prime differential ideal  $\mathfrak{p}$  of  $\mathcal{F}\{y_1, \dots, y_n\}$  is completely determined by its characteristic set  $A$  through the equation  $\mathfrak{p} = [A]:H_A^\infty$ . Thus, if we are given a set  $\Phi \subset \mathcal{F}\{y_1, \dots, y_n\}$ , the problem of finding the components of  $\{\Phi\}$  is equivalent to that of finding characteristic sets of the components. This problem can be separated into the following two problems.

**PROBLEM 1** *To find a finite set  $\mathfrak{A}$  of autoreduced subsets of  $\mathcal{F}\{y_1, \dots, y_n\}$ , each of which is a characteristic set of a prime differential ideal containing  $\Phi$ , such that  $\mathfrak{A}$  contains a characteristic set of each component of  $\{\Phi\}$ .*

**PROBLEM 2** *Given an autoreduced subset of  $\mathcal{F}\{y_1, \dots, y_n\}$ , to determine whether or not it is a characteristic set of a component of  $\{\Phi\}$ .*

(We should, strictly speaking, also include another problem: Given that  $A$  and  $B$  are characteristic sets of prime differential ideals, to determine whether or not these ideals are identical. However, this problem is trivial. See Exercise 1.)

A solution of Problem 2 in the general case is not known, but in an important special case, that in which  $\Phi$  consists of one differential polynomial, a complete solution is given by two theorems of Ritt, the component theorem (Section 14) and the low power theorem (Section 15). Beyond this special case, results are fragmentary.

The problem of finding the components of  $\{\Phi\}$  can be decomposed also into Problem 1 and the following problem.

**PROBLEM 3** *Given that  $A$  and  $B$  are characteristic sets of prime differential ideals  $\mathfrak{p}$  and  $\mathfrak{q}$ , respectively, to determine whether or not  $\mathfrak{p} \subset \mathfrak{q}$ .*

Despite the similarity between this problem and the problem mentioned parenthetically above, Problem 3 seems to be very far from solution. A special case, that in which  $A$  consists of a single irreducible differential polynomial  $A$  (so that  $\mathfrak{p} = \mathfrak{p}_{\mathcal{F}}(A)$ ) and  $\mathfrak{q}$  is the differential ideal  $[y_1, \dots, y_n]$ , is the problem of determining whether the point  $(0, \dots, 0)$  is in the general solution of the

differential equation  $A = 0$ . This is discussed in Section 16, but even here the results are meager.

The main purpose of this section is to give a solution of Problem 1 in the case of finite sets  $\Phi \subset \mathcal{F}\{y_1, \dots, y_n\}$ . We shall do so "in principle" by an inductive procedure that depends on the possibility of solving certain "easier" problems about polynomials in finitely many indeterminates over  $\mathcal{F}$ ; that is, we reduce our problem in algebraic differential equations to a problem in algebraic equations.

To do this we require a criterion for an autoreduced set to be a characteristic set of a prime differential ideal. Let a ranking of  $(y_1, \dots, y_n)$  be fixed. An autoreduced set  $A \subset \mathcal{F}\{y_1, \dots, y_n\}$  is called *coherent* if it is (0)-coherent in the sense of Chapter III, Section 8, that is, whenever  $A, A' \in A$  and  $v$  is a common derivative of  $u_A$  and  $u_{A'}$ , say  $v = \theta u_A = \theta' u_{A'}$ , then  $S_{A'} \theta A - S_A \theta' A' \in (A_v):H_A^\infty$ , where  $A_v$  here denotes the set of differential polynomials  $\theta' A''$  with  $A'' \in A$ ,  $\theta'' \in \Theta$ , and  $\theta'' u_{A''} < v$ . We observe that it suffices to verify this condition when  $v$  is the lowest common derivative of  $u_A, u_{A'}$ . Indeed, let the condition be satisfied for a given  $v$  as above, and let  $w = \delta v = \delta \theta u_A = \delta \theta' u_{A'}$  with  $\delta \in \Delta$ . Since  $S_{A'} \theta A - S_A \theta' A' \in (A_v):H_A^\infty$ , it follows from Chapter I, Section 2, Lemma 1 that  $\delta(S_{A'} \theta A - S_A \theta' A') \in (A_{\delta v}):H_A^\infty = (A_w):H_A^\infty$ , so that

$$\begin{aligned} S_{A'} \delta \theta A - S_A \delta \theta' A' \\ = \delta(S_{A'} \theta A - S_A \theta' A') - \delta S_{A'} \cdot \theta A + \delta S_A \cdot \theta' A' \in (A_w):H_A^\infty. \end{aligned}$$

Therefore we can argue by induction on  $\text{ord } v$ .

The criterion given by the following lemma is due to Rosenfeld [105], who introduced the notion of coherent autoreduced set.

**Lemma 2** *If  $A$  is a characteristic set of a prime differential ideal  $\mathfrak{p}$  of  $\mathcal{F}\{y_1, \dots, y_n\}$ , then  $\mathfrak{p} = [A]:H_A^\infty$ ,  $A$  is coherent, and  $(A):H_A^\infty$  is a prime ideal not containing a nonzero element reduced with respect to  $A$ . Conversely, if  $A$  is a coherent autoreduced subset of  $\mathcal{F}\{y_1, \dots, y_n\}$  such that  $(A):H_A^\infty$  is prime and does not contain a nonzero element reduced with respect to  $A$ , then  $A$  is a characteristic set of a prime differential ideal of  $\mathcal{F}\{y_1, \dots, y_n\}$ .*

**REMARK** Let  $U$  denote any set of derivatives of the differential indeterminates such that  $A \subset \mathcal{F}[U]$ . It is easy to see that the ideal  $(A):H_A^\infty$  of  $\mathcal{F}\{y_1, \dots, y_n\}$  is the ideal generated in  $\mathcal{F}\{y_1, \dots, y_n\}$  by the ideal  $(A):H_A^\infty$  of  $\mathcal{F}[U]$ , and that the ideal  $(A):H_A^\infty$  of  $\mathcal{F}[U]$  is the intersection with  $\mathcal{F}[U]$  of the ideal  $(A):H_A^\infty$  of  $\mathcal{F}\{y_1, \dots, y_n\}$ . It follows that the condition that the ideal  $(A):H_A^\infty$  be prime is independent of the polynomial algebra in which the ideal is taken. In particular, we may take  $U$  to be the set of all derivatives  $\theta y_j$  that are present in at least one element of  $A$ . A similar remark

holds for the condition that  $(A):H_A^\infty$  not contain a nonzero element reduced with respect to  $A$ .

*Proof* Let  $A$  be a characteristic set of a prime differential ideal  $\mathfrak{p}$ . Then  $\mathfrak{p}$  does not contain a nonzero element reduced with respect to  $A$  (see Chapter III, Section 2, the Remark following Lemma 1); therefore  $H_A \notin \mathfrak{p}$ . The remainder with respect to  $A$  of any element of  $\mathfrak{p}$  is in  $\mathfrak{p}$  and is reduced with respect to  $A$ , and therefore is 0. It follows from Chapter I, Section 9, Proposition 1, that  $\mathfrak{p} = [A]:H_A^\infty$ , that whenever  $A, A' \in A$  have leaders with a common derivative  $v = \theta u_A = \theta' u_{A'}$ , then  $S_A \theta' A' - S_{A'} \theta A \in (A_v):H_A^\infty$  (so that  $A$  is coherent), that the ideal  $(A):H_A^\infty$  of  $\mathcal{F}[V]$ , where  $V$  is the set of derivatives of the  $y_j$  that are not proper derivatives of any  $u_A$  ( $A \in A$ ), coincides with  $\mathfrak{p} \cap \mathcal{F}[V]$  and therefore is prime, and that  $(A):H_A^\infty$  contains no nonzero element reduced with respect to  $A$ . Conversely, let  $A$  be a coherent autoreduced set such that  $(A):H_A^\infty$  is prime and contains no nonzero element reduced with respect to  $A$ . By Chapter III, Section 8, Lemma 6,  $[A]:H_A^\infty$  is a prime differential ideal of  $\mathcal{F}\{y_1, \dots, y_n\}$ . By Chapter III, Section 8, Lemma 5, an element of  $[A]:H_A^\infty$  reduced with respect to  $A$  is contained in  $(A):H_A^\infty$  and therefore must be 0. From this it easily follows that  $[A]:H_A^\infty$  does not contain an autoreduced set of lower rank than  $A$ , that is,  $A$  is a characteristic set of  $[A]:H_A^\infty$ .

We are now in a position to solve Problem 1 when posed for a finite set  $\Phi$ . In what follows we enlarge the set of all autoreduced subsets of  $\mathcal{F}\{y_1, \dots, y_n\}$  by adjoining to this set, as a new element, the set  $E$  consisting solely of the element  $1 \in \mathcal{F}$ . We define  $E$  to be of lower rank than every autoreduced set. For every finite set  $\Phi \subset \mathcal{F}\{y_1, \dots, y_n\}$  we let  $A(\Phi)$  denote the set  $E$  in case  $\Phi$  contains a nonzero element of  $\mathcal{F}$  and denote an autoreduced subset of  $\Phi$  of minimal rank otherwise. In general  $A(\Phi)$  is not unique, but its rank is. If  $A(\Phi) = E$ , then  $1 \in \{\Phi\}$ . In this case  $\{\Phi\}$  has no component, so that our problem is solved by taking  $\mathfrak{A} = \emptyset$ .

Let  $A(\Phi) \neq E$ , and assume we can solve Problem 1 when posed for any finite set  $\Psi$  such that  $A(\Psi)$  has lower rank than  $A(\Phi)$ . If  $G \in \mathcal{F}\{y_1, \dots, y_n\}$  is nonzero and reduced with respect to  $A(\Phi)$ , and if we let  $\Phi_G$  denote the union of  $\Phi$  with the set having the one element  $G$ , then  $A(\Phi_G)$  has lower rank than  $A(\Phi)$ . Also, if  $G_1, G_2 \in \mathcal{F}\{y_1, \dots, y_n\}$  and  $G_1 G_2 \in \{\Phi\}$ , then  $\{\Phi\} = \{\Phi_{G_1}\} \cap \{\Phi_{G_2}\}$ , so that if  $\mathfrak{A}_j$  solves Problem 1 posed for  $\Phi_{G_j}$  ( $j = 1, 2$ ), then  $\mathfrak{A}_1 \cup \mathfrak{A}_2$  solves the problem posed for  $\Phi$ . From this we deduce the following general principle: If we can find nonzero differential polynomials  $G_1, \dots, G_s$  reduced with respect to  $A(\Phi)$  such that  $G_1 \dots G_s \in \{\Phi\}$ , then we can solve Problem 1 posed for  $\Phi$ .

The remainder  $R$  of any element of  $\Phi$  with respect to  $A(\Phi)$  is in  $\{\Phi\}$ . Also, if any  $A, A' \in A(\Phi)$  have the property that  $u_A, u_{A'}$  have a lowest common

derivative  $\theta u_A = \theta' u_{A'}$ , then the remainder  $D$  of  $S_{A'} \theta A - S_A \theta' A'$  with respect to  $A(\Phi)$  is in  $\{\Phi\}$ . It follows by the general principle, above, that if some  $R$  or some  $D$  is not 0, then we can solve Problem 1.

Suppose that every  $R$  and  $D$  as above is 0. By the observation preceding Lemma 2 (and by Chapter I, Section 9, Proposition 1)  $A(\Phi)$  is then coherent. If  $(A(\Phi)):H_{A(\Phi)}^\infty$  is not prime, it contains either 1 or a product  $PQ$ , where  $P$  and  $Q$  are not in  $(A(\Phi)):H_{A(\Phi)}^\infty$  and (see the Remark following the statement of Lemma 2) are free of every  $\theta y_j$  not present in the elements of  $A(\Phi)$ . In the latter case, we may replace  $P$  and  $Q$  by their remainders with respect to  $A(\Phi)$ , and may therefore suppose that  $P$  and  $Q$  are reduced with respect to  $A(\Phi)$ . Since  $S_A$  and  $I_A$  are reduced with respect to  $A(\Phi)$  for each  $A \in A(\Phi)$ , we thus see by our general principle that if  $(A(\Phi)):H_{A(\Phi)}^\infty$  is not prime or contains a nonzero differential polynomial reduced with respect to  $A(\Phi)$ , then we can solve our problem.

Suppose, finally, that  $(A(\Phi)):H_{A(\Phi)}^\infty$  is prime and contains no nonzero element reduced with respect to  $A(\Phi)$ . By Lemma 2,  $[A(\Phi)]:H_{A(\Phi)}^\infty$  is a prime differential ideal with characteristic set  $A(\Phi)$ . Also

$$\{\Phi\} = ([A(\Phi)]:H_{A(\Phi)}^\infty) \cap \bigcap_{A \in A(\Phi)} \{\Phi, I_A\} \cap \bigcap_{A \in A(\Phi)} \{\Phi, S_A\}.$$

From this it is apparent that we can solve our problem.

This completes the discussion of Problem 1, except for the following comments. Finding  $A(\Phi)$ , given a finite set  $\Phi$ , is simply a question of making a finite number of comparisons of rank. Finding the remainder of a given differential polynomial with respect to a given autoreduced set is a question of applying the definition of remainder (see Chapter I, Section 9) which is, in effect, an algorithm for computing it. Therefore the effectiveness of the above solution "in principle" of Problem 1 depends on our ability to solve the following algebraic problem.

**PROBLEM (a)** Given a finitely generated polynomial algebra  $\mathcal{F}[X_1, \dots, X_s]$  over  $\mathcal{F}$ , and an  $r \in \mathbb{N}$  with  $r \leq s$ , and  $s-r$  nonzero polynomials  $f_{r+1}, \dots, f_s \in \mathcal{F}[X_1, \dots, X_s]$  such that each  $f_j$  is free of  $X_{j+1}, \dots, X_s$ , is of some degree  $d_j > 0$  in  $X_j$ , and is of degree less than  $d_i$  in  $X_i$  ( $r < i < j$ ), to determine whether or not the ideal  $\mathfrak{k} = (f_{r+1}, \dots, f_s):h^\infty$  of  $\mathcal{F}[X_1, \dots, X_s]$  is prime and contains no nonzero polynomial of degree less than  $d_j$  in  $X_j$  for each  $j$ ,  $h$  here denoting the product  $\prod_{r < j \leq s} l_j \partial f_j / \partial X_j$ , where  $l_j$  is the coefficient of  $X_j^{d_j}$  in  $f_j$  when  $f_j$  is regarded as a polynomial in  $X_j$ ; further, in the event of a negative determination, to find either two polynomials  $g_1, g_2 \notin \mathfrak{k}$  with  $g_1 g_2 \in \mathfrak{k}$  or else one nonzero polynomial in  $\mathfrak{k}$  of degree less than  $d_j$  in  $X_j$  ( $r < j \leq s$ ). If  $r = s$ , this is a trivial matter as then  $\mathfrak{k} = (0)$  and the determination is in the affirmative. If  $r < s$ , and if we set  $\mathfrak{k}' = (f_{r+1}, \dots, f_{s-1}):h'^\infty$  in  $\mathcal{F}[X_1, \dots, X_{s-1}]$ , where  $h' = \prod_{r < j < s} l_j \partial f_j / \partial X_j$ , then it is not very difficult to show that the determina-

tion for  $f$  will be affirmative if and only if the determination for  $f'$  is affirmative and  $f_s(x_1, \dots, x_{s-1}, X_s)$  is irreducible in  $\mathcal{F}(x_1, \dots, x_{s-1})[X_s]$  when  $(x_1, \dots, x_{s-1})$  is a generic zero of  $f'$ .<sup>1</sup>

It should be remarked that although a prime differential ideal  $\mathfrak{p}$  of  $\mathcal{F}\{y_1, \dots, y_n\}$  is determined by its characteristic set  $A$ , it is not always easy, given  $A$ , to find a basis of  $\mathfrak{p}$ . The problem, given a finite set  $\Phi \subset \mathcal{F}\{y_1, \dots, y_n\}$ , of finding finite sets  $\Phi_1, \dots, \Phi_r$  such that  $\{\Phi_1\}, \dots, \{\Phi_r\}$  are the components of  $\{\Phi\}$  is in general an unsolved one. The following proposition, due to Ritt [95, pp. 118–120], is only a partial solution.

**Proposition 5** *Let  $\Phi$  be a finite subset of  $\mathcal{F}\{y_1, \dots, y_n\}$ , and set  $e = \max_{F \in \Phi} \text{ord } F$ . For each  $s \in \mathbb{N}$  let  $A_s$  denote the polynomial algebra  $\mathcal{F}[(\theta y_j)_{\theta \in \Theta(s), 1 \leq j \leq n}]$ ,  $\alpha^{(s)}$  denote the perfect ideal of  $A_{e+s}$  generated by  $\Theta(s)\Phi$ , and  $\mathfrak{X}^{(s)}$  denote the set of components of  $\alpha^{(s)}$  in  $A_{e+s}$ . Then, for every sufficiently big  $s \in \mathbb{N}$ , the components of  $\{\Phi\}$  in  $\mathcal{F}\{y_1, \dots, y_n\}$  are those elements of the set of perfect differential ideals  $\{\mathfrak{p}\}$  ( $\mathfrak{p} \in \mathfrak{X}^{(s)}$ ) that are minimal in that set.*

**REMARK** Thus, to be able to find sets  $\Phi_1, \dots, \Phi_r$  such that  $\{\Phi_1\}, \dots, \{\Phi_r\}$  are the components of  $\{\Phi\}$  it suffices to be able to solve the following three problems: (i) Given  $\Phi$ , to find a value of  $s$  that is sufficiently big in the sense of the proposition. (ii) Given a finite subset  $\Psi$  of a polynomial algebra  $R = \mathcal{F}[X_1, \dots, X_i]$ , to find finite subsets  $\Psi_1, \dots, \Psi_u$  of  $R$  such that the perfect ideals of  $R$  generated by the  $\Psi_i$  are the components of the perfect ideal of  $R$  generated by  $\Psi$ . (iii) Given an  $s \in \mathbb{N}$  and two finite subsets  $\Psi_1$  and  $\Psi_2$  of  $A_s$  such that the perfect ideals  $\mathfrak{p}_1$  and  $\mathfrak{p}_2$  that they generate in  $A_s$  are prime, to determine whether or not  $\{\mathfrak{p}_1\} \subset \{\mathfrak{p}_2\}$ .

Problem (ii) can be effectively handled provided the algebraic Problem (a) mentioned above can be solved (see Ritt [95, Chapter IV, especially pp. 95–103]). Problem (iii) can be reduced to Problem 1 and therefore to Problem (a) as follows: By solving Problem 1 posed for  $\Psi_2$ , we find characteristic sets  $A_1, \dots, A_q$  of prime differential ideals containing  $\mathfrak{p}_2$ . A necessary and sufficient condition that  $\{\mathfrak{p}_1\} \subset \{\mathfrak{p}_2\}$  is that the remainder of every element of  $\Psi_1$  with respect to each  $A_i$  be 0.

The status of Problem (i) is much less satisfactory. There is no way known in general to tell in advance how big  $s$  must be or even to recognize whether a given  $s$  will do.

*Proof of Proposition 5* Let  $\mathfrak{p}_1, \dots, \mathfrak{p}_r$  denote the components of  $\{\Phi\}$ , and let  $\Psi_k$  be a finite set with  $\{\Psi_k\} = \mathfrak{p}_k$  ( $1 \leq k \leq r$ ). The finite set  $\Psi_1 \cdots \Psi_r$  is

<sup>1</sup> For an introductory discussion of the question of factorization in finitely many steps, see B. L. van der Waerden, "Moderne Algebra," Vol. I, 2nd ed., §§ 25, 42. Julius Springer, Berlin, 1937.

contained in  $\{\Phi\}$ , hence in  $\alpha^{(s)}$  for sufficiently big  $s$ , and hence in every  $\mathfrak{p} \in \mathfrak{X}^{(s)}$ . Fixing  $s$  big enough, we see that each  $\mathfrak{p} \in \mathfrak{X}^{(s)}$  must contain some  $\Psi_k$ , so that each  $\{\mathfrak{p}\}$  with  $\mathfrak{p} \in \mathfrak{X}^{(s)}$  (in particular, each minimal one) must contain some  $\mathfrak{p}_k$ . On the other hand,  $\mathfrak{p}_k \supset \{\Phi\} = \{\Theta(s)\Phi\} = \{\alpha^{(s)}\} = \{\bigcap_{\mathfrak{p} \in \mathfrak{X}^{(s)}} \mathfrak{p}\} = \bigcap_{\mathfrak{p} \in \mathfrak{X}^{(s)}} \{\mathfrak{p}\}$ , so that each  $\mathfrak{p}_k$  must contain some minimal  $\{\mathfrak{p}\}$  with  $\mathfrak{p} \in \mathfrak{X}^{(s)}$ .

### EXERCISES

- (a) Let  $\mathfrak{p}$  be a prime differential ideal of  $\mathcal{F}\{y_1, \dots, y_n\}$ , let  $A$  be a characteristic set of  $\mathfrak{p}$ , and let  $F \in \mathcal{F}\{y_1, \dots, y_n\}$ . Show that  $F \in \mathfrak{p}$  if and only if the remainder of  $F$  with respect to  $A$  is 0.  
(b) Let  $\mathfrak{p}$ , respectively  $\mathfrak{q}$ , be a prime differential ideal of  $\mathcal{F}\{y_1, \dots, y_n\}$  with characteristic set  $A$ , respectively  $B$ . Show that  $\mathfrak{p} = \mathfrak{q}$  if and only if  $B \subset \mathfrak{p}$ ,  $H_B \notin \mathfrak{p}$  and  $A \subset \mathfrak{q}$ ,  $H_A \notin \mathfrak{q}$ .
- (Ritt [90; 95, pp. 144–146]) Show that if  $\alpha = (\alpha_1, \dots, \alpha_n)$  is a zero of multiplicity 1 of  $F \in \mathcal{U}\{y_1, \dots, y_n\}$ , then  $\alpha$  is a zero of only one component of  $\{F\}$ . (*Hint:* Let  $u$  be the leader, relative to an orderly ranking, of the linear part of  $F(\alpha_1 + y_1, \dots, \alpha_n + y_n)$ . Show that  $\det(\partial(\theta F)/\partial(\theta' u))_{\theta \in \Theta(s), \theta' \in \Theta(s)}$  does not vanish at  $\alpha$ , and apply Chapter 0, Section 16, Corollary 4 of Proposition 11, and Proposition 5 just proved.)
- (Ritt [95, pp. 10, 172]) Let  $\mathfrak{p}$  be a prime differential ideal of  $\mathcal{F}\{y_1, \dots, y_n\}$  and let  $A$  be a characteristic set of  $\mathfrak{p}$  (relative to a fixed ranking). Prove that  $\mathfrak{p} = \{A\} : \prod_{A \in A} S_A$ . (*Hint:* For any  $F \in \mathfrak{p}$ , let  $\tilde{F}$  denote the partial remainder of  $F$  with respect to  $A$ , let  $v_1, \dots, v_q$  be derivatives of the  $y_j$  that are reduced with respect to  $u_A$  ( $A \in A$ ) such that  $\tilde{F}$  and each  $A \in A$  are elements of the polynomial algebra  $R = \mathcal{F}[v_1, \dots, v_q, (u_A)_{A \in A}]$ , and let  $\mathfrak{p}_0$  denote any component not containing  $\prod_{A \in A} S_A$  of the perfect ideal of  $R$  generated by  $A$ . Using Chapter 0, Section 16, Corollary 4 to Proposition 11, show that  $\dim \mathfrak{p}_0 = q$  and  $\mathfrak{p}_0 \cap \mathcal{F}[v_1, \dots, v_q] = (0)$ . Infer that no nonzero element of  $R$  that is reduced with respect to  $A$  can be in  $\mathfrak{p}_0$ , and therefore that  $\mathfrak{p}_0 = (A) : H_A^\infty$ ,  $\tilde{F} \in \mathfrak{p}_0$ , and  $F \in \{A\} : \prod_{A \in A} S_A$ .)

### 10 The leading coefficient theorem

Let  $c$  be a transcendental constant in an extension of  $\mathcal{U}\langle y_1, \dots, y_n \rangle$ , and let  $\mathcal{F}$  denote an arbitrary differential subfield of  $\mathcal{U}$ . Then (see Chapter I, Section 12) we may form the differential algebra  $\mathcal{F}\{y_1, \dots, y_n\}((c))$  of power series in  $c$  over  $\mathcal{F}\{y_1, \dots, y_n\}$ .

For each power series  $P \in \mathcal{F}\{y_1, \dots, y_n\}((c))$  we denote the series-order of  $P$  by  $\nu(P)$ . If  $\nu(P) \neq \infty$ , that is, if  $P \neq 0$ , we denote the leading coefficient of  $P$  by  $J_P$ ; thus,  $P = J_P c^{\nu(P)} + \dots$ , the dots denoting a power series of series-order greater than  $\nu(P)$ .

**Theorem 4** Let  $A$  and  $B$  be nonzero power series in  $\mathcal{F}\{y_1, \dots, y_n\}((c))$  such that  $B \in \{A\}$  in  $\mathcal{F}\{y_1, \dots, y_n\}((c))$ . Then  $J_B \in \{J_A\}$  in  $\mathcal{F}\{y_1, \dots, y_n\}$ .

*Proof* Because  $p = 0$ , some power  $B^h$  of  $B$  is in  $[A]$  (see Chapter III, Section 1). Since  $J_{B^h} = J_B^h$ , we may replace  $B$  by  $B^h$ , that is, we may suppose that  $B \in [A]$ , so that

$$B = \sum_{\theta \in \Phi} M_\theta \theta A, \tag{3}$$

where  $\Phi$  is a finite nonempty subset of  $\Theta$  and for each  $\theta \in \Phi$ ,  $M_\theta \in \mathcal{F}\{y_1, \dots, y_n\}((c))$ . Multiplying both members of this equation by a suitable power of  $c$ , we may even suppose that  $v(A) = 0$  and  $v(M_\theta) \geq 0$  ( $\theta \in \Phi$ ), from which it follows that  $v(B) \geq 0$ . Thus, we may write

$$\left. \begin{aligned} A &= \sum_{k \geq 0} A_k c^k, & A_k &\in \mathcal{F}\{y_1, \dots, y_n\} & (k \geq 0), & A_0 \neq 0, \\ M_\theta &= \sum_{k \geq 0} M_{\theta,k} c^k, & M_{\theta,k} &\in \mathcal{F}\{y_1, \dots, y_n\} & (k \geq 0) & (\theta \in \Phi), \\ B &= \sum_{k \geq b} B_k c^k, & B_k &\in \mathcal{F}\{y_1, \dots, y_n\} & (k \geq b), & B_b \neq 0, \end{aligned} \right\} \tag{4}$$

so that  $b = v(B) \geq 0$ ,  $J_A = A_0$ ,  $J_B = B_b$ . By Theorem 1, it therefore suffices to prove that every zero of  $A_0$  is a zero of  $B_b$ . However, if  $(\eta_1, \dots, \eta_n)$  is any zero of  $A_0$ , then the substitution of  $(\eta_1 + y_1, \dots, \eta_n + y_n)$  for  $(y_1, \dots, y_n)$ , which is an automorphism of  $\mathcal{U}\{y_1, \dots, y_n\}$ , extends in an obvious way to an automorphism of  $\mathcal{U}\{y_1, \dots, y_n\}((c))$  (each  $\sum C_k(y_1, \dots, y_n) c^k$  being mapped onto  $\sum C_k(\eta_1 + y_1, \dots, \eta_n + y_n) c^k$ ). This extended automorphism transforms (3) into a similar equation, and shows that it suffices to prove the following assertion: Given (3) and (4), if  $A_0$  vanishes at  $(0, \dots, 0)$ , then so does  $B_b$ .

Denoting the multiplicity of  $(0, \dots, 0)$  as a zero of  $A_0$  by  $t_0$ , we suppose inductively that our assertion is valid for lower values of  $(t_0, b)$  in the lexicographically well-ordered set  $\mathbb{N}^2$ , and then prove its validity in the present case. To do this we assume that  $B_b(0, \dots, 0) \neq 0$  and seek a contradiction.

Obviously

$$B_b = \sum_{\theta \in \Phi} \sum_{0 \leq k \leq b} M_{\theta, b-k} \theta A_k,$$

so that there exists a smallest  $h \in \mathbb{N}$  with  $A_h(0, \dots, 0) \neq 0$ ; of course  $0 < h \leq b$ . We denote by  $t_k$  the multiplicity of  $(0, \dots, 0)$  as a zero of  $A_k$  ( $0 < k < h$ ), and define  $\rho = \max_{0 \leq k < h} (h-k)/t_k$ . Since  $\rho$  is a strictly positive rational number, we may write  $\rho = r/s$ , where  $r$  and  $s$  are relatively prime nonzero natural numbers. Substituting  $(c^s, c^r y_1, \dots, c^r y_n)$  for  $(c, y_1, \dots, y_n)$ , we obtain from (3) and (4) similar equations

$$B' = \sum_{\theta \in \Phi} M'_\theta \theta A' \tag{3'}$$

and

$$\left. \begin{aligned} A' &= \sum_{k \geq h_s} A'_k c^k, & A'_{h_s} &= A_h(0, \dots, 0) + \sum_{\substack{0 \leq k < h \\ (h-k)/t_k = \rho}} A_{k_s} \\ & & (A_{k_s} \text{ denoting the homogeneous part of } A_k \text{ of degree } t_k), \\ M'_\theta &= \sum_{k \geq 0} M'_{\theta,k} c^k & (\theta \in \Phi), \\ B' &= \sum_{k \geq b_s} B'_k c^k, & B'_{b_s} &= B_b(0, \dots, 0). \end{aligned} \right\} \tag{4'}$$

Clearly  $A'_{h_s} \neq 0$  and  $0 < \deg A'_{h_s} \leq t_0$ , and  $\deg A'_{h_s} = t_0$  if and only if  $\rho t_0 = h$ . Since  $p = 0$  this implies, in particular, that  $A'_{h_s}$  has a zero (for example, any zero of the general component of an irreducible factor of  $A'_{h_s}$  in  $\mathcal{U}\{y_1, \dots, y_n\}$ ). Let  $(\alpha_1, \dots, \alpha_n)$  be a zero of  $A'_{h_s}$  of minimal multiplicity  $\bar{t}_0$ . Then  $0 < \bar{t}_0 \leq t_0$ , and  $\bar{t}_0 = t_0$  only if  $\rho t_0 = h$  and every zero of  $A'_{h_s}$  has multiplicity  $t_0$ . It follows from Section 8, Lemma 1, that if  $\bar{t}_0 = t_0$ , then  $\rho t_0 = h$  and  $A'_{h_s} = \varphi \cdot (\beta + H)^{t_0}$  for suitable  $\varphi, \beta \in \mathcal{F}$  with  $\varphi \neq 0$  and nonzero homogeneous linear  $H \in \mathcal{F}\{y_1, \dots, y_n\}$ ; by (4') then

$$\varphi \cdot (\beta^{t_0} + t_0 \beta^{t_0-1} H + \dots + H^{t_0}) = A_h(0, \dots, 0) + \sum_{\substack{0 \leq k < h \\ (h-k)/t_k = \rho}} A_{k_s} \tag{5}$$

whence  $\varphi \cdot \beta^{t_0} = A_h(0, \dots, 0)$ , so that  $\beta \neq 0$  and hence the homogeneous part of degree 1 of the left member of (5) is different from 0; therefore there must exist a  $k \in \mathbb{N}$  with  $0 \leq k < h$ ,  $(h-k)/t_k = \rho$ ,  $t_k = 1$ , that is, with  $\rho = h-k$ . Therefore if  $\bar{t}_0 = t_0$ , then  $\rho \in \mathbb{N}$  so that  $s = 1$ .

Substituting  $(\alpha_1 + y_1, \dots, \alpha_n + y_n)$  for  $(y_1, \dots, y_n)$  in (3') and then dividing both members by  $c^{h_s}$ , we find by (3') and (4') equations

$$\bar{B} = \sum_{\theta \in \Phi} \bar{M}_\theta \theta \bar{A}$$

and

$$\begin{aligned} \bar{A} &= \sum_{k \geq 0} \bar{A}_k c^k, & \bar{A}_0 &= A'_{h_s}(\alpha_1 + y_1, \dots, \alpha_n + y_n) \neq 0, \\ \bar{M}_\theta &= \sum_{k \geq 0} \bar{M}_{\theta,k} c^k & (\theta \in \Phi), \\ \bar{B} &= \sum_{k \geq \bar{b}} \bar{B}_k c^k, & \bar{b} &= b_s - h_s, & \bar{B}_{\bar{b}} &= B'_{b_s} = B_b(0, \dots, 0) \neq 0, \end{aligned}$$

so that  $\bar{b} = v(\bar{B})$  and  $\bar{t}_0$  is the multiplicity of  $(0, \dots, 0)$  as a zero of  $\bar{A}_0$ . By what we have seen, either  $\bar{t}_0 < t_0$ , or else  $\bar{t}_0 = t_0$ ,  $s = 1$ ,  $\bar{b} = b_s - h_s = b - h < b$ . Thus, in either case  $(\bar{t}_0, \bar{b}) < (t_0, b)$  in the lexicographic order on  $\mathbb{N}^2$ . By the induction hypothesis then  $\bar{B}_{\bar{b}}$  must vanish at  $(0, \dots, 0)$ . This contradiction proves the theorem.

It is easy to see that if  $\mathcal{R}$  and  $\mathcal{R}'$  are differential algebras over  $\mathbf{Q}$ , if  $a \in \mathcal{R}$ , and if  $f: \mathcal{R} \rightarrow \mathcal{R}'$  is a ring homomorphism such that  $f(\theta a) \in \{f(a)\}$  for every derivative operator  $\theta$  of  $\mathcal{R}$ , then  $f$  maps  $\{a\}$  into  $\{f(a)\}$ . We therefore have the following corollary to Theorem 4.

**Corollary 1** *Let  $\mathcal{R}$  be a differential algebra over  $\mathbf{Q}$ , let  $a, b \in \mathcal{R}$ , and let  $f: \mathcal{R} \rightarrow \mathcal{U}\{y_1, \dots, y_n\}((c))$  be a ring homomorphism such that  $f(a)f(b) \neq 0$  and  $f(\theta a) \in \{f(a)\}$  for every  $\theta \in \Theta$ . If  $b \in \{a\}$ , then  $J_{f(b)} \in \{J_{f(a)}\}$ .*

Ring homomorphisms like  $f$  above can be constructed as follows. Let  $\mathcal{F}_0$  and  $\mathcal{F}$  be differential subfields of  $\mathcal{U}$  with  $\mathcal{F}_0 \subset \mathcal{F}$ , and suppose given an  $m \times m$  matrix  $C = (C_{ii'})_{1 \leq i \leq m, 1 \leq i' \leq m}$  over  $\mathcal{K}((c))$  with  $\det C \neq 0$  and a ring homomorphism  $f_0: \mathcal{F} \rightarrow \mathcal{U}((c))$  such that

$$f_0(\delta_i \varphi) = \sum_{1 \leq i' \leq m} C_{ii'} \delta_{i'} f_0(\varphi) \quad (1 \leq i \leq m)$$

for every  $\varphi \in \mathcal{F}_0$ . Choose any  $n$ -tuple  $P = (P_j)_{1 \leq j \leq n} \in \mathcal{U}((c))^n$  and any  $n \times n$  matrix  $Q = (Q_{jj'})_{1 \leq j \leq n, 1 \leq j' \leq n}$  over  $\mathcal{U}((c))$  with  $\det Q \neq 0$ . There exists a unique ring homomorphism  $f: \mathcal{F}\{y_1, \dots, y_n\} \rightarrow \mathcal{U}\{y_1, \dots, y_n\}((c))$  extending  $f_0$  such that

$$f(\delta_1^{e_1} \dots \delta_m^{e_m} y_j) = \left( \sum_{1 \leq i' \leq m} C_{1i'} \delta_{i'} \right)^{e_1} \dots \left( \sum_{1 \leq i' \leq m} C_{mi'} \delta_{i'} \right)^{e_m} \left( P_j + \sum_{1 \leq j' \leq n} Q_{jj'} y_{j'} \right) \quad (6)$$

for every  $(e_1, \dots, e_m) \in \mathbf{N}^m$  and every  $y_j$ . It is now easy to see, for any  $A \in \mathcal{F}_0\{y_1, \dots, y_n\}$ , that  $f(\delta_i A) = \sum_{1 \leq i' \leq m} C_{ii'} \delta_{i'} f(A)$  ( $1 \leq i \leq m$ ), and therefore that  $f(\theta A) \in [f(A)]$  ( $\theta \in \Theta$ ). Hence  $f$  has the desired property.

Given  $\mathcal{F}$  and an  $A \in \mathcal{F}\{y_1, \dots, y_n\}$ , we define an  $A$ -permissible homomorphism to be any ring homomorphism

$$f: \mathcal{F}\{y_1, \dots, y_n\} \rightarrow \mathcal{U}\{y_1, \dots, y_n\}((c))$$

that can be obtained in the manner just described. That is,  $f$  is  $A$ -permissible if  $f$  maps  $\mathcal{F}$  into  $\mathcal{U}((c))$  and if there exist an invertible  $m \times m$  matrix  $C = (C_{ii'})$  over  $\mathcal{K}((c))$ , an  $n$ -tuple  $P = (P_j)$  over  $\mathcal{U}((c))$ , and an invertible  $n \times n$  matrix  $Q = (Q_{jj'})$  over  $\mathcal{U}((c))$ , such that  $f(\delta_i \varphi) = \sum_{1 \leq i' \leq m} C_{ii'} \delta_{i'} f(\varphi)$  ( $1 \leq i \leq m$ ) for every element  $\varphi$  of the differential field generated by the coefficients in  $A$  and such that (6) holds for all  $(e_1, \dots, e_m) \in \mathbf{N}^m$  and  $1 \leq j \leq n$ . It is evident that  $C, P, Q$  are unique for a given  $f$ .

**Corollary 2** *Let  $\mathcal{F}$  be a differential subfield of  $\mathcal{U}$ , let  $A$  and  $B$  be nonzero elements of  $\mathcal{F}\{y_1, \dots, y_n\}$ , and let  $f: \mathcal{F}\{y_1, \dots, y_n\} \rightarrow \mathcal{U}\{y_1, \dots, y_n\}((c))$  be an  $A$ -permissible homomorphism. If  $B \in \{A\}$ , then  $J_{f(B)} \in \{J_{f(A)}\}$ .*

*Proof* This is a special case of Corollary 1.

An example of an  $A$ -permissible homomorphism is given by the substitution of  $(c^{v_1} y_1, \dots, c^{v_n} y_n)$  for  $(y_1, \dots, y_n)$ ,  $v_1, \dots, v_n$  denoting arbitrary rational integers. Here  $C$  is the unity matrix,  $P = (0)$ , and  $Q$  is the diagonal matrix with main diagonal  $(c^{v_1}, \dots, c^{v_n})$ . In this case  $J_{f(A)}$  coincides with  $A_*$ , the nonzero homogeneous part of  $A$  of lowest degree relative to the differential permissible grading of  $\mathcal{F}\{y_1, \dots, y_n\}$  determined by  $v_1, \dots, v_n, 0, \dots, 0$  (see Chapter I, Section 7). If we use  $-v_1, \dots, -v_n$  instead of  $v_1, \dots, v_n$ , then  $J_{f(A)}$  coincides with  $A^*$ , the nonzero homogeneous part of  $A$  of highest degree relative to the same grading. If the coefficients in  $A$  all are constants and  $(\mu_1, \dots, \mu_m) \in \mathbf{Z}^m$ , then the  $\mathcal{F}$ -algebra homomorphism  $\mathcal{F}\{y_1, \dots, y_n\} \rightarrow \mathcal{U}\{y_1, \dots, y_n\}((c))$  mapping  $\delta_1^{e_1} \dots \delta_m^{e_m} y_j$  onto  $c^{v_j + \mu_1 e_1 + \dots + \mu_m e_m} \delta_1^{e_1} \dots \delta_m^{e_m} y_j$  ( $(e_1, \dots, e_m) \in \mathbf{N}^m, 1 \leq j \leq n$ ) is also  $A$ -permissible. Here  $C$  is the diagonal matrix with diagonal  $(c^{\mu_1}, \dots, c^{\mu_m})$  and  $P, Q$  are as before. In this case  $J_{f(A)} = A_*$  is the nonzero homogeneous part of  $A$  of lowest degree relative to the permissible grading of  $\mathcal{F}\{y_1, \dots, y_n\}$  determined by  $v_1, \dots, \mu_n, \mu_1, \dots, \mu_m$ . Corollary 2 therefore has the following special case.

**Corollary 3** *Let  $A$  and  $B$  be elements of  $\mathcal{F}\{y_1, \dots, y_n\}$  with  $AB \neq 0$  (respectively with  $AB \neq 0$  and the coefficients in  $A$  constant). Fix an arbitrary differential permissible grading (respectively arbitrary permissible grading), and, for each nonzero  $F \in \mathcal{F}\{y_1, \dots, y_n\}$ , let  $F_*$  denote the nonzero homogeneous part of  $F$  of lowest degree relative to this grading and let  $F^*$  denote that of highest degree. If  $B \in \{A\}$ , then  $B_* \in \{A_*\}$  and  $B^* \in \{A^*\}$ .*

This corollary is false without the hypothesis  $p = 0$  (see Exercise 2).

We shall say that an  $A$ -permissible homomorphism  $f$  is *strictly positive* if the  $C, P, Q$  that correspond to  $f$  as above have the properties

$$\begin{aligned} v(C_{ii'}) &\geq 0 & (1 \leq i \leq m, 1 \leq i' \leq m) & \quad \text{and} \quad v(\det C) = 0, \\ v(P_j) &> 0 & (1 \leq j \leq n), \\ v(Q_{jj'}) &> 0 & (1 \leq j \leq n, 1 \leq j' \leq n). \end{aligned}$$

When  $f$  is the  $A$ -permissible homomorphism associated with a differential permissible grading (or, if the coefficients in  $A$  are constants, with a permissible grading) in the manner described directly after Corollary 2,  $f$  is strictly positive if and only if the grading is (see Chapter I, Section 7).

### EXERCISES

- Suppose that the differential subfield  $\mathcal{F}$  of  $\mathcal{U}$  is the differential field of quotients of  $K[[X_1, \dots, X_n]]$ ,  $K$  being a field of characteristic 0 and  $\delta_i$

operating on  $K[[X_1, \dots, X_n]]$  according to the formula  $\delta_i \varphi = \partial \varphi / \partial X_i$  ( $1 \leq i \leq m$ ). Let  $(C_{ii})$  be an  $m \times m$  matrix over  $K((c))$  with inverse  $(D_{ii})$ , let  $(P_i) \in \mathcal{U}((c))^m$ , and let  $(Q_{jj'})$  be an invertible  $n \times n$  matrix over  $\mathcal{U}((c))$ . Show that there exists a unique ring homomorphism  $f: \mathcal{F}\{y_1, \dots, y_n\} \rightarrow \mathcal{U}\{y_1, \dots, y_n\}((c))$  that coincides on  $K[[X_1, \dots, X_m]]$  with the substitution of  $(\sum_{1 \leq i' \leq m} D_{i'i} X_{i'})_{1 \leq i \leq m}$  for  $(X_i)_{1 \leq i \leq m}$  and that maps  $\delta_1^{e_1} \dots \delta_m^{e_m} y_j$  onto

$$\left( \sum_{1 \leq i_1 \leq m} C_{ii_1} \delta_{i_1} \right)^{e_1} \dots \left( \sum_{1 \leq i_m < m} C_{mi_m} \delta_{i_m} \right)^{e_m} \left( P_j + \sum_{1 \leq j' \leq m} Q_{jj'} y_{j'} \right)$$

$(e_1, \dots, e_m) \in \mathbb{N}^m$ ,  $1 \leq j \leq n$ . Show that  $f$  is  $A$ -permissible for every nonzero  $A \in \mathcal{F}\{y_1, \dots, y_n\}$ .

2. Working over an ordinary differential field of characteristic  $q \neq 0$ , let  $A = y''^q + y^{q+1} + y' y''^{q+1}$  and  $B = A'$ . Show that relative to the usual grading  $B_* \notin \{A_*\}$ .
3. Let  $\mathcal{F}$  be a differential subfield of  $\mathcal{U}$ , let  $A \in \mathcal{F}\{y_1, \dots, y_n\}$ ,  $A \notin \mathcal{F}$ , and let  $\theta \in \Theta$ .

(a) Let  $\mathfrak{p}$  be a component of  $\{\theta A\}$  in  $\mathcal{F}\{y_1, \dots, y_n\}$ , let  $\eta = (\eta_1, \dots, \eta_n)$  be a generic zero of  $\mathfrak{p}$ , and let  $f$  denote the substitution of  $(\eta_i + y_i c, \dots, \eta_n + y_n c)$  for  $(y_1, \dots, y_n)$ . Show that if  $F \in \mathfrak{p}$ , then  $J_{f(F)} \in \{\theta J_{f(A)}\}$  in  $\mathcal{F}\langle \eta \rangle\{y_1, \dots, y_n\}$ . (Hint: Let  $E \notin \mathfrak{p}$  be in every other component of  $\{\theta A\}$ , so that  $EF \in \{\theta A\}$ , and apply Corollary 2 of Theorem 4.)

(b) Prove the following result of Hillman: *If  $\text{ord } \theta > 0$ , then every component of  $\{A\}$  properly contains a component of  $\{\theta A\}$ .* (Hint: If a component  $\mathfrak{p}$  of  $\{A\}$  were also a component of  $\{\theta A\}$ , part (a) would yield  $J_{f(A)} \in \{\theta J_{f(A)}\}$ .)

(c) Prove the following result of Hillman: *If  $\text{ord } \theta > \text{ord } A$  (more generally, if a separant of  $A$  is reduced with respect to  $\theta y_1, \dots, \theta y_n$ ), then  $\{\theta A\}$  is prime.* (Hint: Show that  $\{\theta A\}$  has precisely one component not containing  $S_A$ . Assuming that  $\{\theta A\}$  has another component  $\mathfrak{p}$ , apply part (a) to  $F = S_A$ .)

### 11 Levi's lemma

In this section we deal with differential polynomials over  $\mathbb{Q}$  in  $z_1, \dots, z_r$  and a number of other differential indeterminates which we denote by  $u_{\rho\gamma}$  ( $1 \leq \rho \leq r$ ,  $0 \leq \gamma \leq g_\rho$ ). Here  $r, g_1, \dots, g_r$  are natural numbers with  $r \neq 0$ . The words "degree" and "homogeneous" refer to the usual grading. We also use the notions of "weight" and "isobaric" as defined in Chapter I, Section 7.

**Lemma 3** *Let  $G_1, \dots, G_r$  be differential polynomials in*

$$\mathbb{Q}\{z_1, \dots, z_r, (u_{\rho\gamma})_{1 \leq \rho \leq r, 0 \leq \gamma \leq g_\rho}\}$$

*of the form*

$$G_\rho = u_{\rho 0} z_\rho^{q_\rho} + \sum_{1 \leq \gamma \leq g_\rho} u_{\rho\gamma} M_{\rho\gamma} \quad (1 \leq \rho \leq r),$$

*where (for each  $\rho$ )  $q_\rho \in \mathbb{N}$  and  $M_{\rho 1}, \dots, M_{\rho g_\rho}$  are differential monomials in  $(z_1, \dots, z_r)$  of degree greater than  $q_\rho$ . Then there exist a monomial  $U = u_{10}^{d_1} \dots u_{r0}^{d_r}$ , and a differential polynomial*

$$Z \in \mathbb{Q}\{z_1, \dots, z_r, (u_{\rho\gamma})_{1 \leq \rho \leq r, 0 \leq \gamma \leq g_\rho}\}$$

*with  $Z \in [z_1, \dots, z_r]$  and with  $Z$  homogeneous in  $(\theta u_{\rho\gamma})_{\theta \in \Theta, 0 \leq \gamma \leq g_\rho}$  of degree  $d_\rho$  ( $1 \leq \rho \leq r$ ) and with the degree of  $Z$  in  $(\theta u_{\rho 0})_{\theta \in \Theta, 1 \leq \rho \leq r}$  strictly smaller than  $d_1 + \dots + d_r$ , such that*

$$z_\rho(U + Z) \in \{G_1, \dots, G_r\} \quad (1 \leq \rho \leq r).$$

*Proof* Replacing  $G_\rho$  by  $z_\rho^{q_\rho - q} G_\rho$ , where  $q \geq q_\rho$  ( $1 \leq \rho \leq r$ ), we may suppose that  $q_1, \dots, q_r$  all have the same value  $q$  and that  $q > 0$ .

Let  $k$  denote the maximum of all the numbers  $\text{wt } M_{\rho\gamma}$  ( $1 \leq \rho \leq r$ ,  $1 \leq \gamma \leq g_\rho$ ). By Chapter I, Section 7, Lemma 4 (case  $l = 0$ ), there exists a natural number  $e = e(r, k, q, m)$  such that every differential monomial  $N$  in  $(z_1, \dots, z_r)$  of degree  $e$  and weight less than or equal to  $ke$  is in one of the differential ideals  $[z_\rho^q]$ . Since each derivative  $\theta(z_\rho^q)$  is homogeneous of degree  $q$  and isobaric of weight  $\text{ord } \theta$ , we may write

$$N = \sum_{\text{ord } \theta \leq \text{wt } N} A_\theta \theta(z_\rho^q),$$

where  $A_\theta \in \mathbb{Q}\{z_1, \dots, z_r\}$  is homogeneous of degree  $e - q$  and isobaric of weight  $\text{wt } N - \text{ord } \theta$ . However, by Chapter I, Section 2, Lemma 1, we may also write

$$u_{\rho 0}^{1 + \text{ord } \theta} \theta(z_\rho^q) = \sum_{\theta' | \theta} U_{\theta, \theta', \rho} \theta'(u_{\rho 0} z_\rho^q),$$

where  $U_{\theta, \theta', \rho} \in \mathbb{Z}\{u_{\rho 0}\}$  is homogeneous of degree  $\text{ord } \theta$ . Furthermore,  $u_{\rho 0} z_\rho^q \equiv -\sum_{1 \leq \gamma \leq g_\rho} u_{\rho\gamma} M_{\rho\gamma} \pmod{[G_\rho]}$ , so that

$$\begin{aligned} \theta'(u_{\rho 0} z_\rho^q) &\equiv - \sum_{1 \leq \gamma \leq g_\rho} \theta'(u_{\rho\gamma} M_{\rho\gamma}) \\ &\equiv \sum_{1 \leq \gamma \leq g_\rho} \sum_{\theta'' \theta''' = \theta'} b_{\theta'', \theta'''} \theta'' u_{\rho\gamma} \theta''' M_{\rho\gamma} \pmod{[G_\rho]}, \end{aligned}$$

where  $b_{\theta'', \theta'''} \in \mathbb{Z}$ . Therefore

$$u_{\rho 0}^{1 + ke} N \equiv \sum_{\text{ord } \theta \leq \text{wt } N} \sum_{\theta' | \theta} \sum_{1 \leq \gamma \leq g_\rho} \sum_{\theta'' \theta''' = \theta'} A_\theta u_{\rho 0}^{ke - \text{ord } \theta} U_{\theta, \theta', \rho} b_{\theta'', \theta'''} \theta'' u_{\rho\gamma} \theta''' M_{\rho\gamma} \pmod{[G_\rho]},$$

Consider any differential monomial  $L$  appearing with a nonzero coefficient in any  $A_\theta \theta^m M_{\rho\gamma}$  here. Clearly,  $\deg L \geq e - q + q + 1 = e + 1$  and  $\text{wt } L = \text{wt } N - \text{ord } \theta + \text{ord } \theta^m + \text{wt } M_{\rho\gamma} \leq ke + k$ . If all the derivatives of  $z_1, \dots, z_r$  dividing  $L$  have order less than or equal to  $k$ , then the product of any  $e$  of them is a differential monomial of degree  $e$  and weight less than or equal to  $ke$ , whereas if one of these derivatives has order greater than  $k$ , then the product of  $e$  of the others has weight less than  $ke$ . Thus, in either case,  $L$  is divisible by a differential monomial in  $(z_1, \dots, z_r)$  of degree  $e$  and weight less than or equal to  $ke$ . Let us denote all these differential monomials by  $N_1, \dots, N_h$ . What we have done shows that for each  $N_j$  there exists an index  $\rho = \rho(j)$  such that

$$u_{\rho(j)}^{1+ke} N_j \equiv \sum_{1 \leq j' \leq h} V_{jj'} N_{j'} \pmod{[G_1, \dots, G_r]},$$

where  $V_{jj'} \in \mathbf{Q}\{z_1, \dots, z_r, (u_{\rho(j)\gamma})_{0 \leq \gamma \leq g_\rho}\}$  is homogeneous in  $(\theta u_{\rho(j)\gamma})_{\theta \in \Theta}$  of degree  $ke$ , is homogeneous in  $(\theta u_{\rho(j)\gamma})_{\theta \in \Theta, 1 \leq \gamma \leq g_\rho(j)}$  of degree 1, and is an element of  $[z_1, \dots, z_r]$ . Transposing the sum to the left side, we obtain a system of homogeneous linear congruences in  $N_1, \dots, N_h$ . The determinant of this system can evidently be written in the form  $U + Z$  with  $U$  and  $Z$  as described in the statement of the lemma. Solving the system of congruences we therefore find that  $(U + Z) N_j \equiv 0 \pmod{[G_1, \dots, G_r]}$  for every  $j$ . Since each  $z_\rho^e$  is an  $N_j$  we see finally that  $z_\rho(U + Z) \in \{G_1, \dots, G_r\}$  ( $1 \leq \rho \leq r$ ).

**12 The domination lemma**

Before applying the results of the last two sections to the study of differential equations, we generalize the case  $r = 1$  of Levi's lemma. To this end we introduce some definitions and two preliminary lemmas.

As before, we deal with differential monomials in  $(z_1, \dots, z_r)$ . By a *prime factor* of such a differential monomial  $M$ , we mean (as in Chapter I, Section 6) a derivative  $\theta z_k$  that divides  $M$ . For any set  $V$  of derivatives  $\theta z_k$  we let  $M_V$  denote the product of all the prime factors  $w$  of  $M$  with  $w \in \Theta V$ , each  $w$  taken the same number of times as it occurs in  $M$ . Thus, if  $\Theta V$  contains no prime factor of  $M$ , then  $M_V = 1$ , whereas if  $\Theta V$  contains every prime factor of  $M$ , then  $M_V = M$ .

Let  $M$  and  $N$  be differential monomials. We shall say that  $N$  *dominates*  $M$  if, for every set  $V$  of derivatives  $\theta z_k$ , the following condition is satisfied:

$$\text{either } \deg M_V < \deg N_V \quad \text{or} \quad M_V = N_V.$$

Since  $M_V = M_{\Theta V} = M_{(\Theta V) \cap V(M)}$ , where  $V(M)$  denotes the set of all prime factors of  $M$ , it suffices to verify this condition for every nonempty set  $V$

with  $V \subset V(M)$ . If, for every nonempty  $V$  with  $V \subset V(M)$ ,  $N$  satisfies the stronger condition

$$\deg M_V < \deg N_V,$$

then we shall say that  $N$  *strongly dominates*  $M$ .

If  $N_\gamma$  dominates (respectively strongly dominates)  $M_\gamma$  ( $1 \leq \gamma \leq g$ ), then  $\prod_{1 \leq \gamma \leq g} N_\gamma$  dominates (respectively strongly dominates)  $\prod_{1 \leq \gamma \leq g} M_\gamma$ . If  $N_\gamma$  dominates  $M$  ( $1 \leq \gamma \leq g$ ) and, for at least one  $\gamma$ ,  $N_\gamma$  strongly dominates  $M$ , then  $\prod_{1 \leq \gamma \leq g} N_\gamma$  strongly dominates  $M^g$ . It follows that if  $v_1, \dots, v_t$  are the distinct prime factors of  $M$  and  $M = v_1^{a_1} \dots v_t^{a_t}$ , and if  $N$  can be written in the form  $N = \prod_{1 \leq \tau \leq t} Q_\tau$  with  $Q_\tau$  dominating (respectively strongly dominating)  $v_\tau^{a_\tau}$  ( $1 \leq \tau \leq t$ ), then  $N$  dominates (respectively strongly dominates)  $M$ . We shall say in such a case that  $N$  dominates (respectively strongly dominates)  $M$  *factorially*.

If  $N_\gamma$  dominates (respectively strongly dominates)  $M_\gamma$  factorially ( $1 \leq \gamma \leq g$ ), then  $\prod_{1 \leq \gamma \leq g} N_\gamma$  dominates (respectively strongly dominates)  $\prod_{1 \leq \gamma \leq g} M_\gamma$  factorially. If  $N_\gamma$  dominates  $M$  factorially ( $1 \leq \gamma \leq g$ ) and, for at least one  $\gamma$ ,  $N_\gamma$  strongly dominates  $M$  factorially, then  $\prod_{1 \leq \gamma \leq g} N_\gamma$  strongly dominates  $M^g$  factorially.

It is easy to see that there exists a biggest set  $W$  of prime factors of  $M$  such that  $M_W = N_W$ . It is clear that if  $N$  dominates  $M$ , then a necessary and sufficient condition that  $N$  strongly dominate  $M$  is that  $W$  be empty. We call  $W$  the *weakness* of  $N$  over  $M$ . If  $N_\gamma$  dominates  $M$  ( $1 \leq \gamma \leq g$ ) and the weakness of  $N_\gamma$  over  $M$  is  $W_\gamma$ , then the weakness of  $\prod_{1 \leq \gamma \leq g} N_\gamma$  over  $M^g$  is  $\bigcap_{1 \leq \gamma \leq g} W_\gamma$ .

**Lemma 4** *If  $N_\gamma$  strongly dominates  $M$  ( $1 \leq \gamma \leq g$ ), then, for all  $(i_1, \dots, i_g) \in \mathbf{N}^g$  for which the sum  $h = \sum_{1 \leq \gamma \leq g} i_\gamma$  is sufficiently big,  $\prod_{1 \leq \gamma \leq g} N_\gamma^{i_\gamma}$  strongly dominates  $M^h$  factorially.*

*Proof* Write  $M = \prod_{k \in K} v_k^{a_k}$  with  $K$  a finite set and the  $v_k$  ( $k \in K$ ) the distinct prime factors of  $M$ . For each nonempty set  $J \subset K$  let  $x_J^\gamma$  denote the number of prime factors  $v$  of  $N_\gamma$  such that  $v$  is a derivative of  $v_k$  for every  $k \in J$  and  $v$  is not a derivative of  $v_k$  for any  $k \in K - J$  (each  $v$  being counted as many times as it occurs in  $N_\gamma$ ). Because  $N_\gamma$  strongly dominates  $M$  we have, for each  $\gamma$ ,

$$\sum_{J \in \mathfrak{P}'(K) - \mathfrak{P}'(K - I)} x_J^\gamma > \sum_{i \in I} a_i \quad (I \in \mathfrak{P}'(K)),$$

where, for any set  $S$ ,  $\mathfrak{P}'(S)$  denotes the set of nonempty subsets of  $S$ . By Chapter 0, Section 18, Corollary to Lemma 17, there exists an  $h_0 \in \mathbf{N}$  and, for each  $(J, j)$  with  $J \in \mathfrak{P}'(K)$  and  $j \in J$ , there exists a  $y_{j,j}^\gamma \in \mathbf{N}$ , such that  $\sum_{j \in J} y_{j,j}^\gamma = h_0 x_J^\gamma$  and  $\sum_{j \in J} y_{j,j}^\gamma > h_0 a_j$ . It follows that we may write  $N_\gamma^{h_0} = \prod_{j \in K} N_{\gamma j}$ , where, for each  $j \in K$ ,  $N_{\gamma j}$  is a differential monomial in  $(z_1, \dots, z_r)$

of which the degree in  $(\theta v_j)_{\theta \in \Theta}$  is greater than or equal to  $h_0 a_j + 1$ . Let  $(i_1, \dots, i_g) \in \mathbb{N}^g$  and write  $i_\gamma = q_\gamma h_0 + r_\gamma$  with  $q_\gamma, r_\gamma \in \mathbb{N}$  and  $r_\gamma < h_0$ . Then

$$\prod_{1 \leq \gamma \leq g} N_\gamma^{i_\gamma} = \prod_{1 \leq \gamma \leq g} N_\gamma^{q_\gamma h_0} \cdot \prod_{1 \leq \gamma \leq g} N_\gamma^{r_\gamma} = \prod_{j \in K} \prod_{1 \leq \gamma \leq g} N_{\gamma_j}^{q_\gamma} \cdot \prod_{1 \leq \gamma \leq g} N_\gamma^{r_\gamma}.$$

For each  $j \in K$  the degree of  $\prod_{1 \leq \gamma \leq g} N_{\gamma_j}$  in  $(\theta v_j)_{\theta \in \Theta}$  is greater than or equal to

$$\begin{aligned} \sum_{1 \leq \gamma \leq g} q_\gamma (h_0 a_j + 1) &= \sum_{1 \leq \gamma \leq g} (i_\gamma - r_\gamma) h_0^{-1} (h_0 a_j + 1) \\ &\geq (h - g(h_0 - 1)) h_0^{-1} (h_0 a_j + 1), \end{aligned}$$

where  $h = \sum_{1 \leq \gamma \leq g} i_\gamma$ , so that this degree is greater than  $a_j h$  provided  $h > g(h_0 - 1)(h_0 a_j + 1)$ . Therefore  $\prod_{1 \leq \gamma \leq g} N_\gamma$  strongly dominates  $M^h$  factorially whenever  $h$  is sufficiently big.

In the next lemma  $(u_0, u_1, \dots, u_g)$  denotes a family of differential intermediates over  $\mathbb{Q}\langle z_1, \dots, z_r \rangle$ .

**Lemma 5** Let  $F = \sum_{0 \leq \gamma \leq g} u_\gamma M_\gamma \in \mathbb{Q}\langle z_1, \dots, z_r, u_0, u_1, \dots, u_g \rangle$ , where  $M_0, M_1, \dots, M_g$  are differential monomials in  $(z_1, \dots, z_r)$  with  $M_0 \neq 0$  and  $M_\gamma \neq M_0$  ( $1 \leq \gamma \leq g$ ). If each  $M_\gamma$  with  $\gamma \neq 0$  dominates (respectively strongly dominates)  $M_0$ , then the ideal  $(F)$  contains a differential polynomial  $G = u_0^a M_0^a + \sum_{1 \leq \beta \leq b} U_\beta N_\beta$ , where  $a \in \mathbb{N}$ ,  $a \neq 0$ , each  $U_\beta$  is a monomial in  $(u_0, u_1, \dots, u_g)$  other than  $u_0^a$  of degree  $a$ , and each  $N_\beta$  is a differential monomial in  $(z_1, \dots, z_r)$  other than  $M_0^a$  that dominates (respectively strongly dominates)  $M_0^a$  factorially.

*Proof* Assume that each  $M_\gamma$  with  $\gamma \neq 0$  satisfies the stronger of the two hypotheses, that is, strongly dominates  $M_0$ . If we raise both sides of the congruence  $u_0 M_0 \equiv -\sum_{1 \leq \gamma \leq g} u_\gamma M_\gamma \pmod{F}$  to the  $a$ th power, with  $a$  odd, we find the congruence  $u_0^a M_0^a \equiv -\sum u_{\gamma_1} \dots u_{\gamma_a} M_{\gamma_1} \dots M_{\gamma_a} \pmod{F}$ . By Lemma 4 we may choose  $a$  so that each  $M_{\gamma_1} \dots M_{\gamma_a}$  strongly dominates  $M_0^a$  factorially. Then the differential polynomial  $G = u_0^a M_0^a + \sum u_{\gamma_1} \dots u_{\gamma_a} M_{\gamma_1} \dots M_{\gamma_a}$  is in  $(F)$  and satisfies the stronger of the two conclusions.

Now assume merely that  $M_\gamma$  dominates  $M_0$  ( $1 \leq \gamma \leq g$ ). Let  $\Gamma_0$  denote the set of indices  $\gamma$  with  $\gamma \neq 0$  such that  $M_\gamma$  dominates  $M_0$  factorially. For each index  $\gamma$  with  $\gamma \neq 0$  and  $\gamma \notin \Gamma_0$  the weakness of  $M_\gamma$  over  $M_0$  is a subset of the set of prime factors of  $M_0$ . Denote the distinct weaknesses of the various  $M_\gamma$  with  $\gamma \neq 0$  and  $\gamma \notin \Gamma_0$  by  $W_1, \dots, W_k$ , and for each  $\kappa \in \mathbb{N}$  with  $1 \leq \kappa \leq k$  let  $\Gamma_\kappa$  denote the set of indices  $\gamma$  with  $\gamma \neq 0$  and  $\gamma \notin \Gamma_0$  such that the weakness of  $M_\gamma$  over  $M_0$  is  $W_\kappa$ . Then

$$F = u_0 M_0 + \sum_{0 \leq \kappa \leq k} \sum_{\gamma \in \Gamma_\kappa} u_\gamma M_\gamma.$$

Set  $\pi = \text{Card} \left( \bigcup_{1 \leq \kappa \leq k} \mathfrak{P}(W_\kappa) \right)$ , where, for any set  $S$ ,  $\mathfrak{P}(S)$  denotes the set of all subsets of  $S$ .

If  $\pi = 0$ , then  $k = 0$  and we may take  $G = F$ .

Let  $\pi > 0$  and suppose the result proved for lower values of  $\pi$ . Then  $k > 0$ . We may choose the notation so that  $W_\kappa$  is not a subset of any  $W_\kappa$  with  $\kappa \neq k$ . Let  $h \in \mathbb{N}$  be odd. Raising to the  $h$ th power both sides of the congruence  $u_0 M_0 + \sum_{\gamma \in \Gamma_0} u_\gamma M_\gamma \equiv -\sum_{1 \leq \kappa \leq k} \sum_{\gamma \in \Gamma_\kappa} u_\gamma M_\gamma \pmod{F}$ , we obtain on the left  $u_0^h M_0^h$  plus a number of terms  $UN$  with  $U$  a monomial in  $(u_0, (u_\gamma)_{\gamma \in \Gamma_0})$  different from  $u_0^h$  of degree  $h$  and with  $N$  a differential monomial in  $(z_1, \dots, z_r)$  different from  $M_0^h$  which dominates  $M_0^h$  factorially. On the right we obtain a sum of terms  $-UN = -u_{\gamma_1} \dots u_{\gamma_h} M_{\gamma_1} \dots M_{\gamma_h}$ . For any such term either some index  $\gamma_i$  is in a  $\Gamma_\kappa$  with  $1 \leq \kappa < k$  or  $\gamma_i \in \Gamma_k$  ( $1 \leq i \leq h$ ). In the former case the weakness of  $N$  over  $M_0^h$  is a subset of  $W_\kappa$  for some  $\kappa$  with  $1 \leq \kappa < k$ . In the latter case we may write  $M_{\gamma_i} = M'_{\gamma_i} M_{\gamma_i, W_\kappa} = M'_{\gamma_i} M_{0, W_\kappa}$  ( $1 \leq i \leq h$ ) and  $M_0 = M'_0 M_{0, W_\kappa}$ , and each  $M'_{\gamma_i}$  strongly dominates  $M'_0$ . By Lemma 4 then we may choose  $h$  so that  $M'_{\gamma_1} \dots M'_{\gamma_h}$  strongly dominates  $M_0^h$  factorially, in which case  $N = M_{\gamma_1} \dots M_{\gamma_h} = M'_{\gamma_1} \dots M'_{\gamma_h} M_{0, W_\kappa}^h$  dominates  $M_0^h = M_0^h M_{0, W_\kappa}^h$  factorially. Transposing to the left side all the terms on the right, we obtain on the left a differential polynomial

$$F^* = U_0^* M_0^* + \sum_{0 \leq \kappa \leq k^*} \sum_{\gamma \in \Gamma_\kappa^*} U_\gamma^* M_\gamma^* \in (F),$$

where  $\Gamma_0^*, \Gamma_1^*, \dots, \Gamma_{k^*}^*$  are disjoint finite sets not containing 0,  $U_0^* = u_0^{*h}$ , each  $U_\gamma^*$  with  $\gamma \neq 0$  is a monomial in  $(u_0, u_1, \dots, u_g)$  different from  $u_0^{*h}$  of degree  $h$ ,  $M_0^* = M_0^{*h}$ , every  $M_\gamma^*$  with  $\gamma \in \Gamma_0^*$  is a differential monomial in  $(z_1, \dots, z_r)$  other than  $M_0^{*h}$  that dominates  $M_0^{*h}$  factorially, for each index  $\kappa$  with  $1 \leq \kappa \leq k^*$  all the  $M_\gamma^*$  with  $\gamma \in \Gamma_\kappa^*$  are differential monomials in  $(z_1, \dots, z_r)$  other than  $M_0^{*h}$  that dominate  $M_0^{*h}$  and have over  $M_0^{*h}$  one and the same weakness  $W_\kappa^*$ , and each of these weaknesses  $W_1^*, \dots, W_{k^*}^*$  is a subset of some  $W_\kappa$  with  $1 \leq \kappa < k$ . It follows from the last remark that the number  $\pi^* = \text{Card} \left( \bigcup_{1 \leq \kappa \leq k^*} \mathfrak{P}(W_\kappa^*) \right)$  has the property that  $\pi^* < \pi$ . Therefore we may apply the lemma to  $F^*$ , and the existence of a differential polynomial  $G \in (F)$  with the required properties quickly follows. This completes the proof of Lemma 5.

We now come to the main point of this section, namely, the following domination lemma that considerably generalizes the case  $r = 1$  of Levi's lemma. The notation is the same as in Lemma 5.

**Lemma 6** Let  $F = \sum_{0 \leq \gamma \leq g} u_\gamma M_\gamma \in \mathbb{Q}\langle z_1, \dots, z_r, u_0, u_1, \dots, u_g \rangle$ , where  $M_0, M_1, \dots, M_g$  are differential monomials in  $(z_1, \dots, z_r)$  with  $M_0 \neq 1$  and  $M_\gamma \neq M_0$  ( $1 \leq \gamma \leq g$ ). If each  $M_\gamma$  with  $\gamma \neq 0$  dominates (respectively strongly



dominates)  $M_0$ , then there exist a nonzero  $e \in \mathbb{N}$ , and a differential polynomial  $Z \in \mathbb{Q}\{z_1, \dots, z_r, u_0, u_1, \dots, u_g\}$  with  $Z \in [z_1, \dots, z_r]$  (respectively with  $Z \in \{M_0\}$ ) and with  $Z$  homogeneous in  $(\theta u_\gamma)_{\theta \in \Theta, 0 \leq \gamma \leq g}$  of degree  $e$  and with the degree of  $Z$  in  $(\theta u_0)_{\theta \in \Theta}$  strictly smaller than  $e$ , such that

$$M_0(u_0^e + Z) \in \{F\}.$$

*Proof* Write  $M_0 = v_1^{q_1} \dots v_t^{q_t}$  where  $v_1, \dots, v_t$  are the distinct prime factors of  $M_0$ . Suppose first that  $t = 1$ . For each index  $\gamma$  with  $\gamma \neq 0$ , either  $M_\gamma$  is divisible by  $v_1^{q_1}$  or else  $M_\gamma$  strongly dominates  $v_1^{q_1}$ . Therefore, we may write

$$F = \left( u_0 + \sum_{\gamma \in \Gamma'} u_\gamma L_\gamma \right) v_1^{q_1} + \sum_{\gamma \in \Gamma''} u_\gamma L_\gamma N_\gamma (v_1),$$

where  $\Gamma', \Gamma''$  are disjoint sets whose union is the set of indices  $1, 2, \dots, g$  ( $\Gamma'$  being empty if each  $M_\gamma$  with  $\gamma \neq 0$  strongly dominates  $M_0$ ), each  $L_\gamma$  is a differential monomial in  $(z_1, \dots, z_r)$ ,  $\deg L_\gamma > 0$  ( $\gamma \in \Gamma'$ ), and each  $N_\gamma$  with  $\gamma \in \Gamma''$  is a differential monomial (in some new differential indeterminate  $z'$ ) of degree greater than  $q_1$ . We may apply Section 11, Lemma 3 (case  $r = 1$ ) to the differential polynomial  $F' = u_0' z' + \sum_{\gamma \in \Gamma'} u_\gamma' N_\gamma$  ( $u_0'$  and  $u_\gamma'$  ( $\gamma \in \Gamma''$ ) here denoting additional differential indeterminates) to prove the existence of a differential polynomial  $Z' (u_0^e + Z') \in \{F'\}$  with  $Z' \in [z']$  and with  $Z'$  homogeneous in  $((\theta u_0')_{\theta \in \Theta}, (\theta u_\gamma')_{\theta \in \Theta, \gamma \in \Gamma''})$  of degree  $e$  and with the degree of  $Z'$  in  $(\theta u_0')_{\theta \in \Theta}$  strictly smaller than  $e$ . Since substitution of  $(v_1, u_0 + \sum_{\gamma \in \Gamma'} u_\gamma L_\gamma, (u_\gamma L_\gamma)_{\gamma \in \Gamma''})$  for  $(z', u_0', (u_\gamma')_{\gamma \in \Gamma''})$  maps  $F'$  onto  $F$ , the desired result follows.

Now let  $t > 1$ , and suppose the lemma proved for lower values of  $t$ . By Lemma 5, the ideal  $(F)$  contains a differential polynomial

$$G = u_0^a v_1^{q_1 a} v_2^{q_2 a} \dots v_t^{q_t a} + \sum_{1 \leq \beta \leq b} U_\beta N_\beta N_{\beta'},$$

where each  $U_\beta$  is a monomial in  $(u_0, u_1, \dots, u_g)$  other than  $u_0^a$  of degree  $a$ , each  $N_\beta$  is a differential monomial in  $(z_1, \dots, z_r)$  that dominates (respectively strongly dominates)  $v_1^{q_1 a}$ , each  $N_{\beta'}$  is a differential monomial in  $(z_1, \dots, z_r)$ , that dominates (respectively strongly dominates)  $v_2^{q_2 a} \dots v_t^{q_t a}$ , and  $N_\beta N_{\beta'} \neq M_0^a$ . We observe that if  $N_{\beta_1}$  and  $N_{\beta_2}$  both equal  $v_2^{q_2 a} \dots v_t^{q_t a}$ , then  $N_{\beta_1}$  and  $N_{\beta_2}$  both differ from  $v_1^{q_1 a}$ , and therefore both have degree greater than or equal to  $q_2 a + 1$  in  $(\theta v_1)_{\theta \in \Theta}$ . Then  $N_{\beta_1} N_{\beta_2}$  can be written in the form  $N \theta v_1$ , where  $N$  dominates  $v_1^{2q_1 a}$ , so that  $N_{\beta_1} N_{\beta_1} \cdot N_{\beta_2} N_{\beta_2}$  can be written in the form  $NN'$  where  $N'$  dominates  $v_2^{2q_2 a} \dots v_t^{2q_t a}$  and is distinct from it. Since we may evidently replace  $G$  by  $(u_0^a M_0^a)^3 + (\sum_{1 \leq \beta \leq b} U_\beta N_\beta N_{\beta'})^3$ , it follows that we may suppose that  $N_{\beta'} \neq v_2^{q_2 a} \dots v_t^{q_t a}$  ( $1 \leq \beta \leq b$ ).

Then we may apply our lemma (case  $t-1$ ) to the differential polynomial  $F' = u_0' v_2^{q_2 a} \dots v_t^{q_t a} + \sum_{1 \leq \beta \leq b} u_\beta' N_{\beta'}$  in  $\mathbb{Q}\{z_1, \dots, z_r, u_0', u_1', \dots, u_b'\}$ , to prove

the existence of a nonzero  $e' \in \mathbb{N}$  and a  $Z' \in \mathbb{Q}\{z_1, \dots, z_r, u_0', u_1', \dots, u_b'\}$  with  $Z' \in [z_1, \dots, z_r]$  (respectively with  $Z' \in \{v_2 \dots v_t\}$ ) and with  $Z'$  homogeneous in  $(\theta u_\beta')_{\theta \in \Theta, 0 \leq \beta \leq b}$  of degree  $e'$  and with the degree of  $Z'$  in  $(\theta u_0')_{\theta \in \Theta}$  strictly smaller than  $e'$ , such that  $v_2 \dots v_t (u_0^{e'} + Z') \in \{F'\}$ . Substituting  $(u_0^a v_1^{q_1 a}, U_1 N_1, \dots, U_b N_b)$  for  $(u_0', u_1', \dots, u_b')$ , we find that  $\{F\}$  contains a differential polynomial  $v_2 \dots v_t (u_0^a v_1^{q_1 a} + \sum_{\lambda \in \Lambda_1} U_{1\lambda} M_{1\lambda})$ , where  $a_1$  and  $c_1$  are nonzero natural numbers, each  $U_{1\lambda}$  is the product of a rational number with a differential monomial in  $(u_0, u_1, \dots, u_g)$  of degree  $a_1$  having degree less than  $a_1$  in  $(\theta u_0)_{\theta \in \Theta}$ , and each  $M_{1\lambda}$  is a differential monomial in  $(z_1, \dots, z_r)$  different from  $v_1^{c_1}$  that dominates (respectively strongly dominates)  $v_1^{c_1}$ . Let  $\Lambda_1'$  denote the set of indices  $\lambda \in \Lambda_1$  such that  $M_{1\lambda}$  strongly dominates  $v_1^{c_1}$ , and set  $\Lambda_1'' = \Lambda_1 - \Lambda_1'$  (so that under the strong hypothesis, namely that each  $M_\gamma$  with  $\gamma \neq 0$  strongly dominate  $M_0$ ,  $\Lambda_1' = \emptyset$ ). For each  $\lambda \in \Lambda_1''$  we may write  $M_{1\lambda} = L_{1\lambda} v_1^{c_1}$  with  $L_{1\lambda}$  a differential monomial in  $(z_1, \dots, z_r)$  of degree greater than 0. Thus,  $\{F\}: M_0$  contains  $(u_0^a + \sum_{\lambda \in \Lambda_1'} U_{1\lambda} L_{1\lambda}) v_1^{c_1} + \sum_{\lambda \in \Lambda_1''} U_{1\lambda} M_{1\lambda}$ . Similarly, for each  $\tau \in \mathbb{N}$  with  $1 \leq \tau \leq t$ ,  $\{F\}: M_0$  contains a differential polynomial

$$\left( u_0^a + \sum_{\lambda \in \Lambda_\tau'} U_{\tau\lambda} L_{\tau\lambda} \right) v_\tau^{c_\tau} + \sum_{\lambda \in \Lambda_\tau''} U_{\tau\lambda} M_{\tau\lambda}$$

with entirely analogous properties. An easy application of Section 11, Lemma 3 (case  $r = t$ ) now completes the proof.

### 13 Preparations

Let  $\mathfrak{p}$  be a prime differential ideal of  $\mathcal{F}\{y_1, \dots, y_n\}$ . Fix a ranking of  $(y_1, \dots, y_n)$ , let  $A$  be a characteristic set of  $\mathfrak{p}$ , and denote the elements of  $A$  by  $A_1, \dots, A_r$ . For each element  $v \in \bigcup_{1 \leq k \leq r} \Theta u_{A_k}$  there exist a  $\theta \in \Theta$  and a  $k \in \mathbb{N}$  with  $1 \leq k \leq r$  such that  $v = \theta u_{A_k}$ , but the pair  $(\theta, k)$  need not be unique. We may, of course, choose for each  $v$  a particular pair  $(\theta_v, k(v))$  with  $v = \theta_v u_{A_{k(v)}}$ . We shall call the resulting function  $v \mapsto (\theta_v, k(v))$  a *choice function* for the characteristic set  $A_1, \dots, A_r$ .

Let there be given such a choice function  $v \mapsto (\theta_v, k(v))$ , and consider any differential polynomial  $F \in \mathcal{F}\{y_1, \dots, y_n\}$ . By a *preparation equation* of  $F$  with respect to  $A_1, \dots, A_r$  we shall mean an equation

$$HF = \sum_{0 \leq \gamma \leq g} C_\gamma M_\gamma(A_1, \dots, A_r),$$

where  $H, C_0, \dots, C_g$  are elements of  $\mathcal{F}\{y_1, \dots, y_n\}$  not contained in  $\mathfrak{p}$ , and  $M_0, \dots, M_g$  are distinct differential monomials in  $(z_1, \dots, z_r)$  every prime factor of which is of the form  $\theta_v z_{k(v)}$ . This notion depends not only on  $F$  and on  $A_1, \dots, A_r$  but also on the ranking and the choice function. It is an

easy consequence of Chapter I, Section 9, Lemma 7, that a preparation equation always exists.

Suppose  $F \neq 0$ , and set  $q = \min_{0 \leq \gamma \leq g} \deg M_\gamma$ . If we denote the differential monomials  $M_\gamma$  of degree  $q$  by  $N_1, \dots, N_l$ , then the preparation equation yields a congruence

$$HF \equiv \sum_{1 \leq \lambda \leq l} D_\lambda N_\lambda(A_1, \dots, A_r) \pmod{[A_1, \dots, A_r]^{q+1}},$$

where  $l \in \mathbb{N}$ ,  $l \neq 0$ ,  $H, D_1, \dots, D_l$  are elements of  $\mathcal{F}\{y_1, \dots, y_n\}$  not contained in  $\mathfrak{p}$ , and  $N_1, \dots, N_l$  are distinct differential monomials in  $(z_1, \dots, z_r)$  of degree  $q$  all the prime factors of which are of the form  $\theta_v z_{k(v)}$ . We shall call any such congruence a preparation congruence of  $F$  with respect to  $A_1, \dots, A_r$ . This notion, too, depends on  $F$ , on  $A_1, \dots, A_r$ , on the ranking, and on the choice function. Moreover, given these, the preparation congruence is in general not unique. However, the set of differential monomials  $N_1, \dots, N_l$  is unique. This is an almost immediate consequence of the following lemma due to Hillman.

**Lemma 7** *If  $A_1, \dots, A_r$  are the elements of a characteristic set of a prime differential ideal  $\mathfrak{p}$  of  $\mathcal{F}\{y_1, \dots, y_n\}$ , and  $N_1, \dots, N_l$  are  $l (\neq 0)$  distinct differential monomials in  $(z_1, \dots, z_r)$  of the same degree  $q$  having the property that whenever  $\theta z_k, \theta' z_{k'}$  are distinct prime factors of  $N_1 \cdots N_l$ , then  $\theta u_{A_k} \neq \theta' u_{A_{k'}}$ , and  $D_1, \dots, D_l$  are elements of  $\mathcal{F}\{y_1, \dots, y_n\}$  such that  $\sum D_\lambda N_\lambda(A_1, \dots, A_r) \equiv 0 \pmod{[A_1, \dots, A_r]^{q+1}}$ , then  $D_\lambda \in \mathfrak{p}$  ( $1 \leq \lambda \leq l$ ).*

*Proof* Let  $\eta = (\eta_1, \dots, \eta_n)$  be a generic zero of  $\mathfrak{p}$ . For each  $G \in \mathcal{F}\{y_1, \dots, y_n\}$  let  $G'$  denote the sum of the nonzero terms of  $G(\eta_1 + y_1, \dots, \eta_n + y_n)$  of lowest degree. Since  $\partial A_k / \partial u_{A_k} = S_{A_k} \notin \mathfrak{p}$ ,  $A_k'$  has degree 1 and leader  $u_{A_k}$ . It follows that, for every  $\theta \in \Theta$ ,  $\theta A_k' (= (\theta A_k)')$  has degree 1 and leader  $\theta u_{A_k}$ . Hence, if  $\theta_1 z_{k(1)}, \dots, \theta_s z_{k(s)}$  are the distinct prime factors of  $N_1 \cdots N_l$ , then  $\theta_1 A_{k(1)}', \dots, \theta_s A_{k(s)}'$  are algebraically independent over  $\mathcal{U}$ . Substituting  $(\eta_1 + y_1, \dots, \eta_n + y_n)$  for  $(y_1, \dots, y_n)$  in the congruence of the lemma, and then looking at the terms of degree  $q$ , we find the equation

$$\sum_{1 \leq \lambda \leq l} D_\lambda(\eta) N_\lambda(A_1', \dots, A_r') = 0.$$

Therefore  $D_\lambda(\eta) = 0$ , whence  $D_\lambda \in \mathfrak{p}$  ( $1 \leq \lambda \leq l$ ).

The same substitution applied to the above preparation congruence of  $F$  with respect to  $A_1, \dots, A_r$  shows that  $q = \deg F'$  is the multiplicity of  $F$  at  $\eta$ , and that

$$H(\eta) F' = \sum_{1 \leq \lambda \leq l} D_\lambda(\eta) N_\lambda(A_1', \dots, A_r').$$

In particular,  $q$  depends only on  $F$  and  $\mathfrak{p}$ , being independent of the preparation congruence, the choice function, the characteristic set, and the ranking. Also, if  $q \neq 0$ , then the highest derivative  $v = \theta u_{A_k}$  such that  $\theta z_k$  divides  $N_1 \cdots N_l$  is the leader of  $F'$ . Thus,  $v$  depends only on  $F, \mathfrak{p}$ , and the ranking, being independent of the preparation congruence, the choice function, and the characteristic set.

The case  $r = 1$  deserves special mention. In this case if we take  $A_1$  irreducible, then  $\mathfrak{p} = \mathfrak{p}_{\mathcal{F}}(A_1)$  and  $A_1$  constitutes a characteristic set of  $\mathfrak{p}$  relative to every ranking of  $(y_1, \dots, y_n)$ . Furthermore, for distinct derivative operators  $\theta_1, \theta_2$  the derivatives  $\theta_1 u_{A_1}, \theta_2 u_{A_1}$  are distinct, so that the question of choice function does not arise (there being only one).

### 14 The component theorem

We saw in Section 5 that if an irreducible differential polynomial  $A \in \mathcal{F}\{y_1, \dots, y_n\}$  is pseudo-led (which, under the present circumstance  $p = 0$ , is always the case), then the set of components of  $\{A\} = \{A\}_{\mathcal{F}}$  consists of the general component  $\mathfrak{p}_{\mathcal{F}}(A)$  and a certain number (perhaps zero) of singular components. The following theorem shows that each singular component is the general component of some other irreducible differential polynomial in  $\mathcal{F}\{y_1, \dots, y_n\}$ .

**Theorem 5** *Let  $\mathcal{F}$  be a differential subfield of  $\mathcal{U}$  and let  $F$  be a nonzero differential polynomial in  $\mathcal{F}\{y_1, \dots, y_n\}$ . If  $\mathfrak{p}$  is any component of  $\{F\}$  in  $\mathcal{F}\{y_1, \dots, y_n\}$ , then there exists an irreducible differential polynomial  $B \in \mathcal{F}\{y_1, \dots, y_n\}$  such that  $\mathfrak{p} = \mathfrak{p}_{\mathcal{F}}(B)$ .*

*Proof* Let  $B_1, \dots, B_r$  be the elements of a characteristic set of  $\mathfrak{p}$  relative to some ranking of  $(y_1, \dots, y_n)$ , so that  $\mathfrak{p} = \{B_1, \dots, B_r\} : I_{B_1} S_{B_1} \cdots I_{B_r} S_{B_r}$ . We may suppose the notation chosen so that  $u_{B_1} < \cdots < u_{B_r}$ , and we may take  $B_1$  irreducible. Let

$$HF \equiv \sum_{1 \leq \lambda \leq l} D_\lambda N_\lambda(B_1, \dots, B_r) \pmod{[B_1, \dots, B_r]^{q+1}}$$

be a preparation congruence of  $F$  with respect to  $B_1, \dots, B_r$ . Let  $\eta = (\eta_1, \dots, \eta_n)$  be a generic zero of  $\mathfrak{p}$ , and for each nonzero differential polynomial  $P \in \mathcal{F}\{y_1, \dots, y_n\}$  let  $P'$  denote the sum of the nonzero terms of lowest degree of  $P(\eta_1 + y_1, \dots, \eta_n + y_n)$ . Then (see Section 13)  $\deg F' = q$ , so that  $q > 0$  (since  $F(\eta) = 0$ ), and  $u_{F'}$  is the highest derivative  $\theta u_{B_k}$  such that  $\theta z_k$  is present in  $N_1 \cdots N_l$ . Therefore  $u_{B_1} \leq u_{F'}$ . Letting  $G$  denote an irreducible factor of  $F'$  in  $\mathcal{F}\langle \eta \rangle\{y_1, \dots, y_n\}$  with leader  $u_{F'}$ , we see that  $B_1'$  is partially reduced with respect to  $G$ .

There exists an  $E \in \mathcal{F}\{y_1, \dots, y_n\}$  with  $E \notin \mathfrak{p}$  that is contained in every component of  $\{F\}$  in  $\mathcal{F}\{y_1, \dots, y_n\}$  other than  $\mathfrak{p}$ . For each  $k$ ,  $EB_k \in \{F\}$  so that  $E(\eta_1 + y_1, \dots, \eta_n + y_n)B_k(\eta_1 + y_1, \dots, \eta_n + y_n) \in \{F(\eta_1 + y_1, \dots, \eta_n + y_n)\}$  in  $\mathcal{F}\langle \eta \rangle\{y_1, \dots, y_n\}$ . We conclude from Section 10, Corollary 3 to Theorem 4 that  $E(\eta)B_k' = (EB_k)' \in \{F'\}$ , whence  $B_k' \in \{G\}$ . Since  $B_1'$  is partially reduced with respect to  $G$  this implies (by Section 6, Theorem 3(b)) that  $B_1'$  is divisible by  $G$ . Because  $\deg B_1' = 1$  this means that  $B_1' = \varphi G$  for some nonzero  $\varphi \in \mathcal{F}\langle \eta \rangle$ . If  $r$  were greater than 1, then  $B_2'$  would be a nonzero element of  $\{B_1'\}$  reduced with respect to  $B_1'$ . Therefore  $r = 1$  so that  $\mathfrak{p} = \{B_1\} : I_{B_1}, S_{B_1} = \mathfrak{p}_{\mathcal{F}}(B_1) : I_{B_1} = \mathfrak{p}_{\mathcal{F}}(B_1)$ .

**Corollary** Let  $\mathfrak{p}$  be a singular component of an irreducible differential polynomial  $A \in \mathcal{F}\{y_1, \dots, y_n\}$ . Then  $\mathfrak{p} = \mathfrak{p}_{\mathcal{F}}(B)$  for an irreducible differential polynomial  $B \in \mathcal{F}\{y_1, \dots, y_n\}$ ,  $A$  involves a proper derivative of the leader  $u_B$  relative to any ranking, and  $\text{ord } B < \text{ord } A$ .

*Proof* The first assertion is the essential content of Theorem 5. We know  $A$  is not divisible by  $B$ , for otherwise  $\mathfrak{p}$  would be  $\mathfrak{p}_{\mathcal{F}}(A)$ . Therefore by Section 6, Theorem 3(b),  $A$  is not partially reduced with respect to  $B$ ; that is, the second assertion is correct. Since we can use an orderly ranking, this implies the final assertion.

EXERCISES

- Let  $A \in \mathcal{F}\{y_1, \dots, y_n\}$  be irreducible and of order 0. Show that  $\{A\}$  is prime. (This result is false when  $p \neq 0$ ; see Section 6, Exercise 3(d). For a considerable generalization, see Section 17, Proposition 10.)
- Show that Theorem 5 is false when  $\mathcal{F}$  has nonzero characteristic. (See Section 6, Exercise 3(c) and (d).)
- (a) Let  $B \in \mathcal{F}\{y_1, \dots, y_n\}$  be of order  $b$ ,  $B \notin \mathcal{F}$ , and let  $B_0$  be an irreducible factor of  $B$  of order  $b$ . Show that  $\delta_1 B$  has a unique irreducible factor  $B_1$  of order  $b+1$  and that  $\mathfrak{p}_{\mathcal{F}}(B_0) \supset \mathfrak{p}_{\mathcal{F}}(B_1)$ . (Hint: Show that  $\mathfrak{p}_{\mathcal{F}}(B_0)$  is a component of  $\{B\}$ , and by Section 10, Exercise 3(b), deduce that  $\mathfrak{p}_{\mathcal{F}}(B_0)$  properly contains a component  $\mathfrak{p}$  of  $\{\delta_1 B\}$ . Show that  $\mathfrak{p}$  is a component of an irreducible factor  $B_1$  of  $\delta_1 B$ , and by the corollary to Theorem 5 deduce that  $\mathfrak{p} = \mathfrak{p}_{\mathcal{F}}(C)$ , where either  $C = B_1$  or  $\text{ord } C < \text{ord } B_1$ . Show that  $\text{ord } B_1 \leq b+1$ , and by Section 7, Proposition 4 and Chapter III, Section 5, Proposition 2 that  $\text{ord } C > b$ , and conclude that  $C = B_1$  and  $\text{ord } B_1 = b+1$ .)  
 (b) (Hillman [19, Section 13]) Let  $A_k \in \mathcal{F}\{y_1, \dots, y_n\}$  be irreducible and of order  $e_k$  ( $1 \leq k \leq r$ ), and set  $e = \max(e_1, \dots, e_r)$ . Show that  $\delta_1(\prod_{1 \leq k \leq r} \delta_1^{-e_k} A_k)$  has a unique irreducible factor  $A$  of order  $e+1$  and that  $\mathfrak{p}_{\mathcal{F}}(A) \subset \bigcap_{1 \leq k \leq r} \mathfrak{p}_{\mathcal{F}}(A_k)$ .

- Let  $F, G$  be nonzero elements of  $\mathcal{F}\{y_1, \dots, y_n\}$  without common divisor. Show that every singular component of  $zG - F$  in  $\mathcal{F}\{y_1, \dots, y_n, z\}$  is of the form  $\mathfrak{p}_{\mathcal{F}}(B)$ , with  $B \in \mathcal{F}\{y_1, \dots, y_n, z\}$  irreducible, differentially free of  $z$ , and of lower order than  $FG$ .

15 The low power theorem

We are now in a position to solve the following problem (in the statement of which  $\mathcal{F}$  is an arbitrary differential subfield of  $\mathcal{U}$ ): Given a differential polynomial  $F \in \mathcal{F}\{y_1, \dots, y_n\}$ , to determine the components of  $\{F\}$  in  $\mathcal{F}\{y_1, \dots, y_n\}$ .

We may suppose that  $F \notin \mathcal{F}$ . Fixing a ranking of  $(y_1, \dots, y_n)$ , we find, according to the methods of Section 9, a finite set  $\mathfrak{A}$  of autoreduced sets, each of which is a characteristic set of a prime differential ideal containing  $\{F\}$ , such that each component of  $\{F\}$  has a characteristic set that is an element of  $\mathfrak{A}$ . According to Section 14, Theorem 5, each component  $\mathfrak{p}$  of  $\{F\}$  is the general component  $\mathfrak{p}_{\mathcal{F}}(A)$  of some irreducible  $A \in \mathcal{F}\{y_1, \dots, y_n\}$ . It follows that if  $A \in \mathfrak{A}$  is a characteristic set of  $\mathfrak{p}$ , then  $A$  consists of a single element, that element being a multiple of  $A$  by a nonzero differential polynomial of lower rank than  $u_A$ . Thus, if we discard from  $\mathfrak{A}$  every autoreduced set containing more than one element, and replace each remaining autoreduced set  $A$  by the irreducible factor of its element that involves the leader of that element, we obtain a finite set of irreducible differential polynomials  $A_1, \dots, A_s \in \mathcal{F}\{y_1, \dots, y_n\}$  such that every component of  $\{F\}$  is  $\mathfrak{p}_{\mathcal{F}}(A_i)$  for some index  $i$ . It remains to find a criterion, given an arbitrary irreducible differential polynomial  $A \in \mathcal{F}\{y_1, \dots, y_n\}$ , for  $\mathfrak{p}_{\mathcal{F}}(A)$  to be a component of  $\{F\}$ . Such a criterion is provided by the low power theorem.

**Theorem 6** Let  $A$  and  $F$  be differential polynomials in  $\mathcal{F}\{y_1, \dots, y_n\}$ , with  $A$  irreducible and  $F \neq 0$ . Let

$$HF \equiv \sum_{1 \leq \lambda \leq l} D_{\lambda} N_{\lambda}(A) \pmod{[A]^{q+1}}$$

be a preparation congruence of  $F$  with respect to  $A$ . A necessary and sufficient condition that  $\mathfrak{p}_{\mathcal{F}}(A)$  be a component of  $\{F\}$  is that  $q \neq 0$ ,  $l = 1$ , and  $N_1 = z^q$ .

**REMARK 1** Thus (see Section 6, Exercise 2)  $[y]$  is a component of the ordinary differential polynomial  $y'^2 - 4y$ , but not of  $y'^2 - 4y^3$ .

**REMARK 2** For differential fields of nonzero characteristic the condition is neither necessary nor sufficient. (See Section 6, Exercise 3.)

Following Ritt, we obtain Theorem 6 as a special case of a theorem concerning the components of  $\{F\}$  contained in a given prime differential ideal. Because we use the domination lemma instead of Levi's lemma in proving the second half of the latter theorem, our version is considerably stronger than Ritt's. The weaker version is, of course, adequate for Theorem 6.

**Theorem 7** Let  $\mathfrak{p}$  be a prime differential ideal of  $\mathcal{F}\{y_1, \dots, y_n\}$ , let  $A_1, \dots, A_r$  be the elements of a characteristic set of  $\mathfrak{p}$  relative to some ranking of  $(y_1, \dots, y_n)$ , and let  $F \in \mathfrak{p}$ ,  $F \neq 0$ .

(a) Let  $HF \equiv \sum_{1 \leq \lambda \leq l} D_\lambda N_\lambda(A_1, \dots, A_r) \pmod{[A_1, \dots, A_r]^{q+1}}$  be a preparation congruence of  $F$  with respect to  $A_1, \dots, A_r$ . Let  $\theta z_k$  denote the prime factor of  $N_1 \cdots N_l$  for which the rank of  $\theta u_{A_k}$  is highest. Then  $\{F\}$  has a component  $\mathfrak{p}_{\mathcal{F}}(B) \subset \mathfrak{p}$  such that  $B$  involves a derivative of  $\theta u_{A_k}$ .

(b) Let  $HF = \sum_{0 \leq \gamma \leq g} C_\gamma M_\gamma(A_1, \dots, A_r)$  be a preparation equation of  $F$  with respect to  $A_1, \dots, A_r$ , and suppose, for each  $\gamma \neq 0$ , that  $M_\gamma$  dominates and is distinct from  $M_0$ . Let  $\theta_\lambda z_{k(\lambda)}$  ( $\lambda \in \Lambda$ ) denote the distinct prime factors of  $M_0$ , let  $\Lambda_1$  denote the set of all indices  $\kappa \in \Lambda$  such that no proper derivative of  $\theta_\kappa z_{k(\kappa)}$  is equal to any  $\theta_\lambda z_{k(\lambda)}$  ( $\lambda \in \Lambda$ ), and let  $\Lambda_0$  denote the set of all indices  $\kappa \in \Lambda$  such that no proper derivative of  $\theta_\kappa u_{A_{k(\kappa)}}$  is equal to any  $\theta_\lambda u_{A_{k(\lambda)}}$  ( $\lambda \in \Lambda$ ). Then every component of  $\{F\}$  contained in  $\mathfrak{p}$  is one of the ideals  $\{\theta_\kappa A_{k(\kappa)}\} : S_{A_{k(\kappa)}}$  with  $\kappa \in \Lambda_1$ , and every ideal  $\{\theta_\kappa A_{k(\kappa)}\} : S_{A_{k(\kappa)}}$  with  $\kappa \in \Lambda_0$  is a component of  $\{F\}$  contained in  $\mathfrak{p}$ .

REMARK 1 In part (b) obviously  $\Lambda_0 \subset \Lambda_1$ . The conclusion is strongest when  $\Lambda_0 = \Lambda_1$ . This certainly happens when either  $r = 1$  or  $m = 1$ .

REMARK 2 The necessity of the condition in the Low power theorem is a special case of part (a), and the sufficiency a special case of part (b). Indeed, if the condition is not satisfied, then the prime factor  $\theta z$  of  $N_1 \cdots N_l$  for which the rank of  $\theta u_A$  is highest has order greater than 0, so that by Theorem 7(a), there exists an irreducible  $B$  with  $u_B > u_A$  such that  $\{F\} \subset \mathfrak{p}_{\mathcal{F}}(B) \subset \mathfrak{p}_{\mathcal{F}}(A)$ . By Section 6, Theorem 3(b),  $A \notin \mathfrak{p}_{\mathcal{F}}(B)$  so that the inclusion  $\mathfrak{p}_{\mathcal{F}}(B) \subset \mathfrak{p}_{\mathcal{F}}(A)$  is strict and hence  $\mathfrak{p}_{\mathcal{F}}(A)$  is not a component of  $\{F\}$ . On the other hand, if the condition is satisfied, then by Theorem 7(b),  $\{A\} : S_A$  is the unique component of  $\{F\}$  contained in  $\mathfrak{p}_{\mathcal{F}}(A)$ , that is  $\mathfrak{p}_{\mathcal{F}}(A)$  is a component of  $\{F\}$ .

*Proof of Theorem 7* (a) By Section 14, Theorem 5, the components of  $\{F\}$  contained in  $\mathfrak{p}$  can be written as  $\mathfrak{p}_{\mathcal{F}}(B_1), \dots, \mathfrak{p}_{\mathcal{F}}(B_s)$ . There evidently exists a  $B_0 \notin \mathfrak{p}$  contained in all the other components of  $\{F\}$ , and  $\prod_{0 \leq i \leq s} B_i \in \{F\}$ . Let  $\eta = (\eta_1, \dots, \eta_n)$  be a generic zero of  $\mathfrak{p}$  (if  $\mathcal{U}$  is not semiuniversal over  $\mathcal{F}$ , we first replace  $\mathcal{F}$  by a suitable smaller differential field). For each  $P \in \mathcal{F}\{y_1, \dots, y_n\}$  let  $P'$  denote the sum of the nonzero terms of the lowest

degree in  $P(\eta_1 + y_1, \dots, \eta_n + y_n)$ . Clearly,  $\prod_{0 \leq i \leq s} B_i(\eta_1 + y_1, \dots, \eta_n + y_n) \in \{F(\eta_1 + y_1, \dots, \eta_n + y_n)\}$  in  $\mathcal{F}\langle \eta \rangle \{y_1, \dots, y_n\}$ , whence, by Section 10, Corollary 3 of Theorem 4,  $\prod_{0 \leq i \leq s} B_i' \in \{F'\}$ . Since  $F(\eta) = 0$ , the degree of  $F'$  is not 0 and therefore (by Section 13)  $F'$  has as leader the highest  $\theta u_{A_k}$  for which  $\theta z_k$  is a prime factor of  $N_1 \cdots N_l$ . Letting  $G$  be an irreducible factor of  $F'$  in  $\mathcal{F}\langle \eta \rangle \{y_1, \dots, y_n\}$  with  $u_G = u_{F'}$ , we see that  $\prod_{0 \leq i \leq s} B_i' \in \mathfrak{p}_{\mathcal{F}\langle \eta \rangle}(G)$ , so that  $B_i' \in \mathfrak{p}_{\mathcal{F}\langle \eta \rangle}(G)$  for some  $i$ . Since  $B_0' = B_0(\eta) \neq 0$ , this  $i$  is not 0 so that  $\mathfrak{p}_{\mathcal{F}}(B_i)$  is a component of  $\{F\}$  contained in  $\mathfrak{p}$ . By Section 6, Theorem 3(b),  $B_i'$  is not reduced with respect to  $G$ , so that  $B_i'$  involves a derivative of  $u_G = u_{F'} = \theta u_{A_k}$ , whence  $B_i(\eta_1 + y_1, \dots, \eta_n + y_n)$  does, also, and so too does  $B_i$ .

(b) Any  $\theta A_k$  has only one irreducible factor with leader  $\theta u_{A_k}$ . If we denote this factor by  $A$  and write  $\theta A_k = AE$ , then  $S_{A_k} = S_{\theta A_k} = S_A E$ , so that  $\{\theta A_k\} : S_{A_k} = \{A\} : S_A = \mathfrak{p}_{\mathcal{F}}(A)$ . This shows that  $\{\theta A_k\} : S_{A_k}$  is prime. It obviously is contained in  $\mathfrak{p}$ . We claim that if  $\{\theta' A_{k'}\} : S_{A_{k'}} \subset \{\theta A_k\} : S_{A_k}$  for some  $(\theta', k') \neq (\theta, k)$ , then  $\theta' u_{A_{k'}}$  is a derivative of  $\theta u_{A_k}$ . Indeed, by Section 6, Theorem 3(b),  $\theta' A_{k'}$  is not reduced with respect to  $A$ , but  $A_{k'}$  is reduced with respect to  $A$  (because it is reduced with respect to  $\theta A_k$ ). This implies that  $\theta' \neq 1$ , so that  $\theta' A_{k'} = S_{A_{k'}} \theta' u_{A_{k'}} + T$ , where  $S_{A_{k'}}$  and  $T$  are lower than  $\theta' u_{A_{k'}}$ . By Chapter I, Section 9, Proposition 2, we may write

$$I_A^j S_A^i S_{A_{k'}} \equiv S', \quad I^j S^i T \equiv T' \pmod{[A]}$$

with  $S', T'$  reduced with respect to  $A$  and free of  $\theta' u_{A_{k'}}$ , and (because  $S_{A_{k'}} \notin \mathfrak{p}_{\mathcal{F}}(A) \subset \mathfrak{p}$ ) with  $S' \neq 0$ , and evidently  $S' \theta' u_{A_{k'}} + T' \in \mathfrak{p}_{\mathcal{F}}(A)$ . This differential polynomial is not reduced with respect to  $A$ , and therefore  $\theta' u_{A_{k'}}$  is a derivative of  $u_A = \theta u_{A_k}$  as claimed. This being the case, consider any component  $\mathfrak{q}$  of  $\{F\}$  with  $\mathfrak{q} \subset \mathfrak{p}$ . By the domination lemma there exists an  $e \in \mathbb{N}$  and a  $Z \in \mathbb{Q}\{z_1, \dots, z_r, u_0, u_1, \dots, u_g\}$  with  $Z \in [z_1, \dots, z_r]$  such that  $M_0 \cdot (u_0^e + Z) \in \{\sum_{0 \leq \gamma \leq g} u_\gamma M_\gamma\}$ . Substituting  $(A_1, \dots, A_r, C_0, \dots, C_g)$  for  $(z_1, \dots, z_r, u_0, \dots, u_g)$  we find a relation

$$M_0(A_1, \dots, A_r) \cdot (C_0^e + P) \in \mathfrak{q},$$

where  $P = Z(A_1, \dots, A_r, C_0, \dots, C_g) \in \mathfrak{p}$ . As  $C_0^e + P \notin \mathfrak{p}$ , and hence  $C_0^e + P \notin \mathfrak{q}$ , we infer that  $M_0(A_1, \dots, A_r) \in \mathfrak{q}$ . It follows that  $\theta_\lambda A_{k(\lambda)} \in \mathfrak{q}$  for some  $\lambda \in \Lambda$ , and therefore that  $\theta_\kappa A_{k(\kappa)} \in \mathfrak{q}$  for some  $\kappa \in \Lambda_1$ , so that  $\{\theta_\kappa A_{k(\kappa)}\} : S_{A_{k(\kappa)}} \subset \mathfrak{q}$ . Since  $HF = \sum C_\gamma M_\gamma(A_1, \dots, A_r)$  and each  $M_\gamma$  dominates  $M_0$ , and  $H \notin \mathfrak{q}$  (because  $H \notin \mathfrak{p}$ ), we have  $\{F\} \subset \{\theta_\kappa A_{k(\kappa)}\} : S_{A_{k(\kappa)}} \subset \mathfrak{q}$ , so that  $\mathfrak{q} = \{\theta_\kappa A_{k(\kappa)}\} : S_{A_{k(\kappa)}}$ . Starting afresh, for any  $\kappa \in \Lambda_0$  we find as above that  $\{F\} \subset \{\theta_\kappa A_{k(\kappa)}\} : S_{A_{k(\kappa)}} \subset \mathfrak{p}$ , so that the prime differential ideal  $\{\theta_\kappa A_{k(\kappa)}\} : S_{A_{k(\kappa)}}$  contains a component  $\mathfrak{q}$  of  $\{F\}$  that is contained in  $\mathfrak{p}$ . By what we have already proved,  $\mathfrak{q} = \{\theta_{\kappa'} A_{k(\kappa')}\} : S_{A_{k(\kappa' )}}$  for some  $\kappa' \in \Lambda_1$ . If the inclusion  $\mathfrak{q} \subset \{\theta_\kappa A_{k(\kappa)}\} : S_{A_{k(\kappa)}}$  were strict, then (by the claim established above)  $\theta_{\kappa'} u_{A_{k(\kappa' )}}$  would be a proper derivative of  $\theta_\kappa u_{A_{k(\kappa)}}$ , contradicting the hypothesis that  $\kappa \in \Lambda_0$ . Therefore  $\{\theta_\kappa A_{k(\kappa)}\} : S_{A_{k(\kappa)}}$  is a component of  $\{F\}$  contained in  $\mathfrak{p}$ .

**Corollary** Let the notation and hypothesis be as in Theorem 7(a), and suppose that  $F$  is irreducible. If  $\theta u_{A_*} = u_F$ , then  $\mathfrak{p}_{\mathcal{F}}(F) \subset \mathfrak{p}$ .

*Proof* By Theorem 7(a),  $\{F\}$  has a component  $\mathfrak{p}_{\mathcal{F}}(B) \subset \mathfrak{p}$  with  $B$  involving a derivative of  $u_F$  and therefore with  $F$  partially reduced with respect to  $B$ . By Section 14, the corollary to Theorem 5, then  $\mathfrak{p}_{\mathcal{F}}(B) = \mathfrak{p}_{\mathcal{F}}(F)$ .

### EXERCISES

- Let  $F, G$  be nonzero elements of  $\mathcal{F}\{y\}$  of order less than or equal to 1 without common divisor, and suppose that  $F(0) = G(0) = 0$ . Let  $t$  be an element of  $\mathcal{U}$  differentially transcendental over  $\mathcal{F}$  and set  $u = F(t)/G(t)$ . Prove the following result of Ritt [84]: If  $[y]$  is a component of  $zG - F$  in  $\mathcal{F}\{y, z\}$ , then either there exists a unique  $\zeta \in \mathcal{U}$  such that  $(0, \zeta)$  is a differential specialization of  $(t, u)$  over  $\mathcal{F}$  and then  $\zeta \in \mathcal{F}$ , or else  $(0, 0)$  is a differential specialization of  $(t, u^{-1})$  over  $\mathcal{F}$ . If, on the other hand,  $[y]$  is not a component of  $zG - F$ , then  $(0, \zeta)$  is a differential specialization of  $(t, u)$  over  $\mathcal{F}$  for every  $\zeta \in \mathcal{U}$ . (Hint: See Section 6, Exercise 8, and Section 14, Exercise 4.)
- Let  $n \in \mathbb{N}$ ,  $n \neq 0$ , and let  $A$  be an irreducible differential polynomial in  $\mathcal{F}\{y\}$  of order  $n$  that is free of every derivative  $\theta y$  such that  $0 < \text{ord } \theta < n$ . Show that if  $0$  is a zero of  $A$ , but not of  $\mathfrak{p}_{\mathcal{F}}(A)$ , then  $[y]$  is a component of  $A$ . (Hint: Using Section 14, the corollary to Theorem 5, prove that there exists a nonzero  $B \in \mathcal{F}\{y\}$  of order less than  $n$  contained in every component of  $A$  having  $0$  as a zero; then show there exists a  $C \in \mathcal{F}\{y\}$  with  $C(0) \neq 0$  contained in all the other components. Using the usual grading, apply Section 10, Corollary 3 of Theorem 4, to the relation  $BC \in \{A\}$  to show that  $\text{ord } A_* < n$  and hence that  $\text{ord } A_* = 0$ , and then use the low power theorem.)

### 16 The Ritt problem

If  $F$  is a differential polynomial in  $\mathcal{F}\{y_1, \dots, y_n\}$  not in  $\mathcal{F}$ , and  $\eta = (\eta_1, \dots, \eta_n)$  is a zero of  $\mathcal{F}$ , then  $\eta$  is a zero of at least one of the components of  $\{F\}$  in  $\mathcal{F}\{y_1, \dots, y_n\}$ . It is natural to try to determine all the components of  $\{F\}$  that admit  $\eta$  as a zero. By the methods of Section 9 and the low power theorem we can determine a finite set  $A_1, \dots, A_r$  of irreducible differential polynomials in  $\mathcal{F}\{y_1, \dots, y_n\}$  such that  $\mathfrak{p}_{\mathcal{F}}(A_1), \dots, \mathfrak{p}_{\mathcal{F}}(A_r)$  are distinct and are the components of  $\{F\}$ . Thus, we are led to the following type of problem: Given an irreducible  $A \in \mathcal{F}\{y_1, \dots, y_n\}$  and a point  $\eta = (\eta_1, \dots, \eta_n)$ , to determine whether  $\eta$  is a zero of  $\mathfrak{p}_{\mathcal{F}}(A)$ . By Section 6, Theorem 3(c),  $\eta$  is a zero of

$\mathfrak{p}_{\mathcal{F}}(A)$  if and only if  $\eta$  is a zero of  $\mathfrak{p}_{\mathcal{F}\langle \eta \rangle}(B)$  for some irreducible factor  $B$  of  $A$  in  $\mathcal{F}\langle \eta \rangle\{y_1, \dots, y_n\}$ . Hence if we can find the irreducible factors of  $A$  over  $\mathcal{F}\langle \eta \rangle$ , the problem reduces (on replacing  $\mathcal{F}$  by  $\mathcal{F}\langle \eta \rangle$ ) to the special case in which each coordinate  $\eta_j$  is in  $\mathcal{F}$ . Since we may then translate by  $\eta$ , we arrive at the following problem posed by Ritt: Given an irreducible differential polynomial  $A \in \mathcal{F}\{y_1, \dots, y_n\}$  vanishing at  $(0, \dots, 0)$ , to determine whether  $(0, \dots, 0)$  is a zero of  $\mathfrak{p}_{\mathcal{F}}(A)$ .

If  $(0, \dots, 0)$  is not a zero of any singular component of  $A$ , then of course  $(0, \dots, 0)$  is a zero of  $\mathfrak{p}_{\mathcal{F}}(A)$ . Also, if we have a basis of  $\mathfrak{p}_{\mathcal{F}}(A)$ , the problem is trivial. However, a solution of the general Ritt problem appears to be remote at present. Even the case  $m = n = 1$  (ordinary differential polynomial in one differential indeterminate) is not settled. When  $\text{ord } A = 1$  this case presents no difficulty (see Exercise 1 below). When  $\text{ord } A = 2$  this case was treated by Ritt himself [85] who obtained a complete solution to the problem, a solution that is too long and complicated to state here. In what follows in this section we give some results that are sometimes useful in connection with the Ritt problem.

To say that  $(0, \dots, 0)$  is a zero of  $\mathfrak{p}_{\mathcal{F}}(A)$  is to say that  $\mathfrak{p}_{\mathcal{F}}(A)$  is contained in the prime differential ideal  $[y_1, \dots, y_n]$ . Thus, the Ritt problem is concerned with the special case  $\mathfrak{p} = [y_1, \dots, y_n]$  of the situation considered in Section 15, Theorem 7. To prove that  $(0, \dots, 0)$  is a zero of  $\mathfrak{p}_{\mathcal{F}}(A)$ , we therefore have the sufficient condition provided by the corollary to that theorem. However, in this special case, that result can be considerably generalized, as in the following proposition.

**Proposition 6** Let  $A \in \mathcal{F}\{y_1, \dots, y_n\}$  be irreducible with  $A(0, \dots, 0) = 0$ , and let  $f: \mathcal{F}\{y_1, \dots, y_n\} \rightarrow \mathcal{U}\{y_1, \dots, y_n\}((c))$  be a strictly positive  $A$ -permissible homomorphism (see Section 10). Fix a ranking of  $(y_1, \dots, y_n)$ . If the leader of  $f(A)$  is present in  $J_{f(A)}$  or if  $J_{f(S_A)} \notin \{J_{f(A)}\}$ , then  $(0, \dots, 0)$  is a zero of  $\mathfrak{p}_{\mathcal{F}}(A)$ .

**REMARK 1** It is clear that  $\mathcal{U}((c))\{y_1, \dots, y_n\} \subset \mathcal{U}\{y_1, \dots, y_n\}((c))$  and that  $f(A) \in \mathcal{U}((c))\{y_1, \dots, y_n\}$ ,  $f(A) \notin \mathcal{U}((c))$ . Therefore  $f(A)$  is a differential polynomial in  $(y_1, \dots, y_n)$  and has a leader.

**REMARK 2** When  $f$  is associated with a strictly positive differential permissible grading (or, if the coefficients in  $A$  are constants, with a strictly positive permissible grading) in the manner described in Section 10, right after Corollary 2 to Theorem 4, the proposition states that if  $A_*$  has leader  $u_A$  or if  $(S_A)_* \notin \{A_*\}$ , then  $(0, \dots, 0)$  is a zero of  $\mathfrak{p}_{\mathcal{F}}(A)$ , a result due to Hillman (whose proof we follow here). For the usual grading the result goes back to Ritt (special case of the corollary to Theorem 7).

**REMARK 3** Examples occur (even with  $m = n = 1$ ) to which the proposition is applicable but for which it is necessary to use an  $f$  such that the

corresponding  $P = (P_j)_{1 \leq j \leq n} \in \mathcal{U}((c))^n$  (see Section 10) is suitably chosen different from  $(0)$ . (See Exercises 2 and 3 below.)

*Proof* Assume that  $(0, \dots, 0)$  is not a zero of  $\mathfrak{p}_{\mathcal{F}}(A)$ , i.e., that there exists a  $Y \in [y_1, \dots, y_n]$  with  $1+Y \in \mathfrak{p}_{\mathcal{F}}(A)$ . Then  $(1+Y)S_A \in \{A\}$ . Because  $f$  is  $A$ -permissible this implies that  $(1+f(Y))f(S_A) \in \{f(A)\}$ . The ideal  $(f(S_A), f(A))$  in  $\mathcal{U}((c))\{y_1, \dots, y_n\}$  (see Remark 1, above) obviously contains a nonzero element  $G$  free of every derivative of  $u_{f(A)}$ , and of course  $(1+f(Y))G \in \{f(A)\}$  in  $\mathcal{U}\{y_1, \dots, y_n\}((c))$ . Because  $f$  is strictly positive  $J_{(1+f(Y))G} = J_G$  and  $J_{(1+f(Y))f(S_A)} = J_{f(S_A)}$ . By Section 10, Theorem 4, therefore  $J_G \in \{J_{f(A)}\}$  and  $J_{f(S_A)} \in \{J_{f(A)}\}$ . The former relation here implies that  $J_G \in \mathfrak{p}_{\mathcal{U}}(B)$ , where  $B$  is any irreducible factor of  $J_{f(A)}$  in  $\mathcal{U}\{y_1, \dots, y_n\}$  involving  $u_{J_{f(A)}}$ . By Section 6, Theorem 3(b),  $J_G$  must therefore involve a derivative of  $u_{J_{f(A)}}$ , so that  $G$  must too; whence  $u_{J_{f(A)}} \neq u_{f(A)}$ .

In order to prove that  $(0, \dots, 0)$  is *not* a zero of  $\mathfrak{p}_{\mathcal{F}}(A)$ , our main tool is the domination lemma. We formulate the following result.

**Proposition 7** *Let  $\mathfrak{p}$  be a prime differential ideal of  $\mathcal{F}\{y_1, \dots, y_n\}$  and suppose that  $\mathfrak{p}$  contains a differential polynomial of the form  $\sum_{0 \leq \gamma \leq g} C_{\gamma} M_{\gamma}(A_1, \dots, A_r)$ , where  $C_{\gamma} \in \mathcal{F}\{y_1, \dots, y_n\}$  ( $0 \leq \gamma \leq g$ ) and  $C_0(0, \dots, 0) \neq 0$ ,  $A_{\rho} \in \mathcal{F}\{y_1, \dots, y_n\}$  and  $A_{\rho}(0, \dots, 0) = 0$  ( $1 \leq \rho \leq r$ ), and  $M_0, M_1, \dots, M_g$  are differential monomials in  $(z_1, \dots, z_r)$  with  $M_{\gamma} \neq M_0$  ( $1 \leq \gamma \leq g$ ) such that  $M_0(A_1, \dots, A_r) \notin \mathfrak{p}$  and  $M_{\gamma}$  dominates  $M_0$  ( $1 \leq \gamma \leq g$ ). Then  $(0, \dots, 0)$  is not a zero of  $\mathfrak{p}$ .*

*Proof* By Section 12, Lemma 6,  $\mathfrak{p}$  contains a differential polynomial  $M_0(A_1, \dots, A_r)(C_0^e + Z(A_1, \dots, A_r))$ , where  $e \in \mathbb{N}$  and  $Z \in [z_1, \dots, z_r]$  in  $\mathcal{F}\{C_0, C_1, \dots, C_g, z_1, \dots, z_r\}$ , so that  $\mathfrak{p}$  contains the differential polynomial  $C_0^e + Z(A_1, \dots, A_r)$  which does not vanish at  $(0, \dots, 0)$ .

As a special case of Proposition 7, we see that *if an irreducible  $A \in \mathcal{F}\{y_1, \dots, y_n\}$  has at least two nonzero terms and one of them is dominated by all the others, then  $(0, \dots, 0)$  is not a zero of  $\mathfrak{p}_{\mathcal{F}}(A)$ .*

In much the same way, but using Section 11, Lemma 3, instead of Lemma 6, we can prove that *if, for each  $y_j$ ,  $\mathfrak{p}$  contains a differential polynomial  $y_j^{q_j} + Y_j$  with  $q_j \in \mathbb{N}$  and  $Y_j \in [y_1, \dots, y_n]^{q_j+1}$ , and if  $\mathfrak{p} \neq [y_1, \dots, y_n]$ , then  $(0, \dots, 0)$  is not a zero of  $\mathfrak{p}$ .*

It is sometimes possible to establish the condition here with the help of the notion of  $\mathfrak{k}$ -value (see Chapter 0, Section 19, and Chapter I, Section 7, corollary to Lemma 4),  $\mathfrak{k}$  being taken as the differential ideal  $\mathfrak{k} = ([y_1, \dots, y_n] + \mathfrak{p})/\mathfrak{p}$  of

the differential residue ring  $\mathcal{R} = \mathcal{F}\{y_1, \dots, y_n\}/\mathfrak{p}$ . To simplify the notation, for each  $P \in \mathcal{F}\{y_1, \dots, y_n\}$  define

$$\bar{v}_{\mathfrak{p}}(P) = v_1(\bar{P}),$$

$\bar{P}$  denoting the canonical image of  $P$  in  $\mathcal{R}$ . Thus,  $0 \leq \bar{v}_{\mathfrak{p}}(P) \in \mathbb{R}$  or  $\bar{v}_{\mathfrak{p}}(P) = \infty$ ,  $\bar{v}_{\mathfrak{p}}(P+Q) \geq \min(\bar{v}_{\mathfrak{p}}(P), \bar{v}_{\mathfrak{p}}(Q))$ ,  $\bar{v}_{\mathfrak{p}}(PQ) \geq \bar{v}_{\mathfrak{p}}(P) + \bar{v}_{\mathfrak{p}}(Q)$ , and  $\bar{v}_{\mathfrak{p}}(P^r) = r\bar{v}_{\mathfrak{p}}(P)$  for every nonzero  $r \in \mathbb{N}$ . To say that  $\bar{v}_{\mathfrak{p}}(P) > \alpha$ , where  $\alpha \in \mathbb{R}$  and  $\alpha \geq 0$ , is to say that there exist  $q, r \in \mathbb{N}$  with  $r > q\alpha$  such that  $P^q \in [y_1, \dots, y_n]^r + \mathfrak{p}$ .

We therefore have the following result.

**Proposition 8** *Let  $\mathfrak{p}$  be a prime differential ideal of  $\mathcal{F}\{y_1, \dots, y_n\}$  different from  $[y_1, \dots, y_n]$ . If  $\bar{v}_{\mathfrak{p}}(y_j) > 1$  ( $1 \leq j \leq n$ ), then  $(0, \dots, 0)$  is not a zero of  $\mathfrak{p}$ .*

EXERCISES

In all the following exercises  $\mathcal{F}$  denotes a differential subfield of  $\mathcal{U}$ .

1. Let  $A \in \mathcal{F}\{y\}$  be irreducible and of order 1, and let  $A(0) = 0$ . A necessary and sufficient condition that 0 fail to be a zero of  $\mathfrak{p}_{\mathcal{F}}(A)$  is that  $A \equiv ay^q \pmod{[y]^{q+1}}$  for some  $q \in \mathbb{N}$  and some nonzero  $a \in \mathcal{F}$ .
2. (Elaboration of an example of Ritt) Let  $m = 1$  (that is, let  $\mathcal{U}$  be an ordinary differential field), and let

$$A = (yy'' + yy' - 2y'^2)^2 - a \prod_{1 \leq i \leq r} (y' - y + b_i y^2)^{h_i},$$

where  $r \in \mathbb{N}$  and  $r \neq 0$ ,  $a \in \mathcal{F}$  and  $a \neq 0$ ,  $b_1, \dots, b_r \in \mathcal{F}$  and  $b_1, \dots, b_r$  are distinct,  $h_1, \dots, h_r \in \mathbb{N}$  and  $h_1 \cdots h_r \neq 0$ , and either  $h_1, \dots, h_r$  are not all even or else  $a$  is not a square in  $\mathcal{F}$ . Show that  $A$  is irreducible in  $\mathcal{F}\{y\}$ . Prove that 0 is a zero of  $\mathfrak{p}_{\mathcal{F}}(A)$  except when *either*  $r = 2$ ,  $h_1 = h_2 = 1$ ,  $b_1$  and  $b_2$  are constants, *or*  $r = 1$ ,  $h_1 = 1$ ,  $b_1$  is a constant. (*Hint*: Set  $B_i = y' - y + b_i y^2$  so that  $yB_i' - 2y'B_i - b_i' y^3 = yy'' + yy' - 2y'^2$ , and let  $\varepsilon$  be a nonzero element of  $U$  with  $\varepsilon' = \varepsilon$ . If  $\sum h_i \geq 3$ , or if  $\sum h_i \leq 2$  and some  $b_i' \neq 0$ , let  $f$  denote the substitution of  $\varepsilon c + y c^2$  for  $y$  and apply Proposition 6 (if  $\sum h_i \geq 4$ , the simpler substitution of  $yc$  for  $y$  suffices). If  $r = 1$ ,  $h_1 = 2$ , and  $b_1' = 0$ , show with the help of the low power theorem that  $A$  has no singular component. If  $r = 1$ ,  $h_1 = 1$ , and  $b_1' = 0$  observe that  $A = aB_1 + (yB_1' - 2y'B_1)^2$  and apply Proposition 7. If  $r = 2$ ,  $h_1 = h_2 = 1$ , and  $b_1' = b_2' = 0$ , observe that  $A = CB_1 + y^2 B_2^2$ , where  $C = aB_2 + 4y^2 B_1 - 4yy'B_1'$ ; examining  $CA' - C'A$ , show that  $C^2 - 4y^2 C'B_1' + 2yy'CB_1' + 2y^2 CB_1'' \in \mathfrak{p}_{\mathcal{F}}(A)$ ; writing  $o(P)$  for  $\bar{v}_{\mathfrak{p}_{\mathcal{F}}(A)}(P)$ , show from this that  $o(C) \geq 2 + o(B_1)$ , and therefore that  $o(B_2) \geq 2 + o(B_1)$ ; interchanging  $B_1$  and  $B_2$ , deduce that  $o(B_1) = o(B_2) = \infty$ , and therefore that  $o(y) = \frac{1}{2}o(y^2) = \frac{1}{2}o(B_1 - B_2) = \infty$ , and apply Proposition 8.)

3. (Hillman) Let  $m = 1$ , and let  $A = (y' + y''')^t + y'(y + y'') + ay^s$ , where  $s, t \in \mathbb{N}$ ,  $st \neq 0$ , and  $a \in \mathcal{F}$ . Show that  $A$  is irreducible in  $\mathcal{F}\{y\}$ . Prove that if  $a = 0$  and  $t > 2$ , or if  $a \neq 0$  and  $t > 1$  and  $s = 1$ , then 0 is not a zero of  $p_{\mathcal{F}}(A)$ , but that in all other cases 0 is a zero of  $p_{\mathcal{F}}(A)$ .
4. Let  $m \geq 2$ , and let  $A = (\delta_1^3 y)(\delta_1 \delta_2 y)(\delta_2^2 y)^2 + a_1(\delta_1^3 \delta_2^2 y)^k + a_2(\delta_1^3 y) \times (\delta_1^2 \delta_2^2 y)^2 (\delta_2^3 y)^2 + a_3 y (\delta_1^3 y)(\delta_1 \delta_2 y)(\delta_2^2 y)^2$ , where  $k \in \mathbb{N}$ ,  $k \neq 0$ ,  $a_1, a_2, a_3 \in \mathcal{F}$ , and  $a_1 \neq 0$ . Show that  $A$  is irreducible in  $\mathcal{F}\{y\}$ . Prove that 0 is a zero of  $p_{\mathcal{F}}(A)$  if and only if  $k \leq 4$ .
5. (Ritt) (a) Let

$$A = \prod_{1 \leq l \leq s} (y_1 + c_l y_2) + y_3 \prod_{1 \leq k \leq r} (y_1 \delta_{i(k)} y_2 - y_2 \delta_{i(k)} y_1),$$

where  $r, s \in \mathbb{N}$ ,  $r \geq 2$ ,  $s \geq 2r + 1$ ,  $c_1, \dots, c_s$  are distinct constants in  $\mathcal{F}$ , and  $i(k)$  is one of the numbers  $1, 2, \dots, m$  ( $1 \leq k \leq r$ ). Show that  $A$  is irreducible over  $\mathcal{U}$  and that  $\{p_{\mathcal{F}}(A) + [y_3]\} = [y_1, y_2, y_3]$ . (Hint: Show that  $(0, 0, 0)$  is a zero of  $p_{\mathcal{F}}(A)$ , so that  $p_{\mathcal{F}}(A) + [y_3] \subset [y_1, y_2, y_3]$ . Show that if  $\mathfrak{p}$  is any component of  $\{p_{\mathcal{F}}(A) + [y_3]\}$ , then  $\mathfrak{p}$  contains  $y_1 + c_{l_0} y_2$  for some  $l_0$ , and use Levi's lemma or the domination lemma to show that  $p_{\mathcal{F}}(A)$  contains a differential polynomial  $\prod_{l \neq l_0} (y_1 + c_l y_2)^d + Y$  with  $d > 0$  and  $Y \in [y_3]$ , whence  $\mathfrak{p} \supset [y_1, y_2, y_3]$ .)

(b) Generalize the example of part (a) to produce, for any  $n \geq 3$ , an irreducible closed set in  $\mathcal{U}^n$  of differential dimension  $n - 1$  that intersects the hyperplane defined by the equation  $y_n = 0$  in the single point  $(0, \dots, 0)$  (anomaly of differential dimension of intersections).

### 17 Systems of bounded order

Consider a set  $\Sigma$  of differential polynomials in  $(y_1, \dots, y_n)$  such that, for each index  $j$ , no element of  $\Sigma$  involves a derivative of  $y_j$  of order greater than a given natural number  $e_j$ . We shall show (Proposition 9) that if  $\mathfrak{p}$  is any component of  $\{\Sigma\}$  having differential type  $m - 1$ , then the typical differential dimension of  $\mathfrak{p}$  must be less than or equal to  $e_1 + \dots + e_n$ . In other words, when we write the differential dimension polynomial as  $\omega_{\mathfrak{p}} = \sum_{0 \leq i \leq m} a_i (X^i)$ , the condition  $a_m = 0$  implies the condition  $a_{m-1} \leq e_1 + \dots + e_n$ . For ordinary differential polynomials (i.e., for  $m = 1$ ) this proposition reduces to a result found by Ritt ([82, Part II], or [95, Chapter VII, Sections 3-4]). In the case of a system of order 0 ( $e_1 = \dots = e_n = 0$ ), the proposition is not very informative; we shall prove for this case a much more precise result (Proposition 10).

**Lemma 8** Let  $\delta \in \Delta$ , and let  $\Delta_0$  denote the set of elements of  $\Delta$  other than  $\delta$ . Let  $e_1, \dots, e_n \in \mathbb{N}$ , and let  $\Sigma$  be a subset of  $\mathcal{F}\{(\delta^k y_j)_{1 \leq j \leq n, 0 \leq k \leq e_j}\}_{\Delta_0}$ . Let  $\mathfrak{p}$  be a component of  $\{\Sigma\}$  in  $\mathcal{F}\{y_1, \dots, y_n\}_{\Delta}$ , let  $\eta = (\eta_1, \dots, \eta_n)$  be a generic

zero of  $\mathfrak{p}$ , and set  $\mathcal{G} = \mathcal{F}\langle \eta \rangle_{\Delta}$ . If the differential dimension of  $\mathfrak{p}$  is 0, then the  $\Delta_0$ -transcendence degree of  $\mathcal{G}$  over  $\mathcal{F}$  is less than or equal to  $e_1 + \dots + e_n$ .

*Proof* We first show by a classical transformation that it suffices to consider the case in which  $e_j \leq 1$  for each  $j$ . Let  $(z_{jk})_{1 \leq j \leq n, 0 \leq k \leq e_j}$  be a family of  $\Delta$ -indeterminates, and consider the substitution homomorphism

$$\sigma : \mathcal{F}\{(z_{jk})_{1 \leq j \leq n, 0 \leq k \leq e_j}\}_{\Delta} \rightarrow \mathcal{F}\{y_1, \dots, y_n\}_{\Delta}$$

mapping  $z_{jk}$  onto  $\delta^k y_j$  ( $1 \leq j \leq n, 0 \leq k \leq e_j$ ). It is easy to see that  $\sigma$  maps  $\mathcal{F}\{(z_{jk})_{1 \leq j \leq n, 0 \leq k \leq e_j}\}_{\Delta_0}$  bijectively onto  $\mathcal{F}\{(\delta^k y_j)_{1 \leq j \leq n, 0 \leq k \leq e_j}\}_{\Delta_0}$ , that  $\sigma$  is surjective, and that the kernel of  $\sigma$  is the  $\Delta$ -ideal  $[K]$ , where  $K$  denotes the set of differential polynomials  $z_{j, k+1} - \delta z_{jk}$  ( $1 \leq j \leq n, 0 \leq k < e_j$ ). Therefore there exists a unique set  $T_0 \subset \mathcal{F}\{(z_{jk})_{1 \leq j \leq n, 0 \leq k \leq e_j}\}_{\Delta_0}$  such that  $\sigma(T_0) = \Sigma$ . Setting  $T = T_0 \cup K$ , we see that

$$T \subset \mathcal{F}\{(z_{jk})_{1 \leq j \leq n, 0 \leq k \leq e_j}, (\delta z_{jk})_{1 \leq j \leq n, 0 \leq k \leq e_j}\}_{\Delta_0}$$

and that  $\{T\} = \sigma^{-1}(\{\Sigma\})$ . It readily follows that the ideal  $\mathfrak{q} = \sigma^{-1}(\mathfrak{p})$  is a component of  $\{T\}$  in  $\mathcal{F}\{(z_{jk})_{1 \leq j \leq n, 0 \leq k \leq e_j}\}_{\Delta}$ . Also, the point  $\zeta = (\delta^k \eta_j)_{1 \leq j \leq n, 0 \leq k \leq e_j}$  is a generic zero of  $\mathfrak{q}$ , and  $\mathcal{F}\langle \zeta \rangle_{\Delta} = \mathcal{G}$ . The number for  $T$  analogous to the number  $e_1 + \dots + e_n$  for  $\Sigma$  is, moreover, equal to  $e_1 + \dots + e_n$ . Thus, we may replace  $\Sigma$  by  $T$ , that is, we may suppose that each  $e_j$  is either 0 or 1.

This being the case, we may, on permuting the indices  $1, \dots, n$ , even suppose that  $\Sigma$  is contained in the  $\Delta_0$ -algebra  $\mathcal{R}_0 = \mathcal{F}\{y_1, \dots, y_n, \delta y_1, \dots, \delta y_n\}_{\Delta_0}$ ,  $v$  being an integer with  $0 \leq v \leq n$ . We then must prove that the  $\Delta_0$ -transcendence degree of  $\mathcal{G}$  over  $\mathcal{F}$  is less than or equal to  $v$ .

Now,  $\mathcal{R}_0$  is a  $\Delta_0$ -polynomial algebra over  $\mathcal{F}$  in the family of  $\Delta_0$ -indeterminates  $(y_1, \dots, y_n, \delta y_1, \dots, \delta y_n)$ . Setting  $\mathfrak{p}_0 = \mathfrak{p} \cap \mathcal{R}_0$ , we see that  $\mathfrak{p}_0$  is a prime  $\Delta_0$ -ideal of  $\mathcal{R}_0$ . Since  $\Sigma \subset \mathfrak{p}_0 \subset \mathfrak{p}$ ,  $\mathfrak{p}$  is a component of  $\{\mathfrak{p}_0\}$  in  $\mathcal{F}\{y_1, \dots, y_n\}_{\Delta}$ . It is evident that  $(\eta_1, \dots, \eta_n, \delta \eta_1, \dots, \delta \eta_n)$  is a generic zero of  $\mathfrak{p}_0$ . Letting  $\mu$  denote the  $\Delta_0$ -transcendence degree of  $\mathcal{F}\langle \eta_1, \dots, \eta_n \rangle_{\Delta_0}$  over  $\mathcal{F}$ , we may, on permuting the indices  $1, \dots, v$ , suppose that  $(\eta_1, \dots, \eta_\mu)$  is a  $\Delta_0$ -transcendence basis of  $\mathcal{F}\langle \eta_1, \dots, \eta_n \rangle_{\Delta_0}$  over  $\mathcal{F}$ ; of course  $0 \leq \mu \leq v$ . It is then easy to see that for each index  $i$  with  $\mu < i \leq v$  the element  $\delta \eta_i$  is  $\Delta_0$ -algebraic over  $\mathcal{F}\langle \eta_1, \dots, \eta_\mu, \delta \eta_1, \dots, \delta \eta_\mu \rangle_{\Delta_0}$ .

Let  $\lambda$  denote the  $\Delta_0$ -transcendence degree of  $\mathcal{F}\langle \eta_1, \dots, \eta_\mu, \delta \eta_1, \dots, \delta \eta_\mu \rangle_{\Delta_0}$  over  $\mathcal{F}\langle \eta_1, \dots, \eta_\mu \rangle_{\Delta_0}$ , so that  $0 \leq \lambda \leq \mu$ . Permuting the indices  $1, \dots, \mu$ , we may suppose that  $(\delta \eta_1, \dots, \delta \eta_\lambda)$  is a  $\Delta_0$ -transcendence basis of  $\mathcal{F}\langle \eta_1, \dots, \eta_\mu, \delta \eta_1, \dots, \delta \eta_\mu \rangle_{\Delta_0}$  over  $\mathcal{F}\langle \eta_1, \dots, \eta_\mu \rangle_{\Delta_0}$ . Similarly, we may also suppose that  $(\eta_{v+1}, \dots, \eta_\pi)$ , with  $v \leq \pi \leq n$ , is a  $\Delta_0$ -transcendence basis of  $\mathcal{F}\langle \eta_1, \dots, \eta_n, \delta \eta_1, \dots, \delta \eta_n \rangle_{\Delta_0}$  over  $\mathcal{F}\langle \eta_1, \dots, \eta_v, \delta \eta_1, \dots, \delta \eta_v \rangle_{\Delta_0}$ . Then

$$(\eta_1, \dots, \eta_\mu, \delta \eta_1, \dots, \delta \eta_\lambda, \eta_{v+1}, \dots, \eta_\pi)$$

is a  $\Delta_0$ -transcendence basis of  $\mathcal{F}\langle \eta_1, \dots, \eta_n, \delta \eta_1, \dots, \delta \eta_n \rangle_{\Delta_0}$  over  $\mathcal{F}$ .

We are going to introduce a ranking of the family of  $\Delta$ -indeterminates  $(y_1, \dots, y_n)$ . To this end let  $\Theta_0$  denote the set of all  $\Delta_0$ -derivative operators (that is, of all elements of  $\Theta$  that are products of elements of  $\Delta_0$ ). Let  $\Theta_0$  be ordered by fixing in any way whatever a ranking of a single  $\Delta_0$ -indeterminate  $z$  and then defining  $\theta_0 < \theta_0'$  to mean that  $\theta_0 z$  is of lower rank than  $\theta_0' z$ . Let  $q(j) = 1$  or  $2$  according as  $1 \leq j \leq v$  or  $v < j \leq n$ . We can now order the set of derivatives  $\theta_0 \delta^k y_j$  ( $\theta_0 \in \Theta_0$ ,  $k \in \mathbb{N}$ ,  $1 \leq j \leq n$ ) lexicographically with respect to  $(q(j), k, j, \theta_0)$ . The set of these derivatives is of course the set of derivatives  $\theta y_j$  ( $\theta \in \Theta$ ,  $1 \leq j \leq n$ ), and it is an easy matter to see that this order is a ranking of the family of  $\Delta$ -indeterminates  $(y_1, \dots, y_n)$ . We call it *the  $\Delta$ -ranking*.

The induced order on the set consisting of the derivatives  $\theta_0 y_j$  ( $\theta_0 \in \Theta_0$ ,  $1 \leq j \leq n$ ) and the derivatives  $\theta_0 \delta y_i$  ( $\theta_0 \in \Theta_0$ ,  $1 \leq i \leq v$ ) is a ranking of the family of  $\Delta_0$ -indeterminates  $(y_1, \dots, y_n, \delta y_1, \dots, \delta y_v)$ . We call it *the  $\Delta_0$ -ranking*.

Let  $A_0$  be a characteristic set of  $p_0$  relative to the  $\Delta_0$ -ranking. Since  $(\eta_1, \dots, \eta_n, \delta \eta_1, \dots, \delta \eta_v)$  is a generic zero of  $p_0$ , it follows from our earlier considerations that the leader  $u_A$  of an element  $A \in A_0$  must be of one of the following three types: (I)  $\theta_0 y_j$  with  $\theta_0 \in \Theta_0$  and  $\mu < j \leq v$ ; (II)  $\theta_0 \delta y_j$  with  $\theta_0 \in \Theta_0$  and  $\lambda < j \leq v$ ; (III)  $\theta_0 y_j$  with  $\theta_0 \in \Theta_0$  and  $\pi < j \leq n$ . We shall need the following key fact: If  $A \in A_0$  has leader  $u_A = \theta_0 y_j$  of type (I), then there exists a  $B \in A_0$  such that *either*  $\delta u_A$  is a proper  $\Delta_0$ -derivative of  $u_B$  or *else*  $\delta u_A = u_B$  and the degree of  $B$  in  $u_B$  is 1.

Indeed, suppose there is an  $A$  as above for which no such  $B$  exists. Now,  $\delta A = S_A \delta u_A + T$  where  $T = \sum_{v < u_A} (\partial A / \partial v) \delta v + A^\delta$ , so that  $\delta A \in \mathcal{R}_0$ . There exists (by Chapter I, Section 9, Proposition 2) a product  $P = \prod_{C \in A_0} I_C^c S_C^c$  such that  $PS_A \equiv U$ ,  $PT \equiv V \pmod{[A_0]}$  in  $\mathcal{R}_0$ , where  $U$  and  $V$  are  $\Delta_0$ -reduced with respect to  $A_0$  and are lower than  $\delta u_A$ , and  $U \notin p_0$ . By what we have supposed,  $\delta u_A$  is not a proper  $\Delta_0$ -derivative of any  $u_B$  with  $B \in A_0$ , and if  $\delta u_A = u_B$ , then the degree of  $B$  in  $u_B$  is greater than 1. Therefore  $U \delta u_A + V$  is a nonzero element of  $\mathcal{R}_0$  that is  $\Delta_0$ -reduced with respect to  $A_0$ , hence is not in  $p_0$ . However,  $\delta A \in p$ , so that  $S_A \delta u_A + T \in p \cap \mathcal{R}_0 = p_0$ , whence  $U \delta u_A + V \in p_0$ . This contradiction proves the key fact stated above.

This being the case, let  $B$  denote the set of all elements  $B \in A_0$  such that  $u_B = \delta u_A$  for some  $A \in A_0$  and the degree of  $B$  in  $u_B$  is 1; set  $A = A_0 - B$ . We are going to show that  $A$  is a  $\Delta$ -autoreduced set in  $\mathcal{F}\{y_1, \dots, y_n\}$  (i.e., is autoreduced relative to the  $\Delta$ -ranking). Indeed, let  $A$  and  $C$  be any two distinct elements of  $A$  with, say  $A$ , of lower rank than  $C$ . We must show that  $C$  is  $\Delta$ -reduced with respect to  $A$ . Since  $A_0$  is  $\Delta_0$ -autoreduced, the degree of  $C$  in  $u_A$  is smaller than that of  $A$ , and no proper  $\Delta_0$ -derivative of  $u_A$  is present in  $C$ . Also, since  $C \in \mathcal{R}_0$ , no  $\Delta$ -derivative  $\theta_0 \delta^k u_A$  with  $\theta_0 \in \Theta_0$  and  $k > 1$  is present in  $C$ . Suppose that  $\theta_0 \delta u_A$  is present in  $C$ . Then  $u_A$  must be of type

(I) and, by the key fact, there exists a  $B \in A_0$  either with  $\delta u_A$  a proper  $\Delta_0$ -derivative of  $u_B$  or *else* with  $\delta u_A = u_B$  and  $B$  of degree 1 in  $u_B$ . Since  $C$  cannot contain a proper  $\Delta_0$ -derivative of  $u_B$ , the latter possibility must prevail and  $\theta_0 = 1$ , so that  $B \in B$ , whence  $C \neq B$ , and  $C$  is not  $\Delta_0$ -reduced with respect to  $B$ . This contradiction shows that  $A$  is  $\Delta$ -autoreduced.

Consider an arbitrary element  $F \in \mathcal{R}_0$ , and let  $A_F$  denote the set of all derivatives  $\theta A$  ( $\theta \in \Theta$ ,  $A \in A$ ) with  $\text{rank } \theta A \leq \text{rank } F$ . We claim that there exists a congruence

$$\prod_{A \in A} S_A^i I_A^j \cdot F \equiv F_0 \pmod{(A_F)} \quad (7)$$

with  $F_0$  in  $\mathcal{R}_0$  and  $\Delta$ -reduced with respect to  $A$ , and that for any such congruence,  $F \in p_0$  if and only if  $F_0 = 0$ .

It is clear from the key fact proved above that an element of  $\mathcal{R}_0$  is  $\Delta$ -reduced with respect to  $A$  if and only if it is  $\Delta_0$ -reduced with respect to  $A_0$ . From this, the second part of the claim is immediate. Also, when  $F$  is  $\Delta_0$ -reduced with respect to  $A_0$ , then a congruence (7) exists (take  $F_0 = F$  and  $s_A = i_A = 0$  for every  $A \in A$ ). Therefore in proving the first part of the claim we may suppose that  $F$  is not  $\Delta_0$ -reduced with respect to  $A_0$ . Let  $v(F)$  denote the highest  $\Delta_0$ -derivative of a leader of an element of  $A_0$  that is present in  $F$  and that either is proper or else appears in  $F$  to at least as high a degree as in the element of  $A_0$ ; say  $v(F) = \theta_0 u_B$ , where  $\theta_0 \in \Theta_0$ ,  $B \in A_0$ , and either  $\theta_0 \neq 1$  or else  $\theta_0 = 1$  and  $\text{deg}_{v(F)} F \geq \text{deg}_B B$ . It is easy to see that  $v(F)$  is also the highest  $\Delta$ -derivative of a leader of an element of  $A$  that is present in  $F$  and that either is proper or else appears in  $F$  to at least as high a degree as in the element of  $A$ . We argue by induction on  $v(F)$ . Setting  $e(F) = \text{deg}_{v(F)} F$ , we distinguish three cases. *First*, suppose that  $B \in A$  and  $\theta_0 \neq 1$ , so that  $\theta_0 B = S_B v(F) + T \in \mathcal{R}_0$  with  $T$  lower than  $v(F)$ . Dividing  $F$  by  $\theta_0 B$ , we find a congruence  $S_B^{e(F)} F \equiv G \pmod{\theta_0 B}$ , where  $G \in \mathcal{R}_0$  and either  $G$  is  $\Delta$ -reduced with respect to  $A$  or  $v(G) < v(F)$ . Therefore there exists for  $G$  a congruence

$$\prod_{A \in A} S_A^i I_A^j \cdot G \equiv G_0 \pmod{(A_G)}$$

of the form (7). Evidently  $A_G \subset A_F$ , so that

$$\prod_{A \in A} S_A^i I_A^j \cdot S_B^{e(F)} F \equiv G_0 \pmod{(A_F)},$$

which is a congruence for  $F$  of the form (7). *Second*, suppose that  $B \in A$  and  $\theta_0 = 1$ , so that  $v(F) = u_B$  and  $e(F) \geq b = \text{deg}_{u_B} B$ . Dividing  $F$  by  $B$ , we find a congruence  $I_B^{e(F)-b+1} F \equiv G \pmod{B}$ , where  $G \in \mathcal{R}_0$  and either  $G$  is  $\Delta$ -reduced with respect to  $A$  or  $v(G) < v(F)$ . The second case is then handled in the same way as the first. *Third*, suppose that  $B \notin A$  (that is, that  $B \in B$ ). Then  $u_B = \delta u_A$  with  $A \in A_0$  and  $\text{deg}_{u_B} B = 1$ . The leader of  $A$  must be of type (I), and this implies that  $A \in A$ , and that  $A \in \mathcal{F}\{y_1, \dots, y_n\}_{\Delta_0}$ , whence



$\delta A \in \mathcal{R}_0$ . Therefore  $\delta A \in \mathfrak{p} \cap \mathcal{R}_0 = \mathfrak{p}_0$  and  $\theta_0 \delta A = S_A v(F) + T \in \mathcal{R}_0$  with  $T$  lower than  $v(F)$ . Dividing  $F$  by  $\theta_0 \delta A$ , we may write  $S_A^{e(F)} F \equiv G \pmod{\theta_0 \delta A}$ , where  $G \in \mathcal{R}_0$  and either  $G$  is  $\Delta$ -reduced with respect to  $A$  or  $v(G) < v(F)$ . The third case is then finished in the same way as the first two. This proves the claim made in the preceding paragraph.

We are now going to show that  $A$  is a characteristic set (relative to the  $\Delta$ -ranking) of a prime  $\Delta$ -ideal of  $\mathcal{F}\{y_1, \dots, y_n\}$ . By Section 9, Lemma 2, it suffices to show that  $A$  is coherent and that the ideal  $(A):H_A^\infty$  is prime and contains no nonzero element  $\Delta$ -reduced with respect to  $A$ .

To settle the first point, let  $A$  and  $C$  be distinct elements of  $A$  such that  $u_A$  and  $u_C$  have a lowest common  $\Delta$ -derivative  $\theta u_A = \theta' u_C$ . Because of the type possibilities for a leader of an element of  $A$ , either  $\theta$  and  $\theta'$  are both in  $\Theta_0$ , or else one of the leaders, say  $u_A$ , can be written  $u_A = \theta_0 y_j$  with  $\theta_0 \in \Theta_0$  and  $\mu < j \leq v$ , and the other leader  $u_C$  can then be written  $u_C = \theta_0' \delta y_j$  with  $\theta_0' \in \Theta_0$ , in which case  $\theta \in \Theta_0 \delta$  and  $\theta' \in \Theta_0$ . In either case the difference  $F = S_C \theta A - S_A \theta' C$  is an element of  $\mathfrak{p}$  and of  $\mathcal{R}_0$ , that is, is an element of  $\mathfrak{p}_0$ . Therefore there exists for  $F$  a congruence (7) as above with  $F_0 = 0$ . By the observation in Section 9 preceding Lemma 2, we conclude that  $A$  is coherent.

In proving the second point we may work in the algebra over  $\mathcal{F}$  generated by any set of derivatives  $\theta y_j$  that includes all the derivatives present in the elements of  $A$  (see the Remark in Section 9 following Lemma 2). An element of  $(A):H_A^\infty$  in  $\mathcal{R}_0$  that is  $\Delta$ -reduced with respect to  $A$  is an element of  $\mathfrak{p}_0$  that is  $\Delta_0$ -reduced with respect to  $A_0$ , and therefore is 0. To show that  $(A):H_A^\infty$  is prime we work in the algebra  $\mathcal{R}_{00}$  generated by just the derivatives present in the elements of  $A$ ; of course  $\mathcal{R}_{00} \subset \mathcal{R}_0$ . Let  $F, G \in \mathcal{R}_{00}$ ,  $F, G \notin (A):H_A^\infty$  in  $\mathcal{R}_{00}$ . Because of the nature of  $\mathcal{R}_{00}$ , neither  $F$  nor  $G$  can involve a proper  $\Delta$ -derivative of any  $u_A$  with  $A \in A$ . Therefore there exist congruences

$$\prod_{A \in A} I_A^{i_A} \cdot F \equiv F_0 \pmod{(A)}, \quad \prod_{A \in A} I_A^{j_A} \cdot G \equiv G_0 \pmod{(A)}$$

in  $\mathcal{R}_{00}$  with  $F_0$  and  $G_0$   $\Delta$ -reduced with respect to  $A$  (and therefore  $\Delta_0$ -reduced with respect to  $A_0$ ). Since  $F, G \notin (A):H_A^\infty$ ,  $F_0$  and  $G_0$  are not 0 and therefore are not in  $\mathfrak{p}_0$ , whence  $F_0 G_0 \notin \mathfrak{p}_0$ ; a fortiori  $F_0 G_0 \notin (A):H_A^\infty$  in  $\mathcal{R}_{00}$ , so that  $FG \notin (A):H_A^\infty$ . This completes the proof of the fact that  $A$  is a characteristic set of a prime  $\Delta$ -ideal of  $\mathcal{F}\{y_1, \dots, y_n\}$ . We denote this prime  $\Delta$ -ideal by  $\mathfrak{q}$ . By Section 9, Lemma 2,  $\mathfrak{q} = [A]:H_A^\infty$ .

It is now apparent that  $\mathfrak{p}_0 \subset \mathfrak{q} \subset \mathfrak{p}$ . Since  $\mathfrak{p}$  is a component of  $\{\mathfrak{p}_0\}$  in  $\mathcal{F}\{y_1, \dots, y_n\}$ , it follows that  $\mathfrak{p} = \mathfrak{q}$ . That is,  $A$  is a characteristic set of  $\mathfrak{p}$ .

We now make use of the hypothesis that the differential dimension of  $\mathfrak{p}$  is 0, to prove that  $\lambda = 0$  and  $\pi = v$ . If  $\lambda$  were not 0, a  $\Delta$ -derivative of  $y_1$  could

not be a leader of an element of  $A$ , and therefore every element of  $\mathcal{F}\{y_1\}_\Delta$  would be reduced with respect to  $A$ . Then  $\mathfrak{p}$  could not contain a nonzero element of  $\mathcal{F}\{y_1\}_\Delta$ , and therefore  $\mathfrak{p}$  would not be of differential dimension 0. Therefore  $\lambda = 0$ . Similarly,  $\pi = v$ .

This means that  $(\eta_1, \dots, \eta_\mu)$  is a  $\Delta_0$ -transcendence basis of

$$\mathcal{F}\langle \eta_1, \dots, \eta_n, \delta \eta_1, \dots, \delta \eta_v \rangle_{\Delta_0}$$

over  $\mathcal{F}$ . In particular, each  $\eta_j$  with  $v < j \leq n$  is  $\Delta_0$ -algebraic over  $\mathcal{F}\langle \eta_1, \dots, \eta_\mu \rangle_{\Delta_0}$ , so that  $\delta \eta_j$  is  $\Delta_0$ -algebraic over  $\mathcal{F}\langle \eta_1, \dots, \eta_\mu, \delta \eta_1, \dots, \delta \eta_\mu \rangle_{\Delta_0}$  and hence over  $\mathcal{F}\langle \eta_1, \dots, \eta_\mu \rangle_{\Delta_0}$ . Therefore the statement " $\mathcal{F}\langle (\delta^k \eta_j)_{1 \leq j \leq n, 0 \leq k \leq r} \rangle_{\Delta_0}$  is  $\Delta_0$ -algebraic over  $\mathcal{F}\langle \eta_1, \dots, \eta_\mu \rangle_{\Delta_0}$ " is true for  $r = 1$ . An easy induction argument now shows that this statement is true for every  $r \in \mathbb{N}$ , and hence shows that  $\mathcal{G}$  is  $\Delta_0$ -algebraic over  $\mathcal{F}\langle \eta_1, \dots, \eta_\mu \rangle_{\Delta_0}$ . This proves that the  $\Delta_0$ -transcendence degree of  $\mathcal{G}$  over  $\mathcal{F}$  is equal to  $\mu \leq v$ , and completes the proof of the lemma.

**Proposition 9** Let  $e_1, \dots, e_n \in \mathbb{N}$ , let  $\Sigma$  be a subset of  $\mathcal{F}[(\theta y_j)_{\theta \in \Theta(e_j), 1 \leq j \leq n}]$ , and let  $\mathfrak{p}$  be a component of  $\{\Sigma\}$  in  $\mathcal{F}\{y_1, \dots, y_n\}$ . If the differential type of  $\mathfrak{p}$  is  $m-1$ , then the typical differential dimension of  $\mathfrak{p}$  is less than or equal to  $e_1 + \dots + e_n$ .

*Proof* This proposition is an almost immediate corollary of Lemma 8, and Chapter II, Section 13, Theorem 7.

It is likely that Proposition 9 can be generalized to yield a bound for the typical differential dimension  $d^*$  of  $\mathfrak{p}$  without the assumption that the differential type  $\tau$  is  $m-1$ . There are reasons for conjecturing that

$$d^* \leq \sum_{1 \leq j \leq n} \binom{e_j - 1 + m - \tau}{m - \tau}.$$

Under certain special circumstances the bound given in Proposition 9 can be improved. Ritt considered the case in which  $m = 1$  (ordinary differential polynomials) and  $\Sigma$  consists of precisely  $n$  elements  $F_1, \dots, F_n$ . Denoting by  $e_{ij}$  the smallest natural number such that  $F_i$  does not involve a derivative of  $y_j$  of order greater than  $e_{ij}$ , he set  $h = \max_\pi (e_{1, \pi(1)} + \dots + e_{n, \pi(n)})$ ,  $\pi$  running over the whole symmetric group  $S_n$ . (This situation was considered by Jacobi<sup>2</sup> who concluded heuristically, without precise definitions, that the number of arbitrary constants in the solution of the system of differential equations  $P = 0$  ( $P \in \Sigma$ ) is less than or equal to  $h$ .)

<sup>2</sup> See C. G. J. Jacobi, De investigando ordine systematis aequationum differentialium vulgarium cujuscunque, *Borchart J. Reine Angew. Math.* 64, 297-32 (or "Gesammelte Werke," Vol. 5, pp. 191-216, Georg Reimer, Berlin, 1890).

Ritt showed that if each element of  $\Sigma$  is linear, or if  $n = 2$ , then every component  $p$  of  $\{\Sigma\}$  that is of differential dimension 0 has order less than or equal to  $h$  (where *order* means the transcendence degree of  $\mathcal{F}\langle\eta\rangle$  over  $\mathcal{F}$ ,  $\eta$  denoting a generic zero of  $p$ ); to be sure, in the linear case,  $\{\Sigma\} = [\Sigma]$  has at most one component. Whether or not this Jacobi–Ritt bound extends to sets  $\Sigma$  with  $n > 2$  and with not necessarily linear elements,<sup>3</sup> and whether or not it extends to partial differential polynomials, are open questions. For proofs of these special results see Ritt [83; or 95, Chapter VII, Section 6]. The case  $n = 2$  may be thought of as a result on the intersection of two closed (or  $\mathcal{F}$ -closed) sets  $\mathfrak{Z}(F_1), \mathfrak{Z}(F_2)$ . It is natural to conjecture that the same result would apply to the intersection of the  $\mathcal{F}$ -closed sets  $\mathfrak{Z}(p_{\mathcal{F}}(F_1)), \mathfrak{Z}(p_{\mathcal{F}}(F_2))$  under the assumption that  $F_1, F_2$  are irreducible over  $\mathcal{F}$ . Ritt verified this conjecture in the very special case in which  $e_{11}, e_{12}, e_{21}, e_{22}$  are all less than or equal to 1, but showed by counter-example that in general the conjecture is false. See Ritt [92; or 95, Chapter VII, Sections 7–15], and Exercise 1 below.

Consider the situation in Proposition 9 when  $e_1 = \dots = e_n = 0$ . If  $\tau_0$  denotes the perfect ideal generated by  $\Sigma$  in  $\mathcal{F}[y_1, \dots, y_n]$  and  $p_{01}, \dots, p_{0r}$  denote the components of  $\tau_0$  in  $\mathcal{F}[y_1, \dots, y_n]$ , then a component  $p$  of  $\{\Sigma\}$  in  $\mathcal{F}\{y_1, \dots, y_n\}$  is a component of some  $\{p_{0k}\}$  in  $\mathcal{F}\{y_1, \dots, y_n\}$ . Thus, in the present special case, Proposition 9 asserts that if  $p_0$  is a prime ideal of  $\mathcal{F}[y_1, \dots, y_n]$ , then the differential type of every component of  $\{p_0\}$  in  $\mathcal{F}\{y_1, \dots, y_n\}$  is different from  $m-1$ . The state of affairs in this particular case is much more precisely described by the following proposition.

**Proposition 10** Let  $p_0$  be a prime ideal of  $\mathcal{F}[y_1, \dots, y_n]$  of dimension  $d$ . Then  $\{p_0\}$  is a prime differential ideal of  $\mathcal{F}\{y_1, \dots, y_n\}$  having differential dimension polynomial  $\omega_{\{p_0\}} = d\binom{x+m}{m}$ .

**REMARK** The proposition becomes false if  $\mathcal{F}$  is permitted to have non-zero characteristic. See Section 6, Exercise 3(d).

*Proof* Let  $x = (x_1, \dots, x_n)$  be a generic zero of the polynomial ideal  $p_0$ , in the sense of Chapter 0, Section 11. We may suppose that  $(x_1, \dots, x_d)$  is a transcendence basis of  $\mathcal{F}(x)$  over  $\mathcal{F}$ . Then, for each  $j \in \mathbb{N}$  with  $d < j \leq n$ ,  $x_j$  is algebraic over  $\mathcal{F}(x_1, \dots, x_{j-1})$  of degree say  $a_j$ . Therefore there exists an irreducible  $A_j \in p_0$  that is free of  $y_{j+1}, \dots, y_n$ , that has degree  $a_j$  in  $y_j$ , and that has degree less than  $a_j$  in  $y_{j'}$  ( $d < j' < j$ ). On the other hand  $p_0$  does not contain a nonzero polynomial having degree less than  $a_j$  in  $y_j$  for every  $j$  with  $d < j \leq n$ . Now, there exists an orderly ranking of  $(y_1, \dots, y_n)$  such

<sup>3</sup> The case in which each element of  $\Sigma$  is of order less than or equal to 1 has recently been treated by Lando [48].

that  $y_i < y_{d+1} < y_{d+2} < \dots < y_n$  ( $1 \leq i \leq d$ ) (for example, the one obtained by ordering the set of derivatives  $\delta_1^{e_1} \dots \delta_m^{e_m} y_j$  lexicographically with respect to  $(e_1 + \dots + e_m, j, e_1, \dots, e_m)$ ); fix any such ranking. Then the set  $A$  consisting of  $A_{d+1}, \dots, A_n$  becomes autoreduced, and  $p_0 = (A):H_A^\infty$  in  $\mathcal{F}[y_1, \dots, y_n]$ . Furthermore, the leaders of distinct elements of  $A$  cannot have a common derivative, so that  $A$  is coherent. It follows by Section 9, Lemma 2, that  $A$  is a characteristic set of a prime differential ideal  $p$  of  $\mathcal{F}\{y_1, \dots, y_n\}$ , and  $p = [A]:H_A^\infty$ . By Chapter II, Section 12, Theorem 6(d), and Chapter 0, Section 17, Lemma 16(c) and (d),  $\omega_p = d\binom{x+m}{m}$ .

It is clear that  $\{p_0\} \subset p$ . Let  $(\alpha_1, \dots, \alpha_n)$  be any zero of  $p_0$ . By Chapter 0, Section 16, Corollary 3 to Proposition 11, there exist power series  $Q_1, \dots, Q_n \in \mathcal{U}[[c]]$  such that each element of  $p_0$  vanishes at  $(Q_1, \dots, Q_n)$ ,  $H_A$  does not, and  $Q_j(0) = \alpha_j$  ( $1 \leq j \leq n$ ). Now,  $\mathcal{U}$  is universal over some differential field of definition  $\mathcal{F}_0 \subset \mathcal{F}$  of  $p$  that is also a field of definition of  $p_0$ . Therefore there exists a point  $(\xi_1, \dots, \xi_n)$  that is a generic differential specialization of  $(Q_1, \dots, Q_n)$  over  $\mathcal{F}_0$ . It is clear that  $(\xi_1, \dots, \xi_n)$  is a zero of  $A$  but not of  $H_A$ , hence is a zero of  $p = [A]:H_A^\infty$ , and that  $(\alpha_1, \dots, \alpha_n)$  is a differential specialization of  $(\xi_1, \dots, \xi_n)$  over  $\mathcal{F}_0$ . It follows that  $(\alpha_1, \dots, \alpha_n)$  is a zero of  $p$ . Therefore (by Section 2, Theorem 1)  $p \subset \{p_0\}$ , whence  $p = \{p_0\}$ .

### EXERCISE

- (Ritt) Let  $\mathcal{U}$  be an ordinary differential field, let  $r \in \mathbb{N}$ ,  $r \geq 4$ , and set  $A = y' - z^{(r-1)}y^2$ ,  $B = A^4 - (y^{(r-1)})^8$ ,  $C = y^{(r-1)}A' - 2y^{(r)}A$ ,  $F = B - y^6C^2$ .
  - Show that  $F$  is irreducible in  $\mathcal{U}\{y, z\}$  and that  $p_{\mathcal{U}}(F)$  contains a differential polynomial  $(z^{(2r-3)}y^d + Y$  with  $d > 0$  and  $Y \in [y]$ . (*Hint*: For the irreducibility observe that  $F$  is a quadratic polynomial in  $y^{(r)}$  with discriminant not a square. For the second point, note first that  $AB' - 4BA' = 4(y^{(r-1)})^7C$ . Replacing  $B$  here by  $y^6C^2 + F$ , conclude that  $2(y^{(r-1)})^7 - y^5(3y'AC + yAC' - 2yA'C) \in p_{\mathcal{U}}(F)$ . Next, using the notion of  $\mathfrak{k}$ -value (see Chapter 0, Section 19, and Chapter I, Section 7, corollary to Lemma 4) with  $\mathfrak{k}$  equal to the differential ideal  $([y] + p_{\mathcal{U}}(F))/p_{\mathcal{U}}(F)$  of the differential residue ring  $\mathcal{U}\{y, z\}/p_{\mathcal{U}}(F)$ , and writing  $o(P)$  for  $v_1(\bar{P})$ , where  $\bar{P}$  denotes the canonical image in  $\mathcal{U}\{y, z\}/p_{\mathcal{U}}(F)$  of an element  $P$  of  $\mathcal{U}\{y, z\}$ , show in succession that  $o(B) \geq 10$ ,  $o(A) \geq 2$ ,  $o(y') \geq 2$ ,  $o(C) \geq 4$ ,  $o(B) \geq 14$ ,  $o(A) \geq 7/2$ ,  $o(C) \geq 11/2$ ,  $o(B) \geq 17$ ,  $o(A) \geq 4$ ,  $o(C) \geq 6$ ,  $o(y^{(r-1)}) \geq 16/7$ ,  $o(y'' - z^{(r)}y^2) = o(A' + 2z^{(r-1)}yy') \geq 3$ ,  $o((z^{(r)}y^2)^{(r-3)}) \geq 16/7$ ,  $o(z^{(2r-3)}y^2) \geq 16/7$ . Finally, apply Levi's lemma.)
  - Show that if  $\zeta$  is any zero of  $z^{(2r-3)}$ , then  $F(y, \zeta)$  is irreducible in  $\mathcal{U}\{y\}$  and that 0 is a zero of  $p_{\mathcal{U}}(F(y, \zeta))$ . (*Hint*: The irreducibility can be proved as in (a). For the rest, use the substitution homomorphism

$f: \mathcal{U}\{y\} \rightarrow \mathcal{U}\{y\}$  ((c)) with  $f(y) = \sum_{1 \leq j \leq 6} (\zeta^{(r-2)})^{j-1} c^j + y c^6$ , show that  $J_{f(S_F(y, \zeta))} \notin \{J_{f(F(y, \zeta))}\}$ , and apply Section 16, Proposition 6.)  
 (c) Show that  $\{[y] + p_{\mathcal{U}}(F)\} = [y, z^{(2r-3)}]$ . (Hint: The inclusion “ $\supset$ ” follows from (a). For the inclusion “ $\subset$ ”, show that if  $G \in p_{\mathcal{U}}(F)$ , then  $G(y, \zeta) \in p_{\mathcal{U}}(F(y, \zeta))$  for every zero  $\zeta$  of  $z^{(2r-3)}$ , so that by (b),  $G(0, \zeta) = 0$ ; then apply Section 2, Theorem 1.)

18 Substitution of powers

Consider elements  $\eta_1, \dots, \eta_n \in \mathcal{U}$  and nonzero natural numbers  $e_1, \dots, e_n$ . It is obvious that if  $(0, \dots, 0)$  is a differential specialization of  $(\eta_1, \dots, \eta_n)$  over  $\mathcal{F}$ , then  $(0, \dots, 0)$  is also a differential specialization of  $(\eta_1^{e_1}, \dots, \eta_n^{e_n})$  over  $\mathcal{F}$ . The converse is not so obvious. We shall establish the converse as a corollary to a result of Levi on differential polynomial ideals (Proposition 11, below). But first a lemma.

**Lemma 9** *Let  $M$  be a differential monomial in  $y$  and let  $e \in \mathbb{N}$ ,  $e \neq 0$ . There exists a homogeneous and isobaric differential polynomial  $H_{M, e} \in \mathbb{Q}\{y\}$ , of degree and weight equal to the weight of  $M$ , such that  $y^{e \text{ wt}(M)} M(y) = y^{\text{deg}(M)} H_{M, e}(y^e)$ .*

*Proof* It evidently suffices to prove that for each derivative operator  $\theta \in \Theta$  there exists a homogeneous and isobaric  $H_{\theta, e} \in \mathbb{Q}\{y\}$ , of degree and weight equal to  $\text{ord } \theta$ , such that  $y^{e \text{ ord } \theta} \theta y = y H_{\theta, e}(y^e)$ . If  $\text{ord } \theta = 0$  (that is,  $\theta = 1$ ), we may take  $H_{1, e} = 1$ . If  $\text{ord } \theta > 0$ , so that  $\theta = \delta \theta'$  with  $\delta \in \Delta$  and  $\theta' \in \Theta$  and  $\text{ord } \theta' = \text{ord } \theta - 1$ , and if  $H_{\theta', e}$  exists, then

$$\begin{aligned} y^{e \text{ ord } \theta} \theta y &= y^{e \text{ ord } \theta} \delta (y^{1 - e \text{ ord } \theta'} H_{\theta', e}(y^e)) \\ &= y^{e \text{ ord } \theta} \delta (y^{1 + e - e \text{ ord } \theta'} H_{\theta', e}(y^e)) \\ &= (1 + e - e \text{ ord } \theta) e^{-1} y \delta (y^e) H_{\theta', e}(y^e) + y^{1 + e} \delta H_{\theta', e}(y^e), \end{aligned}$$

and we may take  $H_{\theta, e} = (1 + e - e \text{ ord } \theta) e^{-1} (\delta y) H_{\theta', e} + y \delta H_{\theta', e}$ .

**Proposition 11** (Levi [49, p. 559]) *Let  $e_1, \dots, e_n$  be nonzero natural numbers, and let  $f: \mathcal{F}\{y_1, \dots, y_n\} \rightarrow \mathcal{F}\{y_1, \dots, y_n\}$  denote the substitution homomorphism with  $f(y_j) = y_j^{e_j}$  ( $1 \leq j \leq n$ ). Let  $\mathfrak{p}$  be a prime differential ideal of  $\mathcal{F}\{y_1, \dots, y_n\}$  such that  $y_1 \cdots y_n \notin \mathfrak{p}$  and  $\mathfrak{p} \subset [y_1, \dots, y_n]$ . Then  $\{f(\mathfrak{p})\}$  has a component  $\mathfrak{p}'$  such that  $y_1 \cdots y_n \notin \mathfrak{p}'$  and  $\mathfrak{p}' \subset [y_1, \dots, y_n]$ .*

*Proof* Assume the conclusion false. Let  $p_i$  ( $i \in I$ ) denote the components of  $\{f(\mathfrak{p})\}$ , let  $I'$  denote the set of indices  $i \in I$  such that  $y_1 \cdots y_n \notin p_i$ , and set  $I'' = I - I'$ . By assumption, for each  $i \in I'$ ,  $p_i$  contains an element not

in  $[y_1, \dots, y_n]$ , that is, an element  $1 + Y_i$  with  $Y_i \in [y_1, \dots, y_n]$ . Set  $Y = \prod_{i \in I'} (1 + Y_i) - 1$ , so that  $Y \in [y_1, \dots, y_n]$  and  $1 + Y \in p_i$  ( $i \in I'$ ). Then  $y_1 \cdots y_n (1 + Y) \in \{f(\mathfrak{p})\}$  so that, for some  $s \in \mathbb{N}$ ,  $y_1^s \cdots y_n^s (1 + Y)^s \in [f(\mathfrak{p})]$ . Set  $Z = (1 + Y)^s - 1$ , so that  $Z \in [y_1, \dots, y_n]$  and  $y_1^s \cdots y_n^s (1 + Z) \in \mathcal{F}\{y_1, \dots, y_n\} f(\mathfrak{p})$ . Thus,  $y_1^s \cdots y_n^s (1 + Z)$  can be written as a sum of terms of the form  $M_1(y_1) \cdots M_n(y_n) f(P)$ , where  $M_j(y_j)$  is a differential monomial in  $y_j$  and  $P \in \mathfrak{p}$ . However, by Lemma 9,

$$y_j^{e_j \text{ wt}(M_j)} M_j(y_j) = y_j^{\text{deg}(M_j)} H_{M_j, e_j}(y_j^{e_j}).$$

Therefore if  $t \in \mathbb{N}$  is sufficiently big, we find, on multiplying by  $y_1^{e_1 t} \cdots y_n^{e_n t - s}$ , that  $y_1^{e_1 t} \cdots y_n^{e_n t} (1 + Z) \in \mathcal{F}[y_1, \dots, y_n] f(\mathfrak{p})$ . Finally, since  $y_j^{e_j} = f(y_j)$ , we find an equation

$$y_1^{e_1 t} \cdots y_n^{e_n t} (1 + Z) = \sum_{0 \leq i_1 < e_1, \dots, 0 \leq i_n < e_n} y_1^{i_1} \cdots y_n^{i_n} f(P_{i_1, \dots, i_n}), \tag{8}$$

where  $P_{i_1, \dots, i_n} \in \mathfrak{p}$  for every  $(i_1, \dots, i_n)$ .

Every nonzero term in  $Z$  can be written in the form  $b N_1(y_1) \cdots N_n(y_n)$ , where  $b \in \mathcal{F}$  and  $N_j(y_j)$  is a differential monomial in  $y_j$ . Writing  $\text{deg } N_j(y_j) = q_j e_j + r_j$  with  $q_j, r_j \in \mathbb{N}$  and  $r_j < e_j$ , we find by Lemma 9 that

$$\begin{aligned} y_j^{e_j t} N_j(y_j) &= y_j^{e_j t + q_j e_j + r_j - e_j \text{ wt } N_j} H_{N_j, e_j}(y_j^{e_j}) \\ &= y_j^t f(y_j^{t + q_j - \text{wt } N_j} H_{N_j, e_j}(y_j)), \end{aligned}$$

where we have supposed, as permitted, that  $t$  has been chosen so big that  $t + q_j - \text{wt } N_j \geq 0$  ( $1 \leq j \leq n$ ) for every nonzero term  $b N_1(y_1) \cdots N_n(y_n)$  in  $Z$ . We observe that if  $r_j = 0$ , then either  $q_j > 0$ , whence

$$\text{deg } y_j^{t + q_j - \text{wt } N_j} H_{N_j, e_j}(y_j) > t,$$

or else  $q_j = 0$ , whence  $\text{deg } N_j = 0$  and  $\text{wt } N_j = 0$  so that  $y_j^{t + q_j - \text{wt } N_j} H_{N_j, e_j}(y_j)$  is a multiple of  $y_j^t$ . In other words, if  $r_j = 0$ , then  $y_j^{t + q_j - \text{wt } N_j} H_{N_j, e_j}(y_j)$  dominates  $y_j^t$ . Referring to (8), we find an equation

$$\begin{aligned} f(y_1^t \cdots y_n^t) + \sum_{0 \leq i_1 < e_1, \dots, 0 \leq i_n < e_n} y_1^{i_1} \cdots y_n^{i_n} f(H_{i_1, \dots, i_n}) \\ = \sum_{0 \leq i_1 < e_1, \dots, 0 \leq i_n < e_n} y_1^{i_1} \cdots y_n^{i_n} f(P_{i_1, \dots, i_n}), \end{aligned} \tag{9}$$

where  $H_{i_1, \dots, i_n} \in \mathcal{F}\{y_1, \dots, y_n\}$  for every  $(i_1, \dots, i_n)$ , and each term of  $H_{0, \dots, 0}$  dominates  $y_1^t \cdots y_n^t$ .

We claim that the family  $(y_1^{i_1} \cdots y_n^{i_n})_{0 \leq i_1 < e_1, \dots, 0 \leq i_n < e_n}$  is linearly independent over the ring  $f(\mathcal{F}\{y_1, \dots, y_n\}) = \mathcal{F}\{y_1^{e_1}, \dots, y_n^{e_n}\}$ . Indeed, if  $F_{i_1, \dots, i_n} \in \mathcal{F}\{y_1, \dots, y_n\}$  ( $0 \leq i_1 < e_1, \dots, 0 \leq i_n < e_n$ ) and

$$\sum_{0 \leq i_1 < e_1, \dots, 0 \leq i_n < e_n} y_1^{i_1} \cdots y_n^{i_n} F_{i_1, \dots, i_n}(y_1^{e_1}, \dots, y_n^{e_n}) = 0,$$

then the differential polynomial on the left has the property that all its terms that, for each  $j$ , have degree in  $(\theta y_j)_{\theta \in \mathfrak{e}}$  congruent (mod  $e_j$ ) to a given  $r_j < e_j$ , add up to 0, that is,  $y_1^{r_1} \cdots y_n^{r_n} F_{r_1, \dots, r_n}(y_1^{e_1} \cdots y_n^{e_n}) = 0$ . Since this is so for every choice of  $(r_1, \dots, r_n)$ , the claim is established.

This being the case, we infer from (9) that

$$f(y_1^t \cdots y_n^t) + f(H_{0 \dots 0}) = f(P_{0 \dots 0}).$$

Since the homomorphism  $f$  is injective (because  $y_1^{e_1}, \dots, y_n^{e_n}$  are differentially algebraically independent over  $\mathcal{F}$ ), this implies that

$$y_1^t \cdots y_n^t + H_{0 \dots 0} = P_{0 \dots 0}.$$

As  $P_{0 \dots 0} \in \mathfrak{p}$  and  $y_1^t \cdots y_n^t$  is dominated by every nonzero term in  $H_{0 \dots 0}$ , it follows from the domination lemma that  $\mathfrak{p}$  contains a differential polynomial  $y_1 \cdots y_n(1+X)$  where  $X \in [y_1, \dots, y_n]$ . Hence either  $y_1 \cdots y_n \in \mathfrak{p}$  or  $\mathfrak{p} \not\subset [y_1, \dots, y_n]$ . This contradicts the hypothesis, and completes the proof.

**Corollary** Let  $\eta_1, \dots, \eta_n \in \mathcal{U}$ , and let  $e_1, \dots, e_n \in \mathbb{N}$  and  $e_1 \cdots e_n \neq 0$ . If  $(0, \dots, 0)$  is a differential specialization of  $(\eta_1^{e_1}, \dots, \eta_n^{e_n})$  over  $\mathcal{F}$ , then  $(0, \dots, 0)$  is a differential specialization of  $(\eta_1, \dots, \eta_n)$  over  $\mathcal{F}$ .

*Proof* We evidently may suppose that  $\eta_j \neq 0$  ( $1 \leq j \leq n$ ). Let  $\mathfrak{p}$  denote the defining differential ideal of  $(\eta_1^{e_1}, \dots, \eta_n^{e_n})$  in  $\mathcal{F}\{y_1, \dots, y_n\}$ . Then  $y_1 \cdots y_n \notin \mathfrak{p}$  and  $\mathfrak{p} \subset [y_1, \dots, y_n]$ . For each  $\varepsilon = (\varepsilon_1, \dots, \varepsilon_n)$  such that  $\varepsilon_j$  is an  $e_j$ th root of 1 ( $1 \leq j \leq n$ ), let  $\mathfrak{q}_\varepsilon$  denote the defining differential ideal of  $(\varepsilon_1 \eta_1, \dots, \varepsilon_n \eta_n)$  in  $\mathcal{F}\{y_1, \dots, y_n\}$ . Obviously  $y_1 \cdots y_n \notin \mathfrak{q}_\varepsilon$ . Let  $f: \mathcal{F}\{y_1, \dots, y_n\} \rightarrow \mathcal{F}\{y_1, \dots, y_n\}$  denote the same homomorphism as in Proposition 11. For any  $P \in \mathcal{F}\{y_1, \dots, y_n\}$  it is clear that  $P$  vanishes at  $(\eta_1^{e_1}, \dots, \eta_n^{e_n})$  if and only if  $f(P)$  vanishes at  $(\varepsilon_1 \eta_1, \dots, \varepsilon_n \eta_n)$ , so that  $P \in \mathfrak{p}$  if and only if  $f(P) \in \mathfrak{q}_\varepsilon$ . It follows that

$$f(\mathfrak{p}) = \mathcal{F}\{y_1^{e_1}, \dots, y_n^{e_n}\} \cap \mathfrak{q}_\varepsilon. \tag{10}$$

Consider any  $G \in \bigcap_\varepsilon \mathfrak{q}_\varepsilon$ . We can write  $G = \sum b M_1(y_1) \cdots M_n(y_n)$ , where in each term  $b \in \mathcal{F}$ ,  $b \neq 0$ , and  $M_j(y_j)$  is a differential monomial in  $y_j$  ( $1 \leq j \leq n$ ), and where distinct terms have distinct  $(M_1(y_1), \dots, M_n(y_n))$ . By Lemma 9,

$$M_j(y_j) = y_j^{\deg(M_j) - e_j \text{wt}(M_j)} H_{M_j, e_j}(y_j^{e_j}).$$

Writing  $\deg(M_j) = q_j e_j + r_j$ , with  $q_j, r_j \in \mathbb{N}$  and  $r_j < e_j$ , and choosing sufficiently big  $t \in \mathbb{N}$ , we find that

$$y_j^{e_j t} M_j(y_j) = y_j^{e_j(t + q_j - \text{wt}(M_j))} H_{M_j, e_j}(y_j^{e_j}) y_j^{r_j},$$

with  $t + q_j - \text{wt}(M_j) \geq 0$  ( $1 \leq j \leq n$ ) for every term in  $G$ . Hence we may write

$$y_1^{e_1 t} \cdots y_n^{e_n t} G = \sum_{0 \leq r_1 < e_1, \dots, 0 \leq r_n < e_n} F_{r_1, \dots, r_n}(y_1^{e_1}, \dots, y_n^{e_n}) y_1^{r_1} \cdots y_n^{r_n},$$

where  $F_{r_1, \dots, r_n} \in \mathcal{F}\{y_1, \dots, y_n\}$  for each  $(r_1, \dots, r_n)$ . Since  $G \in \bigcap_\varepsilon \mathfrak{q}_\varepsilon$ , this implies that

$$\sum_{0 \leq r_1 < e_1, \dots, 0 \leq r_n < e_n} F_{r_1, \dots, r_n}(\eta_1^{e_1}, \dots, \eta_n^{e_n}) \eta_1^{r_1} \cdots \eta_n^{r_n} \varepsilon_1^{r_1} \cdots \varepsilon_n^{r_n} = 0$$

for every  $\varepsilon = (\varepsilon_1, \dots, \varepsilon_n)$  with  $\varepsilon_j$  an  $e_j$ th root of 1 ( $1 \leq j \leq n$ ). However, if  $\mathbf{P}_\varepsilon$  denotes the group of  $e$ th roots of 1, the matrix  $(\rho^r)_{\rho \in \mathbf{P}_\varepsilon, 0 \leq r < e}$  is invertible (it has a Vandermonde determinant). Applying this remark successively to  $\mathbf{P}_{e_n}, \mathbf{P}_{e_{n-1}}, \dots, \mathbf{P}_{e_1}$ , we infer from the last equations that

$$F_{r_1, \dots, r_n}(\eta_1^{e_1}, \dots, \eta_n^{e_n}) = 0 \quad (0 \leq r_1 < e_1, \dots, 0 \leq r_n < e_n),$$

so that  $F_{r_1, \dots, r_n} \in \mathfrak{p}$  for every  $(r_1, \dots, r_n)$ . This shows that for each  $G \in \bigcap_\varepsilon \mathfrak{q}_\varepsilon$  there exists a  $t \in \mathbb{N}$  such that  $y_1^{e_1 t} \cdots y_n^{e_n t} G \in \{f(\mathfrak{p})\}$ . It follows, because of (10), that

$$\bigcap_\varepsilon \mathfrak{q}_\varepsilon = \{f(\mathfrak{p})\} : y_1 \cdots y_n.$$

By Proposition 11, some component  $\mathfrak{p}'$  of  $\{f(\mathfrak{p})\}$  satisfies the two conditions  $y_1 \cdots y_n \notin \mathfrak{p}'$  and  $\mathfrak{p}' \subset [y_1, \dots, y_n]$ . Because of the former condition,  $\mathfrak{p}'$  is a component of  $\{f(\mathfrak{p})\} : y_1 \cdots y_n$ , and hence  $\mathfrak{p}' = \mathfrak{q}_\varepsilon$  for some  $\varepsilon$ . Thus, for this  $\varepsilon$ ,  $\mathfrak{q}_\varepsilon \subset [y_1, \dots, y_n]$ . This means that  $(0, \dots, 0)$  is a zero of  $\mathfrak{q}_\varepsilon$ , that is, that  $(0, \dots, 0)$  is a differential specialization of  $(\varepsilon_1 \eta_1, \dots, \varepsilon_n \eta_n)$  over  $\mathcal{F}$ , or equivalently, that there exists a homomorphism  $\mathcal{F}\{\varepsilon_1 \eta_1, \dots, \varepsilon_n \eta_n\} \rightarrow \mathcal{U}$  over  $\mathcal{F}$  with  $\varepsilon_j \eta_j \mapsto 0$  ( $1 \leq j \leq n$ ). Let  $\mathcal{F}' = \mathcal{F}\langle \varepsilon_1, \dots, \varepsilon_n \rangle$ . Evidently  $\mathcal{F}' = \mathcal{F}[\varepsilon_1, \dots, \varepsilon_n]$ , so that  $\mathcal{F}'\{\varepsilon_1 \eta_1, \dots, \varepsilon_n \eta_n\}$  is an integral overring of  $\mathcal{F}\{\varepsilon_1 \eta_1, \dots, \varepsilon_n \eta_n\}$ . Hence (by Chapter 0, Section 14, Proposition 9(a)) the above homomorphism can be extended to a homomorphism  $\mathcal{F}'\{\varepsilon_1 \eta_1, \dots, \varepsilon_n \eta_n\} \rightarrow \mathcal{U}$ . This latter homomorphism must, for each  $j$ , map  $\varepsilon_j$  onto an element  $\varepsilon_j'$  conjugate to  $\varepsilon_j$  over  $\mathcal{F}$ , and hence is a differential homomorphism. As it maps the element  $\eta_j = \varepsilon_j^{e_j - 1} \cdot \varepsilon_j \eta_j$  onto the element  $\varepsilon_j'^{e_j - 1} \cdot 0 = 0$ , we conclude that  $(0, \dots, 0)$  is a differential specialization of  $(\eta_1, \dots, \eta_n)$  over  $\mathcal{F}$ .

## Bibliography for Chapters I–IV

1. C. I. Andreian. Inele diferențiale, *Acad. R. P. Romine. Bul. Ști. Sect. Ști. Mat. Fiz.* 3 (1951), 319–332.
2. J. Ax. On Shenuel's conjectures, *Ann. of Math.* 93 (1971), 252–268.
3. A. Babakhanian. On primitive elements in differentially algebraic extension fields, *Trans. Amer. Math. Soc.* 134 (1968), 71–83.
4. R. Baer. Algebraische Theorie der differentiiierbaren Funktionenkörper, *S.-B. Heidelberger Akad. Wiss. Math-Natur. Kl.*, 1927, 8. Abh., 15–32.
5. P. Blum. Complete models of differential fields, *Trans. Amer. Math. Soc.* 137 (1969), 309–325.
6. P. Blum. Extending differential specializations, *Proc. Amer. Math. Soc.* 24 (1970), 471–474.
7. P. Blum. Rational functions on differential closed sets, *Amer. J. Math.* 94 (1972), 676–684.
8. S. Böge. Algebraische Beweis eines Satzes von Ritt aus der Theorie der algebraischen Differentialgleichungen, *Arch. Math. (Basel)* 19 (1968), 125–130.
9. J. Brzezinski. On differentially integral elements, *Bull. Acad. Polon. Sci. Sér. Sci. Math. Astronom. Phys.* 10 (1962), 325–328.
10. P. J. Cassidy. Differential algebraic groups, *Amer. J. Math.* 94 (1972), 891–954.
11. R. M. Cohn. On the analog for differential equations of the Hilbert–Netto theorem, *Bull. Amer. Math. Soc.* 47 (1941), 268–270.
- 11a. J. Cozzens and J. Johnson. Some applications of differential algebra to ring theory, *Proc. Amer. Math. Soc.* 31 (1972), 354–356.
12. G. Dahmen. Zur Theorie der Differentialpolynome I, *Ann. Univ. Sarav. Sci.* 6 (1957), 311–323.
13. G. Dahmen. Zur Theorie der Differentialpolynome II, *Ann. Univ. Sarav. Sci.* 6 (1957), 323–336.
14. L. Goldman. Algebraic structure of the manifold of solutions of the  $N$ -body problem, *Proc. Amer. Math. Soc.* 25 (1970), 417–422.

- 14a. H. E. Gorman. Differential rings and modules, *Scripta Math.*, to appear.
- 14b. H. E. Gorman. Radical regularity in differential rings, *Canad. J. Math.* 23 (1971), 197–201.
- 14c. H. E. Gorman. Zero divisors in differential rings, *Pacific J. Math.* 39 (1971), 163–171.
15. E. Gourin. On irreducible systems of algebraic differential equations, *Bull. Amer. Math. Soc.* 39 (1933), 593–595.
16. S. Halfin and A. Robinson. Local partial differential algebra, *Trans. Amer. Math. Soc.* 109 (1963), 165–180.
17. J.-C. Herz. Sur les systèmes de polynomes différentiels, *C. R. Acad. Sci. Paris* 235 (1952), 1085–1087.
18. A. P. Hillman. A note on differential polynomials, *Bull. Amer. Math. Soc.* 49 (1943), 711–712.
19. A. P. Hillman. On the differential algebra of a single differential polynomial, *Ann. of Math.* 56 (1952), 157–168.
20. A. P. Hillman and D. G. Mead. On the Ritt polygon process, *Amer. J. Math.* 84 (1962), 629–634.
21. A. P. Hillman, D. G. Mead, K. B. O'Keefe, and E. S. O'Keefe. Ideals generated by products, *Proc. Amer. Math. Soc.* 17 (1966), 717–719.
22. A. P. Hillman, D. G. Mead, K. B. O'Keefe and E. S. O'Keefe. A dynamical programming generalization of  $xy$  to  $n$  variables, *Proc. Amer. Math. Soc.* 17 (1966), 720–723.
23. A. Jaeger. Eine algebraische Theorie vertauschbarer Differentiationen für Körper beliebiger Charakteristik, *J. Reine Angew. Math.* 190 (1952), 1–21.
24. A. Jaeger. Gewöhnliche Differentialgleichungen in Körper von Primzahlcharakteristik, *Monatsh. Math.* 56 (1952), 181–219.
25. A. Jaeger. Partielle Differentialgleichungen in Körper von Primzahlcharakteristik, *Monatsh. Math.* 56 (1952), 266–287.
26. A. Jaeger. Die Riccatische Differentialgleichungen in Körpern der Charakteristik 2, *Arch. Math. (Basel)* 5 (1954), 423–428.
27. A. Jaeger. On partial differential equations in a field of prime characteristic, *Canad. J. Math.* 7 (1955), 539–542.
28. A. Jaeger. A representation of multidifferential polynomials in a field of prime characteristic, *Math. Ann.* 130 (1955), 1–6.
29. A. Jaeger. A relation between adjoint multidifferential polynomials and transposed matrices for fields of prime characteristic, *Math. Ann.* 130 (1955), 7–10.
30. J. Johnson. Differential dimension polynomials and a fundamental theorem on differential modules, *Amer. J. Math.* 91 (1969), 239–248.
31. J. Johnson. Kähler differentials and differential algebra, *Ann. of Math.* 89 (1969), 92–98.
32. J. Johnson. A notion of Krull dimension for differential rings, *Comment. Math. Helv.* 44 (1969), 207–216.
33. I. Kaplansky. "An Introduction to Differential Algebra." Hermann, Paris, 1957.
34. F. Kasch. Über die Riccatische Differentialgleichung in Körpern der Charakteristik  $p$ , *Arch. Math. (Basel)* 4 (1953), 17–22.
35. E. R. Kolchin. On the basis theorem for infinite systems of differential polynomials, *Bull. Amer. Math. Soc.* 45 (1939), 923–926.
36. E. R. Kolchin. On the exponents of differential ideals, *Ann. of Math.* 42 (1941), 740–777.

37. E. R. Kolchin. On the basis theorem for differential systems, *Trans. Amer. Math. Soc.* **52** (1942), 115-127.
38. E. R. Kolchin. Extensions of differential fields I, *Ann. of Math.* **43** (1942), 724-729.
39. E. R. Kolchin. Extensions of differential fields II, *Ann. of Math.* **45** (1944), 358-361.
40. E. R. Kolchin. Extensions of differential fields III, *Bull. Amer. Math. Soc.* **53** (1947), 397-401.
41. E. R. Kolchin. Rational approximation to solutions of algebraic differential equations, *Proc. Amer. Math. Soc.* **10** (1959), 238-244.
42. E. R. Kolchin. Le théorème de la base finie pour les polynômes différentiels, *Sémin. Dubreil-Pisot* **14**, 1960/1961, No. 7. Secrétariat Mathématique, Paris, 1963.
43. E. R. Kolchin. The notion of dimension in the theory of algebraic differential equations, *Bull. Amer. Math. Soc.* **70** (1964), 570-573.
44. E. R. Kolchin. Singular solutions of algebraic differential equations and a lemma of Arnold Shapiro, *Topology* **3** (1965), *Suppl.* **2**, 309-318.
45. E. R. Kolchin. Some problems in differential algebra, *Proc. Int. Congr. Math. (Moscow-1966)*, pp. 269-276. Moscow, 1968.
46. J. Kovacic. An Eisenstein criterion for noncommutative polynomials, *Proc. Amer. Math. Soc.* **34** (1972), 25-29.
47. F. Kuiper. On algebraic independence in differential rings, *Proc. Kon. Ned. Akad. Wetensch. Ser. A* **67** [= *Indag. Math.* **26**] (1964), 90-103.
48. B. A. Lando. Jacobi's bound for the order of systems of first order differential equations, *Trans. Amer. Math. Soc.* **152** (1970), 119-135.
- 48a. Y. Lequain. Differential simplicity and complete integral closure, *Pacific J. Math.* **36** (1971), 741-751.
49. H. Levi. On the structure of differential polynomials and on their theory of ideals, *Trans. Amer. Math. Soc.* **51** (1942), 532-568.
50. H. Levi. The low power theorem for partial differential polynomials, *Ann. of Math.* **46** (1945), 113-119.
51. D. G. Mead. Differential ideals, *Proc. Amer. Math. Soc.* **6** (1955), 420-432.
52. D. G. Mead. Sublinear differential polynomials, *Trans. Amer. Math. Soc.* **95** (1960), 124-136.
53. D. G. Mead. A note on the ideal  $[uw]$ , *Proc. Amer. Math. Soc.* **14** (1963), 607-608.
54. D. G. Mead. A necessary and sufficient condition for membership in  $[uw]$ , *Proc. Amer. Math. Soc.* **17** (1966), 470-473.
55. D. G. Mead and B. D. McLemore. Ritt's question on the Wronskian, *Pacific J. Math.* **35** (1970), 467-472.
56. J. G. Mikusiński. Sur la dérivée algébrique, *Fund. Math.* **40** (1953), 99-105.
- 56a. M. E. Newton. The differential ideals  $[y^#z]$ , *Proc. Amer. Math. Soc.* **30** (1971), 229-234.
57. H. Nishimura. On differentially integral elements, *Proc. Japan Acad.* **40** (1964), 145-149.
58. K. B. O'Keefe. A property of the differential ideal  $[y^#]$ , *Trans. Amer. Math. Soc.* **94** (1960), 483-497.
59. K. B. O'Keefe. A symmetry theorem for the differential ideal  $[uw]$ , *Proc. Amer. Math. Soc.* **12** (1961), 654-657.
60. K. B. O'Keefe. Unusual power products in the ideal  $[y^2]$ , *Proc. Amer. Math. Soc.* **17** (1966), 757-758.
61. K. B. O'Keefe. On a problem of J. F. Ritt, *Pacific J. Math.* **17** (1966), 149-157.
62. K. B. O'Keefe and E. S. O'Keefe. The differential ideal  $[uw]$ , *Proc. Amer. Math. Soc.* **17** (1966), 750-757.

63. K. Okugawa. Basis theorem concerning differential polynomials, *Mem. Coll. Sci. Univ. Kyoto Ser. A* **25** (1949), 93-97.
64. K. Okugawa. On the rings with derivations, *Math. Japon.* **1** (1949), 152-163.
65. K. Okugawa. Basis theorem for D-polynomials, *Math. Japon.* **2** (1950), 35-39.
66. K. Okugawa. Extensions of the ground field in the theory of algebraic differential equations, *Mem. Coll. Sci. Univ. Kyoto Ser. A* **27** (1953), 257-265.
67. K. Okugawa. On differential algebra of arbitrary characteristic, *Mem. Coll. Sci. Univ. Kyoto Ser. A* **28** (1953), 97-107.
68. K. Okugawa. Basic properties of differential fields of an arbitrary characteristic and the Picard-Vessiot theory, *J. Math. Kyoto Univ.* **2** (1963), 295-322.
- 68a. O. Ore. Formale Theorie der linearen Differentialgleichungen, I, *J. Reine Angew. Math.* **167** (1932), 221-234.
- 68b. O. Ore. Formale Theorie der linearen Differentialgleichungen, II, *J. Reine Angew. Math.* **168** (1933), 233-252.
- 68c. C. F. Osgood. An effective lower bound on the "Diophantine approximation" of algebraic functions by rational functions, *Mathematika*, to appear.
69. E. C. Posner. Differentiably simple rings, *Proc. Amer. Math. Soc.* **11** (1960), 337-343.
70. E. C. Posner. Integral closure of differential rings, *Pacific J. Math.* **10** (1960), 1393-1396.
71. E. C. Posner. Integral closure of rings of solutions of linear differential equations, *Pacific J. Math.* **12** (1962), 1417-1422.
72. H. W. Raudenbush, Jr. Differential fields and ideals of differential forms, *Ann. of Math.* **34** (1933), 509-517.
73. H. W. Raudenbush, Jr. Ideal theory and algebraic differential equations, *Trans. Amer. Math. Soc.* **36** (1934), 361-368.
74. H. W. Raudenbush, Jr. Hypertranscendental adjunctions to partial differential fields, *Bull. Amer. Math. Soc.* **40** (1934), 714-720.
75. H. W. Raudenbush, Jr. On the analog for differential equations of the Hilbert-Netto theorem, *Bull. Amer. Math. Soc.* **42** (1936), 371-373.
76. R. H. Risch. The problem of integration in finite terms, *Trans. Amer. Math. Soc.* **139** (1969), 167-189.
77. R. H. Risch. The solution of the problem of integration in finite terms, *Bull. Amer. Math. Soc.* **76** (1970), 605-608.
78. J. F. Ritt. Transcendental transcendency of certain functions of Poincaré, *Math. Ann.* **95** (1926), 671-682.
79. J. F. Ritt. Manifolds of functions defined by systems of algebraic differential equations, *Trans. Amer. Math. Soc.* **32** (1930), 569-598.
80. J. F. Ritt. Systems of algebraic differential equations, *Proc. Nat. Acad. Sci. U.S.A.* **17** (1931), 366-368.
81. J. F. Ritt. "Differential Equations from the Algebraic Standpoint," Amer. Math. Soc. Colloq. Publ., Vol. 14. Amer. Math. Soc., New York, 1932.
82. J. F. Ritt. Systems of algebraic differential equations, *Ann. of Math.* **36** (1935), 293-302.
83. J. F. Ritt. Jacobi's problem on the order of a system of differential equations, *Ann. of Math.* **36** (1935), 303-312.
84. J. F. Ritt. Indeterminate expressions involving an analytic function and its derivatives, *Monatsh. Math.* **43** (1936), 97-104.
85. J. F. Ritt. On the singular solutions of algebraic differential equations, *Ann. of Math.* **37** (1936), 552-617.

86. J. F. Ritt. On certain points in the theory of algebraic differential equations, *Amer. J. Math.* **60** (1938), 1-43.
87. J. F. Ritt. Algebraic aspects of the theory of differential equations, *Amer. Math. Soc. Semicentennial Pubs., Vol. II, Semicentennial Addresses*, pp. 35-55. Amer. Math. Soc., New York, 1938.
88. J. F. Ritt. On ideals of differential polynomials, *Proc. Nat. Acad. Sci. U.S.A.* **25** (1939), 90-91.
89. J. F. Ritt. On the intersections of algebraic differential manifolds, *Proc. Nat. Acad. Sci. U.S.A.* **25** (1939), 214-215.
90. J. F. Ritt. On the intersections of irreducible components in the manifold of a differential polynomial, *Proc. Nat. Acad. Sci. U.S.A.* **26** (1940), 354-356.
91. J. F. Ritt. On a type of algebraic differential manifold, *Trans. Amer. Math. Soc.* **48** (1940), 542-552.
92. J. F. Ritt. Bezout's theorem and algebraic differential equations, *Trans. Amer. Math. Soc.* **53** (1943), 74-82.
93. J. F. Ritt. On the manifolds of partial differential polynomials, *Ann. of Math.* **46** (1945), 102-112.
94. J. F. Ritt. "Integration in Finite Terms." Columbia Univ. Press, New York, 1948.
95. J. F. Ritt. "Differential Algebra." Amer. Math. Soc. Colloq. Publ., Vol. 33. Amer. Math. Soc., New York, 1950.
96. J. F. Ritt. Associative differential operations, *Ann. of Math.* **51** (1950), 756-765.
97. J. F. Ritt. Differential groups and formal Lie theory for an infinite number of parameters, *Ann. of Math.* **52** (1950), 708-726.
98. J. F. Ritt. Differential groups of order two, *Ann. of Math.* **53** (1951), 491-519.
99. J. F. Ritt. Subgroups of differential groups, *Ann. of Math.* **54** (1951), 110-146.
100. J. F. Ritt. Differential groups, *Proc. Int. Congr. Math., 1950*, Vol. I, pp. 207-208. Amer. Math. Soc., Providence, Rhode Island, 1952.
101. J. F. Ritt and E. Gourin. An assemblage-theoretic proof of the existence of transcendently transcendental functions, *Bull. Amer. Math. Soc.* **33** (1927), 182-184.
102. J. F. Ritt and E. R. Kolchin. On certain ideals of differential polynomials, *Bull. Amer. Math. Soc.* **45** (1939), 895-898.
103. A. Robinson. On the concept of differentially closed field, *Bull. Res. Council. Isr. Sect. F* **8** (1959), 113-128.
104. A. Robinson. Local differential algebra, *Trans. Amer. Math. Soc.* **97** (1960), 427-456.
- 104a. A. Robinson. "Introduction to Model Theory and the Metamathematics of Algebra," pp. 132-137 and 209-214. North-Holland Publ., Amsterdam, 1963.
105. A. Rosenfeld. Specializations in differential algebra, *Trans. Amer. Math. Soc.* **90** (1959), 394-407.
106. M. Rosenlicht. Liouville's theorem on functions with elementary integrals, *Pacific J. Math.* **24** (1968), 153-161.
107. M. Rosenlicht. On the explicit solvability of certain transcendental equations, *Inst. Haute Etudes Sci. Publ. Math.* **36** (1969), 15-22.
- 107a. G. E. Sacks. The differential closure of a differential field, *Bull. Amer. Math. Soc.* **78** (1972), 629-634.
108. A. Seidenberg. Some basic theorems in differential algebra (characteristic  $p$ , arbitrary), *Trans. Amer. Math. Soc.* **73** (1952), 174-190.
109. A. Seidenberg. On separating transcendency bases for differential fields, *Proc. Amer. Math. Soc.* **6** (1955), 726-728.
110. A. Seidenberg. An elimination theory for differential algebra, *Univ. Calif. Publ. Math. (N.S.)* **3** (1956), 31-66.

111. A. Seidenberg. Abstract differential algebra and the analytic case, *Proc. Amer. Math. Soc.* **9** (1958), 159-164.
112. A. Seidenberg. Some basic theorems in partial differential algebra, *Mem. Coll. Sci. Univ. Kyoto Ser. A* **31** (1958), 1-8.
113. A. Seidenberg. Derivations and integral closure, *Pacific J. Math.* **16** (1966), 167-173.
114. A. Seidenberg. Differential ideals in rings of finitely generated type, *Amer. J. Math.* **89** (1967), 22-42.
115. A. Seidenberg. Abstract differential algebra and the analytic case II, *Proc. Amer. Math. Soc.* **23** (1969), 689-691.
116. W. C. Strodt. Irreducible systems of algebraic differential equations, *Trans. Amer. Math. Soc.* **45** (1939), 276-297.
117. I. Zuckerman. A new measure of a partial differential field extension, *Pacific J. Math.* **15** (1965), 357-371.

## CHAPTER V

## Algebraic Groups

*In this chapter  $U$  denotes a field, fixed once for all and called the universal field, that is algebraically closed and of infinite transcendence degree over its prime field. The characteristic of  $U$  is denoted by  $p$ . All fields introduced, except those for which the contrary is stated or is obvious, are tacitly assumed to be subfields of  $U$  over which the transcendence degree of  $U$  is infinite. This applies, in particular, to the field of quotients of a subring of  $U$ . For any field  $K$ , the algebraic closure of  $K$  is denoted by  $K_a$ , the separable closure of  $K$  is denoted by  $K_s$ , and the smallest perfect field containing  $K$  is denoted by  $K_1$ . The group of automorphisms of  $U$  over  $K$  is denoted by  $\text{Aut}(U|K)$ . We permit ourselves (in this chapter only) to write "extension" instead of "field extension."*

## 1 Introduction

The purpose of the present chapter is to develop the theory of algebraic groups in a form and to an extent suitable for its application, in the final chapter, to the Galois theory of differential fields.

An algebraic group is an algebraic set (that is, a not necessarily irreducible algebraic variety) on which there is given a group structure for which the group law  $(x, y) \mapsto xy$  and the group symmetry  $x \mapsto x^{-1}$  are rational mappings. An algebraic group is said to be *defined over* a given field  $K$  if  $K$  is a field of definition of the algebraic set and of the two rational mappings.

For example, the universal field  $U$  has a natural structure of algebraic

set (one-dimensional affine space) and a natural group structure (the additive group of  $U$ ). Since the mappings defined by the formulae  $(x, y) \mapsto x + y$  and  $x \mapsto -x$  are rational, we have an algebraic group; it is sometimes denoted by  $G_a$  ("additive group"). Similarly, the set  $U^* = U - \{0\}$  is an algebraic set and is a group (the multiplicative group of the field  $U$ ). Since the mappings defined by the formulae  $(x, y) \mapsto xy$  and  $x \mapsto x^{-1}$  are rational, we have an algebraic group; it is sometimes denoted by  $G_m$  ("multiplicative group"). More complicated examples are obtained by considering the set of all invertible square matrices over  $U$  of a given degree  $n$ . This set has a natural structure of algebraic set (affine space  $U^{n^2}$  minus the hypersurface with equation  $\det(X_{ij})_{1 \leq i \leq n, 1 \leq j \leq n} = 0$ ) and has a natural group structure (the group law being matrix multiplication in the usual sense). Since matrix multiplication and matrix inversion are rational mappings, we have an algebraic group; it is often denoted by  $\text{GL}(n)$  ("general linear group" of degree  $n$ ). All the algebraic groups  $G_a$ ,  $G_m$ ,  $\text{GL}(n)$  are defined over the prime field.

If  $G$  is any subgroup of  $\text{GL}(n)$  and if there exists a set  $\Sigma$  of polynomials  $P \in K[(X_{ij})]$  such that an element  $(x_{ij})$  of  $\text{GL}(n)$  is in  $G$  if and only if  $P((x_{ij})) = 0$  ( $P \in \Sigma$ ), then  $G$  is an algebraic group. When the perfect ideal of  $K[(X_{ij})]$  consisting of all polynomials that vanish on  $G$  is separable over  $K$ , then  $G$  is defined over  $K$ . For example, the special linear group  $\text{SL}(n)$  (given by the equation  $\det(X_{ij}) - 1 = 0$ ), the orthogonal group  $\text{O}(n)$  (given by the equations

$$\sum_{1 \leq v \leq n} X_{iv} X_{jv} = 0 \quad (1 \leq i < j \leq n) \quad \text{and} \quad \sum_{1 \leq v \leq n} X_{jv}^2 - 1 = 0 \quad (1 \leq j \leq n),$$

the triangular group  $\text{T}(n)$  (given by the equations  $X_{ij} = 0$  ( $1 \leq j < i \leq n$ )), for each  $k \in \mathbb{N}$  with  $1 \leq k \leq n$  the subgroup  $\text{T}(n, k)$  of  $\text{T}(n)$  (given by the equations  $X_{ij} = 0$  ( $1 \leq j < i \leq n$ ),  $X_{jj} - 1 = 0$  ( $1 \leq j \leq n$ ),  $X_{ij} = 0$  ( $1 \leq i < j < i + k$ )), and the diagonal group  $\text{D}(n)$  (given by the equations  $X_{ij} = 0$  ( $i \neq j$ )) are all algebraic groups defined over the prime field. Of course  $G_m$ ,  $\text{GL}(1)$ ,  $\text{T}(1)$ ,  $\text{D}(1)$  all are the same algebraic group. Also, the formula  $x \mapsto \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$  defines a birational isomorphism  $G_a \approx \text{T}(2, 1)$ .

Some algebraic groups are not birationally isomorphic to an algebraic group of matrices. The most accessible examples are provided by elliptic curves. Suppose for the sake of simplicity that  $p \neq 2$ , and fix elements  $g_2, g_3 \in U$  with  $g_2^3 - 27g_3^2 \neq 0$ . Sixteen times this expression is the discriminant of the polynomial  $4X^3 - g_2X - g_3$ , so that the condition here means that this polynomial has no root in common with its derivative  $12X^2 - g_2$ . Setting

$$P = X_0 X_2^2 - (4X_1^3 - g_2 X_0^2 X_1 - g_3 X_0^3),$$

we see that  $P$  is homogeneous and absolutely irreducible. The equation



$P = 0$  defines a curve in the projective plane  $\mathbf{P}(2)$ . This curve, which we denote by  $\mathbf{W}(g_2, g_3)$  or simply by  $\mathbf{W}$ , has only one point on the line "at infinity" given by the equation  $X_0 = 0$ , namely the point  $(0:0:1)$ . There is a unique rational mapping of  $\mathbf{W} \times \mathbf{W}$  into  $\mathbf{W}$  that takes a general point  $((1:x_1:y_1), (1:x_2:y_2))$  onto the point  $(1:x:y)$  with

$$x = -(x_1 + x_2) + \frac{1}{4} \left( \frac{y_1 - y_2}{x_1 - x_2} \right)^2,$$

$$y = -\frac{1}{2}(y_1 + y_2) + \frac{3}{2}(x_1 + x_2) \frac{y_1 - y_2}{x_1 - x_2} - \frac{1}{4} \left( \frac{y_1 - y_2}{x_1 - x_2} \right)^3.$$

This mapping is obviously holomorphic at every point  $((1:a_1:b_1), (1:a_2:b_2))$  with  $a_1 \neq a_2$ . By rather tedious computations it is not difficult to show that the rational mapping is holomorphic at every point of  $\mathbf{W} \times \mathbf{W}$ . For example, if the point is  $((1:a:b), (1:a:b))$  we write

$$(1:x:y) = ((y_1 + y_2)^3 : (y_1 + y_2)^3 x : (y_1 + y_2)^3 y)$$

and use the computation

$$(y_1 + y_2) \frac{y_1 - y_2}{x_1 - x_2} = \frac{y_1^2 - y_2^2}{x_1 - x_2} = \frac{4x_1^3 - g_2 x_1 - g_3 - (4x_2^3 - g_2 x_2 - g_3)}{x_1 - x_2} = 4(x_1^2 + x_1 x_2 + x_2^2) - g_{22}$$

whereas if the point is  $((1:a:b), (1:a:-b))$  with  $b \neq 0$ , we merely write  $(1:x:y) = ((x_1 - x_2)^3 : (x_1 - x_2)^3 x : (x_1 - x_2)^3 y)$ . Furthermore, this rational mapping is, when considered as a law of composition on  $\mathbf{W}$ , both commutative and associative, the point  $(0:0:1)$  is a neutral element, and every element  $(1:a:b)$  has inverse  $(1:a:-b)$ . Thus, the rational mapping is a commutative group law, and  $\mathbf{W}$  is an algebraic group. It is defined over any field containing  $g_2$  and  $g_3$ .

**REMARK** The group law here is, in the case  $U = \mathbf{C}$ , intimately related to the addition formula for the elliptic function  $\wp$  of Weierstrass. This function satisfies the ordinary differential equation  $\wp'^2 = 4\wp^3 - g_2\wp - g_3$ , so that for any point  $z \in \mathbf{C}$  that is not a pole of  $\wp$ ,  $(1:\wp(z):\wp'(z))$  is a point of  $\mathbf{W}$ . When  $z$  is a pole of  $\wp$ , we adopt the convention that  $(1:\wp(z):\wp'(z))$  denotes the point  $(0:0:1)$ . The addition formula for  $\wp$  is then expressed through the group law on  $\mathbf{W}$  by the equation

$$(1:\wp(z_1 + z_2):\wp'(z_1 + z_2)) = (1:\wp(z_1):\wp'(z_1))(1:\wp(z_2):\wp'(z_2)).$$

Thus, the formula  $z \mapsto (1:\wp(z):\wp'(z))$  defines a group homomorphism  $\mathbf{C} \rightarrow \mathbf{W}$ . The kernel is the lattice of periods of  $\wp$ . This homomorphism is not a rational one, but when  $\mathbf{C}$  and  $\mathbf{W}$  are given their usual complex analytic structures, it is everywhere holomorphic.

If  $G$  is any algebraic group defined over a field  $K$ , for each point  $x \in G$  we have the extension  $K(x)$  of  $K$  obtained by adjoining to  $K$  the coordinates of  $x$ , we have the notion of specialization over  $K$  (we write  $x \xrightarrow{K} x'$  to indicate that  $x'$  is a specialization of  $x$  over  $K$ ), and when  $x'$  is a generic specialization of  $x$  over  $K$  (in symbols,  $x \xleftrightarrow{K} x'$ ) we have an isomorphism  $K(x) \approx K(x')$  over  $K$  that maps each coordinate of  $x$  onto the corresponding coordinate of  $x'$ . These extensions, specializations, and isomorphisms, together with the group law, have certain formal properties. In the following two sections we shall set down these properties as *axioms*, and shall then develop the theory *ab initio* on their basis; at the same time we shall develop the corresponding notion of homogeneous space.

2 Pre-K-sets

Let  $K$  be a field. By a *pre-K-set* (relative to the universal field  $U$ ) we shall mean a set  $A$  for which there are given:

- (i) for each element  $x \in A$ , a finitely generated extension  $K(x)$  of  $K$ ,
- (ii) a pre-order on  $A$  (for which we shall use the notation  $x \xrightarrow{K} x'$ , and in connection with which we shall write  $x \xleftrightarrow{K} x'$  to denote the relation " $x \xrightarrow{K} x'$  and  $x' \xrightarrow{K} x$ "), and
- (iii) for each pair  $(x, x') \in A^2$  with  $x \xleftrightarrow{K} x'$ , a field isomorphism

$$S_{x',x}^K : K(x) \approx K(x') \text{ over } K,$$

all subject to the following axioms.

**AS 1** (a) If  $x, x' \in A$  and  $x \xrightarrow{K} x'$ , but not  $x' \xrightarrow{K} x$ , then  $\text{tr deg } K(x)/K > \text{tr deg } K(x')/K$ .

(b)  $A$  has a finite subset  $\Phi$  such that for every  $x \in \Phi$ ,  $K(x)$  is separable over  $K$ , and for each  $x' \in A$ , there exists an  $x \in \Phi$  with  $x \xrightarrow{K} x'$ .

**AS 2** (a) If  $x, x', x'' \in A$ ,  $x \xleftrightarrow{K} x'$ , and  $x' \xleftrightarrow{K} x''$ , then  $S_{x',x}^K \circ S_{x'',x'}^K = S_{x'',x}^K$ .

(b) If  $x \in A$  and  $S : K(x) \approx K'$  is a field isomorphism over  $K$ , then there exists a unique  $x' \in A$  with  $x \xleftrightarrow{K} x'$  such that  $K(x') = K'$  and  $S_{x',x}^K = S$ .

Consider an extension  $L$  of  $K$ , over which the transcendence degree of  $U$  need not be infinite. An element  $x$  of the pre-K-set  $A$  will be called *rational* over  $L$  if  $K(x) \subset L$ . Similarly,  $x$  will be called *algebraic* (respectively *separable*, respectively *regular*) over  $L$  if  $LK(x)$  is an algebraic (respectively separable,

respectively regular) extension of  $L$ . The transcendence degree of  $LK(x)$  over  $L$  will be called the *dimension* of  $x$  over  $L$ , and will be denoted by  $\dim_L x$ . The set of elements of  $A$  that are rational over  $L$  will be denoted by  $A_L$ . In particular,  $A_U = A$ . It is easy to see that when  $L$  is algebraically closed and of infinite transcendence degree over  $K$ , then  $A_L$ , with the extensions  $K(x)$  ( $x \in A_L$ ) and the induced pre-order  $x \xrightarrow{K} x'$  ( $x, x' \in A_L$ ) and the isomorphisms  $S_{x',x}^K$  ( $x, x' \in A_L, x \xleftrightarrow{K} x'$ ), is a pre- $K$ -set relative to the universal field  $L$ .

We shall indicate the relation  $x \xrightarrow{K} x'$  (respectively  $x \xleftrightarrow{K} x'$ ) by saying that  $x'$  is a *specialization* (respectively *generic specialization*) of  $x$  over  $K$ . When  $x$  is algebraic over  $K$  there are only finitely many specializations of  $x$  over  $K$ . They all are generic and are called the *conjugates* of  $x$  over  $K$ .

When there is no danger of confusion, we shall usually write  $x \rightarrow x'$  instead of  $x \xrightarrow{K} x'$ ,  $x \leftrightarrow x'$  instead of  $x \xleftrightarrow{K} x'$ , and  $S_{x',x}$  instead of  $S_{x',x}^K$ .

It follows from AS 2(a) that  $S_{x,x} = id_{K(x)}$  and that  $S_{x,x'} = S_{x',x}^{-1}$ .

It follows from AS 2(b) that if  $\sigma : L \approx L'$  is an isomorphism of extensions of  $K$  (over which  $U$  need not have infinite transcendence degrees), then for each  $x \in A_L$  there is a unique  $x' \in A_{L'}$  such that  $x \leftrightarrow x'$ ,  $K(x') = \sigma(K(x))$ , and  $\sigma$  coincides with  $S_{x',x}$  on  $K(x)$ ; we denote this element  $x'$  by  $\sigma x$ . Thus, the isomorphism  $\sigma : L \approx L'$  over  $K$  induces a bijection of  $A_L$  onto  $A_{L'}$ . If  $x_1, x_2 \in A_L$  and  $x_1 \rightarrow x_2$ , then  $\sigma x_1 \rightarrow \sigma x_2$ , and if  $x_1 \leftrightarrow x_2$ , then  $\sigma x_1 \leftrightarrow \sigma x_2$  and  $S_{\sigma x_2, \sigma x_1} = \sigma S_{x_2, x_1} \sigma^{-1}$  for every  $\alpha \in K(\sigma x_1)$ . If  $\tau : L' \approx L''$  is another isomorphism of extensions of  $K$ , then  $(\tau\sigma)x = \tau(\sigma x)$  for every  $x \in A_L$ .

A subset  $V$  of the pre- $K$ -set  $A$  is called  *$K$ -irreducible* (in  $A$ ) if there exists an  $x \in A$  such that  $V$  is the set of all specializations of  $x$  over  $K$ ; any such  $x$  is called a  *$K$ -generic* element of  $V$ . Every element of  $A$  is a  $K$ -generic element of a unique  $K$ -irreducible subset of  $A$ , called the *locus* of  $x$  over  $K$ .

If a subset  $A'$  of  $A$  is the union of finitely many  $K$ -irreducible subsets of  $A$  each of which has a  $K$ -generic element that is separable over  $K$ , then the pre- $K$ -set structure on  $A$  induces, by restriction to  $A'$ , a pre- $K$ -set structure on  $A'$ . We then say that  $A'$  is a *pre- $K$ -subset* of  $A$ . A pre- $K$ -subset of a pre- $K$ -subset of  $A$  is a pre- $K$ -subset of  $A$ . A  $K$ -irreducible subset  $V$  of  $A$  is a pre- $K$ -subset of  $A$  if and only if  $V$  has a  $K$ -generic element that is separable over  $K$ .

A maximal  $K$ -irreducible subset of  $A$  is called a  *$K$ -component* of  $A$ . By AS 1(b), the  $K$ -components of  $A$  are finite in number and their union is  $A$ , each  $K$ -component of  $A$  is a pre- $K$ -subset of  $A$ , and every  $K$ -irreducible subset of  $A$  is a subset of a  $K$ -component of  $A$ . The set of all the  $K$ -generic elements of the  $K$ -components of  $A$  will be denoted by  $\Gamma_{A/K}$ .

By AS 1(a) and (b), the set of natural numbers  $\dim_K x$  ( $x \in A$ ) is bounded, so that if  $A$  is not empty, then  $\max_{x \in A} \dim_K x$  exists. This natural number is called the *dimension* of  $A$  and is denoted by  $\dim A$ . It equals the maximum

of the dimensions of the  $K$ -components of  $A$ . If  $V$  and  $V'$  are  $K$ -irreducible pre- $K$ -subsets of  $A$  with  $V \supset V'$  and  $V \neq V'$ , then  $\dim V > \dim V'$ , and  $\Gamma_{V/K}$  is the set of all elements  $x \in V$  such that  $\dim_K x = \dim V$ .

When  $L$  is an algebraically closed extension of  $K$  of infinite transcendence degree ( $U$  not necessarily of infinite transcendence degree over  $L$ ), and  $V_1, \dots, V_m$  are the  $K$ -components of  $A$ , then  $V_{1L}, \dots, V_{mL}$  are the  $K$ -components of the pre- $K$ -set  $A_L$ , and  $\dim A_L = \dim A$ .

By a *pre- $K$ -mapping* of a pre- $K$ -set  $A$  into a pre- $K$ -set  $B$  we shall mean a mapping  $f$  of a subset  $A_f$  of  $A$  into  $B$  with the following four properties:

- (i)  $\Gamma_{A_f/K} \subset A_f$ ;
- (ii) if  $x \in A_f$ , then  $K(x) \supset K(f(x))$ ;
- (iii) if  $x \in A, x' \in A_f, x \rightarrow x'$ , then  $x \in A_f$  and  $f(x) \rightarrow f(x')$ ;
- (iv) if  $x, x' \in A_f$  and  $x \leftrightarrow x'$ , then  $S_{x',x}$  is an extension of  $S_{f(x'),f(x)}$ .

If  $A_0$  is any subset of  $A_f$  that contains  $\Gamma_{A_f/K}$  and contains an element  $x$  whenever it contains a specialization of  $x$  over  $K$ , then the restriction of  $f$  to  $A_0$  also is a pre- $K$ -mapping of  $A$  into  $B$ ; in particular,  $A_0$  can be  $\Gamma_{A_f/K}$ . In general, if  $V_1, \dots, V_m$  are the  $K$ -components of  $A$  and  $x_i$  is a  $K$ -generic element of  $V_i$  ( $1 \leq i \leq m$ ), then  $f(x_i)$  is separable over  $K$  and hence its locus over  $K$  is a  $K$ -irreducible pre- $K$ -subset  $W_i$  of  $B$ ; the set  $W_1 \cup \dots \cup W_m$  is the smallest pre- $K$ -subset of  $B$  containing  $f(A_f)$ . When  $A'$  and  $B'$  are pre- $K$ -subsets of  $A$  and  $B$ , respectively, with  $\Gamma_{A'/K} \subset A_f$  and  $f(\Gamma_{A'/K}) \subset B'$ , then the restriction of  $f$  to  $A' \cap A_f$  is a pre- $K$ -mapping of  $A'$  into  $B'$  (said to be *induced* by  $f$ ).

The pre- $K$ -mapping  $f$  of  $A$  into  $B$  is said to be *everywhere defined* (on  $A$ ) if  $A_f = A$ . When  $f$  is everywhere defined and bijective, and the inverse  $f^{-1}$  is an everywhere defined pre- $K$ -mapping of  $B$  into  $A$ , then for any  $x \in A$ ,  $K(x) = K(f(x))$ , and for any  $x, x' \in A$ ,  $x \rightarrow x'$  if and only if  $f(x) \rightarrow f(x')$ . Hence, when such is the case, for any pre- $K$ -subset  $C$  of  $A$  the image  $f(C)$  is a pre- $K$ -subset of  $B$ ,  $K$ -irreducible if and only if  $C$  is  $K$ -irreducible.

The pre- $K$ -mapping  $f$  is said to be *separable* if, for every  $x \in \Gamma_{A_f/K}$ ,  $K(x)$  is a separable extension of  $K(f(x))$ . To prove  $f$  separable it suffices to verify this condition for one  $K$ -generic element of each  $K$ -component of  $A$ .

If  $L$  is an extension of  $K$ , then the restriction  $f_L$  of  $f$  to  $A_f \cap A_L$  maps  $A_f \cap A_L$  into  $B_L$ . In the special case in which  $L$  is algebraically closed and of infinite transcendence degree over  $K$ ,  $f_L$  is a pre- $K$ -mapping of  $A_L$  into  $B_L$  (these being pre- $K$ -sets relative to the universal field  $L$ ). If  $\sigma$  is any isomorphism over  $K$  of  $L$  onto an extension of  $K$ , and if  $x \in A_f \cap A_L$ , then  $\sigma x \in A_f \cap A_{\sigma L}$  and  $\sigma(f(x)) = f(\sigma x)$ .

Let  $(x_i)_{i \in I}$  be a family of elements of (the same or different) pre- $K$ -sets. The family is (or the elements  $x_i$  are) said to be *independent* over  $K$  if, for each index  $i_0 \in I$ , the fields  $K(x_{i_0})$  and  $K(\bigcup_{i \neq i_0} K(x_i))$  are linearly disjoint over  $K$ . If for each  $i_0$  these fields are merely algebraically disjoint over  $K$ ,

then we shall say that the family is (or the elements  $x_i$  are) *quasi-independent* over  $K$ . Finitely many elements  $x_1, \dots, x_m$  are quasi-independent over  $K$  if and only if

$$\text{tr deg } K(x_1) \cdots K(x_m)/K = \sum_{1 \leq i \leq m} \dim_K x_i.$$

Given any sequence  $x_1, x_2, \dots, x_m, \dots$  of elements of pre- $K$ -sets, it is easy to prove, by an induction argument based on AS 2(b), that there exists a sequence  $x'_1, x'_2, \dots, x'_m, \dots$  quasi-independent over  $K$  such that  $x_i = x'_i$  and  $x_m \leftrightarrow x'_m$  ( $m > 1$ ). For any family  $(x_i)_{i \in I}$ , if all the elements  $x_i$  are regular over  $K$  (or even if all but one are), then quasi-independence implies independence.

Given some homomorphisms  $h_i: R_i \rightarrow R'_i$  ( $i \in I$ ) of subrings of  $U$ , we shall call them *compatible* if there exists a homomorphism of subrings of  $U$  that is an extension of every  $h_i$ . If every  $h_i$  is an isomorphism, and if the isomorphisms  $h_i$  are compatible and their inverses are compatible, then we shall call them *bicompatible*. If the family  $(x_i)_{i \in I}$  is independent over  $K$ , and if  $x_i \leftrightarrow x'_i$  ( $i \in I$ ), then the isomorphisms  $S_{x'_i, x_i}$  ( $i \in I$ ) are compatible.

**Lemma 1** Let  $K, L_0, L$  be fields with  $K \subset L_0 \subset L$ , let  $A_1, \dots, A_m$  be pre- $K$ -sets, and let  $x_i \in A_i$  ( $1 \leq i \leq m$ ). For each index  $i$  there exist finitely many elements  $x_{i1}, \dots, x_{in_i} \in A_i$  such that  $x_i \leftrightarrow x_{ij}$  ( $1 \leq j \leq n_i$ ), such that  $\text{id}_{L_0}$  and  $S_{x_{ij}, x_i}$  are bicompatible ( $1 \leq j \leq n_i$ ), and such that the following conditions are satisfied.

(a) Whenever  $x'_i \in A_i$ ,  $x_i \leftrightarrow x'_i$ , and  $\text{id}_{L_0}$  and  $S_{x'_i, x_i}$  are compatible ( $1 \leq i \leq m$ ), then there exist indices  $j(1), \dots, j(m)$  such that  $\text{id}_L, S_{x'_1, x_{1j(1)}}, \dots, S_{x'_m, x_{mj(m)}}$  are compatible.

(b) 
$$\text{tr deg } L \left( \bigcup_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n_i}} K(x_{ij}) \right) / L = \sum_{1 \leq i \leq m} n_i \dim_{L_0} x_i.$$

(c) If  $x_i$  is separable over  $L_0$ , then  $x_{ij}$  is separable over  $L$  ( $1 \leq j \leq n_i$ ).

(d) If  $x_i$  is regular over  $L_0$ , then  $n_i = 1$  and  $x_{i1}$  is regular over  $L$ .

Because of AS 2(b), this is an immediate consequence of Chapter 0, Section 12, Corollary 3 to Proposition 7 (with  $K$  there replaced by  $L_0$ ).

**REMARK** When  $x_i$  is separable over  $L_0$  we have the following converse to part (d) of the lemma: If  $n_i = 1$  for every extension  $L$  of  $L_0$ , then  $x_i$  is regular over  $L_0$ . (See Chapter 0, the remark at the end of Section 12.)

### 3 $K$ -Groups and homogeneous $K$ -spaces. $K$ -Sets

By a  $K$ -group (relative to the universal field  $U$ ) we shall mean a set  $G$  on which there is given a group structure (which we shall usually write multi-

plicatively) and a pre- $K$ -set structure (relative to the universal field  $U$ ), subject to the following axioms.

**AG 1** (a) If  $x, y \in G$ , then  $K(xy) \subset K(x)K(y)$ .

(b) If  $x, y \in G$ , then  $K(x^{-1}y) \subset K(x)K(y)$ .

**AG 2** (a) If  $x, y, x', y' \in G$ , and  $x \leftrightarrow x', y \leftrightarrow y'$ , and  $S_{x', x}, S_{y', y}$  are compatible, then  $xy \rightarrow x'y'$ . If moreover  $xy \leftrightarrow x'y'$  and  $h$  is a homomorphism of subrings of  $U$  such that  $h, S_{x', x}, S_{y', y}$  are compatible, then  $h, S_{x'y', xy}$  are compatible.

(b) If  $x, y, x', y' \in G$ , and  $x \rightarrow x', y \rightarrow y'$ , then there exist elements  $x^*, y^* \in G$  with  $x \leftrightarrow x^*, y \leftrightarrow y^*$  such that  $x^*, y^*$  are quasi-independent over  $K$  and  $x^*y^* \rightarrow x'y'$ , and such that when  $x^*y^* \leftrightarrow x'y', y^* \leftrightarrow y'$ , then  $S_{x'y', x^*y^*}, S_{y', y^*}$  are compatible.

(c) If  $x, y, x', y' \in G$ , and  $x \leftrightarrow x', y \leftrightarrow y'$ , and  $S_{x', x}, S_{y', y}$  are compatible, then  $x^{-1}y \rightarrow x'^{-1}y'$ . If moreover  $x^{-1}y \leftrightarrow x'^{-1}y'$  and  $h$  is a homomorphism of subrings of  $U$  such that  $h, S_{x', x}, S_{y', y}$  are compatible, then  $h, S_{x'^{-1}y', x^{-1}y}$  are compatible.

(d) If  $x, y, x', y' \in G$ , and  $x \rightarrow x', y \rightarrow y'$ , then there exist elements  $x^*, y^* \in G$  with  $x \leftrightarrow x^*, y \leftrightarrow y^*$  such that  $x^*, y^*$  are quasi-independent over  $K$  and  $x^{*-1}y^* \rightarrow x'^{-1}y'$ .

**AG 3** The unity element 1 of  $G$  is contained in a  $K$ -component of  $G$  having a  $K$ -generic element that is regular over  $K$ .

**REMARK** It is easy to verify that if  $L$  is an algebraically closed extension of  $K$  of infinite transcendence degree (over which  $U$  need not have infinite transcendence degree), then  $G_L$ , with its pre- $K$ -set structure relative to the universal field  $L$  and with its group structure as a subgroup of  $G$ , is a  $K$ -group relative to the universal field  $L$ .

Before investigating the consequences of these axioms, we introduce a related definition. Recall that a homogeneous space for an abstract group  $g$  is defined as a set  $m$  together with an external law of composition  $m \times g \rightarrow m$  (for which we usually use the multiplicative notation  $(v, x) \mapsto vx$ ) such that

$$v(xy) = (vx)y \quad (v \in m, x \in g, y \in g),$$

$$v1 = v \quad (v \in m),$$

$$vg = m \quad (v \in m).$$

The homogeneous space is said to be *principal* if, for each pair  $(v, w) \in m^2$ , the element  $z \in g$  with  $vz = w$  is unique. When this is the case, this unique

element may be denoted by  $v^{-1}w$ , and the following identities can be derived:

$$\begin{aligned} v(v^{-1}w) &= w, & v^{-1}v &= (v^{-1}w)^{-1}, \\ (u^{-1}v)(v^{-1}w) &= u^{-1}w, & v^{-1}v &= 1, \\ (vx)^{-1}(wy) &= x^{-1}(v^{-1}w)y \end{aligned}$$

( $u \in m, v \in m, w \in m, x \in g, y \in g$ ). To see an example of a homogeneous space for  $g$ , consider any subgroup  $h$  of  $g$  and the set  $g/h$  of right cosets of  $h$  in  $g$ . If  $x = hx_0$  is such a coset and if  $y \in g$ , then the set  $xy = hx_0y$  (consisting of all products  $xy$  with  $x \in x$ ) is also such a coset, and the formula  $(x, y) \mapsto xy$  defines an external law of composition  $(g/h) \times g \rightarrow g/h$  that makes  $g/h$  a homogeneous space for  $g$ . This gives the so-called canonical structure on  $g/h$  of homogeneous space for  $g$ . Conversely, if  $m$  is any homogeneous space for  $g$  and if we choose an element  $w \in m$ , the set  $h$  of elements  $x \in g$  such that  $wx = w$  is a subgroup of  $g$ , there is a unique mapping  $g/h \rightarrow m$  such that  $hx \mapsto wx$  for all  $x \in g$ , and this mapping is an isomorphism of homogeneous spaces for  $g$ .

Let  $G$  be a  $K$ -group. By a *homogeneous  $K$ -space* for  $G$  (relative to the universal field  $U$ ) we shall mean a set  $M$  on which there is given a structure of homogeneous space for the group  $G$  and a structure of pre- $K$ -set (relative to the universal field  $U$ ), subject to the following axioms.

**AH 1** (a) If  $v \in M, x \in G$ , then  $K(vx) \subset K(v)K(x)$ .

**AH 2** (a) If  $v, v' \in M, x, x' \in G$ , and  $v \leftrightarrow v', x \leftrightarrow x'$ , and  $S_{v',v}, S_{x',x}$  are compatible, then  $vx \rightarrow v'x'$ . If moreover  $vx \leftrightarrow v'x'$  and  $h$  is a homomorphism of subrings of  $U$  such that  $h, S_{v',v}, S_{x',x}$  are compatible, then  $h, S_{v'x',vx}$  are compatible.

(b) If  $v, v' \in M, x, x' \in G$ , and  $v \rightarrow v', x \rightarrow x'$ , then there exist elements  $v^* \in M, x^* \in G$  with  $v \leftrightarrow v^*, x \leftrightarrow x^*$  such that  $v^*, x^*$  are quasi-independent over  $K$  and  $v^*x^* \rightarrow v'x'$ , and such that when  $v^*x^* \leftrightarrow v'x', x^* \leftrightarrow x'$ , then  $S_{v'x',v^*x^*}, S_{x',x^*}$  are compatible.

We shall call the homogeneous  $K$ -space for  $G$  *principal* if it is principal as a homogeneous space for the group  $G$  and satisfies the following additional axioms.

**AH 1** (b) If  $v, w \in M$ , then  $K(v^{-1}w) \subset K(v)K(w)$ .

**AH 2** (c) If  $v, w, v', w' \in M$ , and  $v \leftrightarrow v', w \leftrightarrow w'$ , and  $S_{v',v}, S_{w',w}$  are compatible, then  $v^{-1}w \rightarrow v'^{-1}w'$ . If moreover  $v^{-1}w \leftrightarrow v'^{-1}w'$  and  $h$  is a homomorphism of subrings of  $U$  such that  $h, S_{v',v}, S_{w',w}$  are compatible, then  $h, S_{v'^{-1}w',v^{-1}w}$  are compatible.

(d) If  $v, w, v', w' \in M$ , and  $v \rightarrow v', w \rightarrow w'$ , then there exist elements  $v^*, w^* \in M$  with  $v \leftrightarrow v^*, w \leftrightarrow w^*$  such that  $v^*, w^*$  are quasi-independent over  $K$  and  $v^*w^* \rightarrow v'^{-1}w'$ .

**REMARK** It is easy to verify that if  $L$  is an algebraically closed extension of  $K$  of infinite transcendence degree (over which  $U$  need not have infinite transcendence degree), then  $M_L$ , with its pre- $K$ -set structure relative to the universal field  $L$  and with the external law of composition  $M_L \times G_L \rightarrow M_L$  induced by the external law of composition  $M \times G \rightarrow M$ , is a homogeneous  $K$ -space for the  $K$ -group  $G_L$ , and is a principal one when  $M$  is a principal homogeneous  $K$ -space for  $G$ .

It is immediate from the axioms that a  $K$ -group  $G$  has a natural structure of principal homogeneous  $K$ -space for  $G$ , the external law of composition being the group law. We call this the *regular  $K$ -space* for  $G$ . Because of this fact, all results obtained for principal homogeneous  $K$ -spaces are valid for  $K$ -groups. (Another structure on  $G$  of principal homogeneous  $K$ -space for  $G$  is obtained by defining the external law of composition by the formula  $(v, x) \mapsto x^{-1}v$  ( $v \in G, x \in G$ ).

**Proposition 1** Let  $G$  be a  $K$ -group and  $M$  be a homogeneous  $K$ -space for  $G$ . Let  $v, w, v', w' \in M, x, y, x' \in G$ .

(a)  $K(x^{-1}) = K(x), K(1) = K, K(v)K(x) = K(vx)K(x)$ . When  $M$  is principal,  $K(v)K(x) = K(v)K(vx)$ .

(b) If  $\sigma$  is an isomorphism over  $K$  of an overfield of  $K(v)K(x)$  onto an extension of  $K$ , then  $\sigma(vx) = (\sigma v)(\sigma x)$ . When  $M$  is principal, if  $\sigma$  is an isomorphism over  $K$  of an overfield of  $K(v)K(w)$  onto an extension of  $K$ , then  $\sigma(v^{-1}w) = (\sigma v)^{-1}(\sigma w)$ .

(c) If  $v, x$  are quasi-independent over  $K$ , then  $\dim_K vx \geq \dim_K v$ . When  $M$  is principal then also  $\dim_K vx \geq \dim_K x$ , and if  $v, w$  are quasi-independent over  $K$ , then  $\dim_K v^{-1}w \geq \max(\dim_K v, \dim_K w)$ .

(d) If  $v, x$  are independent over  $K$  and  $v \rightarrow v', x \rightarrow x'$ , then  $vx \rightarrow v'x'$ . If moreover  $vx \leftrightarrow v'x', x \leftrightarrow x'$ , then  $S_{v'x',vx}, S_{x',x}$  are compatible. When  $M$  is principal, if  $v, w$  are independent over  $K$  and  $v \rightarrow v', w \rightarrow w'$ , then  $v^{-1}w \rightarrow v'^{-1}w'$ .

*Proof* (a) By AG 1(b),  $K(1) = K(x^{-1}x) \subset K(x)$ . Since  $x$  can be  $\sigma 1$  for any  $\sigma \in \text{Aut}(U/K)$ ,  $K(1) \subset \sigma(K(1))$  for every such  $\sigma$ , so that  $K(1)$  is algebraic over  $K$ . However, by AG 3,  $x$  can be regular over  $K$ , so that  $K(1) = K$ . Hence, by AG 1(b),  $K(x^{-1}) = K(x^{-1}1) \subset K(x)$ , whence  $K(x^{-1}) = K(x)$ . Therefore, by AH 1(a),

$$\begin{aligned} K(vx)K(x) &\subset K(v)K(x) = K(vx \cdot x^{-1})K(x) \subset K(vx)K(x^{-1})K(x) \\ &= K(vx)K(x), \end{aligned}$$

and when  $M$  is principal, by AH 1(a) and (b),

$$K(v)K(vx) \subset K(v)K(x) = K(v)K(v^{-1} \cdot vx) \subset K(v)K(vx).$$

(b) Since  $S_{\sigma v, v}, S_{\sigma x, x}, S_{\sigma(vx), vx}$  are restrictions of  $\sigma$ , they are bicompatible. By AH 2(a) therefore  $S_{\sigma(vx) \cdot vx}, S_{(\sigma v)(\sigma x), vx}$  are compatible and hence equal, so that by AS 2(b),  $\sigma(vx) = (\sigma v)(\sigma x)$ . When  $M$  is principal and we take  $x = v^{-1}w$ , this shows that  $\sigma(v^{-1}w) = (\sigma v)^{-1}(\sigma w)$ .

(c) If  $v, x$  are quasi-independent over  $K$ , then by part (a) of the proposition,  $\dim_K vx \geq \dim_{K(x)} vx = \dim_{K(x)} v = \dim_K v$ . When  $M$  is principal, also by part (a),  $\dim_K vx \geq \dim_{K(v)} vx = \dim_{K(v)} x = \dim_K x$ , and if  $v, w$  are quasi-independent over  $K$ , then, again by part (a),  $\dim_K v^{-1}w \geq \dim_{K(w)} v^{-1}w = \dim_{K(w)} v = \dim_K v$  and similarly  $\dim_K v^{-1}w \geq \dim_K w$ .

(d) Let  $v^*, x^*$  be as in AH 2(b). Since  $v, x$  are independent over  $K$ , the isomorphisms  $S_{v^*, v}$  and  $S_{x^*, x}$  can be extended to a surjective homomorphism  $\sigma : K[K(v) \cup K(x)] \rightarrow K[K(v^*) \cup K(x^*)]$ . Because  $v^*, x^*$  are quasi-independent over  $K$ , the transcendence degrees over  $K$ , left and right, are the same, so that  $\sigma$  is an isomorphism. By part (b) of the proposition then  $vx \leftrightarrow \sigma(vx) = (\sigma v)(\sigma x) = v^*x^* \rightarrow v'x'$ , and in the event that  $vx \leftrightarrow v'x', x \leftrightarrow x'$ , then  $S_{v'x', vx}, S_{x', x}$  are compatible. When  $M$  is principal, a similar argument, using AH 2(d) instead of AH 2(b), shows that  $v^{-1}w \rightarrow v'^{-1}w'$ .

REMARK 1 If  $x \rightarrow x'$ , then  $x^{-1} \rightarrow x'^{-1}$ . If  $x \leftrightarrow x'$ , then  $x^{-1} \leftrightarrow x'^{-1}$  and  $S_{x'^{-1}, x^{-1}} = S_{x', x}$ . Indeed, by part (a) of the proposition,  $x, 1$  are independent over  $K$ , and of course  $1 \rightarrow 1$ , so that the first assertion follows from the second half of part (d) of the proposition. It follows that if  $x \leftrightarrow x'$ , then  $x^{-1} \leftrightarrow x'^{-1}$ , and by part (b),  $S_{x', x}(x^{-1}) = (S_{x', x}^{-1})^{-1} = x'^{-1} = S_{x'^{-1}, x^{-1}}(x^{-1})$ , so that  $S_{x'^{-1}, x^{-1}} = S_{x', x}$ .

REMARK 2 The axioms AG 2(a) and (c), and AH 2(a) and (if  $M$  is principal) (c) are capable of self-improvement. Let  $h : R \rightarrow R'$  be a homomorphism of subrings of  $U$ , let  $v_1 \leftrightarrow v_1', \dots, v_m \leftrightarrow v_m'$  in  $M$  and  $x_1 \leftrightarrow x_1', \dots, x_n \leftrightarrow x_n'$  in  $G$ , and suppose that  $h$  and the isomorphisms  $S_{v_1', v_1}, \dots, S_{v_m', v_m}, S_{x_1', x_1}, \dots, S_{x_n', x_n}$  are compatible. Let  $U_1, \dots, U_m, X_1, \dots, X_n$  be noncommuting indeterminates, and by induction define the sets of "monomials":

$$\begin{aligned} \mathfrak{X}_0 &= \mathfrak{M}_0 = \{1\}, & \mathfrak{X}_1 &= \{1, X_1, X_1^{-1}, \dots, X_n, X_n^{-1}\}, \\ \mathfrak{X}_k &= \mathfrak{X}_{k-1} \mathfrak{X}_1 \quad \text{or} \quad \mathfrak{X}_{k-1} \mathfrak{X}_1 \cup \bigcup_{\substack{1 \leq \mu \leq m \\ 1 \leq \mu' \leq m}} \mathfrak{X}_{k-2} U_\mu^{-1} U_{\mu'} \quad (k \geq 2) \end{aligned}$$

according as  $M$  is not or is principal,

$$\begin{aligned} \mathfrak{M}_k &= \mathfrak{X}_k \cup \bigcup_{1 \leq \mu \leq m} U_\mu \mathfrak{X}_{k-1} \quad (k \geq 1), \\ \mathfrak{M} &= \bigcup_{k \in \mathbb{N}} \mathfrak{M}_k. \end{aligned}$$

For each  $W \in \mathfrak{M}$  denote by  $w$ , respectively  $w'$ , the element of  $M$  or  $G$  obtained by substituting  $(v_1, \dots, v_m, x_1, \dots, x_n)$ , respectively  $(v_1', \dots, v_m', x_1', \dots, x_n')$ , for  $(U_1, \dots, U_m, X_1, \dots, X_n)$  in  $W$ . By Remark 1,  $w \leftrightarrow w'$  ( $W \in \mathfrak{M}_1$ ), and  $h$  and the isomorphisms  $S_{w', w}$  ( $W \in \mathfrak{M}_1$ ) are compatible. It easily follows, by AG 2(a) and (c) and AH 2(a) and (when appropriate) (c), that  $w \rightarrow w'$  ( $W \in \mathfrak{M}_2$ ). Furthermore, if we let  $\mathfrak{M}_2'$  denote the set of  $W \in \mathfrak{M}_2$  for which  $w \leftrightarrow w'$  and set  $\mathfrak{X}_2' = \mathfrak{M}_2' \cap \mathfrak{X}_2$ , then  $h$  and the isomorphisms  $S_{w', w}$  ( $W \in \mathfrak{M}_2'$ ) are compatible. This improvement process can be continued to yield specializations  $w \rightarrow w'$  ( $W \in \mathfrak{M}_2' \mathfrak{X}_2'$ ), etc. In particular, if the isomorphisms  $S_{v_1', v_1}, \dots, S_{v_m', v_m}, S_{x_1', x_1}, \dots, S_{x_n', x_n}$  are bicompatible, then  $w \leftrightarrow w'$  ( $W \in \mathfrak{M}$ ), and  $h$  and all the isomorphisms  $S_{w', w}$  ( $W \in \mathfrak{M}$ ) are compatible. In Section 10 a much stronger result (Proposition 13) is obtained.

REMARK 3 If  $G$  is a  $K$ -group, then the pre- $K$ -set structure on  $G$  and the opposite group structure on  $G$  (for which the product  $xy$  is defined as the product  $yx$  for the given group structure) determine on the set  $G$  a  $K$ -group structure. (All the axioms are obvious with the possible exception of AG 2(b). However, if  $x \rightarrow x', y \rightarrow y'$ , then we may apply AG 2(b) in  $G$  to the specializations  $x^{-1} \rightarrow x'^{-1}, y^{-1} \rightarrow y'^{-1}$  to establish AG 2(b) for the opposite group structure.) The  $K$ -group thus obtained is called the  $K$ -group *opposite* to  $G$ . If  $M$  is a homogeneous  $K$ -space for the  $K$ -group  $G$ , the formula  $(v, x) \mapsto vx^{-1}$  defines an external law of composition  $M \times G \rightarrow M$  that makes  $M$  a homogeneous space for the opposite group. This homogeneous space structure and the given pre- $K$ -set structure on  $M$  determine on  $M$  a structure of homogeneous  $K$ -space for the  $K$ -group opposite to  $G$ .

**Theorem 1** Let  $G$  be a  $K$ -group and  $M$  be a homogeneous  $K$ -space for  $G$ . The  $K$ -components of  $M$  are pairwise disjoint and all have the same dimension. The  $K$ -component  $G^\circ$  of  $G$  that contains 1 is a normal subgroup of  $G$  of finite index. Each  $K$ -component  $V$  of  $M$  is the union of a finite number of orbits of  $G^\circ$  in  $M$ , this number being 1 if  $M$  is a principal homogeneous  $K$ -space for  $G$  and  $V$  has a  $K$ -generic element that is regular over  $K$ .

*Proof* By AG 3,  $G$  has a  $K$ -component  $G^\circ$  containing 1 and having a  $K$ -generic element  $t$  that is regular over  $K$ . Let  $V$  be any  $K$ -component of  $M$  and fix a  $K$ -generic element  $v$  of  $V$  such that  $v$  and  $t$  are quasi-independent (and hence independent) over  $K$ . By Proposition 1(d),  $vt \rightarrow v1 = v$ , whence  $vt \leftrightarrow v$ , so that  $vt$  is a  $K$ -generic element of  $V$ . In the special case in which  $M$  is the regular  $K$ -space for  $G$  and  $1 \in V$ , the same argument shows that  $vt$  is a  $K$ -generic element of  $G^\circ$ , so that  $V = G^\circ$ . Therefore  $G^\circ$  is the unique  $K$ -component of  $G$  containing 1. In the general case, let  $W$  be any other  $K$ -component of  $M$ , and let  $w \in \Gamma_{W/K}$ . Fixing  $x \in G$  with  $vx = w$ , setting  $v' = v$ ,  $x' = x$ , and then fixing elements  $v^* = M, x^* \in G$  as in AH 2(b), we find with

the help of Proposition 1(c), that  $\dim W = \dim_K W = \dim_K v^*x^* \geq \dim_K v^* = \dim V$ ; similarly  $\dim V \geq \dim W$ . Therefore all the  $K$ -components of  $M$  have the same dimension.

Starting afresh, let  $v_0 \in M$  and choose  $t \in \Gamma_{G^\circ/K}$  so that  $v_0, t$  are independent over  $K$ . If  $V$  is any  $K$ -component of  $M$  containing  $v_0$ , let  $v \in \Gamma_{V/K}$ , fix  $x \in G$  with  $vx = v_0$ , and fix  $s \in \Gamma_{G^\circ/K}$  so that  $K(s)$  and  $K(v_0)K(v)K(x)$  are linearly disjoint over  $K$ . Then

$$\dim G \geq \dim_K xs \geq \dim_{K(v)} xs \geq \dim_{K(v)K(x)} xs = \dim_{K(v)K(x)} s = \dim_K s = \dim G;$$

whence  $\dim_K xs = \dim_{K(v)} xs$ , that is,  $v$  and  $xs$  are quasi-independent over  $K$ , so that  $\dim_K v_0 s = \dim_K vxs \geq \dim_K v = \dim M$ . Since (by Proposition 1(d))  $vs \rightarrow v1 = v$  and  $vs \rightarrow v_0 s$  and  $v_0 t \leftrightarrow v_0 s$ , we infer that  $v_0 t \in \Gamma_{V/K}$ . Since  $V$  is any  $K$ -component of  $M$  that contains  $v_0$ , there can be just one such  $K$ -component. This shows that the  $K$ -components of  $M$  are pairwise disjoint.

Continuing the above notation, we see that if  $t_0$  is any element of  $G^\circ$ , then (by Proposition 1(d))  $v_0 t \rightarrow v_0 t_0$ . Since  $v_0 t \in V$  this implies that  $v_0 t_0 \in V$ . Thus,  $V G^\circ = V$ . In the special case in which  $M$  is the regular  $K$ -space for  $G$  and  $V = G^\circ$  this shows that  $G^\circ G^\circ = G^\circ$ . By Remark 1 following Proposition 1,  $t^{-1} \rightarrow 1$  whence  $t^{-1} \in G^\circ$ , and also  $t^{-1} \rightarrow t_0^{-1}$  whence  $t_0^{-1} \in G^\circ$ , so that  $(G^\circ)^{-1} = G^\circ$ . Therefore  $G^\circ$  is a subgroup of  $G$ .

Let  $X$  be a  $K$ -component of  $G$  and let  $x \in \Gamma_{X/K}$ . By Section 2, Lemma 1 (with  $L_0 = K, L = K_\bullet$ ) there exist elements  $x_1, \dots, x_n \in \Gamma_{X/K}$ , quasi-independent over  $K$  and with  $n = 1$  if  $x$  is regular over  $K$ , having the property that for every  $x' \in \Gamma_{X/K}$  there is an index  $j$  such that  $S_{x', x_j}$  can be extended to an isomorphism  $S' : K_\bullet K(x_j) \approx K_\bullet K(x')$  over  $K_\bullet$ . When  $x', x_j$  are quasi-independent over  $K$ , then  $K_\bullet K(x'), K_\bullet K(x_j)$  are linearly disjoint over  $K_\bullet$  so that  $S'$  can be extended to a homomorphism  $K_\bullet [K(x') \cup K(x_j)] \rightarrow K_\bullet K(x')$  over  $K_\bullet K(x')$ ; in this case  $S_{x', x_j}, S_{x', x'}$  are compatible, so that by the axiom AG 2(c)  $x_j^{-1} x' \rightarrow x'^{-1} x' = 1$ , whence  $x_j^{-1} x' \in G^\circ$ . Thus, for any element  $x' \in \Gamma_{X/K}$  such that  $K(x'), K(x_1) \cdots K(x_n)$  are algebraically disjoint over  $K$ ,  $x' \in \bigcup_{1 \leq j \leq n} x_j G^\circ$ . However, for any element  $x_0 \in X$  whatsoever, there exists an element  $t \in \Gamma_{G^\circ/K}$  such that  $K(t), K(x_0)K(x_1) \cdots K(x_n)$  are linearly disjoint over  $K$ , so that  $x_0 t \in \bigcup_{1 \leq j \leq n} x_j G^\circ$ , whence  $x_0 \in \bigcup_{1 \leq j \leq n} x_j G^\circ$ . Thus,  $X = \bigcup_{1 \leq j \leq n} x_j G^\circ$ , that is, every  $K$ -component is the union of finitely many orbits (= left cosets) of  $G^\circ$  in  $G$ . It follows from this that  $G^\circ$  is of finite index in  $G$ . Furthermore, if  $X_1, \dots, X_m$  are the  $K$ -components of  $G$  and if  $X_i = \bigcup_{1 \leq j \leq n_i} x_{ij} G^\circ$  ( $1 \leq i \leq m$ ), then, for any element  $v_0 \in M$ ,

$$M = v_0 G = \bigcup_{1 \leq i \leq m} v_0 X_i = \bigcup_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n_i}} v_0 x_{ij} G^\circ.$$

Since the  $K$ -component  $V$  of  $M$  is disjoint from any other  $K$ -component of

$M$ , and since  $WG^\circ = W$  for every  $K$ -component  $W$  of  $M$ , it follows that  $V$  is the union of those orbits  $v_0 x_{ij} G^\circ$  of  $G^\circ$  for which  $v_0 x_{ij} \in V$ .

Suppose that  $M$  is a principal homogeneous  $K$ -space for  $G$  and that some (and therefore every)  $K$ -generic element of  $V$  is regular over  $K$ . If  $v_0$  is any element of  $V$  and  $v$  is any  $K$ -generic element of  $V$  such that  $v, v_0$  are quasi-independent (and hence independent) over  $K$ , then  $v \rightarrow v_0$  and  $v_0 \rightarrow v_0$ , whence (by Proposition 1(d))  $v^{-1} v_0 \rightarrow v_0^{-1} v_0 = 1$ , so that  $v^{-1} v_0 \in G^\circ$  and  $v_0 G^\circ = v G^\circ$ . However, for any two elements  $v_1, v_2 \in V$ , there exists an element  $v \in \Gamma_{V/K}$  such that  $K(v)$  and  $K(v_1)K(v_2)$  are algebraically disjoint over  $K$ , and by what we have just proved  $v_1 G^\circ = v G^\circ = v_2 G^\circ$ . Therefore in this case  $V$  is an orbit of  $G^\circ$ .

To complete the proof of the theorem it remains to prove the normality of the subgroup  $G^\circ$  of  $G$ , that is, to show for any  $t_0 \in G^\circ$  and  $x_0 \in G$  that  $x_0 t_0 x_0^{-1} \in G^\circ$ . To this end fix  $t \in \Gamma_{G^\circ/K}$  such that  $K(t), K(t_0)K(x_0)$  are linearly disjoint over  $K$ . We shall show that  $x_0 t x_0^{-1} \rightarrow x_0 t_0 x_0^{-1}$ . This will suffice because in the special case in which  $t_0 = 1$  it will prove that  $x_0 t x_0^{-1} \in G^\circ$  and therefore in the general case it will prove that  $x_0 t_0 x_0^{-1} \in G^\circ$ . Fixing an element  $s \in \Gamma_{G^\circ/K}$  such that  $K(s)$  and  $K(x_0)K(t_0)K(t)$  are linearly disjoint over  $K$ , we know that  $ts \leftrightarrow t_0 s$  and of course  $x_0 \leftrightarrow x_0, s \leftrightarrow s$ . Since  $ts, x_0, s$  are evidently independent over  $K$ ,  $S_{t_0 s, ts}, S_{x_0, x_0}, S_{s, s}$  are compatible. Therefore  $x_0 ts \rightarrow x_0 t_0 s, x_0 s \rightarrow x_0 s$ , and because evidently  $\dim_K x_0 ts = \dim G = \dim_K x_0 t_0 s$  the former specialization here is generic, so that  $S_{x_0 t_0 s, x_0 ts}, S_{x_0 s, x_0 s}$  are compatible. Therefore  $x_0 ts (x_0 s)^{-1} \rightarrow x_0 t_0 s (x_0 s)^{-1}$ , that is,  $x_0 t x_0^{-1} \rightarrow x_0 t_0 x_0^{-1}$ . This completes the proof of the theorem.

REMARK 1 In the proof of the theorem it was shown that if  $v \in M, t \in \Gamma_{G^\circ/K}$ , and  $v, t$  are independent over  $K$ , then  $vt$  is a  $K$ -generic element of the  $K$ -component of  $M$  that contains  $v$ . Actually, for any element  $x \in \Gamma_{G/K}$  such that  $v, x$  are quasi-independent over  $K, vx \in \Gamma_{M/K}$ . Indeed, it is easy to see that if we fix  $t \in \Gamma_{G^\circ/K}$  so that  $K(t), K(v)K(x)$  are linearly disjoint over  $K$  (whence, by the above,  $vxt \in \Gamma_{M/K}$ ), then  $xt \leftrightarrow x$  and  $S_{v, v}, S_{x, xt}$  are bicompatible, so that  $vxt \leftrightarrow vx$  and  $vx \in \Gamma_{M/K}$ .

REMARK 2 Let  $v, v' \in M$  and fix  $t, t' \in \Gamma_{G^\circ/K}$  such that  $v, t$  are independent over  $K$  and  $v', t'$  are too. Then the following two conditions are equivalent.

- (i)  $vt \leftrightarrow v't'$  and  $S_{v't', vt}, S_{t', t}$  are compatible.
- (ii)  $v \rightarrow v'$ .

This follows from Proposition 1(d), and Remark 1, above.

REMARK 3 Let  $h : R \rightarrow R'$  be a homomorphism of subrings of  $U$ , let  $x, x' \in G$ , and fix  $s, t, s', t' \in \Gamma_{G^\circ/K}$  such that  $s, t$  are independent over  $K$  and  $K(s)K(t), K[K(x) \cup R]$  are linearly disjoint over  $K$ , and such that  $s', t'$  are

independent over  $K$  and  $K(s')K(t')$ ,  $K[K(x') \cup R']$  are linearly disjoint over  $K$ . Then the following three conditions are equivalent.

- (i)  $sx \leftrightarrow s'x'$  and  $h, S_{s'x', sx}, S_{s', s}$  are compatible.
- (ii)  $xt \leftrightarrow x't'$  and  $h, S_{x't', xt}, S_{t', t}$  are compatible.
- (iii)  $sxt \leftrightarrow s'x't'$  and  $h, S_{s'x't', sxt}, S_{s', s}, S_{t', t}$  are compatible.

This follows from Remark 2 following Proposition 1.

REMARK 4 If  $L$  is any algebraically closed extension of  $K$  of infinite transcendence degree, then  $(G^\circ)_L = (G_L)^\circ$ . Therefore we may use the notation  $G_L^\circ$ .

Consider a subset  $H$  of the  $K$ -group  $G$ . If  $H$  is a subgroup of the group  $G$  and is a pre- $K$ -subset of the pre- $K$ -set  $G$ , then evidently  $H$  satisfies all the axioms for a  $K$ -group with the possible exception of AG 3. When AG 3 is satisfied, too, we call  $H$  a  $K$ -subgroup of  $G$ . We shall see later (Section 8) that this is always the case. For the present we observe that  $G^\circ$  is a  $K$ -subgroup of  $G$ , as is the trivial subgroup of  $G$ . If  $H$  is a  $K$ -subgroup of  $G$  and  $I$  is a  $K$ -subgroup of  $H$ , then  $I$  is a  $K$ -subgroup of  $G$ .

A  $K$ -homomorphism of a  $K$ -group  $G$  into a  $K$ -group  $G'$  is defined as a mapping  $f: G \rightarrow G'$  that is a group homomorphism and an everywhere defined pre- $K$ -mapping (see Section 2). If  $H, H'$  are  $K$ -subgroups of  $G, G'$ , respectively, and if  $f: G \rightarrow G'$  is a  $K$ -homomorphism such that  $f(H) \subset H'$ , then  $f$  induces by restriction a  $K$ -homomorphism  $H \rightarrow H'$ . In particular, since  $id_G$  is a  $K$ -homomorphism of  $G$  into  $G$ , the inclusion mapping  $in_{G, H}: H \subset G$  is a  $K$ -homomorphism of  $H$  into  $G$ . The composite of  $K$ -homomorphisms  $f: G \rightarrow G'$  and  $f': G' \rightarrow G''$  of  $K$ -groups is a  $K$ -homomorphism  $f' \circ f: G \rightarrow G''$ . If there exists a  $K$ -homomorphism  $g: G' \rightarrow G$  such that  $g \circ f = id_G$  and  $f \circ g = id_{G'}$ , then  $f$  is called a  $K$ -isomorphism, and  $g$  is then unique, being the inverse mapping  $f^{-1}$ . Composites and inverses of  $K$ -isomorphisms are  $K$ -isomorphisms.

Now consider two homogeneous  $K$ -spaces  $M$  and  $M'$  for the  $K$ -group  $G$ . By a  $K$ -homomorphism of  $M$  into  $M'$  we mean a mapping  $f: M \rightarrow M'$  that is a homomorphism of homogeneous spaces for the group  $G$  (that is, that satisfies the identity  $f(vx) = f(v)x$ ) and is an everywhere defined pre- $K$ -mapping. A  $K$ -homomorphism of homogeneous  $K$ -spaces for  $G$  is necessarily surjective. Composites of such  $K$ -homomorphisms are themselves  $K$ -homomorphisms, and a  $K$ -homomorphism  $f: M \rightarrow M'$  is a  $K$ -isomorphism if there exists a  $K$ -homomorphism  $g: M' \rightarrow M$  such that  $g \circ f = id_M$  and  $f \circ g = id_{M'}$ . Composites and inverses of  $K$ -isomorphisms are  $K$ -isomorphisms.

$K$ -endomorphisms and  $K$ -automorphisms (of a  $K$ -group  $G$  or of a homogeneous  $K$ -space for  $G$ ) are defined as expected.

For any element  $y \in G$  the mapping  $\lambda_y: G \rightarrow G$  defined by the formula  $\lambda_y x = yx$  is a bijective one, with inverse  $\lambda_{y^{-1}}$ . If  $y \in G_K$ , then  $\lambda_y$  is a  $K$ -automorphism of the regular  $K$ -space for  $G$  (but not, in general, of the  $K$ -group). The mapping  $\rho_y: G \rightarrow G$  defined by the formula  $\rho_y x = xy$  is also bijective, with inverse  $\rho_{y^{-1}}$ . If  $y \in G_K$ , then  $\rho_y$  is a  $K$ -automorphism of the regular  $K$ -space for the  $K$ -group opposite to  $G$  (see Remark 3 following the proof of Proposition 1). More generally, if  $M$  is a homogeneous  $K$ -space for  $G$  and  $w \in M$ , the mapping  $\lambda_w: G \rightarrow M$  defined by the formula  $\lambda_w x = wx$  is surjective (and when  $M$  is principal, is bijective with inverse given by the formula  $v \rightarrow w^{-1}v$ ). If  $w \in M_K$ , then  $\lambda_w$  is a  $K$ -homomorphism of the regular  $K$ -space for  $G$  into  $M$  (and when  $M$  is principal, it is a  $K$ -isomorphism). The mapping  $\rho_y: M \rightarrow M$  defined by the formula  $\rho_y v = vy$  is bijective, with inverse  $\rho_{y^{-1}}$ . If  $y \in G_K$ , then  $\rho_y$  is an everywhere defined pre- $K$ -mapping, but is not, in general, a  $K$ -automorphism of  $M$ . The symmetry mapping  $\iota: G \rightarrow G$  defined by the formula  $\iota x = x^{-1}$  is not a  $K$ -automorphism of the  $K$ -group  $G$  (unless  $G$  is commutative), but is a  $K$ -isomorphism of  $G$  onto the  $K$ -group opposite to  $G$  (and also of the opposite  $K$ -group onto  $G$ ).

By a  $K$ -set we shall mean a pre- $K$  subset of a homogeneous  $K$  space for a  $K$ -group. A pre- $K$ -subset of a  $K$ -set  $A$  is obviously a  $K$ -set, and will be called a  $K$ -subset of  $A$ .

#### 4 Extending the universal field

Let  $\mathfrak{U}$  be an algebraically closed extension of the universal field  $U$ . We are going to describe a method for embedding any  $K$ -group  $G$  relative to the universal field  $U$  in a  $K$ -group  $\mathfrak{G}$  relative to the universal field  $\mathfrak{U}$  in such a way that  $G = \mathfrak{G}_U$ , and also for embedding any homogeneous  $K$ -space  $M$  for  $G$  relative to the universal field  $U$  in a homogeneous  $K$ -space  $\mathfrak{M}$  for  $\mathfrak{G}$  relative to the universal field  $\mathfrak{U}$  in such a way that  $M = \mathfrak{M}_U$ .

First consider any pre- $K$ -set  $A$  relative to the universal field  $U$ . Let  $A^\dagger$  denote the set of all triples  $(x, \mathfrak{R}, \mathfrak{S})$  such that  $x \in A$ ,  $\mathfrak{R}$  is an extension of  $K$  in  $\mathfrak{U}$ , and  $\mathfrak{S}$  is an isomorphism  $K(x) \approx \mathfrak{R}$  over  $K$ . Call two such triples  $(x_1, \mathfrak{R}_1, \mathfrak{S}_1), (x_2, \mathfrak{R}_2, \mathfrak{S}_2)$  equivalent if

$$x_1 \leftrightarrow x_2, \quad \mathfrak{R}_1 = \mathfrak{R}_2, \quad \mathfrak{S}_2 \circ S_{x_2, x_1} = \mathfrak{S}_1.$$

(This obviously defines an equivalence relation on  $A^\dagger$ .) Let  $\mathfrak{A}$  denote the set of equivalence classes in  $A^\dagger$ .

If  $\mathfrak{x} \in \mathfrak{A}$ , then all the representatives  $(x, \mathfrak{R}, \mathfrak{S})$  of  $\mathfrak{x}$  have the same second coordinate  $\mathfrak{R}$ , which we shall denote by  $K(\mathfrak{x})$ . This is a finitely generated extension of  $K$  in  $\mathfrak{U}$ .

Let  $\mathfrak{x}, \mathfrak{x}' \in \mathfrak{A}$ . If a pair of representatives  $(x, \mathfrak{R}, \mathfrak{S})$  of  $\mathfrak{x}$  and  $(x', \mathfrak{R}', \mathfrak{S}')$  of  $\mathfrak{x}'$  have the property that  $x \rightarrow x'$ , then all such pairs of representatives have

this property. We define  $\mathfrak{x} \rightarrow \mathfrak{x}'$  to mean that this is the case. The relation  $\mathfrak{x} \rightarrow \mathfrak{x}'$  obviously is a pre-order on  $\mathfrak{A}$ .

If  $\mathfrak{x} \leftrightarrow \mathfrak{x}'$  (that is,  $\mathfrak{x} \rightarrow \mathfrak{x}'$  and  $\mathfrak{x}' \rightarrow \mathfrak{x}$ ), and if we choose a pair of representatives  $(x, \mathfrak{R}, \mathfrak{S}), (x', \mathfrak{R}', \mathfrak{S}')$  as before, then  $x \leftrightarrow x'$  and  $\mathfrak{S}' \circ S_{x',x} \circ \mathfrak{S}^{-1}$  is an isomorphism  $K(\mathfrak{x}) \approx K(\mathfrak{x}')$  over  $K$ . This isomorphism does not depend on the choice of representatives; we shall denote it by  $S_{\mathfrak{x}',\mathfrak{x}}$ .

It is easy to verify that the set  $\mathfrak{A}$ , together with the extensions  $K(\mathfrak{x})$ , the pre-order  $\mathfrak{x} \rightarrow \mathfrak{x}'$ , and the isomorphisms  $S_{\mathfrak{x}',\mathfrak{x}}$ , satisfies AS 1 and AS 2 of Section 2, so that  $\mathfrak{A}$  is a pre- $K$ -set relative to the universal field  $\mathfrak{U}$ . For any element  $x \in A$  the triple  $(x, K(x), S_{x,x})$  is an element of  $A^\dagger$ , and therefore its equivalence class  $(x)$  is an element of  $\mathfrak{A}$ . Furthermore, if  $y \in A$  and  $(x) = (y)$ , then  $x \leftrightarrow y$ ,  $K(x) = K(y)$ , and  $S_{y,y} \circ S_{y,x} = S_{x,x}$ , whence  $S_{y,x} = S_{x,x}$ , so that  $x = y$ . Therefore the formula  $x \mapsto (x)$  defines an injection  $A \rightarrow \mathfrak{A}$ . By means of this injection we identify  $A$  with a subset of  $\mathfrak{A}$ , and therefore write  $A \subset \mathfrak{A}$ . It is a simple matter to verify that  $A = \mathfrak{A}_U$ . The construction of  $\mathfrak{A}$  and the identification of  $A$  with  $\mathfrak{A}_U$  is canonical.

Consider any two pre- $K$ -sets  $A, B$  relative to the universal field  $U$ , and a pre- $K$ -mapping  $f$  of  $A$  into  $B$ . Let  $\mathfrak{A}, \mathfrak{B}$  denote the  $K$ -sets relative to the universal field  $\mathfrak{U}$  canonically associated with  $A, B$ , respectively. For any  $\mathfrak{x} \in \mathfrak{A}$ , if a representative  $(x, \mathfrak{R}, \mathfrak{S})$  has the property that  $x \in A_f$ , where  $A_f$  denotes the set of elements of  $A$  at which  $f$  is defined, then every representative of  $\mathfrak{x}$  has this property. Let  $\mathfrak{A}_f$  denote the set of elements  $\mathfrak{x} \in \mathfrak{A}$  the representatives of which have this property. For any  $\mathfrak{x} \in \mathfrak{A}_f$ , choose a representative  $(x, \mathfrak{R}, \mathfrak{S})$ . Since  $K(f(x)) \subset K(x)$ ,  $\mathfrak{S}$  restricts to an isomorphism  $\mathfrak{T} : K(f(x)) \approx \mathfrak{Q}$ , where  $\mathfrak{Q}$  is a subfield of  $\mathfrak{R}$ , and evidently  $(f(x), \mathfrak{Q}, \mathfrak{T}) \in B^\dagger$ . The equivalence class of  $(f(x), \mathfrak{Q}, \mathfrak{T})$  in  $B^\dagger$  is easily seen to be independent of the choice of representative  $(x, \mathfrak{R}, \mathfrak{S})$ , and therefore may be denoted by  $\mathfrak{f}(\mathfrak{x})$ . Thus, we have a mapping  $\mathfrak{f} : \mathfrak{A}_f \rightarrow \mathfrak{B}$ , and it is easy to verify that  $\mathfrak{f}$  is a pre- $K$ -mapping of  $\mathfrak{A}$  into  $\mathfrak{B}$ , and that  $\mathfrak{f}_U = f$ . In fact,  $\mathfrak{f}$  is the unique pre- $K$ -mapping of  $\mathfrak{A}$  into  $\mathfrak{B}$  such that  $\mathfrak{f}_U = f$ .

Now consider any  $K$ -group and a homogeneous  $K$ -space  $M$  for  $G$ , both relative to the universal field  $U$ . Let  $\mathfrak{G}$  and  $\mathfrak{M}$  denote the pre- $K$ -sets relative to the universal field  $\mathfrak{U}$  that are canonically associated with the pre- $K$ -sets  $G$  and  $M$ , respectively. We show that if  $v \in \mathfrak{M}$ ,  $\mathfrak{x} \in \mathfrak{G}$ , then there exist representatives  $(v, K(v), \mathfrak{S}_v)$  of  $v$  and  $(x, K(x), \mathfrak{S}_x)$  of  $\mathfrak{x}$  such that  $\mathfrak{S}_v, \mathfrak{S}_x$  are bicompatible. Indeed, let  $(v', K(v), \mathfrak{S}_{v'})$  and  $(x', K(x), \mathfrak{S}_{x'})$  be any representatives of  $v$  and  $\mathfrak{x}$ , respectively, choose some isomorphism  $\varphi$  over  $K$  of  $K(v)K(x)$  onto a subfield of  $U$ , let  $\varphi_v : K(v) \approx \varphi(K(v))$  and  $\varphi_x : K(x) \approx \varphi(K(x))$  denote the two isomorphisms obtained by restricting  $\varphi$  as indicated, and set  $\mathfrak{S}_v = \varphi_v^{-1}$  and  $\mathfrak{S}_x = \varphi_x^{-1}$ . Then  $\varphi_v \circ \mathfrak{S}_v$  is an isomorphism of  $K(v')$  onto  $\varphi(K(v))$  over  $K$ , and therefore by axiom AS 2(b) there is an element  $v \in M$  with  $v' \leftrightarrow v$ ,  $K(v) = \varphi(K(v))$ , and  $S_{v,v'} = \varphi_v \circ \mathfrak{S}_{v'}$ , and, similarly,

there is an element  $x \in G$  with  $x' \leftrightarrow x$ ,  $K(x) = \varphi(K(x))$ , and  $S_{x,x'} = \varphi_x \circ \mathfrak{S}_{x'}$ . It is now easy to see that  $(v, K(v), \mathfrak{S}_v) \in v$  and  $(x, K(x), \mathfrak{S}_x) \in \mathfrak{x}$  and that  $\mathfrak{S}_v, \mathfrak{S}_x$  are bicompatible.

This being the case, for any  $v \in \mathfrak{M}$ ,  $\mathfrak{x} \in \mathfrak{G}$ , choose respective representatives  $(v, K(v), \mathfrak{S}_v), (x, K(x), \mathfrak{S}_x)$  such that  $\mathfrak{S}_v, \mathfrak{S}_x$  are bicompatible. There exists a unique isomorphism  $K(v)K(x) \approx K(v)K(x)$  that extends  $\mathfrak{S}_v$  and  $\mathfrak{S}_x$ , and this isomorphism restricts to an isomorphism  $\mathfrak{S}$  of the subfield  $K(vx)$  of  $K(v)K(x)$  onto a subfield  $\mathfrak{R}$  of  $K(v)K(x)$ . The class of the triple  $(vx, \mathfrak{R}, \mathfrak{S})$  does not depend on the choice of representatives  $(v, K(v), \mathfrak{S}_v), (x, K(x), \mathfrak{S}_x)$  as above, and therefore can be denoted by  $v\mathfrak{x}$ .

In the special case in which  $M = G$  of course  $\mathfrak{M} = \mathfrak{G}$ , and the formula  $(v, \mathfrak{x}) \mapsto v\mathfrak{x}$  defines an internal law of composition on  $\mathfrak{G}$ . A tedious but straightforward argument shows that this is a group law (so that  $\mathfrak{G}$  is a group), that  $G$  is a subgroup of  $\mathfrak{G}$ , and that  $\mathfrak{G}$ , with its group structure and its structure of pre- $K$ -set relative to the universal field  $\mathfrak{U}$ , is a  $K$ -group. It is canonically determined by  $G$ . In the general case, the formula  $(v, \mathfrak{x}) \mapsto v\mathfrak{x}$  defines an external law of composition  $\mathfrak{M} \times \mathfrak{G} \rightarrow \mathfrak{M}$  on  $\mathfrak{M}$ . An equally tedious and equally straightforward argument shows that this makes  $\mathfrak{M}$  a homogeneous space for the group  $\mathfrak{G}$ , and that  $\mathfrak{M}$ , with its structure of homogeneous space for  $\mathfrak{G}$  and its structure of  $K$ -set relative to the universal field  $\mathfrak{U}$ , is a homogeneous  $K$ -space for  $\mathfrak{G}$ . It is canonically determined by  $\mathfrak{M}$ . It is easy to see that  $\mathfrak{G}_U$  is identical to  $G$  as a  $K$ -group relative to the universal field  $U$ , and that  $\mathfrak{M}_U$  is identical to  $M$  as a homogeneous  $K$ -space for  $\mathfrak{G}_U = G$  relative to the universal field  $U$ . When  $M$  is a principal homogeneous  $K$ -space for  $G$ , then  $\mathfrak{M}$  is a principal homogeneous  $K$ -space for  $\mathfrak{G}$ , and conversely.

If  $f$  is a  $K$ -homomorphism of  $K$ -groups (or of homogeneous  $K$ -spaces for a  $K$ -group) relative to the universal field  $U$ , and if  $\mathfrak{f}$  denotes the pre- $K$ -mapping between the canonically associated  $K$ -groups (or homogeneous  $K$ -spaces) relative to the universal field  $\mathfrak{U}$  such that  $\mathfrak{f}_U = f$ , then  $\mathfrak{f}$  is a  $K$ -homomorphism. When  $f$  is a  $K$ -isomorphism, then so is  $\mathfrak{f}$ , and conversely.

EXERCISE

1. Let  $\mathfrak{U}$  be an algebraically closed extension of  $U$ . For any pre- $K$ -set  $\mathfrak{A}$  relative to the universal field  $\mathfrak{U}$ , form the pre- $K$ -set  $\mathfrak{A}_U$  relative to the universal field  $U$ , and then let  $\mathfrak{A}'$  denote the pre- $K$ -set relative to the universal field  $\mathfrak{U}$  canonically associated with  $\mathfrak{A}_U$ . For every element  $\mathfrak{x} \in \mathfrak{A}$  let  $\mathfrak{x}'$  denote the set of all triples  $(x, K(x), \mathfrak{S})$  such that  $x \in \mathfrak{A}_U$ ,  $x \leftrightarrow \mathfrak{x}$ ,  $\mathfrak{S} = S_{\mathfrak{x},x}$ . Show that the formula  $\mathfrak{x} \mapsto \mathfrak{x}'$  defines a bijective mapping  $\varphi_{\mathfrak{A}} : \mathfrak{A} \rightarrow \mathfrak{A}'$ , and that  $\varphi_{\mathfrak{A}}$  and  $\varphi_{\mathfrak{A}}^{-1}$  are everywhere defined



pre- $K$ -mappings. Show that when  $\mathfrak{G}$  is a  $K$ -group and  $\mathfrak{M}$  is a homogeneous  $K$ -space for  $\mathfrak{G}$  (both relative to the universal field  $\mathfrak{U}$ ), then  $\varphi_{\mathfrak{G}}: \mathfrak{G} \rightarrow \mathfrak{G}'$  is a  $K$ -isomorphism of  $K$ -groups and  $\varphi_{\mathfrak{M}}: \mathfrak{M} \rightarrow \mathfrak{M}'$  has the property that  $\varphi_{\mathfrak{M}}(vx) = \varphi_{\mathfrak{M}}(v)\varphi_{\mathfrak{G}}(x)$  ( $v \in \mathfrak{M}, x \in \mathfrak{G}$ ).

5 Extending the basic field

Let  $L$  be an extension of  $K$ . Consider a  $K$ -group  $G$  and an  $L$ -group  $H$ . By an  $(L, K)$ -homomorphism of  $H$  into  $G$  we shall mean a group homomorphism  $f: H \rightarrow G$  that satisfies the following three conditions:

- (i) if  $y \in H$ , then  $L(y) \supset K(f(y))$ ;
- (ii) if  $y, y' \in H$  and  $y \xrightarrow{L} y'$ , then  $f(y) \xrightarrow{K} f(y')$ ;
- (iii) if  $y, y' \in H$  and  $y \xleftrightarrow{L} y'$ , then  $S_{y',y}^L$  extends  $S_{f(y'),f(y)}^K$ .

When  $L = K$ , the notion of  $(L, K)$ -homomorphism reduces to that of  $K$ -homomorphism. If  $f: H \rightarrow G$  is an  $(L, K)$ -homomorphism and  $g: I \rightarrow H$  is an  $(L, L)$ -homomorphism ( $L$  being an extension of  $L$  and  $I$  being an  $L$ -group), then  $f \circ g$  is an  $(L, K)$ -homomorphism of  $I$  into  $G$ .

An  $L$ -group structure on  $G$  will be said to be *induced* (by the given  $K$ -group structure on  $G$ ) if the following two conditions are satisfied:

- (i)  $id_G$  is an  $(L, K)$ -homomorphism;
- (ii) every  $(L, K)$ -homomorphism of an  $L$ -group into  $G$  is an  $L$ -homomorphism.

It is easy to see that if the  $K$ -group  $G$  has an induced  $L$ -group structure, then it is unique; in that case we speak of the *induced  $L$ -group* (of the  $K$ -group  $G$ ). Evidently the induced  $L$ -group of the induced  $L$ -group of the  $K$ -group  $G$  is the induced  $L$ -group of the  $K$ -group  $G$ .

Suppose the induced  $L$ -group structure on the  $K$ -group  $G$  exists, and consider a homogeneous  $K$ -space  $M$  for  $G$  and a homogeneous  $L$ -space  $N$  for  $G$ . By an  $(L, K)$ -homomorphism of  $N$  into  $M$  we shall mean a homomorphism  $f: N \rightarrow M$  of homogeneous spaces for the group  $G$  that satisfies the following three conditions:

- (i) if  $w \in N$ , then  $L(w) \supset K(f(w))$ ;
- (ii) if  $w, w' \in N$  and  $w \xrightarrow{L} w'$ , then  $f(w) \xrightarrow{K} f(w')$ ;
- (iii) if  $w, w' \in N$  and  $w \xleftrightarrow{L} w'$ , then  $S_{w',w}^L$  extends  $S_{f(w'),f(w)}^K$ .

When  $L = K$  this notion of  $(L, K)$ -homomorphism reduces to that of  $K$ -homomorphism of homogeneous  $K$ -spaces for  $G$ . Again, if  $f$  is an  $(L, K)$ -

homomorphism of  $N$  into  $M$  and  $g$  is an  $(L, L)$ -homomorphism of  $P$  into  $N$  ( $P$  being a homogeneous  $L$ -space for  $G$ , it being assumed that the  $L$ -group structure for  $G$  exists), then  $f \circ g$  is an  $(L, K)$ -homomorphism of  $P$  into  $M$ .

A structure on  $M$  of homogeneous  $L$ -space for  $G$  (that is, for the induced  $L$ -group of  $G$ ) will be said to be *induced* if the following two conditions are satisfied:

- (i)  $id_M$  is an  $(L, K)$ -homomorphism;
- (ii) every  $(L, K)$ -homomorphism into  $M$  of a homogeneous  $L$ -space for  $G$  is an  $L$ -homomorphism.

If the induced structure on  $M$  of homogeneous  $L$ -space for  $G$  exists, then it is unique, and we speak of the *induced homogeneous  $L$ -space* (of the homogeneous  $K$ -space  $M$ ). The induced homogeneous  $L$ -space of the induced homogeneous  $L$ -space of the homogeneous  $K$ -space  $M$  is the induced homogeneous  $L$ -space of the homogeneous  $K$ -space  $M$ .

The following theorem shows that the induced structures always exist.

**Theorem 2** Let  $G$  be a  $K$ -group,  $M$  be a homogeneous  $K$ -space for  $G$ , and  $L$  be an extension of  $K$ .

(a) The induced  $L$ -group structure on  $G$  exists, as does the induced structure on  $M$  of homogeneous  $L$ -space for  $G$ . When the homogeneous  $K$ -space  $M$  is principal, then so is the induced homogeneous  $L$ -space. If  $v \in M$ , then  $L(v) = LK(v)$ . If  $v, v' \in M$ , then  $v \xrightarrow{L} v'$  if and only if  $vt \xrightarrow{K} v't'$  and the isomorphisms  $id_L, S_{v',vt}^K, S_{t',t}^K$  are compatible (when  $t, t' \in \Gamma_{G \circ K}$ , and  $L(v), K(t)$  are linearly disjoint over  $K$ , and  $L(v'), K(t')$  are, too). If  $v, v' \in M$ , then  $v \xleftrightarrow{L} v'$  if and only if  $v \xleftrightarrow{K} v'$  and  $id_L, S_{v',v}^K$  are bicompatible, and when this is the case, then  $S_{v',v}^L$  is the unique isomorphism  $L(v) \approx L(v')$  that is a common extension of  $id_L$  and  $S_{v',v}^K$ . If  $\sigma$  is any isomorphism over  $L$  of an extension of  $L(v)$  onto an extension of  $L$ , then the meaning of  $\sigma v$  is independent of whether  $M$  is considered as a homogeneous  $K$ -space or a homogeneous  $L$ -space for  $G$ .

(b) If  $v \in M$ , then there exist finitely many elements  $v_1, \dots, v_n \in M$  with  $v \xleftrightarrow{K} v_j$  and  $\dim_L v_j = \dim_K v$  ( $1 \leq j \leq n$ ) such that for each element  $v' \in M$  with  $v \xrightarrow{K} v'$  there is an index  $j$  with  $v_j \xrightarrow{L} v'$ . When  $v$  is separable over  $K$ , then each  $v_j$  is separable over  $L$ . When  $v$  is regular over  $K$ , then  $n = 1$  and  $v_1$  is regular over  $L$ .

(c) Each  $K$ -subset  $V$  of  $M$  is an  $L$ -subset of  $M$ , and the dimension of  $V$  as a  $K$ -set equals its dimension as an  $L$ -set. When  $V$  is  $K$ -irreducible, then all its  $L$ -components have the same dimension and an  $L$ -generic element of any one of them is a  $K$ -generic element of  $V$ . When, in addition, a  $K$ -generic element

of  $V$  is regular over  $K$ , then  $V$  is  $L$ -irreducible and an  $L$ -generic element of  $V$  is regular over  $L$ .

REMARK In the statement of the theorem,  $M$  can be  $G$  (that is, the regular  $K$ -space for  $G$ ). In particular, it follows from part (c) that  $G^\circ$ , the  $K$ -component of  $G$  that contains 1, is also the  $L$ -component of  $G$  that contains 1, and hence there is no need for special notation to distinguish the two (and  $G^\circ$  may be referred to simply as the *component of 1 of  $G$* ). Similarly, the notion of dimension of a  $K$ -subset of  $G$  or of  $M$  is invariant under passage to the induced  $L$ -group or homogeneous  $L$ -space. Henceforth, when we speak of a given  $K$ -group or homogeneous  $K$ -space as an  $L$ -group or homogeneous  $L$ -space, it will always refer to the induced structure. It is easy to see that in  $M$  the relation  $v \xrightarrow{K} v'$  is equivalent to the relation  $v \xrightarrow{K_1} v'$ , and therefore a subset of  $M$  is a  $K_1$ -subset if and only if it is a union of finitely many  $K$ -irreducible subsets of  $M$ .

Proof For each  $v \in M$ , define  $L(v) = LK(v)$ . Then  $L(v)$  is a finitely generated extension of  $L$ .

For  $v, v' \in M$  define  $v \xrightarrow{L} v'$  to mean that when  $t, t' \in \Gamma_{G^\circ/K}$  (whence  $t \xleftrightarrow{K} t'$ ) and  $K(t), L(v)$  are linearly disjoint over  $K$  and  $K(t'), L(v')$  are, too, then  $vt \xleftrightarrow{K} v't'$  and  $id_L, S_{v't, vt}^K, S_{t', t}^K$  are compatible. It is obvious that  $v \xrightarrow{L} v$ , and that if  $v \xrightarrow{L} v'$  and  $v' \xrightarrow{L} v''$ , then  $v \xrightarrow{L} v''$ , that is, the relation  $v \xrightarrow{L} v'$  on  $M$  is a pre-order. Furthermore, if  $v \xrightarrow{L} v'$  and  $\text{tr deg } L(v)/L = \text{tr deg } L(v')/L$ , then, because  $L(t), L(v)$  are linearly disjoint over  $L$  and  $L(t'), L(v')$  are, too, the transcendence degree of  $LK(t)K(vt) = LK(t)K(v) = L(t)L(v)$  over  $L$  equals that of  $LK(t')K(v't')$ , so that the homomorphism  $K[L \cup K(vt) \cup K(t)] \rightarrow K[L \cup K(v't') \cup K(t')]$  extending  $id_L, S_{v't, vt}, S_{t', t}$  is an isomorphism, and  $v \xleftrightarrow{L} v'$ . This verifies axiom AS 1(a).

Let  $v \in M$  and fix an element  $t \in \Gamma_{G^\circ/K}$  such that  $K(t), L(v)$  are linearly disjoint over  $K$ . If  $v$  is separable, respectively regular, over  $K$ , then  $K(t)K(v)$  is separable, respectively regular, over  $K(t)$ . By Section 2, Lemma 1 (with  $L, L_0, m$  now  $L(t), K(t), 1$ ), there exist elements of  $M$ , that we shall denote by  $v_1 t, \dots, v_n t$ , such that  $vt \xleftrightarrow{K} v_j t$  and  $S_{t, t}^K, S_{v_j t, vt}^K$  are bicompatible ( $1 \leq j \leq n$ ), enjoying the following properties.

(a) For each  $v' \in M$  with  $v \xrightarrow{K} v'$  and  $v', t$  independent over  $K$  (and therefore with  $vt \xleftrightarrow{K} v't$  and  $id_{K(t)}, S_{v't, vt}^K$  compatible) there exists an index  $j$  such that  $id_{L(t)}, S_{v't, v_j t}^K$  are compatible.

(b)  $\text{tr deg } L(t)L(v_j t)/L(t) = \text{tr deg } K(t)K(vt)/K(t)$  ( $1 \leq j \leq n$ ).

(c) If  $v$  is separable over  $K$ , then  $L(t)L(v_j t)$  is separable over  $L(t)$  ( $1 \leq j \leq n$ ).

(d) If  $v$  is regular over  $K$ , then  $n = 1$  and  $L(t)L(v_1 t)$  is regular over  $L(t)$ .

It is now easy to see that part (b) of the theorem is true for the special case in which  $v', t$  are independent over  $K$ . However, since for any  $v' \in M$  there evidently exists an element  $v'' \in M$  with  $v' \xleftrightarrow{L} v''$  and  $v'', t$  independent over  $K$ , part (b) of the theorem is true in general. Since the conclusion in part (b) about the arbitrary element  $v \in M$  can be applied to a  $K$ -generic element of each  $K$ -component of  $M$ , axiom AS 1(b) is verified.

If  $v, v' \in M$  and  $v \xleftrightarrow{L} v'$ , then evidently  $v \xleftrightarrow{K} v'$  and  $id_L, S_{v', v}^K$  are bi-compatible. Define  $S_{v', v}^L$  to be the unique isomorphism  $LK(v) \approx LK(v')$  that extends  $id_L$  and  $S_{v', v}^K$ . It is evident that if  $v \xleftrightarrow{L} v'$  and  $v' \xleftrightarrow{L} v''$ , then  $S_{v', v}^L \circ S_{v', v}^L = S_{v', v}^L$ , and that if  $S: L(v) \approx L'$  is an isomorphism over  $L$ , then there exists a unique  $v' \in M$  with  $v \xleftrightarrow{L} v'$  such that  $L(v') = L'$  and  $S_{v', v}^L = S$ . This verifies axiom AS 2, and shows that we have a pre- $L$ -set structure on  $M$ . Since  $M$  can be  $G$ , we have a pre- $L$ -set structure on  $G$ , too.

We have already proved part (b) of the theorem, and part (b) evidently implies part (c). This being the case, it follows that  $G^\circ$ , the  $K$ -component of  $G$  containing 1, is an  $L$ -component of  $G$  and has an  $L$ -generic element that is regular over  $L$ . This verifies axiom AG 3. It remains to verify axioms AH 1(a), AH 2(a) and (b), and, under the additional hypothesis that  $M$  be a principal homogeneous  $K$ -space for the  $K$ -group  $G$ , AH 1(b), and AH 2(c) and (d). Of these, AH 1(a) and (b) are obvious.

Suppose that  $h: R \rightarrow R'$  is a homomorphism of subrings of  $U$ , that  $v \xleftrightarrow{L} v', x \xleftrightarrow{L} x'$ , and that  $h, S_{v', v}^L, S_{x', x}^L$  are compatible. Fixing an element  $t \in \Gamma_{G^\circ/K}$  such that  $K(t), K[R \cup R' \cup L \cup K(v) \cup K(x) \cup K(v') \cup K(x')]$  are linearly disjoint over  $K$ , we see that  $v \xleftrightarrow{K} v', x \xleftrightarrow{K} x', t \xleftrightarrow{K} t$  and that  $h, id_L, S_{v', v}^K, S_{x', x}^K, S_{t, t}^K$  are compatible. Referring to Section 3, Remark 2 following Proposition 1, we find that  $vxt \xleftrightarrow{K} v'x't$  and that  $h, id_L, S_{v'x't, vxt}^K, S_{t, t}^K$  are compatible, and if also  $id_L, S_{v'x', vxt}^K, S_{t, t}^K$  are bicompatible, then  $h, id_L, S_{v'x', vx}^K$  are compatible, that is,  $vx \xrightarrow{L} v'x'$ , and if  $vx \xleftrightarrow{L} v'x'$ , then  $h, S_{v'x', vx}^L$  are compatible. This verifies axiom AH 2(a). A similar argument takes care of AH 2(c) when  $M$  is a principal homogeneous  $K$ -space for  $G$ .

Now suppose that  $v \xrightarrow{L} v', x \xrightarrow{L} x'$ , and fix elements  $s, t \in \Gamma_{G^\circ/K}$  such that  $s, t$  are independent over  $K$  and  $K(s)K(t), L(v)L(x)L(v')L(x')$  are linearly disjoint over  $K$ . We seek elements  $v^*, x^*$ , as in axiom AH 2(b). Referring to Section 3, Remark 3 following Theorem 1, we see that  $vs \xleftrightarrow{K} v's$  and  $id_{L(s)L(t)}, S_{v's, vs}^K$  are compatible and that  $s^{-1}xt \xleftrightarrow{K} s^{-1}x't$  and  $id_{L(s)L(t)}, S_{s^{-1}x't, s^{-1}xt}^K$  are compatible. By Section 2, Lemma 1 (with

$L_0, L, m$  now  $L(s)L(t), L(s)L(t), 2$ , there exist elements of  $M$  that we shall denote by  $v_1 s, \dots, v_n s$  and elements of  $G$  that we shall denote by  $s^{-1}x_1 t, \dots, s^{-1}x_r t$  such that

$$\begin{aligned} vs &\xrightarrow{K} v_j s \text{ and } id_{L(s)L(t)}, S_{v_j s, vs}^K \text{ are bicompatible } (1 \leq j \leq n), \\ s^{-1}xt &\xrightarrow{K} s^{-1}x_k t \text{ and } id_{L(s)L(t)}, S_{s^{-1}x_k t, s^{-1}xt}^K \text{ are bicompatible} \\ &(1 \leq k \leq r), \end{aligned}$$

all having the following properties:

(a) Whenever  $\bar{v} \in M, \bar{x} \in G$ , and

$$\begin{aligned} vs &\xrightarrow{K} \bar{v}s \text{ and } id_{L(s)L(t)}, S_{\bar{v}s, vs}^K \text{ are compatible,} \\ s^{-1}xt &\xrightarrow{K} s^{-1}\bar{x}t \text{ and } id_{L(s)L(t)}, S_{s^{-1}\bar{x}t, s^{-1}xt}^K \text{ are compatible,} \end{aligned}$$

then there exist indices  $j, k$  such that  $id_{L(s)L(t)}, S_{\bar{v}s, v_j s}^K, S_{s^{-1}\bar{x}t, s^{-1}x_k t}^K$  are compatible.

(b) For  $1 \leq j \leq n, 1 \leq k \leq r$ ,

$$\begin{aligned} \text{tr deg } L(s)L(t)K(v_j s)K(s^{-1}x_k t)/L(s)L(t) &= \text{tr deg } L(s)L(t)K(vs)/L(s)L(t) \\ &+ \text{tr deg } L(s)L(t)K(s^{-1}xt)/L(s)L(t). \end{aligned}$$

Fix indices  $j, k$  that work in (a) when  $\bar{v} = v', \bar{x} = x'$ . It follows from (b) that  $s, t, v_j, x_k$  are quasi-independent over  $L$  and that  $K(s)K(t), L(v_j)L(x_k)$  are linearly disjoint over  $K$ ; also,  $v \xrightarrow{L} v_j$  and  $x \xrightarrow{L} x_k$ . Property (a) shows that  $v_j x_k t = v_j s \cdot s^{-1}x_j t \xrightarrow{K} v' s \cdot s^{-1}x' t = v' x' t$  and hence (because  $v' x' t \in \Gamma_{M/K}$ ) even  $v_j x_k t \xrightarrow{K} v' x' t$ , so that the isomorphisms  $id_{L(s)L(t)}, S_{v' x' t, v_j x_k t}^K, S_{s' x' t, s^{-1}x_k t}^K$  are compatible. Therefore  $v_j x_k \xrightarrow{L} v' x'$ . If moreover  $v_j x_k \xrightarrow{K} v' x'$  and  $x_k \xrightarrow{K} x'$ , then  $id_{L(s)L(t)}, S_{v' x', v_j x_k}^K, S_{x', x_k}^K$  are compatible, so that if  $v_j x_k \xrightarrow{L} v' x'$  and  $x_k \xrightarrow{L} x'$ , then  $S_{v' x', v_j x_k}^L, S_{x', x_k}^L$  are compatible. This verifies axiom AH 2(b). A similar argument takes care of AH 2(d) when  $M$  is a principal homogeneous  $K$ -space for  $G$ .

Since  $M$  can be  $G$ , this completes the proof that we have an  $L$ -group structure on  $G$ , and hence also that we have on  $M$  a structure of homogeneous  $L$ -space for the  $L$ -group  $G$  (which is principal when the homogeneous  $K$ -space  $M$  is principal). To prove Theorem 2 it remains to show that these structures of  $L$ -group and homogeneous  $L$ -space are induced by the given structures of  $K$ -group and homogeneous  $K$ -space.

The proof that  $id_G$  and  $id_M$  are  $(L, K)$ -homomorphisms is trivial. Therefore what we must show is that if  $f: H \rightarrow G$  (respectively  $g: N \rightarrow M$ ) is an  $(L, K)$ -homomorphism of an  $L$ -group  $H$  into  $G$  (respectively a homogeneous  $L$ -space  $N$  for  $G$  into  $M$ ), then  $f$  (respectively  $g$ ) is an  $L$ -homomorphism. Let

$y \in H$ . Then  $L(y) \supset K(f(y))$ , so that  $L(y) \supset LK(f(y)) = L(f(y))$ . Suppose that  $y \xrightarrow{L} y'$ . Then  $yt \xrightarrow{L} y't$  and  $S_{y't, yt}^L, S_{t, t}^L$  are compatible ( $t$  being an  $L$ -generic element of  $H^0$  such that  $L(t), L(y)L(y')$  are linearly disjoint over  $L$ ), so that  $f(y)f(t) = f(yt) \xrightarrow{K} f(y't) = f(y')f(t)$  and  $id_L, S_{f(y')f(t), f(y)f(t)}^K, S_{f(t), f(t)}^K$  are compatible. Hence these and  $S_{s, s}^K$  are compatible (where  $s \in \Gamma_{G^0/K}$  and  $K(s), LK(y)K(y')K(t)$  are linearly disjoint over  $K$ ), so that

$$f(y)f(t)s \xrightarrow{K} f(y')f(t)s$$

and  $id_L, S_{f(y')f(t)s, f(y)f(t)s}^K, S_{f(t)s, f(t)s}^K$  are compatible, whence (because, evidently,  $f(t)s \in \Gamma_{G^0/K}$  and  $K(f(t)s), LK(f(y))K(f(y'))$  are linearly disjoint over  $K$ )  $f(y) \xrightarrow{L} f(y')$ . Suppose that  $y \xleftarrow{L} y'$ . By what we have just proved,  $f(y) \xleftarrow{L} f(y')$ , and by the definition of specialization over  $L$  in  $G, S_{f(y'), f(y)}^L$  extends  $S_{f(y'), f(y)}^K$ . However,  $S_{y', y}^L$  extends  $S_{f(y'), f(y)}^K$ , so that  $S_{y', y}^L$  and  $S_{f(y'), f(y)}^L$  coincide on  $K(f(y))$  and hence on  $LK(f(y)) = L(f(y))$ , that is,  $S_{y', y}^L$  extends  $S_{f(y'), f(y)}^L$ . Thus,  $f$  is an  $L$ -homomorphism. A similar argument shows that  $g$  is an  $L$ -homomorphism, and completes the proof of Theorem 2.

REMARK If a  $K$ -irreducible  $K$ -subset  $V$  of  $M$  is  $L$ -irreducible for every extension  $L$  of  $K$ , then a  $K$ -generic element of  $V$  is regular over  $K$ . (See the Remark at the end of Section 2.)

**Corollary 1** *Let  $M$  be a homogeneous  $K$ -space for the  $K$ -group  $G$ , let  $L$  be an extension of  $K$ , let  $V$  be an  $L$ -irreducible  $L$ -subset of  $M$ , and let  $v \in \Gamma_{V/L}$ . A necessary and sufficient condition that  $V$  be a  $K$ -subset of  $M$  is that  $v$  be separable over  $K$ , and  $L$  and  $K(v)$  be linearly disjoint over  $K$ .*

*Proof* Suppose the condition satisfied. Then the locus  $V_0$  of  $v$  over  $K$  is a  $K$ -irreducible  $K$ -subset of  $M$  with  $V_0 \supset V$  and  $\dim V_0 = \dim_K v = \dim_L v = \dim V$ , so that  $V$  is an  $L$ -component of  $V_0$ . An  $L$ -generic element  $w$  of any  $L$ -component of  $V_0$  is a  $K$ -generic element of  $V_0$ , and  $\dim_L w = \dim_L v$ . By linear disjointness the isomorphisms  $id_L, S_{w, v}^K$  are compatible, so that  $v \xrightarrow{L} w$ , whence  $v \xleftarrow{L} w$ . This shows that  $V$  is the only  $L$ -component of  $V_0$ , so that  $V = V_0$ .

Conversely, suppose  $V$  a  $K$ -subset of  $G$ . Clearly,  $V$  is  $K$ -irreducible and  $v \in \Gamma_{V/K}$  so that  $v$  is separable over  $K$ . Every isomorphism over  $K$  of  $K(v)$  onto an extension of  $K$  is an isomorphism  $S_{v', v}^K$  for some  $v' \in V$  with  $v \xrightarrow{K} v'$ . Since  $v \xrightarrow{L} v', id_L$  and  $S_{v', v}^K$  are compatible. However, two extensions of  $K$ , at least one of which is separable, that have the property that the identity mapping of one is compatible with every isomorphism of the other, are linearly disjoint over  $K$  (this is well known and easy to prove). Hence  $L, K(v)$  are linearly disjoint over  $K$ .

**Corollary 2** *Let  $M$  be a homogeneous  $K$ -space for the  $K$ -group  $G$ , let  $L$  be an extension of  $K$ , and let  $A$  be an  $L$ -subset of  $M$ . Then  $L$  contains a finitely generated extension  $L'$  of  $K$  such that  $A$  is an  $L'$ -subset of  $M$ .*

*Proof* Replacing  $A$  by each of its finitely many  $L$ -components, we may suppose that  $A$  is  $L$ -irreducible. Let  $v \in \Gamma_{A/L}$ . Because  $K(v)$  is a finitely generated extension of  $K$  and  $L(v)$  is separable over  $L$ ,  $L$  contains a finitely generated extension  $L'$  of  $K$  such that  $L, L'(v)$  are linearly disjoint over  $L$  and  $L'(v)$  is separable over  $L'$ . By Corollary 1,  $A$  is an  $L'$ -subset of  $M$ .

**6 Zariski topology;  $K$ -topology**

Let  $M$  be a homogeneous  $K$ -space for a  $K$ -group  $G$ , let  $V$  be a  $K$ -irreducible  $K$ -subset of  $M$ , let  $v \in \Gamma_{V/K}$ , and fix  $t \in \Gamma_{G^\circ/K(v)}$  (that is, fix  $t \in \Gamma_{G^\circ/K}$  such that  $v, t$  are independent over  $K$ ). Given an element  $\alpha \in K[K(vt) \cup K(t)]$  and an element  $v' \in V$ , we shall say that  $\alpha$  *vanishes* at  $v'$ , or that  $v'$  is a *zero* of  $\alpha$ , if  $\alpha$  is mapped onto 0 by the homomorphism

$$K[K(vt) \cup K(t)] \rightarrow K[K(v't') \cup K(t')]$$

that extends  $S_{v't', vt}, S_{t', t}$  ( $t'$  denoting an element of  $\Gamma_{G^\circ/K(v')}$ ). We shall say that  $\alpha$  vanishes on a subset  $A$  of  $V$  if  $\alpha$  vanishes at every element of  $A$ , and that  $v'$  is a zero of a subset  $\mathfrak{a}$  of  $K[K(vt) \cup K(t)]$  if  $v'$  is a zero of every element of  $\mathfrak{a}$ .

**Proposition 2** *Let  $M$  be a homogeneous  $K$ -space for a  $K$ -group  $G$ , let  $V$  be a  $K$ -irreducible  $K$ -subset of  $M$ , let  $v \in \Gamma_{V/K}$ , and let  $t \in \Gamma_{G^\circ/K(v)}$ .*

(a) *Let  $A$  be any  $K_1$ -subset of  $V$  and let  $\mathfrak{a}$  denote the set of elements of  $K[K(vt) \cup K(t)]$  that vanish on  $A$ . Then  $\mathfrak{a}$  is a perfect ideal, and the set of zeros of  $\mathfrak{a}$  is  $A$ . The set  $A$  is a  $K$ -subset of  $V$  if and only if the ideal  $\mathfrak{a}$  is separable over  $K(t)$ , and  $A$  is  $K$ -irreducible if and only if  $\mathfrak{a}$  is prime, and then the dimension of  $A$  equals the transcendence degree of  $K[K(vt) \cup K(t)]/\mathfrak{a}$  over  $K(t)$ .*

(b) *If  $\mathfrak{a}$  is any subset of  $K[K(vt) \cup K(t)]$ , then the set  $A$  of zeros of  $\mathfrak{a}$  is a  $K_1$ -subset of  $V$ .*

**REMARK** In part (b), if  $\mathfrak{a}$  is a prime ideal, the set of zeros of  $\mathfrak{a}$  need not be  $K$ -irreducible. See the proof.

*Proof* (a) If  $A_1, \dots, A_m$  are the  $K_1$ -components of  $A$  and  $\mathfrak{a}_j$  denotes the set of elements of  $K[K(vt) \cup K(t)]$  that vanish on  $A_j$ , then evidently  $\bigcap \mathfrak{a}_j = \mathfrak{a}$ , and if  $A_j'$  denotes the set of zeros of  $\mathfrak{a}_j$ , then  $\bigcup A_j'$  is the set of zeros of  $\mathfrak{a}$ . It follows from this that we may suppose  $A$  to be  $K$ -irreducible (see Section 5, the final sentence of the remark following Theorem 2, and also Chapter 0, Section 9, the remark following Theorem 1). Let  $u \in \Gamma_{A/K}$  and

fix  $s \in \Gamma_{G^\circ/K(u)}$ . For every  $v' \in A$  we have  $v \rightarrow u \rightarrow v'$ , and therefore we have the homomorphisms

$$K[K(vt) \cup K(t)] \xrightarrow{f} K[K(us) \cup K(s)] \xrightarrow{g_{v'}} K[K(v't') \cup K(t')]$$

with  $f$  extending  $S_{us, vt}, S_{s, t}$  and  $g_{v'}$  extending  $S_{v't', us}, S_{t', s}$  ( $t'$  denoting an element of  $\Gamma_{G^\circ/K(v')}$ ). Since

$$\begin{aligned} \text{Ker}(f) &\subset \bigcap_{v' \in A} \text{Ker}(g_{v'} \circ f) \\ &= \text{the set of elements of } K[K(vt) \cup K(t)] \text{ vanishing on } A \\ &= \mathfrak{a} \subset \text{Ker}(f), \end{aligned}$$

we see that  $\text{Ker}(f) = \mathfrak{a}$ , whence  $K[K(vt) \cup K(t)]/\mathfrak{a} \approx K[K(us) \cup K(s)]$ . In particular,  $\mathfrak{a}$  is prime, and is separable over  $K(t)$  if and only if the field  $K(us)K(s) = K(u)K(s)$  is separable over  $K(s)$ , that is,  $u$  is separable over  $K$ , or equivalently,  $A$  is a  $K$ -subset of  $V$ . Furthermore, if  $v''$  is any element of  $V$  that is a zero of  $\mathfrak{a}$ , and we fix  $t'' \in \Gamma_{G^\circ/K(v'')}$ , then the kernel of the homomorphism  $K[K(vt) \cup K(t)] \rightarrow K[K(v''t'') \cup K(t'')]$  extending  $S_{v''t'', vt}, S_{t'', t}$  contains  $\text{Ker}(f)$ , so that there exists a homomorphism  $K[K(us) \cup K(s)] \rightarrow K[K(v''t'') \cup K(t'')]$  extending  $S_{v''t'', us}, S_{t'', s}$ , whence  $u \rightarrow v''$  and  $v'' \in A$ . Therefore  $A$  is the set of zeros of  $\mathfrak{a}$ .

(b) The perfect ideal generated by  $\mathfrak{a}$  in the ring  $K[K(vt) \cup K(t)]$  evidently has the same set of zeros as  $\mathfrak{a}$ . Also, this ring is a ring of quotients of a finitely generated overring of  $K$  and hence is Noetherian, so that a perfect ideal is an intersection of finitely many prime ideals. It follows that we may suppose  $\mathfrak{a}$  to be a prime ideal. Then  $\mathfrak{a}$  is the kernel of a homomorphism of  $K[K(vt) \cup K(t)]$  into  $U$  over  $K$ , and therefore (by axiom AS 2(b)) of a homomorphism  $K[K(vt) \cup K(t)] \rightarrow K[K(\bar{v}\bar{t}) \cup K(\bar{t})]$  extending  $S_{\bar{v}\bar{t}, vt}, S_{\bar{t}, t}$  (where  $\bar{t}$  is an element of  $G$  with  $t \leftrightarrow \bar{t}$  and  $\bar{v}$  is an element of  $M$  with  $vt \leftrightarrow \bar{v}\bar{t}$ ). This implies that  $\bar{t} \in \Gamma_{G^\circ/K}$ , and that  $v \rightarrow \bar{v}$ , whence  $\bar{v} \in V$  (but does not imply that  $\bar{v}$  is a zero of  $\mathfrak{a}$ , as there is no assurance that  $\bar{v}, \bar{t}$  are independent over  $K$ ). Fixing  $s \in \Gamma_{G^\circ/K(v)K(t)}$ ,  $\bar{s} \in \Gamma_{G^\circ/K(\bar{v})K(\bar{t})}$ , and referring to Section 3, Remark 2 following Proposition 1, we easily infer that there exists a homomorphism

$$\bar{T}: K[K(vs) \cup K(s) \cup K(t)] \rightarrow K[K(\bar{v}\bar{s}) \cup K(\bar{s}) \cup K(\bar{t})]$$

extending  $S_{\bar{v}\bar{s}, vs}, S_{\bar{s}, s}, S_{\bar{t}, t}$ . Set  $\bar{\mathfrak{r}} = \text{Ker}(\bar{T})$ .

Consider any elements  $v^\dagger \in M$ ,  $s^\dagger \in G$  with  $vs \leftrightarrow v^\dagger s^\dagger$ ,  $s \leftrightarrow s^\dagger$  such that  $S_{v^\dagger s^\dagger, vs}, S_{s^\dagger, s}$  are compatible. Then  $s^\dagger \in \Gamma_{G^\circ/K}$ ,  $v \rightarrow v^\dagger$ , whence  $v^\dagger \in V$ , and there exists a homomorphism

$$K[K(vs) \cup K(s)] \rightarrow K[K(v^\dagger s^\dagger) \cup K(s^\dagger)]$$

extending  $S_{v^\dagger s^\dagger, vs}, S_{s^\dagger, s}$ . Denote the kernel of this homomorphism by  $\mathfrak{p}^\dagger$ . We claim that  $v^\dagger \in A$  if and only if  $K[K(vs) \cup K(s) \cup K(t)]\mathfrak{p}^\dagger \supset \bar{\mathfrak{r}}$ . Before

establishing this, we fix an element  $t^\dagger \in \Gamma_{G^\circ/K(v^\dagger)K(s^\dagger)}$  and observe that because  $K(v)K(s), K(t)$  are linearly disjoint over  $K, S_{t^\dagger, t}$ , the above homomorphism with kernel  $p^\dagger$  can be extended to a homomorphism

$$T^\dagger : K[K(vs) \cup K(s) \cup K(t)] \rightarrow K[K(v^\dagger s^\dagger) \cup K(s^\dagger) \cup K(t^\dagger)].$$

Because  $K(v^\dagger)K(s^\dagger), K(t^\dagger)$  are linearly disjoint over  $K$ , it is easy to see that  $\text{Ker}(T^\dagger) = K[K(vs) \cup K(s) \cup K(t)]p^\dagger$ .

Suppose that  $v^\dagger \in A$ . Then  $\alpha$ , the kernel of the homomorphism  $K[K(vt) \cup K(t)] \rightarrow K[K(\bar{v}\bar{t}) \cup K(\bar{i})]$  introduced earlier, is contained in the kernel of the homomorphism  $K[K(vt) \cup K(t)] \rightarrow K[K(v^\dagger t^\dagger) \cup K(t^\dagger)]$  extending  $S_{v^\dagger t^\dagger, vt}, S_{t^\dagger, t}$ , and therefore there exists a homomorphism  $K[K(\bar{v}\bar{t}) \cup K(\bar{i})] \rightarrow K[K(v^\dagger t^\dagger) \cup K(t^\dagger)]$  extending  $S_{v^\dagger t^\dagger, \bar{v}\bar{t}}, S_{t^\dagger, \bar{i}}$ . Because  $K(\bar{v})K(\bar{i}), K(\bar{s})$  are linearly disjoint over  $K$ , this homomorphism and  $S_{s^\dagger, \bar{s}}$  are compatible, and hence (refer again to Section 3, Remark 2 following Proposition 1) there exists a homomorphism

$$K[K(\bar{v}\bar{s}) \cup K(\bar{s}) \cup K(\bar{i})] \rightarrow K[K(v^\dagger s^\dagger) \cup K(s^\dagger) \cup K(t^\dagger)]$$

extending  $S_{v^\dagger s^\dagger, \bar{v}\bar{s}}, S_{s^\dagger, \bar{s}}, S_{t^\dagger, \bar{i}}$ . The composite of this homomorphism and  $\bar{T}$  is evidently  $T^\dagger$ , and therefore

$$K[K(vs) \cup K(s) \cup K(t)]p^\dagger = \text{Ker}(T^\dagger) \supseteq \text{Ker}(\bar{T}) = \bar{\epsilon}.$$

Conversely, suppose that  $K[K(vs) \cup K(s) \cup K(t)]p^\dagger \supseteq \bar{\epsilon}$ , that is, that  $\text{Ker}(T^\dagger) \supseteq \text{Ker}(\bar{T})$ . Then  $T^\dagger$  is the composite with  $\bar{T}$  of a homomorphism

$$K[K(\bar{v}\bar{s}) \cup K(\bar{s}) \cup K(\bar{i})] \rightarrow K[K(v^\dagger s^\dagger) \cup K(s^\dagger) \cup K(t^\dagger)]$$

that evidently extends  $S_{v^\dagger s^\dagger, \bar{v}\bar{s}}, S_{s^\dagger, \bar{s}}, S_{t^\dagger, \bar{i}}$ . It follows that  $S_{v^\dagger t^\dagger, \bar{v}\bar{t}}, S_{t^\dagger, \bar{i}}$  are compatible, that is, have a common extension  $K[K(\bar{v}\bar{t}) \cup K(\bar{i})] \rightarrow K[K(v^\dagger t^\dagger) \cup K(t^\dagger)]$ . This homomorphism, composed with the homomorphism  $K[K(vt) \cup K(t)] \rightarrow K[K(\bar{v}\bar{t}) \cup K(\bar{i})]$  the kernel of which is  $\alpha$ , yields the homomorphism  $K[K(vt) \cup K(t)] \rightarrow K[K(v^\dagger t^\dagger) \cup K(t^\dagger)]$  extending  $S_{v^\dagger t^\dagger, \bar{v}\bar{t}}, S_{t^\dagger, \bar{i}}$ . Hence the kernel of the last homomorphism contains  $\alpha$ , that is,  $v^\dagger \in A$ . This establishes our claim.

For each  $v' \in A$  fix an element  $s' \in \Gamma_{G^\circ/K(v')K(s')}$ , and let  $p_{v'}$  denote the kernel of the homomorphism  $K[K(vs) \cup K(s)] \rightarrow K[K(v's') \cup K(s')]$  that extends  $S_{v's', vs}, S_{s', s}$ . Then  $p_{v'}$  is a prime ideal, and  $K[K(vs) \cup K(s) \cup K(t)]p_{v'} \supseteq \bar{\epsilon}$ . Set  $\mathfrak{b} = \bigcap_{v' \in A} p_{v'}$ . Then  $\mathfrak{b}$  is a perfect ideal and (see Chapter 0, Section 10, Lemma 9)

$$K[K(vs) \cup K(s) \cup K(t)]\mathfrak{b} = \bigcap_{v' \in A} K[K(vs) \cup K(s) \cup K(t)]p_{v'} \supseteq \bar{\epsilon}.$$

Because the ring  $K[K(vs) \cup K(s)]$  is Noetherian,  $\mathfrak{b} = p_1 \cap \dots \cap p_n$  for suitable prime ideals  $p_1, \dots, p_n$  of this ring. By axiom AS 2(b), for each

$p_j$  there exist elements  $v_j \in M, s_j \in G$  with  $vs \leftrightarrow v_j s_j, s \leftrightarrow s_j$  such that  $S_{v_j s_j, vs}, S_{s_j, s}$  are compatible and  $p_j$  is the kernel of the homomorphism  $K[K(vs) \cup K(s)] \rightarrow K[K(v_j s_j) \cup K(s_j)]$  extending  $S_{v_j s_j, vs}, S_{s_j, s}$ . Clearly  $K[K(vs) \cup K(s) \cup K(t)]p_j \supseteq \bar{\epsilon}$ , so that  $v_j \in A$ , and the locus of  $v_j$  over  $K$  is a  $K$  irreducible subset  $A_j$  of  $A$ . For any  $v' \in A$  the kernel  $p_{v'}$  of the homomorphism  $K[K(vs) \cup K(s)] \rightarrow K[K(v's') \cup K(s')]$  contains  $\mathfrak{b}$  and hence contains  $p_j$  for some  $j$ . For such a  $j$  there exists a homomorphism  $K[K(v_j s_j) \cup K(s_j)] \rightarrow K[K(v's') \cup K(s')]$  extending  $S_{v' s', v_j s_j}, S_{s', s_j}$ , and therefore  $v_j \rightarrow v'$  and  $v' \in A_j$ . This shows that  $A = A_1 \cup \dots \cup A_n$ , so that  $A$  is a  $K_i$ -subset of  $V$ , and completes the proof of Proposition 2.

The intersection of two  $K$ -subsets of the homogeneous  $K$ -space  $M$  need not be a  $K$ -subset of  $M$ . For example, when  $p \neq 0$  and  $K$  contains an element  $c \notin K^p$ , then the curve in  $U^2$  defined by the equation  $Y - X^p + c = 0$  is a  $K$ -subset of  $U^2$ , as is the line defined by the equation  $Y = 0$ , but their intersection is not, since the point  $(c^{1/p}, 0)$  is not separable over  $K$ . It turns out that if the field  $K$  is perfect, then such a phenomenon cannot arise. The proof of this fact is the main part of the proof of the following theorem.

**Theorem 3** *Let  $M$  be a homogeneous  $K$ -space for a  $K$ -group  $G$ .*

- (a) *The subsets  $A$  of  $M$ , such that  $A$  is an  $L$ -subset of  $M$  for some extension  $L$  of  $K$ , are the closed sets of a Noetherian topology on  $M$ .*
- (b) *The  $K_i$ -subsets of  $M$  are the closed sets of a Noetherian topology on  $M$ .*

*Proof* If  $A$  is a subset of  $M$  of the type considered in part (a), then  $A$  is an  $L$ -subset of  $M$  for some algebraically closed  $L$ . Letting  $n_i(A)$  denote the number of  $L$ -components of  $A$  of dimension  $i$  ( $0 \leq i \leq d = \dim M$ ), we see by Section 5, Theorem 2, that the element  $n(A) = (n_d(A), \dots, n_1(A), n_0(A))$  of the lexicographically well-ordered set  $\mathbb{N}^{d+1}$  is independent of the choice of  $L$  as above. It is easy to see that if  $A'$  is another subset of  $M$  of the type considered in part (a), and if  $A \supseteq A'$ , then  $n(A) \geq n(A')$ , the inequality being strict if the inclusion is. It follows that every nonempty set of subsets of  $M$  of the type considered in part (a) has a minimal element. The same holds, *a fortiori*, for the sets considered in part (b). In each part then, if we do have a topology, it is Noetherian.

If  $A, A'$  are any two sets of the type considered in either (a) or (b), then  $A \cup A'$  is such a set, too. To prove that all these sets form a topology it remains to show that the intersection of any family of such sets is itself such a set. If we can do this for any two sets, an induction argument then will give a proof for any finite family. For any family, among the intersections of the finite subfamilies there will, by the above, be a minimal such intersection, which evidently must be the intersection of the whole family. Thus,

to prove the theorem it suffices to show that if  $A, A'$  are  $K$ -subsets of  $M$ , and  $K$  is perfect, then  $A \cap A'$  is a  $K$ -subset of  $M$ . We may evidently suppose that  $A$  and  $A'$  are  $K$ -irreducible. Each of them is then contained in a  $K$ -component of  $M$ . If the two  $K$ -components are distinct, then  $A \cap A' = \emptyset$ , so that we may suppose that  $A$  and  $A'$  are in the same  $K$ -component  $V$  of  $M$ . Fixing elements  $v \in \Gamma_{V/K}, t \in \Gamma_{G^\sigma/K(v)}$ , we know by Proposition 2(a), that  $A$ , respectively  $A'$ , is the set of zeros of an ideal  $\mathfrak{a}$ , respectively  $\mathfrak{a}'$ , of  $K[K(vt) \cup K(t)]$ . Evidently  $A \cap A'$  is the set of zeros of  $\mathfrak{a} \cup \mathfrak{a}'$ , and therefore by Proposition 2(b),  $A \cap A'$  is a  $K$ -subset of  $M$ .

The topology defined in part (a) of Theorem 3 is called the *Zariski topology* on  $M$ . The topology in part (b) is called the  *$K$ -topology* on  $M$ . When we use topological terms such as "open," "closed," etc., they will always refer to the Zariski topology. When we want to refer to the  $K$ -topology we shall say " $K$ -open," " $K$ -closed," etc.

**Corollary** *Let  $M$  and  $N$  be homogeneous  $K$ -spaces for  $K$ -groups, let  $A$  and  $B$  be  $K$ -subsets of  $M$  and  $N$ , respectively, and let  $f$  be a bijective mapping of  $A$  onto  $B$  such that  $f$  and  $f^{-1}$  are everywhere defined pre- $K$ -mappings of  $A$  into  $B$  and  $B$  into  $A$ , respectively. Then  $f$  is a  $K$ -homeomorphism.*

*Proof* If  $v, v' \in A$ , then  $v \rightarrow v'$  if and only if  $f(v) \rightarrow f(v')$ . Therefore  $f$  maps a  $K$ -irreducible subset of  $A$  onto a  $K$ -irreducible subset of  $B$ , and hence maps a  $K$ -closed subset of  $A$  onto a  $K$ -closed subset of  $B$ . Therefore  $f^{-1}$  is  $K$ -continuous. Similarly,  $f$  is  $K$ -continuous.

7 Closed sets

Consider a homogeneous  $K$ -space  $M$  for a  $K$ -group  $G$ . For any automorphism  $\sigma \in \text{Aut}(U/K)$ , and any elements  $v \in M, x \in G$ , we know (see Section 3, Proposition 1(b)) that  $\sigma(vx) = \sigma v \cdot \sigma x$ . Also, if  $v' \in M$  and  $v \xrightarrow{K} v'$ , then (see Section 2)  $\sigma v \xrightarrow{K} \sigma v'$ . It follows easily from this that if  $L$  is an extension of  $K$  and  $v \xrightarrow{L} v'$ , then  $\sigma v \xrightarrow{\sigma L} \sigma v'$ . This implies that if  $A$  is an  $L$ -subset of  $M$ , then  $\sigma A$  is a  $\sigma L$ -subset of  $M$ .

**Theorem 4** *Let  $M$  be a homogeneous  $K$ -space for a  $K$ -group, and let  $A$  be a closed subset of  $M$ . Among the extensions  $L$  of  $K$  such that  $A$  is an  $L$ -subset of  $M$ , there is a smallest one, which we denote by  $K(A)$ . It is finitely generated over  $K$ . If  $\sigma \in \text{Aut}(U/K)$ , then a necessary and sufficient condition that  $\sigma A = A$  is that  $\sigma \in \text{Aut}(U/K(A))$ .*

*Proof* Fix any extension  $L$  of  $K$  such that  $A$  is an  $L$ -subset of  $M$ . Let  $v_{ij}$  ( $1 \leq i \leq m, 1 \leq j \leq n_i$ ) be  $L$ -generic elements of the  $L$ -components of  $A$ , indexed so that

$$v_{ij} \xleftrightarrow{K} v_{i'j'} \quad \text{and} \quad \dim_L v_{ij} = \dim_L v_{i'j'}$$

if and only if  $i = i'$ . For each index  $i$  let  $\xi_{i11}, \dots, \xi_{i1r_i}$  be elements of  $K(v_{i1})$  such that  $K(\xi_{i11}, \dots, \xi_{i1r_i}) = K(v_{i1})$  and for each  $j$  with  $1 < j \leq n_i$  set  $\xi_{ijk} = S_{v_{ij}, v_{i1}}^K \xi_{i1k}$  ( $1 \leq k \leq r_i$ ). Evidently  $K(\xi_{ij1}, \dots, \xi_{ijr_i}) = K(v_{ij})$ . Let  $\mathfrak{p}_{ij}$  be the defining ideal of  $(\xi_{ij1}, \dots, \xi_{ijr_i})$  in  $L[X_1, \dots, X_{r_i}]$ , and set  $\mathfrak{a}_i = \mathfrak{p}_{i1} \cap \dots \cap \mathfrak{p}_{in_i}$ . Each ideal  $\mathfrak{p}_{ij}$  is separable over  $L$ , and therefore  $\mathfrak{a}_i$  is too. By Chapter I, Section 5, Lemma 3(a) (see also Chapter III, Section 3), the ideal  $\mathfrak{a}_i$  has a smallest field of definition  $L_i$ . Set  $L_0 = KL_1 \cdots L_m$ . We shall show that  $L_0$  is the field  $K(A)$  that we are seeking.

The first step is to show that  $A$  is an  $L_0$ -subset of  $M$ . Set  $\mathfrak{a}_{i0} = \mathfrak{a}_i \cap L_0[X_1, \dots, X_{r_i}]$ . Since  $L_0$  is a field of definition of  $\mathfrak{a}_i$ ,  $L_0 \mathfrak{a}_{i0} = \mathfrak{a}_i$ . By a remark in Chapter III, Section 3, the ideal  $\mathfrak{a}_{i0}$  is separable over  $L_0$ . We now refer to Chapter 0, Section 12, Proposition 7. If  $\mathfrak{p}$  is a component of  $\mathfrak{a}_{i0}$ , then  $L_0 \mathfrak{p}$  is separable over  $L_0$  and the components of  $L_0 \mathfrak{p}$  are components of  $L_0 \mathfrak{a}_{i0} = \mathfrak{a}_i$ , have dimension equal to that of  $\mathfrak{p}$ , and intersect  $L_0[X_1, \dots, X_{r_i}]$  in  $\mathfrak{p}$ . Furthermore, as  $\mathfrak{p}$  runs over the set of all components of  $\mathfrak{a}_{i0}$ , then the components of the various  $L_0 \mathfrak{p}$  give us all the components of  $\mathfrak{a}_i$ , that is, give us  $\mathfrak{p}_{i1}, \dots, \mathfrak{p}_{in_i}$ . Thus, the generic zero  $(\xi_{ij1}, \dots, \xi_{ijr_i})$  of  $\mathfrak{p}_{ij}$  is a generic zero of a component of  $\mathfrak{a}_{i0}$ , and has the same dimension over  $L_0$  as over  $L_0$ . Hence  $\dim_L v_{ij} = \dim_{L_0} v_{ij}$  and  $v_{ij}$  is separable over  $L_0$ . Therefore  $v_{ij}$  is an  $L_0$ -generic element of an  $L_0$ -irreducible  $L_0$ -subset  $V_{ij}$  of  $M$ , and every  $L$ -component of  $V_{ij}$  has dimension equal to  $\dim V_{ij} = \dim_{L_0} v_{ij} = \dim_L v_{ij}$ , so that  $v_{ij}$  is an  $L$ -generic element of an  $L$ -component of  $V_{ij}$ . If  $v$  is any  $L$ -generic element of any  $L$ -component of  $V_{ij}$ , then  $v$  is an  $L_0$ -generic element of  $V_{ij}$ , and  $\dim_L v = \dim V_{ij} = \dim_L v_{ij}$ . Setting  $\xi_k = S_{v, v_{ij}}^{L_0} \xi_{ij k}$  ( $1 \leq k \leq r_i$ ), we see that  $(\xi_1, \dots, \xi_{r_i})$  is, like  $(\xi_{ij1}, \dots, \xi_{ijr_i})$ , a generic zero of  $\mathfrak{p}_{ij} \cap L_0[X_1, \dots, X_{r_i}]$ , hence a zero of  $\mathfrak{a}_{i0}$ , hence a zero of  $\mathfrak{a}_i$ , and hence a zero of  $\mathfrak{p}_{ij'}$  for some  $j'$ . Since  $\dim_L(\xi_1, \dots, \xi_{r_i}) = \dim_L v = \dim_L v_{ij} = \dim_L v_{ij'} = \dim \mathfrak{p}_{ij'}$ ,  $(\xi_1, \dots, \xi_{r_i})$  is a generic zero of  $\mathfrak{p}_{ij'}$ , and therefore there is an isomorphism  $L(\xi_{ij'1}, \dots, \xi_{ij'r_i}) \approx L(\xi_1, \dots, \xi_{r_i})$  over  $L$  with  $\xi_{ij'k} \mapsto \xi_k$  ( $1 \leq k \leq r_i$ ), that is, an isomorphism extending  $id_L$  and  $S_{v, v_{ij'}}^K$ . Therefore  $v_{ij'} \xleftrightarrow{L} v$ , so that  $v$  is an  $L$ -generic element of an  $L$ -component of  $A$ . This shows that the  $L$ -components of each  $V_{ij}$  are  $L$ -components of  $A$ . However, for any element  $v' \in A$ , there is an  $(i, j)$  with  $v_{ij} \xrightarrow{L} v'$  so that  $v_{ij} \xrightarrow{L_0} v'$  and  $v' \in V_{ij}$ . Therefore  $A = \bigcup_{i,j} V_{ij}$  and  $A$  is an  $L_0$ -subset of  $M$ .

The next step is to show that if  $L'$  is an extension of  $K$  such that  $A$  is an  $L'$ -subset of  $M$  and such that  $L' \subset L$ , then  $L_0 \subset L'$ . By Section 5, Theorem 2, each  $L$ -component of  $A$  is an  $L$ -component of some  $L'$ -com-

ponent of  $A$  of the same dimension, and an  $L$ -generic element of the  $L$ -component is also an  $L$ -generic element of the  $L'$ -component. Therefore  $\dim_{L'} v_{ij} = \dim_L v_{ij}$ , so that  $\dim_{L'}(\xi_{ij_1}, \dots, \xi_{ij_{r_i}}) = \dim_L(\xi_{ij_1}, \dots, \xi_{ij_{r_i}})$ , whence  $\dim(\mathfrak{p}_{ij} \cap L'[X_1, \dots, X_{r_i}]) = \dim \mathfrak{p}_{ij}$ . Since  $(\xi_{ij_1}, \dots, \xi_{ij_{r_i}})$  is, like  $v_{ij}$ , separable over  $L'$ , we infer that the ideal  $\mathfrak{p}'_{ij} = \mathfrak{p}_{ij} \cap L'[X_1, \dots, X_{r_i}]$  is prime and separable over  $L'$ , and  $\mathfrak{p}_{ij}$  is a component of  $L\mathfrak{p}'_{ij}$ . If  $(\xi_1, \dots, \xi_{r_i})$  is any generic zero of any component of  $L\mathfrak{p}'_{ij}$ , then  $(\xi_1, \dots, \xi_{r_i})$  is a generic zero of  $\mathfrak{p}'_{ij}$ , so that there exists an isomorphism  $S: L'(\xi_{ij_1}, \dots, \xi_{ij_{r_i}}) \approx L'(\xi_1, \dots, \xi_{r_i})$  over  $L'$  with  $\xi_{ijk} \mapsto \xi_k$  ( $1 \leq k \leq r_i$ ). Hence there exists an element  $v \in M$  with  $v_{ij} \xrightarrow{L'} v$  such that  $L'(v) = L'(\xi_1, \dots, \xi_{r_i})$  and  $S_{v, v_{ij}}^L = S$ . Evidently  $v_{ij} \xrightarrow{K} v$  and  $\dim_L v_{ij} = \dim_L v$ , and  $v$  is an  $L$ -generic element of an  $L$ -component of  $A$  so that  $v \xrightarrow{L} v_{i'j'}$  for some  $(i', j')$ . It follows that  $i' = i$ , so that  $(\xi_1, \dots, \xi_{r_i})$  is a zero of  $\mathfrak{p}_{i'j'}$ . This shows that the components of  $L\mathfrak{p}'_{ij}$  are some of the ideals  $\mathfrak{p}_{i_1}, \dots, \mathfrak{p}_{i_{m_i}}$  including  $\mathfrak{p}_{ij}$ . Therefore

$$\alpha_i = \bigcap_j \mathfrak{p}_{ij} = \bigcap_j L\mathfrak{p}'_{ij} = L \bigcap_j \mathfrak{p}'_{ij} = L \cdot (\alpha_i \cap L'[X_1, \dots, X_{r_i}]),$$

so that  $L'$  is a field of definition of  $\alpha_i$ , whence  $L_i \subset L'$ . Since this is the case for every  $i$ ,  $L_0 \subset L'$ .

The final step is to show that if  $L'$  is any extension of  $K$  (not necessarily contained in  $L$ ) such that  $A$  is an  $L'$ -subset of  $M$ , then  $L_0 \subset L'$ . We have proved above that in the extension  $L$  of  $K$  with the property that  $A$  is an  $L$ -subset of  $M$  there is a smallest extension  $L_0$  of  $K$  with this property. Applying this result to  $LL'$  instead of  $L$ , we see that in  $LL'$  there is a smallest extension  $L_0'$  of  $K$  having this property. Since  $L \subset LL'$  and  $L' \subset LL'$ , we have  $L_0' \subset L$  and  $L_0' \subset L'$ . The former of these two inclusions shows that  $L_0 \subset L_0'$  and then the latter shows that  $L_0 \subset L'$ .

Thus,  $L_0$  is our field  $K(A)$ . It follows from Section 5, Corollary 2 to Theorem 2, that  $L_0$  is a finitely generated extension of  $K$ . In the remainder of the proof we may suppose that the extension  $L$  of  $K$  fixed at the beginning coincides with the field  $L_0 = K(A)$ . Let  $\sigma \in \text{Aut}(U/K)$ . As remarked in the first paragraph of this section,  $\sigma A$  is a  $\sigma L$ -subset of  $M$ , and for each  $L$ -component  $V_{ij}$  of  $A$ ,  $\sigma V_{ij}$  is a  $\sigma L$ -component of  $\sigma A$ . If  $\sigma A = A$ , this implies that  $L = K(A) \subset \sigma L$ , and since the same conclusion holds for  $\sigma^{-1}$  instead of  $\sigma$ , therefore  $\sigma L = L$ . Thus,  $\sigma V_{ij}$  is an  $L$ -component of  $A$ , and  $\dim \sigma V_{ij} = \dim V_{ij}$  so that  $\sigma V_{ij} = V_{i'j'}$  for some  $j'$ . This shows that  $\sigma$  permutes the  $L$ -components  $V_{i_1}, \dots, V_{i_{m_i}}$ , and from this fact it easily follows that  $\sigma$  permutes the prime ideals  $\mathfrak{p}_{i_1}, \dots, \mathfrak{p}_{i_{m_i}}$  so that  $\alpha_i^\sigma = \alpha_i$ . By Chapter I, Section 5, Lemma 3(a), this implies that  $\sigma \in \text{Aut}(U/L_i)$ . Since this occurs for every  $i$ , and  $K(A) = KL_1 \cdots L_{m_i}$ , then  $\sigma \in \text{Aut}(U/K(A))$ . The converse, that if  $\sigma \in \text{Aut}(U/K(A))$ , then  $\sigma A = A$ , is trivial. Therefore the proof of Theorem 4 is complete.

We shall consistently use the notation of Theorem 4; that is, when  $A$  is a closed subset of a homogeneous  $K$ -space  $M$ , we shall denote by  $K(A)$  the smallest extension  $L$  of  $K$  such that  $A$  is an  $L$ -subset of  $M$ . (**Caution:** This is not in keeping with the notation commonly used in algebraic geometry. There, if  $A$  is an algebraic variety defined over  $K$ , then  $K(A)$  denotes the field of rational functions on  $A$  that are defined over  $K$ .) When  $A$  is the set consisting of a single element  $v \in M$ , then  $A$  is closed and  $K(A)$  coincides with the extension  $K(v)$  of  $K$  associated to  $v$  by the  $K$ -set structure of  $M$ .

**Corollary 1** *Let  $A$  be a closed subset of a homogeneous  $K$ -space  $M$ , and let  $\sigma \in \text{Aut}(U/K)$ . Then  $\sigma A$  is a closed subset of  $M$ , and  $K(\sigma A) = \sigma(K(A))$ . If  $\tau \in \text{Aut}(U/K)$ , then  $\tau A = \sigma A$  if and only if  $\tau$  coincides with  $\sigma$  on  $K(A)$ .*

**Corollary 2** *Let  $A$  be a closed subset of a homogeneous  $K$ -space, let  $\Sigma$  be a subset of  $\text{Aut}(U/K)$ , and let  $K'$  denote the field of invariants of  $\Sigma$ . A necessary and sufficient condition that  $A$  be a  $K'$ -set is that  $\sigma A = A$  ( $\sigma \in \Sigma$ ). In particular,  $A$  is  $K$ -closed if and only if  $\sigma A = A$  ( $\sigma \in \text{Aut}(U/K)$ ).*

**REMARK** Let  $L$  be an extension of  $K$  and  $A$  be an  $L$ -subset of a homogeneous  $K$ -space  $M$ . If  $\gamma$  is any isomorphism over  $K$  of  $L$  onto an extension of  $K$  such that  $U$  has the same transcendence degree over  $\gamma L$  as over  $L$ , then  $\gamma$  can be extended to an automorphism  $\sigma$  of  $U$ , and  $\sigma A$  is a  $\gamma L$ -subset of  $M$ . Even though  $\sigma$  is not uniquely determined by  $\gamma$ , Corollary 1 shows that  $\sigma A$  is. Hence  $\sigma A$  can be denoted by  $\gamma A$ . In particular,  $\gamma$  can be an automorphism of  $L$  over  $K$ , and it is easy to see the formula  $(\gamma, A) \mapsto \gamma A$  defines an operation of  $\text{Aut}(L/K)$  on the set of  $L$ -subsets of  $M$ . Corollary 2 shows that when  $L$  is a Galois extension of  $K$ , and we denote its Galois group by  $\mathfrak{g}(L/K)$ , then  $K(A) = K$  if and only if  $\gamma A = A$  ( $\gamma \in \mathfrak{g}(L/K)$ ).

A closed subset  $V$  of the homogeneous  $K$ -space  $M$  for the  $K$ -group  $G$  may be  $K(V)$ -irreducible and not be  $L$ -irreducible for some  $L \supset K(V)$ . When  $V$  is  $L$ -irreducible for every  $L \supset K(V)$  we say that  $V$  is *irreducible*. By Section 5, Theorem 2(b), and the remark just preceding Corollary 1 to that theorem, the closed set  $V$  is irreducible if and only if it is  $K(V)$ -irreducible and has a  $K(V)$ -generic element that is regular over  $K(V)$ . Thus,  $G^\circ$  is irreducible. For any closed subset  $A$  of  $M$ , the  $K(A)_s$ -components of  $A$  are irreducible; we call them the *components* of  $A$ . An irreducible closed (respectively  $K$ -irreducible,  $K$ -closed) subset of  $M$  is connected (respectively  $K$ -connected), but not in general conversely. Since the components (respectively  $K$ -components) of  $M$  are pairwise disjoint, they are the connected (respectively  $K$ -connected) components of  $M$  in the topological sense. In particular, the following five conditions on  $G$  are equivalent:  $G$  is connected;  $G$  is  $K$ -connected;  $G$  is irreducible;  $G$  is  $K$ -irreducible;  $G = G^\circ$ .

**Proposition 3** Let  $M$  be a homogeneous  $K$ -space for the  $K$ -group  $G$ , let  $V$  be a  $K$ -irreducible  $K$ -subset of  $M$ , let  $A$  be a  $K$ -closed subset of  $V$  with  $V \neq A$ , let  $v \in \Gamma_{V/K}$ , and let  $R$  be a subring of  $U$  with  $R \supset K$ . There exists a nonzero element  $\alpha \in R$  with the following property: For every homomorphism  $h: R \rightarrow U$  over  $K$  with  $h(\alpha) \neq 0$ , there exists an element  $v' \in V - A$ , algebraic over  $K(h(R))$  (and separable over  $K(h(R))$ ) if  $v$  is separable over  $K(R)$  such that if  $t \in \Gamma_{G^\circ/K(R)K(v)}$  and  $t' \in \Gamma_{G^\circ/K(h(R))K(v')}$ , then  $h, S_{v',t}, S_{t',t}$  are compatible.

*Proof* Fix  $t \in \Gamma_{G^\circ/K(R)K(v)}$ . By Section 6, Proposition 2, there exists a nonzero element  $\alpha_0 \in K[K(vt) \cup K(t)]$  that vanishes at every element of  $A$ . Put the other way around, if  $\alpha_0$  fails to vanish at a particular  $v' \in V$ , then  $v' \notin A$ .

Fix  $s \in \Gamma_{G^\circ/K(R)K(v)K(t)}$ , and choose elements  $\mu_1, \dots, \mu_l$  such that  $K(\mu_1, \dots, \mu_l) = K(s)$ , elements  $v_1, \dots, v_l$  such that  $K(v_1, \dots, v_l) = K(t)$ , elements  $\xi_1, \dots, \xi_m$  such that  $K(\xi_1, \dots, \xi_m) = K(v)$ , elements  $\eta_1, \dots, \eta_n = K(vs)$ , and elements  $\zeta_1, \dots, \zeta_n$  such that  $K(\zeta_1, \dots, \zeta_n) = K(vt)$ . Now,  $K(v)K(s) = K(vs)K(s) \supset K(v)K(vs)$ ,  $\dim_{K(v)} s = \dim G$ , and (see Section 3, Remark 2 following Theorem 1)  $\dim_{K(v)} vs = \dim M$ . Therefore  $K(\xi_1, \dots, \xi_m, \mu_1, \dots, \mu_l) = K(\eta_1, \dots, \eta_n, \mu_1, \dots, \mu_l)$  and we may suppose that this field is an algebraic extension of  $K(\xi_1, \dots, \xi_m, \eta_1, \dots, \eta_n, \mu_1, \dots, \mu_d)$ , where  $d = \dim G - \dim M$ . It follows that there exist nonzero elements  $\alpha_1 \in K[\eta_1, \dots, \eta_n, \mu_1, \dots, \mu_d]$ ,  $\alpha_2 \in K[\xi_1, \dots, \xi_m, \mu_1, \dots, \mu_d]$ , and  $\alpha_3 \in K[\xi_1, \dots, \xi_m, \eta_1, \dots, \eta_n, \mu_1, \dots, \mu_d]$  such that

$$K[\alpha_1 \xi_1, \dots, \alpha_1 \xi_m] \subset K[\eta_1, \dots, \eta_n, \mu_1, \dots, \mu_d],$$

$$K[\alpha_2 \eta_1, \dots, \alpha_2 \eta_n] \subset K[\xi_1, \dots, \xi_m, \mu_1, \dots, \mu_d],$$

$$\alpha_3 \mu_1, \dots, \alpha_3 \mu_l \text{ are integral over } K[\xi_1, \dots, \xi_m, \eta_1, \dots, \eta_n, \mu_1, \dots, \mu_d].$$

A similar argument shows that there exist nonzero elements  $\alpha_4 \in K[\zeta_1, \dots, \zeta_n, v_1, \dots, v_l]$ ,  $\alpha_5 \in K[\xi_1, \dots, \xi_m, v_1, \dots, v_l]$ , and

$$\alpha_6 \in K[\xi_1, \dots, \xi_m, \zeta_1, \dots, \zeta_n, v_1, \dots, v_d]$$

such that

$$K[\alpha_4 \zeta_1, \dots, \alpha_4 \zeta_n] \subset K[\xi_1, \dots, \xi_m, v_1, \dots, v_l],$$

$$K[\alpha_5 \xi_1, \dots, \alpha_5 \xi_m] \subset K[\xi_1, \dots, \xi_m, v_1, \dots, v_l],$$

$$\alpha_6 v_1, \dots, \alpha_6 v_l \text{ are integral over } K[\xi_1, \dots, \xi_m, \zeta_1, \dots, \zeta_n, v_1, \dots, v_d].$$

Set  $\alpha^* = \alpha_0 \alpha_1 \dots \alpha_6$ .

By Chapter 0, Section 14, Proposition 9(c), there exists a nonzero element  $\alpha' \in R[\xi_1, \dots, \xi_m, \mu_1, \dots, \mu_l, v_1, \dots, v_l]$  such that every homomorphism

$$h': R[\xi_1, \dots, \xi_m, \mu_1, \dots, \mu_l, v_1, \dots, v_l] \rightarrow U$$

with  $h'(\alpha') \neq 0$  can be extended to a homomorphism

$$h^*: R[\xi_1, \dots, \xi_m, \eta_1, \dots, \eta_n, \zeta_1, \dots, \zeta_n, \mu_1, \dots, \mu_l, v_1, \dots, v_l] \rightarrow U$$

with  $h^*(\alpha^*) \neq 0$ . We may write  $\alpha' = \alpha_1' \beta_1' + \dots + \alpha_g' \beta_g'$  with elements  $\alpha_1', \dots, \alpha_g' \in R[\xi_1, \dots, \xi_m]$  different from 0 and elements  $\beta_1', \dots, \beta_g' \in K[\mu_1, \dots, \mu_l, v_1, \dots, v_l]$  that are linearly independent over  $K$ . By linear disjointness then  $\beta_1', \dots, \beta_g'$  are linearly independent over  $R[\xi_1, \dots, \xi_m]$ .

Again by Chapter 0, Section 14, Proposition 9(c), there exists a nonzero element  $\alpha \in R$  such that every homomorphism  $h: R \rightarrow U$  over  $K$  with  $h(\alpha) \neq 0$  can be extended to a homomorphism  $\bar{h}: R[\xi_1, \dots, \xi_m] \rightarrow U$  with  $\bar{h}(\alpha_1') \neq 0$  and  $\bar{h}(R[\xi_1, \dots, \xi_m])$  algebraic over  $h(R)$  (and separable over  $h(R)$  if  $R[\xi_1, \dots, \xi_m]$  is separable over  $R$ ).

Fix

$$t' \in \Gamma_{G^\circ/K(h(R[\xi_1, \dots, \xi_m]))} \quad \text{and} \quad s' \in \Gamma_{G^\circ/K(\bar{h}(R[\xi_1, \dots, \xi_m]))K(t')}.$$

Since  $K(R)K(v), K(s)K(t)$  are linearly disjoint over  $K$ ,  $\bar{h}$  can be extended to a homomorphism

$$h': R[\xi_1, \dots, \xi_m, \mu_1, \dots, \mu_l, v_1, \dots, v_l] \rightarrow U$$

that on  $K[\mu_1, \dots, \mu_l]$  coincides with  $S_{s',s}$  and on  $K[v_1, \dots, v_l]$  coincides with  $S_{t',t}$ . Then  $h'$  maps  $K[\mu_1, \dots, \mu_l, v_1, \dots, v_l]$  isomorphically over  $K$ , so that  $h'(\beta_1'), \dots, h'(\beta_g')$  are linearly independent over  $K$  and therefore, by linear disjointness, are linearly independent over  $h'(R[\xi_1, \dots, \xi_m])$ . Since  $h'(\alpha_1') = \bar{h}(\alpha_1') \neq 0$ , this implies that  $h'(\alpha') = h'(\alpha_1')h'(\beta_1') + \dots + h'(\alpha_g')h'(\beta_g') \neq 0$ . By what we proved in the preceding paragraph, it follows that this  $h'$  can be extended to a homomorphism  $h^*$  as above, with  $h^*(\alpha^*) \neq 0$ .

In what follows we set  $\mu_k' = h^*(\mu_k)$ ,  $v_k' = h^*(v_k)$ ,  $\xi_i' = h^*(\xi_i)$ ,  $\eta_j' = h^*(\eta_j)$ ,  $\zeta_j' = h^*(\zeta_j)$ ,  $K' = Q(h^*(R))$ . Because  $\alpha^* = \alpha_0 \alpha_1 \dots \alpha_6$  and  $h^*(\alpha^*) \neq 0$ , we see from the above that

$$K(\xi_1', \dots, \xi_m', \mu_1', \dots, \mu_l') = K(\eta_1', \dots, \eta_n', \mu_1', \dots, \mu_l'),$$

$$\mu_1', \dots, \mu_l' \text{ are algebraic over } K(\xi_1', \dots, \xi_m', \eta_1', \dots, \eta_n', \mu_1', \dots, \mu_d'),$$

$$K(\xi_1', \dots, \xi_m', v_1', \dots, v_l') = K(\zeta_1', \dots, \zeta_n', v_1', \dots, v_l'),$$

$$v_1', \dots, v_l' \text{ are algebraic over } K(\xi_1', \dots, \xi_m', \zeta_1', \dots, \zeta_n', v_1', \dots, v_d').$$



Therefore, since  $K'(\xi_1', \dots, \xi_m')$  is algebraic over  $K'$ ,

$$\begin{aligned} & \text{tr deg } K(\eta_1', \dots, \eta_n')/K \\ & \geq \text{tr deg } K'(\eta_1', \dots, \eta_n')/K' \\ & = \text{tr deg } K'(\xi_1', \dots, \xi_m', \eta_1', \dots, \eta_n')/K' \\ & = \text{tr deg } K'(\xi_1', \dots, \xi_m', \mu_1', \dots, \mu_l')/K' \\ & \quad - \text{tr deg } K'(\xi_1', \dots, \xi_m', \mu_1', \dots, \mu_l')/K'(\xi_1', \dots, \xi_m', \eta_1', \dots, \eta_n') \\ & \geq \text{tr deg } K'(\mu_1', \dots, \mu_l')/K' - d \\ & = \text{tr deg } K(\mu_1', \dots, \mu_l')/K - (\dim G - \dim M) \\ & = \dim_K s' - \dim G + \dim M \\ & = \dim M = \dim_K vs = \dim_K(\eta_1, \dots, \eta_n), \end{aligned}$$

so that  $h^*$  maps  $K[\eta_1, \dots, \eta_n]$  isomorphically onto  $K[\eta_1', \dots, \eta_n']$ . Hence (see axiom AS 2(b)),  $M$  contains an element, which we shall denote by  $v's'$ , such that  $vs \leftrightarrow v's'$  and such that  $S_{v's', vs}, h^*$  coincide on  $K[\eta_1, \dots, \eta_n]$ . In the same way it follows that  $M$  contains an element  $v''t'$  such that  $vt \leftrightarrow v''t'$  and such that  $S_{v''t', vt}, h^*$  coincide on  $K[\zeta_1, \dots, \zeta_n]$ . It is clear that the five homomorphisms  $h, S_{v's', vs}, S_{v''t', vt}, S_{s', s}, S_{t', t}$  are compatible, so that  $v \rightarrow v'$  and  $v' \in V$ , and (see Section 3, Remark 2 following Proposition 1)  $s^{-1}t \leftrightarrow s'^{-1}t', vt \leftrightarrow v't'$ , and the five homomorphisms and  $S_{v't', vt}$  are compatible. Hence  $S_{v't', vt} = S_{v''t', vt}, v''t' = v't'$ , and  $v'' = v'$ . Furthermore,

$$\begin{aligned} K(v') & \subset K(v's')K(s') = \overline{K(\eta_1', \dots, \eta_n', \mu_1', \dots, \mu_l')} \\ & = K(\xi_1', \dots, \xi_m', \mu_1', \dots, \mu_l') = K(\xi_1', \dots, \xi_m')K(s') \end{aligned}$$

and similarly  $K(v') \subset K(\xi_1' \dots, \xi_m')K(t')$ . Since  $s', t'$  are independent over  $K(\xi_1', \dots, \xi_m')$ , then  $K(v') \subset K(\xi_1', \dots, \xi_m')$ . This shows that  $v'$  is algebraic over the field  $K' = K(h(R))$ , and is separable over  $K'$  when  $v$  is separable over  $K(R)$ . It also shows that  $v', t'$  are independent over  $K$ . Since  $h^*$  extends  $S_{v't', vt}, S_{t', t}$  and since  $h^*(\alpha_0)h^*(\alpha_1) \dots h^*(\alpha_6) = h^*(\alpha) \neq 0$ , we see that  $\alpha_0$  does not vanish at  $v'$  so that  $v' \notin A$ . This completes the proof of Proposition 3.

**Corollary** *If  $B$  is any  $K$ -set, then  $B_{K_s}$  is dense in  $B$ .*

*Proof* We must show that if  $C$  is a closed subset of  $B$  with  $B \neq C$ , then  $B - C$  contains an element that is separable and algebraic over  $K$ . First suppose that  $C$  is  $K$ -closed. Then for some  $K$ -component  $V$  of  $B$  the set  $A = V \cap C$  is  $K$ -closed and distinct from  $V$ . An element  $v \in \Gamma_{V/K}$  is separable over  $K$  and not in  $A$ , so the desired conclusion follows from the proposition.

Now no longer suppose that  $C$  is  $K$ -closed. The intersection  $C' = \bigcap_{\sigma} \sigma C$ , where  $\sigma$  runs over  $\text{Aut}(U/K)$ , is a  $K$ -closed subset of  $C$  (see Corollary 2 to

Theorem 4). By the above,  $B_{K_s}$  contains an element  $v' \notin C'$ . Then  $v' \notin \sigma C$  for some  $\sigma$ , so that  $\sigma^{-1}v' \in B_{K_s}$  and  $\sigma^{-1}v' \notin C$ .

We conclude this section with a criterion for a subset of a  $K$ -closed set to be  $K$ -open in it.

**Proposition 4** *Let  $A$  be a  $K$ -closed subset of a homogeneous  $K$ -space for a  $K$ -group, let  $E$  be a subset of  $A$ , and suppose that the following two conditions are satisfied:*

- (a) *if  $v \in A, v' \in E, v \rightarrow v'$ , then  $v \in E$ ;*
- (b) *if  $V$  is a  $K$ -irreducible subset of  $A$  with  $V \cap E \neq \emptyset$ , then  $V \cap E$  has a nonempty subset that is  $K$ -open in  $V$ .*

*Then  $E$  is  $K$ -open in  $A$ .*

*Proof* If  $V_1, \dots, V_m$  are the  $K_i$ -components of the  $K_i$ -set  $A$ , then  $E = A - \bigcup (V_\mu - (V_\mu \cap E))$ . Hence it suffices to prove for each  $\mu$  that  $V_\mu \cap E$  is  $K$ -open in  $V_\mu$ . Therefore we may suppose that  $A$  is  $K$ -irreducible. We may suppose, too, that  $E \neq \emptyset$ . Taking  $V = A$  in condition (b), we see that some nonempty set  $\emptyset \subset E$  is  $K$ -open in  $A$ . Let  $W_1, \dots, W_n$  denote the  $K_i$ -components of the  $K_i$ -set  $A - \emptyset$ . Clearly,  $\dim W_\nu < \dim A$  for every  $\nu$ . Arguing by induction on  $\dim A$ , we may suppose that  $W_\nu \cap E$  is  $K$ -open in  $W_\nu$ , so that the set  $W'_\nu = W_\nu - (W_\nu \cap E)$  is  $K$ -closed in  $W_\nu$  and hence also in  $A$ . Let  $F$  denote the smallest  $K$ -closed subset of  $A$  containing  $A - E$ . Since

$$\begin{aligned} A - E & = (\emptyset \cup \bigcup W_\nu) - (\emptyset \cup \bigcup (W_\nu \cap E)) \\ & = (\bigcup W_\nu) - (\bigcup (W_\nu - W'_\nu)) \subset \bigcup W'_\nu, \end{aligned}$$

we see that  $F \subset \bigcup W'_\nu$ . For any  $x \in E - \emptyset$ , if  $x \in W_\nu$ , then  $x \in W_\nu \cap E = W_\nu - W'_\nu$ , whence  $x \notin W'_\nu$ , and if  $x \notin W_\nu$ , then again  $x \notin W'_\nu$ . Hence  $x \notin \bigcup W'_\nu$ , so that  $x \in A - F$ . It follows that  $E = \emptyset \cup (A - F)$ , so that  $E$  is  $K$ -open in  $A$ .

### 8 $K$ -Subgroups

Recall (Section 3) that a subset  $H$  of a  $K$ -group  $G$  that is both a subgroup of  $G$  and a  $K$ -subset of  $G$  is a  $K$ -subgroup of  $G$  provided some  $K$ -component of  $H$  that contains 1 has a  $K$ -generic element that is regular over  $K$ . That this is always the case is half the content of the following proposition.

**Proposition 5** *Let  $H$  be a nonempty  $K$ -subset of the  $K$ -group  $G$  such that  $HH \subset H$ . Then  $H$  is a  $K$ -subgroup of  $G$ .*

*Proof* Let  $y \in H$ . Then  $\rho_y$  is an everywhere defined pre- $K(y)$ -mapping of  $G$  into  $G$  with inverse  $\rho_{y^{-1}}$ , so that the set  $Hy = \rho_y(H)$  is a  $K(y)$ -subset of  $G$ , and it obviously has the same number of  $K(y)$ -components of a given dimension as  $H$  has. By hypothesis  $Hy \subset H$ , so that  $Hy = H$ . Therefore  $y \in Hy$ , so that  $1 \in H$ . Hence  $1 \in Hy$ , so that  $y^{-1} \in H$ . This shows that  $H$  is a subgroup of  $G$ .

Every element of  $G$  is regular over  $K_a$ . Therefore  $H$  is a  $K_a$ -subgroup of  $G$ . Let  $y \in \Gamma_{H \circ K_a}$ . By Section 5, Theorem 2,  $y$  is a  $K$ -generic element of a  $K$ -component of  $H$  that contains 1. Therefore it suffices to show that  $y$  is regular over  $K$ . Because  $y \xrightarrow{K_a} 1$  and  $\sigma 1 = 1$  for every  $\sigma \in \text{Aut}(U/K)$ , we infer (see the first paragraph of Section 7) that  $\sigma y \xrightarrow{K_a} 1$ . Because  $\dim_{K_a} \sigma y = \dim_{K_a} y = \dim H^\circ$ ,  $\sigma y \in \Gamma_{H \circ K_a}$  so that  $y \xleftrightarrow{K_a} \sigma y$ . This means that  $S_{\sigma y, y}, id_{K_a}$  are compatible, so that  $\sigma$  leaves invariant every element of  $K(y) \cap K_a$ . Thus,  $K(y) \cap K_a$  is a purely inseparable algebraic extension of  $K$ . However,  $y$  is a  $K$ -generic element of a  $K$ -component of the  $K$ -set  $H$ , so that  $K(y)$  is separable over  $K$ . Therefore  $K(y) \cap K_a = K$ , and  $y$  is regular over  $K$ .

**Proposition 6** *Let  $\mathfrak{h}$  be a subgroup of the  $K$ -group  $G$ , and let  $H$  be the smallest closed subset of  $G$  that contains  $\mathfrak{h}$ . Then  $H$  is a closed subgroup of  $G$ . If  $\sigma \mathfrak{h} = \mathfrak{h}$  for every  $\sigma \in \text{Aut}(U/K)$ , then  $H$  is  $K$ -closed.*

*Proof* For any  $y \in \mathfrak{h}$  and any extension  $L$  of  $K(y)$ ,  $\rho_y: G \rightarrow G$  is a bijective everywhere defined pre- $L$ -mapping with inverse  $\rho_{y^{-1}}$ . It follows that the set  $\rho_y(H) = Hy$  is the smallest closed set containing  $\rho_y(\mathfrak{h}) = \mathfrak{h}y = \mathfrak{h}$ , so that  $Hy = H$ . Thus  $H\mathfrak{h} = H$ . Similarly, for every  $y \in H$ , the set  $\lambda_y(H) = yH$  is the smallest closed set containing  $\lambda_y(\mathfrak{h}) = y\mathfrak{h} \subset H\mathfrak{h} = H$ , so that  $yH \subset H$ ; hence  $HH \subset H$ . By Proposition 5 then  $H$  is a closed subgroup of  $G$ . For every  $\sigma \in \text{Aut}(U/K)$ , evidently  $\sigma H$  is the smallest closed subset of  $G$  that contains  $\sigma \mathfrak{h}$ , so that if  $\sigma \mathfrak{h} = \mathfrak{h}$  for every  $\sigma$ , then  $\sigma H = H$  and, by Section 7, Corollary 2 to Theorem 4,  $H$  is  $K$ -closed.

**Proposition 7** *Let  $G$  be a  $K$ -group, let  $V_1, \dots, V_m$  be  $K$ -irreducible  $K$ -subsets of  $G$  each of which contains 1 and has a  $K$ -generic element that is regular over  $K$ , and let  $H$  denote the subgroup of  $G$  generated by  $V_1 \cup \dots \cup V_m$ . Then  $H$  is a connected  $K$ -subgroup of  $G$ . There exists a number  $n \in \mathbb{N}$  such that a  $K$ -generic element of  $H$  can be written in the form*

$$x_{11} \cdots x_{m1} x_{12} \cdots x_{m2} \cdots x_{1n} \cdots x_{mn},$$

where the family  $(x_{ij})_{1 \leq i \leq m, 1 \leq j \leq n}$  is independent over  $K$  and  $x_{ij} \in \Gamma_{V_{ij}K}$  for every  $(i, j)$ .

**REMARK** Every element  $y \in H$  can be written as a product of two  $K$ -generic elements of  $H$  (take  $t \in \Gamma_{H/K(y)}$  and write  $y = yt^{-1} \cdot t$ ). Therefore  $H = (V_1 \cdots V_m)^{2n}$ .

*Proof* Fix  $x_{ij} \in \Gamma_{V_{ij}K}$  ( $1 \leq i \leq m, 1 \leq j < \infty$ ) so that the family  $(x_{ij})_{1 \leq i \leq m, 1 \leq j < \infty}$  is independent over  $K$ . Define the elements  $y_n$  ( $1 \leq n < \infty$ ) inductively by the formulae  $y_1 = x_{11} \cdots x_{m1}$ ,  $y_n = y_{n-1} x_{1n} \cdots x_{mn}$  ( $n > 1$ ). Evidently  $y_{n-1}, x_{1n}, \dots, x_{mn}$  are independent over  $K$ . Hence, for any  $x_1 \in V_1, \dots, x_m \in V_m$ , we have  $y_n \rightarrow y_{n-1} x_1 \cdots x_m$ . Taking  $x_1 = \dots = x_m = 1$ , we find that  $y_n \rightarrow y_{n-1}$ . As  $y_n$  is obviously regular over  $K$ , the locus  $W_n$  of  $y_n$  over  $K$  is an irreducible  $K$ -subset of  $G$ , and

$$V_1 \cdots V_m \subset W_1 \subset W_2 \subset \dots \subset W_n \subset \dots$$

Since  $\dim W_n \leq \dim G$  for every  $n$ , there exists an index  $n$  such that  $W_n = W_r$  for every  $r > n$ . Setting  $y_n' = y_n^{-1} y_{2n}$ , we see that  $y_n, y_n'$  are independent over  $K$  and that  $y_n' \in \Gamma_{W_n/K}$ . It follows that  $W_n W_n \subset W_n$ , and therefore (by Proposition 5)  $W_n$  is a connected  $K$ -subgroup of  $G$  that contains  $V_1 \cdots V_m$  and hence contains  $H$ . Any  $K$ -generic element of  $W_n$  is, like  $y_n$ , an element of  $H$ . As each element of  $W_n$  is a product of two  $K$ -generic elements, we conclude that  $H = W_n$ .

**9  $K$ -Homomorphisms**

It is easy to verify that a  $K$ -homomorphism of  $K$ -groups (or of homogeneous  $K$ -spaces for a  $K$ -group) is also an  $L$ -homomorphism for every extension  $L$  of  $K$ . (Indeed, since this refers to the induced structures of  $L$ -group (or of homogeneous  $L$ -space), it is enough to check that it is an  $(L, K)$ -homomorphism.) Therefore the following result is applicable to such  $K$ -homomorphisms.

**Proposition 8** *Let  $A$  and  $B$  be  $K$ -sets,  $L$  be an extension of  $K$ , and  $f$  be a pre- $K$ -mapping of  $A$  into  $B$  that is also a pre- $L$ -mapping. Then  $f$  is separable as a pre- $K$ -mapping if and only if it is separable as a pre- $L$ -mapping.*

*Proof* Let  $v$  be an  $L$ -generic element of an  $L$ -component of  $A$ . Then  $v$  is a  $K$ -generic element of a  $K$ -component of  $A$ , and  $L, K(v)$  are algebraically disjoint over  $K$ .

If  $f$  is separable as a pre- $K$ -mapping, then  $K(v)$  has a separating transcendence basis over  $K(f(v))$ . As this is evidently a separating transcendence basis also of  $L(v)$  over  $L(f(v))$ ,  $f$  is separable as a pre- $L$ -mapping.

Conversely, suppose  $f$  separable as a pre- $L$ -mapping. Then, for some finitely generated extension  $L'$  of  $K$ ,  $f$  is separable as a pre- $L'$ -mapping.

Replacing  $L$  by  $L'$ , we may suppose that  $L$  is finitely generated over  $K$ . Arguing by induction on the number of generators, we may even suppose that  $L = K(\alpha)$  where the element  $\alpha$  of  $L$  either is transcendental over  $K$ , or is separably algebraic over  $K$ , or has the property that  $\alpha^p \in K$ ,  $\alpha \notin K$ ,  $p \neq 0$ . Let  $\mathfrak{X}$  be a finite set of generators of  $K(v)$  over  $K(f(v))$ . Then  $\mathfrak{X}$  is a finite set of generators of  $L(v)$  over  $L(f(v))$ , so that some subset  $\mathfrak{X}'$  of  $\mathfrak{X}$  is a separating transcendence basis of  $L(v)$  over  $L(f(v))$ , and every element of  $K(v)$  is separably algebraic over  $L(f(v))(\mathfrak{X}') = K(f(v))(\mathfrak{X}')(\alpha)$ . If  $\alpha$  is separably algebraic over  $K$ , then  $K(f(v))(\mathfrak{X}')(\alpha)$  is separably algebraic over  $K(f(v))(\mathfrak{X}')$ . In the other two cases it is easy to see that  $K(v), K(f(v))(\mathfrak{X}')(\alpha)$  are linearly disjoint over  $K(f(v))(\mathfrak{X}')$  (because  $K(v), K(\alpha)$  are linearly disjoint over  $K$ ). Hence in all three cases every element of  $K(v)$  is separably algebraic over  $K(f(v))(\mathfrak{X}')$ , and therefore  $K(v)$  is separable over  $K(f(v))$ . As every  $K$ -component of  $A$  has a  $K$ -generic element that is an  $L$ -generic element of an  $L$ -component of  $A$ , this shows that  $f$  is separable as a pre- $K$ -mapping and completes the proof of the proposition.

A  $K$ -homomorphism is actually determined by weaker conditions than those given in its definition. Recall (Section 3, Remark 1 following Theorem 1) that if  $M$  is a homogeneous  $K$ -space for a  $K$ -group  $G$  and if  $v \in M$ ,  $x \in \Gamma_{G/K(v)}$ , then  $vx \in \Gamma_{M/K}$ . By a *pre- $K$ -homomorphism* of  $G$  into a  $K$ -group  $H$  we mean a pre- $K$ -mapping  $f_0$  of  $G$  into  $H$  such that  $f_0(x'x) = f_0(x')f_0(x)$  whenever  $x' \in G_{f_0}$  and  $x \in \Gamma_{G/K(x)}$  ( $G_{f_0}$  denoting the subset of  $G$  on which  $f_0$  is defined). Similarly, if  $M$  and  $N$  are homogeneous  $K$ -spaces for  $G$ , by a *pre- $K$ -homomorphism* of  $M$  into  $N$  we mean a pre- $K$ -mapping  $f_0$  of  $M$  into  $N$  such that  $f_0(vx) = f_0(v)x$  whenever  $v \in M_{f_0}$  and  $x \in \Gamma_{G/K(v)}$ .

If  $f$  is a  $K$ -homomorphism of  $G$  into  $H$ , and  $G_0$  is any subset of  $G$  that contains  $\Gamma_{G/K}$  and contains an element  $x \in G$  whenever it contains an element  $x'$  with  $x \rightarrow x'$ , then the restriction of  $f$  to  $G_0$  is a pre- $K$ -homomorphism of  $G$  into  $H$ . In particular, we may take  $G_0 = \Gamma_{G/K}$ . A similar circumstance obtains for a  $K$ -homomorphism of  $M$  into  $N$ . Conversely, we have the following result.

**Proposition 9** *A pre- $K$ -homomorphism (either of  $K$ -groups, or of homogeneous  $K$ -spaces for a  $K$ -group) can be extended to a unique homomorphism (of the groups, or of the homogeneous spaces), and this homomorphism is a  $K$ -homomorphism.*

*Proof* We give the proof for  $K$  groups; the proof for homogeneous  $K$  spaces is the same. For any  $x \in G$ , we can fix  $s \in \Gamma_{G^0/K(x)}$  and then write  $x = xs^{-1} \cdot s$ ; hence  $G = \Gamma_{G/K} \cdot \Gamma_{G/K}$ . It follows that if the pre  $K$  homomorphism  $f_0$  can be extended to a homomorphism  $f$ , then  $f$  is unique.

We claim that if  $x_1, x_2, x_1', x_2' \in G_{f_0}$  and  $x_1 x_2 = x_1' x_2'$ , then  $f_0(x_1)f_0(x_2) = f_0(x_1')f_0(x_2')$ . Indeed, fix  $s \in \Gamma_{G^0/G(x_1)K(x_2)K(x_1')K(x_2')}$ . Then also  $x_2 s \in \Gamma_{G/K(x_1)}$  so that

$$f_0(x_1 x_2 s) = f_0(x_1)f_0(x_2 s) = f_0(x_1)f_0(x_2)f_0(s),$$

and similarly

$$f_0(x_1' x_2' s) = f_0(x_1')f_0(x_2')f_0(s),$$

whence  $f_0(x_1)f_0(x_2) = f_0(x_1')f_0(x_2')$ .

This being the case, given  $x \in G$ , we can define  $f(x) = f_0(x)f_0(x_2)$ , where  $x_1, x_2$  are any elements of  $G_{f_0}$  with  $x_1 x_2 = x$ . For any  $x, x' \in G$  we can fix

$$s \in \Gamma_{G^0/K(x)K(x')} \quad \text{and} \quad s' \in \Gamma_{G^0/K(x)K(x')K(s)}$$

and then perform the computation

$$\begin{aligned} f(xx') &= f(xs^{-1} \cdot sx') = f_0(xs^{-1})f_0(sx') \\ &= f_0(xs^{-1})f_0(sx's'^{-1}s') \\ &= f_0(xs^{-1})f_0(sx's'^{-1})f_0(s') \\ &= f_0(xs^{-1})f_0(s)f_0(x's'^{-1})f_0(s') \\ &= f(x)f(x'). \end{aligned}$$

This shows that  $f$  is a homomorphism. When  $x \in G_{f_0}$ , then

$$f(x) = f(xs^{-1} \cdot s) = f_0(xs^{-1})f_0(s) = f_0(x)f_0(s^{-1})f_0(s) = f_0(x)f(1) = f_0(x).$$

Therefore  $f$  is an extension of  $f_0$ .

It remains to show that  $f$  is a pre- $K$ -mapping. Keeping the same notation, we find that  $K(f(x)) = K(f_0(xs^{-1})f_0(s)) \subset K(xs^{-1})K(s) = K(x)K(s)$ , and similarly that  $K(f(x)) \subset K(x)K(s')$ . Since  $K(x)K(s)$  and  $K(x)K(s')$  are evidently linearly disjoint over  $K(x)$ , we conclude that  $K(f(x)) \subset K(x)$ . If  $x \rightarrow x'$ , then  $xs \leftrightarrow x's'$ ,  $s \leftrightarrow s'$  and the isomorphisms  $S_{x's', xs}, S_{s', s}$  are compatible; then  $f_0(xs) \leftrightarrow f_0(x's')$ ,  $f_0(s) \leftrightarrow f_0(s')$ , and  $S_{f_0(x's'), f_0(xs)}, S_{f_0(s'), f_0(s)}$  are compatible, so that  $f_0(xs)f_0(s)^{-1} \rightarrow f_0(x's')f_0(s')^{-1}$ , that is,  $f(x) \rightarrow f(x')$ . If  $x \leftrightarrow x'$ , then  $S_{x', x}, S_{s', s}$  are compatible, that is, extend to an isomorphism  $S : K(x)K(s) \approx K(x')K(s)$ ; this  $S$  extends  $S_{x's', xs}$  too, and therefore extends  $S_{f_0(x's'), f_0(xs)}, S_{f_0(s'), f_0(s)}$ , and hence also extends

$$S_{f_0(x's')f_0(s')^{-1}, f_0(xs)f_0(s)^{-1}} = S_{f(x'), f(x)}.$$

This shows that  $f$  is a pre- $K$ -mapping, and completes the proof.

**Corollary 1** *Let  $G$  and  $H$  be  $K$ -groups, and let  $M$  and  $N$  be homogeneous  $K$ -spaces for  $G$ . Let  $f$  be a homomorphism of groups  $G \rightarrow H$  (or of homo-*

ogeneous spaces  $M \rightarrow N$ ). If the restriction of  $f$  to  $\Gamma_{G/K}$  (or to  $\Gamma_{M/K}$ ) is a pre- $K$ -mapping, then  $f$  is a  $K$ -homomorphism.

**Corollary 2** Let  $f$  be a  $K_s$ -homomorphism of  $K$ -groups  $G \rightarrow H$  (or of homogeneous  $K$ -spaces  $M \rightarrow N$ ). If  $\sigma(f(v)) = f(\sigma v)$  for every  $v \in \Gamma_{G/K}$  (or  $\Gamma_{M/K}$ ) and every  $\sigma \in \text{Aut}(U/K)$ , then  $f$  is a  $K$ -homomorphism.

*Proof* For any  $v \in \Gamma_{G/K}$  (or  $\Gamma_{M/K}$ ),  $\sigma(f(v)) = f(\sigma v) = f(v)$  ( $\sigma \in \text{Aut}(U/K(v))$ ), so that every element of  $K(f(v))$  is purely inseparably algebraic over  $K(v)$ ; however,  $K_s(f(v)) \subset K_s(v)$ , so that every element of  $K(f(v))$  is separably algebraic over  $K(v)$ ; hence  $K(f(v)) \subset K(v)$ . Starting afresh, if  $v, v' \in \Gamma_{G/K}$  (or  $\Gamma_{M/K}$ ) and  $v \mapsto v'$ , then  $v' = \sigma v$  for some  $\sigma \in \text{Aut}(U/K)$ , so that  $\sigma(f(v)) = f(v')$ ; therefore  $f(v) \mapsto f(v')$  and  $S_{v',v}$  is an extension of  $S_{f(v'),f(v)}$ . Thus, the restriction of  $f$  to  $\Gamma_{G/K}$  (or  $\Gamma_{M/K}$ ) is a pre- $K$ -mapping, and  $f$  is a  $K$ -homomorphism by Corollary 1.

The following result will make it possible to consider a  $K$ -homomorphism of  $K$ -groups as a  $K$ -homomorphism of homogeneous  $K$ -spaces. See the remark following the proof.

**Proposition 10** Let  $f: G \rightarrow H$  be a  $K$ -homomorphism of  $K$ -groups.

- (a) The image  $f(G)$  is a  $K$ -subgroup of  $H$ .
- (b) If  $f$  is surjective, and if  $N$  is a homogeneous  $K$ -space for  $H$ , then  $f$  induces on the  $K$ -set  $N$  a structure of homogeneous  $K$ -space for  $G$ , the external law of composition  $N \times G \rightarrow N$  being given by the formula  $(w, x) \mapsto wf(x)$ .

*Proof* (a) Let  $X_1, \dots, X_m$  be the  $K$ -components of  $G$ , let  $x_i \in \Gamma_{X_i/K}$ , let  $Y_i$  be the locus of  $f(x_i)$  over  $K$ , and set  $G' = Y_1 \cup \dots \cup Y_m$ . Then  $G'$  is the smallest  $K$ -set in  $H$  that contains  $f(G)$ . Replacing  $K$  by  $K_i$ , we see that  $G'$  is the smallest  $K$ -closed set in  $H$  that contains  $f(G)$ . It follows from Section 8, Proposition 6, that  $G'$  is a  $K$ -subgroup of  $H$ . Every element of  $\Gamma_{G'/K}$  is of the form  $f(x)$ , where  $x \in \Gamma_{G/K}$ , and hence is in  $f(G)$ . Since every element of  $G'$  can be expressed as a product of two elements of  $\Gamma_{G'/K}$ ,  $G' \subset f(G)f(G) = f(G)$ . Therefore  $f(G) = G'$ , so that  $f(G)$  is a  $K$ -subgroup of  $H$ .

(b) It is easy to see that the indicated external law of composition makes  $N$  a homogeneous space for the group  $G$ , and to verify the axioms AH 1(a), AH 2(a). The only sticky point is AH 2(b). Consider elements  $x, x' \in G$  with  $x \mapsto x'$  and elements  $w, w' \in N$  with  $w \mapsto w'$ . The locus  $X$  of  $x$  over  $K$  is certainly a  $K_a$ -subset of  $G$  and contains  $x'$ ; choose a  $K_a$ -generic element  $x^*$  of a  $K_a$ -component of  $X$  containing  $x'$ . The locus  $W$  of  $w$  over  $K$  is a  $K_a$ -subset of  $N$  containing  $w'$ ; choose a  $K_a$ -generic element  $w^*$  of a  $K_a$ -component of  $W$  containing  $w'$  such that  $w^*, x^*$  are quasi-independent (and

therefore independent) over  $K_a$ . We then see that

$$w \longleftrightarrow w^*, \quad x \longleftrightarrow x^*,$$

and also that

$$w^* \xrightarrow{K_a} w', \quad x^* \xrightarrow{K_a} x', \quad f(x^*) \xrightarrow{K_a} f(x')$$

and that  $w^*$  and  $f(x^*)$  are independent over  $K_a$ . Hence, by Section 3, Proposition 1(d),  $w^*f(x^*) \xrightarrow{K_a} w'f(x')$ , so that, *a fortiori*,  $w^*f(x^*) \longrightarrow w'f(x')$ .

Now suppose that

$$w^*f(x^*) \longleftrightarrow w'f(x'), \quad x^* \longleftrightarrow x'$$

and hence, by axiom AS 1(a), also

$$w^*f(x^*) \xleftrightarrow{K_a} w'f(x'), \quad x^* \xleftrightarrow{K_a} x'.$$

To verify axiom AH 2(b) it remains to show that the isomorphisms

$$S_{w'f(x'), w^*f(x^*)}, \quad S_{x', x^*}$$

are compatible. To this end, fix an element

$$t \in \Gamma_{H^0/K(w^*)K(w')K(x^*)K(x')K_a}.$$

By Section 3, Remark 2 following the proof of Theorem 1,  $w^*t \xleftrightarrow{K_a} w't$  and the two isomorphisms

$$S_{w't, w^*t}, \quad S_{t, t}$$

are compatible. Because the fields  $K(w^*t)K(t)K_a$  and  $K(x^*)K_a$  are linearly disjoint over  $K_a$ ,  $S_{x', x^*}$  and the preceding two isomorphisms are compatible, and hence the four isomorphisms

$$S_{w't, w^*t}, \quad S_{t, t}, \quad S_{x', x^*}, \quad S_{f(x'), f(x^*)}$$

are compatible. Referring to Section 3, Remark 2 following Proposition 1, we see that  $t^{-1}f(x^*) \longleftrightarrow t^{-1}f(x')$  and that  $S_{t^{-1}f(x'), t^{-1}f(x^*)}$  and the preceding four isomorphisms are compatible, and hence that  $S_{w'f(x'), w^*f(x^*)}, S_{x', x^*}$  are compatible. This completes the proof.

**REMARK** A  $K$ -homomorphism  $f: G \rightarrow H$  can be considered as a surjective  $K$ -homomorphism of  $G$  into  $f(G)$  (which is, by part (a) of the proposition, a  $K$ -group). By part (b) then  $f$  induces on the regular  $K$ -space for  $f(G)$  a structure of homogeneous  $K$ -space for  $G$ . It is clear that  $f$  is a  $K$ -homomorphism, into this homogeneous  $K$ -space for  $G$ , of the regular  $K$ -space for  $G$ . Because of this, results about  $K$ -homomorphisms of homogeneous  $K$ -spaces yield, as special cases, results about  $K$ -homomorphisms of  $K$ -groups.

**Theorem 5** Let  $f: M \rightarrow N$  be a  $K$ -homomorphism of homogeneous  $K$ -spaces for a  $K$ -group  $G$ .

(a) If  $A$  is a  $K$ -subset of  $M$  and  $C$  denotes the smallest closed subset of  $N$  containing  $f(A)$ , then  $C$  is a  $K$ -subset of  $N$  and  $f(A)$  has a subset that is  $K$ -open and dense in  $C$ .

(b)  $f(M) = N$  and  $f(\Gamma_{M/K}) = \Gamma_{N/K}$ .

(c) If  $B$  is a  $K$ -subset of  $N$ , then  $f^{-1}(B)$  is a  $K$ -closed subset of  $M$  and

$$\dim f^{-1}(B) - \dim B = \dim M - \dim N.$$

When  $f$  is separable, then every  $K_i$ -component of  $f^{-1}(B)$  of dimension equal to  $\dim B + \dim M - \dim N$  is a  $K$ -set.

*Proof* (a) Let  $V_1, \dots, V_m$  be the  $K$ -components of  $A$ , let  $v_i \in \Gamma_{V_i/K}$ , set  $w_i = f(v_i)$ , and let  $W_i$  denote the locus of  $w_i$  over  $K$ . Then  $W_i$  is a  $K$ -irreducible  $K$ -subset of  $N$ , and  $W_1 \cup \dots \cup W_m$  is the smallest  $K$ -closed subset of  $N$  containing  $f(A)$ . For any  $\sigma \in \text{Aut}(U/K)$ ,  $\sigma C$  is the smallest closed set containing  $\sigma(f(A)) = f(\sigma A) = f(A)$ , so that  $\sigma C = C$ . By Section 7, Corollary 2 to Theorem 4, then  $C$  is  $K$ -closed. Therefore  $C = W_1 \cup \dots \cup W_m$ .

Fix  $s \in \Gamma_{G^\circ/K(v_i)}$ ; obviously  $s \in \Gamma_{G^\circ/K(w_i)}$ . For any  $w \in W_i$ ,  $w_i \rightarrow w$ , and hence there is a homomorphism

$$h: K[K(w_i s) \cup K(s)] \rightarrow K[K(ws') \cup K(s')]$$

that extends  $S_{ws', w_i s}, S_{s', s}$  (where  $s' \in \Gamma_{G^\circ/K(w)}$ ). By Section 7, Proposition 3 (with  $V = V_i$ ,  $R = K[K(w_i s) \cup K(s)]$ ), there exists a nonzero element  $\alpha \in K[K(w_i s) \cup K(s)]$  with the following property: If  $h(\alpha) \neq 0$ , then there is an element  $v \in V_i$  such that, when  $t \in \Gamma_{G^\circ/K(w_i)K(s)K(v_i)}$  and  $t' \in \Gamma_{G^\circ/K(w)K(s')K(v)}$ , the homomorphisms  $h, S_{vt', v_i t}, S_{t', t}$  are compatible. Since the isomorphism  $S_{f(v)t', w_i t} = S_{f(vt'), f(v)t}$  is a restriction of  $S_{vt', v_i t}$ , this shows that the isomorphisms  $S_{ws', w_i s}, S_{s', s}, S_{f(v)t', w_i t}, S_{t', t}$  are compatible, and hence so are these and  $S_{s^{-1}t', s^{-1}t}$ , and therefore  $S_{wt', w_i t}, S_{f(v)t', w_i t}$  are compatible. Hence  $wt' = f(v)t'$ ,  $w = f(v)$ . By Section 6, Proposition 2, the set  $W_i'$  of elements  $w \in W_i$  with  $h(\alpha) = 0$  is a  $K$ -closed proper subset of  $W_i$ , and what we have just proved is that if  $w \in W_i - W_i'$ , then  $w \in f(V_i)$ . Thus,  $f(A)$  contains the  $K$ -open dense subset  $C - W_1' \cup \dots \cup W_m'$  of  $C$ .

(b) Consider the above in the special case in which  $A = M$ . For any  $v \in M$ ,  $f(vG) = f(v)G = N$ , so that  $f(M) = N$  and in this case  $C = N$ . Thus, every  $K$ -component of  $N$  is one of the sets  $W_i$ . However, for any  $W_i$  evidently  $v_i s \leftrightarrow v_i$ , whence  $w_i s = f(v_i s) \leftrightarrow f(v_i) = w_i$  so that  $\dim W_i = \dim_K w_i s = \dim N$ , and hence  $W_i$  is a  $K$ -component of  $N$ . Since evidently  $f(\Gamma_{V_i/K}) = \Gamma_{W_i/K}$ , this shows that  $f(\Gamma_{M/K}) = \Gamma_{N/K}$ .

(c) Continue the same notation (still taking  $A = M$ ). By Section 6, Proposition 2, the  $K$ -closed set  $B \cap W_i$  is the set of zeros in  $W_i$  of a subset

$b_i$  of  $K[K(w_i t) \cup K(t)]$ . Of course,  $b_i$  is a subset also of  $K[K(v_i t) \cup K(t)]$ , and the set  $A_i$  of zeros of  $b_i$  in  $V_i$  is a  $K$ -closed subset of  $V_i$ . Consider any element  $v \in V_i$ , and fix an element  $t' \in \Gamma_{G^\circ/K(v)}$ . Then  $v \in f^{-1}(B)$  if and only if  $f(v) \in B \cap W_i$ , that is, if and only if the homomorphism

$$K[K(w_i t) \cup K(t)] \rightarrow K[K(f(v)t') \cup K(t')]$$

that extends  $S_{f(v)t', w_i t}$  and  $S_{t', t}$  annihilates  $b_i$ . However, this homomorphism is a restriction of the homomorphism

$$K[K(v_i t) \cup K(t)] \rightarrow K[K(vt') \cup K(t')]$$

that extends  $S_{vt', v_i t}$  and  $S_{t', t}$  so that  $v \in f^{-1}(B)$  if and only if  $v \in A_i$ . Therefore  $f^{-1}(B) = A_1 \cup \dots \cup A_m$  and  $f^{-1}(B)$  is  $K$ -closed.

Consider any  $K$ -component  $W$  of  $B$ . Then  $f^{-1}(W)$  is  $K$ -closed. Let  $V$  be a  $K_i$ -component of  $f^{-1}(W)$ , and fix  $v \in \Gamma_{V/K}$  and  $t' \in \Gamma_{G^\circ/K(v)}$ . Then

$$\begin{aligned} \dim_K v &= \dim_{K(t')} v = \dim_{K(t')} vt' \\ &= \dim_{K(t')} f(v)t' + \dim_{K(t')K(f(v)t')} vt' \\ &\leq \dim_{K(t')} f(v) + \dim_{K(f(v)t')} vt' \\ &= \dim_K f(v) + \dim_K vt' - \dim_K f(v)t' \\ &= \dim_K f(v) + \dim M - \dim N. \end{aligned}$$

It follows that

$$\dim V \leq \dim W + \dim M - \dim N,$$

and that if  $f(v) \notin \Gamma_W$ , then this inequality is a strict one. Of course, for at least one  $K_i$ -component  $V$ ,  $f(v) \in \Gamma_{W/K}$ . Supposing that this is the case, we see by Section 2, Lemma 1 (with  $L = K(f(v))K(t')$ ,  $L_0 = K(f(v)t')$ ,  $m = 1$ ), that there exist elements  $u_1, \dots, u_n \in M$  such that  $vt' \leftrightarrow u_j t' (1 \leq j \leq n)$ ,  $id_{K(f(v)t')}$  and  $S_{u_j t', vt'}$  are bicompatible ( $1 \leq j \leq n$ ) and the following three conditions are satisfied:

(a) Whenever  $v' \in M$ ,  $vt' \leftrightarrow v'$ , and  $id_{K(f(v)t')}$  and  $S_{v', vt'}$  are compatible, then for some index  $j$ ,  $id_{K(f(v))K(t')}$  and  $S_{v', u_j t'}$  are compatible.

(b)  $\dim_{K(f(v))K(t')} u_j t' = \dim_{K(f(v)t'} vt' (1 \leq j \leq n)$ .

(c) If  $K(vt')$  is separable over  $K(f(v)t')$ , then  $K(f(v))K(t')K(u_j t')$  is separable over  $K(f(v))K(t') (1 \leq j \leq n)$ .

Because  $id_{K(f(v)t')}$  and  $S_{u_j t', vt'}$  are compatible, so are  $S_{f(v)t', f(v)t'}$  and  $S_{f(u_j)t', f(v)t'}$ ; hence  $f(u_j)t' = f(v)t'$  so that  $f(u_j) = f(v) \in \Gamma_{W/K}$  and  $u_j \in f^{-1}(W) (1 \leq j \leq n)$ . Because  $vt' \leftrightarrow vt'$ , and  $id_{K(f(v)t')}$  and  $S_{vt', vt'}$  are compatible, condition (a) implies that, for some index  $j$ ,  $id_{K(f(v))K(t')}$  and  $S_{vt', u_j t'}$  are compatible, so that  $S_{vt', vt'}$  and  $S_{vt', u_j t'}$  are compatible, whence  $u_j \rightarrow v$ .

Since  $u_j \in f^{-1}(W)$  and  $v \in \Gamma_{V/K} \subset \Gamma_{f^{-1}(W)/K}$ , this means that  $u_j \leftrightarrow v$  so that  $u_j \in \Gamma_{V/K}$ . Therefore

$$\begin{aligned} \dim V &= \dim_K u_j = \dim_K f(u_j) + \dim_{K(f(u_j))} u_j \\ &= \dim W + \dim_{K(f(v))} u_j \\ &\geq \dim W + \dim_{K(f(v))K(t')} u_j \\ &= \dim W + \dim_{K(f(v))K(t')} u_j t' \\ &= \dim W + \dim_{K(f(v)t'} vt' \quad (\text{by condition (b)}) \\ &= \dim W + \dim_K vt' - \dim_K f(v)t' \\ &= \dim W + \dim M - \dim N. \end{aligned}$$

Together with the previous inequality this shows that  $\dim V = \dim W + \dim M - \dim N$ . Furthermore, when  $f$  is separable, then, because of condition (c), the field  $K(f(v))K(t')K(u_j t') = K(t')K(u_j)$  is separable over  $K(f(v))$  because  $t' \in \Gamma_{G^\circ/K(f(v))}$  and  $G^\circ$  is a  $K(f(v))$ -set, and  $K(f(v))$  is separable over  $K$  because  $f(v) \in \Gamma_{W/K}$  and  $W$  is a  $K$ -set. Therefore  $K(t')K(u_j)$  is separable over  $K$ . Thus, the element  $u_j \in \Gamma_{V/K}$  is separable over  $K$ , so that  $V$  is a  $K$ -set.

**Corollary 1** *A  $K$ -homomorphism of homogeneous  $K$ -spaces is  $K$ -continuous (and therefore  $L$ -continuous for every extension  $L$  of  $K$ , and therefore continuous).*

*Proof* Apply part (c) of the theorem to  $f$  considered as a  $K_1$ -homomorphism.

**Corollary 2** *If  $f: G \rightarrow H$  is a  $K$ -homomorphism of  $K$ -groups, then the image of  $f$  is a  $K$ -subgroup of  $H$ , the kernel of  $f$  is a normal  $K$ -closed subgroup of  $G$ , and*

$$\dim \text{Ker}(f) + \dim \text{Im}(f) = \dim G.$$

*When  $f$  is separable, then the kernel is a  $K$ -subgroup of  $G$ .*

**Corollary 3** *Let  $f: M \rightarrow N$  and  $g: N \rightarrow P$  be  $K$ -homomorphisms of homogeneous  $K$ -spaces. If  $f$  and  $g$  are separable, then  $g \circ f$  is separable.*

*Proof* By part (b) of the theorem, if  $v \in \Gamma_{M/K}$ , then  $f(v) \in \Gamma_{N/K}$ , and therefore  $K(v)$  is separable over  $K(f(v))$  and  $K(f(v))$  is separable over  $K(g(f(v)))$ , so that  $v$  is separable over  $K(g(f(v)))$ .

**Corollary 4** *A  $K$ -homomorphism  $f: M \rightarrow N$  of homogeneous  $K$ -spaces that is injective and separable is a  $K$ -isomorphism.*

*Proof* By part (b) of the theorem,  $f$  is bijective and maps  $\Gamma_{M/K}$  onto  $\Gamma_{N/K}$ . If  $v \in \Gamma_{M/K}$ , then  $K(v)$  is separable over  $K(f(v))$ . For every  $\sigma \in \text{Aut}(U/K(f(v)))$ ,  $f(\sigma v) = \sigma(f(v)) = f(v)$  whence  $\sigma v = v$ , so that  $K(v) = K(f(v))$ . Thus, if  $w \in \Gamma_{N/K}$ , then  $K(w) = K(f^{-1}(w))$ . If  $v, v' \in \Gamma_{M/K}$  and  $f(v) \leftrightarrow f(v')$ , then, for some  $\sigma \in \text{Aut}(U/K)$ ,  $\sigma(f(v)) = f(v')$ , whence  $f(\sigma v) = f(v')$  so that  $\sigma v = v'$ ; hence  $v \leftrightarrow v'$  and  $S_{f(v), f(v)} = S_{v', v}$ . Thus, if  $w, w' \in \Gamma_{N/K}$  and  $w \leftrightarrow w'$ , then  $f^{-1}(w) \leftrightarrow f^{-1}(w')$  and  $S_{w', w} = S_{f^{-1}(w'), f^{-1}(w)}$ . This shows that the restriction of  $f^{-1}$  to  $\Gamma_{N/K}$  is a pre- $K$ -mapping of  $N$  into  $M$ . It is obvious that  $f^{-1}$  is a homomorphism of homogeneous spaces. Hence, by Corollary 1 to Proposition 9,  $f^{-1}$  is a  $K$ -homomorphism so that  $f$  is a  $K$ -isomorphism.

**Corollary 5** *A  $K$ -homomorphism  $f: G \rightarrow H$  of  $K$ -groups that is bijective and separable is a  $K$ -isomorphism.*

*Proof* By the remark following Proposition 10,  $f$  can be regarded as a  $K$ -homomorphism of homogeneous  $K$ -spaces for  $G$ . Therefore Corollary 4 applies.

When a group  $g$  operates on a set  $m$  (say on the right), and  $v \in m$ , the set of elements  $x \in g$  such that  $vx = v$  is a subgroup of  $g$ ; it is called the *stability* (or sometimes the *isotropy*) *group* of  $v$  in  $g$ , and is denoted by  $g_v$ .

**Corollary 6** *Let  $M$  be a homogeneous  $K$ -space for a  $K$ -group  $G$ , and let  $v \in M$ . The stability group  $G_v$  is a  $K(v)$ -closed subgroup of  $G$  and  $\dim G_v = \dim G - \dim M$ .*

*Proof* The mapping  $\lambda_v: G \rightarrow M$  defined by the formula  $\lambda_v(x) = vx$  is a  $K(v)$ -homomorphism of the regular  $K(v)$ -space for  $G$  into  $M$ , and  $G_v = \lambda_v^{-1}(v)$ . Since the set  $\{v\}$  is a  $K(v)$ -subset of  $M$  of dimension 0, part (c) of the theorem applies.

EXERCISE

- Let  $M$  be a homogeneous  $K$ -space for a  $K$ -group  $G$ , let  $A$  and  $B$  be subsets of  $M$  and suppose that  $B$  is  $K$ -closed. The *transporter* of  $A$  into  $B$  is the set  $T_{A, B}$  of all elements  $x \in G$  such that  $Ax \subset B$ . Prove that  $T_{A, B}$  is closed, and that if  $A$  is  $K$ -closed, then  $T_{A, B}$  is  $K$ -closed.

10 Direct products

Let  $G_1, \dots, G_n$  be  $K$ -groups. By a *direct product of the  $K$ -groups  $G_1, \dots, G_n$* , we mean a  $K$ -group  $G$ , together with  $K$ -homomorphisms  $p_j: G \rightarrow G_j$

( $1 \leq j \leq n$ ) of  $K$ -groups, enjoying the following property: Whenever  $H$  is a  $K$ -group with  $K$ -homomorphisms  $q_j: H \rightarrow G_j$  ( $1 \leq j \leq n$ ), then there exists a unique  $K$ -homomorphism  $f: H \rightarrow G$  such that  $p_j \circ f = q_j$  ( $1 \leq j \leq n$ ). The  $K$ -homomorphisms  $p_j$  are then called the *projections* of the direct product. If we take for  $H$  the  $K$ -group  $G_{j_0}$ , and define  $q_{j_0}$  as the identity automorphism of  $G_{j_0}$ , and for  $j \neq j_0$ , define  $q_j$  as the trivial homomorphism  $G_{j_0} \rightarrow G_j$ , we find that the projection  $p_{j_0}$  is surjective.

If  $G'$  is also a direct product of  $G_1, \dots, G_n$ , with projections  $p'_1, \dots, p'_n$ , it is easy to see that there is a unique  $K$ -isomorphism  $f: G' \approx G$  such that  $p_j \circ f = p'_j$  ( $1 \leq j \leq n$ ). This fact is sometimes expressed by saying that a direct product is unique up to a unique  $K$ -isomorphism. For any permutation  $\pi$  of the set of indices  $1, \dots, n$ ,  $G$  is a direct product of  $G_{\pi(1)}, \dots, G_{\pi(n)}$  with projections  $p_{\pi(1)}, \dots, p_{\pi(n)}$ . Because of this fact we say that direct "multiplication" of  $K$ -groups is commutative. If  $(G_{jk})_{1 \leq j \leq n, 1 \leq k \leq r}$  is a family of  $K$ -groups, and if, for each index  $j$ ,  $G_j$  is a direct product of  $G_{j1}, \dots, G_{jk_1}$  with projections  $p_{j1}, \dots, p_{jk_1}$ , and if  $G$  is a direct product of  $G_1, \dots, G_n$  with projections  $p_1, \dots, p_n$ , then  $G$  is a direct product of the  $G_{jk}$  with projections  $p_{jk} \circ p_j$  ( $1 \leq j \leq n, 1 \leq k \leq r_j$ ). Because of this, we say that direct multiplication is associative.

Let  $G$  be a direct product of the  $K$ -groups  $G_1, \dots, G_n$  with projections  $p_j^G$  ( $1 \leq j \leq n$ ). For each index  $j$  let  $M_j$  be a homogeneous  $K$ -space for  $G_j$ . In accord with Section 9, Proposition 10(b),  $p_j^G$  induces on  $M_j$  a structure of homogeneous  $K$ -space for  $G$ . By a *direct product of the homogeneous  $K$ -spaces*  $M_1, \dots, M_n$ , we mean a homogeneous  $K$ -space  $M$  for  $G$  together with  $K$ -homomorphisms  $p_j^M: M \rightarrow M_j$  ( $1 \leq j \leq n$ ) of homogeneous  $K$ -spaces for  $G$ , enjoying the following property: Whenever  $N$  is a homogeneous  $K$ -space for  $G$  with  $K$ -homomorphisms  $q_j: N \rightarrow M_j$  ( $1 \leq j \leq n$ ), then there exists a unique  $K$ -homomorphism  $f: N \rightarrow M$  such that  $p_j^M \circ f = q_j$  ( $1 \leq j \leq n$ ). As with a direct product of  $K$ -groups, the  $K$ -homomorphisms  $p_j^M$  are called the *projections* of the direct product  $M$ .

A direct product of homogeneous  $K$ -spaces is unique up to a unique  $K$ -isomorphism, and direct multiplication of homogeneous  $K$ -spaces is commutative and associative, in the same sense that direct multiplication of  $K$ -groups is. It is easy to see that the regular  $K$ -space for  $G$ , with the projections  $p_1, \dots, p_n$ , is a direct product of the regular  $K$ -spaces for  $G_1, \dots, G_n$ . In this sense, a direct product of  $K$ -groups is a direct product of homogeneous  $K$ -spaces.

Because of the associativity, to prove the existence of direct products for an arbitrary finite family  $G_1, \dots, G_n$  (or  $M_1, \dots, M_n$ ) it suffices to consider the case  $n = 2$  (the cases  $n = 0$  and  $n = 1$  being trivial). The proof in this case is facilitated by the following lemma.

**Lemma 2** Let  $G_1, G_2$  be  $K$ -groups, and let  $x_i, x'_i \in G_i$  ( $i = 1, 2$ ). Fix  $s_i, t_i \in \Gamma_{G_i \circ / K(x_i)K(x_2)}$  and  $s'_i, t'_i \in \Gamma_{G_i \circ / K(x'_i)K(x_2')}$  ( $i = 1, 2$ ) such that  $s_1, t_1, s_2, t_2$  are independent over  $K(x_1)K(x_2)$  and  $s'_1, t'_1, s'_2, t'_2$  are independent over  $K(x'_1)K(x'_2)$ . Then the following three conditions are equivalent:

(a)  $s_1 x_1 \leftrightarrow s'_1 x'_1, s_2 x_2 \leftrightarrow s'_2 x'_2$ , and the isomorphisms

$$S_{s'_1 x'_1, s_1 x_1}, S_{s'_2 x'_2, s_2 x_2}, S_{s'_1, s_1}, S_{s'_2, s_2}$$

are compatible.

(b)  $x_1 t_1 \leftrightarrow x'_1 t'_1, x_2 t_2 \leftrightarrow x'_2 t'_2$ , and the isomorphisms

$$S_{x'_1 t'_1, x_1 t_1}, S_{x'_2 t'_2, x_2 t_2}, S_{t'_1, t_1}, S_{t'_2, t_2}$$

are compatible.

(c)  $s_1 x_1 t_1 \leftrightarrow s'_1 x'_1 t'_1, s_2 x_2 t_2 \leftrightarrow s'_2 x'_2 t'_2$ , and the isomorphisms

$$S_{s'_1 x'_1 t'_1, s_1 x_1 t_1}, S_{s'_2 x'_2 t'_2, s_2 x_2 t_2}, S_{s'_1, s_1}, S_{t'_1, t_1}, S_{s'_2, s_2}, S_{t'_2, t_2}$$

are compatible.

*Proof* This is immediate in the light of Section 3, Remark 2 following Proposition 1.

The lemma is analogous to Remark 2 following Theorem 1 in Section 3 and serves an analogous purpose. It should be noted that when  $G_1, G_2, x_1, x'_1, x_2, x'_2$  are given, then there always exist eight elements  $s_1, t_1, s'_1, t'_1, s_2, s'_2, t_2, t'_2$  with the required properties, and that the conditions (a)–(c) are independent of the choice of these eight elements. If the conditions are satisfied, then  $x_i \rightarrow x'_i$  ( $i = 1, 2$ ). In the opposite direction, if  $x_i \leftrightarrow x'_i$  ( $i = 1, 2$ ) and  $S_{x'_1, x_1}, S_{x'_2, x_2}$  are compatible, or if  $x_i \rightarrow x'_i$  ( $i = 1, 2$ ) and  $x_1, x_2$  are independent, then the conditions are satisfied. It is clear that the conditions remain equivalent to each other when the word "compatible" is replaced by the word "bicompatible," and that the three conditions strengthened in this way are equivalent to the following condition:  $x_1 \leftrightarrow x'_1, x_2 \leftrightarrow x'_2$ , and the isomorphisms  $S_{x'_1, x_1}, S_{x'_2, x_2}$  are bicompatible.

Similarly, if  $M_i$  is a homogeneous  $K$ -space for  $G_i$  ( $i = 1, 2$ ), and if  $v_i, v'_i \in M_i$  ( $i = 1, 2$ ), we can choose elements  $t_i \in \Gamma_{G_i \circ / K(v_i)K(v_2)}$  ( $i = 1, 2$ ) such that  $t_1, t_2$  are independent over  $K(v_1)K(v_2)$  and elements  $t'_i \in \Gamma_{G_i \circ / K(v'_i)K(v_2')}$  ( $i = 1, 2$ ) such that  $t'_1, t'_2$  are independent over  $K(v'_1)K(v'_2)$ . Then we can consider the following condition generalizing condition (b) in Lemma 2.

(b')  $v_1 t_1 \leftrightarrow v'_1 t'_1, v_2 t_2 \leftrightarrow v'_2 t'_2$ , and the isomorphisms

$$S_{v'_1 t'_1, v_1 t_1}, S_{v'_2 t'_2, v_2 t_2}, S_{t'_1, t_1}, S_{t'_2, t_2}$$

are compatible.

Here, too, the condition is independent of the choice of  $t_1, t_2, t_1', t_2'$ , and when the condition is strengthened by replacing the word "compatible" by the word "bicompatible," then it becomes equivalent to the following condition:  $v_1 \leftrightarrow v_1', v_2 \leftrightarrow v_2'$ , and the isomorphisms  $S_{v_1', v_1}, S_{v_2', v_2}$  are bicompatible.

The next theorem shows that direct products of  $K$ -groups and of homogeneous  $K$ -spaces always exist.

**Theorem 6** Let  $G_1, G_2$  be  $K$ -groups and let  $M_1, M_2$  be homogeneous  $K$ -spaces for  $G_1, G_2$ , respectively. For each element  $(x_1, x_2)$  (respectively  $(v_1, v_2)$ ) of the Cartesian product  $G_1 \times G_2$  (respectively  $M_1 \times M_2$ ) define  $K((x_1, x_2)) = K(x_1)K(x_2)$  (respectively  $K((v_1, v_2)) = K(v_1)K(v_2)$ ). For  $(x_1, x_2), (x_1', x_2') \in G_1 \times G_2$  (respectively  $(v_1, v_2), (v_1', v_2') \in M_1 \times M_2$ ) define  $(x_1, x_2) \rightarrow (x_1', x_2')$  (respectively  $(v_1, v_2) \rightarrow (v_1', v_2')$ ) to mean that condition (b) in Lemma 2 (respectively condition (b') above) is satisfied. For  $(x_1, x_2), (x_1', x_2') \in G_1 \times G_2$  with  $(x_1, x_2) \leftrightarrow (x_1', x_2')$  define  $S_{(x_1', x_2'), (x_1, x_2)}$  to be the unique isomorphism  $K((x_1, x_2)) \approx K((x_1', x_2'))$  that extends  $S_{x_1', x_1}, S_{x_2', x_2}$ . For  $(v_1, v_2), (v_1', v_2') \in M_1 \times M_2$  with  $(v_1, v_2) \leftrightarrow (v_1', v_2')$  define  $S_{(v_1', v_2'), (v_1, v_2)}$  to be the unique isomorphism  $K((v_1, v_2)) \approx K((v_1', v_2'))$  that extends  $S_{v_1', v_1}, S_{v_2', v_2}$ .

(a) These data define on each of  $G_1 \times G_2, M_1 \times M_2$  a structure of pre- $K$ -set. The pre- $K$ -set structure on  $G_1 \times G_2$  together with the product group structure on  $G_1 \times G_2$  define a  $K$ -group structure on  $G_1 \times G_2$ . The pre- $K$ -set structure on  $M_1 \times M_2$  together with the product structure on  $M_1 \times M_2$  of homogeneous space for  $G_1 \times G_2$  define on  $M_1 \times M_2$  a structure of homogeneous  $K$ -space for  $G_1 \times G_2$  (which is principal when  $M_1$  and  $M_2$  are principal homogeneous  $K$ -spaces for  $G_1$  and  $G_2$ , respectively).

(b) If  $V_i$  is a  $K$ -irreducible  $K$ -subset of  $G_i$  (respectively  $M_i$ ) ( $i = 1, 2$ ), then  $V_1 \times V_2$  is a  $K$ -subset of  $G_1 \times G_2$  (respectively  $M_1 \times M_2$ ). Every  $K$ -component of  $V_1 \times V_2$  has dimension equal to  $\dim V_1 + \dim V_2$ . If one of  $V_1, V_2$  has a  $K$ -generic element that is regular over  $K$ , then  $V_1 \times V_2$  is  $K$ -irreducible. If both do, then a  $K$ -generic element of  $V_1 \times V_2$  is regular over  $K$ .

(c) The canonical projections  $pr_i : G_1 \times G_2 \rightarrow G_i$  (respectively  $M_1 \times M_2 \rightarrow M_i$ ) ( $i = 1, 2$ ) are separable surjective  $K$ -homomorphisms of  $K$ -groups (respectively of homogeneous  $K$ -spaces for  $G_1 \times G_2$ ). The  $K$ -group  $G_1 \times G_2$  (respectively homogeneous  $K$ -space  $M_1 \times M_2$ ) with its canonical projections is a direct product of the  $K$ -groups  $G_1, G_2$  (respectively of the homogeneous  $K$ -spaces  $M_1, M_2$ ).

The proof of Theorem 6 makes use of Lemma 2 much as the proof of Theorem 2 in Section 5 makes use of Remark 2 following Theorem 1 in

Section 3. Since the proof of Theorem 6 is long and tedious, and is easy to improvise by following the proof of Theorem 2, we shall omit it.

We call the structure of  $K$ -group on  $G_1 \times G_2$  (respectively of homogeneous  $K$ -space on  $M_1 \times M_2$ ) defined in Theorem 6 the *product  $K$ -group* (respectively homogeneous  $K$ -space) structure. We usually write  $K(x_1, x_2)$  (respectively  $K(v_1, v_2)$ ) instead of  $K((x_1, x_2))$  (respectively  $K((v_1, v_2))$ ).

If  $G_i'$  is a  $K$ -subgroup of  $G_i$  ( $i = 1, 2$ ), then  $G_1' \times G_2'$  is (by Theorem 6(b)) a  $K$ -subgroup of  $G_1 \times G_2$ . It is easy to see that the  $K$ -group structure that  $G_1' \times G_2'$  has as a  $K$ -subgroup of  $G_1 \times G_2$  is the same as the product  $K$ -group structure on  $G_1' \times G_2'$ .

It follows from Theorem 6(b) that  $(G_1 \times G_2)^o = G_1^o \times G_2^o$ .

Starting with homogeneous  $K$ -spaces  $M_1, M_2$  and an extension  $L$  of  $K$ , we can first form the direct product of the homogeneous  $K$ -spaces and then the induced homogeneous  $L$ -space. Alternatively, we can first form the induced homogeneous  $L$ -spaces and then the direct product of these homogeneous  $L$ -spaces. A routine verification shows that the end result is the same.

If  $G_1, \dots, G_n$  are  $K$ -groups and, for each index  $j$ ,  $M_j$  is a homogeneous  $K$ -space for  $G_j$ , we can identify the product sets  $\chi_{1 \leq j \leq n} G_j$  and  $\chi_{1 \leq j \leq n} M_j$  with the Cartesian products  $(\chi_{1 \leq j \leq n-1} G_j) \times G_n$  and  $(\chi_{1 \leq j \leq n-1} M_j) \times M_n$ , respectively. Therefore an induction argument enables us to use Theorem 6 to introduce on  $\chi_{1 \leq j \leq n} G_j$  a  $K$ -group structure such that the  $K$ -group  $\chi_{1 \leq j \leq n} G_j$  with its canonical projections is a direct product of  $G_1, \dots, G_n$ , and to introduce on  $\chi_{1 \leq j \leq n} M_j$  a structure of homogeneous  $K$ -space for  $\chi_{1 \leq j \leq n} G_j$  such that the homogeneous  $K$ -space  $\chi_{1 \leq j \leq n} M_j$  with its canonical projections is a direct product of  $M_1, \dots, M_n$ . In both cases, the canonical projections  $pr_j$  are separable surjective  $K$ -homomorphisms. If  $(v_1, \dots, v_n)$  and  $(v_1', \dots, v_n')$  are elements of  $\chi M_j$ , and if  $(t_1, \dots, t_n)$  and  $(t_1', \dots, t_n')$  are  $K$ -generic elements of  $(\chi G_j)^o = \chi G_j^o$  such that  $(v_1, \dots, v_n), (t_1, \dots, t_n)$  are independent over  $K$  and  $(v_1', \dots, v_n'), (t_1', \dots, t_n')$  are, too, then a necessary and sufficient condition that  $(v_1, \dots, v_n) \rightarrow (v_1', \dots, v_n')$  is that  $v_j t_j \leftrightarrow v_j' t_j'$  ( $1 \leq j \leq n$ ) and the  $2n$  isomorphisms  $S_{v_j t_j, v_j' t_j'} (1 \leq j \leq n), S_{t_j, t_j'} (1 \leq j \leq n)$  be compatible.

**Proposition 11** Let  $f_j : M_j \rightarrow N_j$  be a  $K$ -homomorphism of homogeneous  $K$ -spaces for a  $K$ -group  $G_j$  ( $1 \leq j \leq n$ ), and let  $f : \chi M_j \rightarrow \chi N_j$  be the mapping defined by the formula  $f(v_1, \dots, v_n) = (f_1(v_1), \dots, f_n(v_n))$ . Then  $f$  is a  $K$ -homomorphism of homogeneous  $K$ -spaces for  $\chi G_j$ .

*Proof* For each index  $j'$  the mapping  $f_{j'} \circ pr_{j'} : \chi M_j \rightarrow N_{j'}$  is a  $K$ -homomorphism of homogeneous  $K$ -spaces for  $\chi G_j$ ; therefore there is a unique  $K$ -homomorphism  $f' : \chi M_j \rightarrow \chi N_j$  such that  $pr_{j'} \circ f' = f_{j'} \circ pr_{j'} (1 \leq j' \leq n)$



that is, such that  $f'(v_1, \dots, v_n) = (f_1(v_1), \dots, f_n(v_n))$  for every  $(v_1, \dots, v_n) \in \chi M_j$ . Therefore  $f = f'$  and  $f$  is a  $K$ -homomorphism.

**Proposition 12** Let  $M_j$  be a homogeneous  $K$ -space for a  $K$ -group  $G_j$  and let  $v_j, v_j'$  be elements of  $M_j$  with  $v_j \leftrightarrow v_j'$  ( $1 \leq j \leq n$ ). A necessary and sufficient condition that  $(v_1, \dots, v_n) \rightarrow (v_1', \dots, v_n')$  is that  $S_{v_1', v_1}, \dots, S_{v_n', v_n}$  be compatible.

*Proof* By linear disjointness the condition is evidently equivalent to the condition that  $S_{v_1', v_1}, \dots, S_{v_n', v_n}, S_{t_1', t_1}, \dots, S_{t_n', t_n}$  be compatible ( $t_j, t_j'$  being elements of  $\Gamma_{G_j/K}$  with the usual properties). Because of axiom AH 2(a), this is equivalent to the condition that  $v_j t_j \leftrightarrow v_j' t_j'$  ( $1 \leq j \leq n$ ) and  $S_{v_1' t_1', v_1 t_1}, \dots, S_{v_n' t_n', v_n t_n}, S_{t_1', t_1}, \dots, S_{t_n', t_n}$  be compatible, that is, to the condition that  $(v_1, \dots, v_n) \rightarrow (v_1', \dots, v_n')$ .

In the light of Proposition 12, we see that the following result goes beyond what we observed in Section 3, Remark 2 following Proposition 1.

**Proposition 13** Let  $M$  be a homogeneous  $K$ -space for a  $K$ -group  $G$ , and let  $v_i, v_i' \in M$  ( $1 \leq i \leq m$ ) and  $x_j, x_j' \in G$  ( $1 \leq j \leq n$ ). Let  $U_1, \dots, U_m, X_1, \dots, X_n$  be noncommuting indeterminates, and let  $\mathfrak{B}$  denote the same set of "monomials" in these indeterminates as  $\mathfrak{B}$  denotes in Section 3, Remark 2 following Proposition 1. For each  $W \in \mathfrak{B}$ , let  $w$  respectively  $w'$  denote the element of  $M$  or  $G$  obtained by substituting  $(v_1, \dots, v_m, x_1, \dots, x_n)$  respectively  $(v_1', \dots, v_m', x_1', \dots, x_n')$  for  $(U_1, \dots, U_m, X_1, \dots, X_n)$  in  $W$ . Let  $W_1, \dots, W_r \in \mathfrak{B}$ .

If  $(v_1, \dots, v_m, x_1, \dots, x_n) \rightarrow (v_1', \dots, v_m', x_1', \dots, x_n')$ , then  $(w_1, \dots, w_r) \rightarrow (w_1', \dots, w_r')$ .

*Proof* Let  $g = \max(r, m+n+1)$ , and choose elements  $t_1, \dots, t_g \in \Gamma_{G \circ L}$  that are independent over the field

$$L = K(v_1, \dots, v_m, x_1, \dots, x_n, v_1', \dots, v_m', x_1', \dots, x_n').$$

Let  $h \in \mathbb{N}$ , and let  $\mathfrak{B}_h$  have the same meaning as in Section 2, Remark 2 following Proposition 1. We claim that  $w t_k \leftrightarrow w' t_k$  ( $1 \leq k \leq g$ ,  $W \in \mathfrak{B}_h$ ) and that the isomorphisms  $S_{w' t_k, w t_k}$  ( $1 \leq k \leq g$ ,  $W \in \mathfrak{B}_h$ ) are compatible. For a sufficiently big value of  $h$ ,  $\mathfrak{B}_h$  contains  $1, W_1, \dots, W_r$ , and therefore the claim, once established, will show that  $w_k t_k \leftrightarrow w_k' t_k$  ( $1 \leq k \leq r$ ) and that the  $2r$  isomorphisms  $S_{w_k' t_k, w_k t_k}$  ( $1 \leq k \leq r$ ) and  $S_{t_k, t_k}$  ( $1 \leq k \leq r$ ) are compatible, that is, will show that  $(w_1, \dots, w_r) \rightarrow (w_1', \dots, w_r')$ .

To begin with, observe that because

$$(v_1, \dots, v_m, x_1, \dots, x_n) \rightarrow (v_1', \dots, v_m', x_1', \dots, x_n')$$

the  $2(m+n)$  isomorphisms  $S_{v_i' t_i, v_i t_i}$  ( $1 \leq i \leq m$ ),  $S_{x_j' t_{m+j}, x_j t_{m+j}}$  ( $1 \leq j \leq n$ )  $S_{t_k, t_k}$  ( $1 \leq k \leq m+n$ ) make sense and are compatible. Therefore these and

the  $g-m-n$  isomorphisms  $S_{t_k, t_k}$  ( $m+n < k \leq g$ ) are compatible. Using axiom AH 2(a) as in Section 3, Remark 2 following Proposition 1, we find that the  $(m+2n+1)g$  isomorphisms

$$\begin{aligned} S_{v_i' t_k, v_i t_k} & \quad (1 \leq i \leq m, \quad 1 \leq k \leq g), \\ S_{x_j' t_k, x_j t_k} & \quad (1 \leq j \leq n, \quad 1 \leq k \leq g), \\ S_{x_j'^{-1} t_k, x_j^{-1} t_k} & \quad (1 \leq j \leq n, \quad 1 \leq k \leq g), \\ S_{t_k, t_k} & \quad (1 \leq k \leq g) \end{aligned}$$

make sense and are compatible. This is the claim for  $h = 1$ . Now suppose that the claim is established for a given  $h \geq 1$ , that is, that the isomorphisms  $S_{w' t_k, w t_k}$  ( $1 \leq k \leq g$ ,  $W \in \mathfrak{B}_h$ ) make sense and are compatible. By the same method as before, we find that these and the following isomorphisms make sense and are compatible:

$$\begin{aligned} S_{t_k^{-1} x_j' t_l, t_k^{-1} x_j t_l} & \quad (1 \leq j \leq n, \quad 1 \leq k \leq g, \quad 1 \leq l \leq g, \quad k \neq l); \\ S_{t_k^{-1} x_j'^{-1} t_l, t_k^{-1} x_j^{-1} t_l} & \quad (1 \leq j \leq n, \quad 1 \leq k \leq g, \quad 1 \leq l \leq g, \quad k \neq l); \end{aligned}$$

if the homogeneous  $K$ -space  $M$  is principal

$$\begin{aligned} S_{t_k^{-1} v_i'^{-1} v_i' t_l, t_k^{-1} v_i^{-1} v_i t_l} & \quad (1 \leq i \leq m, \quad 1 \leq i' \leq m, \quad 1 \leq k \leq g, \quad 1 \leq l \leq g, \quad k \neq l); \\ S_{w' x_j' t_l, w x_j t_l} & \quad (1 \leq j \leq n, \quad W \in \mathfrak{B}_h, \quad 1 \leq l \leq g); \\ S_{w' x_j'^{-1} t_l, w x_j^{-1} t_l} & \quad (1 \leq j \leq n, \quad W \in \mathfrak{B}_h, \quad 1 \leq l \leq g); \end{aligned}$$

if  $M$  is principal

$$S_{w' v_i'^{-1} v_i' t_l, w v_i^{-1} v_i t_l} \quad (1 \leq i \leq m, \quad 1 \leq i' \leq m, \quad W \in \mathfrak{B}_{h-1}, \quad 1 \leq l \leq g).$$

Since  $\mathfrak{B}_{h+1}$  is the union of the sets  $\bigcup_{i \leq j \leq n} \mathfrak{B}_h X_j$  and  $\bigcup_{i \leq j \leq n} \mathfrak{B}_h X_j^{-1}$  and (if  $M$  is principal)  $\bigcup_{1 \leq i \leq m, 1 \leq i' \leq m} \mathfrak{B}_{h-1} U_i^{-1} U_{i'}$ , this establishes the claim for  $h+1$  and hence in general.

**Corollary 1** Let  $G, M, U_1, \dots, U_m, X_1, \dots, X_n, W_1, \dots, W_r$  have the same meaning as in Proposition 13. Let the elements  $e_{\mu+1}, \dots, e_m \in M_K$  and  $a_{v+1}, \dots, a_n \in G_K$  be fixed, and set  $Z = (\prod_{1 \leq i \leq \mu} M_i) \times (\prod_{1 \leq j \leq v} G_j)$ . For each element  $z = (v_1, \dots, v_\mu, x_1, \dots, x_v) \in Z$  and each index  $k$  ( $1 \leq k \leq r$ ) let

$$f_k(z) = W_k(v_1, \dots, v_\mu, e_{\mu+1}, \dots, e_m, x_1, \dots, x_v, a_{v+1}, \dots, a_n),$$

and set  $f(z) = (f_1(z), \dots, f_r(z))$ , so that  $f(z)$  is an element of the direct product  $P$  of  $r$  homogeneous  $K$ -spaces each of which is  $M$  or  $G$ . Then  $f$  is a  $K$ -continuous everywhere defined pre- $K$ -mapping of  $Z$  into  $P$ .

*Proof* Set  $Z^* = (\prod_{1 \leq i \leq m} M_i) \times (\prod_{1 \leq j \leq n} G_j)$ , and consider the sequence of mappings

$$Z \xrightarrow{h} Z^* \xrightarrow{f^*} Z^* \times P \xrightarrow{pr} P,$$

where  $h$  is defined by the formula

$$h(v_1, \dots, v_\mu, x_1, \dots, x_\nu) = (v_1, \dots, v_\mu, e_{\mu+1}, \dots, e_m, x_1, \dots, x_\nu, a_{\nu+1}, \dots, a_n),$$

$f^*$  is defined by the formula

$$f^*(z^*) = (z^*, (W_1(z^*), \dots, W_r(z^*))),$$

and  $pr$  denotes the canonical projection on the second factor. If an element  $((v_1', \dots, v_m', x_1', \dots, x_n'), (w_1', \dots, w_r'))$  of  $Z^* \times P$  is a specialization over  $K$  of an element  $(z^*, (W_1(z^*), \dots, W_r(z^*)))$ , where  $z^* = (v_1, \dots, v_m, x_1, \dots, x_n)$ , then  $(v_1, \dots, v_m, x_1, \dots, x_n) \rightarrow (v_1', \dots, v_m', x_1', \dots, x_n')$  and (as is easy to see by Proposition 13)  $w_k' = W_k(v_1', \dots, v_m', x_1', \dots, x_n')$  ( $1 \leq k \leq r$ ). In other words, if  $z^* \in Z^*$ , then every specialization of  $f^*(z^*)$  over  $K$  is in  $\text{Im}(f^*)$ . Furthermore (also by Proposition 13), for any elements  $z^*, z^{*'} \in Z^*$ ,  $z^* \rightarrow z^{*'}$  if and only if  $f^*(z^*) \rightarrow f^*(z^{*'})$ . It follows that  $\text{Im}(f^*)$  is a  $K$ -set, that  $f^*$  maps  $Z^*$  bijectively onto  $\text{Im}(f^*)$ , and that  $f^*$  and the inverse mapping  $\text{Im}(f^*) \rightarrow Z^*$  are everywhere defined pre- $K$ -mappings. Hence (by Section 6, the corollary to Theorem 3)  $f^*$  is  $K$ -continuous. Because  $h$  and  $pr$  are evidently  $K$ -continuous everywhere defined pre- $K$ -mappings, and because  $pr \circ f^* \circ h = f$ , the corollary is proved.

**Corollary 2** Let  $G$  be a  $K$ -group and  $A$  be a subset of  $G$ .

(a) When  $A$  is  $K$ -closed then the normalizer  $N_A$  of  $A$  in  $G$  is a  $K$ -closed subgroup of  $G$ .

(b) The centralizer  $C_A$  of  $A$  is a closed subgroup of  $G$ . When  $A$  is  $K$ -closed, then  $C_A$  is  $K$ -closed.

(c) The center of  $G$  is a  $K$ -closed subgroup of  $G$ .

*Proof* (a) For each  $y \in G$  define mappings  $f_y, g_y$  of  $G$  into  $G$  by the formulas  $f_y(x) = xyx^{-1}$ ,  $g_y(x) = x^{-1}yx$ . They are continuous by Corollary 1, and  $N_A = \bigcap_{y \in A} f_y^{-1}(A) \cap \bigcap_{y \in A} g_y^{-1}(A)$ . Since  $A$  is  $K$ -closed,  $N_A$  is closed and, for every  $\sigma \in \text{Aut}(U/K)$ ,  $\sigma(N_A) = N_{\sigma A} = N_A$ . Therefore  $N_A$  is  $K$ -closed.

(b) For each  $y \in A$ ,  $\{y\}$  is closed, so that by part (a),  $C_{\{y\}}$  is closed. Since  $C_A = \bigcap_{y \in A} C_{\{y\}}$ ,  $C_A$  is closed. When  $A$  is  $K$ -closed, then  $\sigma(C_A) = C_{\sigma A} = C_A$  for every  $\sigma \in \text{Aut}(U/K)$ , so that  $C_A$  is  $K$ -closed.

(c) Set  $A = G$  in part (b).

In order to derive another consequence of Proposition 13 we need the following lemma on abstract groups due to Baer [1]. Recall that if  $a, b$  are

elements of a group  $g$ , then the commutator of  $a$  and  $b$  is the element  $aba^{-1}b^{-1}$ . If  $h$  and  $j$  are subsets of  $g$ , the subgroup of  $g$  generated by the set of all commutators  $aba^{-1}b^{-1}$  with  $a \in h$  and  $b \in j$  is called the commutator group of  $h$  and  $j$  and is denoted by  $[h, j]$ . The group  $[g, g]$ , called the commutator group of  $g$ , is the smallest normal subgroup  $n$  of  $g$  such that  $g/n$  is commutative.

**Lemma 3** Let  $h, h_0, j, j_0$  be normal subgroups of a group  $g$  such that  $h \supset h_0$  and  $j \supset j_0$ ,  $h/h_0$  and  $j/j_0$  are finite, and  $[h, j_0] = [h_0, j] = 1$ . Then  $[h, j]$  is finite.

*Proof* In the special case in which  $h = j = g$  and  $h_0 = j_0 = \mathfrak{z}$  = the center of  $g$ , the lemma states that if  $\mathfrak{z}$  is of finite index in  $g$ , then  $[g, g]$  is finite. We first prove this special case. In the proof, the letter  $c$  with various indices always denotes a suitable commutator of two elements of  $g$ , and  $l$  denotes the index  $(g:\mathfrak{z})$ .

The formula

$$(aba^{-1}b^{-1})^k = (ab)^k(a^{-1}b^{-1})^k c_1 \cdots c_{k-1}$$

is obviously valid when  $k = 1$ . If  $k > 1$  and the formula is valid for lower values of  $k$ , then

$$\begin{aligned} (aba^{-1}b^{-1})^k &= aba^{-1}b^{-1}(ab)^{k-1}(a^{-1}b^{-1})^{k-1}c_1 \cdots c_{k-2} \\ &= (ab)^k(ab)^{-k+1}(a^{-1}b^{-1})(ab)^{k-1}(a^{-1}b^{-1})^{-1}(a^{-1}b^{-1})^k c_1 \cdots c_{k-2} \\ &= (ab)^k c_0 (a^{-1}b^{-1})^k c_1 \cdots c_{k-2} \\ &= (ab)^k (a^{-1}b^{-1})^k c_1 \cdots c_{k-1}; \end{aligned}$$

hence the formula is valid for all  $k$ . This being so, let  $a_1, \dots, a_l$  be representatives of the cosets of  $\mathfrak{z}$  in  $g$ . Every commutator in  $g$  equals one of the  $l^2$  commutators  $a_i a_j a_i^{-1} a_j^{-1}$ . Hence in a product  $P$  of  $(l-1)l^2 + 1$  commutators there must exist  $l$  equal factors. These  $l$  factors can be brought to the left provided the other factors are replaced by conjugates of themselves (which also are commutators). Thus we may write  $P = (a_i a_j a_i^{-1} a_j^{-1})^l P'$ , where  $P'$  is a product of  $l^3 - l^2 - l + 1$  commutators. However, by our formula,

$$(a_i a_j a_i^{-1} a_j^{-1})^l = (a_i a_j)^l (a_i^{-1} a_j^{-1})^l c_1 \cdots c_{l-1},$$

and by hypothesis  $(a_i a_j)^l \in \mathfrak{z}$ , whence  $(a_i a_j)^l = a_i (a_i a_j)^l a_i^{-1} = (a_i a_j)^l$ ; hence  $P$  equals a product of  $l^3 - l^2$  commutators. This shows that every product of commutators in  $g$  equals a product of  $l^3 - l^2$  commutators. Therefore the order of  $[g, g]$  is less than or equal to  $l^{2(l^3 - l^2)}$ .

We now turn to the general lemma. Let  $m = (h:h_0)$ ,  $n = (j:j_0)$ , and let  $x_1, \dots, x_m$  (respectively  $y_1, \dots, y_n$ ) be a system of representatives of the

cosets of  $h_0$  in  $h$  (respectively of  $j_0$  in  $j$ ). It is easy to verify that every commutator of an element of  $h$  and an element of  $j$  equals one of the elements  $x_i y_j x_i^{-1} y_j^{-1}$ , so that these  $mn$  commutators generate the group  $\mathfrak{d} = [h, j]$ . Since  $h$  and  $j$  are normal subgroups of  $g$ ,  $\mathfrak{d} \subset h \cap j$ . This implies first that  $\mathfrak{d}/(\mathfrak{d} \cap h_0) \approx \mathfrak{d}h_0/h_0 \subset h/h_0$ , and second that  $\mathfrak{d} \cap h_0$  is contained in the center of  $\mathfrak{d}$ . Hence the center of  $\mathfrak{d}$  is of finite index in  $\mathfrak{d}$ . By the special case of the lemma,  $[\mathfrak{d}, \mathfrak{d}]$  is finite. To prove  $\mathfrak{d}$  finite it suffices to show that  $\mathfrak{d}/[\mathfrak{d}, \mathfrak{d}]$  is finite. As this group is commutative, it is enough to show that the elements of a finite set of generators all are of finite order. Hence it suffices to show that when  $x \in h$  and  $y \in j$ , then  $(xyx^{-1}y^{-1})^m \in [\mathfrak{d}, \mathfrak{d}]$ .

For any  $u \in \mathfrak{d}$ ,  $u^m \in h_0$  whence  $yuy^{-1}u^{-1} = u^m$ . Therefore

$$u^m = (yuy^{-1})^m = (yuy^{-1}u^{-1}u)^m \equiv (yuy^{-1}u^{-1})^m u^m \pmod{[\mathfrak{d}, \mathfrak{d}]},$$

so that  $(yuy^{-1}u^{-1})^m \in [\mathfrak{d}, \mathfrak{d}]$ . Also, for any  $k \geq 1$ ,

$$\begin{aligned} xy^k x^{-1} y^{-k} &= xy^{k-1} x^{-1} y^{-k+1} \cdot y^{k-1} (xyx^{-1}y^{-1}) y^{-k+1} (xyx^{-1}y^{-1})^{-1} \cdot xyx^{-1}y^{-1}, \end{aligned}$$

whence by induction, for any  $k \geq 0$ ,

$$xy^k x^{-1} y^{-k} \equiv (xyx^{-1}y^{-1})^k \prod_{1 \leq i < k} y^i (xyx^{-1}y^{-1}) y^{-i} (xyx^{-1}y^{-1})^{-1} \pmod{[\mathfrak{d}, \mathfrak{d}]}.$$

When  $k = n$ , then the left member of this congruence equals 1 (because  $[h, j_0] = 1$ ), and each factor  $y^i (xyx^{-1}y^{-1}) y^{-i} (xyx^{-1}y^{-1})^{-1}$  on the right is of the form  $y'u'y'^{-1}u'^{-1}$  with  $y' \in j$  and  $u' \in \mathfrak{d}$ . Therefore when we set  $k = n$  and then raise to the  $m$ th power, we find that

$$1 \equiv (xyx^{-1}y^{-1})^{mn} \pmod{[\mathfrak{d}, \mathfrak{d}]}.$$

This completes the proof of the lemma.

**Proposition 14** *Let  $H$  and  $J$  be normal  $K$ -subgroups of the  $K$ -group  $G$ . Then  $[H, J]$  is  $K$ -closed. When  $H$  and  $J$  are connected,  $[H, J]$  is a connected  $K$ -subgroup of  $G$ .*

*Proof* First suppose that either  $K$  is algebraically closed or  $H$  and  $J$  are connected. Then by Section 3, Theorem 1, the cosets of  $H^\circ$  in  $H$  (respectively  $J^\circ$  in  $J$ ) are the  $K$ -components of  $H$  (respectively  $J$ ). Let  $x_1, \dots, x_m$  (respectively  $y_1, \dots, y_n$ ) be a set of representatives of the cosets of  $H^\circ$  in  $H$  (respectively  $J^\circ$  in  $J$ ). By Section 7, the Corollary to Proposition 3, we may suppose all the elements  $x_i$  and  $y_i$  are rational over  $K$ . (Of course, if  $H$  and  $J$  are connected, then  $m = n = 1$  and we may take  $x_1 = y_1 = 1$ .) Let  $(x, y) \in \Gamma_{H^\circ \times J^\circ / K}$ , and let  $V_i$  (respectively  $W_j$ ) be the locus over  $K$  of  $(x_i x) y (x_i x)^{-1} y^{-1}$  (re-

spectively  $x(y_j y) x^{-1} (y_j y)^{-1}$ ). By Proposition 13, every commutator of an element of  $x_i H^\circ$  and an element of  $J^\circ$  (respectively of an element of  $H^\circ$  and an element of  $y_j J^\circ$ ) is in  $V_i$  (respectively  $W_j$ ). In particular,  $1 \in V_i, 1 \in W_j$ . It follows, by Section 8, Proposition 7 and the remark thereafter, that the normal subgroup  $E = [H, J^\circ][H^\circ, J]$  of  $G$  is the subgroup of  $G$  generated by  $V_1 \cup \dots \cup V_m \cup W_1 \cup \dots \cup W_n$  and is a  $K$ -group. When  $H$  and  $J$  are connected, evidently  $E = [H, J]$ .

Consider the four groups  $H/E, H^\circ[H, J^\circ]/E, J/E, J^\circ[H^\circ, J]/E$ . These are normal subgroups of  $G/E$ , and evidently  $H/E \supset H^\circ[H, J^\circ]/E, J/E \supset J^\circ[H^\circ, J]/E, (H/E)/(H^\circ[H, J^\circ]/E) \approx H/H^\circ[H, J^\circ]$ , which is finite, and similarly  $(J/E)/(J^\circ[H^\circ, J]/E)$  is finite. Also  $[H/E, J^\circ[H^\circ, J]/E] = [H, J^\circ[H^\circ, J]]/E = 1$ , and similarly  $[J/E, H^\circ[H, J^\circ]/E] = 1$ . It therefore follows from Lemma 3 that the group  $[H/E, J/E] = [H, J]/E$  is finite. Letting  $z_1, \dots, z_r$  be representatives of the cosets of  $E$  in  $[H, J]$ , we see that  $[H, J]$  is the union of the closed sets  $Ez_k$ , and hence is closed.

Now relinquish the supposition that  $K$  be algebraically closed or  $H$  and  $J$  be connected. Since we may use  $K_a$  instead of  $K$ , we still find that  $[H, J]$  is closed. For every  $\sigma \in \text{Aut}(U/K), \sigma[H, J] = [\sigma H, \sigma J] = [H, J]$ . Therefore  $[H, J]$  is  $K$ -closed.

### 11 Quotients

Let  $G$  be a  $K$ -group and  $H$  be a normal  $K$ -subgroup of  $G$ . A  $K$ -group quotient of  $G$  by  $H$  is defined as a  $K$ -group  $Q$  with a  $K$ -homomorphism  $\pi: G \rightarrow Q$  that is trivial on  $H$  and has the following property: Whenever  $G'$  is a  $K$ -group with a  $K$ -homomorphism  $f: G \rightarrow G'$  that is trivial on  $H$ , then there exists a unique  $K$ -homomorphism  $g: Q \rightarrow G'$  such that  $g \circ \pi = f$ . The  $K$ -homomorphism  $\pi$  is called the *quotient mapping* of the  $K$ -group quotient.

If  $Q$  and  $Q'$  are two  $K$ -group quotients of  $G$  by  $H$ , with the respective quotient mappings  $\pi$  and  $\pi'$ , then there is a unique  $K$ -homomorphism  $g: Q \rightarrow Q'$  such that  $g \circ \pi = \pi'$ , and it is easy to see that  $g$  is a  $K$ -isomorphism. We express this by saying that a  $K$ -group quotient is unique up to a unique  $K$ -isomorphism.

Starting afresh, let  $H$  be any  $K$ -subgroup of  $G$  (not necessarily a normal one), and consider  $G$  as a homogeneous  $K$ -space for  $G$ , that is, consider the regular  $K$ -space for  $G$ . By a *homogeneous  $K$ -space quotient* of  $G$  by  $H$  we mean a homogeneous  $K$ -space  $Q$  for  $G$  with a  $K$ -homomorphism  $\pi: G \rightarrow Q$  that is constant on each right coset of  $H$  in  $G$  and has the following property: Whenever  $M$  is a homogeneous  $K$ -space for  $G$  with a  $K$ -homomorphism  $f: G \rightarrow M$  that is constant on each right coset of  $H$  in  $G$ , then there exists a

unique  $K$ -homomorphism  $g: Q \rightarrow M$  such that  $g \circ \pi = f$ . Here, too,  $\pi$  is called the *quotient mapping*. Also, a homogeneous  $K$ -space quotient of  $G$  by  $H$  is unique up to a unique  $K$ -isomorphism.

We shall prove that quotients (both  $K$ -group and homogeneous  $K$ -space) always exist. The proof will be facilitated by the following lemma.

**Lemma 4** *Let  $H$  be a  $K$ -subgroup of a  $K$ -group  $G$  and let  $\mathfrak{x}, \mathfrak{x}'$  be right cosets of  $H$  in  $G$ .*

(a) *The following three conditions are equivalent: (i) there exist elements  $x \in \mathfrak{x}, x' \in \mathfrak{x}'$  such that  $x \rightarrow x'$ ; (ii) for every  $x' \in \mathfrak{x}'$ , there exists an  $x \in \mathfrak{x}$  such that  $x \rightarrow x'$ ; (iii) for every  $x' \in \Gamma_{x'/K(x')}$ , there exists an  $x \in \Gamma_{x/K(x)}$  such that  $x \rightarrow x'$ .*

(b) *The following three conditions are equivalent: (i) there exist elements  $x_1 \in \mathfrak{x}, x_1' \in \mathfrak{x}'$  such that  $x_1 \rightarrow x_1'$  and elements  $x_2 \in \mathfrak{x}, x_2' \in \mathfrak{x}'$  such that  $x_2' \rightarrow x_2$ ; (ii) there exist elements  $x \in \mathfrak{x}, x' \in \mathfrak{x}'$  such that  $x \leftrightarrow x'$ ; (iii) for every  $x' \in \Gamma_{x'/K(x')}$ , there exists an  $x \in \Gamma_{x/K(x)}$  such that  $x \leftrightarrow x'$ .*

(c) *If the conditions in part (b) are satisfied and elements  $x \in \mathfrak{x}, x' \in \mathfrak{x}'$  are chosen with  $x \leftrightarrow x'$ , then  $S_{x',x}$  induces, by restriction, an isomorphism  $K(\mathfrak{x}) \approx K(\mathfrak{x}')$  over  $K$ ; this isomorphism is independent of the choice of  $x, x'$ .*

(d) *If  $x \in \Gamma_{x/K(x)}$ , then  $\dim_K x = \text{tr deg } K(\mathfrak{x})/K + \dim H$ .*

**REMARK** If  $x \in \mathfrak{x}$ , then  $\mathfrak{x} = Hx$ , so that  $\mathfrak{x}$  is a  $K(x)$ -subset of  $G$ .  $K(\mathfrak{x})$  denotes the smallest extension  $L$  of  $K$  such that  $\mathfrak{x}$  is an  $L$ -subset of  $G$  (see Section 7, Theorem 4); therefore  $K(\mathfrak{x}) \subset K(x)$ .

*Proof* (a) It is obvious that (iii) implies (i). Suppose that  $x_0 \in \mathfrak{x}, x_0' \in \mathfrak{x}'$ , and  $x_0 \rightarrow x_0'$ , and let  $x' \in \mathfrak{x}'$ . Then  $x' = yx_0'$ , where  $y \in H$ . Let  $X$  (respectively  $Y$ ) be the locus of  $x_0$  (respectively  $y$ ) over  $K$ . Then  $(y, x_0') \in Y \times X$ . Let  $(y^*, x^*)$  be a  $K$ -generic element of a  $K$ -component of  $Y \times X$  containing  $(y, x_0')$ . Then  $(y^*, x^*) \rightarrow (y, x_0')$ , so that  $y^*x^* \rightarrow yx_0' = x'$ . Evidently  $x^* \in \Gamma_{x^*/K}$ , whence  $x^* \leftrightarrow x_0$ , so that there exists some  $\sigma \in \text{Aut}(U/K)$  such that  $\sigma x^* = x_0$ . Setting  $x = \sigma y^* \cdot x_0$ , we conclude that  $x \in Hx_0 = \mathfrak{x}$  and  $x = \sigma(y^*x^*) \leftrightarrow y^*x^* \rightarrow x'$ . Thus, (i) implies (ii). Finally, suppose that (ii) holds, and let  $x' \in \Gamma_{x'/K(x')}$ . By (ii) there exists an  $x_0 \in \mathfrak{x}$  with  $x_0 \rightarrow x'$ . Let  $x$  be a  $K(\mathfrak{x})$ -generic element of a  $K(\mathfrak{x})$ -component of  $\mathfrak{x}$  containing  $x_0$ . Then  $x \in \Gamma_{x/K(x)}$  and  $x \rightarrow x_0$  whence  $x \rightarrow x'$ . Thus, (ii) implies (iii).

(b) It is obvious that (iii) implies (ii) and (ii) implies (i). Suppose that  $x_1, x_2 \in \mathfrak{x}$  and  $x_1', x_2' \in \mathfrak{x}'$  and  $x_1 \rightarrow x_1', x_2' \rightarrow x_2$ , and consider any  $x' \in \Gamma_{x'/K(x')}$ . By part (a) there exists an  $x \in \Gamma_{x/K(x)}$  such that  $x \rightarrow x'$ , and again by part (a) there exists an  $x'' \in \Gamma_{x''/K(x')}$  such that  $x'' \rightarrow x$ . Then  $x'' \rightarrow x'$  and  $\dim_K x'' \geq \dim_K x \geq \dim_K x'$ . By part (d) (the proof of which does not require the present part)  $\dim_K x'' = \dim_K x'$ , so that  $x \leftrightarrow x'$ . Therefore (i) implies (iii).

(c) Choose  $x \in \mathfrak{x}, x' \in \mathfrak{x}'$  with  $x \leftrightarrow x'$ . Then  $S_{x',x}$  can be extended to some  $\sigma \in \text{Aut}(U/K)$ , and  $\sigma(x) = \sigma(Hx) = H\sigma x = Hx' = \mathfrak{x}'$ . It follows, by Section 7, Corollary 1 to Theorem 4, that  $S_{x',x}$  maps  $K(\mathfrak{x})$  onto  $K(\mathfrak{x}')$  and that the induced isomorphism  $K(\mathfrak{x}) \approx K(\mathfrak{x}')$  does not depend on the choice of  $x, x'$ .

(d) For any  $x \in \mathfrak{x}, \mathfrak{x} = Hx = \rho_x(H)$ . It follows that every component of  $\mathfrak{x}$  has dimension equal to  $\dim H$ , and hence every  $K(\mathfrak{x})$ -component does too. Therefore, if  $x \in \Gamma_{x/K(x)}$ , then

$$\dim_K x = \text{tr deg } K(\mathfrak{x})/K + \text{tr deg } K(x)/K(\mathfrak{x}) = \text{tr deg } K(\mathfrak{x})/K + \dim H.$$

We now prove the existence of quotients by actual construction.

**Theorem 7** *Let  $H$  be a  $K$ -subgroup of a  $K$ -group  $G$ , and let  $G/H$  denote the set of right cosets of  $H$  in  $G$ . For  $\mathfrak{x} \in G/H$  define  $K(\mathfrak{x})$  to be the smallest extension  $L$  of  $K$  such that  $\mathfrak{x}$  is an  $L$ -subset of  $G$ . For  $\mathfrak{x}, \mathfrak{x}' \in G/H$  define  $\mathfrak{x} \rightarrow \mathfrak{x}'$  to mean that the equivalent conditions in Lemma 4(a) are satisfied. For  $\mathfrak{x}, \mathfrak{x}' \in G/H$  with  $\mathfrak{x} \leftrightarrow \mathfrak{x}'$  define  $S_{\mathfrak{x}',\mathfrak{x}}$  to be the isomorphism  $K(\mathfrak{x}) \approx K(\mathfrak{x}')$  induced as in Lemma 4(c) by the isomorphisms  $S_{x',x}$  with  $x \in \mathfrak{x}, x' \in \mathfrak{x}', x \leftrightarrow x'$ .*

(a) *These data define a pre- $K$ -set structure on  $G/H$ . The canonical mapping  $\pi_{G/H}: G \rightarrow G/H$  is a separable pre- $K$ -mapping. If  $f: G \rightarrow A$  is any everywhere defined pre- $K$ -mapping of  $G$  into a  $K$ -set  $A$  such that  $f$  is constant on each right coset of  $H$  in  $G$ , then the mapping  $g: G/H \rightarrow A$  such that  $g \circ \pi_{G/H} = f$  is a pre- $K$ -mapping;  $f$  is separable if and only if  $g$  is.*

(b) *The pre- $K$ -set structure on  $G/H$  and the canonical structure on  $G/H$  of homogeneous space for the group  $G$  define on  $G/H$  a structure of homogeneous  $K$ -space for  $G$ ;  $\pi_{G/H}$  is a  $K$ -homomorphism of homogeneous  $K$ -spaces, and  $G/H$  with  $\pi_{G/H}$  is a homogeneous  $K$ -space quotient of  $G$  by  $H$ .*

(c) *When  $H$  is a normal subgroup of  $G$ , the pre- $K$ -set structure on  $G/H$  and the canonical group structure on  $G/H$  define on  $G/H$  a structure of  $K$ -group;  $\pi_{G/H}$  is a  $K$ -homomorphism of  $K$ -groups, and  $G/H$  with  $\pi_{G/H}$  is a  $K$ -group quotient of  $G$  by  $H$ .*

*Proof* (a) It is apparent that if  $\mathfrak{x} \in G/H$ , then  $K(\mathfrak{x})$  is a finitely generated extension of  $K$ , that the relation  $\mathfrak{x} \rightarrow \mathfrak{x}'$  is a pre-order on  $G/H$ , and that if  $\mathfrak{x} \leftrightarrow \mathfrak{x}'$ , then  $S_{\mathfrak{x}',\mathfrak{x}}: K(\mathfrak{x}) \approx K(\mathfrak{x}')$  is an isomorphism over  $K$ . We must verify the axioms in Section 2. If  $\mathfrak{x} \rightarrow \mathfrak{x}'$ , but not  $\mathfrak{x}' \rightarrow \mathfrak{x}$ , and we choose  $x \in \Gamma_{x/K(x)}$  and  $x' \in \Gamma_{x'/K(x')}$  with  $x \rightarrow x'$ , then we do not have  $x' \rightarrow x$ . Hence  $\dim_K x > \dim_K x'$ , so that by Lemma 4(d),  $\text{tr deg } K(\mathfrak{x})/K > \text{tr deg } K(\mathfrak{x}')/K$ . This verifies axiom AS 1(a). Let  $x_1, \dots, x_m$  be  $K$ -generic elements of the  $K$ -components of  $G$ , and set  $\mathfrak{x} = Hx_i$  ( $1 \leq i \leq m$ ). For any  $\mathfrak{x} \in G/H$  and any  $x \in \mathfrak{x}$ , we have  $x_i \rightarrow x$  for some  $i$  and therefore  $\mathfrak{x}_i \rightarrow \mathfrak{x}$ . Since  $K(\mathfrak{x}_i) \supset K(\mathfrak{x}_i) \supset K$  and  $K(\mathfrak{x}_i)$

is separable over  $K$ ,  $K(x_i)$  is separable over  $K$ , too. This verifies axiom AS 1(b). Let  $\bar{x}, \bar{x}', \bar{x}'' \in G/H$  and  $\bar{x} \leftrightarrow \bar{x}'$ ,  $\bar{x}' \leftrightarrow \bar{x}''$ . Fixing an  $x'' \in \Gamma_{x''/K(x'')}$ , we can find an  $x' \in \Gamma_{x'/K(x')}$  with  $x' \leftrightarrow x''$  and then find an  $x \in \Gamma_{x/K(x)}$  with  $x \leftrightarrow x'$ . Since  $S_{x'',x'} \circ S_{x',x} = S_{x'',x}$  and  $S_{x',x}, S_{x'',x'}, S_{x'',x}$  are restrictions of  $S_{x',x}, S_{x'',x'}, S_{x'',x}$ , we conclude that  $S_{x'',x'} \circ S_{x',x} = S_{x'',x}$ . This verifies axiom AS 2(a). If  $\bar{x} \in G/H$ , and if  $S: K(\bar{x}) \approx K'$  is an isomorphism over  $K$ , we can fix an  $x \in \bar{x}$  and then extend  $S$  to an isomorphism  $T: K(x) \approx L$ . There exists a unique  $x' \in G$  with  $x \leftrightarrow x'$  such that  $K(x') = L$  and  $S_{x',x} = T$ , and if we set  $\bar{x}' = Hx'$ , then  $\bar{x} \leftrightarrow \bar{x}'$ ,  $S_{x',x} = S$ , and  $K(\bar{x}') = S_{x',x}(K(x)) = S(K(x)) = K'$ . To prove the uniqueness of  $\bar{x}'$ , suppose that also  $\bar{x}'' \in G/H$ ,  $\bar{x} \leftrightarrow \bar{x}''$ ,  $K(\bar{x}'') = K'$ , and  $S_{x'',x} = S$ . Then  $\bar{x}' \leftrightarrow \bar{x}''$ ,  $K(\bar{x}') = K(\bar{x}'')$ , and  $S_{x',x'} = id_{K(x')}$ , so that there exist elements  $z' \in \bar{x}'$  and  $z'' \in \bar{x}''$  with  $z' \leftrightarrow z''$  and with  $S_{z',z''}$  an extension of  $id_{K(x')}$ ;  $S_{z',z''}$  can be extended to some  $\sigma \in \text{Aut}(U/K(\bar{x}'))$ , and on the one hand (by Section 7, Theorem 4)  $\sigma\bar{x}' = \bar{x}'$ , and on the other hand  $\sigma\bar{x}' = \sigma(Hz') = \sigma H \cdot \sigma z' = Hz'' = \bar{x}''$ , whence  $\bar{x}' = \bar{x}''$ . This verifies axiom AS 2(b), and therefore shows that we have a pre- $K$ -set structure on  $G/H$ .

It follows immediately from the definitions that if  $x \in G$ , then  $K(x) \supset K(\pi_{G/H}(x))$ , that if  $x \rightarrow x'$ , then  $\pi_{G/H}(x) \rightarrow \pi_{G/H}(x')$ , and that if  $x \leftrightarrow x'$ , then  $S_{x',x}$  is an extension of  $S_{\pi_{G/H}(x'), \pi_{G/H}(x)}$ . Therefore  $\pi_{G/H}$  is a pre- $K$ -mapping. We saw above that each  $K$ -component of  $G/H$  has as a  $K$ -generic element one of the cosets  $\bar{x}_i = Hx_i$ , where  $x_1, \dots, x_m$  are  $K$ -generic elements of the  $K$ -components of  $G$ . For each  $i$ , we may evidently replace  $x_i$  by a  $K(x_i)$ -generic element of a  $K(x_i)$ -component of  $\bar{x}_i$  containing  $x_i$ ; that is, we may suppose that  $x_i \in \Gamma_{x_i/K(x_i)}$ . Then  $x_i$  is separable over  $K(x_i) = K(\pi_{G/H}(x_i))$  and (by Lemma 4(d))  $\dim_K x_i = \dim G - \dim H$  for every index  $i$ . The first conclusion here shows that the pre- $K$ -mapping  $\pi_{G/H}$  is separable; the second conclusion shows that each  $\bar{x}_i$  is a  $K$ -generic element of a  $K$ -component of  $G/H$ .

Let  $f: G \rightarrow A$  be any everywhere defined pre- $K$ -mapping such that  $f(x) = f(x')$  whenever  $\pi_{G/H}(x) = \pi_{G/H}(x')$ . Then there exists a unique mapping  $g: G/H \rightarrow A$  such that  $g \circ \pi_{G/H} = f$ . For any  $\bar{x} \in G/H$ , if we fix  $x \in \Gamma_{x/K(x)}$ , then we find that  $K(x)$  is separable over  $K(\bar{x})$ , and that  $g(\bar{x}) = f(x)$ , whence  $K(g(\bar{x})) \subset K(x)$ . Since  $\sigma x \in \sigma \bar{x} = \bar{x}$  for every  $\sigma \in \text{Aut}(U/K(\bar{x}))$ , and therefore  $\sigma(g(\bar{x})) = \sigma(f(x)) = f(\sigma x) = g(\bar{x})$ , we conclude that  $K(g(\bar{x})) \subset K(\bar{x})$ . If  $\bar{x} \rightarrow \bar{x}'$ , then  $x \rightarrow x'$  for some  $x \in \bar{x}$ ,  $x' \in \bar{x}'$ , and  $g(\bar{x}) = f(x) \rightarrow f(x') = g(\bar{x}')$ . If  $\bar{x} \leftrightarrow \bar{x}'$ , then  $x \leftrightarrow x'$  for some  $x \in \bar{x}$ ,  $x' \in \bar{x}'$ . Since  $S_{x',x}$  extends  $S_{x',x}$  and also extends the isomorphism  $S_{f(x'), f(x)} = S_{g(\bar{x}'), g(\bar{x})}$ , we conclude that  $S_{x',x}$  extends  $S_{g(\bar{x}'), g(\bar{x})}$ . This shows that  $g$  is a pre- $K$ -mapping. Finally, for each index  $i$ ,

$$K(x_i) \supset K(\bar{x}_i) \supset K(g(\bar{x}_i)) = K(f(x_i))$$

and  $K(x_i)$  is separable over  $K(x_i)$ . Therefore  $K(x_i)$  is separable over  $K(f(x_i))$  if and only if  $K(\bar{x}_i)$  is separable over  $K(g(\bar{x}_i))$ . We have seen above that each  $K$ -component of  $G/H$  has some  $\bar{x}_i$  as a  $K$ -generic element and that each  $\bar{x}_i$  is a  $K$ -generic element of a  $K$ -component of  $G/H$ , so that  $f$  is separable if and only if  $g$  is.

(b) We must verify the axioms AH 1(a) and AH 2(a) and (b). Let  $v \in G/H$ ,  $x \in G$ . Then  $\rho_x$  (right multiplication by  $x$ ) and its inverse  $\rho_{x^{-1}}$  are bijective pre- $L$ -mappings of  $G$  into  $G$  for every field  $L \supset K(x)$ , and  $v$  is an  $L$ -subset of  $G$  for every field  $L \supset K(v)$ . Taking  $L = K(v)K(x)$ , we infer that  $\rho_x(v)$  is a  $K(v)K(x)$ -subset of  $G$ , that is,  $K(vx) \subset K(v)K(x)$ . This verifies AH 1(a). Now let  $v, v' \in G/H$ ,  $x, x' \in G$ ,  $v \leftrightarrow v'$ ,  $x \leftrightarrow x'$ , and suppose that  $S_{v',v}, S_{x',x}$  are compatible, that is, that there exists a homomorphism

$$S_0: K[K(v) \cup K(x)] \rightarrow K[K(v') \cup K(x')]$$

extending  $S_{v',v}$  and  $S_{x',x}$ . By Section 7, corollary to Proposition 3,  $v$  contains an element  $v$  that is algebraic over  $K(v)$ , and evidently the ring  $K[K(v) \cup K(x)]$  is integral over  $K[K(v) \cup K(x)]$  so that (by Chapter 0, Section 14, Proposition 9)  $S_0$  can be extended to a homomorphism  $S$  of  $K[K(v) \cup K(x)]$  onto a subring of  $U$ . By axiom AS 2(b), there is an element  $v' \in G$  with  $v \leftrightarrow v'$  such that  $S$  coincides on  $K(v)$  with  $S_{v',v}$ , and by what precedes it follows that  $S_{\pi_{G/H}(v'), v} = S_{v',v}$  and  $v' \in v'$ . Hence  $S_{v',v}, S_{x',x}$  are compatible, so that  $v'x \rightarrow v'x'$ , whence, by definition,  $v'x \rightarrow v'x'$ . Moreover, if  $h: R \rightarrow R'$  is a homomorphism of subrings of  $U$  such that  $h, S_{v',v}, S_{x',x}$  are compatible, then the above construction can be carried out so that  $h, S_{v',v}, S_{x',x}$  are compatible, and therefore so that  $h, S_{v',v}, S_{x',x}, S_{v',v}$  are compatible, where

$$t \in \Gamma_{H \circ K(R)K(R')K(v)K(v')K(x)K(x')}$$

and hence so that  $h, S_{v',v}, S_{x',x}$  are compatible and  $tv'x \rightarrow tv'x'$ . However,  $tv'x \in \Gamma_{v'x/K(v'x)}$ , whence  $\dim_K tv'x = \dim_K v'x + \dim H$  and, similarly,  $\dim_K tv'x' = \dim_K v'x' + \dim H$ . Therefore in case  $v'x \leftrightarrow v'x'$ , then  $\dim_K tv'x = \dim_K tv'x'$  and  $tv'x \leftrightarrow tv'x'$ , and  $h, S_{tv'x', tv'x}$  are compatible. Since  $S_{tv'x', tv'x}$  is an extension of  $S_{v',v'x}$ , we conclude that in this case  $h, S_{v',v'x}$  are compatible. This verifies axiom AH 2(a). Now let  $v, v' \in G/H$ ,  $v \rightarrow v'$  and  $x, x' \in G$ ,  $x \rightarrow x'$ . Fixing elements  $v \in \Gamma_{v/K(v)}$ ,  $v' \in \Gamma_{v'/K(v')}$  with  $v \rightarrow v'$ , and letting  $V$ , respectively  $X$ , denote the locus of  $v$ , respectively  $x$ , over  $K$ , we see that  $(v', x') \in V \times X$ , and therefore we can fix a  $K$  generic element  $(v^*, x^*)$  of a  $K$  component of  $V \times X$  containing  $(v', x')$ . Letting  $t \in \Gamma_{H \circ K(v^*)K(x^*)K(v)K(x)}$ , we see that  $(v^*, x^*, t) \rightarrow (v', x', t)$  and hence  $(tv^*x^*, x^*) \rightarrow (tv'x', x')$ , so that  $tv^*x^* \rightarrow tv'x'$  and  $x^* \rightarrow x'$ , and if both these specializations are generic, then  $S_{tv'x', tv^*x^*}, S_{x', x^*}$  are compatible. It follows that  $\pi_{G/H}(tv^*x^*) \rightarrow \pi_{G/H}(tv'x')$ , that is, that  $v^*x^* \rightarrow v'x'$  (where we have set  $v^* = \pi_{G/H}(v^*)$ ), and also that if  $v^*x^* \leftrightarrow v'x'$  (so that  $\dim_K v^*x^* =$

$\dim_K v'x'$ , whence  $\dim_K tv^*x^* = \dim_K tv'x'$  by Lemma 4(d), and therefore  $tv^*x^* \leftrightarrow tv'x'$  and  $x^* \leftrightarrow x'$ , then  $S_{v'x', v^*x^*}, S_{x', x^*}$  are compatible. This verifies axiom AH 2(b), and shows that we have a structure on  $G/H$  of homogeneous  $K$  space for  $G$ .

The canonical mapping  $\pi_{G/H}: G \rightarrow G/H$  is, of course, a homomorphism of homogeneous spaces for the group  $G$ . By part (a), it is a pre- $K$ -mapping, and hence it is a  $K$ -homomorphism of homogeneous  $K$ -spaces.

If  $f: G \rightarrow M$  is any  $K$ -homomorphism of homogeneous  $K$ -spaces for  $G$  such that  $f(x) = f(x')$  whenever  $\pi_{G/H}(x) = \pi_{G/H}(x')$  and if  $g$  is the mapping  $G/H \rightarrow M$  such that  $g \circ \pi_{G/H} = f$ , then  $g$  is a homomorphism of homogeneous spaces. By part (a),  $g$  is a pre- $K$ -mapping, and hence is a  $K$ -homomorphism of homogeneous  $K$ -spaces. This shows that  $G/H$  with  $\pi_{G/H}$  is a homogeneous  $K$ -space quotient of  $G$  by  $H$ .

(c) Now suppose that  $H$  is normal in  $G$ . We must verify the axioms AG 1(a) and (b), AG 2(a)–(d), and AG 3. Consider any  $x, \eta \in G/H$ . For any  $y \in \eta$ ,  $K(x\eta) = K(x)y \subset K(x)K(y)$  by part (b) of the theorem. Since  $y$  can (by Section 7, the corollary to Proposition 3) be taken separable and algebraic over  $K(\eta)$ , we infer that every element of  $K(x\eta)$  is separably algebraic over  $K(x)K(\eta)$ . However, for any  $\sigma \in \text{Aut}(U/K(x)K(\eta))$ ,  $\sigma(x\eta) = (\sigma x)(\sigma \eta) = x\eta$ , and therefore (by Section 7, Corollary 2 to Theorem 4) every element of  $K(x\eta)$  is purely inseparably algebraic over  $K(x)K(\eta)$ . Therefore  $K(x\eta) \subset K(x)K(\eta)$ . Furthermore, the symmetry mapping  $\iota$  of  $G$  is an everywhere defined pre- $K$ -mapping of  $G$  into  $G$  that is its own inverse, and therefore  $K(x^{-1}) = K(\iota(x)) = K(x)$ . Hence, by what we have just shown above,  $K(x^{-1}\eta) \subset K(x^{-1})K(\eta) = K(x)K(\eta)$ . Thus, we have verified axioms AG 1(a) and (b). The verification of AG 2(a)–(d) is very similar to that of AH 2(a) and (b) in the proof of part (b) of the theorem, and will be omitted. Finally, we saw in the proof of part (a) that if  $x \in \Gamma_{G/H}$ , then  $\pi_{G/H}(x) \in \Gamma_{(G/H)/K}$ . Taking  $x \in \Gamma_{G^0/K}$ , we easily find that  $\pi_{G/H}(x)$  is a  $K$ -generic element of a  $K$ -component of  $G/H$  containing the element  $\pi_{G/H}(1) = 1$  of the group  $G/H$ . Since  $K(x) \supset K(\pi_{G/H}(x)) \supset K$ ,  $\pi_{G/H}(x)$  is regular over  $K$ . This verifies AG 3, and shows that we have a  $K$ -group structure on  $G/H$ . The canonical mapping  $\pi_{G/H}: G \rightarrow G/H$  is, of course, a group homomorphism, and we saw in part (a) that it is a pre- $K$ -mapping. Therefore it is a  $K$ -homomorphism of  $K$ -groups. If  $f: G \rightarrow G'$  is a  $K$ -homomorphism of  $K$ -groups with kernel containing  $H$ , then there is a unique mapping  $g: G/H \rightarrow G'$  such that  $g \circ \pi_{G/H} = f$ , and  $g$  is, of course, a group homomorphism. By part (a),  $g$  is a pre- $K$ -mapping, and therefore is a  $K$ -homomorphism of  $K$ -groups. This shows that  $G/H$  with  $\pi_{G/H}$  is a  $K$ -group quotient of  $G$  by  $H$ .

**Corollary 1** *Let  $H$  and  $J$  be  $K$ -subgroups of the  $K$ -group  $G$  with  $J$  normal in  $G$  and  $H \supset J$ . Then  $H/J$  is a  $K$ -subgroup of the  $K$ -group  $G/J$ , and the canonical*

*mapping  $g: G/H \rightarrow (G/J)/(H/J)$  is a  $K$ -isomorphism of homogeneous  $K$ -spaces for  $G$ . When  $H$  is normal in  $G$  (and therefore  $H/J$  is normal in  $G/J$ ), then  $g$  is a  $K$ -isomorphism of  $K$ -groups.*

*Proof* By Theorem 7,  $\pi_{G/J}$  is a surjective separable  $K$ -homomorphism of  $K$ -groups. Its restriction to  $H$  is a  $K$ -homomorphism of  $K$ -groups and by Section 9, Proposition 10(a), the image  $\pi_{G/J}(H) = H/J$  is a  $K$ -subgroup of  $G/J$  (normal in  $G/J$  when  $H$  is normal in  $G$ ). It is obviously equal to the  $K$ -group quotient of  $H$  by  $J$ . Again by Theorem 7,  $\pi_{(G/J)/(H/J)}$  is a separable  $K$ -homomorphism of homogeneous  $K$ -spaces for  $G/J$ , and hence also of homogeneous  $K$ -spaces for  $G$  (and is a surjective separable  $K$ -homomorphism of  $K$ -groups, when  $H$  is normal in  $G$ ). Therefore  $\pi_{(G/J)/(H/J)} \circ \pi_{G/J}$  is a surjective separable  $K$ -homomorphism  $G \rightarrow (G/J)/(H/J)$  of homogeneous  $K$ -spaces for  $G$  (of  $K$ -groups, when  $H$  is normal). Since it evidently is constant on each right coset of  $H$  in  $G$ , there is a unique mapping  $g: G/H \rightarrow (G/J)/(H/J)$  such that  $g \circ \pi_{G/H} = \pi_{(G/J)/(H/J)} \circ \pi_{G/J}$  (this is the canonical mapping), and by Theorem 7,  $g$  is a surjective separable  $K$ -homomorphism of homogeneous  $K$ -spaces for  $G$  (of  $K$ -groups, when  $H$  is normal). As  $g$  is evidently injective, it follows from Section 9, Corollaries 4 and 5 to Theorem 5, that  $g$  is a  $K$ -isomorphism.

**Corollary 2** *Let  $H$  and  $J$  be  $K$ -subgroups of the  $K$ -group  $G$  with  $J$  normal in  $G$ . Then  $HJ$  is a  $K$ -subgroup of  $G$ ,  $H \cap J$  is a normal  $K$ -closed subgroup of  $H$ , and the canonical group isomorphism  $h: H/(H \cap J) \rightarrow HJ/J$  is a  $K$ -homomorphism. When  $H \cap J$  happens to be a  $K$ -subgroup of  $H$ ,  $h$  is a  $K$ -homomorphism.*

*Proof* By Theorem 7,  $\pi_{G/J}$  is a  $K$ -homomorphism of  $K$ -groups. So is the inclusion mapping  $j: H \rightarrow G$ , and hence  $\pi_{G/J} \circ j$  is too. By Section 9, Proposition 10(a), the image  $(\pi_{G/J} \circ j)(H) = \pi_{G/J}(H)$  is a  $K$ -subgroup of  $G/J$ , and therefore by Section 9, Theorem 5, the inverse image  $\pi_{G/J}^{-1}(\pi_{G/J}(H)) = HJ$  is a  $K$ -subgroup of  $G$ . This being the case, the inclusion mapping  $j': H \rightarrow HJ$  followed by the mapping  $\pi_{HJ/J}: HJ \rightarrow HJ/J$  is a surjective  $K$ -homomorphism of  $K$ -groups, and its kernel is  $H \cap J$  which is  $K$ -closed, that is, is a normal  $K$ -subgroup of  $H$ . It follows by Theorem 7 that the mapping  $h: H/(H \cap J) \rightarrow HJ/J$  with  $h \circ \pi_{H/(H \cap J)} = \pi_{HJ/J} \circ j'$  is a  $K$ -homomorphism (and is a  $K$ -homomorphism when  $H \cap J$  is a  $K$ -group).

## 12 Galois cohomology

For any Galois extension  $L$  of the field  $K$ , denote the Galois group of  $L$  over  $K$  by  $g(L/K)$ . We recall (see for example Bourbaki [5, Appendix II]) that  $g(L/K)$  is a topological group (compact and totally disconnected).

In the topology (usually called the *Krull topology*), a fundamental system of neighborhoods of the unity element  $1 = id_L$  is the set of all groups  $g(L/E)$  with  $E$  a subfield of  $L$  that is a Galois extension of  $K$  of finite degree. (When  $L$  is of finite degree over  $K$ , the Krull topology is discrete.) Given another Galois extension  $L'$  of  $K$ , with  $L' \subset L$ , we can consider the mapping  $\rho_{L',L}: g(L/K) \rightarrow g(L'/K)$  that sends each  $\gamma \in g(L/K)$  onto its restriction to  $L'$ ;  $\rho_{L',L}$  is a continuous surjective homomorphism with kernel  $g(L/L')$ . It follows that if  $\mathfrak{E} = \mathfrak{E}(L/K)$  denotes the set of all Galois extensions  $E$  of  $K$  of finite degree with  $E \subset L$ , then the formula  $\gamma \mapsto (\rho_{E,L}(\gamma))_{E \in \mathfrak{E}}$  defines a continuous injective homomorphism  $g(L/K) \rightarrow \prod_{E \in \mathfrak{E}} g(E/K)$  (when the topology on the direct product is the product topology) and a homeomorphism between  $g(L/K)$  and its image. The image is the set of all families  $(\sigma_E) \in \prod_{E \in \mathfrak{E}} g(E/K)$  such that  $\sigma_{E_1}, \sigma_{E_2}$  coincide on  $E_1 \cap E_2$  for all  $E_1, E_2 \in \mathfrak{E}$ , that is, is the projective limit of the projective system  $((g(E/K))_{E \in \mathfrak{E}}, (\rho_{E',E})_{E, E' \in \mathfrak{E}, E' \subset E})$ . Hence,  $g(L/K)$  can be identified with this projective limit:

$$g(L/K) = \varprojlim g(E/K).$$

Consider any pre- $K$ -set  $A$ . We recall from Section 2 that each element  $\gamma \in g(L/K)$  induces a bijection  $x \mapsto \gamma x$  of  $A_L$  onto itself, and we have an operation of  $g(L/K)$  on  $A_L$ :

$$g(L/K) \times A_L \rightarrow A_L, \quad (\gamma, x) \mapsto \gamma x.$$

We regard  $A$  as a topological space with discrete topology and  $A_L$  as a subspace; then the operation is continuous. An element  $x \in A_L$  is an invariant of  $g(L/K)$  if and only if  $x \in A_K$ . This set  $A_K$  of invariants is sometimes called the *0th cohomology set of  $g(L/K)$  in  $A$* , and is then denoted by  $H^0(L/K, A)$ . Of course, for all Galois extensions  $L$  of  $K$ ,  $H^0(L/K, A)$  is one and the same set  $A_K$ . It is sometimes called the *0th Galois cohomology set of  $K$  in  $A$  and is then denoted by  $H^0(K, A)$ .*

Now let  $A$  be a  $K$ -group  $G$ . The set  $H^0(K, G) = G_K$  is now a subgroup of  $G$  (called the *0th Galois cohomology group of  $K$  in  $G$* ), as is  $G_L$ , and the elements of  $g(L/K)$  operate on  $G_L$  as group automorphisms:

$$\gamma(xy) = (\gamma x)(\gamma y).$$

A *one-dimensional cocycle of  $g(L/K)$  into  $G$*  is defined as a continuous mapping  $f: g(L/K) \rightarrow G$  such that  $f(g(L/K)) \subset G_L$  and

$$f(\gamma\gamma') = f(\gamma) \cdot \gamma(f(\gamma')) \quad (\gamma, \gamma' \in g(L/K)).$$

The set of all such cocycles is denoted by  $Z^1(L/K, G)$ . For any  $f \in Z^1(L/K, G)$ ,  $f(1) = 1$  and  $f(\gamma) \cdot \gamma(f(\gamma^{-1})) = 1$ . It follows that the *kernel* of  $f$  (the set of all elements  $\gamma \in g(L/K)$  with  $f(\gamma) = 1$ ) is an open and closed subgroup of

$g(L/K)$ . Given two cocycles  $f$  and  $g$ ,  $g$  is *cohomologous to  $f$*  if there exists an element  $x \in G_L$  such that  $g(\gamma) = x^{-1}f(\gamma)\gamma x$  for all  $\gamma \in g(L/K)$ . The relation “ $g$  is cohomologous to  $f$ ” is an equivalence on  $Z^1(L/K, G)$ . The set of equivalence classes (called *cohomology classes*) is called the *1st cohomology set of  $g(L/K)$  in  $G$*  and is denoted by  $H^1(L/K, G)$ . For any element  $x \in G_L$  the formula  $\gamma \mapsto x^{-1}\gamma x$  defines a one-dimensional cocycle of  $g(L/K)$  into  $G$ . The cocycles of this form are called *coboundaries*, and the set of all of them is denoted by  $B^1(L/K, G)$ . It consists of the elements of  $Z^1(L/K, G)$  that are cohomologous to the cocycle given by the formula  $\gamma \mapsto 1$ , and therefore is an element of  $H^1(L/K, G)$ . As such, it is denoted by  $1$  (or by  $0$  when the group  $G$  is commutative and written additively). Thus,  $H^1(L/K, G)$  has a structure of pointed set.

REMARK A *pointed set* is a set with a distinguished element. A pointed set is *trivial* if it has no other element. A *homomorphism* of a pointed set  $X$  into a pointed set  $Y$  is a mapping  $X \rightarrow Y$  that sends the distinguished element of  $X$  onto that of  $Y$ . The *kernel* of such a homomorphism is the set of elements of  $X$  that are mapped onto the distinguished element of  $Y$ . The homomorphism is *trivial* if its kernel is  $X$ . A sequence of homomorphisms of pointed sets is *exact* if each homomorphism but the last has image equal to the kernel of the next homomorphism in the sequence.

For any Galois extension  $L'$  of  $K$  with  $L' \subset L$ , the formula  $f' \mapsto f' \circ \rho_{L',L}$  ( $f' \in Z^1(L'/K, G)$ ) defines a mapping  $Z^1(L'/K, G) \rightarrow Z^1(L/K, G)$ . Suppose  $f', g' \in Z^1(L'/K, G)$ . If  $x \in G_L$  and  $g'(\gamma') = x^{-1}f'(\gamma')\gamma' x$  ( $\gamma' \in g(L'/K)$ ), then

$$\begin{aligned} (g' \circ \rho_{L',L})(\gamma) &= g'(\rho_{L',L}(\gamma)) = x^{-1}f'(\rho_{L',L}(\gamma))\rho_{L',L}(\gamma) x \\ &= x^{-1}(f' \circ \rho_{L',L})(\gamma)\gamma x \quad (\gamma \in g(L/K)). \end{aligned}$$

Conversely, if  $x \in G_L$  and  $(g' \circ \rho_{L',L})(\gamma) = x^{-1}(f' \circ \rho_{L',L})(\gamma)\gamma x$  ( $\gamma \in g(L/K)$ ), then  $1 = x^{-1}\gamma x$  ( $\gamma \in g(L/L')$ ), so that  $x \in G_{L'}$  and  $g'(\gamma') = x^{-1}f'(\gamma')\gamma' x$  ( $\gamma' \in g(L'/K)$ ). This shows that  $g'$  is cohomologous to  $f'$  if and only if  $g' \circ \rho_{L',L}$  is cohomologous to  $f' \circ \rho_{L',L}$ , so that the mapping  $Z^1(L'/K, G) \rightarrow Z^1(L/K, G)$  induces an injective homomorphism

$$\rho_{L',L}^*: H^1(L'/K, G) \rightarrow H^1(L/K, G)$$

of pointed sets.

It is now an easy matter to see that

$$((H^1(E/K, G))_{E \in \mathfrak{E}}, (\rho_{E',E}^*)_{E, E' \in \mathfrak{E}, E' \subset E})$$

is an inductive system ( $\mathfrak{E} = \mathfrak{E}(L/K)$  denoting, as before, the set of Galois extensions of  $K$  of finite degree that are contained in  $L$ ). Hence we may form the inductive limit  $\varinjlim H^1(E/K, G)$ . The canonical homo-

morphisms  $\rho_{E'}^* : H^1(E'/K, G) \rightarrow \lim H^1(E/K, G)$ , defined for each  $E' \in \mathfrak{E}$ , have the property that  $\rho_{E'}^* \circ \rho_{E'', E'}^* = \rho_{E''}^*$  when  $E'' \subset E'$ ; because also  $\rho_{E', L}^* \circ \rho_{E'', E'}^* = \rho_{E', L}^*$  when  $E'' \subset E'$ , there exists a unique homomorphism  $g : \lim H^1(E/K, G) \rightarrow H^1(L/K, G)$ , such that  $g \circ \rho_E^* = \rho_{E, L}^*$  ( $E \in \mathfrak{E}$ ). Now, for any  $f \in Z^1(L/K, G)$ , the kernel of  $f$  is an open subgroup of  $\mathfrak{g}(L/K)$  and therefore contains  $\mathfrak{g}(L/E)$  for some  $E \in \mathfrak{E}$ . Evidently  $f$  is constant on each coset of  $\mathfrak{g}(L/E)$  in  $\mathfrak{g}(L/K)$ , and from this it follows that if  $\gamma \in \mathfrak{g}(L/K)$ , then, for every  $\gamma' \in \mathfrak{g}(L/E)$ ,

$$\gamma' f(\gamma) = f(\gamma') \gamma' f(\gamma) = f(\gamma' \gamma) = f(\gamma \cdot \gamma^{-1} \gamma' \gamma) = f(\gamma) \gamma f(\gamma^{-1} \gamma' \gamma) = f(\gamma),$$

whence  $f(\gamma) \in G_E$ . It also follows, since  $\mathfrak{g}(L/K)/\mathfrak{g}(L/E) \approx \mathfrak{g}(E/K)$ , that there is a unique mapping  $f_E : \mathfrak{g}(E/K) \rightarrow G$  such that  $f_E \circ \rho_{E, L} = f$ , and we easily infer that  $f_E \in Z^1(E/K, G)$ . This shows that the cohomology class of  $f$  is contained in  $\rho_{E, L}^*(H^1(E/K, G))$ , and therefore (see Bourbaki [4, § 1, Proposition 10]) that  $g$  is surjective. On the other hand, if for some  $E \in \mathfrak{E}$  and two cocycles  $f_E, g_E \in Z^1(E/K, G)$  the cocycles  $f_E \circ \rho_{E, L}, g_E \circ \rho_{E, L} \in Z^1(L/K, G)$  are cohomologous, then there exists some  $x \in G_L$  such that  $g_E(\rho_{E, L}(\gamma)) = x^{-1} f_E(\rho_{E, L}(\gamma)) \gamma x$  ( $\gamma \in \mathfrak{g}(L/K)$ ). Evidently  $x \in G_{E'}$  for some  $E' \in \mathfrak{E}$  with  $E \subset E'$ , and

$$g_E(\rho_{E, E'}(\rho_{E', L}(\gamma))) = x^{-1} f_E(\rho_{E, E'}(\rho_{E', L}(\gamma))) \rho_{E', L}(\gamma) x \quad (\gamma \in \mathfrak{g}(L/K)),$$

so that  $(g_E \circ \rho_{E, E'})(\gamma') = x^{-1} (f_E \circ \rho_{E, E'})(\gamma') \gamma' x$  ( $\gamma' \in \mathfrak{g}(E'/K)$ ), that is, the cocycles  $f_E \circ \rho_{E, E'}, g_E \circ \rho_{E, E'} \in Z^1(E'/K, G)$  are cohomologous. This shows (see Bourbaki, *loc. cit.*) that  $g$  is injective. Thus, the homomorphism  $g$  is an isomorphism, and may be used to identify  $H^1(L/K, G)$  with  $\lim H^1(E/K, G)$ .

When the  $K$ -group  $G$  is commutative, then  $Z^1(L/K, G)$  is a commutative group (the product of two one-dimensional cocycles  $f$  and  $g$  being defined by the formula  $(fg)(\gamma) = f(\gamma)g(\gamma)$ ),  $B^1(L/K, G)$  is a subgroup, and  $H^1(L/K, G)$  is the quotient group  $Z^1(L/K, G)/B^1(L/K, G)$ . Furthermore the mappings  $\rho_{E, L}^*, \rho_E^*, g$  above then are homomorphisms of groups, not merely of pointed sets.

The largest Galois extension of  $K$  is its separable closure  $K_s$ . The cohomology set  $H^1(K_s/K, G)$  is called the 1st Galois cohomology set of  $K$  in  $G$ , and for brevity is usually denoted by  $H^1(K, G)$ . Correspondingly,  $Z^1(K_s/K, G)$  is denoted by  $Z^1(K, G)$  and  $B^1(K_s/K, G)$  is denoted by  $B^1(K, G)$ . As explained above,  $H^1(K, G)$  contains (a canonically isomorphic image of)  $H^1(L/K, G)$  for every Galois extension  $L$  of  $K$ , and may be regarded as the inductive limit of the pointed sets  $H^1(E/K, G)$  with  $E$  running over the set of all Galois extensions of  $K$  of finite degree.

Consider a  $K$ -homomorphism  $\varphi : G \rightarrow G'$  of  $K$ -groups. If  $f \in Z^1(K, G)$ , then, as is easy to verify,  $\varphi \circ f \in Z^1(K, G')$ . If, also,  $g \in Z^1(K, G)$  and  $x \in G_{K_s}$ , then  $\varphi(x) \in G'_{K_s}$  and the condition

$$g(\gamma) = x^{-1} f(\gamma) \gamma x \quad (\gamma \in \mathfrak{g}(K_s/K))$$

implies the condition

$$(\varphi \circ g)(\gamma) = \varphi(x)^{-1} (\varphi \circ f)(\gamma) \gamma \varphi(x) \quad (\gamma \in \mathfrak{g}(K_s/K)).$$

Therefore the formula  $f \mapsto \varphi \circ f$  defines a mapping  $Z^1(K, G) \rightarrow Z^1(K, G')$  which induces a mapping

$$\varphi^1 : H^1(K, G) \rightarrow H^1(K, G').$$

It is obvious that  $\varphi^1$  is a homomorphism of pointed sets (and of groups when  $G$  and  $G'$  are commutative). Also, since  $\varphi(x) \in G'_K$  whenever  $x \in G_K$ ,  $\varphi$  induces a group homomorphism

$$\varphi^0 : H^0(K, G) \rightarrow H^0(K, G').$$

This induced mapping  $\varphi^0$  is defined even when  $G$  and  $G'$  are merely pre- $K$ -sets and  $\varphi$  is merely an everywhere defined pre- $K$ -mapping. Furthermore, when each of  $G$  and  $G'$  is a pointed pre- $K$ -set (a pre- $K$ -set with a distinguished element that is rational over  $K$ ) and  $\varphi$  is a  $K$ -homomorphism of pointed pre- $K$ -sets (an everywhere defined pre- $K$ -mapping that maps the distinguished element of  $G$  onto that of  $G'$ ), then  $\varphi^0$  is a homomorphism of pointed sets. If we have a second  $K$ -homomorphism of  $K$ -groups  $\psi : G' \rightarrow G''$ , then evidently  $(\psi \circ \varphi)^i = \psi^i \circ \varphi^i$  ( $i = 0, 1$ ). Also,  $(id_G)^i = id_{H^i(K, G)}$ . It follows that if  $\varphi$  is a  $K$ -isomorphism, then  $\varphi^i$  is an isomorphism ( $i = 0, 1$ ).

Starting afresh, let  $G'$  be a  $K$ -subgroup of the  $K$ -group  $G$  and consider the homogeneous  $K$ -space  $G/G'$  of right cosets of  $G'$  in  $G$ . Let  $in$  denote the inclusion homomorphism  $G' \rightarrow G$  and  $\pi$  denote the canonical mapping  $\pi_{G/G'} : G \rightarrow G/G'$ . By Section 7, Corollary to Proposition 3, for any element  $x \in (G/G')_K$  there exists an element  $x \in G_{K_s}$  such that  $\pi(x) = x$ , and  $x$  is evidently unique up to a left factor in  $G'_{K_s}$ , that is,  $x$  can be replaced by any element of  $G'_{K_s} x$  but by no other element; it is easy to see that the formula  $\gamma \mapsto x \gamma x^{-1}$  ( $\gamma \in \mathfrak{g}(K_s/K)$ ) defines an element of  $Z^1(K, G')$ , and that the cohomology class of this element is independent of the choice of  $x$ , that is, is determined by  $x$ . We denote this cohomology class by  $\delta x$ . When  $x$  is the distinguished element of the pointed set  $G/G'$ , that is, is the coset  $G'$ , we can take  $x = 1$ , so that then  $\delta x = 1$ . Thus, we have a homomorphism

$$\delta : H^0(K, G/G') \rightarrow H^1(K, G')$$

of pointed sets.



**Theorem 8** Let  $G'$  be a  $K$ -subgroup of the  $K$ -group  $G$ . Then the sequence

$$1 \longrightarrow H^0(K, G') \xrightarrow{\text{in}^0} H^0(K, G) \xrightarrow{\pi^0} H^0(K, G/G') \xrightarrow{\delta} H^1(K, G') \xrightarrow{\text{in}^1} H^1(K, G)$$

of homomorphisms of pointed sets is exact. When  $G'$  is normal in  $G$ , then also the sequence

$$H^1(K, G') \xrightarrow{\text{in}^1} H^1(K, G) \xrightarrow{\pi^1} H^1(K, G/G')$$

of homomorphisms of pointed sets is exact.

*Proof* It is obvious that the former sequence is exact at  $H^0(K, G')$  and at  $H^0(K, G)$ . Let  $x \in H^0(K, G/G') = (G/G')_K$ , and choose an element  $x \in G_{K_s}$  with  $\pi(x) = x$ , that is, with  $x \in \mathfrak{x}$ . Then

$$\begin{aligned} \delta x = 1 &\Leftrightarrow \text{there exists an } x' \in G'_{K_s} \text{ such that } x'^{-1} \gamma x' = x \gamma x^{-1} \ (\gamma \in \mathfrak{g}(K_s/K)) \\ &\Leftrightarrow \text{there exists an } x' \in G'_{K_s} \text{ such that } x' x \in G_K \\ &\Leftrightarrow \text{there exists a } y \in G_K \text{ such that } \pi^0 y = x. \end{aligned}$$

Therefore the sequence is exact at  $H^0(K, G/G')$ . Now let  $f' \in H^1(K, G')$  and fix an  $f' \in \bar{f}'$  (so that  $f' \in Z^1(K, G')$ ). Then

$$\begin{aligned} \text{in}^1(\bar{f}') = 1 &\Leftrightarrow \text{in} \circ f' \in B^1(K, G) \\ &\Leftrightarrow \text{there exists an } x \in G_{K_s} \text{ such that } f'(\gamma) = x \gamma x^{-1} \ (\gamma \in \mathfrak{g}(K_s/K)) \\ &\quad \text{(so that } \sigma(G'x) = G'x \ (\sigma \in \text{Aut}(U/K)), \text{ whence } G'x \in (G/G')_K) \\ &\Leftrightarrow \text{there exists an } \mathfrak{x} \in (G/G')_K \text{ such that } \delta \mathfrak{x} = \bar{f}'. \end{aligned}$$

Therefore the sequence is exact at  $H^1(K, G')$ , and hence is exact. Finally, suppose that  $G'$  is a normal  $K$ -subgroup of  $G$ , let  $\bar{f} \in H^1(K, G)$ , and fix  $f \in \bar{f}$  (so that  $f \in Z^1(K, G)$ ). Then

$$\begin{aligned} \pi^1(\bar{f}) = 1 &\Leftrightarrow \pi \circ f \in B^1(K, G/G') \\ &\Leftrightarrow \text{there exists an } \mathfrak{x} \in (G/G')_{K_s} \text{ such that } (\pi \circ f)(\gamma) = \mathfrak{x}^{-1} \gamma \mathfrak{x} \ (\gamma \in \mathfrak{g}(K_s/K)) \\ &\Leftrightarrow \text{there exists an } x \in G_{K_s} \text{ such that } f(\gamma) \in G' x^{-1} \gamma x, \\ &\quad \text{that is, such that, } x f(\gamma) \gamma x^{-1} \in G' \ (\gamma \in \mathfrak{g}(K_s/K)) \\ &\Leftrightarrow \text{there exists a } g \in \bar{f} \text{ such that } g(\mathfrak{g}(K_s/K)) \subset G'_{K_s} \\ &\Leftrightarrow \text{there exists a } g' \in Z^1(K, G') \text{ such that } \text{in} \circ g' \in \bar{f} \\ &\Leftrightarrow \text{there exists a } \bar{g}' \in H^1(K, G') \text{ such that } \text{in}^1(\bar{g}') = \bar{f}. \end{aligned}$$

This shows that the second sequence is exact, and completes the proof.

**Corollary** Let  $G'$  be a normal  $K$ -subgroup of the  $K$ -group  $G$ , and suppose that  $H^1(K, G') = 1$  and  $H^1(K, G/G') = 1$ . Then  $H^1(K, G) = 1$ .

*Proof* By the theorem, the sequence  $H^1(K, G') \xrightarrow{\text{in}^1} H^1(K, G) \xrightarrow{\pi^1} H^1(K, G/G')$  is exact. Since  $H^1(K, G/G') = 1$ , the kernel of  $\pi^1$  is  $H^1(K, G)$ . By exactness, the image of  $\text{in}^1$  is  $H^1(K, G)$ . Since  $H^1(K, G') = 1$ , the image of  $\text{in}^1$  is 1. Hence  $H^1(K, G) = 1$ .

**Theorem 9** Let  $G$  be a  $K$ -group.

(a) Each of the following six conditions is sufficient for  $H^1(K, G)$  to be trivial: (i)  $G = \mathbf{G}_a$ ; (ii)  $G = \mathbf{G}_m$ ; (iii)  $G = \mathbf{GL}(n)$ ; (iv)  $G = \mathbf{SL}(n)$ ; (v)  $K = K_s$ ; (vi)  $K$  is finite and  $G$  is connected.

(b) If  $G$  is commutative, then every element of the commutative group  $H^1(K, G)$  has finite order.

*Proof* Since  $H^1(K, G)$  is the inductive limit of the pointed sets  $H^1(L/K, G)$  with  $L$  a Galois extension of  $K$  of finite degree, it suffices to prove the corresponding statements for the sets  $H^1(L/K, G)$ .

(a) The facts that  $H^1(L/K, \mathbf{G}_a) = 0$  and  $H^1(L/K, \mathbf{G}_m) = 1$  are the additive and multiplicative parts of the well-known generalization of Hilbert's "Theorem 90" (for example, see Lang [22, Chapter VIII, § 10, Theorem 17]).

In showing that  $H^1(L/K, \mathbf{GL}(n)) = 1$ , we may suppose that  $K$  is infinite, for the finite case comes under (vi). For any  $f \in Z^1(L/K, \mathbf{GL}(n))$ , the polynomial  $\det(\sum_{\gamma \in \mathfrak{g}(L/K)} X_\gamma f(\gamma))$  in  $L[(X_\gamma)_{\gamma \in \mathfrak{g}(L/K)}]$  is not 0, because it does not vanish when one  $X_\gamma$  is replaced by 1 and the others are replaced by 0. Therefore (see, for example, Lang [22, Chapter VIII, § 11, Theorem 19], or Bourbaki [5, Chapter V, § 10, Theorem 4]) there exists an element  $\alpha \in L$  such that this polynomial does not vanish at  $(\gamma \alpha)_{\gamma \in \mathfrak{g}(L/K)}$ , that is, such that the matrix  $x = \sum_{\gamma} \gamma \alpha \cdot f(\gamma)$  is in  $\mathbf{GL}(n)$ . The computation

$$\gamma' x = \sum_{\gamma} \gamma' \gamma \alpha \cdot \gamma' f(\gamma) = \sum_{\gamma} \gamma' \gamma \alpha \cdot f(\gamma')^{-1} f(\gamma' \gamma) = f(\gamma')^{-1} x$$

shows that  $f(\gamma') = x \gamma' x^{-1}$  ( $\gamma' \in \mathfrak{g}(L/K)$ ), whence  $f \in B^1(L/K, \mathbf{GL}(n))$ . Hence  $H^1(L/K, \mathbf{GL}(n)) = 1$ .

The  $K$ -homomorphism  $\det: \mathbf{GL}(n) \rightarrow \mathbf{G}_m$  is surjective and separable, and has kernel  $\mathbf{SL}(n)$ . Hence there is a  $K$ -isomorphism  $g: \mathbf{G}_m \approx \mathbf{GL}(n)/\mathbf{SL}(n)$  such that  $g \circ \det = \pi (= \pi_{\mathbf{GL}(n)/\mathbf{SL}(n)})$ . Since  $\det$  evidently maps  $\mathbf{GL}_K(n)$  onto  $K^* = (\mathbf{G}_m)_K$ , this implies that  $\pi$  maps  $\mathbf{GL}_K(n)$  onto  $(\mathbf{GL}(n)/\mathbf{SL}(n))_K$ . In other words if, in the first exact sequence of Theorem 8, we take  $G = \mathbf{GL}(n)$  and  $G' = \mathbf{SL}(n)$ , then  $\pi^0$  is surjective. By exactness then  $\delta$  is trivial and  $\text{in}^1$

is injective. However,  $H^1(K, \mathbf{GL}(n)) = 1$ , so that  $in^1$  is trivial. Hence  $H^1(K, \mathbf{SL}(n)) = 1$ .

If  $K = K_s$ , then  $g(K_s/K) = 1$ , so that  $H^1(K, G) = 1$  for any  $G$ .

That  $H^1(K, G) = 1$  whenever  $K$  is finite and  $G$  is connected was proved by Lang. As we shall not need this result, we refer to Exercise 3(c), below.

(b) Suppose that  $G$  is commutative, and consider any  $f \in Z^1(L/K, G)$ . Set  $x = \prod_{\gamma \in g(L/K)} f(\gamma)^{-1}$ . Then  $x \in G_L$  and

$$\gamma'x = \prod_{\gamma} \gamma'f(\gamma)^{-1} = \prod_{\gamma} (f(\gamma'\gamma)^{-1}f(\gamma)) = xf(\gamma')^d,$$

where  $d = [L:K]$ , so that  $f^d \in B^1(L/K, G)$ . Hence, every element of  $H^1(L/K, G)$  has order dividing  $d$ .

EXERCISES

1. (a) Show that if  $G_1$  and  $G_2$  are  $K$ -groups, then there exists a canonical isomorphism  $H^1(K, G_1 \times G_2) \approx H^1(K, G_1) \times H^1(K, G_2)$ .  
 (b) Show that if a  $K$ -group  $G$  has a normal sequence of  $K$ -groups  $G = G_0 \supset \dots \supset G_r = 1$  such that  $H^1(K, G_{k-1}/G_k) = 1$  ( $1 \leq k \leq r$ ), then  $H^1(K, G) = 1$ .  
 (c) Show that whenever  $G$  is one of the  $K$ -groups  $\mathbf{D}(n), \mathbf{T}(n), \mathbf{T}(n, k)$  described in Section 1 then  $H^1(K, G) = 1$ .
2. (Kolchin and Lang [19, Proposition 2]) Let  $A$  be an algebra over  $U$  with finite basis  $(e_1, \dots, e_n)$ , let  $K$  be a field such that  $e_i e_j \in \sum_{1 \leq l \leq n} K e_l$  ( $1 \leq i \leq n, 1 \leq j \leq n$ ), and let  $A^*$  denote the group of invertible elements of  $A$ .  
 (a) Show that there exists a polynomial  $D \in K[X_1, \dots, X_n]$  such that an element  $\sum \alpha_i e_i \in A$  is in  $A^*$  if and only if  $D(\alpha_1, \dots, \alpha_n) \neq 0$ , and then define on  $A^*$  a structure of  $K$ -group.  
 (b) Prove that  $H^1(K, A^*) = 1$  (generalization of Theorem 9(a), case (iii)).
3. (Lang [20]) Let  $K$  be the finite field with  $q = p^e$  elements, and let  $\varphi$  denote the automorphism of  $U$  defined by the formula  $\varphi(\alpha) = \alpha^q$ . Let  $G$  be a connected  $K$ -group.  
 (a) Prove that if  $y \in G$  and  $x \in \Gamma_{G/K(y)}$ , then  $\varphi(x)yx^{-1} \in \Gamma_{G/K(y)}$ . (Hint: Observe that  $K(y)K(\varphi(x)yx^{-1})K(x)^q = K(y)K(\varphi(x)yx^{-1})K(\varphi(x)) = K(y)K(x)$ , and use the following well-known fact: If  $E$  is an extension of a field  $F$  of characteristic  $p$ , then a necessary and sufficient condition that  $E$  be separably algebraic over  $F$  is that  $FE^q = E$ .)  
 (b) Prove that if  $y \in G$ , then there exists a  $z \in G$  such that  $z^{-1}\varphi(z) = y$ . (Hint: Fix  $x \in \Gamma_{G/K(y)}$ , show by part (a) that  $\varphi(x)x^{-1} \xleftrightarrow{K(y)} \varphi(x)y^{-1}x^{-1}$ ,

and infer the existence of a  $\tau \in \text{Aut}(U/K(y))$  such that  $\tau(\varphi(x)x^{-1}) = \varphi(x)y^{-1}x^{-1}$ . Then set  $z = \tau x^{-1} \cdot x$  and observe that  $\varphi \circ \tau = \tau \circ \varphi$ .)

(c) Prove that if  $K_d$  denotes the extension of  $K$  of degree  $d$  (where  $d \in \mathbf{N}, d \geq 1$ ), then  $H^1(K_d/K, G) = 1$ . (Hint: Let  $f \in Z^1(K_d/K, G)$  and let  $\gamma$  denote the restriction of  $\varphi$  to  $K_d$ . Observe that  $g(K_d/K)$  is cyclic of order  $d$  and is generated by  $\gamma$ . By part (b) fix  $z \in G$  with  $z^{-1}\varphi(z) = f(\gamma)$ , and show that  $f(\gamma^n) = z^{-1}\varphi^n(z)$  ( $n \in \mathbf{N}$ ). Set  $n = d$ , infer that  $z \in G_{K_d}$ , and conclude that  $f \in B^1(K_d/K, G)$ .)

(d) Let  $M$  be a homogeneous  $K$ -space for  $G$ . Show that  $M_K \neq \emptyset$ . (Hint: Fix  $v \in M, y \in G$  with  $vy = \varphi(v), z \in G$  with  $z^{-1}\varphi(z) = y$ , and show that  $yz^{-1} \in M_K$ .)

13 Principal homogeneous  $K$ -spaces

The purpose of the present section is to explain the well-known classification of principal homogeneous  $K$ -spaces for a given  $K$ -group  $G$  in terms of the Galois cohomology set  $H^1(K, G)$ . This classification was first obtained in certain special cases by Châtelet [7].

Consider a principal homogeneous  $K$ -space  $M$  for  $G$ . By Section 7, corollary to Proposition 3,  $M_{K_s} \neq \emptyset$ . For any element  $v \in M_{K_s}$ , the formula  $\Phi_{M, v}(\gamma) = v^{-1}\gamma v$  defines a mapping  $\Phi_{M, v}: g(K_s/K) \rightarrow G$ . Letting  $E_v$  denote the Galois extension of  $K$  generated by  $K(v)$ , we see for any  $\gamma \in g(K_s/K)$  that  $\Phi_{M, v}$  is constant on the neighborhood  $\gamma g(K_s/E_v)$  of  $\gamma$  in  $g(K_s/K)$ ; hence  $\Phi_{M, v}$  is continuous. For any  $\gamma, \gamma' \in g(K_s/K), \Phi_{M, v}(\gamma\gamma') = v^{-1}\gamma v \cdot \gamma(v^{-1}\gamma'v) = \Phi_{M, v}(\gamma)\gamma(\Phi_{M, v}(\gamma'))$ . Therefore  $\Phi_{M, v} \in Z^1(K, G)$ .

**Theorem 10** Let  $G$  be a  $K$ -group.

- (a) For every pair  $(M, v)$  such that  $M$  is a principal homogeneous  $K$ -space for  $G$  and  $v \in M_{K_s}, \Phi_{M, v} \in Z^1(K, G)$ .
- (b) For two such pairs  $(M, v)$  and  $(M', v')$ ,  $M$  is  $K$ -isomorphic to  $M'$  if and only if  $\Phi_{M, v}$  is cohomologous to  $\Phi_{M', v'}$ .
- (c) Each element of  $Z^1(K, G)$  is  $\Phi_{M, v}$  for some such pair  $(M, v)$ .

**REMARK** Given a  $K$  group  $G$ , a one-dimensional cocycle  $f \in Z^1(K, G)$ , and a principal homogeneous  $K$ -space  $M$  for  $G$ , if there exists an element  $v \in M_{K_s}$  such that  $f = \Phi_{M, v}$ , then we say that  $f$  splits in  $M$ . By the theorem, every one-dimensional cocycle splits in some principal homogeneous  $K$ -space  $M$  for  $G$ , and  $M$  is unique up to  $K$ -isomorphism.

*Proof* Part (a) is already proved. To prove part (b), first observe that if  $F: M \approx M'$  is a  $K$ -isomorphism, then for every  $\gamma \in g(K_s/K), \gamma(F(v)) =$

$F(\gamma v) = F(v \cdot v^{-1} \gamma v) = F(v) v^{-1} \gamma v$ . Hence if we set  $x = F(v)^{-1} v'$ , then  $x \in G_{K_s}$  and

$$\begin{aligned} \Phi_{M',v'}(\gamma) &= v'^{-1} \gamma v' = v'^{-1} F(v) \cdot F(v)^{-1} \gamma F(v) \cdot \gamma (F(v)^{-1} v') \\ &= x^{-1} \cdot v^{-1} \gamma v \cdot \gamma x = x^{-1} \Phi_{M,v}(\gamma) \gamma x, \end{aligned}$$

so that  $\Phi_{M,v}$  is cohomologous to  $\Phi_{M',v'}$ . Conversely, if  $\Phi_{M,v}$  is cohomologous to  $\Phi_{M',v'}$ , that is, if there exists an  $x \in G_{K_s}$  such that  $\Phi_{M',v'}(\gamma) = x^{-1} \Phi_{M,v}(\gamma) \gamma x$  for every  $\gamma \in \mathfrak{g}(K_s/K)$ , then we define the mapping  $F: M \rightarrow M'$  by the formula  $F(w) = v' \cdot (vx)^{-1} w$ , and evidently  $F$  is a  $K_s$ -isomorphism (indeed,  $F = \lambda_v \circ \lambda_{vx}^{-1}$ ). For any  $\sigma \in \text{Aut}(U/K)$  the restriction of  $\sigma$  to  $K_s$  is an element  $\gamma$  of  $\mathfrak{g}(K_s/K)$ , and

$$\begin{aligned} \sigma(F(w)) &= \gamma v' \cdot \gamma (vx)^{-1} \sigma w = v' \Phi_{M',v'}(\gamma) \cdot \gamma (vx)^{-1} \sigma w \\ &= v' x^{-1} \Phi_{M,v}(\gamma) \gamma x \cdot \gamma (vx)^{-1} \sigma w = v' (vx)^{-1} \sigma w = F(\sigma w), \end{aligned}$$

so that by Section 9, Corollary 2 to Proposition 9,  $F$  is a  $K$ -isomorphism. This proves part (b).

Now let  $f \in Z^1(K, G)$ . We shall construct a pair  $(M, v)$  such that  $f = \Phi_{M,v}$  by a process known as *twisting*  $G$  by the cocycle  $f$ .

Because  $f$  is a continuous mapping of  $\mathfrak{g}(K_s/K)$  (Krull topology) into  $G$  (discrete topology), the kernel of  $f$  is an open and closed subgroup of  $\mathfrak{g}(K_s/K)$ . Since it is closed, the kernel is  $\mathfrak{g}(K_s/L)$  for some extension  $L$  of  $K$  in  $K_s$ . Since it is open, the kernel contains  $\mathfrak{g}(K_s/E')$  for some Galois extension  $E'$  of  $K$  of finite degree. Hence  $L \subset E'$ , so that  $[L:K]$  is finite. Letting  $E$  denote the Galois extension of  $K$  generated by  $L$ , we see that  $[E:K]$  is finite and  $\mathfrak{g}(K_s/E)$  is contained in the kernel of  $f$ .

Consider any  $\gamma \in \mathfrak{g}(K_s/K)$ . For any  $\gamma' \in \mathfrak{g}(K_s/L)$ ,  $f(\gamma\gamma') = f(\gamma)\gamma(f(\gamma')) = f(\gamma)$ , so that  $f$  is constant on the coset  $\gamma\mathfrak{g}(K_s/L)$ , and hence also on the coset  $\gamma\mathfrak{g}(K_s/E) = \mathfrak{g}(K_s/E)\gamma$ . Therefore, for every  $\gamma' \in \mathfrak{g}(K_s/E)$ ,  $\gamma'(f(\gamma)) = f(\gamma')\gamma'(f(\gamma)) = f(\gamma')\gamma = f(\gamma)$ , so that  $f(\gamma) \in G_E$ . Thus, the image of  $f$  is contained in  $G_E$ .

For any  $\sigma \in \text{Aut}(U/K)$ , the restriction of  $\sigma$  to  $K_s$  is an element  $\gamma \in \mathfrak{g}(K_s/K)$ . We permit ourselves to denote  $f(\gamma)$  simply by  $f(\sigma)$ . Then  $f(\sigma) \in G_E$  ( $\sigma \in \text{Aut}(U/K)$ ),  $f(\sigma\tau) = f(\sigma)f(\tau)$  ( $\sigma, \tau \in \text{Aut}(U/K)$ ), and  $f(\sigma) = 1$  if and only if  $\sigma \in \text{Aut}(U/L)$ .

Fix a set  $M$  having the same cardinal number as  $G$ , fix a bijection  $\Lambda: G \rightarrow M$ , and set  $v = \Lambda(1)$ . We are going to define on  $M$  a structure of principal homogeneous  $K$ -space for  $G$  such that  $v \in M_{K_s}$  and  $v^{-1} \gamma v = f(\gamma)$  ( $\gamma \in \mathfrak{g}(K_s/K)$ ). This will prove part (c) and complete the proof of theorem.

For any  $(w, x) \in M \times G$  define  $wx = \Lambda(\Lambda^{-1}(w)x)$ . It is easy to verify that  $w1 = w$  ( $w \in M$ ),  $(wx)y = w(xy)$  ( $w \in M, x \in G, y \in G$ ), and  $wG = M$  ( $w \in M$ ). For any  $(w_1, w_2) \in M^2$  define  $w_1^{-1}w_2 = \Lambda^{-1}(w_1)^{-1}\Lambda^{-1}(w_2)$ . Then

$w^{-1}(wx) = \Lambda^{-1}(w)^{-1}\Lambda^{-1}(\Lambda(\Lambda^{-1}(w)x)) = \Lambda^{-1}(w)^{-1}\Lambda^{-1}(w)x = x$  ( $w \in M, x \in G$ ). Thus,  $M$  is a principal homogeneous space for  $G$ .

For any  $x \in G$ , let  $\mathfrak{g}(x)$  denote the set of all  $\sigma \in \text{Aut}(U/K)$  such that  $f(\sigma)\sigma x = x$ . Because of the identity  $f(\sigma\tau) = f(\sigma)\sigma(f(\tau))$ , it is easy to see that  $\mathfrak{g}(x)$  is a subgroup of  $\text{Aut}(U/K)$ . If  $\sigma \in \mathfrak{g}(x)$ , then  $\sigma(E(x)) = E(\sigma x) = E(f(\sigma)^{-1}x) = E(x)$ . Therefore the restriction  $\sigma_{E(x)}$  of  $\sigma$  to  $E(x)$  is an automorphism of  $E(x)$  over  $K$ . If two elements  $\sigma, \tau \in \mathfrak{g}(x)$  coincide on  $E$ , then  $f(\sigma) = f(\tau)$  whence  $\sigma x = \tau x$ , and therefore  $\sigma, \tau$  coincide on  $E(x)$ . This shows that the formula  $\sigma \mapsto \sigma_{E(x)}$  defines a homomorphism of  $\mathfrak{g}(x)$  onto a finite subgroup  $\mathfrak{g}(x)_{E(x)}$  of  $\text{Aut}(E(x)/K)$ .

Given any  $w \in M$ , if we set  $x = \Lambda^{-1}(w)$ , then, since  $v = \Lambda(1)$ , evidently  $x = v^{-1}w$ . We define  $K(w)$  to be the field of invariants of the finite group  $\mathfrak{g}(x)_{E(x)}$ . Then  $K \subset K(w) \subset E(x)$ ,  $K(w)$  is a finitely generated extension of  $K$ , and  $K(w)$  is separable over  $K$  whenever  $E(x)$  is separable over  $E$ . Furthermore,  $E(x)$  is a Galois extension of  $K(w)$  of finite degree, and  $\mathfrak{g}(x) = \text{Aut}(U/K(w))$ .

Given any  $w, w' \in M$ , we set  $x = \Lambda^{-1}(w)$ ,  $x' = \Lambda^{-1}(w')$ , and define  $w \xrightarrow{K} w'$  to mean that  $f(\sigma)\sigma x \xrightarrow{E} x'$  for some  $\sigma \in \text{Aut}(U/K)$ . Obviously,  $w \xrightarrow{K} w$ . If  $f(\sigma)\sigma x \xrightarrow{E} x'$  and  $f(\sigma')\sigma'x' \xrightarrow{E} x''$ , then (because  $f(\sigma') \in G_E$ )  $f(\sigma')\sigma'\sigma x = f(\sigma')\sigma'(f(\sigma))\sigma'\sigma x = f(\sigma')\sigma'(f(\sigma)\sigma x) \xrightarrow{E} f(\sigma')\sigma'x' \xrightarrow{E} x''$ . This shows that if  $w \xrightarrow{K} w'$  and  $w' \xrightarrow{K} w''$ , then  $w \xrightarrow{K} w''$ . Therefore the relation  $w \xrightarrow{K} w'$  on  $M$  is a pre-order. We observe that if  $w \xrightarrow{K} w'$ , then

$$\begin{aligned} \text{tr deg } K(w)/K &= \text{tr deg } E(x)/E = \text{tr deg } E(f(\sigma)\sigma x)/E \\ &\geq \text{tr deg } E(x')/E = \text{tr deg } K(w')/K, \end{aligned}$$

and that if  $\text{tr deg } K(w)/K = \text{tr deg } K(w')/K$ , then  $f(\sigma)\sigma x \xleftrightarrow{E} x'$ , whence  $f(\sigma^{-1})\sigma^{-1}x' \xrightarrow{E} x$  and  $w' \xrightarrow{K} w$ . This shows that if  $w \xrightarrow{K} w'$  but not  $w \xrightarrow{K} w$ , then  $\text{tr deg } K(w)/K > \text{tr deg } K(w')/K$ . It also shows that if  $w \xleftrightarrow{K} w'$ , then  $f(\sigma)\sigma x \xleftrightarrow{E} x'$  for some  $\sigma \in \text{Aut}(U/K)$ , so that for some  $\sigma' \in \text{Aut}(U/E)$ ,  $x' = \sigma'(f(\sigma)\sigma x) = f(\sigma')\sigma'(f(\sigma)\sigma x) = f(\sigma'\sigma)\sigma'\sigma x$ . Thus, a necessary and sufficient condition that  $w \xleftrightarrow{K} w'$  is that  $f(\sigma)\sigma x = x'$  for some  $\sigma \in \text{Aut}(U/K)$ .

Continuing the above notation, let  $w \xleftrightarrow{K} w'$  and fix  $\sigma \in \text{Aut}(U/K)$  with  $f(\sigma)\sigma x = x'$ . A straightforward computation shows that  $\sigma\mathfrak{g}(x)\sigma^{-1} = \mathfrak{g}(x')$ . Since  $\sigma(E(x)) = E(\sigma x) = E(f(\sigma)^{-1}x') = E(x')$ , this implies that  $\sigma$  maps the field of invariants of  $\mathfrak{g}(x)$  in  $E(x)$  onto the field of invariants of  $\mathfrak{g}(x')$  in  $E(x')$ , that is,  $\sigma$  restricts to an isomorphism  $K(w) \approx K(w')$ . Since two different automorphisms  $\sigma$  with  $f(\sigma)\sigma x = x'$  determine the same left coset

$\sigma g(x)$  and hence coincide on  $K(w)$ , we can define  $S_{w',w}^K: K(w) \approx K(w')$  to be the isomorphism obtained by restricting  $\sigma$ .

If  $w, w', w'' \in M$  and  $w \xleftrightarrow{K} w' \xleftrightarrow{K} w''$ , and we set  $x = \Lambda^{-1}(w)$ ,  $x' = \Lambda^{-1}(w')$ ,  $x'' = \Lambda^{-1}(w'')$ , then there exist  $\sigma, \sigma' \in \text{Aut}(U/K)$  such that  $f(\sigma)\sigma x = x'$  and  $f(\sigma')\sigma' x' = x''$ , and for these,

$$f(\sigma'\sigma)\sigma'\sigma x = f(\sigma')\sigma'(f(\sigma)\sigma x) = f(\sigma')\sigma'x' = x''.$$

This shows that  $S_{w',w}^K \circ S_{w'',w'}^K = S_{w'',w}^K$ . Again, if  $w \in M$  and  $S: K(w) \approx K'$  is an isomorphism over  $K$ , where  $K'$  is an extension of  $K$ , then  $S$  can be extended to an element  $\sigma \in \text{Aut}(U/K)$  and we can set  $x = \Lambda^{-1}(w)$ ,  $x' = f(\sigma)\sigma x$ , and  $w' = \Lambda(x')$ . Evidently  $w \xleftrightarrow{K} w'$ ,  $K(w') = K'$ , and  $S_{w',w}^K = S$ . To prove that  $w'$  is unique, let also  $w'' \in M$ ,  $w \xleftrightarrow{K} w''$ ,  $S_{w'',w}^K = S$ , and  $x'' = \Lambda^{-1}(w'')$ . There exists a  $\tau \in \text{Aut}(U/K)$  such that  $f(\tau)\tau x = x''$  and  $\tau$  extends  $S$ , and evidently  $\sigma^{-1}\tau \in \text{Aut}(U/K(w)) = g(x)$ , so that

$$x'' = f(\tau)\tau x = f(\sigma\sigma^{-1}\tau)\sigma(\sigma^{-1}\tau x) = f(\sigma)\sigma(f(\sigma^{-1}\tau)\sigma^{-1}\tau x) = f(\sigma)\sigma x = x'$$

and  $w'' = w'$ . We note for use below that we have shown, for any  $w \in M$  and any  $\sigma \in \text{Aut}(U/K)$ , that  $\sigma w = \Lambda(f(\sigma)\sigma(\Lambda^{-1}(w)))$ .

We have now verified that  $M$ , with the above definitions of the extensions  $K(w)$ , the pre-order  $w \xrightarrow{K} w'$ , and the isomorphisms  $S_{w',w}^K$ , satisfies all the axioms in Section 2 with the possible exception of AS 1(b). However,  $G$  has a finite subset  $\Psi$  consisting of an  $E$ -generic element of each  $E$ -component of  $G$ , and we may set  $\Phi = \Lambda(\Psi)$ . For every  $x \in \Psi$ ,  $E(x)$  is separable over  $E$ . As remarked above, it follows for every  $w \in \Phi$  that  $K(w)$  is separable over  $K$ . Given any  $w' \in M$ , we can set  $x' = \Lambda^{-1}(w')$  and then find an element  $x \in \Psi$  such that  $x \xrightarrow{E} x'$ . Setting  $w = \Lambda(x)$ , we find that  $w \in \Phi$  and  $w \xrightarrow{K} w'$ . This verifies axiom AS 1(b) and established  $M$  as a pre- $K$ -set.

To show that  $M$  is a principal homogeneous  $K$ -space for the  $K$ -group  $G$ , we must verify the appropriate axioms in Section 3.

Consider any  $(w, y) \in M \times G$ , and set  $x = \Lambda^{-1}(w)$ . Then  $E(x)$  is a Galois extension of  $K(w)$ , so that  $E(x)K(y)$  is a Galois extension of  $K(w)K(y)$ . Because  $\text{Aut}(U/K(w)) = g(x)$ , for every  $\sigma \in \text{Aut}(U/K(w)K(y))$  we have  $f(\sigma)\sigma(xy) = f(\sigma)\sigma x \cdot \sigma y = xy$ , that is,  $\sigma \in g(xy)$ . However,  $\Lambda(xy) = \Lambda(\Lambda^{-1}(w)y) = wy$ , so that  $g(xy) = \text{Aut}(U/K(wy))$ . Hence  $\text{Aut}(U/K(w)K(y)) \subset \text{Aut}(U/K(wy))$ . Since  $K(wy) \subset E(xy) \subset E(x)K(y)$ , this implies that  $K(wy) \subset K(w)K(y)$ . Starting afresh, consider any  $(w, w') \in M^2$ , and set  $x = \Lambda^{-1}(w)$ ,  $x' = \Lambda^{-1}(w')$ . Then  $w^{-1}w' = x^{-1}x'$ , whence  $K(w^{-1}w') \subset E(x)E(x')$ , and  $E(x)E(x')$  is a Galois extension of  $K(w)K(w')$ . For any  $\sigma \in \text{Aut}(U/K(w)K(w')) = \text{Aut}(U/K(w)) \cap \text{Aut}(U/K(w')) = g(x) \cap g(x')$ ,

$$\sigma(w^{-1}w') = \sigma(x^{-1}x') = (f(\sigma)^{-1}x)^{-1}(f(\sigma)^{-1}x') = x^{-1}x' = w^{-1}w'.$$

This implies that  $K(w^{-1}w') \subset K(w)K(w')$ . Thus, we have verified axioms AH 1(a) and (b).

Consider any  $(w, w', y, y') \in M^2 \times G^2$ , and any homomorphism  $h: R \rightarrow R'$  of subrings of  $U$ , and suppose that  $w \xleftrightarrow{K} w'$  and  $y \xleftrightarrow{K} y'$ , and that the homomorphisms  $h, S_{w',w}^K, S_{y',y}^K$  are compatible, that is, that there is a homomorphism

$$S: K[R \cup K(w) \cup K(y)] \rightarrow K[R' \cup K(w') \cup K(y')]$$

extending  $h, S_{w',w}^K, S_{y',y}^K$ . Set  $x = \Lambda^{-1}(w)$ ,  $x' = \Lambda^{-1}(w')$ . Because  $w \xleftrightarrow{K} w'$ , there exists an element  $\sigma \in \text{Aut}(U/K)$  with  $f(\sigma)\sigma x = x'$ , and  $\sigma$  is an extension of  $S_{w',w}^K$ . Since the ring  $K[R \cup E(x) \cup K(y)]$  is obviously integral over  $K[R \cup K(w) \cup K(y)]$ ,  $S$  can be extended to a homomorphism of the former, and the image is evidently  $K[R' \cup E(x') \cup K(y')]$ ; that is,  $S$  can be extended to a homomorphism

$$T: K[R \cup E(x) \cup K(y)] \rightarrow K[R' \cup E(x') \cup K(y')]$$

that maps  $E(x)$  onto  $E(x')$ . Then  $T$  coincides on  $E(x)$  with some  $\tau \in \text{Aut}(U/K)$ . Evidently  $\sigma$  and  $\tau$  coincide on  $K(w)$ . Hence  $\sigma^{-1}\tau \in \text{Aut}(U/K(w)) = g(x)$ , so that

$$f(\tau)\tau x = f(\sigma\sigma^{-1}\tau)\sigma(\sigma^{-1}\tau x) = f(\sigma)\sigma(f(\sigma^{-1}\tau)\sigma^{-1}\tau x) = f(\sigma)\sigma x = x'.$$

The formula  $\alpha \mapsto T\tau^{-1}\alpha$  defines a homomorphism.

$$K[\tau(R) \cup E(x') \cup K(\tau y)] \rightarrow K[R' \cup E(x') \cup K(y')]$$

that on  $\tau(R)$  coincides with  $h \circ \tau_R^{-1}$  ( $\tau_R$  denoting the restriction  $R \approx \tau(R)$  of  $\tau$ ), on  $E(x')$  coincides with  $id_{E(x')} = S_{x',x'}^E$ , and on  $K(\tau y)$  coincides with  $S_{y',\tau y}^K$ . In particular,  $S_{x',x'}^E$  and  $S_{y',\tau y}^K$  are compatible, so that  $(f(\tau)\tau x, \tau y) = (x', \tau y) \xrightarrow{E} (x', y')$ , whence  $f(\tau)\tau(xy) \xrightarrow{E} x'y'$ , and therefore  $wy \xrightarrow{K} w'y'$ . Furthermore, if  $wy \xleftrightarrow{K} w'y'$ , then  $f(\tau)\tau(xy) \xleftrightarrow{E} x'y'$ , and  $h \circ \tau_R^{-1}$  and  $S_{x'y', f(\tau)\tau(xy)}^E$  are compatible, so that  $h$  and  $S_{x'y', f(\tau)\tau(xy) \circ \tau_{E(xy)}}$  are compatible ( $\tau_{E(xy)}$  denoting the restriction  $E(xy) \approx E(\tau(xy)) = E(f(\tau)\tau(xy))$  of  $\tau$ ). However,  $S_{x'y', f(\tau)\tau(xy)}^E$  can be extended to some  $\rho \in \text{Aut}(U/E)$ , and  $f(\rho\tau)\rho\tau(xy) = f(\rho)\rho f(\tau)\rho\tau(xy) = 1 \cdot \rho(f(\tau)\tau(xy)) = x'y'$ . It follows that  $\rho\tau$  (and hence also  $S_{x'y', f(\tau)\tau(xy) \circ \tau_{E(xy)}}$ ) extends  $S_{w'y', wy}^E$ , and therefore  $h$  and  $S_{w'y', wy}^E$  are compatible. This verifies axiom AH 2(a).

Now consider any  $(w_1, w_2, w_1', w_2') \in M^4$ , and any homomorphism  $h: R \rightarrow R'$  of subrings of  $U$ , and suppose that  $w_1 \xleftrightarrow{K} w_1'$  and  $w_2 \xleftrightarrow{K} w_2'$ , and that  $h, S_{w_1',w_1}^K, S_{w_2',w_2}^K$  are compatible; that is, that there exists a homomorphism

$$S: K[R \cup K(w_1) \cup K(w_2)] \rightarrow K[R' \cup K(w_1') \cup K(w_2')]$$

that extends  $h, S_{w_1', w_1}^K, S_{w_2', w_2}^K$ . Set  $x_i = \Lambda^{-1}(w_i)$  and  $x_i' = \Lambda^{-1}(w_i')$  ( $i=1, 2$ ). Because  $w_i \xrightarrow{K} w_i'$ , there exists a  $\sigma_i \in \text{Aut}(U/K)$  such that  $f(\sigma_i)\sigma_i x_i = x_i'$ , and  $\sigma_i$  is an extension of  $S_{w_i', w_i}^K$ . Since  $K[R \cup E(x_1) \cup E(x_2)]$  is integral over  $K[R \cup K(w_1) \cup K(w_2)]$ ,  $S$  can be extended to a homomorphism

$$T: K[R \cup E(x_1) \cup E(x_2)] \rightarrow K[R' \cup E(x_1') \cup E(x_2')]$$

that maps  $E(x_i)$  onto  $E(x_i')$ . Then  $T$  coincides on  $E(x_i)$  with some  $\tau_i \in \text{Aut}(U/K)$ , and  $\sigma_i$  and  $\tau_i$  coincide on  $K(w_i)$ , so that  $\sigma_i^{-1}\tau_i \in \text{Aut}(U/K(w_i)) = \mathfrak{g}(x_i)$  and

$$x_i' = f(\sigma_i)\sigma_i x_i = f(\sigma_i)\sigma_i(f(\sigma_i^{-1}\tau_i)\sigma_i^{-1}\tau_i x_i) = f(\tau_i)\tau_i x_i = \tau_i(f(\tau_i^{-1})^{-1}x_i).$$

It follows that  $(f(\tau_1^{-1})^{-1}x_1, f(\tau_2^{-1})^{-1}x_2) \xrightarrow{K} (x_1', x_2')$ . Since  $\tau_1^{-1}$  and  $\tau_2^{-1}$  evidently coincide on  $E$ ,  $f(\tau_1^{-1}) = f(\tau_2^{-1})$ . Hence we conclude that

$$w_1^{-1}w_2 = x_1^{-1}x_2 = (f(\tau_1^{-1})^{-1}x_1)^{-1}(f(\tau_2^{-1})^{-1}x_2) \xrightarrow{K} x_1'^{-1}x_2' = w_1'^{-1}w_2',$$

and that if  $w_1^{-1}w_2 \xrightarrow{K} w_1'^{-1}w_2'$  then  $h$  and  $S_{w_1'^{-1}w_2', w_1^{-1}w_2}$  are compatible.

This verifies axiom AH 2(c).

Next, let  $(w, w', y, y') \in M^2 \times G^2$  and suppose that  $w \xrightarrow{K} w', y \xrightarrow{K} y'$ . Set  $x = \Lambda^{-1}(w)$ ,  $x' = \Lambda^{-1}(w')$ . By definition, there exists a  $\sigma \in \text{Aut}(U/K)$  with  $f(\sigma)\sigma x \xrightarrow{E} x'$ . Set  $x^* = f(\sigma)\sigma x$  and  $w^* = \Lambda(x^*)$ , so that  $w \xleftarrow{K} w^*$ . Let  $X^*$  denote the locus of  $x^*$  over  $E$  and  $Y$  denote the locus of  $y$  over  $K$ . Evidently  $X^* \times Y$  is an  $E$ -subset of  $G^2$  containing  $(x', y')$ . Let  $(x_1, y_1)$  be an  $E$ -generic element of an  $E$ -component of  $X^* \times Y$  that contains  $(x', y')$ . Then  $(x_1, y_1) \xrightarrow{E} (x', y')$ , and also  $x^* \xleftarrow{E} x_1, y \xleftarrow{K} y_1$ , so that there exists a  $\rho \in \text{Aut}(U/E)$  such that  $x_1 = \rho x^* = \rho(f(\sigma)\sigma x) = f(\rho)\rho(f(\sigma)\sigma x) = f(\rho\sigma)\rho\sigma x$ . Set  $y^* = \rho^{-1}y_1$ ; of course,  $y \xleftarrow{K} y^*$ . It is clear that  $(x_1, y_1)$  are quasi-independent over  $K$ , so that  $x^*, y^*$  are too, and therefore  $w^*, y^*$  are quasi-independent over  $K$ . Since  $(\rho x^*, \rho y^*) = (x_1, y_1) \xrightarrow{E} (x', y')$ , we know that

$$(\rho x^*, \rho y^*, \rho(x^*y^*)) \xrightarrow{E} (x', y', x'y'). \tag{*}$$

Hence  $\rho(x^*y^*) \xrightarrow{E} x'y'$ , so that (because  $f(\rho) = 1$ , and  $x^*y^* = \Lambda^{-1}(w^*y^*)$  and  $x'y' = \Lambda^{-1}(w'y')$ )  $w^*y^* \xrightarrow{K} w'y'$ . Furthermore, if  $w^*y^* \xleftarrow{K} w'y', y^* \xleftarrow{K} y'$ , then  $\rho(x^*y^*) \xleftarrow{E} x'y', \rho y^* \xleftarrow{E} y'$ , and therefore by (\*)  $S_{x'y', \rho(x^*y^*)}^E, S_{y', \rho y^*}^E$  are compatible. Also, then there exists a  $\tau \in \text{Aut}(U/E)$  such that  $x'y' = \tau\rho(x^*y^*)$ , and  $\tau\rho$  is an extension of  $S_{w'y', w^*y^*}^K$ , so that  $S_{x'y', x^*y^*}^E$  is, too. As we may evidently write

$$S_{x'y', x^*y^*}^E = S_{x'y', \rho(x^*y^*)}^E \circ S_{\rho(x^*y^*), x^*y^*}^E \quad \text{and} \quad S_{y', y^*}^E = S_{y', \rho y^*}^E \circ S_{\rho y^*, y^*}^E,$$

we infer that the two isomorphisms  $S_{x'y', x^*y^*}^E, S_{y', y^*}^E$  are compatible. As they are extensions respectively of  $S_{w'y', w^*y^*}^K, S_{y', y^*}^K$ , these are compatible too. This verifies axiom AH 2(b).

Finally, let  $(w_1, w_1', w_2, w_2') \in M^4$  and suppose that  $w_1 \xrightarrow{K} w_1', w_2 \xrightarrow{K} w_2'$ . For each  $i$  ( $i=1, 2$ ), set  $x_i = \Lambda^{-1}(w_i)$ ,  $x_i' = \Lambda^{-1}(w_i')$ . Then there exists a  $\sigma_i \in \text{Aut}(U/K)$  such that  $f(\sigma_i)\sigma_i x_i \xrightarrow{E} x_i'$ . Let  $X_i$  denote the locus of  $f(\sigma_i)\sigma_i x_i$  over  $E$ . Let  $(x_1^*, x_2^*)$  be an  $E$ -generic element of an  $E$ -component of  $X_1 \times X_2$  that contains  $(x_1', x_2')$ . Set  $w_i^* = \Lambda(x_i^*)$ . Then  $f(\sigma_i)\sigma_i x_i \xleftarrow{E} x_i^*$ , so that  $w_i \xleftarrow{K} w_i^*$ . Also,  $x_1^*, x_2^*$  are quasi-independent over  $K$ , so that  $w_1^*, w_2^*$  are quasi-independent over  $K$ . Now  $(x_1^*, x_2^*) \xrightarrow{E} (x_1', x_2')$ , so that  $x_1^{*-1}x_2^* \xrightarrow{E} x_1'^{-1}x_2'$ . However,

$$w_1^{*-1}w_2^* = \Lambda^{-1}(w_1^*)^{-1}\Lambda^{-1}(w_2^*) = x_1^{*-1}x_2^*,$$

and similarly  $x_1'^{-1}x_2' = w_2'^{-1}w_1'$ . Therefore  $w_1^{*-1}w_2^* \xrightarrow{K} w_1'^{-1}w_2'$ . This verifies AH 2(d), and shows that  $M$  is a principal homogeneous  $K$ -space for the  $K$ -group  $G$ .

We now show that  $v \in M_{K_s}$  and that  $v^{-1}\gamma v = f(\gamma)$  ( $\gamma \in {}_w(K_s/K)$ ). We have already remarked that this will complete the proof of the theorem. Recall that by definition  $v = \Lambda(1)$ , whence  $K(v) \subset E(1) = E$ , so that  $v \in M_{K_s}$ . As noted above, for any  $w \in M$  and any  $\sigma \in \text{Aut}(U/K)$ ,  $\sigma w = \Lambda(f(\sigma)\sigma(\Lambda^{-1}(w)))$ . Therefore, for every  $\sigma \in \text{Aut}(U/K)$ ,

$$v^{-1}\sigma v = v^{-1}\Lambda(f(\sigma)\sigma(\Lambda^{-1}(v))) = v^{-1}\Lambda(f(\sigma)) = \Lambda^{-1}(v)^{-1}f(\sigma) = f(\sigma),$$

whence  $v^{-1}\gamma v = f(\gamma)$  ( $\gamma \in \mathfrak{g}(K_s/K)$ ).

**Corollary** Let  $\mathcal{P}_K(G)$  denote the set of  $K$ -isomorphism classes of principal homogeneous  $K$ -spaces for the  $K$ -group  $G$ . There exists a bijection  $\mathcal{P}_K(G) \rightarrow H^1(K, G)$  that, for each principal homogeneous  $K$ -space  $M$  for  $G$  and any  $v \in M_{K_s}$ , sends the  $K$ -isomorphism class of  $M$  to the cohomology class of  $\Phi_{M, v}$ .

### 14 Holomorphicity at a specialization

Let  $M$  and  $N$  be homogeneous  $K$ -spaces for  $K$ -groups  $G$  and  $H$ , respectively.

If  $v \rightarrow v'$  is a specialization over  $K$  of elements of  $M$ , and we choose  $(s, t) \in \Gamma_{G \times H \circ K(v)}$  and  $(s', t') \in \Gamma_{G \times H \circ K(v')}$ , then  $(v, s, t) \rightarrow (v', s', t')$ , whence  $(vs, s, t) \rightarrow (v's', s', t')$ . Since evidently  $vs \leftrightarrow v's', s \leftrightarrow s', t \leftrightarrow t'$ , there exists a unique homomorphism

$$S: K[K(vs) \cup K(s) \cup K(t)] \longrightarrow K[K(v's') \cup K(s') \cup K(t')]$$

extending  $S_{v's',vs}, S_{s',s}, S_{t',t}$ . For any surjective ring homomorphism  $F: R \rightarrow R'$  with prime kernel, say  $\mathfrak{p}$ , we denote the local ring  $R_{\mathfrak{p}}$  by  $\mathfrak{o}_F$ , and denote the induced homomorphism of  $\mathfrak{o}_F$  into the field of quotients of  $R'$  by  $\bar{F}$ ; this  $\bar{F}$  is always surjective. In particular, we have the homomorphism

$$\bar{S} : \mathfrak{o}_S \rightarrow K(v', s', t').$$

The properties of  $S, \mathfrak{o}_S$ , and  $\bar{S}$  do not depend on the choice of  $(s, t)$  and  $(s', t')$  in the sense that if  $S_1$  is the analogous homomorphism obtained by choosing  $(s_1, t_1)$  and  $(s'_1, t'_1)$  instead of  $(s, t)$  and  $(s', t')$ , then the unique isomorphism

$$X : K[K(vs) \cup K(s) \cup K(t)] \approx K[K(vs_1) \cup K(s_1) \cup K(t_1)]$$

extending  $S_{vs_1,vs}, S_{s_1,s}, S_{t_1,t}$  and the unique isomorphism

$$X' : K[K(v's') \cup K(s') \cup K(t')] \approx K[K(v's'_1) \cup K(s'_1) \cup K(t'_1)]$$

extending  $S_{v's'_1,v's'}, S_{s'_1,s'}, S_{t'_1,t'}$  have the property that  $S_1 \circ X = X' \circ S$ , and  $X, X'$  induce isomorphisms  $Y : \mathfrak{o}_S \approx \mathfrak{o}_{S_1}, Y' : K(v', s', t') \approx K(v', s'_1, t'_1)$ , respectively, such that  $\bar{S}_1 \circ Y = Y' \circ \bar{S}$ . For this reason we permit ourselves to call  $S$  (respectively  $\bar{S}$ ) the homomorphism (respectively local homomorphism) of  $v \rightarrow v'$  relative to  $H$ .

Continuing, consider any element  $w \in N_{K(v)}$ . If  $w$  has the property that  $K(wt) \subset \mathfrak{o}_S$ , then  $\bar{S}$  maps  $K(wt)$  isomorphically onto a subfield of  $K(v', s', t')$ , and, by axiom AS 2(b) and the fact that  $N$  is a homogeneous space for  $H$ , there is a unique element  $w' \in N$  such that  $wt \leftrightarrow w't'$  and  $S_{w't',wt}$  coincides with  $\bar{S}$  on  $K(wt)$ . When  $w$  has this property, then we say that  $w$  is *holomorphic at  $v \rightarrow v'$* , and call  $w'$  the *value of  $w$  at  $v \rightarrow v'$* .

The isomorphism  $Y : \mathfrak{o}_S \approx \mathfrak{o}_{S_1}$  introduced above extends to an isomorphism  $\bar{Y} : K(v, s, t) \approx K(v, s_1, t_1)$  that extends  $id_{K(v)}, S_{s_1,s}, S_{t_1,t}$  and hence extends  $id_{K(w)}$  too. Evidently  $wt \leftrightarrow wt_1$  and  $Y$  extends  $S_{wt_1,wt}$ . It follows that the condition that  $w$  be holomorphic at  $v \rightarrow v'$  is independent of the choice of  $(s, t)$  and  $(s', t')$ , and that when this condition is satisfied, then  $w'$ , the value of  $w$  at  $v \rightarrow v'$ , is independent of this choice.

It does seem, however, that the condition and, when it is satisfied, the value of  $w$  at  $v \rightarrow v'$  are relative notions, depending on the containing homogeneous  $K$ -spaces  $M$  and  $N$ . The following lemma shows that in a certain precise sense they are not. We first observe that if  $G_0$  is a  $K$ -subgroup of  $G$  and  $M_0$  is a  $K$ -subset of  $M$  such that some element  $v_0 \in M_0$  has the property that  $v_0 G_0 = M_0$ , then every element of  $M_0$  has this property and  $M_0$  has a natural structure of homogeneous  $K$ -space for  $G_0$ .

**Lemma 5** Let  $G_0$  be a  $K$ -subgroup of  $G, M_0$  be a  $K$ -subset of  $M$ , and suppose that  $M_0$  is a homogeneous  $K$ -space for  $G_0$  as described above. Similarly, let

$H_0$  be a  $K$ -subgroup of  $H, N_0$  be a  $K$ -subset of  $N$ , and suppose that  $N_0$  is a homogeneous  $K$ -space for  $H_0$ . Let  $v, v' \in M_0$  and  $v \rightarrow v'$ , and let  $w \in (N_0)_{K(v)}$ . A necessary and sufficient condition that  $w$  be holomorphic at  $v \rightarrow v'$  relative to  $M$  and  $N$  is that  $w$  be holomorphic at  $v \rightarrow v'$  relative to  $M_0$  and  $N_0$ .

*Proof* Fix  $(s, s_0, t) \in \Gamma_{G_0 \times G_0 \times H_0/K(v)}$  and  $(s', s'_0, t) \in \Gamma_{G_0 \times G_0 \times H_0/K(v')}$ ; Then there exists a homomorphism

$$S^* : K[K(vs_0, s) \cup K(s_0, s) \cup K(t)] \rightarrow K[K(v's'_0, s') \cup K(s'_0, s') \cup K(t')]$$

extending  $S_{(v's'_0, s'), (vs_0, s)}, S_{(s'_0, s'), (s_0, s)}, S_{t', t}$ . This  $S^*$  provides, by restriction, two homomorphisms

$$S_0 : K[K(vs_0) \cup K(s_0) \cup K(t)] \rightarrow K[K(v's'_0) \cup K(s'_0) \cup K(t')],$$

$$S_1 : K[K(vs_0 s) \cup K(s_0 s) \cup K(t)] \rightarrow K[K(v's'_0 s') \cup K(s'_0 s') \cup K(t')].$$

Obviously  $\mathfrak{o}_{S_0} \subset \mathfrak{o}_{S^*}$  and  $\mathfrak{o}_{S_1} \subset \mathfrak{o}_{S^*}$ . We claim that every element  $\alpha \in K(wt)$  that is in  $\mathfrak{o}_{S^*}$  is also in  $\mathfrak{o}_{S_0}$  and  $\mathfrak{o}_{S_1}$ . Indeed, it is easy to see that the condition  $\alpha \in \mathfrak{o}_{S^*}$  implies that  $\alpha = \beta/\gamma$ , where  $\beta, \gamma \in K[K(s_0) \cup K(vs_0 s) \cup K(s_0 s) \cup K(t)]$  and  $S^*(\gamma) \neq 0$ . Fixing a basis  $(e_i)$  of  $K(s_0)$  over  $K$ , we can write  $\beta = \sum \beta_i e_i$ ,  $\gamma = \sum \gamma_i e_i$ , where  $\beta_i, \gamma_i \in K[K(vs_0 s) \cup K(s_0 s) \cup K(t)]$  for all  $i$  and  $S^*(\gamma_i) \neq 0$  for some  $i$ , so that  $\sum (\alpha\gamma_i - \beta_i)\gamma_i = 0$ . Since  $(e_i)$  evidently is linearly independent over  $K(v, s, t)$ , it follows when  $\alpha \in K(wt) \subset K(v, t)$  that  $\alpha\gamma_i - \beta_i = 0$  for all  $i$ , whence  $\alpha \in \mathfrak{o}_{S_1}$ . A similar argument, expressing  $\alpha$  as a quotient of two elements of  $K[K(s) \cup K(vs_0) \cup K(s_0) \cup K(t)]$  and using a basis of  $K(s)$  over  $K$ , shows that  $\alpha \in \mathfrak{o}_{S_0}$ . This establishes the claim. It follows that the three conditions

$$K(wt) \subset \mathfrak{o}_{S^*}, \quad K(wt) \subset \mathfrak{o}_{S_0}, \quad K(wt) \subset \mathfrak{o}_{S_1}$$

are equivalent. Since  $(s_0 s, t) \in \Gamma_{G_0 \times H_0/K(v)}$  and  $(s'_0 s', t') \in \Gamma_{G_0 \times H_0/K(v')}$ , this shows that  $w$  is holomorphic at  $v \rightarrow v'$  relative to  $M$  and  $N$  if and only if  $w$  is holomorphic at  $v \rightarrow v'$  relative to  $M_0$  and  $N_0$ .

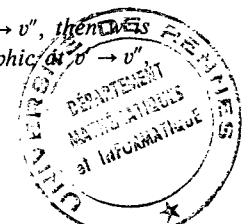
An entirely similar argument takes care of the case  $M$  and  $N_0$ . Finally, the two cases together yield the general case  $M_0$  and  $N_0$ .

**Lemma 6** Let  $M$  and  $N$  be homogeneous  $K$ -spaces for the  $K$ -groups  $G$  and  $H$ , respectively. Let  $v \in M$  and let  $V$  denote the locus of  $v$  over  $K$ . Let  $w \in N_{K(v)}$ .

(a) If  $v' \in V$  and  $w$  is holomorphic at  $v \rightarrow v'$ , and if  $w'$  denotes the value of  $w$  at  $v \rightarrow v'$ , then  $w' \in N_{K(v')}$  and  $w'$  is the unique element of  $N$  such that  $(v, w) \rightarrow (v', w')$ .

(b) If  $v' \in \Gamma_{V/K}$ , then  $w$  is holomorphic at  $v \rightarrow v'$ .

(c) If  $v', v'' \in V$  and  $v' \rightarrow v''$ , and if  $w$  is holomorphic at  $v \rightarrow v''$ , then  $w$  is holomorphic at  $v \rightarrow v'$ , the value  $w'$  of  $w$  at  $v \rightarrow v'$  is holomorphic at  $v' \rightarrow v''$  and the value of  $w$  at  $v \rightarrow v''$  equals the value of  $w'$  at  $v' \rightarrow v''$ .



(d) If  $\mathcal{O}'$  is a  $K$ -open subset of  $N$ , and  $\mathcal{O}$  denotes the set of elements  $v' \in V$  such that  $w$  is holomorphic at  $v \rightarrow v'$  and the value of  $w$  at  $v \rightarrow v'$  is in  $\mathcal{O}'$ , then  $\mathcal{O}$  is  $K$ -open in  $V$ .

*Proof* (a) Using our previous notation, we have the homomorphisms  $S$  and  $\bar{S}$ . Because  $K(w't') = \bar{S}(K(wt)) \subset \bar{S}(\mathfrak{o}_S) = K(v', s', t')$ , we infer that  $K(w') \subset K(v', s', t')$ . Because  $(s', t')$  can be replaced by any element  $(s'_1, t'_1) \in \Gamma_{G^0 \times H^0/K(v')}$ , we conclude that  $K(w') \subset K(v')$ , whence  $w' \in N_{K(v')}$ . Therefore  $(s', t') \in \Gamma_{G^0 \times H^0/K(v', w')}$  so that  $(v's', w't') = (v', w')(s', t') \in \Gamma_{M \times N/K}$ , whence  $(vs, wt) \leftrightarrow (v's', w't')$ . Since also  $(s, t) \leftrightarrow (s', t')$ , and since  $S_{(v's', w't'), (vs, wt)}$  and  $S_{(s', t'), (s, t)}$  are compatible (they have the common extension  $\bar{S}$ ), we infer that

$$(vs, wt)(s, t)^{-1} \rightarrow (v's', w't')(s', t')^{-1},$$

that is, that  $(v, w) \rightarrow (v', w')$ . If  $w_0'$  is any element of  $N$  such that  $(v, w) \rightarrow (v', w_0')$ , we can choose  $(s', t')$  above to be in  $\Gamma_{G^0 \times H^0/K(v', w_0')}$ . Then there exists a homomorphism

$$T: K[K(vs) \cup K(wt) \cup K(s) \cup K(t)] \rightarrow K[K(v's') \cup K(w_0't') \cup K(s') \cup K(t')]$$

that extends the four isomorphisms  $S_{v's', vs}, S_{w_0't', wt}, S_{s', s}, S_{t', t}$ , and this  $T$  evidently extends  $S$ . Since  $K(wt) \subset \mathfrak{o}_S$ ,  $T$  and  $\bar{S}$  coincide on  $K(wt)$  so that  $w_0't' = w't'$  and  $w_0' = w'$ . Therefore  $w'$  is unique.

(b) If  $v \leftrightarrow v'$ , then  $S$  is an isomorphism and  $\mathfrak{o}_S = K(v, s, t)$ , so that  $K(wt) \subset K(w, t) \subset \mathfrak{o}_S$ .

(c) Extending our familiar notation in a self-explanatory way, we have the consecutive surjective homomorphisms

$$K[K(vs) \cup K(s) \cup K(t)] \xrightarrow{S} K[K(v's') \cup K(s') \cup K(t')] \xrightarrow{S'} K[K(v''s'') \cup K(s'') \cup K(t'')].$$

These can be embedded in a commutative diagram

$$\begin{array}{ccccc} K[K(vs) \cup K(s) \cup K(t)] & \xrightarrow{S} & K[K(v's') \cup K(s') \cup K(t')] & \xrightarrow{S'} & K[K(v''s'') \cup K(s'') \cup K(t'')] \\ \downarrow \mathfrak{o}_{S \circ S} & \xrightarrow{S} & \downarrow \mathfrak{o}_S & \longrightarrow & \downarrow K(v'', s'', t'') \\ \mathfrak{o}_S & \xrightarrow{S} & K(v', s', t') & & \end{array}$$

Here all the vertical arrows are inclusions and all the horizontal arrows are surjective. If  $w$  is holomorphic at  $v \rightarrow v''$ , then  $K(wt) \subset \mathfrak{o}_{S \circ S} \subset \mathfrak{o}_S$ , so that

$w$  is holomorphic at  $v \rightarrow v'$ , and if we denote its value there by  $w'$ , then  $K(w't') = \bar{S}(K(wt)) \subset \mathfrak{o}_S$ , so that  $w'$  is holomorphic at  $v' \rightarrow v''$ . Denoting its value there by  $w''$  we see that  $(v, w) \rightarrow (v', w') \rightarrow (v'', w'')$ , so that  $w''$  is the value of  $w$  at  $v \rightarrow v''$ .

(d) If  $v' \in V, v'' \in \mathcal{O}, v' \rightarrow v''$ , then part (c) shows that  $v' \in \mathcal{O}$ . Consider any  $K$ -irreducible subset  $V'$  of  $V$  with  $V' \cap \mathcal{O} \neq \emptyset$ . We shall show that  $V' \cap \mathcal{O}$  has a nonempty subset that is  $K$ -open in  $V'$ . By Section 7, Proposition 4, this will imply that  $\mathcal{O}$  is  $K$ -open in  $V$  and will complete the proof of the lemma.

Fix an element  $v' \in \Gamma_{V'/K}$ . By what we have just seen,  $v' \in \mathcal{O}$ ; that is,  $w$  is holomorphic at  $v \rightarrow v'$  and its value  $w'$  there is in  $\mathcal{O}'$ , so that  $K(wt) \subset \mathfrak{o}_S$  (where  $S$  is the homomorphism of  $v \rightarrow v'$  relative to  $H$ ). Fix elements  $\zeta_1, \dots, \zeta_m \in K(wt)$  such that  $K(\zeta_1, \dots, \zeta_m) = K(wt)$  and elements  $\tau_1, \dots, \tau_n \in K(t)$  such that  $K(\tau_1, \dots, \tau_n) = K(t)$ . Since  $\bar{S}$  maps  $K(wt)$  and  $K(t)$  isomorphically onto  $K(w't')$  and  $K(t')$ ,  $K(\zeta'_1, \dots, \zeta'_m) = K(w't')$  and  $K(\tau'_1, \dots, \tau'_n) = K(t')$ , where, in general, we write  $\zeta' = \bar{S}(\zeta)$  for any element  $\zeta \in \mathfrak{o}_S$ . We may suppose that  $(\tau'_1, \dots, \tau'_d)$  is a transcendence basis of  $K(v's', s', t')$  over  $K(v's', s', w't')$ . Here

$$d = \dim_{K(v's', s', w't')} t' = \dim_{K(v's', s')} t' - \dim_{K(v's', s')} w't' = \dim H - \dim N.$$

Then, for each index  $j$  with  $d < j \leq n$ ,  $\tau'_j$  is algebraic over  $K(v's', s')$  ( $\zeta'_1, \dots, \zeta'_m, \tau'_1, \dots, \tau'_d$ ), say of degree  $e_j$ , so that there exist polynomials

$$P_{j\varepsilon} \in K[K(v's') \cup K(s')] [Z_1, \dots, Z_m, T_1, \dots, T_d] \quad (0 \leq \varepsilon \leq e_j)$$

with  $P_{je}(\zeta'_1, \dots, \zeta'_m, \tau'_1, \dots, \tau'_d) \neq 0$  such that

$$\sum_{0 \leq \varepsilon \leq e_j} P_{j\varepsilon}(\zeta'_1, \dots, \zeta'_m, \tau'_1, \dots, \tau'_d) \tau_j^\varepsilon = 0.$$

Since  $K(wt) \subset \mathfrak{o}_S$  there exist elements  $\xi_0, \xi_1, \dots, \xi_m \in K[K(vs) \cup K(s) \cup K(t)]$  with  $\xi_0' \neq 0$  such that  $\zeta_i = \xi_i/\xi_0$  ( $1 \leq i \leq m$ ). Setting  $h_j = \deg_{(Z_1, \dots, Z_m)} P_{je}$  and  $\pi_j = \xi_0^{h_j} P_{je}(\zeta_1, \dots, \zeta_m, \tau_1, \dots, \tau_d)$  ( $d < j \leq n$ ), and then setting  $\pi = \xi_0 \pi_{d+1} \cdots \pi_n$ , we see that  $\pi \in K[K(vs) \cup K(s) \cup K(t)]$  and  $\pi' \neq 0$ .

Consider any element  $v'' \in V'$  and let  $S'$  denote the homomorphism of  $v' \rightarrow v''$  relative to  $H$ . Then  $S$  and  $S'$  can be embedded in the commutative diagram displayed in the proof of part (c). Evidently  $S' \circ S$  is the homomorphism of  $v \rightarrow v''$  relative to  $H$ . For any element  $\xi \in \mathfrak{o}_{S \circ S}$  we set  $\xi'' = (S' \circ S)(\xi) = S'(\xi')$ . If  $v''$  has the property that  $\pi'' \neq 0$ , then  $\zeta_i = \xi_i/\xi_0 \in \mathfrak{o}_{S \circ S}$  ( $1 \leq i \leq m$ ), and  $\tau'_j$  is algebraic over  $K(v''s'', s'')$  ( $\zeta''_1, \dots, \zeta''_m, \tau''_1, \dots, \tau''_d$ ) ( $d < j \leq n$ ) so that  $K(v''s'', s'', t'')$  is an algebraic extension of

$$K(v''s'', s'')(\zeta''_1, \dots, \zeta''_m, \tau''_1, \dots, \tau''_d).$$

It follows that then

$$\begin{aligned} \text{tr deg } K(\zeta_1'', \dots, \zeta_m'')/K &\geq \text{tr deg } K(v''s'', s'')(\zeta_1'', \dots, \zeta_m'')/K(v''s'', s'') \\ &= \text{tr deg } K(v''s'', s'', t'')/K(v''s'', s'') \\ &\quad - \text{tr deg } K(v''s'', s'', t'')/K(v''s'', s'')(\zeta_1'', \dots, \zeta_m'') \\ &\geq \dim H - d = \dim N \\ &= \text{tr deg } K(wt)/K = \text{tr deg } K(\zeta_1, \dots, \zeta_m)/K, \end{aligned}$$

so that  $\widetilde{S' \circ S}$  maps  $K[\zeta_1, \dots, \zeta_m]$  isomorphically and  $K(wt) = K(\zeta_1, \dots, \zeta_m) \subset \mathfrak{o}_{S' \circ S}$  and  $w$  is holomorphic at  $v \rightarrow v''$ . Letting  $w''$  denote the value of  $w$  at  $v \rightarrow v''$  (and hence also the value of  $w'$  at  $v' \rightarrow v''$ ), we see that the middle line of the commutative diagram mentioned above restricts to a sequence of homomorphisms

$$K[K(wt) \cup K(t)] \rightarrow K[K(w't') \cup K(t')] \rightarrow K[K(w''t'') \cup K(t'')].$$

By Section 6, Proposition 2(a), there exists a nonempty set  $\mathfrak{b} \subset K[K(wt) \cup K(t)]$  such that  $w'' \notin \mathfrak{O}'$  if and only if  $\beta'' = 0$  for every  $\beta \in \mathfrak{b}$ . Since  $w' \in \mathfrak{O}'$ , we must have  $\beta' \neq 0$  for some  $\beta \in \mathfrak{b}$ . This shows that there exists an element  $\beta \in \mathfrak{o}_{S' \circ S}$  with  $\beta' \neq 0$  such that if  $v''$  has the property that  $\beta'' \neq 0$  (in addition to the property that  $\pi'' \neq 0$ ), then  $v'' \in \mathfrak{O}$ .

Write  $\beta = \eta_1/\eta_0$  with  $\eta_0, \eta_1 \in K[K(vs) \cup K(s) \cup K(t)]$  and  $\eta_0' \neq 0$ . Then  $\eta_1' \neq 0$ , and we see that if the element  $v'' \in V''$  has the property that  $\pi''\eta_0''\eta_1'' \neq 0$ , then  $v'' \in \mathfrak{O}$ . Now, we can write  $\pi\eta_0\eta_1 = \sum \alpha_k \gamma_k$  with  $\alpha_k \in K[K(vs) \cup K(s)]$  and  $\gamma_k \in K(t)$  for every  $k$  and the elements  $\gamma_k$  linearly independent over  $K$ . Since  $K(v''s'', s'')$  and  $K(t'')$  are linearly disjoint over  $K$ , we infer that  $\pi''\eta_0''\eta_1'' = 0$  if and only if  $\alpha_k'' = 0$  for every  $k$ , that is (in the language of Section 6), each  $\alpha_k$  vanishes at  $v''$ . Referring to Section 6, Proposition 2(b), we see that this happens if and only if  $v''$  is an element of a certain  $K$ -closed subset  $F$  of  $V$ . The set  $V' \cap (V - F)$  is  $K$ -open in  $V'$  and is nonempty because it contains  $v'$ . As remarked above, this completes the proof of the lemma.

The following lemma shows how holomorphicity at a specialization depends on the ground field.

**Lemma 7** *Let  $M$  and  $N$  be homogeneous  $K$ -spaces for the  $K$ -groups  $G$  and  $H$ , respectively, and let  $L$  be an extension of  $K$ . Let  $v \in M$ ,  $v' \in M$ ,  $w \in N_{K(v)}$ , and suppose that  $v \xrightarrow{L} v'$ .*

(a) *If  $w$  is holomorphic at  $v \xrightarrow{K} v'$ , then  $w$  is holomorphic at  $v \xrightarrow{L} v$ , and  $w$  has the same value at  $v \xrightarrow{K} v'$  as at  $v \xrightarrow{L} v'$ .*

(b) *If  $w$  is holomorphic at  $v \xrightarrow{L} v'$ , and  $K(v)$  and  $L$  are linearly disjoint over  $K$ , then  $w$  is holomorphic at  $v \xrightarrow{K} v'$ .*

**REMARK** The linear disjointness condition in part (b) can not be weakened to algebraic disjointness. See Exercise 1 below.

*Proof* Fix  $(s, t) \in \Gamma_{G \circ \times H \circ / L(v)}$  and  $(s', t') \in \Gamma_{G \circ \times H \circ / L(v')}$ . The homomorphism

$$S^L : L[L(vs) \cup L(s) \cup L(t)] \rightarrow L[L(v's') \cup L(s') \cup L(t')]$$

of  $v \xrightarrow{L} v'$  relative to  $H$  is an extension of the homomorphism

$$S^K : K[K(vs) \cup K(s) \cup K(t)] \rightarrow K[K(v's') \cup K(s') \cup K(t')]$$

of  $v \xrightarrow{K} v'$  relative to  $H$ .

If  $w$  is holomorphic at  $v \xrightarrow{K} v'$ , then  $K(wt) \subset \mathfrak{o}_{S^K} \subset \mathfrak{o}_{S^L}$ , whence  $L[K(wt)] \subset \mathfrak{o}_{S^L}$ . Therefore  $S^L$  restricts to a homomorphism  $L[K(wt)] \subset L[K(w't')]$  over  $L$ , and since

$$\text{tr deg } L(K(wt))/L = \dim_L wt = \dim N = \dim_L w't' = \text{tr deg } L(K(w't'))/L$$

(because  $wt, w't' \in \Gamma_{N/L}$ ), this homomorphism is an isomorphism, so that  $L(wt) \subset \mathfrak{o}_{S^L}$  and  $w$  is holomorphic at  $v \xrightarrow{L} v'$ . Furthermore, when  $w'$  denotes the value of  $w$  at  $v \xrightarrow{L} v'$ , then  $(v, w) \xrightarrow{L} (v', w')$ , so that  $(v, w) \xrightarrow{K} (v', w')$ , and hence (by Lemma 6(a))  $w'$  is the value of  $w$  at  $v \xrightarrow{K} v'$ .

Conversely, if  $w$  is holomorphic at  $v \xrightarrow{L} v'$ , then  $K(wt) \subset L(wt) \subset \mathfrak{o}_{S^L}$ , so that every element  $\zeta \in K(wt)$  can be expressed in the form  $\zeta = \xi/\eta$  with  $\xi, \eta \in L[L(vs) \cup L(s) \cup L(t)]$  and  $S^L(\eta) \neq 0$ . Because  $L(vs)$ , respectively  $L(s)$ , respectively  $L(t)$ , is the field of quotients of  $L[K(vs)]$ , respectively  $L[K(s)]$ , respectively  $L[K(t)]$ , we may even suppose that

$$\xi, \eta \in L[K(vs) \cup K(s) \cup K(t)].$$

Then we can write  $\zeta = \sum \lambda_k \xi_k$  and  $\eta = \sum \lambda_k \eta_k$ , where

$$\xi_k, \eta_k \in K[K(vs) \cup K(s) \cup K(t)]$$

and  $\lambda_k \in L$  for every  $k$ , the elements  $\lambda_k$  are linearly independent over  $K$ , and  $S^K(\eta_k) \neq 0$  for some  $k$ . Hence  $\sum \lambda_k (\eta_k \zeta - \xi_k) = \eta \zeta - \xi = 0$ . When  $K(v)$  and  $L$  are linearly disjoint over  $K$ , then so too are  $K(vs, s, t)$  and  $L$ , and therefore  $\eta_k \zeta - \xi_k = 0$  for every  $k$ , whence  $\zeta \in \mathfrak{o}_{S^K}$ . Thus,  $K(wt) \subset \mathfrak{o}_{S^K}$  and  $w$  is holomorphic at  $v \xrightarrow{K} v'$ .

We conclude this section with the easy observation that, under the hypothesis of Lemma 7, if  $w$  is holomorphic at  $v \xrightarrow{L} v'$  and its value there is denoted



by  $w'$ , and if  $\sigma$  is any automorphism of  $U$  over  $K$ , then  $\sigma w$  is holomorphic at  $\sigma v \xrightarrow{\sigma L} \sigma v'$  and its value there is  $\sigma w'$ .

EXERCISE

- Let  $K = \mathbb{Q}$  and  $L = \mathbb{Q}(2^{1/3}, e^{2\pi i/3})$ , where  $i^2 = -1$ . Let  $V$  be the  $K$ -irreducible  $K$ -subset of the affine plane  $\mathbb{G}_a^2$  defined by the equation  $X_1^3 - 2X_2^3 = 0$ . Let  $(v_1, v_2) \in \Gamma_{V/K} = \Gamma_{V/L}$ , and set  $w = v_1^2/v_2 \in \mathbb{G}_a$ . (Regard  $\mathbb{G}_a^2$  and  $\mathbb{G}_a$  as the regular  $K$ -spaces for the  $K$ -groups  $\mathbb{G}_a^2$  and  $\mathbb{G}_a$ , respectively.) Show that  $w$  is holomorphic at  $(v_1, v_2) \xrightarrow{L} (0, 0)$  but not at  $(v_1, v_2) \xrightarrow{K} (0, 0)$ .

15  $K$ -Mappings

Let  $A$  and  $B$  be  $K$ -sets. Consider pre- $K$ -mappings of  $A$  into  $B$  (see Section 2). Call two such pre- $K$ -mappings  $K$ -equivalent if they coincide on  $\Gamma_{A/K}$ . This defines an equivalence relation on the set of all pre- $K$ -mappings of  $A$  into  $B$ .

Call a pre- $K$ -mapping of  $A$  into  $B$   $K$ -minimal if its domain of definition is  $\Gamma_{A/K}$ . Since the restriction to  $\Gamma_{A/K}$  of any pre- $K$ -mapping of  $A$  into  $B$  is itself a pre- $K$ -mapping of  $A$  into  $B$ , each  $K$ -equivalence class has a unique  $K$ -minimal representative.

Let  $L$  be an extension of  $K$ . It is easy to verify that a  $K$ -minimal pre- $K$ -mapping  $f_0$  of  $A$  into  $B$  is also a pre- $L$ -mapping of  $A$  into  $B$ . Associating to each  $K$ -equivalence class of pre- $K$ -mappings of  $A$  into  $B$  the  $L$ -equivalence class of its  $K$ -minimal representative, we obtain a canonical injection of the set of  $K$ -equivalence classes into the set of  $L$ -equivalence classes.

The  $K_s$ -components of  $A$  are irreducible, that is, the components of  $A$  are its  $K_s$ -components. For each component  $V$  of  $A$  choose an element  $v_V \in \Gamma_{V/K_s}$ . Given a pre- $K$ -mapping  $f_0$  of  $A$  into  $B$ , it is easy to see that the following two conditions on an element  $v_0 \in A$  are equivalent.

- For every  $v \in \Gamma_{A/K}$  with  $v \xrightarrow{K_s} v_0$ ,  $f_0(v)$  is holomorphic at  $v \xrightarrow{K_s} v_0$  and its value there is independent of  $v$ .
- For every component  $V$  of  $A$  that contains  $v_0$ ,  $f_0(v_V)$  is holomorphic at  $v_V \xrightarrow{K_s} v_0$  and its value there is independent of  $V$ .

The set of all elements  $v' \in A$  such that every element  $v_0 \in A$  with  $v_0 \xrightarrow{K_s} v'$  satisfies these equivalent conditions will be called the *habitat* of  $f_0$ . It is obvious that  $K$ -equivalent pre- $K$ -mappings have the same habitat, so that we may speak of the habitat of a  $K$ -equivalence class. It is easy to see, with the help of Section 14, Lemma 7, that the habitat of a  $K$ -equivalence class

of pre- $K$ -mappings is also the habitat of the associated  $L$ -equivalence class of pre- $L$ -mappings. When  $A$  is irreducible and  $v \in \Gamma_{A/K}$ , the habitat of  $f_0$  is the set of all elements  $v' \in A$  such that  $f_0(v)$  is holomorphic at  $v \xrightarrow{K} v'$ .

If  $A_0$  is the habitat of a pre- $K$ -mapping  $f_0$  of  $A$  into  $B$ , then  $\Gamma_{A/K} \subset A_0$ . For any automorphism  $\sigma \in \text{Aut}(U/K)$ ,  $\sigma A = A$ , as  $V$  runs over the set of components of  $A$  so does  $\sigma V$ ,  $\sigma(\Gamma_{A/K}) = \Gamma_{A/K}$ , and evidently  $f_0(\sigma v) = \sigma(f_0(v))$  for every  $v \in \Gamma_{A/K}$ . It follows from the definition, and the observation at the end of Section 14, that  $\sigma A_0 = A_0$ .

**Definition** Let  $A$  and  $B$  be  $K$ -sets. A  $K$ -mapping of  $A$  into  $B$  is a pre- $K$ -mapping  $f$  of  $A$  into  $B$  with the following two properties:

- The domain of definition of  $f$  is its habitat.
- If  $v'$  is in the domain of definition of  $f$ , and  $v \in \Gamma_{A/K}$  and  $v \xrightarrow{K_s} v'$ , then  $f(v')$  is the value of  $f(v)$  at  $v \xrightarrow{K_s} v'$ .

**REMARK** This notion is not quite analogous to the notion of rational mapping defined over  $K$  of one algebraic set defined over  $K$  into another, as used in algebraic geometry. In general, such a rational mapping is a pre- $K$ -mapping and its domain of holomorphicity is a subset of its habitat. However, a point in the habitat can fail to be in the domain of holomorphicity only if the point is in at least two components of the algebraic set  $A$  (see Section 16, Exercise 1). A method of introducing an analog of the latter notion into the present theory is treated in Section 16, Exercise 2.

It is clear that  $K$ -mappings of  $A$  into  $B$  that are  $K$ -equivalent are identical. On the other hand, if  $f_0$  is any pre- $K$ -mapping of  $A$  into  $B$  and  $A_0$  denotes its habitat, we can define a mapping  $f: A_0 \rightarrow B$  by the formula

$$f(v') = \text{the value of } f_0(v) \text{ at } v \xrightarrow{K_s} v' \text{ when } v \in \Gamma_{A/K} \text{ and } v \xrightarrow{K_s} v'.$$

We shall show that  $f$  is a  $K$ -mapping of  $A$  into  $B$  that is  $K$ -equivalent to  $f_0$ . It evidently suffices to show that  $f$  is a pre- $K$ -mapping that coincides with  $f_0$  on  $\Gamma_{A/K}$ .

Since  $\Gamma_{A/K} \subset A_0$  and, for any  $v \in \Gamma_{A/K}$ , the value of  $f_0(v)$  at  $v \xrightarrow{K_s} v$  is obviously  $f_0(v)$ ,  $f$  coincides with  $f_0$  on  $\Gamma_{A/K}$ .

If  $v' \in A_0$ , then by Section 14, Lemma 6(a),  $K(f(v')) \subset K_s(v')$ . However, for any  $\sigma \in \text{Aut}(U/K)$  and for  $v \in \Gamma_{A/K}$  with  $v \xrightarrow{K_s} v'$ , we have  $\sigma v' \in A_0$  and  $\sigma v \in \Gamma_{A/K}$  and  $\sigma v \xrightarrow{K_s} \sigma v'$ , so that  $f(\sigma v')$  is the value of  $f_0(\sigma v)$  at  $\sigma v \xrightarrow{K_s} \sigma v'$ . Since

$$(\sigma v, f_0(\sigma v)) = (\sigma v, \sigma(f_0(v))) = \sigma(v, f_0(v)) \xrightarrow{K_s} \sigma(v', f(v')) = (\sigma v', \sigma(f(v'))),$$

we infer from Section 14, Lemma 6(a), that  $f(\sigma v') = \sigma(f(v'))$ . In particular, if  $\sigma \in \text{Aut}(U/K(v'))$ , then  $\sigma(f(v')) = f(v')$ . Since  $K(v') \subset K(v', f(v')) \subset K_s(v')$  and hence  $K(v', f(v'))$  is separable over  $K(v')$ , it follows that  $K(f(v')) \subset K(v')$ .

If  $v_0 \in A, v' \in A_0, v_0 \xrightarrow{K} v'$ , then the locus of  $v_0$  over  $K$  contains  $v'$ . Some  $K_s$ -component of this locus contains  $v'$ , and therefore a  $K_s$ -generic element  $v_1$  of this  $K_s$ -component has the property that  $v_1 \xrightarrow{K_s} v'$  and  $v_0 = \sigma v_1$  for some  $\sigma \in \text{Aut}(U/K)$ , whence  $v_0 \xrightarrow{K_s} \sigma v'$ . Evidently  $v_1 \in A_0$ , so that  $v_0 \in \sigma A_0 = A_0$ . Fixing an element  $v \in \Gamma_{A/K}$  with  $v \xrightarrow{K_s} v_0$ , we therefore see from Section 14, Lemma 6(c) and (a), that

$$(v_0, f(v_0)) \xrightarrow{K_s} (\sigma v', f(\sigma v')) = (\sigma v', \sigma(f(v'))),$$

whence

$$(v_0, f(v_0)) \xrightarrow{K} (v', f(v')) \quad \text{and} \quad f(v_0) \xrightarrow{K} f(v').$$

If  $v_0, v' \in A_0$  and  $v_0 \xleftrightarrow{K} v'$ , then, by what we have just seen,  $(v_0, f(v_0)) \xleftrightarrow{K} (v', f(v'))$  so that  $S_{v', v_0}$  and  $S_{f(v'), f(v_0)}$  are compatible. Since  $K(v_0) \supset K(f(v_0))$  by the above,  $S_{v', v_0}$  is an extension of  $S_{f(v'), f(v_0)}$ . This completes the proof that  $f$  is a  $K$ -mapping of  $A$  into  $B$   $K$ -equivalent to  $f_0$ .

It follows from what we have shown that every  $K$ -equivalence class of pre- $K$ -mappings of  $A$  into  $B$  has a unique representative that is a  $K$ -mapping of  $A$  into  $B$ .

Since the habitat of a  $K$  equivalence class of pre  $K$ -mappings is the habitat of the associated  $L$ -equivalence class of pre- $L$ -mappings, we see with the help of Section 14, Lemma 7(a), that every  $K$ -mapping of  $A$  into  $B$  is an  $L$ -mapping of  $A$  into  $B$ .

If a  $K$ -mapping  $f$  of  $A$  into  $B$  is defined at every element of a subset  $\Sigma$  of  $A$ , we say that  $f$  is defined on  $\Sigma$ . We denote the set of all  $K$ -mappings of  $A$  into  $B$  by  $\mathfrak{M}_K(A, B)$ , and denote the set of all  $K$ -mappings of  $A$  into  $B$  that are defined at  $v$  (respectively defined on  $\Sigma$ ) by  $\mathfrak{M}_{K,v}(A, B)$  (respectively  $\mathfrak{M}_{K,\Sigma}(A, B)$ ).

**Proposition 15** Let  $A$  and  $B$  be  $K$ -sets, let  $f \in \mathfrak{M}_K(A, B)$ , let  $A_0$  denote the domain of definition of  $f$ , and let  $C$  denote the smallest closed subset of  $B$  that contains  $f(A_0)$

- (a)  $A_0$  is  $K$ -open and dense in  $A$ .
- (b)  $f$  is continuous and  $K$ -continuous.
- (c)  $C$  is a  $K$ -subset of  $B$ .
- (d)  $f(A_0)$  contains a  $K$ -open dense subset of  $C$ .

*Proof* (a) For each component  $V$  of  $A$ , fix an element  $v_V \in \Gamma_{V/K_s}$ . Let  $F_V$  denote the set of elements  $v \in V$  such that  $f(v_V)$  is not holomorphic at  $v_V \xrightarrow{K_s} v$ . By Section 14, Lemma 6(d),  $F_V$  is  $K_s$ -closed for each  $V$ , and therefore the set  $F = \bigcup_V F_V$  is too. Evidently  $F \cap A_0 = \emptyset$ .

For each pair  $(V, V')$  of distinct components of  $A$  and each component  $X$  of  $V \cap V'$  with  $X \not\subset F$ , fix an element  $v_X \in \Gamma_{X/K_s}$ . Then  $v_X \notin F$ , so that  $f(v_V)$  is holomorphic at  $v_V \xrightarrow{K_s} v_X$  and  $f(v_{V'})$  is holomorphic at  $v_{V'} \xrightarrow{K_s} v_X$ . Let  $E_{V,V'}$  denote the union of all those components  $X$  of  $V \cap V'$  with  $X \not\subset F$  such that the value of  $f(v_V)$  at  $v_V \xrightarrow{K_s} v_X$  does not equal the value of  $f(v_{V'})$  at  $v_{V'} \xrightarrow{K_s} v_X$ . Set  $E = \bigcup_{(V,V')} E_{V,V'}$ . Then  $E$  is  $K_s$ -closed and  $E \cap A_0 = \emptyset$ . Thus,  $A_0 \subset A - (F \cup E)$ .

Consider any  $v \in A - (F \cup E)$  and any  $v_0 \in A$  with  $v_0 \xrightarrow{K_s} v$ . Obviously  $v_0 \in A - (F \cup E)$ . If  $v_0 \in V$  for a particular component  $V$  of  $A$ , then, because  $v_0 \notin F$ ,  $f(v_V)$  is holomorphic at  $v_V \rightarrow v_0$  and we may denote its value there by  $w_{0,V}$ . If also  $v_0 \in V'$ , where  $V'$  is another component of  $A$ , then  $v_0 \in X$  for some component  $X$  of  $V \cap V'$ , and

$$v_V \xrightarrow{K_s} v_X \xrightarrow{K_s} v_0, \quad v_{V'} \xrightarrow{K_s} v_X \xrightarrow{K_s} v_0.$$

Because  $v_0 \notin F$ , we have  $X \not\subset F$  and because  $v_0 \notin E$ , the value of  $f(v_V)$  at  $v_V \xrightarrow{K_s} v_X$  equals the value of  $f(v_{V'})$  at  $v_{V'} \xrightarrow{K_s} v_X$ . It follows by Section 14, Lemma 6(c), that  $w_{0,V} = w_{0,V'}$ , that is, that  $w_{0,V}$  is independent of  $V$ , whence  $v \in A_0$ .

This shows that  $A_0 = A - (F \cup E)$ , so that  $A_0$  is  $K_s$ -open and dense in  $A$ . Since  $\sigma A_0 = A_0$  ( $\sigma \in \text{Aut}(U/K)$ ),  $A_0$  is  $K$ -open in  $A$ .

(b) Let  $\mathcal{O}'$  be any  $K$ -open subset of  $B$ . For any component  $V$  of  $A$ , let  $\mathcal{O}_V$  denote the set of all elements  $v \in V$  such that  $f(v_V)$  is holomorphic at  $v_V \xrightarrow{K_s} v$  and its value there is in  $\mathcal{O}'$ . Then  $V \cap f^{-1}(\mathcal{O}') = \mathcal{O}_V \cap A_0$ , so that by Section 14, Lemma 6(d),  $V \cap f^{-1}(\mathcal{O}')$  is  $K_s$ -open in  $V \cap A_0$ . However, evidently  $f^{-1}(\mathcal{O}') = A_0 - \bigcup_V (V \cap A_0 - V \cap f^{-1}(\mathcal{O}'))$ , and therefore  $f^{-1}(\mathcal{O}')$  is  $K_s$ -open in  $A_0$  (and hence also in  $A$ ). Since  $\sigma A_0 = A_0$  and  $\sigma \mathcal{O}' = \mathcal{O}'$  and  $\sigma(f(v)) = f(\sigma v)$  ( $v \in A_0$ ) for every  $\sigma \in \text{Aut}(U/K)$ , we infer that  $\sigma(f^{-1}(\mathcal{O}')) = f^{-1}(\mathcal{O}')$  for every such  $\sigma$ , so that  $f^{-1}(\mathcal{O}')$  is  $K$ -open in  $A_0$ . This shows that  $f$  is  $K$ -continuous. Since  $f \in M_L(A, B)$  for every extension  $L$  of  $K$ ,  $f$  is  $L$ -continuous for every  $L$ . Hence  $f$  is continuous.

(c) If  $\sigma \in \text{Aut}(U/K)$ , then  $\sigma A_0 = A_0$ , so that  $\sigma(f(A)) = f(A)$ , whence  $\sigma C = C$ . Therefore  $C$  is  $K$ -closed. Letting  $V_1, \dots, V_m$  be the  $K$ -components of  $A$ , and then fixing  $v_i \in \Gamma_{V_i/K}$  and setting  $W_i$  equal to the locus of  $f(v_i)$  over  $K$  ( $1 \leq i \leq m$ ), we see that  $W_1 \cup \dots \cup W_m$  is a  $K$ -subset of  $B$ . Since  $C$  is  $K$ -closed and contains each  $f(v_i)$ ,  $C$  contains each  $W_i$ . On the other hand, if  $v \in A_0 \cap V_i$ , then  $v_i \rightarrow v$  and  $f(v_i) \rightarrow f(v)$ , whence  $f(v) \in W_i$ . Hence  $f(A_0) \subset$

$W_1 \cup \dots \cup W_m$ , so that  $C \subset W_1 \cup \dots \cup W_m$ . Thus,  $C = W_1 \cup \dots \cup W_m$  and  $C$  is a  $K$ -subset of  $B$ .

(d) Continuing the same notation, and fixing  $t \in \Gamma_{H \circ K(f(v_i))}$ ,  $s \in \Gamma_{G \circ K(v_i, t)}$  (where  $G$ , respectively  $H$ , is the  $K$ -group for which there is a homogeneous  $K$ -space containing  $A$ , respectively  $B$ ), we know by Section 7, Proposition 3, that there exists a nonzero element  $\alpha \in K[K(f(v_i)t) \cup K(t)]$  such that, for every homomorphism  $h : K[K(f(v_i)t) \cup K(t)] \rightarrow U$  over  $K$  with  $h(\alpha) \neq 0$ , there exists an element  $v' \in V_i \cap A_0$  such that when  $s' \in \Gamma_{G \circ h(K(f(v_i)t)h(K(t))K(v'))}$ , then  $h, S_{v's', vs}, S_{s', s}$  are compatible. For any  $w' \in W_i$  and  $t' \in \Gamma_{W_i/K(w')}$ , we have the homomorphism  $h_w : K[K(f(v_i)t) \cup K(t)] \rightarrow K[K(w't') \cup K(t')]$  extending  $S_{w't', f(v_i)t}, S_{t', t}$ . By what we have just said, if  $h_w(\alpha) \neq 0$ , then there is an element  $v' \in V_i \cap A_0$  such that  $w' = f(v') \in f(V_i \cap A_0)$ . By Section 6, Proposition 2(b), the set of elements  $w' \in W_i$  with  $h_w(\alpha) \neq 0$  is  $K$ -open in  $W_i$ , and as it obviously contains  $w_i$  it is dense in  $W_i$ . Thus, for each  $i$ ,  $f(A_0) \cap W_i$  contains a  $K$ -open dense subset of  $W_i$ , so that  $f(A_0)$  contains a  $K$ -open dense subset of  $C$ . This completes the proof of the proposition.

We call the set  $C$  in Proposition 15 the *closed image of  $f$* .

Again, let  $V_1, \dots, V_m$  be the  $K$ -components of  $A$ , and fix elements  $v_i \in \Gamma_{V_i/K}$  ( $1 \leq i \leq m$ ). If  $f \in \mathfrak{M}_K(A, B)$ , then  $f$  is defined at  $v_i$  ( $1 \leq i \leq m$ ), and  $(f(v_1), \dots, f(v_m)) \in B_{K(v_1)} \times \dots \times B_{K(v_m)}$ . Conversely, if  $(w_1, \dots, w_m)$  is any element of  $B_{K(v_1)} \times \dots \times B_{K(v_m)}$ , then there exists a unique minimal pre- $K$ -mapping  $f_0$  of  $A$  into  $B$  such that  $f_0(v_i) = w_i$  ( $1 \leq i \leq m$ ), and hence there exists a unique  $K$ -mapping  $f$  of  $A$  into  $B$  such that  $f(v_i) = w_i$  ( $1 \leq i \leq m$ ). It follows that the formula  $f \mapsto (f(v_1), \dots, f(v_m))$  defines a bijection  $\mathfrak{M}_K(A, B) \rightarrow B_{K(v_1)} \times \dots \times B_{K(v_m)}$ ; it is determined by the choice of  $(v_1, \dots, v_m)$ . These remarks applied to  $V_i$  instead of  $A$  show that  $v_i$  determines a bijection  $\mathfrak{M}_K(V_i, B) \rightarrow B_{K(v_i)}$ . Therefore there is unique bijection

$$\mathfrak{M}_K(A, B) \rightarrow \mathfrak{M}_K(V_1, B) \times \dots \times \mathfrak{M}_K(V_m, B)$$

with the property that if  $f \mapsto (f_1, \dots, f_m)$ , then  $f(v_i) = f_i(v_i)$  (and hence also  $f(v) = f_i(v)$  for every  $v \in \Gamma_{V_i/K}$ ) for each index  $i$ . This bijection is canonical, not depending on the choice of  $(v_1, \dots, v_m)$ .

Of course,  $\mathfrak{M}_K(A, B)$  may be empty, since  $B_{K(v_i)}$  may be empty for some  $i$ . However, when  $B$  is a  $K$ -group  $H$ , this difficulty does not arise because  $H_{K(v_i)}$  always contains the unity element 1. Moreover, each  $H_{K(v_i)}$  has a natural group structure ( $H_{K(v_i)}$  is a subgroup of  $H$ ), and therefore  $H_{K(v_1)} \times \dots \times H_{K(v_m)}$  does, too. By means of the bijection  $\mathfrak{M}_K(A, H) \rightarrow H_{K(v_1)} \times \dots \times H_{K(v_m)}$  this group structure can be transported to  $\mathfrak{M}_K(A, H)$ . The group structure obtained on  $\mathfrak{M}_K(A, H)$  in this way is canonical, being independent of the choice of  $(v_1, \dots, v_m)$ . The canonical bijection  $\mathfrak{M}_K(A, H) \rightarrow \mathfrak{M}_K(V_1, H) \times \dots \times \mathfrak{M}_K(V_m, H)$  is a group isomorphism.

**Proposition 16** Let  $A, B, C$  be  $K$ -sets, let  $f \in \mathfrak{M}_K(A, B)$ ,  $g \in \mathfrak{M}_K(B, C)$ , and suppose that  $g$  is defined on  $f(\Gamma_{A/K})$ . Then there exists a unique  $h \in \mathfrak{M}_K(A, C)$  such that  $h(v) = g(f(v))$  for every  $v \in \Gamma_{A/K}$ . If  $v'$  is any element of  $A$  such that  $f$  is defined at  $v'$  and  $g$  is defined at  $f(v')$ , then  $h$  is defined at  $v'$  and  $h(v') = g(f(v'))$ .

**REMARK** We call the  $K$ -mapping  $h$  the *generic composite* of  $f$  and  $g$ , and denote it by  $g \circ f$ . It is in general not the composite. For example, there can very well exist an element of  $A$  at which  $h$  is defined and  $f$  is not. We sometimes express the condition that  $g$  be defined on  $f(\Gamma_{A/K})$  by saying that  $g \circ f$  exists. For example, for every  $f \in \mathfrak{M}_K(A, B)$ ,  $f \circ id_A$  and  $id_B \circ f$  exist and equal  $f$ . The proposition implies that if  $A_1, A_2, A_3, A_4$  are  $K$ -sets and  $f_i \in \mathfrak{M}_K(A_i, A_{i+1})$  ( $1 \leq i \leq 3$ ) and  $f_2 \circ f_1, f_3 \circ f_2, f_3 \circ (f_2 \circ f_1), (f_3 \circ f_2) \circ f_1$  all exist, then  $f_3 \circ (f_2 \circ f_1) = (f_3 \circ f_2) \circ f_1$ .

*Proof* The formula  $v \rightarrow g(f(v))$  ( $v \in \Gamma_{A/K}$ ) evidently defines a minimal pre- $K$ -mapping of  $A$  into  $C$ . It is  $K$ -equivalent to a unique  $K$ -mapping, which we denote by  $h$ . To complete the proof it suffices to show that if  $v' \in A$ ,  $f$  is defined at  $v'$ , and  $g$  is defined at  $f(v')$ , then  $h$  is defined at  $v'$  and  $h(v') = g(f(v'))$ . Now,  $A, B, C$  are  $K$ -subsets of homogeneous  $K$ -spaces for certain  $K$ -groups. Denote these  $K$ -groups by  $G, H, I$ , respectively.

Consider any  $v \in \Gamma_{A/K}$  with  $v \xrightarrow{K_s} v'$ , and fix

$$(s, t, u) \in \Gamma_{G \circ H \circ I \circ K(v)}, \quad (s', t', u') \in \Gamma_{G \circ H \circ I \circ K(v')}$$

There exists a homomorphism

$$\begin{aligned} S_1 : K_s[K_s(vs) \cup K_s(s) \cup K_s(t) \cup K_s(u)] \\ \rightarrow K_s[K_s(v's') \cup K_s(s') \cup K_s(t') \cup K_s(u')] \end{aligned}$$

that extends  $S_{v's', vs}^{K_s}, S_{s', s}^{K_s}, S_{t', t}^{K_s}, S_{u', u}^{K_s}$ . On restriction  $S_1$  yields two homomorphisms

$$S : K_s[K_s(vs) \cup K_s(s) \cup K_s(t)] \rightarrow K_s[K_s(v's') \cup K_s(s') \cup K_s(t')],$$

$$S_0 : K_s[K_s(vs) \cup K_s(s) \cup K_s(u)] \rightarrow K_s[K_s(v's') \cup K_s(s') \cup K_s(u')].$$

Because  $f$  is defined at  $v'$ ,  $K_s(f(v)t) \subset \mathfrak{o}_S \subset \mathfrak{o}_{S_1}$  and the local ring homomorphism  $\tilde{S}_1 : \mathfrak{o}_{S_1} \rightarrow K_s(v', s', t', u')$  coincides with  $S_{f(v), t}^{K_s}$  on  $K_s(f(v)t)$ . Because  $g$  is defined at  $f(v')$ , if we choose some  $w \in \Gamma_{B/K}$  with  $w \xrightarrow{K_s} f(v)$ , then by Section 14, Lemma 6(c), the element  $h(v) = g(f(v))$  of  $C$  is holomorphic at  $f(v) \xrightarrow{K_s} f(v')$  and its value there is  $g(f(v'))$ . Hence, when  $\tilde{S}_1$  is restricted to a homomorphism

$$S_2 : K_s[K_s(f(v)t) \cup K_s(t) \cup K_s(u)] \rightarrow K_s[K_s(f(v')t') \cup K_s(t') \cup K_s(u')],$$

then  $K_s(h(v)u) \subset \mathfrak{o}_{S_2} \subset \mathfrak{o}_{S_1}$ , and  $\bar{S}_1$  coincides with  $S_{g(f(v))u', h(v)u}^{K_s}$  on  $K_s(h(v)u)$ . Thus, every element  $\alpha \in K_s(h(v)u)$  can be expressed in the form  $\alpha = \beta/\gamma$  with  $\beta, \gamma \in K_s[K_s(vs) \cup K_s(s) \cup K_s(t) \cup K_s(u)]$  and  $S_1(\gamma) \neq 0$ . Fixing a basis  $(\tau_i)$  of  $K_s(t)$  over  $K_s$ , we can write  $\beta = \sum \beta_i \tau_i$ ,  $\gamma = \sum \gamma_i \tau_i$ , where  $\beta_i, \gamma_i \in K_s[K_s(vs) \cup K_s(s) \cup K_s(u)]$  for every  $i$  and  $S_0(\gamma_i) = S_1(\gamma_i) \neq 0$  for some  $i$ . Then  $\sum (\alpha \gamma_i - \beta_i) \tau_i = 0$  and, because  $K_s(v, s, u)$  and  $K_s(t)$  are linearly disjoint over  $K_s$ ,  $\alpha \gamma_i - \beta_i = 0$  for every  $i$ , whence  $\alpha \in \mathfrak{o}_{S_0}$ . Therefore  $K_s(h(v)u) \subset \mathfrak{o}_{S_0}$  and  $S_0$  coincides with  $S_{g(f(v))u', h(v)u}^{K_s}$  on  $K_s(h(v)u)$ , that is, the element  $h(v) \in C_{K(v)}$  is holomorphic at  $v \xrightarrow{K_s} v'$  and its value there is  $g(f(v'))$ . Since everything proved here for  $v'$  is valid for any element  $v_0 \in A$  with  $v_0 \xrightarrow{K_s} v'$ , we conclude that  $h$  is defined at  $v'$  and  $h(v') = g(f(v'))$ .

**Lemma 8** Let  $f \in \mathfrak{M}_K(A, B)$  and let  $L$  be an extension of  $K$ .

- (a) A necessary and sufficient condition that  $f(\Gamma_{A/K}) \subset$  (respectively  $\supset$ )  $\Gamma_{B/K}$  is that  $f(\Gamma_{A/L}) \subset$  (respectively  $\supset$ )  $\Gamma_{B/L}$ .
- (b) If there exists a  $g \in \mathfrak{M}_L(B, A)$  such that  $g \circ f$  and  $f \circ g$  exist and equal  $id_A$  and  $id_B$ , respectively, then  $g$  is unique and  $g \in \mathfrak{M}_K(B, A)$ .

*Proof* (a) Let  $f(\Gamma_{A/K}) \subset \Gamma_{B/K}$ . If  $v \in \Gamma_{A/L}$ , then  $v \in \Gamma_{A/K}$  and  $K(v), L$  are algebraically disjoint over  $K$ , so that  $f(v) \in \Gamma_{B/K}$  and  $K(f(v)), L$  are algebraically disjoint over  $K$ , whence  $f(v) \in \Gamma_{B/L}$ . Therefore  $f(\Gamma_{A/L}) \subset \Gamma_{B/L}$ . Now let  $f(\Gamma_{A/K}) \supset \Gamma_{B/K}$ . If  $w \in \Gamma_{B/L}$ , then  $w = f(v')$  for some  $v' \in \Gamma_{A/K}$ . For some  $\sigma \in \text{Aut}(U/K(w))$ ,  $K(w, \sigma v')$  and  $L(w)$  are algebraically disjoint over  $K(w)$ , and for such a  $\sigma$  evidently  $\sigma v' \in \Gamma_{A/L}$  and  $f(\sigma v') = \sigma(f(v')) = \sigma w = w$ . Therefore  $f(\Gamma_{A/L}) \supset \Gamma_{B/L}$ .

Conversely, let  $f(\Gamma_{A/L}) \subset \Gamma_{B/L}$ . If  $v \in \Gamma_{A/K}$ , then  $\sigma v \in \Gamma_{A/L}$  for some  $\sigma \in \text{Aut}(U/K)$ , and  $f(v) = \sigma^{-1}(f(\sigma v)) \in \sigma^{-1}(\Gamma_{B/L}) \subset \sigma^{-1}(\Gamma_{B/K}) = \Gamma_{B/K}$ . Therefore  $f(\Gamma_{A/K}) \subset \Gamma_{B/K}$ . Now let  $f(\Gamma_{A/L}) \supset \Gamma_{B/L}$ . If  $w \in \Gamma_{B/K}$ , then  $\tau w \in \Gamma_{B/L}$  for some  $\tau \in \text{Aut}(U/K)$ , so that  $\tau w = f(v')$  for some  $v' \in \Gamma_{A/L}$ . Then  $\tau^{-1}v' \in \tau^{-1}(\Gamma_{A/L}) \subset \tau^{-1}(\Gamma_{A/K}) = \Gamma_{A/K}$  and  $f(\tau^{-1}v') = \tau^{-1}(f(v')) = w$ , so that  $w \in f(\Gamma_{A/K})$ . Hence  $f(\Gamma_{A/K}) \supset \Gamma_{B/K}$ .

- (b) If  $g_1, g_2$  are two elements of  $\mathfrak{M}_L(B, A)$  with the properties ascribed to  $g$ , then  $g_1 = g_1 \circ id_B = g_1 \circ (f \circ g_2) = (g_1 \circ f) \circ g_2 = id_A \circ g_2 = g_2$ , that is, if  $g$  exists, it is unique. Let it exist. We must show that  $g \in \mathfrak{M}_K(B, A)$ .

For any  $v \in \Gamma_{A/L}$  there is a  $w \in \Gamma_{B/L}$  such that  $w \xrightarrow{L} f(v)$ . Since  $v \in \Gamma_{A/L}$  and  $g(w) \xrightarrow{L} g(f(v)) = v$ , we have  $g(w) \xleftrightarrow{L} v$ , whence  $w = f(g(w)) \xleftrightarrow{L} f(v)$ , so that  $f(v) \in \Gamma_{B/L}$ . This shows that  $f(\Gamma_{A/L}) \subset \Gamma_{B/L}$  and therefore that  $\Gamma_{A/L} = g(f(\Gamma_{A/L})) \subset g(\Gamma_{B/L})$ . Because the roles of  $f$  and  $g$  in this argument can be interchanged, it follows that  $f(\Gamma_{A/L}) = \Gamma_{B/L}$  and hence, by part (a), that  $f(\Gamma_{A/K}) = \Gamma_{B/K}$ . For any  $v_1, v_2 \in \Gamma_{A/K}$  there exists a  $\sigma \in \text{Aut}(U/K)$  such

that  $\sigma(K(v_1, v_2))$  and  $L$  are algebraically disjoint over  $K$ , and therefore such that  $\sigma v_1, \sigma v_2 \in \Gamma_{A/L}$ . If  $f(v_1) = f(v_2)$ , then

$$\sigma v_1 = g(f(\sigma v_1)) = g(\sigma(f(v_1))) = g(\sigma(f(v_2))) = g(f(\sigma v_2)) = \sigma v_2$$

whence  $v_1 = v_2$ . Thus,  $f$  maps  $\Gamma_{A/K}$  bijectively onto  $\Gamma_{B/K}$ .

For any  $v \in \Gamma_{A/L}$ ,  $L(v) = L(g(f(v))) \subset L(f(v)) \subset L(v)$ , so that  $L(v) = L(f(v))$ . In particular,  $L(v)$  is a separable extension of  $L(f(v))$ . Hence (see Section 9, Proposition 8), for any  $v \in \Gamma_{A/K}$ ,  $K(v)$  is separable over  $K(f(v))$ . Since  $f(\sigma v) = \sigma(f(v)) = f(v)$  for every  $\sigma \in \text{Aut}(U/K(f(v)))$ , and therefore also  $\sigma v = v$  for every such  $\sigma$ , it follows that  $K(v) = K(f(v))$  ( $v \in \Gamma_{A/K}$ ). The mapping  $g_0: \Gamma_{B/K} \rightarrow A$  such that  $g_0(f(v)) = v$  for every  $v \in \Gamma_{A/K}$ , has the property that  $g_0(\Gamma_{B/K}) = \Gamma_{A/K}$  and  $K(g_0(w)) = K(w)$  for every  $w \in \Gamma_{B/K}$ . Also, for any  $\sigma \in \text{Aut}(U/K)$ ,  $g_0(\sigma(f(v))) = g_0(f(\sigma v)) = \sigma v = \sigma(g_0(f(v)))$  ( $v \in \Gamma_{A/K}$ ), that is,  $g_0(\sigma w) = \sigma(g_0(w))$  ( $w \in \Gamma_{B/K}$ ). It follows that  $g_0$  is a pre- $K$ -mapping of  $B$  into  $A$ . The  $K$ -mapping of  $B$  into  $A$   $K$ -equivalent to  $g_0$  is obviously  $L$ -equivalent to  $g$  and hence is  $g$ . Therefore  $g \in \mathfrak{M}_K(B, A)$ .

A  $K$ -mapping  $f$  of  $A$  into  $B$  is said to be *generically surjective* if  $f(\Gamma_{A/K}) \supset \Gamma_{B/K}$ . It is obvious that  $f$  is generically surjective if and only if the closed image of  $f$  is  $B$ . We say that  $f$  is *generically invertible* if there exists a  $K$ -mapping  $g$  of  $B$  into  $A$  such that  $g \circ f$  and  $f \circ g$  exist and equal  $id_A$  and  $id_B$ , respectively. This  $g$ , which by Lemma 8 is unique, then is called the *generic inverse* of  $f$ . We shall denote the generic inverse by  $f^-$ .

The following omnibus proposition identifies a number of  $K$ -mappings. In combination with Proposition 16, it provides a tool for proving that various mappings are  $K$ -mappings.

**Proposition 17** (a) If  $M$  is a homogeneous  $K$ -space for a  $K$ -group  $G$ , the homogeneous space law  $\mu_M: M \times G \rightarrow M$  (given by the formula  $\mu_M(v, x) = vx$ ) is a  $K$ -mapping of  $M \times G$  into  $M$ . When the homogeneous  $K$ -space is principal, the corresponding mapping  $\psi_M: M \times M \rightarrow G$  (given by the formula  $\psi_M(v, w) = v^{-1}w$ ) is a  $K$ -mapping of  $M \times M$  into  $G$ .

(b) Every  $K$ -homomorphism, either of  $K$ -groups or of homogeneous  $K$ -spaces for a  $K$ -group, is a  $K$ -mapping.

(c) Multiplication in the additive group  $G_a$  is a  $K$ -mapping of  $G_a \times G_a$  into  $G_a$ . The mapping  $G_a - \{0\} \rightarrow G_a$  given by the formula  $x \mapsto 1/x$  is a  $K$ -mapping of  $G_a$  into  $G_a$ .

(d) If  $A_1, \dots, A_m$  are  $K$ -sets, then, for each index  $i$ , the canonical projection  $pr_i: A_1 \times \dots \times A_m \rightarrow A_i$  is a  $K$ -mapping of  $A_1 \times \dots \times A_m$  into  $A_i$ .

(e) If  $A$  and  $B$  are  $K$ -sets and  $w \in B$ , the constant mapping  $k_w: A \rightarrow B$  with value  $w$  is a  $K(w)$ -mapping of  $A$  into  $B$ .

(f) If  $B$  is a  $K$ -set and  $B'$  is a  $K$ -subset of  $B$ , then the inclusion mapping  $in_{B, B'}: B' \rightarrow B$  is a  $K$ -mapping of  $B'$  into  $B$ . If also  $A$  is a  $K$ -set and  $f' \in \mathfrak{M}_K(A, B')$ , then  $in_{B, B'} \circ f'$  exists, has the same domain of definition as  $f'$ , and has closed image contained in  $B'$ . For any  $f \in \mathfrak{M}_K(A, B)$  with closed image contained in  $B'$  there exists a unique  $f' \in \mathfrak{M}_K(A, B')$  with  $in_{B, B'} \circ f' = f$ .

(g) If  $A, B_1, \dots, B_n$  are  $K$ -sets and  $f_j \in \mathfrak{M}_K(A, B_j)$  ( $1 \leq j \leq n$ ), then there exists a unique  $K$ -mapping  $f_1 \times \dots \times f_n$  of  $A$  into  $B_1 \times \dots \times B_n$  such that  $pr_j \circ (f_1 \times \dots \times f_n) = f_j$  ( $1 \leq j \leq n$ ). The domain of definition of  $f_1 \times \dots \times f_n$  is the intersection of the domains of definition of the  $f_j$ .

*Proof* The proof reduces to a number of routine verifications. We give the details in just one case, the homogeneous space law  $\mu_M$  in part (a). In the other cases the technique is similar.

It evidently suffices to show that if  $(v, x), (v', x') \in M \times G$  and  $(v, x) \rightarrow (v', x')$  then  $vx$  is holomorphic at  $(v, x) \rightarrow (v', x')$  and its value there is  $v'x'$ . Fixing  $(s_1, s_2, t) \in \Gamma_{G^0 \times G^0 \times G^0/K(v, x)}$  and  $(s_1', s_2', t') \in \Gamma_{G^0 \times G^0 \times G^0/K(v', x')}$ , we consider the homomorphism

$$S: K[K(v s_1, x s_2) \cup K(s_1, s_2) \cup K(t)] \rightarrow K[K(v' s_1', x' s_2') \cup K(s_1', s_2') \cup K(t')]$$

that extends  $S_{(v' s_1', x' s_2'), (v s_1, x s_2), S_{(s_1', s_2'), (s_1, s_2), S_{t', t}}$ . Since  $S$  maps  $K[K(s_1, s_2) \cup K(t)]$  isomorphically, we know that  $K(s_1, s_2, t) \subset \mathfrak{o}_S$  and  $\bar{S}$  extends  $S_{(s_1', s_2', t'), (s_1, s_2, t)}$ . Hence  $K(s_1^{-1}, s_2^{-1} t) \subset \mathfrak{o}_S$  and  $\bar{S}$  extends  $S_{(s_1', s_2', t'), (s_1^{-1}, s_2^{-1} t)}$ . Evidently  $\bar{S}$  maps  $K[K(x s_2) \cup K(s_1^{-1}, s_2^{-1} t)]$  isomorphically, so that  $K(x s_2, s_1^{-1}, s_2^{-1} t) \subset \mathfrak{o}_S$  and  $\bar{S}$  extends

$$S_{(x' s_2', s_1'^{-1}, s_2'^{-1} t'), (x s_2, s_1^{-1}, s_2^{-1} t)}$$

Hence  $K(s_1^{-1} x t) \subset \mathfrak{o}_S$  and  $\bar{S}$  extends  $S_{s_1'^{-1} x' t', s_1^{-1} x t}$ . Finally,  $\bar{S}$  maps  $K[K(v s_1) \cup K(s_1^{-1} x t)]$  isomorphically, so that  $K(v s_1, s_1^{-1} x t) \subset \mathfrak{o}_S$  and  $\bar{S}$  extends  $S_{(v' s_1', s_1'^{-1} x' t'), (v s_1, s_1^{-1} x t)}$ . Hence  $K(v x t) \subset \mathfrak{o}_S$  and  $\bar{S}$  extends  $S_{v' x' t', v x t}$ . This completes the proof.

REMARK 1 By part (a), the group law  $\mu_G: G \times G \rightarrow G$  is a  $K$ -mapping of  $G \times G$  into  $G$ . Also, by parts (a), (b), (e), and (g), and Proposition 16, the group symmetry  $\iota_G: G \rightarrow G$  (given by the formula  $\iota_G(x) = x^{-1}$ ) is a  $K$ -mapping of  $G$  into  $G$  (because  $\iota_G = \psi_{G^0} \circ (id_G \times k_1)$ , where  $k_1 \in \mathfrak{M}_K(G, G)$ ).

REMARK 2 For each  $x \in G$  the mapping  $\rho_x: M \rightarrow M$  (given by the formula  $\rho_x(v) = vx$ ) is a  $K(x)$ -mapping of  $M$  into  $M$ , for each  $v \in M$  the mapping  $\lambda_v: G \rightarrow M$  (given by the formula  $\lambda_v(x) = vx$ ) is a  $K(v)$ -mapping of  $G$  into  $M$  and, when the homogeneous  $K$ -space  $M$  is principal, the mapping  $M \rightarrow G$  given by the formula  $w \mapsto v^{-1} w$  is a  $K(v)$ -mapping of  $M$  into  $G$ . In the case of  $\rho_x$ , for example, this can be seen by the formula  $\rho_x = \mu_M \circ (id_M \times k_x)$ , where  $k_x \in \mathfrak{M}_{K(x)}(M, G)$ .

REMARK 3 If  $f \in \mathfrak{M}_K(A, B)$  and  $C$  is the closed image of  $f$ , the unique element  $g \in \mathfrak{M}_K(A, C)$  with  $in_{B, C} \circ g = f$  (see part (f) of the proposition) is generically surjective.

REMARK 4 If  $V_1, \dots, V_m$  are the  $K$ -components of  $A$ , the canonical bijection  $\mathfrak{M}_K(A, B) \rightarrow \mathfrak{M}_K(V_1, B) \times \dots \times \mathfrak{M}_K(V_m, B)$  is given by the formula  $f \mapsto (f \circ in_{A, V_1}, \dots, f \circ in_{A, V_m})$ .

REMARK 5 When  $H$  is a  $K$ -group, the group law of the group  $\mathfrak{M}_K(A, H)$  is given by the formula  $(f, g) \mapsto \mu_H \circ (f \times g)$  and the group symmetry of  $\mathfrak{M}_K(A, H)$  is given by the formula  $f \mapsto \iota_H \circ f$ . It follows that, for any  $v \in A$ ,  $\mathfrak{M}_{K, v}(A, H)$  is a subgroup of  $\mathfrak{M}_K(A, H)$  and the formula  $f \mapsto f(v)$  defines a group homomorphism  $\mathfrak{M}_{K, v}(A, H) \rightarrow H_{K(v)}$ .

Let  $f \in \mathfrak{M}_K(A, B)$  and  $v \in A$ . If  $f$  is generically invertible and  $f$  is defined at  $v$  and the generic inverse  $f^{-1}$  is defined at  $f(v)$ , we say that  $f$  is *bidefined at  $v$* . It is clear from Proposition 16 and the remark following it that then  $f^{-1}(f(v)) = v$  and  $f^{-1}$  is bidefined at  $f(v)$ . If  $f$  is bidefined at every element of a subset  $\Sigma$  of  $A$ , we say that  $f$  is *bidefined on  $\Sigma$* . We call the set of all elements of  $A$  at which  $f$  is bidefined the *domain of bidefinition of  $f$* .

**Proposition 18** Let  $A$  and  $B$  be  $K$ -subsets of homogeneous  $K$ -spaces, let  $f \in \mathfrak{M}_K(A, B)$ , and suppose that  $f$  is generically invertible. The domain of bidefinition of  $f$  is  $K$ -open and dense in  $A$ .

*Proof* Let  $A_0$  and  $B_0$  denote the domains of definition of  $f$  and  $f^{-1}$ , respectively. The domain of bidefinition of  $f$  is the set of elements  $v \in A_0$  such that  $f(v) \in B_0$ . Therefore the result follows from Proposition 15(a) and (b).

For any extension  $L$  of  $K$ ,  $\mathfrak{M}_K(A, B) \subset \mathfrak{M}_L(A, B)$ . As always, it is assumed here that the transcendence degree of  $U$  over  $L$  is infinite. If  $L'$  is an extension of  $K$  in  $U$  over which the transcendence degree of  $U$  is finite, we define  $\mathfrak{M}_{L'}(A, B) = \bigcup_L \mathfrak{M}_L(A, B)$ , where  $L$  ranges over the set of all extensions of  $K$  in  $L'$  over which the transcendence degree of  $U$  is infinite, and we call the elements of the set  $\mathfrak{M}_{L'}(A, B)$   $L'$ -mappings of  $A$  into  $B$ . The most inclusive set of this kind is  $\mathfrak{M}_U(A, B)$ , which we generally denote simply by  $\mathfrak{M}(A, B)$ . Any  $U$ -mapping we call also a *rational mapping*. When  $V_1', \dots, V_r'$  are the components of  $A$ , then the formula  $f \mapsto (f \circ in_{A, V_1'}, \dots, f \circ in_{A, V_r'})$  defines a canonical bijection  $\mathfrak{M}(A, B) \rightarrow \mathfrak{M}(V_1', B) \times \dots \times \mathfrak{M}(V_r', B)$ . When  $H$  is  $K$ -group then  $\mathfrak{M}(A, H)$  is a group, of which  $\mathfrak{M}_L(A, K)$  is a subgroup for every extension  $L$  of  $K$ , and the canonical bijection  $\mathfrak{M}(A, H) \rightarrow \mathfrak{M}(V_1', H) \times \dots \times \mathfrak{M}(V_r', H)$  is a group isomorphism. For any element  $v \in A$  (respectively set  $\Sigma \subset A$ ) we let  $\mathfrak{M}_{L', v}(A, B)$  (respectively  $\mathfrak{M}_{L', \Sigma}(A, B)$ )

denote the set of elements of  $\mathfrak{M}_L(A, B)$  that are defined at  $v$  (respectively on  $\Sigma$ ). Instead of  $\mathfrak{M}_{U,v}(A, B)$  (respectively  $\mathfrak{M}_{U,\Sigma}(A, B)$ ) we usually write  $\mathfrak{M}_v(A, B)$  (respectively  $\mathfrak{M}_\Sigma(A, B)$ ). Of course,  $\mathfrak{M}_v(A, H)$  is a subgroup of  $\mathfrak{M}(A, H)$ , and the formula  $f \mapsto f(v)$  defines a group homomorphism  $\mathfrak{M}_v(A, H) \rightarrow H$ .

If  $f \in \mathfrak{M}(A, B)$ , then  $id_A \times f \in \mathfrak{M}(A, A \times B)$  and the domains of definition of  $f$  and  $id_A \times f$  are the same (see Proposition 17(g)). We call the closed image of  $id_A \times f$  the *closed graph* of  $f$ .

**Proposition 19** *Let  $A$  and  $B$  be  $K$ -sets, let  $f \in \mathfrak{M}(A, B)$ , let  $Z$  denote the closed graph of  $f$ , and let  $L$  be an extension of  $K$ . If  $f \in \mathfrak{M}_L(A, B)$ , then  $Z$  is an  $L$ -subset of  $A \times B$ , and conversely.*

*Proof* If  $f$  is an  $L$ -mapping, then so is  $id_A \times f$ , and (by Proposition 15(c))  $Z$  is an  $L$ -set. Conversely, let  $Z$  be an  $L$ -set. Then  $pr_1 \circ in_{A \times B, Z} \in \mathfrak{M}_L(Z, A)$ . By Proposition 17(f), there exists a unique  $g \in \mathfrak{M}(A, Z)$  such that  $in_{A \times B, Z} \circ g = id_A \times f$ . This  $g$  has the same domain of definition as  $id_A \times f$  and hence as  $f$ , and for any element  $v$  of this domain,

$$\begin{aligned} (g \circ (pr_1 \circ in_{A \times B, Z}))(v, f(v)) &= g(v) = (in_{A \times B, Z} \circ g)(v) \\ &= (id_A \times f)(v) = id_Z(v, f(v)). \end{aligned}$$

Since the image of  $id_A \times f$  is dense in  $Z$ , this means that  $g \circ (pr_1 \circ in_{A \times B, Z}) = id_Z$ . On the other hand,

$$(pr_1 \circ in_{A \times B, Z}) \circ g = pr_1 \circ (in_{A \times B, Z} \circ g) = pr_1 \circ (id_A \times f) = id_A.$$

Therefore  $pr_1 \circ in_{A \times B, Z}$  is generically invertible and  $g$  is its generic inverse, so that  $g \in \mathfrak{M}_L(A, Z)$ . Since  $f = pr_2 \circ (id_A \times f) = pr_2 \circ (in_{A \times B, Z} \circ g)$ , it follows that  $f \in \mathfrak{M}_L(A, B)$ .

**Corollary** *Let  $A, B, f, Z$  be as in Proposition 19. Then  $K(Z)$  is the smallest extension  $L$  of  $K$  such that  $f \in \mathfrak{M}_L(A, B)$ .*

*Proof* See Section 7, Theorem 4.

If  $L$  is any extension of  $K$  and  $C$  is an  $L$ -subset of a homogeneous  $K$ -space  $M$  for a  $K$ -group  $G$ , then, for any  $\sigma \in \text{Aut}(U/K)$ ,  $\sigma C$  is a  $\sigma L$ -subset of  $M$  and  $\sigma$  maps each  $L$ -open subset of  $C$  onto a  $\sigma L$ -open subset of  $\sigma C$ . If  $D$  is an  $L$ -subset of a homogeneous  $K$ -space  $N$  for a  $K$ -group  $H$ , and if  $f \in \mathfrak{M}_L(C, D)$  and  $C_0$  denotes the domain of definition of  $f$ , we can define a mapping  $\sigma C_0 \rightarrow \sigma D$  by the formula  $\sigma v \mapsto \sigma(f(v))$ . Because  $(v, s, t) \in \Gamma_{C \times G \times H \circ L}$  if and only if  $(\sigma v, \sigma s, \sigma t) \in \Gamma_{\sigma C \times G \times H \circ \sigma L}$ , it is easy to see that this mapping is a  $\sigma L$ -mapping of  $\sigma C$  into  $\sigma D$ . We denote it by  $\sigma(f)$ . Thus,  $\sigma(f)$  is defined at  $\sigma v$  if and only if  $f$  is defined at  $v$ , and when this is the case then  $\sigma(f(v)) = (\sigma(f))(\sigma v)$ . If  $D'$  and  $Z$  are the closed image and closed

graph of  $f$ , then  $\sigma D'$  and  $\sigma Z$  are the closed image and closed graph of  $\sigma(f)$ . It is obvious that  $\sigma(\tau(f)) = (\sigma\tau)(f)$  for all  $\sigma, \tau \in \text{Aut}(U/K)$  and that  $id_U(f) = f$ . An easy computation shows that if  $E$  is an  $L$ -set, and if  $g \in \mathfrak{M}_L(D, E)$  and  $g \circ f$  exists, then  $\sigma(g) \circ \sigma(f)$  exists and is  $\sigma(g \circ f)$ . For fixed  $\sigma$ , the formula  $f \mapsto \sigma(f)$  defines a bijection  $\mathfrak{M}_L(C, D) \rightarrow \mathfrak{M}_{\sigma L}(\sigma C, \sigma D)$  that for each  $v \in C$ , maps  $\mathfrak{M}_{L,v}(C, D)$  onto  $\mathfrak{M}_{\sigma L, \sigma v}(\sigma C, \sigma D)$ . When  $D$  is an  $L$ -group the bijection is a group homomorphism.

**Proposition 20** *Let  $A$  and  $B$  be  $K$ -sets, let  $\Sigma$  be a subset of  $\text{Aut}(U/K)$ , let  $K'$  denote the field of invariants of  $\Sigma$ , and let  $f \in \mathfrak{M}(A, B)$ . A necessary and sufficient condition that  $f \in \mathfrak{M}_{K'}(A, B)$  is that  $\sigma(f) = f$  for every  $\sigma \in \Sigma$ .*

*Proof* If  $f \in \mathfrak{M}_{K'}(A, B)$  and  $\tau \in \text{Aut}(U/K')$ , then  $f(\tau v) = \tau(f(v)) = \tau(f)(\tau v)$  for every  $v$  at which  $f$  is defined, whence  $\tau(f) = f$ . Thus,  $\sigma(f) = f$  for every  $\sigma \in \Sigma$ . Conversely, if  $\sigma(f) = f$  for every  $\sigma \in \Sigma$ , and if we let  $Z$  denote the closed graph of  $f$ , then for each  $\sigma$ ,  $\sigma Z$  is the closed graph of  $\sigma(f) = f$  so that  $\sigma Z = Z$ ; by Section 7, Corollary 2 to Theorem 4,  $Z$  is a  $K'$ -set, and by Proposition 19 then  $f \in \mathfrak{M}_{K'}(A, B)$ .

Let us return to the arbitrary extension  $L$  of  $K$ , the  $L$ -sets  $C$  and  $D$ , and the  $L$ -mapping  $f \in \mathfrak{M}_L(C, D)$ , and let us recall Section 7, the remark following Corollary 2 to Theorem 4. Any isomorphism  $\gamma : L \approx L'$  over  $K$  of  $L$  onto an extension  $L'$  of  $K$  with  $\text{tr deg } U/L = \text{tr deg } U/L'$  can be extended to some  $\sigma \in \text{Aut}(U/K)$ , and for this  $\sigma$  we have  $\sigma(f) \in \mathfrak{M}_{\gamma L}(\gamma C, \gamma D)$ . Although  $\sigma$  is not uniquely determined by  $\gamma$ ,  $\sigma(f)$  is. Indeed, if  $\tau \in \text{Aut}(U/K)$  is another extension of  $\gamma$ , then  $\sigma^{-1}\tau \in \text{Aut}(U/L)$  and therefore  $\tau(f) = \sigma(\sigma^{-1}\tau(f)) = \sigma(f)$  by Proposition 20. It follows that we can denote  $\sigma(f)$  by  $\gamma(f)$ . It is easy to see that if  $\gamma' : L' \approx L'$  is an isomorphism over  $K$  with  $\text{tr deg } U/L' = \text{tr deg } U/L'$ , then  $\gamma'(\gamma(f)) = (\gamma'\gamma)(f)$ . Also,  $id_{L'}(f) = f$ . In particular, the group  $\text{Aut}(L/K)$  operates on  $\mathfrak{M}_L(A, B)$ .

**Corollary** *Let  $A$  and  $B$  be  $K$ -sets, let  $L$  be an extension of  $K$ , let  $\mathfrak{E}$  be a subset of  $\text{Aut}(L/K)$  such that the field of invariants of  $\mathfrak{E}$  is  $K$ , and let  $f \in \mathfrak{M}_L(A, B)$ . A necessary and sufficient condition that  $f \in \mathfrak{M}_K(A, B)$  is that  $\gamma(f) = f$  for every  $\gamma \in \mathfrak{E}$ .*

EXERCISES

- Let  $(x, y)$  be a  $K$ -generic point of the affine plane  $\mathbf{G}_a^2 = \mathbf{G}_a \times \mathbf{G}_a$ , and define  $f \in \mathfrak{M}_K(\mathbf{G}_a^2, \mathbf{G}_a^2)$ ,  $g \in \mathfrak{M}_K(\mathbf{G}_a^2, \mathbf{G}_a^2)$ ,  $h \in \mathfrak{M}_K(\mathbf{G}_a^2, \mathbf{G}_a)$  by the conditions

$$f(x, y) = (0, 0), \quad g(x, y) = (0, y), \quad h(x, y) = x/y.$$

Show that  $g \circ f, h \circ g, (h \circ g) \circ f$  exist but that  $h \circ (g \circ f)$  does not.

- Let  $\mathbf{M}(n)$  denote the algebra over  $U$  of all  $n \times n$  matrices with coordinates in  $U$ . Then  $\mathbf{M}(n)$  has a natural structure of  $K$ -group (in which the group law is the algebra addition) and may be identified with  $\mathbf{G}_a^{n^2}$ . Show that if  $G$  is any  $K$ -subgroup of  $\mathbf{GL}(n)$ , then the inclusion mapping  $G \rightarrow \mathbf{M}(n)$  is a  $K$ -mapping.

16  $K$ -Functions

$K$ -mappings into the  $K$ -group  $\mathbf{G}_a$  have a special terminology and notation. Let  $A$  be a  $K$ -set. A  $K$ -mapping of  $A$  into  $\mathbf{G}_a$  is called a  $K$ -function on  $A$ . We shall denote the set of all  $K$ -functions on  $A$  by  $\mathfrak{F}_K(A)$ , that is, we set  $\mathfrak{F}_K(A) = \mathfrak{M}_K(A, \mathbf{G}_a)$ . Similarly, we set  $\mathfrak{F}(A) = \mathfrak{M}(A, \mathbf{G}_a)$ , for any  $v \in A$  we set  $\mathfrak{F}_v(A) = \mathfrak{M}_v(A, \mathbf{G}_a)$  and  $\mathfrak{F}_{K,v}(A) = \mathfrak{M}_{K,v}(A, \mathbf{G}_a)$ , and for any subset  $\Sigma$  of  $A$  we set  $\mathfrak{F}_\Sigma(A) = \mathfrak{M}_\Sigma(A, \mathbf{G}_a)$  and  $\mathfrak{F}_{K,\Sigma}(A) = \mathfrak{M}_{K,\Sigma}(A, \mathbf{G}_a)$ . We call any element of  $\mathfrak{F}(A)$  a *rational function on  $A$* .

As we saw in Section 15,  $\mathfrak{F}(A)$  has a group structure (which is commutative and which we write additively): If  $\varphi, \psi \in \mathfrak{F}(A)$  and if  $\alpha$  denotes addition (the group law) in  $\mathbf{G}_a$ , then  $\varphi + \psi = \alpha \circ (\varphi \times \psi)$ . Similarly, if  $\mu$  denotes multiplication in  $\mathbf{G}_a$ , we can define a multiplication in  $\mathfrak{F}(A)$  by the formula  $\varphi\psi = \mu \circ (\varphi \times \psi)$ . This makes  $\mathfrak{F}(A)$  a commutative ring. The mapping  $U \rightarrow \mathfrak{F}(A)$  that carries each element  $b \in U$  onto the constant mapping  $k_b: A \rightarrow \mathbf{G}_a$  with value  $b$  is a ring homomorphism (injective when  $A \neq \emptyset$ ). By virtue of this homomorphism  $\mathfrak{F}(A)$  is an algebra over  $U$  and  $\mathfrak{F}_v(A)$  is a subalgebra for every  $v \in A$ , and when  $A \neq \emptyset$ , then we may identify  $U$  with its image in  $\mathfrak{F}(A)$ . Of course,  $\mathfrak{F}_K(A)$  is a subring of  $\mathfrak{F}(A)$  and is an algebra over  $K$  of which  $\mathfrak{F}_{K,v}(A)$  is a subalgebra. If  $V_1, \dots, V_m$  are the  $K$ -components of  $A$ , the canonical bijection  $\mathfrak{F}_K(A) \rightarrow \mathfrak{F}_K(V_1) \times \dots \times \mathfrak{F}_K(V_m)$  is an isomorphism of algebras over  $K$ , as is the bijection  $\mathfrak{F}_K(A) \rightarrow K(v_1) \times \dots \times K(v_m)$  determined by an element  $(v_1, \dots, v_m)$  of  $\Gamma_{V_1/K} \times \dots \times \Gamma_{V_m/K}$ . Therefore  $\mathfrak{F}_K(A)$  is a direct product of finitely many finitely generated separable extensions of  $K$ , and  $\mathfrak{F}_K(A)$  is a field if and only if  $A$  is  $K$ -irreducible (and is a regular extension of  $K$  if and only if  $A$  is irreducible). Similarly, if  $V'_1, \dots, V'_r$  are the components of  $A$ , the canonical bijection  $\mathfrak{F}(A) \rightarrow \mathfrak{F}(V'_1) \times \dots \times \mathfrak{F}(V'_r)$  is an isomorphism of algebras over  $U$ , and each  $\mathfrak{F}(V'_k)$  is a finitely generated extension of  $U$ .

REMARK In the case of an irreducible  $K$ -subset  $V$  of  $\mathbf{G}_a^n$  it is easy to describe the  $K$ -functions on  $V$  that are defined at a given element  $v' \in V$ : If  $\varphi \in \mathfrak{F}_K(V)$ , then a necessary and sufficient condition that  $\varphi \in \mathfrak{F}_{K,v'}(V)$  is that there exist polynomials  $P, Q \in K[X_1, \dots, X_n]$  with  $Q(v') \neq 0$  such that  $\varphi(v) = P(v)/Q(v)$  when  $v \in \Gamma_{V/K}$ . The sufficiency being obvious, let us suppose

that  $\varphi$  is defined at  $v'$ . Fixing  $(s, t) \in \Gamma_{\mathbf{G}_a^n \times \mathbf{G}_a/K(v)}$  and  $(s', t') \in \Gamma_{\mathbf{G}_a^n \times \mathbf{G}_a/K(v')}$  we have our usual homomorphism

$$S : K_s[K_s(v+s) \cup K_s(s) \cup K_s(t)] \rightarrow K_s[K_s(v'+s') \cup K_s(s') \cup K_s(t')],$$

and we know that  $\varphi(v) + t \in \mathfrak{o}_S$ , whence  $\varphi(v) \in \mathfrak{o}_S$ . However,  $S$  restricts to a homomorphism

$$S' : K_s[v+s, s, t] \rightarrow K_s[v'+s', s', t']$$

and evidently  $\mathfrak{o}_S = \mathfrak{o}_{S'}$ . Therefore there exist polynomials

$$P, Q \in K_s[X_1, \dots, X_n, Y_1, \dots, Y_n, Z]$$

with  $Q(v', s', t') \neq 0$  such that  $\varphi(v) = P(v, s, t)/Q(v, s, t)$ . Fixing a basis  $(\alpha_i)$  of  $K_s$  over  $K$ , we can write

$$P = \sum P_{ij_1 \dots j_n k} \alpha_i Y_1^{j_1} \dots Y_n^{j_n} Z^k, \quad Q = \sum Q_{ij_1 \dots j_n k} \alpha_i Y_1^{j_1} \dots Y_n^{j_n} Z^k$$

with  $P_{ij_1 \dots j_n k}, Q_{ij_1 \dots j_n k} \in K[X_1, \dots, X_n]$  for every  $(i, j_1, \dots, j_n, k)$ . Then  $Q_{ij_1 \dots j_n k}(v') \neq 0$  for some  $(i, j_1, \dots, j_n, k)$ , and

$$\sum (\varphi(v) Q_{ij_1 \dots j_n k}(v) - P_{ij_1 \dots j_n k}(v)) \alpha_i s_1^{j_1} \dots s_n^{j_n} t^k = 0,$$

so that  $\varphi(v) Q_{ij_1 \dots j_n k}(v) - P_{ij_1 \dots j_n k}(v) = 0$  for every  $(i, j_1, \dots, j_n, k)$  (because  $K(v)$  is regular over  $K$  and hence  $K(v)$  and  $K_s$  are linearly disjoint over  $K$ ). This proves the necessity of the condition.

Consider a subset  $\Sigma$  of  $A$ . We shall say that  $\Sigma$  is  *$K$ -affine in  $A$* , or that  $\Sigma$  is a  *$K$ -affine subset of  $A$* , if there exist a natural number  $n$ , a  $K$ -subset  $B$  of the direct product  $\mathbf{G}_a^n = \mathbf{G}_a \times \dots \times \mathbf{G}_a$ , and a generically invertible  $K$ -mapping of  $A$  into  $B$  that is bidefined on  $\Sigma$ .

If  $\Sigma$  is  $K$ -affine in  $A$ , then so is every subset of  $\Sigma$ . By Section 15, Proposition 18, if  $\Sigma$  is  $K$ -affine in  $A$ , then  $\Sigma$  is contained in a  $K$ -affine  $K$ -open dense subset of  $A$ .

**Lemma 9** *Let  $A_1$  and  $A_2$  be  $K$ -subsets of some  $K$ -set such that no  $K$ -component of either of them contains a  $K$ -component of the other, and let  $\Sigma_1$  and  $\Sigma_2$  be subsets of  $A_1$  and  $A_2$ , respectively, such that  $\Sigma_1 \cap A_2 = A_1 \cap \Sigma_2 = \emptyset$ . If  $\Sigma_i$  is  $K$ -affine in  $A_i$  ( $i = 1, 2$ ), then  $\Sigma_1 \cup \Sigma_2$  is  $K$ -affine in  $A_1 \cup A_2$ .*

*Proof* For each  $i$  ( $= 1, 2$ ) there exist an  $n_i$ , a  $K$ -subset  $B_i$  of  $\mathbf{G}_a^{n_i}$ , and a generically invertible  $f_i \in \mathfrak{M}_K(A_i, B_i)$  such that  $f_i$  is bidefined on  $\Sigma_i$ . Set  $n = n_1 + n_2 + 1$ . Identifying  $\mathbf{G}_a^n$  with its canonical image  $\mathbf{G}_a^{n_1} \times \mathbf{0}^{n_2} \times \mathbf{1}$  in

$G_a^{n_2} \times G_a^{n_2} \times G_a = G_a^n$ , and  $G_a^{n_2}$  with  $0^{n_1} \times G_a^{n_2} \times 0$ , we may suppose that  $B_i \subset G_a^{n_i}$  ( $i = 1, 2$ ) and  $B_1 \cap B_2 = \emptyset$ . The  $K$ -components of  $A_1$  and  $A_2$  are distinct from each other and are the  $K$ -components of  $A_1 \cup A_2$ , and likewise for the  $K$ -components of  $B_1$  and  $B_2$ . It follows that there is a unique  $f \in \mathfrak{M}_K(A_1 \cup A_2, B_1 \cup B_2)$  such that  $f \circ \text{in}_{A_1 \cup A_2, A_i} = f_i$  ( $i = 1, 2$ ), and that  $f$  is generically invertible. Because  $\Sigma_1 \cap A_2 = A_1 \cap \Sigma_2 = \emptyset$ , we see that  $f$  is generically invertible. Because  $\Sigma_1 \cap A_2 = A_1 \cap \Sigma_2 = \emptyset$ , we see that if  $v' \in \Sigma_i$  and  $v_0 \in A_1 \cup A_2$ ,  $v \in \Gamma_{A_1 \cup A_2/K}$ ,  $v \xrightarrow{K_*} v_0 \xrightarrow{K_*} v'$ , then  $v_0 \in A_i$ ,  $v \in \Gamma_{A_i/K}$ . Because  $f_i$  is defined at  $v'$ , the element  $f(v) = f_i(v)$  is holomorphic at  $v \xrightarrow{K_*} v_0$  and its value there is independent of the choice of  $v$ . Therefore  $f$  is defined on  $\Sigma_1 \cup \Sigma_2$ . A similar argument shows that  $f^{-1}$  is defined on the set  $f(\Sigma_1 \cup \Sigma_2) = f_1(\Sigma_1) \cup f_2(\Sigma_2)$ . Therefore  $f$  is bidefined on  $\Sigma_1 \cup \Sigma_2$ , and  $\Sigma_1 \cup \Sigma_2$  is  $K$ -affine  $A_1 \cup A_2$ .

**Corollary 1** *Let  $A$  be a  $K$ -set. There exists a  $K$ -affine  $K$ -open dense subset of  $A$ .*

*Proof* By the observation preceding Lemma 9, it suffices to show that  $\emptyset$  is  $K$ -affine in  $A$ , and by Lemma 9 it is enough to show that  $\emptyset$  is  $K$ -affine in each  $K$ -component of  $A$ . Let  $V$  be any  $K$ -component of  $A$ . Then  $\mathfrak{F}_K(V)$  is a finitely generated extension of  $K$ , say  $\mathfrak{F}_K(V) = K(\xi_1, \dots, \xi_n)$ . The closed image  $W$  of the  $K$ -mapping  $\xi_1 \times \dots \times \xi_n$  is a  $K$ -subset of  $G_a^n$  and obviously is  $K$ -irreducible. By Section 15, Remark 3 following Proposition 17, there exists a generically surjective  $f \in \mathfrak{M}_K(V, W)$  such that  $\text{in}_{G_a^n, W} \circ f = \xi_1 \times \dots \times \xi_n$ . For  $v \in \Gamma_{V/K}$  evidently  $f(v) = (\xi_1(v), \dots, \xi_n(v)) \in \Gamma_{W/K}$  and  $K(v) = K(f(v))$ . It follows from this that  $f$  is generically invertible. Since  $f$  is bidefined on  $\emptyset$ ,  $\emptyset$  is  $K$ -affine  $V$ .

**Corollary 2** *Let  $A$  be a  $K$ -set,  $A'$  be a  $K$ -subset of  $A$ , and  $\Sigma$  be a subset of  $A'$ . If  $\Sigma$  is  $K$ -affine in  $A$ , then  $\Sigma$  is  $K$ -affine in  $A'$ .*

*Proof* Let  $f \in \mathfrak{M}_K(A, B)$  be generically invertible and bidefined on  $\Sigma$ , where  $B$  is a  $K$ -subset of  $G_a^n$ . Let  $V_1, \dots, V_m$  be the  $K$ -components of  $A'$  that contain an element of  $\Sigma$ , let  $A_1 = V_1 \cup \dots \cup V_m$ , and let  $A_2$  be the union of the other  $K$ -components of  $A'$ . Fixing  $v_i \in \Gamma_{V_i/K}$ , we see that  $f$  is bidefined at  $v_i$  so that  $K(v_i) = K(f(v_i))$ . The locus of  $f(v_i)$  over  $K$  is a  $K$ -subset  $W_i$  of  $B$ . Set  $B_1 = W_1 \cup \dots \cup W_m$ . Evidently  $W_1, \dots, W_m$  are the  $K$ -components of  $B_1$ , and each of them contains an element of  $f(\Sigma)$ . There exists an  $f_1 \in \mathfrak{M}_K(A_1, B_1)$  such that  $f_1(v_i) = f(v_i)$  ( $1 \leq i \leq m$ ), and evidently  $f_1$  is generically invertible. Also,  $f \circ \text{in}_{A, A_1} = \text{in}_{B, B_1} \circ f_1$  and  $f^{-1} \circ \text{in}_{B, B_1} = \text{in}_{A, A_1} \circ f_1^{-1}$ . It follows from these equations and Section 15, Proposition 17(f), that  $f_1$  is defined on  $\Sigma$  and  $f_1^{-1}$  is defined on  $f_1(\Sigma)$ , that is, that  $f_1$  is bidefined on  $\Sigma$ . Therefore  $\Sigma$  is  $K$ -affine on  $A_1$ . As  $\emptyset$  is  $K$ -affine in  $A_2$  (by Corollary 1), Lemma 9 shows that  $\Sigma$  is  $K$ -affine in  $A'$ .

It is obvious that if  $\Sigma$  is  $K$ -affine in  $A$ , then, for any extension  $L$  of  $K$ ,  $\Sigma$  is  $L$ -affine in  $A$ . In order to prove a result in the opposite direction, we first establish two lemmas (taken from Serre [26, pp. 58, 110]).

**Lemma 10** *Let  $R$  be a Noetherian ring,  $J$  be a finitely generated algebra over  $R$ , and  $I$  be a subalgebra of  $J$ . If  $J$  is integral over  $I$ , then  $I$  is finitely generated over  $R$ .*

*Proof* We have  $J = R[x_1, \dots, x_n]$  and, for each  $j$ , there exists a unitary polynomial  $P_j \in I[X]$  such that  $P_j(x_j) = 0$ . Let  $b_1, \dots, b_r$  be the coefficients in  $P_1, \dots, P_n$ , and set  $I' = R[b_1, \dots, b_r]$ . Each  $x_j$  is integral over  $I'$  and therefore  $J$  is a finitely generated  $I'$ -module. Since  $R$  is Noetherian and hence  $I'$  is, too, this implies that every submodule of the  $I'$ -module  $J$  is finitely generated. In particular, we may write  $I = \sum_{1 \leq i \leq m} I' y_i$ , so that  $I = R[b_1, \dots, b_r, y_1, \dots, y_m]$ .

**Lemma 11** *Let  $A$  be a  $K$ -set, let  $\varphi \in \mathfrak{F}_{K_*}(A)$ , and let  $\varphi_1, \dots, \varphi_m$  be the conjugates of  $\varphi$  over  $K$ . There exist elements  $\psi_1, \dots, \psi_n \in \mathfrak{F}_K(A)$  such that  $K_*[\varphi_1, \dots, \varphi_m] = K_*[\psi_1, \dots, \psi_n]$ .*

*Proof* By Section 15, Proposition 19, and Section 7, Theorem 4, there exists a Galois extension  $L$  of  $K$  of finite degree, say  $m'$ , such that  $\varphi$  (and hence each  $\varphi_i$ ) is in  $\mathfrak{F}_L(A)$ . The algebra  $J = L[\varphi_1, \dots, \varphi_m]$  over  $K$  is finitely generated. The Galois group  $\mathfrak{g} = \mathfrak{g}(L/K)$  operates on  $J$ , and the set  $I$  of invariants of  $\mathfrak{g}$  in  $J$  is a subalgebra of  $J$ . For any  $\zeta \in J$ , the coefficients in the polynomial  $\prod_{\gamma \in \mathfrak{g}} (X - \gamma(\zeta))$  are elements of  $I$ . Hence  $J$  is integral over  $I$ . Thus, Lemma 10 applies and we can write  $I = K[\psi_1, \dots, \psi_n]$ . By Section 15, the Corollary to Proposition 20,  $\psi_j \in \mathfrak{F}_K(A)$  ( $1 \leq j \leq n$ ).

Let  $E$  denote the free  $L$ -module  $\sum_{\gamma \in \mathfrak{g}} L\gamma$  on  $\mathfrak{g}$  considered as a vector space over  $K$ . For any element  $\sum_{\gamma \in \mathfrak{g}} \alpha_\gamma \gamma$  of  $E$  the formula  $\lambda \mapsto \sum_{\gamma \in \mathfrak{g}} \alpha_\gamma \gamma(\lambda)$  defines an endomorphism of the  $m'$ -dimensional vector space  $L$  over  $K$ , and (because distinct automorphisms of a field are linearly independent over that field) distinct elements of  $E$  yield distinct endomorphisms of  $L$ . Thus, we have an injection  $E \rightarrow \text{End}_K(L)$  that evidently is linear, that is, we can identify  $E$  with a subspace of the vector space  $\text{End}_K(L)$  over  $K$ . Because  $\dim_K E = [L:K] \dim_L E = m'^2 = \dim_K \text{End}_K(L)$ , we have  $E = \text{End}_K(L)$ . Therefore the identification gives  $E$  a structure of  $K$ -algebra. More precisely,  $E$  is a simple  $K$ -algebra and every  $E$ -module is a direct sum of simple  $E$ -modules isomorphic to the simple  $E$ -module  $L$ . Because  $J$  is evidently an  $E$ -module (the element  $\sum_{\gamma \in \mathfrak{g}} \alpha_\gamma \gamma$  of  $E$  operating on the element  $\chi = F(\varphi_1, \dots, \varphi_m)$  of  $J$  to produce the element  $\sum_{\gamma \in \mathfrak{g}} \alpha_\gamma \gamma(\chi) = \sum_{\gamma \in \mathfrak{g}} \alpha_\gamma F(\gamma(\varphi_1), \dots, \gamma(\varphi_m))$  of  $J$ ), there exists a direct sum decomposition  $J = \sum_k L_k$  in which each  $L_k$  is an  $E$ -module isomorphic to  $L$ . The  $E$ -module



$L$ , when considered as a module over the subring  $L \cdot id_L$  of  $E$ , has a basis consisting of a single element (namely, 1) that is invariant under the subset  $\mathfrak{g}$  of  $E$ . The same must be true for each  $L_k$ , so that  $L_k = L \cdot \varepsilon_k$  where the element  $\varepsilon_k \in L_k \subset J$  is invariant under  $\mathfrak{g}$ , that is,  $\varepsilon_k \in I$ . This shows that  $L[\varphi_1, \dots, \varphi_m] = L[\psi_1, \dots, \psi_n]$  and completes the proof.

We can now prove the following result about “descent” from  $K_s$  to  $K$ .

**Proposition 21** *Let  $A$  be a  $K$ -set and let  $\mathcal{O}$  be a  $K$ -open subset of  $A$ . If  $\mathcal{O}$  is  $K_s$ -affine in  $A$ , then  $\mathcal{O}$  is  $K$ -affine in  $A$ .*

*Proof* By Section 15, Proposition 19, and Section 7, Theorem 4, there exists a Galois extension  $L$  of  $K$  of finite degree, say  $m$ , such that  $\mathcal{O}$  is  $L$ -affine in  $A$ . For some  $n$  and some  $L$ -subset  $B$  of  $\mathbf{G}_a^n$ , there exists a generically invertible  $f \in \mathfrak{M}_L(A, B)$  that is bidefined on  $\mathcal{O}$ . Let  $\gamma_1, \dots, \gamma_m$  be the elements of the Galois group  $\mathfrak{g}(L/K)$ , with  $\gamma_1 = id_L$ . For each  $i$ ,  $\gamma_i B$  is an  $L$ -subset of  $\mathbf{G}_a^n$  and  $\gamma_i(f)$  is a generically invertible  $L$ -mapping of  $A$  into  $\gamma_i B$  that is bidefined on  $\mathcal{O}$ . This implies that  $\gamma_1(f) \times \dots \times \gamma_m(f) \in \mathfrak{M}_L(A, \gamma_1 B \times \dots \times \gamma_m B)$ , that the closed image  $B'$  of  $\gamma_1(f) \times \dots \times \gamma_m(f)$  is an  $L$ -subset of  $\mathbf{G}_a^{nm}$ , and that the unique  $L$ -mapping  $f' \in \mathfrak{M}_L(A, B')$  with  $in_{\gamma_1 B \times \dots \times \gamma_m B, B'} \circ f' = \gamma_1(f) \times \dots \times \gamma_m(f)$  is defined on  $\mathcal{O}$ . Letting  $p_1$  denote the canonical projection  $\gamma_1 B \times \dots \times \gamma_m B \rightarrow \gamma_1 B = B$ , we see that  $f' \circ (p_1 \circ in_{\gamma_1 B \times \dots \times \gamma_m B, B'})$  exists and is an element of  $\mathfrak{M}_L(B', A)$  and that its two generic composites with  $f'$  exist and equal  $id_A$  and  $id_{B'}$ . It follows that  $f'$  is generically invertible and that  $f'$  is bidefined on  $\mathcal{O}$ . Thus,  $nm, B', f'$  have the same properties as  $n, B, f$  and have the further property that the  $nm$   $L$ -functions  $pr_k \circ in_{\mathbf{G}_a^{nm}, B'} \circ f'$  ( $1 \leq k \leq nm$ ) are permuted by the elements of the Galois group  $\mathfrak{g}(L/K)$ . Replacing  $n, B, f$  by  $nm, B', f'$ , we may suppose, accordingly, that the  $n$   $L$ -functions

$$\xi_j = pr_j \circ in_{\mathbf{G}_a^n, B} \circ f \quad (1 \leq j \leq n)$$

are permuted by the elements of  $\mathfrak{g}(L/K)$ .

It follows from Lemma 11 that there exist elements  $\eta_1, \dots, \eta_r \in \tilde{\mathfrak{F}}_{K, \mathcal{O}}(A)$  such that  $K_s[\xi_1, \dots, \xi_n] = K_s[\eta_1, \dots, \eta_r]$ . The closed image  $C$  of  $\eta_1 \times \dots \times \eta_r$  is a  $K$ -subset of  $\mathbf{G}_a^r$ , and there is a generically surjective  $g \in \mathfrak{M}_{K, \mathcal{O}}(A, C)$  such that  $in_{\mathbf{G}_a^r, C} \circ g = \eta_1 \times \dots \times \eta_r$ . There exist polynomials  $P_1, \dots, P_r \in K_s[X_1, \dots, X_n]$  and  $Q_1, \dots, Q_n \in K_s[Y_1, \dots, Y_r]$  such that

$$P_k(\xi_1, \dots, \xi_n) = \eta_k \quad (1 \leq k \leq r) \quad \text{and} \quad Q_j(\eta_1, \dots, \eta_r) = \xi_j \quad (1 \leq j \leq n).$$

The formulae  $(x_1, \dots, x_n) \mapsto (P_k(x_1, \dots, x_n))_{1 \leq k \leq r}$  and  $(y_1, \dots, y_r) \mapsto (Q_j(y_1, \dots, y_r))_{1 \leq j \leq n}$  give everywhere defined  $K_s$ -mappings of  $\mathbf{G}_a^n$  into  $\mathbf{G}_a^r$  and  $\mathbf{G}_a^r$  into  $\mathbf{G}_a^n$ , respectively. By what we have just shown, these induce everywhere defined  $K_s$ -mappings  $h \in \mathfrak{M}_{K_s}(B, C)$  and  $h' \in \mathfrak{M}_{K_s}(C, B)$ , re-

spectively, that are generically invertible and generically inverse to each other, and  $h \circ f = g$ . This shows that  $g$  is generically invertible and bidefined on  $\mathcal{O}$ , and completes the proof of the proposition.

We are now in a position to prove the following important result.

**Theorem 11** *Let  $A$  be a  $K$ -set. Every finite subset of  $A$  is  $K$ -affine in  $A$ .*

*Proof* Let  $A$  be a  $K$ -subset of a homogeneous  $K$ -space  $M$  for a  $K$ -group  $G$ . By Corollary 2 to Lemma 9, it suffices to show that an arbitrary finite set  $\Phi \subset M$  is  $K$ -affine in  $M$ , that is, is contained in a  $K$ -affine  $K$ -open subset of  $M$ . Now, every element  $v \in \Phi$  has a specialization  $v'$  over  $K$  that is algebraic over  $K$ . A  $K$ -open subset of  $M$  that contains  $v'$  must contain  $v$ , too. It follows that we may suppose that  $\Phi \subset M_{K_a}$ . Since  $\Phi$  then has only finitely many conjugates over  $K$ , we may replace  $\Phi$  by the union of all of them, that is, we may suppose that  $\sigma(\Phi) = \Phi$  for every  $\sigma \in \text{Aut}(U/K)$ .

By Corollary 1 to Lemma 9, there exists a set  $\mathcal{O} \subset M$  that is  $K$ -affine  $K$ -open and dense in  $M$ . For any  $v \in M_{K_a}$ , we know that  $\lambda_v \in \mathfrak{M}_{K_a}(G, M)$  (see Section 15, Remark 2 following Proposition 17), and hence that  $\lambda_v$  is  $K_s$ -continuous (see Section 15, Proposition 15(b)), so that  $\lambda_v^{-1}(\mathcal{O})$  is  $K_s$ -open in  $G$ . Since  $\lambda_v^{-1}(\mathcal{O}) \supset \Gamma_{M/K}$  (Section 3, Remark 1 following Theorem 1),  $\lambda_v^{-1}(\mathcal{O})$  is dense in  $G$ . It follows that the set  $E = \bigcap_{v \in \Phi} \lambda_v^{-1}(\mathcal{O})$  is  $K_s$ -open and dense in  $G$ , and because  $\sigma E = \bigcap_{v \in \Phi} \sigma(\lambda_v^{-1}(\mathcal{O})) = \bigcap_{v \in \Phi} \lambda_{\sigma v}^{-1}(\sigma \mathcal{O}) = \bigcap_{v \in \Phi} \lambda_v^{-1}(\mathcal{O}) = E$  for every  $\sigma \in \text{Aut}(U/K)$ ,  $E$  is  $K$ -open in  $G$ . Now,  $E$  contains an element  $x$  that is separably algebraic over  $K$ , and hence contains the conjugates  $x_1 = x, x_2, \dots, x_r$  of  $x$  over  $K$ . For each  $k$ ,  $x_k \in \lambda_v^{-1}(\mathcal{O})$  ( $v \in \Phi$ ), that is,  $\Phi x_k \subset \mathcal{O}$ . Therefore, if we set  $\mathcal{O}' = \bigcap_{1 \leq k \leq r} \rho_{x_k}^{-1}(\mathcal{O})$ , then  $\Phi \subset \mathcal{O}'$ . We see, as we saw for  $E$ , that  $\mathcal{O}'$  is a  $K$ -open dense subset of  $M$ . Because  $\mathcal{O}$  is  $K$ -affine in  $M$  (and hence also  $K_s$ -affine) and  $\rho_x$  is a generically invertible everywhere bidefined  $K_s$ -mapping of  $M$  into  $M$  (with generic inverse  $\rho_x^{-1}$ ),  $\rho_x^{-1}(\mathcal{O})$  is  $K_s$ -affine in  $M$ , and therefore so is its subset  $\mathcal{O}'$ . It follows, finally, by Proposition 21, that  $\mathcal{O}'$  is  $K$ -affine in  $M$ .

**Corollary** *Let  $A$  be a  $K$ -set, and let  $\Phi$  be a finite subset of  $A$ . Then  $A$  has a finite covering by  $K$ -affine  $K$ -open dense subsets that contain  $\Phi$ .*

*Proof* By the theorem, for each  $v \in A$ , there exists a  $K$ -affine  $K$ -open dense subset  $\mathcal{O}_v$  of  $A$  that contains  $v$  and every element of  $\Phi$ . The family  $(\mathcal{O}_v)_{v \in A}$  obviously covers  $A$ . Because the  $K$ -topology on  $A$  is Noetherian, some finite subfamily covers  $A$ .

**REMARK** The axioms in Sections 2 and 3 were taken so that if  $G'$  is an algebraic group, in the context of Weil's “abstract algebraic varieties” [27]

and their natural generalization to “abstract algebraic sets” (according to which an abstract algebraic variety is an irreducible abstract algebraic set), and if  $G'$  is defined over  $K$ , then  $G'$  is (more precisely, has a natural structure of) a  $K$ -group. Also, an algebraic homogeneous space for  $G'$  that is defined over  $K$  is a homogeneous  $K$ -space for  $G'$ . The corollary implies that, conversely, any  $K$ -group  $G$  is  $K$ -isomorphic to an algebraic group  $G'$  defined over  $K$ , and that a homogeneous  $K$ -space for  $G$  is (when considered as a homogeneous  $K$ -space for  $G'$  via a  $K$ -isomorphism  $G' \approx G$ )  $K$ -isomorphic to an algebraic homogeneous space for  $G'$  defined over  $K$ .

Now let  $A$  and  $B$  be  $K$ -sets, let  $f \in \mathfrak{M}_K(A, B)$ , and suppose that  $f$  has the property that  $f(\Gamma_{A/K}) \subset \Gamma_{B/K}$  (see Section 15, Lemma 8(a)). Then  $\psi \circ f$  exists for every  $\psi \in \mathfrak{F}(B)$ , and we can define a mapping

$$f^* : \mathfrak{F}(B) \rightarrow \mathfrak{F}(A)$$

by the formula  $f^*(\psi) = \psi \circ f$ . It is clear that  $f^*$  is a homomorphism of algebras over  $U$ , that  $f^*$  restricts to a homomorphism  $\mathfrak{F}_K(B) \rightarrow \mathfrak{F}_K(A)$  of algebras over  $K$ , and that if  $f$  is defined at an element  $v \in A$ , then  $f^*$  restricts to a homomorphism  $\mathfrak{F}_{f(v)}(B) \rightarrow \mathfrak{F}_v(A)$  of algebras over  $U$ . Also,  $f^*$  is injective if and only if  $f$  is generically surjective. If  $C$  is a  $K$ -set, and if  $g \in \mathfrak{M}_K(B, C)$  and  $g(\Gamma_{B/K}) \subset \Gamma_{C/K}$ , then  $g \circ f$  exists and maps  $\Gamma_{A/K}$  into  $\Gamma_{C/K}$ , and  $(g \circ f)^* = f^* \circ g^*$ . Furthermore,  $(id_A)^* = id_{\mathfrak{F}(A)}$ . It follows that if  $f$  is generically invertible, then  $f^*$  is an isomorphism and  $(f^*)^{-1} = (f^{-1})^*$ .

The following proposition describes the relation between  $U$  and  $\mathfrak{F}_K(A)$  in  $\mathfrak{F}(A)$ .

**Proposition 22** *Let  $A$  be a  $K$ -set, and let  $L$  be an extension of  $K$ .*

(a) *If  $\Sigma$  is a  $K$ -affine subset of  $A$ , then  $\mathfrak{F}_L(A)$  is the complete ring of quotients of  $L[\mathfrak{F}_{K,\Sigma}(A)]$ .*

(b)  *$L$  and  $\mathfrak{F}_K(A)$  are linearly disjoint over  $K$ .*

(c) *Let  $\mathcal{O}$  be a  $K$ -open dense subset of  $A$  that satisfies the following condition: Whenever the intersection of two components of  $A$  contains an element of  $\mathcal{O}$ , some component of the intersection contains that element and is a  $K_s$ -subset of  $A$ . Then  $\mathfrak{F}_{L,\mathcal{O}}(A) = L[\mathfrak{F}_{K,\mathcal{O}}(A)]$ .*

**REMARK 1** Because of Theorem 11, (a) shows, for any  $v \in A$ , that  $\mathfrak{F}_L(A) = Q(L[\mathfrak{F}_{K,v}(A)])$ . In particular,  $\mathfrak{F}_K(A) = Q(\mathfrak{F}_{K,v}(A))$ . Also, if  $A \subset \mathbf{G}_a^n$ , then  $\mathfrak{F}_L(A) = Q(L[\mathfrak{F}_{K,A}(A)])$ .

**REMARK 2** The condition in (c) is satisfied when  $p = 0$  (because then every  $K_s$ -closed set is a  $K_s$ -set), and when the components of  $A$  are pairwise disjoint (for example, when  $A$  is a homogeneous  $K$ -space).

**REMARK 3** When the condition in (c) is satisfied, (b) and (c) show that the canonical homomorphism  $L \otimes_K \mathfrak{F}_{K,\mathcal{O}}(A) \rightarrow \mathfrak{F}_{L,\mathcal{O}}(A)$  is an isomorphism.

*Proof* (a) If there exist a  $K$ -set  $B \subset \mathbf{G}_a^n$  and a generically invertible  $f \in \mathfrak{M}_K(A, B)$  that is bidefined on  $\Sigma$ , then  $f^*$  maps  $\mathfrak{F}_L(B)$  isomorphically onto  $\mathfrak{F}_L(A)$  and maps  $\mathfrak{F}_{K,f(\Sigma)}(B)$  isomorphically onto  $\mathfrak{F}_{K,\Sigma}(A)$ . It is easy to see that  $\mathfrak{F}_L(B) = Q(L[F_{K,f(\Sigma)}(B)])$ . Therefore  $\mathfrak{F}_L(A) = Q(L[\mathfrak{F}_{K,\Sigma}(A)])$ .

(b) We show that if  $K$ -functions  $\varphi_1, \dots, \varphi_n$  on  $A$  are linearly dependent over  $U$ , then they are linearly dependent over  $K$ . Arguing by induction on  $n$ , we may suppose that  $n > 1$  and  $\varphi_1, \dots, \varphi_{n-1}$  are linearly independent over  $U$ . Then there exist elements  $\alpha_1, \dots, \alpha_n \in U$  with  $\alpha_n \neq 0$  such that  $\sum_{1 \leq j \leq n} \alpha_j \varphi_j = 0$ . Dividing by  $\alpha_n$ , we may suppose that  $\alpha_n = 1$ . For any  $\sigma \in \text{Aut}(U/K)$ , we have  $\sum_{1 \leq j \leq n} (\sigma \alpha_j) \varphi_j = \sigma(\sum_{1 \leq j \leq n} \alpha_j \varphi_j) = 0$ , so that  $\sum_{1 \leq j \leq n-1} (\sigma \alpha_j - \alpha_j) \varphi_j = 0$ , whence  $\sigma \alpha_j = \alpha_j$  ( $1 \leq j \leq n$ ). Therefore  $\alpha_j \in K_1$  ( $1 \leq j \leq n$ ). For each  $v \in \Gamma_{A/K}$ , fix a basis  $(\beta_{vl})_{l \in \Lambda(v)}$  of  $K(v)$  over  $K$ . As  $K(v)$  is separable over  $K$ ,  $(\beta_{vl})_{l \in \Lambda(v)}$  is linearly independent over  $K_1$ . Writing  $\varphi_j(v) = \sum_l c_{vjl} \beta_{vl}$ , where  $c_{vjl} \in K$ , we find that  $\sum_l (\sum_j c_{vjl} \alpha_j) \beta_{vl} = \sum_j \alpha_j \varphi_j(v) = 0$ , so that  $\sum_j c_{vjl} \alpha_j = 0$ . Thus, the system of homogeneous linear equations

$$\sum_{1 \leq j \leq n} c_{vjl} X_j = 0 \quad (v \in \Gamma_{A/K}, l \in \Lambda(v))$$

with coefficients in  $K$  has a nontrivial solution. Hence the system has a nontrivial solution  $(a_1, \dots, a_n) \in K^n$ . Evidently  $\sum_{1 \leq j \leq n} a_j \varphi_j(v) = 0$  ( $v \in \Gamma_{A/K}$ ), so that  $\sum_{1 \leq j \leq n} a_j \varphi_j = 0$ .

(c) Let  $(\lambda_l)_{l \in \Lambda}$  be a basis of  $L$  over  $K$ , and let  $\varphi \in \mathfrak{F}_{L,\mathcal{O}}(A)$ . By part (b), if there exist  $K$ -functions  $\varphi_l$  ( $l \in \Lambda$ ) such that  $\varphi = \sum \lambda_l \varphi_l$ , then they are unique. We shall show that they do exist and that they are defined on  $\mathcal{O}$ . For the second point, it suffices to show that they are defined on every set belonging to some covering of  $\mathcal{O}$ . Hence, by the corollary to Theorem 11, we may suppose that  $\mathcal{O}$  is  $K$ -affine in  $A$ . Then there exist a  $K$ -subset  $B$  of some  $\mathbf{G}_a^n$  and a generically invertible  $f \in \mathfrak{M}_K(A, B)$  that is bidefined on  $\mathcal{O}$ . Clearly,  $f(\mathcal{O})$  is  $K$ -open and dense in  $B$ , and if the intersection of two components of  $B$  contains an element of  $f(\mathcal{O})$ , then some component of the intersection contains that element and is a  $K_s$ -subset of  $B$ . Also,  $(f^{-1})^*(\varphi) \in \mathfrak{F}_{L,f(\mathcal{O})}(B)$ . If we can show that  $(f^{-1})^*(\varphi) = \sum \lambda_l \psi_l$  with  $\psi_l \in \mathfrak{F}_{K,f(\mathcal{O})}(B)$  for each  $l$ , then we shall have  $\varphi = f^*((f^{-1})^*(\varphi)) = \sum \lambda_l f^*(\psi_l)$  with  $f^*(\psi_l) \in \mathfrak{F}_{K,\mathcal{O}}(A)$  for each  $l$ . This shows that we may replace  $A, \mathcal{O}, \varphi$  by  $B, f(\mathcal{O}), (f^{-1})^*(\varphi)$ , that is, that we may suppose that  $A$  is a  $K$ -subset of  $\mathbf{G}_a^n$ .

First consider the case in which  $K = K_s$  and  $A$  is irreducible. The set  $C = A - \mathcal{O}$  is  $K$ -closed and  $C \neq A$ . Therefore if we let  $\mathfrak{p}$ , respectively  $\mathfrak{c}$ , denote the defining ideal in  $K[X_1, \dots, X_n]$  of  $A$ , respectively  $C$ , then  $\mathfrak{c} \supset \mathfrak{p}$  and  $\mathfrak{c} \neq \mathfrak{p}$ . Fix an element  $v \in \Gamma_{A/K}$ . By the remark made near the beginning of Section 16, for each  $v' \in \mathcal{O}$  there exist polynomials  $P_{v'}, Q_{v'} \in L[X_1, \dots, X_n]$

with  $Q_{v'}(v) \neq 0$  such that  $\varphi(v)Q_{v'}(v) = P_{v'}(v)$ . Every zero of the ideal  $Lp + \sum_{v' \in \mathcal{C}} L[X_1, \dots, X_n]Q_{v'}$  of  $L[X_1, \dots, X_n]$  is a zero of  $c$ . Hence there is a power  $c^e$  of  $c$  with the property that if we fix a finite basis  $R_1, \dots, R_r$  of the ideal  $c^e$  of  $K[X_1, \dots, X_n]$ , then

$$R_k \equiv \sum_{1 \leq i \leq m} D_{ik} Q_{v_i} \pmod{Lp} \quad (1 \leq k \leq r)$$

for suitable elements  $v_1, \dots, v_m \in \mathcal{O}$  and polynomials  $D_{ik} \in L[X_1, \dots, X_n]$ . Then

$$\varphi(v) R_k(v) = \sum_i D_{ik}(v) \varphi(v) Q_{v_i}(v) = \sum_i D_{ik}(v) P_{v_i}(v) = S_k(v),$$

where  $S_k = \sum_i D_{ik} P_{v_i} \in L[X_1, \dots, X_n]$ . For each  $k$  we can write  $S_k = \sum_l \lambda_l S_{kl}$ , where  $S_{kl} \in K[X_1, \dots, X_n]$  ( $l \in \Lambda$ ). Then there is a unique  $\varphi_{kl} \in \mathfrak{F}_K(A)$  such that  $\varphi_{kl}(v) = S_{kl}(v)/R_k(v)$ , and evidently  $\varphi_{kl}$  is defined at every element  $v' \in A$  with  $R_k(v') \neq 0$ , and  $\varphi = \sum_l \lambda_l \varphi_{kl}$  ( $1 \leq k \leq r$ ). By part (b), for each  $l \in \Lambda$ , then  $\varphi_{1l}, \dots, \varphi_{rl}$  are one and the same  $K$ -function, which we denote by  $\varphi_l$ . Thus  $\varphi = \sum_l \lambda_l \varphi_l$ , and each  $\varphi_l$  is defined at any element  $v' \in B$  such that  $R_k(v') \neq 0$  for at least one  $k$ , so that each  $\varphi_l$  is defined on  $\mathcal{O}$ .

Next, consider the more inclusive case in which  $K = K_s$  but  $A$  need not be irreducible. Let  $V_1, \dots, V_m$  be the components of  $A$ . It is clear that for each  $i$  the  $L$ -function  $\varphi \circ \text{in}_{A, V_i}$  on  $V_i$  is defined on  $\mathcal{O} \cap V_i$ , which is  $K$ -open and dense in  $V_i$ . By the case already treated, we can write  $\varphi \circ \text{in}_{A, V_i} = \sum_l \lambda_l \varphi_{il}$  with  $\varphi_{il} \in \mathfrak{F}_{K, \mathcal{C} \cap V_i}(V_i)$  for every  $l \in \Lambda$ . For each  $l$  let  $\varphi_l$  denote the  $K$ -function on  $A$  such that  $\varphi \circ \text{in}_{A, V_i} = \varphi_{il}$  ( $1 \leq i \leq m$ ). Evidently  $\varphi = \sum_l \lambda_l \varphi_l$ . To show that each  $\varphi_l$  is defined on  $\mathcal{O}$ , consider any  $v' \in \mathcal{O}$ , and fix  $v_i \in \Gamma_{V_i/L}$  ( $1 \leq i \leq m$ ). If  $v' \in V_i$  then for each  $l \in \Lambda$ ,  $\varphi_{il}$  is defined at  $v'$ . Suppose also that  $v' \in V_{i'}$  with  $i \neq i'$ , so that also  $\varphi_{i'l}$  is defined at  $v'$  and some component  $W$  of  $V_i \cap V_{i'}$  containing  $v'$  is a  $K$ -set (and hence has an  $L$ -generic element  $w$  that is separable over  $K$ ). Because  $w \rightarrow v'$ , we have  $w \in \mathcal{O}$ ,  $\varphi_{il}$  and  $\varphi_{i'l}$  are defined at  $w$ , and  $\sum_l \lambda_l \varphi_{il}(w) = (\varphi \circ \text{in}_{A, V_i})(w) = \varphi(w) = (\varphi \circ \text{in}_{A, V_{i'}})(w) = \sum_l \lambda_l \varphi_{i'l}(w)$ . Since  $K(w)$  is separable (and hence regular) over  $K = K_s$ , and  $L$  and  $K(w)$  are evidently algebraically disjoint over  $K$ ,  $L$  and  $K(w)$  must be linearly disjoint over  $K$ , and the preceding equation shows that  $\varphi_{il}(w) = \varphi_{i'l}(w)$  for each  $l$ . Since  $\varphi_{il}$  and  $\varphi_{i'l}$  are defined at  $v'$  and since  $w \rightarrow v'$ , we infer that  $\varphi_{il}(v') = \varphi_{i'l}(v')$ . Thus the value of  $\varphi_{il}(v')$  is independent of the choice of the index  $i$  with  $v' \in V_i$ . This implies, for each  $l$ , that  $\varphi_l$  is defined at  $v'$ .

Finally, consider the general situation in which we make no special hypothesis about  $K$ . By the case we have just treated,  $\varphi$  can be expressed as a linear combination over  $LK_s$  of elements of  $\mathfrak{F}_{K_s, \mathcal{C}}(A)$ , and by Lemma 11, they in turn can be expressed as linear combinations over  $K_s$  of elements of  $\mathfrak{F}_{K, \mathcal{C}}(A)$ . It follows that if we fix elements  $\alpha_j \in K_s$  ( $j \in J$ ) such that they and 1 form a

basis of  $LK_s$  over  $L$  (and hence such that the elements  $\lambda_l$  ( $l \in \Lambda$ ) and  $\alpha_j \lambda_l$  ( $j \in J, l \in \Lambda$ ) form a basis of  $LK_s$  over  $K$ ), then there exist  $K$ -functions  $\varphi_l \in \mathfrak{F}_{K, \mathcal{C}}(A)$  ( $l \in \Lambda$ ) and  $\varphi_{jl} \in \mathfrak{F}_{K, \mathcal{C}}(A)$  ( $j \in J, l \in \Lambda$ ) such that  $\varphi = \sum_l \lambda_l \varphi_l + \sum_{j,l} \alpha_j \lambda_l \varphi_{jl}$ . Then

$$\left( \sum_l \lambda_l \varphi_l - \varphi \right) 1 + \sum_j \left( \sum_l \lambda_l \varphi_{jl} \right) \alpha_j = 0.$$

Since, by part (b), the elements 1 and  $\alpha_j$  ( $j \in J$ ) are linearly independent over  $\mathfrak{F}_L(A)$ , we conclude that  $\varphi = \sum_l \lambda_l \varphi_l$ . This completes the proof.

For an example of an algebra homomorphism  $f^*: \mathfrak{F}(B) \rightarrow \mathfrak{F}(A)$  induced by a  $K$ -mapping  $f \in \mathfrak{M}_K(A, B)$ , consider two  $K$ -subsets  $A_1$  and  $A_2$  of homogeneous  $K$ -spaces  $M_1$  and  $M_2$ , respectively. Then  $A_1 \times A_2$  is a  $K$ -subset of the homogeneous  $K$ -space  $M_1 \times M_2$ , and the two projections  $pr_h: A_1 \times A_2 \rightarrow A_h$  are  $K$ -mappings (being restrictions of the analogous projections  $M_1 \times M_2 \rightarrow M_h$ , which are  $K$ -homomorphisms). Obviously  $pr_h(\Gamma_{A_1 \times A_2/K}) = \Gamma_{A_h/K}$ , and therefore each of the induced homomorphisms  $pr_h^*: \mathfrak{F}(A_h) \rightarrow \mathfrak{F}(A_1 \times A_2)$  exists and is injective and maps  $\mathfrak{F}_K(A_h)$  into  $\mathfrak{F}_K(A_1 \times A_2)$ . The following result is analogous to Proposition 22.

**Proposition 23** *Let  $A_1$  and  $A_2$  be  $K$ -sets.*

- (a) *If  $\Sigma_h$  is a  $K$ -affine subset of  $A_h$  ( $h = 1, 2$ ), then  $\mathfrak{F}_K(A_1 \times A_2) = Q(K[pr_1^*(\mathfrak{F}_{K, \Sigma_1}(A_1)) \cup pr_2^*(\mathfrak{F}_{K, \Sigma_2}(A_2))])$ .*
- (b)  *$pr_1^*(\mathfrak{F}_K(A_1))$  and  $pr_2^*(\mathfrak{F}_K(A_2))$  are linearly disjoint over  $K$ .*
- (c) *For each  $A_h$ , let  $\mathcal{O}_h$  be a  $K$ -open dense subset of  $A_h$  that satisfies, relative to  $A_h$ , the condition in Proposition 22(c), that  $\mathcal{O}$  satisfies relative to  $A$ . Then*

$$\mathfrak{F}_{K, \mathcal{C}_1 \times \mathcal{C}_2}(A_1 \times A_2) = K[pr_1^*(\mathfrak{F}_{K, \mathcal{C}_1}(A_1)) \cup pr_2^*(\mathfrak{F}_{K, \mathcal{C}_2}(A_2))].$$

*Proof* (b) Let  $\psi_1, \dots, \psi_n \in \mathfrak{F}_K(A_2)$  and suppose that  $pr_2^*(\psi_1), \dots, pr_2^*(\psi_n)$  are linearly dependent over  $pr_1^*(\mathfrak{F}_K(A_1))$ ; that is, that there exist  $\varphi_1, \dots, \varphi_n \in \mathfrak{F}_K(A_1)$  not all 0 such that  $\sum pr_1^*(\varphi_j) pr_2^*(\psi_j) = 0$ . Fixing  $v \in \Gamma_{A_1/K}$  such that  $\varphi_j(v) \neq 0$  for some  $j$ , we see for any  $w \in \Gamma_{A_2/K(v)}$  that each  $pr_1^*(\varphi_j) pr_2^*(\psi_j)$  is defined at  $(v, w)$  and its value there is  $\varphi_j(v) \psi_j(w)$ , so that  $\sum \varphi_j(v) \psi_j(w) = 0$ , whence  $\sum \varphi_j(v) \psi_j = 0$ . Thus,  $\psi_1, \dots, \psi_n$  are linearly dependent over  $K(v)$ . By Proposition 22(b), they are linearly dependent over  $K$ , so that  $pr_2^*(\psi_1), \dots, pr_2^*(\psi_n)$  are too.

(c) Fix a basis  $(\varphi_i)_{i \in I}$  of  $\mathfrak{F}_K(A_1)$  over  $K$  such that, for some subset  $I'$  of  $I$ ,  $(\varphi_i)_{i \in I'}$  is a basis of  $\mathfrak{F}_{K, \mathcal{O}_1}(A_1)$  over  $K$ , and fix a basis  $(\psi_j)_{j \in J}$  of  $\mathfrak{F}_K(A_2)$  over  $K$  such that, for some subset  $J'$  of  $J$ ,  $(\psi_j)_{j \in J'}$  is a basis of  $\mathfrak{F}_{K, \mathcal{O}_2}(A_2)$ . Consider any  $\zeta \in \mathfrak{F}_{K, \mathcal{O}_1 \times \mathcal{O}_2}(A_1 \times A_2)$ . It follows from part (b) and the fact that  $pr_h^*$  maps  $\mathfrak{F}_K(A_h)$  injectively into  $\mathfrak{F}_K(A_1 \times A_2)$  ( $h = 1, 2$ ) that if there

exist  $a_{ij} \in K$  ( $i \in I, j \in J$ ) such that  $\zeta = \sum_{i \in I, j \in J} a_{ij} pr_1^*(\varphi_i) pr_2^*(\psi_j)$ , then  $(a_{ij})_{i \in I, j \in J}$  is unique. It suffices to show that the elements  $a_{ij}$  exist and that  $a_{ij} = 0$  whenever  $i \notin I'$  or  $j \notin J'$ .

Let  $V_1, \dots, V_r$  be the components of  $A_1$ . For each  $V_l$ , fix  $v_l \in \Gamma_{V_l/K}$  and let  $k_l$  denote the constant mapping  $A_2 \rightarrow A_1$  with value  $v_l$ . Then  $k_l \times id_{A_2} \in \mathfrak{M}_{K(v_l), A_2}(A_2, A_1 \times A_2)$ .  $\zeta \circ (k_l \times id_{A_2})$  exists and is in  $\mathfrak{F}_{K(v_l), \theta_2}(A_2)$ , and for each  $w \in \mathcal{O}_2$ ,  $(\zeta \circ (k_l \times id_{A_2}))(w) = \zeta(v_l, w)$ . By Proposition 22(c), there exist  $\beta_{lj} \in K(v_l)$  ( $j \in J'$ ) such that  $\zeta \circ (k_l \times id_{A_2}) = \sum_{j \in J'} \beta_{lj} \psi_j$ . For each  $j \in J'$ , there exists an  $\eta_j \in \mathfrak{F}_K(A_1)$  such that  $\eta_j(v_l) = \beta_{lj}$  ( $1 \leq l \leq r$ ). For each  $j \in J - J'$ , set  $\eta_j = 0$ . There exist unique  $a_{ij} \in K$  ( $i \in I, j \in J$ ) such that  $\eta_j = \sum_{i \in I} a_{ij} \varphi_i$  ( $j \in J$ ). Thus  $\zeta(v_l, w) = \sum_{j \in J'} \beta_{lj} \psi_j(w) = \sum_{j \in J} \eta_j(v_l) \psi_j(w) = \sum_{i \in I, j \in J} a_{ij} \varphi_i(v_l) \psi_j(w)$  ( $1 \leq l \leq r, w \in \Gamma_{A_2/K}$ ), so that

$$\zeta = \sum_{i \in I, j \in J} a_{ij} pr_1^*(\varphi_i) pr_2^*(\psi_j).$$

Therefore the elements  $a_{ij}$  exist. Because  $\eta_j = 0$  whenever  $j \notin J'$ , we see that  $a_{ij} = 0$  whenever  $j \notin J'$ . Interchanging  $A_1$  and  $A_2$ , we see that  $a_{ij} = 0$  whenever  $i \notin I'$ .

(a) Fix a  $K$ -affine  $K$ -open dense subset  $\mathcal{O}_h$  of  $A_h$  with  $\Sigma_h \subset \mathcal{O}_h$ . By Proposition 22(a),  $\mathfrak{F}_K(A_1 \times A_2) = \mathcal{Q}(\mathfrak{F}_{K, \sigma_1 \times \sigma_2}(A_1 \times A_2))$ , and evidently

$$\begin{aligned} & \mathcal{Q}(K[pr_1^*(\mathfrak{F}_{K, \Sigma_1}(A_1)) \cup pr_2^*(\mathfrak{F}_{K, \Sigma_2}(A_2))]) \\ &= \mathcal{Q}(K[pr_1^*(\mathfrak{F}_{K, \sigma_1}(A_1)) \cup pr_2^*(\mathfrak{F}_{K, \sigma_2}(A_2))]). \end{aligned}$$

Hence we can apply part (c).—

**Corollary** Let  $M$  be a homogeneous  $K$ -space for a  $K$ -group  $G$ , and let  $\Phi$  be a finite subset of  $\mathfrak{F}_{K, M}(M)$ . Then there exist finitely many elements  $\varphi_1, \dots, \varphi_n \in \mathfrak{F}_{K, M}(M)$  with the following properties: (a)  $\Phi \subset \sum K\varphi_j$ . (b)  $\varphi_1, \dots, \varphi_n$  are linearly independent over  $U$ . (c) There exist elements  $\psi_{jj'} \in \mathfrak{F}_{K, G}(G)$  ( $1 \leq j \leq n, 1 \leq j' \leq n$ ) such that  $\rho_x^*(\varphi_{j'}) = \sum_{1 \leq j \leq n} \psi_{jj'}(x) \varphi_j$  ( $1 \leq j' \leq n, x \in G$ ) and the formula  $x \mapsto (\psi_{jj'}(x))$  defines a  $K$ -homomorphism  $G \rightarrow \mathbf{GL}(n)$ .

*Proof* The homogeneous space law  $\mu_M : M \times G \rightarrow M$  is in

$$\mathfrak{M}_{K, M \times G}(M \times G, M),$$

so that  $\xi \circ \mu_M \in \mathfrak{F}_{K, M \times G}(M \times G)$  for every  $\xi \in \Phi$ . Hence, by part (c) of the proposition, there exist elements  $\varphi_1, \dots, \varphi_n \in \mathfrak{F}_{K, M}(M)$  and, for each  $\xi \in \Phi$ , elements  $\psi_{1\xi}, \dots, \psi_{n\xi} \in \mathfrak{F}_{K, G}(G)$  such that

$$\xi \circ \mu_M = \sum pr_1^*(\varphi_j) pr_2^*(\psi_{j\xi}) \quad (\xi \in \Phi).$$

Taking  $n$  minimal, we see that  $\varphi_1, \dots, \varphi_n$  are linearly independent over  $K$  (and hence over  $U$ ), and that  $(\psi_{1\xi})_{\xi \in \Phi}, \dots, (\psi_{n\xi})_{\xi \in \Phi}$  are, too. Obviously

$\rho_x^*(\xi) = \sum \varphi_j \psi_{j\xi}(x)$  ( $\xi \in \Phi, x \in G$ ). Of course, we have a similar result for the finite set of  $K$ -functions  $\varphi_1, \dots, \varphi_n$  instead of  $\Phi$ . Therefore there exist elements  $\varphi_1', \dots, \varphi_r' \in \mathfrak{F}_{K, M}(M)$ , with  $\varphi_1, \dots, \varphi_n, \varphi_1', \dots, \varphi_r'$  linearly independent over  $U$ , and elements  $\psi_{jj'}, \psi'_{kj'} \in \mathfrak{F}_{K, G}(G)$  ( $1 \leq j \leq n, 1 \leq j' \leq n, 1 \leq k \leq r$ ) such that  $\rho_x^*(\varphi_{j'}) = \sum_j \varphi_j \psi_{jj'}(x) + \sum_k \varphi_k' \psi'_{kj'}(x)$  ( $1 \leq j' \leq n, x \in G$ ). The computation

$$\begin{aligned} \sum_j \varphi_j \psi_{j\xi}(xy) &= \rho_{xy}^*(\xi) = \rho_x^*(\rho_y^*(\xi)) \\ &= \rho_x^*\left(\sum_{j'} \varphi_{j'} \psi_{j'\xi}(y)\right) \\ &= \sum_j \varphi_j \sum_{j'} \psi_{jj'}(x) \psi_{j'\xi}(y) + \sum_k \varphi_k' \sum_{j'} \psi'_{kj'}(x) \psi_{j'\xi}(y) \end{aligned}$$

shows that  $\sum_{j'} \psi'_{kj'}(x) \psi_{j'\xi}(y) = 0$  ( $x \in G, y \in G, \xi \in \Phi, 1 \leq k \leq r$ ), whence  $\sum_{j'} \psi'_{kj'}(x) \psi_{j'\xi} = 0$  ( $x \in G, \xi \in \Phi, 1 \leq k \leq r$ ). Since  $(\psi_{1\xi})_{\xi \in \Phi}, \dots, (\psi_{n\xi})_{\xi \in \Phi}$  are linearly independent over  $U$ , we infer that  $\psi'_{kj'}(x) = 0$  ( $x \in G, 1 \leq k \leq r, 1 \leq j' \leq n$ ). Therefore  $\rho_x^*(\varphi_{j'}) = \sum_j \varphi_j \psi_{jj'}(x)$  ( $1 \leq j' \leq n, x \in G$ ) and the above computation shows that the formula  $x \mapsto (\psi_{jj'}(x))$  defines a  $K$ -homomorphism  $G \rightarrow \mathbf{GL}(n)$ .

## EXERCISES

- Let  $x \in U$  be transcendental over  $K$ , let  $V_1$  be the locus over  $K$  of  $(x, x^2)$  in  $\mathbf{G}_a^2$ , let  $V_2$  be the locus over  $K$  of  $(x, 0)$ , and set  $A = V_1 \cup V_2$ . Let  $\varphi$  denote the  $K$ -function on  $A$  such that  $\varphi(x, x^2) = x$  and  $\varphi(x, 0) = 0$ . Prove that  $\varphi$  is defined at  $(0, 0)$ , but that there do not exist polynomials  $P, Q \in K[X, Y]$  with  $Q(0, 0) \neq 0$  such that  $P(x, x^2)/Q(x, x^2) = x$  and  $P(x, 0)/Q(x, 0) = 0$ .
- Let  $A$  be a  $K$ -subset of a homogeneous  $K$ -space  $M$ , let  $v \in A$ , and let  $\varphi \in \mathfrak{F}_K(A)$ . Call a  $K$ -subset  $A'$  of  $M$   $A$ -special if  $A \subset A'$  and the components of  $A'$  are pairwise disjoint. (Thus,  $M$  is  $A$ -special.)
  - Show that if  $\varphi$  is defined at  $v$  and some  $A$ -special  $K$ -subset  $A'$  of  $M$  has the property that there exists a  $\varphi' \in \mathfrak{F}_{K, v}(A')$  such that  $\varphi' \circ in_{A', A}$  exists and equals  $\varphi$ , then every  $A$ -special  $K$ -subset of  $M$  has this property. (*Hint*: Show that if  $A'$  is  $A$ -special, then  $A'$  has the property if and only if  $M$  has.)
  - Show that if  $v$  is contained in only one component of  $A$  and  $\varphi$  is defined at  $v$ , then  $M$  has the property described in part (a).

Call the  $K$ -function  $\varphi$  on  $A$  *holomorphic at  $v$*  if  $\varphi$  is defined at  $v$  and some (hence every)  $A$ -special  $K$ -subset of  $M$  has the property described in part (a).

- (c) Show that if  $\xi \in \mathfrak{F}_K(\mathbf{G}_a)$ , then there exist unique polynomials  $P, Q \in K[X]$  with  $Q \neq 0$ ,  $Q$  unitary,  $P$  and  $Q$  relatively prime, and  $\xi(x) = P(x)/Q(x)$  ( $x \in \Gamma_{\mathbf{G}_a/K}$ ), and then show that for an element  $x_0 \in \mathbf{G}_a$  the following three conditions are equivalent: (i)  $\xi$  is defined at  $x_0$ ; (ii)  $\xi$  is holomorphic at  $x_0$ ; (iii)  $Q(x_0) \neq 0$ .
- (d) Show that  $\varphi$  is holomorphic at  $v$  if and only if  $\varphi$  is defined at  $v$  and, for every  $\xi \in \mathfrak{F}_K(\mathbf{G}_a)$  that is holomorphic at  $\varphi(v)$ ,  $\xi \circ \varphi$  is holomorphic at  $v$ .

If  $B$  is a  $K$ -set, call a  $K$ -mapping  $f \in \mathfrak{M}_K(A, B)$  *holomorphic at  $v$*  when  $f$  is defined at  $v$  and, for every  $\psi \in \mathfrak{F}_K(B)$  such that  $\psi$  is holomorphic at  $f(v)$  and  $\psi \circ f$  exists,  $\psi \circ f$  is holomorphic at  $v$ ; call the set of all elements of  $A$  at which  $f$  is holomorphic the *domain of holomorphicity* of  $f$ .

- (e) Show that the domain of holomorphicity of any  $f \in \mathfrak{M}_K(A, B)$  is  $K$ -open and dense in  $A$ .
3. Let  $G$  be a connected  $K$ -group and let  $L$  be an extension of  $K$  (over which the transcendence degree of  $U$  need not be infinite). Prove that any derivation  $\delta$  of  $L$  over  $K$  can be extended to a unique derivation  $\delta^*$  of  $\mathfrak{F}_L(G)$  over  $\mathfrak{F}_K(G)$ , and show that if  $K' = \text{Ker}(\delta)$ , then  $\mathfrak{F}_{K'}(G) = \text{Ker}(\delta^*)$ . Show that the formula  $\delta \mapsto \delta^*$  defines an injective homomorphism  $\text{Der}(L/K) \rightarrow \text{Der}(\mathfrak{F}_L(G)/\mathfrak{F}_K(G))$  of Lie rings and of vector spaces over  $L$ . Show that if  $z \in G_{K'}$  and  $\varphi \in \mathfrak{F}_{L,z}(G)$ , then  $\delta^*\varphi \in \mathfrak{F}_{L,z}(G)$  and  $(\delta^*\varphi)(z) = \delta(\varphi(z))$ .

17 *K*-Cohomology

Let  $A$  be a  $K$ -set and let  $G$  be a  $K$ -group. A *one-dimensional  $K$ -cocycle* (or simply a *one- $K$ -cocycle*, or even, when there is no danger of confusion, a  *$K$ -cocycle*) of  $A$  into  $G$  is defined as a  $K$ -mapping  $f \in \mathfrak{M}_K(A^2, G)$  such that

$$f(u, w) = f(u, v)f(v, w)$$

for all  $(u, v, w) \in \Gamma_{A^2/K}$ . Of course, if  $f$  is such a  $K$ -cocycle, then the above equation holds for all  $(u, v, w) \in A^3$  such that  $f$  is defined at  $(u, v)$ ,  $(v, w)$ , and  $(u, w)$ . It is clear, moreover, that if the  $K$ -cocycle  $f$  is defined at any two of these elements of  $A^2$ , then  $f$  is defined at all three. The set of all one- $K$ -cocycles of  $A$  into  $G$  is denoted by  $Z_K^1(A, G)$ .

An example is given by the constant mapping  $A^2 \rightarrow G$  with value 1. This is the *trivial  $K$ -cocycle* and is denoted by 1. (When  $G$  is commutative and written additively, the trivial cocycle is the constant mapping with value 0, and is denoted by 0, of course.) More generally, for any  $K$ -mapping  $h \in \mathfrak{M}_K(A, G)$ , the  $K$ -mapping  $\delta h \in \mathfrak{M}_K(A^2, G)$  such that

$$\delta h(v, w) = h(v)^{-1}h(w)$$

for all  $(v, w) \in \Gamma_{A^2/K}$ , is obviously an element of  $Z_K^1(A, G)$ . The  $K$ -cocycles of this type are called *one-dimensional  $K$ -coboundaries of  $A$  into  $G$* , and the set of all of them is denoted by  $B_K^1(A, G)$ .

If  $f_1, f_2 \in Z_K^1(A, G)$  and if there exists an  $h \in \mathfrak{M}_K(A, G)$  such that

$$f_2(v, w) = h(v)^{-1}f_1(v, w)h(w)$$

for all  $(v, w) \in \Gamma_{A^2/K}$ , then  $f_2$  is said to be  *$K$ -cohomologous* to  $f_1$ . The relation “ $f_2$  is  $K$ -cohomologous to  $f_1$ ” is an equivalence on  $Z_K^1(A, G)$ . The set of equivalence classes (called  *$K$ -cohomology classes*) is called the *one-dimensional  $K$ -cohomology set of  $A$  into  $G$*  and is denoted by  $H_K^1(A, G)$ . It is clear that  $B_K^1(A, G)$  is the set of  $K$ -cocycles that are  $K$ -cohomologous to 1, so that  $B_K^1(A, G)$  is an element of  $H_K^1(A, G)$ . As such, it is denoted by 1 (or by 0 when  $G$  is commutative and written additively). Thus,  $Z_K^1(A, G)$ ,  $B_K^1(A, G)$ ,  $H_K^1(A, G)$  each has a natural structure of pointed set, and the canonical mapping  $Z_K^1(A, G) \rightarrow H_K^1(A, G)$ , that sends each element of  $Z_K^1(A, G)$  to its  $K$ -cohomology class, is a homomorphism of pointed sets with kernel  $B_K^1(A, G)$  (see Section 12 for the relevant definitions).

When the  $K$ -group  $G$  is commutative, then  $Z_K^1(A, G)$  is a commutative group (subgroup of the group  $\mathfrak{M}_K(A^2, G)$ ),  $B_K^1(A, G)$  is a subgroup of  $Z_K^1(A, G)$ , and  $H_K^1(A, G)$  is the quotient group  $Z_K^1(A, G)/B_K^1(A, G)$ .

**Proposition 24** *Let  $A$  be a  $K$ -set, let  $G$  be a  $K$ -group, and let  $f \in Z_K^1(A, G)$ .*

(a) *There exists a  $K$ -open dense subset  $P_f$  of  $A$  such that  $P_f^2$  is the domain of definition of  $f$ .*

(b) *If  $u, v \in P_f$ , then  $f(u, u) = 1$  and  $f(v, u) = f(u, v)^{-1}$ .*

*Proof* (a) Let  $D$  denote the domain of definition of  $f$ , so that  $D \subset A^2 = A \times A$ . If  $v \in pr_2(D)$ , then there exists an element  $u \in A$  with  $(u, v) \in D$ . Setting  $w = v$ , we see that  $f$  is defined at  $(u, v)$  and  $(u, w)$ , and hence is defined at  $(v, w)$ , so that  $v \in pr_1(D)$  and  $(v, v) \in D$ . A similar argument shows that if  $v \in pr_1(D)$ , then  $v \in pr_2(D)$ . Let  $P_f = pr_1(D) = pr_2(D)$ . Then  $P_f^2 = D$ . Therefore (by Section 15, Proposition 15(a))  $P_f^2$  is  $K$ -open in  $A^2$ . The diagonal  $\Delta_A$  of  $A \times A$  is evidently a  $K$ -subset of  $A^2$ , and the formula  $(v, v) \mapsto v$  gives an everywhere bidefined generically invertible  $K$ -mapping of  $\Delta_A$  into  $A$  (with everywhere bidefined generic inverse given by the formula  $v \mapsto (v, v)$ ). Since this mapping carries the  $K$ -open subset  $P_f^2 \cap \Delta_A$  of  $\Delta_A$  onto the subset of  $P_f$  of  $A$ ,  $P_f$  must be  $K$ -open in  $A$ . Finally, for any  $v \in \Gamma_{A/K}$ , there exists an element  $w \in A$  such that  $(v, w) \in \Gamma_{A^2/K}$  and hence such that  $(v, w) \in D$ , so that  $v \in P_f$ . Therefore  $P_f$  is dense in  $A$ .

(b) Since  $f(u, v)f(v, w) = f(u, w)$  whenever  $f$  is defined at  $(u, v)$ ,  $(v, w)$ , and  $(u, w)$ , when  $u \in P_f$  we can write  $f(u, u)f(u, u) = f(u, u)$  so that  $f(u, u) = 1$ , and when  $u, v \in P_f$  we can write  $f(u, v)f(v, u) = f(u, u) = 1$  so that  $f(v, u) = f(u, v)^{-1}$ .

The following theorem gives Serre's method of injecting  $H_K^1(A, G)$  into the Galois cohomology set  $H^1(K, G)$  defined in Section 12 (see Corollary 1 below).

**Theorem 12** *Let  $A$  be a  $K$ -set and let  $G$  be a  $K$ -group.*

(a) *For every pair  $(f, u)$  such that  $f \in Z_K^1(A, G)$  and  $u \in P_f \cap A_{K_s}$ , there exists an  $f_u \in Z^1(K, G)$  such that  $f_u(\gamma) = f(u, \gamma u)$  ( $\gamma \in \mathfrak{g}(K_s/K)$ ).*

(b) *For two such pairs  $(f, u)$  and  $(f', u')$ ,  $f$  is  $K$ -cohomologous to  $f'$  if and only if  $f_u$  is cohomologous to  $f'_{u'}$ .*

*Proof* (a) Let  $f_u$  denote the mapping of  $\mathfrak{g}(K_s/K)$  into  $G$  defined by the formula  $f_u(\gamma) = f(u, \gamma u)$ . For any  $\gamma, \gamma' \in \mathfrak{g}(K_s/K)$ ,

$$\begin{aligned} f_u(\gamma\gamma') &= f(u, \gamma\gamma'u) = f(u, \gamma u)f(\gamma u, \gamma\gamma'u) \\ &= f(u, \gamma u)\gamma(f(u, \gamma'u)) = f_u(\gamma)\gamma(f_u(\gamma')). \end{aligned}$$

If  $E$  is the Galois extension of  $K$  generated by  $K(u)$ , then  $\gamma\mathfrak{g}(K_s/E)$  is a neighborhood of  $\gamma$ , and for any  $\gamma' \in \mathfrak{g}(K_s/E)$ ,

$$f_u(\gamma\gamma') = f_u(\gamma)\gamma(f_u(\gamma')) = f_u(\gamma)\gamma(f(u, \gamma'u)) = f_u(\gamma)\gamma(f(u, u)) = f_u(\gamma)$$

by Proposition 24(b). Therefore  $f_u$  is continuous, so that  $f_u \in Z^1(K, G)$ .

(b) If  $f$  is  $K$ -cohomologous to  $f'$ , there exists an  $h \in \mathfrak{M}_K(A, G)$  such that  $f'(v, w) = h(v)^{-1}f(v, w)h(w)$  whenever  $v, w \in \Gamma_{A/K}$ . Fix an element  $u'' \in P_f \cap P_{f'} \cap A_{K_s}$  at which  $h$  is defined. Then, for any  $\gamma \in \mathfrak{g}(K_s/K)$ ,

$$\begin{aligned} f'_{u'}(\gamma) &= f'(u', \gamma u') \\ &= f'(u', u'')f'(u'', \gamma u'')f'(\gamma u'', \gamma u') \\ &= f'(u', u'')h(u'')^{-1}f(u'', \gamma u'')h(\gamma u'')f'(\gamma u'', \gamma u') \\ &= f'(u', u'')h(u'')^{-1}f(u'', u)f(u, \gamma u)f(\gamma u, \gamma u'')h(\gamma u'')f'(\gamma u'', \gamma u') \\ &= x^{-1}f(u, \gamma x)\gamma u = x^{-1}f_u(\gamma)\gamma x, \end{aligned}$$

where  $x = f(u, u'')h(u'')f'(u'', u) \in G_{K_s}$ . Therefore  $f_u$  is cohomologous to  $f'_{u'}$ .

Conversely, let  $f_u$  be cohomologous to  $f'_{u'}$ , and fix  $x \in G_{K_s}$  such that  $f'_{u'}(\gamma) = x^{-1}f_u(\gamma)\gamma x$  ( $\gamma \in \mathfrak{g}(K_s/K)$ ). Then, for any  $v, w \in \Gamma_{A/K}$  and any  $\gamma \in \mathfrak{g}(K_s/K)$ ,

$$\begin{aligned} f'(v, w) &= f'(v, u')f'(u', \gamma u')f'(\gamma u', w) \\ &= f'(v, u')f'_{u'}(\gamma)f'(\gamma u', w) \\ &= f'(v, u')x^{-1}f_u(\gamma)\gamma x f'(\gamma u', w) \\ &= f'(v, u')x^{-1}f(u, \gamma u)\gamma x f'(\gamma u', w) \\ &= f'(v, u')x^{-1}f(u, v)f(v, w)f(w, \gamma u)\gamma x f'(\gamma u', w) \\ &= (f(v, u)xf'(u', v))^{-1}f(v, w)(f(w, \gamma u)\gamma x f'(\gamma u', w)). \end{aligned}$$

When  $w = v$  this shows that  $f(v, \gamma u)\gamma x f'(\gamma u', v) = f(v, u)xf'(u', v)$ , and hence that the element  $f(v, u)xf'(u', v)$  of  $G_{K_s(v)}$  is invariant under every automorphism of  $K_s(v)$  over  $K(v)$ , so that  $f(v, u)xf'(u', v) \in G_{K(v)}$ . Since then  $\sigma(f(v, u)xf'(u', v)) = f(\sigma v, \sigma u)\sigma x f'(\sigma u', \sigma v) = f(\sigma v, u)xf'(u', \sigma v)$  for every  $\sigma \in \text{Aut}(U/K)$ , it follows that there exists an  $h \in \mathfrak{M}_K(A, G)$  such that  $h(v) = f(v, u)xf'(u', v)$  whenever  $v \in \Gamma_{A/K}$ , and that for this  $h$ ,  $h(v) = f(v, \gamma u)\gamma x f'(\gamma u', v)$  for any  $\gamma \in \mathfrak{g}(K_s/K)$ . Therefore  $f'(v, w) = h(v)^{-1}f(v, w)h(w)$  whenever  $v, w \in \Gamma_{A/K}$ , and  $f$  is  $K$ -cohomologous to  $f'$ .

**Corollary 1** *There exists an injection  $H_K^1(A, G) \rightarrow H^1(K, G)$  that, for each  $f \in Z_K^1(A, G)$  and any  $u \in P_f \cap A_{K_s}$ , sends the  $K$ -cohomology class of  $f$  to the cohomology class of  $f_u$ . This injection is a homomorphism of pointed sets, and when  $G$  is commutative is a group homomorphism.*

*Proof* This is now clear.

For any principal homogeneous  $K$ -space  $M$  for  $G$  and any  $K$ -mapping  $h \in \mathfrak{M}_K(A, M)$ , there exists a unique  $K$ -mapping  $\delta h \in \mathfrak{M}_K(A^2, G)$  such that  $(\delta h)(v, w) = h(v)^{-1}h(w)$  for all  $(v, w) \in \Gamma_{A^2/K}$ , and obviously  $\delta h \in Z_K^1(A, G)$ . Given  $A, G, M$  and  $f \in Z_K^1(A, G)$ , if there exists an  $h \in \mathfrak{M}_K(A^2, M)$  such that  $f = \delta h$ , then we say that  $f$   $K$ -splits in  $M$ . In particular,  $f$   $K$ -splits in  $G$  precisely when  $f$  is a  $K$ -coboundary.

**Corollary 2** *Let  $(f, u)$  be a pair as in Theorem 12(a), and let  $M$  be a principal homogeneous  $K$ -space for  $G$ . Then  $f$   $K$ -splits in  $M$  if and only if  $f_u$  splits in  $M$ .*

*Proof* If  $f$   $K$ -splits in  $M$ , then  $f(w_1, w_2) = h(w_1)^{-1}h(w_2)$  ( $w_1, w_2 \in \Gamma_{A/K}$ ), where  $h \in \mathfrak{M}_K(A, M)$ , and we can fix an element  $u' \in P_f \cap A_{K_s}$  at which  $h$  is defined. For any  $\gamma \in \mathfrak{g}(K_s/K)$ ,

$$\begin{aligned} f_u(\gamma) &= f(u, \gamma u) = f(u, u')f(u', \gamma u')f(\gamma u', \gamma u) \\ &= f(u, u') \cdot h(u')^{-1}h(\gamma u') \cdot f(\gamma u', \gamma u) = v^{-1}\gamma v, \end{aligned}$$

where  $v = h(u')f(u', u) \in M_{K_s}$ , and therefore (see Section 13, the remark right after Theorem 10)  $f_u$  splits in  $M$ . Conversely, suppose that  $f_u$  splits in  $M$  and fix  $v \in M_{K_s}$  such that  $f_u(\gamma) = v^{-1}\gamma v$  ( $\gamma \in \mathfrak{g}(K_s/K)$ ). For any  $w_1, w_2 \in \Gamma_{A/K}$  and any  $\gamma \in \mathfrak{g}(K_s/K)$ ,

$$\begin{aligned} f(w_1, w_2) &= f(w_1, u)f(u, \gamma u)f(\gamma u, w_2) = f(w_1, u)f_u(\gamma)f(\gamma u, w_2) \\ &= f(w_1, u)(v^{-1}\gamma v)f(\gamma u, w_2) = (vf(u, w_1))^{-1}(\gamma v \cdot f(\gamma u, w_2)). \end{aligned}$$

When  $w_2 = w_1$ , this shows that  $\gamma v \cdot f(\gamma u, w) = vf(u, w)$  for every  $w \in \Gamma_{A/K}$  and hence that the element  $vf(u, w) \in M_{K_s(w)}$  is invariant under the Galois group  $\mathfrak{g}(K_s(w)/K(w))$ , so that  $vf(u, w) \in M_{K(w)}$ . Since  $\sigma(vf(u, w)) = \sigma v \cdot f(\sigma u, \sigma w) =$

$vf(u, \sigma w)$  for every  $\sigma \in \text{Aut}(U/K)$ , it follows that there exists an  $h \in \mathfrak{M}_K(A, M)$  such that  $h(w) = vf(u, w)$  for every  $w \in \Gamma_{A/K}$ , and that for this  $h$ ,  $h(w) = \gamma v \cdot f(\gamma u, w)$  for every  $\gamma \in \mathfrak{g}(K_s/K)$  and every  $w \in \Gamma_{A/K}$ . Then  $f(w_1, w_2) = h(w_1)^{-1}h(w_2)$ , so that  $f$   $K$ -splits in  $M$ .

**Corollary 3** Let  $F \in \mathfrak{M}_K(B, A)$  be a generically invertible  $K$ -mapping of  $K$ -sets and let  $F_2$  denote the induced element of  $\mathfrak{M}_K(B^2, A^2)$ , that is,  $F_2 = (F \circ pr_1) \times (F \circ pr_2)$ .

(a) The formula  $f \mapsto f \circ F_2$  defines a bijection  $Z_K^1(A, G) \rightarrow Z_K^1(B, G)$  that induces an isomorphism  $F^1 : H_K^1(A, G) \rightarrow H_K^1(B, G)$  of pointed sets (and of  $K$ -groups when  $G$  is commutative).

(b) The diagram

$$\begin{array}{ccc} H_K^1(A, G) & \xrightarrow{F^1} & H_K^1(B, G) \\ & \searrow & \swarrow \\ & H^1(K, G) & \end{array}$$

(in which the arrows other than  $F^1$  denote the injections that exist in accordance with Corollary 1) is commutative.

*Proof* Straightforward.

**18 Invariant derivations and differentials. The Lie algebra**

Let  $V$  be an irreducible  $K$ -set. As we saw in Section 16,  $\mathfrak{F}(V)$  is a field of which  $U$  and  $\mathfrak{F}_K(V)$  are subfields, and  $\mathfrak{F}_K(V)$  is a finitely generated regular extension of  $K$ . By Proposition 22,  $\mathfrak{F}_K(V)$  and  $U$  are linearly disjoint over  $K$  and their compositum is  $\mathfrak{F}(V)$ .

A derivation of  $\mathfrak{F}(V)$  over  $U$  (that is, a derivation of the field  $\mathfrak{F}(V)$  that is trivial on  $U$ ) is called a *derivation on  $V$* . We denote the set of all derivations on  $V$  by  $\mathfrak{D}(V)$ . If  $D_1, D_2$  are derivations on  $V$ , then so are  $D_1 + D_2, \varphi D_1$  ( $\varphi \in \mathfrak{F}(V)$ ), and the commutator  $[D_1, D_2] = D_1 D_2 - D_2 D_1$ . Also,  $[D_1, \alpha D_2] = \alpha [D_1, D_2]$  ( $\alpha \in U$ ). Thus,  $\mathfrak{D}(V)$  has natural structures of vector space over  $\mathfrak{F}(V)$  and Lie algebra over  $U$ . When  $p \neq 0$ , if  $D \in \mathfrak{D}(V)$ , then  $D^p \in \mathfrak{D}(V)$ .

By a  $K$ -*derivation on  $V$*  we mean a derivation  $D \in \mathfrak{D}(V)$  such that  $D(\mathfrak{F}_K(V)) \subset \mathfrak{F}_K(V)$ . The set  $\mathfrak{D}_K(V)$  of all  $K$ -derivations on  $V$  is a vector space over  $\mathfrak{F}_K(V)$  and a Lie algebra over  $K$ . If  $D \in \mathfrak{D}_K(V)$ , the restriction of  $D$  to  $\mathfrak{F}_K(V)$  is a derivation of this field over  $K$ . The mapping, that to each such  $D$  associates its restriction to  $\mathfrak{F}_K(V)$ , is an isomorphism (of vector

spaces over  $\mathfrak{F}_K(V)$  as well as of Lie algebras over  $K$ ) of  $\mathfrak{D}_K(V)$  onto the vector space and Lie algebra of derivations of  $\mathfrak{F}_K(V)$  over  $K$ . This isomorphism provides a canonical identification of  $\mathfrak{D}_K(V)$  with this vector space and Lie algebra. If  $(\xi_1, \dots, \xi_n)$  is a separating transcendence basis of  $\mathfrak{F}_K(V)$  over  $K$  (and therefore also of  $\mathfrak{F}(V)$  over  $U$ ), then  $n = \dim V$  and  $(\partial/\partial \xi_1, \dots, \partial/\partial \xi_n)$  is a basis of the vector space  $\mathfrak{D}_K(V)$  (and also of the vector space  $\mathfrak{D}(V)$ ). It follows that  $\mathfrak{F}(V)$  and  $\mathfrak{D}_K(V)$  are linearly disjoint over  $\mathfrak{F}_K(V)$  and  $\mathfrak{F}_L(V) \cdot \mathfrak{D}_K(V) = \mathfrak{D}_L(V)$  for every extension  $L$  of  $K$ .

The elements of the vector space  $\mathfrak{D}^*(V)$  dual to  $\mathfrak{D}(V)$  are called *differentials on  $V$* . Thus, a differential on  $V$  is a linear form on  $\mathfrak{D}(V)$ . We often denote the value of a differential  $\omega$  on  $V$  at the derivation  $D$  on  $V$  by  $\langle D, \omega \rangle$ . By a  $K$ -*differential on  $V$*  we mean a differential  $\omega \in \mathfrak{D}^*(V)$  such that  $\langle D, \omega \rangle \in \mathfrak{F}_K(V)$  for every  $D \in \mathfrak{D}_K(V)$ . The set of  $K$ -differentials on  $V$  is a vector space over  $\mathfrak{F}_K(V)$  that we denote by  $\mathfrak{D}_K^*(V)$ . The mapping that to each  $\omega \in \mathfrak{D}_K^*(V)$  associates its restriction to  $\mathfrak{D}_K(V)$  is an isomorphism of  $\mathfrak{D}_K^*(V)$  onto the vector space dual to  $\mathfrak{D}_K(V)$ , and provides a canonical identification of  $\mathfrak{D}_K^*(V)$  with this dual.

For any  $U$ -function  $\varphi \in \mathfrak{F}(V)$ , the formula  $D \mapsto D\varphi$  ( $D \in \mathfrak{D}(V)$ ) defines a differential on  $V$ ; it is called the *differential of  $\varphi$*  and is denoted by  $d\varphi$ . Thus,  $d\varphi$  is characterized by the equation

$$\langle D, d\varphi \rangle = D\varphi.$$

When  $\varphi \in \mathfrak{F}_K(V)$ , then  $d\varphi \in \mathfrak{D}_K^*(V)$ . It is easy to see that if  $(\xi_1, \dots, \xi_n)$  is a separating transcendence basis of  $\mathfrak{F}_K(V)$  over  $K$ , then  $(d\xi_1, \dots, d\xi_n)$  is the basis of  $\mathfrak{D}_K^*(V)$  (and of  $\mathfrak{D}_K(V)$ ) dual to the basis  $(\partial/\partial \xi_1, \dots, \partial/\partial \xi_n)$  of  $\mathfrak{D}_K(V)$  (and of  $\mathfrak{D}(V)$ ). Hence  $\mathfrak{F}(V)$  and  $\mathfrak{D}_K^*(V)$  are linearly disjoint over  $\mathfrak{F}_K(V)$  and  $\mathfrak{F}_L(V) \cdot \mathfrak{D}_K^*(V) = \mathfrak{D}_L^*(V)$  for every extension  $L$  of  $K$ . The formula  $\varphi \mapsto d\varphi$  defines a homomorphism  $\mathfrak{F}(V) \rightarrow \mathfrak{D}^*(V)$  of vector spaces over  $U$  such that  $d(\varphi_1 \varphi_2) = \varphi_2 d\varphi_1 + \varphi_1 d\varphi_2$  ( $\varphi_1, \varphi_2 \in \mathfrak{F}(V)$ ). The kernel of the homomorphism is easily seen to be  $U \cdot (\mathfrak{F}(V))^p$ .

For any  $D \in \mathfrak{D}(V)$  and any  $\sigma \in \text{Aut}(U/K)$ , the formula  $\varphi \mapsto \sigma(D(\sigma^{-1}(\varphi)))$  defines a derivation on  $V$  that we denote by  $\sigma(D)$ . For any  $D \in \mathfrak{D}(V)$ , it is obvious that if  $\sigma, \tau \in \text{Aut}(U/K)$ , then  $\sigma(\tau(D)) = (\sigma\tau)(D)$ , and that  $id_U(D) = D$ . Evidently

$$\sigma(D_1 + D_2) = \sigma(D_1) + \sigma(D_2), \quad \sigma(\varphi D) = \sigma(\varphi)\sigma(D),$$

$$\sigma([D_1, D_2]) = [\sigma(D_1), \sigma(D_2)] \quad (D_1, D_2, D \in \mathfrak{D}(V), \varphi \in \mathfrak{F}(V)).$$

In particular, for fixed  $\sigma \in \text{Aut}(U/K)$  the formula  $D \mapsto \sigma(D)$  defines an automorphism of  $\mathfrak{D}(V)$  as a vector space over  $\mathfrak{F}_K(V)$  and as a Lie algebra over  $K$ , and it is easy to see that  $\sigma(\mathfrak{D}_L(V)) = \mathfrak{D}_{\sigma L}(V)$  for every extension  $L$  of  $K$ .

For any  $\omega \in \mathfrak{D}^*(V)$  and any  $\sigma \in \text{Aut}(U/K)$ , the formula  $D \mapsto \sigma(\langle \sigma^{-1}(D), \omega \rangle)$  defines a linear form on  $\mathfrak{D}(V)$ , that is, a differential on  $V$ ; we denote it by  $\sigma(\omega)$ . Obviously  $\sigma(\tau(\omega)) = (\sigma\tau)(\omega)$  and  $id_U(\omega) = \omega$ , and

$$\begin{aligned} \sigma(\omega_1 + \omega_2) &= \sigma(\omega_1) + \sigma(\omega_2), & \sigma(\varphi\omega) &= \sigma(\varphi)\sigma(\omega), \\ \sigma(\langle D, \omega \rangle) &= \langle \sigma(D), \sigma(\omega) \rangle. \end{aligned}$$

In particular, the formula  $\omega \mapsto \sigma(\omega)$  defines an automorphism of  $\mathfrak{D}^*(V)$  as a vector space over  $\mathfrak{F}_K(V)$ , and  $\sigma(\mathfrak{D}_L^*(V)) = \mathfrak{D}_{\sigma L}^*(V)$  for every extension  $L$  of  $K$ .

Referring to Section 15, Proposition 20, we find that if  $\Sigma$  is a subset of  $\text{Aut}(U/K)$  and  $K'$  denotes the field of invariants of  $\Sigma$  in  $U$ , then, for a derivation  $D$  on  $V$ ,

$$D \in \mathfrak{D}_{K'}(V) \iff \sigma(D) = D \quad (\sigma \in \Sigma).$$

When  $L$  is any extension of  $K$  and  $D \in \mathfrak{D}_L(V)$ , then evidently  $\sigma(D) = \sigma'(D)$  for any  $\sigma, \sigma' \in \text{Aut}(U/K)$  that agree on  $L$ . Hence, for any isomorphism  $\gamma: L \approx L'$  over  $K$ , where  $L'$  is an extension of  $K$  for which  $\text{tr deg } U/L = \text{tr deg } U/L'$ , we can define  $\gamma(D)$  to be  $\sigma(D)$  for any  $\sigma \in \text{Aut}(U/K)$  that extends  $\gamma$ . Referring to Section 15, the Corollary to Proposition 20 and the discussion just before it, we see that this defines an operation of  $\text{Aut}(L/K)$  on  $\mathfrak{D}_L(V)$ , and that if  $\mathfrak{S}$  is a subset of  $\text{Aut}(L/K)$  such that the field of invariants of  $\mathfrak{S}$  is  $K$ , and  $D \in \mathfrak{D}_L(V)$ , then

$$D \in \mathfrak{D}_K(V) \iff \gamma(D) = D \quad (\gamma \in \mathfrak{S}).$$

Similar remarks are valid for  $\mathfrak{D}^*(V)$ .

Now let  $W$  also be an irreducible  $K$ -set, and let  $f \in \mathfrak{M}_K(V, W)$  be generically invertible. Then (see Section 16)  $f^*: \mathfrak{F}(W) \rightarrow \mathfrak{F}(V)$  is an isomorphism over  $U$  that maps  $\mathfrak{F}_K(W)$  onto  $\mathfrak{F}_K(V)$ , and  $(f^*)^{-1} = (f^-)^*$ . For any  $D \in \mathfrak{D}(V)$ , it is evident that  $(f^*)^{-1} \circ D \circ f^*$  is a derivation on  $W$ . Therefore we can define a mapping

$$f^{**}: \mathfrak{D}(V) \rightarrow \mathfrak{D}(W)$$

by the formula  $f^{**}(D) = (f^*)^{-1} \circ D \circ f^*$ . This  $f^{**}$  is an isomorphism of Lie algebras over  $U$  such that  $f^{**}(\varphi D) = (f^*)^{-1}(\varphi)f^{**}(D)$  for all  $\varphi \in \mathfrak{F}(V)$  and  $D \in \mathfrak{D}(V)$ , and  $f^{**}(\mathfrak{D}_K(V)) = \mathfrak{D}_K(W)$ . It is obvious that  $(id_V)^{**} = id_{\mathfrak{D}(V)}$ , and that when  $g$  is a generically invertible  $K$ -mapping of  $W$  into an irreducible  $K$ -set  $X$ , then  $(g \circ f)^{**} = g^{**} \circ f^{**}$ . Hence  $(f^{**})^{-1} = (f^-)^{**}$ .

For any  $\omega' \in \mathfrak{D}^*(W)$ ,  $f^* \circ \omega' \circ f^{**}$  is a differential on  $V$ . Therefore we can define a mapping

$$f^{***}: \mathfrak{D}^*(W) \rightarrow \mathfrak{D}^*(V)$$

by the formula  $f^{***}(\omega') = f^* \circ \omega' \circ f^{**}$ . This  $f^{***}$  is an isomorphism of vector spaces over  $U$  such that  $f^{***}(\varphi' \omega') = f^{**}(\varphi')f^{***}(\omega')$  for all  $\varphi' \in \mathfrak{F}(W)$  and  $\omega' \in \mathfrak{D}^*(W)$ , and  $f^{***}(\mathfrak{D}_K^*(W)) = \mathfrak{D}_K^*(V)$ . We have  $(id_V)^{***} = id_{\mathfrak{D}^*(V)}$ , and when  $g \in \mathfrak{M}_K(W, X)$  as above, then  $(g \circ f)^{***} = f^{***} \circ g^{***}$ . Hence  $(f^{***})^{-1} = (f^-)^{***}$ . By definition,

$$\langle D, f^{***}(\omega') \rangle = f^*(\langle f^{**}(D), \omega' \rangle)$$

when  $D \in \mathfrak{D}(V)$  and  $\omega' \in \mathfrak{D}^*(W)$ . When  $\omega' = d\varphi'$  for some  $\varphi' \in \mathfrak{F}(W)$ , this reduces to the equation  $\langle D, f^{***}(d\varphi') \rangle = \langle D, d(f^*(\varphi')) \rangle$ . Therefore

$$f^{***}(d\varphi') = d(f^*(\varphi')).$$

We suppose for the rest of this section that  $V$  is a homogeneous  $K$ -space for a connected  $K$ -group  $G$ . Then  $V$  is irreducible (because for a fixed  $v \in V_{K^*}$ ,  $\lambda_v: G \rightarrow V$  is a  $K_s$ -homomorphism of homogeneous  $K_s$ -spaces for  $G$ ). For any  $x \in G$ , the mapping  $\rho_x: V \rightarrow V$  is a generically invertible  $K(x)$ -mapping of  $V$  into  $V$  (with generic inverse  $\rho_{x^{-1}}$ ). Therefore the preceding discussion applies when we replace  $(K, V, W, f)$  by  $(K(x), V, V, \rho_x)$ . In particular, we have the automorphisms

$$\rho_x^*: \mathfrak{F}(V) \approx \mathfrak{F}(V), \quad \rho_x^{**}: \mathfrak{D}(V) \approx \mathfrak{D}(V), \quad \rho_x^{***}: \mathfrak{D}^*(V) \approx \mathfrak{D}^*(V).$$

It is easy to verify, for any  $\sigma \in \text{Aut}(U/K)$ , that

$$\begin{aligned} \rho_{\sigma x} &= \sigma(\rho_x), \\ \rho_{\sigma x}^*(\varphi) &= \sigma(\rho_x^*(\sigma^{-1}(\varphi))) & (\varphi \in \mathfrak{F}(V)), & (1^*) \\ \rho_{\sigma x}^{**}(D) &= \sigma(\rho_x^{**}(\sigma^{-1}(D))) & (D \in \mathfrak{D}(V)), & (1^{**}) \\ \rho_{\sigma x}^{***}(\omega) &= \sigma(\rho_x^{***}(\sigma^{-1}(\omega))) & (\omega \in \mathfrak{D}^*(V)), & (1^{***}) \end{aligned}$$

and that entirely analogous equations hold for  $\lambda_v: G \rightarrow V$  instead of  $\rho_x$ .

A derivation  $D$  (respectively differential  $\omega$ ) on the homogeneous  $K$ -space  $V$  for  $G$  is said to be *invariant* if  $\rho_x^{**}(D) = D$  (respectively  $\rho_x^{***}(\omega) = \omega$ ) for every  $x \in G$ .

When  $D \in \mathfrak{D}_K(V)$  (respectively  $\omega \in \mathfrak{D}_K^*(V)$ ) it suffices to verify this condition for one element  $x \in \Gamma_{G/K}$ . Indeed, Eq. (1\*\*) (respectively Eq. (1\*\*\*)) then establishes the condition for every element of  $\Gamma_{G/K}$ , and the fact that every element  $x \in G$  is a product  $x = x_1 x_2$  with  $x_1, x_2 \in \Gamma_{G/K}$  and the identity  $\rho_x^{**} = \rho_{x_2}^{**} \circ \rho_{x_1}^{**}$  (respectively  $\rho_x^{***} = \rho_{x_1}^{***} \circ \rho_{x_2}^{***}$ ) thereupon establish the condition in general.

The set of invariant derivations on  $V$  is a Lie algebra over  $U$ , called the *Lie algebra of  $V$* ; we denote it by  $\mathfrak{Q}(V)$ . When  $p \neq 0$  then  $D^p \in \mathfrak{Q}(V)$  for every  $D \in \mathfrak{Q}(V)$ . We set  $\mathfrak{Q}_K(V) = \mathfrak{Q}(V) \cap \mathfrak{D}_K(V)$ ; this is a Lie algebra over  $K$ . The set of invariant differentials on  $V$  is a vector space over  $U$ ; we denote it by  $\mathfrak{Q}^*(V)$ , and set  $\mathfrak{Q}_K^*(V) = \mathfrak{Q}^*(V) \cap \mathfrak{D}_K^*(V)$ .



It follows from Eq. (1\*\*) (respectively Eq. (1\*\*\*)) that  $\sigma(\mathfrak{Q}(V)) = \mathfrak{Q}(V)$  (respectively  $\sigma(\mathfrak{Q}^*(V)) = \mathfrak{Q}^*(V)$ ) for every  $\sigma \in \text{Aut}(U/K)$ .

We already know that  $U$  and  $\mathfrak{F}_K(V)$  are linearly disjoint over  $K$ , and that  $\mathfrak{F}(V)$  and  $\mathfrak{D}_K(V)$  are linearly disjoint over  $\mathfrak{F}_K(V)$ . If  $L$  is any extension of  $K$ , and if  $D_1, \dots, D_m \in \mathfrak{Q}_L(V)$  are linearly dependent over  $\mathfrak{F}_L(V)$  but  $D_1, \dots, D_{m-1}$  are not (so that  $D_1, \dots, D_{m-1}$  are linearly independent over  $\mathfrak{F}(V)$ ), then there exist  $\varphi_1, \dots, \varphi_m \in \mathfrak{F}_L(V)$  with  $\varphi_m = 1$  such that  $\sum_{1 \leq i \leq m} \varphi_i D_i = 0$ ; for any  $x \in G$ , then

$$\sum_{1 \leq i \leq m} \rho_x^*(\varphi_i) D_i = \rho_{x^{-1}}^{**} \left( \sum_{1 \leq i \leq m} \varphi_i D_i \right) = 0,$$

so that  $\sum_{1 \leq i \leq m-1} (\rho_x^*(\varphi_i) - \varphi_i) D_i = 0$ , whence  $\rho_x^*(\varphi_i) = \varphi_i$  and therefore  $\varphi_i \in U \cap \mathfrak{F}_L(V) = L$  ( $1 \leq i \leq m$ ). This shows that  $\mathfrak{F}_K(V)$  and  $\mathfrak{Q}_K(V)$  are linearly disjoint over  $K$ , and that  $\mathfrak{F}(V)$  and  $\mathfrak{Q}(V)$  are linearly disjoint over  $U$ . It follows that  $U$  and  $\mathfrak{Q}_K(V)$  are linearly disjoint over  $K$ .

Similar statements are valid for differentials on  $V$ .

If  $D \in \mathfrak{Q}_K(V)$  and  $\omega \in \mathfrak{Q}_K^*(V)$ , then  $\langle D, \omega \rangle \in K$ . This follows from the computation  $\rho_x^*(\langle D, \omega \rangle) = \rho_x^*(\langle \rho_x^{**}(D), \omega \rangle) = \langle D, \rho_x^{***}(\omega) \rangle = \langle D, \omega \rangle$ .

The following theorem shows that when the homogeneous  $K$ -space  $V$  is principal then the vector spaces  $\mathfrak{Q}(V)$  over  $U$  and  $\mathfrak{Q}_K(V)$  over  $K$  have the same dimension  $n = \dim V = \dim G$  as the vector spaces  $\mathfrak{D}(V)$  over  $\mathfrak{F}(V)$  and  $\mathfrak{D}_K(V)$  over  $\mathfrak{F}_K(V)$ , and that  $\mathfrak{Q}^*(V)$  and  $\mathfrak{Q}_K^*(V)$  can be regarded as the dual spaces to  $\mathfrak{Q}(V)$  and  $\mathfrak{Q}_K(V)$ , respectively.

**Theorem 13** *Let  $V$  be a principal homogeneous  $K$ -space for the connected  $K$ -group  $G$ . Every basis of  $\mathfrak{Q}_K(V)$  (respectively of  $\mathfrak{Q}_K^*(V)$ ) is a basis  $\mathfrak{D}_K(V)$  and of  $\mathfrak{Q}(V)$  and of  $\mathfrak{D}(V)$  (respectively of  $\mathfrak{D}_K^*(V)$  and of  $\mathfrak{Q}^*(V)$  and of  $\mathfrak{D}^*(V)$ ). If  $(D_1, \dots, D_n)$  is a basis of  $\mathfrak{D}(V)$  and  $(\omega_1, \dots, \omega_n)$  is the dual basis of  $\mathfrak{D}^*(V)$ , then a necessary and sufficient condition that every  $D_j$  be invariant is that every  $\omega_j$  be invariant.*

*Proof* The second assertion follows from the equations  $\langle D_i, \rho_x^{***}(\omega_j) \rangle = \rho_x^*(\langle \rho_x^{**}(D_i), \omega_j \rangle)$ . To prove the first assertion it suffices, because of the linear disjointness established above, to show that some basis of  $\mathfrak{D}_K(V)$  consists of invariant derivations. To this end let  $(D_1, \dots, D_n)$  be any basis of  $\mathfrak{D}_K(V)$ . For each  $x \in G$ ,  $(\rho_x^{**}(D_1), \dots, \rho_x^{**}(D_n))$  is a basis of  $\mathfrak{D}_{K(x)}(V)$ , as is  $(D_1, \dots, D_n)$ . Therefore there exist elements  $\varphi_{xij} \in \mathfrak{F}_{K(x)}(V)$  with  $\det(\varphi_{xij})_{1 \leq i \leq n, 1 \leq j \leq n} \neq 0$  such that

$$\rho_x^{**}(D_j) = \sum_{1 \leq i \leq n} \varphi_{xij} D_i \quad (1 \leq j \leq n).$$

Fixing  $(v, x, y) \in \Gamma_V \times G^2/K$ , we see that each  $\varphi_{xij}$  is defined at  $v$  and that  $(\varphi_{xij}(v))_{1 \leq i \leq n, 1 \leq j \leq n} \in \mathbf{GL}_{K(v, vx^{-1})}(n) = \mathbf{GL}_{K(v, vx^{-1})}(n)$ ; also,  $(v, vx^{-1}) \in \Gamma_V/K$ .

Therefore there exists a unique  $K$ -mapping  $f \in \mathfrak{M}_K(V^2, \mathbf{GL}(n))$  such that  $f(v, vx^{-1}) = (\varphi_{xij}(v))_{1 \leq i \leq n, 1 \leq j \leq n}$ .

For any  $\sigma \in \text{Aut}(U/K)$ ,

$$\begin{aligned} \sum_i \varphi_{\sigma xij} D_i &= \rho_{\sigma x}^{**}(D_j) = \sigma(\rho_x^{**}(\sigma^{-1}(D_j))) \\ &= \sigma(\rho_x^{**}(D_j)) = \sigma \left( \sum_i \varphi_{xij} D_i \right) = \sum_i \sigma(\varphi_{xij}) D_i, \end{aligned}$$

so that  $\varphi_{\sigma xij} = \sigma(\varphi_{xij})$ , whence  $\varphi_{\sigma xij}(\sigma v) = (\sigma(\varphi_{xij}))(\sigma v) = \sigma(\varphi_{xij}(v))$ . Therefore  $(\varphi_{\sigma xij}(\sigma v))_{1 \leq i \leq n, 1 \leq j \leq n} = \sigma(f(v, vx^{-1})) = f(\sigma v, \sigma v \cdot \sigma x^{-1})$ . It follows from this that

$$(\varphi_{sij}(w))_{1 \leq i \leq n, 1 \leq j \leq n} = f(w, ws^{-1})$$

for every  $(w, s) \in \Gamma_V \times G/K$ . However,

$$\begin{aligned} \sum_i \varphi_{xyij} D_i &= \rho_{xy}^{**}(D_j) = (\rho_y \circ \rho_x)^{**}(D_j) = \rho_y^{**}(\rho_x^{**}(D_j)) \\ &= \rho_y^{**} \left( \sum_v \varphi_{xvj} D_v \right) = \sum_i \sum_v \varphi_{yiv} \rho_{y^{-1}}^*(\varphi_{xvj}) D_i, \end{aligned}$$

so that  $\varphi_{xyij} = \sum_v \varphi_{yiv} \rho_{y^{-1}}^*(\varphi_{xvj})$  ( $1 \leq i \leq n, 1 \leq j \leq n$ ). Hence

$$\begin{aligned} f(v, vy^{-1}x^{-1}) &= f(v, v(xy)^{-1}) = (\varphi_{xyij}(v))_{1 \leq i \leq n, 1 \leq j \leq n} \\ &= \left( \sum_v \varphi_{yiv}(v) \varphi_{xvj}(vy^{-1}) \right)_{1 \leq i \leq n, 1 \leq j \leq n} \\ &= f(v, vy^{-1})f(vy^{-1}, vy^{-1}x^{-1}). \end{aligned}$$

Since evidently  $(v, vy^{-1}, vy^{-1}x^{-1}) \in \Gamma_V/K$ , this means that  $f \in Z_K^1(V, \mathbf{GL}(n))$ .

It follows by Section 17, Corollary 1 to Theorem 12, and Section 12, Theorem 9, that  $f = \delta h$  for some  $h \in \mathfrak{M}_K(V, \mathbf{GL}(n))$ , that is, that  $f(v, vx^{-1}) = h(v)^{-1}h(vx^{-1})$ . Writing  $h(v) = (\beta_{ij}(v))_{1 \leq i \leq n, 1 \leq j \leq n}$ , where  $\beta_{ij} \in \mathfrak{F}_K(V)$  and  $\det(\beta_{ij}) \neq 0$ , and setting  $(\gamma_{ij}) = (\beta_{ij})^{-1}$ , so that  $\gamma_{ij} \in \mathfrak{F}_K(V)$  and  $\det(\gamma_{ij}) \neq 0$ , we find that

$$(\varphi_{xij}(v)) = f(v, vx^{-1}) = (\gamma_{ij}(v)) (\beta_{ij}(vx^{-1})),$$

whence

$$(\varphi_{xij})(\rho_{x^{-1}}^*(\gamma_{ij})) = (\gamma_{ij}).$$

Now set  $D_j' = \sum_{1 \leq i \leq n} \gamma_{ij} D_i$  ( $1 \leq j \leq n$ ). By what we have just shown,  $(D_1', \dots, D_n')$  is a basis of  $\mathfrak{D}_K(V)$  and, for each index  $j$ ,

$$\begin{aligned} \rho_x^{**}(D_j') &= \sum_v \rho_{x^{-1}}^*(\gamma_{vj}) \rho_x^{**}(D_v) \\ &= \sum_i \sum_v \varphi_{xiv} \rho_{x^{-1}}^*(\gamma_{vj}) D_i \\ &= \sum_i \gamma_{ij} D_i = D_j'. \end{aligned}$$

This shows that each  $D_j'$  is invariant, and completes the proof of the theorem.

We conclude this section with some examples.

EXAMPLE 1 Let  $\xi$  denote the canonical coordinate function on the additive group  $G_a = U$  (that is, let  $\xi = id_{G_a}$ ). Then  $\mathfrak{F}(G_a) = U(\xi)$ ,  $d/d\xi$  is a basis of  $\mathfrak{D}(G_a)$ , and  $d\xi$  is the dual basis of  $\mathfrak{D}^*(G_a)$ . For any  $x \in G_a$ ,  $\rho_x^{***}(d\xi) = d(\rho_x^*(\xi)) = d(\xi + x) = d\xi$ . Hence  $d\xi$  is a basis of  $\mathfrak{D}^*(G_a)$  and  $d/d\xi$  is a basis of  $\mathfrak{Q}(G_a)$ .

EXAMPLE 2 Let  $\xi$  denote the canonical coordinate function on the multiplicative group  $G_m = U^*$  (that is, let  $\xi$  be the inclusion mapping  $U^* \rightarrow U$ ). Then  $\mathfrak{F}(G_m) = U(\xi)$ ,  $\xi d/d\xi$  is a basis of  $\mathfrak{D}(G_m)$ , and  $\xi^{-1}d\xi$  is the dual basis of  $\mathfrak{D}^*(G_m)$ . For any  $x \in G_m$ ,

$$\begin{aligned} \rho_x^{***}(\xi^{-1}d\xi) &= \rho_x^*(\xi^{-1})d(\rho_x^*(\xi)) = (\xi x)^{-1}d(\xi x) \\ &= x^{-1}\xi^{-1}x d\xi = \xi^{-1}d\xi. \end{aligned}$$

Hence  $\xi^{-1}d\xi$  is a basis of  $\mathfrak{D}^*(G_m)$  and  $\xi d/d\xi$  is a basis of  $\mathfrak{Q}(G_m)$ .

EXAMPLE 3 Let  $p \neq 2$ , and let  $\xi, \eta$  denote the canonical coordinate functions on the elliptic curve  $W = W(g_2, g_3)$  (see Section 1). They are defined at every element of  $W$  other than  $(0:0:1)$ , and if  $z = (1:x:y)$  is any such element, then  $\xi(z) = x$ ,  $\eta(z) = y$ . Then  $\mathfrak{F}(W) = U(\xi, \eta)$ ,  $\xi$  is a separating transcendence basis of  $\mathfrak{F}(W)$  over  $U$ ,  $\eta d/d\xi$  is a basis of  $\mathfrak{D}(W)$ , and  $\eta^{-1}d\xi$  is the dual basis of  $\mathfrak{D}^*(W)$ . Also,  $\eta^2 = 4\xi^3 - g_2\xi - g_3$ , so that  $d\eta/d\xi = (6\xi^2 - \frac{1}{2}g_2)\eta^{-1}$ . From the equations of the group law we find that

$$\begin{aligned} \rho_x^*(\xi) &= -\xi - x + \frac{1}{4}(\xi - x)^{-2}(\eta - y)^2, \\ \rho_x^*(\eta) &= -\frac{1}{2}(\eta + y) + \frac{3}{2}(\xi + x)(\xi - x)^{-1}(\eta - y) - \frac{1}{4}(\xi - x)^{-3}(\eta - y)^3. \end{aligned}$$

Therefore

$$\begin{aligned} \eta \frac{d}{d\xi}(\rho_x^*(\xi)) \\ = \eta \left( -1 - \frac{1}{2}(\xi - x)^{-3}(\eta - y)^2 + \frac{1}{2}(\xi + x)^{-2}(\eta - y)(6\xi^2 - \frac{1}{2}g_2)\eta^{-1} \right). \end{aligned}$$

A straightforward computation shows that the right side here equals  $\rho_x^*(\eta)$ . Hence

$$\left( \rho_x^{**} \left( \eta \frac{d}{d\xi} \right) \right) \xi = \rho_x^{-1*} \left( \eta \frac{d}{d\xi}(\rho_x^*(\xi)) \right) = \eta = \eta \frac{d}{d\xi} \xi,$$

so that  $\rho_x^{**}(\eta d/d\xi) = \eta d/d\xi$ . Therefore  $\eta d/d\xi$  is a basis of  $\mathfrak{Q}(W)$  and  $\eta^{-1}d\xi$  is a basis of  $\mathfrak{D}^*(W)$ .

EXAMPLE 4 The Group  $G_m$  of Example 2 is the case  $n = 1$  of the group  $GL(n)$ , which we now consider for arbitrary  $n$ . Let  $\xi = (\xi_{ij})_{1 \leq i \leq n, 1 \leq j \leq n}$  denote the matrix of canonical coordinate functions on  $GL(n)$ ; for arbitrary  $x = (x_{ij}) \in GL(n)$ , we have  $\xi_{ij}(x) = x_{ij}$ . Then the matrix  $\xi = (\xi_{ij})$  is an algebraically independent family of generators of the extension  $\mathfrak{F}(GL(n))$  of  $U$ . Set  $\xi^{-1} = (\eta_{ij})$ . The matrix  $(\sum_v \xi_{iv} \partial/\partial \xi_{jv})$ , which we permit ourselves to write as the matrix product  $\xi \partial/\partial(\xi)$ , is a basis of  $\mathfrak{D}(GL(n))$ . The matrix  $(\sum_v \eta_{vi} d\xi_{jv})$ , which we write as the matrix product  ${}^t \xi^{-1} d(\xi)$ , is a basis of  $\mathfrak{D}^*(GL(n))$ . It is easy to verify that these two bases are dual to each other. Evidently  $\rho_x^*(\xi) = \xi x$ , and we can write

$$\begin{aligned} \rho_x^{***}({}^t \xi^{-1} d(\xi)) &= \rho_x^*({}^t \xi^{-1}) d(\rho_x^*(\xi)) = ({}^t \xi x)^{-1} d({}^t \xi x) \\ &= {}^t \xi^{-1} \cdot {}^t x^{-1} \cdot {}^t x \cdot d({}^t \xi) = {}^t \xi^{-1} d({}^t \xi). \end{aligned}$$

Therefore  ${}^t \xi^{-1} d({}^t \xi)$  is a basis of  $\mathfrak{D}^*(GL(n))$  and  $\xi \partial/\partial(\xi)$  is a basis of  $\mathfrak{Q}(GL(n))$ .

### EXERCISES

- (Chevalley [9, Chapter II, §8]) Let  $G$  be a  $K$ -subgroup of  $GL(n)$ , and let  $\mathfrak{a}$  be the set of polynomials in  $U[X] = [(X_{ij})_{1 \leq i \leq n, 1 \leq j \leq n}]$  that vanish at every element of  $G$ . (Thus,  $\mathfrak{a}$  is a perfect ideal of  $U[X]$  and the unity matrix  $1_n$  is a zero of  $\mathfrak{a}$ .) For each matrix  $u = (u_{ij})$  in the algebra  $\mathbf{M}(n)$  of all  $n \times n$  matrices over  $U$ , let  $D(u)$  denote the derivation of the field  $U(X)$  over  $U$  such that  $D(u)X_{ij} = \sum_{1 \leq v \leq n} u_{iv} X_{vj}$  ( $1 \leq i \leq n, 1 \leq j \leq n$ ) (or, briefly, such that  $D(u)X = uX$ .) Let  $T$  be an indeterminate.
  - Show, for  $u \in \mathbf{M}(n)$ , that the following three conditions are equivalent: (i)  $P(1_n + Tu) \equiv 0 \pmod{T^2}$  for every  $P \in \mathfrak{a}$ ; (ii)  $\sum_{i,j} \partial P / \partial X_{ij}(1_n) u_{ij} = 0$  for every  $P \in \mathfrak{a}$ ; (iii)  $D(u)\mathfrak{a} \subset \mathfrak{a}$ .
  - Let  $I(G)$  denote the set of all matrices  $u \in \mathbf{M}(n)$  that satisfy the equivalent conditions in part (a), and set  $I_K(G) = I(G) \cap \mathbf{M}_K(n)$ . Show that  $I(G) = U \cdot I_K(G)$  and that  $I(G)$  respectively  $I_K(G)$  is a Lie algebra over  $U$  respectively  $K$  (that is, is a subspace of the vector space  $\mathbf{M}(n)$  respectively  $\mathbf{M}_K(n)$  over  $U$  respectively  $K$ , and is stable with respect to the Lie multiplication  $(u, v) \mapsto [u, v] = vu - uv$ , where  $uv$  and  $vu$  denote the usual matrix products). Show that when  $p \neq 0$ , then  $u^p \in I(G)$  for every  $u \in I(G)$ .
  - Show that  $I(G) = I(G^0)$ .
  - Let  $G$  be connected, and let  $\xi = (\xi_{ij})_{1 \leq i \leq n, 1 \leq j \leq n}$  be the matrix of canonical coordinate functions on  $G$  (for every  $x = (x_{ij})_{1 \leq i \leq n, 1 \leq j \leq n} \in G$ ,  $\xi_{ij}(x) = x_{ij}$ ). Show that  $\mathfrak{F}_K(G) = K(\xi)$ . Show that for each  $u \in I(G)$

there exists a unique invariant derivation  $\Delta(u) \in \mathfrak{L}(G)$  such that  $\Delta(u)\zeta = u\zeta$ . Show that for each  $D \in \mathfrak{L}(G)$  there exists a unique matrix  $\nabla(D) = (\nabla_{ij}(D))_{1 \leq i \leq n, 1 \leq j \leq n} \in \mathfrak{l}(G)$  such that  $D\zeta = \nabla(D)\zeta$ . Prove that the mappings

$$\Delta : \mathfrak{l}(G) \rightarrow \mathfrak{L}(G), \quad \nabla : \mathfrak{L}(G) \rightarrow \mathfrak{l}(G)$$

are Lie algebra isomorphisms, inverse to each other, such that  $\Delta(\mathfrak{l}_K(G)) \subset \mathfrak{L}_K(G)$  and  $\nabla(\mathfrak{L}_K(G)) \subset \mathfrak{l}_K(G)$ , and (if  $p \neq 0$ ) such that  $\Delta(u^p) = \Delta(u)^p$  ( $u \in \mathfrak{l}(G)$ ) and  $\nabla(D^p) = \nabla(D)^p$  ( $D \in \mathfrak{L}(G)$ ).

- The Lie algebras  $\mathfrak{l}(\mathbf{GL}(n)), \mathfrak{l}(\mathbf{SL}(n)), \mathfrak{l}(\mathbf{O}(n))$  are usually denoted by  $\mathfrak{gl}(n), \mathfrak{sl}(n), \mathfrak{o}(n)$ , respectively. Show that  $\mathfrak{gl}(n)$  is the Lie algebra of all  $n \times n$  matrices over  $U$ , that  $\mathfrak{sl}(n)$  consists of all matrices  $u \in \mathfrak{gl}(n)$  such that  $\text{Tr} u = 0$ , and that when  $p \neq 2$ , then  $\mathfrak{o}(n)$  consists of all matrices  $u \in \mathfrak{gl}(n)$  such that  ${}^t u + u = 0$ . Show that when  $p = 2$ , then  $\mathfrak{o}(n)$  consists of all  $u = (u_{ij}) \in \mathfrak{gl}(n)$  such that  ${}^t u + u = 0$  and  $\sum_{1 \leq i \leq n} u_{ii} = 0$  ( $1 \leq i \leq n$ ). (*Hint:* For  $\mathfrak{o}(n)$ , use Exercise 1(d), to show that  $\dim \mathfrak{o}(n) = \dim \mathbf{O}(n)$ , and infer that if  $\mathfrak{g}$  is a Lie algebra with  $\mathfrak{g} \supset \mathfrak{o}(n)$  and  $\dim \mathfrak{g} = \dim \mathbf{O}(n)$ , then  $\mathfrak{g} = \mathfrak{o}(n)$ .)
- (Chevalley [9, Chapter II, §10, V]) Let  $p \neq 0$ , and let  $G$  respectively  $H$  denote the set of all matrices

$$\begin{pmatrix} a & 0 & 0 \\ 0 & a^p & b \\ 0 & 0 & 1 \end{pmatrix} \quad \text{respectively} \quad \begin{pmatrix} a & 0 & 0 \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix}$$

with  $a \in U^*$  and  $b \in U$ .

- Show that  $G$  and  $H$  are connected  $K$ -subgroups of  $\mathbf{GL}(3)$ , that the center of  $G$  is trivial, and that  $H$  is commutative.
- Show that  $\mathfrak{l}(G)$  and  $\mathfrak{l}(H)$  are identical, consisting of all the matrices

$$\begin{pmatrix} u & 0 & 0 \\ 0 & 0 & v \\ 0 & 0 & 0 \end{pmatrix}$$

with  $u, v \in U$ .

- Let  $G$  be a connected  $K$ -group, and let  $L$  be an extension of  $K$  (over which the transcendence degree of  $U$  need not be infinite). For any derivation  $\delta$  of  $L$  over  $K$  let  $\delta^*$  denote the derivation of  $\mathfrak{F}_L(G)$  over  $\mathfrak{F}_K(G)$  that extends  $\delta$  (see Section 16, Exercise 3). For each  $D \in \mathfrak{D}_L(G)$  define  $\delta^{**}(D) = [\delta^*, D_L]$ , where  $D_L$  denotes the restriction of  $D$  to  $\mathfrak{F}_L(G)$ .

(a) Show that  $\delta^{**}$  is a derivation of the Lie ring  $\mathfrak{D}_L(G)$  such that  $\delta^{**}(\varphi D) = (\delta^* \varphi) D + \varphi \delta^{**}(D)$  ( $\varphi \in \mathfrak{F}_L(G)$ ,  $D \in \mathfrak{D}_L(G)$ ). Show that if  $D \in \mathfrak{D}_K(G)$ , then  $\delta^{**}(D) = 0$ .

(b) Show that if  $(D_1, \dots, D_n)$  is a basis of  $\mathfrak{L}_K(G)$  and  $\varphi_1, \dots, \varphi_n \in \mathfrak{F}_L(G)$ , then  $\delta^{**}(\sum \varphi_j D_j) = \sum (\delta^* \varphi_j) D_j$ . Infer that  $\delta^{**}$  induces by restriction a derivation  $\delta^*$  of the Lie ring  $\mathfrak{L}_L(G)$  such that  $\delta^*(aD) = (\delta a) D + a \delta^*(D)$  ( $a \in L$ ,  $D \in \mathfrak{L}_L(G)$ ). Show that if  $K' = \text{Ker}(\delta)$ , then  $\mathfrak{L}_{K'}(G) = \text{Ker}(\delta^*)$  and  $\mathfrak{D}_{K'}(G) = \text{Ker}(\delta^{**})$ .

(c) Show that the formula  $\delta \mapsto \delta^*$  defines a homomorphism  $\text{Der}(L/K) \rightarrow \text{Der}(\mathfrak{L}_L(G))$  of Lie rings and of vector spaces over  $L$ .

### 19 Local rings

Let  $V$  be an irreducible  $K$ -set and let  $v \in V$ . Then  $\mathfrak{F}_v(V)$  is a subalgebra of the extension  $\mathfrak{F}(V)$  of  $U$ , and  $\mathfrak{F}_{K,v}(V)$  is a subalgebra of the extension  $\mathfrak{F}_K(V)$  of  $K$ . The set  $\mathfrak{m}_v(V)$  of all  $\varphi \in \mathfrak{F}_v(V)$  that vanish at  $v$  is an ideal of  $\mathfrak{F}_v(V)$ . Every element of  $\mathfrak{F}_v(V) - \mathfrak{m}_v(V)$  is evidently a unit of the ring  $\mathfrak{F}_v(V)$ . Therefore  $\mathfrak{F}_v(V)$  is a local ring and  $\mathfrak{m}_v(V)$  is its maximal ideal. Similarly,  $\mathfrak{F}_{K,v}$  is a local ring and the intersection  $\mathfrak{m}_{K,v}(V) = \mathfrak{m}_v(V) \cap \mathfrak{F}_K(V)$  is its maximal ideal.  $\mathfrak{F}_v(V)$  is called the *local ring on  $V$  at  $v$* .

Consider a  $K$ -mapping  $f \in \mathfrak{M}_{K,v}(V, W)$ , where  $W$  is an irreducible  $K$ -set. For every  $\psi \in \mathfrak{F}_{f(v)}(W)$ ,  $\psi \circ f$  exists and is an element of  $\mathfrak{F}_v(V)$ . Therefore the formula  $\psi \mapsto \psi \circ f$  defines a mapping

$$f_v^* : \mathfrak{F}_{f(v)}(W) \rightarrow \mathfrak{F}_v(V),$$

and evidently  $f_v^*$  is a homomorphism of algebras over  $U$  such that  $f_v^*(\mathfrak{F}_{K,f(v)}(W)) \subset \mathfrak{F}_{K,v}(V)$ . When  $f$  is generically surjective (and hence, because  $V$  is irreducible, has the property that  $f(\Gamma_{V/K}) = \Gamma_{W/K}$ ), then  $f_v^*$  is a restriction of the injective homomorphism  $f^* : \mathfrak{F}(W) \rightarrow \mathfrak{F}(V)$  described in Section 16 (just before Proposition 22), and hence is injective.

If  $X$ , too, is an irreducible  $K$ -set, and  $g \in \mathfrak{M}_{K,f(v)}(W, X)$ , then  $g \circ f$  exists and is in  $\mathfrak{M}_{K,v}(V, X)$ , and  $(g \circ f)_v^* = f_v^* \circ g_{f(v)}^*$ . Also,  $(id_V)_v^* = id_{\mathfrak{F}_v(V)}$ . It follows that when  $f$  is generically invertible and bidedined at  $v$ , then  $f_v^*$  is an isomorphism and  $(f_v^*)^{-1} = (f^{-1})_{f(v)}^*$ .

If  $W$  is an irreducible  $K$ -subset of some  $\mathbf{G}_a^n$  and  $f \in \mathfrak{M}_{K,v}(V, W)$  and  $f$  is generically surjective, and if we set  $\xi_j = pr_{j \circ in_{\mathbf{G}_a^n, W}} \circ f$  ( $1 \leq j \leq n$ ), then  $\xi_1, \dots, \xi_n \in \mathfrak{F}_{K,v}(V)$  and  $in_{\mathbf{G}_a^n, W} \circ f = \xi_1 \times \dots \times \xi_n$ . Conversely, if  $\xi_1, \dots, \xi_n \in \mathfrak{F}_{K,v}(V)$  and we set  $W$  equal to the closed image of  $\xi_1 \times \dots \times \xi_n$ , then  $W$  is an irreducible  $K$ -subset of  $\mathbf{G}_a^n$ , there exists a unique  $K$ -mapping  $f$  of  $V$  into  $W$  with  $in_{\mathbf{G}_a^n, W} \circ f = \xi_1 \times \dots \times \xi_n$ , and  $f$  has the property that  $f \in \mathfrak{M}_{K,v}(V, W)$ ,  $f$  is generically surjective, and  $\xi_j = pr_{j \circ in_{\mathbf{G}_a^n, W}} \circ f$  ( $1 \leq j \leq n$ ). When  $f$  is

generically invertible and bidefined at  $v$ , then  $(\xi_1, \dots, \xi_n)$  is said to be a system of  $K$ -affine coordinates on  $V$  at  $v$ .

**Proposition 25** *Let  $V$  be an irreducible  $K$ -set and let  $v \in V$ . There exists a system of  $K$ -affine coordinates on  $V$  at  $v$ . If  $(\xi_1, \dots, \xi_n)$  is any such system, then  $K(v) = K(\xi_1(v), \dots, \xi_n(v))$  and, for any extension  $L$  of  $K$ ,  $\mathfrak{F}_{L,v}(V)$  is the localization of  $L[\xi_1, \dots, \xi_n]$  at its prime ideal  $L[\xi_1, \dots, \xi_n] \cap \mathfrak{m}_v(V)$ .*

*Proof* The existence follows from Section 16, Theorem 11. Defining  $W$  and  $f$  as above, we know that  $K(v) = K(f(v)) = K(\xi_1(v), \dots, \xi_n(v))$ , and that the mapping  $f_v^* : \mathfrak{F}_{f(v)}(W) \rightarrow \mathfrak{F}_v(V)$  is an isomorphism that maps  $\mathfrak{F}_{L,f(v)}(W)$  onto  $\mathfrak{F}_{L,v}(V)$ . By the remark near the beginning of Section 16, if  $\varphi \in \mathfrak{F}_{L,v}(V)$ , then there exist  $P, Q \in L[X_1, \dots, X_n]$  with  $Q(\xi_1(v), \dots, \xi_n(v)) \neq 0$  such that  $\varphi = P(\xi_1, \dots, \xi_n)/Q(\xi_1, \dots, \xi_n)$ , and conversely.

**Corollary 1** *The local rings  $\mathfrak{F}_v(V)$  and  $\mathfrak{F}_{K,v}(V)$  are Noetherian, and  $\mathfrak{F}_v(V)$  is the localization of  $U[\mathfrak{F}_{K,v}(V)]$  at its prime ideal  $U[\mathfrak{F}_{K,v}(V)] \cap \mathfrak{m}_v(V)$ .*

This is evident from the proposition.

**Corollary 2** *Let  $(\xi_1, \dots, \xi_n)$  be a system of  $K$ -affine coordinates on  $V$  at  $v$ . Let  $\mathfrak{q}$  denote the ideal of polynomials  $Q \in K[X_1, \dots, X_n]$  such that  $Q(\xi_1, \dots, \xi_n) = 0$ . Then  $\mathfrak{q}$  is prime and regular over  $K$ , the rank of the matrix*

$$J = ((\partial Q / \partial X_j)(\xi_1(v), \dots, \xi_n(v)))_{Q \in \mathfrak{q}, 1 \leq j \leq n}$$

*is less than or equal to  $n - \dim V$ , and the smallest number of elements of  $\mathfrak{m}_{K,v}(V)$  that can generate  $\mathfrak{m}_{K,v}(V)$  equals the dimension of the vector space  $\mathfrak{m}_{K,v}(V)/\mathfrak{m}_{K,v}(V)^2$  over  $\mathfrak{F}_{K,v}(V)/\mathfrak{m}_{K,v}(V)$ . This dimension is greater than or equal to  $\dim V - \dim_K v$ . If the rank equals  $n - \dim V$ , then the dimension equals  $\dim V - \dim_K v$  and the local ring  $\mathfrak{F}_{K,v}(V)$  is integrally closed.*

*Proof* It is clear that  $\mathfrak{q}$  is prime and regular over  $K$ . Let  $\mathfrak{p}$  denote the ideal of polynomials  $P \in K[X_1, \dots, X_n]$  such that  $P(\xi_1, \dots, \xi_n) \in \mathfrak{m}_v(V)$ . Then  $\mathfrak{p}$  is prime and  $\mathfrak{p} \supset \mathfrak{q}$ . Set  $\mathfrak{o} = K[X_1, \dots, X_n]_{\mathfrak{p}}$ ,  $\mathfrak{m} = \mathfrak{o}\mathfrak{p}$ ,  $\mathfrak{n} = \mathfrak{o}\mathfrak{q}$ . Then  $\mathfrak{o}$  is a local integral domain,  $\mathfrak{m}$  is its maximal ideal, and  $\mathfrak{n}$  is a prime ideal of  $\mathfrak{o}$ . Also, there is an isomorphism  $\mathfrak{o}/\mathfrak{n} \approx \mathfrak{F}_{K,v}(V)$  such that  $P + \mathfrak{n} \mapsto P(\xi_1, \dots, \xi_n)$  for every  $P \in K[X_1, \dots, X_n]$ , which maps  $\mathfrak{m}/\mathfrak{n}$  onto  $\mathfrak{m}_{K,v}(V)$ . Therefore the corollary follows by Chapter 0, Section 16, Corollary 5 to Proposition 11 (see also Chapter 0, Remark 3 near the end of Section 14).

We recall (Section 15, Proposition 15(f)) that if  $B'$  is any  $K$ -subset of a  $K$ -set  $B$ , then the inclusion mapping  $\text{in}_{B,B'} : B' \rightarrow B$  is a  $K$ -mapping.

**Corollary 3** *Let  $V'$  be an irreducible  $K$ -subset of  $V$  with  $v \in V'$ . The  $U$ -algebra-homomorphism  $(\text{in}_{V,V'})^* : \mathfrak{F}_v(V) \rightarrow \mathfrak{F}_v(V')$  is surjective.*

*Proof* Let  $(\xi_1, \dots, \xi_n)$  be a system of  $K$ -affine coordinates on  $V$  at  $v$ . It is easy to see that  $(\xi_1 \circ \text{in}_{V,V'}, \dots, \xi_n \circ \text{in}_{V,V'})$  is a system of  $K$ -affine coordinates on  $V'$  at  $v$ . Given any  $\varphi' \in \mathfrak{F}_v(V')$ , we know by the proposition that there exist polynomials  $P, Q \in U[X_1, \dots, X_n]$  with  $Q(\xi_1(v), \dots, \xi_n(v)) \neq 0$  such that  $\varphi' = P(\xi_1 \circ \text{in}_{V,V'}, \dots, \xi_n \circ \text{in}_{V,V'}) / Q(\xi_1 \circ \text{in}_{V,V'}, \dots, \xi_n \circ \text{in}_{V,V'})$ . Setting  $\varphi = P(\xi_1, \dots, \xi_n) / Q(\xi_1, \dots, \xi_n)$  we find that  $\varphi \in \mathfrak{F}_v(V)$  and  $(\text{in}_{V,V'})^*(\varphi) = \varphi'$ .

When  $v \in V_K$  and we set  $\zeta_j(v) = a_j$  ( $1 \leq j \leq n$ ), then  $L[\xi_1, \dots, \xi_n] \cap \mathfrak{m}_v(V)$  is the ideal  $(\xi_1 - a_1, \dots, \xi_n - a_n)$  of  $L[\xi_1, \dots, \xi_n]$  and  $\mathfrak{m}_{L,v}(V)$  is the ideal  $(\xi_1 - a_1, \dots, \xi_n - a_n)$  of  $\mathfrak{F}_{L,v}(V)$ . It follows then that  $\mathfrak{m}_v(V)$  is the ideal  $(\xi_1 - a_1, \dots, \xi_n - a_n)$  of  $\mathfrak{F}_v(V)$ , so that  $\mathfrak{m}_v(V) = \mathfrak{F}_v(V)\mathfrak{m}_{K,v}(V)$ . Hence, for any  $k \in \mathbb{N}$  with  $k \neq 0$ , the vector spaces  $\mathfrak{m}_v(V)/\mathfrak{m}_v(V)^k$  over  $U$  and  $\mathfrak{m}_{K,v}(V)/\mathfrak{m}_{K,v}(V)^k$  over  $K$  are finite dimensional. Moreover, since  $\mathfrak{F}_K(V)$  and  $U$  are linearly disjoint over  $K$ , the canonical  $K$ -linear mapping  $\mathfrak{m}_{K,v}(V)/\mathfrak{m}_{K,v}(V)^k \rightarrow \mathfrak{m}_v(V)/\mathfrak{m}_v(V)^k$ , induced by the inclusion mapping  $\mathfrak{m}_{K,v}(V) \rightarrow \mathfrak{m}_v(V)$ , is injective and its image generates  $\mathfrak{m}_v(V)/\mathfrak{m}_v(V)^k$ . Thus, when  $v \in V_K$ , we have a canonical identification of  $\mathfrak{m}_{K,v}(V)/\mathfrak{m}_{K,v}(V)^k$  with a  $K$ -subspace of the vector space  $\mathfrak{m}_v(V)/\mathfrak{m}_v(V)^k$ , and after the identification a basis of  $\mathfrak{m}_{K,v}(V)/\mathfrak{m}_{K,v}(V)^k$  is a basis of  $\mathfrak{m}_v(V)/\mathfrak{m}_v(V)^k$ , too.

If  $f \in \mathfrak{M}_{K,v}(V, W)$ , where  $W$  is again any irreducible  $K$ -set, then  $f_v^*(\mathfrak{m}_{f(v)}(W)) \subset \mathfrak{m}_v(V)$  and  $f_v^*(\mathfrak{m}_{K,f(v)}(W)) \subset \mathfrak{m}_{K,v}(V)$ , whence also  $f_v^*(\mathfrak{m}_{f(v)}(W)^k) \subset \mathfrak{m}_v(V)^k$  and  $f_v^*(\mathfrak{m}_{K,f(v)}(W)^k) \subset \mathfrak{m}_{K,v}(V)^k$ . Therefore  $f_v^*$  induces a homomorphism

$$f_v^{(k)} : \mathfrak{m}_{f(v)}(W)/\mathfrak{m}_{f(v)}(W)^k \rightarrow \mathfrak{m}_v(V)/\mathfrak{m}_v(V)^k$$

of vector spaces over  $U$ , and  $f_v^{(k)}$  maps  $\mathfrak{m}_{K,f(v)}(W)/\mathfrak{m}_{K,f(v)}(W)^k$  into  $\mathfrak{m}_{K,v}(V)/\mathfrak{m}_{K,v}(V)^k$ .

To see an example, consider a  $K$ -group  $G$ . For each  $x \in G$ , the inner automorphism  $\tau_x$  of  $G$  is a  $K(x)$ -automorphism of  $G$  that restricts to a  $K(x)$ -automorphism of  $G^\circ$  that we denote by  $\tau_x^\circ$ . The automorphism  $(\tau_x^\circ)_1^*$  of the local ring  $\mathfrak{F}_1(G^\circ)$  at  $1 \in G^\circ$  induces an automorphism  $(\tau_x^\circ)_1^{(k)}$  of the vector space  $\mathfrak{m}_1(G^\circ)/\mathfrak{m}_1(G^\circ)^k$ . If we fix  $\varphi_1, \dots, \varphi_{r(k)} \in \mathfrak{F}_{K,1}(G^\circ)$  such that the corresponding cosets  $\bar{\varphi}_1, \dots, \bar{\varphi}_{r(k)}$  relative to  $\mathfrak{m}_1(G^\circ)^k$  form a basis of  $\mathfrak{m}_1(G^\circ)/\mathfrak{m}_1(G^\circ)^k$ , the matrix  $a^{(k)}(x) = (a_{ij}^{(k)}(x))$  of  $(\tau_x^\circ)_1^{(k)}$  with respect to this basis will be in  $\mathbf{GL}_{K(x)}(r(k))$ , and we shall have a group homomorphism

$$a^{(k)} : G \rightarrow \mathbf{GL}(r(k)).$$

Now, for any  $\sigma \in \text{Aut}(U/K)$  and any  $z \in G^\circ$ ,  $\sigma(\tau_x^\circ \cdot)(z) = \sigma(\tau_x^\circ \cdot)(\sigma^{-1}z) = \sigma(x^{-1}(\sigma^{-1}z)x) = (\sigma x)^{-1}z\sigma x = \tau_{\sigma x}^\circ(z)$ , whence

$$\sigma(\tau_x^\circ \cdot) = \tau_{\sigma x}^\circ \cdot.$$

Therefore, for any  $\varphi \in \mathfrak{F}_{K,1}(G^\circ)$ ,

$$\sigma((\tau_{x^{-1}}^\circ)_1^*(\varphi)) = \sigma(\varphi \circ \tau_{x^{-1}}^\circ) = \sigma(\varphi) \circ \sigma(\tau_{x^{-1}}^\circ) = \varphi \circ \tau_{\sigma x}^\circ = (\tau_{\sigma x^{-1}}^\circ)_1^*(\varphi).$$

In particular,

$$\sigma((\tau_{x^{-1}}^\circ)_1^*(\varphi_j)) = (\tau_{\sigma x^{-1}}^\circ)_1^*(\varphi_j) \equiv \sum_i a_{ij}^{(k)}(\sigma x) \varphi_i \pmod{\mathfrak{m}_1(G^\circ)^k}.$$

Since also

$$\sigma((\tau_{x^{-1}}^\circ)_1^*(\varphi_j)) \equiv \sigma\left(\sum_i a_{ij}^{(k)}(x) \varphi_i\right) \equiv \sum_i \sigma(a_{ij}^{(k)}(x)) \varphi_i \pmod{\mathfrak{m}_1(G^\circ)^k},$$

we infer that  $\sigma(a^{(k)}(x)) = a^{(k)}(\sigma x)$ . It follows from this that  $a^{(k)}$  is a  $K$ -homomorphism. The kernel  $N^{(k)}$  of  $a^{(k)}$  is a normal  $K$ -closed subgroup of  $G$  that contains the centralizer of  $G^\circ$  in  $G$ . Evidently  $N^{(k)} \supset N^{(k+1)}$  for every  $k$ , and therefore there exists an  $h \in \mathbb{Q}$  such that  $N^{(k)} = N^{(h)}$  for every  $k \geq h$ .

If  $x$  is not in the centralizer of  $G^\circ$  in  $G$ , then  $\tau_{x^{-1}}(s) \neq s$  when  $s \in \Gamma_{G^\circ/K(x)}$ , and therefore, for some  $\varphi \in \mathfrak{F}_{K,1}(G^\circ)$ ,  $\varphi(\tau_{x^{-1}}(s)) \neq \varphi(s)$ , whence  $(\tau_{x^{-1}}^\circ)_1^*(\varphi) \neq \varphi$ . Since  $\bigcap_{k \in \mathbb{N}} \mathfrak{m}_1(G^\circ)^k = 0$  by Krull's theorem (see Chapter 0, Section 14, Remark 2), it follows that  $(\tau_{x^{-1}}^\circ)_1^*(\varphi) \not\equiv \varphi \pmod{\mathfrak{m}_1(G^\circ)^k}$  for some  $k$ , so that  $(\tau_{x^{-1}}^\circ)_1^{(k)} \neq id$  and  $x \notin N^{(h)}$ . This shows that  $N^{(h)}$  is the centralizer of  $G^\circ$  in  $G$ .

EXERCISE

- Let  $G$  be a  $K$ -group and  $(\xi_1, \dots, \xi_n)$  be a system of  $K$ -affine coordinates on  $G$  at 1, and consider the three everywhere defined surjective  $K$ -mappings  $\mu, pr_1, pr_2$  of  $G^2$  into  $G$ . Show that

$$(pr_1^*(\xi_1), \dots, pr_1^*(\xi_n), pr_2^*(\xi_1), \dots, pr_2^*(\xi_n))$$

is a system of  $K$ -affine coordinates on  $G^2$  at  $(1, 1)$ , and infer that there exist rational expressions  $R_1, \dots, R_n \in K(X_1, \dots, X_n, Y_1, \dots, Y_n)$  with denominators not vanishing at  $(\xi_1(1), \dots, \xi_n(1), \xi_1(1), \dots, \xi_n(1))$  such that

$$\mu^*(\xi_j) = R_j(pr_1^*(\xi_1), \dots, pr_1^*(\xi_n), pr_2^*(\xi_1), \dots, pr_2^*(\xi_n))$$

for every  $j$ .

20 Tangent spaces

Let  $V$  be an irreducible  $K$ -set, and let  $v \in V$ . If  $R$  is a subring of  $\mathfrak{F}_v(V)$ , a local derivation of  $R$  at  $v$  is defined as an  $(R \cap U)$ -linear mapping  $\mathfrak{d} : R \rightarrow U$  such that

$$\mathfrak{d}(\varphi\psi) = \mathfrak{d}\varphi \cdot \psi(v) + \varphi(v) \cdot \mathfrak{d}\psi$$

for all  $\varphi, \psi \in R$ . It is easy to see that when  $\psi$  is a unit in  $R$ , then also

$$\mathfrak{d}(\varphi/\psi) = (\psi(v)\mathfrak{d}\varphi - \varphi(v)\mathfrak{d}\psi)/\psi(v)^2.$$

When  $\Sigma$  is a multiplicatively stable subset of  $R$  no element of which vanishes at  $v$ , the proof that shows that a derivation of  $R$  can be extended to a unique derivation of the ring of quotients  $\Sigma^{-1}R$  can be copied to show that a local derivation of  $R$  at  $v$  can be extended to a unique local derivation of  $\Sigma^{-1}R$  at  $v$ . In particular,  $\Sigma^{-1}R$  can be the local ring  $R_{R \cap \mathfrak{m}_v(V)}$ , the localization of  $R$  at its prime ideal  $R \cap \mathfrak{m}_v(V)$ .

A local derivation of  $\mathfrak{F}_v(V)$  at  $v$  is called a tangent vector to  $V$  at  $v$ . The set of all tangent vectors to  $V$  at  $v$  is a vector space over  $U$ , called the tangent space to  $V$  at  $v$ , which we denote by  $\mathfrak{T}_v(V)$ .

The restriction to  $\mathfrak{F}_{K,v}(V)$  of any tangent vector to  $V$  at  $v$  is a local derivation of  $\mathfrak{F}_{K,v}(V)$  at  $v$ . Conversely, any local derivation  $T_0$  of  $\mathfrak{F}_{K,v}(V)$  at  $v$  can be extended to a unique tangent vector to  $V$  at  $v$ . Indeed, because  $U$  and  $\mathfrak{F}_{K,v}(V)$  are linearly disjoint over  $K$  (by Section 16, Proposition 22(b)),  $T_0$  can be extended to a unique  $U$ -linear mapping  $T_1$  of  $U[\mathfrak{F}_{K,v}(V)]$  into  $U$ , and it is easy to verify that  $T_1$  is a local derivation at  $v$ ; also, we saw in Section 19 (Corollary 1 to Proposition 25) that  $\mathfrak{F}_v(V)$  is the localization of  $U[\mathfrak{F}_{K,v}(V)]$  at its prime ideal  $U[\mathfrak{F}_{K,v}(V)] \cap \mathfrak{m}_v(V)$ , and therefore  $T_1$  can be extended to a unique tangent vector to  $V$  at  $v$ .

Let  $L$  be an extension of  $K(v)$ . The set of tangent vectors  $T \in \mathfrak{T}_v(V)$  such that  $T(\mathfrak{F}_{L,v}(V)) \subset L$  is a vector space over  $L$ ; we denote it by  $\mathfrak{T}_{L,v}(V)$ . If  $u_1, \dots, u_n$  are elements of  $U$  that are linearly independent over  $L$  and  $T_1, \dots, T_n$  are elements of  $\mathfrak{T}_{L,v}(V)$  such that  $\sum u_j T_j = 0$ , then  $\sum u_j T_j \varphi = 0$  ( $\varphi \in \mathfrak{F}_{L,v}(V)$ ), whence  $T_j \varphi = 0$  ( $\varphi \in \mathfrak{F}_{L,v}(V)$ ,  $1 \leq j \leq n$ ), so that  $T_j = 0$  ( $1 \leq j \leq n$ ) by what we proved in the preceding paragraph. Thus,  $U$  and  $\mathfrak{T}_{L,v}(V)$  are linearly disjoint over  $L$ , and

$$\dim_L \mathfrak{T}_{L,v}(V) \leq \dim_v \mathfrak{T}_v(V).$$

An element of the vector space  $\mathfrak{T}_v^*(V)$  dual to  $\mathfrak{T}_v(V)$  is called a cotangent vector to  $V$  at  $v$ , and  $\mathfrak{T}_v^*(V)$  itself is called the cotangent space to  $V$  at  $v$ . The subset of  $\mathfrak{T}_v^*(V)$  consisting of all cotangent vectors  $\chi$  such that  $\langle T, \chi \rangle \in L$  for every  $T \in \mathfrak{T}_{L,v}(V)$  is a vector space over  $L$ ; we denote it by  $\mathfrak{T}_{L,v}^*(V)$ .

Let  $W$  be another irreducible  $K$ -set and let  $f \in \mathfrak{M}_{K,v}(V, W)$ . For any  $T \in \mathfrak{T}_v(V)$  the composite mapping

$$\mathfrak{F}_{f(v)}(W) \xrightarrow{f^*} \mathfrak{F}_v(V) \xrightarrow{T} U$$

is evidently a tangent vector to  $W$  at  $f(v)$  and maps  $\mathfrak{F}_{L,f(v)}(W)$  into  $L$  if  $T$  maps  $\mathfrak{F}_{L,v}(V)$  into  $L$ . Therefore the formula  $T \mapsto T \circ f_v^*$  defines a mapping

$$f_v^{**} : \mathfrak{T}_v(V) \rightarrow \mathfrak{T}_{f(v)}(W).$$

$f_v^{**}$  is a homomorphism of vector spaces over  $U$  that maps  $\mathfrak{T}_{L,v}(V)$  into  $\mathfrak{T}_{L,f(v)}(W)$ . The transpose of  $f_v^{**}$ , which we denote by  $f_v^{***}$ , is a vector space homomorphism

$$f_v^{***} : \mathfrak{T}_{f(v)}^*(W) \rightarrow \mathfrak{T}_v^*(V)$$

that maps  $\mathfrak{T}_{L,f(v)}^*(W)$  into  $\mathfrak{T}_{L,v}^*(V)$ . Evidently  $(id_V)_v^{**} = id_{\mathfrak{T}_v(V)}$  and  $(id_V)^{***} = id_{\mathfrak{T}_v^*(V)}$ , and if  $g \in \mathfrak{M}_{K,f(v)}(W, X)$ , where  $X$  is an irreducible  $K$ -set, then

$$(g \circ f)_v^{**} = g_{f(v)}^{**} \circ f_v^{**}, \quad (g \circ f)_v^{***} = f_v^{***} \circ g_{f(v)}^{***}.$$

It follows that if  $f$  is generically invertible and bidefined at  $v$ , then  $f_v^{**}$  and  $f_v^{***}$  are isomorphisms.

Now suppose that we are in the situation considered in Section 19, in which  $W$  is an irreducible  $K$ -subset of  $G_a^n$  and  $f$  is generically invertible and bidefined at  $v$ . As before, let  $(\xi_1, \dots, \xi_n)$  denote the system of  $K$ -affine coordinates on  $V$  at  $v$  given by the equations  $\xi_j = pr_j \circ in_{G_a^n, W} \circ f$ , and set  $(a_1, \dots, a_n) = f(v)$ ,  $\mathfrak{q}$  equal to the defining ideal of  $W$  in  $K[X_1, \dots, X_n]$ , and  $\mathcal{O}_v$  equal to the domain of bidefinition of  $f$ . For any extension  $L$  of  $K(v)$  (even for  $L = U$ ),  $L\mathfrak{q}$  is the defining ideal of  $W$  in  $L[X_1, \dots, X_n]$ ,  $\mathfrak{F}_{L,v}(V) = L[X_1, \dots, X_n]_{(\xi_1 - a_1, \dots, \xi_n - a_n)}$ , and  $\mathfrak{m}_{L,v}(V)$  is the ideal of  $\mathfrak{F}_{L,v}(V)$  generated by  $\xi_1 - a_1, \dots, \xi_n - a_n$ . If  $T$  is any element of  $\mathfrak{T}_{L,v}$ , then

$$TP(\xi_1, \dots, \xi_n) = \sum \frac{\partial P}{\partial X_j}(f(v)) T\xi_j \quad (P \in U[X_1, \dots, X_n]),$$

so that  $(T\xi_1, \dots, T\xi_n)$  is a solution in  $L^n$  of the system of homogeneous linear equations

$$\sum \frac{\partial Q}{\partial X_j}(f(v)) Y_j = 0 \quad (Q \in \mathfrak{q})$$

with coefficients in  $K(v)$ . Conversely, if  $(b_1, \dots, b_n)$  is any solution of this system, then the kernel of the  $U$ -linear mapping  $U[X_1, \dots, X_n] \rightarrow U$  defined by the formula  $P \mapsto \sum (\partial P / \partial X_j)(f(v)) b_j$  contains the kernel  $U\mathfrak{q}$  of the substitution homomorphism  $U[X_1, \dots, X_n] \rightarrow U[\xi_1, \dots, \xi_n]$ , and therefore there is a unique  $U$ -linear mapping  $U[\xi_1, \dots, \xi_n] \rightarrow U$  such that  $P(\xi_1, \dots, \xi_n) \mapsto \sum (\partial P / \partial X_j)(f(v)) b_j$  for every  $P \in U[X_1, \dots, X_n]$ . It is easy to see that this mapping is a local derivation of  $U[\xi_1, \dots, \xi_n]$  at  $v$  and hence can be extended to a unique tangent vector  $T$  to  $V$  at  $v$ , and that  $T \in \mathfrak{T}_{L,v}(V)$  when  $(b_1, \dots, b_n) \in L^n$ . Thus, the formula  $T \mapsto (T\xi_1, \dots, T\xi_n)$  defines an isomorphism

$$\mathfrak{T}_v(V) \approx \mathcal{S}$$

of the tangent space to  $V$  at  $v$  onto the vector space  $\mathcal{S}$  over  $U$  consisting of the solutions of the above system of linear equations, and for every exten-

sion  $L$  of  $K(v)$  this isomorphism maps  $\mathfrak{T}_{L,v}(V)$  onto the vector space  $\mathcal{S} \cap L^n$  over  $L$ . It follows that  $\dim_U \mathfrak{T}_v(V) = \dim_L \mathfrak{T}_{L,v}(V) = n - r(v)$ , where  $r(v)$  is the rank of the matrix

$$J = \left( \frac{\partial Q}{\partial X_j}(f(v)) \right)_{Q \in \mathfrak{q}, 1 \leq j \leq n}.$$

When the element  $v$  is  $K$ -generic on  $V$ , then  $\mathfrak{F}_{K,v}(V) = \mathfrak{F}_K(V)$ , and the canonical isomorphism  $K(v) \approx \mathfrak{F}_K(V)$  followed by any  $T \in \mathfrak{T}_{K(v),v}(V)$  (or rather by the restriction of  $T$  to  $\mathfrak{F}_K(V)$ ) is readily seen to be a derivation of  $K(v)$  over  $K$ . Also, the canonical isomorphism  $\mathfrak{F}_K(V) \approx K(v)$  followed by any derivation of  $K(v)$  over  $K$  and then by the inclusion mapping  $K(v) \rightarrow U$  is a local derivation of  $\mathfrak{F}_K(V)$  at  $v$  and hence can be extended to a unique element of  $\mathfrak{T}_{K(v),v}(V)$ . Thus, when  $v \in \Gamma_{V/K}$ , we have a mapping from  $\mathfrak{T}_{K(v),v}(V)$  into the space of derivations of  $K(v)$  over  $K$ , and also a mapping in the opposite direction, and these mappings are evidently  $K(v)$ -linear and inverse to each other. Since  $K(v)$  is separable over  $K$  and of transcendence degree equal to  $\dim V$ , this shows that  $r(v) = n - \dim_{K(v)} \mathfrak{T}_{K(v),v}(V) = n - \dim V$ . Because each minor of the matrix

$$\left( \frac{\partial Q}{\partial X_j}(\xi_1, \dots, \xi_n) \right)_{Q \in \mathfrak{q}, 1 \leq j \leq n}$$

is a  $K$ -function on  $V$  that is defined on  $\mathcal{O}_v$ , we infer that  $\dim_U \mathfrak{T}_v(V) \geq \dim V$  for every  $v \in V$  and that the set of all  $v \in V$  such that  $\dim_U \mathfrak{T}_v(V) = \dim V$  is dense and  $K$ -open in  $V$ .

Referring to Section 19, Corollary 2 to Proposition 25, we see that we have proved the following result.

**Proposition 26** *Let  $V$  be an irreducible  $K$ -set. For any element  $v \in V$  and any extension  $L$  of  $K(v)$ ,*

$$\dim_U \mathfrak{T}_v(V) = \dim_L \mathfrak{T}_{L,v}(V) \geq \dim V.$$

*The set  $\mathcal{O}_V$ , consisting of the elements  $v \in V$  with  $\dim_U \mathfrak{T}_v(V) = \dim V$ , is dense and  $K$ -open in  $V$ . If  $v \in \mathcal{O}_V$ , then the local rings  $\mathfrak{F}_v(V)$  and  $\mathfrak{F}_{L,v}(V)$  are integrally closed; also, then the smallest number of elements that generate the maximal ideal  $\mathfrak{m}_{L,v}(V)$  is  $\dim V$ , and the cosets modulo  $\mathfrak{m}_{L,v}(V)^2$  of  $\dim V$  such generators form a basis of the vector space  $\mathfrak{m}_{L,v}(V) / \mathfrak{m}_{L,v}(V)^2$  over  $L$ .*

An element of  $V$  is said to be *simple* on  $V$  if it is in  $\mathcal{O}_V$ . By the proposition, if  $v$  is simple, then  $\dim_U \mathfrak{T}_v^*(V) = \dim_L \mathfrak{T}_{L,v}^*(V) = \dim V$ . In particular, then  $\mathfrak{T}_{L,v}^*(V)$  can be identified with the dual space to  $\mathfrak{T}_{L,v}(V)$ . A family  $(\xi_1, \dots, \xi_{\dim V})$  of generators of  $\mathfrak{m}_{L,v}(V)$  is called a system of *uniformizing parameters* on  $V$  at  $v$  over  $L$ .

In order to establish a connection between tangent vectors and derivations, it is helpful to introduce the following definitions. A derivation  $D$  on  $V$  is *holomorphic* at a given element  $v \in V$  if  $D(\mathfrak{F}_v(V)) \subset \mathfrak{F}_v(V)$ ; a differential  $\omega$  on  $V$  is *holomorphic* at  $v$  if  $\langle D, \omega \rangle \in \mathfrak{F}_v(V)$  for every derivation  $D$  on  $V$  that is holomorphic at  $v$ . We denote the set of all derivations (respectively differentials) on  $V$  that are holomorphic at  $v$  by  $\mathfrak{D}_v(V)$  (respectively  $\mathfrak{D}_v^*(V)$ ). It is obvious that  $\mathfrak{D}_v(V)$  and  $\mathfrak{D}_v^*(V)$  are  $\mathfrak{F}_v(V)$ -modules.

Given any  $D \in \mathfrak{D}_K(V)$ , we can fix  $\xi_1, \dots, \xi_n \in \mathfrak{F}_K(V)$  such that  $K(\xi_1, \dots, \xi_n) = \mathfrak{F}_K(V)$ . Then there exist polynomials  $P_0, P_1, \dots, P_n \in K[X_1, \dots, X_n]$  with  $P_0(\xi_1, \dots, \xi_n) \neq 0$  such that

$$D\xi_j = \frac{P_j(\xi_1, \dots, \xi_n)}{P_0(\xi_1, \dots, \xi_n)}$$

for every  $j$ . It follows that for each  $D \in \mathfrak{D}_K(V)$  there exists a dense  $K$ -open subset  $\mathcal{O}_D$  of  $V$  such that  $D \in \mathfrak{D}_v(V)$  for every  $v \in \mathcal{O}_D$ .

Given any  $v \in V$  and any  $D \in \mathfrak{D}_v(V)$ , there is a mapping  $D_v : \mathfrak{F}_v(V) \rightarrow \mathcal{U}$  defined by the formula  $D_v\varphi = (D\varphi)(v)$ , and it is clear that  $D_v \in \mathfrak{I}_v(V)$ .  $D_v$  is called the *local component of  $D$  at  $v$* . The formula  $D \mapsto D_v$  defines a canonical  $\mathcal{U}$ -linear mapping

$$\mathfrak{D}_v(V) \rightarrow \mathfrak{I}_v(V)$$

that maps  $\mathfrak{D}_v(V) \cap \mathfrak{D}_L(V)$  into  $\mathfrak{I}_{L,v}(V)$  for any extension  $L$  of  $K(v)$ . It is easy to see that if  $D_v = 0$  for every  $v \in \mathcal{O}_D$  (or even for one  $K'$ -generic element  $v$  of  $V$ , where  $K'$  is an extension of  $K$  with  $D \in \mathfrak{D}_{K'}(V)$ ), then  $D = 0$ .

We now consider the special case in which  $V$  is a *homogeneous  $K$ -space for a connected  $K$ -group  $G$* . For each  $x \in G$ , the mapping  $\rho_x : V \rightarrow V$  given by the formula  $\rho_x(v) = vx$  is an everywhere bidefined  $K(x)$ -mapping of  $V$  into  $V$  and  $\rho_{x^{-1}}$  is its (generic) inverse. Therefore, for each  $v \in V$ , the three homomorphisms

$$\begin{aligned} (\rho_x)_v^* &: \mathfrak{F}_{vx}(V) \rightarrow \mathfrak{F}_v(V), \\ (\rho_x)_v^{**} &: \mathfrak{I}_v(V) \rightarrow \mathfrak{I}_{vx}(V), \\ (\rho_x)_v^{***} &: \mathfrak{I}_{vx}^*(V) \rightarrow \mathfrak{I}_v^*(V) \end{aligned}$$

are isomorphisms and they induce by restriction isomorphisms

$$\begin{aligned} \mathfrak{F}_{L,vx}(V) &\rightarrow \mathfrak{F}_{L,v}(V), \\ \mathfrak{I}_{L,v}(V) &\rightarrow \mathfrak{I}_{L,vx}(V), \\ \mathfrak{I}_{L,vx}^*(V) &\rightarrow \mathfrak{I}_{L,v}^*(V) \end{aligned}$$

for every extension  $L$  of  $K(v, x)$ . Given  $v$ , there exists  $x$  such that  $vx \in \mathcal{O}_v$ , so that  $\dim \mathfrak{I}_v(V) = \dim \mathfrak{I}_{vx}(V) = \dim V$  and  $v \in \mathcal{O}_v$ , whence  $\mathcal{O}_v = V$ . Thus, *in a homogeneous  $K$ -space every element is simple*.

Now,  $(\rho_x)_v^*$  is the restriction to  $\mathfrak{F}_{vx}(V)$  of the automorphism  $\rho_x^*$  of  $\mathfrak{I}(V)$ . Also, for each  $D \in \mathfrak{D}(V)$ ,  $\rho_x^{**}(D) = \rho_{x^{-1}}^* \circ D \circ \rho_x^*$ . Therefore

$$\rho_x^{**}(\mathfrak{D}_v(V)) = \mathfrak{D}_{vx}(V) \quad (v \in V, \quad x \in G). \tag{2}$$

Furthermore, for any  $\psi \in \mathfrak{F}_{vx}(V)$ ,

$$\begin{aligned} (\rho_x^{**}(D))_{vx}(\psi) &= (\rho_x^{**}(D)\psi)(vx) = (\rho_{x^{-1}}^*(D(\rho_x^*(\psi))))(vx) \\ &= (D(\rho_x^*(\psi)))(v) = D_v((\rho_x)_v^*(\psi)) \\ &= ((\rho_x)_v^{**}(D_v))(\psi), \end{aligned}$$

so that

$$(\rho_x)_v^{**}(D_v) = (\rho_x^{**}(D))_{vx} \quad (D \in \mathfrak{D}_v(V), \quad v \in V, \quad x \in G). \tag{3}$$

Since for any  $D$  there exists a  $v$  such that  $D \in \mathfrak{D}_v(V)$ , Eq. (2) shows that *an invariant derivation on the homogeneous  $K$ -space  $V$  is holomorphic at every element of  $V$* . Equation (3) then shows that

$$(\rho_x)_v^{**}(D_v) = D_{vx} \quad (D \in \mathfrak{Q}(V), \quad v \in V, \quad x \in G). \tag{4}$$

It follows from this that if  $D$  is invariant and  $D_v = 0$  for one element  $v \in V$ , then  $D_v = 0$  for every  $v \in V$ , whence  $D = 0$ . Therefore for each  $v \in V$  the canonical  $\mathcal{U}$ -linear mapping  $\mathfrak{D}_v(V) \rightarrow \mathfrak{I}_v(V)$  injects  $\mathfrak{Q}(V)$  into  $\mathfrak{I}_v(V)$  and injects  $\mathfrak{Q}_L(V)$  into  $\mathfrak{I}_{L,v}(V)$  for every extension  $L$  of  $K(v)$ .

For the rest of this section we suppose that  $V$  is a *principal homogeneous  $K$ -space for the connected  $K$ -group  $G$* . Then  $\mathfrak{Q}(V)$  and  $\mathfrak{I}_v(V)$  both have dimension equal to that of  $V$ , as do  $\mathfrak{Q}_L(V)$  and  $\mathfrak{I}_{L,v}(V)$  for any  $L \supset K(v)$ . Hence we have a canonical vector space isomorphism

$$\mathfrak{Q}(V) \approx \mathfrak{I}_v(V)$$

that maps  $\mathfrak{Q}_L(V)$  onto  $\mathfrak{I}_{L,v}(V)$  for every extension  $L$  of  $K(v)$ . The transpose of this isomorphism is a canonical isomorphism

$$\mathfrak{I}_v^*(V) \approx \mathfrak{Q}^*(V)$$

that maps  $\mathfrak{I}_{L,v}^*(V)$  onto  $\mathfrak{Q}_L^*(V)$  for every  $L \supset K(v)$ . The inverse of this transpose maps an invariant differential  $\omega$  on  $V$  onto a cotangent vector to  $V$  at  $v$  that we denote by  $\omega_v$  and that is called the *local component of  $\omega$  at  $v$* . By definition,

$$\langle D_v, \omega_v \rangle = \langle D, \omega \rangle \quad (D \in \mathfrak{Q}(V), \quad \omega \in \mathfrak{Q}^*(V)).$$

Now suppose that we have a  $K$ -mapping  $f \in \mathfrak{M}_K(V, W)$ , where  $W$  is, like  $V$ , a principal homogeneous  $K$ -space for a connected  $K$ -group. For any  $v \in V$  at which  $f$  is defined we then have the composite linear mapping

$$\Omega(V) \approx \mathfrak{I}_v(V) \xrightarrow{f_v^{**}} \mathfrak{I}_{f(v)}(W) \approx \Omega(W),$$

which we denote by

$$f_v^{\#} : \Omega(V) \rightarrow \Omega(W).$$

For any extension  $L$  of  $K(v)$ ,  $f_v^{\#}$  maps  $\Omega_L(V)$  into  $\Omega_L(W)$ . The transpose of  $f_v^{\#}$ , that is, the composite mapping

$$\Omega^*(W) \approx \mathfrak{I}_{f(v)}^*(W) \xrightarrow{f_v^{**}} \mathfrak{I}_v^*(V) \approx \Omega^*(V),$$

we denote by

$$f_v^{\#\#} : \Omega^*(W) \rightarrow \Omega^*(V).$$

For any  $L \supset K(v)$ ,  $f_v^{\#\#}$  maps  $\Omega_L^*(W)$  into  $\Omega_L^*(V)$ . It is easy to verify that if  $g$  is a  $K$ -mapping of  $W$  into a homogeneous  $K$ -space for some connected  $K$ -group, and  $g$  is defined at  $f(v)$ , then

$$(g \circ f)_v^{\#} = g_{f(v)}^{\#} \circ f_v^{\#}, \quad (g \circ f)_v^{\#\#} = f_v^{\#\#} \circ g_{f(v)}^{\#\#}. \quad (5)$$

Also,  $(id_V)_v^{\#} = id_{\Omega(V)}$ . Equation (4) shows that

$$(\rho_x)_v^{\#} = id_{\Omega(V)} \quad (v \in V, \quad x \in G) \quad (6)$$

and hence also that

$$(\rho_x)_v^{\#\#} = id_{\Omega^*(V)}.$$

For any  $D \in \Omega(V)$  and  $\sigma \in \text{Aut}(U/K)$  we have, for every  $\psi \in \mathfrak{F}_{K, f(v)}(W)$ ,

$$\begin{aligned} \sigma(f_v^{\#}(D))_{\sigma(f(v))} \psi &= (\sigma(f_v^{\#}(D)) \psi) (\sigma(f(v))) = (\sigma(f_v^{\#}(D) \psi)) (\sigma(f(v))) \\ &= \sigma((f_v^{\#}(D) \psi) (f(v))) = \sigma(f_v^{\#}(D)_{f(v)} \psi) = \sigma(f_v^{\#\#}(D_v) \psi) \\ &= \sigma(D_v (f_v^{\#}(\psi))) = \sigma(D(f_v^{\#}(\psi)) (v)) = (\sigma(D) \sigma(f_v^{\#}(\psi))) (\sigma v) \\ &= \sigma(D)_{\sigma v} \sigma(\psi \circ f) = \sigma(D)_{\sigma v} (\psi \circ \sigma(f)) \\ &= \sigma(D)_{\sigma v} (\sigma(f)_{\sigma v}^{\#}(\psi)) = (\sigma(f)_{\sigma v}^{\#\#}(\sigma(D)_{\sigma v})) (\psi) \\ &= (\sigma(f)_{\sigma v}^{\#}(\sigma(D)))_{\sigma(f(\sigma v))} \psi = (\sigma(f)_{\sigma v}^{\#}(\sigma(D)))_{\sigma(f(v))} \psi, \end{aligned}$$

and therefore

$$\sigma(f_v^{\#}(D)) = \sigma(f)_{\sigma v}^{\#}(\sigma(D)).$$

It easily follows that also, for any  $\omega \in \Omega^*(V)$ ,

$$\sigma(f_v^{\#\#}(\omega)) = \sigma(f)_{\sigma v}^{\#\#}(\sigma(\omega)).$$

EXERCISES

- Let  $V$  be an irreducible  $K$ -set, let  $V'$  be an irreducible  $K$ -subset of  $V$ , and let  $v \in V'$ . Prove that the vector space homomorphism

$$(in_V, v')_v^{**} : \mathfrak{I}_v(V') \rightarrow \mathfrak{I}_v(V)$$

is injective. (*Hint:* See Section 19, Corollary 3 of Proposition 25.)

- Let  $V$  be an irreducible  $K$ -set and let  $v \in V$ . Show that each  $T \in \mathfrak{I}_v(V)$  induces a linear form  $T' : \mathfrak{m}_v(V)/\mathfrak{m}_v(V)^2 \rightarrow U$ , and prove that the formula  $T \mapsto T'$  defines a vector space isomorphism  $\mathfrak{I}_v(V) \approx (\mathfrak{m}_v(V)/\mathfrak{m}_v(V)^2)^*$ .

21 Crossed  $K$ -homomorphisms

We now generalize the notion of homogeneous  $K$ -space for a  $K$ -group  $G$ .

Let  $M$  be a  $K$ -set, and suppose given an everywhere defined  $K$ -mapping  $M \times G \rightarrow M$  (for which we shall use the notation  $(v, x) \mapsto vx$  and which we shall regard as an external law of composition) such that

$$\begin{aligned} v(x_1 x_2) &= (vx_1)x_2 & (v \in M, \quad x_1 \in G, \quad x_2 \in G), \\ v1 &= v & (v \in M). \end{aligned}$$

We then say that  $M$  is a  $K$ -space for  $G$ . By Section 15, Proposition 17(a), every homogeneous  $K$ -space for  $G$  is a  $K$ -space for  $G$ . It is easy to verify that a  $K$ -space  $M$  for  $G$  is homogeneous if and only if  $vG = M$  for some (and hence every)  $v \in M$ .

Suppose that  $M$  is a  $K$ -space for  $G$ . For each  $x \in G$ , the mapping  $\rho_x : M \rightarrow M$  given by the formula  $\rho_x(v) = vx$  is an everywhere bidefined generically invertible  $K(x)$ -mapping of  $M$  into  $M$ , and  $\rho_{x^{-1}}$  is its generic inverse and inverse. For each  $v \in M$ , the mapping  $\lambda_v : G \rightarrow M$  given by the formula  $\lambda_v(x) = vx$  is a  $K(v)$ -mapping of  $G$  into  $M$ . If  $N$  is another  $K$ -space for  $G$ , a  $K$ -homomorphism of  $M$  into  $N$  is defined as an everywhere defined  $K$ -mapping  $f \in \mathfrak{M}_K(M, N)$  such that  $f(vx) = f(v)x$  ( $v \in M, x \in G$ ). By Section 15, Proposition 17(b), when  $M$  and  $N$  are homogeneous, a  $K$ -homomorphism  $M \rightarrow N$  of  $K$ -spaces is the same thing as a  $K$ -homomorphism  $M \rightarrow N$  of homogeneous  $K$ -spaces. The mapping  $\lambda_v : G \rightarrow M$  is a  $K(v)$ -homomorphism.

If  $M'$  is a  $K$ -space for a  $K$ -group  $G'$ , then any  $K$ -homomorphism of  $K$ -groups  $g : G \rightarrow G'$  induces on  $M'$  a structure of  $K$ -space for  $G$ , the external law of composition being given by the formula  $(v', x) \mapsto v'g(x)$ . It follows that if  $h$  is an everywhere defined  $K$ -mapping of  $M$  into  $M'$  such that

$$h(vx) = h(v)g(x) \quad (v \in M, \quad x \in G),$$



then  $h$  is a  $K$ -homomorphism of  $K$ -spaces for  $G$ . We sometimes refer to the pair  $(h, g)$  as a  $K$ -homomorphism of  $(M, G)$  into  $(M', G')$ . When  $h$  is an everywhere defined  $K$ -mapping of  $M$  into  $M'$  for which there exists a  $K$ -homomorphism of  $K$ -groups  $g: G \rightarrow G'$  such that  $(h, g)$  is a  $K$ -homomorphism of  $(M, G)$  into  $(M', G')$ , we call  $h$  a *relative  $K$ -homomorphism of  $M$  into  $M'$*  and refer to  $g$  as being *associated to  $h$* .

In the special case in which  $M'$  is a principal homogeneous  $K$ -space for  $G'$ , on the one hand any  $K$ -homomorphism  $(h, g)$  of  $(M, G)$  into  $(M', G')$  has the property that  $h(v)^{-1}h(vx) = g(x)$  for every  $(v, x) \in M \times G$ , and on the other hand, for any everywhere defined  $K$ -mapping  $h$  of  $M$  into  $M'$  with the special property that  $h(v)^{-1}h(vx)$  is independent of  $v$ , the formula  $g(x) = h(v)^{-1}h(vx)$  defines a  $K$ -mapping of  $G$  into  $G'$  such that  $(h, g)$  is a  $K$ -homomorphism of  $(M, G)$  into  $(M', G')$ . Thus, in this special case,  $h$  completely determines  $g$ . When  $M$  too is principal homogeneous, we have the identity

$$g(v_1^{-1}v_2) = h(v_1)^{-1}h(v_2).$$

Any  $K$ -homomorphism of  $G$  into  $G'$  is also a relative  $K$ -homomorphism of the regular  $K$ -space for  $G$  into that for  $G'$  and is its own associated  $K$ -homomorphism.

If  $M_1$  is a  $K$ -subset of  $M$  and  $G_1$  is a  $K$ -subgroup of  $G$  such that  $M_1G_1 \subset M_1$ , then  $M_1$  has a natural structure of  $K$ -space for  $G_1$ . When  $M_1G \subset M_1$ , we call  $M_1$  a  *$K$ -subspace for  $G$  of  $M$* .

To see an example, consider a  $K$ -homomorphism  $f: M \rightarrow N$  of  $K$ -spaces for  $G$ , and let  $C$  denote the closed image of  $f$ . By Section 15, Proposition 15(c),  $C$  is a  $K$ -subset of  $N$ . If  $w \in C$  and  $y \in G$ , we can fix  $(v, x) \in \Gamma_{M \times G/K}$  with  $f(v) \xrightarrow{K_s} w$  and  $x \xrightarrow{K_s} y$ , and then evidently  $f(vx) = f(v)s \rightarrow wy$ , so that  $wy \in C$ . Thus, the closed image of the  $K$ -homomorphism  $M \rightarrow N$  is a  $K$ -subspace for  $G$  of  $N$ .

Let  $G$  and  $G'$  be  $K$ -groups. By a  *$K$ -operation of  $G$  on  $G'$*  we mean a structure on  $G'$  of  $K$ -space for  $G$  such that

$$(x_1'x_2')x = (x_1'x)(x_2'x) \quad (x_1' \in G', \quad x_2' \in G', \quad x \in G),$$

that is, such that for each  $x \in G$  the formula  $x' \mapsto x'x$  defines a group automorphism of  $G'$  (and therefore, evidently, a  $K(x)$ -automorphism of  $G'$ ).

Now let  $M'$  be a  $K$ -space for  $G'$ . By a  *$K$ -operation of  $G$  on  $(M', G')$*  we mean a structure on  $M'$  of  $K$ -space for  $G$  together with a  $K$ -operation of  $G$  on  $G'$  such that

$$(v'x')x = (v'x)(x'x) \quad (v' \in M', \quad x' \in G', \quad x \in G),$$

that is, such that for each  $x \in G$ , the formulas  $v' \mapsto v'x$  and  $x' \mapsto x'x$  define mappings  $\gamma_x: M' \rightarrow M'$  and  $\gamma_x': G' \rightarrow G'$  for which  $(\gamma_x, \gamma_x')$  is a  $K(x)$ -

automorphism of  $(M', G')$ . (Note that  $\gamma_x$  respectively  $\gamma_x'$  is the  $K(x)$ -mapping  $\rho_x$  of the  $K$ -space  $M'$  respectively  $G'$  for  $G$ .) By a  *$K$ -operation of  $G$  on  $M'$*  we mean a structure on  $M'$  of  $K$ -space for  $G$  that, for some  $K$ -operation of  $G$  on  $G'$ , gives a  $K$ -operation of  $G$  on  $(M', G')$ . We then refer to the  $K$ -operation of  $G$  on  $G'$  as *associated*.

When a  $K$ -operation of  $G$  on  $G'$  respectively  $(M', G')$  respectively  $M'$  is given, we say that  $G$   *$K$ -operates on  $G'$*  respectively  $(M', G')$  respectively  $M'$ .

In the special case in which  $M'$  is a principal homogeneous  $K$ -space for  $G'$ , on the one hand any  $K$ -operation of  $G$  on  $(M', G')$  has the property that  $(v'x)^{-1}((v'x')x) = x'x$  for every  $(v', x', x) \in M' \times G' \times G$  and  $(v_1'^{-1}v_2')x = (v_1'x)^{-1}(v_2'x)$  for every  $(v_1', v_2', x) \in M' \times M' \times G$ , and on the other hand for any structure on  $M'$  of  $K$ -space for  $G$  with the special property that  $(v'x)^{-1}((v'x')x)$  is independent of  $v'$ , the formula  $(x', x) \mapsto (v'x)^{-1}((v'x')x)$  defines a  $K$ -operation of  $G$  on  $G'$  such that the given structure on  $M'$  of  $K$ -space for  $G$  together with this  $K$ -operation of  $G$  on  $G'$  is a  $K$ -operation of  $G$  on  $(M', G')$ . Thus, in this special case, a  $K$ -operation of  $G$  on  $(M', G')$  is completely determined by a structure on  $M'$  of  $K$ -space for  $G$  having the special property mentioned above.

For example, any  $K$ -operation of  $G$  on  $G'$  is also a  $K$ -operation of  $G$  on the regular  $K$ -space for  $G'$  that is its own associated  $K$ -operation of  $G$  on  $G'$ .

We now describe a generalization of the notion of  $K$ -homomorphism. Let  $G$   $K$ -operate on  $G'$ . A *crossed  $K$ -homomorphism of  $G$  into  $G'$*  means an everywhere defined  $K$ -mapping  $f$  of  $G$  into  $G'$  such that

$$f(xy) = f(x)y \cdot f(y) \quad (x, y \in G).$$

It is easy to see that the *kernel* of a crossed  $K$ -homomorphism  $f$  (that is, the set of all  $x \in G$  such that  $f(x) = 1$ ) is a  $K$ -closed subgroup of  $G$ . When the  $K$ -operation of  $G$  on  $G'$  is trivial (that is, when  $x'x = x'$  ( $x' \in G', x \in G$ )), the notion of crossed  $K$ -homomorphism of  $G$  into  $G'$  reduces to that of  $K$ -homomorphism of  $G$  into  $G'$ .

Now let  $M$  and  $M'$  be  $K$ -spaces for  $G$  and  $G'$ , respectively, and suppose that  $G$   $K$ -operates on  $(M', G')$ . By a *crossed  $K$ -homomorphism of  $(M, G)$  into  $(M', G')$*  we mean a pair  $(h, g)$  such that  $h$  is an everywhere defined  $K$ -mapping of  $M$  into  $M'$ ,  $g$  is a crossed  $K$ -homomorphism of  $G$  into  $G'$ , and

$$h(vx) = h(v)x \cdot g(x) \quad (v \in M, \quad x \in G).$$

When  $(h, g)$  is such a pair, we also call  $h$  a *crossed  $K$ -homomorphism of  $M$  into  $M'$*  and refer to  $g$  as an *associated crossed  $K$ -homomorphism of  $G$  into  $G'$* .

In the special case in which  $M'$  is a principal homogeneous  $K$ -space for  $G'$ , on the one hand any crossed  $K$ -homomorphism  $(h, g)$  of  $(M, G)$  into

$(M', G')$  has the property that  $(h(v)x)^{-1}h(vx) = g(x)$  for every  $(v, x) \in M \times G$ , and on the other hand for any everywhere defined  $K$ -mapping  $h$  of  $M$  into  $M'$  with the special property that  $(h(v)x)^{-1}h(vx)$  is independent of  $v$ , the formula  $g(x) = (h(v)x)^{-1}h(vx)$  defines a  $K$ -mapping  $g$  of  $G$  into  $G'$  such that  $(h, g)$  is a crossed  $K$ -homomorphism of  $(M, G)$  into  $(M', G')$ . Thus, in this special case,  $h$  completely determines  $(h, g)$ . When both  $M$  and  $M'$  are principal homogeneous  $K$ -spaces, we have the identity

$$g(v_1^{-1}v_2) = (h(v_1)(v_1^{-1}v_2))^{-1}h(v_2).$$

Any crossed  $K$ -homomorphism of  $G$  into  $G'$  is also a crossed  $K$ -homomorphism of the regular  $K$ -space for  $G$  into the regular  $K$ -space for  $G'$  that is its own associated crossed  $K$ -homomorphism.

When the  $K$ -operation of  $G$  on  $(M', G')$  is trivial (that is, when  $v'x = v'$  ( $v' \in M', x \in G$ ) and  $x'x = x'$  ( $x' \in G, x \in G$ )), the notion of crossed  $K$ -homomorphism of  $(M, G)$  into  $(M', G')$  reduces to that of  $K$ -homomorphism of  $(M, G)$  into  $(M', G')$ .

We now return to the situation and notation of the last part of Section 20.

**Proposition 27** *Let  $G$  and  $G'$  be connected  $K$ -groups and let  $V$  and  $V'$  be principal homogeneous  $K$ -spaces for  $G$  and  $G'$ , respectively. Suppose that  $G$   $K$ -operates on  $V'$ , and for each  $x \in G$  let  $\gamma_x$  denote the relative  $K(x)$ -automorphism of  $V'$  given by the formula  $\gamma_x(v') = v'x$ . If  $h$  is any crossed  $K$ -homomorphism of  $V$  into  $V'$ , then*

$$\begin{aligned} h_{vx}^\# &= (\gamma_x \circ h)_v^\# = (\gamma_x)_{h(v)}^\# \circ h_v^\#, \\ h_{vx}^{\#\#} &= (\gamma_x \circ h)_v^{\#\#} = h_v^{\#\#} \circ (\gamma_x)_{h(v)}^{\#\#} \end{aligned}$$

for all  $v \in V$  and  $x \in G$ .

*Proof* For each  $x \in G$ , the identity  $h(vx) = h(v)x \cdot g(x)$  in  $v$  can be expressed in the form  $h \circ \rho_x = \rho_{g(x)} \circ \gamma_x \circ h$ . Referring to Eqs. (5) and (6) near the end of Section 20, we find that

$$\begin{aligned} h_{vx}^\# &= h_{vx}^\# \circ (\rho_x)_v^\# = (h \circ \rho_x)_v^\# = (\rho_{g(x)} \circ \gamma_x \circ h)_v^\# \\ &= (\rho_{g(x)})_{h(v)x}^\# \circ (\gamma_x)_{h(v)}^\# \circ h_v^\# \\ &= (\gamma_x)_{h(v)}^\# \circ h_v^\# = (\gamma_x \circ h)_v^\#. \end{aligned}$$

The rest quickly follows.

**Corollary 1** *If  $f: V \rightarrow V'$  is a relative  $K$ -homomorphism of principal homogeneous  $K$ -spaces for connected  $K$ -groups, then the linear mapping  $f_v^\#: \mathfrak{L}(V) \rightarrow \mathfrak{L}(V')$  is a Lie algebra homomorphism that is independent of  $v \in V$ .*

*Proof* For the trivial  $K$ -operation of  $G$  on  $V'$ ,  $\gamma_x = id_{V'}$  ( $x \in G$ ) and hence  $f$  is a crossed  $K$ -homomorphism of  $V$  into  $V'$ . Hence by the proposition,  $f_{vx}^\# = f_v^\#$  ( $v \in V, x \in G$ ), so that  $f_v^\#$  is independent of  $v$  and therefore may be denoted simply by  $f^\#$ .

To show that  $f^\#$  is a Lie algebra homomorphism, consider any  $D \in \mathfrak{L}(V)$  and any  $\varphi' \in \mathfrak{F}(V')$  such that  $\varphi' \circ f$  exists. For any  $v \in V$  such that  $\varphi' \in \mathfrak{F}_{f(v)}(V')$ , we can write

$$\begin{aligned} ((f^\#(D)\varphi') \circ f)(v) &= (f^\#(D)\varphi')(f(v)) = f^\#(D)_{f(v)}\varphi' \\ &= f_v^{\#\#}(D_v)\varphi' = D_v(f_v^\#(\varphi')) \\ &= D_v(\varphi' \circ f) = D(\varphi' \circ f)(v), \end{aligned}$$

so that  $(f^\#(D)\varphi') \circ f = D(\varphi' \circ f)$ , that is,

$$f_v^*(f^\#(D)\varphi') = D(f_v^*(\varphi')).$$

Therefore for any  $D, E \in \mathfrak{L}(V)$  and any  $\varphi'$  and  $v$  as above,

$$\begin{aligned} (f^\#(D)f^\#(E)\varphi')(f(v)) &= f^\#(D)_{f(v)}f^\#(E)\varphi' = f_v^{\#\#}(D_v)f^\#(E)\varphi' \\ &= D_v(f_v^*(f^\#(E)\varphi')) = D_v(E(f_v^*(\varphi'))) \\ &= D(E(f_v^*(\varphi')))(v). \end{aligned}$$

Interchanging  $D$  and  $E$  here, and then subtracting, we find that

$$\begin{aligned} [f^\#(D), f^\#(E)]_{f(v)}\varphi' &= ([f^\#(D), f^\#(E)]\varphi')(f(v)) = ([D, E]f_v^*(\varphi'))(v) \\ &= [D, E]_v(f_v^*(\varphi')) = f_v^{\#\#}([D, E]_v)\varphi' \\ &= f^\#([D, E])_{f(v)}\varphi', \end{aligned}$$

so that

$$f^\#([D, E])_{f(v)} = [f^\#(D), f^\#(E)]_{f(v)},$$

whence  $f^\#([D, E]) = [f^\#(D), f^\#(E)]$ .

**REMARK** We shall consistently use the notation  $f^\#$  for  $f_v^\#$  when  $f$  is a relative  $K$ -homomorphism of principal homogeneous  $K$ -spaces. Of course,  $f_v^{\#\#}$  is also independent of  $v$  and hence can be denoted by  $f^{\#\#}$ . We know that  $f^\#$  maps  $\mathfrak{L}_K(V)$  into  $\mathfrak{L}_{K(w)}(V')$  for every  $v$ , and hence that  $f^\#$  maps  $\mathfrak{L}_K(V)$  into  $\mathfrak{L}_K(V')$ . A proof similar to that of Corollary 1 shows that when the field characteristic  $p$  is not 0, then  $f^\#(D^p) = f^\#(D)^p$  for every  $D \in \mathfrak{L}(V)$ .

**Corollary 2** *Let  $H$  be a connected  $K$ -subgroup of the connected  $K$ -group  $G$ , and write  $in = in_{G, H}$  and  $\pi = \pi_{G/H}$ . The homomorphism  $in^\#: \mathfrak{L}(H) \rightarrow \mathfrak{L}(G)$  is injective. If  $H$  is normal in  $G$ , then  $in^\#(\mathfrak{L}(H))$  is an ideal of  $\mathfrak{L}(G)$  and the sequence*

$$0 \longrightarrow \mathfrak{L}(H) \xrightarrow{in^\#} \mathfrak{L}(G) \xrightarrow{\pi^\#} \mathfrak{L}(G/H) \longrightarrow 0$$

is exact.

*Proof* If  $E \in \text{Ker}(in^\#)$ , then the local component  $E_1$  is in  $\text{Ker}(in_1^{*\#})$ , that is,  $E_1 \circ in_1^{*\#} = 0$ . Since  $in_1^{*\#}$  is surjective by Section 19, Corollary 3 to Proposition 25, then  $E_1 = 0$ , whence  $E = 0$ . Thus,  $in^\#$  is injective. Now let  $H$  be normal. Since  $\pi^\# \circ in^\# = (\pi \circ in)^\# = 0$  (see Example 1, below),  $\text{Ker}(\pi^\#) \supset \text{Im}(in^\#)$ . If  $D \in \text{Ker}(\pi^\#)$ , then, for any  $\psi \in \mathfrak{F}(G/H)$ , we can fix an extension  $L$  of  $K$  with  $D \in \mathfrak{L}_L(G)$  and  $\psi \in \mathfrak{F}_L(G/H)$  and then fix  $x \in \Gamma_{G/L}$ . Then  $D(\pi^*(\psi))(x) = D_x(\pi_x^*(\psi)) = \pi_x^{*\#}(D_x)\psi = \pi^\#(D)_{\pi(x)}\psi = 0$ , whence  $D(\pi^*(\psi)) = 0$ . Thus,  $\text{Ker}(\pi^\#)$  is contained in the space of all derivations of the extension  $\mathfrak{F}(G)$  over  $\pi^*(\mathfrak{F}(G/H))$ . Since this extension is separable and of transcendence degree equal to  $\dim H = \dim \text{Im}(in^\#)$ , this space has dimension equal to this transcendence degree, so that  $\dim \text{Ker}(\pi^\#) \leq \dim \text{Im}(in^\#)$ , whence  $\text{Ker}(\pi^\#) = \text{Im}(in^\#)$ . A dimension argument now shows that  $\pi^\#$  is surjective and completes the proof.

We conclude this section with some examples.

**EXAMPLE 1** For any  $v' \in V'$  the constant mapping  $k_{v'}: V \rightarrow V'$  with value  $v'$  is a separable relative  $K(v')$ -homomorphism of  $V$  into  $V'$  and  $k_{v'}^\# = 0$ . Indeed, by Section 15, Proposition 17(e) and the fact that  $k_{v'}(v)^{-1}k_{v'}(vx) = 1$  for all  $(v, x) \in V \times G$ ,  $k_{v'}$  is a separable relative  $K(v')$ -homomorphism of  $V$  into  $V'$  and the associated  $K(v')$ -homomorphism of  $G$  into  $G'$  is the trivial one. For any  $v \in V$ , and for every  $\varphi' \in \mathfrak{F}_{v'}(V')$ ,  $(k_{v'})_v^*(\varphi')$  is a constant function and therefore  $(k_{v'})_v^{*\#}(T)\varphi' = T((k_{v'})_v^*(\varphi')) = 0$  for every  $T \in \mathfrak{D}_v(V)$ , so that  $(k_{v'})_v^{*\#} = 0$ , whence  $k_{v'}^\# = 0$ .

In the opposite direction, if  $f$  is any separable  $K$ -mapping of  $V$  into  $V'$  such that  $f_v^\# = 0$  for  $v \in \Gamma_{V/K}$ , then  $f = k_{v'}$  for some  $v' \in V'_K$ . Indeed, for any  $\varphi' \in \mathfrak{F}_{K, f(v)}(V')$  and any  $D \in \mathfrak{L}_K(V)$ , then  $(D(\varphi' \circ f))(v) = D_v(f_v^*(\varphi')) = f_v^{*\#}(D_v)\varphi' = f_v^\#(D_v)_{f(v)}\varphi' = 0$ , whence  $D(\varphi' \circ f) = 0$ . Hence  $D(\varphi' \circ f) = 0$  for every  $D \in \mathfrak{D}_K(V)$  and every  $\varphi' \in \mathfrak{F}_{K, f(v)}(V')$ , so that  $\delta(\varphi'(f(v))) = 0$  for every derivation  $\delta$  of  $K(v)$  over  $K$ , whence  $\delta(K(f(v))) = 0$ . Since  $K(v)$  is separable over  $K(f(v))$ ,  $f(v)$  must be algebraic over  $K$  and hence, because  $V$  is connected,  $f(v) \in V'_K$  and  $f$  is constant.

**EXAMPLE 2** For any  $x \in G$  the mapping  $\rho_x: V \rightarrow V$  is a  $K(x)$ -mapping of  $V$  into  $V$ . Since  $\rho_x(v)^{-1}\rho_x(vy) = (vx)^{-1}(vyx) = x^{-1}yx = \tau_{x^{-1}}(y)$ ,  $\rho_x$  is a relative  $K(x)$ -automorphism of  $V$  and  $\tau_{x^{-1}}$  is its associated  $K(x)$ -automorphism of  $G$ . We have seen (Section 20, Eq. (6)) that  $\rho_x^\# = id_{\mathfrak{L}(V)}$ .

**EXAMPLE 3** For any  $v \in V$  the mapping  $\lambda_v: G \rightarrow V$  is a  $K(v)$ -isomorphism of the regular  $K$ -space for  $G$  onto  $V$ . Therefore  $\lambda_v^\#: \mathfrak{L}(G) \rightarrow \mathfrak{L}(V)$  is an isomorphism of Lie algebras.

**EXAMPLE 4**  $V^2$  has a natural structure of principal homogeneous  $K$ -space for  $G^2$ . The canonical projections  $pr_1, pr_2$  of  $V^2$  into  $V$  are relative

$K$ -homomorphisms, the associated  $K$ -homomorphisms of  $G^2$  into  $G$  being the canonical projections of  $G^2$  into  $G$ . For each  $v \in V$  the injections  $i_{v_1}, i_{v_2}$  of  $V$  into  $V^2$ , given by the formulae  $i_{v_1}(w) = (w, v)$ ,  $i_{v_2}(w) = (v, w)$ , are relative  $K(v)$ -homomorphisms, the associated  $K(v)$ -homomorphisms of  $G$  into  $G^2$  being the canonical injections  $i_1, i_2$  of  $G$  into  $G^2$ . Evidently  $pr_1 \circ i_{v_1} = pr_2 \circ i_{v_2} = id_V$  and  $pr_1 \circ i_{v_2} = pr_2 \circ i_{v_1} = k_v$ . It follows that if  $a_1, a_2 \in U$  and  $D_1, D_2 \in \mathfrak{L}(V)$  and  $a_1 i_{v_1}^\#(D_1) + a_2 i_{v_2}^\#(D_2) = 0$ , then

$$\begin{aligned} 0 &= a_1 pr_1^\#(i_{v_1}^\#(D_1)) + a_2 pr_1^\#(i_{v_2}^\#(D_2)) \\ &= a_1 id_V^\#(D_1) + a_2 k_v^\#(D_2) = a_1 D_1 \end{aligned}$$

and, similarly,  $a_2 D_2 = 0$ . Thus, if  $a_1, a_2$  are not both 0, then  $a_1 i_{v_1}^\# + a_2 i_{v_2}^\#$  is injective (in particular,  $i_{v_1}^\#$  and  $i_{v_2}^\#$  are linearly independent over  $U$ ), and  $i_{v_1}^\#(\mathfrak{L}(V)) \cap i_{v_2}^\#(\mathfrak{L}(V)) = 0$ . Since

$$\dim \mathfrak{L}(V^2) = \dim V^2 = 2 \dim V = 2 \dim \mathfrak{L}(V),$$

we infer that

$$\mathfrak{L}(V^2) = i_{v_1}^\#(\mathfrak{L}(V)) + i_{v_2}^\#(\mathfrak{L}(V)) \quad (\text{direct sum}).$$

Thus, every element  $\hat{D}$  of  $\mathfrak{L}(V^2)$  can be expressed in the form  $\hat{D} = i_{v_1}^\#(D_1) + i_{v_2}^\#(D_2)$  with unique  $D_1, D_2 \in \mathfrak{L}(V)$ . If  $pr_1^\#(\hat{D}) = 0$ , then  $0 = id_V^\#(D_1) + k_v^\#(D_2) = D_1$ , and if  $pr_2^\#(\hat{D}) = 0$ , then  $D_2 = 0$ . Therefore

$$\text{Ker}(pr_1^\#) \cap \text{Ker}(pr_2^\#) = 0.$$

**EXAMPLE 5** The diagonal mapping  $\Delta_V: V \rightarrow V^2$ , given by the formula  $\Delta_V(w) = (w, w)$ , is a relative  $K$ -homomorphism, the derived  $K$ -homomorphism of  $G$  into  $G^2$  being  $\Delta_G$ . Evidently  $pr_1 \circ \Delta_V = pr_2 \circ \Delta_V = id_V$ , so that  $pr_1^\# \circ (\Delta_V - i_{v_1}^\# - i_{v_2}^\#) = id_V^\# - id_V^\# - k_v^\# = 0$  by Example 1, and similarly  $pr_2^\# \circ (\Delta_V - i_{v_1}^\# - i_{v_2}^\#) = 0$ . It follows from the last equation in Example 4 that

$$\Delta_V^\# = i_{v_1}^\# + i_{v_2}^\# \quad (v \in V).$$

**EXAMPLE 6** The formula  $(x, (x_1, x_2)) \mapsto x_1^{-1}xx_1$  defines a  $K$ -operation of  $G^2$  on  $G$ . For each  $(x_1, x_2) \in G^2$  the corresponding  $K(x_1, x_2)$ -automorphism  $\gamma_{(x_1, x_2)}$  of  $G$  is given by the formula  $\gamma_{(x_1, x_2)}(x) = x_1^{-1}xx_1$ . In particular,  $\gamma_{(1, x)} = id_G$ , whence  $\gamma_{(1, x)}^\# = id_{\mathfrak{L}(G)}$ . The mapping  $\psi: V^2 \rightarrow G$  given by the formula  $\psi(v, w) = v^{-1}w$  is a  $K$ -mapping, and  $\gamma_{(x_1, x_2)}(\psi(v, w))^{-1}\psi(vx_1, wx_2) = x_1^{-1}x_2$ . Therefore  $\psi$  is a crossed  $K$ -homomorphism of  $V^2$  into  $G$ . Evidently  $\lambda_v \circ \psi \circ i_{v_2} = id_V$  and  $\lambda_v \circ \psi \circ \Delta_V = k_v$ , so that  $\lambda_v^\# \circ \psi^\# \circ i_{v_2}^\# = id_{\mathfrak{L}(V)}$  and (by Examples 5 and 1)  $\lambda_v^\# \circ \psi^\# \circ i_{v_1}^\# = \lambda_v^\# \circ \psi^\# \circ (\Delta_V^\# - i_{v_2}^\#) = -id_{\mathfrak{L}(V)}$ . Hence

$$(\lambda_v^\# \circ \psi^\#_{(v, w)} + pr_1^\# - pr_2^\#) \circ i_{v_j}^\# = 0 \quad (j = 1, 2).$$

Since  $\mathfrak{Q}(V^2) = i_{v_1}^*(\mathfrak{Q}(V)) + i_{v_2}^*(\mathfrak{Q}(V))$  by Example 4, we conclude that

$$\lambda_v^* \circ \psi_{(v,w)}^* = pr_2^* - pr_1^* \quad (v, w \in V).$$

EXAMPLE 7 Let the connected  $K$ -group  $G$  be commutative. Then the group law  $\mu : G^2 \rightarrow G$  is a  $K$ -homomorphism. Because

$$\begin{aligned} \mu^* \circ (i_1^* - i_2^*) &= (\mu \circ i_1)^* - (\mu \circ i_2)^* = id_G^* - id_G^* = 0, \\ pr_2^* \circ i_1^* &= 0, \quad pr_1^* \circ i_2^* = 0, \end{aligned}$$

we see that

$$\text{Im}(i_1^* - i_2^*) \subset \text{Ker}(\mu^*), \quad \text{Im}(i_1^*) \subset \text{Ker}(pr_2^*), \quad \text{Im}(i_2^*) \subset \text{Ker}(pr_1^*).$$

However, by Example 4 the linear mappings  $i_1^* - i_2^*, i_1^*, i_2^*$  are injective, so their images have dimension equal to  $\dim \mathfrak{Q}(G)$ ; also

$$\begin{aligned} \dim \text{Ker}(\mu^*) &= \dim \mathfrak{Q}(G^2) - \dim \text{Im}(\mu^*) \\ &\leq 2 \dim \mathfrak{Q}(G) - \dim \text{Im}(\mu^* \circ i_1^*) \\ &= 2 \dim \mathfrak{Q}(G) - \dim \text{Im}(id_{\mathfrak{Q}(G)}) = \dim \mathfrak{Q}(G), \end{aligned}$$

and similarly  $\dim \text{Ker}(pr_2^*) = \dim \text{Ker}(pr_1^*) \leq \dim \mathfrak{Q}(G)$ . Therefore

$$\text{Im}(i_1^* - i_2^*) = \text{Ker}(\mu^*), \quad \text{Im}(i_1^*) = \text{Ker}(pr_2^*), \quad \text{Im}(i_2^*) = \text{Ker}(pr_1^*),$$

so that the three images are ideals of  $\mathfrak{Q}(G^2)$  and (by the last equation in Example 4)

$$\text{Im}(i_1^*) \cap \text{Im}(i_2^*) = 0. \tag{7}$$

It follows that if  $D_1, D_2$  are any elements of  $\mathfrak{Q}(G)$ , then there exists an element  $D_3 \in \mathfrak{Q}(G)$  such that

$$[i_1^*(D_1), i_1^*(D_2) - i_2^*(D_2)] = i_1^*(D_3) - i_2^*(D_3),$$

and also  $[i_1^*(D_1), i_2^*(D_2)] = 0$ , so that

$$\begin{aligned} i_1^*([D_1, D_2]) &= [i_1^*(D_1), i_1^*(D_2) - i_2^*(D_2)] \\ &= i_1^*(D_3) - i_2^*(D_3), \end{aligned}$$

$$i_1^*(D_3 - [D_1, D_2]) = i_2^*(D_3).$$

Since both sides of this equation must be 0 by (7), and since  $i_2^*$  and  $i_1^*$  are injective, we conclude that  $[D_1, D_2] = 0$ . This shows that if  $G$  is commutative, then so is  $\mathfrak{Q}(G)$ . The converse of this statement is false when  $p \neq 0$  (see Section 18, Exercise 3 and Exercise 1(d)) and true when  $p = 0$  (see Section 22, Exercise 3).

EXERCISES

1. Let  $f : V \rightarrow V'$  be a relative  $K$ -homomorphism of principal homogeneous  $K$ -spaces for connected  $K$ -groups, and suppose that  $p \neq 0$ . Prove the remark (made after the proof of the corollary to Proposition 27) that  $f^*(D^p) = f^*(D)^p$  for every  $D \in \mathfrak{Q}(V)$ .
2. (Borel's closed orbit lemma) Let  $M$  be a  $K$ -space for a  $K$ -group  $G$ . For each  $v \in M$  let  $M_v$  denote the smallest closed subset of  $M$  that contains the orbit  $vG$ . Prove that  $M_v$  is a  $K(v)$ -subspace of  $M$  for  $G$ , that the components of  $M_v$  all have the same dimension, that  $vG$  is  $K(v)$ -open in  $M_v$ , and that  $\dim(M_v - vG) < \dim M_v$ . Conclude that when  $v$  is chosen so that  $\dim M_v$  is minimal, then  $vG$  is closed.
3. (Generalization of the result in Example 7) Let  $G$  be a connected  $K$ -group. Denote the commutator subgroup of  $G$  by  $[G, G]$  and the commutator subalgebra of  $\mathfrak{Q}(G)$  by  $[\mathfrak{Q}(G), \mathfrak{Q}(G)]$ , so that  $[G, G]$  is a normal connected  $K$ -subgroup of  $G$  (see Section 10, Proposition 14) and  $[\mathfrak{Q}(G), \mathfrak{Q}(G)]$  is an ideal of  $\mathfrak{Q}(G)$ . Prove that

$$[\mathfrak{Q}(G), \mathfrak{Q}(G)] \subset in^* \mathfrak{Q}([G, G]),$$

where  $in = in_{G, [G, G]}$ . (Hint: Use Example 7 and Corollary 2 of Proposition 27.)

4. Let  $G$  be a connected  $K$ -group, fix a basis  $(D_1, \dots, D_n)$  of  $\mathfrak{Q}_K(G)$ , and for each  $x \in G$  let  $A(x) = (A_{ij}(x))$  denote the matrix such that  $\tau_x^*(D_j) = \sum_{1 \leq i \leq n} A_{ij}(x) D_i$  ( $1 \leq j \leq n$ ). Prove that the formula  $x \mapsto A(x)$  defines a  $K$ -homomorphism  $A : G \rightarrow \text{GL}(n)$  with kernel containing the center of  $G$ . (Hint: Use the penultimate displayed equation in Section 20 to show that  $\sigma(A(x)) = A(\sigma x)$  for every  $\sigma \in \text{Aut}(U/K)$ .)

22 Logarithmic derivatives

Let  $G$  be a connected  $K$ -group and  $V$  be a principal homogeneous  $K$ -space for  $G$ . Let  $L$  be a field (over which  $U$  may have finite transcendence degree) with  $L \supset K$ , and let  $\delta$  be a derivation of  $L$  over  $K$ .

For any element  $v \in V_L$  we can define a mapping  $\mathfrak{F}_{K,v}(V) \rightarrow U$  by the formula  $\varphi \mapsto \delta(\varphi(v))$ . This mapping is evidently a local derivation of  $\mathfrak{F}_{K,v}(V)$  at  $v$  and therefore (see Section 20) can be extended to a unique tangent vector  $\delta_v \in \mathfrak{T}_v(V)$ . The inverse of the canonical isomorphism  $\mathfrak{Q}(V) \approx \mathfrak{T}_v(V)$  (see Section 20) maps  $\delta_v$  onto an invariant derivation that we denote by  $l\delta(v)$  and call the logarithmic derivative of  $v$  (relative to  $\delta$ ). Thus, the invariant derivation  $l\delta(v)$  is characterized by the condition that

$$l\delta(v)_v \varphi = \delta(\varphi(v))$$

for every  $\varphi \in \mathfrak{F}_{K,v}(V)$  (and hence also for every  $\varphi \in F_{L,v}(V)$ , where  $L_\delta$  is the kernel of  $\delta$ ). We call the mapping

$$l\delta : V_L \rightarrow \mathfrak{L}(V)$$

the logarithmic derivation on  $V_L$  (relative to  $\delta$ ).

**Proposition 28** *Let  $L$  be a field (over which  $U$  may have finite transcendence degree) such that  $L \supset K$  and let  $\delta$  be a derivation of  $L$  over  $K$ . Let  $V$  be a principal homogeneous  $K$ -space for a connected  $K$ -group, and let  $v \in V_L$ . Set  $K_v = K(v) \cdot K(\delta(K(v)))$ .*

- (a)  $l\delta(v) \in \mathfrak{L}_{K_v}(V)$ .
- (b) If  $\sigma$  is an isomorphism of  $K_v$  over  $K$  onto an extension of  $K$  lying in  $L$  such that  $\sigma\delta\alpha = \delta\sigma\alpha$  for every  $\alpha \in K(v)$ , then  $\sigma(l\delta(v)) = l\delta(\sigma v)$ .
- (c)  $l\delta(v) = 0$  if and only if  $\delta(K(v)) = 0$ .

*Proof* (a) For any  $\varphi \in \mathfrak{F}_{K,v}(V)$ ,  $l\delta(v)_v\varphi = \delta(\varphi(v)) \in K_v$ , and hence (by Section 19, Proposition 25)  $l\delta(v)_v\varphi \in K_v$  for every  $\varphi \in \mathfrak{F}_{K,v}(V)$ . Thus,  $l\delta(v)_v \in \mathfrak{L}_{K_v,v}(V)$ , whence  $l\delta(v) \in \mathfrak{L}_{K_v}(V)$ .

(b) We have  $\sigma(\mathfrak{F}_{K,v}(V)) = \mathfrak{F}_{K,\sigma v}(V)$  and, for every  $\varphi \in \mathfrak{F}_{K,v}(V)$ ,

$$\begin{aligned} \sigma(l\delta(v))_{\sigma v}\sigma(\varphi) &= (\sigma(l\delta(v))\sigma(\varphi))(\sigma v) = \sigma(l\delta(v)\varphi)(\sigma v) = \sigma((l\delta(v)\varphi)(v)) \\ &= \sigma(l\delta(v)_v\varphi) = \sigma(\delta(\varphi(v))) = \delta(\sigma(\varphi(v))) \\ &= \delta(\sigma(\varphi)(\sigma v)) = l\delta(\sigma v)_{\sigma v}\sigma(\varphi); \end{aligned}$$

therefore  $\sigma(l\delta(v))_{\sigma v} = l\delta(\sigma v)_{\sigma v}$ , whence  $\sigma(l\delta(v)) = l\delta(\sigma v)$ .

(c) By Section 19, Proposition 25, we have

$$\begin{aligned} l\delta(v) = 0 &\Leftrightarrow l\delta(v)_v\varphi = 0 \quad (\varphi \in \mathfrak{F}_{K,v}(V)) \\ &\Leftrightarrow \delta(\varphi(v)) = 0 \quad (\varphi \in \mathfrak{F}_{K,v}(V)) \\ &\Leftrightarrow \delta(K(v)) = 0 \end{aligned}$$

**Proposition 29** *Let  $L$  be an extension of  $K$ , over which  $U$  may have finite transcendence degree, and let  $\delta$  be a derivation of  $L$  over  $K$ . Let  $V$  and  $V'$  be principal homogeneous  $K$ -spaces for connected  $K$ -groups, let  $v \in V_L$ , and let  $f \in \mathfrak{M}_{K,v}(V, V')$ . Then*

$$f_v^*(l\delta(v)) = l\delta(f(v)).$$

*Proof* For any  $\varphi' \in \mathfrak{F}_{K,f(v)}(V')$ ,

$$\begin{aligned} f_v^*(l\delta(v))_{f(v)}\varphi' &= f_v^{**}(l\delta(v)_v)\varphi' = l\delta(v)_v f_v^*(\varphi') \\ &= \delta(f_v^*(\varphi')(v)) = \delta(\varphi'(f(v))) \\ &= l\delta(f(v))_{f(v)}\varphi'. \end{aligned}$$

Therefore  $f_v^*(l\delta(v))_{f(v)} = l\delta(f(v))_{f(v)}$ , whence the desired equation.

Now,  $G$  itself is a principal homogeneous  $K$ -space for  $G$ , and  $\lambda_v$  is an everywhere defined  $K(v)$ -mapping (and even is a  $K(v)$ -isomorphism) of  $G$  into  $V$ . If  $x \in G_L$  and  $v$  satisfies the condition  $\delta(K(v)) = 0$ , it follows from Proposition 29 (with  $K, V, V', v, f$  now  $K(v), G, V, x, \lambda_v$ ) that  $l\delta(vx) = \lambda_v^*(l\delta(x))$ . Without this condition we have the following important generalization.

**Theorem 14** *Let  $L$  be an extension of  $K$ , over which  $U$  may have finite transcendence degree, and let  $\delta$  be a derivation of  $L$  over  $K$ . Let  $V$  be a principal homogeneous  $K$ -space for the connected  $K$ -group  $G$ , and let  $(v, x) \in V_L \times G_L$ . Then*

$$l\delta(vx) = l\delta(v) + \lambda_v^*(l\delta(x)).$$

*Proof* Recall from Section 21, Example 6, that the mapping  $\psi : V^2 \rightarrow G$  given by the formula  $\psi(v_1, v_2) = v_1^{-1}v_2$  is a crossed  $K$ -homomorphism of  $V^2$  into  $G$ , and that  $\lambda_{v_1}^* \circ \psi_{(v_1, v_2)}^* = pr_2^* - pr_1^*$  for all  $v_1, v_2 \in V$ . Therefore

$$\begin{aligned} \lambda_v^*(l\delta(x)) &= \lambda_v^*(l\delta(\psi(v, vx))) \\ &= \lambda_v^*(\psi_{(v, vx)}^*(l\delta(v, vx))) \\ &= (pr_2^* - pr_1^*)(l\delta(v, vx)) \\ &= l\delta(pr_2(v, vx)) - l\delta(pr_1(v, vx)) \\ &= l\delta(vx) - l\delta(v). \end{aligned}$$

**REMARK** When  $V$  is  $G$ , then  $\lambda_v = \tau_v \circ \rho_v$ . Because  $\rho_v^* = id_{\mathfrak{L}(G)}$ , we see that  $\lambda_v^* = \tau_v^*$ . Thus, as a special case of Theorem 14,

$$l\delta(xy) = l\delta(x) + \tau_x^*(l\delta(y)) \quad (x, y \in G_L).$$

Of course, when  $G$  is commutative then this reduces to the identity

$$l\delta(xy) = l\delta(x) + l\delta(y) \quad (x, y \in G_L).$$

**Corollary** *Let  $G$  be a connected commutative  $K$ -group and let  $r \in \mathbb{N}$ ,  $p \nmid r$ . The mapping  $G \rightarrow G$  given by the formula  $x \mapsto x^r$  is a surjective  $K$ -endomorphism of  $G$  with finite kernel.*

*Proof* It is easy to see that the mapping is a  $K$ -endomorphism. Its kernel  $N$  is a  $K$ -closed subgroup of  $G$ . Taking  $x \in \Gamma_{N^0/K_1}$ , we see that if  $\delta$  is any derivation of  $K_i(x)$  over  $K_1$ , then  $rl\delta(x) = l\delta(x^r) = l\delta(1) = 0$  so that  $l\delta(x) = 0$  and  $\delta(K_1(x)) = 0$ . Therefore  $x$  is algebraic over  $K_1$ , so that  $\dim N = 0$  (that is,  $N$  is finite). The image of the endomorphism is a closed subgroup of  $G$  of dimension equal to  $\dim G - \dim N = \dim G$ , and therefore is  $G$ .

We conclude this section with some examples. They should be read in conjunction with the corresponding examples at the end of Section 18, the notation of which we use here.

EXAMPLE 1 For any  $x \in (G_a)_L$ ,

$$l\delta(x)_x \xi = \delta(\xi(x)) = \delta x = ((\delta x)(d/d\xi) \xi)(x) = ((\delta x) d/d\xi)_x \xi.$$

However, by Section 19, Proposition 25,  $\mathfrak{F}_x(G_a)$  is the localization of  $U[\xi]$  at its prime ideal  $U[\xi] \cap \mathfrak{m}_x(G_a)$ , so that  $l\delta(x)_x = ((\delta x) d/d\xi)_x$ , whence  $l\delta(x) = (\delta x) d/d\xi$  and  $\langle l\delta(x), d\xi \rangle = \delta x$ .

EXAMPLE 2 For any  $x \in (G_m)_L$ ,

$$l\delta(x)_x \xi = \delta(\xi(x)) = \delta x = ((\delta x \cdot x^{-1}) \xi (d/d\xi) \xi)(x) = ((\delta x \cdot x^{-1}) \xi d/d\xi)_x \xi.$$

As in Example 1, we conclude with the help of Proposition 25 that  $l\delta(x) = (\delta x \cdot x^{-1}) \xi d/d\xi$  and  $\langle l\delta(x), \xi^{-1} d\xi \rangle = \delta x \cdot x^{-1}$ .

EXAMPLE 3 Let  $p \neq 2$ . For any  $z = (1:x:y) \in \mathbf{W}_L = \mathbf{W}_L(g_2, g_3)$  other than  $(0:0:1)$  and the three elements with  $y = 0$ ,  $l\delta(z)_z \xi = \delta(\xi(z)) = \delta x = ((\delta x \cdot y^{-1}) \eta (d/d\xi) \xi)(z) = ((\delta x \cdot y^{-1}) \eta d/d\xi)_z \xi$ . From the equation  $\eta^2 = 4\xi^3 - g_2 \xi - g_3$  we infer that also  $l\delta(z)_z \eta = ((\delta x \cdot y^{-1}) \eta d/d\xi)_z \eta$ . By Proposition 25, hence  $l\delta(z) = (\delta x \cdot y^{-1}) \eta d/d\xi$  and  $\langle l\delta(z), \eta^{-1} d\xi \rangle = \delta x \cdot y^{-1}$ .

EXAMPLE 4 For any  $x = (x_{ij}) \in \mathbf{GL}_L(n)$ , if we set  $x^{-1} = (y_{ij})$ , then

$$\begin{aligned} l\delta(x)_x \xi_{ij} &= \delta(\xi_{ij}(x)) = \delta x_{ij} \\ &= \left( \sum_{\kappa, \lambda, \mu, \nu} (\delta x_{\kappa\lambda} \cdot y_{\lambda\mu}) \xi_{\mu\nu} (\partial/\partial \xi_{\kappa\nu}) \xi_{ij} \right) (x) \\ &= \left( \sum_{\kappa, \mu} \left( \sum_{\lambda} \delta x_{\kappa\lambda} \cdot y_{\lambda\mu} \right) \sum_{\nu} \xi_{\mu\nu} \partial/\partial \xi_{\kappa\nu} \right)_x \xi_{ij} \end{aligned}$$

for every  $(i, j)$ , and therefore  $l\delta(x) = \sum_{\kappa, \mu} (\sum_{\lambda} \delta x_{\kappa\lambda} \cdot y_{\lambda\mu}) \sum_{\nu} \xi_{\mu\nu} \partial/\partial \xi_{\kappa\nu}$ . In matrix notation this can be written as  $l\delta(x) = \text{Tr}(\delta x \cdot x^{-1} \xi \partial/\partial \xi)$ . An easy computation shows that  $\langle l\delta(x), \sum_{\nu} \eta_{\nu j} d\xi_{i\nu} \rangle_{1 \leq i \leq n, 1 \leq j \leq n} = \delta x \cdot x^{-1}$ .

EXERCISES

1. Let  $G$  be a connected  $K$ -subgroup of  $\mathbf{GL}(n)$  and consider the Lie algebra isomorphism  $\nabla: \mathfrak{L}(G) \approx \mathfrak{l}(G)$  defined in Section 18, Exercise 1. Show that if  $L$  is an extension of  $K$   $x \in G_L$ , and  $\delta$  is a derivation of  $L$  over  $K$ , then  $\nabla(l\delta(x)) = \delta x \cdot x^{-1}$ .
2. Let  $G$  be a connected  $K$ -group,  $L$  be an extension of  $K$  (over which the transcendence degree of  $U$  need not be infinite),  $x \in G_L$ , and  $\delta$  be a derivation of  $L$  over  $K$ . Let  $\delta^*$  denote the derivation of  $\mathfrak{F}_L(G)$  over

$\mathfrak{F}_K(G)$  that extends  $\delta$  (see Section 16, Exercise 3), and let  $\delta^*$  denote the derivation of  $\mathfrak{Q}_L(G)$  defined by the formula  $\delta^*(D) = [\delta^*, D_L]$  (see Section 18, Exercise 4).

(a) Prove that if  $\varphi \in \mathfrak{F}_{K,x}(G)$ , then  $\delta^*(\lambda_x^*(\varphi)) = \lambda_x^*(l\delta(x)\varphi)$ . (Hint: Using the last part of Section 18, Exercise 4, and properties of  $l\delta$ , show that the two  $L$ -functions are defined and agree at every element  $z \in G_K$  at which  $\lambda_x^*(\varphi)$  is defined.)

(b) Prove that if  $D \in \mathfrak{Q}_L(G)$ , then

$$\tau_x^*(\delta^*(D)) = \delta^*(\tau_x^*(D)) + [l\delta(x), \tau_x^*(D)].$$

(Hint: First take  $D \in \mathfrak{Q}_K(G)$  and show that for all  $\varphi \in \mathfrak{F}_{K,x}$

$$\begin{aligned} \tau_x^*(\delta^*(\tau_{x^{-1}}^*(D)))_x \varphi &= (\tau_x^*)^*(\delta^*(\tau_{x^{-1}}^*(D)))_x \varphi \\ &= (\lambda_x)_1^*(\delta^*(\tau_{x^{-1}}^*(D)))_1 \varphi \\ &= \delta^*(\tau_{x^{-1}}^*(D))_1 (\lambda_x^*(\varphi)) \\ &= \delta(\tau_{x^{-1}}^*(D))_1 (\lambda_x^*(\varphi)) - \tau_{x^{-1}}^*(D)_1 (\delta^*(\lambda_x^*(\varphi))) \\ &= \delta(D_1(\tau_{x^{-1}}^*(\lambda_x^*(\varphi)))) - D_1(\tau_{x^{-1}}^*(\lambda_x^*(l\delta(x)\varphi))) \\ &= \delta(D_x \varphi) - D_x(l\delta(x)\varphi) = [l\delta(x), D]_x \varphi, \end{aligned}$$

whence  $\tau_x^*(\delta^*(\tau_{x^{-1}}^*(D))) = [l\delta(x), D]$ . Then infer that, for any  $D \in \mathfrak{Q}_L(G)$ ,  $\tau_x^*(\delta^*(\tau_{x^{-1}}^*(D))) = \delta^*(D) + [l\delta(x), D]$ .)

(c) Prove that if  $\delta_1, \delta_2$  are derivations of  $L$  over  $K$ , then

$$\delta_2^*(l\delta_1(x)) - \delta_1^*(l\delta_2(x)) = [l\delta_1(x), l\delta_2(x)] - l[\delta_1, \delta_2](x).$$

(Hint: Show for any  $\varphi \in \mathfrak{F}_{K,x}(G)$  that

$$\begin{aligned} \tau_x^*(\delta_1^*(\tau_{x^{-1}}^*(l\delta_2(x))))_x \varphi &= \tau_x^*(\delta_1^*(\tau_{x^{-1}}^*(l\delta_2(x))))_1 \rho_x^*(\varphi) \\ &= \delta_1^*(\tau_{x^{-1}}^*(l\delta_2(x)))_1 \lambda_x^*(\varphi) \\ &= \delta_1(\tau_{x^{-1}}^*(l\delta_2(x)))_1 \lambda_x^*(\varphi) \\ &\quad - \tau_{x^{-1}}^*(l\delta_2(x))_1 (\delta_1^*(\lambda_x^*(\varphi))) \\ &= \delta_1(l\delta_2(x))_1 (\rho_x^*(\varphi)) \\ &\quad - l\delta_2(x)_1 (\tau_{x^{-1}}^*(\lambda_x^*(l\delta_1(x)\varphi))) \\ &= \delta_1(l\delta_2(x))_x \varphi - l\delta_2(x)_x l\delta_1(x)\varphi \\ &= \delta_1 \delta_2(\varphi(x)) - l\delta_2(x)_x l\delta_1(x)\varphi, \end{aligned}$$

and infer by part (b) that

$$\delta_1^*(l\delta_2(x))_x \varphi + [l\delta_1(x), l\delta_2(x)]_x \varphi = \delta_1 \delta_2(\varphi(x)) - l\delta_2(x)_x l\delta_1(x)\varphi;$$

then interchange  $\delta_1, \delta_2$  and subtract.)

3. (Partial converse of Section 21, Example 7) Let  $G$  be a connected  $K$ -group and suppose that  $p = 0$ . Prove that if  $\mathfrak{U}(G)$  is commutative, then so is  $G$ . (Hint: Let  $(x, y) \in \Gamma_{G^2/K}$  and consider the  $K$ -homomorphism  $A : G \rightarrow \mathbf{GL}(n)$  in Section 21, Exercise 4. Use Exercise 2(b), to show that  $\delta(K(A(x))) = 0$  for every derivation  $\delta$  of  $K(x)$  over  $K$ , infer that  $K(A(x)) \subset K_{\mathfrak{a}}$ , and hence that  $\tau_x^{\#} = id_{\mathfrak{U}(G)}$ . Deduce by Theorem 14 that  $\delta(xy) = \delta(yx)$  for every derivation  $\delta$  of  $K(x, y)$  over  $K$ , and hence that  $K(x^{-1}y^{-1}xy) \subset K_{\mathfrak{a}}$ , and conclude that  $x^{-1}y^{-1}xy = 1$ .)

### 23 Linear $K$ -groups

#### A. DEFINITION AND ELEMENTARY PROPERTIES

Let  $G$  be a  $K$ -group. If  $G$  is  $K$ -isomorphic to a  $K$ -subgroup of  $\mathbf{GL}(n)$  for some  $n$ , then it is obvious that  $G$  is  $K$ -affine in  $G$  (see the definition in Section 16).

If for some  $n$  there exist a  $K$ -subset  $B$  of  $\mathbf{G}_a^n$  and a generically invertible  $f \in \mathfrak{M}_K(G, B)$  that is bidefined on  $G$ , then  $f(G)$  is a dense  $K$ -open subset of  $B$ , the canonical coordinate functions  $\xi_1, \dots, \xi_n$  on  $B$  (given by the equations  $\xi_j = pr_j \circ in_{\mathbf{G}_a^n, B}$ ) are elements of  $\mathfrak{F}_{K, f(G)}(B)$  with the property that  $\mathfrak{F}_K(B) = Q(K[\xi_1, \dots, \xi_n])$ , and  $\mathfrak{F}_K(G) = f^*(\mathfrak{F}_K(B)) = f^*(Q(K[\xi_1, \dots, \xi_n])) = Q(K[f^*(\xi_1), \dots, f^*(\xi_n)])$ . Since  $f^*(\xi_j) = \xi_j \circ f \in \mathfrak{F}_{K, G}(G)$ , this shows that if  $G$  is  $K$ -affine in  $G$ , then  $\mathfrak{F}_K(G) = Q(\mathfrak{F}_{K, G}(G))$ .

Now suppose that  $\mathfrak{F}_K(G) = Q(\mathfrak{F}_{K, G}(G))$ . Since  $\mathfrak{F}_K(G)$  is the complete ring of quotients of a finitely generated algebra over  $K$  (indeed, is the direct product of a finite number of finitely generated extensions of  $K$ ), it follows that there is a finite subset  $\Phi$  of  $\mathfrak{F}_{K, G}(G)$  such that  $\mathfrak{F}_K(G) = Q(K[\Phi])$ . By Section 16, corollary to Proposition 23, we can write  $\mathfrak{F}_K(G) = Q(K[\varphi_1, \dots, \varphi_n])$  with elements  $\varphi_1, \dots, \varphi_n \in \mathfrak{F}_{K, G}(G)$  that are linearly independent over  $U$  and have the property that  $\rho_x^*(\varphi_j) = \sum_j \psi_{jj'}(x) \varphi_j$  ( $1 \leq j' \leq n, x \in G$ ), the  $\psi_{jj'}$  being everywhere defined  $K$ -functions on  $G$  such that the formula  $x \mapsto (\psi_{jj'}(x))$  defines a  $K$ -homomorphism  $\Psi : G \rightarrow \mathbf{GL}(n)$ . If  $x \in \text{Ker}(\Psi)$ , then  $\rho_x^*(\varphi_j) = \varphi_j$  ( $1 \leq j' \leq n$ ), so that  $\rho_x^*(\xi) = \xi$  for every  $\xi \in Q(K[\varphi_1, \dots, \varphi_n]) = \mathfrak{F}_K(G)$ , whence  $x = 1$ . Thus  $\Psi$  is injective. If  $x \in \Gamma_{G/K}$ , then  $K(x) = K(\varphi_1(x), \dots, \varphi_n(x))$  and  $\varphi_j(x) = \rho_x^*(\varphi_j)(1) = \sum_j \varphi_j(1) \psi_{jj'}(x) \in K(\Psi(x))$ , so that  $K(x) = K(\Psi(x))$ . This shows that  $\Psi$  induces a  $K$ -isomorphism of  $G$  onto the  $K$ -subgroup  $\Psi(G)$  of  $\mathbf{GL}(n)$ .

**Proposition 30** Let  $G$  be a  $K$ -group and choose an extension  $L$  of  $K$ . The following three conditions are equivalent and are independent of the choice of  $L$ .

- (a) For some  $n$ ,  $G$  is  $L$ -isomorphic to an  $L$ -subgroup of  $\mathbf{GL}(n)$ .
- (b)  $G$  is  $L$ -affine in  $G$ .
- (c)  $\mathfrak{F}_L(G) = Q(\mathfrak{F}_{L, G}(G))$ .

*Proof* The preceding discussion, with  $K$  replaced by  $L$ , shows that the three conditions are equivalent. If  $G$  is  $K$ -affine in  $G$ , then obviously  $G$  is  $L$ -affine in  $G$ . To complete the proof, it suffices to show that if (c) is satisfied, then it remains satisfied when  $L$  is replaced by  $K$ , that is, then for any  $\varphi \in \mathfrak{F}_K(G)$ ,  $\varphi \in Q(\mathfrak{F}_{K, G}(G))$ . To show this, fix a basis  $(u_i)_{i \in I}$  of  $L$  over  $K$ . By Section 16, Proposition 22,  $(u_i)$  is a basis of  $\mathfrak{F}_{L, G}(G)$  over  $\mathfrak{F}_{K, G}(G)$  too. Because of (c), there exist  $\psi, \chi \in \mathfrak{F}_{L, G}(G)$ , with  $\chi$  not a divisor of 0, such that  $\varphi\chi - \psi = 0$ . Writing  $\psi = \sum \psi_i u_i$ ,  $\chi = \sum \chi_i u_i$  with  $\psi_i, \chi_i \in \mathfrak{F}_{K, G}(G)$ , we find that  $\sum (\varphi\chi_i - \psi_i) u_i = 0$  and hence that  $\varphi\chi_i - \psi_i = 0$  ( $i \in I$ ). Because  $\chi$  is not a divisor of 0 in  $\mathfrak{F}_{L, G}(G)$ ,  $\chi$  does not vanish at any element of  $\Gamma_{G/L}$ . Letting  $V_1, \dots, V_r$  denote the  $K$ -components of  $G$ , we can, for each index  $k$ , fix  $x_k \in \Gamma_{V_k/K}$  such that  $x_k \in \Gamma_{V_k/L} \subset \Gamma_{G/L}$ . Then there exists an index  $i(k) \in I$  such that  $\chi_{i(k)}(x_k) \neq 0$ . Of course,  $\psi_{i(k)} \circ in_{G, V_k}$  and  $\chi_{i(k)} \circ in_{G, V_k}$  are everywhere defined  $K$ -functions on  $V_k$ . Let  $\xi$  and  $\eta$  denote the unique  $K$ -functions on  $G$  such that

$$\xi \circ in_{G, V_k} = \psi_{i(k)} \circ in_{G, V_k}, \quad \eta \circ in_{G, V_k} = \chi_{i(k)} \circ in_{G, V_k} \quad (1 \leq k \leq r).$$

Evidently  $\xi, \eta \in \mathfrak{F}_{K, G}(G)$ ,  $\eta$  is not a divisor of 0 in  $\mathfrak{F}_{K, G}(G)$ , and  $\varphi\eta - \xi = 0$ . Therefore

$$\varphi \in Q(\mathfrak{F}_{K, G}(G)).$$

A  $K$ -group that satisfies the conditions in Proposition 30 is said to be *linear* (or *affine*). Thus, the groups  $\mathbf{SL}(n), \mathbf{O}(n), \mathbf{T}(n), \mathbf{T}(n, k)$  ( $1 \leq k \leq n$ ),  $\mathbf{D}(n)$  defined in Section 1, all of which are  $K'$ -subgroups of  $\mathbf{GL}(n)$  for every field  $K'$ , are linear, as are  $\mathbf{G}_a$  and  $\mathbf{G}_m$ .

If  $G$  is a  $K$ -subgroup of  $\mathbf{GL}(n)$ , the function  $\xi_{ij} : G \rightarrow \mathbf{G}_a$  that maps an arbitrary matrix  $(x_{ij})_{1 \leq i, j \leq n}$  onto its  $(i, j)$ -coordinate  $x_{ij}$  is an everywhere defined  $K$ -function on  $G$ . The  $n^2$  functions  $\xi_{ij}$  form a system of  $K$ -affine coordinates on  $G$  at each element of  $G$ , and are called the *canonical coordinate functions* on  $G$ . The family (that is, the matrix)  $\xi = (\xi_{ij})_{1 \leq i \leq n, 1 \leq j \leq n}$  has the property that  $\det \xi$  is a unit in the ring  $\mathfrak{F}_{K, G}(G)$ .

**Proposition 31** Let  $G$  be a  $K$ -subgroup of  $\mathbf{GL}(n)$  and let  $\xi = (\xi_{ij})$  denote the matrix of canonical coordinate functions on  $G$ . Then  $\mathfrak{F}_{K, G}(G) = K[\xi, 1/\det \xi]$ .

*Proof* Let  $\varphi \in \mathfrak{F}_{K, G}(G)$ . For any  $x \in G$ , there exist polynomials  $P_x, Q_x \in K[(X_{ij})_{1 \leq i \leq n, 1 \leq j \leq n}]$  with  $Q_x(x) \neq 0$  such that  $Q_x(\xi)\varphi - P_x(\xi) = 0$ . Let  $\mathfrak{a}$  denote the ideal of all polynomials in  $K[(X_{ij})_{1 \leq i \leq n, 1 \leq j \leq n}]$  that vanish at every element of  $G$ . Each zero of  $\mathfrak{a}$  that is not a zero of  $\det(X_{ij})$  is an element

of  $G$ . It follows that a zero of  $\alpha$  that is a zero of every  $Q_x$  must be a zero of  $\det(X_{ij})$ . Therefore some power of  $\det(X_{ij})$  is in the ideal  $\alpha + \sum_{x \in G} (Q_x)$ , that is, there exist an exponent  $e \in \mathbb{N}$ , finitely many elements  $x_1, \dots, x_r \in G$ , and polynomials  $C_1, \dots, C_r \in K[(X_{ij})]$  such that  $\det(X_{ij})^e \equiv \sum C_k Q_{x_k} \pmod{\alpha}$ , whence  $\det \xi^e = \sum C_k(\xi) Q_{x_k}(\xi)$ . Therefore

$$\varphi \det \xi^e = \sum C_k(\xi) Q_{x_k}(\xi) \varphi = \sum C_k(\xi) P_{x_k}(\xi)$$

and  $\varphi \in K[\xi, 1/\det \xi]$ .

**Proposition 32** (a) Every  $K$ -subgroup of a linear  $K$ -group is linear.

(b) A direct product of linear  $K$ -groups is linear.

(c) If  $G$  is a  $K$ -group and  $G^\circ$  is linear, then  $G$  is linear.

(d) If  $G$  is a  $K$ -group and there exists a surjective  $K$ -homomorphism of  $G$  onto a linear  $K$ -group of the same dimension, then  $G$  is linear.

*Proof* (a) and (b) are obvious. Let  $G$  be a  $K$ -group. Each component of  $G$  is of the form  $\rho_x(G^\circ)$  for some  $x \in G_{K_s}$ . Hence, if  $G^\circ$  is  $K_s$ -affine in itself, then so is each component of  $G$ . Since the components are pairwise disjoint,  $G$  is  $K_s$ -affine in  $G$ . This proves (c). Now let  $f: G \rightarrow G'$  be a surjective  $K$ -homomorphism with  $\dim G = \dim G'$  and  $G'$  linear. Because of (c), it suffices to prove that  $G^\circ$  is linear, that is, we may suppose that  $G$  is connected. Then  $\mathfrak{F}_K(G)$  and  $\mathfrak{F}_K(G')$  are fields and, because  $\dim G = \dim G'$ ,  $\mathfrak{F}_K(G)$  is an algebraic extension of the field  $f^*(\mathfrak{F}_K(G')) = f^*(Q(\mathfrak{F}_K(G')))$  =  $Q(f^*(\mathfrak{F}_K(G')))$ , hence *a fortiori* of the field  $Q(\mathfrak{F}_K(G))$ . Thus, for any  $\varphi \in \mathfrak{F}_K(G)$ , there exists a nonzero  $\eta \in \mathfrak{F}_K(G)$  such that  $\varphi\eta$  is integral over  $\mathfrak{F}_K(G)$ , hence over  $\mathfrak{F}_{K(x),x}(G)$  for every  $x \in G$ . Since every  $x$  is simple on  $G$ ,  $\mathfrak{F}_{K(x),x}(G)$  is integrally closed by Section 20, Proposition 26, so that  $\varphi\eta \in \mathfrak{F}_{K(x),x}(G)$  for every  $x \in G$ , whence  $\varphi\eta \in \mathfrak{F}_G(G) \cap \mathfrak{F}_K(G) = \mathfrak{F}_K(G)$  and  $\varphi \in Q(\mathfrak{F}_K(G))$ . This proves (d) and completes the proof of the proposition.

We shall show later (Proposition 34) that a  $K$ -homomorphic image of a linear  $K$ -group is linear. The following subsection prepares the way.

### B. SEMI-INVARIANTS

Let  $G$  be a connected  $K$ -group and  $H$  be a  $K$ -subgroup of  $G$ . An element  $\varphi \in \mathfrak{F}(G)$  such that  $\rho_y^*(\varphi) \in U\varphi$  for every  $y \in H$  is called a *semi-invariant of  $H$  on  $G$* . If  $\varphi$  is a semi-invariant of  $H$  on  $G$  and  $\varphi \neq 0$ , then there is a unique function  $\chi$  on  $H$  with values in  $U^*$  such that  $\rho_y^*(\varphi) = \chi(y)\varphi$  ( $y \in H$ ), and it is easy to see, for any extension  $L$  of  $K$  such that  $\varphi \in \mathfrak{F}_L(G)$ , that  $\chi$  is an  $L$ -homomorphism of  $H$  into  $G_m$ ;  $\chi$  is called the *weight* of the semi-invariant  $\varphi$ . The element  $0 \in \mathfrak{F}(G)$  is obviously a semi-invariant of  $H$  on  $G$ .

We adopt the convention that every  $U$ -homomorphism of  $H$  into  $G_m$  is a weight of 0.

Consider any nonzero  $\xi \in \mathfrak{F}_{K,G}(G)$ , by Section 16, Corollary to Proposition 23 there exist elements  $\varphi_1, \dots, \varphi_m \in \mathfrak{F}_{K,G}(G)$ , linearly independent over  $U$  and elements  $\psi_1, \dots, \psi_m \in \mathfrak{F}_{K,G}(G)$ , such that

$$\rho_x^*(\xi) = \sum \varphi_i \psi_i(x) \quad (x \in G).$$

In particular,  $\xi = \sum \varphi_i \psi_i(1)$ . Of course,  $\psi_1(1), \dots, \psi_m(1) \in K$ , and  $\psi_{i_0}(1) \neq 0$  for some  $i_0$ . Evidently, for  $x \in G$ , the condition  $\rho_x^*(\xi) \in U\xi$  is equivalent to the condition  $\psi_{i_0}(1)\psi_i(x) - \psi_i(1)\psi_{i_0}(x) = 0$  ( $1 \leq i \leq m$ ). It follows that for any subset  $\Xi$  of  $\mathfrak{F}_{K,G}(G)$ , the set of elements  $x \in G$  such that  $\rho_x^*(\varphi) \in U\varphi$  ( $\varphi \in \Xi$ ) is a  $K$ -closed subgroup of  $G$ , and the elements of  $\Xi$  are semi-invariants of it on  $G$ . The following proposition is the converse of this result for the case in which  $G$  is linear.

**Proposition 33** Let  $H$  be a  $K$ -closed subgroup of the connected linear  $K$ -group  $G$ . There exist finitely many semi-invariants  $\varphi_1, \dots, \varphi_m \in \mathfrak{F}_{K,G}(G)$  of  $H$  on  $G$ , all of the same weight, such that  $H$  is the set of elements  $x \in G$  for which  $\rho_x^*(\varphi_i) \in U\varphi_i$  ( $1 \leq i \leq m$ ).

*Proof* If  $p \neq 0$  and  $\varphi \in \mathfrak{F}_{K_1,G}(G)$ , then  $\varphi^{p^e} \in \mathfrak{F}_{K,G}(G)$  for any sufficiently big  $e \in \mathbb{N}$ . Therefore we may suppose that the field  $K$  is perfect, so that  $H$  is a  $K$ -subgroup of  $G$ . By Proposition 31, there exist finitely many  $K$ -functions  $\xi_1, \dots, \xi_n$  on  $G$  such that, for any extension  $L$  of  $K$ ,  $\mathfrak{F}_{L,G}(G) = L[\xi_1, \dots, \xi_n]$  and  $\mathfrak{F}_{L,H}(H) = L[\xi_1 \circ in_{G,H}, \dots, \xi_n \circ in_{G,H}]$ . It follows that the homomorphism  $\mathfrak{F}_G(G) \rightarrow \mathfrak{F}_H(H)$  induced by  $in_{G,H}$  is surjective. Its kernel  $\alpha$  is defined over  $K$ , that is,  $U \cdot (\alpha \cap \mathfrak{F}_{K,G}(G)) = \alpha$ , and an element  $x$  of  $G$  is in  $H$  if and only if  $\xi(x) = 0$  ( $\xi \in \alpha$ ). If  $x \in H$  and  $\xi \in \alpha$ , then  $\rho_x^*(\xi)(y) = \xi(yx) = 0$  ( $y \in H$ ), whence  $\rho_x^*(\xi) \in \alpha$  so that  $\rho_x^*(\alpha) \subset \alpha$ . Conversely, if  $\rho_x^*(\alpha) \subset \alpha$ , then  $\xi(x) = \rho_x^*(\xi)(1) = 0$  ( $\xi \in \alpha$ ), whence  $x \in H$ . Thus  $H$  consists of the elements  $x \in G$  such that  $\rho_x^*(\alpha) \subset \alpha$ .

Since  $\alpha$  is defined over  $K$  and the ring  $\mathfrak{F}_{K,G}(G)$  is obviously Noetherian, there are finitely many elements  $\eta_1, \dots, \eta_r \in \mathfrak{F}_{K,G}(G)$  that generate the ideal  $\alpha$ . We may suppose that  $\eta_1, \dots, \eta_r$  are linearly independent over  $K$  and hence over  $U$ . By Section 16, corollary to Proposition 23, there are finitely many further elements  $\eta_{r+1}, \dots, \eta_s \in \mathfrak{F}_{K,G}(G)$  and an invertible matrix  $(\lambda_{l'l'})_{1 \leq l \leq s, 1 \leq l' \leq s}$  over  $\mathfrak{F}_{K,G}(G)$  such that  $\eta_1, \dots, \eta_s$  are linearly independent over  $U$  and

$$\rho_x^*(\eta_{l'}) = \sum_{1 \leq l \leq s} \lambda_{l'l'}(x) \eta_l \quad (1 \leq l' \leq s)$$

for every  $x \in G$ . If some nontrivial linear combination of  $\eta_{r+1}, \dots, \eta_s$  over



$U$  is in  $\mathfrak{a}$ , then so is some such combination over  $K$ , say  $\zeta = \sum_{r < l \leq s} a_l \eta_l \in \mathfrak{a}$ . Supposing that, say,  $a_{r+1} \neq 0$ , we can replace  $\eta_{r+1}$  by  $\zeta$ . On this basis we see that we may suppose (increasing  $r$  if necessary) that no nontrivial linear combination of  $\eta_{r+1}, \dots, \eta_n$  over  $U$  is in  $\mathfrak{a}$ . Since  $x \in H$  if and only if  $\rho_x^*(\mathfrak{a}) \subset \mathfrak{a}$ , it follows that  $x \in H$  if and only if

$$\rho_x^*(\eta_{k'}) = \sum_{1 \leq k \leq r} \lambda_{kk'}(x) \eta_k \quad (1 \leq k' \leq r),$$

that is, if and only if  $\lambda_{ik'}(x) = 0$  ( $r < l \leq s$ ,  $1 \leq k' \leq r$ ). Thus, the formula  $x \mapsto (\lambda_{il'}(x))_{1 \leq l \leq s, 1 \leq l' \leq s}$  defines a  $K$ -homomorphism  $G \rightarrow \mathbf{GL}(s)$ , and the formula  $y \mapsto (\lambda_{kk'}(y))_{1 \leq k \leq r, 1 \leq k' \leq r}$  defines a  $K$ -homomorphism  $H \rightarrow \mathbf{GL}(r)$ , so that, also, the formula  $y \mapsto \det(\lambda_{kk'}(y))_{1 \leq k \leq r, 1 \leq k' \leq r}$  defines a  $K$ -homomorphism  $\chi: H \rightarrow \mathbf{G}_m$ .

For each family of indices  $(i_1, \dots, i_r)$  with  $1 \leq i_1 < \dots < i_r \leq s$ , set  $\varphi_{i_1 \dots i_r} = \det(\lambda_{ik'}(y))_{1 \leq k \leq r, 1 \leq k' \leq r}$ . Then  $\varphi_{i_1 \dots i_r} \in \mathfrak{F}_{K,G}(G)$  and, for any  $(x, y) \in G \times H$ ,

$$\begin{aligned} \varphi_{i_1 \dots i_r}(xy) &= \det(\lambda_{ik'}(xy))_{1 \leq k \leq r, 1 \leq k' \leq r} \\ &= \det\left(\sum_{1 \leq l \leq s} \lambda_{ikl}(x) \lambda_{lk'}(y)\right)_{1 \leq k \leq r, 1 \leq k' \leq r} \\ &= \det\left(\sum_{1 \leq l \leq r} \lambda_{ikl}(x) \lambda_{lk'}(y)\right)_{1 \leq k \leq r, 1 \leq k' \leq r} \\ &= \varphi_{i_1 \dots i_r}(x) \chi(y), \end{aligned}$$

so that  $\varphi_{i_1 \dots i_r}$  is a semi-invariant of  $H$  on  $G$  of weight  $\chi$ .

Consider any  $x \in G$  such that  $\rho_x^*(\varphi_{i_1 \dots i_r}) \in U\varphi_{i_1 \dots i_r}$  for all  $(i_1, \dots, i_r)$ . When  $(i_1, \dots, i_r) \neq (1, \dots, r)$ , then  $\varphi_{i_1 \dots i_r}(y) = 0$  ( $y \in H$ ) because  $\lambda_{ik'}(y) = 0$  ( $r < l \leq s$ ,  $1 \leq k' \leq r$ ,  $y \in H$ ). Since  $\varphi_{i_1 \dots i_r}(x) = \rho_x^*(\varphi_{i_1 \dots i_r})(1) \in U\varphi_{i_1 \dots i_r}(1)$ , this implies that

$$\varphi_{i_1 \dots i_r}(x) = 0 \quad ((i_1, \dots, i_r) \neq (1, \dots, r)),$$

and hence also that

$$\varphi_{1 \dots r}(x) \neq 0$$

because otherwise all the  $r$ -rowed minors of the matrix  $(\lambda_{ik'}(x))_{1 \leq l \leq s, 1 \leq k' \leq r}$  would vanish and  $\det(\lambda_{il'}(x))_{1 \leq l \leq s, 1 \leq l' \leq s}$  would too. It follows that, for each index  $l$  with  $r < l \leq s$ , the system of equations

$$\sum_{1 \leq k \leq r} \lambda_{kk'}(x) X_k = \lambda_{lk'}(x) \quad (1 \leq k' \leq r)$$

has a unique solution which, by Cramer's rule, must be  $(0, \dots, 0)$ . Therefore  $\lambda_{ik'}(x) = 0$  ( $r < l \leq s$ ,  $1 \leq k' \leq r$ ), so that  $x \in H$ .

### C. $K$ -HOMOMORPHISMS OF LINEAR $K$ -GROUPS

We are now in position to prove the following result.

**Proposition 34** *Let  $f: G \rightarrow G'$  be a  $K$ -homomorphism of  $K$ -groups. If  $G$  is linear, then so is  $f(G)$ .*

*Proof* We may suppose that  $G$  is a  $K$ -subgroup of  $\mathbf{GL}(n)$ . Since  $f(G^\circ) = f(G)^\circ$ , we may (by Proposition 32(c)) suppose also that  $G$  is connected.

First we treat the special case in which  $f$  is injective. When  $p = 0$ , then  $f$  maps  $G$   $K$ -isomorphically onto  $f(G)$  and hence  $f(G)$  is linear. Therefore we suppose in this case that  $p \neq 0$ . Fix  $x = (x_{ij}) \in \Gamma_{G/K}$ . For any  $\sigma \in \text{Aut}(U/K(f(x)))$ ,  $f(\sigma x) = \sigma(f(x)) = f(x)$  so that  $\sigma x = x$  and  $\sigma \in \text{Aut}(U/K(x))$ . Hence  $K(x)$  is a purely inseparable algebraic extension of  $K(f(x))$ , so that  $K((x_{ij}^{p^n})) \subset K(f(x))$  for some  $e \in \mathbf{N}$ . The formula  $(z_{ij}) \mapsto (z_{ij}^{p^n})$  defines a bijective  $K$ -endomorphism of  $\mathbf{GL}(n)$ , and  $G$  is mapped thereby onto a connected  $K$ -subgroup  $G_1$  of  $\mathbf{GL}(n)$ . Because  $f(x) \in \Gamma_{f(G)/K}$ , the above inclusion shows that there is a  $K$ -mapping  $g \in \mathfrak{R}_K(f(G), G_1)$  such that  $g(f(x)) = (x_{ij}^{p^n})$ . Evidently  $g$  is a bijective  $K$ -homomorphism of  $f(G)$  onto  $G_1$ . Since  $G_1$  is linear, Proposition 32(d) shows that  $f(G)$  is linear.

Now we relinquish the assumption that  $f$  is injective. Set  $H = \text{Ker}(f)$  and let  $\pi: G \rightarrow G/H$  denote the canonical homomorphism. By Proposition 33, there exists a finite set  $\Phi \subset \mathfrak{F}_{K,G}(G)$  of semi-invariants of  $H$  on  $G$ , all having the same weight, such that  $H$  is the set of elements  $x \in G$  for which  $\rho_x^*(\xi) \in U\xi$  ( $\xi \in \Phi$ ). By Section 16, corollary to Proposition 23,  $\Phi$  is contained in a finite-dimensional subspace  $V$  of the vector space  $\mathfrak{F}_G(G)$  over  $U$  such that  $\rho_x^*(V) = V$  ( $x \in G$ ). The elements of  $V$  that are semi-invariants of  $H$  of a given weight  $\chi$  form a subspace  $V_\chi$  of  $V$ . It is easy to see that non-zero semi-invariants of  $H$  of distinct weights are linearly independent over  $U$ . It follows that there are finitely many distinct weights  $\chi_1, \dots, \chi_h$  such that  $V_{\chi_i} \neq 0$  ( $1 \leq i \leq h$ ), the sum  $\sum V_{\chi_i}$  is direct, and every semi-invariant of  $H$  on  $G$  that is in  $V$  is in  $V_{\chi_i}$  for some  $i$ .

Because  $H$  is normal in  $G$ , for each  $x \in G$  the inner automorphism  $\tau_{x^{-1}}$  of  $G$  induces a  $K(x)$ -automorphism  $t_x$  of  $H$ . For any  $\varphi \in V_{\chi_i}$ , if  $y \in H$ , then  $\rho_y^*(\rho_x^*(\varphi)) = \rho_x^*(\rho_{x^{-1}yx}^*(\varphi)) = \rho_x^*(\chi_i(x^{-1}yx)\varphi) = (\chi_i \circ t_x)(y)\rho_x^*(\varphi)$ , so that  $\rho_x^*(\varphi)$  is a semi-invariant of  $H$  on  $G$  of weight  $\chi_i \circ t_x$ . Thus,  $\chi_i \circ t_x = \chi_{i'}$  for some index  $i'$ , and  $\rho_x^*(V_{\chi_i}) = V_{\chi_{i'}}$ . However, for each  $y \in H$ , the formula  $x \mapsto \chi_i(x^{-1}yx)$  defines a continuous mapping  $G \rightarrow \mathbf{G}_m$ , so that the set  $X_{ii'}$  of elements  $x \in G$  with  $\chi_i(x^{-1}yx) = \chi_{i'}(y)$  is closed. Hence the set  $X_{ii'} = \bigcap_{y \in H} X_{ii'}$  of elements  $x \in G$  with  $\chi_i \circ t_x = \chi_{i'}$  is closed, too. Since the  $h$  sets  $X_{i_1}, \dots, X_{i_h}$  are pairwise disjoint (because  $\chi_1, \dots, \chi_h$  are distinct), and  $G = X_{i_1} \cup \dots \cup X_{i_h}$ , and  $G$  is connected, this implies that all but one of these  $h$  sets are empty. Since  $1 \in X_{ii}$ , we conclude that  $\rho_x^*(V_{\chi_i}) = V_{\chi_i}$ .

( $x \in G$ ) for each index  $i$ . Now,  $\Phi$  is contained in some  $V_{x_i}$ , say  $\Phi \subset V_{x_1}$ . Enlarging  $K$  if necessary, we may suppose that  $V_{x_1}$  has a basis  $(\varphi_1, \dots, \varphi_n)$  with  $\varphi_j \in \mathfrak{F}_{K,G}(G)$  for each  $j$ . Then, for each  $x \in G$ , there exists a matrix  $\Psi(x) = (\psi_{jj'}(x)) \in \mathbf{GL}_{K(x)}(n)$  such that  $\rho_x^*(\varphi_{j'}) = \sum_j \psi_{jj'}(x) \varphi_j$ , and it easily follows from Section 16, corollary to Proposition 23, that the mapping  $\Psi: G \rightarrow \mathbf{GL}(n)$  is a  $K$ -homomorphism. By the above,  $H$  consists of the elements  $x \in G$  such that  $\Psi(x)$  is a scalar matrix.

Let  $J$  denote the set of all pairs of indices  $(j, j')$  with  $1 \leq j \leq n, 1 \leq j' \leq n$ , and let  $\mathbf{GL}(J)$  denote the set of all invertible square matrices  $(u_{\alpha\beta})_{\alpha, \beta \in J}$  over  $U$ . Then  $\mathbf{GL}(J)$  has an obvious structure of  $K$ -group for which it is  $K$ -isomorphic to  $\mathbf{GL}(n^2)$  and hence is linear. If, for each  $x = (x_{ij}) \in \mathbf{GL}(n)$ , we write  $x^{-1} = (x'_{ij})$ , then the formula  $x \mapsto (x_{ij} x'_{j'i'})_{(i, i') \in J, (j, j') \in J}$  defines a  $K$ -homomorphism  $\Lambda: \mathbf{GL}(n) \rightarrow \mathbf{GL}(J)$ , and the kernel of  $\Lambda$  is the set of all scalar matrices in  $\mathbf{GL}(n)$ . Therefore  $\Lambda \circ \Psi: G \rightarrow \mathbf{GL}(J)$  is a  $K$ -homomorphism with kernel  $H$ , and hence there exists an injective  $K$ -homomorphism  $k: G/H \rightarrow \mathbf{GL}(J)$ . It follows by Proposition 32(d) that  $G/H$  is linear. As there exists a bijective  $K$ -homomorphism  $G/H \rightarrow f(G)$ , we conclude by the special case already treated that  $f(G)$  is linear.

D.  $G_a$  AND  $G_m$

A polynomial  $P \in K[X]$  is said to be *additive* if it satisfies the condition  $P(X+Y) = P(X) + P(Y)$ . It is easy to see that  $P$  is additive if and only if either  $p = 0$  and  $P = cX$  for some  $c \in K$  or else  $p \neq 0$  and  $P = \sum_{0 \leq j \leq n} a_j X^{pj}$  for some  $n \in \mathbb{N}$  and some  $(a_0, \dots, a_n) \in K^{n+1}$ . In the latter case,  $P$  is separable precisely when either  $a_0 \neq 0$  or  $P = 0$ . It is clear that if  $P \in K[X]$  is additive then the formula  $x \mapsto P(x)$  determines a  $K$ -endomorphism of  $G_a$ , which is separable if and only if  $P$  is separable.

**Proposition 35** (a) Every  $K$ -endomorphism of  $G_a$  is determined as above by a unique additive polynomial in  $K[X]$ .

(b) Every  $K$ -subgroup of  $G_a$  is the kernel of some separable  $K$ -endomorphism of  $G_a$ .

(c) If a nontrivial  $K$ -group is a  $K$ -homomorphic image of  $G_a$ , then it is  $K$ -isomorphic to  $G_a$ .

(d) If  $G$  is a  $K$ -group for which there exists a bijective  $K$ -homomorphism  $G \rightarrow G_a$ , then  $G$  is  $K$ -isomorphic to  $G_a$ .

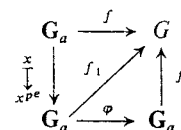
**REMARK** When  $p = 0$ , part (a) shows that every  $K$ -endomorphism of  $G_a$  other than 0 is a  $K$ -automorphism and then (b) shows that 0 is the only closed proper subgroup of  $G_a$ .

*Proof* (a) A  $K$ -endomorphism of  $G_a$  is an everywhere defined  $K$ -function

on  $G_a$  and hence is given by a polynomial in  $K[X]$  which obviously is additive.

(b) When  $p = 0$ , a  $K$ -subgroup of  $G_a$  that contains a nonzero element  $x$  contains the infinite subgroup  $Zx$ , hence is of dimension 1, and therefore coincides with  $G_a$ . When  $p \neq 0$ , a proper  $K$ -subgroup  $F$  of  $G_a$  is finite and hence consists of the roots of the unitary separable polynomial  $P = \prod_{x \in F} (X - x)$ , which must be in  $K[X]$ . For any  $y \in F$ , evidently  $P(X+y) - P(X) = 0$ . Therefore the polynomial  $P(X+Y) - P(X) - P(Y)$  in  $Y$  of degree less than  $\text{ord } F$  vanishes on  $F$  and hence is 0.

(c) Let  $f: G_a \rightarrow G$  be a nontrivial surjective  $K$ -homomorphism. Then  $\text{Ker}(f)$  is a  $K$ -closed proper subgroup of  $G_a$ . When  $p = 0$ , the remark shows that  $\text{Ker}(f) = 0$  so that  $f$  is a  $K$ -isomorphism. Letting  $p \neq 0$ , fix  $t \in \Gamma_{G_a/K}$ . Then there exists a greatest  $e \in \mathbb{N}$  such that  $K(f(t)) \subset K(t^{p^e})$ . Since  $t^{p^e} \in \Gamma_{G_a/K}$  and  $f(t) \in \Gamma_{G/K}$ , this shows that there exists a  $K$ -mapping  $f_1 \in \mathfrak{M}_K(G_a, G)$  such that  $f_1(t^{p^e}) = f(t)$ .



It is now easy to see that  $f_1$  is a *separable* surjective  $K$ -homomorphism. By part (b)  $\text{Ker}(f_1) = \text{Ker}(\varphi)$ , where  $\varphi$  is a separable  $K$ -endomorphism that obviously is surjective. Therefore there exists a  $K$ -isomorphism  $f': G_a \approx G$  such that  $f' \circ \varphi = f_1$ .

(d) We may suppose that  $p \neq 0$  and that  $K = K_i$ . Let  $g: G \rightarrow G_a$  be a bijective  $K$ -homomorphism, and fix  $s \in \Gamma_{G/K}$ . Then  $K(s)$  is a purely inseparable extension of  $K(g(s))$  of finite degree, so that for some  $e \in \mathbb{N}$ ,  $K(s) \subset K(g(s))^{1/p^e} = K(g(s)^{1/p^e})$ . Since  $g(s)^{1/p^e} \in \Gamma_{G_a/K}$  and  $s \in \Gamma_{G/K}$ , this shows that there exists a  $K$ -mapping  $f \in \mathfrak{M}_K(G_a, G)$  such that  $f(g(s)^{1/p^e}) = s$ . Applying an arbitrary  $\sigma \in \text{Aut}(U/K)$ , we find that this equation holds for every  $s \in \Gamma_{G/K}$ . Hence if  $(s_1, s_2) \in \Gamma_{G^2/K}$ , so that  $(g(s_1))^{1/p^e}, (g(s_2))^{1/p^e} \in \Gamma_{G_a^2/K}$ , then

$$\begin{aligned}
 f(g(s_1)^{1/p^e} + g(s_2)^{1/p^e}) &= f(g(s_1 s_2)^{1/p^e}) = s_1 s_2 \\
 &= f(g(s_1)^{1/p^e}) f(g(s_2)^{1/p^e}).
 \end{aligned}$$

Therefore  $f$  is a surjective  $K$ -homomorphism of  $G_a$  into  $G$ . It follows by part (c) that  $G$  is  $K$ -isomorphic to  $G_a$ .

When  $p \neq 0$ , let  $\Xi$  denote the  $K$ -endomorphism of  $G_a$  given by the formula  $\Xi(x) = x^p$ . By part (a) of the proposition, every  $K$ -endomorphism of  $G_a$  can be expressed as a polynomial  $\sum a_j \Xi^j$  with coefficients in  $K$ .

**Corollary 1** Let  $E_K$  denote the ring of  $K$ -endomorphisms of  $G_a$ .

(a) According as  $p = 0$  or  $p \neq 0$ ,  $E_K$  is naturally identified with the field  $K$  or the noncommutative polynomial ring  $K[\Xi]$  in which  $\Xi a = a^p \Xi$  for every  $a \in K$ .

(b) The ring of  $K$ -endomorphisms of  $G_a^n$  is naturally identified with the matrix ring  $M_{E_K}(n)$ .

*Proof* This is clear.

The direct product  $G_a^n$  has a natural structure of vector space over  $U$ . A vector subspace  $V$  of  $G_a^n$  is a connected closed subgroup of  $G_a^n$  and its dimension as a vector space coincides with its dimension as a closed subgroup of  $G_a^n$ ;  $V$  is a  $K$ -group if and only if  $U \cdot (V \cap K^n) = V$ , that is,  $K$  is a field of definition of  $V$  relative to the canonical basis of  $U^n$  (see Chapter I, Section 5), and when this is the case, then  $V$  is  $K$ -isomorphic to  $G_a^d$ , where  $d = \dim V$ . When  $p = 0$ , then every  $K$ -subgroup of  $G_a^n$  is a vector subspace of  $G_a^n$ . Indeed, if  $x = (x_1, \dots, x_n)$  is in a  $K$ -subgroup  $H$ , and  $P \in K[X_1, \dots, X_n]$  vanishes on  $H$ , then the polynomial  $P(Tx_1, \dots, Tx_n) \in U[T]$  vanishes on the infinite set  $Z$  and hence is 0, so that  $P$  vanishes at  $tx$  for every  $t \in U$ , and  $tx \in H$ . When  $p \neq 0$ , a description of the  $K$ -subgroups of  $G_a^n$  is more complicated (see Exercise 1(c)).

**Corollary 2** The only  $K$ -homomorphism of  $G_a$  into  $G_m$  is trivial.

*Proof*  $G_m$  has nontrivial finite subgroups of order not divisible by  $p$ , and  $G_a$  does not, so that  $G_a$  is not isomorphic to  $G_m$ . Therefore the statement follows from part (c) of the proposition.

It is easy to see that an element  $P \in K[X, X^{-1}]$  satisfies the condition  $P(XY) = P(X)P(Y)$  if and only if  $P = X^e$  for some  $e \in \mathbf{Z}$ . For any  $e \in \mathbf{Z}$  the formula  $x \mapsto x^e$  determines a  $K$ -endomorphism of  $G_m$ . It is separable when either  $p \nmid e$  or  $e = 0$ . When  $p \nmid e$ , the kernel of this  $K$ -endomorphism is the group  $P_e$  of  $e$ th roots of 1. When  $e = e'p^k$ , where  $k \in \mathbf{N}$ ,  $e' \in \mathbf{Z}$ ,  $p \nmid e'$ , and  $p \neq 0$ , then the kernel is  $P_{e'}$ .

**Proposition 36** (a) Every  $K$ -endomorphism of  $G_m$  is determined as above by a unique integer  $e \in \mathbf{Z}$ .

(b) The  $K$ -subgroups of  $G_m$  are the groups  $P_e$  ( $e \in \mathbf{N}$ ,  $p \nmid e$ ) and  $G_m$ .

(c) If a nontrivial  $K$ -group is a  $K$ -homomorphic image of  $G_m$ , then it is  $K$ -isomorphic to  $G_m$ .

(d) If  $G$  is a  $K$ -group for which there exists a bijective  $K$ -homomorphism  $G \rightarrow G_m$ , then  $G$  is  $K_1$ -isomorphic to  $G_m$ .

*Proof* Since a  $K$ -endomorphism  $\varphi$  of  $G_m$  followed by the inclusion

$G_m \subset G_a$  is an everywhere defined  $K$ -function on  $G_m$ , and since  $G_m = \mathbf{GL}(1)$ , Proposition 31 shows that there exists a unique element  $P \in K[X, X^{-1}]$  such that  $\varphi(x) = P(x)$  ( $x \in G_m$ ). Since  $P$  must obviously be multiplicative,  $P = X^e$  for some  $e \in \mathbf{Z}$ , which evidently is unique. It is well known that the finite subgroups of  $G_m = U^*$  are the groups  $P_e$  ( $e \in \mathbf{N}$ ,  $p \nmid e$ ). Parts (c) and (d) are proved in the same way as parts (c) and (d) of Proposition 35.

**Corollary 1** (a) The ring of  $K$ -endomorphisms of  $G_m$  is naturally identified with the ring  $\mathbf{Z}$ .

(b) The ring of  $K$ -endomorphisms of  $G_m^n$  is naturally identified with the matrix ring  $M_{\mathbf{Z}}(n)$ .

**Corollary 2** The only  $K$ -homomorphism of  $G_m$  into  $G_a$  is trivial.

For any subset  $\Sigma$  of  $G_m^n$  let  $\Sigma^\perp$  denote the set of all  $(e_1, \dots, e_n) \in \mathbf{Z}^n$  such that  $\prod x_i^{e_i} = 1$  for every  $(x_1, \dots, x_n) \in \Sigma$ . Then  $\Sigma^\perp$  is a subgroup of  $\mathbf{Z}^n$  without  $p$ -torsion, that is, such that  $\mathbf{Z}^n/\Sigma^\perp$  has no  $p$ -torsion. (When  $p = 0$ , every group has no  $p$ -torsion.) Similarly, for any subset  $E$  of  $\mathbf{Z}^n$ , let  $E^\perp$  denote the set of all  $(x_1, \dots, x_n) \in G_m^n$  such that  $\prod x_i^{e_i} = 1$  for every  $(e_1, \dots, e_n) \in E$ . Then  $E^\perp$  is a  $K$ -subgroup of  $G_m^n$ . The following proposition establishes a sort of duality between  $G_m^n$  and  $\mathbf{Z}^n$ .

**Proposition 37** The formula  $G \mapsto G^\perp$  defines a mapping from the set of all  $K$ -subgroups of  $G_m^n$  into the set of all subgroups of  $\mathbf{Z}^n$  without  $p$ -torsion, the formula  $M \mapsto M^\perp$  defines a mapping of the latter set into the former set, and these mappings are bijective and inverse to each other. If  $G$  is any  $K$ -subgroup of  $G_m^n$  and  $d = \dim G$ , there exist a  $K$ -automorphism  $\alpha$  of  $G_m^n$  and  $n-d$  natural numbers  $e_1, \dots, e_{n-d}$  not divisible by  $p$  such that  $\alpha(G) = P_{e_1} \times \dots \times P_{e_{n-d}} \times G_m^d$ .

*Proof* Let  $(\zeta_1, \dots, \zeta_n)$  denote the canonical coordinate system on  $G_m^n$  (so that  $\zeta_j(x) = x_j$  for every  $x = (x_1, \dots, x_n) \in G_m^n$ ). There is an obvious identification of  $G_m^n$  with the diagonal group  $\mathbf{D}(n)$ . It follows by Proposition 31 that  $\mathfrak{F}_{K, G_m^n}(G_m^n) = K[\zeta_1, \dots, \zeta_n, 1/\zeta_1 \dots \zeta_n]$  and hence any nonzero everywhere defined  $K$ -function  $\varphi$  on  $G_m^n$  can be written in the form  $\varphi = P(\zeta_1, \dots, \zeta_n)/(\zeta_1 \dots \zeta_n)^h$  with  $h \in \mathbf{N}$  and  $P = \sum a_{i_1, \dots, i_n} X_1^{i_1} \dots X_n^{i_n} \in K[X_1, \dots, X_n]$ , where  $a_{i_1, \dots, i_n} \neq 0$  for some  $(i_1, \dots, i_n)$ . For any  $x = (x_1, \dots, x_n) \in G_m^n$  then

$$\rho_x^*(\varphi) = P(\zeta_1 x_1, \dots, \zeta_n x_n)/(\zeta_1 x_1 \dots \zeta_n x_n)^h,$$

so that the condition that  $\rho_x^*(\varphi) \in U \cdot \varphi$  is equivalent to the condition that  $\prod x_i^{j-i_{i_0}} = 1$  for all  $(i_1, \dots, i_n)$  with  $a_{i_1, \dots, i_n} \neq 0$ . Given any  $K$ -subgroup  $G$  of  $G_m^n$ , we infer by Proposition 33 that there exists a subset  $E$  of  $\mathbf{Z}^n$  such that  $G = E^\perp$ . Evidently  $E \subset G^\perp$ , whence  $E^\perp \supset G^{\perp\perp}$ , that is,  $G \supset G^{\perp\perp}$ . Since the relation  $G \subset G^{\perp\perp}$  is obvious, we conclude that  $G = G^{\perp\perp}$ .

On the other hand, if  $M$  is any subgroup of  $\mathbf{Z}^n$  without  $p$ -cotorsion, and we put  $r = \text{rank } M$ , then (by the classical theory of free modules over principal rings) there exist  $n$  elements  $f_j = (f_{1j}, \dots, f_{nj}) \in \mathbf{Z}^n$  ( $1 \leq j \leq n$ ) and  $r$  nonzero natural numbers  $e_1, \dots, e_r$  such that  $f_1, \dots, f_r$  form a basis of the  $\mathbf{Z}$ -module  $\mathbf{Z}^n$  and  $e_1 f_1, \dots, e_r f_r$  form a basis of  $M$ . Of course,  $\det(f_{jj}) = \pm 1$  and, because  $M$  has no  $p$ -cotorsion,  $p \nmid e_k$  ( $1 \leq k \leq r$ ). For each  $x = (x_1, \dots, x_n) \in \mathbf{G}_m^n$ , set  $\alpha(x) = (\alpha_1(x), \dots, \alpha_n(x))$ , where  $\alpha_j(x) = \prod_{i=1}^r x_i^{f_{ij}}$  ( $1 \leq j \leq n$ ). Then  $\alpha$  is a  $K$ -automorphism of  $\mathbf{G}_m^n$ , and evidently  $x \in M^\perp$  if and only if  $\alpha_k(x)^{e_k} = 1$  ( $1 \leq k \leq r$ ). Hence  $\alpha(M^\perp) = P_{e_1} \times \dots \times P_{e_r} \times \mathbf{G}_m^{n-r}$ . In particular,  $M^\perp$  is a  $K$ -subgroup of  $\mathbf{G}_m^n$ . For any  $b = (b_1, \dots, b_n) \in \mathbf{Z}^n$ , there exist  $c_1, \dots, c_n \in \mathbf{Z}$  such that  $b = \sum c_j f_j$ , and clearly  $\prod x_j^{b_j} = \prod \alpha_j(x)^{c_j}$ . Therefore  $b \in M^{\perp\perp}$  if and only if  $(c_1, \dots, c_n) \in \alpha(M^\perp)^\perp$ , which by the above happens if and only if  $e_k | c_k$  ( $1 \leq k \leq r$ ) and  $c_j = 0$  ( $r < j \leq n$ ), that is, if and only if  $b \in \sum \mathbf{Z} e_k f_k = M$ . Thus,  $M = M^{\perp\perp}$ . This completes the proof.

**Corollary** Let  $G$  be a closed subgroup of  $\mathbf{G}_m^n$ .

- (a) Then  $G$  is a  $K'$ -subgroup of  $\mathbf{G}_m^n$  for every field  $K'$ , in particular for the prime field.
- (b) The torsion subgroup of  $G$  is dense in  $G$ .

E. JORDAN DECOMPOSITION

A matrix  $x \in \mathbf{GL}(n)$  is said to be *unipotent* if the matrix  $x - 1$  is nilpotent, that is, if all the characteristic values of  $x$  equal 1. Denoting the characteristic polynomial of  $x$  by  $\chi_x$ , we see that  $x$  is unipotent if and only if  $\chi_x = (X - 1)^n$ .

If two unipotent matrices  $x, x' \in \mathbf{GL}(n)$  commute with each other, then  $xx'$  is unipotent (because  $xx' - 1 = (x - 1)x' + x' - 1$ ).

For any  $x \in \mathbf{GL}(n)$  and any  $k \in \mathbf{N}$ ,

$$x^k = (1 + (x - 1))^k = \sum_{i \in \mathbf{N}} \binom{k}{i} (x - 1)^i,$$

and any subgroup  $G$  of  $\mathbf{GL}(n)$  that contains  $x$  contains  $x^k$ . Suppose that  $x$  is unipotent and  $G$  is closed. When  $p = 0$ , the "binomial coefficient" polynomial

$$\binom{T}{i} = T(T-1) \dots (T-i+1)/i!$$

is defined for every  $i \in \mathbf{N}$ , and for any  $t \in U$  we can define  $x^t$  by the formula

$$x^t = \sum \binom{t}{i} (x - 1)^i;$$

every polynomial  $P \in U[(X_{jj})_{1 \leq j \leq n, 1 \leq j' \leq n}]$  that vanishes on  $G$  has the property that the polynomial  $P(\sum_i \binom{t}{i} (x - 1)^i) \in U[T]$  vanishes on  $\mathbf{N}$  and hence vanishes identically, so that  $x^t = G$  ( $t \in U$ ); it is easy to see that the formula  $t \mapsto x^t$  defines a  $K(x)$ -homomorphism  $\mathbf{G}_a \rightarrow \mathbf{GL}(n)$ , injective when  $x \neq 1$ , and that its image is the smallest closed subgroup  $G(x)$  of  $\mathbf{GL}(n)$  that contains  $x$ . When  $p \neq 0$  then, for any  $e \in \mathbf{N}$ ,  $x^{pe} = 1 + (x - 1)^{pe}$ ; since  $(x - 1)^{pe} = 0$  when  $e$  is big,  $x$  is of finite order equal to a power of  $p$ . Thus, regardless of the value of  $p$ , if  $x \in \mathbf{GL}(n)$  is unipotent, then  $G(x)$ , the smallest closed subgroup of  $\mathbf{GL}(n)$  that contains  $x$ , is a  $K(x)$ -group in which every element is unipotent.

The matrix ring  $\mathbf{M}(n)$  has a natural identification with the endomorphism ring of the vector space  $U^n$  over  $U$ , a matrix  $a = (a_{jj})$  operating on a vector  $v = (v_j)$  according to the formula  $av = (\sum_j a_{jj} v_j)$ . (The matrix  $a$  is the matrix, relative to the canonical basis of  $U^n$ , of the endomorphism  $a$ .) For a given  $x \in \mathbf{M}(n)$ ,  $U^n$  has a structure of  $U[X]$ -module such that, for any  $P = \sum a_k X^k \in U[X]$  and any  $v \in U^n$ ,

$$Pv = P(x)v,$$

$P(x)$  denoting the matrix  $\sum a_k x^k$ . The matrix  $x$  is said to be *semisimple* if this  $U[X]$ -module is semisimple, that is, if the vector space  $U^n$  is generated by characteristic vectors of  $x$ . When this is the case, the matrix of the endomorphism  $x$ , relative to a basis consisting of characteristic vectors of  $x$ , is diagonal. It follows that a matrix  $x \in \mathbf{GL}(n)$  is semisimple if and only if there exists a matrix  $a \in \mathbf{GL}(n)$  such that  $x \in a\mathbf{D}(n)a^{-1}$ . Hence if  $x$  is both semisimple and unipotent, then  $x = 1$ . It is easy to see that if  $x$  is semisimple, then  $a$  can be taken rational over the extension  $L$  of  $K$  generated by the coordinates and characteristic values of  $x$ , and hence that  $G(x)$  is an  $L$ -group, conjugate to an  $L$ -subgroup of  $\mathbf{D}(n)$  by an element of  $\mathbf{GL}(n)$ , and that every element of  $G(x)$  is semisimple. Note that  $L$  is a separable algebraic extension of  $K(x)$ , because the minimal polynomial of  $x$  evidently is separable and has coefficients in  $K(x)$ .

We observe that if  $c$  is a characteristic value of a matrix  $x \in \mathbf{M}(n)$ , and  $r \in \mathbf{N}$ , and  $V_{c,r}(x)$  denotes the space of all vectors  $v \in U^n$  such that  $(x - c1)^r v = 0$ , then  $x'V_{c,r}(x) \subset V_{c,r}(x)$  for every  $x' \in \mathbf{M}(n)$  that commutes with  $x$ . Indeed, if  $v \in V_{c,r}(x)$ , then  $(x - c1)^r x'v = x'(x - c1)^r v = 0$  whence  $x'v \in V_{c,r}(x)$ .

An easy consequence of this observation when  $r = 1$  is that if two semisimple matrices commute, then their product is semisimple.

Another easy consequence is the following: If  $G$  is any commutative subgroup of  $\mathbf{GL}(n)$ , then there exist finitely many natural numbers  $n_1, \dots, n_r$ ,

with  $\sum n_k = n$  and a matrix  $a \in \mathbf{GL}(n)$  (that is algebraic over  $K$  when  $G$  is a  $K$ -group) such that, for every  $x \in G$ ,  $axa^{-1}$  decomposes into diagonal blocks

$$axa^{-1} = \begin{pmatrix} x_1 & & 0 \\ & \ddots & \\ 0 & & x_r \end{pmatrix},$$

where, for each index  $k$ ,  $x_k \in \mathbf{T}(n_k)$  and all the coordinates of  $x_k$  on the main diagonal have the same value  $c_k(x)$ . We observe, in particular, that for every commutative subgroup  $G$  of  $\mathbf{GL}(n)$ , there exists a matrix  $a \in \mathbf{GL}(n)$  such that  $aGa^{-1} \subset \mathbf{T}(n)$ .

Now, every matrix  $x \in \mathbf{GL}(n)$  is in some closed commutative subgroup  $G$  of  $\mathbf{GL}(n)$  (for example, in  $G(x)$ ). Using the above decomposition, we can set

$$x_s = a^{-1} \begin{pmatrix} c_1(x) 1_{n_1} & & 0 \\ & \ddots & \\ 0 & & c_r(x) 1_{n_r} \end{pmatrix} a, \quad x_u = x_s^{-1} x.$$

Then  $x_s$  is semisimple,  $x_u$  is unipotent, and  $x_s x_u = x_u x_s = x$ . For each diagonal block  $x_k$ ,  $(x_k - c_k(x) 1_{n_k})^{n_k} = 0$ ; by the Chinese remainder theorem, there exists a polynomial  $P \in U[X]$  such that

$$P \equiv c_k(x) \pmod{(X - c_k(x))^{n_k}} \quad (1 \leq k \leq r);$$

evidently  $x_s = P(x)$ . It follows that any matrix that commutes with  $x$  commutes with  $x_s$  and  $x_u$ , and conversely. In particular, if  $t, v$  are any commuting elements of  $\mathbf{GL}(n)$ , with  $t$  semisimple,  $v$  unipotent, and  $tv = x$ , then  $x_s^{-1}t = x_u v^{-1}$  and the matrices,  $x_s, x_u, t, v$  commute with each other; hence  $x_s^{-1}t$  is semisimple and  $x_u v^{-1}$  is unipotent, whence both are 1. This proves that, to each matrix  $x \in \mathbf{GL}(n)$ , there corresponds a unique pair  $(x_s, x_u) \in \mathbf{GL}(n)^2$  such that  $x_s$  is semisimple,  $x_u$  is unipotent, and  $x = x_s x_u = x_u x_s$ . (This is the Jordan decomposition of  $x$ .)

**Proposition 38** *Let  $G$  be a commutative  $K$ -subgroup of  $\mathbf{GL}(n)$ , and let  $G_s$  respectively  $G_u$  denote the set of semisimple respectively unipotent elements of  $G$ . Then  $G_s$  is a  $K$ -subgroup of  $G$ ,  $G_u$  is a  $K$ -closed subgroup of  $G$ , and the formula  $x \mapsto (x_s, x_u)$  defines a  $K_1$ -isomorphism  $G \approx G_s \times G_u$ .*

*Proof* Using the above decomposition into diagonal blocks, we see that the formulae  $x \mapsto x_s$  and  $x \mapsto x_u$  define  $K(a)$ -homomorphisms  $p_s': G \rightarrow a^{-1}\mathbf{D}(n)a$  and  $p_u': G \rightarrow a^{-1}\mathbf{T}(n, 1)a$ . Since  $p_s'(G)$  is a closed subgroup of  $a^{-1}\mathbf{D}(n)a \approx \mathbf{G}_m^n$ , the torsion subgroup of  $p_s'(G)$  is dense in  $p_s'(G)$  (see corollary to Proposition 37). Hence, to prove that  $p_s'(G) \subset G$  and  $p_u'(G) \subset G$ , it suffices to show that this torsion subgroup is in  $G$ . However, if  $x_s$  is of finite order  $m$ , then  $p \nmid m$  and  $x_u^m = x^m \in G$ , whence  $x_u \in G$  (when  $p = 0$ ,

because  $x_u = (x_u^m)^{1/m} \in G$ , and when  $p \neq 0$ , because  $x_u$  has finite order relatively prime to  $m$ ), so that  $x_s = x x_u^{-1} \in G$ . It follows that  $p_s'(G) = G_s$  and  $p_u'(G) = G_u$ , so that  $G_s$  and  $G_u$  are  $K(a)$ -subgroups of  $G$ , and  $p_s'$  and  $p_u'$  induce  $K(a)$ -homomorphisms  $p_s: G \rightarrow G_s$  and  $p_u: G \rightarrow G_u$ . For any  $\sigma \in \text{Aut}(U/K)$ , evidently  $(\sigma x)_s = \sigma(x_s)$  and  $(\sigma x)_u = \sigma(x_u)$  ( $x \in \mathbf{GL}(n)$ ); hence  $G_s$  and  $G_u$  are  $K$ -closed. When  $p \neq 0$ , there is an  $e \in \mathbf{N}$  such that  $x_u^{pe} = 1$  ( $x \in G$ ), so that the formula  $x \mapsto x^{pe}$  defines a  $K$ -homomorphism  $G \rightarrow G_s$  that evidently is surjective. Therefore  $G_s$  is a  $K$ -group. The  $K(a)$ -homomorphism  $p_s \times p_u: G \rightarrow G_s \times G_u$  and the  $K_1$ -homomorphism  $G_s \times G_u \subset G \times G \xrightarrow{\mu} G$  (where  $\mu$  is the group law of  $G$ ) are obviously inverse to each other. Therefore  $p_s \times p_u$  is a  $K_1$ -isomorphism.

**Corollary 1** *Let  $G$  be a  $K$ -subgroup of  $\mathbf{GL}(n)$ . If  $x \in G$ , then  $x_s \in G$  and  $x_u \in G$ .*

*Proof* Apply the proposition to  $G(x)$ .

**Corollary 2** *Let  $G$  be a  $K$ -subgroup of  $\mathbf{GL}(n)$ , let  $x \in G$ , and let  $G(x)$  denote the smallest closed subgroup of  $G$  that contains  $x$ . A necessary and sufficient condition that  $x$  be unipotent is that either  $p = 0$  and  $G(x)$  have no torsion or  $p \neq 0$  and  $G(x)$  be a finite  $p$ -group. A necessary and sufficient condition that  $x$  be semisimple is that the torsion subgroup of  $G(x)$  be dense in  $G(x)$  and  $G(x)$  have no  $p$ -torsion.*

*Proof* This is clear.

The notions of unipotent element and semisimple element can now be extended to any linear  $K$ -group  $G$ : An element of  $G$  is called unipotent or semisimple when it satisfies the corresponding condition in Corollary 2. Then, for each element  $x \in G$ , there is a unique pair  $(x_s, x_u) \in G^2$  such that  $x_s$  is semisimple,  $x_u$  is unipotent, and  $x = x_s x_u = x_u x_s$ . Proposition 38 and its two corollaries continue to hold in this more general context.

## F. REDUCTION

As in the preceding subsection, we identify  $\mathbf{M}(n)$  with the ring of endomorphisms of the vector space  $U^n$  over  $U$ , and hence identify  $\mathbf{GL}(n)$  with the group of automorphisms of  $U^n$ .

The following proposition generalizes a result of Sophus Lie.

**Proposition 39** *Let  $G$  be a connected solvable  $K$ -subgroup of  $\mathbf{GL}(n)$ , and suppose that  $K$  is algebraically closed. Then there exists a matrix  $a \in \mathbf{GL}_K(n)$  such that  $aGa^{-1} \subset \mathbf{T}(n)$ .*

*Proof* First we claim that it suffices to prove that  $aGa^{-1} \subset \mathbf{T}(n)$  for some  $a \in \mathbf{GL}(n)$ . Indeed, for each  $x \in G$  the mapping  $f_x: \mathbf{GL}(n) \rightarrow \mathbf{GL}(n)$  given by the formula  $f_x(a) = a^{-1}xa$  is continuous, so that  $f_x^{-1}(\mathbf{T}(n))$  is a closed subset of  $\mathbf{GL}(n)$ , and the intersection  $A = \bigcap_{x \in G} f_x^{-1}(\mathbf{T}(n))$  is, too; evidently  $\sigma A = A$  for every  $\sigma \in \text{Aut}(U/K)$ , so that  $A$  is  $K$ -closed. Since  $K$  is algebraically closed, it follows that if  $A$  is not empty, it has an element rational over  $K$ .

Next we claim that it suffices to show that  $U^n$  has a nonzero proper subspace that is invariant under  $G$ . Indeed, if  $V$  is such a subspace, of dimension say  $m$ , we can fix basis vectors  $v_j = (b_{1j}, \dots, b_{mj})$  of  $U^n$  such that  $v_1, \dots, v_m$  form a basis of  $V$ . The matrix  $b = (b_{ij})$  is in  $\mathbf{GL}(n)$ , and for every  $x \in G$  we can write

$$b^{-1}xb = \begin{pmatrix} x_{11} & x_{12} \\ 0 & x_{22} \end{pmatrix}$$

with  $x_{11} \in \mathbf{GL}(m)$  and  $x_{22} \in \mathbf{GL}(n-m)$ . The formulae  $x \mapsto x_{11}$  and  $x \mapsto x_{22}$  define rational homomorphisms of  $G$  onto connected solvable closed subgroups  $G_1$  of  $\mathbf{GL}(m)$  and  $G_2$  of  $\mathbf{GL}(n-m)$ . Arguing by induction on  $n$ , we may suppose that there exist matrices  $a_1 \in \mathbf{GL}(m)$  and  $a_2 \in \mathbf{GL}(n-m)$  such that  $a_1 G_1 a_1^{-1} \subset \mathbf{T}(m)$  and  $a_2 G_2 a_2^{-1} \subset \mathbf{T}(n-m)$ . Setting  $a = \begin{pmatrix} a_1 & 0 \\ 0 & a_2 \end{pmatrix} b^{-1}$  we then find that  $aGa^{-1} \subset \mathbf{T}(n)$ .

The two claims established, we suppose as we may that  $G$  is not trivial. The commutator group  $G' = [G, G]$  is a connected solvable  $K$ -group and  $\dim G > \dim G'$ . Arguing by induction on  $\dim G$ , for fixed  $n$ , we may suppose that  $a'G'a'^{-1} \subset \mathbf{T}(n)$  for some  $a' \in \mathbf{GL}(n)$ . Then there exists a nonzero vector in  $U^n$  that is a common characteristic vector of all the elements of  $G'$ . Let  $V$  denote the vector space generated by the set of all such vectors. If  $v$  is any such vector, then, for any  $x' \in G'$ , there is an element  $c(x') \in U^*$  such that  $x'v = c(x')v$ , and evidently  $c: G' \rightarrow \mathbf{G}_m$  is a rational homomorphism. For any rational homomorphism  $c: G' \rightarrow \mathbf{G}_m$ , the set  $V_c$  of all vectors  $v' \in U^n$  such that  $x'v' = c(x')v'$  ( $x' \in G'$ ) is a subspace of  $V$ , and if  $v' \in V_c$  and  $x \in G$ , then, for every  $x' \in G'$ , we have  $x' \cdot xv' = x \cdot (x^{-1}x'x)v' = xc(x^{-1}x')v' = c(x^{-1}x')xv'$ . Since the mapping  $c': G' \rightarrow \mathbf{G}_m$  defined by the formula  $c'(x') = c(x^{-1}x'x)$  is a rational homomorphism, this shows that  $xV_c = V_{c'}$ . Using these remarks it is easy to see that there exist finitely many rational homomorphisms  $c_k: G' \rightarrow \mathbf{G}_m$  such that each  $V_{c_k}$  is nonzero and  $V = \sum V_{c_k}$  (direct sum), and that each  $x \in G$  permutes the set of subspaces  $V_{c_k}$ . Because  $G$  is connected, all the elements of  $G$  give the same permutation, which of course must be the identity. Thus, the nonzero subspace  $V_{c_1}$  of  $U^n$  is invariant under  $G$ . If  $V_{c_1} \neq U^n$ , the proposition follows from the second claim established above, so we may suppose that  $V_{c_1} = U^n$ . Then for any  $(x, y) \in G^2$ ,  $xyx^{-1}y^{-1}v = c_1(xyx^{-1}y^{-1})v$  ( $v \in U^n$ ) so that  $xyx^{-1}y^{-1}$  is a scalar

matrix. Since  $\det(xyx^{-1}y^{-1}) = 1$ , the scalar  $c_1(xyx^{-1}y^{-1})$  is an  $n$ th root of unity, and because  $xyx^{-1}y^{-1}$  is a continuous function of  $(x, y)$  and  $G^2$  is connected, therefore  $c_1(xyx^{-1}y^{-1}) = 1$ . Thus, in this case  $G$  is commutative, and the proposition follows from an observation made in Subsection E.

**Proposition 40** *Let  $G$  be a  $K$ -subgroup of  $\mathbf{GL}(n)$  every element of which is unipotent. Then there exists a matrix  $a \in \mathbf{GL}_K(n)$  such that  $aGa^{-1} \subset \mathbf{T}(n, 1)$ .*

*Proof* If there exists a nonzero proper subspace  $W$  of  $U^n$  that is invariant under  $G$ , then, as in the proof of Proposition 39, we can argue by induction on  $n$  to prove the existence of a matrix  $b \in \mathbf{GL}(n)$  such that  $bGb^{-1} \subset \mathbf{T}(n, 1)$ . However, then the set  $V$  of vectors that are invariant under  $G$  is a nonzero subspace of  $U^n$  that is defined over  $K_i$  (because evidently  $\sigma V = V$  for every  $\sigma \in \text{Aut}(U/K)$ ). Since  $G_{K_s}$  is dense in  $G$ ,  $v \in V$  if and only if  $xv = v$  for every  $x \in G_{K_s}$ , so that  $V$  is defined over  $K_s$ , and hence over  $K_s \cap K_i = K$ . Using  $V$  instead of  $W$ , we can use the induction argument above to prove the existence of a matrix  $a \in \mathbf{GL}_K(n)$  such that  $aGa^{-1} \subset \mathbf{T}(n, 1)$ . However, if there does not exist a subspace  $W$  as above, then  $G$  contains  $n^2$  linearly independent matrices (this is a theorem due to Burnside; see, e.g., Lang [22, p. 444], or Bourbaki [6, § 4, No. 3]). Since the trace of any unipotent matrix in  $\mathbf{GL}(n)$  is  $n$ , and therefore  $\text{Tr}(x(y-1)) = \text{Tr}(xy) - \text{Tr}(x) = 0$  for all  $x, y \in G$ , it follows in this case that  $y-1 = 0$  for every  $y \in G$ , so that  $G$  is trivial and  $n = 1$ .

**Proposition 41** *Let  $G$  be a connected  $K$ -subgroup of  $\mathbf{GL}(n)$  every element of which is semisimple, and suppose that  $K$  is separably closed. Then there exists a matrix  $a \in \mathbf{GL}_K(n)$  such that  $aGa^{-1} \subset \mathbf{D}(n)$ .*

*Proof* First strengthen the hypothesis by supposing that  $K$  is algebraically closed and is not an algebraic extension of a finite field. Fix  $x \in \Gamma_{G/K}$  and let  $\alpha_1, \dots, \alpha_n$  denote the characteristic values of  $x$  arranged so that  $(\alpha_1, \dots, \alpha_h)$  is a transcendence basis of  $K(\alpha_1, \dots, \alpha_n)$  over  $K$ . For any  $a_1, \dots, a_h \in K$  ( $a_1, \dots, a_h$ ) is a specialization of  $(\alpha_1, \dots, \alpha_h)$  over  $K$ . If  $(a_1, \dots, a_h)$  fails to annul a certain nonzero polynomial over  $K$ , then (see Chapter 0, Section 14, Proposition 9(c)) this specialization can be extended to a specialization  $(a_1, \dots, a_n, u)$  of  $(\alpha_1, \dots, \alpha_n, x)$  over  $K$  with  $a_1, \dots, a_n \in K$ ,  $u \in \mathbf{M}_K(n)$ , and  $\det u \neq 0$ . When  $p = 0$ , then  $a_1, \dots, a_h$  can be chosen as distinct prime numbers, and when  $p \neq 0$  and  $t \in K$  is transcendental over the prime field  $\mathbf{F}_p$ , then  $a_1, \dots, a_h$  can be chosen as distinct irreducible polynomials in  $\mathbf{F}_p[t]$ . Thus, in either case, there is a specialization  $(a_1, \dots, a_n, u)$  of  $(\alpha_1, \dots, \alpha_n, x)$  over  $K$  with  $u \in G_K$  and  $a_1, \dots, a_n \in K$  such that  $\prod_{1 \leq i \leq h} a_i^{\alpha_i} \neq 1$  whenever

$(e_1, \dots, e_n) \neq (0, \dots, 0)$ . Of course,  $a_1, \dots, a_n$  are the characteristic values of  $u$ . For some  $a' \in \mathbf{GL}_K(n)$ ,  $a'ua'^{-1} \in \mathbf{D}(n)$ . Replacing  $G$  by  $a'Ga'^{-1}$ , we suppose that

$$u = \begin{pmatrix} a_1 & & 0 \\ & \ddots & \\ 0 & & a_n \end{pmatrix}.$$

Then the smallest closed subgroup  $D$  of  $G$  that contains  $u$  is a  $K$ -subgroup of  $\mathbf{D}(n)$ . Fixing an element

$$v = \begin{pmatrix} \beta_1 & & 0 \\ & \ddots & \\ 0 & & \beta_n \end{pmatrix} \in \Gamma_{D^\circ/K},$$

we see that some nonzero power of  $u$  is a specialization of  $v$  over  $K$  and therefore by Proposition 37, that  $\beta_1, \dots, \beta_n$  are algebraically independent over  $K$ . Because  $x \rightarrow v$ , we infer that  $\text{tr deg } K(\beta_1, \dots, \beta_n)/K \leq \text{tr deg } K(\alpha_1, \dots, \alpha_n)/K$ . Therefore  $\text{tr deg } K(\beta_1, \dots, \beta_n)/K = h$ .

Assume  $G \not\subset \mathbf{D}(n)$ . Then  $x$  has the following two properties: (i)  $x \notin \mathbf{D}(n)$ ; (ii) every principal minor of  $x$  is different from 0. As  $G_K$  is dense in  $G$ , there exists a matrix  $y \in G_K$  having the same two properties. Of course  $x \rightarrow vy$ . As  $\alpha_1, \dots, \alpha_n$  are integral over  $K[x]$ , this specialization extends to a specialization  $(x, \alpha_1, \dots, \alpha_n) \rightarrow (vy, \gamma_1, \dots, \gamma_n)$  (see Chapter 0, Section 14, Proposition 9(a)), and evidently  $\gamma_1, \dots, \gamma_n$  are the characteristic values of  $vy$  and  $\text{tr deg } K(\gamma_1, \dots, \gamma_n)/K \leq h$ . Letting  $y(i_1, \dots, i_v)$  denote the  $v$ -rowed principal minor of  $y$  in which the row and column indices are  $i_1, \dots, i_v$ , and setting

$$A_v(X_1, \dots, X_n) = \sum_{1 \leq i_1 < \dots < i_v \leq n} y(i_1, \dots, i_v) X_{i_1} \cdots X_{i_v},$$

we readily see that the characteristic polynomial of  $vy$  is

$$X^n - A_1(\beta_1, \dots, \beta_n) X^{n-1} + \dots + (-1)^n A_n(\beta_1, \dots, \beta_n).$$

Now, the only zero of the ideal  $(A_1, \dots, A_n)$  of  $K[X_1, \dots, X_n]$  is  $(0, \dots, 0)$ , because if  $(c_1, \dots, c_n)$  is a zero, then the equation  $A_n(c_1, \dots, c_n) = 0$  implies that some  $c_j$  vanishes, say  $c_n = 0$ , and then the equation  $A_{n-1}(c_1, \dots, c_{n-1}, 0) = 0$  implies that some other  $c_j$  vanishes, say  $c_{n-1} = 0$ , etc. It follows by the Hilbert theorem on zeros that, for some  $r \in \mathbf{N}$  and every index  $j$ ,  $X_j^r \in (A_1, \dots, A_n)$ , that is,  $X_j^r = \sum_{1 \leq j' \leq n} H_{jj'} A_{j'}$ , where each  $H_{jj'} \in K[X_1, \dots, X_n]$  can evidently be taken homogeneous of degree  $r - j'$ . This implies that  $K[X_1, \dots, X_n]$  is a finitely generated  $K[A_1, \dots, A_n]$ -module, so that each  $X_j$  is integral over  $K[A_1, \dots, A_n]$ . Therefore each  $\beta_j$  is integral over  $K[A_1(\beta_1, \dots, \beta_n), \dots, A_n(\beta_1, \dots, \beta_n)]$ , hence *a fortiori* over  $K[\gamma_1, \dots, \gamma_n]$ . It

follows that  $\text{tr deg } K(\gamma_1, \dots, \gamma_n)/K = h$ , so that  $(\alpha_1, \dots, \alpha_n) \leftrightarrow (\gamma_1, \dots, \gamma_n)$ . Because  $x \rightarrow 1_n$ , we see that  $(\alpha_1, \dots, \alpha_n) \rightarrow (1, \dots, 1)$ . Hence  $(\gamma_1, \dots, \gamma_n) \rightarrow (1, \dots, 1)$ , so that

$$(\gamma_1, \dots, \gamma_n, A_1(\beta_1, \dots, \beta_n), \dots, A_n(\beta_1, \dots, \beta_n)) \rightarrow \left(1, \dots, 1, \binom{n}{1}, \dots, \binom{n}{n}\right).$$

Because each  $\beta_j$  is integral over  $K[\gamma_1, \dots, \gamma_n]$ , this specialization can be extended to a specialization

$$\begin{aligned} &(\gamma_1, \dots, \gamma_n, A_1(\beta_1, \dots, \beta_n), \dots, A_n(\beta_1, \dots, \beta_n), \beta_1, \dots, \beta_n) \\ &\rightarrow \left(1, \dots, 1, \binom{n}{1}, \dots, \binom{n}{n}, b_1, \dots, b_n\right) \end{aligned}$$

where evidently  $b_1, \dots, b_n \in K^*$ . Thus, the matrix  $vy \in G$  with characteristic values  $\gamma_1, \dots, \gamma_n$  specializes over  $K$  to the matrix

$$\begin{pmatrix} b_1 & & 0 \\ & \ddots & \\ 0 & & b_n \end{pmatrix} y$$

with characteristic values  $1, \dots, 1$ . Since every matrix in  $G$  is semisimple, we must have

$$\begin{pmatrix} b_1 & & 0 \\ & \ddots & \\ 0 & & b_n \end{pmatrix} y = 1_n,$$

whence  $y \in \mathbf{D}(n)$ . This contradiction completes the proof under the strengthened hypothesis.

Reverting to the original hypothesis, we see by the above that, for some  $a' \in \mathbf{GL}(n)$ ,  $a'Ga'^{-1} \subset \mathbf{D}(n)$ . Therefore the vector space  $U^n$  is generated by the set of common characteristic vectors of the elements of  $G$ . Thus  $U^n$  is a direct sum,  $U^n = \sum_{1 \leq k \leq r} V_k$  of nonzero subspaces  $V_k$  with the following two properties: (i) For each  $k$  and each  $x \in G$ , all the elements of  $V_k$  are characteristic vectors of  $x$  for the same characteristic value; (ii) For any two distinct indices  $k, k'$ , there exists an  $x \in G$  having characteristic value in  $V_k$  distinct from that in  $V_{k'}$ . Evidently  $\bigcup V_k$  is the set of common characteristic vectors of the elements of  $G$ , and hence (because  $G_K$  is dense in  $G$ ) is the set of common characteristic vectors of the elements of  $G_K$ , and therefore is the set of common characteristic vectors of finitely many elements  $x_1, \dots, x_q \in G_K$ . Since each  $x_i$  is semisimple, its characteristic values  $\alpha_{i1}, \dots, \alpha_{in}$  are in  $K$  (see Subsection E), and since the condition that  $v \in U^n$  be a characteristic vector of  $x_i$  is equivalent to the condition that

$$x_i v = \alpha_{i1} v \quad \text{or} \cdots \quad \text{or} \quad x_i v = \alpha_{in} v,$$

it follows that  $\bigcup V_k$  is a  $K$ -subset of  $U^n$ . Its components are obviously  $V_1, \dots, V_r$  and therefore these vector spaces are  $K$ -subsets of  $U^n$ . Hence each  $V_k$  has a basis consisting of elements of  $K^n$ , and from this it follows that there exists a matrix  $a \in \mathbf{GL}_K(n)$  such that  $aGa^{-1} \subset \mathbf{D}(n)$ .

EXERCISES

1. Suppose that  $p \neq 0$  and  $K = K_i$ . Let  $\Xi$  and  $E_K$  have the same significance as in Corollary 1 to Proposition 35. For each  $\varphi = \sum_{0 \leq k \leq r} a_k \Xi^k \in E_K$  with  $a_k \in K$  ( $0 \leq k \leq r$ ) and  $a_r \neq 0$ , define  $\deg \varphi = r$ . Also, define  $\deg 0 = -1$ .
  - (a) Show that if  $\varphi, \psi \in E_K$  and  $\varphi \neq 0$ , then there exist  $\kappa, \rho \in E_K$  with  $\deg \rho < \deg \varphi$  such that  $\psi = \varphi\kappa + \rho$ .
  - (b) Show that if  $f: \mathbf{G}_a^n \rightarrow \mathbf{G}_a$  is a nontrivial  $K$ -homomorphism, then there exists a  $K$ -automorphism  $\alpha$  of  $\mathbf{G}_a^n$  such that  $\text{Ker}(f \circ \alpha) = \mathbf{G}_a^{n-1} \times F$ , where  $F$  is a finite  $K$ -subgroup of  $\mathbf{G}_a$ . (*Hint:* Let  $in_j: \mathbf{G}_a \rightarrow \mathbf{G}_a^n$  denote the  $j$ th canonical injection, set  $\varphi_j = f \circ in_j$ ,  $m = \sum (1 + \deg \varphi_j)$ , and  $d = \min \deg \varphi_j$  ( $1 \leq j \leq n$ ,  $\varphi_j \neq 0$ ). Permuting indices, suppose that  $\deg \varphi_n = d$  and by part (a) write  $\varphi_j = \varphi_n \kappa_j + \rho_j$  with  $\deg \rho_j < d$ . Observe that the formula  $(x_1, \dots, x_n) \mapsto \sum_{1 \leq j < n} \rho_j(x_j) + \varphi_n(x_n)$  defines a nontrivial  $K$ -homomorphism  $f': \mathbf{G}_a^n \rightarrow \mathbf{G}_a$ , and argue by induction on  $m$ .)
  - (c) Show that if  $G$  is a  $K$ -subgroup of  $\mathbf{G}_a^n$  and  $d = \dim G$ , then there exists a  $K$ -automorphism  $\alpha$  of  $\mathbf{G}_a^n$  such that  $\alpha(G) = \mathbf{G}_a^d \times F$ , where  $F$  is a finite  $K$ -subgroup of  $\mathbf{G}_a^{n-d}$ . (*Hint:* First show that  $G$  may be supposed connected with  $d < n$ , that it suffices to prove  $\beta(G) \subset \mathbf{G}_a^{n-1} \times 0$  for some  $K$ -automorphism  $\beta$  of  $\mathbf{G}_a^n$ , that it may be supposed that  $pr_j(G) = \mathbf{G}_a$  ( $1 \leq j \leq n$ ), and that when  $x = (x_1, \dots, x_n) \in \Gamma_{G/K}$ , then  $(x_1, \dots, x_d)$  is a separating transcendence basis of  $K(x)$  over  $K$ . Infer that then the canonical projection  $pr^n: \mathbf{G}_a^n \rightarrow \mathbf{G}_a^{n-1}$  onto the product of the first  $n-1$  factors induces a surjective separable  $K$ -homomorphism  $G \rightarrow G'$  with finite kernel  $G \cap (0^{n-1} \times \mathbf{G}_a) = 0^{n-1} \times F'$ . Arguing by induction on  $n-d$ , fix a  $K$ -automorphism  $\alpha'$  of  $\mathbf{G}_a^{n-1}$  such that  $\alpha'(G') = \mathbf{G}_a^d \times 0^{n-1-d}$ , let  $p': \mathbf{G}_a^{n-1} \rightarrow \mathbf{G}_a^d$  denote the canonical projection onto the product of the first  $d$  factors, and by Proposition 35 fix a  $K$ -endomorphism  $\varphi'$  of  $\mathbf{G}_a$  with kernel  $F'$ . Show that there exists a  $K$ -homomorphism  $f': \mathbf{G}_a^d \rightarrow \mathbf{G}_a$  such that  $f' \circ p' \circ \alpha' \circ pr^n$  coincides with  $\varphi' \circ pr_n$  on  $G$ , and apply part (b) to the difference  $f = f' \circ p' \circ \alpha' \circ pr_n - \varphi' \circ pr_n$ .)
2. Let  $G$  be a connected linear  $K$ -group of dimension 1.
  - (a) Show that either every element of  $G$  is semisimple or every element of  $G$  is unipotent. (*Hint:* Observe that it may be assumed that  $G \subset$

- $\mathbf{GL}(n)$ . Show that when  $x \in \Gamma_{G/K}$  is unipotent, then so is every element of  $G$ . When not, show that  $x_s$  has infinite order, fix  $a \in \mathbf{GL}(n)$  such that  $ax_s a^{-1} \in \mathbf{D}(n)$ , and conclude that  $aGa^{-1} \subset \mathbf{D}(n)$ .)
- (b) Show that if every element of  $G$  is semisimple, then  $G$  is  $K_s$ -isomorphic to  $\mathbf{G}_m$ . (*Hint:* Use Propositions 41 and 37.)
  - (c) Show that if every element of  $G$  is unipotent, then  $G$  is commutative and there exists a separable surjective  $K_i$ -homomorphism  $G \rightarrow \mathbf{G}_a$  the kernel of which is a finite  $K$ -group of order a power of  $p$ . (*Hint:* Use Proposition 40 to reduce to the case in which  $G \subset \mathbf{T}(n, 1)$ , then define  $k \in \mathbf{N}$  such that  $G \subset \mathbf{T}(n, k-1)$  and  $G \not\subset \mathbf{T}(n, k)$ , and show that for some  $h$  with  $1 \leq h \leq n-k+1$  the formula  $(x_{ij}) \mapsto x_{h, h+k-1}$  defines a surjective  $K$ -homomorphism  $G \rightarrow \mathbf{G}_a$  with finite kernel  $N$ ; then use Proposition 35(d) to infer that  $G/N$  is  $K_i$ -isomorphic to  $\mathbf{G}_a$ .)
  - (d) Conclude in the case  $p = 0$  that if every element of  $G$  is unipotent, then  $G$  is  $K$ -isomorphic to  $\mathbf{G}_a$ . (In the case  $p \neq 0$ , when all the polynomials  $X^p - c$  and  $X^p - X - c$  ( $c \in K$ ) have roots in  $K$ , then again  $G$  is  $K$ -isomorphic to  $\mathbf{G}_a$ , but the proof is more delicate. See Chevalley [10, exposé No. 7], or Borel [3, p. 257].)
3. Let  $G$  be a connected  $K$ -group and let  $r \in \mathbf{N}$ ,  $p \nmid r$ . Prove that the subgroup generated by the set of elements  $x^r$  ( $x \in G$ ) is  $G$ . (*Hint:* Denoting the subgroup by  $H$ , use Section 8, Proposition 7 and the remark thereafter, to show that  $H$  is a connected normal  $K$ -subgroup of  $G$ . Replacing  $G$  by  $G/H$ , reduce to the case in which  $H = 1$ . In the special case in which  $G$  is a  $K$ -subgroup of  $\mathbf{GL}(n)$ , observe that the characteristic roots of the elements of  $G$  all are  $r$ th roots of unity, infer from the connectedness of  $G$  that every element of  $G$  is unipotent, and conclude that  $G = 1$ . In general, apply this result to the image of the  $K$ -homomorphism  $a^{(h)}: G \rightarrow \mathbf{GL}(r(h))$  in the discussion at the end of Section 19 to show that  $G$  is commutative, and then use Section 22, Corollary to Theorem 14.)
  4. Let  $f: G \rightarrow G'$  be a  $K$ -homomorphism of linear  $K$ -groups, let  $x \in G$ , and let  $G(x)$  respectively  $G'(f(x))$  denote the smallest closed group containing  $x$  respectively  $f(x)$ .
    - (a) Prove that  $f(G(x)) = G'(f(x))$ .
    - (b) Prove that if  $x$  is unipotent respectively semisimple then so is  $f(x)$ .
  5. Let  $G$  be a connected linear  $K$ -group of dimension 2, and suppose that  $p = 0$ . Prove that  $G$  is solvable. ( $G$  is solvable when  $p \neq 0$ , too, but the proof is more difficult; see Borel [3, p. 265].) (*Hint:* Using Propositions 40 and 41, show that it may be assumed that  $G$  contains connected closed subgroups  $T$  and  $W$  of dimension 1 that consist, respectively, of semisimple elements and of unipotent elements. Letting  $L$  be an extension of  $K$  such that  $T$  and  $W$  are  $L$ -groups, fix



$(t, w) \in \Gamma_{T \times W/L}$  and observe that  $twt^{-1} \xrightarrow{L} w$ . Show that this specialization is generic and conclude that  $W$  is normal in  $G$ .)

6. Let  $G$  be a linear  $K$ -group.

(a) Call  $G$  *K-Liouvillian* if there exists a normal sequence  $G = G_0 \supset G_1 \supset \dots \supset G_r = 1$  of  $K$ -groups such that every  $G_{k-1}/G_k$  either is  $K$ -isomorphic to  $G_a$  or  $G_m$  or is finite. Call  $G$  *Liouvillian* if it is  $L$ -Liouvillian for some extension  $L$  of  $K$ . Prove that the following three conditions are equivalent: (L1)  $G$  is  $K_a$ -Liouvillian; (L2)  $G$  is Liouvillian; (L3)  $G^\circ$  is solvable. (In proving (L3)  $\Rightarrow$  (L1), use is made of Exercise 2; therefore  $K$  must be subject to the same restriction as in Exercise 2(d).)

(b) Let  $i$  be an integer with  $1 \leq i \leq 7$ . Call  $G$  *K-Liouvillian of type (i)* if the normal sequence in part (a) can be chosen so that every  $G_{k-1}/G_k$  is  $K$ -isomorphic to a  $K$ -subgroup of a  $K$ -group in the  $i$ th line of the following list:

- (1)  $G_a, G_m$ , a finite  $K$ -group;
- (2)  $G_a, G_m$ ;
- (3)  $G_a$ , a finite  $K$ -group;
- (4)  $G_m$ , a finite  $K$ -group;
- (5)  $G_a$ ;
- (6)  $G_m$ ;
- (7) a finite  $K$ -group.

Call  $G$  *Liouvillian of type (i)* if  $G$  is  $L$ -Liouvillian of type (i) for some extension  $L$  of  $K$ . Prove, for each (i), that the following three conditions are equivalent: (L(i)1)  $G$  is  $K_a$ -Liouvillian of type (i); (L(i)2)  $G$  is Liouvillian of type (i); (L(i)3)  $G$  satisfies the  $i$ th condition in the following list:

- (1)  $G^\circ$  is solvable;
- (2)  $G$  is solvable;
- (3)  $G^\circ$  consists of unipotent elements,
- (4)  $G^\circ$  consists of semisimple elements,
- (5)  $G$  consists of unipotent elements,
- (6)  $G$  is solvable and consists of semisimple elements,
- (7)  $G^\circ = 1$ .

(See the parenthetical remark at the end of part (a).) For each  $i$ , examine condition (L(i)1) to see whether  $K_a$  can be replaced by a smaller extension of  $K$ .

7. Let  $p = 0$  and let  $G$  be a commutative  $K$ -subgroup of  $\mathbf{GL}(n)$  of dimension  $d$  every element of which is unipotent. Prove that  $G$  is  $K$ -isomorphic to  $G_a^d$ . (Hint: Let  $U_n$  respectively  $N_n$  denote the set of all unipotent respectively nilpotent elements of  $\mathbf{GL}(n)$  respectively  $\mathbf{M}(n)$ . Show

that  $U_n$  respectively  $N_n$  is a  $K$ -subset of  $\mathbf{GL}(n)$  respectively  $\mathbf{M}(n)$  ( $\mathbf{M}(n)$  being identified with  $G_a^{n^2}$ ), define everywhere defined  $K$ -mappings  $\log: U_n \rightarrow N_n$  and  $\exp: N_n \rightarrow U_n$  that are inverse to each other, and show that  $\log$  maps  $G$   $K$ -isomorphically onto a  $K$ -subgroup of  $\mathbf{M}(n)$ .)

8. (Kolchin [18]) A  $K$ -group is said to be *K-simple* if it is infinite and every  $K$ -closed normal proper subgroup is finite.

(a) Show that a  $K$ -simple  $K$ -group is connected, that a connected  $K$ -group of dimension 1 is  $K$ -simple, and that in a noncommutative  $K$ -simple  $K$ -group the center is finite and every  $K$ -closed normal proper subgroup is central.

(b) Prove that if  $G_1, \dots, G_n$  are  $K$ -simple  $K$ -groups and  $G$  is a proper  $K$ -subgroup of  $P = \prod_{1 \leq j \leq n} G_j$ , then either (i) there exists an index  $j$  such that  $pr_j(G) \neq G_j$ , or (ii) there exist distinct indices  $j, k$  with  $G_j$  and  $G_k$  noncommutative, and a finite normal  $K$ -subgroup  $F$  of  $G_k$ , and a surjective  $K$ -homomorphism  $f: G_j \rightarrow G_k/F$  such that  $f(x_j) = \pi(x_k)$  for every  $(x_1, \dots, x_n) \in G$  ( $\pi$  denoting the canonical homomorphism  $G_k \rightarrow G_k/F$ ), or (iii) there exist distinct indices  $j(1), \dots, j(l)$  with  $l \geq 2$  and each  $G_{j(\lambda)}$  commutative, a finite  $K$ -subgroup  $F$  of  $G_{j(1)}$ , and surjective  $K$ -homomorphisms  $f_\lambda: G_{j(\lambda)} \rightarrow G_{j(1)}/F$  ( $1 \leq \lambda \leq l$ ) with  $f_\lambda$  separable such that  $\prod_{1 \leq \lambda \leq l} f_\lambda(x_{j(\lambda)}) = 1$  for every  $(x_1, \dots, x_n) \in G$ . (Hint: Reduce to the case in which  $pr_n \circ in_{P,G}: G \rightarrow G_n$  and  $pr^n \circ in_{P,G}: G \rightarrow \prod_{1 \leq j \leq n-1} G_j$  are surjective and the latter is separable. Then show that  $\text{Ker}(pr^n \circ in_{P,G}) = 1^{n-1} \times F$ , where  $F$  is a finite normal  $K$ -subgroup of  $G_n$ , and ( $\pi$  denoting the canonical homomorphism  $G_n \rightarrow G_n/F$ ) that  $\pi \circ pr^n \circ in_{P,G} = \varphi \circ pr^n \circ in_{P,G}$  for some surjective  $K$ -homomorphism  $\varphi: \prod_{1 \leq j \leq n-1} G_j \rightarrow G_n/F$ . Let  $in_k: G_k \rightarrow \prod_{1 \leq j \leq n-1} G_j$  denote the canonical injection and set  $\varphi_k = \varphi \circ in_k$  ( $1 \leq k \leq n-1$ ). When  $G_n$  is noncommutative, show that there is a unique  $k$  such that  $\varphi_k$  is nontrivial, and set  $f = \varphi_k$ . When  $G_n$  is commutative, let  $j(1), \dots, j(l-1)$  denote the indices  $k$  such that  $\varphi_k$  is nontrivial (and hence surjective), show that each  $G_{j(\lambda)}$  is commutative, and set  $f_\lambda = \varphi_{j(\lambda)}$  ( $1 \leq \lambda \leq l-1$ ),  $j(l) = n$ , and  $f_l = \pi \circ \iota$ , where  $\iota$  denotes the automorphism  $x \mapsto x^{-1}$  of  $G_n$ .)

(c) It is known that  $\mathbf{SL}(r)$  is  $K$ -simple ( $r \geq 2$ ), that the center of  $\mathbf{SL}(r)$  is  $P, 1$ , ( $P$ , denoting the group of  $r$ th roots of unity), that every  $K$ -automorphism of  $\mathbf{SL}(r)/P, 1$ , is induced by a  $K$ -automorphism of  $\mathbf{SL}(r)$ , and that every  $K$ -automorphism of  $\mathbf{SL}(r)$  is of the form  $x \mapsto axa^{-1}$  or of the form  $x \mapsto a\check{x}a^{-1}$  where  $a \in \mathbf{GL}_K(r)$  and  $\check{x}$  denotes the inverse of the transpose of  $x$ . (These facts can either be found or be deduced from what can be found in Dieudonné [13]; complete proofs are given in Kolchin [17].) Using these facts, show that if  $p = 0$  and  $G$  is a proper  $K$ -subgroup of  $\mathbf{SL}(r)^n$  with  $pr_j(G) = \mathbf{SL}(r)$  ( $1 \leq j \leq n$ ),

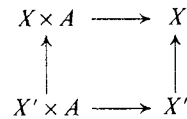
then there exist distinct indices  $j, k$ , and a matrix  $a \in \mathbf{GL}_K(r)$ , and a  $K$ -homomorphism  $\gamma: G \rightarrow \mathbf{P}_r$  such that either  $x_k = \gamma(x)ax_ja^{-1}$  ( $x = (x_1, \dots, x_n) \in G$ ) or  $x_k = \gamma(x)a\bar{x}_ja^{-1}$  ( $x = (x_1, \dots, x_n) \in G$ ). Show that when  $r = 2$ , then the matrix  $a \in \mathbf{GL}(2)$  can be chosen so that  $x_k = \gamma(x)ax_ja^{-1}$  ( $x = (x_1, \dots, x_n) \in G$ ).

(d) Show that if  $p = 0$  and  $G$  is a proper  $K$ -subgroup of the direct product of commutative  $K$ -simple  $K$ -groups  $G_1, \dots, G_n$ , then there exist an index  $k$  and  $K$ -homomorphisms  $f_j: G_j \rightarrow G_k$  ( $1 \leq j \leq n$ ) not all trivial, such that  $\prod_{1 \leq j \leq n} f_j(x_j) = 1$  for every  $(x_1, \dots, x_n) \in G$ .

**24 Abelian  $K$ -groups**

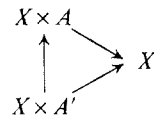
A  $K$ -set  $A$  is said to be *complete* if, for every extension  $L$  of  $K$  and every  $L$ -set  $X$ , the canonical projection  $X \times A \rightarrow X$  is closed (that is, maps every closed subset of  $X \times A$  onto a closed subset of  $X$ ).

When  $X \times A \rightarrow X$  is closed for a particular  $X$  and  $X'$  is any closed subset of  $X$ , then (because the inclusion mapping  $X' \times A \rightarrow X \times A$  is closed and the diagram shown here is commutative) the projection  $X' \times A \rightarrow X'$  is closed too.



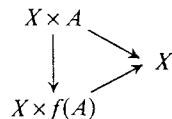
Therefore it suffices to verify the condition that  $X \times A \rightarrow X$  be closed when  $X$  is a homogeneous  $L$ -space.

A similar argument shows that every closed subset of a complete  $K$ -set is complete.



If  $A$  and  $B$  are complete  $K$ -sets, then  $A \times B$  is complete (because, in the composite mapping  $X \times A \times B \rightarrow X \times A \rightarrow X$ , each arrow stands for a closed mapping).

Let  $f: A \rightarrow Y$  be an everywhere defined  $K$ -mapping of  $K$ -sets. It is easy to see that the graph of  $f$  is closed in  $A \times Y$ . Since  $f(A)$  is the projection of the graph into  $Y$  it follows that if  $A$  is complete, then  $f(A)$  is closed in  $Y$ ; because the diagram shown here is commutative,  $f(A)$  is complete, too.



It is easy to see (by Chapter 0, Section 14, Proposition 9(b)) that projective  $n$ -space  $\mathbf{P}(n)$ , which is a homogeneous  $K$ -space for  $\mathbf{GL}(n+1)$ , is complete.

The formula  $x \mapsto (1:x)$  gives an everywhere defined  $K$ -mapping  $\mathbf{G}_a \rightarrow \mathbf{P}(1)$ . The image is the complement of the point  $(0:1)$ , and hence is not closed. Therefore  $\mathbf{G}_a$  is not complete. It follows that if  $A$  is complete and  $f$  is an everywhere defined  $K$ -mapping of  $A$  into  $\mathbf{G}_a^n$ , then  $f(A)$  is finite; when  $A$  is also connected,  $f$  is a constant mapping.

A  $K$ -group is said to be *Abelian* if it is connected and complete. It follows from the above that every connected  $K$ -subgroup of an Abelian  $K$ -group is Abelian, that the direct product of finitely many Abelian  $K$ -groups is Abelian, that a  $K$ -homomorphic image of an Abelian  $K$ -group is Abelian, and that any  $K$ -homomorphism of an Abelian  $K$ -group into a linear  $K$ -group is trivial.

Since a  $K$ -homomorphic image of a linear  $K$ -group is linear (Section 23, Proposition 34), any  $K$ -homomorphism of a connected linear  $K$ -group into an Abelian  $K$ -group is trivial.

Because the quotient of a connected  $K$ -group  $G$  by its center is linear (see Section 23, Proposition 32(d), and the example discussed at the end of Section 19), every Abelian  $K$ -subgroup of  $G$  is central in  $G$ . In particular, every Abelian  $K$ -group is commutative.

It follows that if  $A$  is an Abelian  $K$ -group and  $n \in \mathbf{Z}$ , the formula  $x \mapsto x^n$  defines a  $K$ -endomorphism of  $A$ . By Section 22, corollary to Theorem 14, when  $p \nmid n$ , this  $K$ -endomorphism is surjective and has finite kernel.

In what follows we describe (mostly without proof, but with references) further properties of Abelian  $K$ -groups.

If  $A$  is an Abelian  $K$ -group, then, for *any* nonzero  $n \in \mathbf{Z}$ , the  $K$ -endomorphism  $x \mapsto x^n$  of  $A$  is surjective and has finite kernel. (Lang [21, p. 96] or Mumford [23, pp. 62–64] or Weil [27, p. 127].) More precisely, the order of the kernel divides  $n^{2 \dim A}$ , and equals this number when  $p \nmid n$ . (Mumford [23, pp. 62–64], or Weil [27, p. 127].) This implies that for any prime number  $l \neq p$ , the  $l$ -torsion subgroup of  $A$  (that is, the group consisting of all elements  $x \in A$  such that  $x^l = 1$  for some  $n \in \mathbf{N}$ ) is dense in  $A$ .

A  $K$ -mapping of an irreducible  $K$ -set  $V$  into an Abelian  $K$ -group is defined at every simple point of  $V$ . (Lang [21, p. 20] or Weil [27, p. 27].)

If  $f$  is a  $K$ -mapping of a connected  $K$ -group into an Abelian  $K$ -group and  $f(1) = 1$ , then  $f$  is a  $K$ -homomorphism. (Lang [21, p. 24] or Mumford [23, p. 43].)

If  $A$  is an Abelian  $K$ -subgroup of a connected  $K$ -group  $G$ , then  $G$  has a normal connected  $K$ -closed subgroup  $G_1$  such that  $G_1 \cap A$  is finite and  $G_1 A = G$ ; when  $G_1$  is Abelian, then so is  $G$ . (This is Rosenlicht's generalization of Weil's generalization of Poincaré's "theorem of complete reducibility.")

*Proof* (after Lang [21, pp. 27–29]) Fix  $x \in \Gamma_{G/K}$  and set  $K' = K(xA)$ , so that  $K' \subset K(x)$ . Then  $xA$ , a  $K'$ -subset of  $G$ , has an element  $x_1$  separably algebraic over  $K'$ . Let  $x_1, \dots, x_n$  be the conjugates of  $x_1$  over  $K'$  and set  $y = x^{-1}x_1 \cdots x^{-1}x_n$ . Then  $x^{-1}x_j \in A$ ,  $x_{\pi(1)} \cdots x_{\pi(n)} = xx^{-1}x_{\pi(1)} \cdots xx^{-1}x_{\pi(n)} = x^n y$  for every permutation  $\pi$  of the set  $\{1, \dots, n\}$ , and  $x_1 \cdots x_n$  is rational over  $K'$  hence *a fortiori* over  $K(x)$ , whence  $y \in A_{K(x)}$ . Therefore there exists a  $g \in \mathfrak{M}_K(G, A)$  with  $g(x) = y$ ; this  $g$  is defined at 1 and  $g(1) \in A_K$ , so that there exists an  $f \in \mathfrak{M}_K(G, A)$  with  $f(x) = g(1)^{-1}g(x)$ ;  $f$  is a  $K$ -homomorphism. Set  $G_1 = \text{Ker}(f)^\circ$ . Then  $G_1$  is a normal connected  $K$ -closed subgroup of  $G$ . Now,  $xA$  is a  $K$ -generic element of  $G/A$ , so that  $\text{tr deg } K'/K = \dim G/A$ , whence  $\dim_{K'} x = \dim G - \dim G/A = \dim A$ , and  $x \in \Gamma_{xA/K'}$ . However, for any  $t \in \Gamma_{xA/K(x)}$ , evidently  $xt \in \Gamma_{xA/K'}$ , so that  $x \xleftrightarrow{K'} xt$ . Therefore there exists a  $\sigma \in \text{Aut}(U/K')$  with  $\sigma x = xt$ , so that  $f(xt) = f(\sigma x) = \sigma f(x) = \sigma(g(1)^{-1}g(x)) = g(1)^{-1}\sigma y$

$$= g(1)^{-1}\sigma(x^{-n}x_1 \cdots x_n) = g(1)^{-1}(xt)^{-n}x_1 \cdots x_n = g(1)^{-1}y t^{-n} = f(x)t^{-n}.$$

It follows that  $f(t) = t^{-n}$ , and hence that  $f$  is surjective and that  $\text{Ker}(f) \cap A$  is finite, so that  $G_1 \cap A$  is finite too. The formula  $(z, u) \mapsto zu$  defines a  $K_1$ -homomorphism  $G_1 \times A \rightarrow G$ . Its kernel is finite; hence its image  $G_1 A$  has dimension  $\dim G_1 + \dim A = \dim \text{Ker}(f) + \dim A = \dim G$ , so that  $G_1 A = G$ . When  $G_1$  is Abelian, then so is  $G_1 \times A$  and hence  $G$ , too. This completes the proof.

Before we state the fundamental structure theorem due, independently, to Chevalley and Barsotti, we give two very special cases used in its proof.

A commutative connected  $K$ -group that is not Abelian has a closed subgroup  $U$ -isomorphic to  $\mathbf{G}_a$  or  $\mathbf{G}_m$ . (Rosenlicht [24]. Without assuming commutativity, Rosenlicht proves, beginning on p. 437, that there is a connected linear closed subgroup of strictly positive dimension, he remarks elsewhere that a commutative closed subgroup of  $\mathbf{GL}(n)$  of strictly positive dimension has a closed subgroup  $U$ -isomorphic to  $\mathbf{G}_a$  or  $\mathbf{G}_m$ , which we know from Section 23, Proposition 39, and the fact, alluded to in Section 23, that every connected linear  $K$ -group of dimension one is  $K_a$ -isomorphic to  $\mathbf{G}_a$  or  $\mathbf{G}_m$ .)

If  $H$  is a central  $K$ -subgroup of a connected  $K$ -group  $G$  such that  $H$  is  $K$ -isomorphic to  $\mathbf{G}_a$  or  $\mathbf{G}_m$  and  $G/H$  is linear, then  $G$  is linear. (Rosenlicht [24, p. 438].)

We now state (and even prove) the fundamental structure theorem.

*Let  $G$  be a connected  $K$ -group. Then  $G$  has a connected linear normal  $K$ -closed subgroup  $L$  such that  $G/L$  is Abelian. Every connected linear closed subgroup of  $G$  is a subgroup of  $L$ .*

*Proof* (After Rosenlicht [24, pp. 439–440]) First we show by induction on  $\dim G$  that  $G$  has a connected linear normal closed subgroup  $L$  such that  $G/L$  is Abelian. Let  $C$  denote the center of  $G$ . If  $C^\circ$  is not Abelian, then (by the first special case)  $C^\circ$  has a closed subgroup  $H$  that for some extension  $K'$  of  $K$  is  $K'$ -isomorphic to  $\mathbf{G}_a$  or  $\mathbf{G}_m$ ; because  $\dim G/H < \dim G$ , we may suppose that  $G/H$  has a connected linear normal closed subgroup, which we may write as  $L/H$  with  $L$  a connected normal closed subgroup of  $G$  containing  $H$ , such that  $(G/H)/(L/H)$  is Abelian; then  $G/L$  is Abelian and (by the second special case)  $L$  is linear. If  $C^\circ$  is Abelian, then either  $C^\circ = 1$  or  $C^\circ \neq 1$ . In the former case  $G \approx G/C^\circ$  is linear and we can take  $L = G$ . In the latter case  $G$  has a normal connected  $K$ -closed subgroup  $G_1$  such that  $G_1 \cap C^\circ$  is finite and  $G_1 C^\circ = G$ ; since then  $\dim G_1 < \dim G$ , we may suppose that  $G_1$  has a connected linear normal closed subgroup  $L$  such that  $G_1/L$  is Abelian. Evidently  $L$  is normal in  $G$ , and  $G/L = (G_1 C^\circ)/L = (G_1/L) \cdot (C^\circ L/L)$ ; since the composite  $K_1$ -homomorphism  $C^\circ \rightarrow C^\circ/(C^\circ \cap L) \rightarrow C^\circ L/L$  is surjective,  $C^\circ L/L$  is Abelian, so that  $G_1/L \times C^\circ L/L$  is too, and so is the image of the  $K_1$ -homomorphism  $G_1/L \times C^\circ L/L \rightarrow (G_1/L) \cdot (C^\circ L/L) = G/L$ . This proves the existence of the closed  $L$ . For any connected linear closed subgroup  $L'$  of  $G$ ,  $\pi_{G/L}(L')$  is linear because  $L'$  is, and is Abelian because  $G/L$  is, and hence is trivial, so that  $L' \subset L$ . In particular, for any  $\sigma \in \text{Aut}(U/K)$ ,  $\sigma L \subset L$  and hence  $L$  is  $K$ -closed. This completes the proof.

The  $K$ -groups  $\mathbf{W}(g_2, g_3)$ , which are defined when  $p \neq 2$  and the coefficients  $g_2, g_3 \in K$  have the property that  $g_2^3 - 27g_3^2 \neq 0$ , are closed in  $\mathbf{P}(2)$  and hence are Abelian. Conversely, when  $K$  is a perfect field and  $p \neq 2, 3$ , then every nonlinear connected  $K$ -group of dimension 1 is  $K$ -isomorphic to some  $\mathbf{W}(g_2, g_3)$ .

*Proof* Denote the  $K$ -group by  $G$ . The linear  $K$ -subgroup  $L$  of  $G$  that appears in the Chevalley–Barsotti structure theorem is not  $G$  and hence is trivial, so that  $G$  is Abelian.  $\mathfrak{F}(G)$  is a regular finitely generated extension of transcendence degree 1 of the algebraically closed field  $U$ , and, for each  $x \in G$ ,  $\rho_x^*$  is an automorphism of this extension. By a well-known theorem, going back to Klein and Poincaré when  $U = \mathbf{C}$ , if such an extension has infinitely many automorphisms, then its genus is 0 or 1 (for a proof of the general theorem see Iwasawa and Tamagawa [14]). Since  $K$  is perfect,  $U$  is separable over  $K$  and hence the extension  $\mathfrak{F}_K(G)$  of  $K$  has genus 0 or 1, too (see Chevalley [8, p. 99]). Of course,  $G$  has an element that is rational over  $K$ , namely 1. If the genus were 0, then (see Chevalley [8, Chapter II, § 2]) there would exist a  $K$ -function  $\zeta$  on  $G$  such that  $\mathfrak{F}_K(G) = K(\zeta)$ , and hence there would exist a generically invertible  $K$ -mapping of  $\mathbf{G}_a$  into  $G$ ; since  $G$  is Abelian this would, after translation, be a  $K$ -isomorphism  $\mathbf{G}_a \approx G$ . Therefore the genus is 1. Hence (see Chevalley [8, Chapter II,

§ 2]) there exist  $K$ -functions  $\xi, \eta$  on  $G$  such that  $\mathfrak{F}_K(G) = K(\xi, \eta)$  and  $\eta^2$  is a cubic polynomial in  $\xi$  over  $K$  with distinct roots. Replacing  $(\xi, \eta)$  by  $(a\xi + b, c\eta)$  for suitable  $a, b, c \in K$  with  $ac \neq 0$ , we may even suppose that  $\eta^2 = 4\xi^3 - g_2\xi - g_3$ , where  $g_2, g_3 \in K$  and  $g_2^3 - 27g_3^2 \neq 0$ . Fixing  $x \in \Gamma_{G/K}$ , we see that  $(1:\xi(x):\eta(x)) \in \Gamma_{W/K}$ , where  $W = W(g_2, g_3)$ , so that there exists a generically invertible  $K$ -mapping  $f$  of  $G$  into  $W$ . As  $W$  is Abelian, and every element of  $G$  is simple,  $f$  is everywhere defined, so that we may replace  $f$  by the  $K$ -mapping  $\rho_{f(1)^{-1}} \circ f$ , that is, we may suppose that  $f(1) = 1$ , and then  $f$  is a  $K$ -isomorphism.

In order to describe the conditions under which two  $K$ -groups  $W(g_2, g_3)$  are  $K$ -isomorphic, we introduce the classical *invariant*

$$j(g_2, g_3) = 64 \cdot 27g_2^3 / (g_2^3 - 27g_3^2).$$

It is clear that  $j(g_2, g_3) = 0$  if and only if  $g_2 = 0$ , and that  $j(g_2, g_3) = 64 \cdot 27$  if and only if  $g_3 = 0$ .

Consider two such  $K$ -groups,  $W = W(g_2, g_3)$  and  $W' = W(g_2', g_3')$ , and set  $j = j(g_2, g_3)$  and  $j' = j(g_2', g_3')$ . We claim that if  $W$  and  $W'$  are  $K$ -isomorphic, then  $j = j'$  and there exists a nonzero element  $c \in K$  such that  $g_2' = g_2c^4$  and  $g_3' = g_3c^6$ , and that, conversely, if  $j = j' \neq 0$ ,  $64 \cdot 27$  and  $g_3'/g_3$  is a square in  $K$ , or if  $j = j' = 0$  and  $g_3'/g_3$  is a square and a cube in  $K$ , or if  $j = j' = 64 \cdot 27$  and  $g_2'/g_2$  is a fourth power in  $K$ , then there exists a nonzero element  $c \in K$  such that the formula  $(1:x:y) \mapsto (1:c^2x:c^3y)$  defines a  $K$ -isomorphism  $W \approx W'$ . Indeed let  $\xi$  and  $\eta$  denote the  $K$ -functions on  $W$  such that  $\xi((1:x:y)) = x$  and  $\eta((1:x:y)) = y$ , and let  $\xi'$  and  $\eta'$  denote the analogous  $K$ -functions on  $W'$ ; then  $\xi$  and  $\eta$  have a pole at  $1 = (0:0:1)$  of order 2 and 3, respectively, and have no other pole (see Chevalley [8, p. 5]). The set of  $K_i$ -functions on  $W$  that are of order greater than or equal to  $-2$  respectively  $-3$  at  $(0:0:1)$  and are of order greater than or equal to 0 everywhere else is a vector space over  $K_i$  of dimension 2 respectively 3; this is a consequence of the Riemann-Roch theorem (see Chevalley [8, Chapter II, § 5, Theorem 3 and the corollary to Theorem 6]). If  $f: W \approx W'$  is a  $K$ -isomorphism, evidently  $f^*(\xi')$  and  $f^*(\eta')$  have a pole at  $(0:0:1)$  of order 2 and 3, respectively, and have no other pole, so that, by the above, there exist  $a, a', b, b', b'' \in K_i$  such that

$$f^*(\xi') = a\xi + a', \quad f^*(\eta') = b\eta + b'\xi + b''.$$

Evidently  $ab \neq 0$ , and because  $\mathfrak{F}_K(W)$  and  $K_i$  are linearly disjoint over  $K$ , we have  $a, a', b, b', b'' \in K$ . Because  $\eta'^2 = 4\xi'^3 - g_2'\xi' - g_3'$ , we have

$$(b\eta + b'\xi + b'')^2 = 4(a\xi + a')^3 - g_2'(a\xi + a') - g_3',$$

and because  $\eta^2 = 4\xi^3 - g_2\xi - g_3$ , we infer that  $a' = b' = b'' = 0$ ,  $a^3 = b^2$ ,  $g_2'a = g_2b^2$ , and  $g_3' = b^2g_3$ . Setting  $c = b/a$ , we conclude that  $a = c^2$ ,

$b = c^3$ ,  $g_2' = g_2c^4$ ,  $g_3' = g_3c^6$ , and  $j = j'$ . Conversely, if  $j = j' \neq 0$ ,  $64 \cdot 27$  (so that  $g_2g_3g_2'g_3' \neq 0$ ) and  $g_3'/g_3 = b^2$  with  $b \in K$ , set  $a = g_2g_3'/g_2'g_3$  and  $c = b/a$ . If  $j = j' = 0$  (so that  $g_2 = g_2' = 0$  and  $g_3g_3' \neq 0$ ) and  $g_3'/g_3 = b^2 = a^3$  with  $a, b \in K$ , set  $c = b/a$ . If  $j = j' = 64 \cdot 27$  (so that  $g_3 = g_3' = 0$  and  $g_2g_2' \neq 0$ ) and  $g_2'/g_2 = c^4$  with  $c \in K$ , set  $a = c^2$  and  $b = c^3$ . In all three cases then  $g_2' = g_2c^4$  and  $g_3' = g_3c^6$ , and the formula  $(1:x:y) \mapsto (1:c^2x:c^3y)$  defines a  $K$ -isomorphism  $W \approx W'$ . Thus, our claim is established.

The existence of a nontrivial  $K$ -homomorphism  $f: W \rightarrow W'$  is more difficult to ascertain than that of a  $K$ -isomorphism. For such an  $f$ , and for any extension  $K'$  of  $K$ ,  $\mathfrak{F}_{K'}(W)$  is an extension of  $f^*(\mathfrak{F}_K(W))$  of finite degree, and this degree is independent of  $K'$ . Hence it may be called the *degree of  $f$*  and denoted by  $\text{deg } f$ . The degree is 1 if and only if  $f$  is a  $K$ -isomorphism.

Henceforth let  $K$  be algebraically closed.

For each nonzero  $n \in \mathbb{N}$ , there exists a polynomial  $F_n(X, Y)$ , with coefficients in  $\mathbb{Z}$  when  $p = 0$  and in the prime field when  $p \neq 0$ , such that  $F_n(j, j') = 0$  if and only if there exists a nontrivial  $K$ -homomorphism  $W \rightarrow W'$  of degree  $n$ . (When  $U = \mathbb{C}$  this is a classical result in the theory of elliptic functions; see Weber [28]. For the general result, see Deuring [12].) The polynomials  $F_n$  have the following properties:

$$\begin{aligned} F_1(X, Y) &= X - Y; \\ F_n(Y, X) &= F_n(X, Y) \quad (n \geq 2); \\ F_n(X, Y) &\text{ is unitary as a polynomial in } X \text{ (all } n); \\ F_n(X, X) &\text{ is unitary (all } n \text{ not a square in } \mathbb{N}). \end{aligned}$$

In particular, the condition that there exist a  $K$ -homomorphism  $W \rightarrow W'$  is symmetric in  $W$  and  $W'$ .

Now consider the set  $\text{End}_K(W)$  of  $K$ -endomorphisms of  $W = W(g_2, g_3)$ . Because  $W$  is commutative,  $\text{End}_K(W)$  has a natural ring structure. For any  $n \in \mathbb{Z}$  the formula  $z \mapsto z^n$  defines a  $K$ -endomorphism of  $W$ , and by identifying  $n$  with it we obtain an identification of  $\mathbb{Z}$  with a subring of  $\text{End}_K(W)$ . Any element of  $\text{End}_K(W)$  that is not in  $\mathbb{Z}$  is called a *complex multiplication* of  $W$ . "In general,"  $W$  has no complex multiplication. More precisely, when  $p = 0$ , then  $W$  has complex multiplication if and only if  $F_n(j, j) = 0$  for some  $n \in \mathbb{N}$  that is not a square (in which case  $j$  is an algebraic integer), and when  $p \neq 0$ , then  $W$  has complex multiplication if and only if  $j$  is algebraic over the prime field. (For  $p = 0$ , this is classical; see Weber [28]. For  $p \neq 0$ , see Deuring [12].)

We close this section (and chapter!) with some descriptive remarks about Abelian  $K$ -groups in the classical case in which  $U = \mathbb{C}$ . (In this case every algebraic group has a natural structure of complex analytic manifold.)

These generalize some remarks about the  $K$ -groups  $W(g_2, g_3)$  made in Section I. Proofs can be found in Mumford [23].

Let  $n \in \mathbf{N}$ ,  $n \neq 0$ . A lattice in  $\mathbf{C}^n$  is a subgroup of  $\mathbf{C}^n$  that is generated by a basis of the vector space  $\mathbf{C}^n$  over  $\mathbf{R}$ . Let  $\Lambda$  be a lattice in  $\mathbf{C}^n$ . An Abelian function for  $\Lambda$  is a meromorphic function on  $\mathbf{C}^n$  of which every element of  $\Lambda$  is a period. (Thus, when  $n = 1$ , the notion of Abelian function reduces to that of elliptic function.) The set  $\mathcal{A} = \mathcal{A}(\Lambda)$ , consisting of all the Abelian functions for  $\Lambda$ , is a field, and even a differential field, relative to the set of derivation operators  $\partial/\partial z_1, \dots, \partial/\partial z_n$ , where  $z = (z_1, \dots, z_n)$  denotes the canonical system of coordinate functions on  $\mathbf{C}^n$ . The Abelian function field  $\mathcal{A}$  is degenerate if, by means of some invertible  $\mathbf{C}$ -linear transformation on  $\mathbf{C}^n$ , the elements of  $\mathcal{A}$  can be expressed as meromorphic functions of fewer than  $n$  variables, that is, if there exist complex numbers  $c_1, \dots, c_n$  not all 0 such that  $\sum c_j \partial\varphi/\partial z_j = 0$  ( $\varphi \in \mathcal{A}$ ). A necessary and sufficient condition that  $\mathcal{A}$  be nondegenerate is that there exist a positive definite Hermitian form  $H$  on  $\mathbf{C}^n$  such that the imaginary part of  $H(z, z')$  is in  $\mathbf{Z}$  for every  $(z, z') \in \Lambda \times \Lambda$ . When  $\mathcal{A}$  is nondegenerate, there exist an Abelian variety (that is, an Abelian  $K'$ -group for some finitely generated field  $K' \subset \mathbf{C}$ ), say  $A$ , of dimension  $n$ , and a surjective holomorphic group homomorphism  $P: \mathbf{C}^n \rightarrow A$  with kernel  $\Lambda$ , such that the formula  $\varphi \mapsto \varphi \circ P$  defines an isomorphism of fields  $\mathfrak{F}(A) \approx \mathcal{A}$  ( $\varphi \circ P$  denoting the meromorphic function on  $\mathbf{C}^n$  that is holomorphic and has value  $\varphi(P(c))$  at every point  $c \in \mathbf{C}^n$  with  $\varphi \in \mathfrak{F}_{P(c)}(A)$ ). Conversely, if  $A$  is any Abelian variety of dimension  $n$ , then there exist a lattice  $\Lambda$  in  $\mathbf{C}^n$  with nondegenerate Abelian function field and a surjective holomorphic homomorphism  $\mathbf{C}^n \rightarrow A$  with kernel  $\Lambda$ , exactly as above.

When  $n = 1$ , then every lattice has nondegenerate Abelian (= elliptic) function field. This follows from the fact that we can always construct a nonconstant meromorphic function having as periods two generators  $\omega = \alpha + \beta i$  and  $\omega' = \alpha' + \beta' i$  of the lattice, for example, the corresponding Weierstrass function  $\wp$ . It follows also from the fact that the formula

$$H(z, z') = |\beta\alpha' - \alpha\beta'|^{-1} z\bar{z}'$$

defines a positive definite Hermitian form on  $\mathbf{C}$  such that the imaginary part of  $H(z, z')$  is in  $\mathbf{Z}$  whenever  $z$  and  $z'$  are in the lattice.

When  $n > 1$ , there exist lattices for which the Abelian function fields are degenerate.

## Bibliography for Chapter V

1. R. Baer. Endlichkeitskriterien für Kommutatorgruppen, *Math. Ann.* **124** (1952), 161–177.
2. A. Borel. Groupes linéaires algébriques, *Ann. of Math.* **64** (1956), 20–82.
3. A. Borel. "Linear Algebraic Groups." Benjamin, New York, 1969.
4. N. Bourbaki. "Théorie des Ensembles," Chapter 3. Hermann, Paris, 1956.
5. N. Bourbaki. "Algèbre," Chapters 4 and 5. Hermann, Paris, 1950 or 1959.
6. N. Bourbaki. "Algèbre," Chapter 8. Hermann, Paris, 1958.
7. F. Châtelet. Méthodes Galoisiennes et courbes de genre 1, *Ann. Univ. Lyon Sect. A* **89** (1946), 40–49.
8. C. Chevalley. "Introduction to the Theory of Algebraic Functions of One Variable." Amer. Math. Soc., New York, 1951.
9. C. Chevalley. "Théorie des Groupes de Lie," Vol. II, "Groupes Algébriques." Hermann, Paris, 1951.
10. C. Chevalley. "Classification des Groupes de Lie Algébriques" (Séminaire E.N.S., 1956–1958). Secrétariat Mathématique, Paris, 1958.
11. C. Chevalley and E. R. Kolchin. Two proofs of a theorem on algebraic groups, *Proc. Amer. Math. Soc.* **2** (1951), 126–134.
12. M. Deuring. Die Type der Multiplikatorenringe elliptischer Funktionenkörper, *Abh. Math. Sem. Hansischen Univ.* **14** (1941), 197–272.
13. J. Dieudonné. "La Géométrie des Groupes Classiques" (Ergebnisse der Math., neue Folge, **5**). Springer-Verlag, Berlin, 1955.
14. K. Iwasawa and T. Tamagawa. On the group of automorphisms of a function field, *J. Math. Soc. Japan* **3** (1951), 137–147; and two corrections, *J. Math. Soc. Japan* **4** (1952), 100–101, 203–204.
15. E. R. Kolchin. Algebraic matrix groups and the Picard-Vessiot theory of homogeneous linear ordinary differential equations, *Ann. of Math.* **49** (1948), 1–42.

16. E. R. Kolchin. On certain concepts in the theory of algebraic groups, *Ann. of Math.* **49** (1948), 774–789.
17. E. R. Kolchin. The birational automorphisms of  $SL(n)$  and its quotients, Dept. of Math. Report. Columbia Univ., New York, 1967.
18. E. R. Kolchin. Algebraic groups and algebraic dependence, *Amer. J. Math.* **90** (1968), 1151–1164.
19. E. R. Kolchin and S. Lang. Existence of invariant bases, *Proc. Amer. Math. Soc.* **11** (1960), 140–148.
20. S. Lang. Algebraic groups over finite fields, *Amer. J. Math.* **78** (1956), 555–563.
21. S. Lang. “Abelian Varieties.” Interscience, New York, 1959.
22. S. Lang. “Algebra.” Addison-Wesley, Reading, Massachusetts, 1965.
23. D. Mumford, “Abelian Varieties,” (Tata Inst. Fund. Res., Studies in Math., Vol. 5.) Oxford Univ. Press, London, 1970.
24. M. Rosenlicht. Some basic theorems on algebraic groups, *Amer. J. Math.* **78** (1956), 401–443.
25. M. Rosenlicht. A note on derivations and differentials on algebraic varieties, *Portugal. Math.* **16** (1957), 43–55.
26. J.-P. Serre. “Groups Algébriques et Corps de Classe.” Hermann, Paris, 1959.
27. A. Weil. “Variétés Abéliennes et Courbes Algébriques.” Hermann, Paris, 1948.
28. H. Weber. “Lehrbuch der Algebra,” Vol. III. Vieweg und Sohn, Braunschweig, 1908.

## CHAPTER VI

## Galois Theory of Differential Fields

Throughout this chapter  $\mathcal{U}$  denotes a fixed universal differential field of characteristic 0 with field of constants  $\mathcal{K}$ . The set of derivation operators of  $\mathcal{U}$ , the set of derivative operators of  $\mathcal{U}$ , and the set of derivative operators of  $\mathcal{U}$  of order less than or equal to  $s$  are denoted by  $\Delta$ ,  $\Theta$ , and  $\Theta(s)$ , respectively; the elements of  $\Delta$  are denoted by  $\delta_1, \dots, \delta_m$ . Every differential field considered is tacitly assumed to be a differential subfield of  $\mathcal{U}$ .  $\mathcal{F}$  and  $\mathcal{G}$  always denote differential fields over which  $\mathcal{U}$  is universal.

## 1 Specializations of isomorphisms

By an *isomorphism of  $\mathcal{G}$*  we mean an isomorphism of  $\mathcal{G}$  onto a differential field.

**Lemma 1** Let  $(\sigma_i)_{i \in I}$  and  $(\sigma'_i)_{i \in I}$  be two families of isomorphisms of  $\mathcal{G}$ , both having the same set of indices  $I$ . The following three conditions are equivalent:

- (a)  $(\sigma'_i \alpha)_{i \in I, \alpha \in \mathcal{G}}$  is a differential specialization of  $(\sigma_i \alpha)_{i \in I, \alpha \in \mathcal{G}}$  over  $\mathcal{G}$ .
- (b)  $(\sigma'_i \alpha)_{i \in I, \alpha \in \mathcal{G}}$  is a specialization of  $(\sigma_i \alpha)_{i \in I, \alpha \in \mathcal{G}}$  over  $\mathcal{G}$ .
- (c) The isomorphisms  $\sigma'_i \circ \sigma_i^{-1} : \sigma_i \mathcal{G} \approx \sigma'_i \mathcal{G}$  ( $i \in I$ ) and  $id_{\mathcal{G}}$  are compatible.

*Proof* It is obvious that (a) implies (b), and that (b) implies the existence of a ring homomorphism  $\mathcal{G}[\bigcup_{i \in I} \sigma_i \mathcal{G}] \rightarrow \mathcal{G}[\bigcup_{i \in I} \sigma'_i \mathcal{G}]$  extending  $id_{\mathcal{G}}$  and every  $\sigma'_i \circ \sigma_i^{-1}$ , that is, (c). However,  $\mathcal{G}[\bigcup_{i \in I} \sigma_i \mathcal{G}]$  and  $\mathcal{G}[\bigcup_{i \in I} \sigma'_i \mathcal{G}]$  are

obviously differential rings, and a ring homomorphism between them that extends  $id_{\mathcal{G}}$  and every  $\sigma'_i \circ \sigma_i^{-1}$  is obviously a homomorphism of differential rings. Therefore (c) implies (a).

When  $(\sigma_i)_{i \in I}$  and  $(\sigma'_i)_{i \in I}$  satisfy the conditions in Lemma 1, we say that  $(\sigma'_i)_{i \in I}$  is a *specialization* of  $(\sigma_i)_{i \in I}$ . The relation “ $(\sigma'_i)_{i \in I}$  is a specialization of  $(\sigma_i)_{i \in I}$ ” is a pre-order, being reflexive and transitive.

When  $(\sigma'_i)_{i \in I}$  is a specialization of  $(\sigma_i)_{i \in I}$  such that  $(\sigma_i)_{i \in I}$  is a specialization of  $(\sigma'_i)_{i \in I}$ , we say that  $(\sigma'_i)_{i \in I}$  is a *generic specialization* of  $(\sigma_i)_{i \in I}$ . It is equivalent to say that the isomorphisms  $\sigma'_i \circ \sigma_i^{-1}$  ( $i \in I$ ) and  $id_{\mathcal{G}}$  are bi-compatible.

If  $(\sigma'_i)_{i \in I}$  is a specialization of  $(\sigma_i)_{i \in I}$ , then, for every subset  $J$  of  $I$ ,  $(\sigma'_i)_{i \in J}$  is a specialization of  $(\sigma_i)_{i \in J}$ . Conversely, if the latter condition is satisfied for every *finite* subset  $J$  of  $I$ , then the former condition is satisfied.

A single isomorphism may be regarded as a family for which the set of indices reduces to a single element. Therefore the above definition contains as a special case a definition of specialization of an isomorphism of  $\mathcal{G}$ . Let  $\sigma'$  be a specialization of the isomorphism  $\sigma$  of  $\mathcal{G}$ . For any element  $\alpha \in \mathcal{G}$  with  $\sigma\alpha \in \mathcal{F}$ , it is evident that  $\sigma'\alpha = \sigma\alpha$ . It follows, for a differential subfield  $\mathcal{F}'$  of  $\mathcal{G}$ , that if  $\sigma$  is an isomorphism of  $\mathcal{G}$  over  $\mathcal{F}'$ , then so is  $\sigma'$ . Also, if  $\sigma$  is an automorphism of  $\mathcal{G}$ , then  $\sigma' = \sigma$ .

For isomorphisms of an extension, the definition of specialization can be put in terms of generators.

**Lemma 2** *Let  $\mathcal{G}$  be an extension of  $\mathcal{F}$ , let  $\eta = (\eta_j)_{j \in J}$  be a family of elements of  $\mathcal{G}$  such that  $\mathcal{F}\langle\eta\rangle = \mathcal{G}$  (respectively  $\mathcal{F}(\eta) = \mathcal{G}$ ), and let  $(\sigma_i)_{i \in I}$  and  $(\sigma'_i)_{i \in I}$  be two families of isomorphisms of  $\mathcal{G}$  over  $\mathcal{F}$ . A necessary and sufficient condition that  $(\sigma'_i)_{i \in I}$  be a specialization of  $(\sigma_i)_{i \in I}$  is that  $(\sigma'_i \eta_j)_{i \in I, j \in J}$  be a differential specialization (respectively a specialization) of  $(\sigma_i \eta_j)_{i \in I, j \in J}$  over  $\mathcal{G}$ .*

This is apparent.

An isomorphism of  $\mathcal{G}$  over  $\mathcal{F}$  is said to be *isolated* (over  $\mathcal{F}$ ) if there does not exist an isomorphism of  $\mathcal{G}$  over  $\mathcal{F}$  of which it is a nongeneric specialization.

**Proposition 1** *Let  $\mathcal{G}$  be a finitely generated extension of  $\mathcal{F}$ , and let  $\eta = (\eta_1, \dots, \eta_n)$  be any finite family of elements of  $\mathcal{G}$  with  $\mathcal{F}\langle\eta\rangle = \mathcal{G}$ .*

(a) *If  $\sigma$  is an isomorphism of  $\mathcal{G}$  over  $\mathcal{F}$ , then  $\omega_{\sigma\eta/\mathcal{G}} \leq \omega_{\eta/\mathcal{F}}$ , and  $\sigma$  is isolated if and only if  $\omega_{\sigma\eta/\mathcal{G}} = \omega_{\eta/\mathcal{F}}$ .*

(b) *If  $\sigma'$  is a specialization of an isomorphism  $\sigma$  of  $\mathcal{G}$  over  $\mathcal{F}$ , then  $\omega_{\sigma'\eta/\mathcal{G}} \leq \omega_{\sigma\eta/\mathcal{G}}$ , and the specialization is generic if and only if  $\omega_{\sigma'\eta/\mathcal{G}} = \omega_{\sigma\eta/\mathcal{G}}$ .*

(c) *There exist finitely many isolated isomorphisms  $\sigma_1, \dots, \sigma_r$  of  $\mathcal{G}$  over  $\mathcal{F}$  such that every isomorphism of  $\mathcal{G}$  over  $\mathcal{F}$  is a specialization of one and only one of these. If  $\mathcal{G}$  is regular over  $\mathcal{F}$ , then  $r = 1$ .*

*Proof* For each isomorphism  $\sigma$  of  $\mathcal{G}$  over  $\mathcal{F}$  let  $\mathfrak{p}_\sigma$  denote the defining differential ideal in  $\mathcal{G}\{y_1, \dots, y_n\}$  of  $(\sigma\eta_1, \dots, \sigma\eta_n)$ ; then  $\omega_{\sigma\eta/\mathcal{G}} = \omega_{\mathfrak{p}_\sigma}$ . If  $\sigma'$  is a specialization of  $\sigma$ , then  $\mathfrak{p}_{\sigma'} \supset \mathfrak{p}_\sigma$ , and by Lemma 2, the specialization is generic if and only if  $\mathfrak{p}_{\sigma'} = \mathfrak{p}_\sigma$ . By Chapter III, Section 5, Proposition 2, this means that  $\omega_{\sigma'\eta/\mathcal{G}} \leq \omega_{\sigma\eta/\mathcal{G}}$ , and that the specialization is generic if and only if equality holds here. This proves part (b).

Now let  $\mathfrak{p}$  denote the defining differential ideal of  $(\eta_1, \dots, \eta_n)$  in  $\mathcal{F}\{y_1, \dots, y_n\}$ ; then  $\omega_{\eta/\mathcal{F}} = \omega_{\mathfrak{p}}$ . By Chapter III, Section 6, Proposition 3,  $\mathcal{G}\mathfrak{p}$  is a perfect differential ideal of  $\mathcal{G}\{y_1, \dots, y_n\}$  with finitely many components  $\mathfrak{p}_1, \dots, \mathfrak{p}_r$  ( $r$  being 1 if  $\mathcal{G}$  is regular over  $\mathcal{F}$ ),  $\omega_{\mathfrak{p}_k} = \omega_{\mathfrak{p}}$  for each  $k$ , every generic zero of  $\mathfrak{p}_k$  is a generic zero of  $\mathfrak{p}$ , and every generic zero of  $\mathfrak{p}$  is a zero of a unique  $\mathfrak{p}_k$ . Let  $\eta^{(k)} = (\eta_{k1}, \dots, \eta_{kn})$  be a generic zero of  $\mathfrak{p}_k$ . By the above, there exists an isomorphism  $\sigma_k: \mathcal{F}\langle\eta\rangle \approx \mathcal{F}\langle\eta^{(k)}\rangle$  over  $\mathcal{F}$  with  $\sigma_k \eta_j = \eta_{kj}$  ( $1 \leq j \leq n$ ). Thus,  $\sigma_k$  is an isomorphism of  $\mathcal{G}$  over  $\mathcal{F}$ ,  $\sigma_k \eta$  is a generic zero of  $\mathfrak{p}_k$ , and  $\omega_{\sigma_k \eta/\mathcal{G}} = \omega_{\eta/\mathcal{F}}$ . If  $\sigma$  is any isomorphism of  $\mathcal{G}$  over  $\mathcal{F}$ , then  $\sigma\eta$  is a generic zero of  $\mathfrak{p}$  and hence is a zero of a unique  $\mathfrak{p}_k$ . Then by Lemma 2,  $\sigma$  is a specialization of a unique  $\sigma_k$ . It follows that each  $\sigma_k$  is isolated, that  $\omega_{\sigma\eta/\mathcal{G}} \leq \omega_{\eta/\mathcal{F}}$ , and that  $\sigma$  is isolated if and only if  $\omega_{\sigma\eta/\mathcal{G}} = \omega_{\eta/\mathcal{F}}$ . This completes the proof.

We observe that for an isomorphism  $\sigma$  of  $\mathcal{G}$  over  $\mathcal{F}$  we have  $\omega_{\sigma\eta/\mathcal{G}} = \omega_{\eta/\mathcal{F}}$ . Therefore the condition  $\omega_{\sigma\eta/\mathcal{G}} = \omega_{\eta/\mathcal{F}}$  is equivalent to the condition that, for big values of  $s \in \mathbb{N}$ , any of the elements  $\sigma\theta\eta_j$  ( $\theta \in \Theta(s)$ ,  $1 \leq j \leq n$ ) that are algebraically independent over  $\mathcal{F}$  are algebraically independent over  $\mathcal{G}$ . Thus, an isomorphism  $\sigma$  of  $\mathcal{G}$  over  $\mathcal{F}$  is isolated if and only if  $\mathcal{G}$  and  $\sigma\mathcal{G}$  are algebraically disjoint over  $\mathcal{F}$ .

**Corollary** *Let  $\mathcal{G}$  be a finitely generated extension of  $\mathcal{F}$  of finite transcendence degree, and let  $\sigma$  be an isomorphism of  $\mathcal{G}$  over  $\mathcal{F}$ .*

(a)  *$\text{tr deg } \mathcal{G}\sigma\mathcal{G}/\mathcal{G} \leq \text{tr deg } \mathcal{G}/\mathcal{F}$ , and  $\sigma$  is isolated if and only if equality holds.*

(b) *If  $\sigma'$  is a specialization of  $\sigma$ , then  $\text{tr deg } \mathcal{G}\sigma'\mathcal{G}/\mathcal{G} \leq \text{tr deg } \mathcal{G}\sigma\mathcal{G}/\mathcal{G}$ , and the specialization is generic if and only if equality holds.*

*Proof* If  $\mathcal{L}$  is any differential field and  $\zeta$  is a finite family of elements of  $\mathcal{U}$  such that  $\mathcal{L}\langle\zeta\rangle$  is of finite transcendence degree over  $\mathcal{L}$ , then  $\omega_{\zeta/\mathcal{L}} = \text{tr deg } \mathcal{L}\langle\zeta\rangle/\mathcal{L}$ . Therefore in the present case, parts (a) and (b) of the proposition reduce to parts (a) and (b) of the corollary.

**Proposition 2** Let  $\mathcal{G}$  be a finitely generated extension of  $\mathcal{F}$ , and let  $\mathcal{F}^\circ$  denote the algebraic closure of  $\mathcal{F}$  in  $\mathcal{G}$ . Let  $\sigma$  and  $\sigma'$  be isomorphisms of  $\mathcal{G}$  over  $\mathcal{F}$  such that  $\sigma$  is isolated and  $\sigma'\mathcal{F}^\circ \subset \mathcal{G}$  (whence  $\sigma'\mathcal{F}^\circ = \mathcal{F}^\circ$ ).

- (a)  $\mathcal{G} \cap \sigma\mathcal{G} = \mathcal{F}^\circ \cap \sigma\mathcal{F}^\circ$ .
- (b)  $\sigma'$  is a specialization of  $\sigma$  if and only if  $\sigma$  and  $\sigma'$  coincide on  $\mathcal{F}^\circ$ . When this is the case, then  $\mathcal{G}$  and  $\sigma\mathcal{G}$  are linearly disjoint over  $\mathcal{F}^\circ$ .

*Proof* (a) Since  $\sigma$  is isolated,  $\mathcal{G}$  and  $\sigma\mathcal{G}$  are algebraically disjoint over  $\mathcal{F}$ , so that  $\mathcal{G} \cap \sigma\mathcal{G} \subset \mathcal{F}^\circ$ . Similarly,  $\mathcal{G} \cap \sigma\mathcal{G} \subset \sigma\mathcal{F}^\circ$ . Therefore  $\mathcal{G} \cap \sigma\mathcal{G} = \mathcal{F}^\circ \cap \sigma\mathcal{F}^\circ$ .

(b) Let  $\sigma'$  be a specialization of  $\sigma$ . Then there exists a surjective homomorphism  $\mathcal{G}\{\sigma\mathcal{F}^\circ\} \rightarrow \mathcal{G}\{\sigma'\mathcal{F}^\circ\}$  over  $\mathcal{G}$ . Each element of the differential field  $\sigma\mathcal{F}^\circ$  is algebraic over  $\mathcal{G}$ , so that  $\mathcal{G}\{\sigma\mathcal{F}^\circ\} = \mathcal{G}\sigma\mathcal{F}^\circ$ ; also,  $\mathcal{G}\{\sigma'\mathcal{F}^\circ\} = \mathcal{G}$ . Therefore our homomorphism is actually an isomorphism  $\mathcal{G}\sigma\mathcal{F}^\circ \approx \mathcal{G}$  over  $\mathcal{G}$ , so that  $\sigma\mathcal{F}^\circ \subset \mathcal{G}$ . It follows that  $\sigma'x = \sigma x$  for every  $x \in \mathcal{F}^\circ$ , so that  $\sigma$  and  $\sigma'$  coincide on  $\mathcal{F}^\circ$ . Conversely, let them coincide on  $\mathcal{F}^\circ$ . Then  $\sigma\mathcal{F}^\circ = \sigma'\mathcal{F}^\circ = \mathcal{F}^\circ$  and  $\sigma' \circ \sigma^{-1} : \sigma\mathcal{G} \approx \sigma'\mathcal{G}$  is an isomorphism over  $\mathcal{F}^\circ$ . However,  $\mathcal{G}$  and  $\sigma\mathcal{G}$  are algebraically disjoint over  $\mathcal{F}$  and hence over  $\mathcal{F}^\circ$ , and  $\mathcal{G}$  is regular over  $\mathcal{F}^\circ$ , so that  $\mathcal{G}$  and  $\sigma\mathcal{G}$  are linearly disjoint over  $\mathcal{F}^\circ$ . Therefore  $\sigma' \circ \sigma^{-1}$  can be extended to a homomorphism  $\mathcal{G}[\sigma\mathcal{G}] \rightarrow \mathcal{G}[\sigma'\mathcal{G}]$  over  $\mathcal{G}$ , so that  $\sigma'$  is a specialization of  $\sigma$ .

**Corollary** Let  $\mathcal{G}$  be a finitely generated extension of  $\mathcal{F}$ , and let  $\mathcal{F}^\circ$  denote the algebraic closure of  $\mathcal{F}$  in  $\mathcal{G}$ .

- (a) If  $\sigma_1, \dots, \sigma_r$  are isolated isomorphisms of  $\mathcal{G}$  over  $\mathcal{F}$  having the property described in Proposition 1(c), then the differential field of invariants of  $\sigma_1, \dots, \sigma_r$  is  $\mathcal{F}$ .
- (b) If  $\sigma$  is an isolated isomorphism of  $\mathcal{G}$  over  $\mathcal{F}$  of which  $\text{id}_{\mathcal{G}}$  is a specialization, then the differential field of invariants of  $\sigma$  is  $\mathcal{F}^\circ$ , and an isomorphism  $\sigma'$  of  $\mathcal{G}$  is a specialization of  $\sigma$  if and only if  $\sigma'$  leaves invariant every element of  $\mathcal{F}^\circ$ .

*Proof* (a) Let  $\alpha \in \mathcal{G}$ ,  $\sigma_k \alpha = \alpha$  ( $1 \leq k \leq r$ ). By Proposition 2(a),  $\alpha \in \mathcal{F}^\circ$ . Moreover, every isomorphism of  $\mathcal{G}$  over  $\mathcal{F}$  leaves  $\alpha$  invariant. Since every isomorphism  $\gamma$  of  $\mathcal{F}^\circ$  over  $\mathcal{F}$  can be extended to an isomorphism of  $\mathcal{G}$ , every such  $\gamma$  leaves  $\alpha$  invariant. Hence  $\alpha \in \mathcal{F}$ .

(b) This is an immediate consequence of Proposition 2(b).

**2 Strong isomorphisms**

Let  $\mathcal{C}$  denote the field of constants of the differential field  $\mathcal{G}$ . An isomorphism  $\sigma$  of  $\mathcal{G}$  is said to be *strong* if it satisfies the following two conditions.

**St1**  $\sigma$  leaves invariant every element of  $\mathcal{C}$ .

**St2**  $\sigma\mathcal{G} \subset \mathcal{G}\mathcal{K}$  and  $\mathcal{G} \subset \sigma\mathcal{G} \cdot \mathcal{K}$ .

Of course, the two parts of St2 can be written as the single condition  $\mathcal{G}\mathcal{K} = \sigma\mathcal{G} \cdot \mathcal{K}$ . It is obvious that every automorphism of  $\mathcal{G}$  over  $\mathcal{C}$  is a strong isomorphism.

**REMARK** This notion of strong isomorphisms can be of interest only when (as in the present chapter) the field characteristic  $p$  is 0. Indeed, when  $p \neq 0$ , then St1 and the fact that  $\mathcal{G}^p \subset \mathcal{C}$  imply that the only strong isomorphism of  $\mathcal{G}$  is the identity.

For any isomorphism  $\sigma$  of  $\mathcal{G}$ , let  $\mathcal{C}(\sigma)$  denote the field of constants of  $\mathcal{G}\sigma\mathcal{G}$ . The first inclusion in St2 is equivalent to the inclusion  $\mathcal{G}\sigma\mathcal{G} \subset \mathcal{G}\mathcal{K}$  which, by Chapter II, Section 1, Corollary 2 to Theorem 1, is equivalent to the condition  $\mathcal{G}\sigma\mathcal{G} = \mathcal{G}\mathcal{C}(\sigma)$ . Similarly, the second inclusion in St2 is equivalent to the condition  $\mathcal{G}\sigma\mathcal{G} = \sigma\mathcal{G} \cdot \mathcal{C}(\sigma)$ . Therefore the isomorphism  $\sigma$  of  $\mathcal{G}$  over  $\mathcal{C}$  is strong if and only if

$$\mathcal{G}\mathcal{C}(\sigma) = \mathcal{G}\sigma\mathcal{G} = \sigma\mathcal{G} \cdot \mathcal{C}(\sigma).$$

**Proposition 3** If  $\sigma$  is a strong isomorphism of  $\mathcal{G}$ , then

$$\text{tr deg } \mathcal{G}\sigma\mathcal{G} / \mathcal{G} = \text{tr deg } \mathcal{C}(\sigma) / \mathcal{C}.$$

*Proof* Since  $\mathcal{G}\sigma\mathcal{G} = \mathcal{G}\mathcal{C}(\sigma)$ , this follows from the fact (Chapter II, Section 1, Corollary 1 to Theorem 1) that  $\mathcal{G}$  and  $\mathcal{C}(\sigma)$  are linearly disjoint over  $\mathcal{C}$ .

The utility of strong isomorphisms rests on the following result.

**Proposition 4** Each strong isomorphism of  $\mathcal{G}$  can be extended to a unique automorphism of  $\mathcal{G}\mathcal{K}$  over  $\mathcal{K}$ . Conversely, the restriction to  $\mathcal{G}$  of each automorphism of  $\mathcal{G}\mathcal{K}$  over  $\mathcal{K}$  is a strong isomorphism of  $\mathcal{G}$ .

*Proof* We know  $\mathcal{G}$  and  $\mathcal{K}$  are linearly disjoint over  $\mathcal{C}$ , as are  $\sigma\mathcal{G}$  and  $\mathcal{K}$  ( $\sigma$  denoting any isomorphism of  $\mathcal{G}$  over  $\mathcal{C}$ ). Therefore  $\sigma$  can be extended to a unique isomorphism  $s : \mathcal{G}\mathcal{K} \approx \sigma\mathcal{G} \cdot \mathcal{K}$  over  $\mathcal{K}$ . When  $\sigma$  is strong then  $\sigma\mathcal{G} \cdot \mathcal{K} = \mathcal{G}\mathcal{K}$ , and  $s$  is an automorphism of  $\mathcal{G}\mathcal{K}$ . The converse is obvious.

Proposition 4 provides a canonical identification of the set of all strong isomorphisms of  $\mathcal{G}$  with the set of all automorphisms of  $\mathcal{G}\mathcal{K}$  over  $\mathcal{K}$ . Since the latter set has a natural group structure, this identification makes the set



of all strong isomorphisms of  $\mathcal{G}$  a group. If  $\mathcal{F}$  is a differential subfield of  $\mathcal{G}$ , the set of all strong isomorphisms of  $\mathcal{G}$  over  $\mathcal{F}$  is a subgroup of this group, canonically identified with the group of all automorphisms of  $\mathcal{G}\mathcal{K}$  over  $\mathcal{F}\mathcal{K}$ .

**Proposition 5** *Let  $\sigma$  and  $\tau$  be strong isomorphisms of  $\mathcal{G}$ . Then  $\mathcal{C}(\sigma)\mathcal{C}(\sigma\tau) = \mathcal{C}(\sigma)\mathcal{C}(\tau) = \mathcal{C}(\sigma\tau)\mathcal{C}(\tau)$  and  $\mathcal{C}(\sigma^{-1}) = \mathcal{C}(\sigma)$ .*

*Proof*

$$\mathcal{G}\mathcal{C}(\sigma) = \mathcal{G}\sigma\mathcal{G} = \sigma(\sigma^{-1}\mathcal{G}\cdot\mathcal{G}) = \sigma(\sigma^{-1}\mathcal{G}\cdot\mathcal{C}(\sigma^{-1})) = \mathcal{G}\mathcal{C}(\sigma^{-1}),$$

whence (by Chapter II, Section 1, Corollary 2 to Theorem 1)  $\mathcal{C}(\sigma) = \mathcal{C}(\sigma^{-1})$ . Similarly,

$$\begin{aligned} \mathcal{G}\mathcal{C}(\sigma)\mathcal{C}(\sigma\tau) &= \mathcal{G}\sigma\mathcal{G}\cdot\sigma\tau\mathcal{G} = \mathcal{G}\sigma(\mathcal{G}\tau\mathcal{G}) \\ &= \mathcal{G}\sigma(\mathcal{G}\mathcal{C}(\tau)) = \mathcal{G}\sigma\mathcal{G}\cdot\mathcal{C}(\tau) = \mathcal{G}\mathcal{C}(\sigma)\mathcal{C}(\tau), \end{aligned}$$

whence  $\mathcal{C}(\sigma)\mathcal{C}(\sigma\tau) = \mathcal{C}(\sigma)\mathcal{C}(\tau)$ . Finally, replacing  $\sigma, \tau$  in this equation by  $\tau^{-1}, \sigma^{-1}$ , we find that  $\mathcal{C}(\tau^{-1})\mathcal{C}(\tau^{-1}\sigma^{-1}) = \mathcal{C}(\tau^{-1})\mathcal{C}(\sigma^{-1})$ , that is  $\mathcal{C}(\tau)\mathcal{C}(\sigma\tau) = \mathcal{C}(\sigma)\mathcal{C}(\tau)$ .

We now consider specializations of strong isomorphisms.

**Proposition 6** *Every specialization of a strong isomorphism of  $\mathcal{G}$  is strong.*

*Proof* Let  $\sigma'$  be a specialization of the strong isomorphism  $\sigma$  of  $\mathcal{G}$ , and let  $x \in \mathcal{G}$ . We must show that  $\sigma'x \in \mathcal{G}\mathcal{K}$  and  $x \in \sigma'\mathcal{G}\cdot\mathcal{K}$ . Fix a vector space basis  $(\beta_i)$  of  $\mathcal{G}$  over  $\mathcal{C}$ . Since  $\sigma x \in \mathcal{G}\mathcal{K}$ , there exist constants  $b_i$  not all 0 and constants  $a_i$  such that  $\sigma x = \sum a_i \beta_i / \sum b_i \beta_i$ , that is, such that  $\sum b_i \beta_i \sigma x - \sum a_i \beta_i = 0$ . Therefore the family  $((\beta_i \sigma x), (\beta_i))$  is linearly dependent over  $\mathcal{K}$ . Since this condition is equivalent to the vanishing at  $((\beta_i \sigma x), (\beta_i))$  of certain differential polynomials with coefficients in the prime field  $\mathbf{Q}$  (see Chapter II, Section 1, Theorem 1), we infer that the family  $((\beta_i \sigma'x), (\beta_i))$  is linearly dependent over  $\mathcal{K}$ , so that there exist constants  $a'_i$  and  $b'_i$  not all 0 with  $\sum b'_i \beta_i \sigma'x - \sum a'_i \beta_i = 0$ . However,  $(\beta_i)$  is linearly independent over constants, and therefore  $\sum b'_i \beta_i \neq 0$ . Hence  $\sigma'x = \sum a'_i \beta_i / \sum b'_i \beta_i \in \mathcal{G}\mathcal{K}$ . The proof that  $x \in \sigma'\mathcal{G}\cdot\mathcal{K}$  is similar.

**REMARK** We observe from the proof that if  $\sigma$  is an isomorphism of  $\mathcal{G}$  over  $\mathcal{C}$  satisfying the first (respectively second) inclusion in the condition St2, then every specialization of  $\sigma$  is an isomorphism of  $\mathcal{G}$  over  $\mathcal{C}$  satisfying the first (respectively second) inclusion.

If  $\sigma'$  is a generic specialization of the strong isomorphism  $\sigma$  of  $\mathcal{G}$ , then there exists a unique isomorphism  $\mathcal{G}\sigma'\mathcal{C} \approx \mathcal{G}\sigma'\mathcal{G}$  over  $\mathcal{G}$  that, for each

$x \in \mathcal{G}$ , maps  $\sigma x$  onto  $\sigma'x$ . This isomorphism yields on restriction an isomorphism  $\mathcal{C}(\sigma) \approx \mathcal{C}(\sigma')$  over  $\mathcal{C}$  which we call the isomorphism induced by the generic specialization.

**Proposition 7** *Let  $\sigma$  be a strong isomorphism of  $\mathcal{G}$ .*

- (a) *If  $\sigma'$  is a generic specialization of  $\sigma$ , and  $\sigma''$  is a generic specialization of  $\sigma'$  (and therefore of  $\sigma$ ), then the composite of the induced isomorphisms  $\mathcal{C}(\sigma) \approx \mathcal{C}(\sigma')$  and  $\mathcal{C}(\sigma') \approx \mathcal{C}(\sigma'')$  is the induced isomorphism  $\mathcal{C}(\sigma) \approx \mathcal{C}(\sigma'')$ .*
- (b) *If  $S: \mathcal{C}(\sigma) \approx \mathcal{C}'$  is any isomorphism over  $\mathcal{C}$ , then there exists a unique generic specialization  $\sigma'$  of  $\sigma$  such that  $\mathcal{C}(\sigma') = \mathcal{C}'$  and  $S$  is the induced isomorphism  $\mathcal{C}(\sigma) \approx \mathcal{C}(\sigma')$ .*

*Proof* (a) This follows from the corresponding facts about the isomorphisms  $\mathcal{G}\sigma\mathcal{G} \approx \mathcal{G}\sigma'\mathcal{G}$ ,  $\mathcal{G}\sigma'\mathcal{G} \approx \mathcal{G}\sigma''\mathcal{G}$ , and  $\mathcal{G}\sigma\mathcal{G} \approx \mathcal{G}\sigma''\mathcal{G}$ .

(b)  $\mathcal{C}(\sigma)$  and  $\mathcal{G}$  are linearly disjoint over  $\mathcal{C}$ , as are  $\mathcal{C}'$  and  $\mathcal{G}$ ; therefore  $S$  can be extended to an isomorphism  $T: \mathcal{G}\mathcal{C}(\sigma) \approx \mathcal{G}\mathcal{C}'$  over  $\mathcal{G}$ . The composite mapping  $\mathcal{G} \xrightarrow{\sigma} \sigma\mathcal{G} \subset \mathcal{G}\mathcal{C}(\sigma) \xrightarrow{T} \mathcal{G}\mathcal{C}'$  yields an isomorphism  $\sigma': \mathcal{G} \approx T\sigma\mathcal{G}$  over  $\mathcal{C}$ . Evidently  $T: \mathcal{G}\sigma\mathcal{G} \approx \mathcal{G}\sigma'\mathcal{G}$ , so that  $\sigma'$  is a generic specialization of  $\sigma$ ,  $\mathcal{C}' = \mathcal{C}(\sigma')$ , and  $S$  is the induced isomorphism. The uniqueness is clear.

**Proposition 8** *Let  $\sigma, \sigma', \tau, \tau'$  be strong isomorphisms of  $\mathcal{G}$ .*

- (a) *If  $(\sigma', \tau')$  is a specialization of  $(\sigma, \tau)$ , then  $(\sigma'^{-1}, \sigma'^{-1}\tau')$  is a specialization of  $(\sigma^{-1}, \sigma^{-1}\tau)$ .*
- (b) *Suppose that  $\sigma'$  and  $\tau'$  are generic specializations of  $\sigma$  and  $\tau$ , respectively. If  $(\sigma', \tau')$  is a specialization of  $(\sigma, \tau)$ , then the induced isomorphisms  $\mathcal{C}(\sigma) \approx \mathcal{C}(\sigma')$  and  $\mathcal{C}(\tau) \approx \mathcal{C}(\tau')$  are compatible, and conversely.*
- (c) *Suppose that  $\sigma'$  and  $\tau'$  are generic specializations of  $\sigma$  and  $\tau$ , respectively, and let  $h: \mathcal{D} \rightarrow \mathcal{D}'$  be a homomorphism between subrings of  $\mathcal{K}$ . If  $h$  and the induced isomorphisms  $\mathcal{C}(\sigma) \approx \mathcal{C}(\sigma')$  and  $\mathcal{C}(\tau) \approx \mathcal{C}(\tau')$  are compatible, then  $\sigma'^{-1}$  is a generic specialization of  $\sigma^{-1}$  and  $\sigma'^{-1}\tau'$  is a specialization of  $\sigma^{-1}\tau$ ; when the latter specialization is generic, then  $h$  and the induced isomorphisms  $\mathcal{C}(\sigma^{-1}) \approx \mathcal{C}(\sigma'^{-1})$  and  $\mathcal{C}(\sigma^{-1}\tau) \approx \mathcal{C}(\sigma'^{-1}\tau')$  are compatible.*

*Proof* (a) By hypothesis there exists a homomorphism  $f: \mathcal{G}[\sigma\mathcal{G} \cup \tau\mathcal{G}] \rightarrow \mathcal{G}[\sigma'\mathcal{G} \cup \tau'\mathcal{G}]$  that, for each  $x \in \mathcal{G}$ , maps  $x$  onto  $x$ ,  $\sigma x$  onto  $\sigma'x$ , and  $\tau x$  onto  $\tau'x$ . The formula  $x \mapsto \sigma'^{-1}(f(\sigma x))$  defines a homomorphism

$$\mathcal{G}[\sigma^{-1}\mathcal{G} \cup \sigma^{-1}\tau\mathcal{G}] \rightarrow \mathcal{G}[\sigma'^{-1}\mathcal{G} \cup \sigma'^{-1}\tau'\mathcal{G}]$$

that, for each  $x \in \mathcal{G}$ , maps  $x$  onto  $x$ ,  $\sigma^{-1}x$  onto  $\sigma'^{-1}x$ , and  $\sigma^{-1}\tau x$  onto  $\sigma'^{-1}\tau'x$ .

(b) By hypothesis, the homomorphism  $f$  in the proof of part (a) maps  $\mathcal{G}[\sigma\mathcal{G}]$  and  $\mathcal{G}[\tau\mathcal{G}]$  isomorphically onto  $\mathcal{G}[\sigma'\mathcal{G}]$  and  $\mathcal{G}[\tau'\mathcal{G}]$ , and hence can be extended to a homomorphism  $\mathcal{G}[\mathcal{G}\sigma\mathcal{G} \cup \mathcal{G}\tau\mathcal{G}] \rightarrow \mathcal{G}[\mathcal{G}\sigma'\mathcal{G} \cup \mathcal{G}\tau'\mathcal{G}]$ . This homomorphism is an extension of the induced homomorphisms  $\mathcal{C}(\sigma) \approx \mathcal{C}(\sigma')$  and  $\mathcal{C}(\tau) \approx \mathcal{C}(\tau')$ , so that these are compatible. For the converse, see the proof of part (c).

(c) By hypothesis there exists a homomorphism  $\mathcal{C}[\mathcal{D} \cup \mathcal{C}(\sigma) \cup \mathcal{C}(\tau)] \rightarrow \mathcal{C}[\mathcal{D}' \cup \mathcal{C}(\sigma') \cup \mathcal{C}(\tau')]$  that extends  $h$  and the induced isomorphisms  $\mathcal{C}(\sigma) \approx \mathcal{C}(\sigma')$  and  $\mathcal{C}(\tau) \approx \mathcal{C}(\tau')$ . Because  $\mathcal{G}$  and  $\mathcal{X}$  are linearly disjoint over  $\mathcal{C}$ , this homomorphism can be extended to a homomorphism

$$\mathcal{G}[\mathcal{D} \cup \mathcal{C}(\sigma) \cup \mathcal{C}(\tau)] \rightarrow \mathcal{G}[\mathcal{D}' \cup \mathcal{C}(\sigma') \cup \mathcal{C}(\tau')]$$

over  $\mathcal{G}$ . This homomorphism maps  $\mathcal{G}[\mathcal{C}(\sigma)]$  and  $\mathcal{G}[\mathcal{C}(\tau)]$  isomorphically onto  $\mathcal{G}[\mathcal{C}(\sigma')]$  and  $\mathcal{G}[\mathcal{C}(\tau')]$ , and therefore can be extended to a homomorphism of  $\mathcal{G}[\mathcal{D} \cup \mathcal{G}\mathcal{C}(\sigma) \cup \mathcal{G}\mathcal{C}(\tau)]$  into  $\mathcal{G}[\mathcal{D}' \cup \mathcal{G}\mathcal{C}(\sigma') \cup \mathcal{G}\mathcal{C}(\tau')]$ , that is, to a homomorphism  $\mathcal{G}[\mathcal{D} \cup \mathcal{G}\sigma\mathcal{G} \cup \mathcal{G}\tau\mathcal{G}] \rightarrow \mathcal{G}[\mathcal{D}' \cup \mathcal{G}\sigma'\mathcal{G} \cup \mathcal{G}\tau'\mathcal{G}]$ , which evidently maps  $\alpha$  onto  $\alpha$ ,  $\sigma\alpha$  onto  $\sigma'\alpha$ , and  $\tau\alpha$  onto  $\tau'\alpha$  for each  $\alpha \in \mathcal{G}$ . By restriction, this yields a homomorphism  $g: \mathcal{G}[\mathcal{D} \cup \sigma\mathcal{G} \cup \tau\mathcal{G}] \rightarrow \mathcal{G}[\mathcal{D}' \cup \sigma'\mathcal{G} \cup \tau'\mathcal{G}]$  over  $\mathcal{G}$  such that  $g(\sigma\alpha) = \sigma'\alpha$  and  $g(\tau\alpha) = \tau'\alpha$  for every  $\alpha \in \mathcal{G}$ . This shows that  $(\sigma', \tau')$  is a specialization of  $(\sigma, \tau)$  (and therefore completes the proof of part (b)). Hence, by part (a),  $(\sigma'^{-1}, \tau'^{-1})$  is a specialization of  $(\sigma^{-1}, \tau^{-1})$ , so that  $\sigma'^{-1}$  and  $\tau'^{-1}$  are specializations of  $\sigma^{-1}$  and  $\tau^{-1}$ , respectively. However, if  $\rho'$  is a specialization of a strong isomorphism  $\rho$ , then part (a), applied to  $(\rho, \rho)$  and  $(\rho', \rho')$ , shows that  $\rho'^{-1}$  is a specialization of  $\rho^{-1}$ . Since  $\sigma'$  is a generic specialization of  $\sigma$ , we conclude that  $\sigma'^{-1}$  is a generic specialization of  $\sigma^{-1}$ . If the specialization  $\sigma'^{-1}\tau'$  of  $\sigma^{-1}\tau$  is also generic, then the formula  $x \mapsto \sigma'^{-1}(g(\sigma x))$  defines a homomorphism  $\mathcal{G}[\mathcal{D} \cup \sigma^{-1}\mathcal{G} \cup \sigma^{-1}\tau\mathcal{G}] \rightarrow \mathcal{G}[\mathcal{D}' \cup \sigma'^{-1}\mathcal{G} \cup \sigma'^{-1}\tau'\mathcal{G}]$  over  $\mathcal{G}$  that extends  $h$  and that, for each  $\alpha \in \mathcal{G}$ , maps  $\sigma^{-1}\alpha$  onto  $\sigma'^{-1}\alpha$  and  $\sigma^{-1}\tau\alpha$  onto  $\sigma'^{-1}\tau'\alpha$ , and that maps  $\mathcal{G}[\sigma^{-1}\mathcal{G}]$  and  $\mathcal{G}[\sigma^{-1}\tau\mathcal{G}]$  isomorphically onto  $\mathcal{G}[\sigma'^{-1}\mathcal{G}]$  and  $\mathcal{G}[\sigma'^{-1}\tau'\mathcal{G}]$ , respectively. This homomorphism can then be extended to a homomorphism

$$\mathcal{G}[\mathcal{D} \cup \mathcal{G}\sigma^{-1}\mathcal{G} \cup \mathcal{G}\sigma^{-1}\tau\mathcal{G}] \rightarrow \mathcal{G}[\mathcal{D}' \cup \mathcal{G}\sigma'^{-1}\mathcal{G} \cup \mathcal{G}\sigma'^{-1}\tau'\mathcal{G}],$$

which evidently is a common extension of  $h$  and the induced isomorphisms  $\mathcal{C}(\sigma^{-1}) \approx \mathcal{C}(\sigma'^{-1})$  and  $\mathcal{C}(\sigma^{-1}\tau) \approx \mathcal{C}(\sigma'^{-1}\tau')$ . Therefore  $h$  and these induced isomorphisms are compatible.

**Corollary** (a) *If  $\sigma'$  is a specialization of  $\sigma$ , then  $\sigma'^{-1}$  is a specialization of  $\sigma^{-1}$ . When the former specialization is generic, then so is the latter, and the induced isomorphisms  $\mathcal{C}(\sigma) \approx \mathcal{C}(\sigma')$  and  $\mathcal{C}(\sigma^{-1}) \approx \mathcal{C}(\sigma'^{-1})$  coincide.*

(b) *If  $\sigma'$  and  $\tau'$  are generic specializations of  $\sigma$  and  $\tau$ , respectively, such that the induced isomorphisms  $\mathcal{C}(\sigma) \approx \mathcal{C}(\sigma')$  and  $\mathcal{C}(\tau) \approx \mathcal{C}(\tau')$  are compatible, then  $\sigma'\tau'$  is a specialization of  $\sigma\tau$ . When the last specialization is generic, and  $h: \mathcal{D} \rightarrow \mathcal{D}'$  is a homomorphism between subrings of  $\mathcal{X}$  such that  $h$  and the induced isomorphisms  $\mathcal{C}(\sigma) \approx \mathcal{C}(\sigma')$  and  $\mathcal{C}(\tau) \approx \mathcal{C}(\tau')$  are compatible, then  $h$  and the induced isomorphism  $\mathcal{C}(\sigma\tau) \approx \mathcal{C}(\sigma'\tau')$  are compatible.*

*Proof* (a) The first assertion follows from Proposition 8(a), in the special case in which  $\tau = \sigma$ ,  $\tau' = \sigma'$ . The second assertion follows from Proposition 8(c), in the special case in which  $\tau = \sigma$ ,  $\tau' = \sigma'$ , and  $h$  is the induced isomorphism  $\mathcal{C}(\sigma) \approx \mathcal{C}(\sigma')$ .

(b) Because of part (a), we may replace  $\sigma, \sigma'$  by  $\sigma^{-1}, \sigma'^{-1}$ . The result then follows from Proposition 8(c).

### 3 Strongly normal extensions. Galois groups

By a *strongly normal* extension of the differential field  $\mathcal{F}$  we mean a finitely generated extension  $\mathcal{G}$  of  $\mathcal{F}$  such that every isomorphism of  $\mathcal{G}$  over  $\mathcal{F}$  is strong.

**Proposition 9** *If  $\mathcal{G}$  is a strongly normal extension of  $\mathcal{F}$ , then  $\mathcal{F}$  and  $\mathcal{G}$  have the same field of constants.*

*Proof* By Section 2, condition St1, the constants in  $\mathcal{G}$  are invariant under every isomorphism of  $\mathcal{G}$  over  $\mathcal{F}$ . By Section 1, part (a) of the corollary to Proposition 2, then the constants in  $\mathcal{G}$  are in  $\mathcal{F}$ .

**Proposition 10** *Let  $\mathcal{G}$  be a finitely generated extension of  $\mathcal{F}$  having the same field of constants as  $\mathcal{F}$ . Let  $\sigma_1, \dots, \sigma_r$  be isomorphisms of  $\mathcal{G}$  over  $\mathcal{F}$  such that every isomorphism of  $\mathcal{G}$  over  $\mathcal{F}$  is a specialization of one of these. If  $\sigma_k\mathcal{G} \subset \mathcal{G}\mathcal{X}$  ( $1 \leq k \leq r$ ), then  $\mathcal{G}$  is strongly normal over  $\mathcal{F}$ .*

*Proof* By Section 2, the remark following the proof of Proposition 6,  $\sigma\mathcal{G} \subset \mathcal{G}\mathcal{C}(\sigma)$  for every isomorphism  $\sigma$  of  $\mathcal{G}$  over  $\mathcal{F}$ . The isomorphism  $\sigma^{-1}: \sigma\mathcal{G} \approx \mathcal{G}$  can, because  $\mathcal{U}$  is universal over  $\mathcal{F}$ , be extended to an isomorphism  $\varphi$  of  $\mathcal{G}\sigma\mathcal{G}$ . The restriction of  $\varphi$  to  $\mathcal{G}$  is an isomorphism  $\tau$  of  $\mathcal{G}$  over  $\mathcal{F}$ . Thus, we have an isomorphism  $\varphi: \mathcal{G}\sigma\mathcal{G} \approx \tau\mathcal{G} \cdot \mathcal{G}$  over  $\mathcal{F}$ ,  $\varphi\mathcal{G} = \tau\mathcal{G}$ ,  $\varphi(\sigma\mathcal{G}) = \mathcal{G}$ , and evidently  $\varphi(\mathcal{C}(\sigma)) = \mathcal{C}(\tau)$ . Therefore  $\mathcal{G} = \varphi^{-1}(\tau\mathcal{G}) \subset \varphi^{-1}(\mathcal{G}\mathcal{C}(\tau)) = \varphi^{-1}\mathcal{G} \cdot \varphi^{-1}(\mathcal{C}(\tau)) = \sigma\mathcal{G} \cdot \mathcal{C}(\sigma)$ , so that every isomorphism  $\sigma$  of  $\mathcal{G}$  over  $\mathcal{F}$  is strong.

**Corollary** *Let  $\mathcal{G}_1$  and  $\mathcal{G}_2$  be extensions of  $\mathcal{F}$  such that  $\mathcal{G}_1\mathcal{G}_2$  has the same field of constants as  $\mathcal{F}$ . If  $\mathcal{G}_1$  and  $\mathcal{G}_2$  are strongly normal over  $\mathcal{F}$ , then so is  $\mathcal{G}_1\mathcal{G}_2$ .*

*Proof* Obviously  $\mathcal{G}_1 \mathcal{G}_2$  is a finitely generated extension of  $\mathcal{F}$ . If  $\sigma$  is any isomorphism of  $\mathcal{G}_1 \mathcal{G}_2$  over  $\mathcal{F}$ , then the restriction  $\sigma_i$  of  $\sigma$  to  $\mathcal{G}_i$  is a strong isomorphism of  $\mathcal{G}_i$  so that  $\sigma(\mathcal{G}_1 \mathcal{G}_2) = \sigma_1 \mathcal{G}_1 \cdot \sigma_2 \mathcal{G}_2 \subset \mathcal{G}_1 \mathcal{K} \cdot \mathcal{G}_2 \mathcal{K} = \mathcal{G}_1 \mathcal{G}_2 \cdot \mathcal{K}$ . It follows by Proposition 10 that  $\mathcal{G}_1 \mathcal{G}_2$  is a strongly normal extension of  $\mathcal{F}$ .

**Proposition 11** *Let  $\mathcal{G}$  be a strongly normal extension of  $\mathcal{F}$ , and let  $\mathcal{C}$  denote the field of constants of  $\mathcal{F}$ . Then  $\mathcal{G}$  is finitely generated as a field extension of  $\mathcal{F}$ , and for every isomorphism  $\sigma$  of  $\mathcal{G}$  over  $\mathcal{F}$ ,  $\mathcal{C}(\sigma)$  is a finitely generated field extension of  $\mathcal{C}$ .*

*Proof* The extension  $\mathcal{G}\sigma\mathcal{G}$  of  $\mathcal{G}$  is finitely generated. Hence by Chapter II, Section 11, Corollary 1 to Proposition 14,  $\mathcal{C}(\sigma)$  is a finitely generated field extension of  $\mathcal{C}$ . Take for  $\sigma$  an isolated isomorphism of  $\mathcal{G}$  over  $\mathcal{F}$ , and let  $\eta = (\eta_1, \dots, \eta_n)$  be a finite family of elements of  $\mathcal{G}$  such that  $\mathcal{G} = \mathcal{F}\langle\eta\rangle$ . Then by Section 1, part (a) of the corollary to Proposition 1, and Section 2, Proposition 3,  $\text{tr deg } \mathcal{G}/\mathcal{F} = \text{tr deg } \mathcal{G}\sigma\mathcal{G}/\mathcal{F} = \text{tr deg } \mathcal{C}(\sigma)/\mathcal{C}$  so that  $\text{deg } \omega_{\eta/\mathcal{F}} \leq 0$ . It follows by Chapter II, Section 13, Theorem 7, that  $\mathcal{G}$  is a finitely generated field extension of  $\mathcal{F}$ .

The key to the study of strongly normal extensions is provided by the following theorem.

**Theorem 1** *Let  $\mathcal{G}$  be a strongly normal extension of the differential field  $\mathcal{F}$  with field of constants  $\mathcal{C}$ , and let  $G$  denote the set of all strong isomorphisms of  $\mathcal{G}$  over  $\mathcal{F}$ . For each  $\sigma \in G$  let  $\mathcal{C}(\sigma)$  denote the field of constants of  $\mathcal{G}\sigma\mathcal{G}$ . For each  $(\sigma, \sigma') \in G^2$ , let  $\sigma \rightarrow \sigma'$  mean that  $\sigma'$  is a specialization of  $\sigma$  in the sense of Section 1. For each  $(\sigma, \sigma') \in G^2$  with  $\sigma \leftrightarrow \sigma'$  (that is, with  $\sigma'$  a generic specialization of  $\sigma$ ), let  $S_{\sigma', \sigma}$  denote the induced isomorphism  $\mathcal{C}(\sigma) \approx \mathcal{C}(\sigma')$  in the sense of Section 2. These data define on  $G$  a pre- $\mathcal{C}$ -set structure relative to the universal field  $\mathcal{K}$ . This pre- $\mathcal{C}$ -set structure, and the group structure that  $G$  has by virtue of its canonical identification with the group of automorphisms of  $\mathcal{G}\mathcal{K}$  over  $\mathcal{F}\mathcal{K}$ , define on  $G$  a  $\mathcal{C}$ -group structure. The dimension of the  $\mathcal{C}$ -group  $G$  equals the transcendence degree of  $\mathcal{G}$  over  $\mathcal{F}$ .*

*Proof* We must verify the axioms in Chapter V, Sections 2 and 3. By Proposition 11,  $\mathcal{C}(\sigma)$  is a finitely generated field extension of  $\mathcal{C}$  in  $\mathcal{K}$  for every  $\sigma \in G$ . We saw in Section 1 that the relation  $\sigma \rightarrow \sigma'$  is a pre-order. Part (c) of Proposition 1 (Section 1), and Proposition 3 (Section 2) and part (b) of the corollary to Proposition 1, establish axiom AS1. Proposition 7 (Section 2) establishes axiom AS2. Therefore we have a pre- $\mathcal{C}$ -set structure.

To prove axiom AG3 we must show that if  $\sigma$  is an isolated isomorphism of  $\mathcal{G}$  over  $\mathcal{F}$  with  $\sigma \rightarrow id_{\mathcal{G}}$ , then  $\mathcal{C}(\sigma)$  is regular over  $\mathcal{C}$ , or (since  $\mathcal{G}$  and  $\mathcal{C}(\sigma)$  are linearly disjoint over  $\mathcal{C}$ ) that the field  $\mathcal{G}\mathcal{C}(\sigma) = \mathcal{G}\sigma\mathcal{G}$  is regular over  $\mathcal{G}$ , or

(since, by Section 1, part (b) of Proposition 2,  $\mathcal{G}$  and  $\sigma\mathcal{G}$  are linearly disjoint over  $\mathcal{F}^\circ = \sigma\mathcal{F}^\circ$ ) that  $\sigma\mathcal{G}$  is regular over  $\sigma\mathcal{F}^\circ$ , which is obvious since  $\mathcal{G}$  is regular over  $\mathcal{F}^\circ$ . Axiom AG1 follows from Section 2, Proposition 5. Parts (a) and (c) of axiom AG2 follow from Section 2, part (c) of Proposition 8 and part (b) of the corollary to that proposition. It remains to prove parts (b) and (d) of AG2.

Let  $\sigma, \tau, \sigma', \tau'$  be strong isomorphisms of  $\mathcal{G}$  over  $\mathcal{F}$  with  $\sigma \rightarrow \sigma'$  and  $\tau \rightarrow \tau'$ . Fix a family  $\eta = (\eta_1, \dots, \eta_n)$  of generators of  $\mathcal{G}$  over  $\mathcal{F}$ , and let  $\mathfrak{p}$  respectively  $\mathfrak{q}$  denote the defining differential ideal of  $\sigma^{-1}\eta$  respectively  $\tau\eta$  in the differential polynomial algebras  $\mathcal{G}\{y_1, \dots, y_n\}$  respectively  $\mathcal{G}\{z_1, \dots, z_n\}$  over  $\mathcal{G}$ . Let  $\mathcal{G}_\#$  denote the algebraic closure of  $\mathcal{G}$ , and refer to Chapter III, Section 6, Proposition 3 and its corollary.  $\mathcal{G}_\# \mathfrak{p}$  and  $\mathcal{G}_\# \mathfrak{q}$  have  $\mathcal{G}_\#$ -regular components, say  $\mathfrak{p}_1, \dots, \mathfrak{p}_r$  and  $\mathfrak{q}_1, \dots, \mathfrak{q}_s$ . Each differential ideal  $\tau_{kl} = (\mathfrak{p}_k \cup \mathfrak{q}_l)$  of  $\mathcal{G}_\#\{y_1, \dots, y_n, z_1, \dots, z_n\}$  is prime, and therefore has a generic zero  $(\eta^{(k,l)}, \zeta^{(k,l)})$ , where  $\eta^{(k,l)}$  is a generic zero of  $\tau_{kl} \cap \mathcal{G}_\#\{y_1, \dots, y_n\} = \mathfrak{p}_k$  and therefore of  $\mathfrak{p}_k \cap \mathcal{G}\{y_1, \dots, y_n\} = \mathfrak{p}$ , so that  $\eta^{(k,l)}$  is a generic differential specialization of  $\sigma^{-1}\eta$  over  $\mathcal{G}$  and hence over  $\mathcal{F}$ . Therefore  $\eta^{(k,l)}$  is the image of  $\eta$  by a strong isomorphism of  $\mathcal{G}$  over  $\mathcal{F}$ , which we denote by  $\sigma_{kl}^{-1}$ . By Section 1, Lemma 2,  $\sigma^{-1} \leftrightarrow \sigma_{kl}^{-1}$ . Similarly,  $\zeta^{(k,l)} = \tau_{kl}\eta$  for some strong isomorphism  $\tau_{kl}$  of  $\mathcal{G}$  over  $\mathcal{F}$  with  $\tau \leftrightarrow \tau_{kl}$ . By hypothesis,  $\sigma \rightarrow \sigma'$ , whence  $\sigma^{-1} \rightarrow \sigma'^{-1}$  so that  $\sigma'^{-1}\eta$  is a zero of  $\mathfrak{p}$  and hence of some  $\mathfrak{p}_k$ . Similarly,  $\tau'\eta$  is a zero of some  $\mathfrak{q}_l$ . Thus,  $(\sigma'^{-1}\eta, \tau'\eta)$  is a zero of  $\tau_{kl}$ , that is, is a differential specialization of  $(\sigma_{kl}^{-1}\eta, \tau_{kl}\eta)$  over  $\mathcal{G}_\#$  and hence over  $\mathcal{G}$ . It follows by Section 1, Lemma 2, that  $(\tau', \sigma'^{-1})$  is a specialization of  $(\tau_{kl}, \sigma_{kl}^{-1})$ , and hence by Section 2, Proposition 8(a) and (b), that  $(\tau'^{-1}, \tau'^{-1}\sigma'^{-1})$  is a specialization of  $(\tau_{kl}^{-1}, \tau_{kl}^{-1}\sigma_{kl}^{-1})$  and that if  $\tau_{kl}^{-1}\sigma_{kl}^{-1} \leftrightarrow \tau'^{-1}\sigma'^{-1}$  and  $\tau_{kl}^{-1} \leftrightarrow \tau'^{-1}$ , then the induced isomorphisms  $\mathcal{C}(\tau_{kl}^{-1}\sigma_{kl}^{-1}) \approx \mathcal{C}(\tau'^{-1}\sigma'^{-1})$  and  $\mathcal{C}(\tau_{kl}^{-1}) \approx \mathcal{C}(\tau'^{-1})$  are compatible. By part (a) of the corollary to Proposition 8, then  $\sigma_{kl}\tau_{kl} \rightarrow \sigma'\tau'$  and if  $\sigma_{kl}\tau_{kl} \leftrightarrow \sigma'\tau'$  and  $\tau_{kl} \leftrightarrow \tau'$ , then the induced isomorphisms  $\mathcal{C}(\sigma_{kl}\tau_{kl}) \approx \mathcal{C}(\sigma'\tau')$  and  $\mathcal{C}(\tau_{kl}) \approx \mathcal{C}(\tau')$  are compatible. This proves axiom AG2, part (b), and (because  $\sigma^{-1} \rightarrow \sigma'^{-1}$  whenever  $\sigma \rightarrow \sigma'$ ) also part (d), and establishes  $G$  as a  $\mathcal{C}$ -group.

Finally, let  $\sigma$  be a  $\mathcal{C}$ -generic element of  $G^\circ$ , that is, an isolated isomorphism of  $\mathcal{G}$  over  $\mathcal{F}$  with  $\sigma \rightarrow id_{\mathcal{G}}$ . Because  $\mathcal{G}$  and  $\mathcal{C}(\sigma)$  are linearly disjoint over  $\mathcal{C}$ , and  $\mathcal{G}$  and  $\sigma\mathcal{G}$  are algebraically disjoint over  $\mathcal{F}$ ,

$$\begin{aligned} \text{tr deg } \mathcal{C}(\sigma)/\mathcal{C} &= \text{tr deg } \mathcal{G}\mathcal{C}(\sigma)/\mathcal{G} = \text{tr deg } \mathcal{G}\sigma\mathcal{G}/\mathcal{G} \\ &= \text{tr deg } \sigma\mathcal{G}/\mathcal{F} = \text{tr deg } \mathcal{G}/\mathcal{F}. \end{aligned}$$

This completes the proof of the theorem.

By virtue of Theorem 1, the set of strong isomorphisms of the strongly normal extension  $\mathcal{G}$  of  $\mathcal{F}$  has a natural structure of  $\mathcal{C}$ -group relative to the

universal field  $\mathcal{K}$ . We call this  $\mathcal{C}$ -group the *Galois group* of  $\mathcal{G}$  over  $\mathcal{F}$ , and denote it by  $G(\mathcal{G}/\mathcal{F})$ . We denote the component of the identity of  $G(\mathcal{G}/\mathcal{F})$  by  $G^0(\mathcal{G}/\mathcal{F})$ .

For reasons that will appear later, it is desirable to consider  $\mathcal{C}$ -groups and, more generally,  $\mathcal{F}$ -sets relative to the universal field  $\mathcal{U}$ , and therefore we adopt the convention that *when we refer to a  $\mathcal{C}$ -group that is not the Galois group of a strongly normal extension (or to an  $\mathcal{F}$ -set) we mean, unless the contrary is indicated, a  $\mathcal{C}$ -group (or  $\mathcal{F}$ -set) relative to the universal field  $\mathcal{U}$* . Of course, when  $G$  is such a  $\mathcal{C}$ -group, then  $G_x$  is a  $\mathcal{C}$ -group relative to the universal field  $\mathcal{K}$ . Furthermore, we know by Chapter V, Section 4, that every  $\mathcal{C}$ -group relative to  $\mathcal{K}$  is obtainable in this way from a  $\mathcal{C}$ -group relative to  $\mathcal{U}$ . When  $X$  is an  $\mathcal{F}$ -set and  $\alpha \in X$ ,  $\mathcal{F}\langle\alpha\rangle$  will denote the differential field generated by  $\mathcal{F}\langle\alpha\rangle$ .

Theorem 1 permits us to classify strongly normal extensions of the differential field  $\mathcal{F}$ . If  $G$  is any  $\mathcal{C}$ -group, by  $G$ -extension of  $\mathcal{F}$  we mean any strongly normal extension  $\mathcal{G}$  of  $\mathcal{F}$  such that  $G(\mathcal{G}/\mathcal{F})$  is  $\mathcal{C}$ -isomorphic to a  $\mathcal{C}$ -subgroup of  $G_x$ . When  $G(\mathcal{G}/\mathcal{F})$  is  $\mathcal{C}$ -isomorphic to  $G_x$  itself, we say that the extension is *full*. By a *linear* (respectively *Abelian*) extension of  $\mathcal{F}$  we mean a  $\text{GL}(n)$ -extension of  $\mathcal{F}$  for some  $n \in \mathbb{N}$  (respectively an  $A$ -extension of  $\mathcal{F}$  for some Abelian  $\mathcal{C}$ -group  $A$ ).

The following theorem interprets, for an extension  $\mathcal{C}'$  of  $\mathcal{C}$  in  $\mathcal{K}$ , the induced  $\mathcal{C}'$ -group of the  $\mathcal{C}$ -group  $G(\mathcal{G}/\mathcal{F})$  (see Chapter V, Section 5).

**Theorem 2** *Let  $\mathcal{G}$  be a strongly normal extension of  $\mathcal{F}$ , denote the field of constants of  $\mathcal{F}$  by  $\mathcal{C}$ , and let  $\mathcal{C}'$  be an extension of  $\mathcal{C}$  in  $\mathcal{K}$  such that  $\mathcal{U}$  is universal over  $\mathcal{F}\mathcal{C}'$ . Then  $\mathcal{U}$  is universal over  $\mathcal{G}\mathcal{C}'$ ,  $\mathcal{G}\mathcal{C}'$  is a strongly normal extension of  $\mathcal{F}\mathcal{C}'$  with field of constants  $\mathcal{C}'$ , and the  $\mathcal{C}'$ -group  $G(\mathcal{G}\mathcal{C}'/\mathcal{F}\mathcal{C}')$  is the induced  $\mathcal{C}'$ -group of the  $\mathcal{C}$ -group  $G(\mathcal{G}/\mathcal{F})$ , both these groups being identified with each other by means of their canonical identifications with the group of automorphisms of  $\mathcal{G}\mathcal{K}$  over  $\mathcal{F}\mathcal{K}$ .*

*Proof* Since  $\mathcal{G}\mathcal{C}'$  is finitely generated over  $\mathcal{F}\mathcal{C}'$ , Chapter III, Section 7, Proposition 4(b) shows that  $\mathcal{U}$  is universal over  $\mathcal{G}\mathcal{C}'$ . That  $\mathcal{C}'$  is the field of constants of both  $\mathcal{F}\mathcal{C}'$  and  $\mathcal{G}\mathcal{C}'$  follows from Chapter II, Section 1, Corollary 2 to Theorem 1. If  $\sigma$  is any isomorphism of  $\mathcal{G}\mathcal{C}'$  over  $\mathcal{F}\mathcal{C}'$ , then the restriction of  $\sigma$  to  $\mathcal{G}$  is an isomorphism of  $\mathcal{G}$  over  $\mathcal{F}$  and as such is strong, so that  $\sigma(\mathcal{G}\mathcal{C}') = \sigma\mathcal{G} \cdot \sigma\mathcal{C}' \subset \mathcal{G}\mathcal{K} \cdot \mathcal{C}' = \mathcal{G}\mathcal{C}' \cdot \mathcal{K}$ , and similarly  $\mathcal{G}\mathcal{C}' \subset \sigma(\mathcal{G}\mathcal{C}') \cdot \mathcal{K}$ , and hence  $\sigma$  is strong. Therefore  $\mathcal{G}\mathcal{C}'$  is strongly normal over  $\mathcal{F}\mathcal{C}'$ .

Identifying  $\sigma$  with the automorphism of  $\mathcal{G}\mathcal{C}' \cdot \mathcal{K} = \mathcal{G}\mathcal{K}$  over  $\mathcal{F}\mathcal{C}' \cdot \mathcal{K} = \mathcal{F}\mathcal{K}$  that extends  $\sigma$ , and hence also with the strong isomorphism of  $\mathcal{G}$  over  $\mathcal{F}$  to which  $\sigma$  restricts, we find that  $\mathcal{G}\mathcal{C}'(\sigma) = \mathcal{G}\mathcal{C}' \cdot \mathcal{C}'(\sigma) = \mathcal{G}\mathcal{C}'\sigma(\mathcal{G}\mathcal{C}') = \mathcal{G}\sigma \cdot \mathcal{C}' = \mathcal{G}\mathcal{C}'(\sigma)\mathcal{C}'$ , whence (by Chapter II, Section 1, Corollary 2 to

Theorem 1)  $\mathcal{C}'(\sigma) = \mathcal{C}'(\sigma)\mathcal{C}'$ . If  $\sigma'$  is a specialization of  $\sigma$  in  $G(\mathcal{G}\mathcal{C}'/\mathcal{F}\mathcal{C}')$ , then  $(\sigma'\alpha)_{\alpha \in \mathcal{G}}$  is a differential specialization of  $(\sigma\alpha)_{\alpha \in \mathcal{G}}$  over  $\mathcal{G}\mathcal{C}'$ , hence over  $\mathcal{G}$ , so that  $\sigma'$  is a specialization of  $\sigma$  in  $G(\mathcal{G}/\mathcal{F})$ . When the specialization in  $G(\mathcal{G}\mathcal{C}'/\mathcal{F}\mathcal{C}')$  is generic, there exists an isomorphism  $\mathcal{G}\mathcal{C}'\sigma\mathcal{G} \approx \mathcal{G}\mathcal{C}'\sigma'\mathcal{G}$  over  $\mathcal{G}\mathcal{C}'$  mapping  $\sigma\alpha$  onto  $\sigma'\alpha$  for every  $\alpha \in \mathcal{G}$ , and this restricts to an isomorphism  $\mathcal{G}\sigma\mathcal{G} \approx \mathcal{G}\sigma'\mathcal{G}$  over  $\mathcal{G}$ , so that the specialization in  $G(\mathcal{G}/\mathcal{F})$  is generic; the induced isomorphism  $S_{\sigma',\sigma}^{\mathcal{C}'}$ :  $\mathcal{C}'(\sigma) \approx \mathcal{C}'(\sigma')$  is a restriction of the former of these two isomorphisms, and the induced isomorphism  $S_{\sigma',\sigma}^{\mathcal{C}}$ :  $\mathcal{C}(\sigma) \approx \mathcal{C}(\sigma')$  is a restriction of the latter, and hence  $S_{\sigma',\sigma}^{\mathcal{C}}$  is an extension of  $S_{\sigma',\sigma}^{\mathcal{C}'}$ . This shows that the identity mapping  $G(\mathcal{G}\mathcal{C}'/\mathcal{F}\mathcal{C}') \rightarrow G(\mathcal{G}/\mathcal{F})$  is a  $(\mathcal{C}', \mathcal{C})$ -homomorphism in the sense of Chapter V, Section 5.

Now let  $H$  be any  $\mathcal{C}'$ -group relative to the universal field  $\mathcal{K}$  and  $f: H \rightarrow G(\mathcal{G}/\mathcal{F})$  be a  $(\mathcal{C}', \mathcal{C})$ -homomorphism. To complete the proof of the theorem, we must show that this is a  $\mathcal{C}'$ -homomorphism  $f: H \rightarrow G(\mathcal{G}\mathcal{C}'/\mathcal{F}\mathcal{C}')$ . For any  $y \in H$ ,  $\mathcal{C}'(y) \supset \mathcal{C}(f(y))$  because  $f$  is a  $(\mathcal{C}', \mathcal{C})$ -homomorphism, so that  $\mathcal{C}'(y) \supset \mathcal{C}(f(y))\mathcal{C}' = \mathcal{C}'(f(y))$  by the above. If  $y \xleftrightarrow{\mathcal{C}'} y'$ , then  $f(y) \leftrightarrow f(y')$  in  $G(\mathcal{G}/\mathcal{F})$  and  $S_{y',y}^{\mathcal{C}'}$  extends the induced isomorphism  $S_{f(y'),f(y)}$ , and hence  $S_{f(y'),f(y)}$  and  $id_{\mathcal{C}'}$  are bicompatible. Since  $\mathcal{G}$  and  $\mathcal{C}[\mathcal{C}(f(y)) \cup \mathcal{C}']$  are linearly disjoint over  $\mathcal{C}$ , as are  $\mathcal{G}$  and  $\mathcal{C}[\mathcal{C}(f(y')) \cup \mathcal{C}']$ , it follows that  $id_{\mathcal{G}}$ ,  $S_{f(y'),f(y)}$ ,  $id_{\mathcal{C}'}$  are bicompatible, and hence that there exists an isomorphism  $\mathcal{G}\mathcal{C}'(f(y))\mathcal{C}' \approx \mathcal{G}\mathcal{C}'(f(y'))\mathcal{C}'$  over  $\mathcal{G}\mathcal{C}'$  extending  $S_{f(y'),f(y)}$ , that is, an isomorphism  $\mathcal{G}\mathcal{C}' \cdot f(y)(\mathcal{G}\mathcal{C}') \approx \mathcal{G}\mathcal{C}' \cdot f(y')(\mathcal{G}\mathcal{C}')$  over  $\mathcal{G}\mathcal{C}'$  that maps  $f(y)\alpha$  onto  $f(y')\alpha$  for every  $\alpha \in \mathcal{G}$ . Therefore  $f(y) \leftrightarrow f(y')$  in  $G(\mathcal{G}\mathcal{C}'/\mathcal{F}\mathcal{C}')$  and  $S_{y',y}^{\mathcal{C}'}$  extends the induced isomorphism  $S_{f(y'),f(y)}^{\mathcal{C}'}$ :  $\mathcal{C}'(f(y)) \approx \mathcal{C}'(f(y'))$ . It follows by Chapter V, Section 9, Corollary 1 to Proposition 9, that  $f$  is a  $\mathcal{C}'$ -homomorphism.

**Proposition 12** *Let  $\mathcal{G}$  be a strongly normal extension of  $\mathcal{F}$  with field of constants  $\mathcal{C}$ , and let  $\varphi$  be an isomorphism of  $\mathcal{G}$  over  $\mathcal{C}$  such that  $\mathcal{U}$  is universal over  $\varphi\mathcal{G}$ . Then  $\varphi\mathcal{G}$  is a strongly normal extension of  $\varphi\mathcal{F}$ . There is a unique isomorphism  $\mathcal{G}\mathcal{K} \approx \varphi\mathcal{G} \cdot \mathcal{K}$  over  $\mathcal{K}$  that extends  $\varphi$  (and that we shall permit ourselves to denote by  $\varphi$ ). When  $G(\mathcal{G}/\mathcal{F})$  respectively  $G(\varphi\mathcal{G}/\varphi\mathcal{F})$  is canonically identified with the group of automorphisms of  $\mathcal{G}\mathcal{K}$  over  $\mathcal{F}\mathcal{K}$ , respectively of  $\varphi\mathcal{G} \cdot \mathcal{K}$  over  $\varphi\mathcal{F} \cdot \mathcal{K}$ , the formula  $T_\varphi(\sigma) = \varphi \circ \sigma \circ \varphi^{-1}$  defines a  $\mathcal{C}$ -isomorphism  $T_\varphi: G(\mathcal{G}/\mathcal{F}) \approx G(\varphi\mathcal{G}/\varphi\mathcal{F})$ .*

**REMARK** When  $\varphi$  is an isomorphism of  $\mathcal{G}$  over  $\mathcal{F}$ , then  $\varphi \in G(\mathcal{G}/\mathcal{F})$ . After  $G(\mathcal{G}/\mathcal{F})$  and  $G(\varphi\mathcal{G}/\varphi\mathcal{F})$  are canonically identified with the group of automorphisms of the differential field  $\mathcal{G}\mathcal{K} = \varphi\mathcal{G} \cdot \mathcal{K}$  over  $\mathcal{F}\mathcal{K}$ , then they coincide as groups (but not necessarily as  $\mathcal{C}$ -groups), and  $T_\varphi$  is the inner automorphism determined by  $\varphi$ .

*Proof* Let  $\tau$  be any isomorphism of  $\varphi\mathcal{G}$  over  $\varphi\mathcal{F}$ . The isomorphism

$\varphi^{-1}: \varphi\mathcal{G} \approx \mathcal{G}$  can be extended to some isomorphism  $\psi: \varphi\mathcal{G} \cdot \tau\varphi\mathcal{G} \approx \mathcal{G} \cdot \psi\tau\varphi\mathcal{G}$ , and evidently the formula  $\alpha \mapsto \psi\tau\varphi\alpha$  defines an isomorphism of  $\mathcal{G}$  over  $\mathcal{F}$ . Therefore the field of constants  $\mathcal{C}'$  of  $\mathcal{G} \cdot \psi\tau\varphi\mathcal{G}$  has the property that  $\mathcal{G}\mathcal{C}' = \mathcal{G} \cdot \psi\tau\varphi\mathcal{G} = \psi\tau\varphi\mathcal{G} \cdot \mathcal{C}'$ . Since  $\psi^{-1}$  maps  $\mathcal{G}$  onto  $\varphi\mathcal{G}$  and  $\mathcal{C}'$  onto the field of constants  $\mathcal{C}(\tau)$  of  $\varphi\mathcal{G} \cdot \tau\varphi\mathcal{G}$ , then  $\varphi\mathcal{G} \cdot \mathcal{C}(\tau) = \varphi\mathcal{G} \cdot \tau\varphi\mathcal{G} = \tau\varphi\mathcal{G} \cdot \mathcal{C}(\tau)$ , so that  $\tau$  is strong. Hence  $\varphi\mathcal{G}$  is strongly normal over  $\varphi\mathcal{F}$ .

Since  $\mathcal{G}$  and  $\mathcal{H}$  are linearly disjoint over  $\mathcal{C}$ , as are  $\varphi\mathcal{G}$  and  $\mathcal{H}$ ,  $\varphi$  can be extended to a unique isomorphism  $\mathcal{G}\mathcal{H} \approx \varphi\mathcal{G} \cdot \mathcal{H}$  over  $\mathcal{H}$ , and we denote it, too, by  $\varphi$ . Making the canonical identifications, we see that for each  $\sigma \in G(\mathcal{G}/\mathcal{F})$ ,  $\varphi \circ \sigma \circ \varphi^{-1} \in G(\varphi\mathcal{G}/\varphi\mathcal{F})$ . Therefore we can define a mapping  $T_\varphi: G(\mathcal{G}/\mathcal{F}) \rightarrow G(\varphi\mathcal{G}/\varphi\mathcal{F})$  by the formula  $T_\varphi(\sigma) = \varphi \circ \sigma \circ \varphi^{-1}$ , and it is clear that  $T_\varphi$  is a group isomorphism. Since  $\varphi\mathcal{G} \cdot \mathcal{C}(T_\varphi(\sigma)) = \varphi\mathcal{G} \cdot (\varphi \circ \sigma \circ \varphi^{-1})\varphi\mathcal{G} = \varphi(\mathcal{G}\sigma\mathcal{G}) = \varphi(\mathcal{G}\mathcal{C}(\sigma)) = \varphi\mathcal{G} \cdot \mathcal{C}(\sigma)$ , we infer that  $\mathcal{C}(T_\varphi(\sigma)) = \mathcal{C}(\sigma)$ . Furthermore, if  $\sigma \leftrightarrow \sigma'$ , then there exists an isomorphism  $\mathcal{G}\sigma\mathcal{G} \approx \mathcal{G}\sigma'\mathcal{G}$  over  $\mathcal{G}$  mapping  $\sigma\alpha$  onto  $\sigma'\alpha$  ( $\alpha \in \mathcal{F}$ ) and inducing the isomorphism  $S_{\sigma',\sigma}: \mathcal{C}(\sigma) \approx \mathcal{C}(\sigma')$ . Since  $\varphi$  maps  $\mathcal{G}\sigma\mathcal{G}$  respectively  $\mathcal{G}\sigma'\mathcal{G}$  onto  $\varphi\mathcal{G} \cdot T_\varphi(\sigma)\varphi\mathcal{G}$  respectively  $\varphi\mathcal{G} \cdot T_\varphi(\sigma')\varphi\mathcal{G}$  and leaves constants fixed, we obtain an isomorphism  $\varphi\mathcal{G} \cdot T_\varphi(\sigma)\varphi\mathcal{G} \approx \varphi\mathcal{G} \cdot T_\varphi(\sigma')\varphi\mathcal{G}$  over  $\varphi\mathcal{G}$  mapping  $T_\varphi(\sigma)\varphi\alpha$  onto  $T_\varphi(\sigma')\varphi\alpha$  ( $\alpha \in \mathcal{G}$ ), so that  $T_\varphi(\sigma) \leftrightarrow T_\varphi(\sigma')$  and  $S_{T_\varphi(\sigma'), T_\varphi(\sigma)} = S_{\sigma', \sigma}$ . It follows from Chapter V, Section 9, Corollary 1 to Proposition 9, that  $T_\varphi$  is a  $\mathcal{C}$ -isomorphism.

#### 4 The fundamental theorems

The following theorem establishes a Galois correspondence between the set of intermediate differential fields of a strongly normal extension and the set of  $\mathcal{C}$ -subgroups of its Galois group.

**Theorem 3** *Let  $\mathcal{G}$  be a strongly normal extension of the differential field  $\mathcal{F}$  with field of constants  $\mathcal{C}$ .*

(a) *If  $\mathcal{F}_1$  is a differential field with  $\mathcal{F} \subset \mathcal{F}_1 \subset \mathcal{G}$ , then  $\mathcal{G}$  is strongly normal over  $\mathcal{F}_1$ ,  $G(\mathcal{G}/\mathcal{F}_1)$  is a  $\mathcal{C}$ -subgroup of  $G(\mathcal{G}/\mathcal{F})$ , and the set of invariants of  $G(\mathcal{G}/\mathcal{F}_1)$  in  $\mathcal{G}$  is  $\mathcal{F}_1$ .*

(b) *If  $G_1$  is a  $\mathcal{C}$ -subgroup of  $G(\mathcal{G}/\mathcal{F})$  and  $\mathcal{F}_1$  denotes the set of invariants of  $G_1$  in  $\mathcal{G}$ , then  $\mathcal{F}_1$  is a differential field with  $\mathcal{F} \subset \mathcal{F}_1 \subset \mathcal{G}$  and  $G(\mathcal{G}/\mathcal{F}_1) = G_1$ .*

*Proof* (a) Every isomorphism of  $\mathcal{G}$  over  $\mathcal{F}_1$  is over  $\mathcal{F}$ , too, and hence is strong. Therefore  $\mathcal{G}$  is strongly normal over  $\mathcal{F}_1$  and the Galois group  $G(\mathcal{G}/\mathcal{F}_1)$  is a  $\mathcal{C}$ -group. It is obviously a subgroup and a  $\mathcal{C}$ -subset of  $G(\mathcal{G}/\mathcal{F})$ , and hence (by Chapter V, Section 8, Proposition 5) is a  $\mathcal{C}$ -subgroup of  $G(\mathcal{G}/\mathcal{F})$ . By definition, every element of  $\mathcal{F}_1$  is an invariant of  $G(\mathcal{G}/\mathcal{F}_1)$  in  $\mathcal{G}$ , and by Section 1, part (a) of the corollary to Proposition 2, every such invariant is in  $\mathcal{F}_1$ .

(b) It is obvious that  $\mathcal{F}_1$  is a differential field with  $\mathcal{F} \subset \mathcal{F}_1 \subset \mathcal{G}$ , and therefore, by part (a),  $G(\mathcal{G}/\mathcal{F}_1)$  is a  $\mathcal{C}$ -subgroup of  $G(\mathcal{G}/\mathcal{F})$ . Of course,  $G_1 \subset G(\mathcal{G}/\mathcal{F}_1)$ . We must show that  $G_1 = G(\mathcal{G}/\mathcal{F}_1)$ , and we do this first under the extra hypothesis that  $\mathcal{C}$  is algebraically closed.

Assume, under the extra hypothesis, that  $G_1 \neq G(\mathcal{G}/\mathcal{F}_1)$ . Fix  $\mathcal{C}$ -generic elements  $\sigma_1, \dots, \sigma_r$  of the  $\mathcal{C}$ -components of  $G_1$ . By assumption, there exists an element  $\tau \in G(\mathcal{G}/\mathcal{F}_1)$  that is not a specialization of any  $\sigma_k$ . Fixing elements  $\eta_1, \dots, \eta_n \in \mathcal{G}$  with  $\mathcal{F}\langle \eta_1, \dots, \eta_n \rangle = \mathcal{G}$ , we see by Section 1, Lemma 2, that for each index  $k$  there exists a differential polynomial  $F_k \in \mathcal{G}\{y_1, \dots, y_n\}$  that vanishes at  $(\sigma_k \eta_1, \dots, \sigma_k \eta_n)$  but not at  $(\tau \eta_1, \dots, \tau \eta_n)$ . Considering the product  $\prod F_k$ , we infer that there exists a differential polynomial in  $\mathcal{G}\{y_1, \dots, y_n\}$  that vanishes at  $(\sigma \eta_1, \dots, \sigma \eta_n)$  for every  $\sigma \in G_1$  but not for every  $\sigma \in G(\mathcal{G}/\mathcal{F}_1)$ . Let  $F$  be such a differential polynomial with as few nonzero terms as possible. We suppose, as we may, that one of the coefficients in  $F$  is 1. Consider any  $\sigma' \in G_{1\mathcal{C}}$  (that is, any  $\sigma' \in G_1$  that is rational over  $\mathcal{C}$ , or in other words that is an automorphism of  $\mathcal{G}$ ). Since  $F^\sigma(\sigma \eta_1, \dots, \sigma \eta_n) = \sigma'(F(\sigma'^{-1} \sigma \eta_1, \dots, \sigma'^{-1} \sigma \eta_n))$ ,  $F^\sigma$  vanishes at  $(\sigma \eta_1, \dots, \sigma \eta_n)$  for every  $\sigma \in G_1$ , and therefore  $F - F^\sigma$  does too. Since  $F - F^\sigma$  has fewer nonzero terms than  $F$ ,  $F - F^\sigma$  must vanish at  $(\sigma \eta_1, \dots, \sigma \eta_n)$  for every  $\sigma \in G(\mathcal{G}/\mathcal{F}_1)$ . Hence, for any  $\alpha \in \mathcal{G}$ ,  $F - \alpha(F - F^\sigma)$  vanishes at  $(\sigma \eta_1, \dots, \sigma \eta_n)$  for every  $\sigma \in G_1$  but not for every  $\sigma \in G(\mathcal{G}/\mathcal{F}_1)$ . If  $F - F^\sigma$  were not 0, we could choose  $\alpha$  so that  $F - \alpha(F - F^\sigma)$  had fewer nonzero terms than  $F$ . Therefore  $F - F^\sigma = 0$  for every  $\sigma' \in G_{1\mathcal{C}}$ . Since (by Chapter V, Section 7, the corollary to Proposition 3)  $G_{1\mathcal{C}}$  is dense in  $G_1$ , and since (by part (a)) the set of elements  $\sigma \in G(\mathcal{G}/\mathcal{F})$  with  $F^\sigma = F$  is closed in  $G(\mathcal{G}/\mathcal{F})$ , this means that  $F^\sigma = F$  for every  $\sigma \in G_1$ , so that  $F \in \mathcal{F}_1\{y_1, \dots, y_n\}$ . However, then  $F^\sigma = F$  for every  $\sigma \in G(\mathcal{G}/\mathcal{F}_1)$ , so that  $F(\sigma \eta_1, \dots, \sigma \eta_n) = \sigma(F(\eta_1, \dots, \eta_n)) = 0$  for every such  $\sigma$ . This contradiction shows that  $G_1 = G(\mathcal{G}/\mathcal{F}_1)$  under the extra hypothesis that  $\mathcal{C}$  is algebraically closed.

Now relinquish this hypothesis, and let  $\mathcal{C}_a$  denote the algebraic closure of  $\mathcal{C}$ . Let  $\mathcal{F}'$  denote the set of invariants of  $G_1$  in  $\mathcal{G}\mathcal{C}_a$ . Then  $\mathcal{F}'$  is a differential field with  $\mathcal{F}\mathcal{C}_a \subset \mathcal{F}' \subset \mathcal{G}\mathcal{C}_a$ , and  $\mathcal{G} \cap \mathcal{F}' = \mathcal{F}_1$ . We claim that  $\mathcal{G}$  and  $\mathcal{F}'$  are linearly disjoint over  $\mathcal{F}_1$ . To establish this, consider elements  $\varphi_1, \dots, \varphi_s \in \mathcal{F}'$  that are linearly dependent over  $\mathcal{G}$ . We must show that they are linearly dependent over  $\mathcal{F}_1$ , and in doing this we may suppose that  $s > 1$  and that no  $s-1$  of them are linearly dependent over  $\mathcal{G}$ . Then there exist nonzero elements  $\alpha_1, \dots, \alpha_s \in \mathcal{G}$  with  $\sum_{1 \leq j \leq s} \alpha_j \varphi_j = 0$ . Dividing by  $\alpha_s$ , we may suppose that  $\alpha_s = 1$ . For any  $\sigma \in G_1$ , evidently  $\sum_{1 \leq j \leq s} (\sigma \alpha_j) \varphi_j = 0$ , and therefore  $\sum_{1 \leq j \leq s-1} (\sigma \alpha_j - \alpha_j) \varphi_j = 0$ . Taking  $\sigma \in G_{1\mathcal{C}_a}$ , and denoting the  $\mathcal{C}$ -conjugates of  $\sigma$  by  $\sigma_1, \dots, \sigma_r$ , we therefore may write

$$\sum_{1 \leq j \leq s-1} (\sigma_k \alpha_j - \alpha_j) \varphi_j = 0 \quad (1 \leq k \leq r).$$

If  $\sigma\alpha_1 - \alpha_1$  were not 0, then, for each  $k$ ,  $\sigma_k\alpha_1 - \alpha_1$  would be different from 0, and we would have  $\sum_{1 \leq j \leq s-1} (\sigma_k\alpha_1 - \alpha_1)^{-1} (\sigma_k\alpha_j - \alpha_j) \varphi_j = 0$  ( $1 \leq k \leq t$ ); setting

$$\begin{aligned} \alpha_j' &= \sum_{1 \leq k \leq t} (\sigma_k\alpha_1 - \alpha_1)^{-1} (\sigma_k\alpha_j - \alpha_j) \\ &= \text{Tr}_{\mathcal{G}(\sigma)/\mathcal{G}}(\sigma\alpha_1 - \alpha_1)^{-1} (\sigma\alpha_j - \alpha_j), \end{aligned}$$

we would therefore find that

$$\sum_{1 \leq j \leq s-1} \alpha_j' \varphi_j = 0, \quad \alpha_j' \in \mathcal{G} \quad (1 \leq j \leq s-1), \quad \alpha_1' = \text{Tr}_{\mathcal{G}(\sigma)/\mathcal{G}} 1 \neq 0,$$

contradicting the linear independence of  $\varphi_1, \dots, \varphi_{s-1}$  over  $\mathcal{G}$ . Therefore,  $\sigma\alpha_1 = \alpha_1$  for every  $\sigma \in G_{1\mathcal{G}_a}$ , and hence (because  $G_{1\mathcal{G}_a}$  is dense in  $G_1$ ) for every  $\sigma \in G_1$ , whence  $\alpha_1 \in \mathcal{F}_1$ . Similarly,  $\alpha_k \in \mathcal{F}_1$  for every index  $k$ , so that  $\varphi_1, \dots, \varphi_s$  are linearly dependent over  $\mathcal{F}_1$ . This establishes our claim.

Evidently  $\mathcal{F}_1\mathcal{C}_a \subset \mathcal{F}'$ . Consider any element  $\varphi \in \mathcal{F}'$ . Fixing a basis  $(c_i)$  of  $\mathcal{C}_a$  over  $\mathcal{G}$ , we can write  $\varphi = \sum \beta_i c_i$ , where the  $\beta_i$  are elements of  $\mathcal{G}$ , and therefore  $\varphi - \sum \beta_i c_i = 0$ . Thus  $\varphi$  and the various elements  $c_i$  of  $\mathcal{F}'$  are linearly dependent over  $\mathcal{G}$ . By the claim established above, they must be linearly dependent over  $\mathcal{F}_1$ , that is, there exist elements  $\beta_i'$  and  $\gamma'$  of  $\mathcal{F}_1$ , not all 0, such that  $\gamma'\varphi - \sum \beta_i' c_i = 0$ . However, the elements  $c_i$  of  $\mathcal{C}_a$  are linearly independent over  $\mathcal{G}$ , and therefore  $\gamma' \neq 0$ , so that  $\varphi = \sum \gamma'^{-1} \beta_i' c_i \in \mathcal{F}_1\mathcal{C}_a$ . This shows that  $\mathcal{F}_1\mathcal{C}_a = \mathcal{F}'$ . It follows by Section 3, Theorem 2, and by the present theorem with the extra hypothesis, that  $G(\mathcal{G}/\mathcal{F}_1) = G(\mathcal{G}\mathcal{C}_a/\mathcal{F}_1\mathcal{C}_a) = G(\mathcal{G}\mathcal{C}_a/\mathcal{F}') = G_1$ . This completes the proof of Theorem 3.

**Corollary** Let  $\mathcal{G}$  be a strongly normal extension of  $\mathcal{F}$  with field of constants  $\mathcal{C}$ , and let  $\mathcal{F}_1$  and  $\mathcal{F}_2$  be intermediate differential fields. Then  $G(\mathcal{G}/\mathcal{F}_1\mathcal{F}_2) = G(\mathcal{G}/\mathcal{F}_1) \cap G(\mathcal{G}/\mathcal{F}_2)$ , and  $G(\mathcal{G}/\mathcal{F}_1 \cap \mathcal{F}_2)$  is the smallest  $\mathcal{C}$ -subgroup of  $G(\mathcal{G}/\mathcal{F})$  containing  $G(\mathcal{G}/\mathcal{F}_1)G(\mathcal{G}/\mathcal{F}_2)$ .

*Proof* An isomorphism of  $\mathcal{G}$  leaves invariant every element of  $\mathcal{F}_1\mathcal{F}_2$  if and only if it leaves invariant every element of  $\mathcal{F}_1$  and every element of  $\mathcal{F}_2$ , whence the first assertion. The smallest  $\mathcal{C}$ -subgroup of  $G(\mathcal{G}/\mathcal{F})$  containing  $G(\mathcal{G}/\mathcal{F}_1)G(\mathcal{G}/\mathcal{F}_2)$  is of the form  $G(\mathcal{G}/\mathcal{F}')$ , where evidently  $\mathcal{F}' \subset \mathcal{F}_1$  and  $\mathcal{F}' \subset \mathcal{F}_2$ , that is,  $\mathcal{F}' \subset \mathcal{F}_1 \cap \mathcal{F}_2$ , so that  $G(\mathcal{G}/\mathcal{F}') \supset G(\mathcal{G}/\mathcal{F}_1 \cap \mathcal{F}_2)$ . On the other hand,  $G(\mathcal{G}/\mathcal{F}_1 \cap \mathcal{F}_2)$  is a  $\mathcal{C}$ -subgroup of  $G(\mathcal{G}/\mathcal{F})$  containing  $G(\mathcal{G}/\mathcal{F}_1)$  and  $G(\mathcal{G}/\mathcal{F}_2)$ , so that  $G(\mathcal{G}/\mathcal{F}') \subset G(\mathcal{G}/\mathcal{F}_1 \cap \mathcal{F}_2)$ .

**Theorem 4** Let  $\mathcal{G}$  be a strongly normal extension of  $\mathcal{F}$  with field of constants  $\mathcal{C}$ , and let  $\mathcal{F}_1$  be an intermediate differential field. Then the following four conditions are equivalent.

- (a)  $\mathcal{F}_1$  is a strongly normal extension of  $\mathcal{F}$ .
- (b) For each element  $\alpha \in \mathcal{F}_1$  with  $\alpha \notin \mathcal{F}$ , there exists a strong isomorphism  $\sigma_1$  of  $\mathcal{F}_1$  over  $\mathcal{F}$  such that  $\sigma_1\alpha \neq \alpha$ .
- (c)  $G(\mathcal{G}/\mathcal{F}_1)$  is a normal subgroup of  $G(\mathcal{G}/\mathcal{F})$ .
- (d)  $\sigma\mathcal{F}_1 \subset \mathcal{F}_1\mathcal{K}$  for every  $\sigma \in G(\mathcal{G}/\mathcal{F})$ .

When these conditions are satisfied, then, for each  $\sigma \in G(\mathcal{G}/\mathcal{F})$ , the restriction  $\sigma_1$  of  $\sigma$  to  $\mathcal{F}_1$  is an element of  $G(\mathcal{F}_1/\mathcal{F})$ , and the formula  $\sigma \mapsto \sigma_1$  defines a surjective  $\mathcal{C}$ -homomorphism  $G(\mathcal{G}/\mathcal{F}) \rightarrow G(\mathcal{F}_1/\mathcal{F})$  with kernel  $G(\mathcal{G}/\mathcal{F}_1)$ .

*Proof* If (a) is satisfied, then, by Theorem 3, the set of invariants of  $G(\mathcal{F}_1/\mathcal{F})$  in  $\mathcal{F}_1$  is  $\mathcal{F}$ , so that (b) is satisfied. Let (b) be satisfied. The normalizer  $N$  of  $G(\mathcal{G}/\mathcal{F}_1)$  in  $G(\mathcal{G}/\mathcal{F})$  is a  $\mathcal{C}$ -subgroup of  $G(\mathcal{G}/\mathcal{F})$  containing  $G(\mathcal{G}/\mathcal{F}_1)$  (see Chapter V, Section 10, Corollary 2 to Proposition 13). By Theorem 3, there exists a differential field  $\mathcal{F}_2$  with  $\mathcal{F} \subset \mathcal{F}_2 \subset \mathcal{F}_1$  such that  $G(\mathcal{G}/\mathcal{F}_2) = N$ . If  $\sigma_1$  is any strong isomorphism of  $\mathcal{F}_1$  over  $\mathcal{F}$ ,  $\sigma_1$  can be extended to an isomorphism of  $\mathcal{G}$ , that is, to an element  $\sigma \in G(\mathcal{G}/\mathcal{F})$ . Then, for any  $\tau \in G(\mathcal{G}/\mathcal{F}_1)$  and any  $\beta \in \mathcal{F}_1$ ,  $\sigma\beta = \sigma_1\beta \in \mathcal{F}_1\mathcal{K}$ , whence  $\tau\sigma\beta = \sigma\beta$  and  $\sigma^{-1}\tau\sigma\beta = \beta$ , so that  $\sigma^{-1}\tau\sigma \in G(\mathcal{G}/\mathcal{F}_1)$ . Thus,  $\sigma \in N = G(\mathcal{G}/\mathcal{F}_2)$ , so that  $\sigma_1$  leaves invariant every element of  $\mathcal{F}_2$ . It follows by (b) that  $\mathcal{F}_2 = \mathcal{F}$ , that is,  $N = G(\mathcal{G}/\mathcal{F})$ , and therefore (c) is satisfied. Next, let (c) be satisfied. Consider any  $\sigma \in G(\mathcal{G}/\mathcal{F})$  and any  $\beta \in \mathcal{F}_1$ . For every  $\tau \in G(\mathcal{G}/\mathcal{F}_1)$ , we have  $\sigma^{-1}\tau\sigma \in G(\mathcal{G}/\mathcal{F}_1)$ , so that  $\sigma^{-1}\tau\sigma\beta = \beta$  and  $\tau\sigma\beta = \sigma\beta$ . Since by Section 3, Theorem 2, we can write  $G(\mathcal{G}/\mathcal{F}_1) = G(\mathcal{G}\mathcal{C}(\sigma)/\mathcal{F}_1\mathcal{C}(\sigma))$ , and since  $\sigma\beta \in \mathcal{G}\sigma\mathcal{G} = \mathcal{G}\mathcal{C}(\sigma)$ , we see that  $\sigma\beta$  is an invariant of  $G(\mathcal{G}\mathcal{C}(\sigma)/\mathcal{F}_1\mathcal{C}(\sigma))$  in  $\mathcal{G}\mathcal{C}(\sigma)$ , and hence, by Theorem 3, that  $\sigma\beta \in \mathcal{F}_1\mathcal{C}(\sigma)$ . Therefore (d) is satisfied. Finally, let (d) be satisfied. If  $\sigma_1$  is any isomorphism of  $\mathcal{F}_1$  over  $\mathcal{F}$ , then  $\sigma_1$  can be extended to an element  $\sigma \in G(\mathcal{G}/\mathcal{F})$ . Then because of (d),  $\sigma_1\mathcal{F}_1 = \sigma\mathcal{F}_1 \subset \mathcal{F}_1\mathcal{K}$ . It follows by Section 3, Proposition 10, that (a) is satisfied. Thus, the four conditions are equivalent.

Let the conditions be satisfied. It is obvious that the restriction mapping, defined by the formula  $\sigma \mapsto \sigma_1$ , is a group homomorphism  $G(\mathcal{G}/\mathcal{F}) \rightarrow G(\mathcal{F}_1/\mathcal{F})$  with kernel  $G(\mathcal{G}/\mathcal{F}_1)$ . We have already observed that every isomorphism of  $\mathcal{F}_1$  over  $\mathcal{F}$  can be extended to an isomorphism of  $\mathcal{G}$ , and this shows that the homomorphism is surjective. It remains to prove that it is a  $\mathcal{C}$ -homomorphism. First of all,  $\mathcal{C}(\sigma) = (\mathcal{G}\sigma\mathcal{G}) \cap \mathcal{K} \supset (\mathcal{F}_1\sigma_1\mathcal{F}_1) \cap \mathcal{K} = \mathcal{C}(\sigma_1)$ . Next, if  $\sigma'$  is a specialization of  $\sigma$ , then  $(\sigma'\alpha)_{\alpha \in \mathcal{G}}$  is a differential specialization of  $(\sigma\alpha)_{\alpha \in \mathcal{G}}$  over  $\mathcal{G}$ , so that *a fortiori*  $(\sigma_1'\alpha)_{\alpha \in \mathcal{F}_1}$  is a differential specialization of  $(\sigma_1\alpha)_{\alpha \in \mathcal{F}_1}$  over  $\mathcal{F}_1$ , that is,  $\sigma_1'$  is a specialization of  $\sigma_1$ . Finally, if  $\sigma'$  is a generic specialization of  $\sigma$ , then by the above,  $\sigma_1'$  is a generic specialization of  $\sigma_1$ . Since the induced isomorphism  $S_{\sigma', \sigma} : \mathcal{C}(\sigma) \approx \mathcal{C}(\sigma')$  is a restriction of the isomorphism  $\mathcal{G}\sigma\mathcal{G} \approx \mathcal{G}\sigma'\mathcal{G}$  over  $\mathcal{G}$  mapping  $\sigma\alpha$  onto  $\sigma'\alpha$  ( $\alpha \in \mathcal{G}$ ), and the induced isomorphism  $S_{\sigma_1', \sigma_1} : \mathcal{C}(\sigma_1) \approx \mathcal{C}(\sigma_1')$  is a

restriction of the isomorphism  $\mathcal{F}_1 \sigma_1 \mathcal{F}_1 \approx \mathcal{F}_1 \sigma_1' \mathcal{F}_1$  over  $\mathcal{F}_1$  mapping  $\sigma_1 \alpha$  onto  $\sigma_1' \alpha$  ( $\alpha \in \mathcal{F}_1$ ), it is evident that  $S_{\sigma_1, \sigma_1'}$  is an extension of  $S_{\sigma_1, \sigma_1'}$ . This shows that the restriction mapping is a  $\mathcal{C}$ -homomorphism, and completes the proof of the theorem.

**Corollary 1** Let  $\mathcal{G}$  be a strongly normal extension of  $\mathcal{F}$ , and let  $\mathcal{F}^\circ$  denote the algebraic closure of  $\mathcal{F}$  in  $\mathcal{G}$ . Then  $G(\mathcal{G}/\mathcal{F}^\circ) = G^\circ(\mathcal{G}/\mathcal{F}^\circ)$ ,  $\mathcal{F}^\circ$  is a strongly normal extension of  $\mathcal{F}$ , and  $G(\mathcal{F}^\circ/\mathcal{F}) \approx G(\mathcal{G}/\mathcal{F})/G^\circ(\mathcal{G}/\mathcal{F})$ . In particular, the degree of  $\mathcal{F}^\circ$  over  $\mathcal{F}$  equals the index of  $G^\circ(\mathcal{G}/\mathcal{F})$  in  $G(\mathcal{G}/\mathcal{F})$ , so that  $\mathcal{F}$  is algebraically closed in  $\mathcal{G}$  if and only if  $G(\mathcal{G}/\mathcal{F})$  is connected, and  $\mathcal{G}$  is algebraic over  $\mathcal{F}$  if and only if  $G(\mathcal{G}/\mathcal{F})$  is finite.

*Proof* By Section 1, part (b) of the corollary to Proposition 2, the set of invariants of  $G^\circ(\mathcal{G}/\mathcal{F})$  is  $\mathcal{F}^\circ$ , and therefore by Theorem 3,  $G^\circ(\mathcal{G}/\mathcal{F}) = G(\mathcal{G}/\mathcal{F}^\circ)$ . As  $G^\circ(\mathcal{G}/\mathcal{F})$  is a normal  $\mathcal{C}$ -subgroup of  $G(\mathcal{G}/\mathcal{F})$  (see Chapter V, Section 3, Theorem 1), Theorem 4 shows that  $\mathcal{F}^\circ$  is strongly normal over  $\mathcal{F}$  and  $G(\mathcal{F}^\circ/\mathcal{F}) \approx G(\mathcal{G}/\mathcal{F})/G^\circ(\mathcal{G}/\mathcal{F})$ .

**REMARK** The algebraic extension  $\mathcal{F}^\circ$  of  $\mathcal{F}$  need not be normal (in the usual sense). In other words, a strongly normal algebraic extension may fail to be a normal extension (see Exercise 1). However, if the field of constants  $\mathcal{C}$  is algebraically closed, then this phenomenon does not arise. In fact, if  $\mathcal{G}$  is strongly normal over  $\mathcal{F}$  and  $\mathcal{C}$  is algebraically closed, then the set of invariants in  $\mathcal{G}$  of the group of automorphisms of  $\mathcal{G}$  over  $\mathcal{F}$  is  $\mathcal{F}$ . Indeed, for any  $\alpha \in \mathcal{G}$  with  $\alpha \notin \mathcal{F}$ ,  $G(\mathcal{G}/\mathcal{F}\langle\alpha\rangle)$  is a proper  $\mathcal{C}$ -subgroup of  $G(\mathcal{G}/\mathcal{F})$ . Since the set of elements of  $G(\mathcal{G}/\mathcal{F})$  that are algebraic over  $\mathcal{C}$  is dense (see Chapter V, Section 7, corollary to Proposition 3), there exists an element  $\sigma \in G(\mathcal{G}/\mathcal{F})$  with  $\sigma \notin G(\mathcal{G}/\mathcal{F}\langle\alpha\rangle)$  such that  $\mathcal{C}(\sigma) = \mathcal{C}$ , that is, such that  $\sigma$  is an automorphism of  $\mathcal{G}$ .

**Corollary 2** Let  $\mathcal{G}_1$  and  $\mathcal{G}_2$  be strongly normal extensions of  $\mathcal{F}$  such that  $\mathcal{G}_1 \mathcal{G}_2$  and  $\mathcal{F}$  have the same field of constants  $\mathcal{C}$ . Then  $\mathcal{G}_1 \cap \mathcal{G}_2$  is a strongly normal extension of  $\mathcal{F}$ .

*Proof* By Section 3, the corollary to Proposition 10,  $\mathcal{G}_1 \mathcal{G}_2$  is strongly normal over  $\mathcal{F}$ . By Theorem 4,  $G(\mathcal{G}_1 \mathcal{G}_2/\mathcal{G}_1)$  and  $G(\mathcal{G}_1 \mathcal{G}_2/\mathcal{G}_2)$  are normal  $\mathcal{C}$ -subgroups of  $G(\mathcal{G}_1 \mathcal{G}_2/\mathcal{F})$ , so that their product is too (see Chapter V, Section 11, Corollary 2 to Theorem 7). By the corollary to Theorem 3, the product is  $G(\mathcal{G}_1 \mathcal{G}_2/\mathcal{G}_1 \cap \mathcal{G}_2)$ . Since it is normal in  $G(\mathcal{G}_1 \mathcal{G}_2/\mathcal{F})$ , it follows by Theorem 4 that  $\mathcal{G}_1 \cap \mathcal{G}_2$  is strongly normal over  $\mathcal{F}$ .

**Theorem 5** Let  $\mathcal{G}$  be a strongly normal extension of  $\mathcal{F}$  with field of constants  $\mathcal{C}$ . Let  $\mathcal{E}$  be an extension of  $\mathcal{F}$  such that  $\mathcal{U}$  is universal over  $\mathcal{E}$  and the field of

constants of  $\mathcal{G}$  is  $\mathcal{C}$ . Then  $\mathcal{G}\mathcal{E}$  is a strongly normal extension of  $\mathcal{E}$ , for each element  $\tau \in G(\mathcal{G}\mathcal{E}/\mathcal{E})$  the restriction  $\tau_1$  of  $\tau$  to  $\mathcal{G}$  is an element of  $G(\mathcal{G}/\mathcal{G} \cap \mathcal{E})$ , and the formula  $\tau \mapsto \tau_1$ , defines a  $\mathcal{C}$ -isomorphism  $G(\mathcal{G}\mathcal{E}/\mathcal{E}) \approx G(\mathcal{G}/\mathcal{G} \cap \mathcal{E})$ .

*Proof* For any isomorphism  $\tau$  of  $\mathcal{G}\mathcal{E}$  over  $\mathcal{E}$ ,  $\tau_1$  is obviously an isomorphism of  $\mathcal{G}$  over  $\mathcal{G} \cap \mathcal{E}$  and hence is a strong one. Therefore,  $\mathcal{G}\mathcal{E} \cdot \tau(\mathcal{G}\mathcal{E}) = \mathcal{G}\mathcal{E}\tau_1 \mathcal{G} \cdot \mathcal{E} = \mathcal{G}\mathcal{E}(\tau_1) \cdot \mathcal{E} = \mathcal{G}\mathcal{E}\mathcal{C}(\tau_1)$ . It follows by Section 3, Proposition 10, that  $\mathcal{G}\mathcal{E}$  is strongly normal over  $\mathcal{E}$ , and clearly the formula  $\tau \mapsto \tau_1$  defines an injective group homomorphism  $G(\mathcal{G}\mathcal{E}/\mathcal{E}) \rightarrow G(\mathcal{G}/\mathcal{G} \cap \mathcal{E})$ . It also follows that  $\mathcal{G}\mathcal{E}\mathcal{C}(\tau) = \mathcal{G}\mathcal{E}\mathcal{C}(\tau_1)$ , whence (by Chapter II, Section 1, Corollary 2 to Theorem 1)  $\mathcal{C}(\tau) = \mathcal{C}(\tau_1)$ . If  $\tau, \tau' \in G(\mathcal{G}\mathcal{E}/\mathcal{E})$  and  $\tau \rightarrow \tau'$ , then  $(\tau'\beta)_{\beta \in \mathcal{G}\mathcal{E}}$  is a differential specialization of  $(\tau\beta)_{\beta \in \mathcal{G}\mathcal{E}}$  over  $\mathcal{G}\mathcal{E}$ , so that  $(\tau'\beta)_{\beta \in \mathcal{G}}$  is a differential specialization of  $(\tau\beta)_{\beta \in \mathcal{G}}$  over  $\mathcal{G}$ , whence  $\tau_1 \rightarrow \tau'_1$ . If moreover  $\tau \leftrightarrow \tau'$ , then  $\tau_1 \leftrightarrow \tau'_1$ , and the isomorphism  $\mathcal{G}\mathcal{E}\tau(\mathcal{G}\mathcal{E}) \approx \mathcal{G}\mathcal{E}\tau'(\mathcal{G}\mathcal{E})$  over  $\mathcal{G}\mathcal{E}$  mapping  $\tau\beta$  onto  $\tau'\beta$  ( $\beta \in \mathcal{G}\mathcal{E}$ ) is an extension of the isomorphism  $\mathcal{G}\tau_1 \mathcal{G} \approx \mathcal{G}\tau'_1 \mathcal{G}$  over  $\mathcal{G}$  mapping  $\tau_1\beta$  onto  $\tau'_1\beta$  ( $\beta \in \mathcal{G}$ ). Since these two isomorphisms are extensions of the induced isomorphisms  $S_{\tau, \tau'}: \mathcal{C}(\tau) \approx \mathcal{C}(\tau')$  and  $S_{\tau_1, \tau'_1}: \mathcal{C}(\tau_1) \approx \mathcal{C}(\tau'_1)$ , and since  $\mathcal{C}(\tau) = \mathcal{C}(\tau_1)$  and  $\mathcal{C}(\tau') = \mathcal{C}(\tau'_1)$ , we see that  $S_{\tau, \tau'} = S_{\tau_1, \tau'_1}$ . It follows that the injective group homomorphism is a  $\mathcal{C}$ -homomorphism. Its image is a  $\mathcal{C}$ -subgroup  $G_1$  of  $G(\mathcal{G}/\mathcal{G} \cap \mathcal{E})$ . If an element  $\alpha \in \mathcal{G}$  is an invariant of  $G_1$ , then it is an invariant of  $G(\mathcal{G}\mathcal{E}/\mathcal{E})$ , whence  $\alpha \in \mathcal{E}$ . Thus, the set of invariants of  $G_1$  in  $\mathcal{G}$  is  $\mathcal{G} \cap \mathcal{E}$ , so that  $G_1 = G(\mathcal{G}/\mathcal{G} \cap \mathcal{E})$ . This completes the proof of the theorem.

## EXERCISES

- Let  $\mathcal{F}$  be the ordinary differential field,  $\mathbf{R}(x)$ ,  $x$  being transcendental over  $\mathbf{R}$  and the derivation operator being  $d/dx$ . Let  $\mathcal{G} = \mathcal{F}(u)$ , where  $u$  is a zero of the prime differential ideal  $[y^3 - x]$  of  $\mathcal{F}\{y\}$ . Show that  $\mathcal{G}$  is strongly normal over  $\mathcal{F}$  and that the formula  $\sigma \mapsto u^{-1}\sigma u$  defines an  $\mathbf{R}$ -isomorphism of  $G(\mathcal{G}/\mathcal{F})$  onto the  $\mathbf{R}$ -subgroup  $P_3$  of  $G_m$  consisting of the cube roots of unity.
- Let  $\mathcal{G}$  be a strongly normal extension of  $\mathcal{F}$ , and let  $\mathcal{E}$  be an extension of  $\mathcal{F}$  such that every constant in  $\mathcal{G}\mathcal{E}$  is in  $\mathcal{F}$ . Show that  $\mathcal{G}$  and  $\mathcal{E}$  are linearly disjoint over  $\mathcal{G} \cap \mathcal{E}$ .
- Let  $\mathcal{G}_1, \dots, \mathcal{G}_n$  be strongly normal extensions of  $\mathcal{F}$  with field of constants  $\mathcal{C}$ , and suppose that the field of constants of  $\mathcal{G}_1 \cdots \mathcal{G}_n$  is  $\mathcal{C}$ . For each isomorphism  $\sigma$  of  $\mathcal{G}_1 \cdots \mathcal{G}_n$  let  $\sigma_j$  denote the restriction of  $\sigma$  to  $\mathcal{G}_j$ . Show that  $\mathcal{G}_1 \cdots \mathcal{G}_n$  is strongly normal over  $\mathcal{F}$  and that the formula  $\sigma \mapsto (\sigma_1, \dots, \sigma_n)$  defines an injective  $\mathcal{C}$ -homomorphism  $G(\mathcal{G}_1 \cdots \mathcal{G}_n/\mathcal{F}) \rightarrow \prod_{1 \leq j \leq n} G(\mathcal{G}_j/\mathcal{F})$ .

5 Examples

In this section we consider some very simple examples of a strongly normal extension of the differential field  $\mathcal{F}$ . The field of constants of  $\mathcal{F}$  is denoted by  $\mathcal{C}$ .

A. The formula  $\alpha \mapsto (\delta_1 \alpha, \dots, \delta_m \alpha)$  defines a mapping  $\mathcal{U} \rightarrow \mathcal{U}^m$  that is a group homomorphism (and even a homomorphism of vector spaces over  $\mathcal{K}$ ). The kernel of this homomorphism is  $\mathcal{K}$ . An element  $\alpha \in \mathcal{U}$  is said to be *primitive* over  $\mathcal{F}$  if  $(\delta_1 \alpha, \dots, \delta_m \alpha) \in \mathcal{F}^m$ , that is, if for suitable elements  $a_1, \dots, a_m \in \mathcal{F}$ ,  $\alpha$  satisfies the system of differential equations

$$\delta_i \alpha = a_i \quad (1 \leq i \leq m).$$

When  $\alpha$  is primitive over  $\mathcal{F}$ , evidently  $\mathcal{F}\langle\alpha\rangle = \mathcal{F}(\alpha)$ .

Let  $\alpha$  be primitive over  $\mathcal{F}$  and suppose that the field of constants of  $\mathcal{F}\langle\alpha\rangle$  is  $\mathcal{C}$ . For any isomorphism  $\sigma$  of  $\mathcal{F}\langle\alpha\rangle$  over  $\mathcal{F}$ ,  $(\delta_1(\sigma\alpha), \dots, \delta_m(\sigma\alpha)) = (\sigma(\delta_1\alpha), \dots, \sigma(\delta_m\alpha)) = (\delta_1\alpha, \dots, \delta_m\alpha)$ ; hence the difference  $c(\sigma) = \sigma\alpha - \alpha$  is in the kernel. As  $\mathcal{F}\langle\alpha\rangle\sigma(\mathcal{F}\langle\alpha\rangle) = \mathcal{F}\langle\alpha\rangle\mathcal{F}\langle\alpha+c(\sigma)\rangle = \mathcal{F}\langle\alpha\rangle\mathcal{C}(c(\sigma))$ , we infer that  $\mathcal{F}\langle\alpha\rangle$  is strongly normal over  $\mathcal{F}$ , and that  $\mathcal{C}(\sigma) = \mathcal{C}(c(\sigma))$ . For two elements  $\sigma, \sigma' \in G(\mathcal{F}\langle\alpha\rangle/\mathcal{F})$ ,  $\alpha+c(\sigma\sigma') = \sigma\sigma'\alpha = \sigma(\alpha+c(\sigma')) = \alpha+c(\sigma)+c(\sigma')$ , so that  $c(\sigma\sigma') = c(\sigma)+c(\sigma')$ , and evidently  $c(\sigma) = 0$  only when  $\sigma = id_{\mathcal{F}\langle\alpha\rangle}$ . If  $\sigma'$  is a generic specialization of  $\sigma$ , then there exists an isomorphism  $\mathcal{F}\langle\alpha\rangle\mathcal{F}\langle\sigma\alpha\rangle \approx \mathcal{F}\langle\alpha\rangle\mathcal{F}\langle\sigma'\alpha\rangle$  over  $\mathcal{F}\langle\alpha\rangle$  mapping  $\sigma\alpha$  onto  $\sigma'\alpha$ , and therefore mapping  $c(\sigma)$  onto  $c(\sigma')$ ; therefore  $c(\sigma')$  is a generic specialization of  $c(\sigma)$  over  $\mathcal{C}$ , and the isomorphisms  $S_{\sigma',\sigma}$  and  $S_{c(\sigma'),c(\sigma)}$  coincide. Hence (by Chapter V, Section 9, Corollary 1 to Proposition 9)  $c$  is a  $\mathcal{C}$ -homomorphism. Thus, we have an injective  $\mathcal{C}$ -homomorphism

$$c : G(\mathcal{F}\langle\alpha\rangle/\mathcal{F}) \rightarrow (\mathbf{G}_a)_{\mathcal{X}}.$$

In particular,  $\mathcal{F}\langle\alpha\rangle$  is a  $\mathbf{G}_a$ -extension of  $\mathcal{F}$ .

As the only  $\mathcal{C}$ -subgroups of  $\mathbf{G}_a$  are 0 and  $\mathbf{G}_a$ , either  $\alpha \in \mathcal{F}$ , or else  $\alpha$  is transcendental over  $\mathcal{F}$ . In the latter case the only differential fields between  $\mathcal{F}$  and  $\mathcal{F}\langle\alpha\rangle$  are  $\mathcal{F}$  and  $\mathcal{F}\langle\alpha\rangle$ .

B. If  $\alpha$  and  $\beta$  are nonzero elements of  $\mathcal{U}$ , then  $(\alpha\beta)^{-1}\delta_i(\alpha\beta) = \alpha^{-1}\delta_i\alpha + \beta^{-1}\delta_i\beta$  ( $1 \leq i \leq m$ ). Thus, the formula  $\alpha \rightarrow (\alpha^{-1}\delta_1\alpha, \dots, \alpha^{-1}\delta_m\alpha)$  defines a group homomorphism  $\mathcal{U}^* \rightarrow \mathcal{U}^m$ . Its kernel is  $\mathcal{K}^*$ . An element  $\alpha \in \mathcal{U}^*$  is said to be *exponential* over  $\mathcal{F}$  if  $(\alpha^{-1}\delta_1\alpha, \dots, \alpha^{-1}\delta_m\alpha) \in \mathcal{F}^m$ , that is, if for suitable elements  $a_1, \dots, a_m \in \mathcal{F}$ ,  $\alpha$  satisfies the system of differential equations

$$\delta_i \alpha = a_i \alpha \quad (1 \leq i \leq m).$$

When  $\alpha$  is exponential over  $\mathcal{F}$ , then  $\mathcal{F}\langle\alpha\rangle = \mathcal{F}(\alpha)$ .

Let  $\alpha$  be exponential over  $\mathcal{F}$ , and suppose that  $\mathcal{F}\langle\alpha\rangle$  has field of constants  $\mathcal{C}$ . For any isomorphism  $\sigma$  of  $\mathcal{F}\langle\alpha\rangle$  over  $\mathcal{F}$ ,  $((\sigma\alpha)^{-1}\delta_1(\sigma\alpha), \dots, (\sigma\alpha)^{-1}\delta_m(\sigma\alpha)) = (\sigma(\alpha^{-1}\delta_1\alpha), \dots, \sigma(\alpha^{-1}\delta_m\alpha)) = (\alpha^{-1}\delta_1\alpha, \dots, \alpha^{-1}\delta_m\alpha)$ . Hence the element  $c(\sigma) = \alpha^{-1}\sigma\alpha$  is in the kernel. Just as in the case of an element primitive over  $\mathcal{F}$ , we find that  $\mathcal{F}\langle\alpha\rangle$  is strongly normal over  $\mathcal{F}$ , and that

$$c : G(\mathcal{F}\langle\alpha\rangle/\mathcal{F}) \rightarrow (\mathbf{G}_m)_{\mathcal{X}}$$

is an injective  $\mathcal{C}$ -homomorphism. Thus,  $\mathcal{F}\langle\alpha\rangle$  is a  $\mathbf{G}_m$ -extension of  $\mathcal{F}$ .

If  $\alpha$  is algebraic over  $\mathcal{F}$ , say of degree  $d$ , then  $G(\mathcal{F}\langle\alpha\rangle/\mathcal{F})$  is finite of order  $d$ . Since the only subgroup of  $\mathbf{G}_m$  of order  $d$  is the group  $P_d$  of  $d$ th roots of unity,  $G(\mathcal{F}\langle\alpha\rangle/\mathcal{F})$  is cyclic, say with generator  $\sigma$ , and  $c(\sigma)$  is a primitive  $d$ th root of unity. Then  $\sigma(\alpha^d) = (c(\sigma)\alpha)^d = \alpha^d$ , whence  $\alpha^d \in \mathcal{F}$ .

If  $\alpha$  is transcendental over  $\mathcal{F}$ , then  $c$  is a  $\mathcal{C}$ -isomorphism. For any intermediate differential field  $\mathcal{F}_1$  other than  $\mathcal{F}$ , the element  $\alpha$  is of some finite degree  $d$  over  $\mathcal{F}_1$ . The result proved for the algebraic case shows that  $\alpha^d \in \mathcal{F}_1$ , whence  $\mathcal{F}_1 = \mathcal{F}\langle\alpha^d\rangle$ . Thus, in the transcendental case the only differential fields between  $\mathcal{F}$  and  $\mathcal{F}\langle\alpha\rangle$  are the  $\mathcal{F}\langle\alpha^d\rangle$  with  $d \in \mathbf{N}$ .

C. Let  $g_2, g_3$  be elements of  $\mathcal{C}$  with  $g_2^3 - 27g_3^2 \neq 0$ , and consider the Weierstrass  $\mathcal{C}$ -group  $\mathbf{W} = \mathbf{W}(g_2, g_3)$  described in Chapter V, Section 1. Define a mapping of  $\mathbf{W}$  into  $\mathcal{U}^m$  as follows: When  $\gamma = (1:\alpha:\beta) \in \mathbf{W}$  has the property that  $\beta \neq 0$ , then  $\gamma \mapsto (\beta^{-1}\delta_1\alpha, \dots, \beta^{-1}\delta_m\alpha)$ . When  $\gamma$  is one of the three elements of  $\mathbf{W}$  of order 2 (that is, when  $\gamma = (1:\alpha:0)$  with  $\alpha$  one of the three roots of the polynomial  $4X^3 - g_2X - g_3$ ) or when  $\gamma$  is the element  $1 \in \mathbf{W}$  (that is, when  $\gamma = (0:0:1)$ ), then  $\gamma \mapsto (0, \dots, 0)$ . We claim that this mapping is a group homomorphism, the kernel obviously being  $\mathbf{W}_{\mathcal{X}}$ .

Indeed, by Chapter V, Section 18, Example 3, the Lie algebra of  $\mathbf{W}$  is  $\mathfrak{L}(\mathbf{W}) = \mathcal{U} \cdot \eta d/d\xi$ , where  $\xi, \eta$  denote the  $\mathcal{C}$ -functions on  $\mathbf{W}$  such that  $\xi(1:\alpha:\beta) = \alpha$ ,  $\eta(1:\alpha:\beta) = \beta$ , and by Chapter V, Section 22, Example 3, the logarithmic derivation  $l\delta_i : \mathbf{W} \rightarrow \mathfrak{L}(\mathbf{W})$  is given by the formula  $l\delta_i((1:\alpha:\beta)) = (\beta^{-1}\delta_i\alpha)\eta d/d\xi$  ( $\beta \neq 0$ ),  $l\delta_i(\gamma) = 0$  ( $\gamma^2 = 1$ ). Hence the claim follows from the equation  $l\delta_i(\gamma\gamma') = l\delta_i(\gamma) + l\delta_i(\gamma')$  (see Chapter V, Section 22, remark following Theorem 14).

For any element  $\alpha \in \mathcal{U}$ , there exists an element  $\beta \in \mathcal{U}$  such that the point  $\gamma = (1:\alpha:\beta)$  is an element of  $\mathbf{W}$ . Moreover,  $\beta$  is determined by  $\alpha$  up to a factor  $\pm 1$ , and hence the same is true of the image of  $\gamma$  under the homomorphism. The element  $\alpha$  is said to be *Weierstrassian* over  $\mathcal{F}$  (for the coefficients  $g_2, g_3 \in \mathcal{C}$ ) if the image of  $\gamma$  is in  $\mathcal{F}^m$ , that is, if for suitable elements  $a_1, \dots, a_m \in \mathcal{F}$ ,  $\alpha$  satisfies the system of differential equations

$$(\delta_i \alpha)^2 = a_i^2 (4\alpha^3 - g_2\alpha - g_3) \quad (1 \leq i \leq m).$$

Let  $\alpha$  be Weierstrassian over  $\mathcal{F}$  for the coefficients  $g_2, g_3$ , fix  $\beta$  and  $\gamma = (1:\alpha:\beta)$  as above, and suppose that the field of constants of  $\mathcal{F}\langle\gamma\rangle$  is  $\mathcal{C}$ .



It is easy to see that then  $\mathcal{F}\langle\gamma\rangle = \mathcal{F}\langle\alpha\rangle$ . For any isomorphism  $\sigma$  of  $\mathcal{F}\langle\alpha\rangle$  over  $\mathcal{F}$ ,  $\gamma$  and  $\sigma\gamma$  have the same image under the homomorphism  $\mathbf{W} \rightarrow \mathcal{U}^m$  because when  $\gamma = (1:\alpha:\beta)$  with  $\beta \neq 0$ , then  $(\sigma\beta)^{-1}\delta_i(\sigma\alpha) = \sigma(\beta^{-1}\delta_i\alpha) = \beta^{-1}\delta_i\alpha$ , and when  $\gamma^2 = 1$ , then  $(\sigma\gamma)^2 = 1$  so that  $\gamma$  and  $\sigma\gamma$  both have image  $(0, \dots, 0)$ . Therefore the element  $c(\sigma) = \gamma^{-1}\sigma\gamma$  of  $\mathbf{W}$  is in the kernel  $\mathbf{W}_*$ . Just as for a primitive or exponential element, we find that  $\mathcal{F}\langle\alpha\rangle$  is strongly normal over  $\mathcal{F}$  and that the mapping

$$c : G(\mathcal{F}\langle\alpha\rangle/\mathcal{F}) \rightarrow \mathbf{W}_*$$

is an injective  $\mathcal{C}$ -homomorphism. Thus,  $\mathcal{F}\langle\alpha\rangle$  is a  $\mathbf{W}$ -extension of  $\mathcal{F}$ . When  $\alpha$  is transcendental over  $\mathcal{F}$ , then  $c$  is a  $\mathcal{C}$ -isomorphism.

Let us consider the classical case in which  $\mathcal{F}$  is a differential field of meromorphic functions on some region  $R$  of complex  $m$ -space  $\mathbf{C}^m$ , and  $\mathcal{C}$  is  $\mathbf{C}$ . There exists a lattice  $\Lambda$  in  $\mathbf{C}$  such that  $\wp_\Lambda$ , the doubly periodic Weierstrass function with period group  $\Lambda$ , is a solution of the ordinary differential equation

$$y'^2 = 4y^3 - g_2y - g_3.$$

As noted in Chapter V, Section 1, the formula  $a \mapsto (1:\wp_\Lambda(a):\wp_\Lambda'(a))$  defines a surjective group homomorphism  $\mathbf{C} \rightarrow \mathbf{W}_\mathbf{C}$  with kernel  $\Lambda$ . Now consider a holomorphic function  $\xi$  on a subregion  $R'$  of  $R$ , and suppose that  $\xi$  is primitive over  $\mathcal{F}$  (when meromorphic functions on  $R$  are identified with their restrictions to  $R'$ ). Then the composite function  $\wp_\Lambda(\xi) = \wp_\Lambda \circ \xi$  on  $R'$  is Weierstrassian over  $\mathcal{F}$  for the coefficients  $g_2, g_3$ , and  $\gamma = (1:\wp_\Lambda(\xi):\wp_\Lambda'(\xi))$  is an element of  $\mathbf{W}$ . The differential field  $\mathcal{F}\langle\wp_\Lambda(\xi)\rangle$  contains  $\varphi(\xi)$  for every meromorphic function  $\varphi$  on  $\mathbf{C}$  admitting all the elements of  $\Lambda$  as periods. For any  $\sigma \in G_\mathbf{C}(\mathcal{F}\langle\wp_\Lambda(\xi)\rangle/\mathcal{F})$  we have  $\sigma\gamma = \gamma c(\sigma)$  with  $c(\sigma) \in \mathbf{W}_\mathbf{C}$ , and we can fix  $a \in \mathbf{C}$  such that  $(1:\wp_\Lambda(a):\wp_\Lambda'(a)) = c(\sigma)$ . Then  $\sigma(1:\wp_\Lambda(\xi):\wp_\Lambda'(\xi)) = \sigma\gamma = \gamma c(\sigma) = (1:\wp_\Lambda(\xi):\wp_\Lambda'(\xi))(1:\wp_\Lambda(a):\wp_\Lambda'(a)) = (1:\wp_\Lambda(\xi+a):\wp_\Lambda'(\xi+a))$ , so that  $\sigma(\wp_\Lambda(\xi)) = \wp_\Lambda(\xi+a)$ , whence  $\varphi(\xi) = \varphi(\xi+a)$  for every meromorphic function  $\varphi$  on  $\mathbf{C}$  admitting the elements of  $\Lambda$  as periods.

If  $\wp_\Lambda(\xi)$  is algebraic over  $\mathcal{F}$ , then  $G(\mathcal{F}\langle\wp_\Lambda(\xi)\rangle/\mathcal{F})$  is finite and the numbers  $a \in \mathbf{C}$  such that  $\wp_\Lambda(\xi+a) = \sigma(\wp_\Lambda(\xi))$  for some  $\sigma \in G(\mathcal{F}\langle\wp_\Lambda(\xi)\rangle/\mathcal{F})$  form a subgroup  $\Lambda'$  of  $\mathbf{C}$  with  $\Lambda' \supset \Lambda$  and  $\Lambda'/\Lambda$  isomorphic to  $G(\mathcal{F}\langle\wp_\Lambda(\xi)\rangle/\mathcal{F})$ . Now,  $\wp_\Lambda$  is a meromorphic function on  $\mathbf{C}$ , admitting the elements of  $\Lambda$  as periods, and hence  $\wp_\Lambda(\xi) \in \mathcal{F}\langle\wp_\Lambda(\xi)\rangle$ . Because  $\wp_\Lambda(\xi+a) = \wp_\Lambda(\xi)$  for every  $a \in \Lambda'$ ,  $\wp_\Lambda(\xi)$  is invariant under the Galois group, whence  $\wp_\Lambda(\xi) \in \mathcal{F}$ . Conversely, if  $\Lambda'$  is a lattice,  $\Lambda' \supset \Lambda$ , and  $\wp_{\Lambda'}(\xi) \in \mathcal{F}$ , and if  $\Lambda'$  is minimal with this property, then it is easy to see that  $\wp_\Lambda(\xi)$  is algebraic over  $\mathcal{F}$  and  $G(\mathcal{F}\langle\wp_\Lambda(\xi)\rangle/\mathcal{F})$  is isomorphic to  $\Lambda'/\Lambda$ .

If  $\wp_\Lambda(\xi)$  is transcendental over  $\mathcal{F}$ , then  $G_\mathbf{C}(\mathcal{F}\langle\wp_\Lambda(\xi)\rangle/\mathcal{F}) \approx \mathbf{W}_\mathbf{C} \approx \mathbf{C}/\Lambda$ . The proper  $\mathbf{C}$ -subgroups of  $\mathbf{W}$  are finite and therefore correspond to the

lattices  $\Lambda'$  in  $\mathbf{C}$  such that  $\Lambda' \supset \Lambda$ . The differential fields  $\mathcal{F}\langle\wp_{\Lambda'}(\xi)\rangle$  are between  $\mathcal{F}$  and  $\mathcal{F}\langle\wp_\Lambda(\xi)\rangle$ , and there are no others.

### EXERCISES

In all the following exercises the field of constants of the differential field  $\mathcal{F}$  is denoted by  $\mathcal{C}$ .

- Let  $\mathfrak{I}$  denote the set of all points  $(a_1, \dots, a_m) \in \mathcal{U}^m$  that satisfy the integrability conditions  $\delta_i a_j = \delta_j a_i$  ( $1 \leq i \leq m, 1 \leq j \leq m$ ).
  - Show that  $\mathfrak{I}$  is the image of the homomorphism  $\mathcal{U} \rightarrow \mathcal{U}^m$  introduced in Subsection A. (*Hint:* Use Chapter IV, Section 9, Lemma 2.)
  - Show that if  $(a_1, \dots, a_m) \in \mathfrak{I} \cap \mathcal{F}^m$ , then there exists an element  $\alpha \in \mathcal{U}$ , with  $\alpha \mapsto (a_1, \dots, a_m)$  under the homomorphism, such that either  $\alpha$  is transcendental over  $\mathcal{F}$  and the field of constants of  $\mathcal{F}\langle\alpha\rangle$  is  $\mathcal{C}$ , or  $\alpha \in \mathcal{F}$ . (*Hint:* Use part (a) and Chapter III, Section 10, Proposition 7(d), to find an  $\alpha$  such that every constant in  $\mathcal{F}\langle\alpha\rangle$  is algebraic over  $\mathcal{F}$ . When  $\alpha$  is transcendental show that this  $\alpha$  suffices, and when  $\alpha$  is algebraic of degree  $n$  replace  $\alpha$  by  $n^{-1}$  times its trace.)
- Let  $\mathfrak{I}$  have the same meaning as in Exercise 1.
  - Show that  $\mathfrak{I}$  is the image of the homomorphism  $\mathcal{U}^* \rightarrow \mathcal{U}^m$  introduced in Subsection B.
  - Show that if  $(a_1, \dots, a_m) \in \mathfrak{I} \cap \mathcal{F}^m$ , then there exists an element  $\alpha \in \mathcal{U}^*$ , with  $\alpha \mapsto (a_1, \dots, a_m)$  under the homomorphism, such that the field of constants of  $\mathcal{F}\langle\alpha\rangle$  is  $\mathcal{C}$  and, either  $\alpha$  is transcendental over  $\mathcal{F}$ , or  $\alpha$  is algebraic over  $\mathcal{F}$  of some degree  $n$  and  $\alpha^n \in \mathcal{F}$ . (*Hint:* If there exists an algebraic nonzero  $\alpha$ , choose one of minimal degree  $n$ . Replacing  $\alpha$  by an  $n$ th root of its norm, show that  $\alpha^n \in \mathcal{F}$ . Then show that every constant in  $\mathcal{F}\langle\alpha\rangle = \sum_{0 \leq j < n} \mathcal{F}\alpha^j$  is in  $\mathcal{F}$ .)
- Let  $\mathfrak{I}$  have the same meaning as in Exercise 1.
  - Show that  $\mathfrak{I}$  is the image of the homomorphism  $\mathbf{W} \rightarrow \mathcal{U}^m$  introduced in Subsection C.
  - Show that if  $(a_1, \dots, a_m) \in \mathfrak{I} \cap \mathcal{F}^m$  and  $(a_1, \dots, a_m) \neq (0, \dots, 0)$ , then there exists a  $\gamma = (1:\alpha:\beta) \in \mathbf{W}$ , with  $\beta \neq 0$  and with  $\gamma \mapsto (a_1, \dots, a_m)$  under the homomorphism, such that either  $\alpha$  is transcendental over  $\mathcal{F}$  and the field of constants of  $\mathcal{F}\langle\gamma\rangle$  is  $\mathcal{C}$ , or  $\alpha$  is algebraic over  $\mathcal{F}$  and  $\gamma^n \in \mathbf{W}_\mathcal{F}$  for some nonzero  $n \in \mathbf{N}$ . Show that when  $\mathcal{C}$  is algebraically closed then  $\gamma$  can always be chosen so that the field of constants of  $\mathcal{F}\langle\gamma\rangle$  is  $\mathcal{C}$ .
- (Ostrowski [32a], Kolchin [21]) Let the elements  $\alpha_1, \dots, \alpha_n \in \mathcal{U}$  be algebraically dependent over  $\mathcal{F}$ , and suppose that the field of constants of  $\mathcal{F}\langle\alpha_1, \dots, \alpha_n\rangle$  is  $\mathcal{C}$ .

- (a) Prove that if  $\alpha_1, \dots, \alpha_n$  are primitive over  $\mathcal{F}$ , then there exist constants  $c_1, \dots, c_n \in \mathcal{C}$  not all 0 and an element  $a \in \mathcal{F}$  such that  $\sum c_j \alpha_j = a$ . (*Hint*: Use Example A and Section 4, Exercise 3, to show that  $\mathcal{F}\langle\alpha_1, \dots, \alpha_n\rangle$  is strongly normal over  $\mathcal{F}$  and that the formula  $\sigma \mapsto (\sigma\alpha_1 - \alpha_1, \dots, \sigma\alpha_n - \alpha_n)$  defines a  $\mathcal{C}$ -isomorphism of the Galois group onto a proper  $\mathcal{C}$ -subgroup of  $(G_n^n)_{\mathcal{X}}$ , and hence (see Chapter V, Section 23, Subsection D) into some hyperplane  $\sum c_j X_j = 0$  with  $c_1, \dots, c_n \in \mathcal{C}$ . Then consider the element  $\sum c_j \alpha_j$ .)
- (b) Prove that if  $\alpha_1, \dots, \alpha_n$  are exponential over  $\mathcal{F}$ , then there exist numbers  $e_1, \dots, e_n \in \mathbb{Z}$  not all 0 and an element  $a \in \mathcal{F}^*$  such that  $\prod \alpha_j^{e_j} = a$ .
- (c) Prove that if  $\alpha_1, \dots, \alpha_n$  are Weierstrassian over  $\mathcal{F}$  for coefficients  $g_2, g_3 \in \mathcal{C}$  and  $\alpha_1, \dots, \alpha_n \notin \mathcal{C}$ , and if we fix  $\beta_j \in \mathcal{U}$  so that  $\gamma_j = (1: \alpha_j: \beta_j)$  is a point of  $\mathbf{W}(g_2, g_3)$ , and if  $\mathbf{W}(g_1, g_2)$  is without complex multiplication (see Chapter V, Section 24), then there exist numbers  $e_1, \dots, e_n \in \mathbb{Z}$  not all 0 and an element  $w \in \mathbf{W}_{\mathcal{F}}(g_2, g_3)$  such that  $\prod \gamma_j^{e_j} = w$ . (*Hint*: See Chapter V, Section 23, Exercise 7(d).)
- (d) Let  $k, l \in \mathbb{N}$  and  $k \leq l \leq n$ . Prove that if  $\alpha_1, \dots, \alpha_k$  are primitive over  $\mathcal{F}$  and  $\alpha_{k+1}, \dots, \alpha_l$  are exponential over  $\mathcal{F}$  and  $\alpha_{l+1}, \dots, \alpha_n$  are nonconstant and Weierstrassian over  $\mathcal{F}$ , then either  $\alpha_1, \dots, \alpha_k$  are algebraically dependent over  $\mathcal{F}$ , or  $\alpha_{k+1}, \dots, \alpha_l$  are, or  $\alpha_{l+1}, \dots, \alpha_n$  are.
5. (Kolchin [16]) (a) An extension  $\mathcal{L}$  of  $\mathcal{F}$  is *Liouvillian* if there exist elements  $\alpha_1, \dots, \alpha_r$  with  $\mathcal{F}\langle\alpha_1, \dots, \alpha_r\rangle = \mathcal{L}$  such that, for every index  $k$ ,  $\alpha_k$  is primitive or exponential or algebraic over  $\mathcal{F}\langle\alpha_1, \dots, \alpha_{k-1}\rangle$ . Let  $\mathcal{G}$  be an extension of  $\mathcal{F}$  with field of constants  $\mathcal{C}$ , and suppose that  $\mathcal{C}$  is algebraically closed. Prove that if  $\mathcal{G}$  is contained in a Liouvillian extension of  $\mathcal{F}$ , then  $\mathcal{G}$  is contained in a Liouvillian extension of  $\mathcal{F}$  that has field of constants  $\mathcal{C}$ . (*Hint*: Write  $\mathcal{G} \subset \mathcal{L}$  with  $\mathcal{L} = \mathcal{F}\langle\alpha_1, \dots, \alpha_r\rangle$  as above, show that  $(\alpha_1, \dots, \alpha_r)$  can be replaced by a suitably constrained differential specialization of  $(\alpha_1, \dots, \alpha_r)$  over  $\mathcal{C}$ , and apply Chapter III, Section 10, Proposition 7(d).)
- (b) If in the definition given in part (a) the expression "primitive or exponential or algebraic" is replaced by the  $i$ th expression in the list:
- (1) primitive or exponential or algebraic,
  - (2) primitive or exponential,
  - (3) exponential or algebraic,
  - (4) primitive or algebraic,
  - (5) exponential,
  - (6) primitive,
  - (7) algebraic,

then  $\mathcal{L}$  is a Liouvillian extension of  $\mathcal{F}$  of type (i). Refine the result of part (a) to take account of this hierarchy of types.

## 6 Picard-Vessiot extensions

Denote the set of all  $n \times n$  matrices over  $\mathcal{U}$  by  $\mathbf{M}(n)$  and, for any subfield  $K$  of  $\mathcal{U}$ , let  $\mathbf{M}_K(n)$  denote the set of elements of  $\mathbf{M}(n)$  that have all their coordinates in  $K$ . For any  $\alpha = (\alpha_{jj}) \in \mathbf{M}(n)$  and any  $\delta \in \Delta$ , set  $\delta\alpha = (\delta\alpha_{jj})$ . It is easy to verify that  $\delta(\alpha\beta) = \delta\alpha \cdot \beta + \alpha \cdot \delta\beta$  for all  $\alpha, \beta \in \mathbf{M}(n)$ . Of course,  $\mathbf{M}(n)$  is a vector space over  $\mathcal{U}$  isomorphic to  $\mathcal{U}^{n^2}$ .

The group  $\mathbf{GL}(n)$  of invertible  $n \times n$  matrices over  $\mathcal{U}$  operates on the left on the vector space  $\mathbf{M}(n)$ , or more generally, on the vector space  $\mathbf{M}(n)^k = \mathbf{M}(n) \times \dots \times \mathbf{M}(n)$  for any  $k \in \mathbb{N}$ , by the formula

$$(\alpha, (\xi_1, \dots, \xi_k)) \mapsto T_\alpha(\xi_1, \dots, \xi_k),$$

where  $T_\alpha$  denotes the automorphism of  $\mathbf{M}(n)^k$  defined by the formula

$$T_\alpha(\xi_1, \dots, \xi_k) = (\alpha\xi_1\alpha^{-1}, \dots, \alpha\xi_k\alpha^{-1}).$$

Consider the mapping  $f: \mathbf{GL}(n) \rightarrow \mathbf{M}(n)^m$  defined by the formula

$$f(\alpha) = (\delta_1\alpha\alpha^{-1}, \dots, \delta_m\alpha\alpha^{-1}).$$

A trivial computation shows that

$$f(\alpha\beta) = f(\alpha) + T_\alpha f(\beta) \quad (\alpha, \beta \in \mathbf{GL}(n)).$$

Thus  $f$  is a crossed homomorphism of the group  $\mathbf{GL}(n)$  into the additive group  $\mathbf{M}(n)^m$  for the indicated operation of  $\mathbf{GL}(n)$  on  $\mathbf{M}(n)^m$ . The kernel of  $f$  is  $\mathbf{GL}_{\mathcal{X}}(n)$ . When  $n = 1$  the operation is trivial and the crossed homomorphism is a homomorphism (which we have already met in Section 5, Subsection B), but when  $n > 1$  the operation is not trivial and  $f$  is not a homomorphism.

Suppose that the matrix  $\alpha \in \mathbf{GL}(n)$  satisfies the condition  $f(\alpha) \in \mathbf{M}_{\mathcal{F}}(n)^m$ , that is, that the  $n^2$  coordinates  $\alpha_{jj}$  of  $\alpha$  satisfy a system of  $mn^2$  linear differential equations

$$\delta_i \alpha = a_i \alpha \quad (1 \leq i \leq m)$$

for suitable matrices  $a_1, \dots, a_m \in \mathbf{M}_{\mathcal{F}}(n)$ . If  $\sigma$  is any isomorphism of  $\mathcal{F}\langle\alpha\rangle$  over  $\mathcal{F}$ , then the matrix  $\sigma\alpha = (\sigma\alpha_{jj})$  is an element of  $\mathbf{GL}(n)$  and  $f(\sigma\alpha) = \sigma f(\alpha) = f(\alpha)$ . Hence, if we set  $c(\sigma) = \alpha^{-1}\sigma\alpha$ , so that  $\sigma\alpha = \alpha c(\sigma)$ , then  $c(\sigma)$  is in the kernel of  $f$ , that is,  $c(\sigma) \in \mathbf{GL}_{\mathcal{X}}(n)$ . Just as in the examples in Section 5, we infer that if the field of constants of  $\mathcal{F}\langle\alpha\rangle$  is  $\mathcal{C}$ , the field of constants of  $\mathcal{F}$ , then  $\mathcal{F}\langle\alpha\rangle$  is a strongly normal extension of  $\mathcal{F}$  and the mapping

$$c: G(\mathcal{F}\langle\alpha\rangle/\mathcal{F}) \rightarrow \mathbf{GL}_{\mathcal{X}}(n)$$

is an injective  $\mathcal{C}$ -homomorphism. In particular, then  $\mathcal{F}\langle\alpha\rangle$  is a  $\mathbf{GL}(n)$ -extension of  $\mathcal{F}$ .

An extension  $\mathcal{G}$  of  $\mathcal{F}$  having the two properties, that the field of constants of  $\mathcal{G}$  is  $\mathcal{C}$ , and that, for some  $n \in \mathbf{N}$ , there exists an  $\alpha \in \mathbf{GL}(n)$  such that  $\delta_i \alpha \cdot \alpha^{-1} \in \mathbf{M}_{\mathcal{F}}(n)$  ( $1 \leq i \leq n$ ) and  $\mathcal{F}\langle \alpha \rangle = \mathcal{G}$ , is called a *Picard-Vessiot extension* of  $\mathcal{F}$ . By what we have just seen, every Picard-Vessiot extension of  $\mathcal{F}$  is a linear extension of  $\mathcal{F}$ . It is obvious that if  $\mathcal{G}$  is a Picard-Vessiot extension of  $\mathcal{F}$ , and  $\mathcal{F}_1$  is a differential field with  $\mathcal{F} \subset \mathcal{F}_1 \subset \mathcal{G}$ , then  $\mathcal{G}$  is a Picard-Vessiot extension of  $\mathcal{F}_1$ .

Picard-Vessiot extensions can be characterized in another way. Let the  $n$  elements  $\eta_j = (\eta_{j1}, \dots, \eta_{jr}) \in \mathcal{U}^r$  ( $1 \leq j \leq n$ ) form a fundamental system of zeros of a linear differential ideal of  $\mathcal{F}\{y_1, \dots, y_r\}$  of finite linear dimension  $n$  (see Chapter IV, Section 5). By Chapter II, Section 1, Theorem 1, we can fix derivative operators  $\theta_1, \dots, \theta_n \in \Theta$ , and integers  $k(1), \dots, k(n)$  between 1 and  $r$  inclusive, such that the matrix  $\alpha = (\theta_h \eta_{j, k(h)})_{1 \leq h \leq n, 1 \leq j \leq n}$  is in  $\mathbf{GL}(n)$ . By Chapter IV, Section 5, Corollary 3 to Proposition 2,  $\delta_i \alpha \cdot \alpha^{-1} \in \mathbf{M}_{\mathcal{F}}(n)$  for every  $i$ . Furthermore, if  $\beta_k$  denotes the matrix obtained when the first row in  $\alpha$  is replaced by  $(\eta_{1k}, \dots, \eta_{nk})$ , then  $\beta_k \alpha^{-1} \in \mathbf{M}_{\mathcal{F}}(n)$ , so that  $\mathcal{F}\langle \alpha \rangle = \mathcal{F}\langle \eta_1, \dots, \eta_n \rangle$ . Hence, if the field of constants of  $\mathcal{F}\langle \eta_1, \dots, \eta_n \rangle$  is  $\mathcal{C}$ , then  $\mathcal{F}\langle \eta_1, \dots, \eta_n \rangle$  is a Picard-Vessiot extension of  $\mathcal{F}$ .

Conversely, let  $\mathcal{F}\langle \alpha \rangle$  be any Picard-Vessiot extension of  $\mathcal{F}$ , where  $\alpha = (\alpha_{ji}) \in \mathbf{GL}(n)$  and  $\delta_i \alpha \cdot \alpha^{-1} \in \mathbf{M}_{\mathcal{F}}(n)$  ( $1 \leq i \leq n$ ). We claim, first, that this extension is generated by a fundamental system of zeros of a linear differential ideal of  $\mathcal{F}\{y_1, \dots, y_n\}$  of linear dimension  $n$ , and second, that it is generated by a fundamental system of zeros of a linear differential ideal of  $\mathcal{F}\{y\}$  of linear dimension less than or equal to  $n^2$ . Indeed, for every  $\sigma \in G(\mathcal{F}\langle \alpha \rangle / \mathcal{F})$ ,  $\sigma \alpha = \alpha c(\sigma)$ , where  $c(\sigma) \in \mathbf{GL}_K(n)$ . It follows that for any  $\theta_1, \dots, \theta_n \in \Theta$  and any indices  $k(1), \dots, k(n)$ , the matrix  $\beta = (\theta_h \alpha_{k(h)j})_{1 \leq h \leq n, 1 \leq j \leq n}$  has the property that  $\sigma \beta = \beta c(\sigma)$ , so that  $\sigma(\beta \alpha^{-1}) = \beta \alpha^{-1}$ , whence  $\beta \alpha^{-1} \in \mathbf{M}_{\mathcal{F}}(n)$ . Hence by Chapter IV, Section 5, Corollary 3 to Proposition 2, the  $n$  columns of  $\alpha$  form a fundamental system of zeros of a linear differential ideal of  $\mathcal{F}\{y_1, \dots, y_n\}$  of linear dimension  $n$ . This establishes the first claim. Further, if we fix a maximal set of the elements  $\alpha_{ji}$  that is linearly independent over constants, and denote the elements of this set by  $\eta_1, \dots, \eta_l$ , then  $\mathcal{F}\langle \eta_1, \dots, \eta_l \rangle = \mathcal{F}\langle \alpha \rangle$  and (since each  $\sigma \alpha_{ji}$  is a linear combination over  $\mathcal{K}$  of all the elements  $\alpha_{ji}$ )  $\sigma \eta_i = \sum_{1 \leq h \leq l} \eta_h d_{hi}(\sigma)$  ( $1 \leq i \leq l$ ), where the matrix  $d(\sigma) = (d_{hi}(\sigma))$  is in  $\mathbf{M}_{\mathcal{F}}(l)$ ; for any  $\theta_1, \dots, \theta_l \in \Theta$  evidently  $\sigma(\theta_h \eta_i) = (\theta_h \eta_i) d(\sigma)$ . Fixing  $\theta'_1, \dots, \theta'_l \in \Theta$  such that  $\det(\theta'_h \eta_i) \neq 0$ , we infer first that  $d(\sigma)$  is invertible, so that  $d(\sigma) \in \mathbf{GL}_{\mathcal{K}}(l)$ , and second that  $\sigma((\theta_h \eta_i)(\theta'_h \eta_i)^{-1}) = (\theta_h \eta_i)(\theta'_h \eta_i)^{-1}$ , so that  $(\theta_h \eta_i)(\theta'_h \eta_i)^{-1} \in \mathbf{M}_{\mathcal{F}}(l)$  for all  $\theta_1, \dots, \theta_l \in \Theta$ . Hence by Chapter IV, Section 5, Corollary 3 to Proposition 2, the elements  $\eta_1, \dots, \eta_l$  form a fundamental system of zeros of a linear differential ideal of  $\mathcal{F}\{y\}$  of linear dimension  $l \leq n^2$ . This established the second claim.

Thus, we have the following characterization:  $\mathcal{G}$  is a *Picard-Vessiot extension* of  $\mathcal{F}$  if and only if  $\mathcal{G}$  has the same field of constants as  $\mathcal{F}$  and, for some natural number  $r \geq 1$ ,  $\mathcal{G}$  is an extension of  $\mathcal{F}$  generated by a fundamental system of zeros of a linear differential ideal of  $\mathcal{F}\{y_1, \dots, y_r\}$  of finite linear dimension. Furthermore, when this is the case then  $r$  can be taken equal to 1. When  $\mathcal{G}$  is a Picard-Vessiot extension of  $\mathcal{F}$ , and the  $n$  elements  $\eta_1, \dots, \eta_n \in \mathcal{U}^r$  form a fundamental system of zeros of a linear differential ideal  $I$  of  $\mathcal{F}\{y_1, \dots, y_r\}$  such that  $\mathcal{F}\langle \eta_1, \dots, \eta_n \rangle = \mathcal{G}$ , then the equations

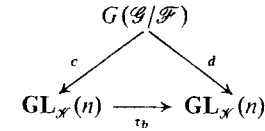
$$\sigma \eta_{j'} = \sum_{1 \leq j \leq n} \eta_j c_{jj'}(\sigma) \quad (1 \leq j' \leq n), \quad c(\sigma) = (c_{jj'}(\sigma))_{1 \leq j \leq n, 1 \leq j' \leq n}$$

define an injective  $\mathcal{C}$ -homomorphism

$$c : G(\mathcal{G}/\mathcal{F}) \rightarrow \mathbf{GL}_{\mathcal{K}}(n)$$

which we call the *representation of  $G(\mathcal{G}/\mathcal{F})$  associated with the fundamental system  $(\eta_1, \dots, \eta_n)$* . The image of  $c$ , which is a  $\mathcal{C}$ -subgroup of  $\mathbf{GL}_{\mathcal{K}}(n)$ , we call the *Galois group of  $I$  relative to  $(\eta_1, \dots, \eta_n)$* . If  $\Lambda$  is any subset of  $I$  with  $[\Lambda] = I$ , we refer to the Galois group of  $I$  relative to  $(\eta_1, \dots, \eta_n)$  also as the *Galois group of  $\Lambda$  over  $\mathcal{F}$  relative to  $(\eta_1, \dots, \eta_n)$* .

If  $(\eta_1, \dots, \eta_n)$  and  $(\zeta_1, \dots, \zeta_n)$  are two fundamental systems of zeros of a linear differential ideal  $I$  of  $\mathcal{F}\{y_1, \dots, y_r\}$ , generating the same Picard-Vessiot extension  $\mathcal{G}$  of  $\mathcal{F}$ , then there exists a matrix  $b = (b_{jj'}) \in \mathbf{GL}_{\mathcal{C}}(n)$  such that  $\eta_{j'} = \sum_{1 \leq j \leq n} \zeta_j b_{jj'}$  ( $1 \leq j' \leq n$ ). Letting  $c$  and  $d$  denote the representations of  $G(\mathcal{G}/\mathcal{F})$  associated with  $(\eta_1, \dots, \eta_n)$  and  $(\zeta_1, \dots, \zeta_n)$ , respectively, we find that  $d(\sigma) = bc(\sigma)b^{-1}$  ( $\sigma \in G(\mathcal{G}/\mathcal{F})$ ), that is, that the accompanying diagram (in which  $\tau_b$  denotes the inner automorphism of  $\mathbf{GL}_{\mathcal{K}}(n)$  determined by  $b$ ) is commutative.



This shows that, given  $\mathcal{G}$  and  $I$ , the Galois group of  $I$  relative to an unspecified fundamental system of zeros generating  $\mathcal{G}$  is unique up to conjugation of  $\mathbf{GL}_{\mathcal{K}}(n)$  by a matrix of  $\mathbf{GL}_{\mathcal{C}}(n)$ .

Now, a given linear differential ideal  $I$  of  $\mathcal{F}\{y_1, \dots, y_r\}$  of finite linear dimension  $n$  need not have a fundamental system of zeros that generates a Picard-Vessiot extension of  $\mathcal{F}$ , that is,  $I$  may have the property that the extension of  $\mathcal{F}$  generated by any fundamental system of zeros of  $I$  contains constants not contained in  $\mathcal{C}$  (see Exercise 1). Furthermore, even when  $I$  has a fundamental system of zeros that generates a Picard-Vessiot extension of  $\mathcal{F}$ , different such fundamental systems will in general generate different

Picard-Vessiot extensions. The following proposition shows that when  $\mathcal{C}$  is algebraically closed then the first difficulty does not arise, and, in any case, that the Galois group of  $\mathcal{I}$ , relative to a fundamental system of zeros that generates a Picard-Vessiot extension of  $\mathcal{F}$ , is (when such a fundamental system exists) determined by  $\mathcal{I}$  up to an inner automorphism  $\tau_b$  of  $\text{GL}_{\mathcal{X}}(n)$  with  $b \in \text{GL}_{\mathcal{C}_a}(n)$  (where, as usual,  $\mathcal{C}_a$  denotes the algebraic closure of  $\mathcal{C}$ ).

**Proposition 13** *Let  $\mathcal{I}$  be a linear differential ideal of  $\mathcal{F}\{y_1, \dots, y_n\}$  of finite linear dimension  $n$ . Denote the field of constants of  $\mathcal{F}$  by  $\mathcal{C}$ .*

(a) *If  $\mathcal{C}$  is algebraically closed, then  $\mathcal{I}$  has a fundamental system of zeros that generates a Picard-Vessiot extension of  $\mathcal{F}$ .*

(b) *If  $(\eta_1, \dots, \eta_n)$  and  $(\zeta_1, \dots, \zeta_n)$  are two fundamental systems of zeros of  $\mathcal{I}$  respectively generating the Picard-Vessiot extensions  $\mathcal{G}$  and  $\mathcal{H}$  of  $\mathcal{F}$ , and if  $c$  and  $d$  denote the representations of  $G(\mathcal{G}/\mathcal{F})$  and  $G(\mathcal{H}/\mathcal{F})$  respectively associated with these fundamental systems, then there exist an isomorphism  $\varphi: \mathcal{G}\mathcal{C}_a \approx \mathcal{H}\mathcal{C}_a$  over  $\mathcal{F}\mathcal{C}_a$  and a matrix  $b \in \text{GL}_{\mathcal{C}_a}(n)$  such that the diagram*

$$\begin{array}{ccc} G(\mathcal{G}\mathcal{C}_a/\mathcal{F}\mathcal{C}_a) & \xrightarrow{T_\varphi} & G(\mathcal{H}\mathcal{C}_a/\mathcal{F}\mathcal{C}_a) \\ \parallel & & \parallel \\ G(\mathcal{G}/\mathcal{F}) & & G(\mathcal{H}/\mathcal{F}) \\ \downarrow c & & \downarrow d \\ \text{GL}_K(n) & \xrightarrow{\tau_b} & \text{GL}_K(n) \end{array}$$

is commutative ( $T_\varphi$  denoting the  $\mathcal{C}_a$ -isomorphism determined as in Proposition 12, and  $\tau_b$  denoting the inner automorphism of  $\text{GL}_{\mathcal{X}}(n)$  determined by  $b$ ).

*Proof* Part (a) is an immediate consequence of Chapter IV, Section 5, Corollary 2 to Proposition 2. In proving part (b) we may replace  $\mathcal{F}, \mathcal{G}, \mathcal{H}$  by  $\mathcal{F}\mathcal{C}_a, \mathcal{G}\mathcal{C}_a, \mathcal{H}\mathcal{C}_a$ , and therefore may suppose that  $\mathcal{C}$  is algebraically closed. We may suppose, too, that  $\text{tr deg } \mathcal{G}/\mathcal{F} \leq \text{tr deg } \mathcal{H}/\mathcal{F}$ . By Chapter II, Section 1, Theorem 1, there exist derivative operators  $\theta_1, \dots, \theta_n \in \Theta$ , and integers  $k(1), \dots, k(n)$  between 1 and  $r$ , such that the differential polynomial  $W = \det(\theta_h y_{j, k(h)})_{1 \leq h \leq n, 1 \leq j \leq n, 1 \leq k \leq r}$  does not vanish at the point  $(\eta_1, \dots, \eta_n) = (\eta_{jk})_{1 \leq j \leq n, 1 \leq k \leq r}$ . By Chapter III, Section 10, Propositions 6 and 7(d), there exists a differential specialization  $(\eta'_1, \dots, \eta'_n)$  of  $(\eta_1, \dots, \eta_n)$  over  $\mathcal{H}$  that is constrained over  $\mathcal{H}$  with constraint  $W$ , and the field of constants of  $\mathcal{H}\langle \eta'_1, \dots, \eta'_n \rangle$  is  $\mathcal{C}$ . By Chapter II, Section 1, Theorem 1,  $(\eta'_1, \dots, \eta'_n)$  is linearly independent over constants and hence is a fundamental system of zeros of  $\mathcal{I}$ . It follows that there exists a matrix  $b = (b_{jj'}) \in \text{GL}_{\mathcal{X}}(n)$  such that  $\eta'_{j'} = \sum_j \zeta_j b_{jj'}$  ( $1 \leq j' \leq n$ ), and since the field of constants of  $\mathcal{H}\langle \eta'_1, \dots, \eta'_n \rangle$  in  $\mathcal{C}$  we even have  $b \in \text{GL}_{\mathcal{C}}(n)$ . Hence  $\mathcal{F}\langle \eta'_1, \dots, \eta'_n \rangle = \mathcal{H}$ . Letting  $c'$  denote the representation of  $G(\mathcal{H}/\mathcal{F})$  associated with

$(\eta'_1, \dots, \eta'_n)$ , we see by an earlier remark that the accompanying diagram is commutative. Now,  $(\eta'_1, \dots, \eta'_n)$  is a differential specialization of  $(\eta_1, \dots, \eta_n)$  over  $\mathcal{F}$ , and because  $\text{tr deg } \mathcal{G}/\mathcal{F} \leq \text{tr deg } \mathcal{H}/\mathcal{F}$  it must be a generic one. Therefore there exists an isomorphism  $\varphi: \mathcal{G} \approx \mathcal{H}$  over  $\mathcal{F}$  with  $\varphi(\eta_j) = \eta'_j$  ( $1 \leq j \leq n$ ), and by Section 3, Proposition

$$\begin{array}{ccc} & G(\mathcal{H}/\mathcal{F}) & \\ c' \swarrow & \downarrow d & \\ \text{GL}_{\mathcal{X}}(n) & \xrightarrow{\tau_b} & \text{GL}_{\mathcal{X}}(n) \end{array}$$

12 and the Remark thereafter, the inner automorphism that  $\varphi$  determines on the group of automorphisms of  $\mathcal{G}\mathcal{K}$  over  $\mathcal{F}\mathcal{K}$  is a  $\mathcal{C}$ -isomorphism  $T_\varphi: G(\mathcal{G}/\mathcal{F}) \approx G(\mathcal{H}/\mathcal{F})$ . For any  $\sigma \in G(\mathcal{G}/\mathcal{F})$ , the computation

$$\begin{aligned} \sum_j \eta'_j c'_{jj'}(T_\varphi \sigma) &= (T_\varphi \sigma) \eta'_j = \varphi \sigma \varphi^{-1} \varphi \eta_j = \varphi \sigma \eta_j \\ &= \varphi \sum_j \eta_j c_{jj'}(\sigma) = \sum_j \eta'_j c_{jj'}(\sigma) \end{aligned}$$

$$\begin{array}{ccc} G(\mathcal{G}/\mathcal{F}) & \xrightarrow{T_\varphi} & G(\mathcal{H}/\mathcal{F}) \\ \downarrow c & \swarrow c' & \\ \text{GL}_{\mathcal{X}}(n) & & \end{array}$$

shows that  $c'(T_\varphi \sigma) = c(\sigma)$ , that is, shows that the accompanying diagram is commutative. Combining this with the preceding diagram, we see that the diagram in the statement of the proposition is commutative.

EXERCISES

- (Seidenberg [39]) Consider  $\mathbf{R}$  as an ordinary differential field of constants, let  $\alpha$  be a zero of  $y'^2 + 4y^2 + 1$  with  $\alpha' \neq 0$ , and set  $\mathcal{F} = \mathbf{R}\langle \alpha \rangle$ . Let  $\eta$  be any zero of  $y'' + y$  with  $\eta \neq 0$ . Show that the field of constants of  $\mathcal{F}$  is  $\mathbf{R}$  and that the field of constants of  $\mathcal{F}\langle \eta \rangle$  is not  $\mathbf{R}$ . (*Hint:* After establishing the first point, show that the elements  $\gamma_1 = \eta^2 + \eta'^2$  and  $\gamma_2 = \alpha\eta^2 + \alpha'\eta\eta' - \alpha\eta'^2$  are constants. If  $\gamma_1, \gamma_2 \in \mathbf{R}$  and  $\gamma_1 \neq 0$ , set  $c = \gamma_2/\gamma_1$  and  $\zeta = \eta'/\eta$ , and then observe that  $\zeta$  is a root of the quadratic polynomial  $(c + \alpha)Z^2 - \alpha'Z + c - \alpha$ , so that the discriminant of this polynomial is a square in  $\mathcal{F}\langle \eta \rangle$ .)
- Let  $\alpha \in \mathcal{U}$  and suppose that the constants in  $\mathcal{F}\langle \alpha \rangle$  are in  $\mathcal{F}$ .
  - Show that if  $\alpha$  is exponential over  $\mathcal{F}$ , then  $\mathcal{F}\langle \alpha \rangle$  is a Picard-Vessiot extension of  $\mathcal{F}$ .
  - Show that if  $\alpha$  is primitive over  $\mathcal{F}$ , then  $\mathcal{F}\langle \alpha \rangle$  is a Picard-Vessiot extension of  $\mathcal{F}$ .
  - Show that if  $\alpha$  is Weierstrassian and transcendental over  $\mathcal{F}$ , then  $\mathcal{F}\langle \alpha \rangle$  is not a Picard-Vessiot extension of  $\mathcal{F}$ .
- Let  $\mathcal{F}_0$  denote a differential field over which  $\mathcal{U}$  is universal,  $\mathcal{C}$  denote the field of constants of  $\mathcal{F}_0$ , and  $G$  be a  $\mathcal{C}$ -subgroup of  $\text{GL}_{\mathcal{X}}(n)$ . Let  $t_1, \dots, t_n \in \mathcal{U}$  be differentially algebraically independent over  $\mathcal{F}_0$ , and

set  $\mathcal{G} = \mathcal{F}_0 \langle t_1, \dots, t_n \rangle$ . Fix distinct  $\theta_1', \dots, \theta_n' \in \Theta$ , and for all choices of  $\theta_1, \dots, \theta_n \in \Theta$ , set  $a_{\theta_1, \dots, \theta_n} = \det(\theta_i' t_j)^{-1} \det(\theta_i t_j)$ . Finally, set  $\mathcal{F} = \mathcal{F}_0 \langle (a_{\theta_1, \dots, \theta_n})_{\theta_1 \in \Theta(1), \dots, \theta_n \in \Theta(n)} \rangle$ .

(a) Prove that the field of constants of  $\mathcal{G}$  is  $\mathcal{C}$  and that  $(t_1, \dots, t_n)$  is a fundamental system of zeros of a linear differential ideal  $I$  of  $\mathcal{F}\{y\}$ , and hence that  $\mathcal{G}$  is a Picard-Vessiot extension of  $\mathcal{F}$ . (Hint: See Chapter II, Section 9, Corollary 5 to Theorem 4, and Chapter IV, Section 5, Corollary 3 to Proposition 2.)

(b) Prove that the Galois group of  $I$  with respect to  $(t_1, \dots, t_n)$  is  $\mathbf{GL}_n(n)$ .

(c) Show that there exists a differential field  $\mathcal{E}$  with  $\mathcal{F} \subset \mathcal{E} \subset \mathcal{G}$  such that the Galois group of  $I$  over  $\mathcal{E}$  with respect to  $(t_1, \dots, t_n)$  is  $G$ .

(d) Prove that in part (c),  $\mathcal{E} = \mathcal{F} \langle \mathcal{E} \cap \mathcal{F}_0((\theta_i' t_j)_{1 \leq i \leq n, 1 \leq j \leq n}) \rangle$ . (Hint: By part (c) there exist distinct  $\theta_1', \dots, \theta_n', \dots, \theta_q' \in \Theta$  such that  $\mathcal{E} = \mathcal{F} \langle \mathcal{E}_q \rangle$ , where  $\mathcal{E}_q = \mathcal{E} \cap \mathcal{F}((\theta_i' t_j)_{1 \leq i \leq q, 1 \leq j \leq n})$ . If  $q > n$ , set

$$M(y) = \det(\theta_i' t_j)^{-1}_{1 \leq i \leq n, 1 \leq j \leq n} \det \begin{pmatrix} \theta_q' y & \theta_q' t_1 & \cdots & \theta_q' t_n \\ \theta_1' y & \theta_1' t_1 & \cdots & \theta_1' t_n \\ \vdots & \vdots & \ddots & \vdots \\ \theta_n' y & \theta_n' t_1 & \cdots & \theta_n' t_n \end{pmatrix}$$

and observe that  $M = \theta_q' y - \sum_{1 \leq j \leq n} a_j \theta_j' y$ , where

$$a_j = a_{\theta_1', \dots, \theta_{j-1}', \theta_q', \theta_{j+1}', \dots, \theta_n'} \in \mathcal{F} \subset \mathcal{E},$$

and that the elements  $\theta_i' t_j$  ( $1 \leq i \leq q-1, 1 \leq j \leq n$ ) and  $a_j$  ( $1 \leq j \leq n$ ) are algebraically independent over  $\mathcal{F}_0$ . Infer first that each  $f \in \mathcal{E}_q$  can be written in the form  $f = A/B$ , where  $A$  and  $B$  are relatively prime polynomials in  $a_1, \dots, a_n$  with coefficients in  $\mathcal{F}_0((\theta_i' t_j)_{1 \leq i \leq q-1, 1 \leq j \leq n})$ , one of the coefficients in  $B$  being 1, and second that each coefficient is in  $\mathcal{E}_{q-1}$ , so that  $\mathcal{E}_q \subset \mathcal{F} \langle \mathcal{E}_{q-1} \rangle$  and  $\mathcal{E} = \mathcal{F} \langle \mathcal{E}_{q-1} \rangle$ .

4. Let  $(\eta_1, \dots, \eta_n)$  be a fundamental system of zeros of a linear differential ideal  $I$  of  $\mathcal{F}\{y\}$  and suppose that  $(\eta_1, \dots, \eta_n)$  generates a Picard-Vessiot extension of  $\mathcal{F}$ . Fix  $\theta_1, \dots, \theta_n \in \Theta$  with  $\det(\theta_i \eta_j) \neq 0$ . Show that the Galois group of  $I$  relative to  $(\eta_1, \dots, \eta_n)$  is a subgroup of  $\mathbf{SL}_n(n)$  if and only if  $\det(\theta_i \eta_j) \in \mathcal{F}$ .

5. Let  $(\eta_1, \dots, \eta_n)$  be a fundamental system of zeros of a linear differential ideal  $I$  of  $\mathcal{F}\{y_1, \dots, y_r\}$ , and suppose that  $\mathcal{F} \langle \eta_1, \dots, \eta_n \rangle$  is a Picard-Vessiot extension of  $\mathcal{F}$ . Let  $G$  be the Galois group of  $I$  relative to  $(\eta_1, \dots, \eta_n)$ , and let  $n' \in \mathbf{N}$ ,  $1 \leq n' < n$ .

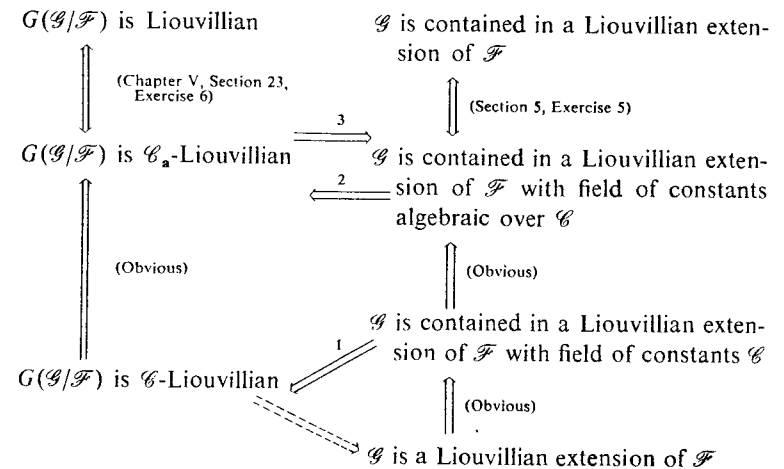
(a) Show that  $(\eta_1, \dots, \eta_n)$  is a fundamental system of zeros of a linear differential ideal of  $\mathcal{F}\{y_1, \dots, y_r\}$  if and only if  $c_{ij} = 0$  ( $n' < i \leq n, 1 \leq j \leq n'$ ) for every  $(c_{ij}) \in G$ .

(b) Show that if  $(\eta_1, \dots, \eta_n)$  is a fundamental system of zeros of a linear differential ideal  $I'$  of  $\mathcal{F}\{y_1, \dots, y_r\}$ , and  $L_1, \dots, L_s$  are linear differential polynomials in  $\mathcal{F}\{y_1, \dots, y_r\}$  such that  $[L_1, \dots, L_s] = I'$ , and we set  $\zeta_j = (L_1(\eta_j), \dots, L_s(\eta_j)) \in \mathcal{U}^s$  ( $n' < j \leq n$ ), then  $(\zeta_{n'+1}, \dots, \zeta_n)$  is a fundamental system of zeros of a linear differential ideal  $I''$  of  $\mathcal{F}\{y_1, \dots, y_r\}$ , and as  $(c_{ij})_{1 \leq i \leq n, 1 \leq j \leq n}$  runs over  $G$ , then  $(c_{ij})_{n' < i \leq n, n' < j \leq n}$  runs over the Galois group of  $I''$  relative to  $(\zeta_{n'+1}, \dots, \zeta_n)$ .

6. (Bialynicki-Birula [5]) A Picard-Vessiot element over  $\mathcal{F}$  is defined as an element  $\alpha \in \mathcal{U}$  such that the vector space  $\sum_{\theta \in \Theta} \mathcal{F} \theta \alpha$  over  $\mathcal{F}$  is finite-dimensional (or, equivalently, an element that is a zero of a linear differential ideal of  $\mathcal{F}\{y\}$  of finite linear dimension). Let  $\mathcal{G}$  be a strongly normal extension of  $\mathcal{F}$  and let  $\mathcal{P}$  denote the set of all Picard-Vessiot elements of  $\mathcal{G}$  over  $\mathcal{F}$ . Prove that  $\mathcal{P}$  is a differential subring of  $\mathcal{G}$  and that  $\mathcal{G}$  is a Picard-Vessiot extension of  $\mathcal{F}$  if and only if  $\mathcal{G}$  is the differential field of quotients of  $\mathcal{P}$ .

7. (Vessiot's theorem on "solubility by quadratures." See Kolchin [15]) Let  $\mathcal{G}$  be a Picard-Vessiot extension of  $\mathcal{F}$ . Denote the field of constants of  $\mathcal{F}$  by  $\mathcal{C}$ .

(a) (Recall the definition of Liouvillian extension given in Section 5, Exercise 5(a), and the definition of Liouvillian (and  $\mathcal{C}$ -Liouvillian)  $\mathcal{G}$ -group given in Chapter V, Section 23, Exercise 6.) Prove the implications 1, 2, 3 in the accompanying diagram. The dotted implication



is to be proved later (Section 9, Exercise 1). (Hint: (1) Suppose  $\mathcal{G} \subset \mathcal{F} \langle \alpha_1, \dots, \alpha_r \rangle$  with  $\alpha_k$  primitive or exponential or algebraic over  $\mathcal{F} \langle \alpha_1, \dots, \alpha_{k-1} \rangle$  and with all constants in  $\mathcal{C}$ , and argue by induction

on  $r$ . Show that when  $\mathcal{F}\langle\alpha_1\rangle$  is strongly normal over  $\mathcal{F}$ , then  $G(\mathcal{G}/\mathcal{G} \cap \mathcal{F}\langle\alpha_1\rangle)$  is  $\mathcal{C}$ -isomorphic to  $G(\mathcal{G}\langle\alpha_1\rangle/\mathcal{F}\langle\alpha_1\rangle)$  and is normal in  $G(\mathcal{G}/\mathcal{F})$  with quotient  $\mathcal{C}$ -isomorphic to  $G(\mathcal{F}\langle\alpha_1\rangle/\mathcal{G} \cap \mathcal{F}\langle\alpha_1\rangle)$ , and that in the contrary case  $G(\mathcal{G}/\mathcal{F}^\circ)$  is  $\mathcal{C}$ -isomorphic to  $G(\mathcal{G}\langle\alpha_1\rangle/\mathcal{F}^\circ\langle\alpha_1\rangle)$ .

(2) Show that  $\mathcal{F}, \mathcal{G}$  may be replaced by  $\mathcal{F}\mathcal{C}_n, \mathcal{G}\mathcal{C}_n$  and then use (1).

(3) Again justify the assumption that  $\mathcal{C}$  is algebraically closed, and use Chapter V, Section 23, Proposition 39, to show that there exists a fundamental system of zeros  $(\eta_1, \dots, \eta_n)$  of a linear differential ideal  $I$  of  $\mathcal{F}\{y\}$  of linear dimension  $n$  such that  $\mathcal{F}\langle\eta_1, \dots, \eta_n\rangle = \mathcal{G}$  and such that the Galois group of  $I$  over  $\mathcal{F}^\circ$  relative to  $(\eta_1, \dots, \eta_n)$  is triangular. Then show that  $\eta_1$  is exponential over  $\mathcal{F}^\circ$  and that, for each  $i$ , a maximal subfamily of  $(\delta_i(\eta_2/\eta_1), \dots, \delta_i(\eta_n/\eta_1))$  that is linearly independent over  $\mathcal{C}$  is a fundamental system of zeros of a linear differential ideal of  $\mathcal{F}^\circ\{y\}$  of linear dimension less than or equal to  $n-1$ , and argue by induction on  $n$ .)

(b) (Recall the definition of Liouvillian extension of type (i) given in Section 5, Exercise 5(b), and the definitions of Liouvillian and  $\mathcal{C}$ -Liouvillian  $\mathcal{C}$ -groups of type (i) given in Chapter V, Section 23, Exercise 6.) Refine the result in part (a) by establishing a diagram "of type (i)" for each  $i$ .

8. Let  $\mathcal{F}_0$  be an ordinary differential field such that  $\mathcal{U}$  is universal over  $\mathcal{F}_0$ . Let  $u_1, \dots, u_n \in \mathcal{U}$  be differentially algebraically independent over  $\mathcal{F}_0$ , and let  $\mathcal{F} = \mathcal{F}_0\langle u_1, \dots, u_n \rangle$ . Set  $L = y^{(n)} + u_1 y^{(n-1)} + \dots + u_n y$ . Prove that every fundamental system of zeros of  $L$  generates a Picard-Vessiot extension of  $\mathcal{F}$  and that the Galois group of  $L$  over  $\mathcal{F}$  relative to any such fundamental system is  $\mathbf{GL}_x(n)$ . (Hint: See Exercise 3.)
9. Let  $\mathcal{F}$  be an ordinary differential field, let  $a_1, \dots, a_n \in \mathcal{F}$ , set  $L = y^{(n)} + a_1 y^{(n-1)} + \dots + a_n y$  and  $M = y' + a_1 y$ , and let  $(\eta_1, \dots, \eta_n)$  be a fundamental system of zeros of  $L$  that generates a Picard-Vessiot extension of  $\mathcal{F}$ . Prove that a necessary and sufficient condition that the Galois group of  $L$  over  $\mathcal{F}$  relative to  $(\eta_1, \dots, \eta_n)$  be contained in  $\mathbf{SL}_x(n)$  is that  $M$  have a nontrivial zero in  $\mathcal{F}$ . (Hint: Show that the Wronskian determinant of  $(\eta_1, \dots, \eta_n)$  is a zero of  $M$ , and refer to Exercise 4.)
10. Let  $\mathcal{F}$  be an ordinary differential field, let  $a_1, a_2 \in \mathcal{F}$ , set  $L = y'' + a_1 y' + a_2 y$ , and consider the Riccati differential polynomial  $R = y' + y^2 + a_1 y + a_2$ .
- (a) Show that the formula  $\eta \mapsto \eta'/\eta$  defines a surjection of the set of nontrivial zeros of  $L$  onto the set of zeros of  $R$ .
- (b) Prove that a necessary and sufficient condition that  $L$  have a fundamental system of zeros generating a Picard-Vessiot extension of  $\mathcal{F}$  relative to which the Galois group of  $L$  over  $\mathcal{F}$  is triangular (that

is, is contained in  $\mathbf{T}(2)$ ), is that  $R$  have a zero in  $\mathcal{F}$ . (Hint: For the sufficiency, use Section 5, Exercises 1(b) and 2(b).)

11. Let  $\mathcal{F}$  be the ordinary differential field  $\mathbf{C}(x)$  of rational functions of a complex variable  $x$ , the derivation operator being  $d/dx$ . Let  $v \in \mathbf{C}$  and consider the Bessel differential polynomial  $B_v = y'' + x^{-1}y' + (1 - v^2 x^{-2})y$ .
- (a) Prove that if  $v - \frac{1}{2} \in \mathbf{Z}$ , then, relative to a suitable fundamental system of zeros,  $B_v$  has a Galois group over  $\mathcal{F}$  consisting of all matrices  $\begin{pmatrix} c & 0 \\ 0 & c^{-1} \end{pmatrix}$  with  $c \in \mathcal{X}^*$ , and therefore the Galois group is  $\mathbf{C}$ -isomorphic to  $(\mathcal{G}_m)_x$ . (Hint: Replacing  $v$  by  $-v$  if necessary, suppose that  $v - \frac{1}{2} = s$ , where  $s \in \mathbf{N}$ , and set

$$\eta_{\pm} = e^{\pm ix} \sum_{0 \leq k \leq s} \frac{(s+k)!}{(s-k)! k!} (\pm i)^k 2^{-k} x^{-k-1/2}.$$

Show that  $(\eta_+, \eta_-)$  is a fundamental system of zeros of  $B_v$ , that  $\eta_+$  and  $\eta_-$  are exponential over  $\mathcal{F}$ , and that their product is in  $\mathcal{F}$ .)

- (b) Prove that if  $v - \frac{1}{2} \notin \mathbf{Z}$ , then the Galois group of  $B_v$  over  $\mathcal{F}$ , relative to any fundamental system of zeros of  $B_v$  that generates a Picard-Vessiot extension of  $\mathcal{F}$ , is  $\mathbf{SL}_x(2)$ . (Hint: Assume not. Use Exercise 9 to show that the group is a proper  $\mathbf{C}$ -subgroup of  $\mathbf{SL}_x(2)$ , then use Chapter V, Sections 23, Exercises 5 and 2, and Chapter V, Section 23, Proposition 39, to show that the fundamental system of zeros can be chosen so that the Galois group of  $B_v$  over  $\mathcal{F}^\circ$  is triangular, and then use Exercise 10 to infer that some algebraic function  $\varphi$  of  $x$  is a zero of the differential polynomial  $R_v = y' + y^2 + x^{-1}y + 1 - v^2 x^{-2}$ . Examining an expansion of  $\varphi$  in (possibly fractional) powers of  $x^{-1}$ , show that no nonintegral exponent occurs, that no negative exponent occurs, and that the term of degree 0 is  $\pm i$ . Similarly, for any  $c \in \mathbf{C}$  with  $c \neq 0$  and any expansion of  $\varphi$  in powers of  $x-c$ , show that nonintegral exponents do not occur and if  $\varphi$  has a pole at  $c$ , it is a simple one with residue 1. Infer that  $\varphi \in \mathcal{F}$ , that the expansion of  $\varphi$  in powers of  $x$  is  $\varphi = bx^{-1} + \dots$ , where  $b = \pm v$ , and hence that  $\varphi = a + bx^{-1} + \sum_{1 \leq k \leq r} (x-c_k)^{-1}$ , where  $c_1, \dots, c_r$  are the poles of  $\varphi$  other than 0, and  $a = \pm i$ . Compute the coefficient of  $x^{2r+1}$  in  $R_v(\varphi)x^2 \prod_{1 \leq k \leq r} (x-c_k)^2$ , and conclude that  $\pm v + r + \frac{1}{2} = 0$ .)
12. (Kolchin [21]) Let  $\mathcal{F}$  be an ordinary differential field and  $\mathcal{C}$  be its field of constants. For each integer  $j$  with  $1 \leq j \leq n$  let

$$L_j = y^{(r)} + p_{j1} y^{(r+1)} + \dots + p_{jr} y,$$

where  $p_{j1}, \dots, p_{jr} \in \mathcal{F}$ , suppose that  $y' + p_{j1} y$  has a nontrivial zero in  $\mathcal{F}$ , let  $(\eta_{j1}, \dots, \eta_{jr})$  be a fundamental system of zeros of  $L_j$ , and set

$\eta_j = (\eta_{jk}^{(-1)})_{1 \leq i \leq r, 1 \leq k \leq r}$ . Suppose that the field of constants of the differential field  $\mathcal{G} = \mathcal{F} \langle (\eta_{jk})_{1 \leq j \leq n, 1 \leq k \leq r} \rangle = \mathcal{F}(\eta_1, \dots, \eta_n)$  is  $\mathcal{C}$ , and set  $\mathcal{G}_j = \mathcal{F} \langle \eta_{j1}, \dots, \eta_{jr} \rangle = \mathcal{F}(\eta_j)$  ( $1 \leq j \leq n$ ).

(a) Show that  $\mathcal{G}$  is a strongly normal extension of  $\mathcal{F}$  and that the formula  $c(\sigma) = (\eta_1^{-1} \sigma \eta_1, \dots, \eta_n^{-1} \sigma \eta_n)$  defines an injective  $\mathcal{C}$ -homomorphism  $c : G(\mathcal{G}/\mathcal{F}) \rightarrow \mathbf{SL}_{\mathcal{X}}(r)^n$ .

(b) Prove that if  $\text{tr deg } \mathcal{G}/\mathcal{F} < n(r^2 - 1)$ , then either there exists an index  $j$  such that  $\text{tr deg } \mathcal{G}_j/\mathcal{F} < r^2 - 1$  or else there exist two distinct indices  $j, j'$ , and a nonzero element  $\alpha \in \mathcal{G}_j \mathcal{G}_{j'}$  with  $\alpha' \in \mathcal{F}$ , and a matrix  $a \in \mathbf{GL}_{\mathcal{F}}(r)$ , and a matrix  $b \in \mathbf{GL}_{\mathcal{C}}(r)$ , such that one of the two conditions

$$\eta_{j'} = \alpha \eta_j b, \quad \eta_{j'} = \alpha \check{\eta}_j b$$

is satisfied, where  $\check{\eta}_j$  denotes the inverse of the transpose of  $\eta_j$ . When  $r = 2$ , the second of these two conditions is superfluous. (*Hint:* Assuming that  $\text{tr deg } \mathcal{G}_j/\mathcal{F} = r^2 - 1$  ( $1 \leq j \leq n$ ), use Chapter V, Section 23, Exercise 8(c), to obtain a relation of the form  $c_j(\sigma) = \gamma(\sigma) b^{-1} c_j(\sigma) b$  ( $\sigma \in G(\mathcal{G}_j/\mathcal{F})$ ) or  $c_j(\sigma) = \gamma(\sigma) b^{-1} \check{c}_j(\sigma) b$  ( $\sigma \in G(\mathcal{G}_j/\mathcal{F})$ ), where  $b \in \mathbf{GL}_{\mathcal{C}}(r)$ ,  $\gamma(\sigma) \in \mathbf{P}_r$ , and for each  $i$ ,  $c_i$  is the composite of the restriction mapping  $G(\mathcal{G}/\mathcal{F}) \rightarrow G(\mathcal{G}_i/\mathcal{F})$  and the representation of  $G(\mathcal{G}_i/\mathcal{F})$  associated with  $(\eta_{i1}, \dots, \eta_{ir})$ . Set  $u = \eta_j b^{-1} \eta_{j'}^{-1}$  or  $u = \eta_j \check{b}^{-1} \eta_{j'}$ , let  $\alpha$  be a nonzero coordinate of  $u$ , and set  $a = \alpha^{-1} u$ .)

7 G-Primitives

In the two preceding sections we saw that when  $G$  is one of the  $\mathcal{C}$ -groups  $\mathbf{G}_a, \mathbf{G}_m, \mathbf{W}(g_2, g_3), \mathbf{GL}(n)$ , then the adjunction to  $\mathcal{F}$  of a solution of a suitable system of differential equations yields, when no new constants are thereby introduced, a  $G$ -extension of  $\mathcal{F}$ . These results are special cases of a general result that applies to any connected  $\mathcal{C}$ -group, where as usual  $\mathcal{C}$  denotes the field of constants of  $\mathcal{F}$ . The present section provides an exposition of this more general result.

Let  $G$  be a connected  $\mathcal{C}$ -group. We recall from Chapter V, Section 22, that to each derivation  $\delta$  of  $\mathcal{U}$  over  $\mathcal{C}$  there corresponds the logarithmic derivation  $l\delta : G \rightarrow \mathfrak{L}(G)$ . Since each of the  $m$  derivation operators  $\delta_i$  may be identified with the derivation of  $\mathcal{U}$  given by the formula  $u \mapsto \delta_i u$ , we have the  $m$  logarithmic derivations  $l\delta_i$  on  $G$ . Consequently we can define a mapping

$$l\Delta : G \rightarrow \mathfrak{L}(G)^m$$

by the formula

$$l\Delta(\alpha) = (l\delta_1(\alpha), \dots, l\delta_m(\alpha)).$$

By Chapter V, Section 22, Proposition 28, we have  $l\Delta(\alpha) \in \mathfrak{L}_{\mathcal{C}\langle\alpha\rangle}(G)^m$  for every  $\alpha \in G$ . Writing  $\tau_\alpha^\#(D_1, \dots, D_m) = (\tau_\alpha^\#(D_1), \dots, \tau_\alpha^\#(D_m))$  for any  $(D_1, \dots, D_m) \in \mathfrak{L}(G)^m$ , we see from Chapter V, Section 22, Theorem 14 and the remark following it, that

$$l\Delta(\alpha\beta) = l\Delta(\alpha) + \tau_\alpha^\#(l\Delta(\beta)) \quad (\alpha, \beta \in G).$$

Thus,  $l\Delta$  is a crossed homomorphism of the group  $G$  into the additive group  $\mathfrak{L}(G)^m$ . By Chapter V, Section 22, Proposition 28,  $l\Delta(\alpha) = 0$  if and only if  $\alpha \in \mathcal{G}_{\mathcal{X}}$ . It follows that  $l\Delta(\alpha) = l\Delta(\beta)$  if and only if  $\alpha^{-1}\beta \in G_{\mathcal{X}}$ .

By a  $G$ -primitive over  $\mathcal{F}$  we mean an element  $\alpha \in G$  such that  $l\Delta(\alpha) \in \mathfrak{L}_{\mathcal{F}}(G)^m$ . If we fix a basis  $(\omega_1, \dots, \omega_r)$  of  $\mathfrak{L}_{\mathcal{F}}^*(G)$ , the condition that an element  $\alpha \in G$  be a  $G$ -primitive over  $\mathcal{F}$  can be expressed as the condition that, for some elements  $a_{ik} \in \mathcal{F}$  ( $1 \leq i \leq m, 1 \leq k \leq r$ ),  $\alpha$  satisfy the system of differential equations

$$\langle l\delta_i(\alpha), \omega_k \rangle = a_{ik} \quad (1 \leq i \leq m, 1 \leq k \leq r).$$

A glance at the examples at the end of Chapter V, Section 22, shows that an element  $\alpha \in \mathcal{U}$  is a  $\mathbf{G}_a$ -primitive over  $\mathcal{F}$  if and only if  $\alpha$  is primitive over  $\mathcal{F}$ , that an element  $\alpha \in \mathcal{U}^*$  is a  $\mathbf{G}_m$ -primitive over  $\mathcal{F}$  if and only if  $\alpha$  is exponential over  $\mathcal{F}$ , that an element  $(1 : \alpha : \beta) \in \mathbf{W} = \mathbf{W}(g_2, g_3)$  is a  $\mathbf{W}$ -primitive over  $\mathcal{F}$  if and only if  $\alpha$  is Weierstrassian over  $\mathcal{F}$  for the coefficients  $g_2, g_3$ , and that a matrix  $\alpha \in \mathbf{GL}(n)$  is a  $\mathbf{GL}(n)$ -primitive over  $\mathcal{F}$  if and only if  $\delta_i \alpha \cdot \alpha^{-1} \in \mathbf{M}_{\mathcal{F}}(n)$  ( $1 \leq i \leq m$ ).

If  $\alpha$  is a  $G$ -primitive over  $\mathcal{F}$ , then, for any  $\varphi \in \mathfrak{F}_{\mathcal{F}, \alpha}(G)$ , we have

$$\delta_i(\varphi(\alpha)) = (l\delta_i(\alpha) \varphi)(\alpha) \in \mathcal{F}(\alpha)$$

(because  $l\delta_i(\alpha) \in \mathfrak{L}_{\mathcal{F}}(G)$ , whence  $l\delta_i(\alpha) \varphi \in \mathfrak{F}_{\mathcal{F}, \alpha}(G)$ ), so that (by Chapter V, Section 19, Proposition 25)  $\delta_i(\mathcal{F}(\alpha)) \subset \mathcal{F}(\alpha)$ . Thus, if  $\alpha$  is a  $G$ -primitive over  $\mathcal{F}$ , then  $\mathcal{F}(\alpha) = \mathcal{F}$ .

By a  $G$ -primitive extension of  $\mathcal{F}$  we mean an extension of  $\mathcal{F}$  of the form  $\mathcal{F}(\alpha)$  where  $\alpha$  is a  $G$ -primitive over  $\mathcal{F}$ . The following theorem shows that every  $G$ -primitive extension of  $\mathcal{F}$  having the same field of constants as  $\mathcal{F}$  is a  $G$ -extension of  $\mathcal{F}$ .

**Theorem 6** Let  $\mathcal{C}$  denote the field of constants of the differential field  $\mathcal{F}$ , let  $G$  be a connected  $\mathcal{C}$ -group, let  $\alpha$  be a  $G$ -primitive over  $\mathcal{F}$ , and suppose that the field of constants of  $\mathcal{F}(\alpha)$  is  $\mathcal{C}$ . Then  $\mathcal{F}(\alpha)$  is a strongly normal extension of  $\mathcal{F}$ , and the formula  $c(\sigma) = \alpha^{-1} \sigma \alpha$  defines an injective  $\mathcal{C}$ -homomorphism  $c : G(\mathcal{F}(\alpha)/\mathcal{F}) \rightarrow G_{\mathcal{X}}$ .

*Proof* By hypothesis  $l\delta_i(\alpha) \in \mathfrak{L}_{\mathcal{F}}(G)$  ( $1 \leq i \leq m$ ). Hence, for any isomorphism  $\sigma$  of  $\mathcal{F}(\alpha)$  over  $\mathcal{F}$ ,  $\sigma(l\delta_i(\alpha)) = l\delta_i(\alpha)$ . However,  $\sigma(l\delta_i(\alpha)) = l\delta_i(\sigma\alpha)$  by Chapter V, Section 22, Proposition 28(b). Therefore  $l\Delta(\sigma\alpha) = l\Delta(\alpha)$ , so that the element  $c(\sigma) = \alpha^{-1} \sigma \alpha$  of  $G$  is rational over  $\mathcal{C}$ . Hence

$\mathcal{F}\langle\alpha\rangle\sigma(\mathcal{F}\langle\alpha\rangle) = \mathcal{F}\langle\alpha, \sigma\alpha\rangle = \mathcal{F}\langle\alpha, c(\sigma)\rangle = \mathcal{F}\langle\alpha\rangle\mathcal{C}(c(\sigma))$ , so that  $\mathcal{F}\langle\alpha\rangle$  is strongly normal over  $\mathcal{F}$  and (by Chapter II, Section 1, Corollary 2 to Theorem 1)  $\mathcal{C}(\sigma) = \mathcal{C}(c(\sigma))$ . For any  $\sigma, \tau \in \mathcal{G}(\mathcal{F}\langle\alpha\rangle/\mathcal{F})$  the computation

$$\alpha c(\sigma\tau) = \sigma\tau\alpha = \sigma(\alpha c(\tau)) = \sigma\alpha \cdot c(\tau) = \alpha c(\sigma)c(\tau)$$

shows that  $c$  is a group homomorphism. If  $\sigma \in \text{Ker}(c)$ , then  $\sigma\alpha = \alpha c(\sigma) = \alpha$  and  $\sigma = \text{id}_{\mathcal{F}\langle\alpha\rangle}$ . Hence  $c$  is injective. Finally, if  $\sigma \leftrightarrow \sigma'$ , then the isomorphism  $\mathcal{F}\langle\alpha\rangle\sigma(\mathcal{F}\langle\alpha\rangle) \approx \mathcal{F}\langle\alpha\rangle\sigma'(\mathcal{F}\langle\alpha\rangle)$  over  $\mathcal{F}\langle\alpha\rangle$  that maps  $\sigma\alpha$  onto  $\sigma'\alpha$  for each  $\alpha \in \mathcal{F}\langle\alpha\rangle$  maps  $\sigma\alpha$  onto  $\sigma\alpha'$  and hence maps  $c(\sigma) = \alpha^{-1}\sigma\alpha$  onto  $c(\sigma') = \alpha^{-1}\sigma'\alpha$ . Therefore  $c(\sigma) \leftrightarrow c(\sigma')$ , and  $S_{c(\sigma), c(\sigma')}$  is obtained by restricting the above isomorphism, that is, is the induced isomorphism  $S_{\sigma', \sigma}$ . By Chapter V, Section 9, this shows that  $c$  is a  $\mathcal{C}$ -homomorphism.

In Section 9 we shall describe circumstances under which, conversely, every  $G$ -extension of  $\mathcal{F}$  is a  $G$ -primitive extension of  $\mathcal{F}$ .

EXERCISES

In the following exercises  $\mathcal{C}$  is the field of constants of  $\mathcal{F}$  and  $G$  is a connected  $\mathcal{C}$ -group. For each  $\delta_i, \delta_i^*$  denotes the derivation of  $\mathfrak{F}(G)$  over  $\mathfrak{F}_\mathcal{X}(G)$  that extends  $\delta_i$  (see Chapter V, Section 16, Exercise 3), and  $\delta_i^*$  denotes the derivation of  $\mathfrak{V}(G)$  given by the formula  $\delta_i^*(D) = [\delta_i^*, D]$  (see Chapter V, Section 22, Exercise 2, and Chapter V, Section 18, Exercise 4). Also  $\mathfrak{I}(G)$  denotes the set of all  $(D_1, \dots, D_m) \in \mathfrak{V}(G)^m$  that satisfy the "integrability conditions"

$$\delta_{i'}^*(D_i) - \delta_i^*(D_{i'}) = [D_i, D_{i'}] \quad (1 \leq i < i' \leq m).$$

1. Prove that  $\mathfrak{I}(G)$  is the image of the crossed homomorphism  $\text{l}\Delta$ . (Hint: For the inclusion  $\text{l}\Delta(G) \subset \mathfrak{I}(G)$ , see Chapter V, Section 22, Exercise 2. For the opposite inclusion, consider any  $(D_1, \dots, D_m) \in \mathfrak{I}(G)$ . Fix  $\xi = (\xi_1, \dots, \xi_n)$  such that  $\mathfrak{F}_\mathcal{C}(G) = \mathcal{C}(\xi)$ , write  $D_i \xi_j = P_{ij}(\xi)/Q(\xi)$ , where  $P_{ij}, Q \in \mathcal{U}[y_1, \dots, y_n]$  and  $Q(\xi) \neq 0$ , let  $A$  denote the set of  $m$  differential polynomials  $A_{ij} = Q\delta_i y_j - P_{ij}$ , and let  $\mathfrak{p}_0$  denote the set of polynomials  $P \in \mathcal{U}[y_1, \dots, y_n]$  such that  $P(\xi) = 0$ . Show for any  $P \in \mathfrak{p}_0 \cap \mathcal{C}[y_1, \dots, y_n]$  that  $\sum_j (\partial P/\partial y_j) P_{ij} \in \mathfrak{p}_0$ . Observe that  $\mathfrak{p}_0$  is a prime ideal defined over  $\mathcal{C}$ , and infer that  $[\mathfrak{p}_0] \subset ([A] + (\mathfrak{p}_0)):Q^\infty$ . Fix an orderly ranking of  $(y_1, \dots, y_n)$ , observe that  $A$  is an autoreduced set in  $\mathcal{U}\{y_1, \dots, y_n\}$ , and show that  $Q^2(\delta_{i'} A_{ij} - \delta_i A_{i'j}) \equiv F_{i'j} \pmod{(A)}$ , where

$$F_{i'j} = \sum_v \left( \frac{\partial Q}{\partial y_v} (P_{i'v} P_{ij} - P_{iv} P_{i'j}) - Q \left( \frac{\partial P_{ij}}{\partial y_v} P_{i'v} - \frac{\partial P_{i'j}}{\partial y_v} P_{iv} \right) \right) + Q(Q^{\delta_{i'}} P_{ij} - Q P_{ij}^{\delta_{i'}} - Q^{\delta_i} P_{i'j} + Q P_{i'j}^{\delta_i}).$$

Apply the integrability conditions to  $\xi_j$  to show that  $F_{i'j} \in \mathfrak{p}_0$ , then refer to Chapter I, Section 2, Lemma 1 to infer for any  $\theta \in \Theta$  that  $Q^{2+\text{ord}\theta}(\theta\delta_{i'} A_{ij} - \theta\delta_i A_{i'j}) \in (\Theta(\text{ord}\theta) \cdot A) + (\mathfrak{p}_0)$  and hence (see Chapter III, Section 8) that  $A$  is  $(\mathfrak{p}_0)$ -coherent. Use Chapter III, Section 8, Exercise 1, to conclude that  $\mathfrak{p} = ([A] + (\mathfrak{p}_0)):Q^\infty$  is a prime differential ideal not containing any element of  $\mathcal{U}[y_1, \dots, y_n] - \mathfrak{p}_0$ . Let  $W$  denote the closed image of  $\xi_1 \times \dots \times \xi_n$ , let  $f \in \mathfrak{M}(G, W)$  be defined by the condition  $\text{in}_{G, W} f = \xi_1 \times \dots \times \xi_n$ , and observe that  $f$  is generically invertible. Let  $\mathcal{O}$  denote the domain of bidefinition of  $f$ , and show that there exists a polynomial  $F \in \mathcal{U}[y_1, \dots, y_n] - \mathfrak{p}_0$  that vanishes at every element of  $W - f(\mathcal{O})$ . Show that there exist a zero  $(a_1, \dots, a_n)$  of  $\mathfrak{p}$  that is not a zero of  $QF$  and an  $\alpha \in \mathcal{O}$  with  $\xi_j(\alpha) = a_j$  ( $1 \leq j \leq n$ ). Finally, show that  $D_{i\alpha} \xi_j = \text{l}\delta_i(\alpha) \xi_j$  ( $1 \leq i \leq m, 1 \leq j \leq n$ ), and conclude that  $(D_1, \dots, D_m) = \text{l}\Delta(\alpha)$ .

2. Let  $(D_1, \dots, D_m) \in \mathfrak{I}(G) \cap \mathfrak{V}_\mathcal{F}(G)^m$ . Show that there exists an  $\alpha \in G$  with  $\text{l}\Delta(\alpha) = (D_1, \dots, D_m)$  such that the field of constants of  $\mathcal{F}\langle\alpha\rangle$  is algebraic over  $\mathcal{C}$ . (Hint: Show that, in the proof in Exercise 1,  $P_{ij}$  and  $Q$  can, under the present conditions, be taken in  $\mathcal{F}[y_1, \dots, y_n]$ , so that  $\mathfrak{p}$  is defined over  $\mathcal{F}$ , and  $F$  can also be taken in  $\mathcal{F}[y_1, \dots, y_n]$ . Then apply Chapter III, Section 10, Propositions 6 and 7(d).)
3. Let  $(D_1, \dots, D_m) \in \mathfrak{V}(G)^m$ , fix a basis  $(D_1', \dots, D_n')$  of  $\mathfrak{V}_\mathcal{C}(G)$  and the dual basis  $(\omega_1', \dots, \omega_n')$  of  $\mathfrak{V}_\mathcal{C}^*(G)$ , let  $c_{jj'v}$  ( $1 \leq j \leq n, 1 \leq j' \leq n, 1 \leq v \leq n$ ) denote the corresponding "structure constants" (so that  $[D_j', D_{j'}'] = \sum_v c_{jj'v} D_v'$ ), and set  $a_{ij} = \langle D_i, \omega_j' \rangle$  ( $1 \leq i \leq m, 1 \leq j \leq n$ ). Prove that  $(D_1, \dots, D_m) \in \mathfrak{I}(G)$  if and only if

$$\delta_{i'} a_{ij} - \delta_i a_{i'j} = \sum_{v,v'} a_{iv} a_{i'v'} c_{vv'j} \quad (1 \leq i \leq m, 1 \leq i' \leq m, 1 \leq j \leq n).$$

4. Suppose further that  $G$  is a  $\mathcal{C}$ -subgroup of  $\text{GL}(n)$ , let  $\text{l}(G)$  denote the Lie algebra defined in Chapter V, Section 18, Exercise 1, let  $\nabla: \mathfrak{V}(G) \approx \text{l}(G)$  denote the isomorphism defined there, and let  $\nabla^{(m)}: \mathfrak{V}(G)^m \approx \text{l}(G)^m$  denote the isomorphism obtained by applying  $\nabla$  coordinatewise. Let  $\text{i}(G)$  denote the set of all  $(\alpha_1, \dots, \alpha_m) \in \text{l}(G)^m$  such that

$$\delta_{i'} \alpha - \delta_i \alpha_{i'} = [\alpha_i, \alpha_{i'}] \quad (1 \leq i < i' \leq m).$$

Prove that  $\nabla^{(m)}(\mathfrak{I}(G)) = \text{i}(G)$ .

8 Differential Galois cohomology

Let  $\mathcal{G}$  be a strongly normal extension of the differential field  $\mathcal{F}$  with field of constants  $\mathcal{C}$ , and let  $G$  be any  $\mathcal{C}$ -group. The elements of the Galois group  $G(\mathcal{G}/\mathcal{F})$  are identified with automorphisms of  $\mathcal{G}\mathcal{X}$  over  $\mathcal{F}\mathcal{X}$ . Therefore  $G(\mathcal{G}/\mathcal{F})$  operates on the group  $G_{\mathcal{G}\mathcal{X}}$ .



By a (one-dimensional) cocycle of  $G(\mathcal{G}/\mathcal{F})$  into  $G$ , we mean a mapping  $f: G(\mathcal{G}/\mathcal{F}) \rightarrow G$  that satisfies the following four conditions (in the statement of which  $\sigma, \sigma', \tau$  denote arbitrary elements of  $G(\mathcal{G}/\mathcal{F})$ ):

- (i)  $f(\sigma) \in G_{\mathcal{G}\sigma\mathcal{G}} = G_{\mathcal{G}\sigma(\sigma)}$ ;
- (ii) if  $\sigma \xrightarrow{\mathcal{G}} \sigma'$ , then  $f(\sigma) \xrightarrow{\mathcal{G}} f(\sigma')$ ;
- (iii) if  $\sigma \xleftrightarrow{\mathcal{G}} \sigma'$ , then the isomorphism  $\mathcal{G}\sigma\mathcal{G} \approx \mathcal{G}\sigma'\mathcal{G}$  over  $\mathcal{G}$  mapping  $\sigma a$  onto  $\sigma'a$  ( $a \in \mathcal{G}$ ) is an extension of  $S_{f(\sigma'), f(\sigma)}^{\mathcal{G}}$ ;
- (iv)  $f(\sigma\tau) = f(\sigma)f(\tau)$ .

We denote the set of all one-dimensional cocycles of  $G(\mathcal{G}/\mathcal{F})$  into  $G$  by  $Z^1(\mathcal{G}/\mathcal{F}, G)$ . It is easy to see that for any  $\alpha \in G_{\mathcal{G}}$ , the mapping  $G(\mathcal{G}/\mathcal{F}) \rightarrow G$  defined by the formula  $\sigma \mapsto \alpha^{-1}\sigma\alpha$  is a cocycle of  $G(\mathcal{G}/\mathcal{F})$  into  $G$ . We call such a cocycle a (one-dimensional) coboundary of  $G(\mathcal{G}/\mathcal{F})$  into  $G$ , and denote the set of all such coboundaries by  $B^1(\mathcal{G}/\mathcal{F}, G)$ . If  $f_1, f_2 \in Z^1(\mathcal{G}/\mathcal{F}, G)$ , we say that  $f_2$  is cohomologous to  $f_1$  when there exists an element  $\alpha \in G_{\mathcal{G}}$  such that  $f_2(\sigma) = \alpha^{-1}f_1(\sigma)\alpha$  for every  $\sigma \in G(\mathcal{G}/\mathcal{F})$ . The relation " $f_2$  is cohomologous to  $f_1$ " is an equivalence relation on  $Z^1(\mathcal{G}/\mathcal{F}, G)$ . We denote the set of equivalence classes by  $H^1(\mathcal{G}/\mathcal{F}, G)$  and call it the (one-dimensional) cohomology set of  $G(\mathcal{G}/\mathcal{F})$  into  $G$ . The set  $B^1(\mathcal{G}/\mathcal{F}, G)$  is an element of  $H^1(\mathcal{G}/\mathcal{F}, G)$  and as such is denoted by 1 (or, when  $G$  is commutative and written additively, by 0). Thus,  $H^1(\mathcal{G}/\mathcal{F}, G)$  has a canonical structure of pointed set. When  $G$  is commutative then  $Z^1(\mathcal{G}/\mathcal{F}, G)$  is a commutative group (subgroup of the group of all mappings of  $G(\mathcal{G}/\mathcal{F})$  into  $G$ ),  $B^1(\mathcal{G}/\mathcal{F}, G)$  is a subgroup of  $Z^1(\mathcal{G}/\mathcal{F}, G)$ , and  $H^1(\mathcal{G}/\mathcal{F}, G) = Z^1(\mathcal{G}/\mathcal{F}, G)/B^1(\mathcal{G}/\mathcal{F}, G)$ , so that  $H^1(\mathcal{G}/\mathcal{F}, G)$  then is a commutative group.

Let  $M$  be a principal homogeneous  $\mathcal{F}$ -space for  $G$ . For any  $\beta \in M_{\mathcal{G}}$  the formula  $\sigma \mapsto \beta^{-1}\sigma\beta$  defines a mapping  $G(\mathcal{G}/\mathcal{F}) \rightarrow G$  and it is easy to see that it is a cocycle of  $G(\mathcal{G}/\mathcal{F})$  in  $G$ . For a given  $f \in Z^1(\mathcal{G}/\mathcal{F}, G)$ , if there exists an element  $\beta \in M_{\mathcal{G}}$  such that  $f(\sigma) = \beta^{-1}\sigma\beta$  for every  $\sigma \in G(\mathcal{G}/\mathcal{F})$ , then we say that  $f$  splits in  $M$ . In particular, to say that  $f$  splits in  $G$  is the same as to say that  $f \in B^1(\mathcal{G}/\mathcal{F}, G)$ .

The following theorem and its first corollary explain how  $H^1(\mathcal{G}/\mathcal{F}, G)$  can, for a suitable  $\mathcal{F}$ -set  $W$ , be injected into the  $\mathcal{F}$ -cohomology set  $H_{\mathcal{F}}^1(W, Y)$  (see Chapter V, Section 17), and can be canonically injected into the Galois cohomology set  $H^1(\mathcal{F}, G)$  (see Chapter V, Section 12).

**Theorem 7** Let  $\mathcal{G}$  be a strongly normal extension of the differential field  $\mathcal{F}$  with field of constants  $\mathcal{C}$ , let  $\eta = (\eta_1, \dots, \eta_n) \in \mathcal{G}^n$  have the property that  $\mathcal{F}(\eta) = \mathcal{G}$ , and let  $W$  denote the locus of  $\eta$  over  $\mathcal{F}$ . Let  $G$  be a  $\mathcal{C}$ -group.

(a) For each  $f \in Z^1(\mathcal{G}/\mathcal{F}, G)$  there is a unique  $f_{\eta} \in Z^1_{\mathcal{F}}(W, G)$  such that  $f_{\eta}(\eta, \sigma\eta) = f(\sigma)$  for every  $\sigma \in G(\mathcal{G}/\mathcal{F})$ .

(b) For any  $f, f' \in Z^1(\mathcal{G}/\mathcal{F}, G)$ ,  $f'$  is cohomologous to  $f$  if and only if  $f'_{\eta}$  is  $\mathcal{F}$ -cohomologous to  $f_{\eta}$ .

*Proof* For any  $\mathcal{C}$ -generic element  $\sigma$  of a  $\mathcal{C}$ -component of  $G(\mathcal{G}/\mathcal{F})$ ,  $\mathcal{G}$  and  $\sigma\mathcal{G}$  are algebraically disjoint over  $\mathcal{F}$ , so that  $\dim_{\mathcal{F}}(\eta, \sigma\eta) = 2 \dim_{\mathcal{F}} \eta = \dim(W^2)$ , and hence  $(\eta, \sigma\eta)$  is an  $\mathcal{F}$ -generic element of an  $\mathcal{F}$ -component of  $W^2$ .

Let  $\mathfrak{p}$  denote the defining differential ideal of  $\eta$  in  $\mathcal{F}\{y_1, \dots, y_n\}$ . Then the intersection  $\mathfrak{p}_0 = \mathfrak{p} \cap \mathcal{F}[y_1, \dots, y_n]$  is the defining ideal of  $\eta$  in  $\mathcal{F}[y_1, \dots, y_n]$ . Referring to Chapter III, Section 6, Proposition 3, let  $\mathfrak{p}_1, \dots, \mathfrak{p}_r$  denote the components of  $\mathcal{G}\mathfrak{p}$ , so that  $\mathcal{G}\mathfrak{p} = \mathfrak{p}_1 \cap \dots \cap \mathfrak{p}_r$ . For each index  $k$ , set  $\mathfrak{p}_{k0} = \mathfrak{p}_k \cap \mathcal{G}[y_1, \dots, y_n]$ , so that

$$\mathfrak{p}_{10} \cap \dots \cap \mathfrak{p}_{r0} = \mathfrak{p}_1 \cap \dots \cap \mathfrak{p}_r \cap \mathcal{G}[y_1, \dots, y_n] = (\mathcal{G}\mathfrak{p}) \cap \mathcal{G}[y_1, \dots, y_n].$$

Fixing a basis  $(y_i)$  of  $\mathcal{G}$  over  $\mathcal{F}$ , we know that for each  $P \in \mathcal{G}\{y_1, \dots, y_n\}$  there exist unique elements  $P_i \in \mathcal{F}\{y_1, \dots, y_n\}$  such that  $P = \sum P_i y_i$ . Evidently

$$P \in \mathcal{G}\mathfrak{p} \iff P_i \in \mathfrak{p} \text{ (every } i),$$

$$P \in \mathcal{G}[y_1, \dots, y_n] \iff P_i \in \mathcal{F}[y_1, \dots, y_n] \text{ (every } i),$$

and therefore

$$P \in (\mathcal{G}\mathfrak{p}) \cap \mathcal{G}[y_1, \dots, y_n] \iff P_i \in \mathfrak{p} \cap \mathcal{F}[y_1, \dots, y_n] \text{ (every } i);$$

that is,

$$(\mathcal{G}\mathfrak{p}) \cap \mathcal{G}[y_1, \dots, y_n] = \mathcal{G}\mathfrak{p}_0.$$

Therefore

$$\mathcal{G}\mathfrak{p}_0 = \mathfrak{p}_{10} \cap \dots \cap \mathfrak{p}_{r0}.$$

Consider a generic zero  $\eta^{(k)}$  of  $\mathfrak{p}_k$ . It is also a generic zero of  $\mathfrak{p}_k \cap \mathcal{F}\{y_1, \dots, y_n\} = \mathfrak{p}$ , so that there exists an isomorphism  $\sigma_k: \mathcal{F}\langle \eta \rangle \approx \mathcal{F}\langle \eta^{(k)} \rangle$  over  $\mathcal{F}$  mapping  $\eta$  onto  $\eta^{(k)}$ . It is easy to see that  $\sigma_1, \dots, \sigma_r$  form a complete set of  $\mathcal{C}$ -generic elements of the  $\mathcal{C}$ -components of  $G(\mathcal{G}/\mathcal{F})$  (that is, every element  $G(\mathcal{G}/\mathcal{F})$  is a specialization over  $\mathcal{C}$  of a unique  $\sigma_k$ .) For each  $k$ ,  $\sigma_k \eta$  is a generic zero of  $\mathfrak{p}_k$ , and hence also of  $\mathfrak{p}$  and of  $\mathfrak{p}_{k0}$ . Now,  $\mathcal{G}$  and  $\sigma_k \mathcal{G}$  are algebraically disjoint over  $\mathcal{F}$ , and hence  $\dim_{\mathcal{F}} \sigma_k \eta = \dim_{\mathcal{F}} \sigma_k \eta = \dim_{\mathcal{F}} \eta = \dim W$ . Therefore if  $\sigma_k \eta$  is a specialization of  $\sigma_l \eta$  over  $\mathcal{G}$ , it is a generic one and hence (by Section 1, Lemma 2) is a generic differential specialization of  $\sigma_l \eta$  over  $\mathcal{G}$ , whence  $k = l$ .

What we have shown implies the following: If  $\sigma_1, \dots, \sigma_r$  are any elements of  $G(\mathcal{G}/\mathcal{F})$  that form a complete set of  $\mathcal{C}$ -generic elements of the  $\mathcal{C}$ -components of  $G(\mathcal{G}/\mathcal{F})$ , then  $\sigma_1 \eta, \dots, \sigma_r \eta$  form a complete set of  $\mathcal{G}$ -generic elements of the  $\mathcal{G}$ -components of  $W$ . Applying this result to the strongly

normal extension  $\mathcal{G}\mathcal{C}(\sigma_k)$  of  $\mathcal{F}\mathcal{C}(\sigma_k)$ , we see that if  $\sigma_{k_1}, \dots, \sigma_{k_{s_k}}$  form a complete set of  $\mathcal{C}(\sigma_k)$ -generic elements of the  $\mathcal{C}(\sigma_k)$ -components of  $G(\mathcal{G}/\mathcal{F})$ , then  $\sigma_{k_1}\eta, \dots, \sigma_{k_{s_k}}\eta$  form a complete set of  $(\mathcal{G}\sigma_k\mathcal{G})$ -generic elements of the  $(\mathcal{G}\sigma_k\mathcal{G})$ -components of  $W$ . This and the preceding result can be restated as follows:

The  $(\eta, \sigma_k\eta)$  with  $1 \leq k \leq r$  form a complete set of  $\mathcal{F}$ -generic elements of the  $\mathcal{F}$ -components of  $W^2$ .

The  $(\eta, \sigma_k\eta, \sigma_{kl}\eta)$  with  $1 \leq k \leq r$  and  $1 \leq l \leq s_k$  form a complete set of  $\mathcal{F}$ -generic elements of the  $\mathcal{F}$ -components of  $W^3$ .

Finally, because

$$\begin{aligned} \text{tr deg } \mathcal{C}(\sigma_k)\mathcal{C}(\sigma_{kl})/\mathcal{C} &= \text{tr deg } \mathcal{G}\mathcal{C}(\sigma_k)\mathcal{C}(\sigma_{kl})/\mathcal{G} = \text{tr deg } \mathcal{G} \cdot \sigma_k\mathcal{G} \cdot \sigma_{kl}\mathcal{G}/\mathcal{G} \\ &= \dim_{\mathcal{F}(\eta)}(\sigma_k\eta, \sigma_{kl}\eta) = \dim(W^2) = \dim(G(\mathcal{G}/\mathcal{F})^2), \end{aligned}$$

we see that  $(\sigma_k, \sigma_{kl})$  is a  $\mathcal{C}$ -generic element of a  $\mathcal{C}$ -component of  $G(\mathcal{G}/\mathcal{F})^2$ , and hence that  $\sigma_k^{-1}\sigma_{kl}$  is a  $\mathcal{C}$ -generic element of a  $\mathcal{C}$ -component of  $G(\mathcal{G}/\mathcal{F})$ .

All this being the case, consider any  $f \in Z^1(\mathcal{G}/\mathcal{F}, G)$ . Then  $f(\sigma_k) \in G_{\mathcal{G}\sigma_k\mathcal{G}} = G_{\mathcal{F}(\eta, \sigma_k\eta)}$ . Therefore (see Chapter V, Section 15, the discussion following the proof of Proposition 15) there exists a unique  $\mathcal{F}$ -mapping  $f_\eta \in \mathcal{M}_{\mathcal{F}}(W^2, G)$  such that  $f_\eta(\eta, \sigma_k\eta) = f(\sigma_k)$  for every  $k$ . For any  $\mathcal{C}$ -generic element  $\sigma$  of a  $\mathcal{C}$ -component of  $G(\mathcal{G}/\mathcal{F})$  there is a unique  $k$  such that  $\sigma_k \leftrightarrow \sigma$ , that is, such that there exists an isomorphism  $\mathcal{F}(\eta, \sigma_k\eta) = \mathcal{G}\sigma_k\mathcal{G} \approx \mathcal{G}\sigma\mathcal{G} = \mathcal{F}(\eta, \sigma\eta)$  over  $\mathcal{F}$  that maps  $(\eta, \sigma_k\eta)$  onto  $(\eta, \sigma\eta)$ . Because  $f_\eta$  is an  $\mathcal{F}$ -mapping and because  $f \in Z^1(\mathcal{G}/\mathcal{F}, G)$ , this isomorphism maps  $f_\eta(\eta, \sigma_k\eta)$  onto  $f_\eta(\eta, \sigma\eta)$  and maps  $f(\sigma_k)$  onto  $f(\sigma)$ . Therefore  $f_\eta(\eta, \sigma\eta) = f(\sigma)$  for every  $\sigma$  that is a  $\mathcal{C}$ -generic element of a  $\mathcal{C}$ -component of  $G(\mathcal{G}/\mathcal{F})$ .

Hence

$$\begin{aligned} f_\eta(\eta, \sigma_k\eta)f_\eta(\sigma_k\eta, \sigma_{kl}\eta) &= f_\eta(\eta, \sigma_k\eta) \cdot \sigma_k(f_\eta(\eta, \sigma_k^{-1}\sigma_{kl}\eta)) \\ &= f(\sigma_k)\sigma_k(f(\sigma_k^{-1}\sigma_{kl})) \\ &= f(\sigma_k \cdot \sigma_k^{-1}\sigma_{kl}) = f(\sigma_{kl}) = f_\eta(\eta, \sigma_{kl}\eta) \end{aligned}$$

for all  $(k, l)$ , so that  $f_\eta \in Z_{\mathcal{F}}^1(W, G)$ .

For any  $\sigma \in G(\mathcal{G}/\mathcal{F})$ , it follows from Chapter V, Section 17, Proposition 24, that  $f_\eta$  is defined at  $(\eta, \sigma\eta)$ . Fixing a  $\mathcal{C}(\sigma)$ -generic element  $\tau$  of  $G^0(\mathcal{G}/\mathcal{F})$ , we see that  $f_\eta$  is defined at  $(\tau\eta, \sigma\eta)$ , too, and that  $\tau^{-1}\sigma$  is a  $\mathcal{C}$ -generic element of a  $\mathcal{C}$ -component of  $G(\mathcal{G}/\mathcal{F})$ . Therefore

$$\begin{aligned} f_\eta(\eta, \sigma\eta) &= f_\eta(\eta, \tau\eta)f_\eta(\tau\eta, \sigma\eta) \\ &= f_\eta(\eta, \tau\eta)\tau(f_\eta(\eta, \tau^{-1}\sigma\eta)) \\ &= f(\tau)\tau(f(\tau^{-1}\sigma)) = f(\tau \cdot \tau^{-1}\sigma) = f(\sigma). \end{aligned}$$

This completes the proof of part (a) of the theorem.

For part (b) we observe that for any  $\mathcal{F}$ -mapping  $h \in \mathcal{M}_{\mathcal{F}}(W, G)$ ,  $h$  is defined at  $\eta$  and  $h(\eta) \in G_{\mathcal{G}}$ , and conversely, for any  $\alpha \in G_{\mathcal{G}} = G_{\mathcal{F}(\eta)}$ , there exists an  $h \in \mathcal{M}_{\mathcal{F}}(W, G)$  such that  $h(\eta) = \alpha$ . Thus, for given cocycles  $f, f' \in Z(\mathcal{G}/\mathcal{F}, G)$ , there exists an  $\alpha \in G_{\mathcal{G}}$  such that  $f'(\sigma) = \alpha^{-1}f(\sigma)\sigma\alpha$  ( $\sigma \in G(\mathcal{G}/\mathcal{F})$ ) if and only if there exists an  $h \in \mathcal{M}_{\mathcal{F}}(W, G)$  such that  $f'_\eta(\eta, \sigma\eta) = h(\eta)^{-1}f_\eta(\eta, \sigma\eta)h(\sigma\eta)$  ( $\sigma \in G(\mathcal{G}/\mathcal{F})$ ), and therefore  $f'$  is cohomologous to  $f$  if and only if  $f'_\eta$  is  $\mathcal{F}$ -cohomologous to  $f_\eta$ .

**Corollary 1** *Let the hypothesis and notation be as in Theorem 7.*

(a) *There exists a unique mapping  $H^1(\mathcal{G}/\mathcal{F}, G) \rightarrow H_{\mathcal{F}}^1(W, G)$  that, for each  $f \in Z^1(\mathcal{G}/\mathcal{F}, G)$ , sends the cohomology class of  $f$  to the  $\mathcal{F}$ -cohomology class of  $f_\eta$ . This mapping is an injective homomorphism of pointed sets, and of groups when  $G$  is commutative.*

(b) *The homomorphism given in part (a) followed by the homomorphism  $H_{\mathcal{F}}^1(W, G) \rightarrow H^1(\mathcal{F}, G)$  given in Chapter V, Section 17, Theorem 12 and its Corollary 1, is an injective homomorphism  $H^1(\mathcal{G}/\mathcal{F}, G) \rightarrow H^1(\mathcal{F}, G)$  that is canonical (being independent of the choice of  $\eta$ ).*

*Proof* Part (a) is an immediate consequence of the theorem. Part (b) follows by Chapter V, Section 17, Corollary 3 to Theorem 12.

**Corollary 2** (a) *Each of the following five conditions is sufficient for  $H^1(\mathcal{G}/\mathcal{F}, G)$  to be trivial: (i)  $G = \mathbf{G}_a$ ; (ii)  $G = \mathbf{G}_m$ ; (iii)  $G = \mathbf{GL}(n)$ ; (iv)  $G = \mathbf{SL}(n)$ ; (v)  $\mathcal{F}$  is algebraically closed.*

(b) *If  $G$  is commutative, then every element of the commutative group  $H^1(\mathcal{G}/\mathcal{F}, G)$  has finite order.*

*Proof* This follows from Corollary 1(b), and Chapter V, Section 12, Theorem 9.

**Corollary 3** *Let the hypothesis and notation be as in Theorem 7. Let  $f \in Z^1(\mathcal{G}/\mathcal{F}, G)$ , let  $\varphi$  be an element of the image of the cohomology class of  $f$  under the canonical injection  $H^1(\mathcal{G}/\mathcal{F}, G) \rightarrow H^1(\mathcal{F}, G)$ , and let  $M$  be a principal homogeneous  $\mathcal{F}$ -space for  $G$ . Then  $f$  splits in  $M$  if and only if  $\varphi$  splits in  $M$ .*

*Proof* There exists an element  $\beta \in M_{\mathcal{G}} = M_{\mathcal{F}(\eta)}$  with  $f(\sigma) = \beta^{-1}\sigma\beta$  for every  $\sigma$  if and only if there exists an  $h \in \mathcal{M}_{\mathcal{F}}(W, M)$  with  $f_\eta(\eta, \sigma\eta) = h(\eta)^{-1}h(\sigma\eta)$  for every  $\sigma$ . Thus  $f$  splits in  $M$  if and only if  $f_\eta$   $\mathcal{F}$ -splits in  $M$ . Therefore the desired conclusion follows from Chapter V, Section 17, Corollary 2 to Theorem 12.

## 9 Applications

We continue with the differential field  $\mathcal{F}$ , its field of constants  $\mathcal{C}$ , and the  $\mathcal{C}$ -group  $G$ . If  $\mathcal{G}$  is a  $G$ -extension of  $\mathcal{F}$ , that is, if  $\mathcal{G}$  is a strongly normal extension of  $\mathcal{F}$  and there exists an injective  $\mathcal{C}$ -homomorphism  $c: G(\mathcal{G}/\mathcal{F}) \rightarrow G_{\mathcal{X}}$ , we can consider  $c$  as a mapping of  $G(\mathcal{G}/\mathcal{F})$  into  $G$ . It is easy to see that then  $c$  satisfies the first three conditions in the definition of a cocycle of  $G(\mathcal{G}/\mathcal{F})$  into  $G$ . Furthermore, since  $c(\tau) \in G_{\mathcal{X}}$  ( $\tau \in G(\mathcal{G}/\mathcal{F})$ ),

$$c(\sigma\tau) = c(\sigma)c(\tau) = c(\sigma)\sigma(c(\tau)) \quad (\sigma, \tau \in G(\mathcal{G}/\mathcal{F})).$$

Therefore  $c \in Z^1(\mathcal{G}/\mathcal{F}, G)$ .

**Theorem 8** Let  $\mathcal{F}$  be a differential field with field of constants  $\mathcal{C}$ , let  $G$  be a connected  $\mathcal{C}$ -group, and let  $\mathcal{G}$  be a  $G$ -extension of  $\mathcal{F}$  and  $c: G(\mathcal{G}/\mathcal{F}) \rightarrow G_{\mathcal{X}}$  be an injective  $\mathcal{C}$ -homomorphism.

(a) If  $c \in B^1(\mathcal{G}/\mathcal{F}, G)$ , then there exists a  $G$ -primitive  $\alpha$  over  $\mathcal{F}$  such that  $\mathcal{G} = \mathcal{F}\langle\alpha\rangle$  and  $\sigma\alpha = \alpha c(\sigma)$  ( $\sigma \in G(\mathcal{G}/\mathcal{F})$ ).

(b) If  $G$  is commutative, then there exist a nonzero  $r \in \mathbf{N}$  and a  $G$ -primitive  $\alpha$  over  $\mathcal{F}$  such that  $\mathcal{F} \subset \mathcal{F}\langle\alpha\rangle \subset \mathcal{G}$ ,  $\mathcal{G}$  is of finite degree over  $\mathcal{F}\langle\alpha\rangle$ , and  $\sigma\alpha = \alpha c(\sigma)^r$  ( $\sigma \in G(\mathcal{G}/\mathcal{F})$ ).

*Proof* (a) Let  $c \in B^1(\mathcal{G}/\mathcal{F}, G)$ . Then there exists an  $\alpha \in G_{\mathcal{G}}$  such that  $c(\sigma) = \alpha^{-1}\sigma\alpha$  ( $\sigma \in G(\mathcal{G}/\mathcal{F})$ ). For any index  $i$ ,  $\sigma(l\delta_i(\alpha)) = l\delta_i(\sigma\alpha) = l\delta_i(\alpha c(\sigma)) = l\delta_i(\alpha)$ , so that  $l\delta_i(\alpha) \in \mathfrak{L}_{\mathcal{F}}(G)$ . Hence  $\alpha$  is a  $G$ -primitive over  $\mathcal{F}$ . Of course,  $\mathcal{F} \subset \mathcal{F}\langle\alpha\rangle \subset \mathcal{G}$ , and if  $\sigma \in G(\mathcal{G}/\mathcal{F}\langle\alpha\rangle)$ , then  $\sigma\alpha = \alpha$ , whence  $c(\sigma) = \alpha^{-1}\sigma\alpha = 1$  so that  $\sigma = id_{\mathcal{G}}$ . Therefore  $\mathcal{F}\langle\alpha\rangle = \mathcal{G}$ .

(b) Let  $G$  be commutative. By Section 8, Corollary 2 to Theorem 7, there is a nonzero  $r \in \mathbf{N}$  such that  $c^r \in B^1(\mathcal{G}/\mathcal{F}, G)$ . Then there exists an  $\alpha \in G_{\mathcal{G}}$  such that  $c(\sigma)^r = \alpha^{-1}\sigma\alpha$  ( $\sigma \in G(\mathcal{G}/\mathcal{F})$ ). As in the proof of part (a), we find that  $\alpha$  is a  $G$ -primitive over  $\mathcal{F}$  and  $\mathcal{F} \subset \mathcal{F}\langle\alpha\rangle \subset \mathcal{G}$ , but this time if  $\sigma \in G(\mathcal{G}/\mathcal{F}\langle\alpha\rangle)$ , then  $c(\sigma)^r = c(\sigma)^r = 1$ , whence  $\sigma^r = id_{\mathcal{G}}$ . However, by Chapter V, Section 22, Corollary to Theorem 14, the group of all elements  $\sigma \in G(\mathcal{G}/\mathcal{F})$  with  $\sigma^r = id_{\mathcal{G}}$  is finite, so that  $G(\mathcal{G}/\mathcal{F}\langle\alpha\rangle)$  is finite, too. Therefore, by Section 4, Corollary 1 to Theorem 4,  $\mathcal{G}$  is algebraic (and hence of finite degree) over  $\mathcal{F}$ .

**Corollary 1** Let  $\mathcal{F}$  be a differential field with field of constants  $\mathcal{C}$  and let  $G$  be a connected  $\mathcal{C}$ -group. If  $H^1(\mathcal{F}, G) = 1$ , then every  $G$ -extension of  $\mathcal{F}$  is a  $G$ -primitive extension of  $\mathcal{F}$ .

*Proof* Let  $\mathcal{G}$  be a  $G$ -extension of  $\mathcal{F}$ . By Section 8, Corollary 1 to Theorem 7,  $H^1(\mathcal{G}/\mathcal{F}, G)$  can be injected into  $H^1(\mathcal{F}, G)$ . Hence if  $H^1(\mathcal{F}, G) = 1$ , then  $Z^1(\mathcal{G}/\mathcal{F}, G) = B^1(\mathcal{G}/\mathcal{F}, G)$ , and the desired conclusion follows from Theorem 8(a).

**Corollary 2** Every  $G_a$ -extension of  $\mathcal{F}$  is an extension by an element that is primitive over  $\mathcal{F}$ . Every  $G_m$ -extension of  $\mathcal{F}$  is an extension by an element that is exponential over  $\mathcal{F}$ . Every linear extension of  $\mathcal{F}$  is a Picard-Vessiot extension of  $\mathcal{F}$ .

*Proof* This follows from Corollary 1 and Section 8, part (a) of Corollary 2 to Theorem 7.

**Corollary 3** Let  $\mathcal{G}$  be a strongly normal extension of  $\mathcal{F}$ , and let  $\mathcal{F}^\circ$  denote the algebraic closure of  $\mathcal{F}$  in  $\mathcal{G}$ . There exist an Abelian  $\mathcal{C}$ -group  $A$  and a differential field  $\mathcal{E}$  between  $\mathcal{F}^\circ$  and  $\mathcal{G}$  such that  $\mathcal{E}$  is an  $A$ -primitive extension of  $\mathcal{F}^\circ$  and  $\mathcal{G}$  is a Picard-Vessiot extension of  $\mathcal{E}$ .

*Proof* By Section 4, Corollary 1 to Theorem 4,  $G(\mathcal{G}/\mathcal{F}^\circ)$  is a connected  $\mathcal{C}$ -group. By the Chevalley-Barsotti structure theorem (Chapter V, Section 24),  $G(\mathcal{G}/\mathcal{F}^\circ)$  has a normal linear connected  $\mathcal{C}$ -subgroup  $L$  such that  $G(\mathcal{G}/\mathcal{F}^\circ)/L$  is Abelian, and by Section 4, Theorem 3, there exists a differential field  $\mathcal{E}^\circ$  between  $\mathcal{F}^\circ$  and  $\mathcal{G}$  such that  $L = G(\mathcal{G}/\mathcal{E}^\circ)$ . Thus  $G(\mathcal{G}/\mathcal{F}^\circ)/L$  is  $\mathcal{C}$ -isomorphic to  $A_{\mathcal{X}}$  for some Abelian  $\mathcal{C}$ -group  $A$ . By Section 4, Theorem 4,  $\mathcal{E}^\circ$  is an  $A$ -extension of  $\mathcal{F}^\circ$ , so that by Theorem 8(b), there exists a differential field  $\mathcal{E}$  between  $\mathcal{F}^\circ$  and  $\mathcal{E}^\circ$  such that  $\mathcal{E}$  is an  $A$ -primitive extension of  $\mathcal{F}^\circ$  and  $\mathcal{E}^\circ$  is algebraic over  $\mathcal{E}$ . Because  $G(\mathcal{G}/\mathcal{E}^\circ) = L$  is connected,  $\mathcal{G}$  is a regular extension of  $\mathcal{E}^\circ$ , so that  $\mathcal{E}^\circ$  is the algebraic closure of  $\mathcal{E}$  in  $\mathcal{G}$ . By Section 4, Corollary 1 to Theorem 4,  $G^\circ(\mathcal{G}/\mathcal{E}) = G(\mathcal{G}/\mathcal{E}^\circ)$ , and since this  $\mathcal{C}$ -group is linear, it follows from Chapter V, Section 23, Proposition 32(c), that  $G(\mathcal{G}/\mathcal{E})$  is linear. Hence by Corollary 2,  $\mathcal{G}$  is a Picard-Vessiot extension of  $\mathcal{E}$ .

## EXERCISES

1. Prove the dotted implication in Section 6, Exercise 7.
2. Let  $\mathcal{G}$  be a Picard-Vessiot extension of  $\mathcal{F}$  and let  $\mathcal{F}_1$  be an intermediate differential field that is strongly normal over  $\mathcal{F}$  (see Section 4, Theorem 4). Prove that  $\mathcal{F}_1$  is a Picard-Vessiot extension of  $\mathcal{F}$ . (*Hint*: See Chapter V, Section 23, Proposition 34.)

10  $V$ -Primitives

Corollary 3 to Theorem 8 does not give a complete description of the strongly normal extensions of a given differential field  $\mathcal{F}$ , not even of the regular ones. For if, for some Abelian  $\mathcal{C}$ -group  $A$ ,  $\mathcal{E}$  is an  $A$ -primitive extension of  $\mathcal{F}$  and  $\mathcal{G}$  is a Picard-Vessiot extension of  $\mathcal{E}$ , then  $\mathcal{G}$  need not be strongly normal over  $\mathcal{F}$ . In what follows we obtain a more complete and precise description.

Let  $G$  be a connected  $\mathcal{C}$ -group, and consider any principal homogeneous  $\mathcal{F}$ -space  $V$  for  $G$ . When  $V$  is not  $\mathcal{F}$ -isomorphic to the regular  $\mathcal{F}$ -space for  $G$ , then  $V$  does not have an element that is rational over  $\mathcal{F}$ , but  $V$  always has an element that is algebraic over  $\mathcal{F}$ . Choose such an element  $u$ . Then  $\lambda_u: G \rightarrow V$  is an  $\mathcal{F}(u)$ -isomorphism of principal homogeneous  $\mathcal{F}$ -spaces for  $G$ . The corresponding Lie algebra isomorphism  $\lambda_u^*: \mathfrak{L}(G) \rightarrow \mathfrak{L}(V)$  maps  $\mathfrak{L}_{\mathcal{F}(u)}(G)$  onto  $\mathfrak{L}_{\mathcal{F}(u)}(V)$ .

There exists a normal field extension of  $\mathcal{F}$  of finite degree containing  $\mathcal{F}(u)$ . Of course such a field extension is an extension of  $\mathcal{F}$  and every automorphism of the field extension is an automorphism of the extension. Choose any such normal extension  $\mathcal{E}$ , and denote its Galois group  $g(\mathcal{E}/\mathcal{F})$  by  $g$ . For each index  $i$  with  $1 \leq i \leq m$ , the formula

$$v \mapsto \frac{1}{[\mathcal{E}:\mathcal{F}]} \sum_{\gamma \in g} \lambda_{\gamma u}^* (l\delta_i(\lambda_{\gamma u}^{-1}(v)))$$

then defines a mapping of  $V$  into  $\mathfrak{L}(V)$ , which evidently is independent of the choice of  $\mathcal{E}$ . We denote this mapping by

$$l_u \delta_i: V \rightarrow \mathfrak{L}(V).$$

**Proposition 14** *Let  $\mathcal{F}$  be a differential field,  $\mathcal{C}$  be its field of constants,  $G$  be a connected  $\mathcal{C}$ -group, and  $V$  be a principal homogeneous  $\mathcal{F}$ -space for  $G$ . Let  $u, u' \in V_{\mathcal{F}_\bullet}$  and  $v, v' \in V$ .*

- (a)  $l_u \delta_i(v) \in \mathfrak{L}_{\mathcal{F}\langle v \rangle}(V)$  ( $1 \leq i \leq m$ ).  
 (b) If  $\sigma$  is any isomorphism of  $\mathcal{F}\langle v \rangle$  over  $\mathcal{F}$ , then

$$\sigma(l_u \delta_i(v)) = l_u \delta_i(\sigma v) \quad (1 \leq i \leq m).$$

- (c) If  $x$  is any element of  $G$ , then

$$l_u \delta_i(vx) = l_u \delta_i(v) + \lambda_v^* (l\delta_i(x)) \quad (1 \leq i \leq m).$$

- (d)  $l_u \delta_i(v) = l_u \delta_i(v')$  ( $1 \leq i \leq m$ ) if and only if  $v^{-1}v' \in G_{\mathcal{F}}$ .  
 (e)  $l_{u'} \delta_i(v) - l_u \delta_i(v) \in \mathfrak{L}_{\mathcal{F}}(V)$  ( $1 \leq i \leq m$ ).

*Proof* Fix a normal extension  $\mathcal{E}$  of  $\mathcal{F}$ , as above. Then  $\mathcal{E}\langle v \rangle$  is a normal extension of  $\mathcal{F}\langle v \rangle$ , and evidently  $l_u \delta_i(v) \in \mathfrak{L}_{\mathcal{E}\langle v \rangle}(V)$ . For any isomorphism  $\tau$  of  $\mathcal{E}\langle v \rangle$  over  $\mathcal{F}$ , and for any  $\gamma \in g$  and  $\delta_i$ , we see from Chapter V, the penultimate equation in Section 20, that

$$\tau(\lambda_{\gamma u}^* (l\delta_i(\lambda_{\gamma u}^{-1}(v)))) = \tau(\lambda_{\gamma u}^* (\tau(l\delta_i(\lambda_{\gamma u}^{-1}(v)))).$$

However, by Chapter V, Section 22, Proposition 28(b),

$$\tau(\lambda_{\gamma u}^* \tau(l\delta_i(\lambda_{\gamma u}^{-1}(v)))) = \lambda_{\tau\gamma u}^* (l\delta_i(\tau(\lambda_{\gamma u}^{-1}(v)))) = \lambda_{\tau\gamma u}^* (l\delta_i(\lambda_{\tau\gamma u}^{-1}(\tau v))).$$

Therefore we have the equation

$$\tau(l_u \delta_i(v)) = l_u \delta_i(\tau v).$$

This shows, in particular, that  $l_u \delta_i(v)$  is invariant under the Galois group  $g(\mathcal{E}\langle v \rangle/\mathcal{F}\langle v \rangle)$ , so that  $l_u \delta_i(v) \in \mathfrak{L}_{\mathcal{F}\langle v \rangle}(V)$ , proving (a). Since any isomorphism  $\sigma$  of  $\mathcal{F}\langle v \rangle$  over  $\mathcal{F}$  can be extended to an isomorphism  $\tau$  of  $\mathcal{E}\langle v \rangle$  over  $\mathcal{F}$ , it proves (b) too.

By Chapter V, Section 22, Theorem 14,

$$\begin{aligned} l_u \delta_i(vx) &= \frac{1}{[\mathcal{E}:\mathcal{F}]} \sum_{\gamma \in g} \lambda_{\gamma u}^* (l\delta_i(\lambda_{\gamma u}^{-1}(vx))) \\ &= \frac{1}{[\mathcal{E}:\mathcal{F}]} \sum_{\gamma \in g} \lambda_{\gamma u}^* (l\delta_i(\lambda_{\gamma u}^{-1}v) + \lambda_{\gamma u}^{-1} \cdot v^* (l\delta_i(x))) \\ &= l_u \delta_i(v) + \frac{1}{[\mathcal{E}:\mathcal{F}]} \sum_{\gamma \in g} \lambda_v^* l\delta_i(x) \\ &= l_u \delta_i(v) + \lambda_v^* (l\delta_i(x)). \end{aligned}$$

This proves (c). Setting  $x = v^{-1}v'$ , we therefore see that

$$\begin{aligned} l_u \delta_i(v) = l_u \delta_i(v') \quad (1 \leq i \leq m) &\Leftrightarrow l\delta_i(x) = 0 \quad (1 \leq i \leq m) \\ &\Leftrightarrow x \in G_{\mathcal{F}}. \end{aligned}$$

This proves (d).

To prove (e) we may suppose that  $\mathcal{E} \supset \mathcal{F}(u, u')$  and set  $y = u^{-1}u'$ . Then  $y \in G_{\mathcal{E}}$  and

$$\begin{aligned} l_{u'} \delta_i(v) &= \frac{1}{[\mathcal{E}:\mathcal{F}]} \sum_{\gamma \in g} \lambda_{\gamma u'}^* (l\delta_i(\lambda_{\gamma u'}^{-1}(v))) \\ &= \frac{1}{[\mathcal{E}:\mathcal{F}]} \sum_{\gamma \in g} \lambda_{\gamma u}^* (l\delta_i(\gamma y^{-1} \cdot \lambda_{\gamma u}^{-1}(v))) \\ &= \frac{1}{[\mathcal{E}:\mathcal{F}]} \sum_{\gamma \in g} \lambda_{\gamma u}^* (l\delta_i(\gamma y^{-1}) + \lambda_{\gamma y^{-1}}^* (l\delta_i(\lambda_{\gamma u}^{-1}(v)))) \\ &= \frac{1}{[\mathcal{E}:\mathcal{F}]} \sum_{\gamma \in g} (\gamma(\lambda_u^* (l\delta_i(y^{-1}))) + \lambda_{\gamma u}^* (l\delta_i(\lambda_{\gamma u}^{-1}(v)))) \\ &= \frac{1}{[\mathcal{E}:\mathcal{F}]} \sum_{\gamma \in g} \gamma(\lambda_u^* (l\delta_i(y^{-1}))) + l_u \delta_i(v). \end{aligned}$$

Since  $y \in G_\delta$  and  $u' \in V_\delta$ , we have  $\lambda_{u'}^\#(I\delta_i(y^{-1})) \in \mathfrak{L}_\delta(V)$ , and hence the sum over  $\mathfrak{g}$  here is in  $\mathfrak{L}_\mathcal{F}(V)$ . This proves (e) and completes the proof of the proposition.

By a  $V$ -primitive over  $\mathcal{F}$  we shall mean an element  $\eta \in V$  having the property that

$$I_u \delta_i(\eta) \in \mathfrak{L}_\mathcal{F}(V) \quad (1 \leq i \leq m)$$

for some element  $u \in V_{\mathcal{F}_\mathfrak{a}}$ . By part (e) of Proposition 14,  $\eta$  must then have this property for every element  $u \in V_{\mathcal{F}_\mathfrak{a}}$ .

The following theorem describes the  $G$ -extensions of  $\mathcal{F}$ .

**Theorem 9** *Let  $\mathcal{F}$  be a differential field,  $\mathcal{C}$  be its field of constants, and  $G$  be a connected  $\mathcal{C}$ -group.*

(a) *If  $V$  is a principal homogeneous  $\mathcal{F}$ -space for  $G$  and  $\eta$  is a  $V$ -primitive over  $\mathcal{F}$  such that the field of constants of  $\mathcal{F}\langle\eta\rangle$  is  $\mathcal{C}$ , then  $\mathcal{F}\langle\eta\rangle$  is a strongly normal extension of  $\mathcal{F}$  and the formula  $c(\sigma) = \eta^{-1}\sigma\eta$  defines an injective  $\mathcal{C}$ -homomorphism  $c: G(\mathcal{F}\langle\eta\rangle/\mathcal{F}) \rightarrow G_\mathcal{X}$ .*

(b) *If  $\mathcal{G}$  is a strongly normal extension of  $\mathcal{F}$  and  $c: G(\mathcal{G}/\mathcal{F}) \rightarrow G_\mathcal{X}$  is an injective  $\mathcal{C}$ -homomorphism, then there exist a principal homogeneous  $\mathcal{F}$ -space  $V$  for  $G$  and a  $V$ -primitive  $\eta$  over  $\mathcal{F}$  such that  $\mathcal{G} = \mathcal{F}\langle\eta\rangle$  and  $\sigma\eta = \eta c(\sigma)$  ( $\sigma \in G(\mathcal{G}/\mathcal{F})$ ).  $V$  is unique up to  $\mathcal{F}$ -isomorphism.*

*Proof* (a) Because of Proposition 14, we can copy the proof of Theorem 6 in Section 7.

(b) As we saw in the beginning of Section 9,  $c \in Z^1(\mathcal{G}/\mathcal{F}, G)$ . The canonical injection  $H^1(\mathcal{G}/\mathcal{F}, G) \rightarrow H^1(\mathcal{F}, G)$  associates to the cohomology class of  $c$  some cohomology class in  $Z^1(\mathcal{F}, G)$ . Fix an element  $\varphi$  of the latter cohomology class. By Chapter V, Section 13, Theorem 10 and the remark thereafter,  $\varphi$  splits in some principal homogeneous  $\mathcal{F}$ -space  $V$  for  $G$ , this  $V$  being unique up to  $\mathcal{F}$ -isomorphism. The desired conclusion now follows from Section 8, Corollary 3 to Theorem 7.

## Bibliography for Chapter VI

1. R. Baer. Gegenwärtig Stand der Picard-Vessiot'schen Theorie, a communication included among remarks by O. Haupt in F. Klein's "Vorlesungen über Hypergeometrische Funktionen." Julius Springer, Berlin, 1933.
2. E. Beke. Die Irreducibilität der homogenen linearen Differentialgleichungen, *Math. Ann.* **45** (1894), 278–294.
3. E. Beke. Die symmetrischen Funktionen bei der linearen homogenen Differentialgleichungen, *Math. Ann.* **45** (1894), 295–300.
4. G. M. Bergman. A counterexample in differential algebra, *Proc. Amer. Math. Soc.* **16** (1965), 1407–1409.
5. A. Bialynicki-Birula. On Galois theory of fields with operators, *Amer. J. Math.* **84** (1962), 89–109.
6. A. Bialynicki-Birula. On the inverse problem of Galois theory of differential fields, *Bull. Amer. Math. Soc.* **16** (1963), 960–964.
7. M. P. Epstein. An existence theorem in the algebraic study of homogeneous linear ordinary differential equations, *Proc. Amer. Math. Soc.* **6** (1955), 33–41.
8. M. P. Epstein. On the theory of Picard-Vessiot extensions, *Ann. of Math.* **62** (1955), 528–547.
9. G. Fano. Ueber lineare homogene Differentialgleichungen mit algebraischen Relationen zwischen den Fundamentallösungen, *Math. Ann.* **53** (1900), 493–590.
10. L. Goldman. Specializations and Picard-Vessiot theory, *Trans. Amer. Math. Soc.* **85** (1957), 327–356.
11. L. Goldman. Lowest order equations for zeros of a homogeneous linear differential polynomial, *Illinois J. Math.* **2** (1958), 567–576.
12. L. Goldman. Solutions of first order differential equations which are solutions of linear differential equations of higher order, *Proc. Amer. Math. Soc.* **10** (1959), 936–939.
13. I. Kaplansky. "An Introduction to Differential Algebra." Hermann, Paris, 1957.

14. E. R. Kolchin. The Picard–Vessiot theory of homogeneous linear ordinary differential equations, *Proc. Nat. Acad. Sci. U.S.A.* **32** (1946), 308–311.
15. E. R. Kolchin. Algebraic matrix groups and the Picard–Vessiot theory of homogeneous linear ordinary differential equations, *Ann. of Math.* **49** (1948), 1–42.
16. E. R. Kolchin. Existence theorems connected with the Picard–Vessiot theory of homogeneous linear ordinary differential equations, *Bull. Amer. Math. Soc.* **54** (1948), 927–932.
17. E. R. Kolchin. Picard–Vessiot theory of partial differential fields, *Proc. Amer. Math. Soc.* **3** (1952), 596–603.
18. E. R. Kolchin. Galois theory of differential fields, *Amer. J. Math.* **75** (1953), 753–824.
19. E. R. Kolchin. On the Galois theory of differential fields, *Amer. J. Math.* **77** (1955), 868–894.
20. E. R. Kolchin. Abelian extensions of differential fields, *Amer. J. Math.* **82** (1960), 779–790.
21. E. R. Kolchin. Algebraic groups and algebraic dependence, *Amer. J. Math.* **90** (1968), 1151–1164.
22. E. R. Kolchin and S. Lang. Algebraic groups and the Galois theory of differential fields, *Amer. J. Math.* **80** (1958), 103–110.
23. E. R. Kolchin and T. Soundararajan. Differential polynomials and strongly normal extensions, *Amer. J. Math.* **94** (1972), 467–472.
24. J. Kovacic. The inverse problem in the Galois theory of differential fields, *Ann. of Math.* **89** (1969), 583–608.
25. J. Kovacic. On the inverse problem in the Galois theory of differential fields, *Ann. of Math.* **93** (1971), 269–284.
26. J. Kovacic. Pro-algebraic groups and the Galois theory of differential fields, *Amer. J. Math.*, to appear.
27. A. Loewy. Ueber die irreduciblen Factoren eines linearen homogenen Differentialausdrückes, *Ber. Verh. Sächs. Ges. Wiss. Leipzig Math.–Phys. Kl.* **54** (1902), 1–13.
28. A. Loewy. Über reduzible lineare homogene Differentialgleichungen, *Math. Ann.* **56** (1902), 549–584.
29. A. Loewy. Die Rationalitätsgruppe einer linearen homogenen Differentialgleichungen, *Math. Ann.* **65** (1908), 129–160.
30. F. Marotte. Les équations différentielles linéaires et la théorie des groupes, *Ann. Fac. Sci. Univ. Toulouse* (1) **12** (1898), H1–H92.
31. H. Matsumura. Automorphism groups of differential fields and group varieties, *Mem. Coll. Sci. Univ. Kyoto Ser. A* **28** (1954), 283–292.
32. K. Okugawa. Basic properties of differential fields of an arbitrary characteristic and the Picard–Vessiot theory, *J. Math. Kyoto Univ.* **2** (1963), 295–322.
- 32a. A. Ostrowski. Sur les relations algébriques entre les intégrales indéfinies, *Acta. Math.* **78** (1946), 315–318.
33. E. Picard. Sur les groupes de transformation des équations différentielles linéaires, *C. R. Acad. Sci. Paris* **96** (1883), 1131–1134.
34. E. Picard. Sur les équations différentielles et les groupes algébriques de transformations, *Ann. Fac. Sci. Univ. Toulouse* (1) **1** (1887), A1–A15.
35. E. Picard. Sur les groupes de transformations des équations différentielles linéaires, *C. R. Acad. Sci. Paris* **119** (1894), 584–589; *Math. Ann.* **46** (1895), 161–166.
36. E. Picard. Sur l’extension des idées de Galois à la théorie des équations différentielles, *C. R. Acad. Sci. Paris* **121** (1895), 789–792; *Math. Ann.* **47** (1896), 155–156.

37. E. Picard. “Traité d’Analyse,” Vol. III, Chapter 17. Gauthier-Villars, Paris, 1898 or 1908 or 1928. Reprinted as “Analogies Entre la Théorie des Équations Différentielles Linéaires et la Théorie des Équations Algébriques.” Gauthier-Villars, Paris, 1936.
38. L. Schlesinger. “Handbuch der Theorie der Lineardifferentialgleichungen,” Vol. II., Teubner, Leipzig, 1897.
39. A. Seidenberg. Contribution to the Picard–Vessiot theory of homogeneous linear differential equations, *Amer. J. Math.* **78** (1956), 808–817.
40. E. Vessiot. Sur les équations différentielles linéaires, *C. R. Acad. Sci. Paris* **112** (1891), 778–780.
41. E. Vessiot. Sur les intégrations des équations différentielles linéaires, *Ann. Sci. Ecole Norm. Sup.* (3) **9** (1892), 192–280.
42. E. Vessiot. Méthodes d’intégrations élémentaires, *Encyclopédie des Sci. Math. Pures et Appl.* Tome II, Vol. 3, Fasc. 1 (1910), pp. 58–170 (esp. pp. 152–165).

## Glossary of Notation

A list of the more or less systematically used symbols, and the pages on which they are first explained.

$P^f, \Sigma^f$	$(P$ a polynomial, $f$ a mapping of the coefficient ring, $\Sigma$ a set of polynomials)	2
$\mathbf{N}, \mathbf{Z}, \mathbf{R}, \mathbf{C}, \mathbf{F}_q$	$(K$ a field)	2
$K_{\mathfrak{a}}, K_{\mathfrak{s}}, K_{\mathfrak{f}}$	$(K$ a field)	2
$\mathfrak{f} : \Sigma, \mathfrak{f} : s, \mathfrak{f} : s^{\infty}$	$(\Sigma$ a subset, $s$ an element, $\mathfrak{f}$ an ideal, of a ring)	2
$\Sigma^{-1}R, \Sigma^{-1}\mathfrak{f}$	$(R$ a ring, $\Sigma$ a multiplicatively stable subset of $R$ , $\mathfrak{f}$ a $\Sigma$ -prime ideal of $R$ )	7
$Q(R)$	$(R$ a ring)	7
$R_{\mathfrak{p}}$	$(R$ a ring, $\mathfrak{p}$ a prime ideal of $R$ )	7
$(\Sigma)_{\mathfrak{C}}$	$(\Sigma$ a subset of a module, $\mathfrak{C}$ a conservative system of the module)	11
$\mathfrak{C} \mathfrak{r}, \mathfrak{C}/\mathfrak{f}, \Sigma^{-1}\mathfrak{C}$	$(\mathfrak{C}$ a conservative system of a ring $R$ , $\mathfrak{r}$ a subring or ideal of $R$ , $\mathfrak{f}$ an ideal of $R$ , $\Sigma$ a multiplicatively stable subset of $R$ )	12
$\mathfrak{J}(\mathfrak{f})$	$(\mathfrak{f}$ an ideal)	16
$\dim \mathfrak{p}$	$(\mathfrak{p}$ a prime polynomial ideal)	20
$R[[X]]$	$(R$ a ring, $X$ a family of indeterminates)	29
$h_k(A)$	$(A$ a power series)	29
$v(A)$	$(A$ a power series)	30, 33
$R((X))$	$(R$ a ring, $X$ an indeterminate)	33

$J_A$	( $A$ a power series in one indeterminate)	33
$N_n$	( $n$ a natural number)	49
$\omega_E$	( $E$ a subset of $N^m$ )	51
$\nu_I(x)$	( $I$ an ideal and $x$ an element of a ring)	57
$\Delta$		58
$\Theta$		59
ord $\theta$	( $\theta$ a derivative operator)	59
$a', a'', a''', a^{(s)}$	( $a$ an element of an ordinary differential ring)	59
$\mathcal{R}_0\{\Sigma\}$	( $\mathcal{R}_0$ a differential subring and $\Sigma$ a subset of a differential ring)	59
$\mathcal{F}_0\langle\Sigma\rangle$	( $\mathcal{F}_0$ a differential subfield and $\Sigma$ a subset of a differential field)	60
$\mathcal{F}_1, \mathcal{F}_2$	( $\mathcal{F}_1, \mathcal{F}_2$ differential subfields of a differential field)	60
$(\theta')$	( $\theta, \theta'$ derivative operators)	60
$[\Sigma]_{\mathcal{A}}, [\Sigma]$	( $\Sigma$ a subset of a differential ring $\mathcal{R}$ )	61
$\mathcal{R}\{\Sigma\}_{\Delta}, \mathcal{F}\langle\Sigma\rangle_{\Delta}$		65
$\sigma_e$	( $e$ a basis of a vector space, $\sigma$ an automorphism of the field of scalars)	66
$P_e(f)$	( $e$ a basis of a vector space, $f$ a family of vectors)	66
$P_e(W)$	( $e$ a basis of a vector space, $W$ a subspace)	67
deg $G$ , deg $_{\Lambda} G$ , ord $G$	( $G$ a differential polynomial)	70
den $A$	( $A$ a differential polynomial)	72
wt $F$	( $F$ a differential polynomial)	73
$u_A, I_A, S_A$	( $A$ a differential polynomial)	75
$H_A$	( $A$ an autoreduced set)	77
$\mathcal{H}\{\{y_1, \dots, y_n\}\}$		85
$\Theta(s)$		86
$\Delta^{(\rho)}$		93
$\Delta_r^{(\rho)}$		94
$F_{\Sigma}$	( $F$ a differential polynomial, $\Sigma$ a set of "points")	95
$\omega_{\eta/\mathcal{F}}$	( $\mathcal{F}$ a differential field, $\eta$ a finite family with coordinates in an extension of $\mathcal{F}$ )	115
$\omega_{\Phi}$	( $\Phi$ a finite subset of a differential vector space)	118
$\{\Sigma\}_{\mathcal{A}}, \{\Sigma\}$	( $\mathcal{A}$ a differential ring, $\Sigma$ a subset of $\mathcal{A}$ )	122
$\{\Sigma\}_{\mathcal{A}/\mathcal{F}}, \{\Sigma\}_{\mathcal{F}}$	( $\mathcal{A}$ a differential algebra over $\mathcal{F}$ , $\Sigma$ a subset of $\mathcal{A}$ )	122
$\omega_p$	( $p$ a prime differential ideal of differential polynomials)	129
$\mathfrak{J}(\Sigma)$	( $\Sigma$ a set of differential polynomials)	145
$\bar{\mathcal{M}}$	( $\mathcal{M}$ a subset of a differential affine space)	146
$\mathfrak{M}(\mathcal{M})$	( $\mathcal{M}$ a subset of a differential affine space)	147
$\omega_V$	( $V$ an irreducible closed subset of a differential affine space)	148
$\mathcal{F}\{y_1, \dots, y_n\}_1$		150

$p_{\mathcal{F}}(A)$	( $A$ a pseudo-led irreducible differential polynomial over $\mathcal{F}$ )	155, 157
$F_*, F^*$	( $F$ a differential polynomial)	175
Aut( $U/K$ )	( $U$ a field, $K$ a subfield)	212
$G_u, G_m$		213
GL( $n$ ), SL( $n$ ), O( $n$ ), T( $n$ ), T( $n, k$ ), D( $n$ )		213
W( $g_2, g_3$ )		213
$K(x)$	( $K$ a field, $x$ an element of a pre- $K$ -set)	214
$x \xrightarrow{K} x', x \xleftarrow{K} x'$		215
$S_{x', x}^K$		215
dim $_L x$		215
$A_L$	( $A$ a pre- $K$ -set, $L$ an extension of $K$ )	216
$x \rightarrow x', x \leftrightarrow x', S_{x', x}$		216
$\sigma x$	( $x$ an element of a pre- $K$ -set, $\sigma$ an isomorphism over $K$ of an overfield of $K(x)$ )	216
$\Gamma_{A/K}$	( $A$ a pre- $K$ -set)	216
dim $A$	( $A$ a pre- $K$ -set)	216
$G^{\circ}$	( $G$ a $K$ -group)	216
$\lambda_y, \rho_y, \lambda_w$		223, 232
$K(A)$	( $A$ a closed subset of a homogeneous $K$ -space)	227
$g_v$	( $g$ a group operating on a set, $v$ an element of the set)	241, 243
$N_A, C_A$	( $A$ a subset of a $K$ -group)	257
$[b, i]$	( $b, i$ subgroups of a group)	264
$\pi_{G/H}$	( $H$ a subgroup of a group $G$ )	265
$g(L/K)$	( $L$ a Galois extension of a field $K$ )	269
$H^{\circ}(L/K, G), H^{\circ}(K, G)$	( $K$ a field, $L$ an extension of $K$ , $G$ a $K$ -group)	273
$Z^1(L/K, G), H^1(L/K, G), B^1(L/K, G)$	( $K$ a field, $L$ an extension of $K$ , $G$ a $K$ -group)	274
$Z^1(K, G), H^1(K, G), B^1(K, G)$	( $K$ a field, $G$ a $K$ -group)	274–275
$\Phi_{M, v}$	( $M$ a principal homogeneous $K$ -space, $v \in M_{K^*}$ )	276
$\mathcal{P}_K(G)$	( $G$ a $K$ -group)	281
$\nu_F, \tilde{F}$	( $F$ a surjective ring homomorphism with prime kernel)	287
$\mathfrak{M}_K(A, B), \mathfrak{M}_{K, v}(A, B), \mathfrak{M}_{K, \Sigma}(A, B)$	( $A$ and $B$ $K$ -sets, $v \in A, \Sigma \subset A$ )	288
$g \circ f$		296
$f^-$		299
$\mu_M$	( $M$ a homogeneous $K$ -space)	301
$\psi_M$	( $M$ a principal homogeneous $K$ -space)	301
$k_w$	( $w$ an element of a $K$ -set)	301
$in_{B, B'}$	( $B'$ a $K$ -subset of a $K$ -set $B$ )	301
$f_1 \times \dots \times f_n$	( $f_j$ a $K$ -mapping of a $K$ -set $A$ into a $K$ -set $B_j$ )	302
$\iota_G$	( $G$ a group)	302
$\mathfrak{M}(A, B), \mathfrak{M}_v(A, B), \mathfrak{M}_{\Sigma}(A, B)$		302



$\mathfrak{F}_K(A), \mathfrak{F}(A), \mathfrak{F}_r(A), \mathfrak{F}_{K,r}(A), \mathfrak{F}_Z(A), \mathfrak{F}_{K,Z}(A)$	306
$f^*$ ( $f$ a $K$ -mapping)	312
$Z_K^1(A, G), B_K^1(A, G), H_K^1(A, G)$ ( $A$ a $K$ -set, $G$ a $K$ -group)	318-319
$P_f$ ( $f$ a $K$ -cocycle)	319
$f_u$ ( $f \in Z_K^1(A, G), u \in P_f \cap A_{K_s}$ )	320
$\mathfrak{D}(V), \mathfrak{D}_K(V)$ ( $V$ an irreducible $K$ -set)	322
$\mathfrak{D}^*(V)$	323
$\langle \mathfrak{D}, \omega \rangle$	323
$\mathfrak{D}_K^*(V)$	323
$d\varphi$	323
$\sigma(D)$ ( $D \in \mathfrak{D}(V), \sigma \in \text{Aut}(U/K)$ )	323
$\sigma(\omega)$ ( $\omega \in \mathfrak{D}^*(V), \sigma \in \text{Aut}(U/K)$ )	324
$f^{**}, f^{***}$ ( $f$ a generically invertible $K$ -mapping)	324
$\mathfrak{V}(V), \mathfrak{V}_K(V), \mathfrak{V}^*(V), \mathfrak{V}_K^*(V)$ ( $V$ a homogeneous $K$ -space)	325
$\mathfrak{m}_r(V), \mathfrak{m}_{K,r}(V)$ ( $V$ an irreducible $K$ -set)	331
$f_r^*$ ( $f$ a $K$ -mapping defined at $v$ )	331
$f_r^{(k)}$ ( $f$ a $K$ -mapping defined at $v, k \in \mathbb{N}$ )	333
$\tau_x, \tau_x^\circ$ ( $x$ an element of a $K$ -group)	333
$\mathfrak{I}_r(V), \mathfrak{I}_{L,r}(V)$ ( $V$ an irreducible $K$ -set)	335
$\mathfrak{I}_r^*(V), \mathfrak{I}_{L,r}^*(V)$	335
$f_r^{**}, f_r^{***}$ ( $f$ a $K$ -mapping defined at $v$ )	335
$\mathcal{O}_v$ ( $V$ an irreducible $K$ -set)	337
$\mathfrak{D}_v(V), \mathfrak{D}_v^*(V)$	338
$D_v$ ( $D \in \mathfrak{D}_v(V)$ )	338
$\omega_r$ ( $\omega \in \mathfrak{V}^*(V)$ )	339
$f_v^\#, f_v^{\#*}$ ( $f$ a $K$ -mapping defined at $v$ )	340
$\gamma_x, \gamma_x'$	342
$f^\#, f^{\#*}$ ( $f$ a relative $K$ -homomorphism of principal homogeneous $K$ -spaces)	345
$i_{v1}, i_{v2}$	347
$\Delta_V, \Delta_G$	347
$l\delta(v)$	349
$l\delta$	350
$P_e$ ( $e \in \mathbb{Z}$ )	362
$x^t$ ( $x$ a unipotent matrix, $t \in U$ )	364
$x_s, x_u$ ( $x \in \mathbf{GL}(n)$ )	366
— ( $x$ an element of a linear $K$ -group)	367
$\mathbf{P}(n)$ ( $n \in \mathbb{N}$ )	377
$\mathcal{C}(\sigma)$ ( $\sigma$ an isomorphism of a differential field, $\mathcal{C}$ the field of constants of the differential field)	389
$\sigma \rightarrow \sigma', \sigma \leftrightarrow \sigma', S_{\sigma', \sigma}$	394
$G(\mathcal{G}/\mathcal{F}), G^\circ(\mathcal{G}/\mathcal{F})$	396

$l\Delta$	418
$Z^1(\mathcal{G}/\mathcal{F}, G), B^1(\mathcal{G}/\mathcal{F}, G), H^1(\mathcal{G}/\mathcal{F}, G)$ ( $\mathcal{G}$ a strongly normal extension of the differential field $\mathcal{F}$ with field of constants $\mathcal{C}$ , $G$ a $\mathcal{C}$ -group)	422
$l_u \delta_i$	428

## Index of Definitions

### A

Abelian extension, 396  
Abelian function, 382  
Abelian  $K$ -group, 377  
Additive polynomial, 360  
 $K$ -Affine coordinates, 331–332  
Affine  $K$ -group, 355  
 $K$ -Affine subset of  $K$ -set, 307  
Algebraic codimension, 4  
Algebraic element of pre- $K$ -set, 215–216  
Algebraic group, 212  
Algebraically dependent (or independent)  
  derivative operators, 96  
Algebraically dependent (or independent)  
  over constants, 93  
Artin–Rees lemma, 39  
Autoreduced set, 77

### B

$\mathcal{G}$ -Basis, 11  
Basis theorem, 126  
  historical remark, 128–129  
Bessel differential polynomial, 417  
Bicompatible isomorphisms, 218

Bidefined, 303  
Birational correspondence, 17  
Birationally equivalent ideals, 17

### C

Canonical coordinate functions on  $K$ -sub-  
  group of  $\mathbf{GL}(n)$ , 355  
Characteristic set, 82  
Choice function for characteristic set, 183  
Closed graph, 304  
Closed image, 298  
Closed set in homogeneous  $K$ -space, 240  
 $K$ -closed set in homogeneous  $K$ -space, 240  
Closed set in  $\mathcal{U}^n$ , 146  
 $\mathcal{F}$ -Closed set in  $\mathcal{U}^n$ , 148  
Coboundary  
   $\mathfrak{g}(L/K)$  into  $G$ , 275  
   $G(\mathcal{G}/\mathcal{F})$  into  $G$ , 422  
 $K$ -Coboundary, 319  
Cocycle  
   $\mathfrak{g}(L/K)$  into  $G$ , 274  
   $G(\mathcal{G}/\mathcal{F})$  into  $G$ , 422  
 $K$ -Cocycle, 318  
Coherent autoreduced set, 136, 167  
   $\mathfrak{f}$ -Coherent autoreduced set, 135–136

Cohomologous cocycles  
 $\mathfrak{g}(L/K)$  into  $G$ , 275  
 $G(\mathcal{G}/\mathcal{F})$  into  $G$ , 422  
*K*-Cohomologous *K*-cocycles, 319  
Cohomology set  
 $\mathfrak{g}(L/K)$  into  $G$ , 275  
 $G(\mathcal{G}/\mathcal{F})$  into  $G$ , 422  
*K*-Cohomology set, 319  
Commutator, 264–265  
Commutator group, 265  
Compatible homomorphisms, 218  
Complete differential ring of quotients, 64  
Complete ring of quotients, 7  
Complete *K*-set, 376  
Complex multiplication, 381  
Component of closed subset of homogeneous *K*-space, 243  
Component of 1 of *K*-group, 232  
Component of perfect ideal, 14  
 $\mathcal{U}$ -Component of perfect  $\mathcal{U}$ -ideal, 13  
*K*-component of pre-*K*-set, 216  
Component theorem, 185  
Conjugates of algebraic element of pre-*K*-set, 216  
Conservative mapping, 11  
Conservative system, 10  
Constant, 60–66  
Constrained family (or element) 142  
Constraint, 142  
Cotangent space, 335  
Cotangent vector, 335  
Crossed *K*-homomorphism  
of *K*-group into *K*-group, 343  
of *K*-space into *K*-space, 343

**D**

Defining differential ideal, 71  
Degenerate Abelian function field, 382  
Denomination, 72  
Dependent (or independent) derivative operators, 97  
Derivation on irreducible *K*-set, 322  
*K*-Derivation on irreducible *K*-set, 322  
Derivation operator, 58  
Derivative, 59  
Derivative operator, 59  
Diagonal group, 213  
Differential  
on irreducible *K*-set, 323  
of rational function, 323

*K*-Differential on irreducible *K*-set, 323  
Differential affine space, 145  
Differential algebra, 69  
Differential basis, 108  
Differential conservative system, 121  
Differential dimension  
of differential vector space, 108  
of irreducible closed set in  $\mathbb{A}^n$ , 148  
of prime differential polynomial ideal, 130  
Differential dimension polynomial  
of irreducible closed set in  $\mathbb{A}^n$ , 148  
of prime differential polynomial ideal, 130  
Differential field, 58  
Differential field of definition  
of closed set in  $\mathbb{A}^n$ , 149  
of differential polynomial ideal, 125  
Differential field of quotients, 64  
Differential field extension, 59–60  
Differential grading, 73  
Differential ideal, 61  
Differential indeterminates, 69  
Differential inseparability basis, 105  
Differential inseparability degree  
of extension, 107  
of prime differential polynomial ideal, 129  
Differential inseparability polynomial  
of finite family, 117  
of prime differential polynomial ideal, 129  
Differential integral domain, 58  
Differential module, 66  
Differential monomial, 70  
Differential overfield, 59–60  
Differential overring, 59  
Differential polynomial, 70  
Differential polynomial algebra, 70  
Differential polynomial function, 95  
Differential power series, 85  
Differential power series algebra, 85  
Differential quotient module, 66  
Differential rational fraction, 71  
Differential residue ring, 61  
Differential ring, 58  
Differential ring of quotients, 64  
Differential specialization  
of differential integral domain, 138–139  
of family of elements, 139  
Differential subfield, 59  
Differential submodule, 66  
Differential subring, 59  
Differential subspace, 66

Differential transcendence basis, 108  
Differential transcendence degree, 109  
Difference transcendence polynomial, 117  
Differential type  
of finitely generated extension 118  
of irreducible closed set in  $\mathbb{A}^n$  148  
of prime differential polynomial ideal, 129  
Differential vector space, 66  
Differential Zariski topology, 146  
relative to  $\mathcal{F}$ , 149  
Differentially algebraic closure in extension (characteristic 0), 102  
Differentially algebraic element, 69  
Differentially algebraic extension, 100  
Differentially algebraically dependent (or independent), 69  
Differentially homogeneous, 71  
Differentially inseparable, 99–100  
Differentially linear, 104  
Differentially linearly independent, 108  
Differentially perfect, 92  
Differentially quasi-perfect, 92  
Differentially separable closure in extension, 102  
Differentially separable element, 99–100  
Differentially separable extension, 100  
Differentially separably dependent (or independent), 99  
Differentially transcendental, 69  
Dimension  
of element of a pre-*K*-set, 216  
of pre-*K*-set, 216  
of prime polynomial ideal, 20  
Direct product  
of *K*-groups, 257–258  
of homogeneous *K*-spaces, 258  
Divisible conservative system, 12  
Domain of bidefinition, 303  
Dominate, 178  
factorially, 179  
strongly, 179  
Domination lemma, 181–182

**E**

*K*-Equivalent pre-*K*-mappings, 294  
Essential order, 83  
Exponential, 404  
Extension (of differential field), 59–60  
*G*-Extension, 396

**F**

Field of constants, 60  
Field of definition  
of polynomial ideal, 125  
of subspace of vector space, 67  
*K*-Function, 306  
Fundamental system of zeros, 151

**G**

Galois cohomology set, 276  
Galois group  
of linear differential ideal, 411  
of set of linear differential polynomials, 411  
of strongly normal extension, 396  
General component, 157  
General irreducible component, 157  
General linear group, 213  
General solution, 157  
 $\mathcal{G}$ -Generated, 11  
Generic composite of *K*-mappings, 299  
Generic differential specialization, 139  
*K*-Generic element, 216  
Generic inverse, 301  
Generic point, 150  
Generic specialization  
of element of pre-*K*-set, 216  
of family of elements of a field extension, 33  
of family of isomorphisms, 386  
Generic zero  
of prime differential polynomial ideal, 146  
of prime polynomial ideal, 19  
Generically invertible, 301  
Generically surjective, 301  
*K*-Group, 218–219  
*K*-Group quotient, 267

**H**

Habitat 294  
Holomorphic at a specialization, 288  
Holomorphic at an element of a *K*-set  
derivation, 338  
differential, 338  
*K*-function, 317  
*K*-mapping, 318  
Homogeneous part, 29  
Homogeneous space, 219

- Homogeneous  $K$ -space, 220–221  
 Homogeneous  $K$ -space quotient, 267  
 Homomorphism  
   of differential modules, 66  
   of differential rings, 61  
   of pointed sets, 275  
 $K$ -Homomorphism  
   of  $K$ -groups, 226  
   of homogeneous  $K$ -spaces, 226  
   of pointed pre- $K$ -sets, 277  
   of  $K$ -spaces, 341  
   of  $(M, G)$  into  $(M', G')$ , 342  
 $(L, K)$ -Homomorphism  
   of  $L$ -group into  $K$ -group, 230  
   of homogeneous  $L$ -space into homogeneous  $K$ -space, 230
- I**
- $\mathcal{G}$ -Ideal, 10  
 Implicit function theorem, 31  
 Independent elements of pre- $K$ -sets, 217  
 Induced  
    $L$ -group, 230  
   homogeneous  $L$ -space, 231  
   pre- $K$ -mapping, 217  
 Initial, 75  
 Inseparability basis, 4  
 Inseparability degree, 4  
 Integrated ranking, 75  
 Invariant derivation, 325  
 Invariant differential, 325  
 $K$ -Irreducible, 216  
 Irreducible closed set in homogeneous  $K$ -space, 243  
 Irreducible component, 147  
 Irreducible topological space, 147  
 Isobaric, 73  
 Isolated isomorphism, 386  
 $K$ -Isomorphism  
   of  $K$ -groups, 226  
   of homogeneous  $K$ -spaces, 226  
 Isotropy group, 257
- K**
- Krull topology, 274  
 Krull's theorem, 39–40
- L**
- Lattice, 382  
 Leader, 75

- Leading coefficient theorem, 172  
 Levi's lemma, 177  
 Lexicographic order, 49  
 Lie algebra of homogeneous  $K$ -space, 325  
 Linear differential polynomial ideal, 150  
 Linear dimension, 151  
 Linear extension, 396  
 Linear  $K$ -group, 355  
 Linearly dependent (or independent) derivative operators, 96  
 Linearly dependent (or independent) over constants, 88  
 Liouvillian extension, 408  
   of type  $(i)$ , 408  
 Liouvillian  $K$ -group, 374  
   of type  $(i)$ , 374  
 $K$ -Liouvillian  $K$ -group, 374  
   of type  $(i)$ , 374  
 Local component  
   of derivation, 338  
   of invariant differential, 339  
 Local derivation, 334–335  
 Local ring on  $V$  at  $v$ , 331  
 Localization at prime ideal, 7  
 Locus, 216  
 Logarithmic derivation, 350  
 Logarithmic derivative, 349  
 Low power theorem, 187
- M**
- $K$ -Mapping, 295  
 $K$ -Minimal, 294  
 $R$ -Morphism of ideals, 17  
 Multiplicity  
   of differential polynomial at point, 164  
   of zero of differential polynomial, 164
- N**
- Nakayama's lemma, 34  
 Noetherian conservative system, 13  
 Noetherian topological space, 147  
 Nonsingular zero or solution, 155  
 Normalization lemma, 43  
 Numerical polynomial, 50
- O**
- $K$ -Operation of  $K$ -group  
   on  $K$ -group, 342  
   on  $K$ -space, 342–343  
 Opposite  $K$ -group, 223

- Order  
   of derivative, 59  
   of derivative operator, 59  
   of differential polynomial, 70  
 Orderly ranking, 75  
 Orthogonal group, 213
- P**
- Partial remainder, 77, 78  
 Partially pseudo-reduced, 83  
 Partially reduced, 77  
 Perfect conservative system, 12  
 Perfect ideal, 7  
 Permissible grading, 73  
 $A$ -Permissible homomorphism, 174  
 Picard–Vessiot element, 415  
 Picard–Vessiot extension, 410  
 Point, 145  
 Pointed pre- $K$ -set, 277  
 Pointed set, 275  
 Positive grading, 73  
 Power series, 29  
 Pre- $K$ -homomorphism  
   of  $K$ -groups, 250  
   of homogeneous  $K$ -spaces, 250  
 Pre- $K$ -mapping, 217  
 Preparation congruence, 184  
 Preparation equation, 183  
 Pre- $K$ -set, 215  
 Pre- $K$ -subset, 216  
 Prime factor of differential monomial, 70  
 $\Sigma$ -Prime ideal, 7  
 Primitive, 404  
 $G$ -Primitive, 419  
 $G$ -Primitive extension, 419  
 $V$ -Primitive, 430  
 Principal homogeneous space, 219  
 Principal homogeneous  $K$ -space, 220–221  
 Product  $K$ -group structure, 261  
 Product homogeneous  $K$ -space structure, 261  
 Product order, 49  
 Proper derivative, 59  
 Pseudo-leader, 83  
 Pseudo-led, 83  
 Pseudo-separant, 83
- Q**
- Quasi-independent, 217–218  
 Quasi-perfect, 5  
 Quasi-separable field extension, 5

- Quasi-separable integral domain, 8  
 Quasi-separable prime ideal, 9

**R**

- Rank comparison  
   of autoreduced sets, 81  
   of derivatives, 75  
   of differential polynomials, 75–76  
 Ranking, 75  
 Rational element, 215  
 Rational function, 306  
 Rational mapping, 303  
 Reduced, 77  
 Regular element of pre- $K$ -set, 215–216  
 Regular field extension, 8  
 Regular ideal, 9  
 Regular integral domain, 8  
 Regular  $K$ -space, 221  
 Relative  $K$ -homomorphism, 342  
 Remainder, 79  
 Restriction of set of derivation operators, 65  
 Riccati differential polynomial, 416  
 Ring of constants, 60  
 Ritt problem, 191  
 Ritt's analog of Lüroth's theorem, 163  
 Rosenfeld's criterion, 167

**S**

- Semi-invariant, 356  
 Semisimple matrix, 365  
 Semisimple element of linear  $K$ -group, 367  
 Semiuniversal extension, 92  
 Separable closure of differential field, 91  
 Separable element of pre- $K$ -set, 215–216  
 Separable ideal, 9  
 Separable overring, 8  
 Separable pre- $K$ -mapping, 217  
 Separably dependent (or independent), 2  
   over constants, 93  
 Separant, 75  
 Separating differential transcendence basis, 108–109  
 Sequential ranking, 75  
 Series-order, 30  
 $K$ -Set, 227  
 Shapiro's lemma, 53  
 Simple element of irreducible  $K$ -set, 337  
 $K$ -Simple  $K$ -group, 375  
 Singular component, 157  
 Singular irreducible component, 157

Singular solution, 155  
 Singular zero, 155  
 Solution, 145  
 $K$ -Space, 341  
 Special linear group, 213  
 Specialization  
   of element of pre- $K$ -set, 216  
   of family of elements of field extension, 33  
   of family of isomorphisms, 386  
   of integral domain, 33  
 Splits, 281, 422  
 $K$ -Splits, 321  
 Stability group, 257  
 Strictly positive  $A$ -permissible homomorphism, 175  
 Strictly positive grading, 73  
 Strong isomorphism, 388–389  
 Strongly normal extension, 393  
 $K$ -Subgroup, 226  
 $K$ -subset, 227  
 $K$ -Subspace, 342  
 Substitution homomorphism  
   of differential algebra of power series, 85  
   of differential polynomial algebra, 71  
   of differential power series algebra, 85

**T**

Tangent space, 335  
 Tangent vector, 335  
 $\mathcal{T}$ -Topology of  $\mathcal{M}$ , 149  
 $K$ -Topology of homogeneous  $K$ -space, 240  
 Transformation of set of derivation operators, 65  
 Transporter, 257  
 Triangular group, 213  
 Twisting, 282

Typical differential dimension  
   of irreducible closed set in  $\mathcal{M}$ , 148  
   of prime differential polynomial ideal, 130  
 Typical differential inseparability degree,  
   of finitely generated extension, 118  
   of prime differential polynomial ideal, 130  
 Typical differential transcendence degree,  
   118

**U**

Uniformizing parameters, 337  
 Unipotent matrix, 364  
 Unipotent element of linear  $K$ -group, 367  
 Universal differential field, 133  
 Universal extension, 133  
 Usual grading, 72

**V**

Value  
   of differential polynomial, 71  
   of element at a specialization, 288  
 $v$ -Value 57

**W**

Weakness 179  
 Weierstrassian, 405  
 Weight  
   of differential polynomial, 73  
   of semi-invariant, 356–357

**Z**

Zariski topology, 240  
 Zero  
   of subset of  $K[K(vt) \cup K(t)]$ , 236  
   of subset of  $\mathcal{M}\{y_1, \dots, y_n\}$ , 145

**Pure and Applied Mathematics****A Series of Monographs and Textbooks**

Editors **Paul A. Smith and Samuel Eilenberg**

Columbia University, New York

- 1: ARNOLD SOMMERFELD. Partial Differential Equations in Physics. 1949 (Lectures on Theoretical Physics, Volume VI)
- 2: REINHOLD BAER. Linear Algebra and Projective Geometry. 1952
- 3: HERBERT BUSEMANN AND PAUL KELLY. Projective Geometry and Projective Metrics. 1953
- 4: STEFAN BERGMAN AND M. SCHIFFER. Kernel Functions and Elliptic Differential Equations in Mathematical Physics. 1953
- 5: RALPH PHILIP BOAS, JR. Entire Functions. 1954
- 6: HERBERT BUSEMANN. The Geometry of Geodesics. 1955
- 7: CLAUDE CHEVALLEY. Fundamental Concepts of Algebra. 1956
- 8: SZE-TSEN HU. Homotopy Theory. 1959
- 9: A. M. OSTROWSKI. Solution of Equations and Systems of Equations. Third Edition, in preparation
- 10: J. DIEUDONNÉ. Treatise on Analysis: Volume I, Foundations of Modern Analysis, enlarged and corrected printing, 1969. Volume II, 1970. Volume III, 1972
- 11: S. I. GOLDBERG. Curvature and Homology. 1962.
- 12: SIGURDUR HELGASON. Differential Geometry and Symmetric Spaces. 1962
- 13: T. H. HILDEBRANDT. Introduction to the Theory of Integration. 1963.
- 14: SHREERAM ABHYANKAR. Local Analytic Geometry. 1964
- 15: RICHARD L. BISHOP AND RICHARD J. CRITENDEN. Geometry of Manifolds. 1964
- 16: STEVEN A. GAAL. Point Set Topology. 1964
- 17: BARRY MITCHELL. Theory of Categories. 1965
- 18: ANTHONY P. MORSE. A Theory of Sets. 1965
- 19: GUSTAVE CHOQUET. Topology. 1966
- 20: Z. I. BOREVICH AND I. R. SHAFAREVICH. Number Theory. 1966
- 21: JOSÉ LUIS MASSERA AND JUAN JORGE SCHAFFER. Linear Differential Equations and Function Spaces. 1966
- 22: RICHARD D. SCHAFER. An Introduction to Nonassociative Algebras. 1966
- 23: MARTIN EICHLER. Introduction to the Theory of Algebraic Numbers and Functions. 1966
- 24: SHREERAM ABHYANKAR. Resolution of Singularities of Embedded Algebraic Surfaces. 1966
- 25: FRANÇOIS TRÉVES. Topological Vector Spaces, Distributions, and Kernels. 1967
- 26: PETER D. LAX AND RALPH S. PHILLIPS. Scattering Theory. 1967.
- 27: OYSTEIN ORE. The Four Color Problem. 1967
- 28: MAURICE HEINS. Complex Function Theory. 1968

- 29: R. M. BLUMENTHAL AND R. K. GETTOOR. Markov Processes and Potential Theory. 1968
- 30: L. J. MORDELL. Diophantine Equations. 1969
- 31: J. BARKLEY ROSSER. Simplified Independence Proofs: Boolean Valued Models of Set Theory. 1969
- 32: WILLIAM F. DONOGHUE, JR. Distributions and Fourier Transforms. 1969
- 33: MARSTON MORSE AND STEWART S. CAIRNS. Critical Point Theory in Global Analysis and Differential Topology. 1969
- 34: EDWIN WEISS. Cohomology of Groups. 1969
- 35: HANS FREUDENTHAL AND H. DE VRIES. Linear Lie Groups. 1969
- 36: LASZLO FUCHS. Infinite Abelian Groups: Volume I, 1970. Volume II, 1973
- 37: KEIO NAGAMI. Dimension Theory. 1970
- 38: PETER L. DUREN. Theory of  $H^p$  Spaces. 1970
- 39: BODO PARÉIGIS. Categories and Functors. 1970
- 40: PAUL L. BUTZER AND ROLF J. NESSEL. Fourier Analysis and Approximation: Volume 1, One-Dimensional Theory. 1971
- 41: EDUARD PRUGOVEČKI. Quantum Mechanics in Hilbert Space. 1971
- 42: D. V. WIDDER: An Introduction to Transform Theory. 1971
- 43: MAX D. LARSEN AND PAUL J. MCCARTHY. Multiplicative Theory of Ideals. 1971
- 44: ERNST-AUGUST BEHRENS. Ring Theory. 1972
- 45: MORRIS NEWMAN. Integral Matrices. 1972
- 46: GLEN E. BREDON. Introduction to Compact Transformation Groups. 1972
- 47: WERNER GREUB, STEPHEN HALPERIN, AND RAY VANSTONE. Connections, Curvature, and Cohomology: Volume I, De Rham Cohomology of Manifolds and Vector Bundles, 1972. Volume II, Lie Groups, Principal Bundles, and Characteristic Classes, in preparation
- 48: XIA DAO-XING. Measure and Integration Theory of Infinite-Dimensional Spaces: Abstract Harmonic Analysis. 1972
- 49: RONALD G. DOUGLAS. Banach Algebra Techniques in Operator Theory. 1972
- 50: WILLARD MILLER, JR. Symmetry Groups and Their Applications. 1972
- 51: ARTHUR A. SAGLE AND RALPH E. WALDE. Introduction to Lie Groups and Lie Algebras. 1973
- 52: T. BENNY RUSHING. Topological Embeddings. 1973
- 53: JAMES W. VICK. Homology Theory: An Introduction to Algebraic Topology. 1973
- 54: E. R. KOLCHIN. Differential Algebra and Algebraic Groups. 1973

*In preparation*

GERALD J. JANUSZ. Algebraic Number Fields

SAMUEL EILENBERG. Automata, Languages, and Machines: Volume A

H. M. EDWARDS. Riemann's Zeta Function

WAYNE ROBERTS AND DALE VARBERG. Convex Functions