Lecture Notes on

Computational Algebraic Geometry

Ruyong Feng Ziming Li

May, 2016

Some concepts from Algebra

Definition 0.1 *A* commutative ring*:* $(R, +, \cdot)$ *satisfies for all* $a, b, c \in R$*,*

(i) $(a + b) + c = a + (b + c)$ *and* $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ *(associative).*

(ii) $a + b = b + a$ *and* $a \cdot b = b \cdot a$ *(commutative).*

(iii) $a \cdot (b + c) = a \cdot b + a \cdot c$ *(distributive).*

(iv) $\exists\ 0, 1 \in R$ *s.t.* $a + 0 = a \cdot 1 = a$ *(identities).*

(v) $\forall\ a \in R, \exists\ b \in R$ *s.t.* $a + b = 0$ *(additive inverses).*

Definition 0.2 *Let* R *be a commutative ring.* R *is a* domain *if whenever* $a, b \in R$ *and* $ab = 0$*, then either* $a = 0$ *or* $b = 0$*.*

Definition 0.3 *A* **field***:* $(k, +, \cdot)$ *satisfies*

(i) $(k, +, \cdot)$ *is a commutative ring.*

(ii) $\forall\ a \in k, \exists\ b \in k$ *s.t.* $a \cdot b = 1$ *(multiplicative inverses).*

Let R be a domain. An element $a \in R \setminus \{0\}$ is called *irreducible* if it is not a unit, and if $a = bc$ with $b \in R$ and $c \in R$, then b or c is a unit. An element $a \in R \setminus \{0\}$ is said to have a *unique factorization into irreducible elements* if there exists a unit u and there are irreducible elements $p_1, \cdots, p_r$ in R such that

$$a = u \prod_{i=1}^{r} p_i,$$

and if given two factorizations into irreducible elements,

$$a = u \prod_{i=1}^{r} p_i = u' \prod_{j=1}^{s} q_j,$$

then we have $r = s$, and after a permutation of the indices i, $p_i = v_i q_i$ for some unit $v_i \in R$, $i = 1, \cdots, r$.

Definition 0.4 *A domain is called a* unique factorization ring *if every nonzero element has a unique factorization into irreducible elements.*

Chapter 1

Affine Algebraic Varieties

1.1 Preliminaries

Throughout the note k stands for a field and $\bar{k}$ is its algebraic closure of k. We do not impose any assumption on the characteristic of k.

Some basic facts about $\bar{k}$ are

1. $\bar{k}$ is algebraically closed;
2. every element of $\bar{k}$ is algebraic over k;
3. every algebraically closed field is infinite;

Definition 1.1 *A* monimial *in $x_1, \ldots, x_n$ is a product of the form*

$$x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_n}$$

where $\alpha_1, \ldots, \alpha_n \in \mathbf{Z}_{\geq 0}$. The **degree** *of this monomial in x_i is α_i and the* **total degree** *of this monomial is $\alpha_1 + \ldots + \alpha_n$. For brief, we denote the above monomial by $\mathbf{x}^\alpha$ where $\mathbf{x} = (x_1, \cdots, x_n)$ and $\alpha = (\alpha_1, \cdots, \alpha_n)$. The total degree of $\mathbf{x}^\alpha$ is denoted by $\deg(\mathbf{x}^\alpha)$, the degree in x_i is denoted by $\deg_{x_i}(\mathbf{x}^\alpha)$.*

Definition 1.2 *A* polynomial *f in $x_1, \ldots, x_n$ with coefficients in k is a finite linear combination of monomials. We will write f in the form*

$$f = \sum_\alpha a_\alpha \mathbf{x}^\alpha, a_\alpha \in k.$$

The set of polynomials in $x_1, \ldots, x_n$ with coefficients in k is denoted by $k[x_1, \cdots, x_n]$, or for abbreviation $k[\mathbf{x}]$.

For a nonzero polynomial f in $k[\mathbf{x}]$, $\deg(f)$ stands for the total degree of f, i.e.

$$\deg(f) = \max_{\alpha}\{\deg(\mathbf{x}^{\alpha})\},$$

and $\deg_{x_i}(f)$ stands for the degree of f in x_i, i.e.

$$\deg_{x_i}(f) = \max_{\alpha}\{\deg_{x_i}(\mathbf{x}^{\alpha})\}.$$

Remark 1.1 *$k[\mathbf{x}]$ is a UFD.*

Every element $f \in k[\mathbf{x}]$ can be viewed as a function from $\bar{k}^n$ to $\bar{k}$ by mapping $\mathbf{p} \in \bar{k}^n$ to $f(\mathbf{p})$.

Proposition 1.1 *Let f be a polynomial in $k[\mathbf{x}]$. If $f(\mathbf{p}) = 0$ for every $\mathbf{p} \in \bar{k}^n$, then $f = 0$.*

Proof. We shall prove it by induction on n. When $n = 1$, since $\bar{k}$ is infinite, this means that f has infinitely many roots, and hence $f = 0$. Otherwise, if $f \neq 0$, then f has at most $\deg(f)$ zeroes in $\bar{k}$. Now suppose that the assertion is true for $n-1$. Assume that $f \neq 0$. Write

$$f = \sum_{i=0}^{m} f_i(x_1, \ldots, x_{n-1})x_n^i, \;\; f_i \in k[x_1, \ldots, x_{n-1}],$$

where $f_m(x_1, \cdots, x_{n-1}) \neq 0$. By the induction hypothesis, there is $\mathbf{a} \in \bar{k}^{n-1}$ such that $f_m(\mathbf{a}) \neq 0$. Then one has $f(\mathbf{a}, x_n) \neq 0$. By the induction hypothesis again, $f(\mathbf{a}, b) \neq 0$ for some $b \in \bar{k}$. This contradicts to the assumption. □

1.2 Affine algebraic varieties

A subset V of $\bar{k}^n$ is called an *affine algebraic k-variety* (or *affine algebraic variety over k*) if there exists a nonempty subset P of $k[\mathbf{x}]$ such that

$$V = \left\{\mathbf{p} \in \bar{k}^n | f(\mathbf{p}) = 0 \,\text{for all}\, f \in P\right\}.$$

We simply say that V is an algebraic variety or a variety defined by P, and denote V by $\mathbf{V}(P)$.

Example 1.1 *1. In $\bar{k}^n$, we have that $\emptyset = \mathbf{V}(1)$ and $\bar{k}^n = \mathbf{V}(0)$;*

2. *$\bar{k}$-varieties in $\bar{k}$ are the empty set, all nonempty finite sets and $\bar{k}$.*

Lemma 1.2 *The intersection of varieties is a variety. The union of finitely many varieties is a variety.*

Proof. Suppose that Λ is an (possibly infinite) index set, and that, for every $\lambda \in \Lambda$, $V_\lambda = \mathbf{V}(P_\lambda)$ for some $P_\lambda \in k[\mathbf{x}]$. Then

$$\bigcap_{\lambda\in\Lambda} V_\lambda = \mathbf{V}\left(\cup_{\lambda\in\Lambda} P_\lambda\right).$$

This proves the first assertion. Assume now that Λ is finite. Putting

$$T = \left\{ \prod_{\lambda\in\Lambda} f_\lambda \;\middle|\; \text{for every } f_\lambda \in P_\lambda \right\}.$$

we have $\cup_{\lambda\in\Lambda} V_\lambda = \mathbf{V}(T)$. □

Set

$$\tau = \{k\text{-varieties in } \bar{k}^n\}.$$

Then τ satisfies

1. both $\emptyset$ and $\bar{k}^n$ are in τ;
2. if $V_1, V_2 \in \tau$, then $V_1 \cup V_2 \in \tau$;
3. Any intersection of elements of τ is an element of τ.

So τ is a topology on $\bar{k}^n$. This topology is referred as Zariski's topology. A variety is also called a *(Zariski)-closed set.* For a subset S of $\bar{k}^n$, the smallest variety (with respect to inclusion) containing S is called the *Zariski closure* of S, which is denoted by $\bar{S}$.

1.3 Ideals

Let R be a (commutative) ring with a multiplicative identity 1. A subset I is called an *ideal* of R if

1. I is closed under addition;
2. for every $r \in R$ and $a \in I$, $ra \in I$.

Let $S \subset R$. We shall use $\langle S \rangle$ to stand for the ideal generated by S, i.e., the smallest ideal in R containing S.

Lemma 1.3 *The sum of two ideals is an ideal. The intersection of any number of ideals is an ideal.*

Proof. Straightforward. □

An ideal I of R is said to be *radical* if whenever a power of an element r in R is in I, then r itself is in I.

Lemma 1.4 *If I is an ideal of R, then the smallest radical ideal containing I is equal to*

$$\sqrt{I} = \{r \in R \,|\, r^m \in I \text{ for some } m \in \mathbf{N}\}.$$

Proof. Every radical ideal containing I clearly contains $\sqrt{I}$. It remains to prove that $\sqrt{I}$ is a radical ideal. Assume that a and b are in $\sqrt{I}$. Then there exists two positive integers i and j such that both a^i and b^j are in I. It follows that $(a+b)^{i+j}$ is in I. Consequently, $a+b$ is in $\sqrt{I}$. For every $r \in R$, the power $(ra)^i$ is in I, and so ra is in $\sqrt{I}$. Hence, $\sqrt{I}$ is an ideal. It is radical by definition. □

Let P be a subset of $k[\mathbf{x}]$. The ideal generated by P is denoted by $\langle P \rangle$. It is evident that

$$\mathbf{V}(P) = \mathbf{V}(\langle P \rangle) = \mathbf{V}\left(\sqrt{\langle P \rangle}\right). \tag{1.1}$$

Assume that the characterstic of k is zero. Let $f \in k[x]$ with $f \neq 0$. We shall call $f/\mathrm{GCD}(f, f')$ the *square-free part* of f, denoted by $\underline{f}$. Then one can verify that $\sqrt{\langle f \rangle} = \langle \underline{f} \rangle$.

1.4 Correspondences

For a subset S of $\bar{k}^n$, we define

$$\mathbf{I}(S) = \{f \in k[\mathbf{x}] \,|\, f(\mathbf{p}) = 0 \text{ for all } \mathbf{p} \in S\}.$$

One can verify that $\mathbf{I}(S)$ is a radical ideal of $k[\mathbf{x}]$, which is called the *vanishing ideal* of S.

Proposition 1.5 *1. If $S_1 \subset S_2 \subset \bar{k}^n$, then $\mathbf{I}(S_1) \supset \mathbf{I}(S_2)$.*

2. If $P_1 \subset P_2 \subset k[\mathbf{x}]$, then $\mathbf{V}(P_1) \supset \mathbf{V}(P_2)$.

Proof. Straightforward. □

We have seen that $\mathbf{I}$ is a map from subsets of $\bar{k}^n$ to the radical ideals of $k[\mathbf{x}]$. This map is inclusion-reversing. Similarly, $\mathbf{V}$ is an inclusion-reversing map from subsets of $k[\mathbf{x}]$ to varieties in $\bar{k}^n$. We say that every variety V in $\bar{k}^n$ corresponds to a radical ideal $\mathbf{I}(V)$, which is the vanishing ideal of V in $k[\mathbf{x}]$, and that every radical ideal I of $k[\mathbf{x}]$ corresponds to a variety $\mathbf{V}(I)$, which is the variety defined by I in $\bar{k}^n$.

The next lemma is useful for constructing Zariski closures.

Lemma 1.6 *If $S \subset \bar{k}^n$ and $V = \mathbf{V}(\mathbf{I}(S))$, then V is the Zariski closure of S, and $\mathbf{I}(V) = \mathbf{I}(S)$.*

Proof. Let $U = \mathbf{V}(P)$ be a Zariski closed subset of $\bar{k}^n$ which containing S, where P is a subset of $k[\mathbf{x}]$. For every $f \in P$, f vanishes on U and then vanishes on S. Thus $f \in \mathbf{I}(S)$. Consequently $P \subset \mathbf{I}(S)$. By Proposition 1.5 (2), we then have that

$$U = \mathbf{V}(P) \supset \mathbf{V}(\mathbf{I}(S)) = V.$$

Therefore V is the Zariski closure of S by definition.

It remains to show that $\mathbf{I}(V) = \mathbf{I}(S)$. By Proposition 1.5 (1), $\mathbf{I}(V) \subset \mathbf{I}(S)$ because $S \subset V$. Suppose that $\mathbf{I}(S) \setminus \mathbf{I}(V) \neq \emptyset$ and let $f \in \mathbf{I}(S) \setminus \mathbf{I}(V)$. Then there exists $\mathbf{p} \in V \setminus S$ such that $f(\mathbf{p}) \neq 0$. Putting

$$T = \mathbf{I}(V) \cup \{f\} \subset k[\mathbf{x}].$$

We have that $T \subset \mathbf{I}(S)$, so $\mathbf{V}(T) \supset \mathbf{V}(\mathbf{I}(S)) = V$. Since $\mathbf{p} \in V$, this implies that $f(\mathbf{p}) = 0$, a contradiction. □

Corollary 1.7 *1. For every variety V,*

$$\mathbf{V}(\mathbf{I}(V)) = V.$$

2. The map $\mathbf{V}$ is surjective from the set of radical ideals in $k[\mathbf{x}]$ to the set of varieties in $\bar{k}^n$.

3. The map $\mathbf{I}$ is injective from the set of varieties in $\bar{k}^n$ to the set of radical ideals in $k[\mathbf{x}]$.

Proof. The first one follows from Lemma 1.6. Others are immediate from the first one. The first assertion follows from (1.1). □

Remark 1.2 *In Section 1.2 of [?], affine varieties are defined as the set of zeroes in k^n of some polynomials in $k[\mathbf{x}]$. All conclusions in Sections 1.2,1.3 and 1.4 remain true if we replace our definition by the definition of Cox, Little and O'Shea. In fact, we have not used the fact that $\bar{k}$ is algebraically closed in Sections 1.2,1.3 and 1.4. Later on, we shall prove a fundamental conclusion in algebraic geometry that both $\mathbf{I}$ and $\mathbf{V}$ are bijective, which hinges on the fact that $\bar{k}$ is algebraically closed.*

Exercises for Chapter 2

1. Let $k = \mathbf{Q}$, the field of rational numbers and $S = \{\sqrt{2}\}$. Prove that S is not a $\mathbf{Q}$-variety in $\bar{\mathbf{Q}}$. What is the Zariski closure of S in $\bar{\mathbf{Q}}$?

2. Give an example to show that the union of infinitely many varieties may not be a variety.

3. Assume that $f \in k[x] \setminus \{0\}$. Let $\underline{f}$ be the square-free part of f. Prove that $\sqrt{\langle f \rangle} = \langle \underline{f} \rangle$.

4. Let $S \subset \bar{k}^n$ and $\mathbf{I}(S)$ be the vanishing ideal of S in $k[\mathbf{x}]$. Prove that $\mathbf{I}(S)$ is a radical ideal.

Chapter 2

Hilbert's Nullstellensatz

Nullstellensatz is a German word formed by three simple words: Null(=Zero), Stellen(=Places), and Satz(=Theorem). An English translation of the title is Hilbert's Zero-Theorem. However, one customarily uses the original German name due to its fundamental importance in algebraic geometry.

2.1 Preliminaries

2.1.1 Sylvester's resultant

Let D be an integral domain. For two polynomials $f, g \in D[x]$ with respective degrees m and n, where $m > 0$ and $n > 0$, we write

$$f = f_m x^m + \cdots + f_0 \quad \text{and} \quad g = g_n x^n + \cdots + g_0.$$

Define the (Sylvester) resultant of f and g with respect to x to be the determinant of the $(m+n) \times (m+n)$ matrix

$$\begin{pmatrix} f_m & f_{m-1} & \cdots & f_0 & 0 & 0 & 0 & \cdots & 0 \\ 0 & f_m & f_{m-1} & \cdots & f_0 & 0 & 0 & \cdots & 0 \\ \cdot & \cdot & \cdot & \cdots & \cdot & \cdot & \cdot & \cdots & \cdot \\ 0 & 0 & 0 & \cdots & 0 & f_m & f_{m-1} & \cdots & f_0 \\ g_n & g_{n-1} & \cdots & g_0 & 0 & 0 & 0 & \cdots & 0 \\ 0 & g_n & g_{n-1} & \cdots & g_0 & 0 & 0 & \cdots & 0 \\ \cdot & \cdot & \cdot & \cdots & \cdot & \cdot & \cdot & \cdots & \cdot \\ 0 & 0 & 0 & \cdots & 0 & g_n & g_{n-1} & \cdots & g_0 \end{pmatrix}. \tag{2.1}$$

The resultant of f and g is denoted by $\mathrm{res}_x(f, g)$.

Example 2.1 *Let* $f = a_2x^2 + a_1x + a_0$. *Then* $f' = 2a_2x + a_1$. *An easy calculation yields that*

$$\mathrm{res}_x(f, f') = -a_2(a_1^2 - 4a_2a_0).$$

Lemma 2.1 *With the notation just introduced, there exist nonzero polynomials* $a, b \in D[x]$ *with* $\deg a < n$ *and* $\deg b < m$ *such that*

$$af + bg = \mathrm{res}_x(f, g). \tag{2.2}$$

Proof. For all i with $1 \leq i \leq m + n - 1$, we multiply the ith column of matrix (2.1) by x^{m+n-i} and add the result to the last column. This results in the matrix

$$M = \begin{pmatrix} f_m & f_{m-1} & \cdots & f_0 & 0 & 0 & 0 & \cdots & 0 & x^{n-1}f \\ 0 & f_m & f_{m-1} & \cdots & f_0 & 0 & 0 & \cdots & 0 & x^{n-2}f \\ \cdot & \cdot & \cdot & \cdots & \cdot & \cdot & \cdot & \cdots & \cdot & \cdot \\ 0 & 0 & 0 & \cdots & 0 & f_m & f_{m-1} & \cdots & f_1 & f \\ g_n & g_{n-1} & \cdots & g_0 & 0 & 0 & 0 & \cdots & 0 & x^{m-1}g \\ 0 & g_n & g_{n-1} & \cdots & g_0 & 0 & 0 & \cdots & 0 & x^{m-2}g \\ \cdot & \cdot & \cdot & \cdots & \cdot & \cdot & \cdot & \cdots & \cdot & \cdot \\ 0 & 0 & 0 & \cdots & 0 & g_n & g_{n-1} & \cdots & g_1 & g \end{pmatrix}.$$

We have that $\mathrm{res}_x(f, g) = \det(M)$. If the resultant is nonzero, then expanding $\det(M)$ according to its last column yields the required a and b. Otherwise, the rows of matrix (2.1) are linearly dependent over the field F of fractions of D, so are the rows of M. In particular, the polynomials

$$x^{n-1}f,\ x^{n-2}f,\ \ldots,\ f,\ x^{m-1}g,\ x^{m-2}g,\ \ldots,\ g$$

are linearly dependent over F. Any nontrivial F-linear relation among them gives us the required a and b. Note that we may clear the denominators appearing in a and b, because $\mathrm{res}_x(f, g) = 0$ in the latter case. □

Equation (2.2) is referred as Bezout's relation in the literature. An important property of resultants is given in the next proposition.

Proposition 2.2 *Let* F *be a field and* f, g *in* $F[x]$ *with positive degrees. Then the following statements are equivalent:*

1. $\mathrm{res}_x(f, g) = 0$
2. $\gcd(f, g)$ *has a positive degree*

3. f and g have a common root in the algebraic closure $\bar{F}$ of F.

Proof. Assume that $\mathrm{res}_x(f,g) = 0$. Then Bezout's relation (2.2) becomes

$$af + bg = 0 \quad \text{where } \deg a < \deg g \text{ and } \deg b < \deg f.$$

Thus the greatest common divisor of f and g is nontrivial.

If $\gcd(f,g)$ has a positive degree, then a root of $\gcd(f,g)$ in $\bar{F}$ is a common root of f and g.

At last, assume that $\alpha \in \bar{F}$ is a common root of f and g. Substituting α for x in (2.2), we have $\mathrm{res}_x(f,\, g) = 0$. □

We now present some immediate applications of resultants.

Corollary 2.3 *If f and g are in $F[\mathbf{x}]$ with positive degrees in x_1, then*

1. *The resultant $\mathrm{res}_{x_1}(f,g)$ is in the ideal $\langle f,g\rangle \cap F[x_2,\ldots,x_n]$*
2. *$\mathrm{res}_{x_1}(f,g) = 0$ if and only if f and g have a common factor whose degree in x_1 is positive.*

Proof. The first assertion is immediate from Lemma 2.1. By Proposition 2.2 (2), f and g have a nontrivial common factor in $F(x_2,\ldots,x_n)[x_1]$. The second assertion then follows from Gauss' lemma □

Corollary 2.4 *Let f and g be two polynomials in $F[\mathbf{x}]$ with positive degrees in x_1. Write*

$$f = f_d x_1^d + f_{d-1}x_1^{d-1} + \cdots + f_0, \text{ where } f_d, f_{d-1}, \ldots, f_0 \in F[x_2,\ldots,x_n].$$

If $f_d(c_2,\ldots,c_n)$ is nonzero for some $c_2,\ldots,c_n \in \bar{k}$, then $f(x_1,c_2,\ldots,c_n)$ and $g(x_1,c_2,\ldots,c_n)$ have a common factor with positive degree if and only if the resultant $\mathrm{res}_{x_1}(f,g)$ vanishes at $(c_2,\ldots,c_n)$.

Proof. Write

$$g = g_s x_1^s + g_{s-1}x_1^{s-1} + \ldots + g_0, \text{ where } g_s, g_{s-1}, \ldots, g_0 \in k[x_2,\ldots,x_n].$$

Denote $h = \mathrm{res}_{x_1}(f,g)$. Due to the Bezout relation, one easily sees that if $f(x_1,c_2,\cdots,c_n)$ and $g(x_1,c_2,\cdots,c_n)$ have a common factor with positive degree then $h(c_2,\cdots,c_n) = 0$. We shall prove the sufficieny by separating two cases. Assume that $h(c_2,\cdots,c_n) = 0$.

Case 1: $\deg(g(x_1, c_2, \ldots, c_n)) < 1$. Then $g(x_1, c_2, \ldots, c_n) = g_0(c_2, \ldots, c_n)$. An easy calculation yields that

$$h(c_2, \ldots, c_n) = f_d(c_2, \ldots, c_n)^s g_0(c_2, \ldots, c_n)^d.$$

Thus $g_0(c_2, \ldots, c_n) = 0$, since $f_d(c_2, \cdots, c_n) \neq 0$. This implies that

$$\gcd(f(x_1, c_2, \cdots, c_n), g(x_1, c_2, \cdots, c_n)) = f(x_1, c_2, \cdots, c_n)$$

whose degree is positive.
Case 2: $\deg(g(x_1, c_2, \ldots, c_n)) \geq 1$. Then one has

$$g_s(c_2, \ldots, c_n) = \ldots = g_{m+1}(c_2, \ldots, c_n) = 0, g_m(c_2, \ldots, x_n) \neq 0$$

for some $1 \leq m < s$. From the definition of the resultant,

$$h(c_2, \ldots, x_n) = f_d(c_2, \ldots, c_n)^{s-m} \mathrm{res}_{x_1}(f(x_1, c_2, \ldots, c_n), g(x_1, c_2, \ldots, c_n)).$$

Hence $h(c_2, \ldots, c_n) = 0$ implies that

$$\mathrm{res}_{x_1}(f(x_1, c_2, \ldots, c_n), g(x_1, c_2, \ldots, c_n)) = 0.$$

Then the corollary follows from Proposition 2.2. □

2.1.2 u-resultants

Let $f, f_1, \ldots, f_m$ be polynomials in $k[\mathbf{x}]$. Assume that both $\deg_{x_1} f$ and $\deg_{x_1} f_1$ are positive. Put

$$g = u_1 f_1 + \cdots + u_m f_m$$

where $u_1, \ldots, u_m$ are new indeterminates. We regard these polynomials as elements in the ring $k[x_1, \ldots, x_n, u_1, \ldots, u_m]$. The resultant r of f and g with respect to x_1 is an element in $k[x_2, \ldots, x_n, u_1, \ldots, u_m]$, i.e.

$$r = \mathrm{res}_{x_1}(f, g) = \sum_{\gamma \in \Gamma} r_\gamma \mathbf{u}^\gamma$$

where $\Gamma \subset \mathbf{N}^m, \gamma = (\gamma_1, \ldots, \gamma_m)$ and $\mathbf{u}^\gamma = u_1^{\gamma_1} \ldots u_m^{\gamma_m}$, $r_\gamma \in k[x_2, \ldots, x_n]$. Let

$$T = \{r_\gamma | \gamma \in \Gamma\}.$$

Then T is a subset of $k[x_2, \ldots, x_n]$. We call T the $\mathbf{u}$-*resultant system* of the (ordered) sequence $f, f_1, \ldots, f_m$ with respect to x_1.

We generalize Corollaries 2.3 and 2.4.

Proposition 2.5 *Let $f, f_1, \ldots, f_m$ be polynomials in $k[\mathbf{x}]$. Assume that both $\deg_{x_1} f$ and $\deg_{x_1} f_1$ are positive. If T is the u-resultant system of the sequence $f, f_1, \ldots, f_m$ with respect to x_1, then*

1. *every element of T belongs to the ideal $\langle f, f_1, \ldots, f_m\rangle \cap k[x_2, \ldots, x_n]$;*
2. *$T = \{0\}$ if and only if f, f_1, $\ldots$, f_m have a common factor with positive degree in x_1.*

Proof. As above, we let $g = u_1 f_1 + \cdots + u_m f_m$ and $r = \mathrm{res}_{x_1}(f, g)$. By Lemma 2.1 there exist $a, b \in k[x_1, x_2, \ldots, x_n, u_1, \ldots, u_m]$ such that

$$af + bg = r.$$

Write

$$a = \sum_{\alpha \in \mathbf{N}^m} a_\alpha \mathbf{u}^\alpha,\ b = \sum_{\beta \in \mathbf{N}^m} b_\beta \mathbf{u}^\beta,$$

where a_α, b_β are in $k[x_1, x_2, \ldots, x_n]$ and $\mathbf{u}^\alpha = u_1^{\alpha_1} \cdots u_m^{\alpha_m}$ for $\alpha = (\alpha_1, \ldots, \alpha_m) \in \mathbf{N}^m$. Then the above Bezout's relation becomes

$$\sum_{\alpha \in \mathbf{N}^m} f a_\alpha \mathbf{u}^\alpha + \sum_{\beta \in \mathbf{N}^m} \sum_{i=1}^{m} f_i b_\beta u_i \mathbf{u}^\beta = \sum_{\gamma \in \mathbf{N}^m} r_\gamma \mathbf{u}^\gamma.$$

Collecting the like terms in $u_1, \ldots, u_m$ yields that every r_γ is in the ideal generated by $f, f_1, \ldots, f_m$. This proves the first assertion.

If f, f_1, $\ldots$, f_m have a common factor with positive degree in x_1, then r is zero by the above Bezout relation. Conversely, suppose that r is zero. Then f and g have a common factor with positive degree in x_1 by Corollary 2.3. This factor is in $k[x_1, x_2, \ldots x_n]$, because it divides f. Thus, it divides each of the f_i, because it divides g. □

2.1.3 Projections and extensions

For every ℓ with $1 \leq \ell \leq n-1$, we define π_ℓ to be the projection from $\bar{k}^n$ to $\bar{k}^{n-\ell}$ that sends $(c_1, \ldots, c_n)$ to $(c_{\ell+1}, \ldots, c_n)$. For a variety V of $\bar{k}^n$, $\pi_\ell(V)$ is called the *ℓth projection* of V. For an ideal I, the contraction ideal $I \cap k[x_{\ell+1}, \ldots, x_n]$ is called *ℓth elimination ideal* of I, which is denoted by $I^{(\ell)}$. If $V = \mathbf{V}(I)$, then $\pi_\ell(V) \subset \mathbf{V}\left(I^{(\ell)}\right)$. But the reversing inclusion does not hold in general. In fact, $\pi_\ell(V)$ is not necessarily a variety.

Example 2.2 *Let $I = \langle x_1 x_2 - 1\rangle$. Then $\pi_1(\mathbf{V}(I)) = \bar{k} \setminus \{0\}$, which is not a variety. It is clear that $I^{(1)} = \langle 0\rangle$ and that $\mathbf{V}\left(I^{(1)}\right) = \bar{k}$.*

The following conclusion is called the extension theorem in some literatures.

Proposition 2.6 *Let I be an ideal of $k[x_1, \ldots, x_n]$ and $V = \mathbf{V}(I)$. If $(c_2, \ldots, c_n)$ is in $\mathbf{V}\left(I^{(1)}\right)$ and if there exists a nonzero polynomial $f \in I$ such that*

$$\deg_{x_1}(f) = \deg_{x_1}(f(x_1, c_2, \ldots, c_n)) > 0,$$

then $(c_2, \ldots, c_n)$ is in $\pi_1(V)$.

Proof. Suppose that $c_{1,1}, \ldots, c_{1,l}$ be all distinct roots of $f(x_1, c_2, \ldots, c_n)$ in $\bar{k}$. Denote $\mathbf{c}_i = (c_{1,i}, c_2, \ldots, c_n)$ for all $1 \leq i \leq l$. We shall show that

$$\{\mathbf{c}_1, \cdots, \mathbf{c}_l\} \cap \mathbf{V}(I) \neq \emptyset.$$

Assume on the contrary that for each $i = 1, \ldots, l$, there is $g_i \in I$ satisfying $g_i(\mathbf{c}_i) \neq 0$. Let $u_1, \ldots, u_l$ be indeterminates. Obviously, $\deg_{x_1}(g_1) > 0$. Otherwise, $g_1 \in I^{(1)}$ and then $g_1(\mathbf{c}_1) = 0$. Consider the $\mathbf{u}$-resultant

$$\mathrm{res}_{x_1}(f, u_1 g_1 + \ldots + u_l g_l) = r(\mathbf{u}, x_2, \ldots, x_n) = \sum r_\gamma \mathbf{u}^\gamma.$$

By Proposition 2.5, $r_\gamma \in I^{(1)}$. Therefore $r(\mathbf{u}, c_2, \ldots, c_n) = 0$. By Corollary 2.4, $f(x_1, c_2, \ldots, c_n)$ and

$$u_1 g_1(x_1, c_2, \ldots, c_n) + \ldots + u_l g_l(x_1, c_2, \ldots, c_n)$$

have a common factor with positive degrees in x_1. Note that $c_{1,1}, \ldots, c_{1,l}$ are all roots of $f(x_1, c_2, \ldots, c_n)$ in $\bar{k}$. This implies that there is j with $1 \leq j \leq l$ such that

$$u_1 g_1(\mathbf{c}_j) + \ldots + u_l g_l(\mathbf{c}_j) = 0.$$

In particular, $g_j(\mathbf{c}_j) = 0$, a contradiction. □

2.1.4 Weierstrass form

We say that a nonzero polynomial f in $k[\mathbf{x}]$ is in *Weierstrass form* with respect to x_1 if

$$f = f_m x_1^m + f_{m-1} x_1^{m-1} + \cdots + f_0,$$

where $f_m \in k \setminus \{0\}$ and $f_{m-1}, \ldots f_0$ are in $k[x_2, \ldots, x_n]$.

Consider a substitution homomorphism ω from $k[\mathbf{x}]$ to itself by sending x_1 to x_1 and x_i to $x_i + x_1^{d_i}$ for all i with $2 \leq i \leq n$. The inverse of ω is given by

$$x_1 \mapsto x_1, \quad \text{and} \quad x_i \mapsto x_i - x_1^{d_i} \quad \text{for } i = 2, \ldots, n.$$

We call ω a *Weierstrass automorphism* with respect to x_1.

Proposition 2.7 *If f is a polynomial in $k[\mathbf{x}] \setminus k$, then there exists a Weierstrass automorphism ω with respect to x_1 such that $\omega(f)$ is in Weierstrass form with respect to x_1.*

Proof. Let $d = 1 + \deg f$ for every i with $2 \leq i \leq n$. Define ω to be the Weierstrass isomorphism (with respect to x_1) that sends x_i to $x_i + x_1^{d^{i-1}}$ for all i with $2 \leq i \leq n$. For a monomial $\mathbf{x}^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$, one sees

$$\omega(\mathbf{x}^\alpha) = x_1^{\alpha_1 + \alpha_2 d + \cdots + \alpha_n d^{n-1}} + g,$$

where $\deg_{x_1} g$ is less than $\alpha_1 + \alpha_2 d + \cdots + \alpha_n d^{n-1}$. It follows that if $\alpha \neq \beta$ then $\deg_{x_1}(\omega(\mathbf{x}^\alpha)) \neq \deg_{x_1}(\omega(\mathbf{x}^\beta))$. Now write

$$f = \sum a_\alpha \mathbf{x}^\alpha,$$

where $a_\alpha \in k$. There is a unique α such that $\deg_{x_1}(\omega(f)) = \deg_{x_1}(\omega(\mathbf{x}^\alpha))$ and the leading coefficient of $\omega(f)$ with respect to x_1 is a_α. This implies that $\omega(f)$ is in Weierstrass form with respect to x_1. □

2.2 Hilbert's basis theorem

Let R be a commutative ring and I an ideal of R. I is said to be finitely generated if there are finitely many elements of I, say $a_1, \ldots, a_m$, such that $I = \langle a_1, \ldots, a_m \rangle$. A commutative ring is said to be *Noetherian* if all its ideals are finitely generated. Let

$$I_1 \subset I_2 \subset I_3 \subset \cdots$$

be an ascending chain of ideals of a ring. We say the chain is stable if there is a positive integer m such that

$$I_m = I_{m+1} = \cdots .$$

Lemma 2.8 *A ring R is Noetherian if and only if every ascending chain of ideals in R is stable.*

Proof. Assume that

$$I_1 \subset I_2 \subset I_3 \subset \cdots$$

is an ascending chain of a Noetherian ring. Then $I = \cup_{i=1}^{\infty} I_i$ is an ideal, which has a finite set of generators. These generators are in some I_m. It follows that

$$I = I_m = I_{m+1} = \cdots .$$

Hence the above chain is stable.

We prove the converse by contradiction. Suppose that there exists an ideal $I \subset R$ that is not finitely generated. Let f_1 be a nonzero polynomial in I. Then $I \setminus \langle f_1 \rangle \neq \emptyset$. Otherwise, I is finitely generated. Let f_2 be an element in $I \setminus \langle f_1 \rangle$. Then $I \setminus \langle f_1, f_2 \rangle \neq \emptyset$. Repeating this process, we have an infinite sequence of ideals

$$\langle f_1 \rangle \subset \langle f_1, f_2 \rangle \subset \langle f_1, f_2, f_3 \rangle \subset \cdots$$

which is not stable. This contradicts to the hypothesis on R. □

The next theorem is known as Hilbert Basis Theorem.

Theorem 2.9 *If R is a Noetherian ring, so is $R[x]$.*

Proof. Suppose the contrary that an ideal I in $R[x]$ is not finitely generated. Put $I_0 = \langle 0 \rangle$. Let f_1 be a non-zero polynomial of least degree in $I \setminus I_0$. Put $I_1 = \langle f_1 \rangle$. Then $I \setminus I_1$ is nonempty. Let f_2 be a non-zero polynomial of least degree in $I \setminus I_1$, and put $I_2 = \langle f_1, f_2 \rangle$. Repeating this process, we have an infinite sequence $f_1, f_2, \ldots$ of non-zero polynomials such that, for all $n \in \mathbf{Z}^+$

1. $f_{n+1} \in I \setminus I_n$ for all $n \in \mathbf{N}$;
2. $\deg f_{n+1} = \min\{\deg f | f \in I \setminus I_n\}$;
3. $\deg f_1 \leq \deg f_2 \leq \cdots$.

Assume that r_n is the leading coefficient of f_n. Consider the chain of ideals:

$$\langle r_1 \rangle \subset \langle r_1, r_2 \rangle \subset \cdots$$

in R. Since R is Noetherian, the chain is stable. So there exists an integer m such that r_{m+1} belongs to $\langle r_1, \ldots, r_m \rangle$. Thus,

$$r_{m+1} = \sum_{i=1}^{m} a_i r_i \quad \text{for some } a_1, \ldots, a_m \in R.$$

Let

$$g = f_{m+1} - \sum_{i=1}^{m} a_i x^{\deg f_{m+1} - \deg f_i} f_i.$$

Note that g is not in I_m, because f_{m+1} is not in I_m. But $\deg g$ is less than $\deg f_{m+1}$, a contradiction. □

A repeated use of Theorem 2.9 yields:

Corollary 2.10 *Every ideal in $k[x_1, \ldots, x_n]$ has a finite basis.*

2.3 Nullstellensatz

Theorem 2.11 (**Weak Nullstellensatz**) *Let I be an ideal of $k[\mathbf{x}]$. Then $\mathbf{V}(I)$ is empty if and only if 1 is in I.*

Proof. Obviously, if $1 \in I$ then $\mathbf{V}(I) = \emptyset$. It remains to prove that if $1 \notin I$ then $\mathbf{V}(I) \neq \emptyset$. Suppose that $1 \notin I$. We shall show that $\mathbf{V}(I) \neq \emptyset$ by induction on n. Note that the case $I = \langle 0 \rangle$ is trivial. In the following, we assume that $I \neq \langle 0 \rangle$. If $n = 1$, the conclusion follows from the fact that $\bar{k}$ is algebraically closed and $k[x_1]$ is a principle ideal domain. Assume now that the assertion holds for $k[x_2, \ldots, x_n]$. Suppose that f is a polynomial in I with $\deg(f) > 0$. By Proposition 2.7 we have a Weierstrass automorphism ω of $k[\mathbf{x}]$ (with respect to x_1) such that $\omega(f)$ is in Weierstrass form. Put $J = \omega(I)$. Since ω is an automorphism, J does not contain 1, so does $J^{(1)}$. By the induction hypothesis $\mathbf{V}\left(J^{(1)}\right)$ is nonempty. Let $(c_2, \ldots . c_n)$ be a point in $\mathbf{V}\left(J^{(1)}\right)$. We have that

$$\deg_{x_1} \omega(f) = \deg_{x_1} \omega(f)(x_1, c_2, \ldots, c_n) > 0.$$

It follows from Proposition 2.6 that $(c_2, \ldots c_n)$ is in $\pi_1(\mathbf{V}(J))$. In other words, $\mathbf{V}(J)$ is nonempty, so is $\mathbf{V}(I)$, because ω is an automorphism. □

Theorem 2.12 (**The Strong Nullstellensatz**) *Let I be an ideal of $k[\mathbf{x}]$. Then*

$$\mathbf{I}(\mathbf{V}(I)) = \sqrt{I}.$$

Proof. Assume that $f \in \mathbf{I}(\mathbf{V}(I))$. Then f vanishes on $\mathbf{V}(I)$. Assume that t is a new indeterminate. Put $J = \langle I \rangle + \langle ft - 1 \rangle$, which is an ideal in $k[\mathbf{x}][t]$. We have that $\mathbf{V}(J)$ is empty. By Theorem 2.11 1 is in J. Thus,

$$1 = \sum_i u_i f_i + v(tf - 1) \quad \text{for some } u_i, v \in k[\mathbf{x}][t] \text{ and } f_i \in I.$$

Substituting $\frac{1}{f}$ for t in the above equality, we obtain

$$f^m = \sum_i v_i f_i \quad \text{for some } m \in \mathbf{N} \text{ and } v_i \in k[\mathbf{x}].$$

Accordingly, f is in $\sqrt{I}$. The converse is evident. □

Theorem 2.13 *Let $\widetilde{R}$ be the set of radical ideals of $k[\mathbf{x}]$ and $\widetilde{V}$ the set of all varieties in $\bar{k}^n$. Define the map*

$$\begin{array}{rccc} \mathbf{V}: & \widetilde{R} & \longrightarrow & \widetilde{V} \\ & I & \mapsto & \mathbf{V}(I) \end{array} \qquad \text{and} \qquad \begin{array}{rccc} \mathbf{I}: & \widetilde{V} & \longrightarrow & \widetilde{R} \\ & V & \mapsto & \mathbf{I}(V) \end{array}$$

where $\mathbf{V}(I)$ is the variety defined by I, and $\mathbf{I}(V)$ is the vanishing ideal of V. Then both $\mathbf{V}$ and $\mathbf{I}$ are bijections and $\mathbf{V}^{-1} = \mathbf{I}$.

Proof. We first show that for any $I \in \widetilde{R}$, $\mathbf{I}(\mathbf{V}(I)) = I$. Suppose that $I \in \widetilde{R}$. By Theorem 2.12,

$$\mathbf{I}(\mathbf{V}(I)) = \sqrt{I}.$$

Since I is radical, i.e. $\sqrt{I} = I$. Thus $\mathbf{I}(\mathbf{V}(I)) = I$. This implies that $\mathbf{V}$ is injective and $\mathbf{I}$ is surjective. By Corollary 1.7(i) and (ii), both $\mathbf{V}$ and $\mathbf{I}$ are bijective.

As the composition of $\mathbf{I}$ and $\mathbf{V}$ is an identity map, i.e. $\mathbf{I} \circ \mathbf{V}(I) = I$ for all $I \in \widetilde{R}$. One sees that $\mathbf{V}^{-1} = \mathbf{I}$. □

Two quick applications of Nullstellensatz are given below.

Proposition 2.14 *Let S be a subset of a variety V in $\bar{k}^n$. Then V is the Zariski closure of S if and only if $\mathbf{I}(S) = \mathbf{I}(V)$.*

Proof. Assume that V is the Zariski closure of S. Then $V = \mathbf{V}(\mathbf{I}(S))$ and $\mathbf{I}(V) = \mathbf{I}(S)$ by Lemma 1.6. Conversely, assume that $\mathbf{I}(S) = \mathbf{I}(V)$. Then

$$\mathbf{V}(\mathbf{I}(S)) = \mathbf{V}(\mathbf{I}(V) = V.$$

By Lemma 1.6 again, $\mathbf{V}(\mathbf{I}(S))$ is the Zariski's closure of S. Thus, V is the Zariski closure of S. □

Proposition 2.15 *Let ℓ be an integer with $1 \leq \ell < n$, and $\pi_\ell : \bar{k}^n \longrightarrow \bar{k}^{n-\ell}$ be the projection that maps $(c_1, c_2, \ldots, c_n)$ to $(c_{\ell+1}, c_{\ell+2}, \ldots, c_n)$. If I is an ideal of $k[\mathbf{x}]$, and $I^{(\ell)}$ is the intersection of I with $k[x_{\ell+1}, x_{\ell+2}, \ldots, n]$, then the Zariski closure of $\pi_\ell(\mathbf{V}(I))$ is equal to $\mathbf{V}\left(I^{(\ell)}\right)$.*

Proof. It is clear that $\pi_\ell(\mathbf{V}(I)) \subset \mathbf{V}(I^{(\ell)})$. If $f \in k[x_{\ell+1}, x_{\ell+2}, \ldots, n]$ vanishes on $\pi_\ell(\mathbf{V}(I))$, it vanishes on $\mathbf{V}(I)$. By Theorem 2.12, f is in the radical ideal of I, and so it is in the radical ideal of $I^{(\ell)}$. Consequently, f vanishes on $\mathbf{V}\left(I^{(\ell)}\right)$. The proposition then follows from Proposition 2.14. □

A subset S of a variety V is said to be *(Zariski) dense* in V if the Zariski closure of S is equal to V. Proposition 2.14 says that S is dense in V if and only if every polynomial vanishing on S must vanish on V, and Proposition 2.15 means that the geometric projection of a variety is dense in its algebraic projection.

Exercises for Chapter 3

1. Let $f = a_n x^n + \ldots + a_0, g = x - c$. Prove that
$$\mathrm{res}_x(f, g) = (-1)^n f(c).$$

2. Suppose that f, g, h are polynomials in $\in k[x]$ with positive degrees. Prove that
$$\mathrm{res}_x(f, gh) = \mathrm{res}_x(f, g)\mathrm{res}_x(f, h).$$

3. Give a domain which is not Noetherian.

4. Let $k = \mathbf{Q}$ and $P \subset k[\mathbf{x}]$. Define
$$\mathbf{V}_k(P) = \{\mathbf{p} \in k^n | f(\mathbf{p}) = 0, \forall f \in P\}.$$
Show that $\mathbf{V}_k(P) = \emptyset$ may not imply $\langle P \rangle = k[\mathbf{x}]$.

Chapter 3

Gröbner Bases

In this chapter we describe a powerful computational tool in polynomial ideal theory. It has many applications in algebraic geometry.

Given a polynomial ring $k[\mathbf{x}]$, we denote by $\mathbf{M}_n$ the commutative monoid of all power products $x_1^{i_1} \cdots x_n^{i_n}$ with $i_i, \ldots, i_n$ being nonnegative integers. An element of $\mathbf{M}_n$ is called a *monomial*.

3.1 Dickson's lemma

For two monomials u and v in $\mathbf{M}_n$, we say that v is a *divisor* of u or u is a *multiple* of v if there exists w in $\mathbf{M}_n$ such that $u = wv$. In this case we write $v|u$.

Lemma 3.1 (Dickson's lemma) *If A is a nonempty subset of $\mathbf{M}_n$, then there exists a finite set B of A such that any monomial of A is a multiple of some element of B.*

Proof. We proceed by induction on n. The lemma evidently holds when $n = 1$. Assume that it holds for $n - 1$. Let w be a monomial of A. We put

$$M_0 = \{v \in A : w|v\}.$$

and

$$M_{ij} = \{v \in A | \deg_{x_i}(v) = j\} \quad \text{for all } j \text{ with } 0 \leq j < \deg_{x_i}(w).$$

Since the degree of all monomials in M_{ij} is fixed to be j with respect to x_i, M_{ij} can be mapped bijectively to a subset of $\mathbf{M}_{n-1}$. By the induction

hypothesis, M_{ij} contains a finite set B_{ij} such that any element of M_{ij} is divisible by some element of B_{ij}. Suppose that $v \in A \setminus M_0$. Then there is i with $1 \leq i \leq n$ such that $\deg_{x_i}(v) < \deg_{x_i}(w)$. So $v \in M_{ij}$ where $j = \deg_{x_i}(v)$. This implies that

$$A = M_0 \cup (\cup_{i,j} M_{ij}) .$$

Now the finite set

$$\{w\} \cup (\cup_{i,j} B_{ij})$$

is what we seek. □

In the situation described in Lemma 3.1, we call B a *(finite) Dickson basis* of A. A subset of $\mathbf{M}_n$ is said to be *autoreduced* if, for any two elements u, v in the subset, neither $u|v$ nor $v|u$.

Proposition 3.2 *Let A be a subset of $\mathbf{M}_n$ and B a Dickson basis of A. The following statements are equivalent:*

(1). B is contained in every Diskson basis of A;

(2). The number of elements in any Dickson basis of A is no less than that of B;

(3). B is autoreduced

Proof. It is obvious that (1) implies (2). If there exist $u, v \in B$ such that $u|v$, then $B \setminus \{v\}$ is again a Dickson basis. Thus, (2) implies (3). Assume now that B is an autoreduced Dickson basis, and C is another Dickson basis. If w were in $B \setminus C$, then there would exist $u \in C$ such that $u|w$, and there would exist $v \in B$ such that $v|u$. We would have $v|w$. Since B is autoreduced, $v = w = u$, a contradiction. So (3) implies (1). □

For a subset A of $\mathbf{M}_n$, the autoreduced Dickson basis of A is called the *canonical Dickson basis*, which is unique by Proposition 3.2.

3.2 Monomial orders

A *binary relation* on $\mathbf{M}_n$ is a subset of $\mathbf{M}_n \times \mathbf{M}_n$. Let S be a binary relation on $\mathbf{M}_n$. Then S is called an *order* (or *partial order*) if it satisfies the following properties:

a. $(u, u) \notin S$ for all $u \in \mathbf{M}_n$;

b. if $(u, v) \in S$ and $(v, w) \in S$ then $(u, w) \in S$;

In the following, to avoid the confusion, we shall write $\succ$ for an order S and write $a \succ b$ for (a, b) in S. An order $\succ$ on $\mathbf{M}_n$ is called *total* or *linear* if for any pair of monomials u and v, one of the three statements

$$u \succ v,\ u = v,\ v \succ u$$

should be true. We shall write $u \succeq v$ if $u \succ v$ or $u = v$. A total order $\succ$ on $\mathbf{M}_n$ is called a *monomial order* if it satisfies

(i) if $u \succ v$ and $w \in \mathbf{M}_n$, then $uw \succ vw$;

(ii) $u \succ 1$ for any monomial $u \neq 1$.

Sometimes for the convenience, we say u is higher than v or v is lower than u if $u \succ v$. Let $\succ$ be a monomial order on $\mathbf{M}_n$. From the definition of monomial order, one easily sees that if $v|u$ then $u \succ v$.

Example 3.1 *Assume that $u, v \in \mathbf{M}_n$. We write $u = \mathbf{x}^\alpha$ and $v = \mathbf{x}^\beta$, where $\alpha, \beta \in \mathbf{Z}^n_{\geq 0}$.*

(1) *(lex order) We say $u \succ v$ if, in the vector difference $\alpha - \beta$, the left-most nonzero entry is positive. We will write $u \succ_{lex} v$.*

(2) *(graded lex order) We say $u \succ v$ if $|\alpha| > |\beta|$ or $|\alpha| = |\beta|$ and $u \succ_{lex} v$.*

An order on $\mathbf{M}_n$ is said to be *Noetherian* if there does not exist any infinite sequence in $\mathbf{M}_n$ which is strictly decreasing, i.e. the sequence

$$u_1 \succ u_2 \succ u_3 \succ \cdots$$

is stable. As a direct consequence of Dickson's lemma.

Proposition 3.3 *Every monomial order $\succ$ on $\mathbf{M}_n$ is Noetherian.*

Proof. Suppose the contrary that there is an infinite sequence

$$u_1 \succ u_2 \succ \cdots$$

in $\mathbf{M}_n$. There exists a Dickson basis $B = \{u_{i_1}, \ldots, u_{i_m}\}$ for the set $\{u_1, u_2, \ldots\}$. Let $l = \max\{i_1, \ldots, i_m\}$. Then u_{l+1} is lower than all elements of B, but it is a multiple of some element in B, a contradiction. □

Let us fix a monomial order $\succ$ on $\mathbf{M}_n$ in the rest of this section. For a polynomial $f \in k[\mathbf{x}]$, we define the *support* of f to be the set of monomials that appear effectively in f, denoted by $\mathrm{supp}(f)$. In other words, write

$$f = \sum_{\alpha} a_\alpha \mathbf{x}^\alpha$$

then

$$\mathrm{supp}(f) = \{\mathbf{x}^\alpha | a_\alpha \neq 0\}.$$

Assume now that f is nonzero. The leading monomial of f, denoted by $\mathrm{lm}(f)$, is defined to be the highest monomial in $\mathrm{supp}(f)$, i.e.

$$\mathrm{lm}(f) = \max_{\succ} \mathrm{supp}(f),$$

and its coefficient is called the leading coefficient of f, denoted by $\mathrm{lc}(f)$. Note that f may have different leading monomials and coefficients with respect to different monomial orders.

Example 3.2 *Let*

$$f = -5x^3 + 7x^2z^2 + 4xyz + 3z^2.$$

(*a*) *With respect to lex order, we would have*

$$\mathrm{lm}(f) = x^3,\ \mathrm{lc}(f) = -5.$$

(*b*) *With respect to graded lex order, we would have*

$$\mathrm{lm}(f) = x^2z^2,\ \mathrm{lc}(f) = 7.$$

We want to extend a monomial order to $k[\mathbf{x}]$. To this end, we define an induced total order on the set of all finite subsets of $\mathbf{M}_n$. For two finite sets A and B, we say that $A \succ B$ if either $A \neq \emptyset$ but $B = \emptyset$, or the highest monomial u in A is higher than the highest monomial v in B, or $u = v$ and $A \setminus \{u\}$ is higher than $B \setminus \{v\}$ according to the previous two rules. It is easy to verify that the induced order is total. Without any confusion arising, we denote this induced total order again by $\succ$.

A useful corollary of Proposition 3.3 is

Corollary 3.4 *If $\succ$ is a monomial order, then its induced order on the set of finite subsets of $\mathbf{M}_n$ is Noetherian.*

Proof. Suppose on the contrary that there is an infinite sequence

$$U_1 \succ U_2 \succ \cdots$$

in which every U_i is a finite subset of $\mathbf{M}_n$. We order the monomials in U_i by

$$u_{i,1} \succ u_{i,2} \succ \cdots \succ u_{i,s_i}.$$

Then we have an infinite decreasing sequence

$$u_{1,1} \succeq u_{2,1} \succeq \cdots .$$

By Proposition 3.3 there exists an integer i_1 such that

$$u_{i_1,1} = u_{i_1+1,1} = \cdots .$$

From the index i_1 on, we have an infinite decreasing sequence

$$u_{i_1,2} \succeq u_{i_1+1,2} \succeq \cdots .$$

The same proposition implies that there exists an integer $i_2 \geq i_1$ such that

$$u_{i_2,2} = u_{i_2+1,2} = \cdots .$$

We have $u_{i_1,1} \succ u_{i_2,2}$. Continuing this process yields an infinite sequence

$$u_{i_1,1} \succ u_{i_2,2} \succ u_{i_3,3} \succ \cdots ,$$

a contradiction to Proposition 3.3. □

A monomial order $\succ$ induces a partial order on $k[\mathbf{x}]$ as follows. We say that a polynomial f is lower than a polynomial g if $\mathrm{supp}(f)$ is lower than $\mathrm{supp}(g)$ with respect to the induced order on the set of finite subsets of $\mathbf{M}_n$. Once again, we denote by $\succ$ the induced order on $k[\mathbf{x}]$. Clearly, neither $f \succ g$ nor $g \succ f$ if and only if $\mathrm{supp}(f) = \mathrm{supp}(g)$.

The next corollary is immediate from Corollary 3.4.

Corollary 3.5 *The order on $k[\mathbf{x}]$ induced by a monomial order is Noetherian.*

3.3 Reduction relations

Let f, h be two nonzero polynomials in $k[\mathbf{x}]$ and g a polynomial in $k[\mathbf{x}]$, we say that f *reduces to* g *by* h if there exists a monomial u in $\mathrm{supp}(f)$ such that

1. $u = v\mathrm{lm}(h)$ for some $v \in \mathbf{M}_n$
2. $g = f - \frac{c}{\mathrm{lc}(h)} vh$, where c is the coefficient of u in f.

So g is obtained by eliminating the term cu from f by the leading term of h. We denote this reduction process by $f \to_h g$. When h is insignificant in the reduction, we may write $\to_h$ as $\to.$. We have the following lemma.

Lemma 3.6 *If $f \to_h g$ for some $h \in k[\mathbf{x}] \setminus \{0\}$, then $f \succ g$. Consequently, there does not exist any infinite sequence*

$$f_1 \to. f_2 \to. \cdots$$

in $k[\mathbf{x}]$.

Proof. Assume that the reduction $f \to_h g$ eliminates a monomial u in f. Then $f = \bar{c}vh + g$ where $\bar{c} \in k$ and $v \in \mathbf{M}_n$ satisfying $u = v\mathrm{lm}(h)$. Set

$$S_1 = \{w \in \mathrm{supp}(f) \,|\, w \succ u\} \quad \text{and} \quad S_2 = \{u\} \cup \{w \in \mathrm{supp}(f) \,|\, u \succ w\}.$$

Then one sees that $S_1 \cap S_2 = \emptyset$ and $\mathrm{supp}(f) = S_1 \cup S_2$. Since $\succ$ is a monomial order,

$$u \succ w, \forall w \in \mathrm{supp}(vh) \setminus \{u\}.$$

Therefore

$$\mathrm{supp}(g) = S_1 \cup \{w \in \mathrm{supp}(g) \,|\, u \succ w\}$$

and so $f \succ g$. The last assertion follows from Corollary 3.5. □

Let H be a subset of $k[\mathbf{x}] \setminus \{0\}$. We say f reduces to g by H, denoted by $f \to_H g$, if there are finitely many elements of H, say $h_1, \ldots, h_m$, such that

$$f \to_{h_1} f_1 \to_{h_2} f_2 \to_{h_3} \ldots \to_{h_m} g.$$

A polynomial f is said to be reduced with respect to H if $f = 0$ or $f \neq 0$ and there does not exist a polynomial g such that $f \to_H g$. It is easy to see that for any nonzero polynomial f, there is $g \in k[\mathbf{x}]$ reduced with respect to H such that $f \to_H g$. Adding one more notation, we denote by $\mathrm{lm}(H)$ the set of leading monomials of the polynomials in H.

Lemma 3.7 *Assume that f is a nonzero polynomial in $k[\mathbf{x}]$. Then f is reduced with respect to H if and only if* $\mathrm{supp}(f) \cap \langle \mathrm{lm}(H) \rangle = \emptyset$.

The following example shows that for a polynomial f, there may exist two distinct polynomials g_1 and g_2 that are reduced with respect to H satisfying that $f \to_H g_i$ for $i = 1, 2$.

Example 3.3 *Let $H = \{xy + y, xz\}$ and $f = xyz$. Consider the lex order $x \succ y \succ z$. Then both 0 and yz are reduced with respect to H, and $f \to_H yz$ and $f \to_H 0$.*

3.4 The notion of Gröbner bases

Let I be an ideal of $k[\mathbf{x}]$ and $I \neq (0)$. We fix a monomial order on $\mathbf{M}_n$ in this section. A finite subset G of $I \setminus \{0\}$ is called a *Gröbner* basis if $\mathrm{lm}(G)$ is a Dickson basis of $\mathrm{lm}(I)$. By Lemma 3.1 there exists a Dickson basis B for $\mathrm{lm}(I)$. For every element $u \in B$, there are polynomials in I whose leading monomials are equal to u. We pick up one of them for each u, and form a finite sets G. Then G is a Gröbner basis. This shows the existence of Gröbner bases with respect to a monomial order.

Two fundamental properties of Gröbner bases are stated in the next theorem.

Theorem 3.8 *Let I be an ideal of $k[\mathbf{x}]$ and $I \neq (0)$. Assume that G is a Gröbner basis of I with respect to a monomial order. Then*

1. *For any $f \in I$, f is reduced with respect to G if and only if $f = 0$;*
2. *if $f \to_G f_1$ and $f \to_G f_2$, both f_1 and f_2 are reduced with respect to G, then $f_1 = f_2$.*

Proof. It suffices to show that if f is reduced with respect to G then $f = 0$. Suppose on the contrary that $f \neq 0$. Since $\mathrm{lm}(f)$ is in $\mathrm{lm}(I)$, there exists $g \in G$ such that $\mathrm{lm}(f) = u\mathrm{lm}(g)$ for some u in $\mathbf{M}_n$. Let

$$h = f - \frac{\mathrm{lc}(f)}{\mathrm{lc}(g)} ug.$$

Then $f \to_G h$. This contradicts to the hypothesis f is reduced with respect to G.

To prove the second assertion, we observe that both $f - f_1$ and $f - f_2$ are in I, and so is $f_1 - f_2$. Since $f_1 - f_2$ is reduced with respect to G, it is equal to zero by the first assertion. □

Corollary 3.9 *For any nonzero polynomial $f \in k[\mathbf{x}]$, $f \in I$ if and only if $f \to_G 0$. Consequently, G is a set of generators of I.*

Proof. It suffices to show that if $f \in I$ then $f \to_G 0$. Suppose $f \in I$. If $f = 0$, there is nothing to prove. Assume that $f \neq 0$. There is $g \in k[\mathbf{x}]$ reduced with respect to G such that $f \to_G g$. One easily sees that $g \in I$. By Theorem 3.8, $g = 0$.

By the first assertion, every element in I is a $k[\mathbf{x}]$-combination of some elements in G. Moreover, for each $f \in G$, $f \to_G 0$. Thus $f \in I$. This proves the second assertion. □

The *membership problem of polynomial ideals* is that: given $f, f_1, \ldots, f_m \in k[\mathbf{x}]$, determine whether f is in the ideal $I = \langle f_1, \ldots, f_m \rangle$. Assume that G is a Gröbner basis of I. We reduce f by $\to_G$ to have a finite sequence

$$f \to_{g_1} \cdot \to_{g_2} \cdots \to_{g_m} \bar{f},$$

where $g_i \in G$. By Theorem 3.8, $\bar{f}$ has to be zero if f is in I, no matter what polynomials in G one chose and what monomial one eliminated in the reduction process. Thus, the membership problem of polynomial ideals will be solved if one can construct a Gröbner basis from the given basis $f_1, \ldots, f_m$. In the next section, we describe an algorithm for computing Gröbner bases.

A Gröbner basis G is said to be *autoreduced* if every element $g \in G$ is reduced with respect to $G \setminus \{g\}$. A Gröbner basis G is said to be *canonical* if it is autoreduced, and the leading coefficient of every polynomial in G is equal to one.

Proposition 3.10 *Let $\succ$ be a monomial order on $\mathbf{M}_n$ and I be a nonzero ideal of $k[\mathbf{x}]$. Then there exists a unique canonical Gröbner basis of I with respect to $\succ$.*

Proof. Assume that G_1 and G_2 are two canonical Gröbner bases of I with respect to $\succ$. Then both $\mathrm{lm}(G_1)$ and $\mathrm{lm}(G_2)$ are autoreduced Dickson basis of $\mathrm{lm}(I)$. By Proposition 3.2, $\mathrm{lm}(G_1) = \mathrm{lm}(G_2)$. If g_1 is in G_1, then there exists g_2 in G_2 such that $\mathrm{lm}(g_1) = \mathrm{lm}(g_2)$. We shall prove that $g_1 = g_2$. Now g_i is reduced with respect to $G_i \setminus \{g_i\}$ for $i = 1, 2$. By Lemma 3.7, $\mathrm{supp}(g_i) \cap \langle \mathrm{lm}(G_i \setminus \{g_i\}) \rangle = \emptyset$ for $i = 1, 2$. Since $\mathrm{lm}(G_2 \setminus \{g_2\}) = \mathrm{lm}(G_1 \setminus \{g_1\})$,

$$\mathrm{supp}(g_1 - g_2) \cap \langle \mathrm{lm}(G_1 \setminus \{g_1\}) \rangle \subset (\mathrm{supp}(g_1) \cup \mathrm{supp}(g_2)) \cap \langle \mathrm{lm}(G_1 \setminus \{g_1\}) \rangle = \emptyset.$$

On the other hand, since $\mathrm{lc}(g_1) = \mathrm{lc}(g_2) = 1$, one has

$$\mathrm{supp}(g_1 - g_2) \subset (\mathrm{supp}(g_1) \cup \mathrm{supp}(g_2)) \setminus \{\mathrm{lm}(g_1)\}.$$

Hence $\mathrm{supp}(g_1 - g_2) \cap \langle \mathrm{lm}(G_1) \rangle = \emptyset$. By Lemma 3.7 again, $g_1 - g_2$ is reduced with respect to G_1. It follows from Theorem 3.8 that $g_1 - g_2 = 0$. Hence, $G_1 \subset G_2$. Likewise, $G_2 \subset G_1$. □

3.5 Buchberger's algorithm

For two nonzero polynomials f and g in $k[\mathbf{x}]$, there exist $u, v \in \mathbf{M}_n$ such that

$$u\mathrm{lm}(f) = v\mathrm{lm}(g) = \mathrm{lcm}(\mathrm{lm}(f), \mathrm{lm}(g)),$$

the least common multiple of $\mathrm{lm}(f)$ and $\mathrm{lm}(g)$. The *S-polynomial* of f and g is defined to be

$$\mathrm{lc}(g)uf - \mathrm{lc}(f)vg,$$

which is denoted by $S(f, g)$. Observe that

$$\mathrm{lm}(\mathrm{lcm}(f, g)) \succ \mathrm{lm}(S(f, g)).$$

The notion of S-polynomials, where S is the initial letter of the word *Subtraction*, is the key to construct Gröbner bases.

Theorem 3.11 (Buchberger's criterion) *Let G be a finite subset of nonzero polynomials in $k[\mathbf{x}]$. Then G is a Gröbner basis of $\langle G \rangle$ if and only if, for all $f, g \in G$,*

$$S(f, g) \to_G 0.$$

Our proof of Theorem 3.11 is divided into several steps.

Lemma 3.12 *Let H be a finite subset of nonzero polynomials in $k[\mathbf{x}]$. If $g \to_H 0$, then there exist $h_1, \ldots, h_m \in H$ and $q_1, \ldots, q_m \in k[\mathbf{x}]$ such that*

1. *$g = q_1 h_1 + \cdots + q_m h_m$, where each of the $\mathrm{lm}(q_i h_i)$ is not higher than $\mathrm{lm}(g)$; and*
2. *$\mathrm{lm}(g) = \mathrm{lm}(q_j h_j)$ for some j with $1 \leq j \leq m$.*

Proof. Let

$$g \to_{h_1} g_1 \to_{h_2} \cdots \to_{h_m} 0.$$

We proceed by induction on m, the number of reduction steps. If the number is one, then

$$g = \frac{lc(g)}{\mathrm{lc}(h_1)} v h_1$$

where $v \in \mathbf{M}_n$. so there is nothing to prove. Assume that g_1 can be written as required in the first assertion of the lemma. By the definition of reduction

$$g = cuh_1 + g_1 \; c \in k$$

where $\mathrm{lm}(uh_1)$ is not higher than $\mathrm{lm}(g)$. The first assertion then follows from the fact $\mathrm{lm}(g) \succeq \mathrm{lm}(g_1)$. The second is obvious. □

Lemma 3.13 *If u, v are in $\mathbf{M}_n$, and f, g are in $k[\mathbf{x}]$ with $fg \neq 0$, then there exists $w \in \mathbf{M}_n$ such that*

$$S(uf,\, vg) = wS(f,\, g).$$

Proof. We have $\mathrm{lm}(uf) = u\mathrm{lm}(f)$ and $\mathrm{lm}(vg) = v\mathrm{lm}(g)$. Thus, the least common multiple of $\mathrm{lm}(uf)$ and $\mathrm{lm}(vg)$ is a multiple of the least common multiple of $\mathrm{lm}(f)$ and $\mathrm{lm}(g)$. Letting t be the latter monomial, we find a monomial w such that

$$\mathrm{lcm}(\mathrm{lm}(uf),\, \mathrm{lm}(vg)) = wt.$$

By the definition of S-polynomials, we compute

$$\begin{aligned} S(uf,\, vg) &= \mathrm{lc}(g)\tfrac{wt}{u\mathrm{lm}(f)}uf - \mathrm{lc}(f)\tfrac{wt}{v\mathrm{lm}(g)}vg \\ &= w\left(\mathrm{lc}(g)\tfrac{t}{\mathrm{lm}(f)}f - \mathrm{lc}(f)\tfrac{t}{\mathrm{lm}(g)}g\right) \\ &= wS(f,\, g). \end{aligned}$$

The lemma is proved. □

Corollary 3.14 *Let H be a subset of nonzero polynomials in $k[\mathbf{x}]$, and let f, g be two nonzero polynomials and u, v two monomials. If $S(f,\, g) \to_H 0$, then $S(uf,\, vg) \to_H 0$.*

The last lemma to be used in our proof of Theorem 3.11 is an application of the telescoping trick.

Lemma 3.15 *Let $f, h_1, \ldots, h_m$ be in $k[\mathbf{x}]$ and*

$$f = c_1h_1 + \cdots + c_mh_m$$

where $c_1, \ldots, c_m$ are nonzero elements in k. If all the $\mathrm{lm}(h_i)$ are equal and higher than $\mathrm{lm}(f)$, then f is a k-linear combination of $S(h_i,\, h_j)$ for all i, j with $1 \leq i < j \leq m$. Furthermore, $\mathrm{lm}(S(h_i, h_j))$ is lower than $\mathrm{lm}(h_i)$ for all i, j.

Proof. Since all the $\mathrm{lm}(h_i)$'s are equal to each other,

$$S(h_i,\, h_j) = \mathrm{lc}(h_j)h_i - \mathrm{lc}(h_i)h_j \quad \text{for all } i,j \text{ with } 1 \le i < j \le m.$$

Obviously, $\mathrm{lm}(S(h_i, h_j))$ is lower than $\mathrm{lm}(h_i)$. We proceed by induction on m. If $m = 2$, then

$$f = \frac{c_1}{\mathrm{lc}(h_2)} S(h_1,\, h_2) + \left(\frac{c_1}{\mathrm{lc}(h_2)} \mathrm{lc}(h_1) + c_2 \right) h_2.$$

Since both $\mathrm{lm}(f)$ and $\mathrm{lm}(S(h_1,\, h_2))$ are lower than $\mathrm{lm}(h_2)$, $c_1\mathrm{lc}(h_1) + c_2 = 0$. When $m > 2$, we write

$$f = \frac{c_1}{\mathrm{lc}(h_2)} S(h_1,\, h_2) + \left(\frac{c_1}{\mathrm{lc}(h_2)} \mathrm{lc}(h_1) + c_2 \right) h_2 + c_3 h_3 + \cdots + c_m h_m.$$

Applying the induction hypothesis to

$$f - \frac{c_1}{\mathrm{lc}(h_2)} S(h_1,\, h_2) = \left(\frac{c_1}{\mathrm{lc}(h_2)} \mathrm{lc}(h_1) + c_2 \right) h_2 + c_3 h_3 + \cdots + c_m h_m$$

yields the lemma. □

We are now ready to prove Buchberger's criterion.

Proof of Theorem 3.11. It suffices to show that G is a Gröbner basis if $S(f,\, g) \to_G 0$ for all $f, g \in G$. By the definition of Gröbner basis, it suffices to show that the leading monomial of every polynomial in $\langle G \rangle$ is divisible by the leading monomial of some element in G. Assume that $G = \{g_1, \cdots, g_m\}$.

Let h be a non-zero polynomial in $\langle G \rangle$. Set

$$S_h = \left\{ (a_1, \cdots, a_m) \in k[\mathbf{x}]^m \,\middle|\, h = \sum_{i=1}^{m} a_i g_i \right\}.$$

With the convention, set $\mathrm{lm}(0) = 1$. Denote

$$u = \min_{\mathbf{a} \in S_h} \max\{\mathrm{lm}(a_1 g_1), \cdots, \mathrm{lm}(a_m g_m)\}.$$

Then $u \succeq \mathrm{lm}(h)$. If $u = \mathrm{lm}(h)$, it is easy to see that $\mathrm{lm}(h)$ is a multiple of some $\mathrm{lm}(g_i)$ and the proof is completed. Now suppose that $u \succ \mathrm{lm}(h)$. Let $(a_1, \cdots, a_m)$ be an element in S_h such that

$$u = \max\{\mathrm{lm}(a_1 g_1), \cdots, \mathrm{lm}(a_m g_m)\}.$$

Write

$$h = \sum_{\mathrm{lm}(a_i g_i)=u} \mathrm{lt}(a_i)g_i + \sum_{\mathrm{lm}(a_i g_i)=u} (a_i - \mathrm{lt}(a_i))g_i + \sum_{u \succ \mathrm{lm}(a_j g_j)} a_j g_j, \qquad (3.1)$$

where $\mathrm{lt}(a_i) = \mathrm{lc}(a_i)\mathrm{lm}(a_i)$. Putting $h' = \sum_{\mathrm{lm}(a_i g_i)=u} \mathrm{lt}(a_i)g_i$, we see that $u \succ \mathrm{lm}(h')$. By Lemma 3.15, h' is a k-linear combination of S-polynomials formed by the elements in

$$\{\mathrm{lm}(a_i)g_i \,|\, \mathrm{lm}(a_i g_i) = u\}.$$

Moreover the leading monomials of these S-polynomials are lower than u. It follows from Corollary 3.14 and the hypothesis that these S-polynomials reduce to 0 by G. Due to Lemma 3.12, there are $a'_1, \cdots, a'_m \in k[\mathbf{x}]^m$ such that $h' = \sum_{i=1}^m a'_i g_i$ and

$$u \succ \mathrm{lm}(h') \succeq \mathrm{lm}(a'_i g_i).$$

Combining this with (3.1) yields $h = \sum b_i g_i$ with $u \succ \mathrm{lm}(b_i g_i)$. This contradicts with the choice of u. □

Theorem 3.11 yields the first algorithm for computing Gröbner bases

Buchberger's algorithm: Given a finite set $H = \{h_1, \ldots, h_m\}$ of nonzero polynomials in $k[\mathbf{x}]$, and a monomial order, compute a Gröbner basis of $\langle H \rangle$ with respect to that order.

(1) set H to be G and $T := \{(h_i, h_j) | 1 \le i < j \le m\}$;

(2) while $T \neq \emptyset$ do

  (2.1) choose (a, b) from T and set $T := T \setminus \{(a, b)\}$;

  (2.2) if $S(a, b)$ is reduced with respect to G, then set $g = S(a, b)$. Otherwise, compute a polynomial g that is reduced with respect to G such that $S(a, b) \to_G g$;

  (2.3) if $g \neq 0$, then $T := T \cup \{(h, g) | h \in G\}$ and $G := G \cup \{g\}$;

(3) return G;

By Theorem 3.11, the algorithm will compute a Grönber basis whenever it terminates. Its termination can be proved as follows. Suppose that it does not stop. Then we have an infinite sequences

$$H = G_0 \subset G_1 \subset G_2 \subset \cdots,$$

in which G_{i+1} is the update of G_i in step (2.3). Each G_{i+1} contains a polynomial whose leading monomial is not divisible by the leading monomial of any element of G_i. So there is an infinite sequence

$$\mathrm{lm}(G_0) \subset \mathrm{lm}(G_1) \subset \mathrm{lm}(G_2) \subset \cdots .$$

For each positive integer i, there exists a monomial in G_i not divisible by any element of G_{i-1}. On the other hand, Lemma 3.1 implies that some G_j is a Dickson basis of the union of all the G_i, a contradiction.

Significant progress has been made to improve the efficiency of Buchberger's algorithm. One trick to avoid reducing unnecessary S-polynomials is the product rule.

Proposition 3.16 *Let f, g be two nonzero polynomials in $k[x_1, \ldots, x_n]$ satisfying $\gcd(\mathrm{lm}(f), \mathrm{lm}(g)) = 1$. If h is a polynomial reduced with respect to $\{f, g\}$ such that $S(f, g) \to_{\{f,g\}} h$, then $h = 0$.*

Proof. Assume on the contrary that $h \neq 0$. Then

$$h = pf - qg,\ p, q \in k[\mathbf{x}].$$

As $h \neq 0$ and h is reduced with respect to $\{f, g\}$, $pq \neq 0$. Choose $p, q \in k[\mathbf{x}]$ such that $h = pf - qg$ and $\max\{\mathrm{lm}(pf), \mathrm{lm}(qg)\}$ is minimal. Denote $u = \max\{\mathrm{lm}(pf), \mathrm{lm}(qg)\}$. Then $u \succeq \mathrm{lm}(h)$. Since h is reduced with respect to $\{f, g\}$, $u \succ \mathrm{lm}(h)$. Thus $\mathrm{lm}(pf) = \mathrm{lm}(qg)$. Since $\gcd(\mathrm{lm}(f), \mathrm{lm}(g)) = 1$, one sees that there is $w \in \mathbf{M}_n$ such that

$$\mathrm{lm}(p) = w\mathrm{lm}(g),\ \mathrm{lm}(q) = w\mathrm{lm}(f).$$

Let $\bar{p} = p - \frac{\mathrm{lc}(p)}{\mathrm{lc}(g)} wg$ and $\bar{q} = q - \frac{\mathrm{lc}(q)}{\mathrm{lc}(f)} wf$. Then

$$h = \bar{p}f - \bar{q}g.$$

Moreover $\mathrm{lm}(qf) \succ \mathrm{lm}(\bar{q}f)$ and $\mathrm{lm}(qg) \succ \mathrm{lm}(\bar{q}g)$. This contradicts with the choice of p and q. Therefore $h = 0$. □

3.6 First applications of Gröbner bases

Gröbner bases have an array of applications in commutative algebra and algebraic geometry. Three applications are given in this section, and others are scattered in the sequent chapters .

3.6.1 Membership problems

Besides the ideal membership problems, Gröbner bases can be used the radical ideal and subalgebra membership problems for polynomials. Assume that $f, f_1, \dots f_m$ are nonzero polynomials in $k[\mathbf{x}]$, and we put $I = \langle f_1, \dots, f_m \rangle$. Let G be a Gröbiner basis of I under some monomial order.

(i) (ideal membership problem) $f \in I$ if and only if $f \to_G 0$.

(ii) (radical ideal membership problem) Let t be a new indeterminate and J the ideal generated by $f_1, \dots, f_m, tf - 1$ in $k[x_1, \dots, x_n, t]$. Then $f \in \sqrt{I}$ if and only if a Gröbner basis of J contains 1.

(iii) (subalgebra membership problem)Let $y_1, \dots, y_m$ be new indeterminates. Set

$$J = \langle y_1 - f_1, \dots, y_m - f_m \rangle \text{ in } k[x_1, \dots, x_n, y_1, \dots, y_m].$$

Let G be a Gröbner basis of J with respect to lex order with $x_1 \succ x_2 \succ \dots \succ x_n \succ y_1 \dots \succ y_m$. Let g be a polynomial in $k[x_1, \dots, x_n, y_1, \dots, y_m]$ reduced with respect to G such that $f \to_G g$. Then $f \in k[f_1, \dots, f_m]$ if and only if $g \in k[y_1, \dots, y_m]$.

3.6.2 Linear bases for $k[\mathbf{x}]/I$

Let G be a Gröbner basis of I. Then

$$\{u + I : u \in \mathbf{M}_n \text{ and } u \text{ is reduced with respect to } G\}$$

is a k-linear basis of $k[\mathbf{x}]/I$.

3.6.3 Elimination property

Let G be a Gröbner basis with respect to the lex order $x_1 > x_2 > \dots > x_n$. Then $G \cap k[x_{\ell+1}, \dots, x_n]$ is a Gröbner basis of $I^{(\ell)}$.

3.6.4 Intersection of ideals

Proposition 3.17 *Let I and J be two ideals of $k[\mathbf{x}]$, and let H be the ideal generated by $tI + (1-t)J$ in $k[\mathbf{x}][t]$. Then*

$$I \cap J = H \cap k[\mathbf{x}].$$

3.6.5 Saturation of an ideal

Let I be an ideal of $k[\mathbf{x}]$ and $f \in k[\mathbf{x}]$. The saturation of I with respect to f is defined to be

$$I : f^{\infty} = \{g \in k[\mathbf{x}] | \exists m \in \mathbf{N} \ s.t. f^m g \in I\}.$$

Proposition 3.18 *Let J be the ideal generated by $I \cup \{tf - 1\}$ in $k[\mathbf{x}][t]$. Then*

$$I : f^{\infty} = J \cap k[\mathbf{x}].$$

Exercises for Chapter 4

1. Verify that both lex order and grade lex order are monomial orders.
2. Let I be the ideal in $k[x_1, x_2]$ generated by the following polynomials:

$$f_1 = x_1^3 - x_1 x_2 + x_2^2, \ f_2 = x_1^2 - x_2.$$

(1). Find a Gröbner basis of I with respect to the lex order $x_1 \succ x_2$.

(2). Compute a basis of $k[x_1, x_2]/I$ as a k-vector space.

Chapter 4

The Algebra-Geometry Dictionary

In this chapter, all varieties will be k-varieties.

4.1 Irreducible varieties and prime ideals

Let U and V be two varieties in $\bar{k}^n$. We say that U is a subvariety of V if $U \subset V$. The variety V is said to be *irreducible* if it is not the union of two proper subvarieties.

Lemma 4.1 *A variety V is irreducible if and only if, for all $f, g \in k[\mathbf{x}]$*

$$fg|_V = 0 \Rightarrow \textit{either } f|_V = 0 \textit{ or } g|_V = 0.$$

Proof. Let $V_f = V \cap \mathbf{V}(f)$ and $V_g = V \cap \mathbf{V}(g)$. Then $fg|_V = 0$ implies that $V = V_f \cup V_g$. If V is irreducible, then either $V_f = V$ or $V_g = V$. It follows that either $f|_V = 0$ or $g|_V = 0$.

Assume that $V = V_1 \cup V_2$ for some varieties V_1 and V_2. Suppose that $V \setminus V_1 \neq \emptyset$. By Corollary 1.7, $\mathbf{I}(V)$ is a proper subset of $\mathbf{I}(V_1)$. Let f be an element in $\mathbf{I}(V_1)$ but not in $\mathbf{I}(V)$. Then for any $g \in \mathbf{I}(V_2)$, $fg|_V = 0$. So $g|_V = 0$, because $f|_V \neq 0$. This implies that $\mathbf{I}(V_2) \subset \mathbf{I}(V)$. Therefore $V = V_2$ and then V is irreducible. □

An ideal P in $k[\mathbf{x}]$ is a *prime* ideal if, for all $f, g \in k[\mathbf{x}]$,

$$fg \in P \Rightarrow \text{either } f \in P \text{ or } g \in P.$$

Lemma 4.2 *An ideal I of $k[\mathbf{x}]$ is prime if and only if $k[\mathbf{x}]/I$ is a domain.*

Proposition 4.3 *A variety V is irreducible if and only if $\mathbf{I}(V)$ is prime.*

An ideal I of $k[\mathbf{x}]$ is called a *maximal ideal* if it is proper and there is no proper ideal containing it. Let M be a maximal ideal and $r \notin M$. Then $M + \langle r \rangle = k[\mathbf{x}]$. So $ar \equiv 1 \bmod M$. It follows that $k[\mathbf{x}]/M$ is a field. Conversely, if the quotient ring is a field, then M is a maximal. So we have

Lemma 4.4 *An ideal M is maximal if and only if $k[\mathbf{x}]/M$ is a field. In particular, a maximal ideal is prime.*

Corollary 4.5 *If I is a maximal ideal of $k[\mathbf{x}]$, then $k[\mathbf{x}]/I$ is a finite algebraic field extension of k.*

Proof. It suffices to show that for each $i = 1, \ldots, n$, $x_i + I$ is algebraic over k, i.e. $I \cap k[x_i] \neq 0$. Assume that $I \cap k[x_i] = 0$ for some i. Let $(c_1, \ldots, c_n)$ be an element of $\mathbf{V}(I)$. Then $c_i \in \bar{k}$. Let $f(x_i)$ be the minimal polynomial of c_i over k. One then has that $(c_1, \ldots, c_n) \in \mathbf{V}(I + \langle f(x_i) \rangle)$. Hence $I + \langle f(x_i) \rangle$ is proper. However I is properly contained in $I + \langle f(x_i) \rangle$ since $f(x_i) \notin I$, a contradiction to the maximality of I. □

Corollary 4.6 *Let $\mathbf{p}$ be in $\bar{k}^n$ and I a maximal ideal of $k[\mathbf{x}]$. Then*

(*a*) *$\mathbf{I}(\mathbf{p})$ is a maximal ideal,*

(*b*) *for any $\mathbf{q} \in \mathbf{V}(I)$, $I = \mathbf{I}(\mathbf{q})$.*

Proof. (*a*) Let J be an ideal containing $\mathbf{I}(\mathbf{p})$. Assume that $J \setminus \mathbf{I}(\mathbf{p}) \neq \emptyset$ and $f \in J \setminus \mathbf{I}(\mathbf{p})$. Then $f(\mathbf{p}) \neq 0$. Let $P(y)$ be the minimal polynomial of $f(\mathbf{p})$ over k. Write $P(y) = y^l + c_{l-1}y^{l-1} + \cdots + c_0$. Then $c_0 \neq 0$. Since $P(f(\mathbf{p})) = 0$, $P(f) \in \mathbf{I}(\mathbf{p}) \subset J$. On the other hand, $P(f) - c_0 \in J$. Thus $c_0 \in J$. This implies that $J = k[\mathbf{x}]$. So $\mathbf{I}(\mathbf{p})$ is maximal.

(*b*) Obviously, $I \subset \mathbf{I}(\mathbf{q})$. Since $\mathbf{I}(\mathbf{q})$ is proper and I is maximal, $I = \mathbf{I}(\mathbf{q})$. □

Corollary 4.7 *If I is a radical ideal, then it is the intersection of all maximal ideals containing I.*

Proof. Let $\{M_\lambda\}_{\lambda \in \Lambda}$ be the set of maximal ideals containing I. Then

$$I \subset \cap_{\lambda \in \Lambda} M_\lambda.$$

Suppose that f is in $\cap_{\lambda \in \Lambda} M_\lambda$. For any $\mathbf{q} \in \mathbf{V}(I)$, $I \subset \mathbf{I}(\mathbf{q})$ and $\mathbf{I}(\mathbf{q})$ is maximal by Corollary 4.6. Hence $f \in \mathbf{I}(\mathbf{q})$, i.e. $f(\mathbf{q}) = 0$. Since I is radical, $f \in I$. □

Remark 4.1 *Assume that Λ is an infinite set and $I = \cap_{\lambda \in \Lambda} J_\lambda$ where I, J_λ are ideals in $k[\mathbf{x}]$. Then the equality $\mathbf{V}(I) = \cup_{\lambda \in \Lambda} \mathbf{V}(J_\lambda)$ may not hold.*

4.2 Irreducible decompositions

Proposition 4.8 *1. A variety is a finite union of irreducible varieties; and*

2. a radical ideal is a finite intersection of prime ideals.

Proof. Let V be a variety. If V is irreducible, then there is nothing to prove. Otherwise, $V = V_1 \cup V_2$ where V_1, V_2 are two proper subvarieties. If both V_1 and V_2 are irreducible, then the first assertion holds. Otherwise, we may apply the same process to V_i, which is reducible. This process must terminate in a finite number of repetitions, for, otherwise, there would be an infinite chain of varieties

$$V = U_0 \supset U_1 \supset U_2 \supset U_3 \supset \cdots$$

in which U_{i+1} is a proper subvarieties of U_i. By the strong Nullstellensatz, we would have an infinite chain of ideals

$$\mathbf{I}(U_0) \subset \mathbf{I}(U_1) \subset \mathbf{I}(U_2) \subset \mathbf{I}(U_3) \subset \cdots$$

in which $\mathbf{I}(U_{i+1})$ is properly contained in $\mathbf{I}(U_i)$, which contradicts to the fact that $k[\mathbf{x}]$ is Noetherian.

Let I be a radical ideal of $k[\mathbf{x}]$. Then there exist irreducible varieties $V_1, \ldots, V_m$ such that

$$\mathbf{V}(I) = V_1 \cup V_2 \cup \cdots \cup V_m$$

by the first assertion. So

$$\mathbf{I}(\mathbf{V}(I)) = \mathbf{I}(V_1 \cup V_2 \cup \cdots \cup V_m) = \mathbf{I}(V_1) \cap \mathbf{I}(V_2) \cap \cdots \cap \mathbf{I}(V_m).$$

Set $P_i = \mathbf{I}(V_i)$, which is prime. Then

$$I = P_1 \cap \cdots \cap P_m$$

by the Strong Nullstellensatz. □

Lemma 4.9 *1. If an irreducible variety V is a contained in a finite union of varieties $V_1, \ldots, V_m$, then $V \subset V_i$ for some i with $1 \leq i \leq m$; and*

2. if a prime ideal P contains a finite intersection of ideals $P_1, \ldots, P_m$, then $P \supset P_i$ for some i with $1 \leq i \leq m$.

Proof. Suppose on the contrary that P contains none of the P_i. Let $a_i \in P_i \setminus P$, $i = 1, \ldots, m$. Then $a = a_1 \cdots a_m \in P$. Since P is prime, $a_j \in P$ for some j with $1 \leq j \leq m$, a contradiction. □

Let $V = V_1 \cup V_2 \cup \cdots \cup V_m$ with V_i irreducible. We say that $V_1, \ldots, V_m$ form an irreducible decomposition of V. An irreducible decomposition is said to be *minimal* if for each i, V_i is not contained in $\cup_{j \neq i} V_j$. Similarly, let I be a radical ideal and $I = \cap_{i=1}^m P_i$ with P_i prime. We say that $P_1, \ldots, P_m$ form a minimal decomposition of I if for each i, $\cap_{j \neq i} P_j$ is not contained in P_i.

Corollary 4.10 *1. Let V be a variety. If $V_1, \ldots, V_m$ and $U_1, \ldots, U_\ell$ are two minimal irreducible decompositions of V, then $m = \ell$ and $V_i = U_i$ for all i with $1 \leq i \leq m$ after a permutation of indices.*

2. Let I be a radical ideal. If $I = \cap_{i=1}^m P_i$ and $I = \cap_{j=1}^\ell Q_j$ are two minimal decompositions of I, then $m = \ell$ and $P_i = Q_i$ for all i with $1 \leq i \leq m$ after a permutation of indices.

Let $V = V_1 \cup \cdots \cup V_m$ be the minimal irreducible decomposition of the variety V. Then $V_1, \ldots, V_m$ are called the irreducible components of V. Likewise, if a radical ideal I has a minimal representation $\cap_{i=1}^m P_i$ as prime ideals, then each P_i is called a minimal prime ideal of I.

4.3 Zariski Closure and Quotient of ideals

Let I and J be two ideals in $k[\mathbf{x}]$. Define

$$I : J = \{f \in k[\mathbf{x}] \,|\, gf \in I \text{ for all } g \in J\}.$$

It is easy to see that $I : J$ is an ideal.

Proposition 4.11 *Let I and J be two ideals in $k[\mathbf{x}]$. Then*

1. $\overline{\mathbf{V}(I) \setminus \mathbf{V}(J)} \subset \mathbf{V}(I : J)$*; and*
2. $\overline{\mathbf{V}(I) \setminus \mathbf{V}(J)} = \mathbf{V}(I : J)$*, provided that I is radical.*

Proof. Assume that $\mathbf{p} \in \mathbf{V}(I) \setminus \mathbf{V}(J)$ and $f \in I : J$. Then $gf \in I$ for all $g \in J$. Thus $g(\mathbf{p})f(\mathbf{p}) = 0$ for all $g \in J$. As $\mathbf{p} \notin \mathbf{V}(J)$, there exists $g \in J$ such that $g(\mathbf{p}) \neq 0$. Therefore $f(\mathbf{p}) = 0$. It follows that $\mathbf{p} \in \mathbf{V}(I : J)$. This proves the first assertion.

Put $S = \mathbf{V}(I) \setminus \mathbf{V}(J)$. Assume that I is radical. Then $I : J$ is radical. Assume that $f \in \mathbf{I}(S)$ i.e. f vanishes on S. Let g be any polynomial in J.

We have that fg vanishes on $\mathbf{V}(I)$. So $fg \in I$, since I is radical. So $f \in I : J$. This implies $\mathbf{I}(S) \subseteq I : J$, and, consequently, $\mathbf{V}(I : J) = \bar{S}$ by Proposition 2.14. □

Assume that $J = \langle f_1, \ldots, f_m \rangle$. Then

$$I : J = \cap_{i=1}^{m} I : \langle f_i \rangle.$$

Lemma 4.12 *Let I be an ideal and g a nonzero element of $k[\mathbf{x}]$. If $\{h_1, \ldots, h_m\}$ is a set of generators of $I \cap \langle g \rangle$, then*

$$\left\{ \frac{h_1}{g}, \ldots, \frac{h_m}{g} \right\}$$

is a set of generators of $I : \langle g \rangle$.

Proof. It is clear that $\frac{h_1}{g}, \ldots, \frac{h_m}{g} \in I : \langle g \rangle$. Let f be in $I : \langle g \rangle$. Then $gf \in I \cap \langle g \rangle$. So

$$gf = \sum_i p_i h_i \quad \text{for some } p_i \in k[x_1, \ldots, x_n].$$

Hence

$$f = \sum_i p_i \frac{h_i}{g}.$$

The proof is completed. □

Note that $\mathbf{V}(I) \setminus \mathbf{V}(J) = \cup_{i=1}^{m} \mathbf{V}(I) \setminus \mathbf{V}(f_i)$. So

$$\overline{\mathbf{V}(I) \setminus \mathbf{V}(J)} = \cup_{i=1}^{m} \overline{\mathbf{V}(I) \setminus \mathbf{V}(f_i)}.$$

If I is radical, then

$$\overline{\mathbf{V}(I) \setminus \mathbf{V}(J)} = \cup_{i=1}^{m} \mathbf{V}(I : \langle f_i \rangle).$$

In general, we have the following proposition.

Proposition 4.13 *Let I be an ideal in $k[\mathbf{x}]$ and $f \in k[\mathbf{x}] \setminus \{0\}$. Then*

$$\overline{\mathbf{V}(I) \setminus \mathbf{V}(f)} = \mathbf{V}(I : f^{\infty}).$$

Proof. Put $S = \mathbf{V}(I) \setminus \mathbf{V}(f)$. We first show that $S \subset \mathbf{V}(I : f^{\infty})$. Assume that $\mathbf{p} \in S$. Then $f(\mathbf{p}) \neq 0$. For any $g \in I : f^{\infty}$, $f^{m_g} g \in I$ for some $m_g \in \mathbf{N}$. Thus $f^{m_g}(\mathbf{p}) g(\mathbf{p}) = 0$ and then $g(\mathbf{p}) = 0$ for all $g \in I : f^{\infty}$. This proves that $S \subset \mathbf{V}(I : f^{\infty})$. Let $g \in \mathbf{I}(S)$. Then fg vanishes on $\mathbf{V}(I)$, i.e. $f^m g^m \in I$ for some $m \in \mathbf{N}$. This implies that $g^m \in I : f^{\infty}$. In other words,

$$g \in \sqrt{I : f^{\infty}} = \mathbf{I}(\mathbf{V}(I : f^{\infty})).$$

The proposition follows from Lemma 1.6.

4.4 Zero-dimensional ideals

Theorem 4.14 *(Finiteness Theorem) Let $I \subset k[\mathbf{x}]$ be an ideal. Then the following conditions are equivalent:*

(a) $\mathbf{V}(I)$ *is a finite set.*

(b) $I \cap k[x_i] \neq 0$ *for all* $i = 1, \ldots, n$.

(c) *If G is a Gröbner basis for I, then for each i with $1 \leq i \leq n$, there is $m_i \in \mathbf{N}$ such that $x_i^{m_i} \in \mathrm{lm}(G)$.*

(d) $k[\mathbf{x}]/I$ *is a finite-dimensional vector space over k.*

Proof. $(b) \Rightarrow (a)$ Obviously.
$(a) \Rightarrow (b)$ If $\mathbf{V}(I) = \emptyset$, then $1 \in I$ by the Weak Nullstellensatz. In this case $1 \in I \cap k[x_i]$ for all $i = 1, \ldots, n$. Now assume that

$$\mathbf{V}(I) = \{\mathbf{c}_1, \cdots, \mathbf{c}_d\}.$$

It is easy to see that for each $i = 1, \cdots, n$, there is $f_i(x_i) \in k[x_i] \setminus \{0\}$ such that $f_i(\mathbf{c}_j) = 0$ for all $1 \leq j \leq d$. Due to Hilbert's Nullstellensatz, $f_i^{m_i}$ is in I for some $m_i \in \mathbf{N}$. Hence, $f_i^{m_i} \in I \cap k[x_i] \setminus \{0\}$.

$(b) \Rightarrow (c)$ Let $g_i \in I \cap k[x_i] \setminus \{0\}$ for each $i = 1, \ldots, n$. Then $\mathrm{lm}(g_i) = x_i^{l_i}$. As $g_i \to_G 0$, there is $u_i \in \mathrm{lm}(G)$ satisfying $u_i | x_i^{l_i}$. This implies that $u_i = x_i^{m_i}$ for some $m_i \in \mathbf{N}$.

$(c) \Rightarrow (d)$ Exercise. Verify that $\dim_k (k[\mathbf{x}]/I) \leq m_1 m_2 \cdots m_n$.

$(d) \Rightarrow (b)$ Let $d = dim_k (k[\mathbf{x}]/I)$. Then for each i with $1 \leq i \leq n$, $1, x_i + I, x_i^2 + I, \ldots, x_i^d + I$ are linearly dependent over k. In other words, there are $c_0, c_1, \ldots, c_d \in k$, not of them are zero, such that

$$c_0 + c_1(x_i + I) + \ldots + c_d(x_i^d + I) = 0.$$

This implies that $c_d x_i^d + \ldots + c_1 x_i + c_0 \in I$. □

An ideal I in $k[\mathbf{x}]$ is said to be zero-dimensional if it satisfies any of the above conditions. By Theorem 4.14, we can decide if $\mathbf{V}(f_1, \ldots, f_m)$ is finite by the Gröbner basis computation.

Proposition 4.15 *If I is a zero-dimensional ideal, then*

(i) *the elimination ideal $I^{(\ell)} = I \cap k[x_{\ell+1}, \ldots, x_n]$ is zero-dimensional; and*

(ii) $\pi_\ell(\mathbf{V}(I)) = \mathbf{V}(I^{(\ell)})$.

Proof. (i) is obvious.

We prove (ii) by induction on ℓ. If $\ell = 1$, then there exists a nonzero polynomial p_1 in $k[x_1] \cap I$. Since $\mathrm{lc}(p_1) = 1$, $\mathbf{V}(I^{(1)}) = \pi_1(\mathbf{V}(I))$ by the Extension Theorem.

Assume that the second argument holds for $\ell - 1$, i.e.,

$$\pi_{\ell-1}(\mathbf{V}(I)) = \mathbf{V}(I^{(\ell-1)}). \tag{4.1}$$

Let

$$\begin{array}{rccc} \tilde{\pi}: & k^{n-(\ell-1)} & \to & k^{n-\ell} \\ & (c_\ell, c_{\ell+1}, \ldots, c_n) & \mapsto & (c_{\ell+1}, \ldots, c_n). \end{array}$$

The application of $\tilde{\pi}$ to (4.1) yields that

$$\pi_\ell(\mathbf{V}(I)) = \tilde{\pi}(\pi_{\ell-1}(\mathbf{V}(I))) = \tilde{\pi}(\mathbf{V}(I^{\ell-1})).$$

By the conclusion made in the base case, we have

$$\tilde{\pi}(\mathbf{V}(I^{\ell-1})) = \mathbf{V}(I^{(\ell)}),$$

which implies that

$$\pi_\ell(\mathbf{V}(I)) = \mathbf{V}(I^{(\ell)}).$$

The proof is completed. □

Let I be a zero-dimensional ideal. For $f \in k[\mathbf{x}]$, define

$$\begin{array}{rccc} L_f: & k[\mathbf{x}]/I & \to & k[\mathbf{x}]/I \\ & g + I & \mapsto & fg + I, \end{array}$$

which is a k-linear map. Let $u_1 = 1, u_2, \cdots, u_l$ be elements in $\mathbf{M}_n$ such that $u_1 + I, \ldots, u_l + I$ constitutes a basis of $k[\mathbf{x}]/I$. Then for $f \in k[\mathbf{x}]$, there is a matrix $M_f \in \mathrm{Mat}_l(k)$ such that

$$L_f \begin{pmatrix} u_1 + I \\ u_2 + I \\ \vdots \\ u_l + I \end{pmatrix} = M_f \begin{pmatrix} u_1 + I \\ u_2 + I \\ \vdots \\ u_l + I \end{pmatrix}.$$

Lemma 4.16 *Suppose that* $\mathbf{V}(I) = \{\mathbf{p}_1, \cdots, \mathbf{p}_m\}$. *Then for* $f \in k[\mathbf{x}]$ *and each* j *with* $1 \le j \le m$, $(u_1(\mathbf{p}_j), u_2(\mathbf{p}_j), \cdots, u_l(\mathbf{p}_j))^T$ *is an eigenvector of* M_f *with eigenvalue* $f(\mathbf{p}_j)$.

Proof. Denote $M_f = (a_{i,j})$. Then one has that $fu_i - \sum_{j=1}^{l} a_{i,j}u_j \in I$ for all $1 \leq i \leq l$. In the sequel,

$$f(\mathbf{p}_\mu)u_i(\mathbf{p}_\mu) - \sum_{j=1}^{l} a_{i,j}u_j(\mathbf{p}_\mu) = 0, \ \forall \ i = 1, \cdots, l, \mu = 1, \cdots, m.$$

Note that $(u_1(\mathbf{p}_\mu), u_2(\mathbf{p}_1), \cdots, u_l(\mathbf{p}_\mu))^T$ is a nonzero vector, since $u_1(\mathbf{p}_\mu) = 1$. Hence it is an eigenvector of M_f with eigenvalue $f(\mathbf{p}_\mu)$. □

Example 4.1 *Let $I = \langle x_1^3 - x_2^2x_1, \ x_1^2x_2 - x_2^2\rangle$. The Gröbner basis with respect to the lex order $x_1 > x_2$ is*

$$G = \{x_1^3 - x_2^2x_1, \ x_1^2x_2 - x_2^2, \ x_2^3x_1 - x_1x_2^2, \ x_2^4 - x_2^3\}.$$

From the last polynomial we have that $x_2 = 0$ or $x_2 = 1$. From $x_2 = 0$ we have $x_1 = 0$, while from $x_2 = 1$ we obtain $x_1^3 - x_1$, $x_1^2 - 1$, and 0, whose gcd is $x_1^2 - 1$. So

$$\mathbf{V}(I) = \{(0,0), (1,1), (-1,1)\}.$$

The set

$$\{1 + I, x_2 + I, x_2^2 + I, x_2^3 + I, x_1 + I, x_1x_2 + I, x_1x_2^2 + I, x_1^2 + I\}$$

is a basis of $k[x_1, x_2]/I$. Let $f = x_1$. Then

$$(x_1 + I)\begin{pmatrix} 1+I \\ x_2+I \\ x_2^2+I \\ x_2^3+I \\ x_1+I \\ x_1x_2+I \\ x_1x_2^2+I \\ x_1^2+I \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}\begin{pmatrix} 1+I \\ x_2+I \\ x_2^2+I \\ x_2^3+I \\ x_1+I \\ x_1x_2+I \\ x_1x_2^2+I \\ x_1^2+I \end{pmatrix}.$$

The minimal polynomial of the above matrix M_f is $x^5 - x^3$. Then its eigenvalues are $0, 1, -1$.

4.5 Zero-dimensional radical ideals

In this section, we assume that k is of characteristic zero.

Proposition 4.17 *A proper ideal is a zero-dimensional prime ideal if and only if it is a maximal ideal.*

Proof. If i is a proper zero-dimensional prime ideal, then $R = k[\mathbf{x}]/I$ is a domain and a finite-dimensional vector spaces. Assume that $f+I$ is nonzero in R. Then there exists $a_0, \ldots, a_m \in k$, not all zero, such that

$$\sum_{i=1}^{m} a_i (f+I)^i = 0.$$

Since R does not contain any zero-divisors and $f + I \neq 0$, we may further assume that $a_0 \neq 0$, which implies that $f+I$ is invertible. So I is a maximal ideal.

Conversely, assume that I is a maximal ideal. Then by Corollary 4.5, R is a finitely algebraic extension of k. Thus it is a k-vector space of finite dimension. By the definition, I is zero-dimensional. □

Let I be a zero-dimensional radical ideal. We shall show that

$$|\mathbf{V}(I)| = \dim_k (k[\mathbf{x}]/I) .$$

We first consider the case that I is a maximal ideal.

Lemma 4.18 (*a*) *Let $p(y) \in k[y]$ be irreducible over k and $g_1, \cdots, g_n \in k[y]$ with $\deg(g_i) \leq \deg(p) - 1$. Let L be a linear polynomial in $k[\mathbf{x}]$ and denote by I the ideal*

$$\langle p(L), x_1 - g_1(L), \cdots, x_n - g_n(L) \rangle.$$

If $I \neq k[\mathbf{x}]$, then I is maximal.

(*b*) *For any maximal ideal I, there are an irreducible polynomial $p(y) \in k[y]$, polynomials $g_1(y), \cdots, g_n(y) \in k[y]$ and a linear polynomial $L \in k[\mathbf{x}]$ such that*

$$I = \langle p(L), x_1 - g_1(L), \cdots, x_n - g_n(L) \rangle.$$

Proof. (*a*) Assume that $I \neq k[\mathbf{x}]$. Let J be an ideal containing I. Suppose that $J \backslash I \neq \emptyset$. We shall prove that $J = k[\mathbf{x}]$, which implies that I is maximal. Let $f(\mathbf{x}) \in J \setminus I$. There is $h(y) \in k[y]$ such that $f(\mathbf{x}) - h(L) \in I \subset J$. If $h(y)$ is divided by $p(y)$, then $h(L)$ is in I and so is $f(\mathbf{x})$. This is impossible. Thus $h(y)$ and $p(y)$ are coprime. Let $a(y), b(y)$ be in $k[y]$ such that $ah + bp = 1$. Then $1 = a(L)h(L) + b(L)p(L) \in J$. Hence $J = k[\mathbf{x}]$.

(*b*) Let $\mathbf{c}$ be an element in $\mathbf{V}(I)$. By Corollary 4.6, $I = \mathbf{I}(\mathbf{c})$. Write $\mathbf{c} = (c_1, c_2, \cdots, c_n)$. Then $k(\mathbf{c}) = k(c_1, c_2, \cdots, c_n)$ is a finite algebraic field extension of k. The Primitive Element Theorem implies that there $a_1, \cdots, a_n \in k$ such that $k(\mathbf{c}) = k(a_1c_1 + \cdots + a_nc_n)$. For each $i = 1, \cdots, n$, let g_i be the polynomial in $k[y]$ satisfying $c_i = g_i(a_1c_1 + \cdots + a_nc_n)$. Set $L = a_1x_1 + \cdots + a_nx_n \in k[\mathbf{x}]$. Let $p(y)$ be the minimal polynomial of $L(\mathbf{c})$ over k. Then the polynomials $p(L), x_1 - g_1(L), \cdots, x_n - g_n(L)$ vanish at $\mathbf{c}$. Thus $p(L), x_1 - g_1(L), \cdots, x_n - g_n(L)$ are all in $\mathbf{I}(\mathbf{c})$. By (*a*), the ideal $\langle p(L), x_1 - g_1(L), \cdots, x_n - g_n(L)\rangle$ is maximal and then it is equal to I. □

Proposition 4.19 *Let I be a maximal ideal in $k[\mathbf{x}]$. Then*

$$\mathbf{V}(I) = \dim_k(k[\mathbf{x}]/I).$$

Proof. Due to Lemma 4.18, there are a linear polynomial $L \in k[\mathbf{x}]$ and $p(y), g_1(y), \cdots, g_n(y) \in k[y]$ with $p(y)$ irreducible and $\deg(g_i) < \deg(p)$ for all $1 \leq i \leq n$ such that

$$I = \langle p(L), x_1 - g_1(L), \cdots, x_n - g_n(L)\rangle .$$

It is easy to verify that $\dim_k(k[\mathbf{x}]/I) = \deg(p)$. So it suffices to show that $|\mathbf{V}(I)| = \deg(p)$. We define a map

$$\begin{array}{rcl} \tau : \mathbf{V}(I) & \longrightarrow & \{\beta \in \bar{k} \mid p(\beta) = 0\} \\ \mathbf{c} & \longrightarrow & L(\mathbf{c}). \end{array}$$

For any $\mathbf{c} = (c_1, \cdots, c_n) \in \mathbf{V}(I)$, one easily sees that $L(\mathbf{c})$ is a zero of $p(y)$. Hence τ is well-defined. We claim that τ is bijective. Since $c_i = g_i(L(\mathbf{c}))$,τ is injective. Let $\beta \in \bar{k}$ satisfy that $p(\beta) = 0$ and let $c_i = g_i(\beta)$ for all $1 \leq i \leq n$. We shall show that

$$\beta = L(c_1, \cdots, c_n),$$

which will imply that $(c_1, \cdots, c_n) \in \mathbf{V}(I)$ and thus τ is surjective. Now set

$$q(y) = y - L(g_1(y), \cdots, g_n(y)).$$

Then $q(L) \in I$. Since $p(L) \in I$ and $p(y)$ is irreducible, $p(y)$ divides $q(y)$. Otherwise, $1 = \gcd(q(y), p(y))$ which means that $1 \in I$. This is impossible. Since $p(\beta) = 0$, $q(\beta) = 0$, i.e. $\beta = L(c_1, \cdots, c_n)$. Thus τ is surjective. So $|\mathbf{V}(I)| = \deg(p)$. □

In the following, we consider the general case. By Propositions 4.8 and 4.17,

$$I = M_1 \cap M_2 \cap \cdots \cap M_\ell$$

where M_i is a maximal ideal containing I. Furthermore, one has the following lemma.

Lemma 4.20 *$k[\mathbf{x}]/I \cong \bigoplus_{i=1}^{\ell} k[\mathbf{x}]/M_i$ as rings.*

Proof. We define a map

$$\begin{aligned} \tau : k[\mathbf{x}]/I &\longrightarrow \bigoplus_{i=1}^{\ell} k[\mathbf{x}]/M_i \\ f + I &\longrightarrow (f + M_1, \ldots, f + M_\ell). \end{aligned}$$

One can easily verify that τ is a ring homomorphism. Since $I = \cap_{i=1}^{\ell} M_i$, τ is injective. It remains to show that τ is surjective. Let $(g_1 + M_1, \cdots, g_\ell + M_\ell)$ be an element of $\bigoplus_{i=1}^{\ell} k[\mathbf{x}]/M_i$. We shall construct an element $f \in k[\mathbf{x}]$ satisfying $f - g_i \in M_i$ for all $1 \leq i \leq \ell$. If such element f exists, then

$$\tau(f) = (g_1 + M_1, \cdots, g_\ell + M_\ell),$$

which implies that τ is surjective. Let $h_i \in (\bigcap_{j=1, j\neq i}^{\ell} M_j) \setminus M_i$. As M_i is maximal, there is $r_i \in k[\mathbf{x}]$ such that $r_i h_i - 1 \in M_i$. Set $f = \sum_{j=1}^{\ell} r_j h_j g_j$. Then for each $i = 1, \ldots, \ell$,

$$f - g_i = (r_i h_i - 1) g_i + \sum_{j=1, j\neq i}^{\ell} r_j h_j g_j \in M_i.$$

□

Proposition 4.21 *Let $I \subseteq k[\mathbf{x}]$ be a zero-dimensional radical ideal. Then*

$$\mathbf{V}(I) = \dim_k \left(k[\mathbf{x}]/I \right).$$

Proof. Suppose $I = M_1 \cap \cdots \cap M_\ell$ where M_i is maximal. Note that $M_i + M_j = k[\mathbf{x}]$ if $i \neq j$. Hence $\mathbf{V}(M_i) \cap \mathbf{V}(M_j) = \emptyset$. This implies that

$$|\mathbf{V}(I)| = \sum_{i=1}^{\ell} |\mathbf{V}(M_i)|.$$

On the other hand, by Lemma 4.20,

$$\dim_k(k[\mathbf{x}]/I) = \sum_{i=1}^{\ell} \dim_k(k[\mathbf{x}]/M_i).$$

Then the proposition follows from Lemma 4.18. □

Corollary 4.22 *Let I be a zero-dimensional ideal in $k[\mathbf{x}]$. Then*

$$|\mathbf{V}(I)| \leq \dim_k(k[\mathbf{x}]/I).$$

Furthermore, the equality holds if and only if I is radical.

Proof. There is a natural homomorphism

$$\begin{array}{rcl} \varphi : k[\mathbf{x}]/I & \longrightarrow & k[\mathbf{x}]/\sqrt{I} \\ f + I & \longrightarrow & f + \sqrt{I}. \end{array}$$

This homomorphism is surjective and it is injective if and only if I is radical. Then the corollary follows from Proposition 4.21. □

Example 4.2 *Assume that I is an ideal in $k[x_1, x_2]$ generated by*

$$g_1 = x_1^3 - x_2^2 x_1 \quad \text{and} \quad g_2 = x_1^2 x_2 - x_2^2.$$

Compute a Grobner basis G of I w.r.t. the lex monomial order $x_1 \succ x_2$. One has

$$G = \{x_1^3 - x_2^2 x_1, x_1^2 x_2 - x_2^2, x_1 x_2^3 - x_1 x_2^2, x_2^4 - x_2^3\}.$$

Hence $\dim_k(k[x_1, x_2]/I) = 8$. *However*

$$\mathbf{V}(I) = \{(0, 0), (1, 1), (-1, 1)\}.$$

Thus $|\mathbf{V}(I)| = 3 < 8$. So I is not radical.

For every $p(x) \in k[x] \setminus \{0\}$, we say $p(x)$ is square-free if $p(x) = \lambda \cdot \underline{p}$ where $\lambda \in k$.

Proposition 4.23 [Seidenberg 92] *Let I be an ideal of $k[\mathbf{x}]$ that is zero-dimensional. If p_i is the generator of $I \cap k[x_i]$ for $i = 1, \ldots, n$, then*

$$\sqrt{I} = I + \langle \underline{p_1}, \ldots, \underline{p_n} \rangle.$$

Our proof of Proposition 4.23 is based on a standard technique in commutative algebra given below.

Let R be a commutative ring. Two ideals I and J are said to be *co-maximal* if $I + J = R$.

Lemma 4.24 *Let $I_1, \ldots, I_m$ be pairwise co-maximal ideals of R. If I is an ideal of R, then*

$$I + \cap_{i=1}^{m} I_i = \cap_{i=1}^{m} (I + I_i).$$

Proof. Use induction on m. We first prove the lemma for the case $m = 2$. Since $I, I_1 \cap I_2 \in I + I_i$ for all $1 \leq i \leq 2$.

$$I + I_1 \cap I_2 \subseteq (I + I_1) \cap (I + I_2).$$

Since $I + I_1$ and $I + I_2$ are co-maximal, there are $a \in I + I_1, b \in I + I_2$ such that $a + b = 1$. For any $f \in (I + I_1) \cap (I + I_2)$,

$$f = f(a + b) = fa + fb \in (I + I_1)(I + I_2) \subseteq I + I_1 I_2 \subseteq I + I_1 \cap I_2.$$

Therefore the lemma holds in the case $m = 2$. Now assume that the lemma holds for $m - 1$. One has that

$$\cap_{i=1}^{m} (I + I_i) = \left(\cap_{i=1}^{m-1} (I + I_i)\right) \cap (I + I_m) = \left(I + \cap_{i=1}^{m-1} I_i\right) \cap (I + I_m).$$

By the base case, it suffices to show that $\cap_{i=1}^{m-1} I_i$ and I_m are co-maximal. As I_i and I_m are co-maximal, there are $a_i \in I_i, b_i \in I_m$ such that $a_i + b_i = 1$ where $i = 1, \cdots, m - 1$. Then

$$1 = \prod_{i=1}^{m-1} (a_i + b_i) = \prod_{i=1}^{m-1} a_i + b$$

where $b \in I_m$. Thus $\cap_{i=1}^{m-1} I_i$ and I_m are co-maximal. □

Lemma 4.25 *Suppose that $p_1(y), \cdots, p_n(y) \in k[y]$ are square-free. Then the ideal in $k[\mathbf{x}]$ generated by*

$$p_1(x_1), p_2(x_2), \cdots, p_n(x_n)$$

is radical.

Proof. Denote $J = \langle p_1(x_1), p_2(x_2), \cdots, p_n(x_n)\rangle$. Then J is obviously zero-dimensional and

$$|\mathbf{V}(J)| = \prod_{i=1}^{n} \deg(p_i).$$

On the other hand, by Buchberger's Criterion, $\{p_1(x_1), \cdots, p_n(x_n)\}$ is a Gröbner basis of J w.r.t the lex monomial order $x_1 \succ x_2 \succ \cdots \succ x_n$. From this, one sees that

$$\dim_k(k[\mathbf{x}]/J) = \prod_{i=1}^{n} \deg(p_i) = |\mathbf{V}(J)|.$$

Corollary 4.22 implies that J is radical. □

We now prove Proposition 4.23.

Put $J = I + \langle \underline{p_1}, \ldots, \underline{p_n}\rangle$. We first show that J is a radical ideal. By Lemma 4.25, $\langle \underline{p_1}, \ldots, \underline{p_n}\rangle$ is a radical ideal. Then it is the intersection of finitely many maximal ideals. Suppose that

$$\langle \underline{p_1}, \ldots, \underline{p_n}\rangle = \cap_{i=1}^{l} M_i$$

where M_i is maximal. Note that all maximal ideals are pairwise co-maximal. By Lemma 4.24,

$$J = I + \langle \underline{p_1}, \ldots, \underline{p_n}\rangle = I + \cap_{i=1}^{l} M_i = \cap_{i=1}^{l} (I + M_i).$$

Since M_i is maximal, either $I + M_i = M_i$ or $I + M_i = k[\mathbf{x}]$. In the sequel, J is the intersection of some maximal ideals. Thus J is radical. As $\underline{p_i} \in \sqrt{I}$ for all $1 \leq i \leq n$, $J \subseteq \sqrt{I}$. Hence $J = \sqrt{I}$. □

Example 4.3 *Compute a basis of the radical of the ideal I generated by*

$$g_1 = x_1^3 - x_2^2 x_1 \quad \text{and} \quad g_2 = x_1^2 x_2 - x_2^2.$$

The ideal I is zero-dimensional. We have

$$I \cap k[x_1] = \langle p_1\rangle \quad \text{and} \quad I \cap k[x_2] = \langle p_2\rangle$$

where $p_1 = x_1^5 - x_1^3$ and $p_2 = x_2^4 - x_2^3$. Since

$$\underline{p_1} = x_1^3 - x_1 \quad \text{and} \quad \underline{p_2} = x_2^2 - x_2,$$

The radical of I has a basis $g_1, g_2, \underline{p_1}, \underline{p_2}$ by Proposition 4.23. It has a Gröbner basis

$$\{x_2^2 - x_2, x_1 x_2 - x_1, x_1^2 - x_2\}.$$

4.6 Prime decomposition of zero-dimensional ideals

In this section, we shall describe a method to compute the irreducible decomposition of a zero-dimensional variety. We will need the following lemmas.

Lemma 4.26 *Assume that $\mathbf{p}_1, \ldots, \mathbf{p}_m$ are elements of $\bar{k}^n \setminus \{0\}$. Then there is a linear homogeneous polynomial L in $k[\mathbf{x}]$ such that for all $i = 1, \ldots, m$, $L(\mathbf{p}_i) \neq 0$.*

Proof. Denote

$$S = \{c_1 x_1 + \ldots + c_n x_n \mid c_i \in k\}$$

and

$$S_i = \{L \in S \mid L(\mathbf{p}_i) = 0\}.$$

Then S is a k-vector spaces of dimension n and S_i is a k-vector space of dimension $\leq n-1$. It suffices to show that $S \setminus \cup_{i=1}^m S_i \neq \emptyset$. Without loss of generality, we may assume that S_1 is not contained in $\cup_{i=2}^m S_i$. Let $L_1 \in S_1 \setminus \cup_{i=2}^m S_i$ and let $L_2 \in S \setminus S_1$. Then we have that if $aL_1 + L_2, bL_1 + L_2 \in S_i$ for some $i = 2, \ldots, m$, where $a, b \in k$ then $a = b$. Otherwise, $(a-b)L_1 \in S_i$, a contradiction. Since $\{cL_1 + L_2 | c \in k\}$ is an infinite set, there is $\bar{c} \in k$ such that $\bar{c}L_1 + L_2 \notin \cup_{i=2}^m S_i$. It is evident that $\bar{c}L_1 + L_2 \notin S_1$. Consequently, $\bar{c}L_1 + L_2 \notin \cup_{i=1}^m S_i$ but $\bar{c}L_1 + L_2 \in S$. □

Corollary 4.27 *Assume that $\mathbf{p}_1, \ldots, \mathbf{p}_m$ are distinct elements of $\bar{k}^n$. Then there is a linear polynomial L in $k[\mathbf{x}]$ such that*

$$L(\mathbf{p}_i) \neq L(\mathbf{p}_j), \forall\ 1 \leq i < j \leq m.$$

Proof. Consider the set

$$S = \{\mathbf{p}_i - \mathbf{p}_j : 1 \leq i < j \leq m\}.$$

Lemma 4.26 implies that there is a linear polynomial L such that $L(\mathbf{q}) \neq 0$ for all $\mathbf{q} \in S$. In other words, $L(\mathbf{p}_i) \neq L(\mathbf{p}_j)$ for all $1 \leq i < j \leq m$. □

Corollary 4.28 *Let I be a zero-dimensional radical ideal in $k[\mathbf{x}]$. There is a linear polynomial L in $k[\mathbf{x}]$ such that*

$$1 + I, L + I, L^2 + I, \cdots, L^{m-1} + I$$

is a basis of $k[\mathbf{x}]/I$, where $m = \dim_k(k[\mathbf{x}]/I)$.

Proof. Suppose that $\mathbf{V}(I) = \{\mathbf{p}_1, \cdots, \mathbf{p}_m\}$. By Corollary 4.27, there are $c_1, \cdots, c_n$ such that $L := c_1x_1 + \cdots + c_nx_n$ satisfies that $L(\mathbf{p}_i) \neq L(\mathbf{p}_j)$ if $i \neq j$. We shall prove that

$$1 + I, L + I, L^2 + I, \cdots, L^{m-1} + I$$

is a basis of $k[\mathbf{x}]/I$. Suppose that there are $a_0, a_1, \ldots, a_{m-1}$ such that

$$a_0(1 + I) + a_1(L + I) + \cdots + a_{m-1}(L^{m-1} + I) = 0.$$

In other words,

$$a_0 + a_1L + \cdots + a_{m-1}L^{m-1} \in I.$$

Let $g(x) = a_0 + a_1x + \cdots + a_{m-1}x^{m-1}$. Then $g(L(\mathbf{p}_i)) = 0$ for all $\mathbf{p}_i \in \mathbf{V}(I)$. As $L(\mathbf{p}_i) \neq L(\mathbf{p}_j)$ if $i \neq j$, $g(x)$ has m distinct roots, while $\deg(g) < m$. Hence $g(x) = 0$, i.e. $a_i = 0$ for all $0 \leq i \leq m-1$. So $1+I, L+I, \cdots, L^{m-1}+I$ are linearly independent over k and then they are a basis of $k[\mathbf{x}]/I$, because $\dim_k(k[\mathbf{x}]/I) = |\mathbf{V}(I)| = m$. □

Lemma 4.29 [The Shape Lemma] *Let I be a zero-dimensional radical ideal. There are a linear polynomial L in $k[\mathbf{x}]$ and $g_0(x), g_1(x), \cdots, g_n(x) \in k[x]$ with $\deg(g_i) < \deg(g_0)$ for all $1 \leq i \leq n$ such that*

$$\{g_0(L), x_1 - g_1(L), \ldots, x_n - g_n(L)\}$$

is a set of generators of I.

Proof. By Corollary 4.28, there is a linear polynomial L in $k[\mathbf{x}]$ such that

$$1 + I, L + I, L^2 + I, \cdots, L^{m-1} + I$$

is a basis of $k[\mathbf{x}]/I$, where $m = \dim_k(k[\mathbf{x}]/I)$. There is $\bar{g}_0(x) \in k[x]$ with $\deg(\bar{g}_0) < m$ such that

$$L^m + I = \bar{g}_0(L + I)$$

and there are $g_1(x), \cdots, g_n(x) \in k[x]$ with $\deg(g_i) < m$ such that

$$x_j + I = g_i(L + I).$$

Let $g_0(x) = x^m - \bar{g}_0(x)$. Then $g_0(L) \in I$ and $x_j - g_j(L) \in I$ for all $1 \leq i \leq n$. In the following, we show that

$$\{g_0(L), x_1 - g_1(L), \cdots, x_n - g_n(L)\}$$

is a set of generators of I. For any $f \in I$, we can write

$$f = \sum_{i=1}^{n} A_i(x_i - g_i(L)) + Bg_0(L) + \bar{f}(L)$$

where $A_i, B \in k[\mathbf{x}]$ and $\bar{f}(x) \in k[x]$ with $\deg(\bar{f}) < m$. Since $f \in I$, $\bar{f}(L) \in I$, i.e. $\bar{f}(L+I) = 0$. However $1+I, L+I, L^{m-1}+I$ are linearly independent over k, so $\bar{f}(x) = 0$. Therefore f is a $k[\mathbf{x}]$-combination of $g_0(L), x_1 - g_1(L), \cdots, x_n - g_n(L)$. □

Using the Shape Lemma, we can obtain an irreducible decomposition of I as follows. Note that since I is radical, $g_0(x)$ is square-free. Decompose $g_0(x)$ into irreducible factors, say $g_0(x) = p_1(x) \cdots p_l(x)$ where $p_i(x)$ is irreducible. Let

$$M_i = \langle p_i(L), x_1 - g_1(L), \cdots, x_n - g_n(L) \rangle.$$

Then by Lemma 4.18, M_i is maximal and

$$I = M_1 \cap M_2 \cap \cdots \cap M_l.$$

The first step is to find the suitable L. This can be done as follows. Suppose that $u_1+I, u_2+I, \cdots, u_m+I$ is a basis of $k[\mathbf{x}]/I$. We assume $c_1, \cdots, c_n$ are indeterminates for a while. One can compute a matrix $M(c_1, \cdots, c_n) \in \mathrm{Mat}_m(k[c_1, \cdots, c_n])$ such that

$$\begin{pmatrix} 1+I \\ c_1x_1 + \cdots + c_nx_n + I \\ (c_1x_1 + \cdots + c_nx_n)^2 + I \\ \vdots \\ (c_1x_1 + \cdots + c_nx_n)^{m-1} + I \end{pmatrix} = M(c_1, \cdots, c_n) \begin{pmatrix} u_1+I \\ u_2+I \\ u_3+I \\ \vdots \\ u_m+I \end{pmatrix}.$$

Corollary 4.28 implies that there are $\bar{c}_1, \cdots, \bar{c}_n \in k$ such that

$$\det(M(\bar{c}_1, \cdots, \bar{c}_n)) \neq 0.$$

Hence $\det(M(c_1, \cdots, c_n)) \neq 0$. Then any $a_1, \cdots, a_n \in k$ satisfying

$$\det(M(a_1, \cdots, a_n)) \neq 0$$

will have the desired property.

Example 4.4 *(Example 5.3 continued) Let I be an ideal generated by*

$$\{x_2^2 - x_2, x_1x_2 - x_1, x_1^2 - x_2\}$$

which is radical. Then $1 + I, x_1 + I, x_2 + I$ is a basis of $k[x_1, x_2]/I$. Let $L = c_1x_1 + c_2x_2$. Then

$$\begin{pmatrix} 1+I \\ c_1x_1 + c_2x_2 + I \\ (c_1x_1 + c_2x_2)^2 + I \end{pmatrix} = \underbrace{\begin{pmatrix} 1 & 0 & 0 \\ 0 & c_1 & c_2 \\ 0 & 2c_1c_2 & c_1^2 + c_2^2 \end{pmatrix}}_{M(c_1,c_2)} \begin{pmatrix} 1+I \\ x_1+I \\ x_2+I \end{pmatrix}.$$

$\det(M(c_1, c_2)) = c_1(c_1^2 - c_2^2)$. *Set* $c_1 = 1, c_2 = 2$. *Then*

$$\det(M(1, 2)) = -3 \neq 0.$$

Let $L = x_1 + 2x_2$. *Then*

$$\begin{aligned} L^3 + I &= 4(L^2 + I) - 3(L + I), \\ x_1 + I &= \frac{2}{3}(L^2 + I) - \frac{5}{3}(L + I), \\ x_2 + I &= -\frac{1}{3}(L^2 + I) + \frac{4}{3}(L + I). \end{aligned}$$

Let $g_0(x) = x^3 - 4x^3 + 3x, g_1(x) = 2/3x^2 - 5/3x, g_2(x) = -1/3x^2 + 4/3x$. *Write* $g_0(x) = x(x - 1)(x - 3)$ *and let*

$$\begin{aligned} M_1 &= \langle L, x_1 - g_1(L), x_2 - g_2(L)\rangle = \langle x_1, x_2\rangle, \\ M_2 &= \langle L - 1, x_1 - g_1(L), x_2 - g_2(L)\rangle = \langle x_1 + 1, x_2 - 1\rangle, \\ M_3 &= \langle L - 3, x_1 - g_1(L), x_2 - g_2(L)\rangle = \langle x_1 - 1, x_2 - 1\rangle. \end{aligned}$$

Then $I = M_1 \cap M_2 \cap M_3$.

Chapter 5

Dimensions

5.1 Transcendence degrees

Let $F \subset E$ be two fields. An element$a \in E$ is said to be *algebraic* over F if there exists a nonzero polynomial $f \in F[x]$ such that $f(a) = 0$. We say that a is transcendental over F if a is not algebraic over F. A nonempty subset S of E is said to be algebraically dependent over F if there exists a nonempty and finite subset $\{a_1, \ldots, a_m\} \subset S$ and a nonzero polynomial $f \in F[x_1, \ldots, x_m]$ such that $f(a_1, \ldots, a_m) = 0$. We say that S is algebraically independent over F if it is not algebraically dependent over F.

Let $\mathcal{T}$ be the set of all algebraically independent subsets of E (over F). Then $\mathcal{T}$ has a maximal element. Such an element is called a *transcendence basis* of E over F.

Let A be a set and $\mathcal{P}(A)$ the set of all subsets of A. A function $s : \mathcal{P}(A) \to \mathcal{P}(A)$ is called a *span* if the following conditions hold:

1. for every $B \subset A$, $B \subset s(B)$;
2. if $a \in s(B)$, then there exists a finite subset B' of B such that $a \in s(B')$;
3. if $B' \subset B \subset A$, then $s(B') \subset s(B)$;
4. for every $B \subset A$, $s(s(B)) = s(B)$;
5. if $b \in s(B \cup \{a\})$ and $b \notin s(B)$, where $a, b \in A$ and $B \subset A$, then $a \in s(B \cup \{b\})$.

A subset G of A is said to be a *generating* system of A if $s(G) = A$. A subset H of A is said to be a *free* subset of A if, for every $h \in H$, $h \notin$

$s(H \setminus \{h\})$. A subset B of A is said to be a *basis* of A with respect to s if it is both a free subset and a generating system.

Example 5.1 *Let V be a k-vector space. Define a map $s : \mathcal{P}(V) \to \mathcal{P}(V)$ as the following: for any $S \subset V$, define $s(S)$ as the vector subspace of V spanned by S. Verify that s is a span. What are the bases of V with respect to s?*

Lemma 5.1 *Let B be a subset of A. The following statements are equivalent*

(a) *B is a basis;*

(b) *B is a minimal generating system, i.e. if $C \subset B$ and $s(C) = A$ then $C = B$;*

(c) *B is a maximal free subset of A, i.e. if $B \subset C$ and C is free then $C = B$.*

We order the elements of $\mathcal{P}(A)$ by set inclusion. Then $\mathcal{P}(A)$ becomes a partially ordered set.

Lemma 5.2 (i) *If $\mathcal{T}$ is a totally ordered subset of $\mathcal{P}(A)$ consisting of free subsets of A, then $\cup_{B \in \mathcal{T}} B$ is free.*

(ii) *Assume that H is a free subset of A and $a \in A$. Then $H \cup \{a\}$ is free if and only if $a \notin s(H)$.*

Proof. (i). Let $H = \cup_{B \in \mathcal{T}} B$. If H is not free, then $h \in s(H \setminus \{h\})$ for some $h \in H$. So there exists a finite subset H' of $H \setminus \{h\}$ such that $h \in s(H')$. As $\mathcal{T}$ is totally ordered set, there exists an element B of $\mathcal{T}$ such that B contains H' and h. We have that $h \in s(B \setminus \{h\})$, a contradiction to the freeness of B.

(ii). ($\Leftarrow$) Suppose that $h \in H$. Then $h \notin s(H \setminus \{h\})$, since H is free. If $h \in s((H \setminus \{h\}) \cup \{a\})$, then by the fifth property of span, $a \in s((H \setminus \{h\}) \cup \{h\}) = s(H)$, a contradiction. Thus $h \notin s((H \setminus \{h\}) \cup \{a\})$, which implies that $H \cup \{a\}$ is free. □

Lemma 5.3 *If L is a free subset and G is a generating system of A, then there exists a subset G' of G such that $L \cup S'$ is a basis of A.*

Proof. Let

$$\mathcal{T} = \{S \subset G \,|\, S \cup L \text{ is free}\}.$$

Assume that $\bar{\mathcal{T}}$ is a totally ordered subset of $\mathcal{T}$. Let $T = \cup_{B \in \bar{\mathcal{T}}} B$. We claim that $T \cup L$ is free. Otherwise, there is $a \in T \cup L$ such that $a \in s((T \cup L) \setminus \{a\})$. Then there is a finite set $S' \subset T \cup L$ such that $a \in s((S' \cup L) \setminus \{a\})$. Since $\bar{\mathcal{T}}$ is totally ordered, there is $S \in \bar{\mathcal{T}}$ satisfying $S' \cup L \subset S \cup L$. Then $a \in s((S \cup L) \setminus a)$. This is impossible, because $S \cup L$ is free. This proves our claim. Thus $T \in \mathcal{T}$ and it is an upper bound of $\bar{\mathcal{T}}$. It follows from Zorn's lemma that $\mathcal{T}$ has a maximal element H. We shall show that $L \cup H$ is a basis. It suffices to show that $L \cup H$ is a generating system. Since G is a generating set, it is sufficient to prove that $G \subset s(L \cup H)$. Let g be an element of $G \setminus H$. Then $H \subset H \cup \{g\} \subset G$. So $(H \cup L) \cup \{g\}$ is not free. By Lemma 5.2 (ii), $g \in s(H \cup L)$. □

Proposition 5.4 *Let s be a span function from $\mathcal{P}(A)$ to $\mathcal{P}(A)$. If A has a finite basis B, then for any basis C of A, $|B| = |C|$.*

Proof. Set

$$m = \min_{G \subset A} \{|G| : s(G) = A\},$$

and denote

$$S_m = \left\{\bar{B} \subset A : s(\bar{B}) = A \text{ and } |\bar{B}| = m\right\}.$$

Then by Lemma 5.1, each element of S_m is a basis. We shall show that for any basis C of A there exists $\tilde{B} \in S_m$ such that $\tilde{B} \subset C$. Then by Lemma 5.1 again, $\tilde{B} = C$ and therefore $|C| = m$. Assume that C is a basis of A. Let $\tilde{B}$ be an element in S_m satisfying that

$$|\tilde{B} \cap C| = \max_{\bar{B} \in S_m} |\bar{B} \cap C|.$$

We claim that $\tilde{B} \subset C$. Suppose on the contrary that $\tilde{B} \setminus C \neq \emptyset$. Let $g \in \tilde{B} \setminus C$. Then there is $h \in C$ such that $h \notin s(\tilde{B} \setminus \{g\})$. Otherwise $C \subseteq s(\tilde{B} \setminus \{g\})$ and then $s(\tilde{B} \setminus \{g\}) = A$, a contradiction. Let $\tilde{B}_1 = (\tilde{B} \setminus \{g\}) \cup \{h\}$. Then $|\tilde{B}_1| = |\tilde{B}|$. Moreover since $h \in s(\tilde{B})$ but $h \notin s(\tilde{B} \setminus \{g\})$, $g \in s(\tilde{B}_1)$ by the definition of span. Therefore $s(\tilde{B}_1) = A$. So $\tilde{B}_1 \in S_m$, while $|\tilde{B}_1 \cap C| = |\tilde{B} \cap C| + 1$, a contradiction. This proves the claim. □

We define

$$\begin{aligned} s: \ \mathcal{P}(E) &\to \mathcal{P}(E) \\ U &\mapsto \{a \in E \,|\, a \text{ is algebraic over } F(U)\}. \end{aligned}$$

Clearly, $s(U)$ is a field. The function s satisfies conditions (i), (ii), (iii) and (iv). We now verify that s satisfies condition (v). Let $a \in E$ be transcendental over $F(U)$ but algebraic over $F(U \cup \{b\})$. Let S be the subset $\{a^i b^j \mid i, j \in \mathbf{N}\}$. Then S is linearly dependent over $F(U)$. So there exist $\lambda_{ij} \in F(U)$, not all zero, such that

$$\sum_{i=1}^{m} \sum_{i=1}^{n} \lambda_{ij} a^{m_i} b^{n_j} = 0$$

where $(m_i, n_j) \neq (m_{i'}, n_{j'})$ whenever $(i, j) \neq (i', j')$. It follows that

$$\sum_{j=1}^{n} \underbrace{\left(\sum_{i=1}^{m} \lambda_{ij} a^{m_i} \right)}_{f_j} b^{n_j} = 0.$$

Since a is transcendental over $F(U)$, $f_j \neq 0$ for some j with $1 \leq j \leq n$. We shall call a basis of E with respect to s a transcendence basis of E over F. Assume that E has a finite transcendence basis T. Define $|T|$ to be the transcendence degree of E over F, which is denoted by tr.deg (E/F).

Proposition 5.5 *Let $F \subset E \subset K$ be three fields. If S is a transcendence basis of E over F, and T is a transcendence basis of K over E, then $S \cup T$ is a transcendence basis of K over F. Consequently,*

$$\text{tr.deg } (E/F) + \text{tr.deg } (K/E) = \text{tr.deg } (K/F)$$

if both $|S|$ and $|T|$ are finite.

Proof. It is clear that $S \cup T$ is algebraically independent over F. It remains to show that every element of K is algebraic over $F(S \cup T)$. Assume $a \in K$. Then a is algebraic over $E(T)$. So there exist $f_0, \ldots, f_m \in E[T]$, not all zero, such that

$$f_m a^m + \cdots + f_1 a + f_0 = 0.$$

Let C be the set of all nonzero coefficients of the f_i, viewed as polynomials in $E[T]$. Then C is a nonempty and finite subset of E whose elements are all algebraic over $F(S)$. Consider the tower:

$$F(S \cup T) \subset F(S \cup T)(C) \subset F(S \cup T)(C, a).$$

We have that the dimension of $F(S \cup T)(C)$ over $F(S \cup T)$ is finite, and the dimension of $F(S \cup T)(C, a)$ over $F(S \cup T)(C)$ is finite. It follows from the telescoping formula that the dimension of $F(S \cup T)(C, a)$ over $F(S \cup T)$ is finite. So a is algebraic over $F(S \cup T)$. □

5.2 Dimensions

Let I be a proper ideal of $k[\mathbf{x}]$.

Definition 5.1 *A subset* $\mathbf{y}$ *of* $\mathbf{x}$ *is said to be* independent *modulo* I *if* $k[\mathbf{y}] \cap I = \{0\}$. *The dimension of* I, *denoted* $\dim(I)$, *is defined to be*

$$\max\{|\mathbf{y}| \,|\, \mathbf{y} \text{ is independent modulo } I\}.$$

Example 5.2 *Let* I *be an ideal of* $k[x]$. *Then there exists an independent and nonempty subset modulo* I *if and only if* $I = \{0\}$.

Let $n = 2$ *and* $I = \langle x_1^2 + x_2^2 + 1\rangle$. *The independent subsets modulo* I *are* $\emptyset, \{x_1\}, \{x_2\}$. *So* $\dim(I) = 1$.

Let $n = 3$ *and* $I = \langle x_1x_3 + x_3, x_2x_3 + x_3\rangle$. *Since the generators form a GB with respect to any graded monomial order, we have that the independent subsets modulo* I *are*

$$\emptyset,\ \{x_1\}, \{x_2\}, \{x_3\}, \{x_1, x_2\}.$$

So $\dim(I) = 2$.

Proposition 5.6 *Let* I *be a proper ideal of* $k[\mathbf{x}]$.

1. *If* I *is a zero-dimensional ideal, then* $\dim(I) = 0$.
2. *If* $I = \langle f\rangle$ *with* $f \neq 0$, *then* $\dim(I) = n - 1$.
3. *If* I *is prime, then* $\dim(I) = \text{tr.deg } (F/k)$ *where* F *is the quotient field of* $k[\mathbf{x}]/I$.
4. $\dim(I) = \dim(\sqrt{I})$.

Proof. Assume that I is zero-dimensional. Then $k[x_i] \cap I \neq \{0\}$ for all i with $1 \leq i \leq n$. Therefore, $\emptyset$ is the only independent set modulo I. Hence, $\dim(I) = 0$.

Assume that $I = \langle f\rangle$. W.l.o.g., we may further assume that $\deg_{x_1}(f) > 0$. Then $k[x_2, \ldots, x_n] \cap I = \{0\}$. So $\dim(I) = n - 1$.

Assume that I is prime. In $k[\mathbf{x}]/I$, write $\bar{x}_i$ for $x_i + I$. Then $F = k(\bar{x}_1, \cdots, \bar{x}_n)$. By Lemma 5.3 there exists a subset $\mathbf{y} = \{y_1, \ldots, y_m\}$ of $\mathbf{x}$ such that $\bar{y}_1, \ldots, \bar{y}_m$ form a transcendence basis of F over k. It follows that $k[\mathbf{y}] \cap I = \{0\}$. So $\dim(I) \geq m$. Assume that $\mathbf{z}$ is an independent set

modulo I. Then $\{\bar{z} \mid z \in \mathbf{z}\}$ is algebraically independent over k. So $|\mathbf{z}| \leq m$, because tr.deg $(F/k) = m$. Consequently, $\dim(I) \leq m$.

Since $I \subset \sqrt{I}$, $\dim(\sqrt{I}) \leq \dim(I)$. Suppose that $\mathbf{y}$ is independent modulo I and that $f \in k[\mathbf{y}] \cap \sqrt{I}$. Then $f^m \in k[\mathbf{y}] \cap I$ for some $m \in \mathbf{N}$. So $f = 0$, that is, $\mathbf{y}$ is independent modulo $\sqrt{I}$. Hence, $\dim(I) \leq \dim(\sqrt{I})$. □

Let V be an algebraic variety. Then the dimension of V is defined to be $\dim(\mathbf{I}(V))$, which is also denoted by $\dim(V)$.

Proposition 5.7 *Let I and J be two ideals of $k[\mathbf{x}]$. If $I \subseteq J$, then* $\dim(J) \leq \dim(I)$.

Proof. It follows from the definition of dimension. □

Proposition 5.8 *If I and J are two ideals, then*

$$\dim(I \cap J) = \max\{\dim(I), \dim(J)\}.$$

Proof. It follows from Proposition 5.7 that

$$\dim(I \cap J) \geq \max\{\dim(I), \dim(J)\}.$$

It remains to show that the former one is not greater than the latter one. Assume that $\dim(I \cap J) = d$. Then there is a subset $\mathbf{y}$ of $\mathbf{x}$ with $|\mathbf{y}| = d$ such that $k[\mathbf{y}] \cap (I \cap J) = \{0\}$. Then one has $k[\mathbf{y}] \cap I = \{0\}$ or $k[\mathbf{y}] \cap J = \{0\}$. Otherwise, let $f \in k[\mathbf{y}] \cap I$ and $g \in k[\mathbf{y}] \cap J$ where $fg \neq 0$. Then $fg \in k[\mathbf{y}] \cap (I \cap J)$, a contradiction. Without loss of generality, assume that $k[\mathbf{y}] \cap I = \{0\}$. Then $\dim(I) \geq d$. Hence $\max\{\dim(I), \dim(J)\} \geq d$. □

Corollary 5.9 *Let I be a radical ideal and $I = P_1 \cap \cdots \cap P_m$, where the P_i are prime ideals. Then*

$$\dim(I) = \max_{1 \leq i \leq m} \dim(P_i).$$

Proposition 5.10 *Let P be a prime ideal and f be a polynomial not in P. If $P + \langle f \rangle \neq k[\mathbf{x}]$, then*

$$\dim(P + \langle f \rangle) < \dim(P).$$

Proof. It follows from Proposition 5.7 that $\dim(P + \langle f \rangle) \leq \dim(P)$. Suppose that $\dim(P + \langle f \rangle) = \dim(P)$ and $d = \dim(P + \langle f \rangle)$. Then there is a subset $\mathbf{y} = \{y_1, \ldots, y_d\}$ of $\mathbf{x}$ such that $k[\mathbf{y}] \cap (P + \langle f \rangle) = \{0\}$. Denote by F the

quotient field of $k[\mathbf{x}]/P$. Then $y_1 + P, \ldots, y_d + P$ is a transcendence basis of F over k. Hence $f + P, y_1 + P, \ldots, y_d + P$ are algebraically dependent over k, i.e. there are polynomials $g_0, \ldots, g_m \in k[\mathbf{y}]$, not all zero, such that

$$(g_m + P)(f + P)^m + \ldots + (g_1 + P)(f + P) + g_0 + P = 0. \tag{5.1}$$

Without loss of generality, we may assume that m is a minimal positive integer such that (5.1) holds. Then $g_0 + P \neq 0$, since $f + P \neq 0$. Note that $g_0 \in k[\mathbf{y}]$. The equality (5.1) implies that $g_0 \in P + \langle f \rangle$, a contradiction to the assumption that $k[\mathbf{y}] \cap (P + \langle f \rangle) = \{0\}$. So $\dim(P + \langle f \rangle) < \dim(P)$. □

Corollary 5.11 *Let P be a prime ideal and Q be an ideal. If P is a proper subset of Q, then* $\dim(Q) < \dim(P)$.

Proof. Let $f \in Q \setminus P$. Then

$$\dim(Q) \leq \dim(P + \langle f \rangle) < \dim(P).$$

□

In the following, all prime ideals are supposed to be proper. We call the sequence

$$P_0 \subsetneqq P_1 \subsetneqq \cdots \subsetneqq P_d$$

where P_i is a prime ideal, a **chain of prime ideals** and d is said to be the **length** of this chain.

Krull dimension: The krull-dimension of a ring R, written $\mathrm{kdim}(R)$, is the supremum of the lengths of chains of prime ideals. Let I be a proper ideal of R. We define the Krull-dimension of I, written $\mathrm{kdim}(I)$, to be $\mathrm{kdim}(R/I)$.

Example 5.3 (1) $\mathrm{kdim}(k[\mathbf{x}]) = n$.

(2) *Let $I = (0)$. Then* $\mathrm{kdim}(I) = n$.

Let I be a proper ideal of $k[\mathbf{x}]$. We shall show $\dim(I) = \mathrm{kdim}(I)$. In this section, we first show that $\dim(I) \geq \mathrm{kdim}(I)$. The inequality $\dim(I) \leq \mathrm{kdim}(I)$ will be proved next chapter.

Lemma 5.12 *Let I be a proper ideal of $k[\mathbf{x}]$. Then* $\mathrm{kdim}(I)$ *is the supremum of the lengths of chains of proper prime ideals which containing I.*

Proposition 5.13 *Let I be a proper ideal of $k[\mathbf{x}]$. Then* $\dim(I) \geq \mathrm{kdim}(I)$.

Proof. Let

$$I \subset P_0 \subsetneqq P_1 \subsetneqq \cdots \subsetneqq P_d$$

be a chain of prime ideals containing I. Due to Proposition 5.7 and Corollary 5.11, we have

$$\dim(I) \geq \dim(P_0) > \dim(P_1) > \cdots > \dim(P_d) \geq 0.$$

Thus $\dim(I) \geq d$. Hence $\dim(I) \geq \mathrm{kdim}(I)$. □

5.3 The Hilbert function

Denote $k[\mathbf{x}]$ by R. For a subset S of $k[\mathbf{x}]$, $S^{\leq m}$ denotes

$$\{f \in S \mid \deg(f) \leq m\},$$

where $\deg(f)$ stands for the total degree of f.

For an ideal I of R, $I^{\leq m}$ is a linear subspace over k. Since $I^{\leq m} \subset R^{\leq m}$, which is a finite-dimensional vector space, $I^{\leq m}$ is also a finite-dimensional vector space. Define

$$\begin{array}{rccc} HF_I & \mathbf{N} & \to & \mathbf{N} \\ & m & \mapsto & \dim_k(R^{\leq m}/I^{\leq m}), \end{array}$$

which is called the *Hilbert function* of I.

We will show that $HF_I(m)$ is a polynomial in m of degree $\dim(I)$ for sufficiently large m.

For a subset $\mathbf{y} \subset \mathbf{x}$, $[\mathbf{y}]$ stands for all the monomials in $\mathbf{y}$. By convention, $[\emptyset] = \{1\}$.

Lemma 5.14 $\dim_k(R^{\leq m}) = \binom{m+n}{n}$.

Proof. It suffices to show that $|[\mathbf{x}]^{\leq m}| = \binom{m+n}{n}$. We compute

$$\begin{array}{rcl} x_1^{\alpha_1} \cdots x_n^{\alpha_n} \in [\mathbf{x}]^{\leq m} & \Leftrightarrow & \alpha_1 + \cdots + \alpha_n \leq m \\ & \Leftrightarrow & \exists\ \alpha_0 \in \mathbf{N},\ \alpha_0 + \alpha_1 + \cdots + \alpha_n = m \\ & \Leftrightarrow & \exists\ \alpha_0 \in \mathbf{N},\ (\alpha_0 + 1) + (\alpha_1 + 1) + \cdots + (\alpha_n + 1) = m + n + 1. \end{array}$$

Hence, $|[\mathbf{x}]^{\leq m}|$ equals the number of positive integer solutions of the equation

$$z_0 + z_1 + \cdots + z_n = n + m + 1,$$

which is $\binom{m+n}{n}$. □

Example 5.4 *Let $f \in k[x]$ be of degree $d > 0$, and $I = \langle f \rangle$. We have*

$$\dim_k(R^{\leq m}) = m + 1 \quad \text{and} \quad \dim_k(I^{\leq m}) = \begin{cases} 0, & m < d \\ m - d + 1, & m \geq d. \end{cases}$$

So

$$HF_I(m) = \begin{cases} m + 1, & m < d \\ d, & m \geq d. \end{cases}$$

Example 5.5 *Let $I = \langle x_1^2 + x_2^2 - 1 \rangle$. We have*

$$\dim_k(R^{\leq m}) = \binom{m+2}{2}.$$

Note that $I^{\leq m} = \{0\}$ for $m = 0, 1$ and

$$I^{\leq m} = \{(x_1^2 + x_2^2 - 1)g \,|\, g \in R^{\leq m-2}\}.$$

So $\dim_k(I^{\leq m}) = \binom{m}{2}$ if $m \geq 2$. It follows that

$$HF_I(m) = \begin{cases} 1, & m = 0 \\ 3, & m = 1 \\ \binom{m+2}{2} - \binom{m}{2} = 2m + 1, & m \geq 2. \end{cases}$$

Let I be a proper ideal of R, and G be a Gröbner basis with respect to a total degree order. In the following, we use M_G to denote the set of monomials that are not multiples of any element in $\mathrm{lm}(G)$.

Proposition 5.15 *The set*

$$B_m = \{u + I^{\leq m} \,|\, u \in M_G^{\leq m}\}$$

is a k-basis of $R^{\leq m}/I^{\leq m}$. In the sequel, $HF_I(m) = |B_m| = |M_G^{\leq m}|$.

Proof. First, we show that B_m is linearly independent over k. Assume that

$$\sum_{u \in M_G^{(m)}} \lambda_u (u + I^{\leq m}) = 0$$

for some $\lambda_u \in k$. Let $f = \sum_{u \in M_G^{\leq m}} \lambda_u u$. Then $f \in I^{\leq m}$, and, hence, $f \in I$. Because none of the elements in $M_G^{\leq m}$ is a multiple of any element in $\mathrm{lm}(G)$,

f is reduced with respect to G. Hence $f = 0$ by Theorem 3.8, i.e. $\lambda_u = 0$ for all $u \in M_G^{\leq m}$.

Next, we show that $R^{\leq m}$ is spanned by elements of $M_G^{\leq m}$ and $I^{\leq m}$ as a vector space. Denote by L the vector space spanned by elements of $M_G^{\leq m}$ and $I^{\leq m}$. Suppose that $R^{\leq m} \setminus L \neq \emptyset$. Then $[\mathbf{x}]^{\leq m} \setminus L \neq \emptyset$. Let w be an element in $[\mathbf{x}]^{\leq m} \setminus L$ with lowest order. Then w is a multiply of some element of $\mathrm{lm}(G)$, otherwise $w \in M_G^{\leq m}$. Hence there is $g \in G$ such that $w = v\mathrm{lm}(g)$. It is evident that $\deg(vg) \leq m$ and then $vg \in I^{\leq m}$. Let $\bar{g} = \mathrm{lc}(g)w - vg$. Then the orders of monomials in $\bar{g}$ are lower than w, which implies that these monomials are in L. Hence $w \in L$, a contradiction. □

Example 5.6 *Let I be the ideal generated by $x_1x_3+x_3$ and $x_2x_3+x_3$. These two generators form a Gröbner basis with respect to any grade order. The set $M_G = [x_1, x_2] \cup [x_3]$. So*

$$M_G^{\leq m} = [x_1, x_2]^{\leq m} \cup [x_3]^{\leq m}.$$

It follows that

$$|M_G^{\leq m}| = \binom{m+2}{2} + \binom{m+1}{1} - 1 = \frac{1}{2}m^2 + \frac{5}{2}m + 1 = HF_I(m).$$

Corollary 5.16 *Let I be a proper ideal of R.*

1. *If $\dim(I) = 0$, then $HF_I(m) = \dim_k(R/I)$ for $m >> 0$.*
2. *If $\dim(I) = d$, then $HF_I(m) \geq \binom{m+d}{d}$.*

Proof. Let G be a Gröbner basis of I with respect to a total degree order, and

$$M_G = \{u_1, \ldots, u_\ell\}$$

be the set of monomials not divisible by any element of $\mathrm{lm}(G)$. Then

$$\dim_k(R/I) = \ell.$$

Let

$$D = \max\{\deg(u_1), \ldots, \deg(u_\ell)\}.$$

For all m with $m \geq D$, $\dim_k(R^{\leq m}/I^{\leq m}) = \ell$. The first assertion holds.

Let $\mathbf{y} \subset \mathbf{x}$ be an independent set modulo I with $|\mathbf{y}| = d$. Then

$$\{y + I^{\leq m} \mid y \in [\mathbf{y}]^{\leq m}\}$$

is k-linearly independent. So $HF_I(m) \geq |[\mathbf{y}]^{\leq m}| = \binom{m+d}{d}$. □

5.4 Translates

To understand HF_I, we need to study $M_{\overline{G}}^{\leq m}$.

For $u \in [\mathbf{x}]$ and, $\mathbf{y} \subset \mathbf{x}$, define

$$u[\mathbf{y}] := \{uv \mid v \in [\mathbf{y}]\}.$$

Such a set of monomials is called a *translate* (of $[\mathbf{y}]$) if $u \in [\mathbf{x} \setminus \mathbf{y}]$, that is, u is free of any element of $\mathbf{y}$. By convention, $u[\emptyset] = u$ is also called a translate, moreover, $\emptyset$ is called the trivial translate.

Example 5.7 *Let* $\mathbf{x} = \{x_1, x_2\}$ *and* $\mathbf{y} = \{x_2\}$. *Then*

$$x_1^2[x_2] = \{u \in [\mathbf{x}] \mid \deg_{x_1}(u) = 2\},$$

which is a translate. But

$$x_1x_2[x_2] = \{u \in [\mathbf{x}] \mid \deg_{x_1}(u) = 1, \deg_{x_2}(u) \geq 1\}$$

is not.

Let $T = u[\mathbf{y}]$. Define

$$\operatorname{ord}(T) = \deg(u) \quad \text{and} \quad \operatorname{len}(T) = |\mathbf{y}|.$$

If $T = \emptyset$, we define $\operatorname{len}(T) = -\infty$.

Lemma 5.17 *Let* $T_1 = u_1[\mathbf{y}_1]$ *and* $T_2 = u_2[\mathbf{y}_2]$ *be two nontrivial translates. If* $T_1 \cap T_2 \neq \emptyset$, *then*

$$T_1 \cap T_2 = \operatorname{lcm}(u_1, u_2)[\mathbf{y}_1 \cap \mathbf{y}_2].$$

Moreover,if $T_1 \neq T_2$, *then* $\operatorname{len}(T_1 \cap T_2) < \max(\operatorname{len}(T_1), \operatorname{len}(T_2))$.

Proof. We first show that $\operatorname{lcm}(u_1, u_2) \in T_1 \cap T_2$. Since $T_1 \cap T_2 \neq \emptyset$, there are $v_1 \in [\mathbf{y}_1]$ and $v_2 \in [\mathbf{y}_2]$ such that $u_1v_1 = u_2v_2$. Then $\operatorname{lcm}(u_1, u_2) | u_1v_1$ and $\operatorname{lcm}(u_1, u_2) | u_2v_2$. One easily sees that $\operatorname{lcm}(u_1, u_2) \in T_1 \cap T_2$. Now suppose that $w \in T_1 \cap T_2$. Then one has $\operatorname{lcm}(u_1, u_2) | w$. Denote $\bar{w} = w/\operatorname{lcm}(u_1, u_2)$. We have $\bar{w} \in [\mathbf{y}_1] \cap [\mathbf{y}_2] = [\mathbf{y}_1 \cap \mathbf{y}_2]$. Therefore

$$w = \operatorname{lcm}(u_1, u_2)\bar{w} \in \operatorname{lcm}(u_1, u_2)[\mathbf{y}_1 \cap \mathbf{y}_2].$$

An easy calculation implies that $\operatorname{lcm}(u_1, u_2)[\mathbf{y}_1 \cap \mathbf{y}_2] \subset T_1 \cap T_2$.

If $T_1 \cap T_2 = \emptyset$, it is obvious. In the following, assume that $T_1 \cap T_2 \neq \emptyset$. Suppose that $\text{len}(T_1 \cap T_2) = \max\{\text{len}(T_1), \text{len}(T_2)\}$, i.e. $|\mathbf{y}_1 \cap \mathbf{y}_2| = \max(|\mathbf{y}_1|, |\mathbf{y}_2|)$. Then $\mathbf{y}_1 = \mathbf{y}_2$. Since both u_1 and u_2 are in $[\mathbf{x} \setminus \mathbf{y}_1]$, $\text{lcm}(u_1, u_2) \in [\mathbf{x} \setminus \mathbf{y}_1]$. On the other hand, $\text{lcm}(u_1, u_2) = u_1\bar{v_1} = u_2\bar{v_2}$ where $\bar{v_1}, \bar{v_2} \in [\mathbf{y}_1]$. Therefore $\bar{v_1} = \bar{v_2} = 1$. Thus $u_1 = u_2$, and, consequently, $T_1 = T_2$. □

Corollary 5.18 *The intersection of two translates is again a translate.*

Proof. Suppose that $T_1 = u_1[\mathbf{y}_1], T_2 = u_2[\mathbf{y}_2]$ are two translates. If $T_1 \cap T_2 = \emptyset$, by the definition, $T_1 \cap T_2$ is a translate. Suppose that $T_1 \cap T_2 \neq \emptyset$. Then by Lemma 5.17, $T_1 \cap T_2 = \text{lcm}(u_1, u_2)[\mathbf{y}_1 \cap \mathbf{y}_2]$. It suffices to show that $\text{lcm}(u_1, u_2) \in [\mathbf{x} \setminus (\mathbf{y}_1 \cap \mathbf{y}_2)]$. Note that $u_1 \in [\mathbf{x} \setminus \mathbf{y}_1] \subset [\mathbf{x} \setminus (\mathbf{y}_1 \cap \mathbf{y}_2)]$ and $u_2 \in [\mathbf{x} \setminus \mathbf{y}_2] \subset [\mathbf{x} \setminus (\mathbf{y}_1 \cap \mathbf{y}_2)]$. Hence $\text{lcm}(u_1, u_2) \in [\mathbf{x} \setminus (\mathbf{y}_1 \cap \mathbf{y}_2)]$. □

Proposition 5.19 *Let I be a proper ideal and G be a Gröbner basis of I with respect to a given grade order. Assume that $\text{lm}(G) = \{u_1, \ldots, u_l\}$. Let*

$$D = \max_{1 \leq i \leq n, 1 \leq j \leq l} \deg_{x_i}(u_j).$$

Then there exist finitely many translates $T_1, \ldots, T_s$ such that

$$M_G = T_1 \cup \cdots \cup T_s$$

with $\text{ord}(T_i) \leq n(D-1)$ for all i with $1 \leq i \leq s$.

Proof. Let S_i be the set of monomials not divisible by u_i. Then

$$S_i = \{u \in [\mathbf{x}] \mid \deg_x(u) < \deg_x(u_i) \text{ for some } x \in \mathbf{x}.\}.$$

So

$$\begin{aligned} S_i &= \cup_{j=1}^{n} \{u \in [\mathbf{x}] \mid \deg_{x_j}(u) < \deg_{x_j}(u_i)\} \\ &= \cup_{j=1}^{n} \cup_{d=1}^{\deg_{x_j}(u_i)-1} \{u \in [\mathbf{x}] \mid \deg_{x_j}(u) = d\} \\ &= \cup_{j=1}^{n} \cup_{d=1}^{\deg_{x_j}(u_i)-1} x_j^d[\mathbf{x} \setminus \{x_j\}]. \end{aligned}$$

So each S_i is a finite union of translates whose order is less than D. Since

$$M_G = S_1 \cap \cdots \cap S_l,$$

it is a finite union of translates by Corollary 5.18. These translates are of order less than or equal to $n(D-1)$ by Lemma 5.17. □

5.5 The Hilbert polynomial

Lemma 5.20 *Let T be a nontrivial translate. If $m \geq \mathrm{ord}(T)$, then*

$$\left|T^{\leq m}\right| = \binom{m - \mathrm{ord}(T) + \mathrm{len}(T)}{\mathrm{len}(T)}.$$

Proof. Let $T = u[\mathbf{x}]$ and $\mathrm{ord}(T) = l$. For $m \geq l$,

$$T^{\leq m} = \{uv \,|\, v \in [\mathbf{y}]^{\leq m-l}\}.$$

Hence

$$\left|T^{\leq m}\right| = \binom{|\mathbf{y}| + m - l}{|\mathbf{y}|}.$$

The proof is completed. □

Theorem 5.21 *Let I be a proper ideal. Then $HF_I(m) = h(m)$ for $m >> 0$. Moreover, $\deg(h) = \dim(I)$ and $\mathrm{lc}(h) > 0$. (We call h the Hilbert polynomial of I and denote it by HP_I.)*

Proof. Let G a Gröbner basis of I with respect to a given total degree order. Assume that $\mathrm{lm}(G) = \{u_1, \ldots, u_l\}$. Put

$$D = \max_{1 \leq i \leq n, 1 \leq j \leq l} \deg_{x_i}(u_j).$$

By Proposition 5.19, there are nontrivial translates $T_1, \ldots, T_s$ with $\mathrm{ord}(T_i) \leq n(D-1)$ such that $M_G = T_1 \cup \cdots \cup T_s$. Then

$$M_G^{\leq m} = T_1^{\leq m} \cup \cdots \cup T_s^{\leq m}.$$

So

$$\begin{aligned} \left|M_G^{\leq m}\right| &= |T_1^{\leq m} \cup \cdots \cup T_s^{\leq m}| \\ &= \textstyle\sum_{i=1}^{s} |T_i^{\leq m}| - \sum_{1 \leq i < j \leq s} |T_i^{\leq m} \cap T_j^{\leq m}| + \cdots \\ &\quad + (-1)^{s-1} |T_1^{\leq m} \cap \cdots \cap T_s^{\leq m}|. \end{aligned}$$

By Lemma 5.20, for $m \geq n(D-1)$, $|T_i^{\leq m}|$ is a polynomial in m of degree $\mathrm{len}(T_i)$ in $\mathbf{Q}[m]$. Moreover, $|T_i^{\leq m}|$ has a positive leading coefficient. Thus, $\sum_{i=1}^{s} |T_i^{\leq m}|$ is a polynomial in m whose degree is the maximal length of the T_i's, which we denote by d. Note that

$$|T_{i_1}^{\leq m} \cap T_{i_2}^{\leq m} \cap \cdots \cap T_{i_l}^{\leq m}|,$$

where $l > 1$ and $i_1 < i_2 < \cdots < i_l$, is a polynomial in m whose degree is less than d. So $|M_G^{\leq m}|$ is a polynomial in m of degree d. We have proved that $HF_I(m)$ is a polynomial of degree d and has a positive coefficient.

It remains to show that $d = \dim(I)$. By Corollary 5.16, $HF_I(m) \geq \binom{m+\dim(I)}{\dim(I)}$, which is a polynomial in m of degree $\dim(I)$. Hence $d \geq \dim(I)$. Suppose that $T_i = v_i[\mathbf{y}_i]$ for all $1 \leq i \leq s$. Then $\mathbf{y}_i$ is an independent set modulo I. So $\text{len}(\mathbf{y}_i) \leq \dim(I)$. Consequently,

$$d = \max_{1 \leq i \leq s} \{\text{len}(\mathbf{y}_i)\} \leq \dim(I).$$

□

Corollary 5.22 *Let I be a proper ideal and G be a Gröbner basis of I with respect to a given graded order. If*

$$M_G = T_1 \cup \cdots \cup T_l,$$

where $T_1, \ldots, T_l$ are translates. then

$$\dim(I) = \max_{1 \leq i \leq l} \{\text{len}(T_i)\}.$$

Exercises for Chapter 6

1. Let I be a proper ideal of $k[\mathbf{x}]$ and G be a Gröbner basis of I with respect to a grade order. Prove that

   $$\dim_k(I^{\leq m}) = \dim_k(\langle \text{lm}(G) \rangle^{\leq m})$$

   for all $m \in \mathbf{N}$. Give an example to show that the above assertion may not be true if the order is not grade.

Chapter 6

Affine Dimension Theorem

Throughout this chapter, all rings are commutative ring with unitary.

6.1 Noether's normalization lemma

Let A and B be two rings. An element $b \in B$ is said to be *integral* over A if there exists a monic polynomial $f \in A[z]$ such that $f(b) = 0$. The ring B is said to be integral over A if all elements of B are integral over A.

Example 6.1 *Let $A = \mathbf{Z}$ and $B = \mathbf{R}$. Then $\sqrt{2}$ is integral over $\mathbf{Z}$, but $\sqrt{\frac{1}{2}}$ is not integral over $\mathbf{Z}$.*

Lemma 6.1 *Let $A \subset B$ be two rings. If $u, v \in B$ are integral over A, so are $u + v$ and uv.*

Proof. Assume that $f, g \in A[x]$ be monic such that $f(u) = g(v) = 0$. Write

$$f = x^m + f_{m-1}x^{m-1} + \cdots + f_0 \quad \text{and} \quad g = x^l + g_{l-1}x^{l-1} + \cdots + g_0.$$

Let $\mathbf{v}$ be the vector consisting of $u^i v^j$ where $0 \leq i \leq m-1, 0 \leq j \leq l-1$. Then there exists a matrix $M \in \mathrm{Mat}_\nu(A)$ where $\nu = lm$ such that

$$(u+v)\mathbf{v} = M\mathbf{v}, \text{ i.e. } ((u+v)I_\nu - A)\mathbf{v} = 0.$$

Let $f(x) = \det(xI_\nu - M)$. Then $f(u+v)\mathbf{v} = 0$. Thus $f(u+v) = 0$. Note that $f(x)$ is a monic polynomial in $A[x]$. So $u+v$ is integral over A. By the similar argument, one can show that uv is integral over A too. □

Proposition 6.2 *Let $A \subset B \subset C$ be three rings. If B is integral over A, and C is integral over B, then C is integral over A.*

Proof. Let $c \in C$ be integral over B. Then there exist $m \in \mathbf{Z}^+$ and $b_{m-1}, \ldots, b_0 \in B$ such that c is a root of

$$x^m + b_{m-1}x^{m-1} + \cdots + b_0.$$

Since b_j is integral over A, there is a monic polynomial $g_j \in A[x]$ such that $g_j(b_j) = 0$. Let $d_j = \deg(g_j)$. Let $\mathbf{v}$ be the vector consisting of $c^j b_0^{i_1} \cdots b_{m-1}^{i_{m-1}}$ where $0 \leq j \leq m-1, 0 \leq i_j \leq d_j$. Then

$$c\mathbf{v} = M\mathbf{v}$$

where M is a matrix in $\mathrm{Mat}_\nu(A)$ with $\nu = md_0 \cdots d_{m-1}$. The argument similar to that in the proof of Lemma 6.1 implies that c is integral over A. □

Let R be a finitely generated k-algebra and S be a nonempty subset of R. We say S is algebraically dependent over k if there exists a nonempty and finite subset $\{a_1, \ldots, a_m\} \subset S$ and a nonzero polynomial $f \in k[y_1, \ldots, y_m]$ such that $f(a_1, \ldots, a_m) = 0$. We say that S is algebraically independent over k if it is not algebraically dependent over k.

Theorem 6.3 *Let R be a finitely generated k-algebra. Then there are $a_1, \ldots, a_d \in R$ such that*

1. *$a_1, \ldots, a_d$ are algebraically independent over k;*
2. *R is integral over $k[a_1, \ldots, a_d]$.*

Proof. Assume that $R = k[\bar{x}_1, \cdots, \bar{x}_n]$. We shall show the theorem by induction on n. Assume $n = 1$. If $\bar{x}_1$ is transcendental over k, then there is nothing to prove. If $\bar{x}_1$ is algebraic over k, it it is clear that R is integral over k. Now assume that the theorem holds for $n-1$. If $\bar{x}_1, \cdots, \bar{x}_n$ are algebraically independent over k, there is nothing to prove. Assume that $\bar{x}_1, \cdots, \bar{x}_n$ are algebraically dependent over k. Then there is $f \in k[\mathbf{x}] \setminus \{0\}$ such that $f(\bar{x}_1, \cdots, \bar{x}_n) = 0$. Let ω be a Weierstrass automorphism of $k[\mathbf{x}]$ with respect to x_n such that

$$\omega(f) = cx_n^m + A_{m-1}x_n^{m-1} + \cdots + A_0$$

where $m > 0, A_i \in k[x_1, \cdots, x_{n-1}]$ and $c \in k \setminus \{0\}$. Suppose that for each $i = 1, \cdots, n-1$, $\omega(x_i) = x_i + x_n^{d_i}$ where $d_i \in \mathbf{N}$. Let $\bar{y}_i = \bar{x}_i - \bar{x}_n^{d_i}$ for all $i = 1, \cdots, n-1$ and $\bar{y}_n = \bar{x}_n$. Then

$$\omega(x_i)|_{x_1=\bar{y}_1,\cdots,x_n=\bar{y}_n} = (x_i + x_n^{d_i})|_{x_i=\bar{y}_i, x_n=\bar{y}_n} = \bar{x}_i$$

for all $i = 1, \cdots, n$. Therefore one has

$$\begin{aligned}\omega(f)|_{x_1=\bar{y}_1,\cdots,x_n=\bar{y}_n} &= c\bar{y}_n^m + A_{m-1}(\bar{y}_1, \cdots, \bar{y}_{n-1})\bar{y}_n^{m-1} + \cdots + A_0(\bar{y}_1, \cdots, \bar{y}_{n-1}) \\ &= f(\bar{x}_1, \cdots, \bar{x}_n) = 0.\end{aligned}$$

In other words, $\bar{y}_n$ is integral over $k[\bar{y}_1, \cdots, \bar{y}_{n-1}]$. By induction hypothesis, there are $b_1, \cdots, b_d \in k[\bar{y}_1, \cdots, \bar{y}_{n-1}]$ such that $b_1, \cdots, b_d$ are algebraically independent over k and $k[\bar{y}_1, \cdots, \bar{y}_{n-1}]$ is integral over $k[b_1, \cdots, b_d]$. Due to Proposition 6.2, $k[\bar{y}_1, \cdots, \bar{y}_n]$ is integral over $k[b_1, \cdots, b_d]$. Then the theorem follows from the fact

$$R = k[\bar{x}_1, \cdots, \bar{x}_n] = k[\bar{y}_1, \cdots, \bar{y}_n].$$

□

We call $k[b_1, \ldots, b_d]$ a Noether's normalization of R.

Example 6.2 *Let $R = k[x_1, x_2]$ and $I = \langle x_1x_2 - 1\rangle$. Then*

$$\bar{x}_1^2 - (\bar{x}_1 + \bar{x}_2)\bar{x}_1 + 1 = 0 \quad \text{and} \quad \bar{x}_2^2 - (\bar{x}_1 + \bar{x}_2)\bar{x}_2 + 1 = 0.$$

Hence $k[\bar{x}_1 + \bar{x}_2]$ is a Noether's normalization of $k[\bar{x}_1, \bar{x}_2]$.

Proposition 6.4 *Let I be a proper ideal of $k[\mathbf{x}]$. If $k[b_1, \ldots, b_d]$ is a Noether's normalization of $k[\mathbf{x}]/I$. then $d = \dim(I)$.*

Proof. We first show that for any proper prime ideal P containing I, $\dim(P) \leq d$. For each $i = 1, \cdots, d$, let $z_i \in k[\mathbf{x}]$ satisfying $b_i = z_i + I$. Assume $a \in k[\mathbf{x}] \setminus P$. Since $a + I$ is integral over $k[b_1, \cdots, b_d]$, there is $f \in k[y_0, y_1, \cdots, y_d] \setminus \{0\}$ which is monic in y_0 such that

$$f(a + I, b_1 + I, \cdots, b_d + I) = 0.$$

In other words, $f(a, z_1, \cdots, z_d) \in I \subset P$. Hence

$$f(a + P, z_1 + P, \cdots, z_d + P) = 0,$$

which implies that $a+P$ is algebraic over $k(z_1+P, \cdots, z_d+P)$ for f is monic in y_0. Hence $\mathrm{tr.deg}(F/k) \leq d$ where F is the quotient field of $k[\mathbf{x}]/P$. So $\dim(P) \leq d$.

Next, we show that there is a proper prime ideal containing I whose dimension equals d. Let $\sqrt{I} = Q_1 \cap Q_2 \cap \cdots \cap Q_l$ be the minimal irreducible decomposition of $\sqrt{I}$. Suppose that for each $i = 1, \cdots, l$, $z_1+Q_i, \cdots, z_d+Q_i$ are algebraically dependent over k. Then for each $i = 1, \cdots, l$, there is $g_i \in k[y_1, \cdots, y_d]$ such that $g_i(z_1 + Q_i, \cdots, z_d + Q_i) = 0$, i.e. $g_i(z_1, \cdots, z_d) \in Q_i$. Therefore

$$h = \prod_{i=1}^{l} g_i(z_1, \cdots, z_d) \in \sqrt{I}.$$

So $h^m(z_1, \cdots, z_d) \in I$ for some $m \in \mathbf{N}$. In the sequel, $z_1 + I, \cdots, z_d + I$ are algebraically dependent over k, a contradiction. Hence there is $i_0 \in \{1, \cdots, l\}$ such that $z_1 + Q_{i_0}, \cdots, z_d + Q_{i_0}$ are algebraically independent over k. So $\dim(Q_{i_0}) = d$. □

6.2 Norms

Let F and E be two fields such that $[E : F] < +\infty$. Assume that $a \in E$. Then

$$\begin{array}{rccc} \phi_a : & E & \to & E \\ & & & \\ & f & \mapsto & af \end{array}$$

is a linear map. Assume that $v_1, \ldots, v_m$ form an F-basis of E. Then

$$\phi_a(v_1, \ldots, v_m)^T = M_a(v_1, \ldots, v_m)^T$$

where M_a is an $m \times m$ matrix over F.

We define $\det(M_a)$ to be the norm of a with respect to $F \subset E$, which is denoted by $N_{E/F}(a)$. Obviously, $N_{E/F}$ is independent of the choice of bases of E over F.

Lemma 6.5 $N_{E/F}(ab) = N_{E/F}(a)N_{E/F}(b)$.

Proof. It follows immediately from $\phi_a \circ \phi_b = \phi_{ab}$. □

Lemma 6.6 *Let $F \subset K \subset E$ be three fields with $[E : F] < \infty$. For every $a \in K$,*

$$N_{E/F}(a) = N_{K/F}(a)^{[E:K]}.$$

Proof. Let $\alpha_1, \ldots, \alpha_d$ be an F-basis of K, and $\beta_1, \ldots, \beta_e$ a K-basis of E. We claim that

$$B = \{\alpha_i \beta_j \,|\, 1 \leq i \leq d,\, 1 \leq j \leq e\}$$

is an F-basis of E. Assume that there are $f_{i,j} \in F$ such that

$$\sum_{i,j} f_{ij} \alpha_i \beta_j = \sum_j \left(\sum_i f_{ij} \alpha_i \right) \beta_j = 0.$$

Then for each $j = 1, \cdots, e$, $\sum_i f_{ij} \alpha_i = 0$ and thus $f_{i,j} = 0$ for all $i = 1, \cdots, d, j = 1, \cdots, e$. This implies that B is linearly independent over F. Since $[E : F] = |B|$, B is an F-basis of E.

Assume that $a(\alpha_1, \ldots, \alpha_d)^T = A(\alpha_1, \ldots, \alpha_d)^T$ where A is a $d \times d$ matrix over F. Then

$$a(\alpha_1, \ldots, \alpha_d)^T \beta_j = A(\alpha_1 \beta_j, \ldots, \alpha_d \beta_j)^T.$$

It follows that

$$a \begin{pmatrix} \vec{\alpha}\beta_1 \\ \vec{\alpha}\beta_2 \\ \vdots \\ \vec{\alpha}\beta_e \end{pmatrix} = \begin{pmatrix} A & 0 & \cdots & 0 \\ 0 & A & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & A \end{pmatrix} \begin{pmatrix} \vec{\alpha}\beta_1 \\ \vec{\alpha}\beta_2 \\ \vdots \\ \vec{\alpha}\beta_e \end{pmatrix},$$

where $\vec{\alpha} = (\alpha_1, \ldots, \alpha_d)^T$. Hence $N_{E/F}(a) = \det(A)^e$. □

Corollary 6.7 *Let $F \subset E$ be two fields with $[E : F] < \infty$. If $a \in E$ has the minimal polynomial*

$$x^d + f_{d-1} x^{d-1} + \cdots + f_0$$

where $f_{d-1}, \ldots, f_0 \in F$. Then $N_{E/F}(a) = (-1)^{[E:F(a)]d} f_0^{[E:F(a)]}$.

Proof. Consider the tower $F \subset F(a) \subset E$. $1, a, \ldots, a^{d-1}$ is an F-basis of $F(a)$. The matrix of ϕ_a relative to this basis is

$$\begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ -f_0 & -f_1 & -f_2 & \cdots & -f_{d-1} \end{pmatrix}.$$

So $N_{F(a)/F}(a) = (-1)^d f_0$. The rest follows from Lemma 6.6. □

Assume that D is a domain. D is said to be integrally closed if any element in F that is integral over D is in D where F is the quotient field of D.

Lemma 6.8 *Let $D \subseteq R$ be two rings with D integrally closed and $a \in R$. Suppose that a is algebraic over F and $g(x) \in F[x]$ is the minimal polynomial of a over F, where F is the quotient field of D. If a is integral over D, then $g(x) \in D[x]$.*

Proof. Note that the coefficients of $g(x)$ are elementary symmetric functions of the roots of $g(x)$. Since all roots of $g(x)$ are integral over D, so are the coefficients of $g(x)$. Hence all coefficients of $g(x)$ are in D, as D is integrally closed. □

6.3 Affine dimension theorem

Let P be a proper prime ideal in $k[\mathbf{x}]$ with $\dim(P) = d$. Denote $R = k[\mathbf{x}]/P$. For an element $f \in k[\mathbf{x}]$, write $\bar{f}$ for the image of f in R. Let D be a Noether's normalization of R. Denote by F the quotient field of D and E the quotient field of R. Then $[E : F] < +\infty$.

Lemma 6.9 *For any $f \in k[\mathbf{x}]$, $N_{E/F}(\bar{f}) \in D$.*

Proof. Observe that D is integrally closed, since it is isomorphic to a polynomial ring with d variables. Then the first assertion follows from Lemma 6.8 and Corollary 6.7 □

For convention, $\langle * \rangle_R$ stands for the ideal in R generated by $*$.

Lemma 6.10 *For any $f \in k[\mathbf{x}]$,*

$$\sqrt{\langle \bar{f} \rangle_R} \cap D = \sqrt{\langle N_{E/F}(\bar{f}) \rangle_D}.$$

Proof. Suppose that $\bar{h} \in \sqrt{\langle \bar{f} \rangle_R} \cap D$. Then there is some positive integer l such that $\bar{h}^l = \bar{a}\bar{f}$ for some $a \in k[\mathbf{x}]$. Therefore

$$N_{E/F}(\bar{h}^l) = N_{E/F}(\bar{a}\bar{f}) = N_{E/F}(\bar{a}) N_{E/F}(\bar{f}).$$

Since $\bar{h} \in D$, $N_{E/F}(\bar{h}) = \bar{h}^m$ for some positive integer m. This together with the above equality implies that $\bar{h}^{lm} \in \langle N_{E/F}(\bar{f}) \rangle_D$, i.e. $\bar{h} \in \sqrt{\langle N_{E/F}(\bar{f}) \rangle_D}$.

It follows from Corollary 6.7 that $N_{E/F}(\bar{f}) \in \langle \bar{f} \rangle_D$. Hence

$$\sqrt{\langle N_{E/F}(\bar{f}) \rangle_D} \subseteq \sqrt{\langle \bar{f} \rangle_R} \cap D.$$

□

Proposition 6.11 *Let P be a proper prime ideal, and f be a polynomial not in P. If $\sqrt{P+\langle f\rangle}$ is prime and proper, then* $\dim(P+\langle f\rangle) = \dim(P) - 1$.

Proof. Let $Q = \sqrt{P+\langle f\rangle}$ and $d = \dim(P)$. By Corollary 5.11, $\dim(Q) < \dim(P)$. We shall show that $\dim(Q) \geq d-1$. Denote by $\bar{Q}$ the image of the ideal Q in $R = k[\mathbf{x}]/P$. Then

$$\bar{Q} = \sqrt{\overline{P+\langle f\rangle}} = \sqrt{\langle \bar{f}\rangle_R}$$

which is a prime ideal in R. Now let D be a Noether's normalization of R. By Lemma 6.10,

$$\bar{Q} \cap D = \sqrt{\langle \bar{f}\rangle_R} \cap D = \sqrt{\langle N_{E/F}(\bar{f})\rangle_D},$$

where E is the quotient field of R and F is the quotient field of D. As Q is proper, so is $\bar{Q}$ and thus $N_{E/F}(\bar{f}) \notin k$. Note that D is a UFD and $\bar{Q} \cap D$ is prime. One has

$$\bar{Q} \cap D = \langle r\rangle$$

where r is the unique irreducible factor of $N_{E/F}(\bar{f})$. It is easy to see that

$$D/\langle r\rangle = D/(\bar{Q} \cap D) \hookrightarrow R/\bar{Q}.$$

On the other hand,

$$R/\bar{Q} \cong k[\mathbf{x}]/Q.$$

Therefore, $D/\langle r\rangle$ can be regarded as a subring of $k[\mathbf{x}]/Q$. So the quotient field of $D/\langle r\rangle$ is a subfield of that of $k[\mathbf{x}]/Q$. Due to Proposition 6.4, D is isomorphic to a polynomial ring with d variables. Thus the transcendence degree of the quotient field of $D/\langle r\rangle$ over k is $d-1$. Hence the transcendence degree of the quotient field of $k[\mathbf{x}]/Q$ is not less than $d-1$. Consequently, $\dim(Q) \geq d-1$. Hence $\dim(P+\langle f\rangle) = d-1$. □

In what below, we shall show that if $\sqrt{P+\langle f\rangle}$ is not prime, then every irreducible component of $\sqrt{P+\langle f\rangle}$ has dimension $\dim(P)-1$. We begin with a lemma.

Lemma 6.12 *If P is a prime ideal of $k[\mathbf{x}]$ and $h \in k[\mathbf{x}] \setminus P$, then*

$$P^h = \langle P\rangle + \langle th-1\rangle$$

in $k[\mathbf{x},t]$ is prime and $\dim(P^h) = \dim(P)$.

Proof. Note that $P^h \cap k[\mathbf{x}] = P : h^\infty$, which equals P since P is prime. For $f_1, f_2 \in k[\mathbf{x}, t]$, there are $m_1, m_2 \in \mathbf{N}$ such that

$$h^{m_1} f_1 = q_1(ht - 1) + r_1 \quad \text{and} \quad h^{m_2} f_2 = q_2(ht - 1) + r_2$$

where $q_1, q_1 \in k[\mathbf{x}, t]$ and $r_1, r_2 \in k[\mathbf{x}]$. If $f_1 f_2 \in P^h$, then $r_1 r_2 \in P^h$. So $r_1 r_2 \in P$. Without loss of generality, assume that $r_1 \in P$. Then $h^{m_1} f_1 \in P^h$. So

$$(t^{m_1} h^{m_1} - 1) f_1 + f_1 \in P^h$$

which implies $f_1 \in P^h$. Hence, P^h is prime.

There is a natural homomorphism

$$\begin{aligned} \varphi : k[\mathbf{x}] &\longrightarrow k[\mathbf{x}, t]/P^h \\ x_i &\longrightarrow x_i + P^h. \end{aligned}$$

One has $\ker(\varphi) = P^h \cap k[\mathbf{x}] = P$. Hence $k[\mathbf{x}]/P$ can be regarded as a subring of $k[\mathbf{x}, t]/P^h$ and the quotient field of $k[\mathbf{x}]/P$ is a subfield of that of $k[\mathbf{x}, t]/P^h$. These two quotient fields have the same transcendence degree, for $t + P^h$ is algebraic over the quotient field of $k[\mathbf{x}]/P$. So $\dim(P) = \dim(P^h)$. This proves the lemma. □

Proposition 6.13 *Let P be a proper prime ideal, and f a polynomial not in P. If $P + \langle f \rangle$ is proper, then every irreducible component of $\sqrt{P + \langle f \rangle}$ has dimension* $\dim(P) - 1$.

Proof. Let $\sqrt{P + \langle f \rangle} = Q_1 \cap Q_2 \cap \cdots \cap Q_l$ be the minimal irreducible decomposition. Let $h_i \in \cap_{j=1, j \neq i} Q_j \setminus Q_i$. Let

$$Q_i^{h_i} = Q_i + \langle t h_i - 1 \rangle, \ P^{h_i} = P + \langle t h_i - 1 \rangle$$

be ideals in $k[\mathbf{x}, t]$. Due to Lemma 6.12, both $Q_i^{h_i}$ and P^{h_i} are prime and

$$\dim(Q_i) = \dim(Q_i^{h_i}), \dim(P) = \dim(P^{h_i}).$$

We claim that $\sqrt{P^{h_i} + \langle f \rangle} = Q_i^{h_i}$. It is clear that $\sqrt{P^{h_i} + \langle f \rangle} \subset Q_i^{h_i}$. Assume that $g \in Q_i^{h_i}$. Then $h_i g \in \sqrt{P^{h_i} + \langle f \rangle}$, since $h_i \in Q_j$ for all $j \neq i$. So $(t h_i - 1) g + g \in \sqrt{P^{h_i} + \langle f \rangle}$, which implies that $g \in \sqrt{P^{h_i} + \langle f \rangle}$. This proves the claim. Now by Proposition 6.11,

$$\dim(P) - 1 = \dim(P^{h_i}) - 1 = \dim(P^{h_i} + \langle f \rangle) = \dim(Q_i^{h_i}) = \dim(Q_i).$$

□

Proposition 6.14 *Let I be a proper ideal of $k[\mathbf{x}]$. Then* $\dim(I) = \mathrm{kdim}(I)$.

Proof. We first show the proposition for the case that I is prime. Let $d = \mathrm{kdim}(I)$. Then there is a chain of ideals

$$I = P_0 \subsetneqq P_1 \subsetneqq \cdots \subsetneqq P_d$$

where the P_i are proper prime ideals and P_d is maximal. Due to Corollary 5.11, one has

$$0 = \dim(P_d) < \cdots < \dim(P_1) < \dim(P_0) = \dim(I).$$

Suppose that $d < \dim(I)$. Then $\dim(P_{i-1}) - \dim(P_i) > 1$ for some i with $1 \leq i \leq d$. Let $f \in P_i \setminus P_{i-1}$. Lemma 4.9 implies that there is an irreducible component of $\sqrt{\langle P_{i-1} + f\rangle}$, say Q, which is contained in P_i. By Proposition 6.13,

$$\dim(Q) = \dim(P_{i-1}) - 1 > \dim(P_i),$$

which implies that $Q \neq P_i$. Now we have a new chain of ideals

$$I \subset P_0 \subsetneqq P_1 \subsetneqq \cdots \subsetneqq P_{i-1} \subsetneqq Q \subsetneqq P_i \subsetneqq \cdots \subsetneqq P_d$$

whose length is greater than d, a contradiction. Thus $d = \dim(I)$.

It is easy to see that if $I \subset J$ then $\mathrm{kdim}(I) \geq \mathrm{kdim}(J)$. Let Q be a prime ideal containing I such that $\dim(I) = \dim(Q)$. Then one has

$$\mathrm{kdim}(I) \geq \mathrm{kdim}(Q) = \dim(Q) = \dim(I).$$

Proposition 5.13 implies that $\mathrm{kdim}(I) = \dim(I)$. □

Lemma 6.15 *Let $I \subset k[\mathbf{x}]$ and $J \subset k[\mathbf{y}]$ be two ideals. Then* $\dim(\langle I, J\rangle) = \dim(I) + \dim(J)$.

Proof. We first show that $\dim(\langle I, J\rangle) \leq \dim(I) + \dim(J)$. Suppose that S is a subset of $\mathbf{x} \cap \mathbf{y}$ with $|S| > \dim(I) + \dim(J)$. Then either $|S \cap \mathbf{x}| > \dim(I)$ or $|S \cap \mathbf{y}| > \dim(J)$, which implies that either $I \cap k[S \cap \mathbf{x}] \neq (0)$ or $J \cap k[S \cap \mathbf{y}] \neq (0)$. Hence $\langle I, J\rangle \cap k[S] \neq (0)$. So $\dim(\langle I, J\rangle) \leq \dim(I) + \dim(J)$. Now suppose that $S_1 \subseteq \mathbf{x}$ is an independent set modulo I with $|S_1| = \dim(I)$ and $S_2 \subseteq \mathbf{y}$ is an independent set modulo J with $|S_1| = \dim(J)$.

Let G be a Grönber basis of I with respect to the lex order $\mathbf{x} \setminus \{S_1\} \succ S_1$ and H be a Gröebner basis of J with respect to the lex order $\mathbf{y} \setminus \{S_2\} \succ S_2$.

Then by Proposition 3.16, $G \cup H$ is a Groebner basis of $\langle I, J\rangle$ with respect to the lex order $\mathbf{x} \setminus \{S_1\} \succ S_1 \succ \mathbf{y} \setminus \{S_2\} \succ S_2$. Assume that $f \in \langle I, J\rangle \cap k[S_1 \cap S_2]$. Then f is reduced w.r.t. $G \cup H$. Since $f \in \langle I, J\rangle$, $f = 0$ by Theorem 3.8. Hence $\langle I, J\rangle \cap k[S_1 \cup S_2] = (0)$. So $\dim(\langle I, J\rangle) \geq \dim(I) + \dim(J)$. □

Let I be an ideal of $k[\mathbf{x}]$ and $\mathbf{y} = \{y_1, y_2, \cdots, y_n\}$. Denote

$$I^{\mathbf{y}} = \{g(\mathbf{y}) : g(\mathbf{x}) \in I\}$$

which is an ideal of $k[\mathbf{y}]$.

Lemma 6.16 *If $I, J \subseteq k[\mathbf{x}]$ are two ideals, then*

$$\dim(\langle I, J^{\mathbf{y}}, y_1 - x_1, \cdots, y_n - x_n\rangle) = \dim(I + J).$$

Proof. Let $K = \langle I, J^{\mathbf{y}}, y_1 - x_1, \cdots, y_n - x_n\rangle$. Let S be a subset of $\mathbf{x}$. We first claim that if S is independent modulo $I + J$ then it is independent modulo K. This claim implies that $\dim(K) \geq \dim(I + J)$. Assume $h \in k[S] \cap K$. Write

$$h = \sum_i a_i f_i(\mathbf{x}) + \sum_j b_j g_j(\mathbf{y}) + \sum_s c_s(y_s - x_s)$$

where $a_i, b_j, c_s \in k[\mathbf{x}, \mathbf{y}]$. Setting $y_s = x_s$ in the above equality results in $h \in I + J$. Therefore $h \in k[S] \cap (I + J)$. So if $k[S] \cap I + J = 0$, then $k[S] \cap K = 0$. This proves the claim.

Next we show that $\dim(I + J) \geq \dim(K)$. Define a ring homomorphism ϕ from $k[\mathbf{x}, \mathbf{y}]$ to $k[\mathbf{x}]$ by setting $\phi(x_i) = x_i$ and $\phi(y_i) = x_i$ for each $i = 1, \cdots, n$. Assume that T be an independent subset of $\mathbf{x} \cup \mathbf{y}$ modulo K with $|T| = \dim(K)$. Then $|\phi(T)| = |T|$. Otherwise, $y_i - x_i \in k[T]$ for some i, which implies that $k[T] \cap K \neq 0$, a contradiction. Suppose that $h \in k[\phi(T)] \cap (I + J)$. It is easy to verify $\phi(K) = I + J$. So there is $a \in K$ such that $h = \phi(a)$. On the other hand, there is $b \in k[T]$ such that $h = \phi(b)$. Then one has $a - b \in \ker(\phi)$. As $\ker(\phi) \subset K$, $b \in k[T] \cap K$. So $b = 0$ and thus $h = 0$. In the sequel, $\phi(T)$ is an independent set modulo $I + J$. Then

$$\dim(I + J) \geq |\phi(T)| = |T| = \dim(K).$$

□

Lemma 6.17 *Assume that I is a prime ideal in $k[\mathbf{x}]$ and J is a prime ideal in $k[\mathbf{y}]$. Then every irreducible component of $\sqrt{\langle I, J\rangle}$ has dimension $\dim(I) + \dim(J)$.*

Proof. We shall use $\langle * \rangle_{\bar{k}}$ to denote the ideal in $\bar{k}[\mathbf{x}]$ (or $\bar{k}[\mathbf{x}, \mathbf{y}]$) generated by $*$. Let S_1 be an independent subset of $\mathbf{x}$ modulo I with $|S_1| = \dim(I)$, and S_2 be an independent subset of $\mathbf{y}$ modulo J with $|S_2| = \dim(J)$. From the proof of Lemma 6.15, one sees that $S_1 \cup S_2$ is an independent subset modulo $\langle I, J \rangle$. Let Q be an irreducible component of $\sqrt{\langle I, J \rangle}$. Suppose that $Q \cap k[S_1 \cup S_2] \neq 0$. Let $f(\mathbf{x}, \mathbf{y})$ be a nonzero element of $Q \cap k[S_1 \cup S_2]$. Then there is $g(\mathbf{x}, \mathbf{y}) \in k[\mathbf{x}, \mathbf{y}]$ but $g(\mathbf{x}, \mathbf{y}) \notin \langle I, J \rangle$ such that $f(\mathbf{x}, \mathbf{y})^d g(\mathbf{x}, \mathbf{y}) \in \langle I, J \rangle$. Write

$$g(\mathbf{x}, \mathbf{y}) = \sum_{i=1}^{l} q_i h_i, \ q_i \in k[\mathbf{x}], h_i \in k[\mathbf{y}].$$

Without loss of generality, we may assume that there does not exist $c_1, \cdots, c_l \in k$, not all zero, such that $\sum_{i=1}^{l} c_i h_i \in I$. If for any $\mathbf{b} \in \mathbf{V}(J)$ one has $f(\mathbf{x}, \mathbf{b})^d g(\mathbf{x}, \mathbf{b}) = 0$, then $f(\mathbf{x}, \mathbf{y})^d g(\mathbf{x}, \mathbf{y}) \in \langle J \rangle$. Since J is prime, so is $\langle J \rangle$. Hence $f(\mathbf{x}, \mathbf{y}) \in \langle J \rangle \subset \langle I, J \rangle$, which contradicts $\langle I, J \rangle \cap k[S_1 \cup S_2] = 0$. Thus, there is $\mathbf{b} \in \mathbf{V}(J)$ such that $f(\mathbf{x}, \mathbf{b})^d g(\mathbf{x}, \mathbf{b}) \neq 0$. Multiplying $f(\mathbf{x}, \mathbf{b})$ with a suitable polynomial in $\bar{k}[S_1]$, one can assume that $f(\mathbf{x}, \mathbf{b}) \in k[S_1]$. Write $g(\mathbf{x}, \mathbf{b}) = \sum_{j=1}^{s} g_j v_j$ where g_j is a nonzero k-linear combination of $h_1, \cdots, h_l$, and $v_1, \cdots, v_s$ are linearly independent over k. Since $h_1, \cdots, h_l$ are k-linearly independent modulo I, $g_j \notin I$ for all $j = 1, \cdots, s$. Now one has

$$f(\mathbf{x}, \mathbf{b})^d g(\mathbf{x}, \mathbf{b}) = \sum_{j=1}^{s} f(\mathbf{x}, \mathbf{b})^d g_j v_j \in \langle I \rangle_{\bar{k}},$$

which implies that $f(\mathbf{x}, \mathbf{b})^d g_j \in I$. Hence $f(\mathbf{x}, \mathbf{b}) \in I$. This contradicts $I \cap k[S_1] = 0$. Thus $Q \cap k[S_1 \cup S_2] = 0$. So $\dim(Q) = \dim(I) + \dim(J)$. □

Theorem 6.18 *(Affine Dimension Theorem) Assume that I and J are two prime ideals in $k[\mathbf{x}]$. If $1 \notin I + J$, then* $\dim(I + J) \geq \dim(I) + \dim(J) - n$.

Proof. Let $K = \sqrt{\langle I, J^{\mathbf{y}}, y_1 - x_1, \cdots, y_n - x_n \rangle}$. It is easy to verify that $K \cap k[\mathbf{x}] = \sqrt{I + J}$. Since $1 \notin I + J$, $1 \notin K$. As $\sqrt{\langle I, J^{\mathbf{y}} \rangle} \subset K$, Lemma 4.9 implies that there is an irreducible component Q of $\sqrt{\langle I, J^{\mathbf{y}} \rangle}$ which is contained in some irreducible component P of K. By Lemma 6.17, $\dim(Q) = \dim(I) + \dim(J)$. If $y_1 - x_1 \in Q$, then $\dim(\langle y_1 - x_1 \rangle + Q) = \dim(Q)$. Otherwise, since $\langle y_1 - x_1 \rangle + Q \subset P$, $1 \notin \langle y_1 - x_1 \rangle + Q$. Then Proposition 6.13 implies that every irreducible component of $\sqrt{\langle y_1 - x_1 \rangle + Q}$ has dimension $\dim(I) + \dim(J) - 1$. By Lemma 4.9 again, there is an irreducible component Q_1 of $\sqrt{\langle y_1 - x_1 \rangle + Q}$ contained in P. Continuing the

applications of Proposition 6.13, we finally have a prime ideal $Q_l \subset P$ with $\dim(Q_l) \geq \dim(I) + \dim(J) - n$. Note that $K \subset Q_l$. Therefore $Q_l = P$. This completes the proof. □

Chapter 7

Regular and Rational Functions

In this chapter, k is supposed to be of characteristic zero. We shall use F_m to denote $(f_1, \cdots, f_m)$ where $f_i \in k[\mathbf{x}]$.

7.1 Regular functions

A map $\phi : \bar{k}^n \to \bar{k}^m$ is said to be *regular* if there exist $f_1, \ldots, f_m \in k[\mathbf{x}]$ such that

$$\forall \mathbf{c} \in \bar{k}^m, \phi(\mathbf{c}) = (f_1(\mathbf{c}), \ldots, f_m(\mathbf{c})).$$

If $\phi = F_m = \tilde{F}_m$, then $F_m = \tilde{F}_m$ since $\bar{k}$ is infinite.

Example 7.1 *Projections, linear transformations and parametric maps $t \to (t, t^2)$ are regular maps.*

Question: Given a regular map $\phi : \bar{k}^n \to \bar{k}^n$, decide whether ϕ has a regular inverse.

Lemma 7.1 *If a regular map $\phi = (f_1(\mathbf{x}), \ldots, f_n(\mathbf{x}))$ has a regular inverse, then*

$$\left| \frac{\partial(f_1, \ldots, f_n)}{\partial(x_1, \ldots, x_n)} \right|$$

is a nonzero element of k.

Proof. Let $\phi^{-1} = (g_1(\mathbf{y}), \ldots, g_n(\mathbf{y}))$ where $\mathbf{y} = (y_1, \ldots, y_n)$. We have

$$g_i(f_1(\mathbf{x}), \ldots, f_n(\mathbf{x})) = x_i, \quad i = 1, \ldots, n.$$

Then

$$\delta_{ij} = \frac{\partial g_i(f_1(\mathbf{x}), \ldots, f_n(\mathbf{x}))}{\partial x_j} = \sum_{\ell=1}^{n} \frac{\partial g_i}{\partial y_\ell}(f_1(\mathbf{x}), \ldots, f_n(\mathbf{x})) \frac{\partial f_\ell}{\partial x_j}.$$

It follows that

$$\frac{\partial(g_1, \ldots, g_n)}{\partial(y_1, \ldots, y_n)}(f_1(\mathbf{x}), \ldots, f_n(\mathbf{x})) \frac{\partial(f_1, \ldots, f_n)}{\partial(x_1, \ldots, x_n)} = 1.$$

Hence $|\frac{\partial(f_1,\ldots,f_n)}{\partial(x_1,\ldots,x_n)}|$ is a nonzero element of k. □

The converse of this lemma is known as Jacobian conjecture.

Lemma 7.2 *Let A and B be two sets, $\phi : A \to B$ and $\psi : B \to A$. Let $G_\phi = \{(a, \phi(a)) | a \in A\}$ and $G_\psi = \{(\psi(b), b) | b \in B\}$. Then $\psi = \phi^{-1}$ if and only if $G_\phi = G_\psi$.*

Proof. Straightforward. □

Let $\phi = (f_1(\mathbf{x}), \ldots, f_m(\mathbf{x}))$ be a regular map from $\bar{k}^n$ to $\bar{k}^m$. Then

$$G_\phi = \{(\mathbf{c}, f_1(\mathbf{c}), \ldots, f_m(\mathbf{c})) | \mathbf{c} \in \bar{k}^n\}.$$

Hence, $G_\phi = \mathbf{V}(y_1 - f_1(\mathbf{x}), \ldots, y_m - f_m(\mathbf{x}))$.

Lemma 7.3 *The ideal $\langle y_1 - f_1(\mathbf{x}), \ldots, y_m - f_m(\mathbf{x})\rangle$ is a prime ideal of dimension n.*

Theorem 7.4 *Let $\phi = (f_1(\mathbf{x}), \ldots, f_m(\mathbf{x})) : \bar{k}^n \to \bar{k}^m$ be a regular map. Then ϕ has a regular inverse if and only if $m = n$, and there exist $g_1(\mathbf{y}), \ldots, g_n(\mathbf{y}) \in k[\mathbf{y}]$ such that*

$$\langle y_1 - f_1(\mathbf{x}), \ldots, y_m - f_m(\mathbf{x})\rangle = \langle x_1 - g_1(\mathbf{y}), \ldots, x_n - g_n(\mathbf{y})\rangle.$$

Proof. Let $I = \langle y_1 - f_1(\mathbf{x}), \ldots, y_m - f_m(\mathbf{x})\rangle$. Suppose that $\psi = (g_1(\mathbf{y}), \ldots, g_n(\mathbf{y}))$ is the regular inverse of ϕ. Then $G_\phi = G_\psi$ by Lemma 7.2. Let $J = \langle x_1 - g_1(\mathbf{y}), \ldots, x_n - g_n(\mathbf{y})\rangle$. One has $\mathbf{V}(I) = \mathbf{V}(J)$, which implies $I = J$ by Lemma 7.3. Since $\dim(I) = \dim(J)$, $m = n$. Conversely, we set ψ as above. Then $I = J$ implies $\mathbf{V}(I) = \mathbf{V}(J)$, i.e. $G_\phi = G_\psi$. Hence $\phi = \psi^{-1}$. □

Note that a set of generators of an ideal of the form

$$\{y_1 - f_1(\mathbf{x}), \cdots, y_n - f_n(\mathbf{x})\}$$

is the canonical Gröbner basis of I with respect to a lex order $\mathbf{y} \succ \mathbf{x}$. The above theorem allows us to check if a given regular map has a regular inverse by Gröbner bases computation. Thus one can verify the Jacobian conjecture for a given regular map.

Example 7.2 *Let* $f_1 = x_1 + (x_1 - x_2)^2, f_2 = x_2 + (x_1 - x_2)^2$. *We have*

$$\frac{\partial(f_1, f_2)}{\partial(x_1, x_2)} = \begin{pmatrix} 1 + 2(x_1 - x_2) & -2(x_1 - x_2) \\ 2(x_1 - x_2) & 1 - 2(x_1 - x_2) \end{pmatrix}$$

and then $|\frac{\partial(f_1,f_2)}{\partial(x_1,x_2)}| = 1$. *Let* $I = \langle y_1 - f_1(\mathbf{x}), y_2 - f_2(\mathbf{x})\rangle$. *With respect to the lex order* $x_1 \succ x_2 \succ y_1 \succ y_2$, *we compute a Gröbner basis of* I *which is*

$$x_2 - y_2 + (y_1 - y_2)^2, x_1 - y_1 + (y_1 - y_2)^2.$$

Therefore the regular map $\phi = (f_1, f_2)$ *has a regular inverse.*

7.2 Regular functions on a variety

Let V be a variety in $\bar{k}^n$. A function $\alpha : V \to \bar{k}$ is said to be *regular* if there exists $f \in k[\mathbf{x}]$ such that $\alpha = f|_V$. Clearly, $\alpha = f|_V = g|_V$ if and only if $f - g \in \mathbf{I}(V)$. Set $O(V)$ to be the set of regular functions on V. Then $O(V)$ is a k-algebra. Actually, one can show that

Proposition 7.5 $O(V) = k[\mathbf{x}]/\mathbf{I}(V)$.

Proof. Straightforward. □

Proposition 7.6 *Let* V *be a variety.*

1. V *is irreducible if and only if* $O(V)$ *is a domain.*
2. $\dim(V)$ *is equal to the maximal number of the algebraically independent elements of* $O(V)$ *over* k *if* V *is irreducible.*

Proof. Straightforward. □

Let $V \subset \bar{k}^n$ and $W \subset \bar{k}^m$ be two varieties. A map $\phi : V \to W$ is said to be *regular* if there exist $f_1, \ldots, f_m \in k[\mathbf{x}]$ such that $\phi = (f_1, \ldots, f_m)|_V$.

Proposition 7.7 *1. If $\phi : V \to W$ is regular, then $\phi^* : O(W) \to O(V)$ defined by $\alpha \mapsto \alpha \circ \phi$ is a k-homomorphism.*

2. If $\psi : O(W) \to O(V)$ is a k-homomorphism, then there exists a unique regular map ψ_* from V to W such that $(\psi_*)^* = \psi$.

Proof. For $\alpha \in O(W)$, $\alpha \circ \phi : V \to W \to \bar{k}$. Let $\phi = (f_1(\mathbf{x}), \ldots, f_m(\mathbf{x}))$ and $\alpha = g(\mathbf{y})|_W$. Then $\alpha \circ \phi = g(f_1(\mathbf{x}), \ldots, f_m(\mathbf{x}))$. It is easy to see that $\alpha \circ \phi$ is independent of the choices of the f_i's and g. Thus $\alpha \circ \phi$ is well-defined and it is a regular function on V.

Assume that $\psi : k[\mathbf{y}]/\mathbf{I}(W) \to k[\mathbf{x}]/\mathbf{I}(V)$ is a k-homomorphism given by $\psi(y_j + \mathbf{I}(W)) = g_j(\mathbf{x}) + \mathbf{I}(V)$ for $j = 1, \ldots, m$. Define

$$\begin{aligned} \psi_* : V &\to W \\ \mathbf{c} &\to (g_1(\mathbf{c}), \ldots, g_n(\mathbf{c})). \end{aligned}$$

For any $h \in \mathbf{I}(W)$, $\psi(h + \mathbf{I}(W)) = 0$, i.e. $h(g_1(\mathbf{x}), \cdots, g_m(\mathbf{x})) \in \mathbf{I}(V)$. Hence, $h(g_1(\mathbf{c}), \ldots, g_m(\mathbf{c})) = 0$ for all $\mathbf{c} \in V$ and all $h \in \mathbf{I}(W)$. Consequently, $(g_1(\mathbf{c}), \ldots, g_m(\mathbf{c})) \in W$ for all $\mathbf{c} \in V/$ So the map $\psi_* : V \to W$ is well-defined. It is straightforward to see that $\psi = (\psi_*)^*$.

Assume that $\xi : V \to W$ is a regular map with $\xi^* = \psi$. Assume that $\xi = (h_1(\mathbf{x}), \ldots, h_m(\mathbf{x}))|_V$. Then for each $j = 1, \cdots, m$

$$\xi^*(y_j + \mathbf{I}(W)) = h_j(\mathbf{x}) + \mathbf{I}(V) = g_j(\mathbf{x}) + \mathbf{I}(V).$$

It follows that $g_j(\mathbf{x}) - h_j(\mathbf{x}) \in \mathbf{I}(V)$ for all $j = 1, \cdots, m$, and, thus, $\xi = \psi_*$. □

Two varieties V and W are said to be isomorphic over k if there are regular maps $\phi : V \to W$ and $\psi : W \to V$ such that $\phi^{-1} = \psi$.

Lemma 7.8 *If $I \subset k[\mathbf{x}]$ is an ideal and*

$$H = \langle y_1 - f_1(\mathbf{x}), \ldots, y_m - f(\mathbf{x}), I \rangle$$

with any $f_i \in k[\mathbf{x}]$, then $k[\mathbf{x}, \mathbf{y}]/H$ and $k[\mathbf{x}]/I$ are isomorphic.

Proof. Let $\theta : k[\mathbf{x}, \mathbf{y}] \to k[\mathbf{x}]/I$ be a homomorphism given by $\theta(x_i) = x_i + I$ and $\theta(y_j) = f_j + I$. Then $\ker(\theta) = H$.Obviously, θ is surjective. □

Remark 7.1 *The ideal I is radical (prime) if and only if H is radical (prime) by the above lemma.*

Theorem 7.9 *Let $\phi : V \to W$ and $\psi : W \to V$ be two regular maps. Assume that $\phi = (f_1(\mathbf{x}), \ldots, f_m(\mathbf{x}))|_V$ and $\psi = (g_1(\mathbf{y}), \ldots, g_n(\mathbf{y})|_W$. Let*

$$I = \langle y_1 - f_1(\mathbf{x}), \ldots, y_m - f_m(\mathbf{x}), \mathbf{I}(V)\rangle \quad \text{and} \quad J = \langle x_1 - g_1(\mathbf{y}), \ldots, x_n - g_n(\mathbf{y}), \mathbf{I}(W)\rangle.$$

Then the followings are equivalent.

1. $\psi = \phi^{-1}$;
2. $\psi^* = (\phi^*)^{-1}$;
3. $I = J$.

Proof. Let $G_\phi = \mathbf{V}(I)$ and $G_\psi = \mathbf{V}(J)$. Then, $\psi = \phi^{-1}$ if and only if $\mathbf{V}(I) = \mathbf{V}(J)$. Since I and J are both radical by Remark 7.1, $I = J$. This proves that the first and third assertions are equivalent.

We now prove that the second and third assertions are equivalent. By Lemma 7.8, we have two k-isomorphisms:

$$\begin{array}{rccc} \Phi: & k[\mathbf{x},\mathbf{y}]/I & \to & k[\mathbf{x}]/\mathbf{I}(V) \\ & x_i & \mapsto & x_i + \mathbf{I}(V) \\ & y_j & \mapsto & f_j(\mathbf{x}) + \mathbf{I}(V) \end{array} \quad \text{and} \quad \begin{array}{rccc} \Psi: & k[\mathbf{x},\mathbf{y}]/J & \to & k[\mathbf{y}]/\mathbf{I}(W) \\ & x_i & \mapsto & g_i(\mathbf{y}) + \mathbf{I}(W) \\ & y_j & \mapsto & y_j + \mathbf{I}(W) \end{array}$$

where $i = 1, \ldots, n$ and $j = 1, \ldots, m$. If $I = J$, $\Phi \circ \Psi^{-1}$ is a k-isomorphism from $k[\mathbf{y}]/\mathbf{I}(W)$ to $k[\mathbf{x}]/\mathbf{I}(V)$, which maps $y_j + \mathbf{I}(W)$ to $f_j(\mathbf{x}) + \mathbf{I}(V)$ for $j = 1, \ldots, m$. Hence, $\Phi \circ \Psi^{-1} = \phi^*$. In the same vein $\Psi \circ \Phi^{-1} = \psi^*$. Conversely, assume that $(\phi^*)^{-1} = \psi^*$. Then $\Psi^{-1} \circ \phi^* \circ \Phi$ is a k-isomorphism from $k[\mathbf{x},\mathbf{y}]/I$ to $k[\mathbf{x},\mathbf{y}]/J$, which sends $x_i + I$ to $x_i + J$, and $y_j + I$ to $y_j + J$. It follows that $I = J$. □

Example 7.3 *Let $\phi : \bar{k} \to \mathbf{V}(y_1^2 - y_2)$ with $\phi(c) = (c, c^2)$. Then*

$$I = \langle y_1 - x, y_2 - x^2\rangle = \langle x - y_1, y_1^2 - y_2\rangle.$$

Hence ϕ is an isomorphism.

Example 7.4 *Let $\phi : \bar{k} \to \mathbf{V}(y_2^2 - y_1^3)$ with $\phi(c) = (c^3, c^2)$. Then*

$$I = \langle y_1 - x^3, y_2 - x^2\rangle = \langle x^2 - y_2, xy_1 - y_2^2, xy_2^2 - y_1, y_2^2 - y_1^3\rangle.$$

Hence ϕ is not an isomorphism.

Example 7.5 *Is $\bar{k}$ isomorphic to $\mathbf{V}(y_1^2+y_2^2-1)$? Consider $\phi : \bar{k} \to \mathbf{V}(y_1^2+y_2^2-1)$ with c being mapped to $(f_1(c), f_2(c))$ for some $f_1, f_2 \in k[x]$. Then $f_1^2+f_2^2=1$ holds in $k[x]$. It follows that*

$$(f_1+\sqrt{-1}f_2)(f_1-\sqrt{-1}f_2)=1$$

holds in $\bar{k}[x]$. Assume that the characteristic of k is not equal to 2. Then $f_1, f_2 \in k$ and ϕ cannot be an isomorphism. If the characteristic of k is equal to 2, then $\mathbf{V}(y_1^2+y_2^2-1)=\mathbf{V}(y_1+y_2-1)$, which is isomorphic to $\bar{k}$ over k.

7.3 Rational maps between irreducible varieties

Let V be a variety. A subset U of V is called an open subset of V if $U = V \setminus Z$ where Z is another variety. An open subset U of V is said to be dense in V if $\bar{U} = V$.

Proposition 7.10 *1. If V is irreducible, then every nonempty open subset of V is dense.*

2. The intersection of two dense open subsets is dense.

Proof. Suppose that U is a nonempty open subset of V. Then $U = V \setminus Z$ for some variety Z. Hence $V = (Z \cap V) \cup \bar{U}$. Since $U \neq \emptyset$, $V \neq Z \cap V$. Thus $V = \bar{U}$.

Assume that $U_i = V \setminus Z_i$ is a dense open subset of V for $i = 1, 2$. Then $U_1 \cap U_2 = V \setminus \{Z_1 \cup Z_2\}$. Let $V = V_1 \cup \cdots \cup V_l$ be the minimal irreducible decomposition of V. One can easily verify that

$$V = \overline{V \cap U_j} = \cup_{i=1}^{l} \overline{V_i \cap U_j}, j = 1, 2.$$

Hence $V_i = \overline{V_i \cap U_j}$ for all $i = 1, \cdots, l$ and $j = 1, 2$. Now we claim that $V_i \cap U_1 \cap U_2 \neq \emptyset$ for all $i = 1, \cdots, l$. This claim will imply that

$$V_i = \overline{V_i \cap U_1 \cap U_2},\ i = 1, \cdots, l.$$

Suppose on the contrary that $V_i \cap U_1 \cap U_2 = \emptyset$. Then $V_i \subseteq Z_1 \cup Z_2$. Since V_i is irreducible, by Lemma 4.9, either $V_i \subseteq Z_1$ or $V_i \subseteq Z_2$. Thus either $V_i \cap U_1 = \emptyset$ or $V_i \cap U_1 = \emptyset$, a contradiction. This proves the claim. Now one has that

$$\overline{V \cap U_1 \cap U_2} = \cup_{i=1}^{l} \overline{V_i \cap U_1 \cap U_2} = \cup_{i=1}^{l} V_i = V.$$

□

In the following, V, W, Z will be used to denote irreducible varieties. Let V be an irreducible variety in $\bar{k}^n$. Elements in the quotient field of $O(V)$ are called rational functions on V. For brevity, denote by $k(V)$ the quotient field of $O(V)$. Assume that α is a rational function on V. Then one may represent α as $h_1)/h_2$ for some $h_1, h_2 \in k[\mathbf{x}]$ with $h_2 \notin \mathbf{I}(V)$. However the representation of α is not unique.

Example 7.6 *Let $V = \mathbf{V}(x_1^2 + x_2^2 - 1)$. Then both of*

$$\frac{x_2 + 1}{x_1} \text{ and } \frac{x_1}{1 - x_2}$$

represent rational functions on V. Actually, these two rational functions are equal, since

$$(x_2 + 1)(1 - x_2) - x_1^2 \in \mathbf{I}(V).$$

Suppose that $\mathbf{c} \in V$. We say α is regular at $\mathbf{c}$ if α can be written in the form h_1/h_2 with $h_2(\mathbf{c}) \neq 0$. In this case, we say $h_1(\mathbf{c})/h_2(\mathbf{c})$ the value of α, denoted by $\alpha(\mathbf{c})$.

Lemma 7.11 *Suppose that $\alpha, \beta \in k(V)$. If there is a nonempty open subset U of V such that both α and β are regular at U and for any $\mathbf{a} \in U$, $\alpha(\mathbf{a}) = \beta(\mathbf{a})$, then $\alpha = \beta$.*

Proposition 7.12 *Let α be a rational function on V and S_α the set of points of V at which α is regular. Then S_α is a nonempty open subset of V.*

Proof. Assume that h_1/h_2 is a representation of α. Since $h_2 \notin \mathbf{I}(V)$, there is $\mathbf{c} \in V$ such that $h_2(\mathbf{c}) \neq 0$, i.e. α is regular at $\mathbf{c}$. Thus $\mathbf{c} \in S_\alpha$. So $S_\alpha \neq \emptyset$. Now consider all possible representations of α, denoted by

$$\left\{ \frac{g_\lambda}{h_\lambda} \middle| \lambda \in \Lambda \right\}.$$

Then $V \setminus \mathbf{V}(h_\lambda)$ is open and $S_\alpha = \cup_{\lambda \in \Lambda}(V \setminus \mathbf{V}(h_\lambda))$. Hence S_α is open. □

Let W be an irreducible variety in $\bar{k}^m$. By a rational map from V to W, we mean a map $\phi = (\phi_1, \cdots, \phi_m)$ satisfying that all the ϕ_i are rational functions on V and there is a nonempty open subset U of V such that for any $\mathbf{c} \in U$, all the ϕ_i are regular at $\mathbf{c}$ and $\phi(\mathbf{c}) = (\phi_1(\mathbf{c}), \cdots, \phi_m(\mathbf{c})) \in W$. We shall say ϕ is regular at $\mathbf{c}$ if all the ϕ_i are regular at $\mathbf{c}$. Let $U \subset \bar{k}^n$. We say ϕ is regular at U if it is regular at all points in U.

Proposition 7.13 *Assume that $\phi = (\phi_1, \cdots, \phi_m) : V \to W$ is a rational map and $\mathbf{b} \in V$. If ϕ is regular at $\mathbf{b}$, then $\phi(\mathbf{b}) \in W$.*

Proof. Assume that U is a nonempty open subset of V at which ϕ is regular and $\phi(U) \subset W$. Let f_i/a be a representation of ϕ_i such that $a(\mathbf{b}) \neq 0$. Set $\bar{U} = U \cap (V \setminus \mathbf{V}(a))$. Then $\bar{U}$ is also a nonempty open subset of V. Suppose that $g \in \mathbf{I}(W)$. There is a positive integer l such that $\tilde{g} = a^l g\,(f_1/a, \cdots, f_m/a)$ is a polynomial in $k[\mathbf{x}]$. Now for any $\mathbf{c} \in \bar{U}$, one has

$$\tilde{g}(\mathbf{c}) = a(\mathbf{c})^l g\,(f_1(\mathbf{c})/a(\mathbf{c}), \cdots, f_m(\mathbf{c})/a(\mathbf{c})) = 0.$$

As $\bar{U}$ is dense in V, $\tilde{g} \in \mathbf{I}(V)$. So $\tilde{g}(\mathbf{b}) = 0$. This implies that

$$g\,(f_1(\mathbf{b})/a(\mathbf{b}), \cdots, f_m(\mathbf{b})/a(\mathbf{b})) = g(\phi(\mathbf{b})) = 0.$$

Therefore $\phi(\mathbf{b}) \in W$. □

Denote by $\mathrm{dom}(\phi)$ the set of points in V at which ϕ is regular. By Propositions 7.12 and 7.10, $\mathrm{dom}(\phi)$ is a nonempty open subset of V.

A rational map ϕ from V to W is said to be *dominant* if $\phi(\mathrm{dom}(\phi))$ is dense in W.

Lemma 7.14 *Assume that $\phi : V \to W$ is a dominant rational map. Then for any nonempty open subset $U \subset \mathrm{dom}(\phi)$, $\phi(U)$ is dense in W.*

Proof. Suppose on the contrary that $\overline{\phi(U)} \subsetneq W$. There is $g \in \mathbf{I}(\phi(U)) \setminus \mathbf{I}(W)$. Then there is $\mathbf{b} \in W$ such that $g(\mathbf{b}) \neq 0$. Such $\mathbf{b}$ can be chosen to be in $\phi(\mathrm{dom}(\phi))$, because $\phi(\mathrm{dom}(\phi))$ is dense in W. This implies that there $\mathbf{c} \in \mathrm{dom}(\phi)$ such that $\phi(\mathbf{c}) = \mathbf{b}$. Write $\phi = (\phi_1, \cdots, \phi_m)$ and suppose that f_i/a is a representation of ϕ_i with $a(\mathbf{c}) \neq 0$ for all $i = 1, \cdots, m$. Let l be an integer large enough such that $q = a^l g(f_1/a, \cdots, f_m/a) \in k[\mathbf{x}]$. Now for any $\mathbf{c}' \in U \setminus \mathbf{V}(a)$, $q(\mathbf{c}') = 0$. As $U \setminus \mathbf{V}(a)$ is dense in V, $q \in \mathbf{I}(V)$. Hence $q(\mathbf{c}) = 0$. This implies that $g(\phi(\mathbf{c})) = 0$, i.e. $g(\mathbf{b}) = 0$, a contradiction. □

Proposition 7.15 *Let $\phi : V \to W$ and $\psi : W \to Z$ be two rational maps. If ϕ is dominant, then $\psi \circ \phi$ is a well-defined rational map from V to Z.*

Proof. Suppose that $\phi = (\phi_1, \cdots, \phi_m)$ and $\psi = (\psi_1, \cdots, \psi_l)$. Then

$$\psi \circ \phi = (\psi_1 \circ \phi, \cdots, \psi_l \circ \phi).$$

We first show that $\psi_j \circ \phi$ is a rational function on V for all $j = 1, \cdots, l$. Let f_i/a be a representation of ϕ_i and g_j/b be a representation of ψ_j. Let ν be an integer large enough such that

$$a^\nu b(f_1/a, \cdots, f_m/a), a^\nu g_1(f_1/a, \cdots, f_,/a), \cdots, a^\nu g_l(f_1/a, \cdots, f_m/a)$$

are all in $k[\mathbf{x}]$.

$\phi^*(\psi_i)$ is a rational function on V. Note that

$$\psi \circ \phi = (\phi^*(\psi_1), \cdots, \phi^*(\psi_\nu)).$$

It remains to show that there is a nonempty open subset U of V such that for all $\mathbf{c} \in U$, ϕ is regular at $\mathbf{c} \in V$ and ψ is regular at $\phi(\mathbf{c})$. Suppose that $\phi = (f_1/a, \cdots, f_m/a)$ and $\psi = (g_1/b, \cdots, g_\nu/b)$. Set

$$q(\mathbf{x}) = a^l b(f_1/a, \cdots, f_m/a) \in k[\mathbf{x}]$$

for some integer l. Let $U = \mathrm{dom}(\phi) \setminus (\mathbf{V}(a) \cup \mathbf{V}(q))$. We claim that U is nonempty. Otherwise $\mathrm{dom}(\phi) \setminus \mathbf{V}(a) \subseteq \mathbf{V}(q)$. As $\mathrm{dom}(\phi) \setminus \mathbf{V}(a)$ is dense in V, $q(\mathbf{x}) \in \mathbf{I}(V)$. Hence

$$\phi^*(b) = b\left(\frac{f_1 + \mathbf{I}(V)}{a + \mathbf{I}(V)}, \cdots, \frac{f_m + \mathbf{I}(V)}{a + \mathbf{I}(V)}\right) = \frac{q(\mathbf{x}) + \mathbf{I}(V))}{a^l + \mathbf{I}(V)} = 0.$$

As ϕ^* is injective, $b \in \mathbf{I}(W)$, a contradiction. This proves the claim. Obviously, for any $\mathbf{c} \in U$, $\phi(\mathbf{c}) \in \mathrm{dom}(\psi)$. □

A rational map $\phi : V \to W$ is biratinal if it has an inverse rational map, i.e. there is a rational map $\psi : W \to V$ such that $\phi \circ \psi$ and $\psi \circ \phi$ are identity maps on some nonempty open subsets in W and V, respectively.

7.4 Birational equivalence

Let ϕ be a rational map from V to W with

$$\phi = \left(\frac{f_1(\mathbf{x})}{a(\mathbf{x})}, \ldots, \frac{f_m(\mathbf{x})}{a(\mathbf{x})}\right).$$

Put

$$I_\phi = \langle a(\mathbf{x})y_1 - f_1(\mathbf{x}), \ldots, a(\mathbf{x})y_m - f_m(\mathbf{x}), \mathbf{I}(V)\rangle : a(\mathbf{x})^\infty.$$

In the following, we shall use τ_m to denote the projection map from $\bar{k}^{n+m}$ to $\bar{k}^m$ given by $\tau_m((\mathbf{u}, \mathbf{v})) = \mathbf{u}$, and use π_n to denote the projection map from $\bar{k}^{n+m}$ to $\bar{k}^n$ given by $\pi_n((\mathbf{u}, \mathbf{v})) = \mathbf{v}$, where $\mathbf{u} \in \bar{k}^n, \mathbf{v} \in \bar{k}^m$.

Lemma 7.16 *1. I_ϕ is prime;*

2. τ_m is a birational map from $\mathbf{V}(I_\phi)$ to V;

Proof. 1. Suppose that $gh \in I_\phi$. Let s_1, s_2 be two integers such that both $\tilde{g}(\mathbf{x}) := a^{s_1} g(\mathbf{x}, f_1/a, \cdots, f_m/a)$ and $\tilde{h}(\mathbf{x}) := a^{s_2} h(\mathbf{x}, f_1/a, \cdots, f_m/a)$ are in $k[\mathbf{x}]$. Then

$$a^{s_1} g(\mathbf{x}, \mathbf{y}) - \tilde{g}(\mathbf{x}), a^{s_2} h(\mathbf{x}, \mathbf{y}) - \tilde{h}(\mathbf{x}) \in \langle a(\mathbf{x})y_1 - f_1(\mathbf{x}), \ldots, a(\mathbf{x})y_m - f_m(\mathbf{x})\rangle.$$

Since $gh \in I_\phi$, there is an integer l such that

$$a^l gh \in \langle a(\mathbf{x})y_1 - f_1(\mathbf{x}), \ldots, a(\mathbf{x})y_m - f_m(\mathbf{x}), \mathbf{I}(V)\rangle.$$

Thus $a^l \tilde{g}\tilde{h} \in \mathbf{I}(V)$. This implies that either $\tilde{g} \in \mathbf{I}(V)$ or $\tilde{h} \in \mathbf{I}(V)$. Therefore either $g \in I_\phi$ or $h \in I_\phi$. In other words, I_ϕ is prime.

2. It is obvious that τ_m is a rational map from $\mathbf{V}(I_\phi)$ to V. Define a map $\psi : V \to \mathbf{V}(I_\phi)$ given by

$$\psi(\mathbf{c}) = \left(\mathbf{c}, \frac{f_1(\mathbf{c})}{a(\mathbf{c})}, \cdots, \frac{f_m(\mathbf{c})}{a(\mathbf{c})}\right), \mathbf{c} \in V \setminus \mathbf{V}(a).$$

Then ψ is also a rational map. Moreover $\tau_m \circ \psi = \mathbf{id}$ on $V \setminus \mathbf{V}(a)$ and $\psi \circ \tau_m = \mathbf{id}$ on $\mathbf{V}(I_\phi) \setminus \mathbf{V}(\langle a\rangle)$. In the sequel, τ_m is birational. □

Obviously, τ_m is dominant and so is ψ. Hence it induces a homomorphism from $\mathrm{Fr}(k[\mathbf{x}]/\mathbf{I}(V))$ to $\mathrm{Fr}(k[\mathbf{x}, \mathbf{y}]/I_\phi)$. Moreover, we have the following lemma.

Lemma 7.17 *The map $\tau_m^* : \mathrm{Fr}(k[\mathbf{x}]/\mathbf{I}(V)) \to \mathrm{Fr}(k[\mathbf{x}, \mathbf{y}]/I_\phi)$ is isomorphic.*

Corollary 7.18 $\dim(I_\phi) = \dim(\mathbf{I}(V))$.

Let V and W be two irreducible varieties in $\bar{k}^n$ and $\bar{k}^m$, respectively. Assume

$$\phi = \left(\frac{f_1(\mathbf{x})}{a(\mathbf{x})}, \ldots, \frac{f_m(\mathbf{x})}{a(\mathbf{x})}\right) : V \to W$$

and

$$\psi = \left(\frac{g_1(\mathbf{y})}{b(\mathbf{y})}, \ldots, \frac{g_n(\mathbf{y})}{b(\mathbf{y})}\right) : W \to V.$$

Let

$$I_\phi = \langle a(\mathbf{x})y_1 - f_1(\mathbf{x}), \ldots, a(\mathbf{x})y_m - f_m(\mathbf{x}), \mathbf{I}(V)\rangle : a(\mathbf{x})^\infty$$

and

$$J_\psi = \langle b(\mathbf{y})x_1 - g_1(\mathbf{y}), \ldots, b(\mathbf{y})x_n - g_n(\mathbf{y}), \mathbf{I}(W)\rangle : b(\mathbf{y})^\infty.$$

Theorem 7.19 *Let $\phi, \psi, I_\phi, J_\psi$ be as above. The followings are equivalent.*

1. $\psi \circ \phi = \mathrm{id}$ *on some nonempty open subset of* V *and* $\phi \circ \psi = \mathrm{id}$ *on some nonempty open subset of* W*;*
2. $I_\phi = J_\psi$
3. $\phi^* = (\psi^*)^{-1}$.

Proof. (1) $\Rightarrow$ (2). Note that the assertion (1) implies that ϕ and ψ are dominant. Assume that S is a nonempty open subset of V on which $\psi \circ \phi = \mathrm{id}$. Let

$$U = \left\{ \left(\mathbf{c}, \frac{f_1(\mathbf{c})}{a(\mathbf{c})}, \cdots, \frac{f_m(\mathbf{c})}{a(\mathbf{c})} \right) : \mathbf{c} \in S \setminus \mathbf{V}(a) \right\}.$$

One sees that U is dense in $\mathbf{V}(I_\phi)$. Consider the rational map

$$\begin{array}{ccccccc} \mathbf{V}(I_\phi) & \xrightarrow{\tau_m} & V & \xrightarrow{\phi} & W & \xrightarrow{\tau_n^{-1}} & \mathbf{V}(J_\psi) \\ (\mathbf{u}, \mathbf{v}) & \longrightarrow & \mathbf{u} & \longrightarrow & \phi(\mathbf{u}) & \longrightarrow & (\psi \circ \phi(\mathbf{u}), \phi(\mathbf{u})) \end{array}$$

where $(\mathbf{u}, \mathbf{v}) \in U$. It is easy to verify that $\phi(\mathbf{u}) = \mathbf{v}$ for any $(\mathbf{u}, \mathbf{v}) \in U$. Since $\psi \circ \phi(\mathbf{u}) = \mathbf{u}$ for all $\mathbf{u} \in S$, $\tau_n^{-1} \circ \phi \circ \tau_m$ is an identity map on U. Thus $U \subset \mathbf{V}(I_\psi)$ and then $\mathbf{V}(I_\phi) \subset \mathbf{V}(I_\psi)$. By Lemma 7.16, I_ϕ is prime. So $I_\psi \subset I_\phi$. Similarly, one can show that $J_\phi \subset I_\psi$.

(2) $\Rightarrow$ (1). Consider the map

$$\begin{array}{ccccc} V & \xrightarrow{\tau_m^{-1}} & \mathbf{V}(I_\phi) = \mathbf{V}(J_\psi) & \xrightarrow{\tau_n} & W \\ \mathbf{u} & \longrightarrow & (\mathbf{u}, \phi(\mathbf{u})) & \longrightarrow & \phi(\mathbf{u}). \end{array}$$

One has that $\phi = \pi_n \circ \tau_m^{-1}$ on $V \setminus \mathbf{V}(a)$. Similarly, one has that $\psi = \tau_m \circ \pi_n^{-1}$ on $W \setminus \mathbf{V}(b)$. This implies that (1) holds.

(2) $\Rightarrow$ (3). Consider the map

$$\begin{array}{ccccc} \mathrm{Fr}(k[\mathbf{y}]/\mathbf{I}(W)) & \xrightarrow{\tau_n^*} & \mathrm{Fr}(k[\mathbf{x}, \mathbf{y}]/J_\psi) = \mathrm{Fr}(k[\mathbf{x}, \mathbf{y}]/I_\phi) & \xrightarrow{(\tau_m^{-1})^*} & \mathrm{Fr}(k[\mathbf{x}]/\mathbf{I}(V)) \\ y_j + \mathbf{I}(W) & \longrightarrow & y_j + J_\psi = y_j + I_\phi & \longrightarrow & \frac{f_j + \mathbf{I}(V)}{a + \mathbf{I}(V)}. \end{array}$$

Hence $\phi^* = (\pi_m^*)^{-1} \circ \tau_n^*$. Similarly, one has that $\psi^* = (\tau_n^*)^{-1} \circ {\pi_m}^*$. Thus (3) holds.

(3) $\Rightarrow$ (2).

□

Let $f \in k[\mathbf{x}] \setminus k$. We shall call $\mathbf{V}(f)$ a hypersurface of $\bar{k}^n$. We say V and W are birationally equivalent if there is a birational map from V to W.

Proposition 7.20 *Assume that V is an irreducible variety in $\bar{k}^n$. Then V is birationally equivalent to a hypersurface in $\bar{k}^m$ for some $m \in \mathbf{N}$.*

Proof. Since V is irreducible, $\mathbf{I}(V)$ is prime. Denote by K the quotient field of $k[\mathbf{x}]/\mathbf{I}(V)$. Write $\bar{x}_i = x_i + \mathbf{I}(V)$ for $i = 1, \cdots, n$. Then $K = k(\bar{x}_1, \cdots, \bar{x}_n)$. Let $d = \dim(V)$. Without loss of generality, assume that $\bar{x}_1, \cdots, \bar{x}_d$ are algebraically independent over k. Then K is a finite algebraic extension of $k(\bar{x}_1, \cdots, \bar{x}_d)$. By the primitive element theorem, there is $\eta \in K$ such that $K = k(\bar{x}_1, \cdots, \bar{x}_d, \eta)$. Let $P \in k[y_1, \cdots, y_d, y_{d+1}]$ be an irreducible polynomial satisfying that $P(\bar{x}_1, \cdots, \bar{x}_d, \eta) = 0$. Then $\mathbf{V}(P)$ is a hypersurface in $\bar{k}^{d+1}$. We shall show that V is birationally equivalent to $\mathbf{V}(P)$. It suffices to show that L is k-isomorphic to K where L is the quotient field of $k[y_1, \cdots, y_{d+1}]/\langle P \rangle$. Define a k-homomorphism $\psi : k[y_1, \cdots, y_{d+1}] \to K$ by $\psi(y_i) = \bar{x}_i$ for $i = 1, \cdots, d$ and $\psi(y_{d+1}) = \eta$. Then $\ker(\psi) = \langle P \rangle$. The map ψ induces a k-homomorphism from L to K and one can easily see that it is surjective. □

7.5 Constructible sets

Let C be a subset of $\bar{k}^n$. We call C a constructible set if there are finitely many varieties $U_1, \cdots, U_l, V_1, \cdots, V_l$ of $\bar{k}^n$ such that

$$C = \cup_{i=1}^{l} (U_i \setminus V_i).$$

A constructible set of the form $U \setminus V$ is called a principle constructible set. One can easily verify the following properties of constructible sets.

Proposition 7.21 *(1) The intersection of finitely many constructible sets is again a constructible set;*

(2) The complement of a constructible set is a constructible set.

Proposition 7.22 *A constructible set can be written as the disjoint union of finitely many principle constructible sets.*

Proof. Assume that $C = \cup_{i=1}^{l} U_i \setminus V_i$ is a constructible set. We shall show the proposition by induction on l. If $l = 1$, there is nothing to prove. Suppose that the assertion holds for $l - 1$. Let $W_i = U_1 \cap U_i$ for all $i = 2, \cdots, l$, $S = \cup_{i=2}^{l} (V_1 \cap W_i) \setminus V_i$ and $T = \cup_{i=2}^{l} U_i \setminus (V_i \cup W_i)$. One can easily verify

that $U_1 \setminus V_1, S, T$ have empty intersections pairwise. In the following, we shall show that

$$C = (U_1 \setminus V_1) \cup S \cup T.$$

Obviously, the right hand side is a subset of C. Suppose that $\mathbf{c} \in C$, i.e. $\mathbf{c} \in U_i \setminus V_i$ for some i. If $\mathbf{c} \in U_1 \setminus V_1$, there is nothing to prove. Assume that $\mathbf{c} \notin U_1 \setminus V_1$. If $\mathbf{c} \notin W_i$, then $\mathbf{c} \in U_i \setminus (V_i \cup W_i)$, which is a subset of T. Otherwise, $\mathbf{c} \in U_1$ and so $\mathbf{c} \in U_1 \cap U_i \cap V_1 = W_i \cap V_1$. On the other hand, $\mathbf{c} \notin V_i$, which implies that $\mathbf{c} \in (V_1 \cap W_i) \setminus V_i$, a subset of S. Hence C is equal to the right hand side. The application of the induction hypothesis to S and T completes the proof. □

Let ϕ be a regular map from $\bar{k}^n$ to $\bar{k}^m$. We are going to prove that the image of a constructible set under ϕ is again a constructible set. We start with the case that ϕ is a projection.

Lemma 7.23 *Let I be a proper ideal of $k[\mathbf{x}]$. Then*

$$\dim(I^{(1)}) \leq \dim(I) \leq \dim(I^{(1)}) + 1.$$

Moreover if I is prime then $\dim(I) = \dim(I^{(1)}) + 1$ if and only if $I = \langle I^{(1)} \rangle$.

Proof. Suppose that S is a subset of $\{x_2, \cdots, x_n\}$ which is independent modulo $I^{(1)}$. In other words, $I^{(1)} \cap k[S] = 0$. Then

$$I \cap k[S] = I \cap k[x_2, \cdots, x_n] \cap k[S] = I^{(1)} \cap k[S] = 0.$$

This implies that S is independent modulo I. Thus $\dim(I) \geq \dim(I^{(1)})$. Now assume that S is a subset of $\mathbf{x}$ independent modulo I. It is easy to see that $S \setminus \{x_1\}$ is independent modulo $I^{(1)}$. Therefore $\dim(I) \leq \dim(I^{(1)}) + 1$.

Consider the homomorphism $\psi : k[x_2, \cdots, x_n] \to k[\mathbf{x}]/I$ given by $\psi(x_i) = x_i + I$ for $i = 2, \cdots, n$. Then $\ker(\psi) = I^{(1)}$. Let E be the quotient field of $k[x_2, \cdots, x_n]/I^{(1)}$ and K the quotient field of $k[\mathbf{x}]/I$. The map ψ induces an embedding of E into K. Write $\bar{x}_i = x_i + I$. Then $K = k(\bar{x}_1, \cdots, \bar{x}_n)$ and $\psi(E) = k(\bar{x}_2, \cdots, \bar{x}_n)$. It is easy to see that $\dim(I) = \dim(I^{(1)}) + 1$ if and only if $\bar{x}_1$ is transcendental over E. If $I \setminus \langle I^{(1)} \rangle \neq \emptyset$, then there is $f \in I \setminus \langle I^{(1)} \rangle$. Write $f = \sum_{i=1}^{l} a_i x_1^i$ where $a_i \in k[x_2, \cdots, x_n]$. As $f \notin \langle I^{(1)} \rangle$, not all of $a_i + I$ are zero, otherwise $a_i \in I^{(1)}$ for all i. Then the equality $\sum_{i=1}^{l} (a_i + I)\bar{x}_1^i = 0$ implies that $\bar{x}_1$ is algebraic over E. Conversely, assume that $\bar{x}_1$ is algebraic over E. In other words, there are $a_0, \cdots, a_l \in k[x_2, \cdots, x_n]$, not all in I, such that $\sum_{i=1}^{l} (a_i + I)\bar{x}_1^i = 0$. This means that $\sum_{i=1}^{l} a_i x_1^i \in I$. Since not all a_i are in I, $\sum_{i=1}^{l} a_i x_1^i \notin \langle I^{(1)} \rangle$. Hence $I \neq \langle I^{(1)} \rangle$. Consequently, $\bar{x}_1$ is algebraic over E if and only if $I \neq \langle I^{(1)} \rangle$. □

Lemma 7.24 *Let P be a proper prime ideal of $k[\mathbf{x}]$ satisfying that $P \neq \langle P^{(1)} \rangle$. Let $f \in k[\mathbf{x}] \setminus P$. Then*

$$P^{(1)} \subsetneqq (P + \langle f \rangle) \cap k[x_2, \cdots, x_n].$$

Proof. Let $Q = P + \langle f \rangle$. By Corollary 5.10, $\dim(Q) = \dim(P) - 1$. Suppose that $Q^{(1)} = P^{(1)}$. Then by Lemma 7.23

$$\dim(Q^{(1)}) = \dim(P^{(1)}) = \dim(P) > \dim(Q).$$

However Lemma 7.23 implies that $\dim(Q) \geq \dim(Q^{(1)})$, a contradiction. □

Proposition 7.25 *Let V be a nonempty irreducible variety of $\bar{k}^n$ and $I = \mathbf{I}(V)$. Let W be a proper subvariety of V. Then there is a proper subvariety U of $\mathbf{V}(I^{(m)})$ such that*

$$\mathbf{V}(I^{(m)}) \setminus U \subset \pi_m(V \setminus W)$$

where $0 < m < n$.

Proof. We shall use the induction on m. We first show the case $m = 1$. Since $W \nsubseteq V$, there is a polynomial f in $\mathbf{I}(W) \setminus I$. We have two cases.

Case 1: $I = \langle I^{(1)} \rangle$. In this case, for any $(c_2, \cdots, c_n) \in \mathbf{V}(I^{(1)})$, $(c_1, \cdots, c_n) \in V$ for all $c_1 \in \bar{k}$. Write $f = \sum_{i=0}^{l} a_i x_1^i$ where $a_i \in k[x_2, \cdots, x_n]$. Let $U = \mathbf{V}(I^{(1)}) \cap \mathbf{V}(a_0, \cdots, a_l)$. Then U is a proper subvariety of $\mathbf{V}(I^{(1)})$. Otherwise, $a_i \in I^{(1)}$ for all $i = 0, \cdots, l$ and then $f \in \langle I^{(1)} \rangle = I$. Now assume that $(c_2, \cdots, c_n) \in \mathbf{V}(I^{(1)}) \setminus U$. Then $f(x_1, c_2, \cdots, c_n)$ is a nonzero polynomial. So there is $c_1 \in \bar{k}$ such that $f(c_1, \cdots, c_n) \neq 0$, i.e. $(c_1, \cdots, c_n) \notin W$. While $(c_1, \cdots, c_n) \in V$. Therefore $(c_2, \cdots, c_n) \in \pi_1(V \setminus W)$.

Case 2: $I \neq \langle I^{(1)} \rangle$. Let $h \in I \setminus \langle I^{(1)} \rangle$. Write $h = \sum_{i=0}^{s} b_i x_1^i$. Without loss of generality, we may assume that $b_s \notin I^{(1)}$. Otherwise, one can replace h by $h - b_s x_1^s$. By Lemma 7.24, there is $v \in k[x_2, \cdots, x_n]$ such that $v \in (I + \langle f \rangle) \setminus I^{(1)}$. Note that $I^{(1)}$ is prime. So $b_s v \notin I^{(1)}$. Let $U = \mathbf{V}(v b_s) \cap \mathbf{V}(I^{(1)})$. Then U is a proper subvariety of $\mathbf{V}(I^{(1)})$. Now assume that $(c_2, \cdots, c_n) \in \mathbf{V}(I^{(1)}) \setminus U$. By Proposition 2.6, there is $c_1 \in \bar{k}$ such that $(c_1, \cdots, c_n) \in V$. On the other hand, $(c_1, \cdots, c_n) \notin W$. Otherwise $f(c_1, \cdots, c_n) = 0$ and then $v(c_2, \cdots, v_n) = 0$, a contradiction. Therefore $(c_1, \cdots, c_n) \in V \setminus W$ and so $(c_2, \cdots, c_n) \in \pi_1(V \setminus W)$.

Now assume that the assertion holds for $m - 1$. By the base case, one has

$$\mathbf{V}(I^{(1)}) \setminus U \subset \pi_1(V \setminus W).$$

Note that $I^{(1)}$ is irreducible. By the induction hypothesis, there is a proper subvariety $\tilde{U}$ of $\mathbf{V}(I^{(m)})$ such that

$$\mathbf{V}(I^{(m)}) \setminus \tilde{U} \subset \pi_{m-1}(\mathbf{V}(I^{(1)}) \setminus U).$$

While one has $\pi_{m-1}(\mathbf{V}(I^{(1)}) \setminus U) \subset \pi_{m-1}(\pi_1(V \setminus W)) = \pi_m(V \setminus W)$. Hence

$$\mathbf{V}(I^{(m)}) \setminus \tilde{U} \subset \pi_m(V \setminus W).$$

□

Corollary 7.26 *Let V be a nonempty variety of $\bar{k}^n$ and $I = \mathbf{I}(V)$. Then there is a proper subvariety U of $\mathbf{V}(I^{(m)})$ such that*

$$\mathbf{V}(I^{(m)}) \setminus U \subset \pi_m(V)$$

where $0 < m < n$.

Proof. Let $I = P_1 \cup P_2 \cup \cdots \cup P_l$ be the minimal prime decomposition of I. By Proposition 7.25, there are varieties U_i such that $U_i \subsetneqq \mathbf{V}(P_i^{(m)})$ and

$$\mathbf{V}(P_i^{(m)}) \setminus U_i \subset \pi_m(\mathbf{V}(P_i)).$$

Then

$$\cup_{i=1}^{l}(\mathbf{V}(P_i^{(m)}) \setminus U_i) \subset \cup_{i=1}^{l}\pi_m(\mathbf{V}(P_i)) = \pi_m(V).$$

Observe that $\mathbf{V}(I^{(m)}) = \cup_{i=1}^{l}\mathbf{V}(P_i^{(m)})$. Let $U = \cup_{i=1}^{l}U_i$. We claim that $U \subsetneqq \mathbf{V}(I^{(m)})$. Since U_i is a proper subvariety of $\mathbf{V}(P_i^{(m)})$ and $\mathbf{V}(P_i^{(m)})$ is irreducible, $\dim(\mathbf{V}(P_i^{(m)})) > \dim(U_i)$. This implies that

$$\dim(\mathbf{V}(I^{(m)})) = \max_{i=1}^{l}\{\mathbf{V}(P_i^{(m)})\} > \max_{i=1}^{l}\{U_i\} = \dim(U).$$

This proves the claim. Now one has

$$\mathbf{V}(I^{(m)}) \setminus U \subset \cup_{i=1}^{l}(\mathbf{V}(P_i^{(m)}) \setminus U) \subset \cup_{i=1}^{l}(\mathbf{V}(P_i^{(m)}) \setminus U_i) \subset \pi_m(V).$$

□

Proposition 7.27 *Let V be a variety of $\bar{k}^n$. Then $\pi_m(V)$ is a constructible set where $0 < m < n$.*

Proof. Suppose that $V = \emptyset$. Then there is nothing to prove. Assume that $V \neq \emptyset$ and $I_0 = \mathbf{I}(V)$. By Corollary 7.26, there is a proper subvariety of $\mathbf{V}(I_0^{(m)})$, say U_0, such that $\mathbf{V}(I_0^{(m)}) \setminus U_0 \subset \pi_m(V)$. Let

$$V_1 = \mathbf{V}\left(I_0 + \langle \mathbf{I}(U_0) \rangle\right).$$

Then $V_1 \subset V$. It is easy to see $\pi_m(V_1) \subset U_0$. If $V_1 = V$, then $\pi_m(V) = \pi_m(V_1) \subset U_0$, which is impossible. Thus $V_1 \subsetneqq V$. For any $\mathbf{c} \in V$. If $\pi_m(\mathbf{c}) \notin \mathbf{V}(I_0^{(m)}) \setminus U_0$, then $\pi_m(\mathbf{c}) \in U_0$. So $\mathbf{c} \in V_1$. In the sequel, $\pi_m(\mathbf{c}) \in \pi_m(V_1)$. Therefore $\pi_m(V) = \pi_m(V_1) \cup (\mathbf{V}(I_0^{(m)}) \setminus U_0)$. Now if $V_1 = \emptyset$. We are done. Suppose that $V_1 \neq \emptyset$. Let $I_1 = \mathbf{I}(V_1)$. By Corollary 7.26, there is a proper subvariety U_1 of $\mathbf{V}(I_1^{(m)})$ such that $\mathbf{V}(I_1^{(m)}) \setminus U_1 \subset \pi_m(V_1)$. Repeating the above construction, we get a variety V_2 such that $V_2 \subsetneqq V_1$ and

$$\pi_m(V) = \pi_m(V_2) \cup (\mathbf{V}(I_1^{(m)}) \setminus U_1) \cup (\mathbf{V}(I_0^{(m)}) \setminus U_0).$$

If $V_2 = \emptyset$, we are done. If not, repeat the above process. Continuing in this way, we eventually have $V_s = \emptyset$ for some $s > 0$. Otherwise, we get a sequences of varieties

$$V \supsetneqq V_1 \supsetneqq V_2 \supsetneqq \cdots$$

which would contradict the Noetherian property of varieties. Once we have $V_s = \emptyset$, we obtain the desired form for $\pi_m(V)$. □

Now we are ready to prove the general case.

Theorem 7.28 *Let $\phi : \bar{k}^n \to \bar{k}^m$ be a regular map. If C is a constructible set of $\bar{k}^n$, then $\phi(C)$ is a constructible set of $\bar{k}^m$.*

Proof. It suffices to show the theorem for the case that C is a principle constructible set. Assume that $C = U \setminus V$ where U, V are varieties of $\bar{k}^n$ and $U \setminus V \neq \emptyset$. Suppose that $\mathbf{I}(U) = \langle f_1, \cdots, f_s \rangle$ and $\mathbf{I}(V) = \langle g_1, \cdots, g_l \rangle$ where $f_i, g_j \in k[\mathbf{x}]$. We further assume that $\phi = (h_1, \cdots, h_m)$ where $h_i \in k[\mathbf{x}]$. Let J be the ideal in $k[\mathbf{x}, \mathbf{y}, \mathbf{z}]$ generated by

$$f_1, \cdots, f_s, \prod_{i=1}^{l}(y_i g_i - 1), z_1 - h_1, \cdots, z_m - h_m.$$

We claim that $\pi_{s+l}(\mathbf{V}(J)) = \phi(C)$. Assume that $\mathbf{c} \in \pi_{s+l}(\mathbf{V}(J))$. Then there are $\mathbf{a} \in \bar{k}^n, \mathbf{b} \in \bar{k}^l$ such that $(\mathbf{a}, \mathbf{b}, \mathbf{c}) \in \mathbf{V}(J)$. This implies that

$$\prod_{i=1}^{l}(b_i g_i(\mathbf{a}) - 1) = 0$$

where $\mathbf{b} = (b_1, \cdots, b_l)$. So $g_i(\mathbf{a}) \neq 0$ for some i and thus $\mathbf{a} \notin V$. In the sequel, $\mathbf{a} \in C$. Therefore $\mathbf{c} \in \phi(C)$ since $\mathbf{c} = \phi(\mathbf{a})$. Now suppose that $\mathbf{c} \in \phi(C)$, i.e. there is $\mathbf{a} \in C$ such that $\mathbf{c} = \phi(\mathbf{a})$. Because $\mathbf{a} \notin V$, one has $g_i(\mathbf{a}) \neq 0$ for some i. Let $\mathbf{b} = (0, \cdots, 0, 1/g_i(\mathbf{a}), 0, \cdots, 0)$. Then it is easy to see that $(\mathbf{a}, \mathbf{b}, \mathbf{c}) \in \mathbf{V}(J)$. Hence $\mathbf{c} \in \pi_{s+l}(\mathbf{V}(J))$. This proves the claim. The theorem then follows from Proposition 7.27. □

Chapter 8

Projective Algebraic Geometry

In this chapter, $\mathbf{x}$ denotes $\{x_0, x_1, \cdots, x_n\}$.

8.1 Projective varieties and homogeneous ideals

We define an equivalence relation in $\bar{k}^{n+1} \setminus \{0\}$. Two elements $\mathbf{a}, \mathbf{b} \in \bar{k}^{n+1} \setminus \{0\}$ are equivalent if there is a nonzero element $\lambda \in \bar{k}$ such that $\mathbf{a} = \lambda \mathbf{b}$. Denote this equivalence relation by $\backsim$ and denote

$$\mathbb{P}^n(\bar{k}) = \bar{k}^{n+1} \setminus \{0\} / \backsim .$$

We call $\mathbb{P}^n(\bar{k})$ a n-dimension projective space. Let $f \in k[\mathbf{x}]$. Let $\mathbf{c} \in \bar{k}^{n+1} \setminus \{0\}$. Then $\mathbf{c}$ defines a point $\mathbf{p}$ of $\mathbb{P}^n(\bar{k})$. We call $\mathbf{c}$ a homogeneous coordinate of $\mathbf{p}$. Write

$$f = \sum_{i=s}^{m} \sum_{|\mathbf{u}|=i} c_{\mathbf{u}} \mathbf{x}^{\mathbf{u}}$$

where $\mathbf{u} \in \mathbf{N}^{n+1}$ and $c_{\mathbf{u}} \in k$. We call $\sum_{|\mathbf{u}|=i} c_{\mathbf{u}} \mathbf{x}^{\mathbf{u}}$ the i-th homogeneous component of f. If f is equal to the i-th homogeneous component of f for some $i \in \mathbf{N}$, then we call f a homogeneous polynomial.

Proposition 8.1 *Let $f \in k[\mathbf{x}]$ be a homogeneous polynomial and $\mathbf{c} \in \bar{k}^{n+1} \setminus \{0\}$. If $f(\mathbf{c}) = 0$, then $f(\lambda \mathbf{c}) = 0$ for all $\lambda \in \bar{k}$.*

The proposition allows one to define a subset of $\mathbb{P}^n(\bar{k})$ by homogeneous polynomials. A subset V of $\mathbb{P}^n(\bar{k})$ is called a projective variety if there is a subset P of $k[\mathbf{x}]$ consisting of homogeneous polynomials such that

$$V = \{\mathbf{p} \in \mathbb{P}^n(\bar{k}) | f(\mathbf{p}) = 0, \ \forall \ f \in P\}$$

where $f(\mathbf{p}) = 0$ means $f(\mathbf{c}) = 0$ for any homogeneous coordinate $\mathbf{c}$ of $\mathbf{p}$.

An ideal I of $k[\mathbf{x}]$ is said to be homogeneous if for each $f \in I$ then the homogeneous components of f are in I as well.

Theorem 8.2 *Let I be an ideal of $k[\mathbf{x}]$. Then the following are equivalent.*

(1) I is homogeneous.

(2) $I = \langle f_1, \cdots, f_m \rangle$ where $f_1, \cdots, f_m$ are homogeneous.

(3) A reduced Gröbner basis of I (with respect to any monomial order) consists of homogeneous polynomials.

As a result of the above theorem, it makes sense to define the following subset of $\mathbb{P}^n(\bar{k})$ for a homogeneous ideal I

$$\mathbf{V}_p(I) = \left\{\mathbf{p} \in \mathbb{P}^n(\bar{k}) | f(\mathbf{p}) = 0, \ \forall \ f \in I\right\}.$$

Conversely, let V be a subset of $\mathbb{P}^n(\bar{k})$ and define

$$\mathbf{I}(V) = \{f \in k[\mathbf{x}] | f(\mathbf{p}) = 0, \ \forall \ \mathbf{p} \in V\}$$

where $f(\mathbf{p}) = 0$ means for all homogeneous coordinate $\mathbf{c}$ of $\mathbf{p}$, $f(\mathbf{c}) = 0$.

Proposition 8.3 $\mathbf{I}(V)$ *is a homogeneous ideal of $k[\mathbf{x}]$.*

Proposition 8.4 *If I is a homogeneous ideal, then so is $\sqrt{I}$.*

Proof. Suppose on the contrary that $\sqrt{I}$ is not homogeneous. In other words, there is a polynomial $f \in \sqrt{I}$ satisfying one of its homogeneous components is not in $\sqrt{I}$. Let $m = \deg(f)$. Without loss of generality, we may assume that the m-th homogeneous component of f is not in $\sqrt{I}$. Write $f = f_m + \bar{f}$ where f_m is the m-th homogeneous component of f and $\bar{f} = f - f_m$. There is an integer $s > 0$ such that

$$f^s = (f_m + \bar{f})^s = f_m^s + \tilde{f} \in I.$$

One easily sees that f_m^s is the ms-homogeneous component of f^s. Thus $f_m^s \in I$ for I is homogeneous. This implies that $f_m \in \sqrt{I}$, a contradiction. □

Theorem 8.5 *Let I be a homogeneous ideal of $k[\mathbf{x}]$. Then the following are equivalent.*

(1) $\mathbf{V}_p(I) \neq \emptyset$.

(2) Let G be a reduced Gröbner basis of I. Then for each $0 \leq i \leq n$, there is a $g \in G$ such that $\mathrm{lm}(g) = x_i^{m_i}$ for some $m_i \geq 0$.

(3) For each $0 \leq i \leq n$, there is an integer $m_i \geq 0$ such that $x_i^{m_i} \in I$.

(4) There is an integer $s \geq 1$ such that $\langle x_0, x_1, \cdots, x_n \rangle^s \subset I$.

Proof. (2) $\Rightarrow$ (1) Suppose that we have a reduced Gröbner basis G of I satisfying that for each $0 \leq i \leq n$, there is $g \in G$ such that $\mathrm{lm}(g) = x_i^{m_i}$ for some $m_i \geq 0$. By Theorem 4.14, $\mathbf{V}(I)$ is finite. But assume that there is a point $\mathbf{p} \in \mathbf{V}_p(I)$. Let $\mathbf{c}$ be a homogeneous coordinate of $\mathbf{p}$. Then $\lambda\mathbf{c} \in \mathbf{V}(I)$ for all $\lambda \in \bar{k}$ and hence $\mathbf{V}(I)$ is infinite. This contradiction implies that $\mathbf{V}_p(I)$ is empty.

(3) $\Rightarrow$ (2) Obviously.

(4) $\Rightarrow$ (3) Obviously.

(1) $\Rightarrow$ (4) If $\mathbf{V}(I)$ contains a nonzero point of $\bar{k}^{n+1}$, then this point will define a point of $\mathbf{V}_p(I)$, which would contradict $\mathbf{V}_p(I) = \emptyset$. Hence $\mathbf{V}(I) \subset \{(0, \cdots, 0)\}$, which implies that $\langle x_0, x_1, \cdots, x_n \rangle \subset \sqrt{I}$. So for a sufficiently large s, $\langle x_0, x_1, \cdots, x_n \rangle^s \subset I$. □

Lemma 8.6 *Let I be a homogeneous ideal of $k[\mathbf{x}]$. If $\mathbf{V}_p(I) \neq \emptyset$, then $\sqrt{I} \subset \langle x_0, x_1, \cdots, x_n \rangle$.*

Proof. Suppose that $f \in I$. Let f_0 be the 0-th homogeneous component of f. Then $f_0 \in I$ since I is homogeneous. If $f_0 \neq 0$, then $I = k[\mathbf{x}]$ and so $\mathbf{V}_p(I) = \emptyset$, a contradiction. Thus $f_0 = 0$ for all $f \in I$. This implies that $I \subset \langle x_0, x_1, \cdots, x_n \rangle$ and hence $\sqrt{I} \subset \langle x_0, x_1, \cdots, x_n \rangle$. □

Theorem 8.7 *Let I be a homogeneous ideal of $k[\mathbf{x}]$. If $\mathbf{V}_p(I)$ is nonempty, then $\mathbf{I}(\mathbf{V}_p(I)) = \sqrt{I}$.*

Proof. We claim that if $\mathbf{V}_p(I) \neq \emptyset$ then $\mathbf{I}(\mathbf{V}(I)) = \mathbf{I}(\mathbf{V}_p(I))$. Suppose that $f \in \mathbf{I}(\mathbf{V}(I))$ and $\mathbf{p} \in \mathbf{V}_p(I)$. Let $\mathbf{c}$ be any homogeneous coordinate of $\mathbf{p}$. Then $\mathbf{c} \in \mathbf{V}(I)$ and so $f(\mathbf{c}) = 0$. Hence $f(\mathbf{p}) = 0$, which implies that $f \in \mathbf{I}(\mathbf{V}_p(I))$. Conversely, suppose that $f \in \mathbf{I}(\mathbf{V}_p(I))$. Since $\mathbf{V}_p(I) \neq \emptyset$, $\mathbf{V}(I) \neq \emptyset$. Now for any $\mathbf{c} \in \mathbf{V}(I)$, if $\mathbf{c}$ is not zero, then $\mathbf{c}$ defines a point of $\mathbf{V}_p(I)$ and hence $f(\mathbf{c}) = 0$. Furthermore $f(\lambda\mathbf{c}) = 0$ for all $\lambda \in \bar{k} \setminus \{0\}$.

From this, one easily sees that the 0-th homogeneous component of f is zero. Therefore $f(0) = 0$. So for any $\mathbf{c} \in \mathbf{V}(I)$, $f(\mathbf{c}) = 0$. Thus $f \in \mathbf{I}(\mathbf{V}(I))$. This proves the claim. Now by Theorem 2.12,

$$\sqrt{I} = \mathbf{I}(\mathbf{V}(I)) = \mathbf{I}(\mathbf{V}_p(I)).$$

□ Denote by

$\mathcal{P} = \{\text{nonempty projective varieties}\}$

$\mathcal{R} = \{\text{radical homogeneous ideals properly contained in } \langle x_0, \cdots, x_n \rangle\}$

Then we have the following bijective maps.

$$\mathbf{I} : \mathcal{P} \to \mathcal{R}, \qquad \mathbf{V}_p : \mathcal{R} \to \mathcal{P}.$$

Bibliography

[1] L. M. Berkovich and V. G. Tsirulik. Differential Resultants and Some of Their Applications. In *Differential'nye Uravneniya* **22**(5), 750–757, 1986.

[2] M. Bronstein and M. Petkovšek. On Ore Rings, Linear Operators and Factorization. *Programming and Comput. Software* **20**, 14–26, 1994.

[3] W. S. Brown. On Euclid's Algorithm and the Computation of Polynomial Greatest Common Divisors. *JACM* **18**, 478–504, 1971.

[4] W. S. Brown and J. F. Traub. On Euclid's Algorithm and the Theory of Subresultants. *JACM* **18**, 505–514, 1971.

[5] M. Chardin. Differential Resultants and Subresultants. In *Proceedings of Fundamentals of Computation Theory, Lecture Notes in Computer Science* **529**, 180–189, 1991.

[6] F. Chyzak. Holonomic Systems and Automatic Proofs of Identities. *Research report*, INRIA, Centre de Diffusion, BP 105–78153 Le Chesnay Cedex, France, 1994.

[7] R. M. Cohn. *Difference Algebra*. Interscience Publishers. 1965.

[8] G. E. Collins. Polynomial Remainder Sequences and Determinants. *American Mathematical Monthly* **73**(7), 709–712, 1966.

[9] G. E. Collins. Subresultant and Reduced Polynomial Remainder Sequences. *JACM* **16**, 708–712, 1967.

[10] G. E. Collins. The Calculation of Multivariate Polynomial Resultants. *JACM* **18**, 515–532, 1971.

[11] G. E. Collins. Quantifier Elimination for the Elementary Theory of Real Closed Fields by Cylindrical Algebraic Decomposition. In *Automata Theory and Formal Languages, 2nd GI Conference, Lecture Note in Computer Science* **33**, 234–183, Berlin, Springer-Verlag, 1975.

[12] G. E. Collins and M. J. Encarnación. Efficient Rational Number Reconstruction. *Technical Report*, no. 94-64, RISC-Linz, Johannes Kepler University, A-4040, Austria. To appear in *Journal of Symbolic Computation.*

[13] G. E. Collins and R. Loos. Real Zeros of Polynomials. In B. Buchberger, G. E. Collins, and R. Loos (eds.), *Computer Algebra, Symbolic and Algebraic Computation,* 83–94. Springer-Verlag, Wien-New York, 1982.

[14] M. J. Encarnación. On a Modular Algorithm for Computing Gcds of Polynomials over Algebraic Number Fields. In *Proceedings of the 1994 International Symposium on Symbolic and Algebraic Computation*, 58–65, ACM Press, 1994.

[15] M. J. Encarnación. *Faster Algorithms for Reconstructing Rationals, Computing Polynomial GCDs, and Factoring Polynomials.* Ph.D. Thesis, RISC-Linz, Johannes Kepler University, A-4040, Linz, Austria. 1995.

[16] K. O. Geddes, S. R. Czapor, and G. Labahn. *Algorithms for Computer Algebra.* Kluwer Academic Publishers. 1992.

[17] L. Gonzàlez-Vega. Determinantal Formula for the Solution Set of Zero-Dimensional Ideals. *Journal of Pure and Applied Algebra* **76**, 57–80, 1991.

[18] D. Yu. Grigor'ev. Complexity of Factoring and Calculating the GCD of Linear Ordinary Differential Operators. *Journal of Symbolic Computation* **10**(1), 7–37, 1990.

[19] J. Johnson. Private Communication, 1994

[20] D. E. Knuth. *The Art of Computer Programming* **2**. Addison-Wesley. 1981.

[21] E. R. Kolchin. *Differential Algebra and Algebraic Groups.* Pure and Applied Math **54**. Academic Press, New York-London, 1973.

[22] T. Y. Lam. *A First Course in Non-commutative Rings*. Graduate Texts in Mathematics **131**, Springer-Verlag. 1991.

[23] Z. Li. An Implementation of the Characteristic Set Method for Solving Algebraic Equations. *Technical Report,* no. 94-86, RISC-Linz, Johannes Kepler University, A-4040, Linz, Austria, 1994.

[24] Z. Li. A Subresultant Theory for Linear Ordinary Differential Polynomials, *Technical Report*, no. 95-35, RISC-Linz, Johannes Kepler University, A-4040, Linz, Austria, 1995.

[25] Z. Li and I. Nemes. A Modular Algorithm for Computing Greatest Common Right Divisors of Ore Polynomials. Submitted to *the 1996 International Symposium on Symbolic and Algebraic Computation.*

[26] R. Loos. Generalized Polynomial Remainder Sequence. In B. Buchberger, G. E. Collins, and R. Loos (eds.), *Computer Algebra, Symbolic and Algebraic Computation,* 115–137. Springer-Verlag, Wien-New York, 1982.

[27] A. M. Mandache. The Gröbner Basis Algorithm and Subresultant Theory. In *Proceedings of the 1994 International Symposium on Symbolic and Algebraic Computation*, 20–23, ACM Press, 1994.

[28] A. M. Mandache. *Gröbner Bases Computation and Gaussian Elimination.* Ph.D. Thesis, RISC-Linz, Johannes Kepler University, A-4040, Linz, Austria. 1995.

[29] L. M. Milne-Thomson. *The Calculus of Finite Differences.* Macmillan & Co. Ltd. 1960.

[30] D. Manocha and J. F. Canny. Algorithm for Implicitizing Rational Parametric Surfaces. *Journal of Computer Aided Geometric Design* **9**, 25–50, 1992.

[31] D. Manocha and J. F. Canny. Implicit Representations of Rational Parametric Surfaces. *Journal of Symbolic Computation* **13**(5) 485–510, 1992.

[32] B. Mishra. *Algorithmic Algebra.* Texts and Monographs in Computer Science, D. Gries D and F. B. Schneider (eds.), Springer-Verlag. 1993.

[33] O. Ore. Theory of Non-Commutative Polynomials. *Annals of Math* **34**, 480–508, 1933.

[34] Peter Paule and Volker Strehl. Symbolic Summation – Some Recent Developments. *Technical Report,* no. 95-11, RISC-Linz, Johannes Kepler University, Linz, A-4040, Austria. To appear in *Computer Algebra in Science and Engineering*, J. Fleascher, J. Grabmeier, F. Hehl, and W. Wüchlin (eds.), World Scientific, Singapore.

[35] E. G. C. Poole. *Introduction to the Theory of Linear Ordinary Differential Equations.* Dover Publications Inc., New York. 1936.

[36] J. F. Ritt. *Differential Algebra.* AMS. 1950.

[37] C. M. Rubald. *Algorithms for Polynomials over a Real Algebraic Number Field.* Ph.D. Thesis, Department of Computer Science, University of Wisconsin. 1973.

[38] B. Salvy, and P. Zimmermann. Gfun: A Maple Package for the Manipulation of Generating and Holonomic Functions in One Variable. *ACM Transactions on Mathematical Software* **20**, 163–177, 1994.

[39] B. Z. Shen. Solving a Congruence on a Graded Algebra by a Subresultant Sequence and Its Application. *Journal of Symbolic Computation* **14**(5), 505–522, 1992.

[40] P. S. Wang. A p-adic Algorithm for Univariate Partial Fractions. In Proceedings of the 1981 Symposium on Symbolic and Algebraic Computation, 212–217, ACM Press, 1981.

[41] P. S. Wang, M. J. T. Guy, and J. H. Davenport. p-adic Reconstruction of Rational numbers. *SIGSAM Bulletin* **16**, 2–3, 1982.

[42] H. S. Wilf and D. Zeilberger. An Algorithmic Proof of Theory for Hypergeometric (Ordinary and "q") Multisum / Integral Identities. *Inventiones Mathematicae* **108**, 575–633, 1992.