MM Research Preprints, 208–211
No. 18, Dec. 1999. Beijing

A Constructive Proof of Lüroth's Theorem in Differential Fields

Tao Xu, Xiao-Shan Gao
Institute of Systems Science
Academia Sinica
Beijing 100080, China

Abstract. In this paper, we present a constructive proof of Lüroth's theorem in differential case. The method is based on Wu's zero decomposition theorem.

Keywords. differential algebra , field extension, Lüroth's theorem.

1. Introduction

In algebraic geometry, we have the following theorems.

Theorem 1.1 Every rational transform of a rational curve is a rational curve.

Theorem 1.2 If λ is transcendental over K and if $K \subset F \subset K(\lambda)$, $F \neq K$, then there is a μ, transcendental over K, such that $F = K(\mu)$.

Suppose that $f(x, y) = 0$ is rational, i.e.,there exists $\phi, \psi \in K(\lambda)$ such that

(i) For all but a finite set of $\lambda_0 \in K$, $f(\phi(\lambda_0), \psi(\lambda_0)) = 0$.

(ii) With a finite number of exceptions, for every x_0, y_0 for which $f(x_0, y_0) = 0$ there is a unique $\lambda_0 \in K$ such that $x_0 = \phi(\lambda_0), y_0 = \psi(\lambda_0)$.

Theorem 1.3 If a curve $f(x, y) = 0$ satisfies (i) for rational functions $\phi(\lambda), \psi(\lambda)$ which are not both constants, then there exist rational functions $\phi'(\lambda), \psi'(\lambda)$ for which both (i) and (ii) are satisfied, and the curve is rational.

Theorems 1.1,1.2 and 1.3 are all equivalent, and are often indiscriminately called Luroth's Theorem. This paper will consider similar theorems in differential case.

Let F be a differential field and F_1 an extension of F. Let σ be any set of elements of F_1. There exists fields which are contained in F_1 and contain F and σ. The intersection of all such fields is a field which will be denoted by $F < \sigma >$ and will be called the field obtained by the adjunction of σ to F. $F < \sigma >$ consists of all rational combinations of elements of σ, and of derivatives of such elements, with coefficients in F. A quality η lying in an extension of F will be said to be differential with respect to F if η annuls a nonzero *d.p.* in one indeterminate over F.

In differential case, we have the following theorem [**?**].

Theorem 1.4 Let F' be any extension of F which is contained in $F < u >$, where u is an indeterminate. Then F' contains an element v such that $F < v >= F'$.

2. A Constructive Proof

Let P be a differential polynomial. The *class* of P, denoted by $cls(P)$, is the largest p such that some x_p actually occurs in P. If $P \in K$, $cls(P) = 0$. Let a polynomial P be

of $cls(P) > 0$. Let j is the largest value such that $x_{p,j}$ appears in P. The class of P is $cls(P) = p$. The order of P is $ord(P, x_p) = j$. The lead of P is $ld(P) = x_{p,j}$. The coefficient of the highest power of $x_{p,j}$ in P considered as a polynomial of $x_{p,j}$ is called the *initial* of P. For polynomials P and G with $class(P) > 0$, let $prem(G; P)$ be the *pseudo remainder* of G wrt P.

P_2 is of higher rank than P_1 in x_i, if either $ord(P_2, x_i) \geq ord(P_1, x_i)$ or $q = ord(P_2, x_i) = ord(P_1, x_i)$ and $deg(P_2, x_{i,q}) \geq deg(P_1, x_{i,q})$. P_2 is reduced wrt P_1 if P_2 is of lower rank than P_1 in $x_{cls(P_1)}$. We say $P_2 > P_1$, if either $cls(P_2) > cls(P_1)$ or $p = cls(P_2) = cls(P_1)$ and P_2 is of higher rank than P_1 in x_p.

A sequence of polynomials $ASC = A_1, ..., A_p$ is said to be an *ascending (*ab. *asc) chain*, if either $p = 1$ and $A_1 \neq 0$ or $0 < class(A_i) < class(A_j)$ for $1 \leq i < j$ and A_k is reduced wrt A_m for $m > k$.

For an asc chain $ASC = \{A_1, ..., A_p\}$ with $class(A_1) > 0$, the pseudo remainder of a polynomial G wrpt ASC is defined inductively as

$$prem(G; ASC) = prem(prem(G; A_p); A_1, ..., A_{p-1}).$$

Let $R = prem(G; ASC)$, then from the computation procedure of the pseudo division procedure, we have the following important *remainder formula*:

$$JG \equiv R \ \ [A_1, \cdots, A_p] \tag{2.1}$$

where J is a product of powers of the initials and separants of the polynomials in ASC (IS-product). For an asc chain ASC, we define

$$PD(ASC) = \{g \mid prem(g, ASC) = 0\}$$

By (2.1), a zero of ASC which does not annul the initials of the polynomials in ASC is a zero of $PD(ASC)$. More precisely, we have

$$Zero(PD(ASC)) = Zero(ASC/J) \bigcup \cup_{d \in J} Zero(PD(ASC) \cup \{d\}) \tag{2.2}$$

where J is the set of initials and separants of the polynomials in ASC.

Theorem 2.1 Let $g_1(u), \cdots, g_r(u)$ be elements of $F < u >$. We have an algorithm to find a $g(u) \in F < u >$ such that $F < g_1, \cdots, g_r >= F < g >$.

Proof. We assume that $g_1, \cdots, g_r$ have the following form,

$$g_1 = \frac{P_1(u)}{Q_1(u)}, \ ..., \ g_r = \frac{P_n(u)}{Q_n(u)} \tag{2.3}$$

We assume not all the $P_i(u)$ and $Q_i(u)$ are constants and $gcd(P_i(u), Q_i(u)) = 1$. For a set of rational dpe's of the form (2.2), let $PS = \{F_1, \cdots, F_n\}$ and $DS = \{Q_1, \cdots, Q_n\}$, where $F_i = Q_i x_i - P_i$, $i = 1, \cdots, n$. It is obvious that

(2.4)

$$IM(P, Q) = \{(x_1, \cdots, x_n) \mid \exists (\tau_1, \cdots, \tau_m) \in E^m (\tau_1, \cdots, \tau_m, x_1, \cdots, x_n) \in Zero(PS/DS)\}$$

Note that under the variable order $u < x_1 < \cdots < x_n$, $PS = \{F_1, \cdots, F_n\}$ is an *irreducible ascending chain* in $K\{u, x\}$. Thus $PD(PS)$ is a prime ideal of dimension m. Note that DS is the set of initials of the polynomials in PS, then we have

$$Zero(PS/DS) = Zero(PD(PS)/DS). \tag{2.5}$$

We can find an irreducible ascending chain ASC under the new variable order $x_1 < \cdots < x_n < u$ such that

$$Zero(PS/DS) = Zero(PD(ASC)/DS). \tag{2.6}$$

ASC has the same dimension m as PS. Hence ASC contains n polynomials. Note that the *parameter set* of ASC is $\{x_1, ..., x_m\}$.

We can find differential polynomial sets PS_i and differential polynomials d_i, $i = 1, ..., t$, such that

$$IM(P, Q) = \cup_{i=1}^{t} Zero(PS_i/\{d_i\}). \tag{2.7}$$

Let $K' = K < P_1/Q_1, ..., P_n/Q_n >$. Note that $P_1(u) - Q_1(u)\lambda = 0$ where $\lambda = P_1(u)/Q_1(u) \in K'$, then u is differential with respect to K'.

Let $DPS = \{P_1(u) - Q_1(u)x_1, P_2(u) - Q_2(u)x_2, \cdots, P_n(u) - Q_n(u)x_n\}$, if we give the variable order $u < x_1 < x_2 < \cdots < x_n$, then the DPS is an ascending chain . Let $QD(AS) = \{P | \exists IS - powerJ, JP \equiv 0\ [AS]\}$, $QD(AS)$ is an ideal for any AS. Now we give another variable order, $x_1 < x_2 < \cdots < x_n < u$, Using the following algorithm,

$$\begin{array}{llll} DPS = PS_1 & PS_2 & \cdots & PS_k \\ BS_1 & BS_2 & \cdots & PS_k = AS \\ RS_1 & RS_2 & \cdots & RS_k = \emptyset \end{array}$$

where

$$BS_i = basicsetofPS_i,$$

$$RS_i = non - zeroremaindersofd - polsinPS_i - BS_iwrtBS_i.$$

$$PS_i = PS_{i-1} \cup RS_{i-1}.$$

We can get a differential polynomial series,

$$\begin{array}{c} A_1(x_1, \cdots, x_{m+1}), \\ \cdots, \\ A_{n-m}(x_1, \cdots, x_n), \\ B(x_1, \cdots, x_n, u) \end{array}$$

Here $B(x_1, \cdots, x_n, u)$ give a relation between the variables $x_1, \cdots, x_n$ and u with lowest rank in u module the curve. In other words, $B'(y) = B(P_1/Q_1, \cdots, P_n/Q_n, y) = 0$ is a polynomial in $K' < y >$ with lowest rank in y such that $B'(u) = 0$. Let $v = initial(B', u)$, Thus $x_i = P_i/Q_i$ can be expressed as rational functions of v, and v can also be expressed as a rational functions of $x_i = P_i/Q_i$. Use Lemma 2.1, we get the result. $\diamond$

References

[1] Chou, S.C. and Gao, X.S., Ritt-Wu's Decomposition Algorithm and Geometry Theorem Proving, *10th International Conference on Automated Deduction*, M.E. Stickel (Ed.) pp 207–220, Lect. Notes in Comp. Sci., No. 449, 1990. Springer-Verlag.

[2] Gao, X.S. and Chou, S.C. , Independent Parameters, Inversions and Proper Parameterization, TR-90-30, Computer Sciences Department, The Univ. of Texas at Austin, September, 1990.

[3] Kolchin, E. R., Differential Algebra and Algebraic Groups, Academic Press. 1973.

[4] Ritt, J. F., Differential Algebra, Amer. Math. Soc., 1950.

[5] Walker, R. , *Algebraic Curves*, Princeton Univ. Press, 1950.

[6] Wu wen-tsün, On the foundation of algebraic differential geometry, Mathematics-Mechanization Research Preprint, No.3, 1989.

[7] Wu, wen-tsün , Basic Principles of Mechanical Theorem Proving in Elementary Geometries, *J. Sys. Sci. & Math. Scis.*, 4(1984), 207 –235, Re-published in *J. Automated Reasoning*, 1986.

[8] Wu, wen-tsün , On a Projection Theorem of Quasi-Varieties in Elimination Theory , *MM Research Preprints*, No. 4, 1989. Ins. of Systems Science, Academia Sinica.