J. Math. Kyoto Univ. (JMKYAZ)
31-1 (1991) 83-88

Differentially separable extension of positive characteristic p

By

Kayoko SHIKISHIMA-TSUJI

§ 0. Introduction

It is well known in the field theory that if $a_1, \ldots, a_s$ are separably algeraic elements of an extension of a field K, there exists an element b such that $K(a_1, \ldots, a_s) = K(b)$. It is interesting to see if this result can be extended to differential fields.

In [2], Kolchin showed that for the usual derivation, such an extension can be done under a condition: if elements $a_1, \ldots, a_s$ of a differential extension of a differential field K are differentially separably dependent over K i.e. for each i $(1 \leq i \leq s)$, there is a differential polynomial $F_i(X_1, \ldots, X_s)$ over K such that $F_i(a_1, \ldots, a_s) = 0$ and $(\partial F_i/\partial(\theta_i X))(a_1, \ldots, a_s) \neq 0$ for some differential operator θ_i, there exists an element b such that the differential field $K\langle a_1, \ldots, a_s\rangle$ i.e. the smallest differential extension field of K containing $a_1, \ldots, a_s$ is equal to $K\langle b\rangle$ (see Proposition 9 of Chapter 2 of [2]).

Since Hasse's differentiation gives more natural results than the usual derivation which in some cases gives pathological results for positive characteristic, we show in this paper that by using Hasse's differentiation a formulation of the extension mentioned at the top of this section can also be performed for positive characteristic p.

§ 1. Definitions*)

Let R be a commutative unitary ring containing some field as a unitary subring. A *derivation* δ of R means an iterative higher derivation of infinite rank i.e. an infinite sequence $\delta = (\delta_\nu;\ \nu \in \mathbf{N}$, the set of natural numbers including 0) of mappings δ_ν of R into R which satisfies the following conditions:

D 1 $\delta_0 = \mathrm{id}_R$ (the identity mapping of R),

D 2 $\delta_\nu(x + y) = \delta_\nu x + \delta_\nu y$,

D 3 $\delta_\nu(xy) = \sum_{\lambda+\mu=\nu} \delta_\lambda x \cdot \delta_\mu y$,

Communicated by Prof. Nagata Feb. 6, 1989

*) At large see Okugara [4]

D 4 $\delta_\lambda \delta_\mu x = \binom{\lambda+\mu}{\lambda} \delta_{\lambda+\mu} x$

for $x, y \in R$ and $\lambda, \mu, \nu \in \mathbf{N}$. Let $\delta = (\delta_\nu; \nu \in \mathbf{N})$ and $\delta' = (\delta'_\nu; \nu \in \mathbf{N})$ be derivations of the ring R. If $\delta_\lambda \delta'_\mu = \delta'_\mu \delta_\lambda$ for all $\lambda, \mu \in \mathbf{N}$, we say that δ *commutes* with δ'.

Let I be a finite or infinite set of indices. A ring R is said to be a *differential ring* if R is associated with a nonempty set $\Delta = \{\delta_i; i \in I\}$ of mutually commutative derivations $\delta_i = (\delta_{i\nu}; \nu \in \mathbf{N})$ $(i \in I)$. If the ring R is a field, it is referred to as a *differential field.*

For every finite number of distinct indices $i_1, \ldots, i_n \in I$ and $\nu_1, \ldots, \nu_n \in \mathbf{N}$, the product $\theta = \delta_{i_1\nu_1} \cdots \delta_{i_n\nu_n}$ is a well-defined endomorphism of the additive group R^+ of the ring R, and called a *derivative operator* of the differential ring R. The number $\nu_1 + \cdots + \nu_n$ is called the *order* of θ and denoted by ord θ. The set of all derivative operators of the differential ring R is denoted by Θ.

Let k be a differential field of positive characteristic p and $k\{X\}$ be a differential polynomial ring in a differential indeterminate X. We say that Θ is *independent on* k if the differential polynomial $A(X) \in k\{X\}$ which vanishes at all elements of k equals zero. An element α of a differential extension field of k is said to be *differentially separable* over k if $k\langle\alpha\rangle$ is separable over k.

We define a partial order of Θ as follows. Let $\delta = (\delta_\nu; \nu \in \mathbf{N})$ be a derivation of k. For two positive integers ν and λ with the p-adic expressions

$$\nu = \sum a_j p^j \qquad (0 \leq a_j \leq p-1)$$

and

$$\lambda = \sum b_j p^j \qquad (0 \leq b_j \leq p-1),$$

we say $\delta_\nu \geq \delta_\lambda$ if $a_j \geq b_j$ for every $j \in \mathbf{N}$.

For $\theta, \theta' \in \Theta$ with $\theta = \prod_{i \in I} \delta_{i\nu_i}$ and $\theta' = \prod_{i \in I} \delta_{i\lambda_i}$, we say $\theta \geq \theta'$ if $\delta_{i\nu_i} \geq \delta_{i\lambda_i}$ for every $i \in I$.

§ 2. Results

The following lemma is Lemma 1 of § 2 of Chapter 0 in Kolchin [2].

Lemma (*Kolchin*). *Let K be a field and $u_1, \ldots, u_r$, $v_1, \ldots, v_s$ with $r < s$ be elements of an extension of K. If each v_h $(1 \leq h \leq s)$ is separably algebraic over $K(u_1, \ldots, u_r)$, then there exists a polynomial $A(X_1, \ldots, X_s) \in K[X_1, \ldots, X_s]$ such that $A(v_1, \ldots, v_s) = 0$ and $(\partial A/\partial X_j)(v_1, \ldots, v_s) \neq 0$ for some j $(1 \leq j \leq s)$.*

Theorem 1. *Let α be an element of a differential extension field of k.*

(a) If tr deg $k\langle\alpha\rangle/k$ *is finite, then there exists a nonzero differential polynomial $F(X) \in k\{X\}$ such that $F(\alpha) = 0$.*

(b) If, in addition, α is differentially separable over k, then there exists a nonzero differential polynomial $G(X) \in k\{X\}$ such that $G(\alpha) = 0$ and

$(\partial G/\partial(\theta X))(\alpha) \neq 0$ *for some* $\theta \in \Theta$.

Proof. Let r be the transcendence degree of $k\langle\alpha\rangle$ over k and $\theta_1, \ldots, \theta_s$ with $s > r$ be distinct s elements of Θ. Since $s > r$, $\theta_1\alpha, \ldots, \theta_s\alpha$ are algebraically dependent over k i.e. there is a nonzero polynomial $M(Y_1, \ldots, Y_s) \in k[Y_1, \ldots, Y_s]$ such that $M(\theta_1\alpha, \ldots, \theta_s\alpha) = 0$. The differential polynomial $F(X) = M(\theta_1 X, \ldots, \theta_s X) \in k\{X\}$ vanishes at α. This proves the part (a) of our theorem. If, in addition, $k\langle\alpha\rangle$ is separable over k, then $k(\theta_1\alpha, \ldots, \theta_s\alpha)$ is separable over k and thus has a finite separating transcendence basis $v_1, \ldots, v_t$ over k. Since each one of $\theta_1\alpha, \ldots, \theta_s\alpha$ is separably algebraic over $k(v_1, \ldots, v_t)$ and $t \leq r < s$, there exists, by Lemma, a nonzero polynomial $A(Y_1, \ldots, Y_s) \in k[Y_1, \ldots, Y_s]$ such that $A(\theta_1\alpha, \ldots, \theta_s\alpha) = 0$ and $(\partial A/\partial Y_j)(\theta_1\alpha, \ldots, \theta_s\alpha) \neq 0$ for some $j (1 \leq j \leq s)$. The differential polynomial $G(X) = A(\theta_1 X, \ldots, \theta_s X) \in k\{X\}$ satisfies the condition of the part (b) of our theorem. q.e.d.

For a differential polynomial F, the set of $\theta \in \Theta$ which appears effectively in F is denoted by $\Theta(F)$.

Corollary 1. *Let α be an element of a differential extension field of k. If α is differentially separable over k and the transcendence degree of $k\langle\alpha\rangle$ over k is finite, then there exists a nonzero differential polynomial $F(X) \in k\{X\}$ which satisfies the following three conditions*:

(i) $\Theta(F)$ *has the highest element* θ_0.

(ii) $F(\alpha) = 0$.

(iii) $(\partial F/\partial(\theta_0 X))(\alpha) \neq 0$.

Proof. By Theorem 1(b), there is a nonzero differential polynomial $G(X) \in k\{X\}$ such that $G(\alpha) = 0$ and

$$(\partial G/\partial(\theta X))(\alpha) \neq 0 \quad \text{for some } \theta \in \Theta(G). \tag{1}$$

Let s be the number of elements of the finite set $\Theta(G)$. Choose a finite number of distinct elements $i_1, \ldots, i_m$ of I such that all the elements of $\Theta(G)$ are $\theta_j = \delta_{i_1 v_{j1}} \cdots \delta_{i_m v_{jm}}$ $(1 \leq j \leq s)$. Each v_{jk} has the p-adic expression

$$v_{jk} = c_{jk0} + c_{jk1}p + \cdots + c_{jke}p^e \quad (0 \leq c_{jkl} \leq p - 1,\ 1 \leq k \leq m,\ 0 \leq l \leq e).$$

We may assume that the condition (1) is satisfied for θ_1. We denote by θ_0 the derivative operator $\delta_{i_1(\lambda - v_{11})} \cdots \delta_{i_m(\lambda - v_{1m})}$ where $\lambda = (p-1) + (p-1)p + \cdots + (p-1)p^e$. If $\theta_0 = \mathrm{id}$, then θ_1 is the highest element of $\Theta(G)$ and thus $G(X)$ satisfies the required three conditions. On the contrary, if $\theta_0 \neq \mathrm{id}$, we denote by $F(X)$ the differential polynomial

$$\begin{aligned} \theta_0 G(X) &= \frac{\partial G}{\partial(\theta_1 X)}(X) \cdot \theta_0\theta_1 X + (\cdots) \\ &= \frac{\partial G}{\partial(\theta_1 X)}(X) \cdot \binom{\lambda}{v_{11}} \cdots \binom{\lambda}{v_{1m}} \delta_{i_1\lambda} \cdots \delta_{i_m\lambda} X + (\cdots). \end{aligned} \tag{2}$$

Taking Lemma 1 of §1.2 of [4] into consideration, we see that

$$\binom{\lambda_{11}}{\nu_{11}}\cdots\binom{\lambda_{1m}}{\nu_{1m}}\not\equiv 0 \pmod{p}$$

and that each θ which appears effectively in $(\cdots)$ of (2) is lower than $\delta_{i_1\lambda}\cdots\delta_{i_m\lambda}$. Now, it is obvious that the above $F(X)$ is the required differential polynomial. q.e.d.

Theorem 2. *Let Θ be independent on k and let α and β be two elements of a differential extension field of k. If the transcendence degree of $k\langle\alpha, \beta\rangle$ over k is finite and $k\langle\alpha, \beta\rangle$ is separable over k, then there exists an element z of k such that $k\langle\alpha, \beta\rangle = k\langle\alpha + z\beta\rangle$.*

Proof. Let X, Y and Z be differential indeterminates over $k\langle\alpha, \beta\rangle$. Since $k\langle Z\rangle$ and $k\langle\alpha, \beta\rangle$ are algebraically disjoint over k and $k\langle\alpha, \beta\rangle$ is separable over k, $k\langle\alpha, \beta, Z\rangle$ is separable over $k\langle Z\rangle$ by Proposition 7 of §9.3 in Bourbaki [1]. By Proposition 6 of §7.4 loc. cit., $\alpha + Z\beta$ is differentially separable over $k\langle Z\rangle$. The following inequalities are obvious:

$$\begin{aligned}\text{tr deg } k\langle Z\rangle\langle\alpha + Z\beta\rangle/k\langle Z\rangle &\leq \text{tr deg } k\langle\alpha, \beta, Z\rangle/k\langle Z\rangle\\ &\leq \text{tr deg } k\langle\alpha, Z\rangle/k\langle Z\rangle + \text{tr deg } k\langle\beta, Z\rangle/k\langle Z\rangle\\ &\leq \text{tr deg } k\langle\alpha\rangle/k + \text{tr deg } k\langle\beta\rangle/k < \infty.\end{aligned}$$

By Corollary 1, there exist a nonzero differential polynomial $F(X)\in k\langle Z\rangle\{X\}$ such that $\Theta(F)$ has the highest element θ_0, $F(\alpha + Z\beta) = 0$ and $(\partial F/\partial(\theta_0 X))(\alpha + Z\beta)\neq 0$. Let $\theta_0, \ldots, \theta_s$ be all the elements of $\Theta(F)$ and n be the degree of $F(X)$ in $\theta_0 X$. Then, we can choose a finite number of monomials $M_0(X), \ldots, M_m(X)$ in $\theta_1 X, \ldots, \theta_s X$ such that $F(X)$ is written in the form

$$\begin{aligned}&\frac{A_{0n}(Z)M_0(X) + \cdots + A_{mn}(Z)M_m(X)}{A(Z)}(\theta_0 X)^n\\ &\quad + \cdots + \frac{A_{01}(Z)M_0(X) + \cdots + A_{m1}(Z)M_m(X)}{A(Z)}(\theta_0 X)\\ &\quad + \frac{A_{00}(Z)M_0(X) + \cdots + A_{m0}(Z)M_m(X)}{A(Z)}\end{aligned}$$

where $A(Y)$, $A_{00}(Y), \cdots, A_{m0}(Y), \cdots, A_{0n}(Y), \cdots, A_{mn}(Y)$ are relatively prime differential polynomials of $k\{Y\}$. The differential polynomial

$$\begin{aligned}B(X, Y) = &(A_{0n}(Y)M_0(X) + \cdots + A_{mn}(Y)M_m(X))(\theta_0 X)^n + \cdots +\\ &(A_{01}(Y)M_0(X) + \cdots + A_{m1}(Y)M_m(X))(\theta_0 X) + A_{00}(Y)M_0(X)\\ &+ \cdots + A_{m0}(Y)M_m(X)\end{aligned}$$

of $k\{X, Y\}$ satisfies the following two conditions:

$$B(\alpha + Z\beta, Z) = 0,$$

$$(\partial B/\partial(\theta_0 X))(\alpha + Z\beta, Z) \neq 0.$$

For every $\theta = \delta_{i_1\nu_1} \cdots \delta_{i_l\nu_l} \in \Theta$, we have

$$\theta(\alpha + Z\beta) = \theta Z \cdot \beta + (\theta\alpha + \sum \delta_{i_1\lambda_1} \cdots \delta_{i_l\lambda_l} Z \cdot \delta_{i_1\mu_1} \cdots \delta_{i_l\mu_l} \beta). \tag{3}$$

where the summation $\sum$ runs over all $(\lambda_1, \ldots, \lambda_l, \mu_1, \ldots, \mu_l) \in \mathbf{N}^{2l}$ with $\lambda_1 + \mu_1 = \nu_1, \ldots, \lambda_l + \mu_l = \nu_l$, $(\lambda_1, \ldots, \lambda_l, \mu_l, \ldots, \mu_l) \neq (\nu_1, \ldots, \nu_l, 0, \ldots, 0)$. Since θ_0 is the highest element of $\{\theta_0, \ldots, \theta_s\}$, the equation (3) implies that none of $M_h(\alpha + Z\beta)$ $(0 \leq h \leq m)$ contains $\theta_0 Z$. Computing $\partial B(\alpha + Z\beta, Z)/\partial(\theta_0 Z)$, we obtain

$$\frac{\partial B}{\partial(\theta_0 X)}(\alpha + Z\beta, Z) \cdot \beta + \frac{\partial B}{\partial(\theta_0 Y)}(\alpha + Z\beta, Z) = 0. \tag{4}$$

We can choose linearly independent elements $c_1, \ldots, c_r$ over k in the coefficients of the differential polynomial $(\partial B/\partial(\theta_0 X))(\alpha + Z\beta, Z)$ of $k\langle\alpha, \beta\rangle\{Z\}$ such that the differential polynomial is written in the form

$$c_1 B_1(Z) + \cdots + c_r B_r(Z)$$

where $B_1(Z), \ldots, B_r(Z) \in k\{Z\}$ and $B_1(Z) \neq 0$. Since $B_1(Z) \neq 0$ and Θ is indeped-ent on k, there is an element z of k such that $B_1(z) \neq 0$ and thus we have

$$\frac{\partial B}{\partial(\theta_0 X)}(\alpha + z\beta, z) = c_1 B_1(z) + \cdots + c_r B_r(z) \neq 0.$$

From the equation (4), we have

$$\beta = -\frac{\dfrac{\partial B}{\partial(\theta_0 Y)}(\alpha + z\beta, z)}{\dfrac{\partial B}{\partial(\theta_0 X)}(\alpha + z\beta, z)} \in k\langle\alpha + z\beta\rangle$$

and then α belongs to $k\langle\alpha + z\beta\rangle$. Thus, we obtain the equality $k\langle\alpha + z\beta\rangle = k\langle\alpha, \beta\rangle$. q.e.d.

The following corollary is an immediate consequence of Theorem 2.

Corollary 2. *Let Θ be independent on k and let $\alpha_1, \ldots, \alpha_n$ be elements of a differential extension field of k. If the transcendence degree of $k\langle\alpha_1, \ldots, \alpha_n\rangle$ over k is finite and $k\langle\alpha_1, \ldots, \alpha_n\rangle$ is separable over k, then there exists an element γ such that $k\langle\alpha_1, \ldots, \alpha_n\rangle = k\langle\gamma\rangle$.*

For a subset Δ' of Δ, k is regarded as a differential field associated with Δ'. Let $\alpha_1, \ldots, \alpha_n$ be elements of a differential extension field of k. We denote the smallest differential extension field associated with Δ' of k containing $\alpha_1, \ldots, \alpha_n$ by $k\langle\alpha_1, \ldots \alpha_n; \Delta'\rangle$. It is easy to prove the following corollary by the proof of Theorem 2.

Corollary 3. *Let $\alpha_1, \ldots, \alpha_n$ be elements of a differential extension field of k associated with Δ. If there exists a nonempty subset Δ' of Δ such that the set Θ' of derivative operators of the differential field k associated with Δ' is independent on k, that the transcendence degree of $k\langle\alpha_1, \ldots, \alpha_n; \Delta'\rangle$ over k is finite and that $k\langle\alpha_1, \ldots, \alpha_n; \Delta'\rangle$* is separable over k, then there exists an element γ such that $k\langle\alpha_1, \ldots, \alpha_n\rangle = k\langle\gamma\rangle$ (as differential extension fields associated with Δ).

§3. Remark

As was mentioned in the introduction, Kolchin's condition of Proposition 9 of Chapter 2 of [2] is simpler than the one we adopted in Corollary 3. This is due to the more complicated structure of the differential field in the case of Hasse's differentiation than in the case of usual derivation. Corollary 2 is adequate for the kind of differential extensions which are considered in the theories of strongly normal extensions, Picard-Vessiot extensions and Liouvillian extensions of [4] or [5] and Corollary 3 is a generalization.

Acknowledgement. The author wishes to express her sincere gratitude to Professor Kôtaro Okugara for his advices. She also wishes to thank Dr. Atsushi Murase for his valuable suggestions.

INSTITUTE OF MATHEMATICS,
YOSHIDA COLLEGE
KYOTO UNIVERSITY

References

[1] N. Bourbaki, "Algèbre", Actualités Sci. Indust., Hermann, Paris, 1967.
[2] W. R. Kolchin, Differential Algebra and Algebraic Groups, Acad. Press, 1973.
[3] K. Okugawa, Basic properties of differential fields of an arbitrary characteristic and the Picard-Vessiot theory, J. Math. Kyoto Univ., **2** (1963), 296–322.
[4] K. Okugawa, Differential Algebra of Nonzero Characteristic, Lectures in Mathematics, Department of Math. Kyoto Univ., **16**, 1987.
[5] K. Shikishima-Tsuji, Galois theory of differential fields of positive characterstic, Pacific J. Math., **138**, (1989), 151–168.