Another Proof of Ostrowski-Kolchin-Hardouin Theorem in Difference Algebra

差分代数における Ostrowski-Kolchin-Hardouin 定理の別証明

Hiroshi Ogawara
Master's Program, Graduate School of Media and Governance, Keio University
小川原 弘士
慶應義塾大学大学院政策・メディア研究科修士課程

This paper gives another proof of an analog of Ostrowski-Kolchin theorem in difference algebra, which was proved by Hardouin. Let K be a field of characteristic 0 and (L,τ) a difference extension of a difference field (K,τ). Denote the invariant field of (L,τ) and that of (K,τ) by C_L, C respectively. Suppose C is an algebraically closed field. Suppose $x_1, \ldots, x_m, y_1, \ldots, y_n$ are nonzero elements of L satisfying $\tau(x_i) = u_i x_i, \tau(y_j) = y_j + v_j$, where $u_1, \ldots, u_m, v_1, \ldots, v_n \in K$. Then the analog states that if $x_1, \ldots, x_m, y_1, \ldots, y_n$ are algebraically dependent over KC_L, there exists a nonzero element $a \in K$ satisfying $\tau(a) = (\prod_{i=1}^{m} u_i^{k_i})\, a$ for a nonzero element $(k_i) \in \mathbb{Z}^m$ or $\tau(a) = a + \sum_{j=1}^{n} a_j v_j$ for a nonzero element $(a_j) \in C^n$.

本論文では Hardouin による Ostrowski-Kolchin の定理の差分化の別証明を与えた。K を標数 0 の体、(L,τ) を (K,τ) の差分拡大とする。(L,τ) と (K,τ) の不変体をそれぞれ C_L, C と表記し、C は代数閉体とする。L の 0 でない元 $x_1, \ldots, x_m, y_1, \ldots, y_n$ が $u_1, \ldots, u_m, v_1, \ldots, v_n \in K$ に対して $\tau(x_i) = u_i x_i, \tau(y_j) = y_j + v_j$ を満たすと仮定する。このとき差分化された定理は次のように記述される : $x_1, \ldots, x_m, y_1, \ldots, y_n$ が KC_L 上代数的従属ならば、ある 0 でない元 $a \in K$ が存在して $\tau(a) = (\prod_{i=1}^{m} u_i^{k_i})\, a$ となる 0 でない $(k_i) \in \mathbb{Z}^m$ が存在する、または $\tau(a) = a + \sum_{j=1}^{n} a_j v_j$ となる 0 でない $(a_j) \in C^n$ が存在する。

Mathematics Subject Classification (2010). Primary 12H10; Secondary 65Q10

Keywords: Difference algebra, Linear difference equations, Module of differentials

1 Introduction

In [1], Hardouin has proved an analog of Ostrowski-Kolchin theorem with one derivation operator [2] using difference Galois theory. The purpose of this paper is to give another proof in difference algebra, in which we use module of differentials and its fundamental propositions instead.

To state our theorem we prepare some notions in difference algebra (cf. [4, pp.103 -115]). We always regard any ring (field) as a commutative ring (field) with characteristic 0. Let K be a field and τ_K an isomorphism from K to itself. We call the pair (K, τ_K) a *difference field* and τ_K the *transforming operator* of K. Let L be an extension of K which is also a difference field with a transforming operator τ_L. We call (L, τ_L) a *difference extension* of (K, τ_K) if $\tau_L|_K = \tau_K$. By C_K, we denote the *invariant field* of (K, τ_K), that is, the field of invariant elements of τ_K. For $\alpha = (\alpha_1, \ldots, \alpha_r) \in K^r$ and $k = (k_1, \ldots, k_r) \in \mathbb{Z}^r$, we put $\alpha^k = \prod_{i=1}^r \alpha_i^{k_i}$. Then we shall show the following theorem:

Theorem Let (L, τ) be a difference extension of a difference field (K, τ) and the invariant field $C = C_K$ an algebraically closed field. Suppose $x_1, \ldots, x_m, y_1, \ldots, y_n$ are nonzero elements of L satisfying

$$\tau(x_i) = u_i x_i,$$
$$\tau(y_j) = y_j + v_j,$$

where $u_1, \ldots, u_m, v_1, \ldots, v_n \in K$. If $x_1, \ldots, x_m, y_1, \ldots, y_n$ are algebraically dependent over KC_L, then there exists a nonzero element $a \in K$ satisfying

$$\tau(a) = \left(\prod_{i=1}^{m} u_i^{k_i}\right) a \qquad (1)$$

for a nonzero element $(k_i) \in \mathbb{Z}^m$ or

$$\tau(a) = a + \sum_{j=1}^{n} a_j v_j \qquad (2)$$

for a nonzero element $(a_j) \in C^n$.

2 Preliminaries

Let A be an algebra over a ring R. There exist an A-module Ω called the *module of differentials* of A over R and an R-linear derivation $d: A \to \Omega$ called the *universal R-linear derivation* if for any A-module M and any R-linear derivation $D: A \to M$ there is a unique A-module homomorphism $f: \Omega \to M$ such that $D = f \circ d$ (cf. [4, pp.91-92]). The following propositions are well-known:

Proposition 1 (Rosenlicht [6]). Let L/K be a field extension and Ω its module of differentials with the universal K-linear derivation d. Then $\eta_1, \ldots, \eta_r \in L$ are algebraically independent over K if and only if $d\eta_1, \ldots, d\eta_r \in \Omega$ are linearly independent over L.

Proposition 2 (Rosenlicht [6]). Let L/K be a field extension and Ω its module of differentials with the universal K-linear derivation d. Suppose $a_1, \ldots, a_r \in K$ are linearly independent over $\mathbb{Q}$. If $\eta, \zeta_1, \ldots, \zeta_r \in L$ satisfy

$$d\eta + \sum_{i=1}^{r} a_i \frac{d\zeta_i}{\zeta_i} = 0,$$

then $d\eta = d\zeta_1 = \cdots = d\zeta_r = 0$.

Proposition 3 (Kubota [3]). Suppose (L, τ) is a difference extension of a difference field (K, τ). Let Ω be the module of differentials of L/K with the universal K-linear derivation d. Then there exists an additive mapping $\tau^*: \Omega \to \Omega$ such that

$$\tau^*(\eta d\zeta) = \tau(\eta) d(\tau(\zeta)) \quad (\eta, \zeta \in L).$$

3 Proof of Theorem

From the assumption, we may suppose that L is finitely generated over K. In fact, there is a nonzero polynomial $F \in KC_L[X_1, \ldots, X_m, Y_1, \ldots, Y_n]$ satisfying

$$F(x_1, \ldots, x_m, y_1, \ldots, y_n) = 0.$$

Let L' be an extension over K generated by $x_1, \ldots, x_m, y_1, \ldots, y_n$ and the elements of C_L being in the coefficients of F. Then we have $\tau(L') \subset L'$, so that $(L', \tau)/(K, \tau)$ is a difference extension. Furthermore, we only have to prove our theorem in case $v_1, \ldots, v_n$ are linearly independent over C.

First, suppose that $x_1, \ldots, x_m$ are algebraically dependent over KC_L and take the minimal number m' such that $x_1, \ldots, x_{m'}$ are algebraically dependent over KC_L. Let Ω be the module of differentials of L/KC_L with the universal KC_L-linear derivation $d : L \to \Omega$. Then there is a nontrivial equation of linear dependence over L,

$$\sum_{i=1}^{m'} a_i \frac{dx_i}{x_i} = 0,$$

where $a_i \in L$ and $a_{m'} = 1$. Applying the additive mapping τ^* of Proposition 3 to this equation, we have

$$\sum_{i=1}^{m'} \tau(a_i) \frac{dx_i}{x_i} = 0.$$

Hence we get by $\tau(a_{m'}) = a_{m'} = 1$,

$$\sum_{i=1}^{m'-1} (\tau(a_i) - a_i) \frac{dx_i}{x_i} = 0.$$

Since $dx_1, \ldots, dx_{m'-1}$ are linearly independent over L from Proposition 1, it follows that $\tau(a_i) = a_i$ for each i. Hence every a_i is a member of C_L. There are elements $c_1, \ldots, c_r \in C_L$ such that they are linearly independent over $\mathbb{Q}$ and satisfy

$$a_i = \sum_{j=1}^{r} n_{ij} c_j \ (n_{ij} \in \mathbb{Z}).$$

Then not all n_{ij} are zero. Putting $z_j = \prod_{i=1}^{m'} x_i^{n_{ij}}$, we have

$$\sum_{j=1}^{r} c_j \frac{dz_j}{z_j} = \sum_{j=1}^{r} c_j \sum_{i=1}^{m'} n_{ij} \frac{dx_i}{x_i} = \sum_{i=1}^{m'} a_i \frac{dx_i}{x_i} = 0.$$

From Proposition 2, each z_j is algebraic over KC_L. Take some z_j of them such that not all $n_{1j}, \ldots, n_{m'j}$ are zero. Considering its minimal polynomial, we can take a nonzero element $z \in KC_L$ satisfying

$$\tau(z) = u^{(r_z n_{ij})} z, \tag{3}$$

where r_z is a positive integer and $(r_z n_{ij}) = (r_z n_{1j}, \ldots, r_z n_{m'j})$.

Next, suppose that $x_1, \ldots, x_m$ are algebraically independent over KC_L. Take the minimal number n' such that $x_1, \ldots, x_m, y_1, \ldots, y_{n'}$ are algebraically dependent over KC_L. There is a nontrivial equation of linear dependence over L,

$$\sum_{i=1}^{m} a_i \frac{dx_i}{x_i} + \sum_{h=1}^{n'} b_h dy_h = 0,$$

where $a_i, b_h \in L$ and $b_{n'} = 1$. Applying τ^* to this equation, we have

$$\sum_{i=1}^{m} \tau(a_i) \frac{dx_i}{x_i} + \sum_{h=1}^{n'} \tau(b_h) dy_h = 0.$$

Hence a_i, b_h are included in C_L. Take $c_1, \ldots, c_r \in C_L$, $n_{ij} \in \mathbb{Z}$ and $z_j \in L$ following the same procedure as above. Then we get

$$\sum_{j=1}^{r} c_j \frac{dz_j}{z_j} + d\left(\sum_{h=1}^{n'} b_h y_h \right) = 0.$$

Hence $\sum_{h=1}^{n'} b_h y_h$ is algebraic over KC_L. There is also an element $w \in KC_L$ satisfying

$$\tau(w) = w - \sum_{h=1}^{n'} r_w b_h v_h \tag{4}$$

for some positive integer r_w.

We can embed C_L into the field of formal power series $C((t))$ over C as a field, since C_L is finitely generated over C. We see C_L and K are linearly disjoint over C, and so are K and $C((t))$. In fact, suppose $a_1, \ldots, a_r \in C_L$ are linearly dependent over K. If $r = 1$, clearly a_1 is linearly dependent over C. Assume that $a_1, \ldots, a_{r-1}$ are linearly independent over K. There are $k_1, \ldots, k_r \in K$ with $k_r = 1$ such that

$$\sum_{i=1}^{r} k_i a_i = 0.$$

Applying τ to this, we have

$$\sum_{i=1}^{r} \tau(k_i) a_i = 0.$$

Hence we obtain $\tau(k_i) = k_i$, so that $k_i \in C$. This means $a_1, \ldots, a_r$ are linearly dependent over C. Next, suppose $k_1, \ldots, k_r \in K$ are linearly dependent over $C((t))$. Then there are formal power series $\sum_{v=p}^{\infty} c_{1v} t^v, \ldots, \sum_{v=p}^{\infty} c_{rv} t^v \in C((t))$ which make a nontrivial equation of linear dependence,

$$\sum_{i=1}^{r} k_i \sum_{v=p}^{\infty} c_{iv} t^v = \sum_{v=p}^{\infty} \left(\sum_{i=1}^{r} k_i c_{iv} \right) t^v = 0.$$

So we get $\sum_{i=1}^{r} k_i c_{iv} = 0$ for all v. Since some c_{iv} is a nonzero element, $k_1, \ldots, k_r$ are linearly dependent over C.

Hence there is an embedding from KC_L into the field of formal power series $K((t))$ over K as a difference field defining $\tau(t) = t$ in $K((t))$. The above z can be described in $K((t))$ as

$$z = \sum_{\mu=p}^{\infty} \alpha_\mu t^\mu \quad (\alpha_\mu \in K,\ \alpha_p \neq 0).$$

From (3), we see

$$\sum_{\mu=p}^{\infty} \tau(\alpha_\mu) t^\mu = \sum_{\mu=p}^{\infty} u^{(r_z n_{ij})} \alpha_\mu t^\mu .$$

Therefore we obtain $\tau(\alpha_p) = u^{(r_z n_{ij})} \alpha_p$, the form of (1). We also put

$$w = \sum_{\mu=q}^{\infty} \gamma_\mu t^\mu ,\quad b_h = \sum_{\mu=q}^{\infty} \beta_{h\mu} t^\mu ,$$

where $\gamma_\mu \in K, \beta_{h\mu} \in C$ and $\beta_{n'0} = 1$. From (4), we see

$$\sum_{\mu=q}^{\infty} \tau(\gamma_\mu) t^\mu = \sum_{\mu=q}^{\infty} \gamma_\mu t^\mu - \sum_{h=1}^{n'} r_w v_h \sum_{\mu=q}^{\infty} \beta_{h\mu} t^\mu =$$

$$\sum_{\mu=q}^{\infty} \left(\gamma_\mu - \sum_{h=1}^{n'} r_w \beta_{h\mu} v_h \right) t^\mu.$$

Since $v_1, \ldots, v_{n'}$ are linearly independent over C from the assumption, we see $\gamma_0 \neq 0$. Therefore γ_0 is a nonzero element satisfying $\tau(\gamma_0) = \gamma_0 - \sum_{h=1}^{n'} r_w \beta_{h0} v_h$, the form of (2).

References

[1] Hardouin, C., Hypertranscendance des systèmes aux différences diagonaux, *Compos. Math.*, 144, No.3, 2008, pp.565-581.

[2] Kolchin, E. R., Algebraic groups and algebraic dependence, *Amer. J. Math.*, 90, No.4, 1968, pp.1151-1164.

[3] Kubota, K. K., On the algebraic independence of holomorphic solutions of certain functional equations and their values, *Math. Ann.*, 227, No.1, 1977, pp.9-50.

[4] Levin, A., *Difference Algebra*, Springer Science+Business Media B.V., 2008.

[5] Matsumura, H., *Commutative Ring Theory*, Cambridge Univ. Press, 1986.

[6] Rosenlicht, M., On Liouville's theory of elementary functions, *Pacific J. Math.*, 65, No.2, 1976, pp.485-492.

〔受付日　2013. 7. 19〕
〔採録日　2013. 10. 30〕