EXISTENCE OF NON-TRIVIAL DEFORMATIONS OF INSEPARABLE ALGEBRAIC EXTENSION FIELDS II*

Dedicated to Professor K. Noshiro on his 60th birthday

HIROSHI KIMURA

Let K be an extension of a field k, and p denotes the characteristic. It was proved by M. Gerstenhaber ([1]) that if K is separable over k, then it is rigid and it was conjectured in [1] that, if K is not separable over k, then it is not rigid. We studied in [4] the above conjecture in certain special case. In this note we shall extend the results of [4] to inseparable algebraic extension fields.

1. **Preliminaries.** Let K be an extension fields of a field k of characteristic p, and V be the underlying vector space over k. Let R and S denote the power series ring $k[[t]]$ over k in one variable t and its quotient field $k((t))$ and V_s be $V \otimes_k S$.
Let a bilinear mapping $f_t : V_s \times V_s \longrightarrow V_s$ expressible in the form

$$f_t(a, b) = ab + tF_1(a, b) + t^2F_2(a, b) + \cdots,$$

where F_i is a bilinear mapping defined over k, be a one-parameter family of deformations of K considered as a commutative k-algebra.
Following [1], we say that f_t is trivial if there is a non-sigular linear mapping Φ_t of V_s onto itself of the form

$$\Phi_t(a) = a + t\varphi_1(a) + t^2\varphi_2(a) + \cdots,$$

where φ_i is a linear mapping defined over k, such that $f_t(a, b) = \Phi_t^{-1}(\Phi_t a \cdot \Phi_t b)$. K is rigid if and only if there is no non-trivial one-parameter family of deformations of K.

From now on, throughout this note, we assume $p \neq 0$.

Received April 21, 1967.
* This work was supported by The Sakkokai Foundation.

It is known ([1]) that, for any derivation φ of K, there exists a one-parameter family f_t of deformations of K such that

$$f_t(a, b) = ab + tF_1(a, b) + t^2F_2(a, b) + \cdots,$$

where $F_1 = Sq_p\varphi = \frac{1}{p}\delta\varphi^p = \sum_{i=1}^{p-1}\frac{1}{p}\,{}_pC_i\ \varphi^{p-i} \cup \varphi^i$ (δ denotes the coboundary operator and $\cup$ denotes the cup product).

2. In this section we shall prove the following lemma and its corollary.

Lemma 1. *Let R be the polynomial ring $k[y]$ and T the non-commutative polynomial ring $R[x_1, \cdots, x_s]$. Let x'_r be the mapping of the set of positive integers into T satisfying the following conditions;*

1) $x'_r(1) = x_r$.
2) $x'_1(n) = nx_1y^{n-1}$.
3) $x'_r(n) = x_ry^{n-1} + x'_r(n-1)y + \sum_{i=1}^{r-1} x_ix'_{r-i}(n-1)$, *for* $r \geqq 2$.

Then, for $r \geqq 2$,

$$x'_r(n) = nx_ry^{n-1} + \sum {}_nC_{\Sigma i_j} x_{r_1}^{i_1} \cdots x_{r_h}^{i_h} y^{n-\Sigma i_j},$$

where the sum is taken over all sets $\{r_1, \cdots, r_h;\ i_1, \cdots, i_h\}$ *such that* $\sum_{j=1}^{h} r_j i_k = r$, $2 \leqq \sum_{j=1}^{h} i_j \leqq n$ *and* $1 \leqq r_j < r$.

Proof. We shall prove this by induction on r and n.

1) The case $r = 2$. If $n = 2$, then the lemma is trivial. If $n > 2$, then

$$\begin{aligned} x'_2(n) &= x_2y^{n-1} + x'_2(n-1)y + x_1x'_1(n-1) \\ &= x_2y^{n-1} + \{(n-1)x_2y^{n-2} + {}_{n-1}C_2x_1^2y^{n-3}\}y \\ &\quad + (n-1)x_1^2y^{n-2} \\ &= nx_2y^{n-2} + {}_nC_2x_1^2y^{n-2} \end{aligned}$$

2) The case $r > 2$.

$$x'_r(2) = 2x_ry + \sum_{i=1}^{r-1} x_ix_{r-i}.$$

We assume $n > 2$. Then

$$\sum_{\substack{\Sigma r_j i_j = r \\ 2 \leq \Sigma i_j \leq n-1 \\ 1 \leq r_j < r}} {}_{n-1}C_{\Sigma i_j} x_{r_1}^{i_1} \cdots x_{r_h}^{i_h} y^{n-\Sigma i_j}$$

$$= \sum_{i=1}^{r-1} x_{r-i} \{ {}_{n-1}C_2 x_i y^{n-2} + \sum_{\substack{\Sigma r_j i_j = i \\ 2 \leq \Sigma i_j \leq n-2 \\ 1 \leq r_j < i}} {}_{n-1}C_{\Sigma i_j+1} x_{r_1}^{i_1} \cdots x_{r_h}^{i_h} y^{n-\Sigma i_j-1} \},$$

and

$$\sum_{i=1}^{r-1} x_{r-i} x_i'(n-1)$$

$$= \sum_{i=1}^{r-1} x_{r-i} \{ (n-1) x_i y^{n-2} + \sum_{\substack{\Sigma r_j i_j = i \\ 2 \leq \Sigma i_j \leq n-2 \\ 1 \leq r_j < i}} {}_{n-1}C_{\Sigma i_j} x_{r_1}^{i_1} \cdots x_{r_h}^{i_h} y^{n-1-\Sigma i_j} + \sum_{\substack{\Sigma r_j i_j = i \\ \Sigma i_j = n-1 \\ 1 \leq r_j < i}} x_{r}^{i_1} \cdots x_{r_h}^{i_h} \}.$$

Hence,

$$x_r'(n) = x_r y^{n-1} + x_r'(n-1) y + \sum_{i=1}^{r-1} x_{r-i} x_i'(n-1)$$

$$= n x_r y^{n-1} + \sum_{i=1}^{r-1} {}_nC_2 x_{r-i} x_i y^{n-2} + \sum_{\substack{\Sigma r_j i_j = r \\ 3 \leq \Sigma i_j \leq n-1 \\ 1 \leq r_j < r}} {}_nC_{\Sigma i_j} x_{r_1}^{i_1} \cdots x_{r_h}^{i_h} y^{n-\Sigma i_j} + \sum_{\substack{\Sigma r_j i_j = r \\ \Sigma i_j = n \\ 1 \leq r_j < r}} x_{r_1}^{i_1} \cdots x_{r_h}^{i_h}$$

$$= n\, x_r y^{n-1} + \sum_{\substack{\Sigma r_j i_j = r \\ 2 \leq \Sigma i_j \leq n \\ 1 \leq r_j < r}} {}_nC_{\Sigma i_j} x_{r_1}^{i_1} \cdots x_{r_h}^{i_h} y^{n-\Sigma i_j}.$$

This ends the proof.

COROLLARY 1. *Let T be the commutative polynomial ring $k[y, x_1, \cdots, x_s]$. Let x_r' be the mapping of positive integers into T satisfying the conditions* 1), 2) *and* 3) *in Lemma* 1. *Then*

$$x_r'(n) = n x_r y^{n-1} + \sum \frac{(\Sigma i_j)!}{\Pi (i_j!)} {}_nC_{\Sigma i_j} x_{r_1}^{i_1} \cdots x_{r_h}^{i_h} y^{n-\Sigma i_j},$$

where the sum is taken over all sets $\{r_1, \cdots, , r_i ; i_1, \cdots, i_h\}$ *such that* $\sum_{j=1}^{h} r_j i_j = r$, $2 \leqq \sum_{j=1}^{h} i_j \leqq n$ *and* $1 \leqq r_1 < \cdots < r_h < r$. *Moreover if* r *is not divisible by* p, *then* $x'_r(p) = 0$ *and if* $r = mp$, *where* m *is a positive integer, then* $x'_{mp}(p) = x_m^p$.

Proof. The first part is trivial by Lemma 1. If $1 \leqq r < v$, then $\sum r_j i_j = r < p$. Therefore ${}_pC_{\Sigma i_j} \equiv 0 \pmod{p}$.

We assume $mp < r < (m+1)p$. If $\sum i_j < p$, then ${}_pC_{\Sigma i_j} \equiv 0 \pmod{p}$. If $\sum i_j = p$, by $\sum r_j i_j = r$, we have $i_j < p$. Hence $\frac{p!}{\Pi(i_j!)} \equiv 0 \pmod{p}$.

Next we assume $r = mp$. If $\sum i_j < p$, then ${}_pC_{\Sigma i_j} \equiv 0 \pmod{p}$. If $\sum i_j = p$ and $i_j < p$, then $\frac{p!}{\Pi(i_j!)} = 0 \pmod{p}$. If $i_1 = p$, then $r_1 = m$. This ends the proof.

Remark 1. In Lemma 1, if the condition (2) is defined for $n < p$, then the condition (3) is defined for $n \leqq p$. Therefore Lemma 1 and Corollary 1 are true for $n \leqq p$ and $r > 1$.

3. Let K be an inseparable extension field over k such that there exists an inseparable algebraic element θ of exponent α such that θ is not contained in $k(K^p)$. Let $f(X) = X^{\beta p^\alpha} - a_{\beta-1}X^{(\beta-1)p^\alpha} - \cdots - a_1 X^{p^\alpha} - a_0$ be the minimum polynomial of θ over k. Then there exists $a_i \neq 0$, $1 \leqq i \leqq \beta$, such that i is not divisible by p (where $a_\beta = 1$).

Let φ be a derivation of K over k such that $\varphi(\theta) = 1$ (see [3]). Let f_t be the one-parameter family of deformations of K constructed from φ in [1], i.e.,

$$f_t(a, b) = ab + tF_1(a, b) + t^2F_2(a, b) + \cdots,$$

where $F_1 = Sq_p\varphi$.

LEMMA 2. *Let* f_t *be as above. Then*

$$F_i(\theta, \theta^n) = 0,$$

for $i > 1$. *And if* $a \in ker\, \varphi$, *then*

$$F_i(a, b) = 0,$$

for every $b \in K$ *and* $i \geqq 1$.

https://doi.org/10.1017/S0027763000026659 Published online by Cambridge University Press

Proof. Let $e_0(t\varphi)$ be as in [1, p 72], i.e., $e_0(t\varphi)$ is the power series of $t\varphi$ with coefficients in k such that the constant term is 1 and

$$e_0(t\varphi)[e_0^{-1}(t\varphi)(a)\cdot e_0^{-1}(t\varphi)(b)]$$
$$= ab + t^p F_1(a, b) + t^{2p} F_2(a, b) + \cdots,$$

for all $a, b \in V_s$. Therefore F_i is expressed in the form

$$\sum_{j=0}^{ip} a_{ij}\varphi^{ip-j} \cup \varphi^j, \quad a_{ij} \in k.$$

Hence, for $i > 1$, we have

$$F_i(\theta, \theta^n) = a_{i\ ip-1}\varphi^{ip-1}(\theta^n) + a_{iip}\theta\varphi^{ip}(\theta^n)$$
$$= 0.$$

On the other hand, if $a \in \ker \varphi$, then $e_0^{-1}(t\varphi)(a) = a$, $e_0(t\varphi)(ab) = ae_0(t\varphi)(b)$ and therefore $e_0(t\varphi)[e_0^{-1}(t\varphi)(a).\ e_0^{-1}(t\varphi)(b)] = ab$. Hence, for $i \geqq 1$ $F_i(a, b) = 0$. This ends the proof.

Let
$$\Phi_t = 1 + t\varphi_1 + t^2\varphi_2 + \cdots$$

be a non-singular linear mapping of V_s onto itself. If we set

$$\Phi_t^{-1} = 1 + t\lambda_1 + t^2\lambda_2 + \cdots,$$

then we have $\lambda_r = -\sum_{i=0}^{r-1} \lambda_i\phi_{r-i} = -\sum_{i=0}^{r-1} \varphi_{r-i}\lambda_i$, where $\lambda_0 = 1$.

LEMMA 3. *If we set*

$$\Phi_t^{-1}(\Phi_t(a)\cdot\Phi_t(b))$$
$$= ab + tG_1(a, b) + t^2G_2(a, b) + \cdots,$$

then G_i satisfies the following conditions;

1) $G_1 = \delta\varphi_1$.

2) *For* $r \geqq 2$.

$$G_r = \delta\varphi_r + \sum_{i=1}^{r-1} (\varphi_{r-i} \cup \varphi_i - \varphi_{r-i}G_i).$$

Proof. 1) is trivial. We may assume $r \geqq 2$. Then

$$\begin{aligned}
G_r(a,b) &= \sum_{j=0}^{r} \lambda_j\Big(\sum_{i=0}^{r-j} \varphi_i(a)\varphi_{r-j-i}(b)\Big) \\
&= \lambda_0\Big(\sum_{i=0}^{r} \varphi_i(a)\varphi_{r-i}(b)\Big) \\
&\quad - (\varphi_1\lambda_0)\Big(\sum_{i=0}^{r-1} \varphi_i(a)\varphi_{r-1-i}(b)\Big) - \cdots \\
&\quad - (\varphi_j\lambda_0 + \cdots + \varphi_1\lambda_{j-1})\Big(\sum_{i=0}^{r-j} \varphi_i(a)\varphi_{r-j-i}(b)\Big) \\
&\quad - \cdots - (\varphi_r\lambda_0 + \cdots + \varphi_1\lambda_{r-1})(ab) \\
&= \delta\varphi_r(a,b) + \sum_{i=1}^{r-1} \varphi_i(a)\varphi_{r-i}(b) \\
&\quad - \varphi_1[\lambda_0\Big(\sum_{i=0}^{r-1} \varphi_i(a)\varphi_{r-1-i}(b)\Big) + \cdots + \lambda_{r-1}(ab)] - \cdots \\
&\quad - \varphi_j[\lambda_0\Big(\sum_{i=0}^{r-j} \varphi_i(a)\varphi_{r-j-i}(b)\Big) + \cdots + \lambda_{r-j}(ab)] - \cdots \\
&\quad - \varphi_{r-1}[\lambda_0(a\varphi_1(b) + \varphi_1(a)b) + \lambda_1(ab)] \\
&= \{\delta\varphi_r + \sum_{i=1}^{r-1} (\varphi_i \cup \varphi_{r-i} - \varphi_i G_{r-i})\}(a,b).
\end{aligned}$$

This ends the proof.

Nowx we assume f_t is trivial, i.e., there exists $\Phi_t = 1 + t\varphi_1 + t^2\varphi_2 + \cdots$ such that

$$f_t(a,b) = \Phi_t^{-1}(\Phi_t a \cdot \Phi_t b).$$

Then $G_i = F_i$ for all i. In [4] we proved $\varphi_1(\theta^n) = n\theta^{n-1}\varphi_1(\theta) + m\theta^{n-p}$ for $mp \leqq n < (m+1)p$.

PROPOSITION 1. *If f_t is trivial, then φ_r satisfies the following consitions;*

1) $\varphi_r(1) = 0$, *for* $r \geqq 1$.

2) $\varphi_{p^m}(\theta^{np^{m+1}}) = n\theta^{(n-1)p^{m+1}}$

3) *If* $r(>1)$ *is not divisible by* p, *then* $\varphi_r(\theta^p) = 0$.

4) *If* r *is not divisible by* $p^m (m > 0)$, *then* $\varphi_r(\theta^{p^{m+1}}) = 0$.

Proof. 1). We shall prove by induction on r. If $r = 1$, then this is trivial. By Lemma 2, $G_r(1,1) = 0$ for $r \geqq 1$. Thereofre, by Lemma 3, $\delta\varphi_r(1,1) = 0$. Hence $\varphi_r(1) = 0$.

3). $\varphi_1(\theta^n) = n\theta^{n-1}\varphi_1(\theta)$ for $n < p$,

and by Lemma 2, $G_i(\theta, \theta^n) = 0$ for $i > 1$. On the other hand $G_1(\theta, \theta^n) = 0$

https://doi.org/10.1017/S0027763000026659 Published online by Cambridge University Press

or -1 for $n \leqq p$. Therefore $\varphi_{r-1}G_1(\theta, \theta^n) = 0$. Hence we have, by Lemma 3,

$$\varphi_r(\theta^n) = \theta^{n-1}\varphi_r(\theta) + \theta\varphi_r(\theta^{n-1}) + \sum_{i=1}^{r-1} \varphi_i(\theta)\varphi_{r-i}(\theta^{n-1}).$$

Hence if we set $x_i = \varphi_i(\theta)$, $x_i'(n) = \varphi_i(\theta^n)$ and $y = \theta$, then, by Remark 1, $\varphi_r(\theta^p) = 0$, where r is not divisible by p and $r > 1$.

2) and 4). By [4, Lemma 2], $\varphi_1(\theta^{np}) = n\theta^{(n-1)p}$.

We shall prove by induction on m.

i) The case $m = 1$. By Lemma 2, $G_i(\theta^p, \theta^{np}) = 0$.

By Lemma 3, we have

$$\varphi_r(\theta^{np}) = \theta^{(n-1)p}\varphi_r(\theta^p) + \theta^p\varphi_r(\theta^{(n-1)p}) + \sum_{i=1}^{r-1} \varphi_i(\theta^p)\varphi_{r-i}(\theta^{(n-1)p}).$$

Set $x_i = \varphi_i(\theta^p)$, $x_i'(n) = \varphi_i(\theta^{np})$ and $y = \theta^p$. Then, by Corollary 1, if r is not divisible by p, then $x_r(p) = \varphi_r(\theta^{p^2}) = 0$. If $1 < i < p$, then $x_i = \varphi_i(\theta^p) = 0$ by 3). Therefore, by Corollary 1, we have

$$\begin{aligned}\varphi_p(\theta^{np^2}) &= x_p(np) \\ &= {}_{np}C_p x_1^p y^{(n-1)p} = n\{\varphi_1(\theta^p)\}^p\theta^{(n-1)p^2} \\ &= n\theta^{(n-1)p^2}.\end{aligned}$$

ii) The case $m > 1$. By $G_i(\theta^{p^m}, \theta^{np^m}) = 0$.

Hence we have

$$\varphi_r(\theta^{np^m}) = \theta^{p^m}\varphi_r(\theta^{(n-1)p^m}) + \theta^{(n-1)p^m}\varphi_r(\theta^{p^m}) + \sum_{i=1}^{r-1} \varphi_i(\theta^{p^m})\varphi_{r-i}(\theta^{(n-1)p^m}).$$

Set $x_i = \varphi_i(\theta^{p^m})$, $x_i'(n) = \varphi_i(\theta^{np^m})$ and $y = \theta^{p^m}$. If r is not divisible by p, then $x_r'(p) = \varphi_r(\theta^p) = 0$ and if $r = up^v$, where u is not divisible by p and $0 < v < m$, then $\varphi_r(\theta^{p^{m+1}}) = x_r'(p) = \{x_{up^{v-1}}\}^p = \{\varphi_{up^{v-1}}(\theta^{p^m})\}^p = 0$. Hence 4) was proved. On the other hand, if i is not divisible by p^{m-1}, then $x_i = \varphi_i(\theta^{p^m}) = 0$ by the assumption of induction. Therefore we have

https://doi.org/10.1017/S0027763000026659 Published online by Cambridge University Press

$$x'_{p^m}(np) = \sum \frac{(\sum i_j)}{\Pi(i_j)} {}_{np}C_{\Sigma i_j} x_{r_1}^{i_1} \cdots x_{r_h}^{i_h} y^{np-\Sigma n_j},$$

where the sum is taken over all sets $\{r_1, \cdots, r_h; i_1, \cdots, i_h\}$ such that $\sum_{j=1}^{h} r_j i_j = p^m$, $2 \leqq \sum i_j \leqq np$, $1 < r_1 < \cdots < r_h < p^m$ and every r_j is divisible by p^{m-1}. We may set $r_j = u_j p^{m-1}$, where $0 < u_j < p$. Hence we have $\sum_{j=1}^{h} u_j i_j = p$ and we may assume $\sum_{j=1}^{h} i_j \leqq p$. If $\sum_{j=1}^{h} i_j < p$, then ${}_{np}C_{\Sigma i_j} \equiv 0$ (mod p), and if $\sum_{j=1}^{h} i_j = p$ and $i_j < p$ for all j, then $\dfrac{(\sum i_j)!}{\Pi(i_j!)} \equiv 0$ (mod p). Therefore we have

$$\begin{aligned} \varphi_{p^m}(\theta^{np^{m+1}}) &= x'_{p^m}(np) = {}_{np}C_p x_{p^{m-1}}^p y^{(n-1)p} \\ &= n\{\varphi_{p^{m-1}}(\theta^{p^m})\}^p \theta^{(n-1)p^{m+1}} \\ &= n\theta^{(n-1)p^{m+1}}. \end{aligned}$$

This completes the proof.

By Proposition 1, we have

$$\varphi_{p^{\alpha-1}}(\theta^{\beta p^\alpha}) = \beta\theta^{(\beta-1)p^\alpha}.$$

On the other hand,

$$\varphi_{p^{\alpha-1}}(\theta^{\beta p^\alpha}) = \varphi_{p^{\alpha-1}}\Big(\sum_{i=0}^{\beta-1} a_i \theta^{ip^\alpha}\Big) = \sum_{i=1}^{\beta-1} i a_i \theta^{(i-1)p^\alpha}.$$

Therefore $\beta \equiv 0$ (mod p) and if $a_i \neq 0$, then $i \equiv 0$ (mod p). Hence θ is an inseparable element of exponent $> \alpha$ over k. This is contradiction, and we have obtained the following.

THEOREM. *Let K be an extension field of a field k of characteristic $p \neq 0$. If there exists an inseparable algebraic element such that it is not contained in $k(K^p)$, then K is not rigid, and a non-trivial integrable element of $H_c^2(K, K)$ is found in the image of Sq_p.*

Remark 2. Let K be an algebraic extension field of a field k. By [1, p 79, Cor. 2] and the above theroem, K is separable over k if and only if considered as an algebra over k, K is rigid.

REFERENCES

[1] M. Gerstenhaber: On the deformation of rings and algebras, Ann. of Math. **79** (1964), 59–103.

[2] D.K. Harrison: Commutative algebras and cohomology, Trans. Amer. Math. Soc., **104** (1962), 191–204.
[3] N. Jacobsen: Lectures in abstract algebra **III**, Van Nastrand, 1964.
[4] H. Kimura: Existence of non-trivial deformations of some inseparable extension fields, Nagoya Math. J. 31 (1968), 37–40.

Nagoya University