Algebra and Discrete Mathematics RESEARCH ARTICLE
Volume 10 **(2010)**. Number 2. pp. 87 – 95

On separable and H-separable polynomials in skew polynomial rings of several variables

Shûichi Ikehata

Communicated by V. V. Kirichenko

Abstract. Let B be a ring with 1, and $\{\rho_1, \cdots, \rho_e\}$ a set of automorphisms of B. Let $B[X_1, \cdots, X_e; \rho_1, \cdots, \rho_e; \{u_{ij}\}]$ be the skew polynomial ring of automorphism type. In this paper, we shall give equivalent conditions that the residue ring of $B[X_1, \cdots, X_e; \rho_1, \cdots, \rho_e; \{u_{ij}\}]$ by the ideal generated by a set $\{X_1^{m_1} - u_1, \cdots, X_e^{m_e} - u_e\}$ to be separable or H-separable over B.

1. Introduction

In [4], K. Hirata and K. Sugano generalized the notion of separable algebras to that of *separable* extensions of a ring. A ring extension T/S is called a *separable* extension if the T-T-homomorphism of $T \otimes_S T$ onto T defined by $a \otimes b \to ab$ splits, and T/S is called an *H-separable* extension if $T \otimes_S T$ is T-T-isomorphic to a direct summand of a finite direct sum of copies of T. As is well known an H-separable extension is a separable extension.

Throughout this paper, B will mean a ring with identity 1, ρ an automorphism of B, and Z the center of B. Let $B[X; \rho]$ be the skew polynomial ring in which the multiplication is given by $bX = X\rho(b)$ $(b \in B)$. A monic polynomial f in $B[X; \rho]$ such that $fB[X; \rho] = B[X; \rho]f$ is called a separable (resp. H-separable) polynomial if the residue ring $B[X; \rho]/fB[X; \rho]$ is a separable (resp. H-separable) extension of B. Separable polynomials in skew polynomial rings are extensively studied by Kishimoto, Nagahara, Miyashita, Szeto, Xue and the author (see References). In [9, 10],

2000 Mathematics Subject Classification: *16S30, 16W20.*

Key words and phrases: *H-separable polynomial, separable extension, skew polynomial ring.*

Kishimoto studied some special type of separable polynomials in skew polynomial rings. In [12], Nagahara gave a thorough investigation of separable polynomials of degree 2. Miyashita [11] studied systematically separable polynomials and Frobenius polynomials. The following is a theorem of Y. Miyashita which characterizes the sparability of $X^n - u$ in $B[X;\rho]$.

Proposition 1.1 ([11, Theorem 3.1])**.** *Let $f = X^n - u$ be in $B[X;\rho]$. Then the following conditions are equivalent:*

(1) *f is a separable polynomial in $B[X;\rho]$.*

(2) (i) *$\rho(u) = u$, and $\alpha u = u\rho^n(\alpha)$ for all $\alpha \in B$,*

(ii) *u is invertible in B^ρ, and there exists an element $z \in Z$ such that*
$z + \rho(z) + \cdots + \rho^{n-1}(z) = 1.$

In [6, 7, 8], the author has studied H-separable polynomials in skew polynomial rings. If the coefficient ring is commutative, the existence of an H-separable polynomial in a skew polynomial ring has been characterized in terms of Azumaya algebras and Galois extensions. Recall that a ring extension T/S is called G-Galois, if there exist a finite group G of automorphisms of T such that $S = T^G$ (the fix ring of G in T) and $\sum_i x_i\sigma(y_i) = \delta_{1,\sigma}$ $(\sigma \in G)$ for some finite number of elements $x_i, y_i \in T$. In [8], the author proved that $B[X;\rho]$ contains an H-separable polynomial of prime degree if and only if the center Z of B is a Galois extension over Z^ρ. In [13], G. Szeto and L. Xue have succeeded in a general degree case.

Proposition 1.2 ([13, Theorem 3.6])**.** *Let $f = X^n - u$ be in $B[X;\rho]$. Then the following conditions are equivalent:*

(1) *f is an H-separable polynomial in $B[X;\rho]$.*

(2) (i) *$\rho(u) = u$, and $\alpha u = u\rho^n(\alpha)$ for all $\alpha \in B$,*

(ii) *u is invertible in B^ρ, and Z/Z^ρ is a G-Galois extension, where G is the group generated by $\rho|Z$ of degree n.*

The purpose of this paper is to generalize these results to the skew polynomial rings in several variables.

2. Preliminaries

First of all, we shall state some elementary properties of separable and H-separable extensions which are useful in our subsequent study.

Lemma 2.1 ([4, Proposition 2.5 (1)]). *Let $R \supset S \supset T$ be ring extensions. If R/S and S/T are separable (resp. H-separable) extensions, then R/T is also a separable (resp. H-separable) extension.*

Lemma 2.2 ([4, Proposition 2.5 (2)]). *Let $R \supset S \supset T$ be ring extensions. If R/T is a separable extension, then R/S is a separable extension.*

Lemma 2.3 ([3, Proposition 4.3]). *Let $R \supset S \supset T$ be ring extensions. If R/T is an H-separable extension and S/T is a separable extension, then R/S is an H-separable extension.*

The following lemma must be well known but we could not find in the literature, so we give a proof.

Lemma 2.4. *Let Z be a commutative ring, and $G = N \times K$ a finite abelian group of automorphisms of Z. If Z/Z^G is a G-Galois extension, Then Z/Z^N is an N-Galois extension and Z^N/Z^G is a K-Galois extension.*

Proof. Since Z/Z^G is a G-Galois extension, there exist a G-Galois coordinate system $\{x_i, y_i\} \subset Z$ such that

$$\sum_i x_i \sigma(y_i) = \delta_{1,\sigma} \quad (\sigma \in G).$$

Then obviously, Z/Z^N is an N-Galois extension. By [2, Lemma 1.6], there exists an element $c \in Z$ such that $\mathrm{tr}_N(c) = \sum_{\sigma \in N} \sigma(c) = 1$. Then we can easily see that

$$\sum_i x_i \tau(\mathrm{tr}_N(y_i)) = \delta_{1,\tau} \quad (\tau \in K).$$

So we have

$$\sum_i \mathrm{tr}_N(x_i c) \tau(\mathrm{tr}_N(y_i)) = \delta_{1,\tau} \quad (\tau \in K).$$

This means $\{\mathrm{tr}_N(x_i c), \mathrm{tr}_N(y_i)\}$ is a K-Galois coordinate system for Z^N/Z^G. □

3. Main results

We need some notations as given by K. Kishimoto [9], S. Ikehata [7] and S. A. Amitsur and D. Saltman [1].

Let ρ_i $(1 \leqq i \leqq e)$ be automorphisms of a ring B, and let u_{ij} $(1 \leqq i, j \leqq e)$ be invertible elements in B such that

(i) $u_{ij} = u_{ji}^{-1}$, and $u_{ii} = 1$,

(ii) $\rho_i \rho_j \rho_i^{-1} \rho_j^{-1} = (u_{ij})_\ell (u_{ij}^{-1})_r$,

(iii) $u_{ij} \rho_j(u_{ik}) u_{jk} = \rho_i(u_{jk}) u_{ik} \rho_k(u_{ij})$.

Then the set of all polynomials in e indeterminates $\{X_1, X_2, \cdots, X_e\}$ is

$$\{\sum X_1^{\nu_1} X_2^{\nu_2} \cdots X_e^{\nu_e} b_{\nu_1\nu_2\cdots\nu_e} \mid b_{\nu_1\nu_2\cdots\nu_e} \in B, \nu_k \geqq 0\}$$

which is an associative ring such that the multiplication is defined by

$$aX_i = X_i\rho_i(a)\ (a \in B) \text{ and } \quad X_iX_j = X_jX_iu_{ij} \ \ (1 \leqq i, j \leqq e).$$

This ring is denoted by $\boldsymbol{R}_e = B[X_1, X_2, \cdots, X_e; \rho_1, \rho_2, \cdots, \rho_e; \{u_{ij}\}]$ and is called a skew polynomial ring of automorphism type.

Moreover, by $\boldsymbol{R}_k$ $(0 \leqq k \leqq e)$, we denote the skew polynomial ring $B[X_1, X_2, \cdots, X_k; \rho_1, \rho_2, \cdots, \rho_k; \{u_{ij}\}]$ which is a subring of $\boldsymbol{R}_e$, where $\boldsymbol{R}_0 = B$.

Remark 3.1. For a permutation π of $\{1, 2, \cdots, k\}$ $(k \leqq e)$, we have a B-ring automorphism

$$\boldsymbol{R}_k \cong B[X_{\pi(1)}, X_{\pi(2)}, \cdots, X_{\pi(k)}; \rho_{\pi(1)}, \rho_{\pi(2)}, \cdots, \rho_{\pi(k)}; \{u_{\pi(i)\pi(j)}\}]$$

which maps X_i to $X_{\pi(i)}$ $(1 \leqq i \leqq k)$.

Now, assume further that there exist elements u_i $(1 \leqq i \leqq e)$ in B such that

(iv) $\quad bu_i = u_i\rho_i^{m_i}(b)\ (b \in B)$

and

(v) $\quad \rho_j(u_i)u_{ji}\rho_i(u_{ji}) \cdots \rho_i^{m_i-1}(u_{ji}) = u_i\ (1 \leqq i \leqq e)$.

Then we have,

$$a(X_i^{m_i} - u_i) = (X_i^{m_i} - u_i)\rho_i^{m_i}(a)\ (a \in B)$$

and

$$X_j(X_i^{m_i} - u_i) = (X_i^{m_i} - u_i)X_ju_{ji}\rho_i(u_{ji}) \cdots \rho_i^{m_i-1}(u_{ji})\ (1 \leqq i, j \leqq e).$$

This means that $(X_i^{m_i} - u_i)\boldsymbol{R}_k = \boldsymbol{R}_k(X_i^{m_i} - u_i)$ is a two-sided ideal of $\boldsymbol{R}_k$ for $i \leqq k \leqq e$. The mapping $\bar{\rho}_i : \boldsymbol{R}_e \to \boldsymbol{R}_e$ defined by

$$\bar{\rho}_i(\sum X_1^{\nu_1} X_2^{\nu_2} \cdots X_e^{\nu_e} b_{\nu_1\nu_2\cdots\nu_e}) = \\ = \sum (X_1u_{1i})^{\nu_1}(X_2u_{2i})^{\nu_2} \cdots (X_eu_{ei})^{\nu_e}\rho_i(b_{\nu_1\nu_2\cdots\nu_e})$$

is an automorphism of $\boldsymbol{R}_e$ which is an extension of ρ_i.

For each i $(1 \leqq i \leqq e)$, we put here

$$\boldsymbol{B}_i = B[X_1, \cdots, X_{i-1}, X_{i+1}, \cdots, X_e; \rho_1, \cdots, \rho_{i-1}, \rho_{i+1}, \cdots, \rho_e; \{u_{ij}\}].$$

Naturally, we have

$$\boldsymbol{R}_e = \boldsymbol{B}_i[X_i; \bar{\rho}_i],$$

and

$$\beta(X_i^{m_i} - u_i) = (X_i^{m_i} - u_i)\bar{\rho}_i^{m_i}(\beta) \ (\beta \in \boldsymbol{B}_i) \ \text{ and } \bar{\rho}_i(u_i) = u_i,$$

where $\bar{\rho}_i$ means $\bar{\rho}_i|\boldsymbol{B}_i$.

Let $\boldsymbol{M} = (X_1^{m_1} - u_1, X_2^{m_2} - u_2, \cdots, X_e^{m_e} - u_e)$ be the two sided ideal of $\boldsymbol{R}_e$ generated by $\{X_1^{m_1} - u_1, X_2^{m_2} - u_2, \cdots, X_e^{m_e} - u_e\}$. Then the residue ring $\boldsymbol{R}_e/\boldsymbol{M}$ is a free ring extension over B with a basis

$$\{x_1^{\nu_1}x_2^{\nu_2}\cdots x_e^{\nu_e} \mid 0 \leqq \nu_i < m_i, 1 \leqq i \leqq e\}, \text{ where } x_i = X_i + \boldsymbol{M} \in \boldsymbol{R}_e/\boldsymbol{M}.$$

Since $\bar{\rho}_i(X_j^{m_j} - u_j) = (X_j^{m_j} - u_j)\rho_j^{m_j-1}(u_{ji})\rho_j^{m_j-2}(u_{ji})\cdots\rho_j(u_{ji})u_{ji}$, we obtain $\bar{\rho}_i(\boldsymbol{M}) = \boldsymbol{M}$. Hence, naturally $\bar{\rho}_i$ induces the automorphism $\bar{\rho}_i : \boldsymbol{R}_e/\boldsymbol{M} \to \boldsymbol{R}_e/\boldsymbol{M}$, where we use the same notation $\bar{\rho}_i$.

Under the above notations, we shall prove our first theorem which is a generalization of Proposition 1.1.

Theorem 3.2. *The following are equivalent.*

(1) $\boldsymbol{R}_e/\boldsymbol{M}$ *is a separable extension of* B.

(2) (i) $u_i \in U(B^{\rho_i}) \quad (1 \leqq i \leqq e)$.

(ii) *There exists an element* $z \in Z$ *such that*

$$\sum_{0\leqq\nu_1<m_1}\sum_{0\leqq\nu_2<m_2}\cdots\sum_{0\leqq\nu_e<m_e}\rho_1^{\nu_1}\rho_2^{\nu_2}\cdots\rho_e^{\nu_e}(z) = 1.$$

(3) $X_i^{m_i} - u_i$ *is a separable polynomial in* $\boldsymbol{B}_i[X_i; \bar{\rho}_i]$ *for each* i $(1 \leqq i \leqq e)$.

(4) (i) $u_i \in U(B^{\rho_i}) \quad (1 \leqq i \leqq e)$.

(ii) *There exist elements* $c_i \in Z^{\rho_1,\rho_2,\cdots,\rho_{i-1},\rho_{i+1},\cdots,\rho_e}$ *such that*

$$c_i + \rho_i(c_i) + \cdots + \rho_i^{m_i-1}(c_i) = 1.$$

Proof. (1) $\Longrightarrow$ (2). Let $\boldsymbol{M}_i$ be the ideal of $\boldsymbol{B}_i$ generated by $\{X_1^{m_1} - u_1, \cdots, X_{i-1}^{m_{i-1}} - u_{i-1}, X_{i+1}^{m_{i+1}} - u_{i+1}, \cdots, X_e^{m_e} - u_e\}$. Since $\bar{\rho}_i(\boldsymbol{M}_i) = \boldsymbol{M}_i$, we have that $\bar{\rho}_i$ induces the automorphism $\bar{\rho}_i : \boldsymbol{B}_i/\boldsymbol{M}_i \to \boldsymbol{B}_i/\boldsymbol{M}_i$. Then we have

$$\boldsymbol{R}_e/\boldsymbol{M} = (\boldsymbol{B}_i/\boldsymbol{M}_i)[X_i; \bar{\rho}_i]/(X_i^{m_i} - u_i)(\boldsymbol{B}_i/\boldsymbol{M}_i)[X_i; \bar{\rho}_i].$$

Since $\boldsymbol{R}_e/\boldsymbol{M} \supset \boldsymbol{B}_i/\boldsymbol{M}_i \supset B$ and $\boldsymbol{R}_e/\boldsymbol{M}$ is a separable extension of B, it follows from Lemma 2.2 that $\boldsymbol{R}_e/\boldsymbol{M}$ is also a separable extension of $\boldsymbol{B}_i/\boldsymbol{M}_i$, that is, $X_i^{m_i} - u_i$ is a separable polynomial in $(\boldsymbol{B}_i/\boldsymbol{M}_i)[X_i; \bar{\rho}_i]$. Then by Proposition 1.1, u_i is invertible in $\boldsymbol{B}_i^{\bar{\rho}_i}$, so is invertible in B^{ρ_i}, and there exists an element y_i in the center of $\boldsymbol{B}_i/\boldsymbol{M}_i$ such that

$$y_i + \bar{\rho}_i(y_i) + \cdots + \bar{\rho}_i^{m_i-1}(y_i) = 1.$$

Let c_i be the constant term of y_i. Then we see that c_i is in $Z^{\rho_1,\rho_2,\cdots,\rho_{i-1},\rho_{i+1},\cdots,\rho_e}$ and $c_i + \rho_i(c_i) + \cdots + \rho_i^{m_i-1}(c_i) = 1$. We put $z = c_1 c_2 \cdots c_e$. Then it is easy to see that

$$\sum_{0 \leqq \nu_1 < m_1} \sum_{0 \leqq \nu_2 < m_2} \cdots \sum_{0 \leqq \nu_e < m_e} \rho_1^{\nu_1} \rho_2^{\nu_2} \cdots \rho_e^{\nu_e}(z) = 1.$$

This completes the proof of (1) $\Longrightarrow$ (2).

(2) $\Longrightarrow$ (3). We put here

$$c_i = \sum_{0 \leqq \nu_1 < m_1} \cdots \sum_{0 \leqq \nu_{i-1} < m_{i-1}} \sum_{0 \leqq \nu_{i+1} < m_{i+1}} \cdots \sum_{0 \leqq \nu_e < m_e} \rho_1^{\nu_1} \cdots \rho_{i-1}^{\nu_{i-1}} \rho_{i+1}^{\nu_{i+1}} \cdots \rho_e^{\nu_e}(z).$$

Then we obtain $c_i \in Z^{\rho_1,\rho_2,\cdots,\rho_{i-1},\rho_{i+1},\cdots,\rho_e}$, and

$$\begin{aligned} c_i + \rho_i(c_i) + \cdots + \rho_i^{m_i-1}(c_i) &= \\ &= \sum_{0 \leqq \nu_1 < m_1} \sum_{0 \leqq \nu_2 < m_2} \cdots \sum_{0 \leqq \nu_e < m_e} \rho_1^{\nu_1} \rho_2^{\nu_2} \cdots \rho_e^{\nu_e}(z) = 1. \end{aligned}$$

Since c_i is in the center of $\boldsymbol{B}_i$, $X_i^{m_i} - u_i$ is a separable polynomial in $\boldsymbol{B}_i[X_i; \bar{\rho}_i]$ by Proposition 1.1.

(3) $\Longrightarrow$ (4). By Proposition 1.1, there exists y_i in the center of $\boldsymbol{B}_i$ such that $y_i + \bar{\rho}_i(y_i) + \cdots + \bar{\rho}_i^{m_i-1}(y_i) = 1$. Considering the constant term of y_i, we have (4).

(4) $\Longrightarrow$ (1). We put here

$$\boldsymbol{S}_0 = B \quad \text{and} \quad \boldsymbol{S}_1 = B[X_1; \rho_1]/(X_1^{m_1} - u_1)B[X_1; \rho_1],$$

and for each $1 \leqq i \leqq e$,

$$\boldsymbol{S}_i = \boldsymbol{S}_{i-1}[X_i; \bar{\rho}_i]/(X_i^{m_i} - u_i)\boldsymbol{S}_{i-1}[X_i; \bar{\rho}_i],$$

where $\bar{\rho}_i : \boldsymbol{S}_{i-1} \to \boldsymbol{S}_{i-1}$ is a natural extension of ρ_i. Then, we have

$$\boldsymbol{R}_e/\boldsymbol{M} = \boldsymbol{S}_e \supset \boldsymbol{S}_{e-1} \supset \cdots \supset \boldsymbol{S}_1 \supset \boldsymbol{S}_0 = B.$$

It is clear that each $X_i^{m_i} - u_i$ is a separable polynomial in $\boldsymbol{S}_{i-1}[X_i; \bar{\rho}_i]$. That is, $\boldsymbol{S}_i$ is a separable extension of $\boldsymbol{S}_{i-1}$. By the Lemma 2.1, we have $\boldsymbol{R}_e/\boldsymbol{M}$ is a separable extension of B. □

The following is a main theorem concerning to an H-separable extension which is a generalization of Proposition 1.2. We also use the notations in the proof of the previous theorem.

Theorem 3.3. *The following are equivalent.*

(1) $\boldsymbol{R}_e/\boldsymbol{M}$ *is an* H*-separable extension of* B*, and the centralizers of* B *in* $\boldsymbol{R}_e/\boldsymbol{M}$*,* $V_{\boldsymbol{R}_e/\boldsymbol{M}}(B) = Z$*.*

(2) $X_i^{m_i} - u_i$ *is an* H*-separable polynomial in* $\boldsymbol{S}_{i-1}[X_i; \bar{\rho}_i]$ *for each* i $(1 \leqq i \leqq e)$*.*

(3) (i) $u_i \in U(B^{\rho_i}) \quad (1 \leqq i \leqq e)$*.*

(ii) *The order of* $(\rho_i|Z) = m_i$ $(1 \leqq i \leqq e)$*, the set* $\{\rho_i|Z\ |1 \leqq i \leqq e\}$ *generates an abelian group* $< \rho_1|Z > \times < \rho_2|Z > \times \cdots \times < \rho_e|Z >= G$*, and* Z/Z^G *is a* G*-Galois extension.*

Proof. (3) $\Longrightarrow$ (2). We consider the following tower

$$Z \supset Z^{\rho_1} \supset Z^{\rho_1,\rho_2} \supset \cdots \supset Z^{\rho_1,\cdots,\rho_e} = Z^G.$$

Since $G =< \rho_1|Z > \times < \rho_2|Z > \times \cdots \times < \rho_e|Z >$ and Z/Z^G is a G-Galois extension of order $m_1 m_2 \cdots m_e$, it follows from Lemma 2.4 that $Z^{\rho_1,\cdots,\rho_{i-1}}/Z^{\rho_1,\cdots,\rho_{i-1},\rho_i}$ is a $< \rho_i|Z^{\rho_1,\cdots,\rho_{i-1}} >$- Galois extension of order m_i for each i $(1 \leqq i \leqq e)$. Then an easy induction shows that the center of $\boldsymbol{S}_{i-1}$ is equal to $Z^{\rho_1,\cdots,\rho_{i-1}}$. Thus, $X_i^{m_i} - u_i$ is an H-separable polynomial in $\boldsymbol{S}_{i-1}[X_i; \bar{\rho}_i]$ by Proposition 1.2.

(2) $\Longrightarrow$ (1), (3). We consider the following tower

$$\boldsymbol{R}_e/\boldsymbol{M} = \boldsymbol{S}_e \supset \cdots \supset \boldsymbol{S}_i \supset \boldsymbol{S}_{i-1} \supset \cdots \supset \boldsymbol{S}_1 \supset \boldsymbol{S}_0 = B.$$

Since $X_i^{m_i} - u_i$ is an H-separable polynomial in $\boldsymbol{S}_{i-1}[X_i; \bar{\rho}_i]$, $\boldsymbol{S}_i/\boldsymbol{S}_{i-1}$ is an H-separable extension. Hence by Lemma 2.1, $\boldsymbol{R}_e/\boldsymbol{M}$ is an H-separable extension of B. To prove $V_{\boldsymbol{R}_e/\boldsymbol{M}}(B) = Z$, we shall show that the group G generated by $\{\rho_1|Z, \rho_2|Z, \cdots, \rho_e|Z\}$ is a direct product $< \rho_1|Z > \times < \rho_2|Z > \times \cdots \times < \rho_e|Z >$, and Z/Z^G is a G-Galois extension. By an induction, it is easy to verify that the center of $\boldsymbol{S}_{i-1}$ is equal to $Z^{\rho_1,\cdots,\rho_{i-1}}$, and $Z^{\rho_1,\cdots,\rho_{i-1}}/Z^{\rho_1,\cdots,\rho_{i-1},\rho_i}$ is a $< \rho_i|Z^{\rho_1,\cdots,\rho_{i-1}} >$- Galois extension of order m_i. Since $(\rho_i|Z)^{m_i} = m_i$ $(1 \leqq i \leqq e)$, G must be a direct product, that is, $G =< \rho_1|Z > \times < \rho_2|Z > \times \cdots \times < \rho_e|Z >$, and Z/Z^G is a G-Galois extension. By a computation using a G-Galois coordinate system for Z/Z^G, we can easily see that $V_{\boldsymbol{R}_e/\boldsymbol{M}}(B) = Z$.

(1) $\Longrightarrow$ (2). Consider the following.

$$\boldsymbol{R}_e/\boldsymbol{M} = (\boldsymbol{B}_i/\boldsymbol{M}_i)[X_i; \bar{\rho}_i]/(X_i^{m_i} - u_i)(\boldsymbol{B}_i/\boldsymbol{M}_i)[X_i; \bar{\rho}_i] \supset \boldsymbol{B}_i/\boldsymbol{M}_i \supset B.$$

By the previous theorem, $\boldsymbol{B}_i/\boldsymbol{M}_i$ is a separable extension of B. Then by Lemma 2.3, we have $\boldsymbol{R}_e/\boldsymbol{M}$ is an H-separable extension of $\boldsymbol{B}_i/\boldsymbol{M}_i$, that is, $X_i^{m_i} - u_i$ is an H-separable polynomial in $(\boldsymbol{B}_i/\boldsymbol{M}_i)[X_i; \bar{\rho}_i]$. Since $V_{\boldsymbol{R}_e/\boldsymbol{M}}(B) = Z$, the center of $\boldsymbol{B}_i/\boldsymbol{M}_i$ is equal to $Z^{\rho_1,\rho_2,\cdots,\rho_{i-1},\rho_{i+1},\cdots,\rho_e}$. Hence $Z^{\rho_1,\rho_2,\cdots,\rho_{i-1},\rho_{i+1},\cdots,\rho_e}$ is a $<\rho_i|Z^{\rho_1,\rho_2,\cdots,\rho_{i-1},\rho_{i+1},\cdots,\rho_e}>$-Galois extension of $Z^{\rho_1,\rho_2,\cdots,\rho_e}$. By using the same Galois coordinate system, we see that $Z^{\rho_1,\rho_2,\cdots,\rho_{i-1}}$ is a $<\rho_i|Z^{\rho_1,\rho_2,\cdots,\rho_{i-1},\rho_i}>$-Galois extension of $Z^{\rho_1,\rho_2,\cdots,\rho_i}$. Thus, $X_i^{m_i} - u_i$ is an H-separable polynomial in $\boldsymbol{S}_{i-1}[X_i; \bar{\rho}_i]$ for each i $(1 \leqq i \leqq e)$ by Proposition 1.2. □

Remark 3.4. In case $e = 1$, the condition $V_{\boldsymbol{R}_e/\boldsymbol{M}}(B) = Z$ in Theorem 3.3 (1) is superfluous.

We conclude our study with an example of non separable extension $\boldsymbol{R}_2/\boldsymbol{M}$ of B, where $\boldsymbol{M} = (X_1^2 - 1, X_2^2 - 1)$ and $\boldsymbol{R}_2 = B[X_1, X_2; \rho_1, \rho_2]$, while each $X_i^2 - 1$ is a separable polynomial in $B[X; \rho_i]$ $(i = 1, 2)$.

Example 3.5. Let k be a field of a characteristic 2, $B = k \oplus k$, and $\rho : B \to B$ an automorphism defined by $\rho(a, b) = (b, a)$. Let $\rho_1 = \rho_2 = \rho$. Then we consider the skew polynomial ring $B[X_1, X_2; \rho_1, \rho_2]$ such that $\alpha X_1 = X_1\rho_1(\alpha), \alpha X_2 = X_2\rho_2(\alpha)$ $(\alpha \in B), X_1X_2 = X_2X_1$, that is, $u_{12} = u_{21} = 1$. Since $(1, 0) + \rho(1, 0) = (1, 1)$, each $X_i^2 - 1$ is a separable polynomial in $B[X; \rho_i]$ $(i = 1, 2)$. We put $\boldsymbol{R} = B[X_1, X_2; \rho_1, \rho_2]$, and $\boldsymbol{M}$ = the ideal generated by $\{X_1^2 - 1, X_2^2 - 1\}$. Then the residue ring $\boldsymbol{R}/\boldsymbol{M}$ is not a separable extension of B. Because for any $(a, b) \in B$, $(a, b) + \rho_1(a, b) + \rho_2(a, b) + \rho_1\rho_2(a, b) = 0$.

Acknowledgement. This work was done while the author was visiting at the Mathematics Department of Bradley University in spring 2009. He expresses his gratitude to Professor George Szeto and Professor Larry Xue for many useful discussions and the hospitality of the Mathematics Department of Bradley University.

References

[1] S. A. Amitsur and D. Saltman, Generic Abelian crossed products and p-algebras, *J. Algebra,* **51** 1978 , no. 1, pp.76–87.

[2] S. U. Chase, D. K. Harrison and A. Rosenberg, Galois theory and Galois cohomology ofcommutative ring, *Mem. Amer. Math. Soc.,* **52** 1965, pp.15–33.

[3] K. Hirata, Separable extensions and centralizers of rings, *Nagoya Math. J.,* **35** 1969, pp.31–45.

[4] K. Hirata and K. Sugano, On semisimple extensions and separable extensions overnon commutative rings, *J. Math. Soc. Japan,* **18** 1966, no. 2, pp.360–373.

[5] S. Ikehata, On separable polynomials and Frobenius polynomials in skew polynomial rings, *Math. J. Okayama Univ.,* **22** 1980, 115–129.

[6] S. Ikehata, Azumaya algebras and skew polynomial rings, *Math, J. Okayama Univ.,* **23** 1981, 19–32.

[7] S. Ikehata, Azumaya algebras and skew polynomial rings. II, *Math. J. Okayama Univ.,* **26** 1984, pp.49–57.

[8] S. Ikehata, On H-separable polynomials of prime degree, *Math. J. Okayama Univ.,* **33** 1991, 21–26.

[9] K. Kishimoto, On abelian extensions of rings. II, *Math. J. Okayama Univ.,* **15** 1971, 57–70.

[10] K. Kishimoto, A classification of free quadratic extensions of rings, *Math. J. Okayama Univ.,* **18** 1976, pp. 139–148.

[11] Y. Miyashita, On a skew polynomial ring, *J. Math. Soc. Japan,* **31** 1979, no. 2, 317–330.

[12] T. Nagahara, On separable polynomials of degree 2 in skew polynomial rings, *Math. J. Okayama Univ.,* **19** 1976, 65–95.

[13] G. Szeto and L. Xue, On the Ikehata theorem for H-separable skew polynomial rings, *Math. J. Okayama Univ.,* **40** 1998, 27–32.

Contact information

S. Ikehata

Department of Environmental and Mathematical Science, Faculty of Environmental Science and Technology, Okayama University, Tsushima, Okayama 700-8530, Japan
E-Mail: ikehata@ems.okayama-u.ac.jp

Received by the editors: 09.04.2009
and in final form 28.02.2011.