Mathematical Journal of Okayama University

Volume 26, *Issue* 1 1984 *Article* 10

JANUARY 1984

On splitting rings of separable skew polynomials

Takasi Nagahara*

*Okayama University

Math. J. Okayama Univ. 26 (1984), 71–85

ON SPLITTING RINGS OF SEPARABLE SKEW POLYNOMIALS

Dedicated to Professor Hirosi Nagao on his 60th birthday

TAKASI NAGAHARA

1. Introduction. In [10], [11] and [12], the author studied some splitting rings of separable polynomials over a commutative ring which are generalizations of usual splitting fields of separable polynomials over fields. These studies are concerned with imbeddings of separable extensions into Galois extensions (cf. [1], [3], [7], [13] and [18]). The present paper is about splitting rings of some type of separable polynomials in a skew polynomial ring of automorphism type.

Let B be an arbitrary ring with identity element 1, and $R = B[X;\rho]$ a skew polynomial ring $\sum_{i=0}^{\infty} X^i B$ whose multiplication is given by $bX = X\rho(b)$ $(b \in B)$ where ρ is an automorphism of B. A monic polynomial $f \in R$ is called to be *separable* if $Rf = fR$ and the factor ring R/fR is separable over B. When this is the case, there holds $X^{n-1}f = fX^{n-1}$ for $n = \deg f$, that is, the coefficients of f are ρ^{n-1}-invariant (see [15, Th. 1(b)] and [16, Lemma 2]). Moreover, $R_{(0)}^{\rho}$ denotes the set of monic polynomials f of R such that $Rf = fR$ and $Xf = fX$. By [5, Lemma 1.1] and [16, Lemma 1], we see that for a monic polynomial $f \in R$ of degree n, f is in $R_{(0)}^{\rho}$ if and only if $Xf = fX$ and $bf = f\rho^n(b)$ for all $b \in B$. Now, let $f = X^n - X^{n-1}a_{n-1} - \cdots - Xa_1 - a_0 \in R_{(0)}^{\rho}$. Then $\rho(a_i) = a_i$ and $ba_i = a_i\rho^{n-i}(b)$ for all $b \in B$ $(i = 0, 1, \ldots, n-1)$. Hence $a_ia_j = a_ja_i$ for each i, j. By C_f, we denote the (commutative) subring of B generated by the coefficients of f. Then $f \in C_f[X] \subset R$, and the factor ring $C_f[X]/C_f[X]f$ is a free C_f-module with a basis $\{1, x, \ldots, x^{n-1}\}$ where $x = X + C_f[X]f$. By t, we denote the trace map of $C_f[X]/C_f[X]f$ to C_f. As in [10], by $\delta(f)$, we denote the determinant of the matrix $\| t(x^ix^j) \|$ $(0 \leqq i, j \leqq n-1)$, which will be called the discriminant of f. If $\delta(f)$ is inversible in B then f will be called to be *s-separable*. Clearly $X^n \in R_{(0)}^{\rho}$ $(n > 0)$, and X is s-separable. Our s-separability coincides with the $\tilde{\rho}$-separability in S. Ikehata [5]. Moreover, any s-separable polynomial is separable (Cor. 5). The converse holds if $\rho = 1$ (cf. [5, Th. 2.2], [10, Th. 2.1]). As to case $\rho \neq 1$, note that for some R, $R_{(0)}^{\rho}$ contains separable polynomials which are not s-separable (cf. [17, Examples]).

In § 2, we shall present a splitting ring for any s-separable polynomial

f, which is universal with respect to the condition of splitting rings and is a Galois extension of B containing the separable extension R/fR of B. In § 3, we shall study splitting rings of s-separable polynomials in case that B is a (two-sided) simple ring, and we shall prove that any s-separable polynomial has a splitting ring which is simple and is unique up to isomorphism. Moreover, we shall study a decomposition of any s-separable polynomial into irreducible s-separable polynomials.

In what follows, we shall summarize the notations and definitions which will be used very often in the subsequent study.

First, we shall give a notion which is a generalization of $R=B[X\,;\,\rho]$. Let $X_1,\dots,X_n$ be indeterminates which are independent. Then, for the semigroup $M=\{X_1^{s_1}\cdots X_n^{s_n}\,;\, s_i\geqq 0(i=1,\dots,n)\}$ $(X_iX_j=X_jX_i$ for all $i, j)$, the skew semigroup ring MB with $by=Y\rho^{\deg Y}(b)$ $(Y\in M,\ b\in B)$ will be denoted by $R_n=B[X_1,\dots,X_n\,;\,\rho]$, which is called the skew polynomial ring of $X_1,\dots,X_n$ with respect to ρ. Clearly, the mapping of R_n into itself defined by $Y_sb_s\to Y_s\rho(b_s)$ is an automorphism, which will be denoted by ρ. Moreover, for any two-sided ideal I of R_n with $\rho(I)=I$, the mapping of the factor ring R_n/I into itself defined by $Y_sb_s+I\to Y_s\rho(b_s)+I$ is an automorphism, which will be also denoted by ρ. For $g+I=g(X_1,\dots,X_n)+I\in R_n/I$, we write $\rho(g+I)=g^{\rho}(X_1,\dots,X_n)+I$.

Next, let A/B be any ring extension with the common identity 1, T a subring of A, and G a group of ring automorphisms of A. Then, we shall use the following conventions :

$T(G)=T^G=\{t\in T\,;\,\sigma(t)=t$ for all $\sigma\in G\}$.
$G(T)=\{\sigma\in G\,;\,\sigma(t)=t$ for all $t\in T\}$.
$G\,|\,T=$ the restriction of G to T.
$\mathrm{Aut}(A/T)=$ the set of T-ring automorphisms of A.
$A\backslash T=$ the complement of T in A.
$V_A(T)=$ the centralizer of T in A.
$C(T)=V_T(T)=$ the center of T.
$U(A)=$ the set of inversible elements in A.

If B is a direct summand of A_B (right B-module A) then $U(A)\cap B=U(B)$,

2. Splitting rings of polynomials in $R_{(0)}^{\rho}$. We shall begin the study with the following

Definition. If a ring extension of B is generated by a subset $E=$

$\{\alpha_1, \dots, \alpha_n\}$ such that $1\alpha_i = \alpha_i$, $\alpha_i\alpha_j = \alpha_j\alpha_i$ and $b\alpha_i = \alpha_i\rho(b)$ for all i, j and $b \in B$ then it will be denoted by $B[E\,;\,\rho]$ (or, abbr. $B[E]$). Let f be a polynomial in $R^{\rho}_{(0)}$ of degree n. If $S = B[E\,;\,\rho]$ and $\prod_{\alpha\in E}(X-\alpha) = f$ in $B^{\rho}[E][X]$ then S will be called *a splitting ring* of f (over B). Moreover, a splitting ring $A = B[x_1,\dots,x_n\,;\,\rho]$ of f is said to be *universal* if for any splitting ring $S = B[\alpha_1,\dots,\alpha_n\,;\,\rho]$ of f, there exists a B-ring homomorphism of $A \to S$ mapping x_i into α_i for $i = 1,\dots,n$.

Lemma 1. *Let f be a polynomial in $R^{\rho}_{(0)}$ of degree n, and $S = B[\alpha_1,\dots, \alpha_n\,;\,\rho]$ any splitting ring of f. Then $\{\alpha_1^{m_1}\cdots\alpha_n^{m_n}\,;\ 0 \leqq m_i \leqq n-i$ $(i = 0, 1, \dots, n-1)\}$ is a system of generators of S_B.*

Proof. In case $n = 1$, the assertion is trivial, and whence, let $n \geqq 2$. As is easily seen, we have $f_2 = (X-\alpha_2)\cdots(X-\alpha_n) \in B^{\rho}[\alpha_1][X]$. By induction methods, we have $f_m = (X-\alpha_m)\cdots(X-\alpha_n) \in B^{\rho}[\alpha_1,\dots,\alpha_{m-1}][X]$ and $B[\alpha_1,\dots,\alpha_{m-1}][\alpha_m] = \sum_{i=0}^{n-m} B[\alpha_1,\dots,\alpha_{m-1}]\,\alpha_m^i$. From this, one will easily see the assertion.

Now, let $f = X^n - X^{n-1}a_{n-1} - \cdots - Xa_1 - a_0 \in R^{\rho}_{(0)}$ and $R_n = B[X_1,\dots, X_n\,;\,\rho]$. Moreover, for elementary symmetric polynomials s_i of $X_1,\dots, X_n$(deg $s_i = i$, $i = 1,\dots,n$), we set $t_i = a_{n-i} - s_i$ and $N_f = \sum_{i=1}^n t_iR_n$. Then $bt_i = t_i\rho^i(b)$ $(b \in B)$ and $t_iX_j = X_jt_i$ $(1 \leqq i, j \leqq n)$. Hence Nf is an ideal of R_n and $\rho(N_f) = N_f$. By R_f, we denote the factor ring R_n/N_f. Under this situation, we shall prove the following

Theorem 2. *Let f be a polynomial in $R^{\rho}_{(0)}$ of degree n. Then R_f is a universal splitting ring of f. Moreover, for any universal splitting ring $A = B[x_1,\dots,x_n\,;\,\rho]$ of f, there holds that*

(1) *A is B-ring isomorphic to R_f under the map $u(x_1,\dots,x_n) \to u(X_1,\dots,X_n) + N_f$.*

(2) $\{x_1^{m_1}\cdots x_n^{m_n}\,;\ 0 \leqq m_i \leqq n-i\ (i = 1,\dots,n)\}$ *is a free B-basis of A_B.*

Proof. First, we shall show that f has a splitting ring which satisfies the condition (2). In case $\deg f = 1$, the assertion is obvious. Assume that $\deg f > 1$ and the assertion holds for every $g \in R^{\rho}_{(0)}$ with $\deg g < \deg f$. We set $B[x_1] = B[X_1\,;\,\rho]/f(X_1)B[X_1\,;\,\rho]$, and $x_1 = X_1 + f(X_1)B[X_1\,;\,\rho]$. Obviously

$$f(X) = (X-x_1)g(X) \text{ in } B[x_1][X\,;\,\rho].$$

Then, $g(X)$ is monic and deg $g(X) = n-1$. Moreover, we have

$$(X-x_1)g^{\rho}(X) = f(X) = (X-x_1)g(X),$$

and for $x_1^m b \in B[x_1]$ $(0 \leqq m \leqq n-1,\ b \in B)$,

$$(X-x_1)x_1^m bg(X) = x_1^m \rho^{-1}(b)(X-x_1)g(X) = x_1^m \rho^{-1}(b)f(X)$$
$$= f(X)x_1^m \rho^{n-1}(b) = (X-x_1)g(X)\rho^{n-1}(x_1^m b).$$

Hence, it follows that $g^{\rho}(X) = g(X)$ and $ug(X) = g(X)\rho^{n-1}(u)(u \in B[x_1])$. This implies

$$g(X) \in B[x_1][X;\rho]^{\rho}_{(0)}.$$

Therefore, by our assumption, $g(X)$ has a splitting ring $B[x_1][x_2,\dots,x_n;\rho]$ which is a free $B[x_1]$-module with a basis

$$\{x_2^{m_2}\cdots x_n^{m_n}\,;\ 0 \leqq m_i \leqq n-i\ \ (i = 2,\dots,n)\}.$$

Since $u(x_1)x_i = x_i u^{\rho}(x_1)(i = 2,\dots,n,\ u(x_1) \in B[x_1])$, we have $x_1 x_i = x_i x_1$ and $bx_i = x_i\rho(b)(i = 2,\dots,n,\ b \in B)$. Moreover, we have

$$f(X) = (X-x_1)g(X) = (X-x_1)(X-x_2)\cdots(X-x_n).$$

in $B^{\rho}[V][X]$ where $V = \{x_1,\dots,x_n\}$. Hence $B[V]$ is a splitting ring of $f(X)$. Since $\{x_1^{m_1}\,;\ 0 \leqq m_1 \leqq n-1\}$ is a free B-basis of $B[x_1]_B$,

$$\{x_1^{m_1}\cdots x_n^{m_n}\,;\ 0 \leqq m_i \leqq n-i\ \ (i = 1,\dots,n)\}$$

is a free B-basis of $B[V]_B$. Now, as is easily seen, the map $\phi\colon R_n \to B[V]$ defined by

$$\sum (X_1^{r_1}\cdots X_n^{r_n})b_r \to \sum (x_1^{r_1}\cdots x_n^{r_n})b_r$$

is a B-ring homomorphism. Since ker $\phi \supset N_f$, ϕ induces a ring homomorphism $\bar{\phi}\colon R_f \to B[V]$, and $N_f \cap B = \{0\}$. Moreover, we see that R_f is a splitting ring of $f(X)$. By Lemma 1,

$$\{X_1^{m_1}\cdots X_n^{m_n}+N_f\,;\ 0 \leqq m_i \leqq n-i\ \ (i = 1,\dots,n)\}$$

is a system of generators of $(R_f)_B$. This implies that $\bar{\phi}$ is an isomorphism. Next, let $A_1 = B[y_1,\dots,y_n;\rho]$ be any universal splitting ring of f. Then, there is a B-ring homomorphism $\psi\colon A_1 \to R_f$ mapping y_i into $X_i + N_f$. for $i = 1,\dots,n$. By Lemma 1, one will easily see that ψ is an isomorphism. This completes the proof.

Now, let $f \in R^{\rho}_{(0)}$, and $B[E;\rho]$ a splitting ring of f. Then $f \in C_f[X]$ and $C_f[E]$ is a splitting ring of f over C_f where C_f is a (commutative) subring of B generated by the coefficients of f (cf. §1). Hence, by virtue of [10, Th. 1.2], we obtain the following

Theorem 3. *Let f be a polynomial in $R_{(0)}^{\rho}$ of degree n, and $B[\alpha_1,\ldots,\alpha_n;\rho]$ any spplitting ring of f. Then $\delta(f)=\Pi_{i<j}(\alpha_i-\alpha_j)^2$.*

Now, for $f\in R_{(0)}^{\rho}$, we consider a univarsal spliting ring $A=B[x_1,\ldots,x_n;\rho]$. Let S_n be the symmetric group of the set $\{1,\ldots,n\}$. Then, for every $\pi\in S_n$, we have a B-ring automorphism π^* of A mapping x_i into $x_{\pi(i)}$ for $i=1,\ldots,n$. Obviously, the mapping (*) : $\pi\to\pi^*$ is a group homomorphism of S_n into the group of B-ring automorphisms of A. In the remaining of this paper, the image of (*) will be denoted by S_V where $V=\{x_1,\ldots,x_n\}$. In case $n>2$, we see that (*) is a monomorphism, that is, $S_n\simeq S_V$ (cf. [10, Remark 1.1]).

Next, let $f\in R_{(0)}^{\rho}$, and $T=R/Rf$. Then, f will be called to be *Galois* if T is Galois over B. Moreover, f will be said *a polynomial of Galois type* if T is imbedded in a G-Galois extension N of B with $N(G(T))=T$. When this is the case, if B is a direct summand of N_B then f is separable by the results of [4, Prop. 3.4] and [8, p.118]. In [14] and [17], we proved that in case $\deg f=2$, f is s-separable if and only if it is Galois, which is equivalent to that f is of Galois type. Further, in [17] we presented some examples of separable polynomials which are not of Galois type and not s-separable.

Now, we shall prove the following

Theorem 4. *Let f be a polynomial in $R_{(0)}^{\rho}$ of degree n, and $A=B[V;\rho]$ ($V=\{x_1,\ldots,x_n\}$) be a universal splitting ring of f. Then, the following conditions are equivalent.*

(a) *f is s-separable.*

(b) *$A/B[V\backslash W]$ is S_W-Galois for every subset W of V.*

(c) *$A/B[V\backslash\{x_1,x_2\}]$ is Galois.*

(d) $x_1-x_2\in U(A)$.

Proof. In case $n=1$, the theorem is trivial, and whence, let $n\geqq 2$. First, we shall show that (a) implies (b). If $n=2$, the assertion follows immediately from the result of [14, Th. 2.5]. Hence, we assume that $n>2$ and the assertion holds for every $g\in R_{(0)}^{\rho}$ with $2\leqq\deg g<n$. Glearly $A=B[x_1][x_2,\ldots,x_n]$ is a universal splitting ring of $g=\Pi_{i\neq 1}(X-x_i)\in B[x_1][X;\rho]$. Since $\delta(f)=\Pi_{i<j}(x_i-x_j)^2\in u(B)$(Th. 3), we have $\delta(g)=$

$\Pi_{1<i<j}(x_i-x_j)^2 \in U(B[x_1])$. This implies that g is s-separable over $B[x_1]$. Hence, by the induction assumption, we see that $A/B[W]$ is $S_{V\setminus W}$-Galois for every subset W of V containing x_1, and whence $A(S_V) \subset B[x_1]$. Let $a = \sum_{k=0}^{n-1} x_1^k b_k$ ($b_k \in B$) be an element of $A(S_V)$. Then

$$\sum_{k=1}^{n-1} x_i^k b_k + (b_0 - a) = 0 \text{ for } i = 1,\dots,n.$$

For the adjoint M of the matrix $\|x_i^k\|$ $(0 < i \leqq n,\ 0 \leqq k < n)$, we have $M\|x_i^k\| = (\det \|x_i^k\|)I = (\pm \Pi_{i<j}(x_i-x_j))I$ where I is the identity matrix of degree n. Then, it follows that $(\Pi_{i<j}(x_i-x_j))(b_0-a) = 0$, and whence $b_0 - a = 0$. This shows $A(S_V) = B$. Clearly, we have

$$\delta(f)^{-1}\,\Pi_{i<j}(x_i-\sigma(x_j))^2 = \delta_{1,\sigma} \quad (\sigma \in S_V)$$

which can be written as $\sum_i u_i\,\sigma(v_i)$ ($\{u_i\}, \{v_i\} \subset A$). This gives a S_V-Galois coordinate system for A/B. Hence A/B is S_V-Galois (cf. [8, p.116]). Thus, we obtain (b). The implication (b) $\Rightarrow$ (c) is obvious. Assume (c), and set $A_1 = B[V\setminus\{x_1, x_2\}]$. Then, we have $g = (X-x_1)(X-x_2) \in A_1[X;\rho]$ and $A \simeq A_1[X;\rho]/gA_1[X;\rho]$ (A_1-ring isomorphism with $x_1 \to X + gA_1[X;\rho]$). Since A is Galois over A_1, it follows from [14, Th. 2.5] that $\delta(g) = (x_1-x_2)^2 \in U(A_1)$, which implies (d). Lastly, we assume (d). For any $1 \leqq i \leqq j \leqq n$, we have $x_i - x_j = \pi^*(x_1-x_2) \in U(A)$ for some $\pi^* \in S_V$. From this and Th. 3, it follows that $\delta(f) = \Pi_{i<j}(x_i-x_j)^2 \in B \cap U(A) = U(B)$, and so, f is s-separable. This completes the proof.

As a direct consequence of Th. 4, we obtain the following

Corollary 5. *Any s-separable polynomial in $R_{(0)}^{\rho}$ is a separable polynomial of Galois type.*

Next, we shall prove the following theorem which is useful in the subsequent consideration.

Theorem 6. *Let f be an s-separable polynomial in $R_{(0)}^{\rho}$ of degree $n \geqq 2$, and $A = B[V;\rho]$ a universal splitting ring of f. Then, there exists a 1–1 correspondence between the set of (two-sided) ideals I of A with $\sigma(I) = I$ for all $\sigma \in S_V$ and the set of ideals J of B with $\rho(J) = J$ such that*

$$I = AJ \longleftrightarrow I \cap B = J.$$

Proof. Let $V = \{x_1,\dots,x_n\}$. Then, we have $bx_i = x_i\rho(b)$ for all $b \in B$ ($i = 1,\dots,n$). Now, let J be an ideal of B with $\rho(J) = J$. Clearly $Jx_i =$

$x_iJ\,(i=1,\dots,n)$. Hence by Th. 2, we have $JA=AJ$ and $\sigma(AJ)=AJ$ for all $\sigma\in S_V$. Moreover, since B is a direct summand of A_B, we have $AJ\cap B=J$. Next, let I be an ideal of A with $\sigma(I)=I$ for all $\sigma\in S_V$, and set $J=I\cap B$. Since $x_1-x_2\in U(A)$, it follows that $(x_1-x_2)^{-1}J(x_1-x_2)=\rho(J)\subset B\cap I$ and $(x_1-x_2)J(x_1-x_2)^{-1}=\rho^{-1}(J)\subset B\cap I$. This implies $\rho(J)=J$. Hence, it suffices to prove that $AJ=I$. Firstly, we consider the case $n=2$, that is, $A=x_1B+B$. Let $a=x_1b_1+b_0\in I\,(b_1,\ b_0\in B)$, and $\sigma\neq 1\in S_V$. Then, we have $\sigma(x_1)=x_2$ and $\sigma(a)-a=(x_2-x_1)b_1$. Since $x_2-x_1\in U(A)$, it follows that $(x_2-x_1)^{-1}(a-\sigma(a))=b_1\in I\cap B=J$, and so, $b_0\in J$. Thus, we obtain $I=AJ$. Now, we assume that $n>2$ and the assertion holds for any s-separable polynomial g in $R^{\rho}_{(0)}$ with $2\leqq \deg g<n$. We set here $B_1=B[x_1]$, and $g=(X-x_2)\cdots(X-x_n)$. Then $g\in B_1[X;\rho]$. Moreover, g is s-separable and A is a universal aplitting ring of g over B_1. Hence $A(I\cap B_1)=I$ by our assumption. Next, we shall show $B_1(I\cap B)=I\cap B_1$. Clearly $B_1(I\cap B)\subset I\cap B_1$. Let $a=\sum_{k=0}^{n-1}x_1^kb_k\in I\cap B_1\,(b_k\in B)$. Then, for any i, there exists an element $\sigma_i\in S_V$ such that $\sigma_i(x_1)=x_i$. Hence we obtain

$$\sigma_i(a)=\sum_k x_i^kb_k\ (i=1,\dots,n)$$

Since the matrix $\|x_i^k\|\ (i=1,\dots,n,\ k=0,1,\dots,n-1)$ is inversible in A, it follows that $b_0,\dots,b_{n-1}\in I\cap B$. Hence $B_1(I\cap B)\ni a$, and so, $B_1(I\cap B)=I\cap B_1$. Thus, we obtain

$$A(I\cap B)=AB_1(I\cap B)=A(I\cap B_1)=I.$$

This completes the proof.

Corollary 7. *Let f be an s-separable polynomial in $R^{\rho}_{(0)}$, and A a universal splitting ring of f.*

(i) *If B is semisimple then so is A.*

(ii) *If B is semiprime then so is A.*

Proof. (i). Let $I=\mathrm{Rad}(A)$, the Jacobson radical of A. Then $\sigma(I)=I$ for all $\sigma\in S_V$, and whence $A(I\cap B)=I$ by Th. 6. Since A is Galois over B (Th. 4), there holds that $I\cap B\subset\mathrm{Rad}(B)$. Hence, if B is semisimple (that is, $\mathrm{Rad}(B)=\{0\}$) then $I=\{0\}$, and so, A is semisimple. (ii). Let N be a nilpotent ideal of A. Then $I=\sum_{\sigma\in S_V}\sigma(N)$ is a nilpotent ideal such that $\sigma(I)=I$ for all $\sigma\in S_V$, and $I\cap B$ is a nilpotent ideal of B. Hence, if B is semiprime then $I=A(I\cap B)=\{0\}$ (Th. 6), and whence, A

is semiprime.

3. On splitting rings of s-separable polynomials in $R^{\rho}_{(0)}$ over a simple ring. In this section, a simple ring means a two-sided simple ring which is not necessarily Artin. Moreover, B will always mean a simple ring. For $f \in R^{\rho}_{(0)}$, a splitting ring of f which is a simple ring will be called *a simple splitting ring* of f. Further, for any splitting ring $B[E\,;\,\rho]$ of f, the notation $B[E\,;\,\rho]$ will be abbreviated to $B[E]$.

First, we shall prove the following

Lemma 8. *Let f be an s-separable polynomial in $R^{\rho}_{(0)}$, and $A = B[V]$ a universal splitting ring of f. Then A is a direct sum of finite number of simple subrings which are ideals of A.*

Proof. Let $\deg f = n$, and $V = \{x_1, \dots, x_n\}$. If $n = 1$ then the assertion is trivial. Hence, we may assume $n \geqq 2$. Noting $1 \in A$, by Zorn's lemma, there exists a maximal ideal M of A. If $M = \{0\}$ then our assertion is obvious. Hence, we shall prove the assertion for the case $M \neq \{0\}$. Now, we set $I = \bigcap_{\sigma \in S_V} \sigma(M)$. Then $\sigma(I) = I$ for all $\sigma \in S_V$. Hence we have $I = \{0\}$ by Th. 6. Let $\{M_1, \dots, M_s\}$ be a minimal subset of $\{\sigma(\mathrm{M})\,;\, \sigma \in S_V\}$ such that $M_1 \cap \cdots \cap M_s = \{0\}$. Then, for all $1 \leqq i \leqq n$, we have $M_i \not\supset \bigcap_{j \neq i} M_j$, that is, $M_i + \bigcap_{j \neq i} M_j = A$, and whence, there exist elements $u_i \in M_i$ and $v_i \in \bigcap_{j \neq i} M_j$ such that $u_i + v_i = 1$. Then, for any elements $a_1, \dots, a_s \in A$, we have

$$a_1 v_1 + \cdots + a_s v_s = a_i \ (\mathrm{mod}\ M_i)$$

Therefore, it follows that A is isomorphic to the (ring) direct sum $A/M_1 \oplus \cdots \oplus A/M_s$ by the mapping $a \to (a + M_1, \dots, a + M_s)$. This shows the assertion.

Corollary 9. *Let f be an s-separable polynomial in $R^{\rho}_{(0)}$, and $A = B[V]$ a universal splitting ring of f. Let E be the set of primitive idempotents of $C(A)$. Then $E \neq \phi$ and $E = \{\sigma(e)\,;\,\sigma \in S_V\}$ for each $e \in E$. Moreover $\sum_{e \in E} e = 1$.*

Proof. By Lemma 8, one will easily see that $E \neq \phi$. Now, for $e \in E$, let $F = \{\sigma(e)\,;\,\sigma \in S_V\} = \{e_1, \dots, e_t\}$ where $e_i \neq e_j$ if $i \neq j$. Then, $d = e_1 + \cdots + e_t$ is an idempotent of $C(A)$, and $\sigma(d) = d$ for all $\sigma \in S_V$. Since A/B is S_V-Galois and B is simple, it follows that $d = 1$, the identity element of B and A. Hence $e' = de' \in F$ for all $e' \in E$. This implies $E = F$.

Lemma 10. *Let f be an s-separable polynomial in $R^{\rho}_{(0)}$, and $A = B[V]$ a universal splitting ring of f. Let e be a primitive idempotent of $C(A)$, and $H = S_V(e)$. Moreover, let $S_V = \sigma_1 H \cup \cdots \cup \sigma_s H$ ($\sigma_1 = 1$) be the decomposition into right cosets relative to the subgroup H. Then, there holds the following*

(i) *eA is a simple ring, $eB \simeq B$, and A is a direct sum of simple rings $\sigma_i(eA)$, $i = 1, \dots, s$.*

(ii) *eA is a $(H | eA)$-Galois extension of eB.*

(iii) *$eA = eB[eV]$ is a splitting ring of the s-separable polynomial ef in $eB[X ; \rho | eB]$.*

Proof. By Lemma 8, eA is a simple ring. Clearly $eB \simeq B$. We set $\sigma_i(e) = e_i$, $i = 1, \dots, s$. Then, $e_i \neq e_j$ if $i \neq j$. Since $\{e_1 = e, e_2, \dots, e_s\} = \{\sigma(e) ; \sigma \in S_V\}$, it follows from Cor. 9 that

$$A = e_1 A \oplus \cdots \oplus e_s A.$$

This shows (i). Next, we shall prove (ii). For any $a_1 \in A(H) \cap e_1 A (\supset e_1 B)$, we set $a_i = \sigma_i(a_1)$ ($i = 1, \dots, s$), and $a = a_1 + \cdots + a_s$. Let τ be an arbitrary element of S_V. Then $\{\tau(e_1), \dots, \tau(e_s)\} = \{e_1, \dots, e_s\}$. If $\tau(e_i) = e_1$ then $\tau\sigma_i \in H$, and so $\tau = \eta\sigma_i^{-1}$ for some $\eta \in H$, which implies $\tau(a_i) = \eta\sigma_i^{-1}(a_i) = \eta(a_1) = a_1$. Moreover, if $\tau(e_j) = e_k$ then $\sigma_k^{-1}\tau(e_j) = e_1$, and whence $\sigma_k^{-1}\tau(a_j) = a_1$, which shows $\tau(a_j) = \sigma_k(a_1) = a_k$. Hence we have $\tau(a) = a$. Thus we obtain $a \in A(S_V) = B$, and so, $a_1 = e_1 a \in e_1 B$. Therefore, it follows that $A(H) \cap e_1 A = e_1 B$, that is, $e_1 B = eB$ is the fixring of $H | eA$ in eA. Let $\{u_i, v_i ; i = 1, \dots, m\}$ be an S_V-Galois coordinate system for A/B. Then $\sum_i u_i \sigma(v_i) = \delta_{1,\sigma}$ ($\sigma \in S_V$). Hence $\sum_i eu_i \eta(ev_i) = e\delta_{1,\eta}$ for $\eta \in H$. Therefore, eA/eB is a $(H | eA)$-Galois extension. As to (iii), let C be the center of $A = B[V]$, $V = \{x_1, \dots, x_n\}$, and c an element of C. Then $(x_1 - x_2)c = c(x_1 - x_2) = (x_1 - x_2)\rho(c)$ where this ρ means the extension of ρ to A which has been defined in §1. Since $x_1 - x_2 \in U(A)$, we have $c = \rho(c)$. Hence, it follows that $\rho | C$ is identity, and so, $\rho(e) = e$. This implies that $\rho | eB$ is an automorphism of eB. Since $ebex_i = ex_i e\rho(b)$ ($i = 1, \dots, n$, $b \in B$), $eA = eB[eV]$ is a splitting ring of $ef (\in eB[X ; \rho | eB])$. Clearly $\delta(ef) = \prod_{i<j}(ex_i - ex_j)^2 = e\prod_{i<j}(x_i - x_j)^2 \in U(eA)$. Hence ef is an s-separable polynomial in $eB[X ; \rho | eB]$, completing

the proof.

Now, by virtue of Lemma 10, we shall prove the following

Theorem 11. *Let f be an s-separable polynomial in $R^{\rho}_{(0)}$.* Then, f has a *simple splitting ring. If $S = B[E]$ and $T = B[F]$ are simple splitting rings of f then there exists a B-ring isomorphism $\Phi : S \to T$ with $\Phi(E) = F$, and moreover, S is a G-Galois extension of B for $G = \{\sigma \in$* Aut(S/B) ; *$\sigma(E) = E\}$.*

Proof. The first assertion is a direct consequence of Lemma 10(i, iii) . Now, let $E = \{\alpha_1, \dots, \alpha_n\}$, $F = \{\beta_1, \dots, \beta_n\}$, and $A = B[V]$ $(V = \{x_1, \dots, x_n\})$ a universal splitting ring of f. Moreovr, let e be a primitive idempotent of $C(A)$. Then, by Lemma 10(i), we have

$$A = eA \oplus \sigma_2(e)A \oplus \cdots \oplus \sigma_s(e)A$$

for some $\sigma_2, \dots, \sigma_s \in S_V$. Further, we have B-ring homomorphisms

$$\phi : A \to S \text{ and } \psi : A \to T$$

where $\phi(x_i) = \alpha_i$ and $\psi(x_i) = \beta_i$ $(i = 1, \dots, n)$. Hence, since the $\sigma_i(e)A$ are simple, there exist some σ_h, σ_k $(\sigma_1 = 1)$ and ring isomorphisms

$$\mu : \sigma_h(e)A \to S \text{ and } \nu : \sigma_k(e)A \to T$$

such that $\mu(\sigma_h(e)b) = b$, $\mu(\sigma_h(e)x_i) = \alpha_i$, $\nu(\sigma_k(e)b) = b$, and $\nu(\sigma_k(e)x_i) = \beta_i$. Then, for $\tau = \sigma_k\sigma_h^{-1}$, we have $\tau(\sigma_h(e)x_i) = \sigma_k(e)\tau(x_i)$ with $\tau(x_i) \in V$ $(i = 1, \dots, n)$. Hence $\Phi = \nu\tau\mu^{-1}$ is a B-ring isomorphism of S onto T with $\Phi(E) = F$. Moreover, by Lemma 10(ii), S/B is a Galois extension with a Galois group K whose restriction to E is a permutation group on E. Now, let $G = \{\sigma \in \mathrm{Aut}(S/B) : \sigma(E) = E\}$. Then $K \subset G$, and whence $S(G) = B$. Noting $\prod_{i<j} (\alpha_i - \alpha_j)^2 = \delta(f) \in U(B)$, we see that $\delta(f)^{-1} \prod_{i<j} (\alpha_i - \sigma(\alpha_j))^2 = \delta_{1,\sigma}$ for all $\sigma \in G$. This gives a G-Galois coordinate system for A/B (cf. [8, p.116]). Thus S/B is G-Galois, and $G = K$ by [8, Prop. 2.2].

Corollary 12. *Let f be an s-separable polynomial in $R^{\rho}_{(0)}$. Then, any splitting ring of f is isomorphic to a direct sum (of finite number) of simple splitting rings of f, which is a Galois extension of B.*

Proof. Let A be a universal splitting ring of f, and T any splitting ring of f. Then, there exists a B-ring homomorphism of A onto T. Hence, it follows from Lemma 10 and Th. 11 that T is B-ring isomorphic to a direct sum T^* of simple rings A_i's such that $A_1 = A_i\,(i = 1,\dots,t)$, and A_1 is a G-Galois extension of B. Now, let G^* be a group of automorphisms σ^* of T^* such that

$$\sigma^* : (a_1,\dots,a_t) \to (\sigma(a_1),\dots,\sigma(a_t))\ (\sigma \in G)$$

and C a cyclic group generated by the automorphism

$$\gamma: (a_1,\dots,a_t) \to (a_2,\ a_3,\dots,a_t,\ a_1).$$

Then $\gamma\sigma^* = \sigma^*\gamma$ for all $\sigma^* \in G^*$. Hence $CG^* = G^*C$, which is a group. Moreover $T^*(CG^*) = B (= \{(b,\dots,b)\ ;\ b \in B\})$. Let $\{(u_i,\ v_i)\ ;\ i = 1,\dots, r\}$ be a G-Galois coordinate system for A_1/B, and $e_1 = (1,\ 0,\dots,0),\dots, e_t = (0,\dots,0,\ 1)$. Then $\sum_{j=1}^{t}\sum_{i=1}^{r}(u_ie_j)\,\tau(v_ie_j) = \delta_{1,\tau}$ for all $\tau \in CG^*$. This implies that T^* is a CG^*-Galois extension of B.

Lemma 13. *Let f be an s-separable polynomial in $R^o_{(0)}$, and $S = B[E]$ a simple splitting ring of f. Then, for any $\alpha \in E$, there holds that $S(G(B[\alpha])) = B[\alpha]$, where $G = \{\sigma \in \mathrm{Aut}(S/B)\ ;\ \sigma(E) = E\}$.*

Proof. Let $A = B[V]$ $(V = \{x_1,\dots,x_n\})$ be a universal splitting ring, e a primitive idempotent of $C(A)$, and $H = S_V(e)$. Then, by Lemma 10, eA is a $(H|eA)$-Galois extension of eB, and $eA = eB[eV]$ is a simple splitting ring of ef. Moreover, $H|eA = \{\tau \in \mathrm{Aut}(eA/eB)\ ;\ \tau(eV) = eV\}$. Hence, by Th. 11, there is a B-ring isomorphism ϕ of eA to $B[E]$ such that $\phi(eV) = E$. Without loss of generality, we may assume that $\phi(ex_1) = \alpha \neq 0$. Let $W = V\backslash\{x_1\}$, and $\{\sigma(e)\ ;\ \sigma \in S_W\} = \{e_1 = \sigma_1(e) = e,\ e_2 = \sigma_2(e),\dots,e_t = \sigma_t(e)\}$ where $\sigma_i \in S_W$, and $e_i \neq e_j$ if $i \neq j$ $(i,\ j = 1,\dots,t)$. Moreover, we set $\varepsilon = e_1+\cdots+e_t$, $\varepsilon' = 1-\varepsilon$, and $B_1 = B[x_1]$. Clearly

$$\sigma(\varepsilon) = \varepsilon \text{ and } \sigma(\varepsilon') = \varepsilon' \text{ for all } \sigma \in S_W$$
$$A = \varepsilon A \oplus \varepsilon' A,\ \varepsilon A = e_1A \oplus \cdots \oplus e_tA$$
$$B_1 = \varepsilon B_1 \oplus \varepsilon' B_1.$$

Since $A(S_W) = B_1$ (Th. 4), we have $\varepsilon A(S_W) = \varepsilon B_1$. Here, we set

$$H_1 = S_W(e_1), \text{ and } B_0 = e_1A(H_1).$$

Clearly $B_0 \supset e_1B_1$. Let $a_1 \in B_0$, and $a = \sum_{i=1}^{t}\sigma_i(a_1)$. Then by making use of the same methods as in the proof of Lemma 10(ii), we have $a \in \varepsilon A(S_W) = \varepsilon B_1$, which implies $a_1 = e_1a = e_1\varepsilon a \in e_1\varepsilon B_1 = e_1B_1$. Thus we obtain $B_0 = e_1B_1$. Since $H_1 \subset S_V(e_1) = H$ and $H_1 \subset H(e_1B_1)$, $e_1B_1 = eB[x_1]$ is the fixring of $H(eB[x_1])$ in eA. Therefore, combining this with the above isomorphism $\phi: eA \to B[E]$ with $\phi(ex_1) = \alpha$, we obtain $B[E](G(B[\alpha])) = B[\alpha]$.

Next, we shall prove the following

Theorem 14. *Let f be an s-separable polynomial in $R^{\rho}_{(0)}$, $S = B[E]$ a simple splitting ring of f, and $G = \{\sigma \in \mathrm{Aut}(S/B)\ ;\ \sigma(E) = E\}$. Then, for any subset F of E, $B[F]$ is a simple ring, $S(G(B[F])) = B[F]$, and if $F \neq \phi, \{0\}$ then $S = B[F] \otimes_K C(S)$ where $K = B[F] \cap C(S)$.*

Proof. Let $E = \{\alpha_1, \ldots, \alpha_n\}$ and $C = C(S)$. Since S is simple and $a\alpha_i = \alpha_i\rho(a)$ for all $a \in S$ $(i = 1, \ldots, n)$, we have $E \subset U(S) \cup \{0\}$, and C is a field. Now, $\alpha \neq 0$ will be an element in E. Then $E \subset \alpha C$ and so $S = B[\alpha]C$. Since $S(G(B[\alpha])) = B[\alpha]$ (Lemma 13), it follows that $P = C \cap B[\alpha]$ is a subfield of C, and C is a $(G(B[\alpha])|C)$-Galois extension of P. This enables us to see $S = B[\alpha] \otimes_P C$. Hence, if J is a proper ideal of $B[\alpha]$ then JC is also a proper ideal of S. Therefore, it follows that $B[\alpha]$ is a simple ring. Next, let F be a subset of E containing α. Then, noting $F \subset \alpha C$, we have $B[F] = B[\alpha] \otimes_P (B[F] \cap C)$, which is a simple ring. Moreover $S = B[F] \otimes_K C$ $(K = B[F] \cap C)$. From this, one will easily see that $S(G(B[F])) = B[F]$.

Lemma 15. *Let $f \in R^{\rho}_{(0)}$, and $f = gh$ in R. If $g \in R^{\rho}_{(0)}$ then $h \in R^{\rho}_{(0)}$. Moreover, $g \in R^{\rho}_{(0)}$ and f is s-separable if and only if g and h are s-separable and $gR + hR = R$.*

Proof. Let $\deg f = n$, $\deg g = s$, and $g \in R^{\rho}_{(0)}$. Then $gXh = Xf = fX = ghX$ and $g\rho^s(b)h = bf = f\rho^n(b) = gh\rho^n(b)$ for all $b \in B$. Since g is monic, this enables us to see that $h \in R^{\rho}_{(0)}$. By Th. 2, g has a universal splitting ring $B[V_1]$. Moreover, h $(\in B[V_1][X\ ;\ \rho])$ has also a universal splitting ring $B[V_1][V_2]$ over $B[V_1]$. Then $B[V_1 \cup V_2]$ is a splitting ring of f over B. Hence, by Th. 3, $\delta(g)$ is a divisor of $\delta(f)$. Now, we assume that f is s-separable. Since $\delta(f) \in U(B)$, we have $\delta(g) \in U(B)$. Hence g is s-separable. Similarly, h is s-separable. Next, let $\alpha \in V_1$. Then $g(\alpha) = 0$, and $h(\alpha) \in U(B[\alpha])$ by Th. 3. Since R/gR is B-ring isomorphic to $B[\alpha]$ under the map $u(X) + gR \to u(\alpha)$, it follows that $gR + hR = R$. As to the converse, we assume that g and h are s-separable and $gR + hR = R$.

Then $\delta(g)$ and $\delta(h)$ are in $U(B)$. Moreover, we see that $h(\alpha) \in U(B[\alpha])$ for every $\alpha \in V_1$ and $g(\beta) \in U(B[\beta])$ for every $\beta \in V_2$. Hence we have $\delta(f) \in U(B)$ by Th. 3. Thus f is s-separable. (Cf. Y. Miyashita [9, Th. 1.10].)

Now, a polynomial $f \in R^{\rho}_{(0)}$ will be called to be *irreducible* in $R^{\rho}_{(0)}$ if $f = gh$ and $g \in R^{\rho}_{(0)}$ then there holds always that either $g = 1$ or $h = 1$.

Next, we shall prove the following

Lemma 16. *Let f be an s-separable polynomial in $R^{\rho}_{(0)}$, $B[E]$ a simple splitting ring of f, and $G = \{\sigma \in \mathrm{Aut}(B[E]/B)\ ;\ \sigma(E) = E\}$. Let g be a factor of f in $R^{\rho}_{(0)}$. Then, g is irreducible in $R^{\rho}_{(0)}$ if and only if R/Rg is a simple ring. When this is the case, there exists an element α in E such that for $\{\sigma(\alpha)\ ;\ \sigma \in G\} = \{\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_s\}$ ($\alpha_i \neq \alpha_j$ if $i \neq j$), $\prod_{i=1}^{s}(X-\alpha_i)$ coincides with g, and $B[\alpha]$ is B-ring isomorphic to R/Rg under the map $u(\alpha) \to u(X) + Rg$.*

Proof. Let $f = gh$. By Lemma 15, g and h are s-separable. If R/Rg is simple then, one will easily see that g is irreducible in $R^{\rho}_{(0)}$. To see the converse, we assume that g is irreducible in $R^{\rho}_{(0)}$. Now, let $B[E_1]$ be a simple splitting ring of g, and $B[E_1][E_2]$ a simple splitting ring of h ($\in B[E_1][X;\rho]$) over $B[E_1]$. Then, $B[E_1 \cup E_2]$ is a splitting ring of f which is a simple ring. By Th. 11, we may assume that $E_1 \cup E_2 = E$. For an element $\alpha \in E_1$, we set $\{\sigma(\alpha)\ ;\ \sigma \in G\} = \{\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_s\}$ ($\alpha_i \neq \alpha_j$ if $i \neq j$), and $g_1 = \prod_{i=1}^{s}(X-\alpha_i)$. Then by Th. 11, we have $g_1 \in R$. Moreover, it is easily seen that g_1 is an s-separable polynomial in $R^{\rho}_{(0)}$, and the set $\{1, \alpha, \ldots, \alpha^{s-1}\}$ is B-free. Hence $R/Rg_1 \simeq B[\alpha]$ which is a simple ring by Th. 14. Noting $g_1(\alpha) = 0$ and $g(\alpha) = 0$, it follows that g_1 is a divisor of g. Since g is irreducible in $R^{\rho}_{(0)}$, we obtain $g = g_1$.

Now, in virtue of Lemma 16, we obtain the following

Theorem 17. *Let f be an s-separable polynomial in $R^{\rho}_{(0)}$ which is irreducible in $R^{\rho}_{(0)}$. Then, R/Rf is a simple ring, which is imbedded in a G-Galois extension N of B such that N is a simple ring and $N(G(R/Rf)) = R/Rf$.*

Lemma 18. *Let f be an s-separable polynomial in $R^{\rho}_{(0)}$, $B[E]$ a simple splitting ring of f, and $G = \{\sigma \in \mathrm{Aut}(B[E]/B)\ ;\ \sigma(E) = E\}$. Let $E = E_1 \cup \cdots \cup E_s$ be the decomposition of E into non-overlapping transitivity sets* *relative to G, and set* $g_i = \prod_{\alpha \in E_i}(X-\alpha)$ $(1 \leqq i \leqq s)$. *Then, for any decomposition* $f = f_1 \cdots f_t$ *into irreducible polynomials in* $R^{\rho}_{(0)}$, *there holds that* $t = s$, $\{f_1, \ldots, f_t\} = \{g_1, \ldots, g_t\}$, *and* $Rf_i + Rf_j = R$ *for all* $i \neq j$.

Proof. Since $f = \prod_{\alpha \in E}(X-\alpha)$, we have $f = g_1 \cdots g_s$. By Lemma 16, we have that for each $1 \leqq i \leqq t$, $f_i = g_j$ for some j. From this fact and Lemma 15, our assertion follows immediately.

In virtue of Lemma 15, Th. 17 and Lemma 18, we can prove the following

Theorem 19. *Let f be an s-separable polynomial in* $R^{\rho}_{(0)}$, *and* $f = f_1 \cdots f_s$ *a decomposition of f such that each* f_i *is irreducible in* $R^{\rho}_{(0)}$. *Then,* such a *decomposition of f is unique, and*

$$R/Rf \simeq R/Rf_1 \oplus \cdots \oplus R/Rf_s$$

where each R/Rf_i *is a simple ring extension of B.*

Proof. Let $f = f_1 \cdots f_s$ where each f_i is irreducible in $R^{\rho}_{(0)}$. Then, by the results of Lemma 17 and Lemma 18, it suffices to prove that $R/Rf \simeq R/Rf_1 \oplus \cdots \oplus R/Rf_s$. By Lemma 15, we have $f_iR + f_jR = R$ for all $i \neq j$. Note $f_if_j = f_jf_i$ and $f_iR = Rf_i$. Then $f_if_jR \subset f_iR \cap f_jR$, where $i \neq j$. Conversely, for any $g \in f_iR \cap f_jR$, we have $g \in gR = g(f_iR + f_jR) = gf_iR + gf_jR \subset f_if_jR$. Hence, it follows that $f_if_jR = f_iR \cap f_jR$. Moreover, for $k \neq i, j$, we have also $f_if_jR + f_kR = R$ and $f_if_jf_kR = f_if_jR \cap f_kR = f_iR \cap f_jR \cap f_kR$. Repeating the same procedures as in the above, we obtain that $\bigcap_{i \neq r} f_iR + f_rR = R$ $(1 \leqq r \leqq s)$ and $\bigcap_{i=1}^{s} f_iR = fR$. Therefore, by making use of the same methods as in the proof of Lemma 8 (i.e., by the Chinese remainder theorem), we obtain a B-ring isomorphism

$$R/Rf \rightarrow R/Rf_1 \oplus \cdots \oplus R/Rf_s$$

mapping $h + fR$ into $(h + f_1R, \ldots, h + f_sR)$.

Remark 20. As in the theory of fields, we can define an *s-separable closure* of (s-separable polynomials in) $R^{\rho}_{(0)}$, and we can prove that there exists an s-separable closure of $R^{\rho}_{(0)}$ which is a simple ring, and such closures are unique up to isomorphism. Moreover, this closure is an infinite Galois extension of B, in which we can construct a Galois theory of Krull's type. Further, we can characterize the s-separable polynomials in $R^{\rho}_{(0)}$ and the s-separable closure of $R^{\rho}_{(0)}$. These results will be detailed in "On splitting rings of separable skew polynomials II" to appear.

References

[1] M. Auslander and O. Goldman : The Brauer group of a commutative ring, Trans. Amer. Math. Soc. **97** (1960), 367—409.
[2] S. U. Chase, D. K. Harrison and Alex Rosenberg : Galois theory and Galois cohomology of commutative rings, Mem. Amer. Math. Soc. **52** (1965), 15—33.
[3] F. DeMeyer : Separable polynomials over a commutative ring, Rocky Mountain J. Math. **2** (1972), 299—310.
[4] K. Hirata and K. Sugano : On semisimple extensions and separable extensions over non commutative rings, J. Math. Soc. Japan, **18** (1966), 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 : On separable polynomials and Frobenius polynomials in skew polynomial rings. II, Math. J. Okayama Univ. **25** (1983), 23—28.
[7] G. J. Janusz : Separable algebras over commutative rings, Trans. Amer. Math. Soc. **122** (1966), 461—479.
[8] Y. Miyashita : Finite outer Galois theory of non-commutative rings, J. Fac. Sci. Hokkaido Univ., Ser. I, **19** (1966), 114—134.
[9] Y. Miyashita : On a skew polynomial ring, J. Math. Soc. Japan, **31** (1979), 317—330.
[10] T. Nagahara : On separable polynomials over a commutative ring II, Math. J. Okayama Univ. **15** (1972), 149—162.
[11] T. Nagahara On separable polynomials over a commutative ring III, Math. J. Okayama Univ. **16** (1974), 189—197.
[12] T. Nagahara : On separable polynomials over a commutative ring IV, Math. J. Okayama Univ. **17** (1974), 49—58.
[13] T. Nagahara : Imbeddings of some separable extensions in Galois extensions II, Math. J. Okayama Univ. **18** (1976), 189—194.
[14] T. Nagahara : On separable polynomials of degree 2 in skew polynomial rings, Math. J. Okayama Univ. **19** (1976), 65—95.
[15] T. Nagahara : On separable polynomials of degree 2 in skew polynomial rings II, Math. J. Okayama Univ. **21** (1979), 167—177.
[16] T. Nagahara : Note on skew polynomials, Math. J. Okayama Univ. **25** (1983), 43—48.
[17] T. Nagahara : A note on imbeddings of non-commutative separable extensions in Galois extensions, to appear in Houston J. of Math.
[18] O. E. Villamayor : Separable algebras and Galois extensions, Osaka J. Math. **4** (1967), 161—171.

Department of Mathematics
Okayama University

(Received November 5, 1983)