

Mathematical Journal of Okayama University

Volume 15, Issue 2

1971

Article 8

OCTOBER 1972

On separable polynomials over a commutative ring II

Takasi Nagahara*

*Okayama University

Copyright ©1971 by the authors. *Mathematical Journal of Okayama University* is produced by
The Berkeley Electronic Press (bepress). <http://escholarship.lib.okayama-u.ac.jp/mjou>

ON SEPARABLE POLYNOMIALS OVER A COMMUTATIVE RING II

Dedicated to Professor MASARU OSIMA on his 60th birthday

TAKASI NAGAHARA

Let B be an arbitrary commutative ring with identity element, X an indeterminate, and $B[X]$ the ring of polynomials in X with coefficients in B where $bX = Xb$ ($b \in B$). A polynomial $f \in B[X]$ is called separable if f is monic and $B[X]/(f)$ is a separable B -algebra. Separable polynomials over commutative rings have been studied in B. L. Elkins [4], G. J. Janusz [5], Y. Miyashita [6], and in the previous ones [7], [8]. The present paper is a study about separable polynomials over arbitrary commutative rings, in which we generalize some of the results about polynomials over fields to the case of a base ring B and we establish some fundamental properties of separable polynomials over B . We also sharpen several results in [4]—[8]. In §1, we consider the notion of splitting rings of monic polynomials in $B[X]$ which plays an important part in the present study. In §2, we characterize the separable polynomials over B in several ways. In §3, we study ring extensions of B which are generated by roots of separable polynomials over B .

Throughout this paper, all rings will be assumed commutative with identity element, and all ring extensions of B will be assumed with identity element 1, the identity element of B . Moreover, ring homomorphisms are tacitly assumed to take the identity element into the identity element. For a ring extension A/T and for a group \mathfrak{G} of ring automorphisms in A , we shall use the following conventions: $\mathfrak{S}(A/T)$ (abbr. $\mathfrak{S}(T)$) = the group of ring automorphisms in A which leave the elements of T fixed; $J(\mathfrak{G})$ = the fixring of \mathfrak{G} in A ; $\mathfrak{G}|T$ = the restriction of \mathfrak{G} to T . If A is a Galois extension of T with a Galois group \mathfrak{G} (in the sense of [3, Def.1.4]) then A is called a \mathfrak{G} -Galois extension of T , and occasionally, A/T is called to be \mathfrak{G} -Galois. Next, all monic polynomials are assumed to be of degree ≥ 1 . Moreover, for any polynomial $f(X)$, we denote by $\deg f(X)$ the degree of $f(X)$. As to other notations and terminologies used in this paper we follow [3] and [7].

1. Splitting rings of monic polynomials. We shall first introduce the notion of splitting rings of monic polynomials in $B[X]$ whose idea is based on the theory of fields.

Definition. Let $f(X)$ be a monic polynomial in $B[X]$. If $B[a_1, a_2, \dots, a_n]$ is a ring extension of B with $f(X) = (X - a_1)(X - a_2)\dots(X - a_n)$ then it is called a *splitting ring* of $f(X)$. Moreover, a splitting ring $B[x_1, x_2, \dots, x_n]$ of $f(X)$ is said to be *free* if for every splitting ring $B[a_1, a_2, \dots, a_n]$ of $f(X)$, there exists a B -ring homomorphism

$$B[x_1, x_2, \dots, x_n] \longrightarrow B[a_1, a_2, \dots, a_n]$$

mapping x_i into a_i for $i = 1, 2, \dots, n$.

Let $B[x_1, x_2, \dots, x_n]$ be a free splitting ring of a monic polynomial $f(X)$ in $B[X]$. Then, for an arbitrary permutation π of the set $\{1, 2, \dots, n\}$, there exists a B -ring endomorphism π^* of $B[x_1, x_2, \dots, x_n]$ mapping x_i into $x_{\pi(i)}$ for $i = 1, 2, \dots, n$. Then we see that π^* is an automorphism. Moreover, any two free splitting rings are B -ring isomorphic. If $\deg f(X) \leq 2$ then $B[X]/(f(X))$ is a free splitting ring of $f(X)$.

Now, let $\theta: B \longrightarrow C$ be a ring homomorphism, c_1, c_2, \dots, c_n elements of C , and X_1, X_2, \dots, X_n indeterminates which are independent. For any element $h(X_1, X_2, \dots, X_n) = \sum b_{k_1, k_2, \dots, k_n} X_1^{k_1} X_2^{k_2} \dots X_n^{k_n}$ of $B[X_1, X_2, \dots, X_n]$, we write $h^\theta(c_1, c_2, \dots, c_n) = \sum \theta(b_{k_1, k_2, \dots, k_n}) c_1^{k_1} c_2^{k_2} \dots c_n^{k_n}$. Then we have a ring homomorphism $B[X_1, X_2, \dots, X_n] \longrightarrow C$ mapping $h(X_1, X_2, \dots, X_n)$ into $h^\theta(c_1, c_2, \dots, c_n)$. We shall prove here our first lemma.

Lemma 1.1. *Let $f(X)$ be a monic polynomial in $B[X]$. Then $f(X)$ has a splitting ring $B[a_1, a_2, \dots, a_n]$ such that if $\theta: B \longrightarrow B_0$ is a ring homomorphism and $B_0[c_1, c_2, \dots, c_n]$ is a splitting ring of $f^\theta(X)$ then there exists a ring homomorphism*

$$B[a_1, a_2, \dots, a_n] \longrightarrow B_0[c_1, c_2, \dots, c_n]$$

mapping $h(a_1, a_2, \dots, a_n)$ into $h^\theta(c_1, c_2, \dots, c_n)$.

Proof. This is clear for monic polynomials of degree 1. Hence we assume it true for monic polynomials of degree $n-1$, and consider a monic polynomial $f(X)$ of $B[X]$ of degree n . Set $B[a_1] = B[X]/(f(X))$ where $a_1 = X + (f(X))$. Then $f(X) = (X - a_1)g(X)$, $g(X) \in B[a_1][X]$, and $\deg g(X) = n-1$. Hence by the induction assumption, $g(X)$ has a

splitting ring $B[a_1][a_2, a_3, \dots, a_n]$ such that if $\psi: B[a_1] \rightarrow T$ is a ring homomorphism and $T[d_2, d_3, \dots, d_n]$ is a splitting ring of $g^\psi(X)$ then there exists a ring homomorphism

$$B[a_1][a_2, a_3, \dots, a_n] \rightarrow T[d_2, d_3, \dots, d_n]$$

mapping $u(a_2, a_3, \dots, a_n)$ into $u^\psi(d_2, d_3, \dots, d_n)$. Clearly $B[a_1, a_2, \dots, a_n]$ is a splitting ring of $f(X)$. Now, let $B_0[c_1, c_2, \dots, c_n]$ be a splitting ring of $f^\theta(X)$. Since $f^\theta(c_1) = 0$, we have a ring homomorphism $\varphi: B[a_1] \rightarrow B_0[c_1]$ mapping $h(a_1)$ into $h^\theta(c_1)$. Then $f^\theta(X) = f^\varphi(X) = (X - c_1)g^\varphi(X)$. Hence $g^\varphi(X) = (X - c_2)(X - c_3)\dots(X - c_n)$. Thus $B_0[c_1][c_2, c_3, \dots, c_n]$ is a splitting ring of $g^\varphi(X)$. Therefore we obtain a ring homomorphism

$$B[a_1][a_2, a_3, \dots, a_n] \rightarrow B_0[c_1][c_2, c_3, \dots, c_n]$$

mapping $u(a_2, a_3, \dots, a_n)$ into $u^\varphi(c_2, c_3, \dots, c_n)$. Since $\varphi|_{B} = \theta$ and $\varphi(a_1) = c_1$, this proves the lemma.

In virtue of Lemma 1.1, we obtain the following

Theorem 1.1. *Every monic polynomial in $B[X]$ has a free splitting ring, which is unique up to isomorphism.*

For the later use, we note the following

Corollary 1.1. *Let $f(X)$ be a monic polynomial in $B[X]$, and $B[x_1, x_2, \dots, x_n]$ a free splitting ring of $f(X)$. Then*

(1) *if $\theta: B \rightarrow B_0$ is a ring homomorphism and $B_0[c_1, c_2, \dots, c_n]$ is a splitting ring of $f^\theta(X)$ then there exists a ring homomorphism*

$$B[x_1, x_2, \dots, x_n] \rightarrow B_0[c_1, c_2, \dots, c_n]$$

mapping $h(x_1, x_2, \dots, x_n)$ into $h^\theta(c_1, c_2, \dots, c_n)$.

(2) *For $m < n$, $f_m(X) = (X - x_{m+1})(X - x_{m+2}) \dots (X - x_n) \in B[x_1, x_2, \dots, x_m][X]$, and $B[x_1, x_2, \dots, x_m][x_{m+1}, x_{m+2}, \dots, x_n]$ is a free splitting ring of $f_m(X)$.*

(3) $B[x_m] \cong B[X]/(f(X)) (h(x_m) \leftarrow \rightarrow h(X) + (f(X))), m = 1, 2, \dots, n$.

(4) $B[x_1, x_2, \dots, x_n]$ is a free B -module, which has a free B -bases $\{x_1^{k_1} x_2^{k_2} \dots x_n^{k_n} \mid 0 \leq k_i \leq n - i\}$.

Proof. Since (1) is immediate from Lemma 1.1, it remains to prove (2)–(4). They are obvious for $n = 1$. Hence we consider the case $n > 1$. Now we set $B[a_1] = B[X]/(f(X))$ where $a_1 = X + (f(X))$. Then $f(X) = (X - a_1)g_1(X)$, $g_1(X) \in B[a_1][X]$. By Th.1.1, $g_1(X)$ has a free splitting

ring $B[a_1][a_2, a_3, \dots, a_n]$. Then, as is shown in the proof of Lemma 1.1, there exists a B -ring homomorphism

$$\varphi : B[a_1, a_2, \dots, a_n] \longrightarrow B[x_1, x_2, \dots, x_n]$$

mapping a_i into x_i for $i=1, 2, \dots, n$. Since $B[x_1, x_2, \dots, x_n]$ is a free splitting ring of $f(X)$, φ is an isomorphism. Noting $g_1^f(X)=f_1(X)$, it follows that $f_1(X) \in B[x_1][X]$, $B[x_1][x_2, x_3, \dots, x_n]$ is a free splitting ring of $f_1(X)$, $B[x_1] \cong B[X]/(f(X))$ ($h(x_1) \longleftrightarrow h(X) + (f(X))$), and $B[x_1]$ has a free B -bases $\{x_1^{k_1} \mid 0 \leq k_1 \leq n-1\}$. From these facts, one will easily see (2)–(4).

Next, we shall prove the following corollary which gives a way of characterizing free splitting rings of monic polynomials.

Corollary 1.2. *Let $f(X) = X^n - b_1X^{n-1} + \dots + (-1)^nb_n \in B[X]$. Let X_1, X_2, \dots, X_n be indeterminates which are independent, $\{s_1, s_2, \dots, s_n\}$ the set of elementary symmetric polynomials in the X_i where $\deg s_i = i$ ($1 \leq i \leq n$), and N an ideal of $B[X_1, X_2, \dots, X_n]$ generated by $\{s_1 - b_1, s_2 - b_2, \dots, s_n - b_n\}$. Then $B \cap N = \{0\}$, and $B[X_1, X_2, \dots, X_n]/N = B[X_1^*, X_2^*, \dots, X_n^*]$ is a free splitting ring of $f(X)$, where $X_i^* = X_i + N$ ($1 \leq i \leq n$).*

Proof. By Th.1.1, there exists a free splitting ring $B[x_1, x_2, \dots, x_n]$ of $f(X)$. Then we have a B -ring homomorphism

$$\varphi : B[X_1, X_2, \dots, X_n] \longrightarrow B[x_1, x_2, \dots, x_n]$$

mapping X_i into x_i for $i=1, 2, \dots, n$. It is obvious that $\varphi(s_i) = b_i$ for every i . This implies $\varphi(N) = \{0\}$ and $B \cap N = \{0\}$. Hence φ induces the following B -ring homomorphism

$$\varphi^* : B[X_1^*, X_2^*, \dots, X_n^*] \longrightarrow B[x_1, x_2, \dots, x_n]$$

mapping X_i^* into x_i for $i=1, 2, \dots, n$. Moreover, it is easily seen that $B[X_1^*, X_2^*, \dots, X_n^*]$ is a splitting ring of $f(X)$. Therefore, from the notion of free splitting rings, it follows φ^* is an isomorphism. This completes the proof.

For a square matrix $\|a_{kl}\|$ with elements a_{kl} in a ring, $\det \|a_{kl}\|$ will denote the determinant of $\|a_{kl}\|$. Let $f(X)$ be a monic polynomial in $B[X]$, t the trace map of the free B -module $B[X]/(f(X))$, and $x = X + (f(X))$. Then we shall call $\det \|t(x^k x^l)\|$ ($0 \leq k, l < n$) the *discriminant* of $f(X)$, and this will be denoted by $\delta(f(X))$.

We shall prove now the following

Theorem 1.2. *Let $f(X)$ be a monic polynomial in $B[X]$. If $B[a_1, a_2, \dots, a_n]$ is a splitting ring of $f(X)$ then $\prod_{i < j} (a_i - a_j)^2 = \delta(f(X))$.*

Proof. By Th.1.1, there exists a free splitting ring $B[x_1, x_2, \dots, x_n]$ of $f(X)$. Then we have a B -ring homomorphism

$$B[x_1, x_2, \dots, x_n] \longrightarrow B[a_1, a_2, \dots, a_n]$$

mapping x_i into a_i for $i=1, 2, \dots, n$. Noting $\prod_{i < j} (x_i - x_j)^2 \in B$, we obtain $\prod_{i < j} (x_i - x_j)^2 = \prod_{i < j} (a_i - a_j)^2$. By Coro.1.1, $B[X]/(f(X))$ and $B[x_i]$ are B -ring isomorphic under the mapping $h(X) + (f(X)) \longrightarrow h(x_i)$. Hence it suffices to prove that $\det \|t(x_i^k x_i^l)\| = \prod_{i < j} (x_i - x_j)^2$ ($0 \leq k, l < n$). Let X, X_1, X_2, \dots, X_n be indeterminates which are independent, $\{s_1, s_2, \dots, s_n\}$ the set of elementary symmetric polynomials in X, X_2, \dots, X_n where $\deg s_i = i$, $1 \leq i \leq n$, and B_0 a subring of $B[X_1, X_2, \dots, X_n]$ generated by $B \cup \{s_1, s_2, \dots, s_n\}$. Now we consider a B -ring homomorphism

$$\varphi : B[X_1, X_2, \dots, X_n][X] \longrightarrow B[x_1, x_2, \dots, x_n][X]$$

mapping $\sum_k h_k(X_1, X_2, \dots, X_n)X^k$ into $\sum_k h_k(x_1, x_2, \dots, x_n)X^k$. Then, noting $\prod_{i=1}^n (X - X_i) = X^n - s_1 X^{n-1} + \dots + (-1)^n s_n$, it is easily seen that $B_0[X_i] = \sum_{k=0}^{n-i} B_0 X_i^k$, $\varphi(B_0) = B$, and $\varphi(X_i) = x_i$. For X_1^m ($m > 0$), we write

$$(1) \quad X_1^m \cdot X_1^k = \sum_{l=0}^{m+k-1} b_{kl} X_1^l, \quad b_{kl} \in B_0, \quad 0 \leq k < n,$$

$$g(X) = \det (XI - \|b_{kl}\|)$$

where I is the identity matrix of degree n . Applying φ to (1), we have

$$(2) \quad x_1^m \cdot x_1^k = \sum_{l=0}^{m+k-1} \varphi(b_{kl}) x_1^l, \quad \varphi(b_{kl}) \in B,$$

$$\varphi(g(X)) = \det (XI - \|\varphi(b_{kl})\|).$$

From (1), it follows that $g(X_1^m) = 0$, so that $g(X_i^m) = 0$ for every i . For $i \neq j$, $X_i^m - X_j^m$ is not a zero divisor of $B[X_1, X_2, \dots, X_n]$. Hence we see that $\prod_{i=1}^n (X - X_i^m)$ is a factor of $g(X)$. Since $g(X)$ is a monic polynomial of degree n , we obtain $g(X) = \prod_{i=1}^n (X - X_i^m)$, and so $\varphi(g(X)) = \prod_{i=1}^n (X - x_i^m)$. From this and (2), it follows that $t(x_i^m) = \sum_{i=1}^m x_i^m$. Hence

$$\det \|t(x_i^k x_i^l)\| = \det \|\sum_i x_i^k x_i^l\| \quad (1 \leq i \leq n, 0 \leq k, l \leq n-1)$$

$$= \det \|x_i^k\|^2$$

$$= \prod_{i < j} (x_i - x_j)^2.$$

This is our desired one, which completes the proof.

Corollary 1.3. *Let $f(X)$ be a monic polynomial in $B[X]$, $\theta : B \rightarrow B_0$ a ring homomorphism. Then $\theta(\delta(f(X))) = \delta(f^\theta(X))$.*

Proof. Let $B[x_1, x_2, \dots, x_n]$ and $B_0[y_1, y_2, \dots, y_n]$ be free splitting rings of $f(X)$ and $f^\theta(X)$ respectively. Then we have a ring homomorphism

$$B[x_1, x_2, \dots, x_n] \longrightarrow B_0[y_1, y_2, \dots, y_n]$$

mapping $h(x_1, x_2, \dots, x_n)$ into $h^\theta(y_1, y_2, \dots, y_n)$. Hence it follows from Th.1.2 that $\theta(\delta(f(X))) = \theta(\prod_{i < j} (x_i - x_j)^2) = \prod_{i < j} (y_i - y_j)^2 = \delta(f^\theta(X))$.

Remark 1.1. Let $f(X)$ be a monic polynomial in $B[X]$, $B[x_1, x_2, \dots, x_n]$ a free splitting ring of $f(X)$, and \mathfrak{S}_n the symmetric group of the set $\{1, 2, \dots, n\}$. Then for every $\pi \in \mathfrak{S}_n$, we have a B -ring automorphism π^* of $B[x_1, x_2, \dots, x_n]$ mapping x_i into $x_{\pi(i)}$ for $i = 1, 2, \dots, n$. Obviously, the mapping $(*) : \pi \rightarrow \pi^*$ is a group homomorphism of \mathfrak{S}_n into the group of B -ring automorphisms of $B[x_1, x_2, \dots, x_n]$. In the remaining of this paper, the image of $(*)$ will be denoted by $\mathfrak{S}_{\{x_1, \dots, x_n\}}$. If $n > 2$ then by Cor.1.1, we have $x_1 \neq x_2$, which shows that $x_i \neq x_j$ for $i \neq j$. Hence, in case $n \neq 2$, we see that $(*)$ is a monomorphism, that is, $\mathfrak{S}_n \cong \mathfrak{S}_{\{x_1, \dots, x_n\}}$. We consider the case $n = 2$. It is clear that $(*)$ is a monomorphism if and only if $x_1 \neq x_2$. We write here $f(X) = X^2 + b_1X + b_2$. Then $x_1 - x_2 = f'(x_1) = 2x_1 + b_1$, where $f'(X)$ is the derivative of $f(X)$. Since $\{x_1, 1\}$ is a free B -bases of $B[x_1]$ (Cor.1.1), it follows that $\mathfrak{S}_2 \cong \mathfrak{S}_{\{x_1, x_2\}}$ if and only if $f'(X) \neq 0$. Next, we shall determine $J(\mathfrak{S}_{\{x_1, x_2\}})$. Let $cx_1 + d \in B[x_1]$ ($= B[x_1, x_2]$) where $c, d \in B$. If $cx_1 + d \in J(\mathfrak{S}_{\{x_1, x_2\}})$ then $0 = c(x_1 - x_2) = (2c)x_1 + cb_1$, and conversely. Hence it follows that $cx_1 + d \in J(\mathfrak{S}_{\{x_1, x_2\}})$ if and only if $c \in N$, the annihilator of $\{2 \cdot 1, b_1\}$ in B . Thus we obtain $J(\mathfrak{S}_{\{x_1, x_2\}}) = Nx_1 + B$. For example, if we consider the ring $B = GF(2) \oplus GF(2)$ and $f(X) = X^2 + (1, 0)X$ then $\mathfrak{S}_2 \cong \mathfrak{S}_{\{x_1, x_2\}}$ and $B[x_1] \cong J(\mathfrak{S}_{\{x_1, x_2\}}) \cong B$. However, if, in general, $n > 2$ then it does not seem to be an easy matter to determine $J(\mathfrak{S}_{\{x_1, \dots, x_n\}})$.

We shall now proceed to show that if $\delta(f(X))$ is not a zero divisor then $J(\mathfrak{S}_{\{x_1, \dots, x_n\}}) = B$. For this and a later application we require the following

Lemma 1.2. *Let A be a ring extension of B and b an element of B .*

(1) Let $A=Bd\oplus M$ where d is B -free and M is a B -submodule. Then, b is invertible in B if and only if so is in A .

(2) Let A be free as B -module. Then, b is not a zero divisor in B if and only if so is in A .

Proof. The assertion (2) is obvious. To see (1), we assume that b is invertible in A , and write $b^{-1}d=b_0d+m$ where $b_0\in B$ and $m\in M$. Then we have $d=bb^{-1}d=b(b_0d+m)=(bb_0)d+bm$. Hence we obtain $bb_0=1$. Thus b is invertible in B . The converse is obvious.

Theorem 1.3. Let $f(X)$ be a monic polynomial in $B[X]$, and $B[x_1, x_2, \dots, x_n]$ a free splitting ring of $f(X)$. Then the following conditions are equivalent.

(a) x_1-x_2 is not a zero divisor in $B[x_1, x_2, \dots, x_n]$.

(b) $f'(x_1)$ is not a zero divisor in $B[x_1]$ where $f'(X)$ is the derivative of $f(X)$.

(c) $\delta(f(X))$ is not a zero divisor in B .

Moreover, if the conditions hold then for every subset E of $\{x_1, x_2, \dots, x_n\}$, $J(\mathfrak{S}(B[E])\cap\mathfrak{S}_{\{x_1, \dots, x_n\}})=B[E]$, and in particular, $J(\mathfrak{S}_{\{x_1, \dots, x_n\}})=B$.

Proof. It is clear that $f'(x_1)=\prod_{j\neq 1}(x_1-x_j)$. For an arbitrary $j>1$, there exists an element π^* in $\mathfrak{S}_{\{x_1, \dots, x_n\}}$ such that $\pi^*(x_1-x_2)=x_1-x_j$. Hence (a) implies (b). Assume (b). Then, by Cor.1.1 and Lemma 1.2, $f'(x_1)$ is not a zero divisor in $B[x_1, x_2, \dots, x_n]$ and, so is $f'(x_i)$ for $i=2, 3, \dots, n$. Hence $\prod_i f'(x_i)=-\delta(f(X))$ is not a zero divisor in $B[x_1, x_2, \dots, x_n]$ and, so is in B . Thus we obtain (c). (c) \Rightarrow (a) follows from Cor.1.1 and Lemma 1.2. We have therefore proved (a) \Leftrightarrow (b) \Leftrightarrow (c). Next, we shall prove the rest of our assertion. This is clear for polynomials of degree 1. Hence we assume it for polynomials of degree $n-1$, and consider a free splitting ring $B[x_1, x_2, \dots, x_n]$ of a monic polynomial $f(X)$ of degree n with conditions (a)–(c). By Cor.1.1, $B[x_1][x_2, x_3, \dots, x_n]$ is a free splitting ring of $\prod_{i\neq 1}(X-x_i)\in B[x_1][X]$. Since x_2-x_3 is not a zero divisor in $B[x_1][x_2, x_3, \dots, x_n]$, we see $J(\mathfrak{S}_{\{x_1, \dots, x_n\}})\subset B[x_1]$ by the induction assumption. If $J(\mathfrak{S}_{\{x_1, \dots, x_n\}})\ni a=\sum_{k=0}^{n-1} x_1^k b_k$ ($b_k\in B$) then $\sum_{k=1}^{n-1} x_1^k b_k + x_1^0(b_0-a)=0$ for all i . For the adjoint M of the matrix $\|x_i^k\|$ ($0<i\leq n, 0\leq k<n$), we have $M\|x_i^k\|=(\det\|x_i^k\|)I=(\pm\prod_{i<j}(x_i-x_j))I$ where I is the identity matrix of degree n . Then it follows that $(\prod_{i<j}(x_i-x_j))(b_0-a)=0$, and hence $b_0-a=0$. This shows $J(\mathfrak{S}_{\{x_1, \dots, x_n\}})=B$. Now, let E be an arbitrary proper subset of $\{x_1, x_2, \dots, x_n\}$ and C the complement of E in

$\{x_1, x_2, \dots, x_n\}$. Then by Cor.1.1, $B[E][C]$ is a free splitting ring of $\prod_{x \in C} (X-x) \in B[E][X]$. Since for distinct $x, y \in C$, $x-y$ is not a zero divisor in $B[E][C]$, it follows that $J(\mathfrak{S}(B[E]) \cap \mathfrak{S}_{\{x_1, \dots, x_n\}}) = B[E]$. This completes the proof.

2. Separable polynomials. First we shall prove the following lemma whose proof is similar to that of [3, Th.1.3 (1.4)].

Lemma 2.1. *Let A be a ring extension of B and $J(\mathfrak{G})=B$ for a group \mathfrak{G} of ring automorphisms in A . Let T be an intermediate ring of A/B , and $\mathfrak{H}=\mathfrak{S}(T) \cap \mathfrak{G}$. Assume the index of \mathfrak{H} in \mathfrak{G} is finite and there exist elements $x_1, x_2, \dots, x_n \in T$; $y_1, y_2, \dots, y_n \in J(\mathfrak{H})$ such that $\sum_i x_i \sigma(y_i) = u \delta_{1, \sigma|_T}$ for all σ in \mathfrak{G} . Then $J(\mathfrak{H})u \subset T$; and if, in particular, u is invertible in A then $J(\mathfrak{H})=T$.*

Proof. Let $\{\sigma_1, \sigma_2, \dots, \sigma_m\}$ be a complete system of representatives of right cosets relative to \mathfrak{H} , so that $\mathfrak{G} = \cup_i \sigma_i \mathfrak{H}$ and the $\sigma_i \mathfrak{H}$ are disjoint. For any $a \in J(\mathfrak{H})$, we set $t(a) = \sum_i \sigma_i(a)$. Then we have $\sigma(t(a)) = t(a)$ for all σ in \mathfrak{G} , which implies $t(a) \in B$. Hence we obtain $T \ni \sum_i x_i t(a y_i) = \sum_i x_i (a y_i) = a \sum_i x_i y_i = a u$. It follows from this that $T \supset J(\mathfrak{H})u$. If u is invertible in A then so is in $J(\mathfrak{H})$, and hence $T = J(\mathfrak{H})$.

Now, the following lemma contains the result of [7, Lemma], and it plays an important role in the subsequent consideration. We shall present here a simple proof, whereas the proof of [7, Lemma] is somewhat complicated.

Lemma 2.2. *Let A be a ring extension of B and $J(\mathfrak{G})=B$ for a group \mathfrak{G} of ring automorphisms in A . Let a an element of A such that the set $\{\sigma(a) | \sigma \in \mathfrak{G}\}$ is finite and for $\sigma(a) \neq a$ ($\sigma \in \mathfrak{G}$), $a - \sigma(a)$ is invertible. Set $\{a_1 = a, a_2, \dots, a_n\} = \{\sigma(a) | \sigma \in \mathfrak{G}\}$ where $a_i \neq a_j$ for $i \neq j$, and $f(X) = (X - a_1)(X - a_2) \cdots (X - a_n)$. Then*

- (1) $f(X) \in B[X]$, and $\delta(f(X))$ is invertible in B .
- (2) $B[a_1, a_2, \dots, a_n]$ is a Galois extension of B with a Galois group $\mathfrak{G} | B[a_1, a_2, \dots, a_n]$, and for every subset E of $\{a_1, a_2, \dots, a_n\}$, $J(\mathfrak{S}(B[E]) \cap \mathfrak{G}) = B[E]$.
- (3) $B[X]/(f(X)) \cong B[a]$ ($h(X) + (f(X)) \longleftrightarrow h(a)$).
- (4) $f(X)$ is a separable polynomial over B .

Proof. It is obvious that $f(X) \in B[X]$. Set $u = \prod_{i \neq j} (a_i - a_j)$ (=

$-\delta(f(X))$). Then it is easily seen that $u \in B$ and $u^{-1} \in J(\mathbb{G}) = B$. For $T = B[a_1, a_2, \dots, a_n]$, we have $u^{-1} \prod_{i \neq j} (a_i - \sigma(a_j)) = \delta_{1, \sigma|T}(\sigma \in \mathbb{G})$, which can be written as $u^{-1} \sum_i x_i \sigma(y_i)$ for some elements $x_1, x_2, \dots, x_m; y_1, y_2, \dots, y_m$ of T , and hence T is a $\mathbb{G}|T$ -Galois extension of B . Next, we set

$$g(X) = (X - a_2)(X - a_3) \cdots (X - a_n) = \sum_{k=0}^{n-1} X^k b_k.$$

Then $f(X) = (X - a)g(X)$ and this gives $g(X) \in B[a][X]$. If $\sigma \in \mathbb{G}$ and $\sigma|B[a] \neq 1$ then $a = \sigma(a_i)$ for some $i > 1$ and then $0 = \prod_{i>1} (a - \sigma(a_i)) = \sum_k a^k \sigma(b_k)$. Thus we obtain $\sum_k a^k \sigma(b_k) = g(a) \delta_{1, \sigma|B[a]}$ for all σ in \mathbb{G} where $a, b_i \in B[a]$ and $g(a)$ is invertible in A . Therefore it follows from Lemma 2.1 that $J(\mathfrak{N}(B[a]) \cap \mathbb{G}) = B[a]$. Hence, if E is a subset of $\{a_1, a_2, \dots, a_n\}$ then we can use induction on the cardinal number of E to obtain $J(\mathfrak{N}(B[E]) \cap \mathbb{G}) = B[E]$. Now, since for $i \neq j$, $a_i - a_j$ is invertible in A and $\{\sigma(a_i) | \sigma \in \mathbb{G}\} = \{a_1, a_2, \dots, a_n\}$, it is easy to see that $B[X]/(f(X))$ and $B[a]$ are B -ring isomorphic under the mapping $h(X) + (f(X)) \rightarrow h(a)$. By [3, Th.2.2], $J(\mathfrak{N}(B[a]) \cap \mathbb{G}) = B[a]$ is separable over B . This shows that $f(X)$ is separable over B .

Now, we shall prove the following theorem which contains some part of the result of [8, Th. 2].

Theorem 2.1. *Let $f(X)$ be a monic polynomial in $B[X]$, and $B[x_1, x_2, \dots, x_n]$ a free splitting ring of $f(X)$. Then the following conditions are equivalent.*

- (a) $x_1 - x_2$ is invertible in $B[x_1, x_2, \dots, x_n]$.
- (b) $f'(x_i)$ is invertible in $B[x_i]$ where $f'(X)$ is the derivative of $f(X)$.
- (c) $\delta(f(X))$ is invertible in B .
- (d) $f(X)$ is separable over B .

Moreover, if the conditions hold then $B[x_1, x_2, \dots, x_n]$ is a $\mathfrak{G}_{|x_1, \dots, x_n|}$ -Galois extension of B and for every subset E of $\{x_1, x_2, \dots, x_n\}$, $J(\mathfrak{N}(B[E]) \cap \mathbb{G}) = B[E]$.

Proof. we have $f'(x_i) = \prod_{j \neq i} (x_i - x_j) \in B[x_i]$ and $\prod_i f'(x_i) = -\delta(f(X)) \in B$. By Cor.1.1, $B[x_1, x_2, \dots, x_n]$ is a free $B[x_i]$ -module as well as a free B -module. Hence Lemma 1.2 enables us to see that (a) \Leftrightarrow (b) \Leftrightarrow (c). Assume (d). Let M be a maximal ideal of B , θ a canonical homomorphism $B \rightarrow B/M = K$, and \bar{K} the algebraic closure of K . Then $\bar{K}[X]/(f^\theta(X)) \cong \bar{K} \otimes_B (B[X]/(f(X)))$ and it is a separable \bar{K} -algebra, which is a semisimple ring. From this we see that $f^\theta(X)$ has no repeated

roots in \bar{K} , whence $\delta(f^\theta(X)) \neq 0$. Since $\theta(\delta(f(X))) = \delta(f^\theta(X))$ (Cor.1.3), we obtain $\delta(f(X)) \notin M$. This implies that $\delta(f(X))$ is invertible in B . Thus we obtain (d) \Rightarrow (c). (c) \Rightarrow (d) and the other assertions follow from Th.1.3 and Lemma 2.2.

In virtue of Th.1.2 and Th.2.1, we obtain the following theorem which is the result of [8, Cor. 1].

Theorem 2.2. *Let $f(X)$ be a monic polynomial in $B[X]$, and $B[a_1, a_2, \dots, a_n]$ a splitting ring of $f(X)$. Then, $f(X)$ is separable over B if and only if $\prod_{i < j} (a_i - a_j)^2$ is invertible in B .*

Now, for a monic polynomial $f(X)$ in $B[X]$ we shall consider the following conditions (i)—(vii).

- (i) $f(X)$ is a separable polynomial.
- (ii) $f'(X) + (f(X))$ is an invertible element of $B[X]/(f(X))$ where $f'(X)$ is the derivative of $f(X)$.

(iii) $\delta(f(X))$ is an invertible element of B .

(iv) There is a ring extension of B which contains elements a_1, a_2, \dots, a_n such that $f(X) = (X - a_1)(X - a_2) \cdots (X - a_n)$ and $\prod_{i < j} (a_i - a_j)^2$ is invertible in B .

(v) There is a \mathbb{G} -Galois extension of B which is generated by elements b_1, b_2, \dots, b_n such that $f(X) = (X - b_1)(X - b_2) \cdots (X - b_n)$, $\prod_{i < j} (b_i - b_j)^2$ is invertible in B , and $\{\sigma(b_i) \mid \sigma \in \mathbb{G}\} = \{b_1, b_2, \dots, b_n\}$.

(vi) For each maximal ideal M of B , the polynomial obtained from $f(X)$ by reducing the coefficients modulo M has no repeated roots in an algebraic closure of B/M .

(vii) For each maximal ideal M of B , $f(X)$ is separable when viewed as a polynomial over the local ring B_M .

Recently, in [4], B. L. Elkins proved that (i) implies (ii). In [7], the present author proved that (iv) implies (i), and moreover, in [8], proved that (i), (ii), (iv) and (v) are equivalent. In [6], Y. Miyashita proved that (i) and (ii) are equivalent for some non-monic polynomials as well as for monic polynomials. Several years ago, G. J. Janusz [5] proved that when B has no proper idempotents, (i), (iii), (vi) and (vii) are equivalent, and (i) implies (iv). (Cf. [8, Remark]).

We shall now prove the following

Theorem 2.3. *For a monic polynomial $f(X)$ in $B[X]$, the conditions (i)—(vii) are equivalent.*

Proof. By Th.1.1, $f(X)$ has a free splitting ring $B[x_1, x_2, \dots, x_n]$. Then by Cor.1.1, $B[X]/(f(X))$ is isomorphic to $B[x_i]$ under the mapping $h(X) + (f(X)) \rightarrow h(x_i)$. Hence by Th.2.1 and Th.2.2, the conditions (i)–(v) are equivalent. Now, we shall prove (iii) \Leftrightarrow (vi). Let M_θ be a maximal ideal of B , θ a canonical homomorphism $B \rightarrow B/M_\theta$. Then by Th.1.2, (vi) holds if and only if $\delta(f^\theta(X)) \neq 0$ for every maximal ideal M_θ of B . Since $\delta(f^\theta(X)) = \theta(\delta(f(X)))$ (Cor.1.3), (vi) is equivalent to that $\delta(f(X))$ is not contained in every maximal ideal M_θ of B , and it is equivalent to (iii). Thus we obtain (iii) \Leftrightarrow (vi). By a similar method, we have (iii) \Leftrightarrow (vii).

3. Roots of separable polynomials. Throughout this section, A will mean a ring extension of B , and \mathfrak{G} a group of B -ring automorphisms in A . A subring T of A is called \mathfrak{G} -strong if, for any $\sigma \in \mathfrak{G}$, $\sigma|T \neq 1$ and $e^2 = e \neq 0 \in A$, there is an element a in T such that $(a - \sigma(a))e \neq 0$. This notion is equivalent to that of \mathfrak{G} -strong subrings of \mathfrak{G} -Galois extensions (cf. [3, Def.2.1]).

We show first the following

Lemma 3.1. *Let $\{T_i | i \in I\}$ be a set of \mathfrak{G} -strong subrings of A , and T the subring generated by $\cup_{i \in I} T_i$. Then T is \mathfrak{G} -strong, and moreover, $\sigma(T)$ is \mathfrak{G} -strong for every $\sigma \in \mathfrak{G}$.*

Proof. Let $\sigma|T \neq 1 \in \mathfrak{G}|T$. Then $\sigma|T_i \neq 1$ for some i . This enables us to see that T is \mathfrak{G} -strong. Now, let $\sigma \in \mathfrak{G}$, $\tau|\sigma(T) \neq 1 \in \mathfrak{G}|\sigma(T)$, and $e^2 = e \neq 0 \in A$. Then $\sigma^{-1}\tau\sigma|T \neq 1$. Since T is \mathfrak{G} -strong there is an element a in T such that $(a - \sigma^{-1}\tau\sigma(a))\sigma^{-1}(e) \neq 0$, and so $(\sigma(a) - \tau\sigma(a))e \neq 0$. Hence $\sigma(T)$ is \mathfrak{G} -strong.

Corollary 3.1. *Let E be a subset of A such that for every $a \in E$ and $\sigma \in \mathfrak{G}$, $\sigma(a) \neq a$, $a - \sigma(a)$ is not a zero divisor in A . Then $B[E]$ is \mathfrak{G} -strong.*

If T_1, T_2 are subrings of A containing B which are separable over B then $T_1[T_2]$ is separable over B (see, [1, Propositions 1.4, 1.5]). Combining this fact with Lemma 3.1, we obtain

Corollary 3.2. *Let $J(\mathfrak{G}) = B$, T a subring of A containing B such that $\mathfrak{G}|T$ is finite, T is separable over B , and \mathfrak{G} -strong. Let N denote the subring generated by $\cup_{\sigma \in \mathfrak{G}} \sigma(T)$. Then N is a $\mathfrak{G}|N$ -Galois extension*

of B .

We shall now prove the following

Theorem 3.1. *Let $J(\mathfrak{G})=B$, E a finite subset of A such that for every $a \in E$, $\{\sigma(a) | \sigma \in \mathfrak{G}\}$ is finite, and elements $a - \sigma(a) \neq 0$ are invertible. Then $B[E]$ is separable over B , and \mathfrak{G} -strong. Moreover, $J(\mathfrak{S}(B[E]) \cap \mathfrak{G}) = B[E]$, and setting $F = \{\sigma(a) | \sigma \in \mathfrak{G}, a \in E\}$, $B[F]$ is a $\mathfrak{G}|B[F]$ -Galois extension of B .*

Proof. By Lemma 2.2 (3,4) and Cor.3.1, $B[E]$ is separable over B , and \mathfrak{G} -strong. Hence by Cor.3.2, $B[F]$ is a $\mathfrak{G}|B[F]$ -Galois extension of B . Moreover, by Lemma 2.2 (2), we have $J(\mathfrak{S}(B[a]) \cap \mathfrak{G}) = B[a]$ for every $a \in E$. Hence we can use induction on the cardinal number of E to obtain $J(\mathfrak{S}(B[E]) \cap \mathfrak{G}) = B[E]$.

We prove next

Theorem 3.2. *Let $J(\mathfrak{G})=B$, F a finite subset of A such that $\sigma(F) \subset F$ for all σ in \mathfrak{G} , and set $f(X) = \prod_{a \in F} (X - a)$. Then $f(X) \in B[X]$ and the following conditions are equivalent.*

- (a) *For $a \neq a'$ in F , $a - a'$ is invertible in A .*
- (b) *$f(X)$ is a separable polynomial over B .*

Proof. Since $\sigma(F) = F$ for all σ in \mathfrak{G} , it follows that $f(X) \in B[X]$. If there holds (a) then $\prod_{a \neq a' \in F} (a - a')$ is invertible in B , and conversely. Hence by Th.2.2, we obtain (a) \Leftrightarrow (b).

Remark 3.1. Let \mathfrak{G} , F , $f(X)$ be as in Th.3.2, and assume the conditions (a), (b) of Th.3.2. For $a \in F$, set $F_a = \{\sigma(a) | \sigma \in \mathfrak{G}\}$, and $f_a = \prod_{a' \in F_a} (X - a')$. Then by Lemma 2.2, f_a is a separable polynomial of $B[X]$, and $B[X]/(f_a) \cong B[a]$ ($h(X) + (f_a) \rightarrow h(a)$). Now, noting $\sigma(F) = F$ for all σ in \mathfrak{G} , we have a decomposition of F into non-overlapping transitivity sets relative to \mathfrak{G} : $F = F_{c_1} \cup F_{c_2} \cup \dots \cup F_{c_m}$. Then we have a factorization $f(X) = f_{c_1} f_{c_2} \dots f_{c_m}$. If A has no proper idempotents then the f_{c_i} are irreducible polynomials of $B[X]$ (cf. [5, Cor.2.10]).

As to case F is a transitivity set relative to \mathfrak{G} , we have the following

Theorem 3.3. *Let $J(\mathfrak{G})=B$, a an element of A such that $F = \{\sigma(a) | \sigma \in \mathfrak{G}\}$ is finite, and set $f(X) = \prod_{a' \in F} (X - a')$. Then the following conditions are equivalent.*

- (a) For $a \neq a'$ in F , $a - a'$ is invertible in A .
- (b) $f(X)$ is a separable polynomial over B .
- (c) $B[a]$ is separable over B , and \mathfrak{G} -strong.

Proof. Since (a) \Leftrightarrow (b) \Rightarrow (c) follows from Th.3.1 and Th.3.2, we need only show that (c) \Rightarrow (a). By Cor.3.2, we may assume that A is a \mathfrak{G} -Galois extension of B , $B[a]$ is separable over B , and \mathfrak{G} -strong. Then for $\mathfrak{H} = \mathfrak{N}(B[a]) \cap \mathfrak{G}$, we have $J(\mathfrak{H}) = B[a]$ by [3, Th.2.2], and hence $t_{\mathfrak{H}}(x) = \sum_{\sigma \in \mathfrak{H}} \sigma(x) \in B[a]$ for all x in A . We suppose that there exists an element τ in \mathfrak{G} such that $a - \tau(a) \neq 0$ and is not invertible in A . Then $N = (a - \tau(a))A$ is a proper ideal of A . For $g(X) \in B[X]$, we have $g(a) - \tau(g(a)) = g(a) - g(\tau(a)) = (a - \tau(a))c \in N$ for some $c \in B[a, \tau(a)]$. This implies $x - \tau(x) \in N$ for all x in $B[a]$. Since A/B is \mathfrak{G} -Galois, there exist elements $u_1, u_2, \dots, u_m; v_1, v_2, \dots, v_m$ such that $\sum_i u_i \sigma(v_i) = \delta_{1,\sigma}$ for all σ in \mathfrak{G} . Then, noting $\mathfrak{H} \cap \tau\mathfrak{H} = \phi$, we obtain $\sum_i u_i t_{\mathfrak{H}}(v_i) = 1$ and $\sum_i u_i \tau(t_{\mathfrak{H}}(v_i)) = 0$. Hence it follows that $1 = \sum_i u_i (t_{\mathfrak{H}}(v_i) - \tau(t_{\mathfrak{H}}(v_i))) \in N$, a contradiction. This proves (c) \Rightarrow (a).

We shall present now a theorem on imbedding of a ring extension $B[a]/B$ in a Galois extension of B .

Theorem 3.4. *For a ring extension $B[a]$ of B , the following conditions are equivalent.*

- (a) $B[a] \cong B[X]/(f(X))$ ($h(a) \longleftrightarrow h(X) + (f(X))$) for some separable polynomial $f(X)$ in $B[X]$.
- (b) $B[a]$ is separable over B and can be imbedded in a \mathfrak{G} -Galois extension of B in which $B[a]$ is \mathfrak{G} -strong.

Proof. The implication (b) \Rightarrow (a) is a direct consequence of Th.3.3 and Lemma 2.2. Assume (a). Then $B[a]$ is separable over B . By Th.1.1 and Cor.1.1, there is a free splitting ring $B[x_1, x_2, \dots, x_n]$ of $f(X)$ with $x_1 = a$. Then, by Th.2.1 and Th.3.1 we know that $B[x_1, x_2, \dots, x_n]/B$ is $\mathfrak{G}_{\{x_1, \dots, x_n\}}$ -Galois and $B[x_1]$ ($= B[a]$) is $\mathfrak{G}_{\{x_1, \dots, x_n\}}$ -strong. Thus we obtain (b).

An application of the preceding theorem is the following

Corollary 3.3. *Let B be a ring without proper idempotents, and $B[a]$ a ring extension of B which is projective and separable over B . Then $B[a]$ can be imbedded in a \mathfrak{G} -Galois extension of B in which $B[a]$ is \mathfrak{G} -strong.*

Proof. By [5, Th.2.9], there exists a separable polynomial $f(X)$ in $B[X]$ such that $B[X]/(f(X))$ is isomorphic to $B[a]$ under the mapping $h(X)+(f(X)) \rightarrow h(a)$. Hence the assertion is immediate from Th.3.4.

REFERENCES

- [1] M. AUSLANDER and O. GOLDMAN: The Brauer group of a commutative rings, Trans. Amer. Math. Soc., **97** (1960), 367—409.
- [2] N. BOURBAKI: Algèbre commutative, Chapitres I-II, Actualités Sci. Ind. No. 1290, Herman, Paris, 1962.
- [3] S. U. CHASE, D. K. HARRISON and A. ROSENBERG: Galois theory and Galois cohomology of commutative rings, Mem. Amer. Math. Soc., No. **52** (1965), 15—33.
- [4] B. L. ELKINS: Characterization of separable ideals, Pacific J. Math., **34** (1970), 45—49.
- [5] G. J. JANUŠZ: Separable algebras over commutative rings, Trans. Amer. Math. Soc., **122** (1966), 461—479.
- [6] Y. MIYASHITA: Commutative Frobenius algebras generated by a single element, J. Fac. Sci. Hokkaido Univ., Ser. I, **21** (1971), 166—176.
- [7] T. NAGAHARA: On separable polynomials over a commutative rings, Math. J. of Okayama Univ., **14** (1970), 175—181.
- [8] T. NAGAHARA: Characterization of separable polynomials over a commutative ring, Proc. Japan Acad., **46** (1970), 1011—1015.

DEPARTMENT OF MATHEMATICS
OKAYAMA UNIVERSITY

(Received February 29, 1972)