ON SEPARABLE POLYNOMIALS OVER A COMMUTATIVE RING III

TAKASHI NAGAHARA

Throughout this paper, all rings will be assumed commutative with identity element, B will mean a ring, and all ring extensions of B will be assumed with identity element 1, the identity element of B. Moreover, $B[X]$ will mean the ring of polynomials in an indeterminate X with coefficients in B, and all monic polynomials will be assumed to be of degree $\geqq 1$. A polynomial $f \in B[X]$ is called *separable* if f is monic and $B[X]/(f)$ is a separable B-algebra.

This paper is about splitting rings of separable polynomials. In § 1, we shall make a remark on ring extensions generated by a single element, which contains an imbedding theorem: Every projective, separable B-algebra $B[a]$ with $\text{rank}_B B[a]$ (in the sense of [2, Def. 2.5.2]) can be imbedded in a $\mathfrak{G}$-Galois extension of B in which $B[a]$ is $\mathfrak{G}$-strong. In §§ 2 and 3, we study splitting rings of separable polynomials in $B[X]$ which are projective over B, and we sharpen the results of DeMeyer [4, Ths. 2.1 and 2.2].

As to notations and terminologies used in this paper we follow [8].

1. Ring extensions generated by a single element. The main purpose of this section is to prove the following imbedding theorem which contains the result of [8, Th. 3.4] and a partial result of [1, Th. A. 7].

Theorem 1.1. *For a ring extension $B[a]$ of B, the following conditions are equivalent.*

(a) $B[a] \cong B[X]/(f)$ $(h(a) \longleftrightarrow h(X) + (f))$ *for some separable polynomial f 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.*

(c) *$B[a]$ is a projective, separable B-algebra with* $\text{rank}_B B[a]$.

Proof. The implications (a) ⇒ (b) ⇒ (c) follow immediately from the results of [8, Th. 3.4] and [3]. We assume (c) and set $\text{rank}_B B[a] = n$. Since $B[a]$ is finitely generated as B-module, by using the result of [2, Prop. 2.5.4], it is showed that for each maximal ideal M of B, the factor module $B[a]/B[a]M$ is a free B/M-module of rank n, that is, $B[a] = B + Ba + \cdots + Ba^{n-1} + B[a]M$. Hence it follows from

[9, Lemma 9.1] that $B[a] = B + Ba + \cdots + Ba^{n-1}$. Let $a^n = b_0 + b_1 a + \cdots + b_{n-1}a^{n-1}$, $b_i \in B$, and set $f = X^n - b_{n-1}X^{n-1} - \cdots - b_1 X - b_0$ ($\in B[X]$). Then we have a B-algebra isomorphism $B[X]/(f) \longrightarrow B[a]$ mapping $X + (f)$ into a (cf. [6, Th. 1.2]). Thus we obtain (a).

Remark 1.1. In [6], Miyashita proved a theorem: *For any monic polynomial f in $B[X]$, $B[X]/(f)$ is a free Frobenius extension of B.* As an alternative to the proof, we shall present a simple proof which is as follows:

Let $f = \sum_{i=0}^{n} b_i X^i$, $b_i \in B$, $b_n = 1$, and $B[X]/(f) = B[u]$, where $u = X + (f)$. Since the assertion is obvious for $n = 1$, we may assume $n \geqq 2$. As is easily seen, $\{1, u, \cdots, u^{n-1}\}$ is a free B-basis of $B[u]$. For $a = \sum_{i=0}^{n-1} c_i u^i \in B[u]$, we set $h(a) = c_{n-1}$. Moreover, we set $v_{n-i} = \sum_{k=0}^{i-1} b_{n-k} u^{i-(k+1)}$, $i = 1, \cdots, n$. Then $\{v_{n-1} = 1, v_{n-2}, \cdots, v_0\}$ is a free B-basis of $B[u]$. If $0 \leqq s < n-i$ then $v_{n-i}u^s = \sum_{k=0}^{i-1} b_{n-k} u^{i-(k+1)+s}$, and $i - (k+1) + s < n - 1$. $v_{n-i}u^{n-i} = \sum_{k=0}^{i-1} b_{n-k} u^{n-(k+1)}$. If $n - i < s \leqq n - 1$ then $v_{n-i}u^s = (v_{n-i}u^{n-i+1})u^{s-(n-i+1)} = (\sum_{k=0}^{i-1} b_{n-k} u^{n-k}) u^{s-(n-i+1)} = (-\sum_{j=0}^{n-i} b_j u^j) u^{s-(n-i+1)}$, and $j + s - (n - i + 1) < n - 1$. Hence we have $h(v_{n-i}u^r) = \delta_{n-i,r}$ (Kronecker's delta), $r = 0, 1, \cdots, n-1$. Since h is a B-homomorphism from $B[u]$ to B, it follows that h is a Frobenius homomorphism. Thus $B[u]$ is a Frobenius extension of B. (Cf. [6, p. 169]).

Moreover, by using the transitivity of Frobenius extensions and the result of [8, Cor. 1.1], we see that for any monic polynomial f in $B[X]$, the free splitting ring of f in the sense of [8, Def.] is a free Frobenius extension of B. (Cf. [6, Prop. 3.1]).

2. Splitting rings of separable polynomials over a connected ring. Throughout the rest of this note, a ring is called *connected* if it has no proper idempotents. Let f be a monic polynomial in $B[X]$ of degree n. As in [8, Def.], a ring extension S of B is called a *splitting ring* of f (over B) if $S = B[a_1, a_2, \cdots, a_n]$ and $f = (X - a_1)(X - a_2)\cdots(X - a_n)$. Moreover, a splitting ring $B[x_1, x_2, \cdots, x_n]$ of f is called *free* if for every splitting ring $B[a_1, a_2, \cdots, a_n]$ of f, there exists a B-algebra homomorphism $B[x_1, x_2, \cdots, x_n] \longrightarrow B[a_1, a_2, \cdots, a_n]$ mapping x_i into a_i for $i = 1, 2, \cdots, n$. By [8, Th. 1.1 and Cor. 1.1], f has a free splitting ring, which is a free B-module of rank $n!$. The following lemma is obtained from the result of Janusz [5, § 2]. However, for the convenience, we present here an alternative proof which is given as an application of the results on free splitting rings.

Lemma 2.1. *Let B be a connected ring, and f a separable poly-*

nomial in $B[X]$. *Then there exists a splitting ring of* f *which is projective over* B *and connected. Such splitting rings are Galois over* B *and unique up to isomorphism.*

Proof. By [8, Th. 1.1], f has a free splitting ring S over B, which is unique up to B-algebra isomorphism, and by [8, Th. 2.1], S is a $\mathfrak{G}$-Galois extension of B. If $S=\sum_{i=1}^{t} S_i$ is a direct decomposition of S into connected B-algebras, then the each S_i is a splitting ring of f which is projective and separable over B. Since the set of the identity elements of the S_i coincides with the set of all the primitive idempotents in S, it follows that the set $\{S_1, \cdots, S_t\}$ is invariant under $\mathfrak{G}$. Moreover, $\mathfrak{G}$ is transitive in the set $\{S_1, \cdots, S_t\}$, else there exists a proper idempotent in S which is invariant under $\mathfrak{G}$, whence is contained in B, contradicting the fact that B is connected. Thus, it follows that all the S_i are B-algebra isomorphic, and the each S_i is Galois over B. Now, let T be a splitting ring of f which is projective over B and connected. Then, recalling that S is a free splitting ring of f, we have a B-algebra epimorphism $\varphi: S \longrightarrow T$. The kernel of φ is generated by an idempotent (cf. [5, Lemma 1.6]). Since T is connected, it follows that $T\cong S/\ker\varphi \cong S_i$ (as B-algebras), $i=1, \cdots, t$. This completes the proof.

Theorem 2.1. *Let* B *be a connected ring, ~~of~~* f *a separable polynomial in* $B[X]$. *Let* S *be a splitting ring of* f *which is projective over* B. *Then* S *is Galois over* B. *If* T *is any splitting ring of* f *which is projective over* B *and with* $\mathrm{rank}_B T=\mathrm{rank}_B S$ *then* T *is* B*-algebra isomorphic to* S, *and conversely.*

Proof. As is easily seen, we have $S=\sum_{i=1}^{t} S_i$, a direct decomposition of S into connected B-algebras. Then the each S_i is a splitting ring of f which is projective over B and connected. Hence by Lemma 2.1, S_1 is a ${}_1\mathfrak{G}$-Galois extension of B, and all the S_i are B-algebra isomorphic. We choose here one isomorphism $\sigma_i: S_1 \longrightarrow S_i$ for each i and construct an automorphism σ of S such that $\sigma|S_i$ (the restriction of σ to S_i) $=\sigma_{i+1}\sigma_i^{-1}$ for $i<t$ and $\sigma|S_t=\sigma_t^{-1}$. For $\tau\in\mathfrak{G}_1$ and for σ^j $(0\leqq j\leqq t-1)$, (τ, σ^j) will mean an automorphism of S such that $(\tau, \sigma^j)|S_i=\sigma^{i+j}\tau\sigma^{-i}$ for each i. Then the set $\mathfrak{G}$ of the automorphisms (τ, σ^j) will be a group, and one will easily see that S is $\mathfrak{G}$-Galois over B. The rest of our assertion will be easily seen by noting the assumption $\mathrm{rank}_B T=\mathrm{rank}_B S$ and the result of Lemma 2.1.

Remark 2.1. Let $f=X^2-X\in B[X]$. Clearly f is separable over B (cf. [8, Th. 2.3]). We show here that if B is not connected then f has a splitting ring which is projective over B and not Galois over B. Let $B = Be_1 \oplus Be_2$, $e_1e_2 = 0$, $e_i^2 = e_i \neq 0$ $(i = 1, 2)$, and $Be_1[x, x_0]$ a free splitting ring of fe_1 over Be_1. We consider here $S = Be_1[x, x_0] \oplus Be_2$, a direct sum of rings. Then we have $S = B[x, x_0 + e_2]$ and $f = (X-x)(X-(x_0 + e_2))$. Hence S is a splitting ring of f over B. Since $Be_1[x, x_0]$ is a free Be_1-module of rank 2, S is a projective B-module, however, without $\mathrm{rank}_B S$, and so, S is not Galois over B.

3. Splitting rings of separable polynomials over an arbitrary ring. As in [10, (2.1)], $\mathscr{B}(B)$ will mean the Boolean ring consisting of all idempotents in B, and Spec $\mathscr{B}(B)$ will mean the Boolean spectrum of B which is the Stone space consisting of all prime ideals of $\mathscr{B}(B)$, where the family of the subsets $U_e = \{y \in \text{Spec } \mathscr{B}(B);\ e \in y\}$ $(e \in \mathscr{B}(B))$ forms a base of the open subsets of $\mathscr{B}(B)$. Now, let x be any element of Spec $\mathscr{B}(B)$. We denote by B_x the ring of residue classes of B modulo the ideal $\sum_{d \in x} Bd$. Then B_x is a connected ring ([10, (2.13)]). Let M be any B-module. Then, M_x denotes the tensor product $B_x \otimes_B M$, and for any element $a \in M$, a_x denotes the image of a under the canonical homomorphism $M \longrightarrow M_x$. Moreover, for any B-module N and for any element φ of $\mathrm{Hom}_B(M, N)$, we denote by φ_x the B_x-homomorphism $M_x \longrightarrow N_x$ sending a_x into $\varphi(a)_x$, and for any subset $\mathfrak{H}$ of $\mathrm{Hom}_B(M, N)$, we denote by $\mathfrak{H}_x$ the set of the homomorphisms φ_x, $\varphi \in \mathfrak{H}$.

First, we shall present the following lemma; this can be verified by making use of the same methods as in the proof of [10, (3.15)], however, will be proved here in some different way.

Lemma 3.1. *Let S be a ring extension of B which is finitely generated and projective over B. Let x be an element of Spec $\mathscr{B}(B)$, $\mathfrak{G}$ a finite group, and S_x a $\mathfrak{G}$-Galois extension of B_x. Then there exists an open neighborhood U_d $(=\{y \in \text{Spec } \mathscr{B}(B);\ d \in y\})$ of x such that $S(1-d)$ is a $\mathfrak{G}$-Galois extension of $B(1-d)$, and the canonical map $S_x \longrightarrow S(1-d)_x$ is both a B-algebra and a $\mathfrak{G}$-module isomorphism, where the $\mathfrak{G}$-module $S(1-d)_x$ is that induced by the $\mathfrak{G}$-module $S(1-d)$.*

Proof. By [10, (2. 14)], we can lift $\mathfrak{G}$ to a set of B-algebra automorphisms of S, which will be denoted by $\overline{\mathfrak{G}}$. The set $U = \{y \in \text{Spec } \mathscr{B}(B);\ \mathrm{rank}_{B_y} S_y = \mathrm{rank}_{B_x} S_x\}$ is open in Spec $\mathscr{B}(B)$ (cf. [2, Th. 2.5.1] and the result of [10, pp. 84 — 85]). Hence, by [10, (2.9)], the multiplication table of $\overline{\mathfrak{G}}$ that holds at x will hold in an open neighborhood U_c $(=\{y \in \text{Spec } \mathscr{B}(B);\ c \in y\})$ of x which is contained in U, that is, if $\sigma_x\tau_x = \rho_x$ $(\sigma, \tau, \rho \in \overline{\mathfrak{G}})$ then $\sigma_y\tau_y = \rho_y$ for every $y \in U_c$. Hence $\overline{\mathfrak{G}}$ will be a group in U_c and $\overline{\mathfrak{G}}|S(1-c)$ is a group which is isomorphic to $\mathfrak{G}$. Since S_x is $\mathfrak{G}$-Galois over B_x, there are elements $a_{1x}, \cdots, a_{nx}$; $b_{1x}, \cdots, b_{nx}$ in S_x such that $\sum_{i=1}^n a_{ix}\sigma_x(b_{ix}) = \delta_{1_x, \sigma_x}$ (Kronecker's delta) for all $\sigma \in \overline{\mathfrak{G}}$, where $a_{ix}=(a_i)_x$, $b_{ix} = (b_i)_x$ for all $i = 1, \cdots, n$. Then in an open neighborhood U_d $(= \{y \in \text{Spec}\,\mathscr{B}(B);\ d \in y\})$ of x which is contained in U_c, there holds that $\sum_{i=1}^n a_{iy}\sigma_y(b_{iy}) = \delta_{1_y, \sigma_y}$ for all $\sigma \in \overline{\mathfrak{G}}$. Hence we have $\sum_{i=1}^n a_i(1-d)\,\sigma\,(b_i(1-d)) = \delta_{1, \sigma}$ for all $\sigma \in \overline{\mathfrak{G}}$. Thus $S(1-d)$ is a Galois extension of $J(\overline{\mathfrak{G}}|S(1-d))$ with Galois group $\overline{\mathfrak{G}}|S(1-d)$. There holds here $\text{rank}_{B(1-d)}S(1-d) = \text{rank}_{B_x}S_x =$ the order of $\mathfrak{G} =$ the order of $\overline{\mathfrak{G}}|S(1-d) = \text{rank}_{J(\overline{\mathfrak{G}}|S(1-d))}S(1-d)$. This implies $B(1-d) = J(\overline{\mathfrak{G}}|S(1-d))$. Since $\overline{\mathfrak{G}}|S(1-d) \cong \mathfrak{G}$, $S(1-d)$ in a $\mathfrak{G}$-Galois extension of $B(1-d)$, and $S(1-d)_x \cong S_x$ as B-algebras and as $\mathfrak{G}$-modules. This completes the proof.

In [10], Zelinsky and Villamayor introduced the notion of weakly Galois extensions. A ring extension S of B is weakly Galois if and only if there exists a finite set of orthogonal non-zero idempotents $\{e_1, \cdots, e_t\}$ in B with $\sum_{i=1}^t e_i = 1$ and with Se_i Galois over Be_i for each i (cf. [10, (3.1) and (3.15)]).

Now, we shall prove the following

Theorem 3.1. *Let f be a separable polynomial in $B[X]$, and S a splitting ring of f which is projective over B. Then S is a weakly Galois extension of B.*

Proof. Let $x \in \text{Spec}\,\mathscr{B}(B)$. Then B_x is a connected ring, f_x $(\in B_x[X])$ is separable over B_x, and S_x is a splitting ring of f_x which is projective over B_x. Hence by Th. 2.1, S_x is a $\mathfrak{G}$-Galois extension of B_x. Therefore by Lemma 3.1, theere exists an open neighborhood U_d $(= \{y \in \text{Spec}\,\mathscr{B}(B);\ d \in y\})$ of x such that $S(1-d)$ is a $\mathfrak{G}$-Galois extension of $B(1-d)$. We employ here the compactness of $\text{Spec}\,\mathscr{B}(B)$ to obtain the theorem.

Lemma 3.2. *Let f be a separable polynomial in $B[X]$, and S, T splitting rings of f which are projective over B. Assume that there exists an element $x \in \text{Spec}\,\mathscr{B}(B)$ with $\text{rank}_{B_x}S_x = \text{rank}_{B_x}T_x$. Then there exists an open neighborhood U_e $(= \{y \in \text{Spec}\,\mathscr{B}(B);\ e \in y\})$ of x such that $S(1-e) \cong T(1-e)$ as $B(1-e)$-algebras.*

Proof. By Th. 2.1, we see that S_x, T_x are $\mathfrak{G}$-Galois extensions of B_x which are B-algebra and $\mathfrak{G}$-module isomorhic. Hence by Lemma 3.1, we can find an open neighborhood U_d ($= \{y \in \text{Spec } \mathscr{B}(B)\, ;\ d \in y\}$) of x such that $S(1-d)$, $T(1-d)$ are $\mathfrak{G}$-Galois extensions of $B(1-d)$ with $\varphi:\ S(1-d)_x \longrightarrow T(1-d)_x$, both a B-algebra and a $\mathfrak{G}$-module isomorphism. Now, by [10, (2.7)], we have the canonical isomorphism

$$\begin{aligned}&\text{Hom}_B(S(1-d)\oplus T(1-d),\ S(1-d)\oplus T(1-d))_x\\ &\cong \text{Hom}_B(S(1-d)_x\oplus T(1-d)_x,\ S(1-d)_x\oplus T(1-d)_x)\end{aligned}$$

which implies $\text{Hom}_B(S(1-d),\ T(1-d))_x \cong \text{Hom}_B(S(1-d)_x,\ T(1-d)_x)$. Hence φ is induced by some element $\bar{\varphi}$ of $\text{Hom}_B(S(1-d),\ T(1-d))$. Let $S(1-d) = Ba_1 + \cdots + Ba_n$. Then, noting that $\bar{\varphi}_x = \varphi$ and is both a B-algebra and a $\mathfrak{G}$-module isomorphism, there is an open neighborhood $U_e (= \{y \in \text{Spec } \mathscr{B}(B)\, ;\ e \in y\})$ of x such that $U_e \subset U_d$, and for every $y \in U_e$, $\bar{\varphi}(1-d)_y = (1-d)_y$, $\bar{\varphi}(a_i a_j)_y = \bar{\varphi}(a_i)_y \bar{\varphi}(a_j)_y$, $\bar{\varphi}(\sigma(a_i))_y = \sigma(\bar{\varphi}(a_i))_y$, where $i, j = 1, \cdots, n$, and σ runs over all the elements of $\mathfrak{G}$ (cf. [10, (2.9)]). Hence $\bar{\varphi}|S(1-e)$ is a B-algebra and $\mathfrak{G}$-module homomorphism, that is, a $B(1-e)$-algebra and $\mathfrak{G}$-module homomorphism from $S(1-e)$ to $T(1-e)$. Since $S(1-e)$ and $T(1-e)$ are $\mathfrak{G}$-Galois over $B(1-e)$, it follows from [3, Th. 3.4] that $\bar{\varphi}|S(1-e)$ is a $B(1-e)$-algebra isomorphism.

Now, by using the result of Lemma 3.2 and the compacteess of Spec $\mathscr{B}(B)$, we can easily check the following

Theorem 3.2. *Let f be a separable polynomial in $B[X]$, and S, T splitting rings of f which are projective over B. If* $\text{rank}_{B_x} S_x = \text{rank}_{B_x} T_x$ *for all* $x \in \text{Spec } \mathscr{B}(B)$ *then* $S \cong T$ *as B-algebras, and conversely.*

As a direct consequence of the theorem, we obtain the following

Corollary 3.1. *Let f be a separable polynomial in $B[X]$, and S, T splitting rings of f which are projective over B and have ranks over B. If* $\text{rank}_B S = \text{rank}_B T$ *then* $S \cong T$ *as B-algebras, and conversely.*

By using the result of Th. 3.2, we shall prove the following corollary which contains the result of DeMeyer [4, Th. 2.2].

Corollary 3.2. *Let f be a separable polynomial in $B[X]$. Assume that f has splitting rings S, T which are projective over B and with* $\mathscr{B}(S) = \mathscr{B}(T) = \mathscr{B}(B)$. *Then* $S \cong T$ *as B-algebras.*

Proof. For every $x \in \text{Spec } \mathscr{B}(B)$, $f_x\ (\in B_x[X])$ is separable over B_x, and S_x, T_x are splitting rings of f_x which are projective over B_x and connected; whence we have $\text{rank}_{B_x} S_x = \text{rank}_{B_x} T_x$ by Lemma 2.1. Therefore the assertion follows immediately from Th. 3.2.

Now, let f be a separable polynomial in $B[X]$, and $x \in \text{Spec } \mathscr{B}(B)$. By Lemma 2.1, f_x has a splitting ring N which is projective over B_x and connected; and then N is a Galois extension of B_x with a Galois group $\mathfrak{G}$, which is unique up to isomorphism. The uniquely determined group $\mathfrak{G}$ will be denoted by $\mathfrak{G}(f_x)$, and the order of $\mathfrak{G}$ will be denoted by $\mu(f_x)$. Next, if S is a splitting ring of f which is projective over B then S_x has a direct decomposition into a finite number of connected B_x-algebras N_i; $i = 1, 2, \cdots, t$. The number t will be denoted by $\nu(S_x, f_x)$. Moreover, we shall use the following conventions: $Z^+ = \{1, 2, \cdots\}$, $\mathscr{F}$ = the set of isomorphism classes of finite groups, and which will be topological spaces with the discrete topology. Now, under this situation, we shall prove the following theorem which contains the result of DeMeyer [4, Th. 2.1].

Theorem 3.3. *Let f be a separable polynomial in $B[X]$. Then the following conditions are equivalent.*

(a) *f has a splitting ring E over B with $\mathscr{B}(E) = \mathscr{B}(B)$ which is projective over B.*

(b) *The map φ_1:* Spec $\mathscr{B}(B) \longrightarrow \mathscr{F}$, $\varphi_1(x) =$ *the class containing* $\mathfrak{G}(f_x)$, *is continuous.*

(c) *The map φ_2:* Spec $\mathscr{B}(B) \longrightarrow Z^+$, $\varphi_2(x) = \mu(f_x)$, *is continuous.*

(d) *For any splitting ring S of f which is projective over B, the map φ_3:* Spec $\mathscr{B}(B) \longrightarrow Z^+$, $\varphi_3(x) = \nu(S_x, f_x)$, *is continuous.*

(e) *Any splitting ring of f which is projective over B contains a subring $E \supset B$ which is a splitting ring of f over B with $\mathscr{B}(E) = \mathscr{B}(B)$ (whence it is projective over B).*

Proof. We shall give a cyclic proof: (e) ⇒ (a) ⇒ (b) ⇒ (c) ⇒ (d) ⇒ (e). By [8, Th. 1.1], f has a splitting ring S which is projective over B. If E is a subring of S containing B which is a splitting ring of f over B then E is a separable B-algebra, which is projective over B by [5, Prop. 1.5]. This implies (e) ⇒ (a). Assume (a), and let E be a splitting ring of f with $\mathscr{B}(E) = \mathscr{B}(B)$ which is projective over B. Let $x \in \text{Spec } \mathscr{B}(B)$. Then E_x is a connected ring. Since E_x is a splitting ring of f_x ($\in B_x[X]$) which is projective over B_x, E_x is a Galois extension of B_x with a Galois group $\mathfrak{G}$; whence $\mathfrak{G} \cong \mathfrak{G}(f_x)$ (Lemma 2.1). Hence by Lemma 3.1, we can find an open neighborhood U_d ($= \{y \in \text{Spec } \mathscr{B}(B);\ d \in y\}$) of x such that $E(1-d)$ is a $\mathfrak{G}$-Galois extension of $B(1-d)$. Then, it is easily seen that for every $y \in U_d$, E_y is a $\mathfrak{G}$-Galois extension of B_y, and so, $\mathfrak{G}(f_y) \cong \mathfrak{G} \cong \mathfrak{G}(f_x)$. Thus we obtain (a) ⇒ (b).

The implication (b) $\Rightarrow$ (c) follows from the fact that φ_2 is the product of φ_1 and the continuous map $\mathscr{F} \longrightarrow Z^+$ sending $C \in \mathscr{F}$ into the order of a group in C. Next, to see that (c) $\Rightarrow$ (d) $\Rightarrow$ (e), S will be a splitting ring of f which is projective over B. Then, by using the results of Lemma 2.1 and [3, Lemma 4.1], it is easily seen that $\mathrm{rank}_{B_x} S_x = \mu(f_x)\nu(S_x, f_x)$ for every $x \in \mathrm{Spec}\, \mathscr{B}(B)$. Since the map $\mathrm{Spec}\, \mathscr{B}(B) \longrightarrow Z^+$ sending x into $\mathrm{rank}_{B_x} S_x$ is continuous, it follows that (c) $\Rightarrow$ (d). Now, let x be an element of $\mathrm{Spec}\, \mathscr{B}(B)$, and set

$$t = \nu(S_x, f_x).$$

Then we have a direct decomposition of S_x into connected B_x-algebras $S_x u_{ix}$ ($u_{ix} = (u_i)_x$, $i = 1, \cdots, t$), where

$$(\mathrm{A}_1) \qquad u_{ix}u_{jx} = \delta_{ij}u_{ix}\ (i,\ j = 1, \cdots, t), \text{ and } \textstyle\sum_{i=1}^{t} u_{ix} = 1_x.$$

Moreover, we have ring isomorphisms $B_x \cong B_x u_{ix}$ ($b_x \longrightarrow b_x u_{ix}$) and B_x-algebra isomorphisms $\sigma_i : S_x u_{1x} \longrightarrow S_x u_{ix}$, where $i = 1, \cdots, t$. Construct a B_x-algebra automorphism σ_x of S_x by demanding that $\sigma_x | S_x u_{ix} = \sigma_{i+1}\sigma_i^{-1}$ for $i < t$ and $\sigma_x | S_x u_{tx} = \sigma_t^{-1}$, and lift σ_x to a B-algebra automorphism of S, which will be denoted by σ (cf. [10, (2.14)]). Then there holds that

$$(\mathrm{A}_2) \qquad \sigma_x(u_{ix}) = u_{i+1x} \text{ for } i < t, \quad \sigma_x(u_{tx}) = u_{1x}.$$

Now, let $S = B[a_1, \cdots, a_n]$ where $f = \prod_{i=1}^{n}(X - a_i)$, and set $a_k' = \sum_{i=0}^{t-1} \sigma^i(a_k u_1)$ ($k = 1, \cdots, n$). As is easily seen, we have that

$$f_x = \Pi_{k=1}^{n}(X1_x - a_{kx}'),$$

$$B[a_1', \cdots, a_n']_x \cong B[a_1', \cdots, a_n']_x u_{1x} = S_x u_{1x}.$$

We shall here assume (d). By [10, (2.9)], we can find an open neighborhood U_e ($= \{y \in \mathrm{Spec}\, \mathscr{B}(B)\,;\ e \in y\}$) of x in which $\nu(S_y, f_y) = t$ (i.e., constant), and there hold the relations (A_1) and (A_2). Then, for every $y \in U_e$, $B[a_1', \cdots, a_n']_y$ is a splitting ring of f_y which is connected. Hence, by using the rresult of [10, (2.11)], it is seen that $B[a_1', \cdots, a_n'](1-e)$ is a splitting ring of $f(1-e)$ over $B(1-e)$ with $\mathscr{B}(B[a_1', \cdots, a_n'] \cdot (1-e)) = \mathscr{B}(B(1-e))$. Employing the compactness of $\mathrm{Spec}\, \mathscr{B}(B)$, it follows that S contains a subring $E \supset B$ which is a splitting ring of f over B with $\mathscr{B}(E) = \mathscr{B}(B)$. Thus we obtain (e). This completes the proof.

Remark 3.1. In [4], DeMeyer introduced the notion of uniform separable polynomials. By the result of Th. 3.3, we see that a separable polynomial f in $B[X]$ is uniform if and only if f satisfies one of the conditions (a) —— (e) in Th. 3.3.

Remark 3.2. Let f be a monic polynomial in $B[X]$ of degree n, and S a splitting ring of f over B which is a projective B-module of rank $n!$. Then S is a free splitting ring of f. Indeed, by [8, Th. 1.1 and Cor. 1.1], f has a free splitting ring T over B which is a free B-module of rank $n!$, and this is B-algebra homomorphic to S. Since $\mathrm{rank}_B T = \mathrm{rank}_B S$, it follows that T and S are B-algebra isomorphic. However, in case f is not separable, we can not see that any two splitting rings S' and T' of f which are projective over B and with $\mathrm{rank}_B S' = \mathrm{rank}_B T'$ are B-algebra isomorphic.

REFERENCES

[1] M. AUSLANDER and O. GOLDMAN: The Brauer group of a commutative ring, 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 Alex ROSENBERG: Galois theory and Galois cohomology of commutative rings, Mem. Amer. Math. Soc., **52** (1965), 15—33.

[4] F. DEMEYER: Separable polynomials over a commutative ring, Rocky Mt. J. Math., **2** (1972), 299—310.

[5] G. J. JANUSZ: Separable algebras over commutative rings, Trans. Amer. Math. Soc., **122** (1966), 361—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 ring, Math. J. of Okayama Univ., **14** (1970), 175—181.

[8] T. NAGAHARA: On separable polynomials over a commutative ring II, Math. J. of Okayama Univ., **15** (1972), 149—162.

[9] D. G. NORTHCOTT: Introduction to homological algebra, Cambridge University Press, 1960.

[10] O. E. VILLAMAYOR and D. ZELINSKY: Galois theory with infinitely many idempotents, Nagoya Math. J., **35** (1969), 83—93.

DEPARTMENT OF MATHEMATICS
OKAYAMA UNIVERSITY

(Received January 10, 1973)