Math. J. Okayama Univ. 31 (1989), 31–55

ON PRIMITIVE ELEMENTS OF GALOIS EXTENSIONS OF COMMUTATIVE SEMI-LOCAL RINGS

Dedicated to Professor Yoshiki Kurata on his 60th birthday

Isao KIKUMASA, Takasi NAGAHARA and Kazuo KISHIMOTO

Throughout this paper, all rings will be assumed commutative, and all Galois extensions will mean Galois extensions in the sense of [1]. Moreover, A will mean a commutative ring with identity element 1, and all ring extensions of A will be assumed with identity element 1, the identity element of A. If A contains only finitely many maximal ideals then A will be called a *semi-local ring*. A ring extension B/A will be called to be *simple* if B is generated by a single element over A, that is, B/A has a primitive element. A Galois extension B/A will be called to be *trivial* if B is A-algebra isomorphic to a direct sum $A \oplus A \oplus \cdots \oplus A$. A G-Galois extension will be called an *abelian* (resp. *cyclic*) G-extension if G is abelian (resp. cyclic). Furthermore, a G-Galois extension B/A will be called to be *of Kummer type* (abbr. *of K-type*) if $|G| = n \in \mathrm{U}(A)$ and A contains a primitive n-th root ζ of 1 with $1-\zeta^i \in \mathrm{U}(A)$ for $i = 1, \ldots, n-1$, where $|G|$ is the order of G and $\mathrm{U}(A)$ is the set of the units in A.

In [4], [5] and etc, the authors made some studies on primitive elements of Galois extensions in several angles. In this paper, we shall make a study on the simplicity of Galois extensions, the construction of primitive elements, and the cardinality of the set of primitive elements. § 1 concerns with primitive elements of Galois extensions (rings) of a field, and so, A will mean a field throughout this section. The study is one maked on a connection of primitive elements and maximal subfields in Galois extensions of A. In [15], J. -D. Thérond made a study for separable extensions of a semi-local ring. In § 2, the first half contains some preliminary results for our studies in the subsequent section, some of which are discussions made on [15]. This contains such a result as all Galois extensions of a semi-local rings of K-type are simple. The latter half is devoted to some characterizations of primitive elements of Galois extensions over a complete Noetherian local ring which contains some generalizations of § 1 to such Galois extensions, and this also may be taken as a continuation of G. J. Janusz [3, § 3]. In § 3, we consider a tensor product B of Galois

extensions of a semi-local ring A and an abelian extension B/A of K-type in order to prove that B/A has a special type of primitive elements which are closely related to the Galois structure of B/A, provided $|A/M| \geqq (\mathrm{rank}_A B)^2/2$ for all maximal ideals M in A. For these purposes, we shall treat A mainly as a semi-local ring in § 2 and § 3.

In what follows, for "a set E, a ring B, a subset C of B, a group G of automorphisms of B, a subset S of G, and an A-module M", we shall use the following conventions :

$|E|$ = the cardinal number of E,

$\langle S \rangle$ = the group generated by S,

$S|C$ = the restriction of S to C,

$B^S = \{b \in B;\ \sigma(b) = b \text{ for all } \sigma \in S\}$,

$G_C = \{\sigma \in G;\ \sigma(c) = c \text{ for all } c \in C\}$,

$\mathrm{U}(B)$ = the set of all the units in B,

$\ell(B)$ = the length of composition series of B-module B,

$[M : A]$ = the rank of A-module M if A is a field,

$\mathrm{rank}_A M = c$ if M_A is projective, finitely generated, and $\mathrm{rank}_{A_p} M_p$ is of constant c for all prime ideals p of A where M_p is the localization of M_A at p.

1. Simplicity of Galois extensions of a field. In this section, we shall study necessary and sufficient conditions of the simplicity for a Galois extension of a field by using its maximal subfields. For this discussion, let A denote a field throughout this section.

The next lemma can be proved by making use of the same methods as in the proofs of [3], [10, Lemma 10] and [16]. However, for the conveniences, we shall here present a direct proof.

Lemma 1.1. *Let C be a local ring. Let B/C be a G-Galois extension, and E the set of primitive idempotents of B. Then, E is non-empty and G is transitive on the set E. Moreover, for any $e, c \in E$, $G_e|eB \cong G_e \cong G_c$, $|G_e||E| = |G_e|\ell(B) = |G|$ and eB/eC is $(G_e|eB)$-Galois. Hence B is C-algebra isomorphic to a C-algebra $\sum_{i=1}^{r} \oplus B_i$ such that $B_i = B_1$ $(1 \leqq i \leqq r)$, B_1/C_1 is H-Galois, $C = \{(a_1, a_1, \ldots, a_1);\ a_1 \in C_1\}$, and B_1 has no proper idempotents. When this is the case, $H \cong G_e$ for any $e \in E$. If, in particular, C is a field then B_1 is also a field, and $r = \ell(B)$.*

Proof. Let M be a unique maximal ideal of C. Then MB is contained

in the Jacobson radical of B. Hence, there are no non-zero idempotents in MB. As is easily seen, the factor ring B/MB is a Galois extension of a field C/M, and whence this is a semi-simple ring. Noting those facts, one will easily see that B has no infinite chains of idempotents. Thus, E is non-empty. Now, let $e \in E$, and set

$$|\sigma(e)\,;\ \sigma \in G| = |\sigma_1(e) = e_1 = e,\ \sigma_2(e) = e_2, \ldots,\ \sigma_r(e) = e_r|$$

where σ_1 is identity, and $e_i \neq e_j$ for each $i \neq j$. We shall here set

$$f = e_1 + \cdots + e_r.$$

Since the e_i are orthogonal and $\sigma(f) = f$ for all $\sigma \in G$, we have $f = 1$, the identity element of $C \subset B$. Hence $|\sigma(e)\,;\ \sigma \in G|$ coincides with E. Moreover, each Be_i is a separable Ce_i-algebra in the sense of [1] and [3] (and if, in particular, C is a field then so is each Be_i). Next, we consider

$$K = G_{e_1},\ B^K \cap Be_1, \text{ and } H = K|Be_1.$$

Obviously r coincides with the index of K in G. Now, for any element $a_1 \in B^K \cap Be_1$, we set

$$a_i = \sigma_i(a_1)\ (1 \leqq i \leqq r), \text{ and } a = a_1 + \cdots + a_r.$$

Let σ be an element of G. For any $i\ (1 \leqq i \leqq r)$, if $\sigma(e_i) = e_j\ (1 \leqq j \leqq r)$ then $\sigma_j^{-1}\sigma\sigma_i(e_1) = e_1$, and so, $\sigma_j^{-1}\sigma\sigma_i(a_1) = a_1$ which implies $\sigma(a_i) = a_j$. It follows that $\sigma(a) = a$ for all $\sigma \in G$, and so, $a \in C$. Hence $a_1 = ae_1 \in Ce_1$. Therefore, we have $B^K \cap Be_1 = Ce_1$. Moreover, for elements $x_1, \ldots, x_m,\ y_1, \ldots, y_m$ in B with $\sum_{i=1}^m x_i\sigma(y_i) = \delta_{1,\sigma}\ (\sigma \in G)$, we have

$$e_1\textstyle\sum_i x_i\tau(y_i) = \sum_i e_1x_i\tau(e_1y_i) = e_1\delta_{1,\tau}\ (\tau \in K),$$

where $\delta_{1,\tau}$ means the Kronecker's delta. Thus, it follows that Be_1/Ce_1 is an H-Galois extension with $H = K|Be_1$, and $|H|r = (\mathrm{rank}_{Ce_1} Be_1)r = \mathrm{rank}_C B = |G| = |K|r$. Obviously $H \cong K$ and $r = \ell(B)$, completing the proof.

Lemma 1.2. *Let B/A be a Galois extension of rank n. Let* F *be the set of maximal subfields of B containing A, and $|e_1, \ldots, e_r|$ the set of primitive idempotents of B. Then, $|\mathrm{F}| = (n/\ell(B))^{\ell(B)-1}$. Moreover, for any $L \in \mathrm{F}$, $B = Le_1 \oplus \cdots \oplus Le_r$, $L \cong Le_i = Be_i\ (1 \leqq i \leqq r)$, $[L : A] = n/\ell(B)$ and L/A is Galois.*

Proof. By Lemma 1, we have

$$B = Be_1 \oplus \cdots \oplus Be_r$$

where Be_1 is a field which is a Galois extension of Ae_1 and this is A-algebra isomorphic to each $Be_i (1 \leqq i \leqq r)$. Let K be an arbitrary subfield of B containing A. Then, for each i, there exists an A-algebra isomorphism $Ke_1 \to Ke_i \subset Be_i$ $(ke_1 \to ke_i,\ k \in K)$, and this can be extended to an A-algebra isomorphism

$$\tau_i : Be_1 \to Be_i$$

since Be_1 is a Galois extension of Ae_1. From this, one will easily see that K is a subfield of

$$T(\tau_2, \ldots, \tau_r) = \{b + \textstyle\sum_{i=2}^{r} \tau_i(b) \ ;\ b \in Be_1\}.$$

If $K \in \mathrm{F}$ then we have $K = T(\tau_2, \ldots, \tau_r)$. Therefore, it follows that $|\mathrm{F}| = (n/r)^{r-1}$. The other assertions will be easily seen.

Remark 1.1. (1) Let N be a group of order r, and $N = \{v_1 = 1, v_2, \ldots, v_r\}$. We consider here a representation π of N into the symmetric group S_r on the set $\{1, \ldots, r\}$ given by $v_{\pi(v)(i)} = vv_i$ $(i = 1, \ldots, r)$, $v \in N$. Let C be a ring with identity 1, and $S = C_1 \oplus \cdots \oplus C_r$ where $C_i = C$ $(1 \leqq i \leqq r)$. Moreover, let $e_i = (0, \ldots, 0, 1, 0, \ldots, 0)$ $(1 \in C_i)$ for $i = 1, \ldots, r$. Then, for a composition $N \times S \to S$ defined by

$$v(\textstyle\sum_{i=1}^{r} c_i e_i) = \sum_{i=1}^{r} c_i e_{\pi(v)(i)} \ (c_i \in C\ ;\ 1 \leqq i \leqq r),$$

we shall prove that S/C is an N-Galois extension where $C = \{(c, \ldots, c)\ ;\ c \in C\}$. Since $\pi(N)$ is transitive on the set $\{1, \ldots, r\}$, N is also transitive on the set $\{e_1, \ldots, e_r\}$. Hence we have $S^N = C$ and $\sum_{i=1}^{r} e_i v(e_i) = \delta_{1,v}$ $(v \in N)$. Hence S/C is an N-Galois extension of C. Now, let T be an H-Galois extension of C. Then $T \otimes_C S$ is an $(H \times N)$-Galois extension and $T \otimes_C S \cong T \oplus \cdots \oplus T$ (r times). Hence, in particular, for any field H-Galois extension L/A and for any finite group N, there exists an $(H \times N)$-Galois extension B/A with $B \supset L \supset A$ such that L is a maximal subfield of B containing A and $\ell(B) = |N|$.

(2) If B_i/A $(i = 1, 2)$ be G_i-Galois extensions of rank n with $B_i \supset L \supset A$ such that L is a maximal subfield of B_i $(i = 1, 2)$ then, by Lemma 1.1 and Lemma 1.2, B_1 and B_2 are A-algebra isomorphic (even for $G_1 \neq G_2$).

(3) Let B/A be a Galois extension. If B has a maximal subfield L

containing A which is a cyclic extension of A then we can choose a cyclic group as a Galois group of B/A because of Lemma 1.1, Lemma 1.2 and [11, Lemma 1.1]. Hence, in case that A is a finite field, we can consider the Galois extension B/A as a cyclic extension.

Now, for the convenience, we shall here present the following lemma whose result is contained in [9].

Lemma 1.3 ([9, Theorem 3.3 and Theorem 3.4]). *Let B be a G-Galois extension over a ring C with $\mathrm{rank}_C B = n$, and b an element of B. Then, b is a primitive element of B/C if and only if $b-\sigma(b) \in \mathrm{U}(B)$ for all $\sigma \neq 1$ in G. When this is the case, $\{1, b, b^2, \ldots, b^{n-1}\}$ is a free C-basis of ${}_CB$.*

Given a field extension E/A of degree $m < \infty$, by $\mathrm{I}_A(E)$, we denote the set of monic irreducible polynomials g in $A[X]$ of degree m with $g(a) = 0$ for some a in E. Then, it is obvious that E/A is simple if and only if $\mathrm{I}_A(E)$ is non-empty.

Now, we shall prove the following proposition which is a special change of ones in [2], [3] and etc. ; however, this is useful in our study and lately the result will be generalized to the case that B is a Galois extension of a complete Noetherian local ring (Theorem 2.6).

Proposition 1.4. *Let B/A be a G-Galois extension. Let L be an arbitrary maximal subfield of B containing A, and $\{e_1, \ldots, e_r\}$ the set of primitive idempotents of B. Then, there hold the following* (1) *and* (2).

(1) *Assume that B/A has a primitive element b. Then $|\mathrm{I}_A(L)| \geqq \ell(B) = r$. Moreover, there exists a pair of a subset $\{b_1, \ldots, b_r\}$ in L and a subset $\{f_1, \ldots, f_r\}$ in $\mathrm{I}_A(L)$ such that $f_i \neq f_j$ for each pair $i \neq j$ $(1 \leqq i, j \leqq r)$, $f_i(b_i) = 0$ for $i = 1, \ldots, r$, and*

$$b = b_1 e_1 + \cdots + b_r e_r.$$

(2) *Assume that $|\mathrm{I}_A(L)| \geqq \ell(B) = r$. Let $\{g_1, \ldots, g_r\}$ be a subset of $\mathrm{I}_A(L)$ with $g_i \neq g_j$ for each pair $i \neq j$ $(1 \leqq i, j \leqq r)$. Then, for any subset $\{c_1, \ldots, c_r\}$ of L such that $g_i(c_i) = 0$ for $i = 1, \ldots, r$, the following*

$$c = c_1 e_1 + \cdots + c_r e_r$$

is a primitive element of B/A, and $\prod_{i=1}^{r} g_i = \prod_{\sigma \in G}(c - \sigma(c))$.

Proof. By Lemma 1.2, we have

$$B = Le_1 \oplus \cdots \oplus Le_r.$$

(1) Let b be a primitive element of B/A. Then

$$b = b_1 e_1 + \cdots + b_r e_r$$

where $b_i \in L$ for $i = 1, \ldots, r$. Let f_i be the (monic) minimal polynomial of b_i over A so that $f_i(b_i) = 0$. We set here

$$\{f_1, \ldots, f_r\} = \{u_1, \ldots, u_t\}, \text{ and } u = u_1 u_2 \cdots u_t$$

where $u_i \neq u_j$ for each pair $i \neq j$ $(1 \leqq i, j \leqq t)$. Then $r \geqq t$ and

$$u(b) = \sum_{i=1}^{r} u(b) e_i = \sum_{i=1}^{r} u(be_i) e_i = \sum_{i=1}^{r} u(b_i) e_i = 0.$$

Let $m = [L : A]$. Then $[B : A] = mr$. Hence by Lemma 1.3, $\{1, b, \ldots, b^{mr-1}\}$ is a free A-basis of ${}_AB$. Since $u(b) = 0$, it follows that $\deg u \geqq mr$. On the other hand, we have $\deg u = \sum_{i=1}^{t} \deg u_i$ and $\deg u_i \leqq m$ for $i = 1, \ldots, t$. Therefore, it follows that $r = t$, and $\deg u_i = m$ for $i = 1, \ldots, r$. This implies that $f_i \in \mathrm{I}_A(L)$ for $i = 1, \ldots, r$.

(2) We assume that $|\mathrm{I}_A(L)| \geqq \ell(B) = r$. Let $\{g_1, \ldots, g_r\} \subset \mathrm{I}_A(L)$ with $g_i \neq g_j$ for each pair $i \neq j$ $(1 \leqq i, j \leqq r)$ and $\{c_1, \ldots, c_r\}$ a subset of L such that $g_i(c_i) = 0$ for $i = 1, \ldots, r$. We set here

$$c = c_1 e_1 + \cdots + c_r e_r.$$

Then, for $g = \prod_{i=1}^{r} g_i$, we have

$$\begin{aligned} A[X]/gA[X] &\simeq A[X]/g_1 A[X] \oplus \cdots \oplus A[X]/g_r A[X] \\ &\simeq A[c_1]e_1 + \ldots + A[c_r]e_r = B \end{aligned}$$

where $X + gA[X]$ corresponds to $c_1 e_1 + \cdots + c_r e_r$. Hence c is a primitive element of B/A. Moreover, we have $g(c) = 0$. Now, we set $h = \prod_{\sigma \in G}(X - \sigma(c))$. Then $h \in A[X]$ and $h(c) = 0$. By Lemma 1.3, elements $1, c, \ldots, c^{mr-1}$ are linearly independent over A. Since $\deg h = |G| = mr = \deg g$, it follows that $h = g$.

Now, let B/A be a Galois extension which is simple and with $\ell(B) = r$. Moreover, let L be a maximal subfield of B containing A. In the rest of this section, by $\mathrm{P}(B/A)$, we denote the set of primitive elements of B/A. Given any $b \in B$, by $f(X; b)$, we denote the monic polynomial f of minimal degree so that $f(b) = 0$. Further, by $\mathrm{S}(\mathrm{I}_A(L)^r)$, we denote the

set of polynomials $f = \prod_{i=1}^{r} f_i$ such that $f_1, \ldots, f_r \in \mathrm{I}_A(L)$ and $f_i \neq f_j$ for each pair $i \neq j$ $(1 \leqq i, j \leqq r)$.

In virtue of Proposition 1.4, we obtain the following

Corollary 1.5. *Let B/A be a Galois extension.*

(1) (cf. [3, Lemma 3.1])

(a) *If $|A| = \infty$ then B/A is simple.*

(b) *If A is of characteristic 0 then B/A is simple.*

(2) *Let $[B : A] = n$, $\ell(B) = r$, and L a maximal subfield of B containing A. If B/A is simple then*

(a) $|f(X; b);\ b \in \mathrm{P}(B/A)| = \mathrm{S}(\mathrm{I}_A(L)^r)$.

(b) *For any $b \in \mathrm{P}(B/A)$, $f(X; b) = \prod_{\sigma \in G}(X - \sigma(b))$.*

(c) *For any $f \in \mathrm{S}(\mathrm{I}_A(L)^r)$, $|| b \in \mathrm{P}(B/A) ;\ f(b) = 0 ||$ $= (n/r)^r r!$.*

Let A be a finite field with $|A| = q$, and B/A a Galois extension of rank n with $r = \ell(B)$ which contains a maximal subfield L containing A. Then L is isomorphic to $\mathrm{GF}(q^{n/r})$. Hence, we denote this Galois extension B/A by $\mathrm{GE}(q, n, r)$. Moreover, $\mathrm{I}_A(L)$ coincides with the set of monic irreducible polynomials in $A[X]$ of degree $[L : A]$. Hence, we denote $\mathrm{I}_A(L)$ by $\mathrm{I}_q(m)$ where $m = [L : A]$. Further, we denote $|\mathrm{I}_q(m)|$ by $\mathrm{N}_q(m)$ which is as in [7]. By [7, Theorem 3.25], there holds that

$$(*) \qquad \mathrm{N}_q(m) = (1/m)\textstyle\sum_{d|m} \mu(d) q^{m/d}$$

where μ is the Moebius function, that is,

$$\mu(d) = \begin{cases} 1 & \text{if } d = 1, \\ (-1)^k & \text{if } d \text{ is the product of } k \text{ distinct primes,} \\ 0 & \text{if } d \text{ is divisible by the square of primes.} \end{cases}$$

Next, we shall prove the following theorem which is about primitive elements of Galois extensions over a finite field.

Theorem 1.6. *Let $A = \mathrm{GF}(q)$ and $B = \mathrm{GE}(q, n, r)$.*

(1) (a) *B/A is simple if and only if $r\ (= \ell(B)) \leqq \mathrm{N}_q(n/r)$.*

(b) *If B/A is simple then*

$$|\mathrm{P}(B/A)| = \binom{\mathrm{N}_q(n/r)}{r} (n/r)^r r!.$$

(2) *Let $r < n$ and $n = z^k$ for some prime z and some integer k.*

(a) *B/A is simple if and only if $n \leqq q^{n/r}-q^{n/(rz)}$, and this is equivalent to that there exists a maximal subfield L of B containing A such that $[L : A] \geqq c(q, z, n)$ where $c(q, z, n) = z \cdot \log_q x_0$ for the root x_0 of the equation $X^z-X = n$ on $(1, \infty)$.*

(b) *If B/A is simple then*

$$|\mathrm{P}(B/A)| = \binom{(r/n)(q^{n/r}-q^{n/(rz)})}{r}(n/r)^r r!\,.$$

(c) *If $B' = \mathrm{GE}(q, n, s)$ and $\mathrm{N}_q(n/s) \geqq s > r$ then*
(i) *If $n \neq 2$ then $|\mathrm{P}(B'/A)| < |\mathrm{P}(B/A)|$.*
(ii) *If $n = 2$ then $|\mathrm{P}(B'/A)| = |\mathrm{P}(B/A)|$.*

Proof. The assertion (1) follows immediately from the result of Proposition 1.4. Now, we shall prove (2)(a). By (*) and (1), we see that B/A is simple if and only if $r \leqq (r/n)(q^{n/r}-q^{n/(rz)})$. Setting $x = q^{n/(rz)}$, this inequality is equivalent to that $n \leqq x^z-x$. Since $f(X) = X^z-X$ is strongly monotone-increasing on $(1, \infty)$, it follows that $n \leqq x^z-x$ if and only if $q^{n/(rz)} = x \geqq x_0$ for the root x_0 of the equation $X^z-X = n$ on $(1, \infty)$, which is equivalent to that $n/r \geqq z \cdot \log_q x_0$. This shows (2)(a). The assertion (2)(b) is a direct consequence of (1)(b).

Next, we shall prove (2)(c).

(i) Let $n \neq 2$. Put $n = z^k = ur = vs$, and let $x = \mathrm{N}_q(u)$ and $y = \mathrm{N}_q(v)$. Then $x = (1/u)(q^u-q^{u/z})$, and $y = (1/v)(q^v-q^{v/z})$ if $n > s$, and $y = q$ if $n = s$. Since $y \geqq s$, $vy \geqq vs = n = ur$. Hence

$$ux-ur \geqq ux-vy \geqq q^u-q^{u/z}-q^v \geqq q^u-2q^{u/z}.$$

Moreover, we note that the following inequality holds : For $a, b, t \geqq a+1 \in \mathbb{N}$ and $(a, b) \neq (1, 1)$,

$$(**) \qquad \frac{t^b-1}{(t-a)^b} > \frac{t^b-2}{(t-a)^b} \geqq 1.$$

(Because $f'(t) \geqq 0$ $(t \geqq a+1)$ and $f(a+1) \geqq 0$ for $f(t) := t^b-2-(t-a)^b$).

Case 1. $s < n$: Since $r < s$, $s = rd$ and $u = vd$ for some integer $d \geqq z$. Let $v/z = a$. Then we have

$$\frac{\mathrm{P}(B/A)}{\mathrm{P}(B'/A)} = \frac{x(x-1)\cdots(x-r+1)u^r}{y(y-1)\cdots(y-s+1)v^s} > \frac{(x-r)^r u^r}{y^s v^s} = \frac{(ux-ur)^r}{(vy)^s}$$
$$\geqq \frac{(q^u-2q^{u/z})^r}{(q^v-q^{v/z})^s} = \frac{(q^{adz}-2q^{ad})^r}{(q^{az}-q^a)^{rd}}$$

$$= \left[\frac{q^{ad}\{q^{ad(z-1)}-2\}}{q^{ad}\{q^{a(z-1)}-1\}^d}\right]^r = \left[\frac{\{q^{a(z-1)}\}^d-2}{\{q^{a(z-1)}-1\}^d}\right]^r \geqq 1 \qquad \text{(by (**))}.$$

Case 2. $s = n$: First let $r = 1$. Then $n = s = u$. Let $u/z = a$. If $a(z-1) = 1$ then $a = 1$ and $z = 2$ because $a, z \in \mathbb{N}$. This implies that $n = ru = rza = 2$, which is a contradiction. Hence $a(z-1) \geqq 2$. Thus we have

$$\begin{aligned}\frac{P(B/A)}{P(B'/A)} &= \frac{q^u-q^{u/z}}{q(q-1)\cdots(q-u+1)} \geqq \frac{q^{za}-q^a}{q^a\cdot(q-a)\cdots(q-u+1)} \\ &= \frac{q^{a(z-1)}-1}{(q-a)\cdots(q-u+1)} \geqq \frac{q^{a(z-1)}-1}{(q-a)^{u-a}} \\ &= \frac{q^{a(z-1)}-1}{(q-a)^{a(z-1)}} > 1 \qquad \text{(by (**))}.\end{aligned}$$

Next let $r \geqq 2$ and let $u/z = a$. Then, by the same ways as in the above, we have

$$\begin{aligned}\frac{P(B/A)}{P(B'/A)} &= \frac{x(x-1)\cdots(x-r+1)u^r}{q(q-1)\cdots(q-s+1)} = \frac{xu(xu-u)\cdots(xu-ru+u)}{q(q-1)\cdots(q-s+1)} \\ &= \frac{xu}{q(q-1)\cdots(q-u+1)}\cdot\frac{(xu-u)\cdots(xu-ru+u)}{(q-u)\cdots(q-s+1)} \\ &> \frac{q^u-q^{u/z}}{q(q-1)\cdots(q-u+1)}\cdot\frac{(xu-ru)^{r-1}}{(q-u)^{s-u}} \\ &\geqq \frac{q^{a(z-1)}-1}{(q-a)^{a(z-1)}}\cdot\frac{(q^u-2q^{u/z})^{r-1}}{(q-u)^{ur-u}} \\ &\geqq 1\cdot\left\{\frac{q^{za}-2q^a}{(q-u)^{za}}\right\}^{r-1} \qquad \text{(by (**))} \\ &= \left[\left\{\frac{q}{(q-u)}\right\}^a\cdot\frac{q^{a(z-1)}-2}{(q-u)^{a(z-1)}}\right]^{r-1} > \left\{\frac{q^{a(z-1)}-2}{(q-u)^{a(z-1)}}\right\}^{r-1} \geqq 1 \\ &\qquad \text{(by (**))}.\end{aligned}$$

(ii) Let $n = 2$. Then $n = s = z = 2 = ru$. It follows from $s > r$ that $r = 1$ and $u = 2$. Hence we obtain

$$P(B/A) = N_q(2)\cdot 2 = q^2-q = \binom{q}{2}\cdot 2 = P(B'/A).$$

2. Simplicity of a Galois extension of a semi-local ring. The following proposition is fundamental and useful in the next section. Some part

of this proposition is proved by making use of the same methods as in one by J. -D. Thérond [16, pp. 33−34].

Proposition 2.1. *Let A be a semi-local ring with $\{M_1, M_2, \ldots, M_m\}$ the set of maximal ideals in A and let B/A be a Galois extension. Then, B is generated by r elements over A if and only if each B/M_iB is generated by r elements over A/M_i $(i = 1, \ldots, m)$. When this is the case, if $\{z_{ij}+M_iB;\ j = 1, \ldots, r\}$ is a generating system of $(B/M_iB)/(A/M_i)$ for each i then there exist elements $a_1, \ldots, a_m$ in A such that $\{\sum_{i=1}^m a_i z_{ij};\ j = 1, \ldots, r\}$ is a generating system of B/A.*

Proof. We first note that, as is well-known, each $(B/M_iB)/(A/M_i)$ is a Galois extension. Clearly, if B is generated by r elements over A then each B/M_iB is generated by r elements over A/M_i $(i = 1, \ldots, m)$. We shall prove the converse.

Let $I = M_1 \cap M_2 \cap \cdots \cap M_m$ and $J = M_1B \cap M_2B \cap \cdots \cap M_mB$. Then, as in Demonstration in [15, p. 33], $I = A \cap J$ and $M_iB + M_jB = B\ (i \neq j)$, and whence, there exist an isomorphism ϕ and elements $a_1, a_2, \ldots, a_m$ in A such that

$$\begin{array}{ccccccccc} B/J & \overset{\phi}{\tilde{\longrightarrow}} & B_0 := & B/M_1B & \oplus & B/M_2B & \oplus \cdots \oplus & B/M_mB \\ \uparrow & & \uparrow & \uparrow & & \uparrow & & \uparrow \\ A/I & \tilde{\longrightarrow} & A_0 := & A/M_1 & \oplus & A/M_2 & \oplus \cdots \oplus & A/M_m \end{array}$$

and $\phi(a_i+J) = (0, \ldots, 0, 1+M_iB, 0, \ldots, 0)$ $(1 \leqq i \leqq m)$. Now, assume that each $(B/M_iB)/(A/M_i)$ has a generating system $\{z_{ij}+M_iB;\ j = 1, \ldots, r\}$. Moreover, set $z_j = \sum_{i=1}^m a_i z_{ij}$ and $z_{0j} = \phi(z_j+J)$ $(1 \leqq j \leqq r)$. Then, $z_{0j} = (z_{1j}+M_1B, z_{2j}+M_2B, \ldots, z_{mj}+M_mB)$ and $A_0[\{z_{0j};\ j = 1, \ldots, r\}] = B_0$. Hence, for $E = \{z_j;\ j = 1, \ldots, r\}$, it follows that $A[E]+J = B$ and so $A[E]+M_iB = B\ (1 \leqq i \leqq m)$. This means that $A[E] = B$ (cf. [13, p. 181, Lemma 1]), completing the proof.

The following corollary is obtained as a direct consequence of [15, Theoreme de l'element primitif]. We here prove it by the result of Theorem 1.6.

Corollary 2.2. *Let A be a semi-local ring and B/A a Galois extension of rank n. If $|A/M| \geqq n$ for all maximal ideals M in A then B/A is simple.*

Proof. Let M be an arbitrary maximal ideal in A. Then, $(B/MB)/(A/M)$ is a Galois extension of rank n. Let $q = |A/M|$ and $t = n/\ell(B/MB)$, and assume that $q \geqq n$. Noting that if $\mathrm{GF}(q^t) = \mathrm{GF}(q)[\alpha]$ then $\mathrm{GF}(q^t) = \mathrm{GF}(q)[\alpha+a]$ for any a in $\mathrm{GF}(q)$, one will easily see that $|\mathrm{P}(\mathrm{GF}(q^t)/\mathrm{GF}(q))| \geqq q$ and $t \cdot \mathrm{N}_q(t) \geqq q$. It follows that $\ell(B/MB) = n/t \leqq q/t \leqq \mathrm{N}_q(t)$. Hence, $(B/MB)/(A/M)$ is simple by Theorem 1.6, and so, B/A is simple by Proposition 2.1.

Corollary 2.3. *Let A be a semi-local ring and B/A a Galois extension of rank n. If A contains n-elements $a_1, a_2, \ldots, a_n$ such that $a_i - a_j \in \mathrm{U}(A)$ for all i and j $(1 \leqq i \neq j \leqq n)$ then B/A is simple.*

Proof. Let a_i be as in the statement of the corollary. Then, for any maximal ideal M in A, we see that

$$\bar{a}_i - \bar{a}_j \in \mathrm{U}(A/M) \text{ for any pair } i \neq j \ (1 \leqq i, j \leqq n)$$

where $\bar{a}_i = a_i + M$, which implies that $|A/M| \geqq n$. Therefore, by Corollary 2.2, B/A is simple.

Proposition 2.4. *Let A be a semi-local ring. If B/A is a Galois extension of K-type then B/A is simple.*

Proof. Let $n = [B : A]$ and ζ a primitive n-th root of 1. Then,

$$\mathrm{U}(A) \ni 1, \zeta, \ldots, \zeta^{n-1}, 1-\zeta^i \ (1 \leqq i \leqq n-1).$$

Hence we see that for any pair (i, j) $(0 \leqq i \neq j \leqq n-1)$,

$$\zeta^i - \zeta^j = \zeta^i(1-\zeta^{j-i}) \in \mathrm{U}(A).$$

It follows from Corollary 2.3 that B/A is simple.

Corollary 2.5. *Let A be a semi-local ring and B/A an abelian G-extension of K-type. Then, for any subgroup H of G, B^H/A is simple.*

Proof. Let $n = |G|$, $r = |H|$ and $s = |G/H|$. Moreover, let ζ be a primitive n-th root of 1. Then, ζ^s is a primitive r-th root of 1, and $\{1-(\zeta^s)^i : i = 1, \ldots, r-1\} \subset \mathrm{U}(A)$. Hence B^H/A is an abelian extension of K-type. Therefore B^H/A is simple by Proposition 2.4.

Example 2.1. Let

$$B = \mathrm{GF}(2^4) \oplus \mathrm{GF}(2^4) \oplus \mathrm{GF}(2^4),$$
$$A = \{(a, a, a) ; a \in \mathrm{GF}(2)\}$$

and τ an automorphism of $\mathrm{GF}(2^4)$ of order 4. Then we have automorphisms σ and ρ of B such that

$$\sigma((x_1, x_2, x_3)) = (x_3, x_1, x_2) \text{ and}$$
$$\rho((x_1, x_2, x_3)) = (\tau(x_1), \tau(x_2), \tau(x_3)).$$

Then B/A is an abelian $\langle\sigma\rangle \times \langle\rho\rangle$-Galois extension, which is not of K-type. Clearly $B^o = \mathrm{GF}(2) \oplus \mathrm{GF}(2) \oplus \mathrm{GF}(2)$. By [7], we have $\mathrm{N}_2(4) = 3$. Hence, by Theorem 1.6, B/A is simple. However, B^o/A is not simple by the theorem.

In the rest of this section, we study the simplicity of Galois extensions of a complete Noetherian local ring. We write $A = (A, M)$ (resp. $(A, M, *)$) if A is a local ring with a unique maximal ideal M (resp. which is Noetherian and complete). By $\bar{A}$, we denote the factor ring A/M, and given an element f in $A[X]$, by $\bar{f}$, we denote the image of f under the canonical homomorphism $A[X] \to \bar{A}[X]$. A polynomial f in $A[X]$ will be called to be *separable* if f is monic and $A[X]/(f)$ is a separable A-algebra where $(f) = A[X]f$. Moreover, given a ring extension B/A, an element b of B will be called to be a *separable element* of B over A if b is a root of some separable polynomial of $A[X]$.

First, for the reader's conveniences, we shall present a remark on local rings which is useful in the subsequent study.

Remark 2.1. Let $A = (A, M)$, and f_1, f_2 monic polynomials in $A[X]$. By $\delta(f_1)$, we denote the discriminant of f_1 in the sense of [9, p. 152]. Moreover, the ideals (f_1) and (f_2) of $A[X]$ will be called to be *comaximal* if $(f_1)+(f_2) = A[X]$. Then

(1) $(f_1)+(f_2) = A[X]$ *if and only if* $(\bar{f}_1)+(\bar{f}_2) = \bar{A}[X]$.

In fact, the part "only if" is obvious. To see the converse, we assume that $(f_1)+(f_2) = \bar{A}[X]$, and set

$$B_i = A[X]/(f_i),\ b_i = X+(f_i)\ (i = 1, 2),$$
$$B = B_1 \oplus B_2, \text{ and } b = b_1+b_2.$$

Then

$$B/MB = B_1/MB_1 \oplus B_2/MB_2.$$

Moreover, one will easily see that $B/MB = \bar{A}[\bar{b}]$. Hence $B = A[b] + MB$, and so $B = A[b]$. From this, we see that the canonical homomorphism

$$\phi : A[X]/(f_1 f_2) \to B$$

is surjective. Clearly, $A[X]/(f_1 f_2)$ and B are projective over A and $\mathrm{rank}_A(A[X]/(f_1 f_2)) = \mathrm{rank}_A B$. Hence ϕ is an isomorphism. This implies that the ideals (f_1) and (f_2) of $A[X]$ are comaximal.

(2) By [9, Theorem 2.1], we have that

$$f_1 \text{ is separable over } A \Leftrightarrow \delta(f_1) \in \mathrm{U}(A) \Leftrightarrow \delta(\bar{f}_1) \in \mathrm{U}(\bar{A}) \Leftrightarrow \bar{f}_1 \text{ is separable over } \bar{A}.$$

(3) By (1) and [9, Theorem 2.2], we have that

$$\begin{aligned} f_1 f_2 \text{ is separable over } A &\Leftrightarrow \delta(f_1 f_2) \in \mathrm{U}(A) \Leftrightarrow \delta(\bar{f}_1 \bar{f}_2) \in \mathrm{U}(\bar{A}) \\ &\Leftrightarrow (\bar{f}_1) + (\bar{f}_2) = \bar{A}[X] \text{ and } \delta(\bar{f}_i) \in \mathrm{U}(\bar{A}) \ (i = 1, 2) \\ &\Leftrightarrow (f_1) + (f_2) = A[X] \text{ and } \delta(f_i) \in \mathrm{U}(A) \ (i = 1, 2) \\ &\Leftrightarrow (f_1) + (f_2) = A[X] \text{ and the } f_i \text{ are separable over } A. \end{aligned}$$

Next, we shall prove the following theorem which is a generalization of Proposition 1.4 (and Lemma 1.2 given for fields) to complete Noetherian local rings. For the proof, we shall frequently use the results of G. J. Janusz [3] which play essential roles.

Theorem 2.6. *Let $A = (A, M, *)$, and B/A a G-Galois extension of rank n. Let F be the set of maximal local subrings of B containing A which are separable over A, and $\{e_1, \ldots, e_r\}$ the set of primitive idempotents of B. Then*

(1) $|\mathrm{F}| = (n/r)^{r-1}$, *and for any* $L \in \mathrm{F}$,

$$B = Le_1 \oplus \cdots \oplus Le_r \text{ with } L \cong Le_i = Be_i \ (1 \leqq i \leqq r),$$

ML is a unique maximal ideal of L, and L/A is a Galois extension.

(2) *Let L be an arbitrary element of* F.

(i) *Assume that B/A has a primitive element b. Then $|\mathrm{I}_{\bar{A}}(L/ML)| \geqq r$. Moreover, there exists a pair of a subset $\{b_1, \ldots, b_r\}$ in L and a subset $\{f_1, \ldots, f_r\}$ in $A[X]$ such that*

(a) $\bar{f}_i \in \mathrm{I}_{\bar{A}}(L/ML) \ (1 \leqq i \leqq r)$,

(b) $\bar{f}_i \neq \bar{f}_j$ *for each pair* $i \neq j \ (1 \leqq i, j \leqq r)$,

(c) $\bar{f}_i(\bar{b}_i) = \bar{0} \ (1 \leqq i \leqq r)$, *and*

$$b = b_1e_1 + \cdots + b_re_r.$$

(ii) *Assume that* $|I_{\bar{A}}(L/ML)| \geqq r$. *Let* $|g_1, \ldots, g_r|$ *be a subset of* $A[X]$ *such that*

(a) $\bar{g}_i \in I_{\bar{A}}(L/ML)$ $(1 \leqq i \leqq r)$,

(b) $\bar{g}_i \neq \bar{g}_j$ *for each pair* $i \neq j$ $(1 \leqq i, j \leqq r)$.

Let $|c_1, \ldots, c_r|$ *be a subset of* L *such that* $\bar{g}_i(\bar{c}_i) = \bar{0}$ $(i = 1, \ldots, r)$. *Then*

$$c = c_1e_1 + \cdots + c_re_r$$

is a primitive element of B/A.

When this is the case, for each i $(1 \leqq i \leqq r)$, *there exists an element* h_i *in* $A[X]$ *such that* h_i *is monic,* $\bar{h}_i = \bar{g}_i$, *and* $h_i(c_i) = 0$. *Moreover, for such the* h_i*'s, there holds that* $\prod_{i=1}^{r} h_i = \prod_{\sigma \in G}(X - \sigma(c)) =: f$, $A[X]/(f) \cong B$ *(as* A*-algebras), and* f *is separable over* A.

Proof. (1) By Lemma 1.1, we have that

$$B = Be_1 \oplus \cdots \oplus Be_r,$$

$A \cong Ae_1$ $(a \to ae_1)$ and Be_1/Ae_1 is a Galois extension. Since $A = (A, M, *)$ (a complete Noetherian local ring) and Be_1 has no proper idempotents, Be_1 is a local ring with a unique maximal ideal MBe_1. Moreover, since G is transitive on the set $|e_1, \ldots, e_r|$, Be_1 is A-algebra isomorphic to each Be_i $(1 \leqq i \leqq r)$. Now, let S be a local subring of B containing A which is separable over A. Since each Se_i is separable over Ae_i, it is projective over Ae_i by [3, Proposition 1.5] $(1 \leqq i \leqq r)$. Hence, by [3, Lemma 1.6], we have A-algebra isomorphisms $S \to Se_i$ $(s \to se_i)$, $i = 1, \ldots, r$. Since the Be_i/Ae_i are Galois and the Be_i are local, it follows from [1, Theorem 2.3] and [3, Lemma 1.3 and Corollary 1.8] that each isomorphism $Se_1 \to Se_i$ $(se_1 \to se_i)$ can be extended to an isomorphism

$$\tau_i : Be_1 \to Be_i.$$

Hence S is a subring of the ring

$$T(\tau_2, \ldots, \tau_r) = |b + \textstyle\sum_{i=2}^{r} \tau_i(b) \ ; \ b \in Be_1|.$$

If $S \in \mathrm{F}$ then we have $S = T(\tau_2, \ldots, \tau_r)$. Moreover, as is easily seen, the cardinality of the set of A-algebra isomorphisms of Be_1 to Be_i coincides with n/r $(1 \leqq i \leqq r)$. Therefore, it follows that $|\mathrm{F}| = (n/r)^{r-1}$. The other assertions in (1) will be easily seen.

(2) Let $L \in \mathrm{F}$ and $m = n/r$ $(= \mathrm{rank}_A L)$. Then by (1), we have that

$$B = Le_1 \oplus \cdots \oplus Le_r,\ Le_i \cong L\ (1 \leqq i \leqq r),\ \text{and}$$
$$B/MB = (L/ML)\bar{e}_1 \oplus \cdots \oplus (L/ML)\bar{e}_r$$
$$\cong L/ML \oplus \cdots \oplus L/ML\ (r \text{ times})$$

which is a Galois extension of a field $\bar{A}$ $(= A/M)$, where $\bar{e}_i = e_i + MB$ $(1 \leqq i \leqq r)$. Moreover, by Lemma 1.2, L/ML is a maximal subfield of B/MB containing $\bar{A}$.

(i) We assume that B/A has a primitive element b. Then, we have

$$b = b_1 e_1 + \cdots + b_r e_r$$

for some elements b_i of L. It is obvious that $\bar{A}[\bar{b}] = B/MB$. Hence, by Proposition 1.4(1), there exists a pair of a subset $\{d_1, \ldots, d_r\}$ in L and a subset $\{f_1, \ldots, f_r\}$ in $A[X]$ such that the f_i satisfy the conditions (a) and (b) of (i), $f_i(\bar{d}_i) = \bar{0}$ $(1 \leqq i \leqq r)$, and

$$\bar{b} = \bar{d}_1 \bar{e}_1 + \cdots + \bar{d}_r \bar{e}_r.$$

Since $\bar{b} = \bar{b}_1 \bar{e}_1 + \cdots + \bar{b}_r \bar{e}_r$ and $\bar{b}_i, \bar{d}_i \in L/ML$ $(1 \leqq i \leqq r)$, it follows that $\bar{b}_i = \bar{d}_i$ $(1 \leqq i \leqq r)$, and this implies the assertion (i).

(ii) We assume that $|\mathrm{I}_{\bar{A}}(L/ML)| \geqq r$. Let $\{g_1, \ldots, g_r\}$ $(\subset A[X])$ and $\{c_1, \ldots, c_r\}$ $(\subset L)$ be as in the (ii) of our theorem. Since L/ML is a maximal subfield of B/MB containing $\bar{A}$, for $c = c_1 e_1 + \cdots + c_r e_r$, it follows from Proposition 1.4(2) that $\bar{A}[\bar{c}] = B/MB$. This implies that

$$A[c] + MB = B \text{ and so } A[c] = B.$$

Thus, c is a primitive element of B/A. Now, since $\bar{g}_i \in \mathrm{I}_{\bar{A}}(L/ML)$ and $\bar{g}_i(\bar{c}_i) = \bar{0}$ $(1 \leqq i \leqq r)$, it follows that $\bar{A}[\bar{c}_i] = L/ML$ $(1 \leqq i \leqq r)$, that is,

$$A[c_i] + ML = L \text{ and so } A[c_i] = L\ (1 \leqq i \leqq r).$$

Combining this with Lemma 1.3, we obtain

$$L = A \oplus Ac_i \oplus \cdots \oplus Ac_i^{m-1}\ (1 \leqq i \leqq r).$$

Hence, for each i, there exists a monic polynomial h_i of degree m with $h_i(c_i) = 0$. Noting $[\bar{A}[\bar{c}_i] : \bar{A}] = [L/ML : \bar{A}] = m$, elements $1, \bar{c}_i, (\bar{c}_i)^2, \ldots, (\bar{c}_i)^{m-1}$ are linearly independent over $\bar{A}$. Since $\bar{h}_i(\bar{c}_i) = \bar{g}_i(\bar{c}_i) = \bar{0}$ and $\deg \bar{h}_i = m = \deg \bar{g}_i$, it follows that $\bar{h}_i = \bar{g}_i$ $(1 \leqq i \leqq r)$. Next, we set $h = \prod_{i=1}^{r} h_i$ and $f = \prod_{\sigma \in G}(X - \sigma(c))$. Then $h(c) = \sum_{i=1}^{r} h(c) e_i = \sum_{i=1}^{r} h(c_i) e_i = 0$ and $f(c) = 0$. By Lemma 1.3, elements $1, c, c^2, \ldots, c^{n-1}$ $(n =$

$\mathrm{rank}_A B$) are linearly independent over A. Hence, noting $\deg h = n = \deg f$, we obtain $h = f$. Moreover, we have $A[X]/(f) \cong A[c] = B$ (as A-algebras) by Lemma 1.3 and [9, Lemma 2.2]. Since B is separable over A, so is f by the definition of separable polynomials.

As a direct consequence of Theorem 2.6, we obtain the following corollary which contains the result of Corollary 1.5(1) and a partial result of [3, Lemma 3.1].

Corollary 2.7. *Let $A = (A, M, *)$, and B/A a Galois extension. Let L be an arbitrary maximal local subring of B containing A which is separable over A. Then, the following conditions are equivalent.*

(a) *B/A is simple.*

(b) *$(B/MB)/\bar{A}$ is simple.*

(c) $|\mathrm{I}_{\bar{A}}(L/ML)| \geqq (\mathrm{rank}_A B)/(\mathrm{rank}_A L)$.

Let $A = (A, M)$. A polynomial f in $A[X]$ will be called to be *decomposable* (resp. *indecomposable*) if $f = f_1 f_2$ in $A[X]$ of degrees $\geqq 1$ (resp. if f is not decomposable). Moreover, by κ_A, we denote the canonical isomorphism $A[X] \to \bar{A}[X]$. Now, let S be a local ring which is a Galois extension of A of rank m. Then, for the unique maximal ideal M' of S, we have that $\mathrm{rank}_{\bar{A}}(S/M') = m = \mathrm{rank}_{\bar{A}}(S/MS)$ which implies $M' = MS$. By $\mathrm{I}_A(S)$, we denote the set of monic indecomposable polynomials f in $A[X]$ of degree m with $f(c) = 0$ for some separable element c of S over A. In addition, let $A = (A, M, *)$. By $\mathrm{T}(S)$, we denote the class of all Galois extensions of A each of which has a maximal local subring L containing A which is separable over A such that $L \cong S$ (as A-algebras).

Under this situation, we have the following theorem which contains some part of corollary 1.5(2).

Theorem 2.8. *Let $A = (A, M, *)$, and S a local ring which is a Galois extension of A. Then*

(1) *$\kappa_A(\mathrm{I}_A(S)) = \mathrm{I}_{\bar{A}}(S/MS)$, and for any f in $\mathrm{I}_A(S)$, $A[X]/(f) \cong S$ (as A-algebras).*

(2) *Let B/A be a Galois extension. Then, the following conditions are equivalent.*

(a) *$B/A \in \mathrm{T}(S)$, and B/A is simple.*

(b) *$B \cong A[X]/(f_1 f_2 \cdots f_r)$ (as A-algebras) for some finite number of f_i's in $\mathrm{I}_A(S)$ such that $\kappa_A(f_i)$ are distinct to each other.*

Proof. (1) Let $f \in \mathrm{I}_A(S)$. Then $f(c) = 0$ for some separable element c in S over A. Since S has no proper idempotents and $A[c]$ is separable over A, S is Galois over $A[c]$ by [1, Theorem 2.2]. Hence, by [9, Theorem 3.4], there exists a monic polynomial g in $A[X]$ such that $\deg g = \mathrm{rank}_A A[c]$ and $g(c) = 0$. This implies that g is a divisor of f. Therefore, it follows that $\mathrm{rank}_A A[c] = \deg g = \deg f = \mathrm{rank}_A S$, and so $A[c] = S$. Moreover, we have $\deg \bar{f} = \deg f = \mathrm{rank}_A S = \mathrm{rank}_{\bar{A}}(S/MS) = \mathrm{rank}_{\bar{A}} \bar{A}[\bar{c}]$ and $\bar{f}(\bar{c}) = \bar{0}$. Hence $\bar{f}(= \varkappa_A(f)) \in \mathrm{I}_{\bar{A}}(S/MS)$ and $A[X]/(f) \cong S$ (as A-algebras) by Theorem 2.6. Next, let $\bar{f} \in \mathrm{I}_{\bar{A}}(S/MS)$. Then $\bar{f}(\bar{c}) = \bar{0}$ for some $c \in S$. Hence, by Theorem 2.6, there exists a separable polynomial h in $A[X]$ such that $\bar{h} = \bar{f}$ and $h(c) = 0$. Then $\deg h = \deg \bar{h} = \deg \bar{f} = \mathrm{rank}_{\bar{A}}(S/MS) = \mathrm{rank}_A S$. Since $\bar{h}$ is indecomposable in $\bar{A}[X]$, so is h in $A[X]$. Hence $h \in \mathrm{I}_A(S)$ and $\varkappa_A(h) = \bar{f}$. Thus, we obtain that $\varkappa_A(\mathrm{I}_A(S)) = \mathrm{I}_{\bar{A}}(S/MS)$.

(2) (a) $\Rightarrow$ (b): We assume (a). Let L be a maximal local subring of B containing A which is separable over A. Then, by Theorem 2.6, there exists a subset $\{h_1, \ldots, h_r\}$ in $A[X]$ such that each h_i is monic, $\bar{h}_i \in \mathrm{I}_{\bar{A}}(L/ML)$, $h_i(c_i) = 0$ for some c_i in L, and $B \cong A[X]/(h_1 h_2 \cdots h_r)$ (as A-algebras). Then $\deg h_i = \deg \bar{h}_i = \mathrm{rank}_{\bar{A}}(L/ML) = \mathrm{rank}_A L$. Since each $\bar{h}_i$ is indecomposable in $\bar{A}[X]$, so is h_i in $A[X]$. Hence, it follows that $h_i \in \mathrm{I}_A(L)$ $(1 \leqq i \leqq r)$. Since $L \cong S$ (as A-algebras), we obtain the assertion (b).

(b) $\Rightarrow$ (a): We assume (b). Then, it is obvious that B/A is simple. By Remark 2.1, the ideals (f_i) of $A[X]$ are pairwise comaximal. Hence we obtain $B \cong A[X]/(f_1 f_2 \cdots f_r) \cong A[X]/(f_1) \oplus \cdots \oplus A[X]/(f_r) \cong S \oplus \cdots \oplus S$ (r times) (by (1)). Therefore, it follows from Theorem 2.6(1) that $B/A \in \mathrm{T}(S)$, completing the proof.

As an addition, we shall prove the following corollary whose proof owes essentially to the result of G. J. Janusz [3, Theorem 4.6].

Corollary 2.9 (cf. [3, Theorem 4.6]). *Let $A = (A, M, *)$. Let $\mathscr{L}$ the set of A-algebra isomorphism classes of all Galois extensions of A, and $\mathscr{F}$ the set of $\bar{A}$-algebra isomorphism classes of all Galois extensions of $\bar{A}$. Then, there exists a one-to-one correspondence $\Phi : \mathscr{L} \to \mathscr{F}$; $\Psi : \mathscr{F} \to \mathscr{L}$ such that $\Phi\Psi = 1$, $\Psi\Phi = 1$, and*

(a) *for $B \in [B] \in \mathscr{L}$, $\Phi([B]) =$ the class of $L/ML \oplus \cdots \oplus L/ML$ (r times) where L is any maximal local subring of B containing A which*

is separable over A, and $r = (\mathrm{rank}_A B)/(\mathrm{rank}_A L)$;

(b) *for $C \in [C] \in \mathscr{F}$, $\Psi([C])$ = the class of $L \oplus \cdots \oplus L$ (r times) where for any maximal subfield E of C containing $\bar{A}$, $r = (\mathrm{rank}_{\bar{A}} C)/(\mathrm{rank}_{\bar{A}} E)$, and L is a local ring containing A which is Galois over A such that L/ML is $\bar{A}$-algebra isomorphic to E.*

When this is the case, $\Psi([C])$ contains simple extensions of A if and only if $[C]$ contains simple extensions of $\bar{A}$.

Proof. Let S be a projective, separable A-algebra without proper idempotents such that $(S/MS)/(A/M)$ is a Galois extension. Then, S is a local ring with a unique maximal ideal MS. By [3, Theorem 1.1], S/A can be imbedded in a G-Galois extension T/A without proper idempotents. Then, T is also a local ring with a unique maximal ideal MT. Moreover, $G \cong G|(T/MT)$, and $(T/MT)/(A/M)$ is a $G|(T/MT)$-Galois extension. We set $H = G_S$ $(= \{\sigma \in G ;\ \sigma(s) = s \text{ for all } s \in S\})$. Then $|H| = \mathrm{rank}_S T = \mathrm{rank}_{(S/MS)}(T/MT)$. Hence $(T/MT)/(S/MS)$ is a $H|(T/MT)$-Galois extension. Since $(S/MS)/(A/M)$ is a Galois extension, $H|(T/MT)$ is a normal subgroup of $G|(T/MT)$. Hence H is also a normal subgroup of G. Thus, S/A is a Galois extension. Moreover, by Remark 1.1(1), we see that any finite direct sum S^r of copies of S is a Galois extension of A. Further, S is A-algebra isomorphic to any maximal local subring of S^r containing A which is separable over A. Combining these facts with [3, Theorem 4.6] and Theorem 2.6, we obtain the corollary.

Remark 2.2. Let $A = (A, M)$, and B/A a Galois extension of rank n. Let $\mathrm{F}(B/A)$ be the set of maximal subrings of B containing A without proper idempotents which are separable over A, and $\{e_1, \ldots, e_r\}$ the set of primitive idempotents of B. Then, by making use of the same methods as in the proof of Theorem 2.6(1), we obtain that $|\mathrm{F}(B/A)| = (n/r)^{r-1}$, and for any $L \in \mathrm{F}(B/A)$,

$B = Le_1 \oplus \cdots \oplus Le_r$ with $L \cong Le_i = Be_i (1 \leqq i \leqq r)$, and L/A is Galois.

Moreover, the results of Theorem 2.6(2) and Corollary 2.7 also hold for $A = (A, M)$ provided $\mathrm{F}(B/A)$ contains a local ring.

Now, let S be a local ring which is a Galois extension of A, and let $\mathrm{T}(S)$ denote the class of all Galois extensions B of A such that for an L in $\mathrm{F}(B/A)$, $L \cong S$ (as A-algebras). Then, by making use of the same methods as in the proof of Theorem 2.8, we obtain the following

Theorem 2.8'. *Let $A = (A, M)$, and S a local ring which is a Galois extension of A. Then*

(1) $\kappa_A(\mathrm{I}_A(S)) = \mathrm{I}_{\bar{S}}(S/MS)$, *and for any f in $\mathrm{I}_A(S)$, $A[X]/(f) \cong S$ (as A-algebras).*

(2) *Let B/A be a Galois extension. Then, the following conditions are equivalent.*

(a) *$B/A \in \mathrm{T}(S)$, and B/A is simple.*

(b) *$B \cong A[X]/(f_1 f_2 \cdots f_r)$ (as A-algebras) for some finite number of f_i's in $\mathrm{I}_A(S)$ such that $\kappa_A(f_i)$ are distinct to each other.*

Remark 2.3. Let $A = (A, M)$ which is Noetherian. Let A^* denote the completion of A. Then A^* is a local ring with a unique maximal ideal MA^* and $A^*/MA^* \cong A/M$. Hence the result of Corollary 2.9 also holds for the set $\mathscr{L}$ of A^*-algebra isomorphism classes of all Galois extensions of A^* and the set $\mathscr{F}$ of $\bar{A}$-algebra isomorphism classes of all Galois extensions of $\bar{A}$ where $\bar{A} = A/M$.

Remark 2.4. Obviously, any Artinian local ring is Noetherian and complete. Hence, Theorem 2.6 and etc. also hold for the replacing of a complete Noetherian local ring A to a (commutative) Artinian local ring.

3. Primitive elements of tensor products of Galois extensions of a semi-local ring. First, we shall prove the following lemma which plays an essential role in this section.

Lemma 3.1. *Let A be a field. Let S_i/A be G_i-Galois, $n_i = |G_i|$ ($i = 1, 2$), $n = n_1 n_2$ and $B = S_1 \otimes_A S_2$. Assume that $|A| \geq n^2/2$ and $S_i = A[x_i]$ for some $x_i \in S_i$ ($i = 1, 2$). Then, there is an element α in A such that $B = A[x_1 + \alpha x_2]$ where $x_1 = x_1 \otimes 1$ and $x_2 = 1 \otimes x_2$.*

Proof. If either $n_1 = 1$ or $n_2 = 1$ then our assertion is trivial. Hence we assume that $n_1 > 1$ and $n_2 > 1$. Let E be the set of (non-zero) primitive idempotents of B. Since B/A is $(G_1 \times G_2)$-Galois, it follows from Lemma 1.1 that given an element z in B, $z \in \mathrm{U}(B)$ if and only if $ze \neq 0$ for all $e \in E$. Now, by Lemma 1.3, we have that $x_1 - \tau(x_1)$, $x_2 - \nu(x_2) \in \mathrm{U}(B)$ for all $\tau \in G_1 \setminus \{1\}$ and $\nu \in G_2 \setminus \{1\}$. For an element e of E, we

set

$$T_e = \{-(\sigma(x_1)-\tau(x_1))(\mu(x_2)-\nu(x_2))^{-1}e\ ;\ \sigma, \tau \in G_1,\ \mu, \nu \in G_2,\ \sigma \neq \tau,\ \mu \neq \nu\},$$
$$A_e = \{a \in A\ ;\ ae \in T_e\} \text{ and } A_E = \bigcup_{f \in E} A_f.$$

Then, one will easily see that $|T_e| \leqq n_1(n_1-1)n_2(n_2-1)/2 < n^2/2 \leqq |A|$. Moreover, for any $\rho \in G_1 \times G_2$, we have $\rho(T_e) = T_{\rho(e)}$, $a\rho(e) = \rho(ae) \in \rho(T_e)$ for every $a \in A_e$, and so $A_e = A_{\rho(e)}$. Since $G_1 \times G_2$ is transitive on E, we have $A_e = A_f$ for all $f \in E$. Hence, it follows that $A_E = A_e$ and $|A_E| = |A_e| \leqq |T_e| < |A|$. Now, let α be an element of $A \backslash A_E$, and $\rho := (\tau, \nu)$ an arbitrary element of $G_1 \times G_2 \backslash \{(1, 1)\}$. Then, setting $z = x_1 + \alpha x_2$, we see that

$$(z-\rho(z))e = ((x_1-\tau(x_1))+\alpha(x_2-\nu(x_2)))e \neq 0 \text{ for all } e \in E.$$

Hence, we obtain $z-\rho(z) \in \mathrm{U}(B)$ for all $\rho \in G_1 \times G_2 \backslash \{(1, 1)\}$. Therefore, by Lemma 1.3, z is a primitive element of B/A.

Lemma 3.2. *Let A be a field and let S_i/A be G_i-Galois, $n_i = |G_i|$ $(i = 1, \ldots, k)$, $n = \prod_{i=1}^{k} n_i$ and $B = S_1 \otimes_A \cdots \otimes_A S_k$. Assume that $|A| \geqq n^2/2$ and $S_i = A[x_i]$ for some $x_i \in S_i$ $(i = 1, \ldots, k)$. Then, there are elements $\alpha_1, \ldots, \alpha_k$ in A such that $B = A[\sum_{i=1}^{k} \alpha_i x_i]$.*

Proof. In case $k = 2$, the assertion is a direct consequence of Lemma 3.1. Hence, for $k > m \geqq 2$, we assume that the assertion holds for $C_m = S_1 \otimes_A \cdots \otimes_A S_m$. Then, there are elements $\alpha_1, \ldots, \alpha_m$ in A such that $C_m = A[\sum_{i=1}^{m} \alpha_i x_i]$. Then, applying Lemma 3.1 again, we obtain $C_{m+1} = C_m \otimes_A S_{m+1} = A[\sum_{i=1}^{m} \alpha_i x_i + \alpha x_{m+1}]$ for some $\alpha \in A$, completing the proof.

Theorem 3.3. *Let A be a semi-local ring. Moreover, let S_i/A be G_i-Galois, $n_i = |G_i|$ $(i = 1, \ldots, k)$, $n = \prod_{i=1}^{k} n_i$, $B_m = S_1 \otimes_A \cdots \otimes_A S_m$ $(m = 1, \ldots, k)$, and $B = B_k$.*

(1) *If $x_1\alpha_1 + x_2\alpha_2 + \cdots + x_k\alpha_k$ with $x_i \in S_i$ and $\alpha_i \in A$ $(1 \leqq i \leqq k)$ is a primitive element of B/A then*

(i) *$\alpha_i \in \mathrm{U}(A)$ for i with $n_i > 1$, and*

(ii) *for any m $(1 \leqq m \leqq k)$, $\sum_{i=1}^{m} x_i\alpha_i$ is a primitive element of B_m/A.*

(2) *Assume that $S_i = A[x_i]$ for some $x_i \in S_i$ $(1 \leqq i \leqq k)$. Then, B/A has a primitive element $x_1\alpha_1 + x_2\alpha_2 + \cdots + x_k\alpha_k$ with $\alpha_i \in A$ $(1 \leqq i \leqq k)$ if one of the following conditions is satisfied:*

(a) $|A/M| \geqq n^2/2$ *for all maximal ideals* M *of* A.

(b) *There exist elements* $a_1, a_2, \ldots, a_{n^2} \in A$ *such that* $a_i - a_j \in \mathrm{U}(A)$ *for each pair* $i \neq j$ $(1 \leqq i, j \leqq n^2)$.

Proof. (1) Let $z = x_1\alpha_1 + x_2\alpha_2 + \cdots + x_k\alpha_k$ $(x_i \in S_i, \ \alpha_i \in A)$ be a primitive element of B/A. Further, for each $\sigma_i \in G_i$, σ_i denotes also an automorphism $f_1 \otimes \cdots \otimes f_k$ of B such that $f_i = \sigma_i$ and $f_j = 1$ if $j \neq i$.

(i) If $n_i > 1$ then, for $\sigma_i \neq 1 \in G_i$, $\alpha_i(x_i - \sigma_i(x_i)) = z - \sigma_i(z) \in \mathrm{U}(B)$ by Lemma 1.3. Hence $\alpha_i \in \mathrm{U}(B)$ and so $\alpha_i \in \mathrm{U}(A)$.

(ii) We set $z_m = x_1\alpha_1 + \cdots + x_m\alpha_m$ and $H_m = G_1 \times \cdots \times G_m$. Then we have $z_m \in B_m$ and, for $\sigma \neq 1 \in H_m$, $z_m - \sigma(z_m) = z - \sigma(z) \in \mathrm{U}(B)$. Hence $z_m - \sigma(z_m) \in \mathrm{U}(B_m)$. Since B_m/A is H_m-Galois, it follows from Lemma 1.3 that $B_m = A[z_m]$.

(2) Case (a): Let $|M_1, \ldots, M_t|$ be the set of all maximal ideals of A. Then

$$B/M_iB = (S_1/M_iS_1) \otimes_{A/M_i} \cdots \otimes_{A/M_i} (S_k/M_iS_k).$$

Since $S_j/M_iS_j = (A/M_i)[x_j + M_iS_j]$ for $j = 1, \ldots, k$, it follows from Lemma 3.2 that $B/M_iB = (A/M_i)[\sum_{j=1}^{k} \alpha_{ij}x_j + M_iB]$ for some $\alpha_{i1}, \ldots, \alpha_{ik} \in A$ $(i = 1, \ldots, t)$. Hence, by Proposition 2.1, we obtain that $B = A[\sum_{i=1}^{t} \beta_i \sum_{j=1}^{k} \alpha_{ij}x_j]$ for some $\beta_1, \ldots, \beta_t \in A$. We set here $\gamma_j = \sum_{i=1}^{t} \beta_i\alpha_{ij}$. Then

$$B = A[\textstyle\sum_{j=1}^{k} \gamma_j x_j], \text{ and}$$

$$\gamma_j \in A \text{ for } j = 1, \ldots, k.$$

Case (b): This is proved by the same argument as in the proof of Corollary 2.3, and by the case (a).

Lastly, we shall prove the following theorem.

Theorem 3.4. *Let* B/A *be an abelian* G*-Galois extension of* K*-type of rank* n *such that* A *is a semi-local ring. Moreover, let* ζ *be a primitive* n*-th root of* 1 *with* $1 - \zeta^i \in \mathrm{U}(A)$ $(1 \leqq i \leqq n-1)$ *(and* $n \in \mathrm{U}(A)$*). Then,* $G = \langle\sigma_1\rangle \times \langle\sigma_2\rangle \times \cdots \times \langle\sigma_k\rangle$ *for some elements* $\sigma_1, \sigma_2, \ldots, \sigma_k$ *in* G *such that* $|\langle\sigma_i\rangle| = n_i$ (> 1) *and* $n_{i+1} | n_i$ $(1 \leqq i \leqq k-1)$. *For this decomposition of* G, *the following* (1)–(3) *hold.*

(1) *There exist elements* $x_1, x_2, \ldots, x_k$ *in* B *such that*

$$B = A[x_1, x_2, \ldots, x_k] = \sum \oplus (x_1^{i_1}x_2^{i_2}\cdots x_k^{i_k})A \ (0 \leqq i_j < n_j),$$

$$x_i^{n_i} = a_i \in \mathrm{U}(A) \text{ and } \sigma_j(x_i) = \begin{cases} x_i\zeta_i & \text{if } i = j \\ x_i & \text{if } i \neq j \end{cases}$$

where $\zeta_i = \zeta^{n/n_i}$.

(2) *If* $z = x_1\alpha_1 + x_2\alpha_2 + \cdots + x_k\alpha_k$ $(\alpha_i \in A)$ *is a primitive element of* B/A *then*

(i) $\alpha_i \in \mathrm{U}(A)$ $(1 \leqq i \leqq k)$,

(ii) *for any subset* $\{j_1, j_2, \ldots, j_m\}$ *of* $\{1, 2, \ldots, k\}$, $\sum_{s=1}^{m} x_{j_s}\alpha_{j_s}$ *is a primitive element of* $A[x_{j_1}, x_{j_2}, \ldots, x_{j_m}]/A$, *and*

(iii) $z \in \mathrm{U}(B)$.

(3) B/A *has a primitive element* $z = x_1\alpha_1 + x_2\alpha_2 + \cdots + x_k\alpha_k$ *with some* $\alpha_i \in A$ *if one of the following conditions is satisfied*:

(a) $|A/M| \geqq n^2/2$ *for all maximal ideals* M *of* A.

(b) *There exist elements* $a_1, \ldots, a_{n^2} \in A$ *such that* $a_i - a_j \in \mathrm{U}(A)$ *for each pair* $i \neq j$ $(1 \leqq i, j \leqq n^2)$.

(c) $A/M \neq (Z[\zeta] + M)/M$ *for all maximal ideals* M *of* A *where* Z *is the subring of* A *generated by* 1.

Proof. By the fundamental theorem of finitely generated abelian groups, we have

$$G = \langle\sigma_1\rangle \times \langle\sigma_2\rangle \times \cdots \times \langle\sigma_k\rangle$$

where $|\langle\sigma_i\rangle| = n_i$ (> 1) and $n_{i+1} | n_i$ for $i = 1, 2, \ldots, k-1$. Clearly $\prod_{i=1}^{k} n_i = n$, and so, $n_i \in \mathrm{U}(A)$. We set here

$$T_i = B^{\langle\sigma_i\rangle'}, \quad i = 1, 2, \ldots, k$$

for $\langle\sigma_i\rangle' = \langle\sigma_1\rangle \times \cdots \times \langle\sigma_{i-1}\rangle \times \langle\sigma_{i+1}\rangle \times \cdots \times \langle\sigma_k\rangle$. Then

$$B = T_1 \otimes_A T_2 \otimes_A \cdots \otimes_A T_k$$

and T_i/A is a cyclic $\langle\sigma_i\rangle$-extension. Since A is semi-local, it is well-known that T_i/A has a $\langle\sigma_i\rangle$-normal basis, that is, there exists an element a in T_i such that

$$T_i = Aa \oplus A\sigma_i(a) \oplus \cdots \oplus A\sigma_i^{n_i-1}(a).$$

We set

$$x_i = a + \zeta_i^{-1}\sigma_i(a) + \cdots + \zeta_i^{-(n_i-1)}\sigma_i^{n_i-1}(a)$$

where $\zeta_i = \zeta^{n/n_i}$. Then, $\sigma_i(x_i) = x_i\zeta_i$ and $\mathrm{N}_{\langle\sigma_i\rangle}(x_i) = x_i^{n_i}\alpha$ for some $\alpha \in \mathrm{U}(A)$, where $\mathrm{N}_{\langle\sigma_i\rangle}(x_i)$ denotes the norm of x_i with respect to $\langle\sigma_i\rangle$. Let M

be a maximal ideal of A. Then $x_i \notin MT_i$ because $\zeta_i^{-1} \notin M$. Since T_i/MT_i is Galois over A/M, T_i/MT_i is semi-simple (Lemma 1.1). If $N_{\langle\sigma_i\rangle}(x_i) \in M$ then $x_i^{n_i} \in M$, and so, $x_i \in MT_i$, which is a contradiction. It follows that $N_{\langle\sigma_i\rangle}(x_i) \in U(A)$, and so, $x_i \in U(T_i)$. Hence T_i/A is a strongly cyclic $(\sigma_i ; n_i ; x_i)$-extension in the sense of [12, Definition 1.1]. Thus, by [12, Theorem 1.2], we have

$$T_i = A[x_i] \cong A[X_i]/(X_i^{n_i}-a_i) \quad (x_i \to X_i+(X_i^{n_i}-a_i))$$

where $a_i = x_i^{n_i}$. From this, the assertion (1) follows immediately.

The assertions (2) (i)(ii) and the cases (a) and (b) of (3) are direct consequences of Theorem 3.3. Hence we shall prove (2) (iii) and the case (c) of (3).

(2) (iii) : Let $z = \sum_{i=1}^{k} x_i a_i$ $(a_i \in A)$ be a primitive element of B/A. For each $1 \leqq i \leqq k$, we have $\sigma_i^{n_i/n_k}(x_i) = x_i\zeta^{n/n_k} = x_i\zeta_k$. We set here

$$\tau = \sigma_1^{n_1/n_k}\sigma_2^{n_2/n_k}\cdots\sigma_{k-1}^{n_{k-1}/n_k}\sigma_k.$$

Then we have $U(B) \ni z-\tau(z) = z-z\zeta_k = z(1-\zeta_k)$. Hence $z \in U(B)$.

(3) Case (c) : Let M be a maximal ideal of A. If $|(Z+M)/M| = \infty$ then $|A/M| = \infty$. If $|(Z+M)/M| < \infty$ then $(Z+M)/M$ is a field and so is $(Z[\zeta]+M)/M$. Hence $[A/M : (Z[\zeta]+M)/M] \geqq 2$, which implies $|A/M| \geqq n^2$. Thus this assertion follows immediately from the case (a).

Corollary 3.5. *Let A be a semi-local ring whose Jacobson radical is zero, and B/A a Galois extension. If one of the following conditions is satisfied then B/A is a cyclic $\langle\sigma\rangle$-extension for some automorphism σ of B :*

(a) *For each primitive idempotent e of A, Be has a maximal subfield containing Ae which is a cyclic extension of Ae.*

(b) $|A| < \infty$.

When this is the case, $B = A[x] = \sum_{i=0}^{n-1} \oplus Ax^i$ for $n = rank_A B$ and some $x \in B$ with $x^n \in U(A)$ provided B/A is of K-type.

Proof. Let $\{e_1, \ldots, e_m\}$ be the set of primitive idempotents of A. If $|Ae_i| < \infty$ then any maximal subfield of Be_i containing Ae_i is a finite field, which is a cyclic extension of Ae_i. Hence the case (b) is contained in the case (a). Now, we assume (a). Then, it follows from Remark 1.1 that each Be_i/Ae_i is a cyclic $\langle\sigma_i\rangle$-extension for some automorphism σ_i of Be_i of order n. We denote here an automorphism σ of $B = \sum_{i=1}^{n} \oplus Be_i$ by

$$\sigma(\textstyle\sum_{i=1}^{m} b_i e_i) = \sum_{i=1}^{m} \sigma_i(b_i e_i)$$

where $b_i \in B$ $(1 \leqq i \leqq m)$. Then, noting $A = \sum_{i=1}^{m} Ae_i$, one will easily see that B/A is a cyclic $\langle\sigma\rangle$-extension with $|\langle\sigma\rangle| = n$. Then other assertions are immediate from the result of Theorem 3.4.

REFERENCES

[1] 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.

[2] F. DEMEYER and E. INGRAHAM : Separable algebras over commutative rings, L. N. M. 181, Springer-Verlag, 1971.

[3] G. J. JANUSZ : Separable algebras over commutative rings, Trans. Amer. Math. Soc. **122** (1966), 461−479.

[4] I. KIKUMASA and T. NAGAHARA : Primitive elements of cyclic extensions of commutative rings, Math. J. Okayama Univ. **29** (1987), 91−102.

[5] K. KISHIMOTO : Notes on biquadratic cyclic extensions of a commutative ring, Math. J. Okayama Univ. **28** (1986), 15−20.

[6] K. KISHIMOTO : On abelian extensions of rings II, Math. J. Okayama Univ. **15** (1971), 57−70.

[7] R. LIDL and NIEDERREITER : Finite fields, Encyclopedia of Mathematics and Its Applications 20, Addison-Wesley, 1983.

[8] A. MICALI, A. PAQUES and A. SOLECKI : Sur le groupe des extensions cubiques, L. N. M. 1197, Springer-Verlag, 1986.

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

[10] T. NAGAHARA : On splitting rings of separable skew polynomials, Math. J. Okayama Univ. **26** (1984), 71−85.

[11] T. NAGAHARA and A. NAKAJIMA : On separable polynomials over a commutative ring IV, Math. J. Okayama Univ. **17** (1974), 49−58.

[12] T. NAGAHARA and A. NAKAJIMA : On strongly cyclic extensions of commutative rings, Math. J. Okayama Univ. **15** (1971), 91−100.

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

[14] R. S. PIERCE : Associative Algebras, G. T. M. 88, Springer-Verlag, 1982.

[15] J.-D. THÉROND : Le théorème de l'élément primitif pour un anneau semi-local, J. Alg. **105** (1987), 29−39.

[16] O. VILLAMAYOR and D. ZELINSKY : Galois theory for rings with finitely many idempotents, Nagoya Math. J. **27** (1966), 721−731.

[17] P. WOLF : Algebraische Theorie der Galoisschen Algebren, VEB Deutscher Verlag der Wissenschaften, 1956.

I. KIKUMASA AND T. NAGAHARA
DEPARTMENT OF MATHEMATICS
OKAYAMA UNIVERSITY
OKAYAMA 700, JAPAN
K. KISHIMOTO
DEPARTMENT OF MATHEMATICS
SHINSHU UNIVERSITY
MATSUMOTO 390, JAPAN

(*Received November 18, 1987*)