Math. J. Okayama Univ. 32 (1990), 13–24

ON PRIMITIVE ELEMENTS OF GALOIS EXTENSIONS OF FINITE COMMUTATIVE ALGEBRAS

Dedicated to Professor Manabu Harada on his 60th birthday

ISAO KIKUMASA and TAKASI NAGAHARA

Throughout this note, all rings will be assumed to be commutative and to have identities, and a subring of a ring will mean one containing the same identity. Moreover, all Galois extensions will mean those in the sense of [1]. A ring extension R/K is called *simple* if R is K-algebra isomorphic to a factor ring $K[X]/(g)$ for some polynomial g in $K[X]$, that is, R/K has a primitive element (cf. [3], [4] and etc.). A Galois extension R/K will be called *trivial* if R is K-algebra isomorphic to the direct sum of copies of K. Unless otherwise provided, K will mean a finite field $\mathrm{GF}(q)$ consisting q elements where q is an s-th power p^s of a prime p. Given a K-algebra R, $[R : K]$ will denote the dimension of K-module R, and $\ell(R)$ the length of composition series of R-module R. Further, by $\mathbb{N}$, we shall denote the set of positive integers.

In this note we first treat a Galois extension R/K whose rank is a power r^n of a prime r, and we shall prove that a non-trivial Galois extension R/K is simple if and only if $\ell(R)$ has some bound which depends to p, s, r and n. Next we show a necessary and sufficient condition for a Galois extension R/K of rank p^n to be simple, which is useful and needs not to distinguish trivial Galois extensions from non-trivial ones. Later we consider the relation between primitive elements of a Galois extension R/K of rank p^n and intermediate fields of R/K, and we shall characterize the simplicity of a Galois extension R of K by maximal subfields of R containing K (§ 1). As an application, we shall present an elementary proof for a counter example of Dedekind which concerns with algebraic number fields (§ 2).

1. On primitive elements of Galois extensions over K. Now, let r be a prime and $n \in \mathbb{N}$. The following results is contained in [6, Theorem 1.6]. However, this will here be stated for the subsequent uses and considerations.

Lemma 0. *Let R/K be a Galois extension of rank u, and set $v = u/\ell(R)$. Then, R/K is simple if and only if $\ell(R) \leq \mathrm{N}_q(v) := (1/v)\cdot \sum_{d|v}\mu(d)q^{v/d}$, where $\mu(d)$ is the Moebius function on the set of natural numbers. In case $u = r^n$ and $v \geq r$, R/K is simple if and only if $\ell(R) \leq (1/v)(q^v - q^{v/r})$.*

We begin our study with the following proposition.

Proposition 1. *Let R/K be a Galois extension and $[R : K] = r^n$. Then*

(1) *In case that R/K is trivial, R/K is simple if and only if $\ell(R) \leq q$.*

(2) *Let R/K be non-trivial. Then, the following conditions are equivalent.*

(i) *R/K is simple.*

(ii) *$\ell(R) \leq sr^n/(n\log_p r + \log_p(1 + x_0(r^n)/r^n))$*

where $x_0(r^n)$ is a unique solution of an equation

$$(*) \qquad X^r - X - r^n = 0 \ (X > 0).$$

Proof. If R/K is a trivial Galois extension then the equivalence condition (1) has been known (cf. Lemma 0). Hence it suffices to show the case (2). Let $f(X) = X^r - X$. Then, as is easily seen, $f(x) > 0$ if $x > 1$, $f(1) = 0$ and $f(x) < 0$ if $0 < x < 1$. Moreover, $f(X)$ is strictly increasing on the interval $[1, \infty)$. Hence the equation $(*)$ has a unique solution $x_0 = x_0(r^n)$ with $x_0 > 1$. Put $r^t = [R : K]/\ell(R)$. Then, the condition (ii) is equivalent to that $\log_p(r^n + x_0) \leq sr^t$, and so, to that $x_0 \leq q^{r^{t-1}}$. Since $f(X)$ is strictly increasing on $[1, \infty)$, this inequality holds if and only if $r^n = f(x_0) \leq f(q^{r^{t-1}}) = q^{r^t} - q^{r^{t-1}}$. Hence we obtain our assertion (2) by Lemma 0, completing the proof.

Let $f(X)$ and x_0 be as in the above. Then

$$f(r^n) - f(x_0) = r^n(r^{n(r-1)} - 2) \geq 0.$$

Hence $r^n \geq x_0$ and so $0 < x_0/r^n \leq 1$. Combining this with Proposition 1, we have the following corollary.

Corollary 2. *Let R/K be a Galois extension of rank r^n. Then*

(1) *If R/K is simple and non-trivial then*

$$\ell(R) < sr^n/(n\log_p r).$$

(2) *If* $\ell(R) \leq sr^n/(n\log_p r+\log_p 2)$ *then* R/K *is simple.*

The equation (*) is easily solved by radicals in case $r = 2$ and $r = 3$. Hence we have the following

Corollary 3. *Let* R/K *be a non-trivial Galois extension of rank* r^n.

(1) *In case* $r = 2$, R/K *is simple if and only if*

$$\ell(R) \leq 2^n s/\log_p(2^n+(1+(1+2^{n+2})^{1/2})/2).$$

(2) *If* $r = 3$ *then*, R/K *is simple if and only if*

$$\ell(R) \leq 3^n s/\log_p(3^n+x_0)$$

where

$$x_0 = (3^n/2+(9^n/4-1/27)^{1/2})^{1/3}+(3^n/2-(9^n/4-1/27)^{1/2})^{1/3}.$$

Proof. The positive roots of the equations

$$x^2-x-2^n = 0 \text{ and } x^3-x-3^n = 0$$

are $(1+(1+2^{n+2})^{1/2})/2$ and the x_0 in the statement (2) of the theorem, respectively. Hence we have (1) and (2) according to Proposition 1.

Now we give a lemma to prove the following proposition.

Lemma 4. *Let* $m \in \mathbb{N}$. *If* $x \geq m^2+1$ *and* $k \geq 2$ $(k \in \mathbb{N})$ *then* $k^x \geq x^m+k$.

Proof. We first examine a special case $k = 2$. Set $\phi(X) = 2^X-X^m-2$. The problem then becomes to show that $\phi(x) \geq 0$ if $x \geq m^2+1$. Our assertion is easily checked in each case $m = 1, 2, 3$ and 4. Hence we may assume that $m \geq 5$. Then, note that $2^m > m^2$ and $2^m \cdot \log 2 > m$ where $\log = \log_e$ is natural logarithm. Now, it suffices to show that $\phi^{(1)}(x)\,(= \phi'(x)) > 0$ if $x > m^2$. For, this implies that $\phi(X)$ is strictly monotone increasing on $x > m^2$, and so we have $\phi(x) > 0$ for $x > m^2$ because $\phi(m^2) = (2^m)^m-(m^2)^m-2 \geq 0$ $(m \geq 5)$. Since it is obvious that

$$\phi^{(m-1)}(x) = 2^x(\log 2)^{m+1} > 0 \text{ for } x > m^2,$$

we assume that $1 \leq i \leq m$ and $\phi^{(i-1)}(x) > 0$ for $x > m^2$. Then

$$\phi^{(i)}(x) = 2^x(\log 2)^i - m(m-1)\cdots(m-i+1)x^{m-i}$$

is strictly monotone increasing on $x > m^2$. Furthermore we have

$$\begin{aligned}\phi^{(i)}(m^2) &> 2^{m^2}\cdot(\log 2)^i - m^i(m^2)^{m-i} \\ &= (2^m)^{m-i}(2^m\cdot\log 2)^i - (m^2)^{m-i}m^i > 0.\end{aligned}$$

It follows therefore that $\phi^{(i)}(x) > 0$ for $x > m^2$. Hence, by an induction method, we obtain that $\phi^{(i)}(x) > 0$ if $x > m^2$ and $1 \leq i \leq m+1$. Next, let $k \geq 3$ and set $c = k-2$. Then

$$\begin{aligned}k^x = (2+c)^x &\geq 2^x + c^x \geq x^m + 2 + c^x \text{ (by the above case)} \\ &\geq x^m + 2 + c = x^m + k.\end{aligned}$$

This completes the proof.

Using the lemma we have the following proposition, which does not be set with the condition about $\ell(R)$, p and s.

Proposition 5. *Let R/K be a non-trivial Galois extension with $[R : K] = r^n$. If $r > n^2$ then R/K is simple.*

Proof. Let x_0 $(= x_0(r^n))$ and $f(X)$ be as in Proposition 1 and its proof. Assume that $r \geq n^2+1$. Then, by Lemma 4,

$$f(q) - f(x_0) = q^r - q - r^n \geq 0.$$

Since $f(X)$ is strictly increasing on $x \geq 1$, this implies that $q \geq x_0$. Hence $r^n + x_0 = x_0^r \leq q^r = p^{sr}$. Therefore we obtain

$$\begin{aligned}\ell(R) \leq r^{n-1} = \frac{sr^n}{sr} &\leq \frac{sr^n}{\log_p(r^n + x_0)} \\ &= sr^n/(n\log_p r + \log_p(1 + x_0/r^n)).\end{aligned}$$

It follows from Proposition 1 that R/K is simple.

Now we consider the case $r = p$ that is $[R : K] = p^n (n \in \mathbb{N})$.

Lemma 6. *Let R/K be a non-trivial Galois extension and $[R : K] = p^n$. Then the following conditions are equivalent.*

(i) *R/K is simple.*
(ii) $\ell(R) < sp^n/n$.
(iii) $\ell(R) \leq sp^n/(n+1)$.

Proof. (ii) $\Rightarrow$ (iii): $\ell(R) < sp^n/n \Rightarrow p^n/\ell(R) > n/s \Rightarrow (p^n/\ell(R))s \geq n+1 \Rightarrow \ell(R) \leq sp^n/(n+1)$. The implications (iii) $\Rightarrow$ (i) $\Rightarrow$ (ii) follow immediately from the result of Corollary 2.

Corollary 7. *Let R/K be a Galois extension of rank p^n. Assume that p, s and n satisfy one of the following conditions:*

(a) *s is not a divisor of n.*

(b) *s is a divisor of n and, n/s and p are relatively prime.*

(c) *n and p are relatively prime.*

Then, the following conditions are equivalent.

(i) *R/K is simple.*

(ii) $\ell(R) \leq sp^n/n$.

Proof. (ii) $\Rightarrow$ (i): If $n \leq s$ then R/K is simple by [13, Le théorème de l'élément primitif]. Let $n > s$. Then, the inequality (ii) implies that $\ell(R) = p^m$ for some integer m with $0 \leq m \leq n-1$. Then $n\ell(R) \neq sp^n$ since, otherwise, $n = sp^k$ for some $k \in \mathbb{N}$, and this contradicts to our assumptions. Hence $\ell(R) < sp^n/n$. Since $\ell(R) \neq p^n$, it follows that R/K is simple by Lemma 6 (ii $\Rightarrow$ i). The (i) $\Rightarrow$ (ii) is easily seen from Proposition 1(1) and Lemma 6.

The following theorem is one of our main results, which does not be set with the additional conditions (a)-(c) in Corollary 7 or "non-trivial".

Theorem 8. *Let R/K be a Galois extension with $[R : K] = p^n$. The the following conditions are equivalent.*

(i) *R/K is simple.*

(ii) $\ell(R) \leq p^n(sp^n-1)/(np^n-1)$.

Proof. (i) $\Rightarrow$ (ii): If $\ell(R) = p^n$ then $n \leq s$ by Proposition 1(1) and so, $np^n-1 \leq sp^n-1$. Hence we obtain (ii). Assume that $\ell(R) \neq p^n$. Then, by Lemma 6 (i $\Rightarrow$ iii), we have

$$\ell(R) \leq sp^n/(n+1) \leq p^n(sp^n-1)/(np^n-1).$$

(ii) $\Rightarrow$ (i): If $s/n \geq 1$ then R/K is simple by [6, Corollary 2.2] (or [13, Le théorème de l'élément primitif]). If $s/n < 1$ then

$$\ell(R) \leq p^n(sp^n-1)/(np^n-1) < sp^n/n$$

and so, $\ell(R) \neq p^n$. Hence we get (i) from Lemma 6.

We here consider the relation between intermediate fields of R/K and primitive elements of R/K.

Theorem 9. *Let R/K be a Galois extension with $[R : K] = p^n$. Moreover, let L be a maximal subfield of R containing K. Then the following conditions are equivalent.*

(i) *R/K is simple.*

(ii) $[L : K] \geq (np^n-1)/(sp^n-1)$.

Proof. By [6, Lemma 1.2], we have $[L : K] = p^n/\ell(R)$. Hence it follows from Theorem 8 that

$$\begin{aligned}(\text{i}) &\Leftrightarrow \ell(R) \leq p^n(sp^n-1)/(np^n-1)\\ &\Leftrightarrow p^n/\ell(R) \geq (np^n-1)/(sp^n-1)\\ &\Leftrightarrow [L : K] \geq (np^n-1)/(sp^n-1).\end{aligned}$$

Corollary 10. *Let R/K be a Galois extension with $[R : K] = p^n$. Moreover, let t be an integer such that*

$$p^{t-1} < (np^n-1)/(sp^n-1) \leq p^t.$$

Then the following conditions are equivalent.

(i) *R/K is simple.*

(ii) *R/K contains an intermediate field $\mathrm{GF}(p^{sp^t})$.*

Proof. (ii) $\Rightarrow$ (i): Clearly, there is a maximal subfield L' in R containing $\mathrm{GF}(p^{sp^t})$ ($\supset \mathrm{GF}(p^s) = K$). Then, by [6, Lemma 1.2] we have

$$[L' : K] = p^n/\ell(R) \geq p^t \geq (np^n-1)/(sp^n-1).$$

Hence our assertion follows from Theorem 9 (ii $\Rightarrow$ i). The assertion (i) $\Rightarrow$ (ii) is a direct consequence of Theorem 9 (i $\Rightarrow$ ii).

Corollary 11. *Let R/K be a Galois extension of rank p^n. Then*

(1) *If $n \leq s$ then R/K is simple.*

(2) *Assume that $n > s$.*

(a) *If $p > n/s$ then, R/K is simple if and only if R/K contains an intermediate field $\mathrm{GF}(p^{sp})$.*

(b) *In case $p = n/s$, R/K is simple if and only if R/K contains an intermediate field $\mathrm{GF}(p^{sp^2})$.*

Proof. Put $d(p, s, n) = (np^n-1)/(sp^n-1)$. Then,

$$d(p, s, n) \leq 1 \text{ if } n \leq s;$$
$$1 < d(p, s, n) \leq p \text{ if } n > s \text{ and } p \geq n/s;$$
$$p < d(p, s, n) < p^2 \text{ if } n > s \text{ and } p = n/s.$$

Therefore we have (1) and (2) by Corollary 10.

Example 1. (1) Let $q = 19$, $[R : K] = 3^8$ and $\ell(R) = 3^7$ (note that there exists such a Galois extension surely). Then, in (2) of Corollary 3, the right-hand side is $2197.3\cdots$. Hence by the corollary we see that R/K is simple in this case because $\ell(R) = 2187$. However we cannot find that the inequality of Corollary 2(2). Indeed,

$$sr^n/(n\log_p r + \log_p 2) = 6561/\log_{19} 13122$$
$$= 2037.3\cdots < 2187 = \ell(R).$$

(2) Let $q = 3^3$, $[R : K] = 3^9$ and $\ell(R) = 3^8$. In this case, the right-hand side in (ii) of Theorem 8 is less than $\ell(R)$. In truth,

$$p^n(sp^n-1)/(np^n-1) = 6560.9\cdots < 6561 = \ell(R).$$

This implies that R/K is not simple because of the theorem.

2. On an example of Dedekind. Let B be a commutative ring with an identity 1, and A a subring of B containing 1 such that B is a finite free A-module with basis $\{d_1, \ldots, d_n\}$. Let π_i be the A-projection of B onto the coefficients of d_i, and set

$$t(z) = \sum_{i=1}^{n} \pi_i(zd_i) \text{ for all } z \in B.$$

An easy computation shows that the map t is independent of the choice of a free basis $\{d_1, \ldots, d_n\}$ for ${}_AB$. This will be called the trace map of B/A. Moreover, we set

$$\delta(d_1, \ldots, d_n) = \det[t(d_id_j)]$$

where $[t(d_id_j)]$ is the $n\times n$ matrix whose (i, j)-entry is $t(d_id_j)$ $(1 \leq i, j \leq n)$. This determinant will be called the discriminant of B/A with respect to $\{d_1, \ldots, d_n\}$.

Now, if B^* is an A-subalgebra of B with a free basis $\{d_1^*, \ldots, d_n^*\}$ for ${}_AB^*$ and $d_i^* = \sum_{j=1}^n a_{ij}d_j$ $(a_{ij} \in A, j = 1, \ldots, n)$ then

$$\delta(d_1^*, \ldots, d_n^*) = (\det[a_{ij}])^2 \delta(d_1, \ldots, d_n)$$

where $[a_{ij}]$ is the $n \times n$ matrix whose (i, j)-entry is a_{ij} $(1 \leq i, j \leq n)$. When $\delta(d_1, \ldots, d_n)$ is not a zero divisor of A, $B^* = B$ if and only if

$$\delta(d_1^*, \ldots, d_n^*) = a^2 \delta(d_1, \ldots, d_n) \text{ for some unit } a \text{ in } A.$$

Hence, in case that A is the ring of rational integers, $\delta(d_1, \ldots, d_n)$ is independent of the choice of a free basis $\{d_1, \ldots, d_n\}$ for ${}_AB$, and whence this will be denoted by $\delta(B)$, which will be called the discriminant of B.

Now, by making use of the same methods as in the proof of [2, Theorem 4.4 in Chapter III], we can prove the following

Lemma 12. *Let B be a commutative ring with an identity 1 and A a subring of B containing 1 such that B is a finite free A-module with basis $\{d_1, \ldots, d_n\}$. Then B is separable over A in the sense of* [2] *if and only if $\delta(d_1, \ldots, d_n)$ is a unit in A.*

Let Z be the ring of rational integers, and Q the field of rational numbers. Then, we obtain the following

Corollary 13. *Let E be an algebraic number field and B the ring of algebraic integers in E. Let p be a rational prime integer $(\in Z)$ which is not a divisor of $\delta(B)$. Then the localization $B_{(p)} = Z_{(p)} \otimes_Z B$ of B at $(p) = pZ$ is a separable algebra over $Z_{(p)}$. Moreover, $B_{(p)}/pB_{(p)} (= B_{(p)}/(pZ_{(p)}B_{(p)})) \cong B/pB$ which is a separable algebra over $Z_{(p)}/pZ_{(p)} \cong Z/pZ \cong \mathrm{GF}(p)$. In particular, if E is Galois over Q then B/pB is Galois over $\mathrm{GF}(p)$. Further, for any rational prime integer r, $B_{(r)}/Z_{(r)}$ is simple if and only if $(B/rB)/\mathrm{GF}(r)$ is simple.*

Proof. Since $rZ_{(r)}$ is the unique maximal ideal (i.e. the radical) of $Z_{(r)}$, it follows from Nakayama's Lemma that $B_{(r)}$ is simple over $Z_{(r)}$ if and only if $B_{(r)}/rZ_{(r)}B_{(r)} (= B_{(r)}/rB_{(r)})$ is simple over $Z_{(r)}/rZ_{(r)}$. Moreover, since rZ is a maximal ideal of Z, we see that $Z_{(r)}/rZ_{(r)} \cong Z/rZ \cong \mathrm{GF}(r)$ and so $B_{(r)}/rB_{(r)} \cong B/rB$. Hence, the extension $B_{(r)}/Z_{(r)}$ is simple if and only if so is $(B/rB)/\mathrm{GF}(r)$. The other assertions follow immediately from Lemma 12.

Corollary 14. *Let $E = Q(a)$ be an algebraic number field and B the ring of algebraic integers of E. Let $f(X)$ be the minimal polynomial of a over Q with $f(a) = 0$, and F the splitting field of $f(X)$ over Q in the field of*

complex numbers. Let G be the Galois group of F/Q, C the ring of algebraic integers of F, and D the composite ring of $\{\sigma(B);\ \sigma \in G\}$. Let p be any rational prime integer which is not a divisor of $\delta(B)$. Then $C_{(p)} = D_{(p)}$ which is a Galois extension of $Z_{(p)}$ with Galois group $G \mid C_{(p)} \cong G$, and p is not a divisor of $\delta(C)$.

Proof. It is obvious that $\sigma(C) = C$ for all $\sigma \in G$. Hence $F \supset C \supset D \supset B \supset Z$, and the fixring of G in C is Z. Moreover, $C_{(p)} \supset D_{(p)} \supset B_{(p)} \supset Z_{(p)}$, $\sigma(C_{(p)}) = C_{(p)}$, $\sigma(D_{(p)}) = D_{(p)}$ for all $\sigma \in G$, and the fixring of G in $C_{(p)}$ coincides with $Z_{(p)}$. As is well-known, $QB = E$ and F is the composite ring of $\{\sigma(E);\ \sigma \in G\}$. Therefore $G \mid D \cong G \cong G \mid C$, and so, $G \mid D_{(p)} \cong G \cong G \mid C_{(p)}$. Now, one will easily see that $D_{(p)}$ is the composite ring of $\{\sigma(B_{(p)});\ \sigma \in G\}$. Since $B_{(p)}/Z_{(p)}$ is separable (Corollary 13), it follows that $D_{(p)}$ is separable over $Z_{(p)}$, and so, $D_{(p)}/Z_{(p)}$ is a $(G \mid D_{(p)})$-Galois extension by [1, Theorem 1.3]. Hence there exists a Galois coordinate system $\{u_1, \ldots, u_s, v_1, \ldots, v_s\}$ in $D_{(p)}$ such that $\sum_i u_i \sigma(v_i) = \delta_{1,\sigma}$ for all $\sigma \in G$ where $\delta_{1,\sigma}$ is the Kronecker's delta. Then, for each c in $C_{(p)}$, we see that $c = \sum_i u_i t_G(cv_i) \in D_{(p)}$, where $t_G(c) = \sum_{\sigma \in G}(c)$. This implies that $D_{(p)} = C_{(p)}$. Since $C_{(p)}/Z_{(p)}$ is separable, $\delta(C_{(p)})$ is a unit of $Z_{(p)}$. Hence p is not a divisor of $\delta(C)$, completing the proof.

Example 2. Let Q be the field of rational numbers, and $Q(a)$ an algebraic number field where a is a root of the irreducible polynomial $f(X) = X^3+X^2-2X+8$. Let B be the ring of algebraic integers of $Q(a)$. Then, as is well-known, $B = Zw_1 \oplus Zw_2 \oplus Zw_3$ for some w_i's in B where Z is the ring of rational integers. Let $B_1 = Z1 + Za + Zb$ for $b = (a+a^2)/2$ and $B_2 = Z1 \oplus Za \oplus Za^2$. Then, noting $b^3-2b^2+3b-10 = 0$, we have $b \in B$ and $B_2 \subsetneqq B_1 \subsetneq B$. A direct computation shows that the discriminant $\delta(B_2)$ of B_2 is $2^2 \cdot (-503)$. Hence, by our remark in the first part of this section we see that $\delta(B_1) = -503$, $\delta(B_1) = \delta(B)$ and

$$B = B_1 = Z1 \oplus Za \oplus Zb$$

(cf. [14, 4-8-20]). However, in [14, 4-9-4, Example (Dedekind)], it has been proved that

$Q(a)$ does not have an integral basis of form $\{1, t, t^2\}$.

For this result, we shall present an alternative proof in which one of our results applies.

By $\bar{B}$, we denote the factor ring $B/2B$ of B modulo $2B$, and for any $c \in B$, we denote $c+2B(\in \bar{B})$ by $\bar{c}$. Clearly $\bar{B}$ contains the factor ring $Z/2Z = \mathrm{GF}(2)$ and

$$\bar{B} = \mathrm{GF}(2)\bar{1} \oplus \mathrm{GF}(2)\bar{a} \oplus \mathrm{GF}(2)\bar{b}.$$

Now, noting $b = (a+a^2)/2$ and $a^3+a^2 = 2a-8$, we see

$$\begin{gathered} a^2 \equiv a \pmod{2B}, \\ b^2 = b-2(1+a) \equiv b \pmod{2B} \text{ and} \\ ab = a-4 \equiv a \pmod{2B}. \end{gathered}$$

Hence we see that elements $e_1 := 1-\bar{b}$, $e_2 := \bar{a}$, and $e_3 := \bar{b}-\bar{a}$ are non-zero idempotents which are orthogonal to each other. It follows therefore that

$$\bar{B} = \mathrm{GF}(2)e_1 \oplus \mathrm{GF}(2)e_2 \oplus \mathrm{GF}(2)e_3$$

which is a trivial Galois extension of $\mathrm{GF}(2)$ (cf. [6, Remark 1.1]). Hence, we see that the extension $\bar{B}/\mathrm{GF}(2)$ is not simple from Proposition 1. Therefore, the extension B/Z is not simple. Thus, $Q(a)$ does not have an integral basis of form $\{1, t, t^2\}$.

Next, we consider the localization $Z_{(2)}$ of Z at the prime ideal $(2) = 2Z$. Noting that the discriminant of B is -503 and $-503 \notin 2B$, we see that $B_{(2)} = Z_{(2)} \otimes_Z B$ is a separable $Z_{(2)}$-algebra. Moreover, the $\mathrm{GF}(2)$-algebra $B_{(2)}/2B_{(2)}$ is algebra isomorphic to $\bar{B} = B/2B$. Since the extension $\bar{B}/\mathrm{GF}(2)$ is not simple, it follows that $B_{(2)}/Z_{(2)}$ is not simple. However, for any positive prime $p \in Z$ with $p \neq 2$, 503, $B_{(p)}$ is a separable $Z_{(p)}$-algebra which has a primitive element $a\,(= a/1)$ over $Z_{(p)}$. Moreover, $B_{(503)}$ is not separable over $Z_{(503)}$, but this has a primitive element a over $Z_{(503)}$. Further, we have

$$\begin{gathered} B_{(3)}/3B_{(3)} \cong \mathrm{GF}(3^3) \text{ and } B_{(7)}/7B_{(7)} \cong \mathrm{GF}(7^3) \\ B_{(5)}/5B_{(5)} \cong \mathrm{GF}(5)[X]/(X+1) \oplus \mathrm{GF}(5)[X]/(X^2-2) \\ \cong \mathrm{GF}(5)e_1 \oplus \mathrm{GF}(5^2)e_2, \text{ and} \\ B_{(503)}/503B_{(503)} \cong \mathrm{GF}(503)[X]/(X-204) \oplus \mathrm{GF}(503)[X]/((X-149)^2) \\ \cong \mathrm{GF}(503)e_1 \oplus (\mathrm{GF}(503) \oplus \mathrm{GF}(503)x)e_2 \end{gathered}$$

where e_1, e_2 are orthogonal idempotents and $x^2 = 0$, because $f(X) = X^3+X^2-2X+8$ is irreducible (mod 3) and (mod 7), respectively, $f(X) = (X+1)(X^2-2)$ (mod 5) and $f(X) = (X-204)(X-149)^2$ (mod 503). These enable us to see that $B_{(5)}/5B_{(5)}$ is separable but is not Galois by [6, Lemma

1.2]. Hence, $Q(a)/Q$ is also not Galois by Corollary 13 (cf. [2, p. 113] and [3, p. 471]).

Lastly, we consider the splitting field F of $f(X) = X^3+X^2-2X+8$ in the field of complex numbers. As is easily seen, F/Q is a Galois extension of rank 6. We shall now prove that

F does not have an integral basis of form $\{1, t, \ldots, t^5\}$.

Let C be the ring of algebraic integers in F, and G the Galois group of F/Q. Then $C_{(2)}$ is a Galois extension of $Z_{(2)}$ with Galois group $G \mid C_{(2)} \cong G$ by Corollary 14. Since $B_{(2)}$ is separable over $Z_{(2)}$, $B_{(2)}$ is a direct summand of $B_{(2)}$-module $C_{(2)}$, that is, $C_{(2)} = B_{(2)} \oplus M$ for some $B_{(2)}$-submodule M of $C_{(2)}$ (cf. [1, Lemma 6]). Then, one will easily see that $C_{(2)}/2C_{(2)} \supset (B_{(2)}+2C_{(2)})/2C_{(2)} \cong B_{(2)}/2B_{(2)}$ and this contains non-zero idempotents e_1, e_2 and e_3 which are orthogonal to each other by the preceding discussion. Hence $\ell(C_{(2)}/2C_{(2)})) \geq 3$. Since $C_{(2)}/2C_{(2)}$ is a Galois extension of $Z_{(2)}/2Z_{(2)} \cong \mathrm{GF}(2)$ of rank 6, it follows from Lemma 0 that $C_{(2)}/2C_{(2)}$ is not simple over $Z_{(2)}/2Z_{(2)}$ and so the extension C/Z is not simple. Thus, F does not have an integral basis of form $\{1, t, \ldots, t^5\}$. This completes the proof.

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, Berlin-Heidelberg-New York, 1971.

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

[4] I. KIKUMASA : On primitive elements of Galois extensions of commutative semi-local rings II, Math. J. Okayama Univ. 31 (1989), 57−71.

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

[6] I. KIKUMASA, T. NAGAHARA and K. KISHIMOTO : On primitive elements of Galois extensions of commutative semi-local rings, Math. J. Okayama Univ. 31 (1989), 31−55.

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

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

[9] T. NAGAHARA : On separable polynomials over a commutative ring II, Math. J. Okayama Univ. 15 (1972), 189−197.

[10] T. NAGAHARA and A. NAKAJIMA : On cyclic extensions of commutative rings, Math. J. Okayama Univ. 15 (1971), 81−90.

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

[12] R. S. PIERCE : Associative Algebras, G. T. M. 88, Springer-Verlag, Berlin-Heidelberg-New York, 1982.
[13] J. -D. THÉROND : Le théorème de l'élément primitif pour un anneau semi-local, J. Alg. **105** (1987), 29−39.
[14] E. WEISS : Algebraic Number Theory, McGraw-Hill, New York, 1963.
[15] P. WOLF : Algebraische Theorie der Galoisschen Algebren, VEB Deutscher Verlag der Wissenschaften, Berlin, 1956.

DEPARTMENT OF MATHEMATICS
FACULTY OF SCIENCE
OKAYAMA UNIVERSITY
TSUSHIMA-NAKA, OKAYAMA-SHI
OKAYAMA 700, JAPAN

(*Received January 10, 1990*)