Math. J. Okayama Univ. 29 (1987), 91−102

PRIMITIVE ELEMENTS OF CYCLIC EXTENSIONS OF COMMUTATIVE RINGS

Dedicated to Professor Hisao Tominaga on his 60th birthday

ISAO KIKUMASA and TAKASI NAGAHARA

Throughout this paper, A will mean a commutative ring with identity element 1 which is an algebra over a finite prime field $GF(p)$, and all ring extensions of A will be assumed with identity element 1, the identity element of A. Moreover, B will mean a Galois extension of A with a cyclic Galois group $G = \langle \sigma \rangle$ generated by σ of order p^n, which will be called a cyclic p^n-extension of A (with a Galois group G). If B is generated by a single element z over A then we say that B/A has a primitive element and z is a primitive element for B/A.

This paper is about the existness of primitive elements for cyclic p^n-extensions. In [2], K. Kishimoto made a study on primitive elements for cyclic 2^2-extensions. In §1, we shall present a sharpening of [2] and some generalizations. In §2, we shall give some applications and generalizations of the results of §1 to cyclic p^n-extensions with $p \geqq 2$ and $n \geqq 1$.

In what follows, given a Galois extension S/R with a Galois group G, we shall use the following conventions: For any subring T of S and any subgroup H of G,

1) $\mathfrak{M}(T) = \{M;\ M$ is a maximal ideal of $T\}$,

2) $G(T) = \{\sigma \in G;\ \sigma(a) = a$ for all $a \in T\}$,

3) $S(H) = \{a \in S;\ \sigma(a) = a$ for all $\sigma \in H\}$,

4) $t_H(a) = \sum_{\sigma \in H} \sigma(a)$ for each $a \in T$, which will be called the H-trace of a. Moreover, for any set V and its subset W,

5) $|V|$ = the cardinal number of V,

6) $V \backslash W$ = the complement of W in V.

Now, we shall here consider a cyclic p^n-extension B/A with a Galois group $G = \langle \sigma \rangle$. Then, there exists an element a in B whose G-trace is 1 ([1, Lemma 1.6]). If, in particular, $|G| = p$ then there exists an element b in B such that $\sigma(b) = b+1$. When this is the case, there holds that $B = A[b]$ and $t_G(b) = 0$ if $p > 2$ ([7, Theorem 1.2]). Such an element b will be called a σ-generator of B/A (cf. [2]). In case $|G| = 2$, an element c in B is a σ-generator of B/A if and only if $t_G(c) = 1$.

1. On primitive elements of cyclic 2^2-extensions. In this section, we shall discuss the case $p=2$ and $n=2$, i.e., $|\langle\sigma\rangle|=4$. Throughout this section, H will mean a subgroup of G generated by σ^2, i.e., $H=\langle\sigma^2\rangle$. Moreover we put $T=B(H)$ and $\sigma|T=\bar{\sigma}$.

First, we shall prove the following theorem which contains the result of K. Kishimoto [2, Lemma 1].

Theorem 1. *The following conditions are equivalent.*

(a) *There exists a primitive element for B/A whose G-trace is zero.*

(b) *There exists an invertible element of T whose $\langle\bar{\sigma}\rangle$-trace is* 1.

Proof. (a) ⇒ (b). Let $B=A[z]$ and $t_G(z)=0$, and set $b=z+\sigma(z)$. Then, we have $\sigma^2(b)=b$. This implies that $b\in T$ and $b+\sigma(b)\in A$. By [4, Theorem 3.3], b and $b+\sigma(b)=z+\sigma^2(z)$ are invertible in B. Hence $x=b(b+\sigma(b))^{-1}$ is an invertible element of T and $t_{\langle\bar{\sigma}\rangle}(x)=1$.

(b) ⇒ (a). Let x be an invertible element of T whose $\langle\bar{\sigma}\rangle$-trace is 1. Then, $\sigma(x)=x+1$. Hence we have $T=A[x]$ by [7, Theorem 1.2]. Since B is a Galois extension of A, there exists an element y in B such that $t_G(y)=1$. Put

$$b=x^2+x \text{ and } z=xy+x\sigma(y)+\sigma(xy+x\sigma(y)).$$

Then, since x is invertible, $\sigma(x)=x+1$ is also invertible and so is $b=x\sigma(x)$. Moreover, since $t_G(y)=1$, we have $\sigma^2(z)=z+1$. Hence $B=T[z]$. Further,

$$\begin{aligned} z+\sigma(z) &= xy+x\sigma(y)+\sigma^2(xy+x\sigma(y)) \\ &= xt_G(y)=x. \end{aligned}$$

Hence we have $\sigma(z)=z+x$. Then we obtain $\sigma(z^2+z+xb)=z^2+z+xb$. Therefore, it follows that $c=z^2+z+xb\in A$, and $x=(z^2+z+c)b^{-1}\in A[z]$. This implies that $A[z]=A[z,x]=T[z]=B$. Moreover, noting $\sigma(z)=z+x$ and $\sigma(x)=x+1$, we have $t_G(z)=0$.

Corollary 2. *Let x be an invertible element of T with $t_{\langle\bar{\sigma}\rangle}(x)=1$ and y an element of B with $t_G(y)=1$. Then*

$$z=xy+x\sigma^2(y)+\sigma(y)+\sigma^2(y)$$

is a primitive element for B/A whose G-trace is zero and so is $z+a$ for any $a\in A$. Moreover

$$z_1 = xy + x\sigma^2(y) + \sigma(y) + \sigma^2(y^2) + y + y^2$$

is also an element which has this property.

Proof. The first part is shown in the proof of Theorem 1. Moreover, it is clear that $A[z+a] = A[z] = B$ and $t_G(z+a) = t_G(z) = 0$ for any $a \in A$. Since $t_G(y) = 1$ and

$$\begin{aligned} z+z_1 &= y+\sigma^2(y)+y^2+\sigma^2(y^2), \\ \sigma(z+z_1) &= (\sigma(y)+\sigma^3(y))+(\sigma(y^2)+\sigma^3(y^2)) \\ &= (y+\sigma^2(y)+1)+(y^2+\sigma^2(y^2)+1) \\ &= z+z_1. \end{aligned}$$

Hence, $z+z_1$ is in A and $z_1 = z+b$ for some $b \in A$. This shows the last part.

Remark 1. Assume that there is an invertible element x in T whose $\langle \bar{\sigma} \rangle$-trace is 1. Then, for any element y of B whose G-trace is 1, we set

$$b = x^2+x,\ z = xy+x\sigma(y)+\sigma(xy+x\sigma(y)),\ c = z^2+z+xb \text{ and}$$
$$f = (X-z)(X-\sigma(z))(X-\sigma^2(z))(X-\sigma^3(z)).$$

Then, noting $\sigma(z) = z+x$, we have

$$f = X^4+(b+1)X^2+bX+(b^3+bc+c^2)$$

and $B = A[z] \cong A[X]/(f)$ by [4, Theorems 3.3 and 3.4]. Clearly $\{1, z, z^2, z^3\}$ is a linearly independent A-basis for B.

Next, for the z_1 in Corollary 2, we set $a = z_1+z\ (\in A)$, and

$$f_1 = (X-z_1)(X-\sigma(z_1))(X-\sigma^2(z_1))(X-\sigma^3(z_1)).$$

Then

$$f_1 = X^4+(b+1)X^2+bX+(b^3+b(c+a^2+a)+(c+a^2+a)^2)$$

and $B = A[z_1] \cong A[X]/(f_1)$. This primitive element z_1 for B/A and the polynomial f_1 are of K. Kishimoto's type in [2, Lemma 1].

Next, we shall present an alternative proof of [2, Lemma 2] which is simple.

Lemma 3 ([K. Kishimoto]). *Assume that B/A has a primitive element. Then, given $M \in \mathfrak{M}(A)$, if $A/M = GF(2)$ then $T/TM = GF(4)$.*

Proof. Let $M \in \mathfrak{M}(A)$ and $A/M = GF(2)$. Moreover, let x and z be primitive elements for T/A and B/A, respectively. Then B/BM is a cyclic 2^2-extension of A/M with a Galois group $\langle \rho \rangle$ where ρ is the automorphism of B/BM induced by σ. We set $r = x+BM$ and $s = z+BM$ in B/BM. Then $B/BM = GF(2)[s]$ and $(B/BM)(\rho^2) = T/TM = GF(2)[r]$. We shall here assume that $r^2-r=0$, i.e., $r^2 = r$. Then, noting $[GF(2)[r] : GF(2)] = 2$, we have $T/TM = GF(2)r \oplus GF(2)(1-r)$. Hence the units of T/TM are only 1. Clearly $s+\rho^2(s) \in T/TM$. By [4, Theorem 3.3], $s+\rho^2(s)$ is a unit in B/BM, and so is in T/TM. Hence $s+\rho^2(s) = 1$, which implies that $t_{(\rho)}(s) = 0$. Thus, by Theorem 1, there exists a unit t in T/TM such that $t+\rho(t) = 1$. For $t = 1$, we have $t+\rho(t) = 0$, and this is a contradiction. Hence $r^2-r \neq 0$, and so, $r^2-r = 1$. Since $f = X^2+X+1$ is irreducible over $GF(2)$, $GF(4) = GF(2)[X]/(f) \cong GF(2)[r]$.

Now, we define here three sets $\mathfrak{M}_0$, $\mathfrak{M}_1$ and $\mathfrak{M}_1'$ as follows:

$$\mathfrak{M}_0 = \{M \in \mathfrak{M}(A);\ TM \in \mathfrak{M}(T)\},$$
$$\mathfrak{M}_1 = \{N \in \mathfrak{M}(T);\ BN \in \mathfrak{M}(B)\} \quad \text{and}$$
$$\mathfrak{M}_1' = \{N \in \mathfrak{M}(T);\ N \cap A \in \mathfrak{M}_0\}.$$

We will often use the sets in the rest of this section.

Lemma 4. (i) *If $N \in \mathfrak{M}(T)$ then $N \cap \sigma(N) = T(N \cap A)$ and*

$$\{N' \in \mathfrak{M}(T);\ N \cap A \subset N'\} = \{N, \sigma(N)\}.$$

(ii) *For $N \in \mathfrak{M}(T)$, there holds $N \in \mathfrak{M}_1'$ if and only if $\sigma(N) = N$; and hence $N \notin \mathfrak{M}_1'$ if and only if $\sigma(N) \neq N$.*

(iii) $\mathfrak{M}_1' = \{TM;\ M \in \mathfrak{M}_0\} \subset \mathfrak{M}_1$.

Proof. (i) Set $N_0 = N \cap \sigma(N)$ and $M_0 = N \cap A$. Then, since

$$\sigma(N_0) = N_0 \text{ and } \sigma(TM_0) = TM_0,$$

T/N_0 and T/TM_0 are Galois extensions over the field A/M_0 of order 2. Hence,

$$[T/N_0 : A/M_0] = [T/TM_0 : A/M_0] = 2.$$

Moreover, since $TM_0 \subset N_0$, we have a natural A/M_0-homomorphism of T/TM_0 to T/N_0. Therefore, $T/TM_0 = T/N_0$ and $TM_0 = N_0$. This shows the first equality.

For any $N' \in \{N' \in \mathfrak{M}(T);\ N \cap A \subset N'\}$,

$$N\sigma(N) \subset N \cap \sigma(N) = T(N \cap A) \subset N'.$$

Thus $N \subset N'$ or $\sigma(N) \subset N'$ because N' is a prime ideal of T. Hence we have $N = N'$ or $\sigma(N) = N'$ by maximality. This implies that

$$\{N' \in \mathfrak{M}(T);\ N \cap A \subset N'\} \subset \{N, \sigma(N)\}.$$

The converse inclusion is trivial.

(ii) Let N be an element of $\mathfrak{M}(T)$. Assume that $N \in \mathfrak{M}_1'$. Then, by (i), $N \cap \sigma(N) = T(N \cap A) \in \mathfrak{M}(T)$. Hence, by maximality,

$$N \cap \sigma(N) = N \text{ and } N \cap \sigma(N) = \sigma(N).$$

It follows therefore that $\sigma(N) = N$.

Conversely, assume that $\sigma(N) = N$. Then, by (i),

$$T(N \cap A) = N \cap \sigma(N) = N \in \mathfrak{M}(T).$$

Thus we obtain $N \in \mathfrak{M}_1'$.

(iii) By (i) and (ii), we can easily see that $\mathfrak{M}_1' = \{TM;\ M \in \mathfrak{M}_0\}$. Let N be any element of $\mathfrak{M}_1'$. Then, $N = TM$ for some $M \in \mathfrak{M}_0$. Since $TM \in \mathfrak{M}(T)$, T/TM is a field. Thus, by [7, Theorem 1.8], B/BM is also a field. Hence

$$BN = B\cdot TM = BM \in \mathfrak{M}(B).$$

This implies that $N \in \mathfrak{M}_1$ and so $\mathfrak{M}_1' \subset \mathfrak{M}_1$.

Theorem 5. *Assume that* $|\mathfrak{M}(A)\backslash\mathfrak{M}_0|$ *is finite and* $T/TM = GF(4)$ *for any* $M \in \mathfrak{M}(A)$ *such that* $A/M = GF(2)$. *Then, there exists an invertible element* y *in* T *with* $t_{(\bar{\sigma})}(y) = 1$. *Therefore* B/A *has a primitive element.*

Proof. First, we shall show that there exists an element y in T such that $y + \sigma(y) = 1$ and $y \notin N$ for all $N \in \mathfrak{M}(T)\backslash\mathfrak{M}_1'$. Since $|\mathfrak{M}(A)\backslash\mathfrak{M}_0|$ is finite, so is $|\mathfrak{M}(T)\backslash\mathfrak{M}_1'|$. Hence by Lemma 4, we can put

$$\mathfrak{M}(T)\backslash\mathfrak{M}_1' = \{N_{11}, N_{12}, N_{21}, N_{22}, \dots, N_{t1}, N_{t2}\}$$

where $\sigma(N_{i1}) = N_{i2}$ $(i = 1, 2, \dots, t)$ and $N_{j1} \neq N_{i1}, N_{i2}$ for $j \neq i$. Moreover, set

$$M_i = A \cap N_{i1}\ (i = 1, 2, \dots, t).$$

Then, if $i \neq j$ then $M_i \neq M_j$. Indeed, if $M_i = M_j$ for some $i \neq j$ then

$$N_{i1} \cap A = N_{j1} \cap A \subset N_{j1} \text{ and } \subset N_{i1}.$$

Since $N_{j1} \neq \sigma(N_{i1})$, this is a contradiction by Lemma 4(i). Therefore, for $I = \bigcap_{i=1}^{t} M_i$, $A/I = A/M_1 \oplus A/M_2 \oplus \cdots \oplus A/M_t$. Since all A/M_i are fields, there exists a set of orthogonal idempotents $\{\bar{e}_1, \bar{e}_2, \ldots, \bar{e}_t\}$ in A/I such that

$$\bar{1} = \bar{e}_1 + \bar{e}_2 + \cdots + \bar{e}_t,$$

$e_i \in A$, $e_i \notin M_i$ and $e_j \in M_i$ $(j \neq i)$. Moreover, by our assumption, A/M_i is a field such that $A/M_i \neq GF(2)$. Indeed, if $A/M_i = GF(2)$ then $T/TM_i = GF(4)$. This means that $TM_i \in \mathfrak{M}(T)$ and $N_{i1} \in \mathfrak{M}'_1$. This is a contradiction. Hence, there exists an element a_i of A such that $a_i e_i \neq e_i$ and $\neq 0$ (mod M_i). This shows that

$$(a_i^2 + a_i)e_i \neq 0 \pmod{M_i}.$$

Now, for an element x in T with $t_{\langle\bar{\sigma}\rangle}(x) = 1$, we define an element y in T as follows:

If $x \notin N_{ik}$ for all i and k then $y = x$ (in this case, it is clear that $y + \sigma(y) = 1$ and $y \notin N$ for all $N \in \mathfrak{M}(T) \backslash \mathfrak{M}'_1$).

If $x \in N_{ik}$ for some i and k then, without loss of generality, we may choose an integer s $(1 \leqq s \leqq t)$ such that

$$x \in N_{i1} \text{ or } x \in N_{i2} \text{ if } 1 \leqq i \leqq s \text{ and}$$
$$x \notin N_{j1} \text{ and } x \notin N_{j2} \text{ if } s < j \leqq t.$$

For the s and the above a_i, we put

$$a = a_1 e_1 + a_2 e_2 + \cdots + a_s e_s \text{ and}$$
$$y = x + a.$$

Then, since $a \in A$, $y + \sigma(y) = x + \sigma(x) = 1$.

Now we shall show that $y \notin N$ for all $N \in \mathfrak{M}(T) \backslash \mathfrak{M}'_1$. As is easily seen,

$$a^2 + a = (a_1^2 + a_1)e_1 + (a_2^2 + a_2)e_2 + \cdots + (a_s^2 + a_s)e_s \pmod{I}.$$

Since $e_j \in M_i$ $(j \neq i)$,

$$a^2 + a = (a_i^2 + a_i)e_i \neq 0 \pmod{M_i} \ (1 \leqq i \leqq s) \text{ and}$$
$$a^2 + a = 0 \pmod{M_j} \ (s < j \leqq t).$$

It follows that $a^2 + a \notin M_i$ $(1 \leqq i \leqq s)$ and $a^2 + a \in M_j$ $(s < j \leqq t)$. We note here that $x\sigma(x)$ is contained in $A = B(\sigma)$ and

$$x\sigma(x) \in N_{i1}N_{i2} \subset N_{i1} \cap N_{i2} \; (1 \leqq i \leqq s).$$

Then

$$x\sigma(x) \in A \cap (\bigcap_{i=1}^{s}(N_{i1} \cap N_{i2})) = \bigcap_{i=1}^{s} M_i.$$

Moreover, $y\sigma(y) = x\sigma(x) + a^2 + a$. Hence, we see that

$$y\sigma(y) \notin M_i \; (1 \leqq i \leqq s).$$

For j $(s < j \leqq t)$, x and $\sigma(x)$ are not in N_{jk} $(k = 1, 2)$ by the definition of s. Since N_{j1} is a prime ideal, $x\sigma(x) \notin N_{j1}$ and so $x\sigma(x) \notin M_j$. Thus we have

$$y\sigma(y) \notin M_j \; (s < j \leqq t).$$

Therefore, $y \notin N_{i1}$ and $\sigma(y) \notin N_{i1}$ $(1 \leqq i \leqq t)$. Since $\sigma(y) \notin N_{i1}$ means that $y \notin N_{i2}$, we see that $y \notin N$ for all $N \in \mathfrak{M}(T) \backslash \mathfrak{M}_1'$.

Now, we are in a position to complete the proof. Indeed, it suffices to show that $y \notin N$ for all $N \in \mathfrak{M}_1'$. Because if $y \notin N$ for all $N \in \mathfrak{M}(T)$ then y is an inversible element of T. In this case, B/A has a primitive element by Theorem 1.

Let N be any element of $\mathfrak{M}_1'$. Then, by Lemma 4, $N = TM$ for some $M \in \mathfrak{M}_0$. Hence, σ induces an automorphism ρ of T/N. Thus, T/N is a Galois extension of $A/(A \cap N)$ with a cyclic Galois group $\langle\rho\rangle$. Since $y + \sigma(y) = 1$, we have $\bar{y} + \rho(\bar{y}) = \bar{1}$ in T/N. Hence $\bar{y} \neq \bar{0}$ and so $y \notin N$.

Corollary 6. *Assume that* $|\mathfrak{M}(A) \backslash \mathfrak{M}_0|$ *is finite. Then the following are equivalent.*

(a) *B/A has a primitive element.*

(b) *B/A has a primitive element whose G-trace is zero.*

Proof. (b) $\Rightarrow$ (a) is trivial.

(a) $\Rightarrow$ (b). By Lemma 3, $T/TM = GF(4)$ for any $M \in \mathfrak{M}(A)$ such that $A/M = GF(2)$. Hence, by Theorem 1 and Theorem 5, we obtain (b).

The following theorem contains the result of [2, Theorem 3].

Theorem 7. *Assume that* $|\{M \in \mathfrak{M}(A);\; A/M \neq GF(2)\}|$ *is finite. Then, the following conditions are equivalent.*

(a) *B/A has a primitive element.*

(b) $T/TM = GF(4)$ *for any* $M \in \mathfrak{M}(A)$ *such that* $A/M = GF(2)$.

Proof. (a) $\Rightarrow$ (b). It is clear by Lemma 3.

(b) $\Rightarrow$ (a). Let M be an element of $\mathfrak{M}(A)$ such that $A/M = GF(2)$. Then, $TM \in \mathfrak{M}(T)$ because $T/TM = GF(4)$ is a field. Hence we have $M \in \mathfrak{M}_0$. Since $|\{M \in \mathfrak{M}(A)\,;\ A/M \neq GF(2)\}|$ is finite, so is $|\mathfrak{M}(A)\setminus\mathfrak{M}_0|$. Thus, by Theorem 5, B has a primitive element over A.

2. On primitive elements of cyclic p^n-extensions. Set $B_i = B(\sigma^{p^i})$ $(i = 0, 1, 2, \ldots, n)$ and $\mathfrak{M}_i = \{M \in \mathfrak{M}(B_i)\,;\ B_{i+1}M \in \mathfrak{M}(B_{i+1})\}$ $(i = 0, 1, 2, \ldots, n-1)$. Then, obviously $B = B_n$ and $A = B_0$. Moreover, B_i is a cyclic p^{i-j}-extension of B_j with a Galois group $\langle \sigma^{p^j} | B_i \rangle$.

Theorem 8. *Assume that* $p = 2$ *and* $|\mathfrak{M}(B_0)\setminus\mathfrak{M}_0|$ *is finite. Then, the following conditions are equivalent.*

(a) B_2/B_0 *has a primitive element.*

(b) B_{k+2}/B_k *has a primitive element for any* k $(0 \leqq k \leqq n-2)$.

Proof. (a) $\Rightarrow$ (b). We note that B_{k+2} is a cyclic 2^2-extension of B_k with a Galois group $\langle \sigma^{2^k} | B_{k+2} \rangle$. First, we shall show that $|\mathfrak{M}(B_k)\setminus\mathfrak{M}_k|$ is finite for each k $(0 \leqq k \leqq n-2)$ by induction. To prove this, let i be any integer such that $0 \leqq i < n-2$ and N an element of $\mathfrak{M}(B_{i+1})$ such that $N \cap B_i \in \mathfrak{M}_i$. Then, by Lemma 4(iii), we have $N \in \mathfrak{M}_{i+1}$. Hence, if $L \in \mathfrak{M}(B_{i+1})\setminus\mathfrak{M}_{i+1}$ then $L \cap B_i \in \mathfrak{M}(B_i)\setminus\mathfrak{M}_i$. Combining this with Lemma 4(i), we see that if $|\mathfrak{M}(B_i)\setminus\mathfrak{M}_i|$ is finite then $|\mathfrak{M}(B_{i+1})\setminus\mathfrak{M}_{i+1}|$ is also finite.

Now, we shall show that B_{k+2}/B_k has a primitive element for all k $(0 \leqq k \leqq n-2)$ by induction. We assume that B_{k+2}/B_k has a primitive element for all k $(0 \leqq k < n-2)$. Then, it is enough to show that $B_{k+1}/N \neq GF(2)$ for any $N \in \mathfrak{M}(B_{k+1})$. Indeed, in this case, we see that B_{k+3}/B_{k-1} has a primitive element by Theorem 5.

Assume that $B_{k+1}/N = GF(2)$ for some $N \in \mathfrak{M}(B_{k+1})$. Then, since

$$B_k/(B_k \cap N) \subset B_{k+1}/N,$$

we obtain $B_k/(B_k \cap N) = GF(2)$. Hence, by Lemma 3, $B_{k+1}/(B_k \cap N)B_{k+1} = GF(4)$, which is a field. Thus, we have $(B_k \cap N)B_{k+1} = N$ by the maximality of $(B_k \cap N)B_{k+1}$. It follows that $B_{k+1}/N = GF(4)$. This is a contradiction.

(b) $\Rightarrow$ (a) is trivial.

Theorem 9. *Assume that* $p=2$ *and* $|\{M \in \mathfrak{M}(A);\ A/M \neq GF(2)\}|$ *is finite. Then, the following conditions are equivalent.*

(a) B_2/B_0 *has a primitive element.*

(b) B_{k+2}/B_k *has a primitive element for any* k $(0 \leqq k \leqq n-2)$.

Proof. (a) $\Rightarrow$ (b). Let M be an element of $\mathfrak{M}(B_0)$ such that $A/M = GF(2)$. Then, by Theorem 7, $B_1/B_1M = GF(4)$. Hence $B_1M \in \mathfrak{M}(B_1)$ and so $M \in \mathfrak{M}_0$. This implies that

$$\mathfrak{M}(B_0)\backslash\mathfrak{M}_0 \subset \{M \in \mathfrak{M}(A);\ A/M \neq GF(2)\}.$$

Thus, $|\mathfrak{M}(B_0)\backslash\mathfrak{M}_0|$ is finite. Therefore, we have (b) by Theorem 8.

(b) $\Rightarrow$ (a). Trivial.

Corollary 10. *When* B/A *is in the situation of Theorem* 8 *or* 9, *this has a system of generating elements consisting of* m *elements where* $m=n/2$ *if* n *is an even number, and* $m=(n+1)/2$ *if* n *is an odd number.*

Proof. The assertion is obvious by Theorems 8 and 9.

Theorem 11. *Assume that* $p \geqq 2$ *and* $\mathfrak{M}(A)=\mathfrak{M}_0$. *Then,* B/A *has a primitive element. Moreover, if* $x \in B$ *with* $t_G(x)=1$ *then* x *is a primitive element for* B/A *and is invertible.*

Proof. Let M be any element of $\mathfrak{M}(A)$. Then, B/BM is a cyclic p^n-extension with a Galois group $\langle\rho\rangle$ where ρ is the automorphism of B/BM induced by σ. Further, $(B/BM)(\rho^p) = B_1/B_1M$ which is a field. Hence, by [7, Theorem 1.8], B/BM is also a field. We will here denote $b+BM$ $(\in B/BM)$ by $\bar{b}$. For an element x of B satisfying $t_G(x)=1$, $\rho^i(\bar{x}) \neq \bar{x}$ for any i $(1 \leqq i \leqq p^n-1)$ since $t_{\langle\rho\rangle}(\bar{x}) = \bar{1}$. Indeed, assume that $\rho^i(\bar{x}) = \bar{x}$ for some i and put $H=\{\tau \in \langle\rho\rangle;\ \tau(\bar{x})=\bar{x}\}$. Then, H is a subgroup of $\langle\rho\rangle$ and hence $|H|=p^s$ for some integer s $(1 \leqq s \leqq n)$.
Since

$$\langle\rho\rangle = \rho_1H \cup \rho_2H \cup \cdots \cup \rho_mH \quad (\rho_i \in \langle\rho\rangle;\ 1 \leqq i \leqq m)$$

for some integer m, we have $t_{\rho_iH}(\bar{x}) = p^s\rho_i(\bar{x}) = \bar{0}$. Hence, $t_{\langle\rho\rangle}(\bar{x}) = \bar{0}$ which is a contradiction. Therefore, by the Galois theory of fields,

$$B/BM = (A/M)[\bar{x}].$$

This implies that $B = A[x]+BM$. Since M is any maximal ideal of A, we have $B=A[x]$ by [8, Theorem 9.1].

Next, we shall prove that the x is invertible. For any $M \in \mathfrak{M}(A)$, $\bar{x} \neq \bar{0}$ because $t_{\langle\rho\rangle}(\bar{x}) = \bar{1}$. Noting that B/BM is a field, we have $(B/BM)\bar{x} = B/BM$. This means that $Bx+BM = B$. Thus, by the same way as in the above, we have $Bx = B$ and so x is invertible.

Remark 2. Let

$$B = GF(3^3) \oplus GF(3^3) \oplus GF(3^3)$$

and τ an automorphism of $GF(3^3)$ of order 3. Moreover, let σ be an automorphism of B defined by

$$\sigma((x_1, x_2, x_3)) = (\tau(x_3), x_1, x_2).$$

Then, by [6, Lemma 1.1], B is a cyclic 3^2-extension of

$$A = \{(a, a, a);\ a \in GF(3)\}$$

with a Galois group $\langle\sigma\rangle$. As is seen in [3, p. 555], the following polynomials are irreducible over $GF(3)$:

$$f_1 = X^3+2X+1,$$
$$f_2 = X^3+2X+2 \text{ and}$$
$$f_3 = X^3+X^2+2.$$

Clearly, each f_i and f_j $(i \neq j)$ are relatively prime. Hence for $g = f_1 f_2 f_3$, we have

$$A[X]/(g) \cong A[X]/(f_1) \oplus A[X]/(f_2) \oplus A[X]/(f_3).$$

Since $A[X]/(f_i) \cong GF(3^3)$ $(i = 1, 2, 3)$, it follows that $A[X]/(g) \cong B$. Noting $A[X]/(g) = A[x]$ for $x = X+(g)$, B/A has a primitive element. However, we have

$$B(\sigma^3) = GF(3) \oplus GF(3) \oplus GF(3)$$

which is not a field. Hence Lemma 3 does not hold for $p = 3$. Clearly, in the extension $B(\sigma^3)/A$, $(2, 1, 1)$ is an invertible element whose trace is 1, but there are not invertible σ-generators. Moreover, there are 8 irreducible polynomials of degree 3 in $GF(3)[X]$. On the other hand, the ones of degree 2 in $GF(2)[X]$ are only X^2+X+1 (cf. [3, pp. 553–555]).

Remark 3. Let B be a cyclic 2^n-extension of $GF(2)$ with a Galois group $\langle\sigma\rangle$, $B_1 = B(\sigma^2)$, and $B_2 = B(\sigma^4)$. If $B_2/GF(2)$ has a primitive element then $B_1 = GF(4)$ by Lemma 3, and whence by [7, Theorem 1.8], B is a field, which has a primitive element over $GF(2)$. However, the converse does not hold. This is seen in the following example. Let

$$B = GF(2^4) \oplus GF(2^4)$$

and τ an automorphism of $GF(2^4)$ of order 4. Then B is a cyclic 2^3-extension of $A = \{(a, a)\,;\ a \in GF(2)\}$ with a Galois group $\langle\sigma\rangle$ where $\sigma((x_1, x_2)) = (\tau(x_2), x_1)$. Now, as is seen in [3, p. 553], the following polynomials in $GF(2)[X]$ are irreducible over $GF(2)$:

$$f_1 = X^4+X^3+1 \text{ and}$$
$$f_2 = X^4+X^3+X^2+X+1.$$

Hence, for $g = f_1 f_2$, we have the A-ring isomorphisms

$$A[X]/(g) \cong A[X]/(f_1) \oplus A[X]/(f_2) \cong GF(2^4) \oplus GF(2^4) = B.$$

Let b be an element of B which corresponds to $X+(g)$ under the above isomorphisms. Then b is a primitive element for B/A. However, since B is not a field, $B_2 = B(\sigma^4)$ has no primitive elements over A by the preceding statement. Moreover, it can be easily checked that $t_{\langle\sigma\rangle}(b) = \alpha(1, 1)$ where α is the sum of the coefficients of X^3 in f_1 and f_2. In this case, $t_{\langle\sigma\rangle}(b) = 0$ because $\alpha = 0$. But if we replace the f_1 by X^4+X+1, which is irreducible over $GF(2)$, then $\alpha = 1$ and so $t_{\langle\sigma\rangle}(b) = 1$. This shows that B/A has at least two primitive elements, each trace of which is 0 and 1.

Remark 4. Let

$$B = GF(4) \oplus \cdots \oplus GF(4)$$

which is the direct sum of 2^3 copies of $GF(4)$. Then B is a cyclic 2^3-extension of $A = \{(a, a, \dots, a)\,;\ a \in GF(4)\}$ with a Galois group $\langle\sigma\rangle$ where $\sigma((x_1, x_2, \dots, x_8)) = (x_8, x_1, \dots, x_7)\ (x_i \in GF(4)\,;\ 1 \leqq i \leqq 8)$. We set here $B_1 = B(\sigma^2)$ and $B_2 = B(\sigma^4)$. Then by Theorem 7, B_2/A has a primitive element. Hence by Theorem 9, B/B_1 has a primitive element. However, B/A has no primitive elements. Indeed, if $B = A[x]$ for some x in B then the elements $1, x, \dots, x^7$ are linearly independent over A by [4, Theorems 3.3 and 3.4]; on the other hand, since $a^4 = a$ for all $a \in GF(4)$, there holds $x^4 = x$, which is a contradiction. As is seen in Corollary 10, B is generated by two elements over A.

Remark 5. Let

$$B = GF(4) \oplus GF(4) \oplus GF(4) \oplus GF(4).$$

Then, B is a cyclic 2^2-extension of $A = \{(a, a, a, a) ; a \in GF(4)\}$ with a Galois group $\langle \sigma \rangle$ where $\sigma((x_1, x_2, x_3, x_4)) = (x_4, x_1, x_2, x_3)$ $(x_i \in GF(4) ; i = 1, 2, 3, 4)$. Then, by Theorem 7, B/A has a primitive element. Let $x = (x_1, x_2, x_3, x_4)$ be any primitive element for B/A. If $x_i = x_j$ for some $i < j$ then $x - \sigma^{j-i}(x)$ is not invertible in B, which is a contradiction by [4, Theorem 3.3]. Hence if $1 \leqq i \neq j \leqq 4$ then $x_i \neq x_j$. It follows therefore that $t_{\langle \sigma \rangle}(x) = 0$ because $\sum_{a \in GF(4)} a = 0$.

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

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

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

[5] T. NAGAHARA : On separable polynomials over a commutative ring III, Math. J. Okayama Univ. 16 (1974), 189–197.

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

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

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

DEPARTMENT OF MATHEMATICS
OKAYAMA UNIVERSITY, OKAYAMA 700, JAPAN

(*Received May 1, 1987*)