*Mathematical Journal of Okayama University*

*Volume* 28, *Issue* 1 1986 *Article* 3

JANUARY 1986

# Notes on biquadratic cyclic extensions of a commutative ring

Kazuo Kishimoto*

*Shinshu University

Math. J. Okayama Univ. 27 (1986), 15–20

# NOTES ON BIQUADRATIC CYCLIC EXTENSIONS OF A COMMUTATIVE RING

To the memory of Professor Akira Hattori

KAZUO KISHIMOTO

**Introduction.** Throughout the present paper, we assume that $A$ is a commutative ring of a prime characteristic $p$ with an identity 1 and $B$ is a commutative $(\sigma)$-cyclic extension of $A$ with a cyclic Galois group $(\sigma)$ of order $p^2$. As is known [3, Theorem 1.4], $B$ is obtained as a factor ring of a polynomial ring $A[X, Y]$ by an ideal $I=(X^p-X-a,\ Y^p-Y-f(X))$ for some $a \in A$ and $f(X) \in A[X]$. Thus $B=A[x, y]=\sum_{i,j=0}^{p-1} \oplus x^i y^j A$ where $x=X+I$ and $y=Y+I$. In this case, $B$ has a primitive element $z$, i.e. $B=A[z]=\sum_{i=0}^{p^2-1} \oplus z^i A$ for some $z \in B$ if $B$ is a field. But the following example shows that this is not true if $B$ is not a field. For let $B=\sum_{i=1}^{4} \oplus A_i = \{(a_1, a_2, a_3, a_4)\ ;\ a_i \in A_i\}$ where each $A_i = GF(2)$ and $A=\{(a_1, a_2, a_3, a_4)\ ;\ a_1=a_2=a_3=a_4\} \cong GF(2)$. Then the map $\sigma: B \to B$ such that $\sigma(a_1, a_2, a_3, a_4)=(a_4, a_1, a_2, a_3)$ gives an automorphism of $B$ of order 4 whose fixed subring $B^\sigma=A$. If we put $e_i$ is the identity of $A_i$ then $\sum_{i=1}^{4} e_i \tau(e_i)=\delta_{1,\tau}$ for each $\tau \in (\sigma)$, and hence $B/A$ is a $(\sigma)$-cyclic extension. Since $B$ is a Boolean ring, $B$ has no primitive element. In this paper, we shall study a necessary and sufficient condition for $B$ to have a primitive element when $p=2$ and $A/J(A)$ is an artinian ring where $J(A)$ is Jacobson radical of $A$.

**1. Prerequisites.** (i) Let $T=B^{\sigma^2}$. Then $T$ has an element $x$ such that $\{1, x\}$ is a linearly independent $A$-basis for $T$, $x^2+x=\alpha \in A$ and $\sigma(x)=x+1$, and so $T=A[x]=A \oplus xA$. We say such an element $x$ is a $\sigma$-generator of $T/A$. If $x$ is a $\sigma$-generator of $T/A$ then $x+a$ is also a $\sigma$-generator for any $a \in A$ and conversely.

(ii) Let $D=\sigma+1$. Then $D$ is a $\sigma$-derivation of $B$ such that $D^4=0$ and $B^D=\{b \in B;\ D(b)=0\}=A$. Since $B_A \oplus > A_A$, there exists an element $t \in B$ such that $D^3(t)=1$. For a $\sigma$-generator $x$ of $T/A$, $D(D^2(t)+x)=0$ implies that $x=D^2(t)+\gamma=D^2(t+D(t)\gamma)$ for some $\gamma \in A$. If we put $v=t+D(t)\gamma$, then $D^3(v)=1$, $D^2(v)=x$ and hence $(D^2(v))^2+D^2(v)(=x^2+x)=\alpha \in A$. Moreover, in this case, $B=A[v, D(v), D^2(v)]$ and $\{D^i(v)\ ;\ 0 \leq i \leq 3\}$ is a linearly independent $A$-basis for $B$ [1].

(iii) Let $M$ be a maximal ideal of $A$. Then $A/M \cong GF(2)$ if and only

if $\{a^2+a;\ a \in A\} \subseteq M$.

Let $I$ be an ideal of $A$. Then $IA'$ is an ideal of $A'$ for each intermediate subring $A'$ of $B/A$. In what follows, for each element $b \in A'$, we denote the coset $b+IA'$ of $A'/IA'$ by $b$ again if it arises no confusion.

**2. A sufficient condition.** The following Lemma gives a sufficient condition for $B$ to have a primitive element.

**Lemma 1.** *$B$ has a primitive element if there exists a $\sigma$-generator $x$ of $T/A$ such that $x^2+x=a \in U(A)$, the unit group of $A$. Moreover, if this is the case $B$ is given by $A[Z]/(Z^4+(1+a)Z^2+aZ+a^3+a\beta+\beta^2)$ for some $\beta \in A$ and $\sigma(z)=z+(z^2+z+\beta)a^{-1}$.*

*Proof.* Let $x$ be a $\sigma$-generator of $T/A$ such that $x^2+x=a \in U(A)$. As is remarked in (ii), there exists an element $v \in B$ such that $D^3(v)=1$, $D^2(v)=x$ and $B=A[v, D(v), D^2(v)]$. We now show that $B=A[D(v)]$ and $\{1, D(v), D(v)^2, D(v)^3\}$ is a linearly independent $A$-basis for $B$. For,

$$D(D(v)^2)=D^2(v)^2=D^2(v)+a=D^2(v)+D^3(v)a$$

implies $D(D(v)^2+D(v)+D^2(v)a)=0$, and hence,

$$D^2(v)a=D(v)^2+D(v)+\beta \text{ for some } \beta \in A.$$

Since $a \in U(A)$, we obtain

$$\begin{aligned} &D^2(v)=(D(v)^2+D(v)+\beta)a^{-1} \in A[D(v)].\\ &D(D(v)D^2(v))=\sigma D(v)+D^2(v)^2=D^2(v)+D(v)+D^2(v)^2\\ &\qquad\qquad =D(v)+a=D(v)+D^3(v)a \end{aligned}$$

implies $v=D(v)D^2(v)+D^2(v)a+\beta$ for some $\beta \in A$, and hence, $v \in A[D(v)]$

Therefore we obtain $B=A[D(v)]$.

$$\begin{aligned} (D(v))^4&=(D(v)^2)^2=(D(v)+D^2(v)a+\beta)^2\\ &=D(v)^2+(D^2(v)+a)a^2+\beta^2\\ &=D(v)^2+(D(v)^2+D(v)+\beta)a^{-1}+a)a^2+\beta^2\\ &=D(v)^2(1+a)+D(v)a+a^3+a\beta+\beta^2. \end{aligned}$$

If we note that

$$D^3(D(v)^3)=D(\sigma^2(D(v))D^2(D(v)^2)+D^3(v)D(v)^2)$$

$$= D(\sigma^2(D(v))+D(v)^2) = \sigma^2(D^2(v))+D^2(v)^2$$
$$= \sigma^2(D^2(v))+D^2(v)+\alpha = \alpha,$$

$u = \sum_{i=0}^{3} a_i D^i(v) = 0$ $(a_i \in A)$ implies $0 = D^3(u) = a_3\alpha$ and hence $a_3 = 0$. Repeating the same procedure, we can see that $\{1, D(v), D(v)^2, D(v)^3\}$ is linearly independent over $A$ and so $B = \sum_{i=0}^{3} \oplus AD(v)^i \cong A[Z]/(Z^4+(1+\alpha)Z^2+\alpha Z+\alpha^3+\alpha\beta+\beta^2)$. Furthermore, $\sigma(D(v)) = D^2(v)+D(v) = (D(v)+D(v)^2+\beta)\alpha^{-1}+D(v)$ shows that $\sigma(z) = z+(z^2+z+\beta)\alpha^{-1}$.

**3. A necessary condition.** The following Lemma gives a necessary condition for $B$ to have a primitive element.

**Lemma 2.** *Assume $B$ has a primitive element. Then for any maximal ideal $M$ of $A$ there hold either*

*(a) $A/M \neq GF(2)$, or*

*(b) $A/M = GF(2)$ and the factor ring $A[x]/M[x] \cong GF(4)$ for every $\sigma$-generator $x$ of $T/A$ where $T = A[x] = B^{\sigma^2}$.*

*Proof.* Let $z$ be a primtive element of $B$ such that $z^4 = \sum_{i=0}^{3} a_i z^i$ for $a_i \in A$ and let $D^3(z) = m \in A$.
Then

$$D^3(z^4) = m^4 = a_1 m+a_2 m^2+a_3 D^3(z^3)\cdots\cdots\cdots(1)$$

We shall prove the assertion distinguishing following two cases.

Case ( i ) $D^3(z) = m \notin U(A)$ : Let $M$ be a maximal ideal of $A$ such that $m \in M$. Then $a_3 D^3(z^3) \in M$ by (1). If $D^3(z^3) \in M$, we have a contradiction that $A = D^3(B) \subseteq M$, and so $D^3(z^3) \notin M$ and $a_3 \in M$. Thus $A = AD^3(z^3)+M$ and hence $D^3(z^3)$ is a unit element modulo $M$. Now we consider the factor ring $A[z]/M[z]$. Then $A[z]/M[z] \cong A/M[z] \cong A/(M[Z]/(Z^4+a_2Z^2+a_1Z+a_0))$, $D^3(z^3)$ is a unit element in $A/M$ and, by [2, Theorem 5.6], $A/M[z]$ is a $(\sigma)$-cyclic extension over $A/M$. Let $A/M = GF(2)$. Then $D^3(z^3) = 1$ in $A/M$ and $A[x]/M[x] \cong GF(2)[x]$ for any $\sigma$-generator $x$ of $T/A$. Hence $x^2+x$ is either 0 or 1 in $A/M$. If $x^2+x = 1$ then $GF(2)[x] = GF(4)$, and hence we assume that $x^2+x = 0$. Since $0 = D^3(z) = D^2(D(z))$, we have either

$$D(z) = \begin{cases} x+\varepsilon \\ \varepsilon \end{cases} \quad \text{in } A/M[z] = GF(2)[z], \text{ where } \varepsilon = 0 \text{ or } 1.$$

If $D(z) = \varepsilon$ then $z = x+\varepsilon$ or $\varepsilon$ and this contradicts to linear independence of $\{z^i ; 0 \leq i \leq 3\}$ over $A/M$. Thus $D(z)$ must be $x+\varepsilon$. Then $D(z^2) = D(z)^2 = (x+\varepsilon)^2 = x+\varepsilon$, and so $D(z^2+z) = 0$. But this is also a contradiction since $z^2+z+\varepsilon = 0$.

Case (ii) $D^3(z) \in U(A)$. $D^3(z)$ is a unit element in $A/M[z]$ for any maximal ideal $M$ of $A$. Let $A/M = GF(2)$. Then $A[x]/M[x] \cong GF(2)[x]$ for any $\sigma$-generator $x$ of $T/A$. If $x^2+x = 1$ in $GF(2)[x]$, then it coincides with $GF(4)$, and hence we assume that $x^2+x = 0$. Since $1 = D^3(z) = D(D^2(z))$ in $A/M[z]$, we have

$$D^2(z) = x+\varepsilon \text{ where } \varepsilon = 0 \text{ or } 1 \cdots\cdots\cdots(2)$$

Since $(x+\varepsilon)^2 = x+\varepsilon$, $D(D(z^2)) = D(D(z)^2) = (D^2(z))^2 = D^2(z)$. This and (2) imply $D(D(z^2)+D(z)) = 0$ and hence

$$z^2+z = \begin{cases} x+\varepsilon' \\ \varepsilon' \text{ where } \varepsilon' = 0 \text{ or } 1. \end{cases} \cdots\cdots\cdots(3)$$

But $z^2+z = \varepsilon'$ is also a contradiction by the same reason as in the case (i), and so $z^3 = z^2+zx+z\varepsilon'$. Consequently, we have

$$\begin{aligned} D^2(z^3) &= D^2(z^2)+D^2(z)x+D^2(z)\varepsilon' \\ &= x+\varepsilon+(x+\varepsilon)x+(x+\varepsilon)\varepsilon' \\ &= x(\varepsilon+\varepsilon')+\varepsilon(1+\varepsilon'). \end{aligned}$$

(a) case $\varepsilon+\varepsilon' = 1$ : $D^3(z^3) = x+\varepsilon$, and hence $D^2(z^3+z) = 0$ by (2). Thus

$$z^3+z = \begin{cases} x+\varepsilon'' \\ \varepsilon'' \text{ where } \varepsilon'' = 0 \text{ or } 1. \end{cases} \quad z^3+z = \varepsilon''$$

is a contradiction. While if $z^3+z = x+\varepsilon''$, then $z^3+z^2 = z^3+z+z^2+z = 0$ or 1 and this is also a contradiction.

(b) case $\varepsilon+\varepsilon' = 0$ : Since $0 = \varepsilon+\varepsilon' = \varepsilon(\varepsilon+\varepsilon') = \varepsilon+\varepsilon\varepsilon' = \varepsilon(1+\varepsilon')$, we have $D^2(z^3) = 0$ and so $z^3$ must be $x+\varepsilon''$ ($\varepsilon''$ is 0 or 1). Then, by (3), we have a contradiction that $z^3+z^2+z = 0$ or 1.

**4. The case of a semi-primary ring.** In this section, we assume that $A$ is a ring such that $A/J(A)$ is artinian. Hence we may assume that there exists a set of maximal ideals $\mathcal{M} = \{M_i ; i = 1,2,\cdots,n\}$ of $A$ such that $J(A) = \bigcap_{i=1}^{n} M_i$. By $\mathcal{M}_1$(resp. $\mathcal{M}_2$) we denote the set of all $M_i \in \mathcal{M}$ such

that $A/M_i = GF(2)$ (resp. $A/M_i \neq GF(2)$).

**Theorem 3.** *$B$ has a primitive element if and only if $A/M[x] = GF(4)$ for any $M \in \mathcal{M}_1$ and a $\sigma$-generator of $T/A$.*

*Proof.* Let $B$ have a primitive element $z$ such that $z^4 = \sum_{i=0}^{3} a_i z^i$ $(a_i \in A)$.

Case I $D^3(z) \in J(A)$: We can see that $a_3 \in J(A)$ and $D^3(z^3) \notin M$ for any maximal ideal $M$ of $A$ by the same reason as in that of Lemma 2, and hence $D^3(z^3)$ is a unit element. For $M \in \mathcal{M}_1$, we can see $A/M[x] = GF(4)$ for any $\sigma$-generator $x$ of $T/A$ by Lemma 2 [See, case (i)].

Case II $D^3(z) \notin J(A)$: There exists $M \in \mathcal{M}$ such that $D^3(z) \notin M$. If $M \in \mathcal{M}_1$, then $A/M[x] = GF(4)$ for any $\sigma$-generator $x$ of $T/A$ by Lemma 2. Further, for any $M \in \mathcal{M}_1$ such that $D^3(z) \in M$, we have $D^3(z^3) = 1$ in $A/M$ by the same reason as in that of Lemma 2. Thus we obtain $A/M[x] = GF(4)$ again by Lemma 2.

Conversely, assume that $A/M[x] = GF(4)$ for any $M \in \mathcal{M}_1$ and a $\sigma$-generator $x$ of $T/A$. Let $x^2+x = a \in A$ for a $\sigma$-generator $x$ of $T/A$. Since $A/J(A) = A/M_1 \oplus A/M_2 \oplus \cdots\cdots \oplus A/M_n$, we may put $a = a_1+a_2+\cdots+a_n$ in $A/J(A)$ where $a_i \in A/M_i$. If $A/M_i = GF(2)$, we may put $a_i = 1$, and if $a_j \in A/M_j \neq GF(2)$, then there exists $c_j \in A$ such that ${c_j}^2+c_j+a_j$ is a unit element in $A/M_j$. Thus we can choose a $\sigma$-generator $x$ of $T/A$ such that $x^2+x = u$ is a unit element in $A/J(A)$. But, for this $x$, $x^2+x$ must be a unit element in $A$.

Let $A$ be a local ring with the unique maximal ideal $M$. Then $B$ is a local ring if and only if $T = A[x]$ is a local ring, and $T$ is a local ring if and only if $M[x]$ is the unique maximal ideal of $T$ [2, Lemma 1.4 and Theorem 1.8]. Combining this with Lemma 2, we have the following

**Corollary 4.** *If $B$ is a local ring then $B$ has a primitive element.*

*Proof.* Since $A[x] = A \oplus xA$ is a local ring for a $\sigma$-generator $x$ of $T/A$, $M[x] = M \oplus xM$ is the unique maximal ideal of $A[x]$. If $x^2+x \in M$ then $M \oplus xA$ becomes a proper ideal of $A[x]$ which contains $M[x]$. This contradicts to the maximality of $M[x]$. Thus $x^2+x$ must be a unit element.

**Remark**: The converse of Corollary 4 is not true. For let $A = GF(2)$. Then $A[X]/(X^2+X+1) = A[x] = GF(4)$, and $B = GF(4)[Y]/(Y^2+Y) \cong GF(4) \oplus GF(4)$ has a primitive element since $x^2+x = 1 \in U(A)$.

## REFERENCES

[1] K. KISHIMOTO : On relative sequences of homomorphisms and Galois extensions of rings, to appear in Math. J. Okayama Univ.

[2] Y. MIYASHITA : Finite outer Galois theory of non-commutative rings, J. Fac. Sci. Hokkaido Univ., 19 (1966), 114−134.

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

DEPARTMENT OF MATHEMATICS
SHINSHU UNIVERSITY
MATSUMOTO 390, JAPAN

(*Received May 2, 1986*)