JOUR. FAC. SCI. SHINSHU UNIV., Vol. 7. pp. 7–12, June 1972

Note on Quadratic Extensions of Rings II

By KAZUO KISHIMOTO

Department of Mathematics, Faculty of Science,
Shinshu University
(Received April 30 1972)

Introduction. Throughout the present paper B will mean a ring with an identity 1, $A = B + xB = B + Bx \supsetneqq B$ an extension ring of B with an identity coinciding with the identity of B.

As an extension of result of [5], T. Nagahara gave characterizations for a commutative ring A to be a Galois extension over B ([7]). The main purpose of this note is to extend the above Nagahara's result to some non commutative case.

Let $A = B \oplus xB = B \oplus Bx$, $dx = xd_1 + d_0$ for each $d \in B$ (d_1, $d_0 \in B$). Then the map $\rho : d \longrightarrow d_1$ is an automorphism of B and the map $D : d \longrightarrow d_0$ is a ρ-derivation of B. Further, if $x^2 = xb_1 + b_0$ for some $b_1, b_0 \in B$, the map σ of A defined by $\sigma(xb' + c') = (xc + b)b' + c'(b, c, b', c' \in B)$ is a B ring epimorphism of A if and only if there hold followings

(I) c is a unit element of Z, the center of B.

(II) $(1-c)D(d) = db - b\rho(d)$ for each $d \in B$.

(III) $cb_1 = c(\rho(c)b_1 + D(c) + b + \rho(b))$.

(IV) $bb_1 + b_0 = c(\rho(c)b_0 + D(b)) + b^2$.

For if σ is a B-homomorphism, we obtain

$\sigma(dx) = d(\sigma(x)) = d(xc+b) = x\rho(d)c + D(d)c + db$ and $\sigma(dx) = \sigma(x\rho(d) + D(d)) = xc\rho(d) + b\rho(d) + D(d)$.

Hence $c \in Z$. Moreover, if σ is an epimorphism, $cB = B$ implies that c is a unit element. Under the assumption that $c \in U(Z)$, the validity of (II)-(IV) is equivalent to that σ is a homomorphism of A by [2].

Now, we set the condition*) as following :

*) If M is a right, as well as left, free A-module of finite rank, then the rank is unique[1].

In all that follows, we assume that A satisfies *).

1. Necessary and sufficient conditions for A to be Galois over B.

We shall begin our study from the following

Lemma 1. *Let A/B be a Galois extension with a Galois group $\mathfrak{G}$. Then*

1) If A is commutative, A satisfies *).

(a) $\mathfrak{G}$ *is of order* 2.

(b) *For* $\sigma(\neq 1) \in \mathfrak{G}$, $x - \sigma(x)$ *is inversible.*

(c) $\{1, x\}$ *is a free* B*-basis for* A[2].

Proof. Let $\sigma(\neq 1) \in \mathfrak{G}$. We suppose that $x - \sigma(x)$ is not right inversible. Then there exists a proper right ideal $\mathfrak{r}$ of A such that $\mathfrak{r} \ni x - \sigma(x)$. On the other hand, since $A = B \oplus xB$, $(1 - \sigma)A = \{y - \sigma(y) | y \in A\}$ is contained in $\mathfrak{r}$. Let $\{x_1, x_2, \cdots, x_n;\ y_1, y_2, \cdots, y_n\}$ be a $\mathfrak{G}$-Galois coordinate system for A/B with $\sum_{i=1}^{n} \tau(x_i)y_i = \delta_{1,\tau}$ for each $\tau \in \mathfrak{G}$. Then we have a contradiction $1 = \sum_{i=1}^{n} (x_i - \sigma(x_i))y_i \in \mathfrak{r}$. Thus $x - \sigma(x)$ is right inversible. Since $A = B \oplus Bx$, the same arguments enable us to see that $x - \sigma(x)$ is left inversible.

Now, let $c' + xb' = 0$ (resp. $c' + b'x = 0$) for some $c', b' \in B$. Then $0 = (c' + xb') - \sigma(c' + xb') = (x - \sigma(x))b'$ (resp. $(c' + b'x) - \sigma(c' + b'x) = b'(x - \sigma(x))$ yields $c' = b' = 0$.

Regarding that $A \otimes_B A$ is a left (resp. right) A-module by $a(b' \otimes c') = ab' \otimes c'$ (resp. $(b' \otimes c')a = b' \otimes c'a$) for each $a, b', c' \in A$, $A \otimes_B A = A \otimes_B (B \oplus Bx) = A \oplus A \otimes_B Bx = A(1 \otimes 1) + A(1 \otimes x)$ (resp. $A \otimes_B A = (B \oplus xB) \otimes_B A = A \oplus xB \otimes_B A = (1 \otimes 1)A + (x \otimes 1)A$) is a free A-module of rank 2. On the other hand, (b), (c), (d) and (e) of [1], Theorem 1.3 are equivalent without assumptions that A and B are commutative[3]. Therefore $A \otimes_B A$ is isomorphic to a direct sum of $|\mathfrak{G}|$-copies of A. Consequently we have $|\mathfrak{G}| = 2$ by *).

Theorem 1.[4] *Let* A *have a relation* $x^2 = xb_1 + b_0$ *for some* $b_0, b_1 \in B$. *Then* A/B *is a Galois extension if and only if there hold that*

(a) $\{1, x\}$ *is a free* B*-basis for* A.

(b) *there exists an element* b *of* B *satisfying*

(i) $2D(d) = db - b\rho(d)$,

(ii) $b + \rho(b) = 2b_1$,

(iii) $bb_1 = b^2 - D(b)$,

(iv) $2x - b$ *is inversible, where* ρ, D *are maps of* B *defined by* $d \longrightarrow d_1$, $d \longrightarrow d_0$ *respectively for each* $d \in B$ *with* $dx = xd_1 + d_0$ $(d_1, d_0 \in B)$.

Moreover, if A *is commutative* (i), (ii) *and* (iii) *of* (b) *are needless and* (iv) *can be replaced* (iv′) $2x - b_1$ *is inversible.*

Proof. Let A/B be a Galois extension. Then by Lemma 1, $\mathfrak{G}$, the group of B-automorphisms of A is $\{1, \sigma\}$ and $\{1, x\}$ is a free B-basis for A.

Let $\sigma(x) = xc + b$. Then $B \ni x + \sigma(x) = x(1+c) + b$ implies $c = -1$, and hence, $x - \sigma(x) = 2x - b$ is inversible by Lemma 1. The validity of (i), (ii) and (iii) of (b) is a direct consequence of (II), (III) and (IV).

2) A free basis means a free right, as well as, left basis.

3) Needless to say a B-algebra homomorphism of [1] replace to a B-module homomorphism.

4) Cf. [7], Lemma 1.

Conversely, assume that A satisfy (a) and (b). Then by (a) and (i), (ii) and (iii) of (b), the map σ defined by $xb' + c' \longrightarrow (-x + b)b' + c'$ ($b', c' \in B$) is a B-automorphism of A. Let $\sigma(xb' + c') = xb' + c'$. Then $(x - \sigma(x))b' = (2x - b)b' = 0$ implies $b' = 0$ by (iv) of (b). Thus $A^{\sigma} = B$. Since $(x - \sigma(x))^{-1}x - (x - \sigma(x))^{-1}\cdot \sigma(x)\cdot 1 = 1$ and $(x - \sigma(x))^{-1}\sigma(x) - (x - \sigma(x))^{-1}\sigma(x)\sigma(1) = 0$, A/B is a Galois extension.

Let A be commutative. Then we have $bb_1 = b^2$ by (iii) of (b), and the map $\eta : xb' + c' \longrightarrow (-x + b_1)b' + c'$ is a B-automorphism of A by (I), (II), (III) and (IV). If $\eta = 1$ then $x = \eta(x) = -x + b_1$, and hence $2x = b_1 = 0$. On the other hand, since $2x - b$ is inversible by (iv) of (b), we can see that b is inversible. But, this contradicts to $b^2 = bb_1$. Thus $\eta = \sigma(\neq 1)$ and $x - \sigma(x) = 2x - b_1$ is inversible by Lemma 1 (*b*).

Let T be a ring, P an automorphism of T, E a P-derivation of T. Then by $T[X; P, E]$ we denote a ring of polynomials $\{\sum X^i t_i \mid t_i \in T\}$ whose multiplication is defined by the distributive laws and the rule $tX = XP(t) + E(t)$ for each $t \in T$. A monic polynomial $f(X) \in T[X; P, E]$ is called *a non-vanishing polynomial* if the right ideal $f(X)T[X; P, E]$ is a two-sided ideal of $T[X; P, E]$, and, an element $t \in T$ is called *a root* of $f(X)$ if $f(t) = 0$ and $X - t$ is non-vanishing[5].

Corollary 1. *Let A/B be a Galois extension with $x^2 = xb_1 + b_0$ ($b_1, b_0 \in B$) and $dx = x\rho(d) + D(d)$ for each $d \in B$. Then the following conditions are equivalent :*

(a) $2\cdot 1 = 0$

(b) *$x - \sigma(x)$ is an element of B.*

(c) *there exists a free B-basis $\{1, y\}$ for A with $\sigma(y) = y - 1$.*

(d) *there exists a free B-basis $\{1, w\}$ for A such that w and $w + 1$ are roots of the polynomial $X^2 - X - (w^2 - w) \in A[X; I_w]$.*[6]

Moreover, if A has no proper central idempotents, then the only roots of the polynomial $X^2 - X - (w^2 - w)$ given in (d) are w and $w + 1$.

Proof. (a)$\longrightarrow$(b). Let $2\cdot 1 = 0$. Then $x + \sigma(x) = x - \sigma(x)$ means that $x - \sigma(x) \in B$.

(b)$\longrightarrow$(c). Let $b = x - \sigma(x) \in B$. Then, by Lemma 1, b is inversible. Hence if we set $y = xb^{-1}$, $\{1, y\}$ is a free B-basis for A and $\sigma(y) = (x-b)b^{-1} = y - 1$.

(c)$\longrightarrow$(d). Since $dy - yd \in B$ for each $d \in B$, $dy = yd + D(d)$, where D is a derivation of B. Now we shall show that $X^2 - X - (y^2 - y) \in A[X; I_y]$ is the requested polynomial. $X(X - y) = (X - y)X$, $X(X - (y + 1)) = (X - (y + 1))X$ and $d(X - y) = Xd - dy + D(d) = (X - y)d$, $d(X - (y + 1)) = (X - (y + 1))d$ show that y and $y + 1$ are roots of $X^2 - X - (y^2 - y)$.

(d)$\longrightarrow$(a). Let $\{1, w\}$ be a free B-basis for A such that w and $w + 1$ are roots of $X^2 - X - (w^2 - w)$. Then $0 = (w + 1)^2 - (w + 1) - (w^2 - w) = 2w$ shows that

5) Cf. [4].

6) I_w means the inner derivation generated by w.

$2\cdot 1 = 0$.

Let A be a ring without proper central idempotents, and let z be a root of $X^2 - X - (w^2 - w)$ given in (d). Then $X(X-z) = (X-z)X = X(X-z) - D(z)$ and $d(X-z) = (Xd - dz + D(d)) = (X-z)d$ for each $d \in B$. Hence we have $D(z) = zw - wz = 0$ and $dw - wd = dz - zd$ respectively. Hence $w + z \in V$, the centralizer of B in A. Since $zw = wz$, we have $w + z \in C$, that is, $z = w + c$ for some $c \in C$. Noting that $2\cdot 1 = 0$, $0 = z^2 - z - (w^2 - w) = (z+w)^2 - (z+w) = c^2 + c$, c is a central idempotents, and hence $c = 0$ or $c = 1$.

Theorem 2. *Let A/B be a Galois extension. Then $2\cdot 1$ is inversible if and only if there exists an element $y \in A$ such that $A = B \oplus yB = B \oplus By$, $y^2 \in B$ and $y\sigma(y) = \sigma(y)y$ for each $\sigma \in \mathfrak{G} = \mathfrak{G}(A/B)$, and if this is the case, y is inversible.*

Proof. Let $2\cdot 1$ be inversible, and let $y = (x - \sigma(x))/2$. Then y is inversible, $\sigma(y) = -y$ and $y^2 \in U(B)$. Since $y^{-1}/2\cdot y + y^{-1}/2\cdot y\cdot 1 = 1$ and $y^{-1}/2\cdot\sigma(y) + y^{-1}/2\cdot y\cdot\sigma(1) = 0$, $B[y] = B + yB = B + By = A$ by [6, Theorem 2.3]. By Lemma 1, $\{1, y\}$ is a free B-basis for A.

Conversely, assume that there exists an element $y \in A$ such that $A = B \oplus yB = B \oplus By$, $y^2 \in B$ and $y\sigma(y) = \sigma(y)y$ for each $\sigma \in \mathfrak{G}$. Then $y(y + \sigma(y)) = y^2 + y\sigma(y) \in B$ yields $y + \sigma(y) = 0$, and hence $\sigma(y) = -y$. Consequently, we can see that $2y$ is inversible by Theorem 1. Thus $2\cdot 1$ and y are inversible.

Corollary 2. *Let A be a Galois extension with $x^2 \in B$, and $dx = x\rho(d) + D(d)$ for each $d \in B$. Then the following conditions are equivalent :*

(a) *$x\sigma(x) = \sigma(x)x$ for each $\sigma \in \mathfrak{G}$.*

(b) *$D = 0$ and $2\cdot 1$, x are inversible.*

(c) *$\rho = \tilde{x}^{-1}|B$ and $2\cdot 1$ is inversible.*

(d) *ρ can be extended to an automorphism P of A with $P(x) = x$, x and $-x$ are distinct roots of $X^2 - x^2$ of $A[X; P]$ in A.*

Proof. Firstly, we shall note that if $\sigma(x) + x = b$ for some $b \in B$, then b satisfies $2D(d) = db - b\rho(d)$ for each $d \in B$ (Theorem. 1 (b), (i)).

(a) ⟶ (b). As is shown in the proof of the sufficiency of Theorem 2, $\sigma(x) = -x$, $2\cdot 1$ and x are inversible. Since $\sigma(x) + x = 0$, we have $D(d) = d(b/2) - (b/2)\rho(d) = 0$ for each $d \in B$,

(b) ⟶ (c). This implication is evident.

(c) ⟶ (d). If $\rho = \tilde{x}^{-1}|B$ then $P = \tilde{x}^{-1}$ is an automorphism of A with $P(x) = x$, and $X(X \pm x) = (X \pm x)X$, $d(X \pm x) = (X \pm x)\rho(d)$ are clear.

(d) ⟶ (a). Since $d(X - x) = (X - x)\rho(d)$ for each $d \in B$, $\rho = \tilde{x}^{-1}|B$. Hence the map σ defined by $\sigma(xb' + c') = -xb' + c'$ $(b', c' \in B)$ is a B-automorphism of A. Thus $x\sigma(x) = \sigma(x)x$ for each $\sigma \in \mathfrak{G}$.

Let A be a ring without proper central idempotents, and let z be a root of $X^2 - x^2$ given in (d). Then $X(x - z) = (X - z)X$ and $d(X - z) = (X - z)\rho(d)$ for each

$d \in B$. Hence we have $xz = zx$, $dz = z\rho(d)$ respectively. Hence $z = xc$ for some $c \in U(C)$ with $c^2 = 1$. Since C is a commutative ring without proper idempotents, $c = \pm 1$ by [3, Corollary 2.5].

The following will be easily seen from Theorem 2 and Corollary 2.

Corollary 3.[7] *Let A have a relation $x^2 \in B$. Then A/B is a Galois extension with $x\sigma(x) = \sigma(x)x$ for each $\sigma \in \mathfrak{G}$ if and only if there holds that*

(a) *$\{1, x\}$ is a free B-basis for A.*

(b) *$2 \cdot 1$ and x are inversible.*

(c) *$D = 0$ where D is the map defined by $dx = x\rho(d) + D(d)$ foreach $d \in B$.*

2. Structure of the centralizer.

In the rest, we shall determine the structure of the centralizer of a quadratic extension.

Let $A = B \oplus xB = B \oplus Bx$ be a $\mathfrak{G} = \{1, \sigma\}$ Galois extension, and let V be the centralizer of B in A. Then we may assume that $x^2 \in U(B)$, $\sigma(x) = -x$ and $dx = x\rho(d)$ for some automorphism ρ of B if $2 \cdot 1$ is inversible for each $d \in B$, and $dx = xd + D(d)$, $\sigma(x) = x + 1$ for some derivation D of B if $2 \cdot 1 = 0$ for each $d \in B$.

Theorem 4. *Let $2 \cdot 1$ be inversible or $2 \cdot 1 = 0$. Then $V = C[Z]$, the composite of the center C of A and the center Z of B. More precisely, $V = C \oplus Z_\sigma$,* where $Z_\sigma = Z \cap J_\sigma$ and $J_\sigma = \{a \in A \mid ay = \sigma(y)a$ *for each* $y \in A\}$.

Proof. It is evident that $V = Z$ if $\sigma = \tilde{v}$ for some $v \in V$. Hence we consider the case $\sigma \neq \tilde{v}$ for each $v \in U(V)$. Firstly, we note that $V = C \oplus J_\sigma$.

case $2 \cdot 1 = 0$. Let $v = xb + c$ $(b, c \in B)$. Then $dv = vd$ for each $d \in B$ imply $xdb + D(d)b + dc = xbd + cd$ and hence

$$b \in Z \tag{1}$$

and $D(d)b = cd - dc$.

Thus,

$$D(b)b = 0 \tag{2}$$

Next, let us assume that $v \in J_\sigma$. Then $J_\sigma \ni \sigma(v) - v = b$ yields $bx = \sigma(x)b = (x + 1)b$, and hence

$$D(b) = b \tag{3}$$

By (2) and (3), we have $b^2 = 0$. Then $1 + b \in U(Z)$ by (1).

On the other hand, since $\sigma \neq \tilde{v}$ for each $v \in U(V)$, $U(Z) \subseteqq C$. Thus we obtain $0 = D(1 + b) = D(b) = b$. Therefore $v = c \in B \cap V = Z$ means that $J_\sigma \subseteqq Z$. Thus

7) Cf. [7], Lemma 2.

$V = C \oplus Z_\sigma = C[Z]$.

case 2•1 is inversible. Let $v = xb + c(b, c \in B)$. Then $dv = vd$ for each $d \in B$ implies $x\rho(d)b + dc = xbd + cd$, and hence

$$\rho(d)b = bd, \quad c \in Z \tag{1}$$

Thus

$$\rho(b)b = b^2 \tag{2}$$

Next, let us assume that $v \in J_\sigma$. Then $J_\sigma \ni 1/2(\sigma(v) - v) = xb$ and $xbx = x^2\rho(b) = \sigma(x)xb = -x^2b$, and hence

$$\rho(b) = -b \tag{3}$$

By (2) and (3), we have $\rho(b)b = b^2 = 0$. Thus $(xb)^2 = x^2\rho(b)b = 0$, and hence $1 - xb \in U(V)$. Since $U(V) \subseteqq U(C)$, we have $xb \in J_\sigma \cap C = 0$. Consequently, $V = C \oplus Z_\sigma = C[Z]$.

References

[1] S. U. CHASE, D. K. HARRISON and A. ROSENBERG : Galois theory and Galois cohomology of commutative rings, Mem. Amer. Math. Soc., No. 52 (1965).

[2] P. M. COHN : Quadratic extensions of skew fields, Proc. London Math. Soc., 11 (1961), 531–556.

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

[4] K. KISHIMOTO : Zeros of polynomials and Galois extensions of simple rings, J. Fac. Sci. Shinshu Univ., 2 (1967), 117–122.

[5] ——— : Note on quadratic extensions of rings, J. Fac. Sci. Shinshu Univ., 5 (1970), 25–28.

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

[7] T. NAGAHARA : A quadratic extension, Proc. Jap. Acad., 47 (1971), 6–7.