A SEMIGROUP OF ISOMORPHISM CLASSES OF SOME QUADRATIC EXTENSIONS OF RINGS

Takasi NAGAHARA (Okayama University)

Throughout this paper, B will mean a (non-commutative) ring with identity element 1 which has an automorphim ρ . By $B[X;\rho]$, we denote the ring of all polynomials $\sum_{i} X^{i}b_{i}$ ($b_{i} \in B$) with an indeterminate X whose multiplication is given by bX = Moreover, by $B[X;\rho]_2$, we denote the subset of $B[X;\rho]$ of all polynomials $f = X^2 - Xa - b$ with $fB[X;\rho] =$ B[X; ρ]f. If $x^2 - Xa - b \in B[X;\rho]_2$ then $\rho(b) = b$. By $B[X;\rho]_{(2)}$, we denote the subset $\{x^2 - Xa - b \in B[X;\rho]_2 \mid$ $\rho(a) = a$. Now, for f, $g \in B[X; \rho]_2$, if the factor rings $B[X;\rho]/fB[X;\rho]$ and $B[X;\rho]/gB[X;\rho]$ are B-ring isomorphic then we write f ~ g. Clearly the relation ~ is an equivalence relation in $B[X;\rho]_2$. By $B[X;\rho]_2^{\sim}$ (resp. $B[X;\rho]_{(2)}^{\sim}$), denote the set of equivalence classes of $B[X;\rho]_2$ (resp. $B[X;\rho]_{(2)}$) with respect to the relation ~. Moreover, for f \in B[X; ρ]₂, if the factor ring B[X; ρ]/fB[X; ρ] is separable (resp. Galois) over B then f will be called to be separable (resp. Galois). As is well known, any Galois polynomial in $B[X;\rho]_2$ is separable. By [6, Th.1], any separable polynomial of $B[X;\rho]_2$ is contained in $B[X;\rho]_{(2)}$. For $f = X^2 - Xa - b$ \in B[X; ρ]₂, we denote $a^2 + 4b$ by $\delta(f)$, which will be called the discriminant of f. We shall use here the convention: integer). If $X^2 - Xa - b \in B[X; \rho]_2$ then $a \in B(\rho)$, $b \in B(\rho^2)$,

 $\rho(b)=b$ (, and conversely). Clearly $a^2+4b\in B(\rho^2)$. An element a of $B(\rho^n)$ is said to be π -regular if there exists an element c in B and an integer $t\geq 0$ such that $a^t=a^{t+1}c$.

Now, in [1], K. Kitamura studied free quadratic extensions of commutative rings and its isomorphism classes. In his study, the set of polynomials of degree 2 plays an important rôle. Indeed, [1] is a study on $B[X;\rho]_2$ and $B[X;\rho]_2^{\sim}$ where B is commutative and $\rho = 1$.

In [2], K. Kishimoto studied the sets $B[X;\rho]_{(2)}$ and $B[X;\rho]_{(2)}$ in case $B[X;\rho]_{(2)}$ contains a Galois polynomial χ^2 - b (and hence 2b is inversible in B).

In [5], the present author studied the sets $B[X;\rho]_{(2)}$ and $B[X;\rho]_{(2)}^{\sim}$ in case $B[X;\rho]_{(2)}$ contains a Galois polynomial X^2 - Xa - b (and hence the discriminant a^2 + 4b is inversible in B). The study contains a generalization of [2]. Moreover, in [1], [2] and [5], it was shown that $B[X;\rho]_{(2)}^{\sim}$ forms an abelian semigroup with identity element under some composition, and the structure of this semigroup was studied to characterize the separable polynomials in $B[X;\rho]_{(2)}^{\sim}$.

In this paper, we shall study the separable polynomials in $B[X;\rho]_{(2)}$ and the structure of $B[X;\rho]_{(2)}^{\sim}$ in case $B[X;\rho]_{(2)}^{\sim}$ contains a separable polynomial whose discriminant is π -regular, and we shall show that $B[X;\rho]_{(2)}^{\sim}$ forms also an abelian semigroup with identity element under some composition such that for $C \in B[X;\rho]_{(2)}^{\sim}$ and $f \in C$, C is inversible in this semigroup if and only if f is separable. Moreover, this semigroup will be studied in various ways.

In the rest of this paper, Z will mean the center of B. Moreover, U(B) denotes the set of inversible elements in B, and for any subset S of B, U(S) denotes the intersection of S and U(B). Clearly, U(Z) coincides with the set of inversible elements in Z. Further, for any subset S of B, we use the following conventions: $S^{\rho} = \{s \in S \mid \rho(s) = s\};$ $\rho^n|_S =$ the restriction of ρ^n to S (where n is any integer). By [5, (2, xvii)] and [6, Th. 1], we see that if B[X; ρ]₂ contains a separable polynomial then $\rho^2|_Z$ is identity. As is easily seen, if an element a of B(ρ^n) $^{\rho}$ is π -regular then there exists an integer $n \ge 0$ and an idempotent ϵ of Z^{ρ} such that $a^n = \epsilon$ B. This idempotent will be denoted by e(a). First, we shall prove the following

Lemma 1. Let 2 be nilpotent, and assume that $B[X;\rho]_2$ contains a separable polynomial X^2 - b. Then, b \in U(B), and there exists an element $z \in Z$ such that $z + \rho(z) = 1$. Moreover, $B(\rho) = \{0\}$, $B(\rho^2) = bz$, $B(\rho^2)^{\rho} = bz^{\rho}$, and $B[X;\rho]_2 = \{x^2 - v \mid v \in B(\rho^2)^{\rho}\}$.

Proof. The first assertion is a direct consequence of [5, Lemma 2.3] and [6, Th.1]. Now, since 2 is nilpotent, there exists an integer n>0 such that $2^n=0$. Let $u\in B(\rho)$. Then, we have $u=u(z+\rho(z))^n=u(z+\rho(z))(z+\rho(z))^{n-1}=2zu(z+\rho(z))^{n-1}=2^nz^nu=0$. The rest assertion will be easily seen.

Next, we shall prove the following

Lemma 2. Let ϵ be an idempotent in Z^{ρ} such that $\epsilon 2^n = 2^n$ for some integer n > 0. Let f be an polynomial in $B[X; \rho]_2$ such that ϵf is Galois in $\epsilon B[X; \rho]$ and $(1 - \epsilon) f$ is separable in $(1 - \epsilon) B[X; \rho]$. Then $\delta(f)$ is π -regular, $e(\delta(f)) B > \epsilon B$, and $(1 - e(\delta(f))) B[X; \rho]_2 = \{(1 - e(\delta(f))) (X^2 - v) \mid v \in B(\rho^2)^{\rho}\}$.

Proof. By [6, Th.2], we have $\varepsilon B = \varepsilon \delta(f) B$. Moreover, f is separable, and so, $f \in B[X;\rho]_{(2)}$. We write here $f = X^2 - Xa - b$. Then, by [5, Lemma 2.2 (2, xix)], we have $a = \delta(f)sa = \delta(f)^{n+1}s^{n+1}a$ for some s in B. Since $\varepsilon 4^n = 4^n$, it follows that $(1-\varepsilon)\delta(f)^n B = (1-\varepsilon)(ac + 4^n b^n) B = (1-\varepsilon)ac B = (1-\varepsilon)\delta(f)^{n+1} B$, and whence, $\delta(f)^n B = \varepsilon \delta(f)^n B + (1-\varepsilon)\delta(f)^n B = \varepsilon \delta(f)^{n+1} B + (1-\varepsilon)\delta(f)^{n+1} B = \delta(f)^{n+1} B$. Thus $\delta(f)$ is π -regular, and $e(\delta(f))B = \delta(f)^n B = \varepsilon \delta(f)^n B = \varepsilon \delta(f) B = \varepsilon B$. Moreover, noting $e(\delta(f))a = a$, the other assertion will be easily seen from the result of Lemma 1.

Corollary 3. Let 2 be $\pi\text{-regular.}$ If $f\in B[X;\rho]_2$ is separable then $\delta(f)$ is $\pi\text{-regular.}$

Proof. Let $f = X^2 - Xa - b$ be a separable polynomial in $B[X;\rho]_2$. Since any inversible element of B is π -regular in B, we may assume that $\delta(f)$ is not inversible in B. If e(2) = 1 then 2 is inversible in B, and so, $\delta(f)$ is inversible in B by [6, Th.3]. Hence $e(2) \neq 1$. First, we assume that e(2) = 0. Then $2^n = 0$ for some integer n > 0. By [5, Lemma 2.2 (2, xix)], we have $a = \delta(f)^n ta = a^2 r$ for some t, $r \in B$. Hence a is π -regular, and e(a) is in Z^ρ .

Since e(a)a is inversible in e(a)B, so is $e(a)\delta(f)$ in e(a)B. Hence, it follows from [6, Th.2] that e(a)f is Galois in $e(a)B[X;\rho]$. Moreover, $1-e(a)\neq 0$, and (1-e(a))f is separable in $(1-e(a))B[X;\rho]$. Therefore, $\delta(f)$ is π -regular by Lemma 2. Next, we assume that $e(2)\neq 0$. Then $e(2)\in \mathbb{Z}^\rho$, $e(2)B=2^nB$, and $e(2)2^n=2^n$ for some integer n>0. Noting that e(2)2 is inversible in e(2)B, e(2)f is Galois in $e(2)B[X;\rho]$ by [6, Th.2]. Moreover, (1-e(2))f is separable in $(1-e(2))B[X;\rho]$. Hence by Lemma 2, $\delta(f)$ is π -regular.

Now, we shall prove the following theorem which is one of our main results.

Theorem 4. Assume that $B[X;\rho]_2$ contains a separable polynomial f whose discriminant is π -regular. Set $\varepsilon = e(\delta(f))$ and $\omega = 1 - \varepsilon$. Then, $\omega 2$ is nilpotent, and $\omega B[X;\rho]_2 = \{\omega(X^2 - v \mid v \in B(\rho^2)^{\rho}\}$. Moreover, $g = X^2 - Xu - v \in B[X;\rho]_2$, the following conditions are equivalent.

- (a) g is separable.
- (b) $\delta(g)$ is π -regular, $e(\delta(g)) = \epsilon$, and $\omega B = \omega v B$.
- (c) $\varepsilon B = \varepsilon \delta(g) B$, and $\omega B = \omega v B$.

Proof. Let $f = X^2 - Xa - b$. If $\epsilon = 1$ then $\delta(f)$ is inversible in B, and whence, the assertion holds obviously. Now, we assume that $\epsilon = 0$. Then, by [5, Lemma 2.2 (2, xix)], 2 is nilpotent and a = 0. Hence by Lemma 1, we ahve $B[X;\rho]_2 = \{X^2 - v \mid v \in B(\rho^2)^{\rho}\}$. Hence by [5, Lemma 2.3], it will be easily seen that (a), (b) and (c) are equivalent.

Next, we shall consider the case $\varepsilon \neq 1$, 0. Since $\varepsilon B =$ $\delta(f)^n B$ for some integer n > 0, it follows that $\rho(\epsilon) = \epsilon$, and $4^n = \delta(f)^n r = \epsilon \delta(f)^n r = \epsilon 4^n$ for some r in B ([5, Lemma 2.2]). Moreover, since $\epsilon\delta(f)$ is inversible in ϵB , ϵf is Galois in $\epsilon B[X; \rho]$. Obviously, ωf is separable in $\omega B[X;\rho]$. Hence by Lemma 2, we have $\omega B[X;\rho]_2 =$ $\{\omega(X^2 - v) \mid v \in B(\rho^2)^{\rho}\}.$ Now, let $g = X^2 - Xu - v \in B[X; \rho]_2.$ Assume (a). Then, since εg is separable in $\varepsilon B[X; \rho]$, it follows from [6, Th.2] that εg is Galois in $\varepsilon B[X; \rho]$. Moreover, ωg is separable in $\omega B[X; \rho]$. Hence by Lemma 2, $\delta(g)$ is π -regular, and $e(\delta(g))B > \varepsilon B = e(\delta(f))B$. By a similar way, we have $e(\delta(g))B \subset e(\delta(f))B$. This implies $e(\delta(g)) = \varepsilon$. Since $\omega g = \omega(x^2 - v)$ is separable in $\omega B[X; \rho]$, ωv is inversible in ωB by [5, Lemma 2.3], that is, ωB = ωvB. Thus we obtain (b). Assume (b). Then εB = e(δ(g))B = $\delta(g)^{m}B$ for some integer m > 0. This shows that $\varepsilon B = \varepsilon \delta(g)B$. Finally, assume (c). Since $\varepsilon B = \varepsilon \delta(g) B$, $\varepsilon \delta(g)$ is inversible in ϵB . Hence ϵg is Galois in $\epsilon B[X;\rho]$ by [6, Th.2], and so, ϵg is separable in $\epsilon B[X; \rho]$. Moreover, ωv is inversible in ωB . Since ωf is separable in $\omega B[X;\rho]$, there exists an element z in ωZ with $z + \rho(z) = \omega$. Hence $\omega g = \omega(X^2 - v)$ is separable in $\omega B[X; \rho]$ by [5, Lemma 2.3]. Therefore g = $\varepsilon g + \omega g$ is separable, completing the proof.

In the rest of this note, we shall deal with the set $B[X;\rho]^{\sim}_{(2)} \text{ (of B-ring isomorphism classes of the ring extensions} \\ B[X;\rho]/gB[X;\rho] \text{ (g } \epsilon \text{ B[X;\rho]}_{(2)} \text{) of B).}$

Now, if $C \in B[X; \rho]^{\sim}$ and $g \in C$ then we write $C = \langle g \rangle$.

Moreover, for $g = x^2 - xu - v$, $g_1 = x^2 - xu_1 - v_1$ and $s \in B$, we write

$$g \times s = x^{2} - xus - vs^{2}$$

 $g \times g_{1} = x^{2} - xuu_{1} - (u^{2}v_{1} + vu_{1}^{2} + 4vv_{1})$
 $g \times s = x^{2} - vs^{2}$
 $g \times g_{1} = x^{2} - vv_{1}$.

If $B[X;\rho]_2$ contains a separable polynomial then $\rho^2|Z=1$, and in this case, for any element α (resp. any subset S) of Z, we denote $\alpha\rho(\alpha)$ (resp. $\{\alpha\rho(\alpha) \mid \alpha \in S\}$) by $N_{\rho}(\alpha)$ (resp. $N_{\rho}(S)$).

Now, by virtue of Lemma 1, [5, Lemma 2. 10] and [3, Lemma 1. 8], we obtain the following

Lemma 5. Let 2 be nilpotent, and assume that $B[X;\rho]_2$ contains a separable polynomial $f = x^2 - b$. Let $g_1 = x^2 - v_1$ and $g_2 = x^2 - v_2 \in B[X;\rho]_{(2)}$ (= $\{x^2 - v \mid v \in B(\rho^2)^{\rho}\}$). Then, $g_1 \sim g_2$ if and only if $v_1 = v_2 N_{\rho}(\alpha)$ for some $\alpha \in U(Z)$.

From the preceding lemma and [5, Lemma 2.3], we obtain

Corollary 6. Let 2 be nilpotent, and assume that $B[X;\rho]_2$ contains a separable polynomial $f=X^2-b$. Let $g_1\sim g_2$ in $B[X;\rho]_{(2)}$, and $h_1\sim h_2$ in $Z[X;\rho|Z]_{(2)}$. Then for any $g\in B[X;\rho]_{(2)}$ and $h\in Z[X;\rho|Z]_{(2)}$, there holds the following

(i)
$$g_1 * g * b^{-1} \sim g_2 * g * b^{-1}$$
 in $Z[X; \rho | Z]_{(2)}$.

(ii)
$$h_1 * h \sim h_2 * h \text{ in } Z[X; \rho | Z]_{(2)}$$
.

- (iii) $h_1 * g \sim h_2 * g \text{ in } B[X; \rho]_{(2)}$.
- (iv) $g_1 * g * f * b^{-1} \sim g_2 * g * f * b^{-1}$ in $B[X; \rho]_{(2)}$.
- (v) $g * f * f * b^{-1} = g$, and $h * f * f * b^{-1} = h$.
- (vi) g is separable in $B[X;\rho]_{(2)}$ if and only if $g*g*f*b^{-1} \sim f$ which is equivalent to that $g*g'*f*b^{-1} \sim f$ for some $g' \in B[X;\rho]_{(2)}$.
- (vii) h is separable in $Z[X;\rho|Z]_{(2)}$ if and only if $h*h\sim f*f*b^{-1}$ which is equivalent to that $h*h'\sim f*f*b^{-1}$ for some $h'\in Z[X;\rho|Z]_{(2)}$.

By making use of Cor. 6, we can prove the next

Lemma 7. Let 2 be nilpotent, and assume that $B[X;\rho]_{(2)}$ contains a separable polynomial $f = X^2 - b$. Then, the set $B[X;\rho]_{(2)}^{\sim}$ (resp. $Z[X;\rho|Z]_{(2)}^{\sim}$) forms an abelian semigroup under the composition $\langle g_1 \rangle \langle g_2 \rangle = \langle g_1 * g_2 * f * b^{-1} \rangle$ (resp. $\langle h_1 \rangle \langle h_2 \rangle = \langle h_1 * h_2 \rangle$) with identity element $\langle f \rangle$ (resp. $\langle f * f * b^{-1} \rangle$), and the subset $\{\langle g \rangle \in B[X;\rho]_{(2)}^{\sim} \mid g$ is separable} (resp. $\{\langle h \rangle \in Z[X;\rho|Z]_{(2)}^{\sim} \mid h$ is separable}) coincides with the set of all inversible elements in the semigroup $B[X;\rho]_{(2)}^{\sim}$ (resp. $Z[X;\rho|Z]_{(2)}^{\sim}$) which is a group of exponent 2. Moreover, $B[X;\rho]_{(2)}^{\sim} \simeq Z[X;\rho|Z]_{(2)}^{\sim}$, which is isomorphic to the multiplicative semigroup $Z^{\rho}/N_{\rho}(U(Z))$.

Now, let ϵ be an idempotent in Z^{ρ} . Then $\epsilon B = (\epsilon B)^{\rho}$, $\epsilon B(\rho) = (\epsilon B)(\rho | \epsilon B)$, and $\epsilon B(\rho)^{\rho} = (\epsilon B)(\rho | \epsilon B)^{\rho}$. Hence we have a bijective map: $\epsilon B[X;\rho]_{(2)} \rightarrow (\epsilon B)[X;\rho | \epsilon B]_{(2)}$ given by

 $\epsilon(X^2 - Xu - v) \rightarrow X^2 - X\epsilon u - \epsilon v$. Hence we shall identify $\epsilon B[X;\rho]_{(2)}$ with $(\epsilon B)[X;\rho|\epsilon B]_{(2)}$, and by $\epsilon B[X;\rho]_{(2)}^{\sim}$, we denote $(\epsilon B)[X;\rho|\epsilon B]_{(2)}^{\sim}$. We set here $\omega = 1 - \epsilon$. Then, as is easily seen, the map:

 $B[X;\rho]_{(2)} \rightarrow \varepsilon B[X;\rho]_{(2)} \times \omega B[X;\rho]_{(2)}$ (direct product) given by $g \rightarrow (\varepsilon g, \omega g)$ is bijective. This induces a bijective map:

 $B[X;\rho]^{\sim}(2) \rightarrow \varepsilon B[X;\rho]^{\sim}(2) \times \omega B[X;\rho]^{\sim}(2)$

where $\langle g \rangle \rightarrow (\langle \epsilon g \rangle, \langle \omega g \rangle)$. Clearly, g is separable in B[X; ρ] if and only if ϵg and ωg are separable in $\epsilon B[X;\rho]$ and $\omega B[X;\rho]$ respectively. If $B[X;\rho]_2$ contains a separable polynomial $f = X^2 - Xa - b$ whose discriminant is π -regular and $\epsilon = e(\delta(f))$ ($\omega = 1 - \epsilon$) then $\epsilon B[X;\rho]_2$ contains a Galois polynomial ϵf , ωf is nilpotent and ωf and ωf contains a separable polynomial $\omega f = \omega(X^2 - b)$ (Th.4, [5, Lemma 2.2], [6, Th.2]).

Now, our main results are the following theorems which can be proved by making use of the preceding remarks, Lemma 7, [5, Th.2.17], Cor. 3, [5, Lemma 2.10], [3, Lemma 1.8], [6, Th.2], [4, Th.1.2], and etc.

Theorem 8. Assume that $B[X;\rho]_2$ contains a separable polynomial $f = X^2 - Xa - b$ whose discriminant is π -regular. Set $\epsilon = e(\delta(f))$ and $\omega = 1 - \epsilon$. Then the set $B[X;\rho]_{(2)}^{\sim}$ (resp. $Z[X;\rho|Z]_{(2)}^{\sim}$) forms an abelian semigroup under the composition

$$\langle g_1 \rangle \langle g_2 \rangle = \langle \epsilon g_1 \times \epsilon g_2 \times \epsilon f \times (\epsilon \delta(f))^{-1} + \omega g_1 * \omega g_2 * \omega f * (\omega b)^{-1} \rangle$$

 $\langle esp. \langle h_1 \rangle \langle h_2 \rangle = \langle \epsilon h_1 \times \epsilon h_2 + \omega h_1 * \omega h_2 \rangle$

with identity element

 (resp.
$$\langle \epsilon f \times \epsilon f \times (\epsilon \delta(f))^{-1} + \omega f \star \omega f \star (\omega b)^{-1} \rangle$$
)

, and the subset

{
$$\langle g \rangle \in B[X; \rho]^{\sim}_{(2)} \mid g \text{ is separable } \}$$

(resp. { $\langle h \rangle \in Z[X; \rho \mid Z]^{\sim}_{(2)} \mid h \text{ is separable} \}$)

coincides with the set of all inversible elements of $B[X;\rho]^{\sim}(2)$ (resp. $Z[X;\rho|Z]^{\sim}(2)$) which is a group of exponent 2. Moreover

$$B[X;\rho]_{(2)}^{\sim} \simeq Z[X;\rho|Z]_{(2)}^{\sim} \simeq \varepsilon Z[X;\rho|\varepsilon Z]_{(2)}^{\sim} \times \omega Z[X;\rho|\omega Z]_{(2)}^{\sim}$$

$$\simeq \varepsilon Z[X;\rho|\varepsilon Z]_{(2)}^{\sim} \times \omega Z^{\rho}/N_{\rho}(U(\omega Z)).$$

Theorem 9. Let 2 be π -regular and assume that B[X; ρ] 2 contains a separable polynomial f. Then, there exists an idempotent ϵ ($\omega=1-\epsilon$) of Z $^{\rho}$ such that

$$B[X;\rho]^{\sim}(2) \simeq \varepsilon Z[X]^{\sim}_{2} \times \omega Z^{\rho}/N_{\rho}(U(\omega Z))$$

where if $e(2) = e(\delta(f))$ then $\epsilon = 0$.

Corollary 10. Let 2=0 and assume that $B[X;\rho]_{(2)}$ contains a separable polynomial. Let $U(B[X;\rho]_{(2)}^{\sim})$ be a group of inversible elements of $B[X;\rho]_{(2)}^{\sim}$. Then, there exists an idempotent ϵ ($\omega=1-\epsilon$) of Z^{ρ} such that

$$U(B[X;\rho]^{\sim}_{(2)}) \simeq \varepsilon Z/\varepsilon \{z^2 - z \mid z \in Z\} \times U(\omega Z)^{\rho}/N_{\rho}(U(\omega Z))$$

where ωZ is an additive subgroup of Z, and if $B[X;\rho]_2$ contains a Galois polynomial then $\omega=0$.

References

- [1] K. Kitamura: On the free quadratic extensions of commutative rings, Osaka J. Math. 10 (1973), 15-20.
- [2] K. Kishimoto: A classification of free quadratic extensions of rings, Math. J. Okayama Univ. 18 (1976), 139-148.
- [3] T. Nagahara and K. Kishimoto: On free cyclic extensions of rings. Proc. 10 th Symp. Ring Theory (Shinshu Univ., Matsumoto, 1977). 1978, 1-25.
- [4] T. Nagahara and A. Nakajima: On cyclic extensions of commutative rings, Math. J. Okayama Univ. 15 (1971), 81-90.
- [5] T. Nagahara: On separable polynomials of degree 2 in skew polynomial rings, Math. J. Okayama Univ. 19 (1976), 65-95.
- [6] T. Nagahara: On separable polynomials of degree 2 in skew polynomial rings II, Math. J. Okayama Univ. 21 (1979), 167-177.
- [7] T. Nagahara: On separable polynomials of degree 2 in skew polynomial rings III, Math. J. Okayama Univ. 22 (1980), 61-64.