

Mathematical Journal of Okayama University

Volume 23, Issue 2

1981

Article 10

DECEMBER 1981

On separable polynomials of degree 2 in skew polynomial rings IV

Takashi Nagahara*

*Okayama University

Copyright ©1981 by the authors. *Mathematical Journal of Okayama University* is produced by
The Berkeley Electronic Press (bepress). <http://escholarship.lib.okayama-u.ac.jp/mjou>

ON SEPARABLE POLYNOMIALS OF DEGREE 2 IN SKEW POLYNOMIAL RINGS IV

Dedicated to Prof. Kentaro MURATA on his 60th birthday

TAKASI NAGAHARA

Throughout B will mean a (non-commutative) ring with identity element 1 which has an automorphism 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 $bX = X\rho(b)$ ($b \in B$). Moreover, by $B[X; \rho]_2$, we denote the subset of $B[X; \rho]$ of all polynomials $f = X^2 - Xa - b$ with $fB[X; \rho] = B[X; \rho]f$. If $X^2 - Xa - b \in B[X; \rho]_2$ then $\rho(b) = b$. By $B[X; \rho]_{(2)}$, we denote the subset of $B[X; \rho]_2$ of all elements $X^2 - Xa - b$ with $\rho(a) = a$. 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 $f \sim g$. Clearly the relation \sim is an equivalence relation in $B[X; \rho]_{(2)}$. By $B[X; \rho]_{(2)}$, we denote the set of equivalence classes of $B[X; \rho]_{(2)}$ with respect to the relation \sim . Moreover, for $f \in B[X; \rho]_2$, if the factor ring $B[X; \rho]/fB[X; \rho]$ 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 $f = X^2 - Xa - b \in B[X; \rho]_2$, we denote $a^2 + 4b$ by $\delta(f)$, which will be called the discriminant of f .

Now, in [1], K. Kitamura studied free quadratic (separable) extensions of commutative rings and its isomorphism classes. Indeed, [1] is a study on $B[X; 1]_{(2)}$ and $B[X; 1]_{(2)}$ where B is commutative, and $1 =$ identity map. In this case, it is obvious that $f = X^2 \pm X$ is Galois. 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 $f = X^2 - b$ (and hence $4b$ is invertible in B ([6, Th. 2])). In [5], the present author studied the sets $B[X; \rho]_{(2)}$ and $B[X; \rho]_{(2)}$ in case $B[X; \rho]_{(2)}$ contains a Galois polynomial $f = X^2 - Xa - b$ (and hence $a^2 + 4b$ is invertible in B). Moreover, in [1], [2] and [5], $B[X; \rho]_{(2)}$ was considered as an abelian semigroup with identity element ($=$ the class of f) to characterize the separable polynomials in $B[X; \rho]_{(2)}$.

In this paper, we shall study the separable polynomials in $B[X; \rho]_{(2)}$ and the structure of $B[X; \rho]_{(2)}$ in case $B[X; \rho]_{(2)}$ contains a separable polynomial f whose discriminant is π -regular, and we shall show that $B[X; \rho]_{(2)}$ forms also an abelian semigroup with identity element ($=$ the class of f)

under some composition such that for $C \in B[X; \rho]_{(2)}$ and $g \in C$, C is invertible in this semigroup if and only if g is separable. Moreover, this semigroup will be studied in various ways.

In what follows, we shall summarize the notations and terminologies which will be used very often in the subsequent study. Throughout Z will mean the center of B , and $U(B)$ denotes the set of invertible elements in B . Moreover, for any subset S of B and for $\sigma = \rho^n$ (with any integer $n \geq 0$), we shall use the following conventions:

$$\begin{aligned} U(S) &= U(B) \cap S, \quad S^\sigma = \{s \in S; \sigma(s) = s\}, \\ \sigma|S &= \text{the restriction of } \sigma \text{ to } S, \\ B(\sigma) &= \{u \in B; au = u\sigma(a) \text{ for all } a \in B\}. \end{aligned}$$

Clearly, $U(Z)$ coincides with the set of invertible elements in Z . By [5, (2, xvii)] and [6, Th. 1], we see that if $B[X; \rho]_2$ contains a separable polynomial then $\rho^2|Z$ is identity. For any element a of $B(\rho^n)$, a is π -regular if and only if there exists an element c in B and an integer $t \geq 0$ such that $a^t = a^{t+1}c$, which is equivalent to that a is right π -regular. If $a \in B(\rho^n)$ (resp. $B(\rho^n)^\rho$) is π -regular then there exists an integer $t > 0$ and an idempotent ε of Z (resp. Z^ρ) such that $a^t B = \varepsilon B$. This idempotent will be denoted by $e(a)$ (cf. [7, p. 61]). For $f = X^2 - Xa - b \in B[X; \rho]$, this is contained in $B[X; \rho]_2$ if and only if $a \in B(\rho)$, $b \in B(\rho^2)^\rho$, and $ba = b\rho(a)$ (cf. [6, p. 168]). When this is the case, we have $\delta(f) \in B(\rho^2)^\rho$; and whence if $\delta(f)$ is π -regular then $e(\delta(f)) \in Z^\rho$. Moreover, there holds that $B[X; \rho]_{(2)} = \{X^2 - Xa - b; a \in B(\rho)^\rho, b \in B(\rho^2)^\rho\}$. Now, let ε be a non-zero idempotent in Z^ρ . Then $\varepsilon B = (\varepsilon B)^\rho$, $\varepsilon B(\rho) = (\varepsilon B)(\rho|\varepsilon B)$, and $\varepsilon B(\rho)^\rho = (\varepsilon B)(\rho|\varepsilon B)^\rho$. Moreover, we have an (εB) -ring isomorphism: $\varepsilon B[X; \rho] \rightarrow (\varepsilon B)[Y; \rho|\varepsilon B]$ ($Y\varepsilon = Y$) defined by $\varepsilon f(X) \rightarrow f(Y)$. Hence, we shall identify $\varepsilon B[X; \rho]$, $\varepsilon f(X)$, $\varepsilon B[X; \rho]_2$, and $\varepsilon B[X; \rho]_{(2)}$ with $(\varepsilon B)[Y; \rho|\varepsilon B]$, $f(Y)$, $(\varepsilon B)[Y; \rho|\varepsilon B]_2$, and $(\varepsilon B)[Y; \rho|\varepsilon B]_{(2)}$ respectively, and by $\varepsilon B[X; \rho]$ etc., we denote $(\varepsilon B)[Y; \rho|\varepsilon B]$ etc.. Moreover, we denote $(\varepsilon B)[Y; \rho|\varepsilon B]_{(2)}$ by $\varepsilon B[X; \rho]_{(2)}$.

1. On separable polynomials in $B[X; \rho]_{(2)}$. First, we shall prove the following

Lemma 1. *Let ρ be nilpotent, and assume that $B[X; \rho]_2$ contains a separable polynomial $X^2 - b$. Then $b \in U(B)$, $B(\rho) = \{0\}$, $B(\rho^2) = bZ$, $B(\rho^2)^\rho = bZ^\rho$, and $B[X; \rho]_2 = B[X; \rho]_{(2)} = \{X^2 - v; v \in B(\rho^2)^\rho\}$. Moreover, for $X^2 - v \in B[X; \rho]_2$, this is separable if and only if $v \in U(B)$.*

Proof. By [5, Lemma 2.3] and [6, Th. 1], we have $b \in U(B)$ and $z + \rho(z) = 1$ for some $z \in Z$. Now, since 2 is nilpotent, there exists an integer $n > 0$ such that $2^n = 0$. Then, for $u \in B(\rho)$, $u = u(z + \rho(z))^n = u(z + \rho(z))(z + \rho(z))^{n-1} = 2zu(z + \rho(z))^{n-1} = 2^n z^n u = 0$. If $v \in U(B(\rho^2)^\rho)$ then $X^2 - v$ is separable by [5, Lemma 2.3]. The other assertions will be easily seen.

Lemma 2. *Let κ be a proper idempotent in Z^ρ such that $\kappa 2^n = 2^n$ for some integer $n > 0$. Let f be a polynomial in $B[X; \rho]_2$ such that κf is Galois in $\kappa B[X; \rho]$ and $(1 - \kappa)f$ is separable in $(1 - \kappa)B[X; \rho]$. Then $\delta(f)$ is π -regular and $e(\delta(f)) \supset \kappa B$.*

Proof. We set $\varepsilon = e(\delta(f))$. If $\varepsilon = 1$ then the assertion is trivial. Hence we assume $\varepsilon \neq 1$. By [6, Th. 2], we have $\kappa B = \kappa \delta(f)B$. 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 $a = \delta(f)ar = \delta(f)^{n+1}ar^{n+1}$ for some r in B . Since $\kappa 4^n = 4^n$, it follows that $(1 - \kappa)\delta(f)^n B = (1 - \kappa) \cdot (ac + 4^n b^n)B = (1 - \kappa)acB \subset (1 - \kappa)\delta(f)^{n+1}B$, and whence $\delta(f)^n B = \kappa \delta(f)^n B + (1 - \kappa)\delta(f)^n B = \kappa \delta(f)^{n+1}B + (1 - \kappa)\delta(f)^{n+1}B = \delta(f)^{n+1}B$. Thus $\delta(f)$ is π -regular, and $\varepsilon B = \delta(f)^n B \supset \kappa \delta(f)^n B = \kappa B$.

Next, we shall prove the following

Theorem 3. *Let 2 be π -regular. If $f \in B[X; \rho]_2$ is separable then $\delta(f)$ is π -regular, and $e(\delta(f)) \geq e(2)$ (that is, $e(\delta(f))B \supset e(2)B$).*

Proof. Let $f = X^2 - Xa - b$ be a separable polynomial in $B[X; \rho]_2$. If either $\delta(f)$ is nilpotent or invertible in B then $\delta(f)$ is π -regular. Hence we assume that $\delta(f)B \neq B$ and $\delta(f)$ is not nilpotent. Then, we have $e(2) \neq 1$ by [6, Th. 3]. First, we consider the case $e(2) = 0$. Then $2^n = 0$ for some integer $n > 0$. By [5, Lemma 2.2 (2, xix)], we have $a = \delta(f)^n ar = a^2 s$ for some $r, s \in B$. Hence a is π -regular, and $e(a)$ is in Z^ρ . Moreover, noting $\delta(f) = a^2 + 4b$, we see that $e(a)$ is proper. Since $e(a)a$ is invertible 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, $(1 - e(a))f$ is separable in $(1 - e(a))B[X; \rho]$. Therefore, $\delta(f)$ is π -regular by Lemma 2. Next, we consider the case $e(2) \neq 0$. Then $e(2) \in Z^\rho$, $e(2)B = 2^m B$, and $e(2)2^m = 2^m$ for some integer $m > 0$. Noting that $e(2)2$ is invertible in $e(2)B$, $e(2)f$ is Galois in $e(2)B[X; \rho]$ by [6, Th. 3]. Moreover, $(1 - e(2))f$ is separable in $(1 - e(2))B[X; \rho]$. Hence by Lemma 2, $\delta(f)$ is π -regular. The last assertion $e(\delta(f)) \geq e(2)$ follows immediately from

the result of [5, Lemma 2.2 (2, xix)].

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, $\omega B(\rho) = \{0\}$, $\omega B[X; \rho]_2 = \omega B[X; \rho]_{(2)} = \{\omega(X^2 - v); v \in B(\rho^2)^\rho\}$. Moreover, for $g = X^2 - Xu - v \in B[X; \rho]_2$, the following conditions are equivalent.*

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

Proof. By the assumption, there exists an integer $n > 0$ such that $\varepsilon B = \delta(f)^n B$. We set here $f = X^2 - Xa - b$. Then, by [5, Lemma 2.2 (2, xix)], we have $a = \delta(f)ar = (\delta(f))^n ar^n = \varepsilon a$ and $4^n = (\delta(f))^n s = \varepsilon 4^n$ for some $r, s \in B$. Hence $\omega a = 0$, $\omega 4^n = 0$, and in case $\omega \neq 0$, $\omega f = \omega(X^2 - b)$ is separable in $\omega B[X; \rho]$. Therefore, it follows from Lemma 1 that $\omega B(\rho) = \{0\}$, and $\omega B[X; \rho]_2 = \{\omega(X^2 - v); v \in B(\rho^2)^\rho\}$. If $\varepsilon = 0$ (i.e., $\omega = 1$) then 2 is nilpotent and $e(\delta(h)) = 0$ for all $h \in B[X; \rho]_2$; whence (a), (b) and (c) are equivalent by Lemma 1. If $\varepsilon = 1$ then f is Galois in $B[X; \rho]$; whence (a), (b) and (c) are equivalent by [6, Th. 2]. Hence we assume that ε is proper. Then, since $\varepsilon \delta(f)$ is invertible in εB , εf is Galois in $\varepsilon B[X; \rho]$ by [6, Th. 2]. Now, let $g = X^2 - Xu - v \in B[X; \rho]_2$. First, we assume (a). Then, since εg is separable in $\varepsilon B[X; \rho]$, it follows from [6, Th. 3] 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 $e(\delta(g))B \supset \varepsilon B = e(\delta(f))B$. By a similar way, we have $e(\delta(g))B \supset e(\delta(f))B$. This implies $e(\delta(g)) = \varepsilon$. Since $\omega g = \omega(X^2 - v)$ is separable in $\omega B[X; \rho]$, it follows from Lemma 1 that ωv is invertible in ωB , that is, $\omega B = \omega v B$. Thus we obtain (b). Next, we assume (b). Then $\varepsilon B = e(\delta(g))B = \delta(g)^m B$ for some integer $m > 0$. This shows that $\varepsilon B = \varepsilon \delta(g) B$. Finally, we assume (c). Since $\varepsilon B = \varepsilon \delta(g) B$, $\varepsilon \delta(g)$ is invertible in εB . Hence εg is Galois in $\varepsilon B[X; \rho]$ by [6, Th. 2]. Moreover, since ωv is invertible in ωB , $\omega g = \omega(X^2 - v)$ is separable in $\omega B[X; \rho]$ by Lemma 1. Therefore, $g = \varepsilon g + \omega g$ is separable, completing the proof.

2. On $B[X; \rho]_{(2)}$. Throughout this section, we shall use the following conventions:

$$\begin{aligned} \langle g \rangle &= \{g' \in B[X; \rho]_{(2)}; g' \sim g\} \in B[X; \rho]_{(2)} \quad (g \in B[X; \rho]_{(2)}), \\ \rho_0 &= \rho|Z, N_\rho(\alpha) = a\rho(\alpha) \text{ for any } \alpha \in Z, \\ N_\rho(S) &= \{N_\rho(\alpha); \alpha \in S\} \text{ for any subset } S \text{ of } Z. \end{aligned}$$

If $B[X; \rho]_{(2)}$ contains a separable polynomial then ρ_0^2 is identity, and hence $N_\rho(Z) \subset Z^\rho$. Moreover, for $g = X^2 - Xu - v, g_1 = X^2 - Xu_1 - v_1 \in B[X; \rho]$ and $s \in S$, we write

$$\begin{aligned} g \times s &= X^2 - Xus - vs^2 \\ g \times g_1 &= X^2 - Xuu_1 - (u^2v_1 + vu_1^2 + 4vv_1) \\ g \circ s &= X^2 - vs^2 \\ g \circ g_1 &= X^2 - vv_1. \end{aligned}$$

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 $X^2 - b$. Let $g_1 = X^2 - v_1$ and $g_2 = X^2 - v_2$ be in $B[X; \rho]_{(2)}$ ($= \{X^2 - v; v \in bZ^\rho\}$). Then, $g_1 \sim g_2$ if and only if $v_1 = v_2 N_\rho(\alpha)$ for some $\alpha \in U(Z)$.*

Now, as in Lemma 5, let 2 be nilpotent, and $f = X^2 - b$ separable in $B[X; \rho]$. Then, by [5, Lemma 2.3], we see that $X^2 - 1$ is separable in $Z[X; \rho_0]$. Hence by Lemma 1, we obtain that $Z(\rho_0) = \{0\}$, $Z[X; \rho_0]_2 = Z[X; \rho_0]_{(2)}$ which coincides with the subset of $Z[X; \rho_0]$ of elements $X^2 - z$ ($z \in Z^\rho$); and for $X^2 - z$ in $Z[X; \rho_0]_{(2)}$, this is separable if and only if $z \in U(Z^\rho)$.

Moreover, if $g_1 \sim g_2$ in $B[X; \rho]_{(2)}$ and $h_1 \sim h_2$ in $Z[X; \rho_0]_{(2)}$ then, for any $g \in B[X; \rho]_{(2)}$ and $h \in Z[X; \rho_0]_{(2)}$, there holds the following

- (i) $g_1 \circ g \circ b^{-1} \sim g_2 \circ g \circ b^{-1}$ in $Z[X; \rho_0]_{(2)}$.
- (ii) $h_1 \circ h \sim h_2 \circ h$ in $Z[X; \rho_0]_{(2)}$.
- (iii) $h_1 \circ g \sim h_2 \circ g$ in $B[X; \rho]_{(2)}$.
- (iv) $g_1 \circ g \circ f \circ b^{-1} \sim g_2 \circ g \circ f \circ b^{-1}$ in $B[X; \rho]_{(2)}$.
- (v) $g \circ f \circ f \circ b^{-1} = g$, and $h \circ f \circ f \circ b^{-1} = h$.
- (vi) g is separable in $B[X; \rho]_{(2)}$ if and only if $g \circ g \circ f \circ b^{-1} \sim f$ which is equivalent to that $g \circ g' \circ f \circ b^{-1} \sim f$ for some $g' \in B[X; \rho]_{(2)}$.
- (vii) h is separable in $Z[X; \rho_0]_{(2)}$ if and only if $h \circ h \sim f \circ f \circ b^{-1}$ which is equivalent to that $h \circ h' \sim f \circ f \circ b^{-1}$ for some $h' \in Z[X; \rho_0]_{(2)}$.

By making use of the preceding remarks, we can prove the next

Lemma 6. *Let 2 be nilpotent, and assume that $B[X; \rho]_{(2)}$ contains a separable polynomial $f = X^2 - b$. Then, the set $B[X; \rho]_{\tilde{(2)}}$ (resp. $Z[X; \rho_0]_{\tilde{(2)}}$) forms an abelian semigroup under the composition $\langle g_1 \rangle \langle g_2 \rangle = \langle g_1 \circ g_2 \circ f \circ b^{-1} \rangle$ (resp. $\langle h_1 \rangle \langle h_2 \rangle = \langle h_1 \circ h_2 \rangle$) with identity element $\langle f \rangle$ (resp. $\langle f \circ f \circ b^{-1} \rangle$), and the subset*

$$\begin{aligned} & \{ \langle g \rangle \in B[X; \rho]_{\tilde{(2)}}; g \text{ is separable} \} \\ & \text{(resp. } \{ \langle h \rangle \in Z[X; \rho_0]_{\tilde{(2)}}; h \text{ is separable} \}) \end{aligned}$$

coincides with the set of all invertible elements in the semigroup $B[X; \rho]_{\tilde{(2)}}$ (resp. $Z[X; \rho_0]_{\tilde{(2)}}$) which is a group of exponent 2. Moreover

$$B[X; \rho]_{\tilde{(2)}} \simeq Z[X; \rho_0]_{\tilde{(2)}} \text{ (by } \langle g \rangle = \langle h \circ f \rangle \leftrightarrow \langle g \circ f \circ b^{-1} \rangle = \langle h \rangle \text{)}$$

which is isomorphic to the multiplicative semigroup $Z^e/N_e(U(Z))$.

Now, by $(B[X; \rho]_{\tilde{(2)}}, \circ f)$ (resp. $(Z[X; \rho_0]_{\tilde{(2)}}, \circ)$), we denote the semigroup $B[X; \rho]_{\tilde{(2)}}$ (resp. $Z[X; \rho_0]_{\tilde{(2)}}$) with the composition as in the preceding lemma. Moreover, if $B[X; \rho]_{(2)}$ contains a Galois polynomial f then $B[X; \rho]_{\tilde{(2)}}$ (resp. $Z[X; \rho_0]_{\tilde{(2)}}$) forms an abelian semigroup with the composition $\langle g_1 \rangle \langle g_2 \rangle = \langle g_1 \times g_2 \times f \times \delta(f)^{-1} \rangle$ (resp. $\langle h_1 \rangle \langle h_2 \rangle = \langle h_1 \times h_2 \rangle$), which will be denoted by $(B[X; \rho]_{\tilde{(2)}}, \times f)$ (resp. $(Z[X; \rho_0]_{\tilde{(2)}}, \times)$). Then $(B[X; \rho]_{\tilde{(2)}}, \times f) \simeq (Z[X; \rho_0]_{\tilde{(2)}}, \times)$ (cf. [5, Ths. 2.16, 2.17]).

Let ε be a proper idempotent in Z^e , and $\omega = 1 - \varepsilon$. Then, as is easily seen, the map:

$$B[X; \rho]_{(2)} \rightarrow \varepsilon B[X; \rho]_{(2)} \times \omega B[X; \rho]_{(2)} \text{ (direct product)}$$

given by $g \rightarrow (\varepsilon g, \omega g)$ is bijective. This induces a bijective map:

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

where $\langle g \rangle \rightarrow (\langle \varepsilon g \rangle, \langle \omega g \rangle)$. Clearly, g is separable in $B[X; \rho]$ if and only if εg and ωg are separable in $\varepsilon B[X; \rho]$ and $\omega B[X; \rho]$ respectively. We have also a bijective map:

$$Z[X; \rho_0]_{\tilde{(2)}} \rightarrow \varepsilon Z[X; \rho_0]_{\tilde{(2)}} \times \omega Z[X; \rho_0]_{\tilde{(2)}}$$

where $\langle h \rangle \rightarrow (\langle \varepsilon h \rangle, \langle \omega h \rangle)$.

Let $f = X^2 - Xa - b$ be a separable polynomial of $B[X; \rho]_{(2)}$ whose discriminant is π -regular. We set $\varepsilon = e(\delta(f))$ and $\omega = 1 - \varepsilon$. Then εf is a Galois polynomial in $\varepsilon B[X; \rho]_{(2)}$, $\omega 2$ is nilpotent and $\omega f = \omega(X^2 - b)$ is a separable polynomial in $\omega B[X; \rho]_{(2)}$ (Th. 4, [6, Th. 2]). Next, we consider

$$h_f = \varepsilon f \times \varepsilon f \times (\varepsilon \delta(f))^{-1} + \omega f \circ \omega f \circ (\omega b)^{-1}$$

where $(\varepsilon c)^{-1}$ (resp. $(\omega c)^{-1}$) denotes the inverse of εc (resp. ωc) in the ring

εB (resp. ωB). Then, it is easy to see that $h_f \in Z[X; \rho_0]_{(2)}$ and $\delta(h_f) = \varepsilon\delta(h_f) + \omega\delta(h_f) = \varepsilon + 4\omega$. Hence $\delta(h_f)$ is π -regular in Z , and $e(\delta(h_f)) = \varepsilon = e(\delta(f))$. Moreover, εh_f is Galois in $\varepsilon Z[X; \rho_0]$, and ωh_f is separable in $\omega Z[X; \rho_0]$ ([5, Lemma 2.3], [6, Th. 2]). This implies that h_f is separable in $Z[X; \rho_0]$.

Now, the following theorem is one of our main results which can be proved by making use of the preceding remarks, Th. 4, Lemma 6, and [5, Ths. 2.16, 2.17].

Theorem 7. *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 the set $B[X; \rho]_{(\tilde{2})}$ (resp. $Z[X; \rho_0]_{(\tilde{2})}$) forms an abelian semigroup under the composition*

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

$$\text{(resp. } \langle h_1 \rangle \langle h_2 \rangle = \langle \varepsilon h_1 \times \varepsilon h_2 + \omega h_1 \circ \omega h_2 \rangle \text{)}$$

with identity element $\langle f \rangle$ (resp. $\langle h_f \rangle$), and the subset

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

$$\text{(resp. } \{ \langle h \rangle \in Z[X; \rho_0]_{(\tilde{2})}; h \text{ is separable} \})$$

coincides with the set of all invertible elements of $B[X; \rho]_{(\tilde{2})}$ (resp. $Z[X; \rho_0]_{(\tilde{2})}$) which is a group of exponent 2. Moreover

$$B[X; \rho]_{(\tilde{2})} \simeq (\varepsilon B[X; \rho]_{(\tilde{2})}, \times \varepsilon f) \times (\omega B[X; \rho]_{(\tilde{2})}, \circ \omega f)$$

$$\simeq (\varepsilon Z[X; \rho_0]_{(\tilde{2})}, \times) \times (\omega Z[X; \rho_0]_{(\tilde{2})}, \circ)$$

$$\simeq (\varepsilon Z[X; \rho_0]_{(\tilde{2})}, \times) \times \omega Z^\circ / \omega N_\rho(U(Z)) \simeq Z[X; \rho_0]_{(\tilde{2})}$$

where in case $\varepsilon = 0$ (resp. $\omega = 0$), the first (resp. second) factor is cutted.

Next, we shall prove the following theorem which contains the result of K. Kishimoto [2, Th. 2.4].

Theorem 8. *Let 2 be π -regular, and assume that $B[X; \rho]_{(2)}$ contains a separable polynomial f . Then*

- (i) *if $e(\delta(f)) = e(2)$ then $B[X; \rho]_{(\tilde{2})} \simeq Z^\circ / N_\rho(U(Z))$.*
- (ii) *If $e(\delta(f)) > e(2)$ then, for $\kappa = e(\delta(f)) - e(2)$ and $\lambda = 1 - \kappa$,*

$$B[X; \rho]_{(\tilde{2})} \simeq (\kappa Z[X]_2, \times) \times \lambda Z^\circ / \lambda N_\rho(U(Z))$$

where $Z[X]_2 = Z[X; 1]_{(2)}$, and in case $\lambda = 0$, the second factor is cutted; moreover

$$U((\kappa Z[X]_2, \times)) = \{ \langle \kappa(X^2 - X - z) \rangle; z \in Z \}.$$

Proof. We set $\varepsilon = e(\delta(f))$, $\omega = 1 - \varepsilon$, $\xi = e(2)$, $\kappa = \varepsilon - \xi$, $\lambda = \xi + \omega$, and $f = X^2 - Xa - b$. Now, let $\kappa \neq 0$. Then, $\kappa 2$ is nilpotent and $\kappa \delta(f)$ is invertible in κB , and whence κa is invertible in κB . For $\kappa z \in \kappa Z$, $(\kappa z)(\kappa a) = (\kappa z)(\kappa \rho(z)) = \kappa \rho(z)(\kappa a)$. This implies that $\rho|_{\kappa Z}$ is identity. Therefore, it follows that

$$(\kappa B[X; \rho]_{(2)}, \times \kappa f) \simeq (\kappa Z[X; \rho_0]_{(2)}, \times) = (\kappa Z[X]_2, \times).$$

Moreover, for $h = \kappa(X^2 - Xr - s) \in \kappa Z[X]_2$,

$$\begin{aligned} \langle h \rangle \in U((\kappa Z[X]_2, \times)) &\Leftrightarrow h \text{ is separable} \\ &\Leftrightarrow \delta(h) \in \kappa U(Z) \Leftrightarrow \kappa r \in \kappa U(Z) \\ &\Leftrightarrow \langle h \rangle = \langle \kappa(X^2 - X - z) \rangle \text{ for some } z \in Z. \end{aligned}$$

Next, let $\xi \neq 0$. Then, $\xi 2$ and $\xi \delta(f)$ are invertible in ξB . As is easily seen, we have

$$\xi Z[X; \rho_0]_{(2)} = \{ \langle \xi(X^2 - v) \rangle ; v \in Z^\rho \}.$$

Moreover, $\langle \xi(X^2 - v) \rangle = \langle \xi(X^2 - v') \rangle$ in $\xi Z[X; \rho_0]_{(2)}$ if and only if $\xi v = \xi v' N_\rho(a)$ for some $\alpha \in U(Z)$ (cf. [5, Lemma 2.10], [3, Lemma 1.8], and [2, Lemma 2.1]). Clearly

$$\langle \xi(X^2 - v_1) \rangle \langle \xi(X^2 - v_2) \rangle = \langle \xi(X^2 - 4v_1v_2) \rangle = \langle \xi(X^2 - v_1v_2) \rangle.$$

Hence, one will easily see

$$(\xi B[X; \rho]_{(2)}, \times \xi f) \simeq (\xi Z[X; \rho_0]_{(2)}, \times) \simeq \xi Z^\rho / \xi N_\rho(U(Z))$$

(cf. [2, Th. 2.4]). Therefore, it follows from Th. 7 that

$$\begin{aligned} B[X; \rho]_{(2)} &\simeq (\varepsilon B[X; \rho]_{(2)}, \times \varepsilon f) \times (\omega B[X; \rho]_{(2)}, \circ \omega f) \\ &\simeq (\kappa B[X; \rho]_{(2)}, \times \kappa f) \times (\xi B[X; \rho]_{(2)}, \times \xi f) \times (\omega B[X; \rho]_{(2)}, \circ \omega f) \\ &\simeq (\kappa Z[X]_2, \times) \times \xi Z^\rho / \xi N_\rho(U(Z)) \times \omega Z^\rho / \omega N_\rho(U(Z)) \\ &\simeq (\kappa Z[X]_2, \times) \times \lambda Z^\rho / \lambda N_\rho(U(Z)). \end{aligned}$$

This completes the proof.

Now, in the preceding theorem, we shall assume that $2 = 0$ and $\kappa \neq 0$. Then,

$$\langle \kappa(X^2 - X - z) \rangle = \langle \kappa(X^2 - X - z') \rangle \text{ in } \kappa Z[X]_2$$

if and only if $\kappa z = \kappa z' + \kappa(a^2 + a)$ for some $\alpha \in Z$. Clearly

$$\kappa(X^2 - X - z_1) \times \kappa(X^2 - X - z_2) = \kappa(X^2 - X - z_1 - z_2).$$

Hence, it follows that

$$U((\kappa Z[X]_2, \times)) \simeq (\kappa Z, +) / \kappa \{ a^2 + a ; a \in Z \} \text{ (cf. [1])}$$

Combining this with Th. 8 and [5, Lemma 2.2 (2, xix)], we obtain the following

Corollary 9. *Let $2 = 0$, and assume that $B[X; \rho]_{(2)}$ contains a separable polynomial $f = X^2 - Xa - b$. Then $aB = a^2B$, $e(a) = e(\delta(f))$, and for $\kappa = e(a)$ ($\lambda = 1 - \kappa$), there holds the following*

$$U((B[X; \rho]_{(2)})) \simeq (\kappa Z, +) / \kappa\{a^2 + \alpha; \alpha \in Z\} \times \lambda U(Z)^{\rho} / \lambda N_{\rho}(U(Z)).$$

where in case $\kappa = 0$ (resp. $\lambda = 0$), the first (resp. second) factor is cutted. (Cf. [8]).

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), 139–158.
- [3] T. NAGAHARA and K. KISHIMOTO: On free cyclic extensions of rings, Proc. 10th 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.
- [8] T. NAGAHARA: A semigroup of isomorphism classes of some quadratic extensions of rings, Kōkyuroku of Res. Inst. Math. Sci. Kyoto Univ. 395 (1980), 18–28.

DEPARTMENT OF MATHEMATICS
OKAYAMA UNIVERSITY

(Received July 7, 1981)