ON SEPARABLE POLYNOMIALS OF DEGREE 2 IN SKEW POLYNOMIAL RINGS

Dedicated to Professor Mikao Moriya on his 70th birthday

TAKASI NAGAHARA

In [1], K. Kitamura studied free quadratic extensions of commutative rings and its isomorphism classes. In [4], K. Kishimoto studied some quadratic extensions of non-commutative rings and its isomorphism classes which are some partial generalization of [1]. In these studies, the set of polynomials of degree 2 plays an important rôle. Indeed, any quadratic extension (considered in [1] and [4]) is determined by some polynomial ring and some polynomial of degree 2. The purpose of this note is to study (separable) polynomials of degree 2 in a skew polynomial ring and is to present some generalization and sharpening of the result of [4].

Throughout this paper, B will mean a (non-commutative) ring with identity element 1, and all ring extensions of B will be assumed to have the the (common) identity element 1. Now, let ρ be an automorphism of B, and D a derivation of B, so that $D(x+y)=D(x)+D(y)$ and $D(xy)=D(x)y+xD(y)$ $(x, y\in B)$. As in [2]-[4], by $B[X;\rho]$ (resp. $B[X;D]$), we denote the ring of all polynomials $\sum_i X^i b_i$ $(b_i\in B)$ with an indeterminate X whose multiplication is defined $bX=X\rho(b)$ (resp. $bX=Xb+D(b)$) for each $b\in B$. For a while, let $B[X;*]$ be one of $B[X;\rho]$ and $B[X;D]$. By $B[X;*]_{(2)}$, we denote the subset of $B[X;*]$ of all polynomials $f=X^2-Xa-b$ with $fB[X;*]=B[X;*]f$ and $Xa=aX$. A polynomial $f=X^2-Xa-b\in B[X;*]_{(2)}$ is called to be separable (resp. Galois) if the factor ring $B[X;*]/fB[X;*]$ is a separable (resp. Galois) extension of B in the sense of [5]. For $f=X^2-Xa-b\in B[X;*]_{(2)}$, we denote a^2+4b by $\delta(f)$, which will be called the discriminant of f. Moreover, for $f,g\in B[X;*]_{(2)}$, if the factor rings $B[X;*]/fB[X;*]$ and $B[X;*]/gB[X;*]$ are B-ring isomorphic then we write $f\sim g$. Clearly the relation $\sim$ is an equivalence relation in $B[X;*]_{(2)}$. By $B[X;*]_{(2)}^{\sim}$, we denote the set of equivalence classes of $B[X;*]_{(2)}$ with respect to the relation $\sim$. As is easily seen, quadratic extensions considered in [1] and [4] can be written as factor rings $B[X;*]/fB[X;*]$ for some B, $*$, and $f\in B[X;*]_{(2)}$. Hence $B[X;*]_{(2)}^{\sim}$ can be regarded as the set of (B-ring) isomorphism classes of free quadratic extensions with multiplication defined by $*$. The details will be given in §2 and §3.

In §1, we shall make some remarks on free quadratic (Galois) extensions, which contains preliminary Lemmas.

In §2, we consider $B[X;\rho]_{(2)}$ and prove that for $f\in B[X;\rho]_{(2)}$, f is Galois if and only if $\delta(f)$ is inversible in B. Moreover, we shall study the set $B[X;\rho]_{\widetilde{(2)}}$ and shall prove that if there exists a Galois polynomial in $B[X;\rho]_{(2)}$ then $B[X;\rho]_{\widetilde{(2)}}$ forms an abelian semigroup (under some composition) such that for $g\in B[X;\rho]_{(2)}$, g is Galois if and only if the element C of $B[X;\rho]_{\widetilde{(2)}}$ with $C\ni g$ is inversible in the semigroup. This study contains the results of Kishimoto [4, §2].

In §3, we consider $B[X;D]_{(2)}$ and study the separable (Galois) polynomials of $B[X;D]_{(2)}$ and the structure of $B[X;D]_{\widetilde{(2)}}$. In the study, the discriminants of polynomials in $B[X;D]_{(2)}$ play important rôles. Indeed, if there exists a separable polynomial in $B[X;D]_{(2)}$ whose discriminant is inversible in B then for $g\in B[X;D]_{(2)}$, g is separable if and only if $\delta(g)$ is inversible in B. Moreover, we shall present some conditions that polynomials in $B[X;D]_{(2)}$ are separable (Galois). Further, we shall study the sets $B[X;D]_{\widetilde{(2)}}$ and $B[X;D]_{\widetilde{(2)},a}=\{C\in B[X;D]_{\widetilde{(2)}};\ C\ni X^2-Xa-b$ (a is fixed)$\}$ which form abelian groups under some conditions. The study also contains some generalizations of the results of Kishimoto [4, Th. 3.5 and its corollary].

1. Preliminary lemmas. For a ring extension A/B and a set $\mathfrak{S}$ of automorphisms in A, we shall use the following conventions: $J(\mathfrak{S}, A)=\{a\in A;\ \sigma(a)=a$ for all $\sigma\in\mathfrak{S}\}$, and $\mathfrak{J}(B,\mathfrak{S})=\{\sigma\in\mathfrak{S};\ \sigma(b)=b$ for all $b\in B\}$. Moreover, a ring extension A/B is called $\mathfrak{G}$-Galois if $\mathfrak{G}$ is a group of B-ring automorphisms in A, $J(\mathfrak{G}, A)=B$, and there are elements $a_1,\cdots,a_n,a_1^*,\cdots,a_n^*$ such that $\sum_i a_i\sigma(a_i^*)=\delta_{1,\sigma}$ (Kronecker's delta) for all σ in $\mathfrak{G}$ (cf. [5]).

First, we shall prove the following

Lemma 1.1. *Let A be a ring extension of B with $A=xB+B$, and assume that there is a B-ring automorphism σ in A such that $x-\sigma(x)$ is inversible in A. Then $\{x, 1\}$ is a right free B-basis of A, and $J(\sigma, A)=B$.*

Proof. Let $0=xb_1+b_0$ where $b_1, b_0\in J(\sigma, A)$. Then $0=(xb_1+b_0)-\sigma(xb_1+b_0)=(x-\sigma(x))b_1$. Since $x-\sigma(x)$ is inversible, we have $b_1=0$, and so, $b_0=0$. Thus $\{x, 1\}$ is right $J(\sigma, A)$-free. Since $B\subset J(\sigma, A)$ and $A=xB+B$, it follows that $\{x, 1\}$ is a right free $J(\sigma, A)$-basis of A, and $B=J(\sigma, A)$.

Lemma 1. 2. *Let A be a $\mathfrak{G}$-Galois extension of B such that $A=xB+B=Bx+B\neq B$. Then $\mathfrak{G}$ is of order 2, and for $\sigma\neq 1$ in $\mathfrak{G}$, $x-\sigma(x)$ is inversible in A. Moreover, $\{x, 1\}$ is a right free B-basis of A and is also a left free B-basis of A.*

Proof. Since A is $\mathfrak{G}$-Galois over B, there exist elements $u_1, \cdots, u_n, v_1, \cdots, v_n$ in A such that

$$\textstyle\sum_i u_i\tau(v_i) = \delta_{1,\tau} \text{ for all } \tau \in \mathfrak{G}.$$

Hence $\sum_i \tau^{-1}(u_i)v_i = \delta_{1,\tau}$ for all $\tau \in \mathfrak{G}$, that is,

$$\textstyle\sum_i \tau(u_i)v_i = \delta_{\tau,1} \text{ for all } \tau \in \mathfrak{G}.$$

Now, we set $v_i=b_ix+c_i$ where b_i, $c_i\in B$, $i=1, \cdots, n$. Then for $\tau\in\mathfrak{G}$, we have

$$\textstyle\sum_i u_i\tau(v_i) = \sum_i u_i\tau(b_ix + c_i) = (\sum_i u_ib_i)\tau(x) + \sum_i u_ic_i.$$

Let $\tau\neq 1$ be an arbitrary element of $\mathfrak{G}$. Then

$$\begin{aligned} 1 &= \textstyle\sum_i u_iv_i - \sum_i u_i\tau(v_i) \\ &= \{(\textstyle\sum_i u_ib_i)x + \sum_i u_ic_i\} - \{(\sum_i u_ib_i)\tau(x) + \sum_i u_ic_i\} \\ &= (\textstyle\sum_i u_ib_i)\,(x - \tau(x)). \end{aligned}$$

This implies that $x - \tau(x)$ has a left inverse. By a similar method, we see that $x - \tau(x)$ has a right inverse. Hence $x - \tau(x)$ is inversible in A. Next, let τ_1, $\tau_2\in\mathfrak{G}$ and $\tau_i\neq 1$ $(i = 1, 2)$. Then $x - \tau_1(x) = (\sum_i u_ib_i)^{-1} = x - \tau_2(x)$, and whence $\tau_1(x)= x - (\sum_i u_ib_i)^{-1} = \tau_2(x)$. Since $A = xB + B$ and the τ_i are B-ring automorphisms of A, it follows that $\tau_1 = \tau_2$. Hence the order of $\mathfrak{G}$ is not greater than 2. Noting $A\neq B$, we see that $\mathfrak{G}$ is of order 2. The other assertions are idrect consequences of Lemma 1. 1.

Lemma 1. 3. *Let A be a ring extension of B such that $A=xB+B$ and $xB\cap B=\{0\}$. Let S be a subset of B such that $BSB\,(=\sum_{s\in S}BsB)\neq B$ and $xs=sx$ for all $s\in S$. Then $ASA=xBSB+BSB$, $ASA\cap B=BSB$, and the factor ring A/ASA is a ring extension of $\bar{B}=(B+ASA)/ASA\cong B/BSB$. If A is separable over B then A/ASA is separable over $\bar{B}$.*

Proof. We set $x^2 = xa + b$. Then, for each $s\in S$, we have $xBsB + BsB \subset AsA=(xB+B)s(xB+B) = (xB+B)\,(sxB+sB)\subset xBxsB+BxsB + xBsB + BsB \subset x(xB + B)sB + (xB + B)sB + xBsB + BsB \subset (xa+b)BsB + xBsB+ BsB = xBsB+ BsB$, and hence $AsA = xBsB+BsB$. This implies that $ASA = xBSB+ BSB$. Since $xB\cap B=\{0\}$, $ASA\cap B=BSB$. Thus the factor ring A/ASA is a ring extension of $\bar{B}(\neq\{0\})$. Now, set

$\bar{A} = A/ASA$,. $\bar{u} = u + ASA$ for each $u \in A$, and assume that A is separable over B. Then, there exists a (left)B-(right)B-homomorphism $\phi : A \otimes_B A \to A$ such that $\phi(a_1 \otimes a_2) = a_1 a_2$ $(a_1, a_2 \in A)$ and ϕ splits. Then, the ϕ induces a (left)$\bar{B}$-(right)$\bar{B}$-homomorphism $\bar{\phi} : \bar{A} \otimes_{\bar{B}} \bar{A} \to \bar{A}$ with $\bar{\phi}(\bar{a}_1 \otimes \bar{a}_2) = \bar{a}_1 \bar{a}_2$ $(\bar{a}_1, \bar{a}_2 \in \bar{A})$. Clearly, the $\bar{\phi}$ splits. Hence $\bar{A}$ is separable over $\bar{B}$.

Lemma 1.4. *Let A be a $\mathfrak{G}$-Galois extension of B such that $A = xB + B = Bx + B \neq B$ and $\mathfrak{G} = \{1, \sigma\}$. Let S be a subset of B such that $BSB \neq B$ and $sx = xs$ for all $s \in S$. Then, $ASA = xBSB + BSB = BSBx + BSB$, $ASA \cap B = BSB$, and the factor ring A/ASA is a Galois extension of $(B + ASA)/ASA \cong B/BSB$ with Galios group $\bar{\mathfrak{G}} = \{\bar{1}, \bar{\sigma}\}$ $(\bar{1} \neq \bar{\sigma})$ where $\bar{1}$ and $\bar{\sigma}$ are automorphisms of A/ASA induced by 1 and σ.*

Proof. By Lemma 1.2, $\{x, 1\}$ is a right free B-basis of A and is also a left free B-basis of A. Hence by Lemma 1.3, we have $ASA = xBSB + BSB = BSBx + BSB$ and $ASA \cap B = BSB$. Now, we set $\bar{A} = A/ASA$, $\bar{B} = (B + ASA)/ASA$, $\bar{B}_0 = J(\bar{\mathfrak{G}}, \bar{A})$ and $\bar{a} = a + ASA$ for each $a \in A$. By Lemma 1.2, $x - \sigma(x)$ is inversible in A, and so is $\bar{x} - \bar{\sigma}(\bar{x})$ in $\bar{A}$. Noting $\bar{B} \subset \bar{B}_0$, we have $\bar{A} = \overline{x B_0} + \bar{B}_0 = \bar{x}\bar{B} + \bar{B}$. Hence, by Lemma 1.1, we obtain $\bar{B} = \bar{B}_0$. Since A is Galois over B, there exist elements $u_1, \cdots, u_n, v_1, \cdots, v_n$ in A such that $\sum_i u_i \tau(v_i) = \delta_{1,\tau}$ for all $\tau \in \mathfrak{G}$. This implies $\sum_i \bar{u}_i \bar{\tau}(\bar{v}_i) = \delta_{\bar{1},\bar{\tau}}$ for all $\bar{\tau} \in \bar{\mathfrak{G}}$. Therefore, we conclude that $\bar{A}$ is a Galois extension of $\bar{B}$.

Next, we shall prove the following

Lemma 1.5. *Let A be a ring extension of B such that $A = xB + B = Bx + B$ and $\{x, 1\}$ is a right free B-basis. Let $x^2 = xa + b = ax + b$ and $ab = ba$. Moreover, write $\beta x = x\beta^* + \beta'$ for each $\beta \in B$ and assume $\beta^{*\prime} = \beta'^{*}$ for all $\beta \in B$. If $a^2 + 4b$ is inversible in B then A is Galois over B.*

Proof. For any $\beta \in B$, we have $\beta(xa + b) = (x\beta^* + \beta')a + \beta b = x\beta^* a + (\beta' a + \beta b)$, and $\beta x^2 = (x\beta^* + \beta')x = x\beta^* x + \beta' x = x(x\beta^{**} + \beta^{*\prime}) + x\beta'^{*} + \beta'' = x^2\beta^{**} + x(\beta^{*\prime} + \beta'^{*}) + \beta'' = (xa + b)\beta^{**} + 2x\beta^{*\prime} + \beta'' = x(a\beta^{**} + 2\beta^{*\prime}) + b\beta^{**} + \beta''$. This implies $\beta^* a = a\beta^{**} + 2\beta^{*\prime}$. Since $\{\beta^* ; \beta \in B\} = B$, it follows that $\beta a = a\beta^* + 2\beta'$ for all $\beta \in B$. Hence we obtain that for any $\beta \in B$,

$$\begin{aligned}\beta(a - x) = \beta a - \beta x = \beta a - x\beta^* - \beta' &= -x\beta^* + (a\beta^* + 2\beta') - \beta' \\ &= (a - x)\beta^* + \beta'.\end{aligned}$$

Moreover, we have

$$(a-x)^2=a^2-2xa+x^2=a^2-2xa+xa+b=(a-x)a+b.$$

Hence the mapping $\sigma : xb_1 + b_0 \to (a - x)b_1 + b_0$ $(b_1,\ b_0 \in B)$ is a B-ring automorphism of A. Now, we assume that a^2+4b is inversible in B. Then, since $(a-2x)^2=a^2-4xa+4x^2=a^2+4b$, the difference $a-2x=(a-x)-x$ is inversible in A. Hence $\sigma \neq 1$ and $\sigma^2=1$. If $xb_1 + b_0 \in J(\sigma,\ A)$ $(b_1,\ b_0 \in B)$ then $xb_1+b_0=\sigma(x)b_1+b_0=(a-x)b_1+b_0$, and so, $(a-2x)b_1=0$, which implies that $b_1=0$. Now, we set $u_1=(a-2x)^{-1}(a-x)$, $u_2=(a-2x)^{-1}$, $v_1=1$, and $v_2=-x$. Then $\sum_i u_i\tau(v_i)=\delta_{1,\tau}$ for all $\tau \in \{1,\ \sigma\}$. Hence, it follows that A is a Galois extension of B with Galois group $\{1,\ \sigma\}$, completing the proof.

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 $b \in B$, b_l (resp. b_r) denotes the left (resp. right) multiplication of B determined by b.

2. On $B[X;\ \rho]_{(2)}$. In this section, we study $B[X;\ \rho]_{(2)}$, the subset of $B[X;\ \rho]$. As in [4], we shall use the following conventions: $B_1=J(\rho,\ B)$; $Z_1=Z\cap B_1$; $B(\rho^n)=\{u \in B\ ;\ \alpha u=u\rho^n(\alpha)$ for all $\alpha \in B\}$ (where n is any integer); $B_1(\rho^n)=B(\rho^n)\cap B_1$.

Now, let $f=X^2-Xa-b \in B[X;\ \rho]_{(2)}$. Then, the factor ring $A=B[X;\ \rho]/fB[X;\ \rho]$ is a quadratic extension of B such that for $x=X+fB[X;\ \rho]$,

$$A=B+xB,\quad \alpha x=x\rho(\alpha)\quad \text{for all } \alpha \in B,$$
$$x^2=xa+b=ax+b,\quad \text{and}$$
$$\{1,\ x\}\ \text{is a right free } B\text{-basis.}$$

Then we have $xa=ax$, $x^3=x(xa+b)=(xa+b)x$, and $\alpha x^2=x^2\rho^2(\alpha)$ for all $\alpha \in B$. From these equalities, it follows that

$$(2,\ 0)\qquad a \in B_1(\rho)\quad \text{and}\quad b \in B_1(\rho^2).$$

Clearly $ab=ba$, $xa=ax$, and $xb=bx$. Conversely, if a system $\{\rho,\ a,\ b\}$ $(a,\ b \in B)$ satisfies the condition (2, 0) then

$$X^2-Xa-b \in B[X;\ \rho]_{(2)}.$$

Hence, it follows that

$$(2,\ \text{i})\qquad B[X;\ \rho]_{(2)}=\{X^2-Xa-b\ ;\ a \in B_1(\rho)\ \text{and}\ b \in B_1(\rho^2)\}.$$

For any $f=X^2-Xa-b \in B[X;\ \rho]_{(2)}$, we denote the factor ring $B[X;\ \rho]/fB[X;\ \rho]$ by $B[x;\ \rho,\ a,\ b]$ (or, by $B[x_f]$) where $x=x_f=X+$

$fB[X\,;\,\rho]$. First, we shall prove the following

Lemma 2.1. *Let $f = X^2 - Xa - b \in B[X\,;\,\rho]_{(2)}$. Then f is separable over B if and only if there exist elements b_1, b_2, b_3 and b_4 in B such that*

(2, ii) $1 = bb_1 + b_4$ (2, iii) $ab_1 + b_2 + b_3 = 0$

(2, iv) $bb_1 = ab_2 + \rho(b_4)$ (2, v) $\rho(b_2) = b_3$

(2, vi) $b_4 \in Z$ (2, vii) $b_1 \in B(\rho^{-2})$

(2, viii) $b_2 \in B(\rho^{-1})$.

Proof. We set $A = B[x\,;\,\rho,\,a,\,b]$ and assume f is separable over B. Then, the (left)B-(right)B-homomorphism

$$\phi : A \otimes_B A \rightarrow A \quad (\textstyle\sum_i a_i \otimes b_i \rightarrow \sum_i a_i b_i)$$

splits. Hence there exists an element e in $A \otimes_B A$ such that $\phi(e) = 1$ and $(c\otimes 1)e = e(1\otimes c)$ for all $c \in A$. Since $A\otimes_B A = (x\otimes x)B + (x\otimes 1)B + (1\otimes x)B + (1\otimes 1)B$, we may write

$$e = (x\otimes x)b_1 + (x\otimes 1)b_2 + (1\otimes x)b_3 + (1\otimes 1)b_4$$

where $b_i \in B$, $i = 1, \cdots, 4$. The equality $\phi(e) = 1$ implies

$$x(ab_1 + b_2 + b_3) + bb_1 + b_4 = 1.$$

Moreover, we have

$(x\otimes 1)e = (x\otimes x)\,(ab_1 + b_3) + (x\otimes 1)\,(ab_2 + b_4) + (1\otimes x)bb_1 + (1\otimes 1)bb_2$

$e(1\otimes x) = (x\otimes x)\,(a\rho(b_1) + \rho(b_2)) + (x\otimes 1)b\rho(b_1) + (1\otimes x)\,(a\rho(b_3) + \rho(b_4)) + (1\otimes 1)b\rho(b_3)$, and for each $\alpha \in B$,

$(\alpha\otimes 1)e = (x\otimes x)\rho^2(\alpha)b_1 + (x\otimes 1)\rho(\alpha)b_2 + (1\otimes x)\rho(\alpha)b_3 + (1\otimes 1)\alpha b_4$

$e(1\otimes\alpha) = (x\otimes x)b_1\alpha + (x\otimes 1)b_2\alpha + (1\otimes x)b_3\alpha + (1\otimes 1)b_4\alpha$.

Hence we obtain

(a) $ab_1 + b_2 + b_3 = 0$ (b) $bb_1 + b_4 = 1$

(c) $ab_1 + b_3 = a\rho(b_1) + \rho(b_2)$ (d) $ab_2 + b_4 = b\rho(b_1)$

(e) $bb_1 = a\rho(b_3) + \rho(b_4)$ (f) $bb_2 = b\rho(b_3)$

(g) $\rho^2(\alpha)b_1 = b_1\alpha$ (h) $\rho(\alpha)b_2 = b_2\alpha$

(i) $\rho(\alpha)b_3 = b_3\alpha$ (j) $\alpha b_4 = b_4\alpha$

where α runs over all the elements of B. Conversely, if there exist elements b_1, b_2, b_3 and b_4 in B which satisfy the conditions (a)—(j) then the map ϕ (stated earlier) splits, that is, A is separable over B. Hence it suffices to prove that the system of conditions (2, ii—viii) is equivalent to that of conditions (a)—(j). Assume (2, ii—viii). Then, (2, vi—viii) imply (g), (h), (j), and (2, v, viii) imply that for each $\alpha \in B$, $\rho(\alpha)b_3 = \rho(\alpha)\rho(b_2) = \rho(\alpha b_2) = \rho(b_2\rho^{-1}(\alpha)) = \rho(b_2)\alpha = b_3\alpha$. Hence we have (i), that is,

$$b_3 \in B(\rho^{-1}). \tag{2, ix}$$

Moreover, (2, vi—ix) and (2, i, ii) imply that for each $i = 1, \cdots, 4$,

$$ab_i = b_i a = a\rho(b_i) = \rho(ab_i) = \rho(b_i a) = \rho(b_i)a \tag{2, x}$$

$$bb_i = b_i b = b\rho^2(b_i) = \rho^2(bb_i) = \rho^2(b_i b) = \rho^2(b_i)b, \tag{2, xi}$$

$$bb_1 = 1 - b_4 = 1 - \rho^2(b_4).$$

As is easily seen, (2, x) and (2, iii, v) imply $ab_1 + \rho(b_2) + \rho(b_3) = 0$ and

$$\rho(b_2) = b_3,\ \rho(b_3) = b_2,\ ab_2 = a\rho(b_2) = ab_3 = a\rho(b_3). \tag{2, xii}$$

Further, (2, x—xii) and (2, iv) imply (c)—(f). Thus, (a)—(j) are contained in (2, ii—viii). Conversely, assume (a)—(j). Then (g)—(j) imply (2, vi—viii). Moreover, (g)—(j) and (2, i) imply (2, x). As is easily seen, (2, x), (a) and (c) imply (2, xii) which contains (2, v). Clearly, (2, xii) and (e) imply (2, iv). Thus, (2, ii—viii) are contained in (a)—(j). This completes the proof.

Now, by (2, viii, ix, xii) and (2, xi), we have

$$b_2^2 = b_2 b_3 = b_3^2 = b_3 b_2 \tag{2, xiii}$$

$$\rho^2(b_4) = b_4. \tag{2, xiv}$$

For $i = 2$ and 3, $b_1 b_i = \rho^2(b_i)b_1 = b_i b_1$ (by (2, vii, xii)). This and (2, vi, x — xiv) imply

(2, xv) $uv = vu$ for each pair $u,\ v \in \{a,\ b,\ b_1,\ b_2,\ b_3,\ b_4,\ \rho(b_4)\}$
$rs = sr$ for each pair $r,\ s \in \{a,\ b,\ \rho(b_1),\ b_2,\ b_3,\ b_4,\ \rho(b_4)\}$.

Moreover, (2, iii, xii, xiii) imply

$$a^2 b_1^2 = 4b_2^2 = 4b_3^2,\ a^2 b_1 + 2ab_2 = a^2 b_1 + 2ab_3 = 0 \tag{2, xvi}$$

and, (2, ii, iv, xii, xiv) imply

$$1 = bb_1 + b_4 = b_4 + \rho(b_4) + ab_2 = b(b_1 + \rho(b_1)) - ab_2. \tag{2, xvii}$$

These equalities will be used lately in our study.

Next, we shall prove the following

Lemma 2.2. *Let $f = X^2 - Xa - b \in B[X;\rho]_{(2)}$ and f separable over B. Let $\{b_1, b_2, b_3, b_4\}$ be a system of elements of B which satisfies the conditions* (2, ii—viii). *Then $\delta(f)B = B\delta(f)$ ($\delta(f) = a^2 + 4b$), and*

$$2(bb_1 + \rho(b_4)) = \delta(f)b_1 \tag{2, xviii}$$

(2, xix) $\quad 4 = \delta(f)\,(b_1 + \rho(b_1)),$ *and* $a = \delta(f)\,(b_1b_4 - b_2^2)a.$

Proof. For each $\alpha \in B$, one will easily see that $\alpha\delta(f) = \alpha(a^2+4b) = (a^2+4b)\rho^2(\alpha) = \delta(f)\rho^2(\alpha)$. Hence $\delta(f)B = B\delta(f)$. Now, we shall prove (2, xviii) and (2, xix).

$$\begin{aligned}
\delta(f)b_1 &= (a^2+4b)b_1 = a^2b_1 + 4bb_1 = a(ab_1) + 4(bb_1) \\
&= a(-b_2 - b_3) + 4(\rho(b_4) + ab_2) && \text{(by (2, iii, iv))} \\
&= -2ab_2 + 4\rho(b_4) + 4ab_2 && \text{(by (2, xii))} \\
&= 2ab_2 + 4\rho(b_4) = 2(ab_2 + 2\rho(b_4)) \\
&= 2(bb_1 - \rho(b_4) + 2\rho(b_4)) && \text{(by (2, iv))} \\
&= 2(bb_1 + \rho(b_4))\,. \\
\delta(f)\,(b_1 + \rho(b_1)) &= \delta(f)b_1 + \delta(f)\rho(b_1) = \delta(f)b_1 + \rho(\delta(f)b_1) \\
&= 2(bb_1 + \rho(b_4)) + 2\rho(bb_1 + \rho(b_4)) && \text{(by (2, xviii))} \\
&= 2bb_1 + 2\rho(b_4) + 2\rho(bb_1) + 2b_4 && \text{(by (2, xiv))} \\
&= 2(bb_1 + b_4) + 2(\rho(bb_1) + \rho(b_4)) \\
&= 2 + 2 = 4 && \text{(by (2, ii)).} \\
\delta(f)(b_1b_4 - b_2^2)a &= (a^2+4b)\,(b_1b_4 - b_2^2)a \\
&= a((a^2+4b)b_1)b_4 - a(a^2+4b)b_2^2 && \text{(by (2, xv))} \\
&= 2a(\rho(b_4) + bb_1)b_4 - a(a^2b_2^2 + b(4b_2^2)) && \text{(by (2, xviii))} \\
&= 2a(b_4 + bb_1)b_4 - a(a^2b_2^2 + ba^2b_1^2) && \text{(by (2, x, xvi))} \\
&= 2ab_4 - a(a^2b_2^2 + b(a^2b_1)b_1) && \text{(by (2, ii))} \\
&= 2ab_4 - a(a^2b_2^2 + b(-2ab_2)b_1) && \text{(by (2, xvi))} \\
&= a(2b_4 - a(ab_2 - 2bb_1)b_2) && \text{(by (2, xv))} \\
&= a(2b_4 - a(bb_1 - \rho(b_4) - 2bb_1)b_2) && \text{(by (2, iv))} \\
&= a(2b_4 - a(-b_4 - bb_1)b_2) && \text{(by (2, x))} \\
&= a(2b_4 + ab_2) && \text{(by (2, ii))} \\
&= a(b_4 + \rho(b_4) + ab_2) && \text{(by (2, x))} \\
&= a(b_4 + bb_1) = a && \text{(by (2, ii, iv)).}
\end{aligned}$$

This completes the proof.

Lemma 2. 3. *Let* $f = X^2 - b \in B[X\,;\,\rho]_{(2)}$. *Then*

(i) f *is separable over* B *if and only if* b *is inversible and there exists an element* z *in* Z *such that* $z + \rho(z) = 1$.

(ii) f *is Galois over* B *if and only if* $2b$ *is inversible.*

Proof. (i). Assume that f is separable over B. Then, by

(2, xvii) and (2, xv), we have $1=b(b_1+\rho(b_1))=(b_1+\rho(b_1))b$. Hence b is inversible in B. Since $\rho(bb_1)=b\rho(b_1)$, $1=bb_1+\rho(bb_1)$. Moreover, by (2, ii, vi), we have $bb_1=1-b_4\in Z$. Conversely, assume that b is inversible in B and there exists an element z in Z such that $z+\rho(z)=1$. Then $1=b(b^{-1}z)+\rho(z)$, $b(b^{-1}z)=\rho(\rho(z))$, $\rho(z)\in Z$, and $b^{-1}z\in B(\rho^{-2})$. Hence, the system $\{b_1=b^{-1}z,\ b_2=b_3=0,\ b_4=\rho(z)\}$ satisfies the conditions (2, ii—viii). Thus f is separable over B. (ii). We set $A=B[x;\rho, 0, b]$. First, we assume that $2b$ is inversible in B. Then $\delta(f)=4b$ is inversible in B. Hence by Lemma 1. 5, A is Galois over B. Conversely, assume that A is $\mathfrak{G}$-Galois over B. By Lemma 1. 2, $\mathfrak{G}$ is of order 2. Hence we may write $\mathfrak{G}=\{1, \sigma\}$ $(1\neq\sigma)$. Then, by [5, Th. 1. 5], A is separable over B, and whence, by (i), b is inversible in B. Now, we suppose that 2 is not inversible in B. Then $2A$ is a proper ideal of A. We set $\bar{A}=A/2A$ (the factor ring of A modulo $2A$), $\bar{B}=(B+2A)/2A$, $\bar{u}=u+2A$ for each $u\in A$, and $\bar{\mathfrak{G}}=\{\bar{1}, \bar{\sigma}\}$ will mean the group of automorphisms of $\bar{A}$ induced by $\{1, \sigma\}$. Then, by Lemma 1. 4, $\bar{A}$ is a Galois extension of $\bar{B}$ with Galois group $\bar{\mathfrak{G}}\neq\{\bar{1}\}$, and $\bar{A}=\bar{x}\bar{B}+\bar{B}=\bar{B}\bar{x}+\bar{B}\neq\bar{B}\,(\bar{2}=\bar{0})$. Hence by Lemma 1. 2, $\{\bar{x}, \bar{1}\}$ is a right free $\bar{B}$-basis of $\bar{A}$, and the difference $\bar{x}-\bar{\sigma}(\bar{x})=\bar{x}+\bar{\sigma}(\bar{x})$ is inversible in $\bar{A}$. We set here $\bar{d}=\bar{x}-\bar{\sigma}(\bar{x})$. Then $\bar{\sigma}(\bar{d})=\bar{\sigma}(\bar{x}+\bar{\sigma}(\bar{x}))=\bar{\sigma}(\bar{x})+\bar{x}=\bar{d}$. Hence $\bar{d}\in\bar{B}$, and so, we may consider d as an element of B. Since $\bar{x}^2=\bar{b}$, we have $\bar{b}=\bar{\sigma}(\bar{x})^2=(\bar{x}+\bar{d})^2=\bar{x}^2+\bar{x}(\bar{d}+\bar{\rho}(\bar{d}))+\bar{d}^2=\bar{x}(\bar{d}+\bar{\rho}(\bar{d}))+\bar{b}+\bar{d}^2$. Since $\{\bar{x}, \bar{1}\}$ is right $\bar{B}$-free, it follows that $\bar{d}^2=\bar{0}$, and whence $\bar{d}$ is not inversible in $\bar{A}$. This is a contradiction. We conclude therefore that 2 is inversible in A.

Remark 2. 4. We shall present an example of $B[X;\rho]_{(2)}$ such that it contains a separable polynomial which is not Galois. Let $F=\mathrm{GF}(2^2)$. Since the extension $F/\mathrm{GF}(2)$ is Galois, there exists an automorphism ρ of F such that $\rho^2=1$ and $\rho\neq1$. Hence there is an element $z\in F$ with $z+\rho(z)=1$. Consider here $F[X;\rho]$. Then $F[X;\rho]_{(2)}=\{X^2,\ X^2+1\}$ By Lemma 2. 3, X^2 is not separable over B, and X^2+1 is separable over B but it is not Galois over B.

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

Theorem 2. 5. *For $f\in B[X;\rho]_{(2)}$, the following conditions are equivalent.*

(a) *f is Galois over B.*

(b) *$\delta(f)$ is inversible in B.*

(b′) *$f'B[X;\rho]+fB[X;\rho]=B[X;\rho]$ where f' is the derivative* *of f.*

Proof. Let $f=X^2-Xa-b\in B[X;\rho]_{(2)}$, and set $A=B[x;\rho,a,b]$. Then $f'=2X-a$ and $(2x-a)^2=4x^2-4xa+a^2=a^2-4xa+4(xa+b)=a^2+4b=\delta(f)$. This shows that (b) and (b′) are equivalent. Moreover, by Lemma 1.5, we see that (b) implies (a). To see the converse, we assume (a) and suppose that $\delta(f)$ is not inversible in B. Then, by Lemma 1.2, A is a Galois extension of B with Galois group of order 2, and by [5, Th. 1.5], f is separable over B. Hence by Lemma 2.2, the elements 4 and a are contained in $\delta(f)B=B\delta(f)\neq B$. Since $\delta(f)\in B_1$, $\delta(f)x=x\delta(f)$. We set here $\bar{A}=A/\delta(f)A$ (the factor ring of A modulo $\delta(f)A$), $\bar{B}=(B+\delta(f)A)/\delta(f)A$, and $\bar{u}=u+\delta(f)A$ for each $u\in A$. Then from Lemma 1.4, it follows that $\bar{A}$ is Galois over $\bar{B}$ and $\bar{A}=\bar{x}\bar{B}+\bar{B}=\bar{B}\bar{x}+\bar{B}\neq\bar{B}$. Hence by Lemma 1.2, $\{\bar{x},\bar{1}\}$ is a right free $\bar{B}$-basis of $\bar{A}$. Since $\rho(\delta(f))=\delta(f)$, ρ induces an automorphism of $\bar{B}$, which will be denoted by $\bar{\rho}$. Then $\bar{\alpha}\bar{x}=\bar{x}\bar{\rho}(\bar{\alpha})$ for each $\bar{\alpha}\in\bar{B}$, and $\bar{x}^2=\bar{b}$. Hence by (2, i), $X^2-\bar{b}$ is a polynomial of $\bar{B}[X;\bar{\rho}]_{(2)}$ which is Galois over $\bar{B}$. Therefore, it follows from Lemma 2.3 (ii) that $\bar{2}$ is inversible in $\bar{B}$. However, since $4\in\delta(f)B$, we have $0=\bar{4}=\bar{2}^2$. This is a contradiction. Thus we conclude that $\delta(f)$ is inversible in B.

Corollary 2.6. *Let $f=X^2-Xa\in B[X;\rho]_{(2)}$. Then the following conditions are equivalent.*

(a) *f is Galois over B.*

(b) *a is inversible in B.*

(c) *f is separable over B.*

Proof. By Th. 2.5, (a) and (b) are equivalent. By [5, Th. 1.5], (a) implies (c). Moreover, by (2, xvii), we see that (c) implies (b). Thus we obtain the assertion.

Next, we consider the following conditions.

(C_1) 2 is inversible in B.

(C_2) $\rho|Z=1$.

(C_3) ρ is an inner automorphism of B.

(C_3') $B_1(\rho)$ contains an inversible element of B.

(C_3'') $B[X;\rho]_{(2)}$ contains an element $f=X^2-Xa$ which is separable over B.

In case (C_1), it follows from the result of K. Kishimoto [4, Th. 1.2] that for $f\in B[X;\rho]_{(2)}$, f is separable over B if and only if f is Galois over B, and this is equivalent to that $\delta(f)$ is inversible in B.

Clearly (C_3) implies (C_2), and (C_3) is equivalent to (C_3'). Moreover, by Cor. 2. 6, (C_3') and (C_3'') are equivalent.

Now, we shall prove the following

Theorem 2. 7. *Assume that there holds one of the conditions* (C_1) — (C_3''). *Then, for* $f \in B[X;\ \rho]_{(2)}$, *the following conditions are equivalent.*

(a) *f is Galois over B.*

(b) *$\delta(f)$ is inversible in B.*

(c) *f is separable over B.*

Proof. In virtue of Th. 2. 5 and [5, Th. 1. 5], it suffices to prove that (c) implies (b). Assume (c). Let $f = X^2 - Xa - b \in B[X;\ \rho]_{(2)}$, and set $A = B[x;\ \rho,\ a,\ b]$.

Case (C_1). The assertion follows from the result of [4, Th. 1. 2]. However, this is also obtained as an easy application of Lemma 2. 3 which is as follows. Set $y = x - 1/2$. Then $y^2 = (a^2 + 4b)/4$, and $A = yB + B$. Clearly $g = Y^2 - (a^2 + 4b)/4 \in B[Y;\ \rho]_{(2)}$, and this is separable over B. Hence, it follows from Lemma 2. 3 that $(a^2 + 4b)/4$ is inversible in B, and hence, $a^2 + 4b\ (= \delta(f))$ is inversible in B.

Case (C_2). Let $\{b_1,\ b_2,\ b_3,\ b_4\}$ be a system of elements of B which satisfies the conditions (2, ii—viii). Then, by (2, xvii, xviii), we have $1 = 2b_4 + ab_2$ and $2 = \delta(f)b_1$. Since $a = \delta(f)(b_1b_4 - b_2^2)a$ (2, xix), we have $1 = 2b_4 + ab_2 = \delta(f)\ (b_1b_4 + (b_1b_4 - b_2^2)ab_2)$. This shows that $\delta(f)$ is inversible in B, completing the proof.

In the rest of this section, we shall deal with the set of B-ring isomorphism classes of the extensions $B[x_f]/B$ ($f \in B[X;\ \rho]_{(2)}$). For elements g and $g_1 \in B[X;\ \rho]_{(2)}$, if $B[x_g] \cong B[x_{g_1}]$ (B-ring isomorphic) then we write $g \sim g_1$. Clearly, the relation $\sim$ is an equivalence relation in $B[X;\ \rho]_{(2)}$. By $B[X;\ \rho]_{\widetilde{(2)}}$, we denote the set of equivalence classes of $B[X;\ \rho]_{(2)}$ with respect to the relation $\sim$, and we write $C = \langle g \rangle$ if $C \in B[X;\ \rho]_{\widetilde{(2)}}$ and $g \in C$.

Now, we consider the following conditions.

(D_1) There is a Galois polynomial in $B[X;\ \rho]_{(2)}$.

(D_2) ρ^2 is an inner automorphism of B determined by some element in $U(B_1)$.

If f is a Galois polynomial in $B[X;\ \rho]_{(2)}$ then, by Th. 2. 5, $\delta(f) \in U(B) \cap B_1(\rho^2)$, which implies $\rho^2 = \delta(f)_l^{-1}\delta(f)_r$. This shows that ($D_1$) implies ($D_2$). In case ($C_1$), if $\rho^2 = \theta_l^{-1}\theta_r$ for some θ in $U(B_1)$ then $\theta \in B(\rho^2) \cap U(B_1)$, and by Th. 2. 5, the polynomial $X^2 - \theta$ is a Galois polynomial in $B[X;\ \rho]_{(2)}$; whence, the conditions (D_1) and (D_2) are equivalent. In [4], K. Kishimoto proved that if the conditions (C_1) and (D_2) are satisfied then the set $B[X;\ \rho]_{(2)}^{\sim}$ forms an abelian semi-group which is isomorphic to the (multiplicative) factor semi-group of Z_1 modulo the subgroup $\{z\rho(z);\ z\in U(Z)\}$. In our consideration, it will be showed that if the condition (D_1) is satisfied then $B[X;\ \rho]_{(2)}^{\sim}$ forms an abelian semi-group under some composition which is somewhat interest.

First, as a preliminary lemma, we shall prove the following

Lemma 2.8. *Assume* $\rho^2=\theta_l^{-1}\theta_r$ *for some* $\theta\in U(B_1)$. *Let* n *be an arbitrary integer. Then* $B(\rho^0)=Z$, $B(\rho^n)B(\rho^n)\subset B(\rho^{2n})=\theta^n Z$, $B_1(\rho^{2n})=\theta^n Z_1$, $\rho(B(\rho^n))=B(\rho^n)$, and $J(\rho^2,\ B)\supset B(\rho^n)$.

Proof. It is obvious that $B(\rho^0)=Z$. Now, let c be an arbitrary element of B. If β and $\beta'\in B(\rho)$ then $c\beta\beta'=\beta\rho(c)\beta'=\beta\beta'\rho^2(c)$. This implies $B(\rho)B(\rho)\subset B(\rho^2)$, and so, $B(\rho^n)B(\rho^n)\subset B(\rho^{2n})$. If $v\in B(\rho^2)$ then $cv=v\rho^2(c)=v\theta^{-1}c\theta$ which shows $v\theta^{-1}\in Z$, that is, $v\in\theta Z$. Conversely, if $z\in Z$ then $c(\theta z)=(c\theta)z=(\theta\rho^2(c))z=(\theta z)\rho^2(c)$, and hence $\theta z\in B(\rho^2)$. Thus we obtain $B(\rho^2)=\theta Z$. Since $\rho^{2n}=\theta_l^{-n}\theta_r^n$, it follows that $B(\rho^{2n})=\theta^n Z$, and $B_1(\rho^{2n})=B_1\cap B(\rho^{2n})=B_1\cap\theta^n Z=\theta^n Z_1$. Next, let β be in $B(\rho^n)$. Then $\rho^{-1}(c)\beta=\beta\rho^{n-1}(c)$, and hence $c\rho(\beta)=\rho(\beta)\rho^n(c)$. This implies $\rho(\beta)\in B(\rho^n)$. Moreover, since $\rho(c)\beta=\beta\rho^{n+1}(c)$, we have $c\rho^{-1}(\beta)=\rho^{-1}(\beta)\rho^n(c)$ which shows $\rho^{-1}(\beta)\in B(\rho^n)$. Hence it follows that $\rho(B(\rho^n))=B(\rho^n)$. Finally, since $\theta\beta=\beta\rho^n(\theta)=\beta\theta$, $\beta=\theta^{-1}\beta\theta=\rho^2(\beta)$, which shows that $B(\rho^n)\subset J(\rho^2,\ B)$.

Corollary 2.9. *Assume* $\rho^2=\theta_l^{-1}\theta_r$ *for some* $\theta\in U(B_1)$. *Let* u, u' $\in B_1(\rho)\cup B(\rho^2)\cup B(\rho^4)\cup Z$, $u_1\in B_1(\rho)$, *and* $\beta\in B(\rho)$. *Then* $uu'=u'u$, $u\beta=\beta u=\beta\rho(u)=\rho(u)\beta$, $u_1\beta=\beta u_1=u_1\rho(\beta)=\rho(\beta)u_1$, *and* $\beta^2=\beta\rho(\beta)=\rho(\beta)\beta$.

Proof. Let v and v' be in $\mathrm{B}(\rho^2)\cup\mathrm{B}(\rho^4)\cup Z$. Then, by Lemma 2.8, we have $vv'=v'v$. Since $\rho^2(\beta)=\beta$, $\theta\beta=\beta\theta$, and whence $v\beta=\beta v$. Moreover $u_1\beta=\beta\rho(u_1)=\beta u_1=u_1\rho(\beta)=\rho(\beta)\rho(u_1)=\rho(\beta)u_1$. Hence $\beta u=u\beta=\beta\rho(u)=\rho(u)\beta$, and $uu'=u'u$. Further, by Lemma 2.8, we have $\beta^2=\beta\rho(\beta)=\rho(\beta)\rho(\beta)=\rho(\beta)\rho^2(\beta)=\rho(\beta)\beta$.

Next, we shall prove the following

Lemma 2.10. *Assume* $\rho^2=\theta_l^{-1}\theta_r$ *for some* $\theta\in U(B_1)$. *Let* $g=X^2-Xu-v$, $g_1=X^2-Xu_1-v_1\in B[X;\ \rho]_{(2)}$. *Then,* $g\sim g_1$ *if and only if there exist elements* α, β *in* B *such that* $\alpha\in U(Z)$, $\beta\in B(\rho)$, $u=u_1\alpha+\beta+\rho(\beta)$, *and* $v=v_1\alpha\rho(\alpha)-u_1\alpha\beta-\beta^2$.

Proof. We consider $B[x_g]$ and $B[x_{g_1}]$. For the convenience, we set $x=x_g$ and $y=x_{g_1}$. First, we assume that there are elements α, $\beta\in B$ such that $\alpha\in U(Z)$, $\beta\in B(\rho)$, $u=u_1\alpha+\beta+\rho(\beta)$, and $v=v_1\alpha\rho(\alpha)-u_1\alpha\beta-\beta^2$. Then, for any $c\in B$, $c(y\alpha+\beta)=y\rho(c)\alpha+c\beta=y\alpha\rho(c)+\beta\rho(c)=(y\alpha+\beta)\rho(c)$, and $(y\alpha+\beta)^2=y(u_1\alpha+\rho(\beta)+\beta)\alpha+v_1\alpha\rho(\alpha)+\beta^2=yu\alpha+v+u_1\alpha\beta+\beta^2+\beta^2=yu\alpha+v+(u_1\alpha+\beta+\rho(\beta))\beta=yu\alpha+v+u\beta=(y\alpha+\beta)u+v$ (by Cor. 2. 9). Hence, noting $\alpha\in U(Z)$, the mapping $xc_1+c_2\rightarrow(y\alpha+\beta)c_1+c_2$ $(c_1, c_2\in B)$ is a B-ring isomorphism of $B[x]$ to $B[y]$. Thus we obtain $g\sim g_1$. Conversely, we assume that there is a B-ring isomorphism $\phi: B[x]\rightarrow B[y]$. Then $\phi(x)=y\alpha+\beta$ for some α, $\beta\in B$. Since $y=(y\alpha+\beta)c_1+c_2$ for some c_1 and $c_2\in B$, the element α is inversible in B. Now, for any $c\in B$, $\phi(cx)=\phi(x\rho(c))=(y\alpha+\beta)\rho(c)=y\alpha\rho(c)+\beta\rho(c)$, and $\phi(cx)=c\phi(x)=c(y\alpha+\beta)=y\rho(c)\alpha+c\beta$. Hence $\alpha\rho(c)=\rho(c)\alpha$ and $\beta\rho(c)=c\beta$ $(c\in B)$. This implies $\alpha\in U(Z)$ and $\beta\in B(\rho)$. Next, we note $\phi(x^2)=\phi(xu+v)=(y\alpha+\beta)u+v=y\alpha u+\beta u+v$ and $\phi(x^2)=\phi(x)^2=(y\alpha+\beta)^2=y(u_1\alpha+\rho(\beta)+\beta)\alpha+v_1\alpha\rho(\alpha)+\beta^2$ (by Cor. 2. 9). Then $\alpha u=(u_1\alpha+\rho(\beta)+\beta)\alpha$ and $\beta u+v=v_1\alpha\rho(\alpha)+\beta^2$. Hence it follows that $u=u_1\alpha+\beta+\rho(\beta)$, and $v=v_1\alpha\rho(\alpha)+\beta^2-\beta u=v_1\alpha\rho(\alpha)+\beta^2-\beta(u_1\alpha+\beta+\rho(\beta))=v_1\alpha\rho(\alpha)-u_1\alpha\beta-\beta^2$ (by Cor. 2. 9). This completes the proof.

Throughout the rest of this section, $\overline{\rho}$ will mean the restriction of ρ to Z. Then, one will easily see that for $p\in Z$, $p\in Z(\overline{\rho^n})$ if and only if $zp=p\rho''(z)$ for all $z\in Z$, where n is any integer. From this and Lemma 2. 10, we obtain the following

Corollary 2. 11. *Assume* $\rho^2=\theta_l^{-1}\theta_r$ *for some* $\theta\in U(B_1)$. *Then* $\overline{\rho}^2=1$, $Z(\overline{\rho})=\{p\in Z\,;\, zp=\rho(z)p$ *for all* $z\in Z\}$, *and* $Z[X;\overline{\rho}]_{(2)}=\{X^2-Xp-q\in Z[X;\overline{\rho}]\,;\, p,\ q\in Z_1$ *and* $p\in Z(\overline{\rho})\}$. *Moreover, for* $h=X^2-Xr-s$ *and* $h_1=X^2-Xr_1-s_1\in Z[X;\ \overline{\rho}]_{(2)}$, $h\sim h_1$ *if and only if there exist elements* α, $\beta\in Z$ *such that* $\alpha\in U(Z)$, $\beta\in Z(\overline{\rho})$, $r=r_1\alpha+\beta+\rho(\beta)$ *and* $s=s_1\alpha\rho(\alpha)-r_1\alpha\beta-\beta^2$.

Remark 2. 12. Assume $\rho^2=\theta_l^{-1}\theta_r$ for some $\theta\in U(B_1)$. Let S denote the subring of B generated by $B_1(\rho)\cup B(\rho^2)\cup Z$, and set $T=\{X^2-Xu-v\in B[X;\ \rho]\,;\ u, v\in S\}$. Then by Cor. 2. 9, S is a commutative ring. Let $f_i=X^2-Xu_i-v_i\in T$ $(i=1,\ 2)$ and $s_1\in S$. We write $f_1\times f_2=X^2-Xu_1u_2-(u_1{}^2v_2+v_1u_2{}^2+4v_1v_2)$, $s_1\times f_1=X^2-Xs_1u_1-s_1{}^2v_1$, and $f_1\times s_1=X^2-Xu_1s_1-v_1s_1{}^2$. Then, this composition is commutative and associative, i. e., $f_1\times f_2=f_2\times f_1$, $s_1\times f_1=f_1\times s_1$, and for $f\in T$, $(f\times f_1)\times f_2=f\times(f_1\times f_2)$, $s_1\times(f_1\times f_2)=(s_1\times f_1)\times f_2=(f_1\times s_1)\times f_2=f_1\times(s_1\times f_2)=f_1\times(f_2\times s_1)=(f_1\times f_2)\times s_1$. Moreover, for $s\in S$, $s\times(s_1\times f_1)=(ss_1)\times f_1=(f_1\times s)\times s_1$.

Hence this composition makes T an abelian S-semigroup. Further, as is easily seen, we have $\delta(f_1\times f_2)=\delta(f_1)\,\delta(f_2)$ and $\delta(f_1\times s_1)=\delta(f_1)s_1{}^2$. We identify the ring $Z[X,\bar{\rho}]$ with the subring of $B[X;\rho]$ consisting of polynomials with coefficients in Z. Then $B[X;\rho]_{(2)}\cup Z[X;\bar{\rho}]_{(2)}\subset T$.

Now, we shall prove the following

Lemma 2.13. *Assume $\rho^2=\theta_l^{-1}\theta_r$ for some $\theta\in U(B_1)$. Let g, $g_1\in B[X;\rho]_{(2)}$, h, $h_1\in Z[X;\rho]_{(2)}$, and $\xi\in U(Z_1)$. Then $g\sim g\times\xi\in B[X;\rho]_{(2)}$, and in particular, $h\sim h\times\xi\in Z[X;\bar{\rho}]_{(2)}$. Moreover, $g\times g_1\times\theta^{-1}\in Z[X;\bar{\rho}]_{(2)}$, $g\times h\in B[X;\rho]_{(2)}$, and $h\times h_1\in Z[X;\bar{\rho}]_{(2)}$.*

Proof. Let $g=X^2-Xu-v$ and $g_1=X^2-Xu_1-v_1$. Then $g\times\xi=X^2-Xu\xi-v\xi^2$, $u\xi\in B_1(\rho)$, and $v\xi^2\in B_1(\rho^2)$. Hence $g\times\xi\in B[X;\rho]_{(2)}$. If we set $\alpha=\xi$ and $\beta=0$ then $u\xi=u\alpha+\beta+\rho(\beta)$ and $v\xi^2=v\alpha\rho(\alpha)+u\alpha\beta+\beta^2$. Hence by Lemma 2.10, we have $g\times\xi\sim g$. Next, we consider $g\times g_1\times\theta^{-1}=X^2-X(uu_1)\theta^{-1}-(u^2v_1+vu_1{}^2+4vv_1)\theta^{-2}$. Then, by Lemma 2.8, we have $uu_1\in\theta Z_1$ and $u^2v_1+vu_1{}^2+4vv_1\in\theta^2Z_1$. Hence $uu_1\theta^{-1}\in Z_1$ and $(u^2v_1+vu_1{}^2+4vv_1)\theta^{-2}\in Z_1$. Moreover, by Cor. 2.9, we have that $(z-\rho(z))uu_1\theta^{-1}=0$ for all $z\in Z$. Hence by Cor. 2.11, we obtain $g\times g_1\times\theta^{-1}\in Z[X;\bar{\rho}]_{(2)}$. The other assertions will be easily seen from Lemma 2.8 and the fact that the sets $B_1(\rho)$, $B_1(\rho^2)$, $Z_1(\bar{\rho})$ and $Z_1(\bar{\rho}^2)$ are Z_1-submodules of B. This completes the proof.

If there is a Galois polynomial f in $B[X;\rho]_{(2)}$ then $\delta(f)\in U(B_1)$, $\rho^2=\delta(f)_l^{-1}\delta(f)_r$ (Th. 2.5); and whence, by Lemma 2.13, we have the mappings

μ_f: $B[X;\rho]_{(2)}\to Z[X;\bar{\rho}]_{(2)}$; $\mu_f(g)=f\times\delta(f)^{-1}\times g$, and

ν_f: $Z[X;\bar{\rho}]_{(2)}\to B[X;\rho]_{(2)}$; $\nu_f(h)=f\times h$.

Now, we shall prove the following lemma which plays an important rôle in our study.

Lemma 2.14. *Assume that there is a Galois polynomial f in $B[X;\rho]_{(2)}$. Then*

(i) *if $g\sim g_1$ in $B[X;\rho]_{(2)}$ then $\mu_f(g)\sim\mu_f(g_1)$.*

(ii) *If $h\sim h_1$ in $Z[X;\bar{\rho}]_{(2)}$ then $\nu_f(h)\sim\nu_f(h_1)$.*

(iii) *For each $g\in B[X;\rho]_{(2)}$, $g\sim\nu_f\mu_f(g)$, and moroever, g is Galois over B if and only if $\mu_f(g)$ is Galois over Z.*

(iv) *For each $h\in Z[X;\bar{\rho}]_{(2)}$, $h\sim\mu_f\nu_f(g)$, and moreover, h is Galois over Z if and only if $\nu_f(h)$ is Galois over B.*

Proof. Let $f=X^2-Xa-b$, and set $\theta=\delta(f)\,(=a^2+4b)$. (i).

Let $g=X^2-Xu-v$, $g_1=X^2-Xu_1-v_1 \in B[X; \rho]_{(2)}$, and $g \sim g_1$. Then, by Lemma 2.10, there exist elements α, $\beta \in B$ such that $\alpha \in U(Z)$, $\beta \in B(\rho)$, $u=u_1\alpha+\beta+\rho(\beta)$, and $v=v_1\alpha\rho(\alpha)-u_1\alpha\beta-\beta^2$. By Lemma 2.8 and Cor. 2.9, we have $au\theta^{-1}=(au_1\alpha+a\beta+a\rho(\beta))\theta^{-1}=au_1\theta^{-1}\alpha+2a\beta\theta^{-1}$ and $a\beta\theta^{-1} \in Z_1(\bar{\rho})$. Next, we note $a^2v+bu^2+4bv=a^2(v_1\alpha\rho(\alpha)-u_1\alpha\beta-\beta^2)+b(u_1\alpha+\beta+\rho(\beta))^2+4b(v_1\alpha\rho(\alpha)-u_1\alpha\beta-\beta^2)=a^2v_1\alpha\rho(\alpha)-a^2u_1\alpha\beta-a^2\beta^2+b(u_1\alpha u_1\alpha+\beta u_1\alpha+\rho(\beta)u_1\alpha+u_1\alpha\beta+\beta^2+\rho(\beta)\beta+u_1\alpha\rho(\beta)+\beta\rho(\beta)+\rho(\beta)\rho(\beta))+b(4v_1\alpha\rho(\alpha)-4u_1\alpha\beta-4\beta^2)$. Then, by Cor. 2.9, we obtain $(a^2v+bu^2+4bv)\theta^{-2}=(a^2v_1+bu_1{}^2+4bv_1)\theta^{-2}\alpha\rho(\alpha)-(au_1\theta^{-1})\alpha(a\beta\theta^{-1})-(a\beta\theta^{-1})^2$. This implies $\mu_f(g)\sim\mu_f(g_1)$ (Cor. 2.11). (ii). $h=X^2-Xr-s$, $h_1=X^2-Xr_1-s_1 \in Z[X; \bar{\rho}]_{(2)}$, and $h \sim h_1$. Then, by Cor. 2.11, there exist elements α, β in Z such that $\alpha \in U(Z)$, $\beta \in Z(\bar{\rho})$, $r=r_1\alpha+\beta+\rho(\beta)$, and $s=s_1\alpha\rho(\alpha)-r_1\alpha\beta-\beta^2$. By Cor. 2.9, we have $ar=ar_1\alpha+2a\beta$, $a\beta \in B_1(\rho)$, and $a^2s+br^2+4bs=a^2(s_1\alpha\rho(\alpha)-r_1\alpha\beta-\beta^2)+b(r_1\alpha+\beta+\rho(\beta))^2+4b(s_1\alpha\rho(\alpha)-r_1\alpha\beta-\beta^2)=(a^2s_1+br_1{}^2+4bs_1)\alpha\rho(\alpha)-(ar_1)\alpha(a\beta)-(a\beta)^2$. This rmplies $\nu_f(h)\sim\beta_f(h_1)$ (Lemma 2.10). (iii). Let $g=X^2-Xu-v \in B[X; \rho]_{(2)}$. Then, by Remark 2.12, we have $\nu_f\mu_f(g)=f\times((f\times\theta^{-1})\times g)=((f\times f)\times g)\times\theta^{-1}=X^2-Xa^2u\theta^{-1}-(a^4v+(2a^2b+4b^2)u^2+4(2a^2b+4b^2)v)\theta^{-2}=X^2-Xa^2u\theta^{-1}-((a^2+4b)^2v+2(a^2+4b)bu^2-4b^2u^2)\theta^{-2}=X^2-Xa^2u\theta^{-1}-(v-u(-2bu\theta^{-1})-(-2bu\theta^{-1})^2)$ (note $a^2+4b=\theta$). Moreover, since $a^2\theta^{-1}+4b\theta^{-1}=1$, we have $a^2u\theta^{-1}=u+2(-2bu\theta^{-1})$ and $-2bu\theta^{-1} \in B_1(\rho)$. This implies $g\sim\nu_f\mu_f(g)$ (Lemma 2.10). By Remark 2.12, we have $\delta(\mu_f(g))=\delta(f\times\theta^{-1}\times g)=\delta(f)\theta^{-2}\delta(g)=\theta^{-1}\delta(g)$, which shows that $\delta(g)$ is inversible in B if and only if $\delta(\mu_f(g))$ is inversible in Z. Hence by Th. 2.5, g is Galois over B if and only if $\mu_f(g)$ is Galois over Z. (iv). Let $h=X^2-Xr-s \in Z[X; \bar{\rho}]_{(2)}$. Then $\mu_j\nu_f(h)=(f\times\theta^{-1})\times(f\times h)=((f\times f)\times h)\times\theta^{-1}=X^2-Xa^2r\theta^{-1}-(a^4s+(2a^2b+4b^2)r^2+4(2a^2b+4b^2)s)\theta^{-2}=X^2-Xa^2r\theta^{-1}-(s-r(-2br\theta^{-1})-(-2br\theta^{-1})^2)$, $a^2r\theta^{-1}=r+2(-2br\theta^{-1})$, and $-2br\theta^{-1} \in Z_1(\rho)$ (Lemma 2.8). This shows that $h\sim\mu_j\nu_f(h)$ (Cor. 2.11). Since $\delta(\nu_f(h))=\delta(f\times h)=\theta\delta(h)$, h is Galois over Z if and only if $\nu_f(h)$ is Galois over B (Remark 2.12 and Th. 2.5). This completes the proof.

Next, we consider the sets $B[X; \rho]_{\widetilde{(2)}}$ and $Z[X; \bar{\rho}]_{\widetilde{(2)}}$ (the sets of equivalence classes in $B[X; \rho]_{(2)}$ and in $Z[X; \bar{\rho}]_{(2)}$ (respectively) with respect to the relations $\sim$). For the convenience, if $C \in B[X; \rho]_{\widetilde{(2)}}$ and $g \in C$ (resp. $C' \in Z[X; \bar{\rho}]_{\widetilde{(2)}}$ and $h \in C'$) then we write $C=\langle g\rangle$ (resp. $C'=\langle h\rangle$).

Now, if there is a Galois polynomial f in $B[X; \rho]_{(2)}$ then, by Lemma 2.14, we have the (well defined) mappings

$$\phi_f:\ B[X; \rho]_{\widetilde{(2)}} \to Z[X; \bar{\rho}]_{\widetilde{(2)}};\ \phi_f(\langle g\rangle)=\langle\mu_f(g)\rangle, \text{ and}$$

$$\psi_f:\ Z[X; \bar{\rho}]_{\widetilde{(2)}} \to B[X; \rho]_{\widetilde{(2)}};\ \psi_f(\langle h\rangle)=\langle\nu_f(h)\rangle$$

such that $\psi_f\phi_f=1$ and $\phi_f\psi_f=1$. Hence we obtain the following

Corollary 2.15. *Assume that there is a Galois polynomial f in $B[X;\rho]_{(2)}$. Then ϕ_f is one-to-one, and $\phi_f^{-1}=\psi_f$. Moreover, for $\langle g\rangle \in B[X;\rho]^{\sim}_{(2)}$ and $h\in\phi_f(\langle g\rangle)$, g is Galois over B if and only if h is Galois over Z.*

Next, we shall prove the following

Theorem 2.16. *Assume that there is a Galois polynomial f in $B[X;\rho]_{(2)}$. Then $Z[X;\overline{\rho}]^{\sim}_{(2)}$ forms an abelian semigroup under the composition $\langle h\rangle\langle k\rangle=\langle h\times k\rangle$ which has the identity element $\phi_f(\langle f\rangle)=\langle f\times f\times\partial(f)^{-1}\rangle$, and the subset $\{\langle h\rangle\in Z[X;\overline{\rho}]^{\sim}_{(2)};\ h$ is Galois over $Z\}$ coincides with the set of all inversible elements in the semigroup $Z[X;\overline{\rho}]^{\sim}_{(2)}$, which is a group of exponent 2.*

Proof. Let $k=X^2-Xp-q$, $h=X^2-Xr-s$, $h_1=X^2-Xr_1-s_1\in Z[X;\overline{\rho}]_{(2)}$, and $h\sim h_1$. Then, by Lemma 2.13, $k\times h$ and $k\times h_1$ are contained in $Z[X;\overline{\rho}]_{(2)}$. Moreover, by Cor. 2.11, there exist elements α, $\beta\in Z$ such that $\alpha\in U(Z)$, $\beta\in Z(\overline{\rho})$, $r=r_1a+\beta+\rho(\beta)$, and $s=s_1\alpha\rho(\alpha)-r_1\alpha\beta-\beta^2$. Hence we have $k\times h=X^2-Xpr-(p^2s+qr^2+4qs)=X^2-Xp(r_1\alpha+\beta+\rho(\beta))-(p^2(s_1\alpha\rho(\alpha)-r_1\alpha\beta-\beta^2)+q(r_1\alpha+\beta+\rho(\beta))^2+4q(s_1\alpha\rho(\alpha)-r_1\alpha\beta-\beta^2)=X^2-X(pr_1\alpha+2p\beta)-((p^2s_1+qr_1{}^2+4qs_1)\alpha\rho(\alpha)-(pr_1)\alpha(p\beta)-(p\beta)^2$, and $p\beta\in Z_1(\overline{\rho})$. This implies $k\times h\sim k\times h_1$ (Cor. 2.11). Further, if $k\sim k_1\in Z[X;\overline{\rho}]_{(2)}$ then $k\times h\sim k\times h_1=h_1\times k\sim h_1\times k_1$. Thus, the composition $\langle k\rangle\langle h\rangle=\langle k\times h\rangle$ in $Z[X;\overline{\rho}]^{\sim}_{(2)}$ is will defined. Moreover, as is easily seen, this composition is associative and commutative. Hence this makes $Z[X;\overline{\rho}]^{\sim}_{(2)}$ into an abelian semigroup. Now, for any $h\in Z[X;\overline{\rho}]_{(2)}$, we have $h\sim\mu_f\nu_f(h)=(f\times\partial(f)^{-1})\times(f\times h)=(f\times f\times\partial(f)^{-1})\times h=\mu_f(f)\times h$, that is, $\langle h\rangle=\langle\mu_f(f)\times h\rangle=\langle\mu_f(f)\rangle\langle h\rangle$. Hence $\langle\mu_f(f)\rangle$ is the identity element of $Z[X;\overline{\rho}]^{\sim}_{(2)}$. Similarly, for any Galois polynomial $g\in B[X;\rho]_{(2)}$, $\langle\mu_g(g)\rangle$ is the identity element of $Z[X;\overline{\rho}]^{\sim}_{(2)}$, and so, $\langle\mu_f(f)\rangle=\langle\mu_g(g)\rangle=\langle g\times g\times\partial(g)^{-1}\rangle$. Next, let h be an arbitrary Galois polynomial in $Z[X;\overline{\rho}]_{(2)}$. Then, by Lemma 2.14, $\nu_f(h)$ is a Galois polynomial in $B[X;\rho]_{(2)}$. Hence $\langle\mu_f(f)\rangle=\langle\nu_f(h)\times\nu_f(h)\times\partial(\nu_f(h))^{-1}\rangle=\langle f\times h\times f\times h\times\partial(h)^{-1}\partial(f)^{-1}\rangle=\langle(f\times f\times\partial(f)^{-1})\times(h\times h\times\partial(h)^{-1}\rangle=\langle\mu_f(f)\rangle\langle h\times h\times\partial(h)^{-1}\rangle=\langle h\times h\times\partial(h)^{-1}\rangle=\langle h\times h\rangle$ (Lemma 2.13). Thus we obtain $\langle\mu_f(f)\rangle=\langle h\rangle^2$. This shows that $\langle h\rangle$ is an inversible element of $Z[X;\overline{\rho}]^{\sim}_{(2)}$ of order 2. Conversely, assume that $\langle h\rangle$ is inversible in $Z[X;\overline{\rho}]^{\sim}_{(2)}$. Then $\langle\mu_f(f)\rangle=\langle h\rangle\langle k\rangle=\langle h\times k\rangle$ for some $\langle k\rangle\in Z[X;\overline{\rho}]^{\sim}_{(2)}$. By Cor. 2.15, $\mu_f(f)$ is Galois over Z, and so is $h\times k$. Hence $\partial(h\times k)=\partial(h)\partial(k)$ is inversible in Z, and so is $\delta(h)$. Thus h is Galois over Z. This completes the proof.

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

Theorem 2.17. *Assume that there is a Galois polynomial f in $B[X; \rho]_{(2)}$. Then $B[X; \rho]_{\widetilde{(2)}}$ forms an abelian semigroup under the composition $\langle g\rangle\langle g_1\rangle = \langle f \times \delta(f)^{-1}) \times (g \times g_1)\rangle$ with the identity element $\langle f\rangle$, and the subset $\{\langle g\rangle \in B[X; \rho]_{\widetilde{(2)}};\ g$ is Galois over $B\}$ coincides with the set of all inversible elements in the semigroup $B[X; \rho]_{\widetilde{(2)}}$, which is a group of exponent 2. Moreover, this semigroup is isomorphic to the semigroup $Z[X; \bar{\rho}]_{\widetilde{(2)}}$ by the map ϕ_f.*

Proof. By Th. 2. 16, $\phi_f(\langle f\rangle) = \langle \mu_f(f)\rangle$ is the identity element of the semigroup $Z[X; \bar{\rho}]_{\widetilde{(2)}}$. Now, let $C = \langle g\rangle$ and $C_1 = \langle g_1\rangle$ be any elements of $B[X; \rho]_{\widetilde{(2)}}$. Then, by Lemma 2.13, we see that $g \times g_1 \times \delta(f)^{-1} \in Z[X; \bar{\rho}]_{(2)}$, and $\nu_f(g \times g_1 \times \delta(f)^{-1}) = f \times g \times g_1 \times \delta(f)^{-1} = f \times \delta(f)^{-1} \times g \times g_1 \in B[X; \rho]_{(2)}$. Moreover, we have $\phi_f^{-1}(\phi_f(C)\phi_f(C_1)) = \phi_f^{-1}(\langle \mu_f(g)\rangle \langle \mu_f(g_1)\rangle) = \phi_f^{-1}(\langle \mu_f(g) \times \mu_f(g_1)\rangle) = \phi_f^{-1}(\langle f \times \delta(f)^{-1} \times g \times f \times \delta(f)^{-1} \times g_1\rangle) = \langle f \times (f \times \delta(f)^{-1} \times (f \times \delta(f)^{-1} \times g \times g_1))\rangle = \langle \nu_f\mu_f(f \times \delta(f)^{-1} \times g \times g_1)\rangle = \langle f \times \delta(f)^{-1} \times g \times g_1\rangle$. This shows that $B[X; \rho]_{\widetilde{(2)}}$ forms an abelian semigroup under the composition $\langle g\rangle\langle g_1\rangle = \langle (f \times \delta(f)^{-1}) \times (g \times g_1)\rangle$ with the identity element $\langle f\rangle$ which is isomorphic to the semigroup $Z[X; \bar{\rho}]_{\widetilde{(2)}}$ by the map ϕ_f. The other assertion follows from the results of Cor. 2. 15 and Th. 2. 16. This completes the proof.

By virtue of Ths. 2. 7 and 2. 17, we obtain the following

Corollary 2.18. *Assume that $\bar{\rho} = 1$ and there is a separable polynomial $f \in B[X; \rho]_{(2)}$. Then $B[X; \rho]_{\widetilde{(2)}}$ forms an abelian semigroup such that $B[X; \rho]_{\widetilde{(2)}} \cong Z[X; 1]_{\widetilde{(2)}}$ and for $g \in B[X; \rho]_{(2)}$, g is separable over B if and only if $\langle g\rangle$ is inversible in the semigroup $B[X; \rho]_{\widetilde{(2)}}$.*

Lastly, for the case (C_3), we shall prove the following

Theorem 2.19. *Assume $\rho = u_l^{-1}u_r$ for some $u \in U(B)$. Then, there exists a one-to-one correspondence between $B[X; \rho]_{(2)}$ and $Z[X; 1]_{(2)}$ in the sense of the following: $g \to \mu(g) = g \times u^{-1}$, In this case, there holds that for g and $g_1 \in B[X; \rho]_{(2)}$,*

(i) *$g \sim g_1$ if and only if $\mu(g) \sim \mu(g_1)$.*

(ii) *g is separable over B if and only if $\mu(g)$ is separable over Z.*

(iii) *$B[x_g] \cong B \otimes_z Z[x_{\mu(g)}]$ (B-ring isomorphic).*

Proof. As is easily seen, we have that $f = X^2 - Xu \in B[X;\ \rho]_{(2)}$, and it is Galois over B. Moreover, for any $g \in B[X;\ \rho]_{(2)}$, $\mu(g) = g \times u^{-1} = f \times \partial(f)^{-1} \times g = \mu_f(g)$, and $\nu_f \mu_f(g) = g$. Further, for any $h \in Z[X;\ 1]_{(2)}$, $\mu_f \nu_f(h) = h$. Hence $\mu\ (= \mu_f)$ is one-to-one, and by Lemma 2.14, the map μ satisfies (i) and (ii). Now, for any $g = X^2 - Xc - d \in B[X;\ \rho]_{(2)}$, we consider $B[x_g]$ and set $y = x_g u^{-1}$. Then, for each $\alpha \in B$, we have $\alpha y = \alpha(x_g u^{-1}) = x_g \rho(\alpha) u^{-1} = x_g u^{-1} \alpha u u^{-1} = (x_g u^{-1})\alpha = y\alpha$. Moreover, $y^2 = (x_g u^{-1})^2 = x_g^2 u^{-2} = (x_g c + d)u^{-2} = x_g c u^{-2} + d u^{-2} = (x_g u^{-1}) c u^{-1} + d u^{-2} = y c u^{-1} + d u^{-2}$. Hence, it follows that $yZ + Z \cong Z[x_{\mu(g)}]$ (Z-ring isomorphic), and $B[x_g] = yB + B = By + B = B(yZ + Z) \cong B \otimes_Z (yZ + Z) \cong B \otimes_Z Z[x_{\mu(g)}]$ (B-ring isomorphic). This shows (iii).

3. On $B[X; D]_{(2)}$. In this section, we study $B[X;\ D]_{(2)}$, the subset of $B[X;\ D]$ (where D is a derivation of B with $D(xy) = D(x)y + xD(y)$ for all x and y in B). As in [4], we shall use the following conventions: $B_0 = \{b \in B;\ D(b) = 0\}$; $Z_0 = Z \cap \mathrm{B}_0$; $I_b = b_r - b_l$ (an inner derivation determined by $b \in B$); $B(D^2 - a_r D) = \{b;\ I_b = D^2 - a_r D\}$; $B(2D) = \{b;\ I_b = 2D\}$; $B_0(D^2 - a_r D) = B(D^2 - a_r D) \cap B_0$; $B_0(2D) = B(2D) \cap B_0$.

Now, let $f = X^2 - Xa - b \in B[X;\ D]_{(2)}$. Then, the factor ring $A = B[X;\ D]/fB[X;\ D]$ is a quadratic extension of B such that for $x = X + fB[X;\ D]$,

$$A = xB + B,\ \alpha x = x\alpha + D(\alpha) \text{ for all } \alpha \in B,$$

$$x^2 = xa + b, \text{ and } \{1,\ x\} \text{ is a right free } B\text{-basis}.$$

Clearly $x^3 = x(xa + b) = (xa + b)x$ and $(\alpha x)x = \alpha(xa + b)$ for all $\alpha \in B$. From these equalities, it follows that

(3, 0) $\qquad a \in B_0(2D)$ and $b \in B_0(D^2 - a_r D)$.

Particularly $ab = ba$, $ax = xa$, and $bx = xb$. Conversely, if a system $\{D,\ a,\ b\}$ $(a,\ b \in B)$ satisfies the condition (3, 0) then

$$X^2 - Xa - b \in B[X;\ D]_{(2)}.$$

Hence, it follows that

(3, i) $\quad B[X;\ D]_{(2)} = \{X^2 - Xa - b;\ a \in B_0(2D) \text{ and } b \in B_0(D^2 - a_r D)\}$.

For any $f = X^2 - Xa - b \in B[X;\ D]_{(2)}$, we denote the factor ring $B[X;\ D]/fB[X;\ D]$ by $B[x;\ D,\ a,\ b]$ (or, by $B[x_f]$) where $x = x_f = X + fB[X;\ D]$. First, we shall prove the following

Lemma 3.1. *Let $f = X^2 - Xa - b \in B[X;\ D]_{(2)}$. Then f is separable over B if and only if there exist elements b_1, b_2, b_3 and b_4 in B such that*

(3, ii) $bb_1 + b_4 = 1$ (3, iii) $ab_1 + b_2 + b_3 = 0$

(3, iv) $ab_2 + b_4 = bb_1 + D(b_2)$ (3, v) $b_1 \in Z$

(3, vi) $b_3 - b_2 = D(b_1)\ (\in Z)$ (3, vii) $I_{b_2} = -(b_1)_r D$

(3, viii) $I_{b_4} = I_{b_2} D - a_r I_{b_2}$.

Proof. We set $A = B[x\,;\ D,\ a,\ b]$ and assume that A is separable over B. Then, the (left)B-(right)B-homomorphism

$$\phi:\ A \otimes_B A \to A \quad (\textstyle\sum_i a_i \otimes b_i \to \sum_i a_i b_i)$$

splits. Hence there exists an element e in $A \otimes_B A$ such that $\phi(e) = 1$ and $(c \otimes 1)e = e(1 \otimes c)$ for all $c \in A$. Since $A \otimes_B A = (x \otimes x)B + (x \otimes 1)B + (1 \otimes x)B + (1 \otimes 1)B$, we may write

$$e = (x \otimes x)b_1 + (x \otimes 1)b_2 + (1 \otimes x)b_3 + (1 \otimes 1)b_4$$

where the b_i's are in B. The equality $\phi(e) = 1$ implies

$$x(ab_1 + b_2 + b_3) + bb_1 + b_4 = 1.$$

Moreover, we have

$$(x \otimes 1)e = (x \otimes x)(ab_1 + b_3) + (x \otimes 1)(ab_2 + b_4) + (1 \otimes x)bb_1 + (1 \otimes 1)bb_2,$$

$$e(1 \otimes x) = (x \otimes x)(ab_1 + D(b_1) + b_2) + (x \otimes 1)(bb_1 + D(b_2)) +$$

$$(1 \otimes x)(ab_3 + D(b_3) + b_4) + (1 \otimes 1)(bb_3 + D(b_4)),$$ and for each $\alpha \in B$,

$$(\alpha \otimes 1)e = (x \otimes x)\alpha b_1 + (x \otimes 1)(D(\alpha)b_1 + \alpha b_2) + (1 \otimes x)(D(\alpha)b_1 + \alpha b_3) +$$

$$(1 \otimes 1)(D^2(\alpha)b_1 + D(\alpha)b_2 + D(\alpha)b_3 + \alpha b_4),$$

$$e(1 \otimes \alpha) = (x \otimes x)b_1\alpha + (x \otimes 1)b_2\alpha + (1 \otimes x)b_3\alpha + (1 \otimes 1)b_4.$$

Hence we obtain

(a) $ab_1 + b_2 + b_3 = 0$ (b) $bb_1 + b_4 = 1$

(c) $ab_1 + b_3 = ab_1 + D(b_1) + b_2$ (d) $ab_2 + b_4 = bb_1 + D(b_2)$

(e) $bb_1 = ab_3 + D(b_3) + b_4$ (f) $bb_2 = bb_3 + D(b_4)$

(g) $\alpha b_1 = b_1\alpha$ (h) $D(\alpha)b_1 + \alpha b_2 = b_2\alpha$

(i) $D(\alpha)b_1 + \alpha b_3 = b_3\alpha$ (j) $D^2(\alpha)b_1 + D(\alpha)b_2 + D(\alpha)b_3 + \alpha b_4 = b_4\alpha$

where α runs over all the elements of B. Conversely, if there exist elements b_1, b_2, b_3 and b_4 in B which satisfy the conditions (a)–(j) then the map ϕ (stated earier) splits, that is, A is separable over B. Hence it suffices to prove that the system of conditions (3, ii–viii) is equivalent to that of the conditions (a)–(j). Assume (a)–(j). Then (g), (c) and (i) imply (3, v, vi, vii). Moreover, (j), (a) and (3, v, vii) imply $I_{b_4} = -(b_1)_r D^2 - (b_2 + b_3)_r D = I_{b_2} D + (ab_1)_r D = I_{b_2} D - a_r I_{b_2}$. Hence (3, ii – viii) are contained in (a)$-$(j). Conversely, we assume (3, ii$-$viii). Then, as is easily seen, we have (a)$-$(d), (g)$-$(j) and $bb_2 = bb_2 + D(1) = bb_2 + D(bb_1 + b_4) = bb_2 + bD(b_1) + D(b_4) = bb_2 + b(b_3 - b_2) + D(b_4) = bb_3 + D(b_4)$. We set here

$$\text{(3, ix)} \qquad z = b_3 - b_2 \ (= D(b_1) \in Z).$$

Then, since $I_a = 2D$ and $I_b = D^2 - a_r D$, we have $D(z) = D^2(b_1) = (I_b + a_r D)(b_1) = a_r D(b_1) = za = az$, and $2D(b_3) = I_a(b_3) = I_a(b_2) = 2D(b_2) = -I_{b_2}(a) = (b_1)_r D(a) = 0$. Hence we obtain

$$\text{(3, x)} \qquad D(z) = az, \text{ and } 2D(b_2) = 2D(b_3) = 0.$$

This and (3, iv) imply $bb_1 = ab_2 - D(b_2) + b_4 = a(b_3 - z) - D(b_3 - z) + b_4 = ab_3 - az - D(b_3) + D(z) + b_4 = ab_3 + D(b_3) + b_4$. Thus (a)$-$(j) are contained in (3, ii$-$viii). This completes the proof.

Now, since $b_1 \in Z$ ((3, v)), we see that $2z = 2D(b_1) = I_a(b_1) = 0$, $z^2 = z(-2b_2 - z) = z(-b_2 - b_3) = zab_1 = a_r(b_1)_r D(b_1) = -a_r I_{b_2}(b_1) = 0$, $zb_1 = D(b_1)b_1 = -I_{b_2}(b_1) = 0$, $b_1 D(b_2) = (b_1)_r D(b_2) = -I_{b_2}(b_2) = 0$, and $D(b_1)D(b_2) = D(b_1 D(b_2)) - b_1 D^2(b_2) = -b_1(a_r D(b_2)) = -a_r(b_1)_r D(b_2) = a_r I_{b_2}(b_2) = 0$. Thus we obtain

$$\text{(3, xi)} \qquad 0 = 2z = z^2 = b_1 z = b_1 D(b_2) = D(b_1)D(b_2).$$

Moreover, by (3, vii, viii), we have $0 = I_{b_2}(a) = I_{b_3}(a) = I_{b_4}(a) = I_{b_2}(b) = I_{b3}(b) = I_{b_4}(b)$, and $I_{b_4}(b_2) = -I_{b_2}(b_4) = -I_{b_2}(1 - bb_1) = 0$. This shows that

$$\text{(3, xii)} \qquad uv = vu \text{ for each pair } u, v \in \{a, b, b_1, b_2, b_3, b_4\}.$$

Next, we shall prove the following.

Lemma 3. 2. *Let $f = X^2 - Xa - b \in B[X; D]_{(2)}$ and f separable over B. Let $\{b_1, b_2, b_3, b_4\}$ be a system of elements of B which satisfies the conditions* (3, ii$-$viii). *Then*

$$\text{(3, xiii)} \qquad 2 = \delta(f)(b_1 + b_2 b_3 - b_2{}^2), \ 4 = \delta(f)(2b_1)$$

where $\delta(f) = a^2 - 4b$, *moreover*

$$\text{(3, xiv)} \qquad a^2 = \delta(f)(b_4 - bb_1)$$

$$\text{(3, xv)} \qquad \delta(f)B = B\delta(f), \ D(\delta(f)B) \subset \delta(f)B$$

$$\text{(3, xvi)} \qquad I_a \equiv 0 \ \ (mod\ \delta(f)B)$$

$$\text{(3, xvii)} \qquad b_1 \equiv 0, \ b_2 \equiv b_3, \ b_4 \equiv 1 \ \ (mod\ \delta(f)B)$$

$$\text{(3, xviii)} \qquad ab_2 + D(b_2) \equiv 1, \ D(b_2)^2 \equiv 1 \ \ (mod\ \delta(f)B)$$

$$\text{(3, xix)} \qquad I_{b_2} \equiv 0 \ \ (mod\ \delta(f)B).$$

Proof. We set $z = b_3 - b_2$. Then

$$\delta(f)(b_1 + b_2 z) = \delta(f)b_1 + (a^2 + 4b)b_2 z = \delta(f)b_1 + a^2 b_2 z \qquad \text{(by (3, xi))}$$

$$\begin{aligned}
&= (a^2 + 4b)b_1 + az + az(1 + ab_2) && \text{(by (2, xi, xii))}\\
&= a^2b_1 + 4bb_1 + az + az(bb_1 + b_4 + ab_2) && \text{(by (3, ii))}\\
&= a(ab_1 + z) + 4bb_1 + az(2bb_1 + D(b_2)) && \text{(by (3, iv))}\\
&= a(-2b_2)+2bb_1+2(1-b_4)+azD(b_2) && \text{(by (3, ii, iii, xi))}\\
&= 2-2ab_2+2bb_1-2b_4+aD(b_1)D(b_2) && \text{(by (3, ix))}\\
&= 2 - 2D(b_2) + aD(b_1)D(b_2) = 2 && \text{(by (3, iv, x, xi)).}
\end{aligned}$$

$$\begin{aligned}
\partial(f)(2b_1) &= \partial(f)(2b_1 + 2b_2z) = 2\partial(f)(b_1 + b_2z) = 4 && \text{(by (3, xi)).}\\
\partial(f)(b_4 - bb_1) &= \partial(f)(1 - 2bb_1) = \partial(f) - \partial(f)(2b_1)b && \text{(by (3, ii))}\\
&= a^2 + 4b - 4b = a^2 && \text{(by (3, xiii)).}\\
\partial(f)B &= (a^2+4b)B \subset a^2B + 2B \subset a(Ba - 2D(B)) + 2B && \text{(by (3, i))}\\
&\subset (aB)a + 2B \subset Ba^2 + B2 \subset B\partial(f) && \text{(by (3, xii, xiii, xiv)).}
\end{aligned}$$

Similarly, we have $B\partial(f) \subset \partial(f)B$, and hence $\partial(f)B = B\partial(f)$. Moreover, since $D(\partial(f)) = 0$, it follows that $D(\partial(f)B) = \partial(f)D(B) \subset \partial(f)B$. In the rest of this proof, $h \equiv k$ denotes the congruence $h \equiv k \pmod{\partial(f)B}$ in B. Then $I_a(B) \equiv 2D(B) \equiv 0$ (by (3, i)), that is, $I_a \equiv 0$. Further,

$$\begin{aligned}
b_1 \equiv b_1(bb_1 + b_4) &\equiv b_1(ab_2 + b_4 - D(b_2) + b_4) && \text{(by (3, ii, iv))}\\
&\equiv b_1ab_2 + 2b_1b_4 - b_1D(b_2) \equiv b_1ab_2 && \text{(by (3, xi))}\\
&\equiv (b_1ab_2)ab_2 \equiv a^2b_1b_2{}^2 \equiv 0 && \text{(by (3, xiv)).}
\end{aligned}$$

Hence by (3, vi, ii, iv, xiii, xiv, vii), we have $b_3 - b_2 \equiv D(b_1) \equiv 0$, $b_4 \equiv 1$, $ab_2 \equiv 1 + D(b_2)$, $D(b_2)^2 \equiv (ab_2 - 1)^2 \equiv a^2b_2{}^2 - 1 \equiv 1$, and $I_{b_2}(B) \equiv D(B)b_1 \equiv 0$. This completes the proof.

Lemma 3.3. *Let $f = X^2 - Xa - b$ and $g = X^2 - Xu - v$ be in $B[X; D]_{(2)}$, and let f be separable over B. Then*

(i) *$a \equiv u \pmod{\partial(f)B}$ and $\partial(f)B \supset \partial(g)B$.*

(ii) *If g is separable over B then $\partial(f)B = \partial(g)B$.*

(iii) *If $aB \equiv B \pmod{\partial(f)B}$ then $\partial(f) \in U(B)$, and conversely.*

(iv) *If D is inner then $\partial(f) \in U(B)$.*

(v) *If $2 \in U(B)$ then $\partial(f) \in U(B)$.*

(vi) *If $2 = 0$ and $D|Z = 0$ then a, $\partial(f) \in U(B)$.*

Proof. Let $\{b_1, b_2, b_3, b_4\}$ be a system of elements of B which satisfies the conditions (3, ii — viii). In the proof, $x \equiv y$ denotes the congruence $x \equiv y \pmod{\partial(f)B}$ in B. Since $I_b = D^2 - a_rD$ and $I_v = D^2 - u_rD$, we have

$$a \equiv D(b_2)D(b_2)a \equiv D(b_2)\,(I_b(b_2) + D(b_2)a) \qquad \text{(by (3, xviii, xix))}$$

$$\equiv D(b_2)\,(I_b+a_rD)\,(b_2)\equiv D(b_2)D^2(b_2)\equiv D(b_2)\,(I_v+u_rD)(b_2)$$
$$\equiv D(b_2)\,(I_v(b_2)+D(b_2)u)\equiv D(b_2)D(b_2)u\equiv u \qquad \text{(by (3, xviii, xix))}.$$

Moreover, $\delta(g)\equiv u^2+4v\equiv u^2\equiv a^2\equiv 0$ (by (3, xiii, xiv)). Thus we obtain (i). If g is separable over B then, by (i), we have also $\delta(g)B\supset\delta(f)B$, and and (i). so, $\delta(g)B=\delta(f)B$. To see (iii), let $aB\equiv B$. Then, since $a^2\equiv 0$ $I_a\equiv 0$, we have $B\equiv(aB)^2\equiv a^2B\equiv 0$, and this shows $B=\delta(f)B$. Conversely, if $B=\delta(f)B$ then $B\equiv(a^2+4b)B\equiv a^2B\equiv a(aB)$ (by (3, xiii)), and this implies $B\equiv aB$. Next, if D is an inner derivation I_a then, by (3, xviii, xix), we have $1\equiv D(b_2)^2\equiv(I_a(b_2))^2\equiv(-I_{b_2}(d))^2\equiv 0$, and whence $\delta(f)B=B$. If $2\in U(B)$ then $D=2^{-1}I_a=I_{2^{-1}a}$ and hence $\delta(f)\in U(B)$ by (iv). Finally, let $2=0$ and $D|Z=0$. Then

$$\begin{aligned} b_1 &= (bb_1+b_4)b_1=(ab_2+b_4-D(b_2)+b_4)b_1 && \text{(by (3, ii, iv))}\\ &= (ab_2+2b_4-D(b_2))b_1=ab_2b_1=(ab_1)b_2 && \text{(by (3, xi))}\\ &= -(b_2+b_3)b_2=D(b_1)b_2=0 && \text{(by (3, iii, v, vi))}. \end{aligned}$$

Hence by (3, vii), we have $I_{b_2}=-(b_1)_rD=0$. This implies $b_2\in Z$, and so, $D(b_2)=0$. Thus we obtain $ab_2=bb_1+D(b_2)-b_4=bb_1+b_4=1$ (by (3, ii, iv)). Therefore, it follows that $aB=B$, and so, $\delta(f)\in U(B)$ (by (iii)). This completes the proof.

Next, we consider the following conditions.

(C_1) $B[X;D]_{(2)}$ contains an element $f=X^2-Xa-b$ such that either $\delta(f)$ or a is inversible in B.

(C_2) D is an inner derivation.

(C_3) 2 is inversible in B.

(C_4) $2=0$ and $D|Z=0$.

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

Theorem 3. 4. *Assume that there holds one of the conditions* (C_1) — (C_4). *Then, for* $g\in B[X;D]_{(2)}$, *the following conditions are equivalent.*

(a) g *is Galois over* B.

(b) $\delta(g)$ *is inversible in* B.

(c) g *is separable over* B.

Proof. By Lemma 1. 5 and [5, Th. 1. 5], we see that (b) implies (a), and (a) implies (c). Hence it suffices to prove that (c) implies (b). We assume (c), and set $g=X^2-Xu-v$. If $\delta(f)$ is inversible in B then, by Lemma 1. 5 and [5, Th. 1. 5], f is separable over B, and hence, by Lemma 3. 3 (ii) and (3, xv), $B = \delta(f)B = \delta(g)B = B\delta(g)$, which implies $\delta(g) \in U(B)$. Next, let a be inversible in B. Then $aB = B$. By Lemma 3. 3 (i), we have $u \equiv a \pmod{\delta(g)}$. This implies $uB \equiv aB \equiv B \pmod{\delta(g)}$. Hence by Lemma 3. 3 (ii), we obtain $\delta(g) \in U(B)$. The other assertions follow from the results of Lemma 3. 3 (iv, v, vi). This completes the proof.

Now, for the cases (C_2) and (C_3), we shall prove the following

Theorem 3. 5. *Let $D = I_c$, an inner derivation. Then, there exists a one-to-one correspondence between $B[X\,;\,D]_{(2)}$ and $Z[X\,;\,0]_{(2)}$ ($= Z[X\,;\,D = 0]_{(2)}$) in the sense of the following*

$$f = X^2 - Xa - b \ \rightarrow\ \phi(f) = X^2 - X(a - 2c) - (b + c(a - 2c) + c^2)$$

such that for f, f_1 and $f_2 \in B[X\,;\,D]_{(2)}$,

(i) *f is separable over B if and only if $\phi(f)$ is separable over Z,*

(ii) *$B[x_f] \cong B \otimes_Z Z[x_{\phi(f)}]$ (B-ring isomorphic),*

(iii) *$B[x_{f_1}] \cong B[x_{f_2}]$ (B-ring isomorphic) if and only if $Z[x_{\phi(f_1)}] \cong Z[x_{\phi(f_2)})]$ (Z-ring isomorphic).*

Proof. Let $f = X^2 - Xa - b \in B[X\,;\,D]_{(2)}$. Since $I_{a-2c} = I_a - 2I_c = 0$, we have $a - 2c \in Z$. We set here $z = a - 2c$. Then

$$\begin{aligned} 0 &= I_b - I_c^2 + a_r I_c = I_b + (a_r - I_c)I_c = I_b + ((2c + z)_r - (c_r - c_l))I_c \\ &= I_b + (c_r + c_l)I_c + z_r I_c = I_b + (c_r + c_l)(c_r - c_l) + I_{cz} \\ &= I_b + I_{c^2} + I_{cz} = I_{b+c^2+cz}\,. \end{aligned}$$

This implies $b + c^2 + cz \in Z$. Moreover, it is obvious that if $f_1 \neq f_2 \in B[X; D]_{(2)}$ then $\phi(f_1) \neq \phi(f_2)$. Hence the ϕ is an injective map of $B[X; D]_{(2)}$ to $Z[X\,;\,0]_{(2)}$. Conversely, let $g = X^2 - Xa' - b' \in Z[X\,;\,0]_{(2)}$. We set here $a = a' + 2c$ and $b = b' - c^2 - ca'$. Then $I_a = I_{a'+c^2} = I_{a'} + I_{c^2} = 2I_c$. Moreover, we have

$$\begin{aligned} I_b &= I_{b'-c^2-ca'} = I_{b'} - I_{c^2} - I_{cu'} = -I_{c^2} - I_{ca'} \\ &= -(c_r + c_l)(c_r - c_l) - a'_r I_c = -(c_r + c_l)I_c - a'_r I_c \\ &= ((c_r - c_l) - 2c_r - a'_r)I_c = ((c_r - c_l) - a_r)I_c = I_c^2 - a_r I_c. \end{aligned}$$

Hence we have $f = X^2 - Xa - b \in B[X\!:\,I_c]_{(2)}$, and $\phi(f) = g$. Thus, the ϕ is surjective, and so, this is one-to-one. Now, let $f = X^2 - Xa - b$, f_1, $f_2 \in B[\,X\,;\,D]_{(2)}$. Then $\delta(f) = a^2 + 4b = (a - 2c)^2 + 4(c(a - 2c) + b + c^2) = \delta(\phi(f))$. Hence the assertion (i) follows from Th. 3. 4. Next, we consider $B[x_f]$ and set $y = x_f - c$. Then, for each $\alpha \in B$,

$$\alpha y = \alpha x_f - \alpha c = x_f \alpha + I_c(\alpha) - \alpha c = x_f \alpha - c\alpha = (x_f - c)\alpha = y\alpha.$$

Moreover, we have

$$\begin{aligned} y^2 &= (x_f - c)^2 = x_f^2 - 2x_f c + c^2 = x_f a + b - 2x_f c + c^2 \\ &= x_f(a-2c) + b + c^2 = (x_f - c)(a-2c) + (c(a-2c) + b + c^2) \\ &= y(a-2c) + (c(a-2c) + b + c^2). \end{aligned}$$

Hence $yZ+Z \cong Z[x_{\phi(f)}]$. Thus, it follows that $B[x_f]=yB+B=By+B=B(yZ+Z) \cong B \otimes_Z Z[x_{\phi(f)}]$. This shows (ii). If $B[x_{f_1}] \cong B[x_{f_2}]$ (B-ring isomorphic) then $Z[x_{\phi(f_1)}] \cong$ (the centralizer of B in $B[x_{f_1}]$) $\cong$ (the centralizer of B in $B[x_{f_2}]$) $\cong Z[x_{\phi(f_2)}]$ (Z-ring isomorphic). The converse is obvious. Thus we obtain (iii). This completes the proof.

Now, for elements g and $g_1 \in B[X; D]_{(2)}$, if $B[x_g] \cong B[x_{g_1}]$ (B-ring isomorphic) then we write $g \sim g_1$. Moreover, by $B[X; D]_{\widetilde{(2)}}$, we denote the set of equivalence classes of $B[X; D]_{(2)}$ with respect to the relation $\sim$, and we write $C = \langle g \rangle$ if $C \in B[X; D]_{\widetilde{(2)}}$ and $g \in C$.

In virtue of Th. 3. 5 and Th. 2. 16, we obtain the following corollary which contains the result of [4, Cor. 1 (2)].

Corollary 3. 6. *Let D be an inner derivation. Then $B[X; D]_{\widetilde{(2)}}$ forms an abelian semigroup under the composition $\langle g_1 \rangle \langle g_2 \rangle = \langle \phi^{-1}(\phi(g_1) \times \phi(g_2)) \rangle$ where ϕ is as in Th.* 3. 5 *and $\phi(g_1) \times \phi(g_2)$ is as in Remark* 2. 12, *so that this group is isomorphic to the group $Z[X; \rho = 1]_{\widetilde{(2)}}$ $(= Z[X; D = 0]_{\widetilde{(2)}})$.*

For the case (C_4), we have the result of Cor. 3. 18 which will be verified lately.

Next, we shall prove the following

Theorem 3. 7. *Assume $2=0$, and let $f=X^2-Xa-b \in B[X; D]_{(2)}$. Then*

(i) *f is separable over B if and only if there exist elements b_1, b_2 in B such that $b_1 \in Z$, $D(b_1)+ab_1=0$, $D(b_2)+ab_2=1$, and $I_{b_2}=(b_1)_r D$.*

(ii) *f is Galois over B if and only if there exists an element s in $U(Z)$ such that $D(s) + as = 1$.*

Proof. (i). Assume that f is separable over B. Then, there exists a system $\{b_1, b_2, b_3, b_4\}$ of elements in B which satisfies the conditions (3, ii – viii). Then, we have $b_1 \in Z$ (by (3, v)), $D(b_1) + ab_1 = b_3 - b_2 - (b_2+b_3) = 0$ (by (3, iii, vi)), and $D(b_2)+b_2 = ab_2+b_4-bb_1+ab_2=b_4+bb_1=1$ (by (3, ii, iv)). Moreover, we have $I_{b_2} = -(b_1)_r D = (b_1)_r D$ (by (3, vii)). Conversely, we assume that there exist elements b_1, b_2 in B such that $b_1 \in Z$, $D(b_1) + ab_1 = 0$, $D(b_2) + ab_2 = 1$, and $I_{b_2} = (b_1)_r D$. We set here

$b_3=ab_1+b_2$ and $b_4=bb_1+1$. Then $ab_2+b_4=ab_2+bb_1+1=ab_2+bb_1+D(b_2)+ab_2=bb_1+D(b_2)$. Moreover, since $I_a=2D=0$ and $I_b=D^2-a_rD$, we have $I_{b_2}D-a_rI_{b_2}=(b_1)_rD^2-I_{ab_2}=(b_1)_r(a_rD+I_b)+I_{ab_2}=a_r(b_1)_rD+(b_1)_rI_b+I_{ab_2}=a_rI_{b_2}+I_{bb_1+ab_2}=I_{ab_2+bb_1+ab_2}=I_{bb_1}=I_{b_4+1}=I_{b_4}$. Thus, the system $\{b_1, b_2, b_3, b_4\}$ satisfies the conditions (3, ii – viii). Hence f is separable over B. (ii). Set $A=B[x\,;\,D, a, b]$ where $x=x_f$, and assume that f is Galois over B. Then, by Lemma 1. 2, A is a Galois extension of B with Galois group $\{1, \sigma\}$ and $x-\sigma(x)=x+\sigma(x)\in U(B)$. We set here $s=(x-\sigma(x))^{-1}$, $y=xs$, and $c=y^2+y$. Then $y+\sigma(y)=1$, and $\sigma(c)=c$. Hence $c\in B$. Let α be an arbitrary element of B. Then $\sigma(\alpha y-y\alpha)=\alpha y-y\alpha$, and so, this is contained in B. Hence the mapping $\alpha\rightarrow\alpha y-y\alpha=E(\alpha)\;(\alpha\in B)$ is a derivation of B. Moreover $\alpha y=\alpha(xs)=(\alpha x)s=(x\alpha+D(\alpha))s=x\alpha s+D(\alpha)s$ and $\alpha y=y\alpha+E(\alpha)=(xs)\alpha+E(\alpha)$. Hence $s\alpha=\alpha s\;(\alpha\in B)$. This implies $s\in Z$. Now, we have $B\ni c=y^2+y=(xs)^2+xs=(xs)\,(xs)+xs=x(xs+D(s))s+xs=x^2s^2+xD(s)s+xs=(xa+b)s^2+x(D(s)s+s)=x(as^2+D(s)s+s)+bs^2$. Hence $as^2+D(s)s+s=0$. Since s is inversible in B, we obtain $D(s)+as=1$. Conversely, we assume that $D(s)+as=1$ for some inversible element s in Z. Then, we see that $(xs)^2+xs=bs^2$. Moreover, one will easily see that the mapping $\alpha\rightarrow D(\alpha)s\;(\alpha\in B)$ is a derivation in B, $\alpha(xs)=(xs)\alpha+D(\alpha)s\;(\alpha\in B)$ and $\{xs, 1\}$ is a right free B-basis of A. By Th. 3. 4, $g=Y^2-Y-bs^2$ is a Galois polynomial of $B[Y\,;\,s_rD]_{(2)}$. Hence A is a Galois extension of B. Thus f is Galois over B, completing the proof.

Corollary 3. 8. *Assume* $2=0$, *and let* $f=X^2-Xa-b\in B[X\,;\,D]_{(2)}$ *so that a is nilpotent. Then,* f *is separable over* B *if and only if there is an element* s *in* Z *such that* $D(s)+as=1$; *and in this case,* $D(s)$ *is inversible in* B.

Proof. Assume that f is separable over B. Then, by Th. 3. 7, there exist elements b_1, b_2 in B such that $b_1\in Z$, $D(b_1)+ab_1=0$, $D(b_2)+ab_2=1$, and $I_{b_2}=(b_1)_rD$. Since $a^n=0$ for some integer $n>0$, it follows that for an integer $2^m\geqq n$, $1=(D(b_2)+ab_2)^{2^m}=D(b_2)^{2^m}+(ab_2)^{2^m}=D(b_2)^{2^m}$, and whence $D(b_2)$ is inversible in B. Hence, noting that $0=I_{b_2}(b_2)=(b_1)_rD(b_2)=D(b_2)b_1$, we obtain $b_1=0$. This implis $I_{b_2}=0$, that is, $b_2\in Z$. Conversely, we assume that there is an element s in Z such that $D(s)+as=1$. Then, for $b_1=0$ and $b_2=s$, we have $b_1\in Z$, $D(b_1)+ab_1=0$, $D(b_2)+ab_2=1$, and $I_{b_2}=(b_1)_rD$. Hence by Th. 3. 7, f is separable over B. This completes the proof.

Next, we shall prove the following

Corollary 3. 9. *Let $f = X^2 - Xa - b \in B[X ; D]_{(2)}$. Then, f is separable (resp. Galois) over B and $\delta(f) = 0$ if and only if $2 = 0$, $a^2 = 0$, and there exists an element s in Z (resp. in $U(Z)$) with $D(s) + as = 1$.*

Proof. If f is separable over B and $\delta(f) = 0$ then, by Lemma 3. 2, we have $2 = 0$ and $a^2 = 0$. Hence the corollary follows from the results of Th. 3. 7 and Cor. 3. 8.

The following corollaries 3. 10 and 3. 11 are direct consequences of Cor. 3. 9.

Corollary 3. 10. *Let $f = X^2 - b \in B[X ; D]_{(2)}$. Then, f is separable (resp. Galois) over B and $\delta(f) = 0$ if and only if $2 = 0$ and there exists an element s in Z (resp. in $U(Z)$) with $D(s) = 1$.*

Corollary 3. 11. *Let either $2 \neq 0$ or $D|Z = 0$. Then, for any separable polynomial f in $B[X ; D]_{(2)}$, there holds $\delta(f) \neq 0$.*

Next, we shall prove the following

Theorem 3. 12. *Assume $2 = 0$, and let $f = X^2 - Xa - b \in B[X ; D]_{(2)}$. If f is separable (resp. Galois) over B then, for all $v \in B_0(D^2 - a_r D)$, $X^2 - Xa - v$ is separable (resp. Galois) over B. Moreover, if f is separable over B and a is nilpotent then, $\{X^2 - Xa - v ; v \in B_0(D^2 - a_r D)\} = B[X ; D]_{(2)}$.*

Proof. The first assertion is a direct consequence of Th. 3. 7. Now, let f be separable over B and let a be nilpotent. Then, by Cor. 3. 8, there exists an element s in Z such that $D(s) + as = 1$, and then, $D(s)$ is inversible in B. Since $D^2(s) = aD(s)$, it follows that $a = D^2(s)\,(D(s))^{-1}$. Next, let $X^2 - Xp - q$ be an element of $B[X ; D]_{(2)}$. Then $I_p = 0$, $I_q = D^2 - p_r D$, and whence $D^2(s) = D(s)p$. This shows that $p = D^2(s)\,(D(s))^{-1} = a$. Hence $X^2 - Xp - q \in \{X^2 - Xa - v ; v \in B_0(D^2 - a_r D)\}$ $(\subset B[X ; D]_{(2)})$. This completes the proof.

In virtue of Cor. 3. 9 and Th. 3. 12, we obtain the following

Corollary 3. 13. *If $B[X ; D]_{(2)}$ contains a separable polynomial $f = X^2 - Xa - b$ with $\delta(f) = 0$ then $B[X ; D]_{(2)} = \{X^2 - Xa - v ; v \in B_0(D^2 - a_r D)\}$. In particular, if $B[X ; D]_{(2)}$ contains a separable polynomial $X^2 - b$ with $4b = 0$ then $B[X ; D]_{(2)} = \{X^2 - v ; v \in B_0(D^2)\}$.*

Now, let $\varepsilon \in B_0$, and set $J = B\varepsilon B$. Moreover, we assume $J \neq B$. Since $D(\varepsilon) = 0$, we have $D(J) \subset J$. We denote the factor ring B/J by B_ε, and for any element c in B, we denote $c + J$ by c_ε. Further, by

D_ε, we denote the derivation of B_ε induced by D. Then, for any $g = X^2 - Xu - v \in B[X; D]_{(2)}$, we have $X^2 - Xu_\varepsilon - v_\varepsilon \in B_\varepsilon[X; D_\varepsilon]_{(2)}$. This will be denoted by g_ε. Under this situation, we shall prove the following

Theorem 3.14. *If there exists a separable (resp. Galois) polynomial f in $B[X; D]_{(2)}$ such that $\varepsilon = \delta(f)$ is not inversible in B then, for any $g \in B[X; D]_{(2)}$, the polynomial g_ε $(\in B_\varepsilon[X; D_\varepsilon]_{(2)})$ is separable (resp. Galois) over B_ε, and the factor ring $B[x_g]/\varepsilon B[x_g]$ is B_ε-ring isomorphic to $B_\varepsilon[x_{g_\varepsilon}]$.*

Proof. Let g be an element of $B[X; D]_{(2)}$, and set $A_g = B[x_g; D, a, b]$. First, we assume that f is separable over B. By (3, xv), we have $\varepsilon B = B\varepsilon \neq B$. Noting $\varepsilon x_g = x_g\varepsilon$, we see that $\varepsilon A_g = A_g\varepsilon$ and $\varepsilon A_g \cap A_g = \varepsilon B$. Then, as is easily seen, the factor ring $A_g/\varepsilon A_g$ is B_ε-ring isomorphic to $B_\varepsilon[x_{g_\varepsilon}; D_\varepsilon, a_\varepsilon, b_\varepsilon]$. Now, since A_f is separable over B, $A_f/\varepsilon A_f$ is separable over B_ε by Lemma 1.3. Hence f_ε is a separable polynomial in $B_\varepsilon[X; D_\varepsilon]$, and the discriminant of f_ε is zero. Hence by Cor, 3.13, g_ε is separable over B_ε. By a similar way, we see that if f is Galois over B then g_ε is Galois over B_ε (by Lemma 1.3 and Cor. 1.13). This completes the proof.

Next, we shall present an example of $B[X; D]_{(2)}$ containing separable polynomials whose discriminants are zero.

Remark 3.15. Let F be a field of characteristic 2 (for example, $F = \mathrm{GF}(2)$), and R the ring of polynomials of x with coefficients in F, where x is an indeterminate. Moreover, let S be the subring of the guotient field of R which is generated by x^{-1} over R, and D the ordinary derivative of S such that $D(\sum_i a_i x^i) = \sum_i i a_i x^{i-1}$. Then $D^2 = 0$, and whence $X^2 \in S[X; D]_{(2)}$ and $X^2 \in R[X; D|R]_{(2)}$. Since $D(x) = 1$ and x is inversible in S, it follows from Cor. 3.10 that X^2 is a Galois polynomial in $S[X; D]_{(2)}$. As is easily seen, there is not an inversible element s in R with $D(s) = 1$. Hence X^2 is not a Galois polynomial in $R[X; D|R]_{(2)}$. However, since $D(x) = 1$ and $x \in R$, it follows from Cor. 3.10 that X^2 is a separable polynomial in $R[X; D|R]_{(2)}$. Moreover $\{b \in S; D(b) = 0\} = F = \{b \in R; D(b) = 0\}$, and whence by Cor. 3.13, we have $S[X; D]_{(2)} = \{X^2 - b; b \in F\}$ and $R[X; D|R]_{(2)} = \{X^2 - b; b \in F\}$.

In the rest of this section, we assume $B[X; D]_{(2)} \neq \emptyset$, and moreover, for a (fixed) element $X^2 - Xa - b \in B[X; D]_{(2)}$, we shall use the following conventions:

$B[X;\ D]_{(2),a} = \{X^2 - Xa - v;\ v \in B_0(D^2 - a_r D)\}\ \ (\subset B[X;\ D]_{(2)})$.

$B[X;\ D]^{\sim}_{(2),a}$ = the set of equivalence classes of $B[X;\ D]_{(2),a}$ with respect to $\sim$; and write $\langle g \rangle = C$ if $C \in B[X;\ D]^{\sim}_{(2),a}$ and $g \in C$. Moreover, as in [4, § 3], we set

$\mathfrak{B}_a(B)$ = the set of all the elements β in B such that $\beta^2 + D(\beta) + \beta a \in Z_0$ and $I_\beta = D + \alpha_r D$ for some $\alpha \in U(Z)$ with $\alpha^2 = 1$ and $a(1+\alpha) = D(\alpha)$.

$\mathfrak{B}_a(B)_\Delta = \{\beta^2 + D(\beta) + \beta a;\ \beta \in B_a(B)\}$.

$Z_\Delta = \{z^2 + D(z) + za;\ z \in Z\}$.

Now, the following lemma will be easily seen.

Lemma 3.15. (Cf. [4, Lemma 3.2]). *Let* $X^2 - Xa - b \in B[X;\ D]_{(2)}$. *Then* $B[X;\ D]_{(2),a} = \{X^2 - Xa - (b + z);\ z \in Z_0\}$.

Next, for case $2 = 0$, we have the following

Lemma 3.16. (Cf. [4, Lemma 3.1]). *Assume* $2 = 0$, *and let* $X^2 - Xa - b \in B[X;\ D]_{(2)}$. *Then* $Z \subset \mathfrak{B}_a(B)$, $Z_\Delta \subset \mathfrak{B}_a(B)_\Delta \subset Z_0$, *and* Z_Δ *is an additive subgroup of* $(Z_0,\ +)$. *If* $\beta\delta = \delta\beta$ *for all* $\beta,\ \delta \in \mathfrak{B}_a(B)$ *then* $\mathfrak{B}_a(B)_\Delta$ *is also an additive subgroup of* $(Z_0,\ +)$.

Proof. Let z be any element of Z, and set $c = z^2 + D(z) + za$. Then $D(c) = D(z^2) + D^2(z) + D(z)a = 2zD(z) + (D^2 - a_r D)(z) = I_b(z) = 0$. Hence $c \in Z_0$. If we set $\alpha = 1$ then $I_z = D + \alpha_r D$, $\alpha \in U(Z)$, $\alpha^2 = 1$, and $a(1+\alpha) = D(\alpha)$. This shows $z \in \mathfrak{B}_a(B)$, and whence $Z \subset \mathfrak{B}_a(B)$. Thus we obtain $Z_\Delta \subset \mathfrak{B}_a(B)_\Delta$. Clearly Z_Δ is an additive subgroup of $(Z_0,\ +)$. The other assertion is proved by making use of the same method as in the proof of [4, Lemma 3.1]. This completes the proof.

Moreover, by making use of the same methods as in the proofs of [4, Lemma 3.3 and Th. 2.4], we obtain the following lemma and theorem.

Lemma 3.17. (Cf. [4, Lemma 3.3]). *Assume* $2 = 0$, *and let* $X^2 - Xa - b \in B[X;\ D]_{(2)}$. *Then, for elements* g *and* h *in* $B[X;\ D]_{(2),a}$, $g \sim h$ *if and only if* $g - h \in \mathfrak{B}_a(B)_\Delta$.

Theorem 3.18. (Cf. [4, Th. 3.4]). *Assume* $2 = 0$, *and let* $f = X^2 - Xa - b \in B[X;\ D]_{(2)}$. *If* $\beta\delta = \delta\beta$ *for all* $\beta,\ \delta \in \mathfrak{B}_a(B)$ *then* $B[X;\ D]^{\sim}_{(2),a}$ *forms an abelian froup of exponent* 2 *under the composition* $\langle g \rangle \langle h \rangle = \langle g + h + f \rangle$ *with the identity element* $\langle f \rangle$, *and this group is isomorphic to the additive group* $(Z_0,\ +)/\mathfrak{B}_a(B)_\Delta$.

Now, we shall prove the following

Theorem 3.19. *Assume $2=0$, and let $f=X^2-Xa-b\in B[X ; D]_{(2)}$. If $Z=\mathfrak{B}_a(B)$ then the group $B[X ; D]^{\sim}_{(2),a}$ is isomorphic to the additive group $(Z_0, +)/Z_\Delta$. Moreover, if f is Galois over B and $Z=\mathfrak{B}_a(B)$ then there exists an element s in $U(Z)$ such that $B[X ; D]^{\sim}_{(2),a}$ is isomorphic to the additive group $(Z, +)/(K_1+K_2)$ where $K_1=\{z\in Z ; sD(z)=z\}$,* and $K_2=\{z^2+z ; z\in Z\}$.

Proof. The first assertion is a direct consequence of Th. 3.18. Now, we assume that f is Galois over B and $Z=\mathfrak{B}_a(B)$. Then, by Th. 3.7, there exists an element s in $U(Z)$ with $D(\mathrm{s})+as=1$. Clearly $s^2\in Z_0$, and the mapping $z_0\to z_0s^2$ $(z_0\in Z_0)$ is an automorphism of $(Z_0, +)$. This shows that $(Z_0, +)/Z_\Delta\cong(Z_0, +)/Z_\Delta s^2$. Since $0=D(1)=D(ss^{-1})=D(s)s^{-1}+sD(s^{-1})=(as+1)s^{-1}+sD(s^{-1})$. we have $D(s^{-1})=(as+1)s^{-2}$. Hence

$$\begin{aligned}
Z_\Delta s^2 &= \{(z^2+az+D(z))s^2 ; z\in Z\}\\
&= \{((zs^{-1})^2+a(zs^{-1})+D(zs^{-1}))s^2 ; z\in Z\}\\
&= \{z^2+azs+(D(z)s^{-1}+zD(s^{-1}))s^2 ; z\in Z\}\\
&= \{z^2+azs+(D(z)s^{-1}+z(as+1)s^{-2})s^2 ; z\in Z\}\\
&= \{z^2+z+s_rD(z) ; z\in Z\}.
\end{aligned}$$

Therefore, it follows that

$$(Z_0, +)/Z_\Delta\cong(Z_0, +)/\{z^2+z+s_rD(z) ; z\in Z\}.$$

Moreover, for any $z\in Z$, we have $D(z+s_rD(z))=D(z^2)+D(z+s_rD(z))=D(z^2+z+s_rD(z))\in D(Z_\Delta s^2)=\{0\}$, which implies $z+s_rD(z)\in Z_0$. Next, we consider the mapping

$$\phi : Z\to Z_0 \quad (z\to z+s_rD(z)).$$

Clearly the map ϕ is additive, and $Z_0\supset\phi(Z)\supset\phi(Z_0)=Z_0$, that is, ϕ is surjective. Further, we have $\ker\phi=K_1$, and for any $z\in Z$, $\phi(z^2+z)=z^2+z+s_rD(z^2+z)=z^2+z+s_rD(z)$, which implies $\phi(K_2)=\{z^2+z+s_rD(z) ; z\in Z\}$. Hence, it follows that

$$(Z, +)/(K_1+K_2)\cong(Z_0, +)/\{z^2+z+s_rD(z) ; z\in Z\}.$$

Thus we obtain $(Z, +)/(K_1+K_2)\cong(Z_0, +)/Z_\Delta\cong B[X ; D]^{\sim}_{(2),a}$ (Th. 3.18), completing the proof.

For case $a\in U(Z)$, we have the following

Corollary 3.20. (Cf. [4, Cor. 1]). *Assume that $2=0$, $D|Z=0$, and there exists a separable polynomial $f=X^2-Xa-b$ in $B[X ; D]_{(2)}$. Then $a\in U(Z)$, and any polynmial in $B[X ; D]_{(2),a}$ is Galois over B; moreover, the group $B[X ; D]^{\sim}_{(2),a}$ is isomorphic to the additive group*

$(Z, +)/\{z^2 + z\,;\ z \in Z\}$.

Proof. By Lemma 3. 3(vi), $\delta(f) = a^2$ is inversible in B. Clearly, for any $g \in B[X\,;\ D]_{(2),a}$, we have $\delta(g) = a^2$, and hence by Th. 3. 4, g is Galois over B. Next, let β be any element of $\mathfrak{B}_a(B)$. Then, there exists an element $\alpha \in U(Z)$ such that $I_\beta = D + \alpha_r D$ and $a(1 + \alpha) = D(\alpha)$. Since $D(\alpha) = 0$ and $a \in U(Z)$, we have $1 = \alpha$, which implies $I_\beta = 0$, that is, $\beta \in Z$. Noting $Z \subset \mathfrak{B}_a(B)$ (Lemma 3. 16), we obtain $Z = \mathfrak{B}_a(B)$. Moreover, for any $s \in Z$, if $z \in Z$ and $sD(z) = z$ then $z = 0$. Hence, it follows from Th. 3. 19 that $B[X\,;\ D]_{\tilde{(2)},a} \cong (Z, +)/\{z^2 + z\,;\ z \in Z\}$, which is our desired one.

Moreover, for case $a \in Z - U(Z)$, we have the following

Theorem 3. 21. *Assume that* $2 = 0$ *and there exists a separable polynomial* $f = X^2 - Xa - b$ *in* $B[X\,;\ D]_{(2)}$ *so that a is nilpotent.* Then $B[X\,;\ D]_{\tilde{(2)}} = B[X\,;\ D]_{\tilde{(2)}),a} \cong (Z_0, +)/Z_{\Delta}$. *If, in particular,* f *is Galois over* B *then there exists an element* s *in* $U(Z)$ *such that* $B[X\,;\ D]_{\tilde{(2)},a} \cong (Z, +)/(K_1 + K_2)$ *where* $K_1 = \{z \in Z\,;\ sD(z) = z\}$, and $K_2 = \{z^2 + z\,;\ z \in Z\}$.

Proof. By Cor. 3. 8 and Th. 3. 12, there exists an element s in Z with $D(s) \in U(Z)$, and $B[X\,;\ D]_{(2),a} = B[X\,;\ D]_{(2)}$. Now, let β be an element of $\mathfrak{B}_a(B)$. Then $I_\beta = D + \alpha_r D$ for some $\alpha \in U(Z)$. Applying this to the element s, we have $0 = I_\beta(s) = D(s) + D(s)\alpha = D(s)(1 + \alpha)$, and hence $\alpha = 1$. Since $2 = 0$, it follows $I_\beta = 0$, that is, $\beta \in Z$. Noting $Z \subset \mathfrak{B}_a(B)$ (Lemma 3. 16), we obtain $Z = \mathfrak{B}_a(B)$. Hence, by Th. 3. 19, we obtain the assertion.

Lastly, as a direct consequence of Cor. 3. 9 and Th. 3. 21, we obtain the following

Corollary 3. 22. *Assume that there exists a separable polynomial* $f = X^2 - Xa - b$ *in* $B[X\,;\ D]_{(2)}$ *with* $\delta(f) = 0$. *Then* $B[X\,;\ D]_{\tilde{(2)}} = B[X\,;\ D]_{\tilde{(2},a)} \cong (Z_0, +)/Z_{\Delta}$. *If, in particular,* f *is Galois over* B *then there exists an element* s *in* $U(Z)$ *such that* $B[X\,;\ D]_{\tilde{(2)}} \cong (Z, +)/(K_1 + K_2)$ *where* $K_1 = \{z \in Z\,;\ sD(z) = z\}$ and $K_2 = \{z^2 + z\,;\ z \in Z\}$.

REFERENCES

[1] K. KITAMURA: On the free quadratic extensions of commutative rings, Osaka J. Math. **10** (1973), 15—20.

[2] R. KISHIMOTO: On abelian extensions of rings I, Math. J. Okayama univ. **14** (1974), 159—174.

[3] K. KISHIMOTO: On abelian extensions of rings II, Math. J. Okayama Univ. **15** (1971),

47—70.

[4] K. KISHIMOTO: A classification of free quadraitc extensions of rings, Math. J. Okayama Univ. **18** (1976), 139—148.

[5] Y. MIYASHITA: Finite outer Galois theory of non-commutative rings, Jour. Fac. Sci. Hokkaido Univ., Ser. I, **19** (1966), 114—134.

[6] T. NAGAHARA: On separable polynomials over a commuttaive ring II, Math. Okayama Univ. **15** (1972), 149—162.

[7] T. NAGAHARA: A quadratic extension, Proc. Japan Acad. **47** (1971), 6—7.

DEPARTMENT OF MATHEMATICS
OKAYAMA UNIVERSITY

(*Received August 21, 1976*)