

# *Mathematical Journal of Okayama University*

---

*Volume 18, Issue 2*

1975

*Article 6*

JUNE 1976

---

## A classification of free quadratic extensions of rings

Kazuo Kishimoto\*

\*Shinshu University

Copyright ©1975 by the authors. *Mathematical Journal of Okayama University* is produced by  
The Berkeley Electronic Press (bepress). <http://escholarship.lib.okayama-u.ac.jp/mjou>

## A CLASSIFICATION OF FREE QUADRATIC EXTENSIONS OF RINGS

Dedicated to Professor Kiiti Morita on his 60th birthday

KAZUO KISHIMOTO

**Introduction.** Throughout this paper,  $B$  will mean a ring with identity 1 and all ring extensions of  $B$  will be assumed with the (common) identity 1. A ring extension  $A$  of  $B$  is called a *free extension* of  $B$  if  $A$  is free as right  $B$ -module and as left  $B$ -module.

The purpose of this paper is to construct a semigroup and a group consisting of  $B$ -ring isomorphism classes of free quadratic extensions (free extensions of rank 2) of  $B$ , and moreover the study contains some characterization of these semigroup and group. In commutative case, such constructions have been studied in [1], [2] and others. Indeed, K. Kitamura proved that if  $B$  is commutative and  $Q_f(B)$  means the set of all  $B$ -algebra isomorphism classes of free quadratic extensions of  $B$  then  $Q_f(B)$  forms an abelian semigroup under a certain composition, and the set of all  $B$ -algebra isomorphism classes of free quadratic separable extensions coincides with  $U(Q_f(B))$ , the set of all invertible elements of  $Q_f(B)$  which is a subgroup of  $Q_f(B)$ ; in particular, if 2 is invertible in  $B$  then  $U(Q_f(B))$  is isomorphic to  $U(B)/U(B)^2$ ,  $U(B)^2 = \{u^2 \mid u \in U(B)\}$ .

In this paper, §0 is devoted to notations and terminologies for the subsequent study. In §§1 and 2, we assume that 2 is invertible in  $B$ . In §1, we shall study on the separability of free quadratic extensions of automorphism type. In §2, we shall show that some isomorphism classes of free quadratic extensions of  $B$  of automorphism type form an abelian semigroup with identity, and we shall determine the structure of the semigroup. Especially, for commutative rings, we see that the semigroup is isomorphic to  $B/U(B)^2$  (cf. [2]). In §3, we assume that  $2=0$  in  $B$ . In this case, any cyclic extension of  $B$  with a Galois group of order 2 is obtained as a free quadratic extension of derivation type (cf. [3]). We shall here show that some isomorphism classes of free quadratic extensions of  $B$  of derivation type form an abelian group, and we shall determine the structure of the group. Especially, for commutative rings, the group is isomorphic to  $(B, +)/\{b^2 + b \mid b \in B\}$ .

**0. Notations and terminologies.** Let  $\rho$  and  $D$  be an automorphism

and a derivation of  $B$  respectively. We use the following conventions :

$Z$  = the center of  $B$ .

$B_1 = B^\rho = \{b \in B \mid \rho(b) = b\}$ ,  $Z_1 = Z \cap B_1$ .

$B(\rho^i) = \{b \in B \mid cb = b\rho^i(c) \text{ for all } c \in B\}$ ,  $B_1(\rho^i) = B_1 \cap B(\rho^i)$ .

$LN_\rho(b; n) = \rho^{n-1}(b)\rho^{n-2}(b)\cdots\rho(b)b$  ( $b \in B$ ).

$LN_\rho(B; n) = \{LN_\rho(b; n) \mid b \in B\}$ ,  $LN(b; n) = LN_1(b; n) = b^n$ .

$\tilde{b} = b_i b_r^{-1}$ , the inner automorphism generated by  $b \in U(B)$ .

$I_b = b_r - b_i$ , the inner derivation generated by  $b \in B$ .

$B_o = B^D = \{b \in B \mid D(b) = 0\}$ ,  $Z_o = B_o \cap Z$ .

$B(a, D) = \{b \in B \mid I_b = D^2 + a_r D\}$ ,  $B_o(a, D) = B_o \cap B(a, D)$ .

$B[X; \rho]$  (resp.  $B[X; D]$ ) = the ring of all polynomials  $\sum_i X^i b_i$  ( $b_i \in B$ ) in an indeterminate  $X$  whose multiplication is defined by  $bX = X\rho(b)$  (resp.  $bX = Xb + D(b)$ ) for each  $b \in B$ .

If  $a \in B_1(\rho)$  and  $b \in B_1(\rho^2)$  then  $(X^2 - Xa - b)B[X; \rho]$  is a two-sided ideal of  $B[X; \rho]$ . In this case, the ring extension of  $B$ ,  $B[X; \rho]/(X^2 - Xa - b)B[X; \rho]$  is called a *free quadratic extension of  $\rho$ -automorphism type*. On the other hand, in case  $2=0$ , if  $a \in Z_o$  and  $b \in B_o(a, D)$  then  $(X^2 - Xa - b)B[X; D]$  is a two-sided ideal of  $B[X; D]$ , and conversely. In this case, the ring extension of  $B$ ,  $B[X; D]/(X^2 - Xa - b)B[X; D]$  is called a *free quadratic extension of  $D$ -derivation type*. Moreover, we use the following notations :

$\Omega_\rho(B) = \{B[X; \rho]/(X^2 - Xa - b)B[X; \rho] \mid a \in B_1(\rho), b \in B_1(\rho^2)\}$ .

$\Omega_b^0(B) = \{B[X; \rho]/(X^2 - b)B[X; \rho] \mid b \in B_1(\rho^2)\}$ .

$\Omega_b^2(B) = \{B[X; D]/(X^2 - Xa - b)B[X; D] \mid b \in B_o(a, D)\}$ , where  $a$  is a (fixed) element of  $U(Z_o)$  and  $2=0$ .

Finally, a ring extension  $A$  of  $B$  is called *separable* over  $B$  if the  $A$ - $A$ -homomorphism  $a \otimes a' \rightarrow aa'$  of  $A \otimes_B A$  onto  $A$  splits. If  $A$  is a Galois extension of  $B$  then  $A/B$  is separable (cf. [5, Th. 1. 5]).

**1. Separability of a free quadratic extension of  $\rho$ -automorphism type.** In this section, we assume that  $2$  is invertible in  $B$ . If  $A = B[X; \rho]/(X^2 - b)B[X; \rho] \in \Omega_b^0(B)$  then we denote  $X + (X^2 - b)B[X; \rho]$  and  $A$  by  $x_b$  and  $B[x_b]$  respectively. Firstly, we shall prove the following

**Lemma 1.1.** *If  $A \in \Omega_\rho(B)$  then  $A$  is  $B$ -ring isomorphic to some  $A' \in \Omega_b^0(B)$ .*

*Proof.* Let  $A = B[X; \rho]/(X^2 - Xa - b)B[X; \rho]$  and  $x = X + (X^2 - Xa - b)B[X; \rho]$  where  $a \in B_1(\rho)$  and  $b \in B_1(\rho^2)$ . Then  $\{1, y = x - a/2\}$  is a free  $B$ -basis for  $A$ . For each  $c \in B$ ,  $cy = c(x - a/2) = x\rho(c) - (a/2)\rho(c) =$

$y\rho(c)$  and  $y^2 = x^2 - xa + a^2/4 = b + a^2/4 \in B_1(\rho^2)$ . Hence, if we set  $c = b + a^2/4$  then  $A$  is  $B$ -ring isomorphic to  $B[x_c] \in \Omega_\rho^0(B)$ .

Now, as in [4], an extension  $A/B$  in  $\Omega_\rho(B)$  will be called *strongly cyclic* if  $A/B$  is  $(\sigma)$ -Galois and  $A$  contains a unit  $a$  with  $\sigma(a) = -a$ . Next, we shall prove the following

**Theorem 1.2.** *Let  $A \in \Omega_\rho(B)$ . Then, the extension  $A/B$  is separable if and only if it is strongly cyclic. In case  $A = B[x_b] \in \Omega_\rho^0(B)$ ,  $A/B$  is separable if and only if  $b$  is invertible in  $B$ .*

*Proof.* By Lemma 1.1, we may assume that  $A = B[x_b] \in \Omega_\rho^0(B)$ . If  $b$  is invertible in  $B$  then, as in [4], there exists an automorphism  $\sigma$  of  $A$  mapping  $x_b$  into  $-x_b$  and  $A/B$  is a Galois extension with a Galois group  $(\sigma)$  of order 2. If  $A/B$  is Galois then it is separable by [5, Th. 1.5]. For the remainder of the proof, we assume that  $A/B$  is separable, and we set  $x = x_b$ . Then there exist elements  $xa_{1i} + a_{0i}, xb_{1i} + b_{0i}$  ( $a_{1i}, a_{0i}, b_{1i}, b_{0i} \in B, i = 1, 2, \dots, m$ ) such that

$$\sum_{i=1}^m (xa_{1i} + a_{0i})(xb_{1i} + b_{0i}) = 1,$$

$$\sum_{i=1}^m (y(xa_{1i} + a_{0i}) \otimes (xb_{1i} + b_{0i})) = \sum_{i=1}^m ((xa_{1i} + a_{0i}) \otimes (xb_{1i} + b_{0i})y) \quad (y \in A).$$

The first equation implies  $1 = \sum_{i=1}^m x(a_{1i}b_{0i} + \rho(a_{0i})b_{1i}) + \sum_{i=1}^m (b\rho(a_{1i})b_{1i} + a_{0i}b_{0i})$ . Hence we have

$$(1) \quad \sum_{i=1}^m (b\rho(a_{1i})b_{1i} + a_{0i}b_{0i}) = 1.$$

While, the second equation implies  $\sum_{i=1}^m (x(xa_{1i} + a_{0i}) \otimes (xb_{1i} + b_{0i})) = \sum_{i=1}^m ((ba_{1i} + xa_{0i}) \otimes (xb_{1i} + b_{0i})) = \sum_{i=1}^m ((x \otimes x)\rho(a_{0i})b_{1i} + (x \otimes 1)a_{0i}b_{0i} + (1 \otimes x)\rho(ba_{1i})b_{1i} + (1 \otimes 1)ba_{1i}b_{0i})$  and this is equal to  $\sum_{i=1}^m ((xa_{1i} + a_{0i}) \otimes (xb_{1i} + b_{0i})x) = \sum_{i=1}^m ((xa_{1i} + a_{0i}) \otimes (b\rho(b_{1i}) + x\rho(b_{0i}))) = \sum_{i=1}^m ((x \otimes x)\rho(a_{1i}b_{0i}) + (1 \otimes x)\rho(a_{0i}b_{0i}) + (x \otimes 1)a_{1i}b\rho(b_{1i}) + (1 \otimes 1)a_{1i}b\rho(b_{1i}))$ .

Comparing the coefficients of  $x \otimes 1$ , we have

$$(2) \quad \sum_{i=1}^m a_{0i}b_{0i} = \sum_{i=1}^m a_{1i}b\rho(b_{1i}) = \sum_{i=1}^m \rho^2(a_{1i})\rho(b_{1i}).$$

By (1) and (2),

$$\begin{aligned} 1 &= \sum_{i=1}^m (b\rho(a_{1i})b_{1i} + a_{0i}b_{0i}) \\ &= \sum_{i=1}^m (b\rho(a_{1i})b_{1i} + b\rho^2(a_{1i})\rho(b_{1i})) \\ &= b \sum_{i=1}^m (\rho(a_{1i})b_{1i} + \rho^2(a_{1i})\rho(b_{1i})). \end{aligned}$$

Hence  $x^2 = b$  is invertible. This completes the proof.

**2. A classification of free quadratic extensions of  $\rho$ -automorphism type.** Throughout the present section, we assume that 2 is invertible in

$B$  and  $\rho$  is an automorphism of  $B$  such that  $\rho^2 = \tilde{u}^{-1}$  for some  $u \in U(B_1)$ .

**Lemma 2.1.** *Let  $B[x_b]$  and  $B[x_c]$  be elements of  $\mathcal{O}'_\rho(B)$ . Then  $B[x_b]$  is  $B$ -ring isomorphic to  $B[x_c]$  if and only if  $b = cs$  for some  $s \in LN_\rho(U(Z); 2)$ , and in this case, if  $s = LN_\rho(\alpha; 2)$  with  $\alpha \in U(Z)$  then there exists a  $B$ -ring isomorphism  $B[x_b] \rightarrow B[x_c]$  mapping  $x_b$  into  $x_c\alpha$ .*

*Proof.* We write  $x = x_b$  and  $y = x_c$ . If  $b = cLN_\rho(\alpha; 2)$  for some  $\alpha \in U(Z)$  then  $(y\alpha)^2 = y^2LN_\rho(\alpha; 2) = x^2$ ,  $d(y\alpha) = (y\alpha)\rho(d)$  for all  $d \in B$ , and hence, the mapping  $ux + v \rightarrow uy\alpha + v$  ( $u, v \in B$ ) is a  $B$ -ring isomorphism of  $B[x]$  onto  $B[y]$ . Conversely, we assume that there exists a  $B$ -ring isomorphism  $\varphi : B[x] \rightarrow B[y]$ . Then  $\varphi(x) = y\alpha + \beta$  for some  $\alpha, \beta \in B$ . If  $d \in B$  then  $y\rho(d)\alpha + d\beta = d(y\alpha + \beta) = \varphi(dx) = \varphi(x\rho(d)) = y\alpha\rho(d) + \beta\rho(d)$ . This shows that  $\alpha \in Z$  and  $\beta \in B(\rho)$ . Since  $y = (y\alpha + \beta)d_1 + d_2$  for some  $d_1, d_2 \in B$ ,  $\alpha$  is contained in  $U(Z)$ . Further  $x^2 = \varphi(x^2) = (y\alpha + \beta)^2 = y^2\rho(\alpha)\alpha + y\alpha(\beta + \rho(\beta)) + \beta^2$  yields  $\beta + \rho(\beta) = 0$ . Noting that  $\beta \in B(\rho)$ , we have  $0 = \rho(\beta + \rho(\beta)) = 2\beta^2$ , and hence  $\beta^2 = 0$ . Therefore  $x^2 = y^2\rho(\alpha)\alpha$ , that is,  $b = cLN_\rho(\alpha; 2)$ ,  $\alpha \in U(Z)$ .

**Lemma 2.2.**  $B_1(\rho^2) = uZ_1$ , and  $Z_1 \cong LN_\rho(U(Z); 2)$  as a multiplicative subgroup. Moreover, if  $b \in B_1(\rho^2)$  then so is  $bcu^{-1}$  for all  $c \in B_1(\rho^2)$ , and  $b \in B_1(\rho^2) \cap U(B)$  if and only if  $bdu^{-1} \in uLN_\rho(U(Z); 2)$  for some  $d \in B_1(\rho^2)$ .

*Proof.* Let  $b \in B_1(\rho^2)$ . If  $d \in B$  then  $db = b\rho^2(d) = bu^{-1}du$ , and so,  $dbu^{-1} = bu^{-1}d$ . This shows that  $bu^{-1} \in Z \cap B_1 = Z_1$ , and hence  $b \in uZ_1$ . Conversely, if  $b \in uZ_1$  then it is clear that  $b \in B_1(\rho^2)$ . Thus we obtain  $B_1(\rho^2) = uZ_1$ . The other assertions will be easily seen.

Now, by  $P_\rho(B)$ , we denote the set of all  $B$ -ring isomorphism classes in  $\mathcal{O}_\rho(B)$ , and if  $C \in P_\rho(B)$  and  $A \in C$  then we write  $C = \langle A \rangle$ . By Lemma 1.1, each  $C \in P_\rho(B)$  meets  $\mathcal{O}'_\rho(B)$ , and hence, if  $C \in P_\rho(B)$  then  $C = \langle A \rangle$  for some  $A \in \mathcal{O}'_\rho(B)$ . Under this situation, we shall prove the following

**Theorem 2.3.**  $P_\rho(B)$  forms an abelian semigroup with  $\mathbf{1} = \langle B[x_u] \rangle$  under the composition  $\langle B[x_b] \rangle \langle B[x_c] \rangle = \langle B[x_{bcu^{-1}}] \rangle$ . Moreover, for an element  $\langle B[x_b] \rangle$  of  $P_\rho(B)$ ,  $\langle B[x_b] \rangle \in U(P_\rho(B))$  if and only if  $b \in U(B)$ .

*Proof.* Let  $\langle B[x_b] \rangle = \langle B[x_{b'}] \rangle$  and  $\langle B[x_c] \rangle = \langle B[x_{c'}] \rangle$ . Then by Lemma 2.1, there exist elements  $s, t \in LN_\rho(U(Z); 2)$  with  $b = b's$  and  $c = c't$ . Hence  $bcu^{-1} = b'c'u^{-1}st \in B_1(\rho^2)$ , and  $st \in LN_\rho(U(Z); 2)$  (Lemma 2.2). This means that  $\langle B[x_{bcu^{-1}}] \rangle = \langle B[x_{b'c'u^{-1}}] \rangle$ , that is, the composition is well defined. The other assertion follows immediately from Lemma 2.2.

**Theorem 2.4.**  $P_\rho(B)$  is isomorphic to the factor semigroup  $Z_1/LN_\rho(U(Z); 2)$ . In particular,  $U(P_\rho(B))$  is isomorphic to  $U(Z_1)/LN_\rho(U(Z); 2)$ , and  $U(P_\rho(B))$  coincides with the subset of  $P_\rho(B)$  consisting of the elements  $\langle A \rangle$  with  $A$  separable over  $B$ .

*Proof.* By Lemma 2.2, the mapping

$$f: z \longrightarrow \langle B[x_{z_n}] \rangle \quad (z \in Z_1)$$

is a semigroup epimorphism of  $Z_1$  onto  $P_\rho(B)$ . For elements  $z, z' \in Z_1$ ,  $f(z) = f(z')$  if and only if  $z = z's$  for some  $s \in LN_\rho(U(Z); 2)$  (Lemma 2.1). This implies that  $Z_1/LN_\rho(U(Z); 2)$  is isomorphic to  $P_\rho(B)$ . Moreover, since  $U(Z_1/LN_\rho(U(Z); 2)) = U(Z_1)/LN_\rho(U(Z); 2)$ ,  $U(Z_1)/LN_\rho(U(Z); 2)$  is isomorphic to  $U(P_\rho(B))$ . The last assertion is a direct consequence of Ths. 1.2 and 2.3.

Now, it is easily seen that for any  $A \in \mathcal{Q}_1(B)$ ,  $A \cong B \otimes_{zA'} A'$  for some  $A' \in \mathcal{Q}_1(Z)$ , where  $1$  is the identity map of  $B$  onto  $B$ . Moreover, as an easy consequence of Th. 2.4, we obtain the following

**Corollary 2.5.** If  $\rho \mid Z$  (the restriction of  $\rho$  on  $Z$ ) = 1 then  $Z/U(Z)^2 \cong P_\rho(B) \cong P_1(B) \cong P_1(Z) = Q_\rho(Z)$ . In particular,

- (1) if  $\rho$  is inner then  $P_\rho(B) \cong P_1(B)$ .
- (2) (Kitamura [2]) If  $B$  is commutative then  $P_1(B) \cong B/U(B)^2$ .

Next, we consider some free quadratic extensions of  $B[X; \rho]$  of automorphism type. The automorphism  $\rho$  can be extended to an automorphism  $\sigma$  of  $B[X; \rho]$  by  $\sigma(\sum_i X^i b_i) = \sum_i X^i \rho(b_i)$ . Then  $\sigma^2 = \tilde{u}^{-1}$  and  $u \in U(B[X; \rho]^\sigma)$ . By C, we denote the center of  $B[X; \rho]$ . Then we have the following

**Theorem 2.6.**  $P_\sigma(B[X; \rho])$  is isomorphic to  $C/U(C)^2$ . If  $U(B[X; \rho]) = U(B)$  then  $U(P_\sigma(B[X; \rho])) \cong U(P_1(Z_1)) \cong U(Z_1)/U(Z_1)^2 \sim U(Z_1)/LN_\rho(U(Z); 2) \cong U(P_\rho(B))$  where  $\sim$  is the canonical epimorphism  $zU(Z_1)^2 \longrightarrow zLN_\rho(U(Z); 2)$ , and in case  $\rho=1$ , this is an isomorphism.

*Proof.* As is easily seen,  $B[X; \rho]^\sigma$  coincides with the centralizer of  $X$  in  $B[X; \rho]$ . This implies that  $B[X; \rho] \supseteq C$ , and so,  $C^\sigma = C$ . Hence by Th. 2.4,  $P_\sigma(B[X; \rho])$  is isomorphic to  $C/U(C)^2$ . Next, we assume that  $U(B[X; \rho]) = U(B)$ . Then  $U(C) \subseteq U(B) \cap U(C^\sigma) \subseteq U(B \cap C^\sigma) \subseteq U((B \cap C)^\sigma) \subseteq U(Z^\sigma) = U(Z_1)$ . Since  $C \supseteq Z_1$ , it follows that  $U(C) = U(Z_1)$ . Hence  $U(C)/U(C)^2 = U(Z_1)/U(Z_1)^2$ . Noting that  $U(Z_1) \supseteq LN_\rho(U(Z); 2) \supseteq U(Z_1)^2$ , we obtain the other assertion by Th. 2.4.

Next, for rings  $B \cong R$ , we shall consider the groups  $P_\rho(B)$ ,  $P_\gamma(R)$ . Let  $R$  be a ring with an automorphism  $\eta$  such that  $\eta^2 = \tilde{v}^{-1}$  for some  $v \in$

$U(R)$  with  $\eta(v)=v$ . Further, by  $W$  we denote the center of  $R$ , and we set  $W_1=W^n$ . Under this situation, we shall prove the following

**Theorem 2.7.** *If there exists a ring isomorphism  $\varphi$  of  $B$  onto  $R$  with  $\varphi\rho=\eta\varphi$ , then  $P_\rho(B)\cong P_\eta(R)$ . In particular, if  $B\cong R$ , then  $P_1(B)\cong P_1(R)$ .*

*Proof.* Since  $\varphi$  is an isomorphism,  $\eta(Z)=W$  is clear. If  $z\in Z_1$  then  $\varphi(z)=\varphi(\rho(z))=\eta(\varphi(z))$ . This shows that  $\varphi(Z_1)\subseteq W_1$ . Symmetrically, we have  $\varphi^{-1}(W_1)\subseteq Z_1$ . Thus we obtain  $\varphi(Z_1)=W_1$ . By a similar method, we also obtain  $\varphi(LN_\rho(U(Z); 2))=LN_\eta(U(W); 2)$ . Hence  $Z_1/LN_\rho(U(Z); 2)$  is isomorphic to  $W_1/LN_\eta(U(W); 2)$ . From this and Th. 2.4, our assertion follows immediately.

**3. A classification of free quadratic extensions of  $D$ -derivation type.** Throughout the present section, we assume that  $2=0$  in  $B$ ,  $D$  is a derivation of  $B$ , and that  $a$  is a (fixed) element of  $U(Z_0)$ . Further, we set

$$\mathfrak{B}_a(B) = \{\beta \in B \mid \beta^2 + D(\beta) + \beta a \in Z_0 \text{ and } I_\beta = D + \alpha_r D \\ \text{for some } \alpha \in U(Z) \text{ with } \alpha^2 = 1 \text{ and } a(1+\alpha) = D(\alpha)\}.$$

$$\mathfrak{D}_a(B) = \{\beta^2 + D(\beta) + \beta a \mid \beta \in \mathfrak{B}_a(B)\}.$$

If we take  $\alpha=1$  and  $\beta=0$  then  $\alpha \in U(Z)$ ,  $\alpha^2=1$  and  $a(1+\alpha)=2\alpha=0=D(1)=D(\alpha)$ . Further  $0=\beta^2 + D(\beta) + \beta a \in Z_0$  and  $0=I_\beta=2D=D+D=D+1_r D$ . Thus  $\mathfrak{B}_a(B) \ni 0$ . This shows that  $\mathfrak{B}_a(B) \neq \emptyset$ , and hence  $\mathfrak{D}_a(B) \neq \emptyset$ .

First, we shall prove the following

**Lemma 3.1.** (1) *If  $\beta\delta=\delta\beta$  for all  $\beta, \delta \in \mathfrak{B}_a(B)$  then  $\mathfrak{D}_a(B)$  is an additive subgroup of  $(Z_0, +)$ .*

(2) *If  $D(z) \neq az$  for each  $z \in Z - \{0\}$  then  $\mathfrak{B}_a(B) \subseteq Z$ .*

*Proof.* (1) Let  $\beta, \delta$  be elements of  $\mathfrak{B}_a(B)$ . Then there exist elements  $\alpha, \gamma$  in  $U(Z)$  such that  $\alpha^2=\gamma^2=1$ ,  $a(1+\alpha)=D(\alpha)$ ,  $a(1+\gamma)=D(\gamma)$ ,  $I_\beta=D + \alpha_r D$  and  $I_\delta=D + \gamma_r D$ . Since  $\beta\delta=\delta\beta$ , we have  $(\beta+\gamma)^2=\beta^2+\gamma^2$ . Hence  $(\beta^2 + D(\beta) + \beta a) + (\delta^2 + D(\delta) + \delta a) = (\beta+\delta)^2 + D(\beta+\delta) + (\beta+\delta)a$ , which is in  $Z_0$ . We set here  $\kappa=1+\alpha+\gamma$ . Then  $\kappa^2=1+\alpha^2+\gamma^2=1$ ,  $\kappa \in U(Z)$ ,  $I_{\beta+\delta}=I_\beta + I_\delta = (\alpha+\gamma)_r D = (\kappa-1)_r D = D + \kappa_r D$ , and  $a(1+\kappa) = a(\alpha+\gamma) = a(1+\alpha) + a(1+\gamma) = D(\alpha+\gamma) = D(\kappa-1) = D(\kappa)$ . Therefore, it follows that  $\mathfrak{D}_a(B)$  is an additive subgroup of  $(Z_0, +)$ .

(2) Let  $\beta$  be an element of  $\mathfrak{B}_a(B)$ . Then  $I_\beta=D + \alpha_r D$  for some  $\alpha \in U(Z)$  with  $\alpha^2=1$ , and  $a(1+\alpha)=D(\alpha)$ . Hence  $a(1+\alpha) = D(\alpha) = D(1+\alpha)$ . Since  $1+\alpha \in Z$ , we have  $1+\alpha=0$ , and so,  $\alpha=1$ . Hence  $I_\beta=2D=0$ , which implies  $\beta \in Z$ . This completes the proof.

In the rest of this section, we assume that  $D^2 + a_r D$  is an inner deriva-

tion determined by an element of  $B_0$ . Then we have  $B_0(a, D) \neq \emptyset$ , and so  $\Omega_D^a(B) \neq \emptyset$ . Moreover, we set

$$P_D^a(B) = \text{the set of all } B\text{-ring isomorphism classes in } \Omega_D^a(B),$$

$$\langle A \rangle = C \text{ if } C \in P_D^a(B) \text{ and } A \in C.$$

Further, if  $A = B[X; D]/(X^2 - Xa - b) \in \Omega_D^a(B)$  then we denote  $X + (X^2 - Xa - b)B[X; D]$  and  $A$  by  $x_b$  and  $B[x_b]$  respectively.

**Lemma 3.2.** *Let  $b$  be an element of  $B_0(a, D)$ . Then*

- (1)  $B_0(a, D) = \{b + z \mid z \in Z_0\}$ .
- (2) *If  $c$  and  $d$  are elements of  $B_0(a, D)$ , then so is  $c + d + b$ .*

*Proof.* Let  $c$  be an element of  $B_0(a, D)$ . Then  $I_c = D^2 + a_r D = I_b$ . This implies  $c = b + z$  for some  $z \in Z_0$ . Conversely, for each  $z \in Z_0$ , it is obvious that  $I_{b+z} = I_b = D^2 + a_r D$ , and hence  $b + z \in B_0(a, D)$ . Thus we obtain (1). The assertion (2) will be easily seen from (1).

**Lemma 3.3.** *Let  $B[x_b]$  and  $B[x_c]$  be elements of  $\Omega_D^a(B)$ . Then  $B[x_b]$  is  $B$ -ring isomorphic to  $B[x_c]$  if and only if  $b + c \in \mathfrak{D}_a(B)$ .*

*Proof.* We write  $x = x_b$  and  $y = x_c$ . First, we assume that  $b + c \in \mathfrak{D}_a(B)$ . Then there exist elements  $\alpha \in U(Z)$  and  $\beta \in B$  such that  $b + c = \beta^2 + D(\beta) + \beta a$ ,  $I_\beta = D + \alpha_r D$ ,  $\alpha^2 = 1$ , and  $a(1 + \alpha) = D(\alpha)$ . Since  $I_\beta(\alpha) = 0$  and  $I_\beta(\beta) = 0$ , we have  $D(\alpha)\alpha = D(\alpha)$  and  $D(\beta)\alpha = D(\beta)$ . We set here  $y_* = y\alpha + \beta$ . Then  $y_*^2 = y(\alpha a^2 + D(\alpha)\alpha) + c\alpha^2 + D(\beta)\alpha + \beta^2 = y(a + D(\alpha)) + c + D(\beta) + \beta^2 = y\alpha a + b + \beta a = y_* a + b$ , and moreover, for each  $d \in B$ ,  $dy_* = yd\alpha + D(d)\alpha + d\beta = y\alpha d + D(d) + \beta d = y_* d + D(d)$ . Hence, the mapping  $ux + v \rightarrow uy_* + v$  ( $u, v \in B$ ) is a  $B$ -ring isomorphism of  $B[x]$  to  $B[y]$ . To see the converse, we assume that there exists a  $B$ -ring isomorphism  $B[x] \rightarrow B[y]$ , which will be denoted by  $\phi$ . Then  $\phi(x) = y\alpha + \beta$  for some  $\alpha, \beta \in B$ ,  $\phi(dx) = d\phi(x)$  for all  $d \in B$ , and  $\phi(x^2) = \phi(x)^2$ . Since, for  $d \in B$ ,  $\phi(dx) = \phi(xd + D(d)) = y\alpha d + \beta d + D(d)$  and  $d\phi(x) = d(y\alpha + \beta) = yd\alpha + D(d)\alpha + d\beta$ , it follows that  $\alpha \in Z$  and  $I_\beta = D + \alpha_r D$ . Noting that  $y = (y\alpha + \beta)d_1 + d_2$  for some  $d_1, d_2 \in B$ , we see that  $\alpha \in U(Z)$ . Moreover, since  $\phi(x^2) = \phi(xa + b) = y\alpha a + \beta a + b$  and  $\phi(x)^2 = (y\alpha + \beta)^2 = y(\alpha a^2 + D(\alpha)\alpha) + c\alpha^2 + D(\beta)\alpha + \beta^2$ , it follows that  $a(1 + \alpha) = D(\alpha)$  and  $b + c\alpha^2 = \beta^2 + D(\beta)\alpha + \beta a$ . The derivation  $\alpha_r D = D - I_\beta$  gives  $D(\alpha)\alpha = D(\alpha)$  and  $D(\beta)\alpha = D(\beta)$ . Hence we obtain  $\alpha^2 = (a^{-1}D(\alpha) - 1)\alpha = a^{-1}D(\alpha)\alpha - \alpha = a^{-1}D(\alpha) - \alpha = 1$  and  $b + c = \beta^2 + D(\beta) + \beta a$ . By Lemma 3.2 (1), the sum  $b + c$  is contained in  $Z_0$ . We have therefore that  $b + c \in \mathfrak{D}_a(B)$ , the desired conclusion.

**Theorem 3.4.** *Assume that  $\beta\delta = \delta\beta$  for all  $\beta, \delta \in \mathfrak{B}_a(B)$ , and let  $b$  be*



an element of  $B_o(a, D)$ . Then  $P_D^a(B)$  forms an abelian group of exponent 2 under the composition  $\langle B[x_c] \rangle \langle B[x_d] \rangle = \langle B[x_{c+d+b}] \rangle$  (with the identity element  $\langle B[x_b] \rangle$ ), and this group is isomorphic to  $(Z_o, +)/\mathfrak{D}_a(B)$ .

*Proof.* Let  $\langle B[x_c] \rangle = \langle B[x_{c'}] \rangle$  and  $\langle B[x_d] \rangle = \langle B[x_{d'}] \rangle$  ( $c, c', d, d' \in B_o(a, D)$ ). Then by Lemma 3.3, the sums  $c+c'$  and  $d+d'$  are contained in  $\mathfrak{D}_a(B)$ . By Lemma 3.1(1),  $\mathfrak{D}_a(B)$  is an additive subgroup of  $(Z_o, +)$ . Hence we have  $(c+c')+(d+d') \in \mathfrak{D}_a(B)$ , that is,  $(c+d+b)+(c'+d'+b) \in \mathfrak{D}_a(B)$ . By Lemma 3.2(2),  $c+d+b$  and  $c'+d'+b$  are in  $B_o(a, D)$ . Therefore, it follows from Lemma 3.3 that  $\langle B[x_{c+d+b}] \rangle = \langle B[x_{c'+d'+b}] \rangle$ . This means that the composition is well defined. Clearly, the composition is associative and commutative. Moreover, we have that  $\langle B[x_c] \rangle \langle B[x_b] \rangle = \langle B[x_{c+b}] \rangle = \langle B[x_c] \rangle$ , and  $\langle B[x_c] \rangle \langle B[x_c] \rangle = \langle B[x_{c+c+b}] \rangle = \langle B[x_b] \rangle$ . Thus our composition makes  $P_D^a(B)$  into a group of exponent 2 with the identity element  $\langle B[x_b] \rangle$ . Now, if  $\langle B[x_c] \rangle \in P_D^a(B)$  then  $c \in B_o(a, D)$ , and conversely. Moreover,  $c \in B_o(a, D)$  if and only if  $c = b+z$  for some  $z \in Z_o$  (Lemma 3.2(1)). Hence the mapping

$$f: z \longrightarrow \langle B[x_{b+z}] \rangle \quad (z \in Z_o)$$

is a group epimorphism of  $Z_o$  to  $P_D^a(B)$ . For an element  $z \in Z_o$ , the result of Lemma 3.3 enables us to see that  $f(z) = \langle B[x_b] \rangle$  (identity element) if and only if  $z = (b+z)+b \in \mathfrak{D}_a(B)$ . This implies that  $(Z_o, +)/\mathfrak{D}_a(B)$  is isomorphic to  $P_D^a(B)$ .

**Remark.** We assume that  $\beta\delta = \delta\beta$  for all  $\beta, \delta \in \mathfrak{B}_a(B)$ , and by  $(P_D^a(B), b)$  we denote the group  $P_D^a(B)$  given in Th. 3.4 whose group composition is related to  $b$ , an element of  $B_o(a, D)$ . Then, for each element  $v \in B_o(a, D)$ , we have a group  $(P_D^a(B), v)$ . If  $b, v \in B_o(a, D)$  and  $b+v \in \mathfrak{D}_a(B)$  then, by Lemma 3.3, we see that the group composition in  $(P_D^a(B), b)$  is different from that in  $(P_D^a(B), v)$ . However, we have  $(Z_o, +)/\mathfrak{D}_a(B) \cong (P_D^a(B), v)$  for each  $v \in B_o(a, D)$  (Th. 3.4). In the rest of this section, we shall understand  $P_D^a(B)$  a group  $(P_D^a(B), b)$  where  $b$  is an element of  $B_o(a, D)$ .

**Lemma 3.5.** *The following conditions are equivalent.*

- (a)  $D(z) \neq az$  for each  $z \in Z - \{0\}$ .
- (b)  $D|Z$  (the restriction of  $D$  on  $Z$ ) = 0.

*Proof.* Clearly (b) implies (a). Conversely, assume (a), and let  $z$  be an arbitrary element of  $Z$ . Then, for each  $c \in B$ ,  $D(z)c = D(zc) - zD(c) = D(cz) - D(c)z = cD(z) + D(c)z - D(c)z = cD(z)$ , and this shows  $D(z) \in Z$ . Now, for an element  $b \in B_o(a, D)$  ( $\neq \emptyset$ ),  $0 = I_b(z) = D^2(z) - a_r D(z) = D^2(z) +$

$D(z)a = D^2(z) + aD(z)$ , that is,  $D(D(z)) = aD(z)$ . Since  $D(z) \in Z$ , it follows that  $D(z) = 0$ . Thus we obtain (b).

**Corollary 1.** (1) *If  $D(z) \neq az$  for each  $z \in Z - \{0\}$  (which is equivalent to that  $D|Z=0$ ) then  $P_D^a(B) \cong (Z, +) / \{z^2 + za \mid za \mid z \in Z\} \cong P_0^a(B) \cong P_0^a(Z)$ .*

(2) *If  $D$  is inner then  $P_D^a(B) \cong P_0^a(B)$ .*

(3) *If  $B$  is commutative then  $P_0^a(B) \cong (B, +) / \{b^2 + ba \mid b \in B\}$ .*

(4) *If  $a=1$  and  $D(z) \neq z$  for each  $z \in Z - \{0\}$  (i. e.,  $D^2 - D$  is an inner derivation determined by an element of  $B_0$  and  $D|Z=0$ ) then  $P_D^1(B) \cong (Z, +) / \{z^2 + z \mid z \in Z\} \cong P_0^1(B)$  and for each  $\langle A \rangle \in P_D^1(B)$ ,  $A$  is a Galois extension of  $B$ .*

*Proof.* (1) By Lemma 3.1(2), we have  $\mathfrak{B}_a(B) \subseteq Z$ . On the other hand, since  $Z = Z_0$ , it follows that  $\mathfrak{B}_a(B) = Z$ . Hence  $\mathfrak{D}_a(B) = \{z^2 + za \mid z \in Z\}$ . The rest is obvious from Th. 3.4. (2) Since  $D|Z=0$ , this is a direct consequence of (1). (3) This is also an easy consequence of (1). Moreover, (4) follows immediately from (1) and the result of [3. Cor. 1.1].

Finally we shall prove the following

**Theorem 3.5.** *Let  $\phi: B \rightarrow R$  be a ring isomorphism, and  $W$  the center of  $R$ . Then  $R$  has a derivation  $E$  with  $\phi D = E\phi$ , which is uniquely determined. If  $\beta\delta \neq \delta\beta$  for all  $\beta, \delta \in \mathfrak{B}_a(B)$  (resp. if  $D(z) \neq az$  for each  $z \in Z - \{0\}$ ) then  $P_D^a(B) \cong P_E^{a(\alpha)}(R)$  (resp.  $P_D^a(B) \cong P_E^{a(\alpha)}(R) \cong (W, +) / \{w^2 + w\phi(a) \mid w \in W\}$ ). In particular,  $P_0^1(B) \cong P_0^1(R)$ .*

*Proof.* Clearly the map  $E = \phi D \phi^{-1}$  of  $R$  into itself is a derivation of  $R$ . This implies the first assertion. Since  $\phi$  is a ring isomorphism, we have  $\phi(Z) = W$ . Moreover,  $E(\phi(B_0)) = \phi(D(B_0)) = 0$  and  $D(\phi^{-1}(R_0)) = \phi^{-1}(E(R_0)) = 0$  where  $R_0 = R^e$ . Hence  $\phi(B_0) \subseteq R_0$  and  $\phi^{-1}(R_0) \subseteq B_0$ . Thus we obtain  $\phi(B_0) = R_0$ , and  $\phi(Z_0) = \phi(Z \cap B_0) = \phi(Z) \cap \phi(B_0) = W \cap R_0 = W_0$ . For any  $b \in B_0(a, D) (\neq \emptyset)$ ,  $I_b = D^2 + a, D$ , and hence,  $I_{\phi(b)} = E^2 + \phi(a), E$  where  $\phi(b)$  is in  $R_0$ . Now, let  $\beta \in \mathfrak{B}_a(B)$ . Then  $\beta^2 + D(\beta) + \beta a \in Z_0$ ,  $I_\beta = D + \alpha, D$  for some  $\alpha \in U(Z)$  with  $\alpha^2 = 1$  and  $a(1 + \alpha) = D(\alpha)$ . Hence  $\phi(\beta)^2 + E(\phi(\beta)) + \phi(\beta)\phi(\alpha) \in \phi(Z_0) = W_0$ ,  $I_{\phi(\beta)} = E + \phi(\alpha), E$ ,  $\phi(\alpha) \in U(W)$ ,  $\phi(\alpha)^2 = 1$ , and  $\phi(a)(1 + \phi(\alpha)) = E(\phi(a))$ . Therefore, it follows that  $\phi(\beta) \in \mathfrak{R}_{\phi(\alpha)}(R) = \{\mu \mid \mu^2 + E(\mu) + \mu\phi(a) \in W_0, I_\mu = E + \nu, E \text{ for some } \nu \in U(W) \text{ with } \nu^2 = 1 \text{ and } \phi(a)(1 + \nu) = E(\nu)\}$ . Moreover, we have that  $\phi(\beta^2 + D(\beta) + \beta a) = \phi(\beta)^2 + E(\phi(\beta)) + \phi(\beta)\phi(a) \in \mathfrak{G}_{\phi(\alpha)}(R) = \{\mu^2 + E(\mu) + \mu a \mid \mu \in \mathfrak{R}_{\phi(\alpha)}(R)\}$ . Thus, we obtain that  $\phi(\mathfrak{B}_a(B)) \subset \mathfrak{R}_{\phi(\alpha)}(R)$  and  $\phi(\mathfrak{D}_a(B)) \subseteq \mathfrak{G}_{\phi(\alpha)}(R)$ ; symmetrically  $\phi^{-1}(\mathfrak{R}_{\phi(\alpha)}(R)) \subseteq \mathfrak{B}_a(B)$  and  $\phi^{-1}(\mathfrak{G}_{\phi(\alpha)}(R)) \subseteq \mathfrak{D}_a(B)$ . Hence  $\phi(\mathfrak{B}_a(B)) = \mathfrak{R}_{\phi(\alpha)}(R)$  and  $\phi(\mathfrak{D}_a(B)) = \mathfrak{G}_{\phi(\alpha)}(R)$ .

Consequently, if  $\beta\delta = \delta\beta$  for all  $\beta, \delta \in \mathfrak{B}_a(B)$  then  $\mu\rho = \rho\mu$  for all  $\mu, \rho \in \mathfrak{G}_{\neq(a)}(R)$ , and hence Theorem 3.4 enables us to obtain that  $P_D^a(B) \cong (Z_0, +)/\mathfrak{D}_a(B) \cong (W_0, +)/\mathfrak{G}_{\neq(a)}(R) \cong P_E^{\neq(a)}(R)$ . Moreover, if  $D(z) \neq az$  for each  $z \in Z - \{0\}$  then  $E(\phi(z)) = \phi(D(z)) \neq \phi(a)\phi(z)$  for each  $z \in Z - \{0\}$ , which implies  $E(w) \neq \phi(a)w$  for each  $w \in W - \{0\}$ ; and whence, by Cor. 1 (of Th. 3.4) we obtain  $P_E^{\neq(a)}(R) \cong (W, +)/\{w^2 + w\phi(a) \mid w \in W\}$ . The other assertion will be easily seen.

#### REFERENCES

- [ 1 ] H. BASS : Lectures on topics in algebraic  $K$ -theory, Tata Institute of Fundamental Research, Bombay, 1967.
- [ 2 ] K. KITAMURA : On the free quadratic extensions of commutative rings, Osaka J. Math. **10** (1973), 15—20.
- [ 3 ] K. KISHIMOTO : On abelian extensions of rings I, Math. J. Okayama Univ. **14** (1974), 159—174.
- [ 4 ] K. KISHIMOTO : On abelian extensions of rings II, Math. J. Okayama Univ. **15** (1971), 57—70.
- [ 5 ] Y. MIYASHITA : Finite outer Galois theory of non-commutative rings, J. Fac. Sci. Hokkaido Univ., Ser. I, **19** (1966), 114—134.

DEPARTMENT OF MATHEMATICS  
SHINSHU UNIVERSITY

(Received December 1, 1975)