



Title	On the free quadratic extensions of a commutative ring
Author(s)	Kitamura, Kazuo
Citation	Osaka Journal of Mathematics. 1973, 10(1), p. 15-20
Version Type	VoR
URL	https://doi.org/10.18910/3522
rights	
Note	

The University of Osaka Institutional Knowledge Archive : OUKA

<https://ir.library.osaka-u.ac.jp/>

The University of Osaka

Kitamura, K.
Osaka J. Math.
10 (1973), 15-20

ON THE FREE QUADRATIC EXTENSIONS OF A COMMUTATIVE RING

KAZUO KITAMURA

(Received May 24, 1972)

Let R be a commutative ring with unit element 1. A quadratic extension of R is an R -algebra which is a finitely generated projective R -module of rank 2. Let $Q(R)$ be the set of all R -algebra isomorphism classes of quadratic extensions of R , and $Q_s(R)$ the set of all R -algebra isomorphism classes of separable quadratic extensions of R . In [2], it was shown that the product in $Q_s(R)$, in the sense of [1], [4] and [5], is extended to $Q(R)$, and $Q(R)$ is an abelian semigroup with unit element. In this note, we study the quadratic extensions of R which are free R -modules. We shall call them the *free quadratic extensions* of R . Let $Q_f(R)$ and $Q_{fs}(R)$ be the sets of all classes which are free R -modules in $Q(R)$ and $Q_s(R)$, respectively. We shall show that $Q_f(R)$ is an abelian semigroup with unit element, and $Q_{fs}(R)$ is an abelian group consisting of all invertible elements in $Q_f(R)$. For some special rings, we shall determine the structures of $Q_f(R)$ and $Q_{fs}(R)$. We remark that $Q_{fs}(R)$, $Q_s(R)$ and $\text{Pic}(R)_2$; the group of isomorphism classes $[U]$ of R -module U such that $U \otimes_R U \cong R$, are closely related by the exact sequence $0 \rightarrow Q_{fs}(R) \rightarrow Q_s(R) \rightarrow \text{Pic}(R)_2$.

Let R be any commutative ring with unit element 1. For a free quadratic extension S of R , we can write $S=R \oplus Rx$ and $x^2=ax+b$ for some a, b in R , then we denote it by $S=(R, a, b)$, and by $[R, a, b]$ the R -algebra isomorphism class containing (R, a, b) .

Lemma 1. *The following two conditions a) and b) are equivalent;*

- a) $(R, a, b) \cong (R, c, d)$ as R -algebras,
- b) *there exist an invertible element α in R and an element β in R such that $c=\alpha(a-2\beta)$ and $d=\alpha^2(\beta a+b-\beta^2)$.*

If (R, a, b) and (R, c, d) satisfy a) or b), then we have

- c) $c^2+4d=\alpha^2(a^2+4b)$ for some invertible element α in R .

Moreover, if 2 is invertible in R , then we have the converse.

Proof. a) \rightarrow b): Let $\sigma: (R, a, b)=R \oplus Rx \rightarrow (R, c, d)=R \oplus Ry$ be an R -algebra isomorphism, and set $\sigma(x)=\alpha y+\beta$ and $\sigma^{-1}(y)=\alpha' x+\beta'$. Since $y=\sigma \cdot \sigma^{-1}(y)=\alpha' \alpha y+\alpha' \beta+\beta'$, we have $\alpha' \alpha=1$, that is, α and α' are invertible. The equalities $(\sigma(x))^2=(\alpha y+\beta)^2=\alpha(\alpha c+2\beta)y+\alpha^2 d+\beta^2$ and $\sigma(x^2)=\sigma(ax+b)=\alpha ay+\beta^2$

$+b+\beta a$ imply that $\alpha c+2\beta=a$ and $\alpha^2d+\beta^2=b+\beta a$. Then we have $c=\alpha'(a-2\beta)$ and $d=\alpha'^2(\beta a+b-\beta^2)$.

$b) \rightarrow a)$: Define a mapping σ : $(R, a, b)=R \oplus Rx \rightarrow (R, c, d)=R \oplus Ry$ by $\sigma(x)=\alpha^{-1}y+\beta$, then σ is an R -algebra isomorphism.

$b) \rightarrow c)$ is obvious. If 2 is invertible, setting $\beta=\frac{1}{2}(a-\alpha^{-1}c)$, we see that $c)$ implies $b)$.

The following lemma is well known.

Lemma 2. (R, a, b) is R -separable if and only if a^2+4b is invertible in R .

We shall define a product in $Q_f(R)$ by $[R, a, b] \cdot [R, c, d]=[R, ac, a^2d+bc^2+4bd]$. From the following Lemma 3, it is easily seen that $Q_f(R)$ is an abelian semigroup with unit element $[R, 1, 0]$.

Lemma 3. (Lemma 3 in [2]). *If $(R, a, b) \cong (R, a', b')$ and $(R, c, d) \cong (R, c', d')$ are isomorphisms as R -algebras, then so is $(R, ac, a^2d+bc^2+4bd) \cong (R, a'c', a'^2d'+b'c'^2+4b'd')$.*

A separable quadratic extension S of R has a unique automorphism $\sigma=\sigma(S)$ of S such that $S^\sigma=\{x \in S; \sigma(x)=x\}=R$. In [1], [4] and [5], the product $S_1 \star S_2$ of separable quadratic extension S_1 and S_2 of R was defined as the fixed subalgebra $(S_1 \otimes_R S_2)^{\sigma_1 \otimes \sigma_2}$, where $\sigma_i=\sigma(S_i)$.

Lemma 4 (Proposition 4 in [2]). *Let (R, a, b) and (R, c, d) be separable quadratic extensions of R . Then we have $[R, a, b] \cdot [R, c, d]=[R, a, b] \star [R, c, d]$.*

Theorem 1. *An element $[R, a, b]$ of $Q_f(R)$ is invertible if and only if $[R, a, b]$ is contained in $Q_{fs}(R)$. Therefore, $Q_{fs}(R)$ is the set of all invertible elements in $Q_f(R)$. It is an abelian group of exponent 2.*

Proof. Let $[R, a, b]$ be any element of $Q_{fs}(R)$. By Lemma 2, a^2+4b is invertible in R . Set $\alpha=(a^2+4b)^{-1}$ and $\beta=-2b$, then we have $\alpha(a^2-2\beta)=1$ and $\alpha^2(\beta a^2+(2a^2b+4b^2)-\beta^2)=0$, hence we have $(R, a^2, 2a^2b+4b^2) \cong (R, 1, 0)$ by Lemma 1. Since $[R, a, b]^2=[R, a^2, 2a^2b+4b^2]$, we have $[R, a, b]^2=[R, 1, 0]$, so $[R, a, b]$ is invertible in $Q_f(R)$. Conversely, we assume $[R, a, b] \cdot [R, c, d]=[R, 1, 0]$, then we have $1=\alpha^2\{(ac)^2+4(a^2d+bc^2+4bd)\}=\alpha^2(a^2+4b)(c^2+4d)$ for some invertible element α in R . Thus, a^2+4b is invertible in R , therefore, $[R, a, b]$ is contained in $Q_{fs}(R)$.

Theorem 2. *Let $\{R_\lambda; \lambda \in \Lambda\}$ be a family of commutative rings with unit elements, and $R=\prod_{\lambda \in \Lambda} R_\lambda$ a direct product of $\{R_\lambda; \lambda \in \Lambda\}$. Then we have isomorphisms $Q_f(R) \cong \prod_{\lambda \in \Lambda} Q_f(R_\lambda)$ and $Q_{fs}(R) \cong \prod_{\lambda \in \Lambda} Q_{fs}(R_\lambda)$ by correspondence $[R, \prod_{\lambda \in \Lambda} a_\lambda, \prod_{\lambda \in \Lambda} b_\lambda] \mapsto \prod_{\lambda \in \Lambda} [R_\lambda, a_\lambda, b_\lambda]$.*

Proof. Let $(R, \prod_{\lambda \in \Lambda} a_\lambda, \prod_{\lambda \in \Lambda} b_\lambda) \cong (R, \prod_{\lambda \in \Lambda} c_\lambda, \prod_{\lambda \in \Lambda} d_\lambda)$. Then, there exist $\alpha=\prod_{\lambda \in \Lambda} \alpha_\lambda$

and $\beta = \prod_{\lambda \in \Lambda} \beta_\lambda$ such that α is invertible in R , $\prod c_\lambda = \alpha(\prod a_\lambda - 2\beta)$ and $\prod d_\lambda = \alpha^2(\beta \prod a_\lambda + \prod b_\lambda - \beta^2)$. It is equivalent to existence of α_λ and β_λ in R_λ such that α_λ is invertible, $c_\lambda = \alpha_\lambda(a_\lambda - 2\beta_\lambda)$ and $d_\lambda = \alpha_\lambda^2(\beta_\lambda a_\lambda + b_\lambda - \beta_\lambda^2)$ for all $\lambda \in \Lambda$, namely, $\prod_{\lambda \in \Lambda} (R_\lambda, a_\lambda, b_\lambda) \cong \prod_{\lambda \in \Lambda} (R_\lambda, c_\lambda, d_\lambda)$. Thus f is injective. It is clear that f is an epimorphism. Therefore, we have an isomorphism $Q_f(R) \cong \prod_{\lambda \in \Lambda} Q_f(R_\lambda)$ as semigroups, so we have the isomorphism $Q_{fs}(R) \cong \prod_{\lambda \in \Lambda} Q_{fs}(R_\lambda)$ as groups by Theorem 1.

Let $U(R)$ be the unit group of a ring R , and $U^2(R)$ the set $\{u^2; u \in U(R)\}$. We define a relation \sim in R as follows; for a and b in R , $a \sim b$ if there exist c and d in $U^2(R)$ such that $ac = bd$. Then the relation \sim is an equivalence relation and we denote by $R/U^2(R)$ the quotient R/\sim . The multiplication in R induces a multiplication in $R/U^2(R)$, and $R/U^2(R)$ is an abelian semigroup with unit element $[1]$, where $[a]$ denotes the class of a in $R/U^2(R)$. It is clear that the set of all invertible elements in $R/U^2(R)$ is $U(R)/U^2(R)$. We define a mapping $D: Q_f(R) \rightarrow R/U^2(R)$ by $D([R, a, b]) = [a^2 + 4b]$, and this is a homomorphism, which carries $[R, 1, 0]$ and $[R, 0, 0]$ to $[1]$ and $[0]$, respectively. Indeed, by Lemma 1, D is well defined, and $D([R, a, b] \cdot [R, c, d]) = [(ac)^2 + 4(a^2d + bc^2 + 4bd)] = [a^2 + 4b][c^2 + 4d]$.

Theorem 3. *If 2 is invertible in R , then D is an isomorphism and this induces an isomorphism $Q_{fs}(R) \cong U(R)/U^2(R)$ as groups. (cf. Proposition 3.3 in [1])*

Proof. By Lemma 1, $[R, a, b] = [R, c, d]$ in $Q_f(R)$ if and only if $[a^2 + 4b] = [c^2 + 4d]$ in $R/U^2(R)$. Thus D is a monomorphism. For any element a in R , $D\left([R, 0, \frac{a}{4}]\right) = [a]$, therefore D is surjective. Thus D is an isomorphism. Furthermore, by Theorem 1, D induces an isomorphism $Q_{fs}(R) \cong U(R)/U^2(R)$ as groups.

In the case where 2 is not invertible in R , we give a sufficient condition such that D is a monomorphism;

Theorem 4. *If R is a unique factorization domain of characteristic $\neq 2$, or a ring such that $2R$ is a prime ideal and 2 is a non-zero-divisor, then D is a monomorphism.*

Proof. In the first place, we remark that if $a = a' + 2r$ then $(R, a, b) \cong (R, a', ra + b - r^2)$ and $a^2 + 4b = a'^2 + 4(ra + b - r^2)$. Let $D([R, a, b]) = D([R, c, d])$, that is, $a^2 + 4b = \alpha^2(c^2 + 4d)$ for some invertible element α in R . Since $(R, a, b) \cong (R, a/\alpha, b/\alpha^2)$, we may assume that $a^2 + 4b = c^2 + 4d$. If $a - c \in 2R$, we may put $a = c$, and so we have $b = d$. Thus, if $a - c \in 2R$, D is a monomorphism. Now, we remain only to show that $a^2 + 4b = c^2 + 4d$ implies $a - c \in 2R$. Let R be a unique factorization domain. If $b = d$, the implication is clear. Let $b \neq d$. Put

$2 = p_1^{e_1} \cdot p_2^{e_2} \cdots p_n^{e_n}$ the prime factorization of 2. For each i , $(1 \leq i \leq n)$, let f_i be an integer such that $a+c = p_i^{f_i} \cdot s_i$ and $p_i \nmid s_i$. Then from $4 \mid (a+c)(a-c)$, we have $p_i^{2e_i-f_i} \mid a-c$. If $f_i \leq e_i$, we have $p_i^{e_i} \mid a-c$ because of $2e_i-f_i \geq e_i$. On the other hand, if $f_i > e_i$, we have $p_i^{e_i} \mid a-c$ because of $a-c = p_i^{f_i} \cdot s_i - 2c$. Thus we have $p_i^{e_i} \mid a-c$ for every i , $(1 \leq i \leq n)$. Therefore, $a-c \in 2R$. Let R be a ring such that $2R$ is a prime ideal. Since $(a+c)(a-c) = 4(d-b)$ is in $2R$, if $a-c \notin 2R$ then $a+c = 2r$ for some r in R , and so $a-c = 2(r-c)$. It is a contradiction. Thus, $a-c \in 2R$.

Corollary 1. *Let \mathbf{Z} be the ring of rational integers. $Q(\mathbf{Z})$ is isomorphic to a multiplicative subsemigroup $\{n; n=4r \text{ or } n=4r+1, r \in \mathbf{Z}\}$ of \mathbf{Z} . Therefore, $Q_s(\mathbf{Z})$ is trivial. (cf. Proposition 4 in [3]).*

Corollary 2. *Let $R = \mathbf{Z}[i]$ be the ring of Gaussian integers. $Q(R) = Q_f(R)$ is isomorphic to the subsemigroup $\{[\alpha] \in R/\{1, -1\}; \alpha = 4b, 4b+1, 4b+2i \text{ for all } b \in R\}$ of $R/U^2(R) = \mathbf{Z}[i]/\{1, -1\}$. And $Q_s(R)$ is trivial.*

Proof. Since $R/2R = \{\bar{0}, \bar{1}, \bar{i}, \bar{1+i}\}$, we get $Q(R) = \{[R, 0, b], [R, 1, b], [R, i, b], [R, 1+i, b]; b \in R\}$. Therefore, we have $Q(R) \cong \text{Im } D = \{[\alpha] \in R/\{1, -1\}; \alpha = 4b, 4b+1, 4b+2i \text{ for all } b \text{ in } R\}$, hence $Q_s(R)$ is trivial..

REMARK 1. In Theorem 4, we can not omit the condition that 2 is a non-zero-divisor. For example, let $R = \mathbf{Z}/(4)$, then we have $Q(R) = \{[R, \bar{0}, \bar{0}], [R, \bar{0}, \bar{1}], [R, \bar{0}, \bar{2}], [R, \bar{0}, \bar{3}], [R, \bar{1}, \bar{0}], [R, \bar{1}, \bar{1}]\}$, $Q_s(R) = \{[R, \bar{1}, \bar{0}], [R, \bar{1}, \bar{1}]\}$, $D(Q(R)) = \{\bar{0}, \bar{1}\} \subset \mathbf{Z}/(4)$ and $D(Q_s(R)) = \{\bar{1}\} \subset \mathbf{Z}/(4)$. Then D is neither monomorphic nor epimorphic.

REMARK 2. In the case where R is not a unique factorization domain, we can not omit the condition in Theorem 4 that $2R$ is a prime ideal. For example, let $R = \mathbf{Z}[\sqrt{5}]$. Then we have $[R, \sqrt{5}, -1] \neq [R, 1, 0]$ but $D([R, \sqrt{5}, -1]) = D([D, 1, 0]) = [1]$. D is not a monomorphism.

Theorem 5. *Let $K = GF(p^n)$ be finite field, then $Q(K)$ is isomorphic to the multiplicative semigroup $\mathbf{Z}/(3)$. Further, the isomorphism induces an isomorphism $Q_s(K) \cong \{\bar{1}, -\bar{1}\} = U(\mathbf{Z}/(3))$.*

Proof. The case $p \neq 2$. In the first place, we note that $(R, a, b) \cong (R, 0, a^2 + 4b)$ and $U(K) = K^* = K - \{0\}$. From Theorem 3 and $(K^*: K^{*2}) = 2$, we have $Q(K) = \{[K, 0, 0], [K, 0, 1], [K, 0, \alpha]\}$, where α is an element K^* which is not contained in K^{*2} . By the correspondence $[K, 0, 0] \mapsto \bar{0}$, $[K, 0, 1] \mapsto \bar{1}$ and $[K, 0, \alpha] \mapsto -\bar{1}$, we have an isomorphism $Q(K) \cong \mathbf{Z}/(3)$ as multiplicative semigroups, and it induces $Q_s(K) \cong \{\bar{1}, -\bar{1}\} = U(\mathbf{Z}/(3))$ as groups.

The case $p = 2$. Since $a^2 + a = a(a+1)$ for a in K , we have $\#\{a^2 + a; a \in K\} = 2^{n-1} < \#(K)$, where $\#(K)$ denotes the number of elements in K . Then, there

exists α in K such that $\alpha \notin \{a^2 + a; a \in K\}$, and the quadratic equation $x^2 + x + \alpha = 0$ has no roots in K . Then, we can see the equalities $\#\{a^2 + a; a \in K\} = \#\{a^2 + a + \alpha; a \in K\} = 2^{r-1}$ and $\{a^2 + a; a \in K\} \cap \{a^2 + a + \alpha; a \in K\} = \emptyset$. For, if $c = a^2 + a$ and $c = b^2 + b + \alpha$ for some a, b in K , then $(a+b)^2 + (a+b) + \alpha = 0$. It is a contradiction. Therefore, we have $K = \{a^2 + a; a \in K\} \cup \{a^2 + a + \alpha; a \in K\}$, (disjoint sum), namely, any element a in K verifies either $\beta^2 + \beta + a = 0$ or $\beta^2 + \beta + a + \alpha = 0$ for some β in K . On the other hand, by Lemma 1, $(K, 1, 0) \cong (K, 1, a)$ if and only if there exists β in K such that $\beta^2 + \beta + a = 0$. And $(K, 1, \alpha) \cong (K, 1, a)$ if and only if there exists β in K such that $\beta^2 + \beta + a + \alpha = 0$. Accordingly, we have $Q_s(K) = \{[K, 1, 0], [K, 1, \alpha]\}$. Furthermore, since $U^2(K) = U(K)$, $(K, 0, 0) \cong (K, 0, a)$ for all a in K , hence $Q(K) = \{[K, 0, 0], [K, 1, 0], [K, 1, \alpha]\}$. By the correspondence $[K, 0, 0] \mapsto \bar{0}$, $[K, 1, 0] \mapsto \bar{1}$ and $[K, 1, \alpha] \mapsto -\bar{1}$ we have the isomorphism $Q(K) \cong \mathbf{Z}/(3)$, and it induces $Q_s(K) \cong \{\bar{1}, -\bar{1}\} = U(\mathbf{Z}/(3))$.

REMARK 3. Let \mathbf{Q} , \mathbf{R} and \mathbf{C} be the fields of rational numbers, real numbers and complex numbers, respectively. By the same argument as the proof of Theorem 5 (in case $p \neq 2$), we can see that $Q(\mathbf{R}) = \{[\mathbf{R}, 0, 0], [\mathbf{R}, 0, 1], [\mathbf{R}, 0, -1]\}$, $Q(\mathbf{C}) = \{[\mathbf{C}, 0, 0], [\mathbf{C}, 1, 0]\}$. Further, $Q_s(\mathbf{Q})$ is an infinite abelian group of exponent 2, $Q_s(\mathbf{R})$ is a group of order 2 and $Q_s(\mathbf{C})$ is trivial.

REMARK 4. In the case $R = \text{GF}(2^r)$, the homomorphism D is not a monomorphism but an epimorphism.

Theorem 6. Let $R = \mathbf{Z}/(n)$, and let $n = p_1^{e_1} \cdot p_2^{e_2} \cdots p_r^{e_r}$ be the prime factorization of n . Then $Q_{fs}(R)$ is the abelian group of type $(2, 2, \dots, 2)$, r -times.

Proof. It is enough to prove that $Q_s(\mathbf{Z}/(p^e))$ is the group of order 2 for any prime integer p . In the case $p \neq 2$, by Theorem 3, $Q_s(\mathbf{Z}/(p^e))$ is isomorphic to the group $U(\mathbf{Z}/(p^e))/U^2(\mathbf{Z}/(p^e))$. The index $(U(\mathbf{Z}/(p^e)) : U^2(\mathbf{Z}/(p^e)))$ is 2, since $U(\mathbf{Z}/(p^e))$ is a cyclic group of order $\varphi(p^e) = (p-1)p^{e-1}$. Thus, $Q_s(\mathbf{Z}/(p^e))$ is the group of order 2. In the case $p=2$, put $\mathbf{Z}/(2^e) = R$. We shall remark that $\{\bar{a}^2 - \bar{a}; \bar{a} \in R\} = 2R$. In fact, let $f: 2R \rightarrow \{\bar{a}^2 - \bar{a}; \bar{a} \in R\}$ be a mapping defined by $f(\bar{a}) = \bar{a}^2 - \bar{a}$. If $f(\bar{a}) = f(\bar{b})$, we have $(a-b)(a+b-1) \equiv 0 \pmod{2^e}$. Since $2 \nmid a+b-1$, we have $2^e \mid a-b$, hence $\bar{a} = \bar{b}$. Furthermore, $\{\bar{a}^2 - \bar{a}; \bar{a} \in R\}$ and $2R$ are finite sets and $\{\bar{a}^2 - \bar{a}; \bar{a} \in R\} \subseteq 2R$. Hence, $\{\bar{a}^2 - \bar{a}; \bar{a} \in R\} = 2R$. Now, we shall show that $(R, \bar{1}, \bar{a+2}) \cong (R, \bar{1}, \bar{a})$ for all integer a . $(R, \bar{1}, \bar{a+2}) \cong (R, \bar{1}, \bar{a})$ if and only if there exist an odd integer α and an integer β such that $1 \equiv \alpha(1-2\beta)$ and $a \equiv \alpha^2(\beta + a + 2 - \beta^2) \pmod{2^e}$, namely, there exists an integer β such that $(4a+1)\beta^2 - (4a+1)\beta - 2 \equiv 0 \pmod{2^e}$. Since $\{\bar{a}^2 - \bar{a}; \bar{a} \in R\} = 2R$, we can take an integer β such that $\bar{\beta}^2 - \bar{\beta} = 2(\bar{4a+1})^{-1}$, and we have $(4a+1)\beta^2 - (4a+1)\beta - 2 \equiv 0 \pmod{2^e}$. Hence, we have $(R, \bar{1}, \bar{a+2}) \cong (R, \bar{1}, \bar{a})$ for all integer a . Accordingly we have $(R, \bar{1}, \bar{2a}) \cong (R, \bar{1}, \bar{0})$ and $(R, \bar{1}, \bar{2a+1}) \cong (R, \bar{1}, \bar{1})$ for all integer a .

But $[R, \bar{1}, \bar{0}] \neq [R, \bar{1}, \bar{1}]$. Therefore, $Q_s(R)$ is the group of order 2.

REMARK 5. Let $R = \mathbf{Z}/(2^e)$. Then we have following;

- i) if $e=1$, $Q(R) = \{[R, \bar{0}, \bar{0}], [R, \bar{1}, \bar{0}], [R, \bar{1}, \bar{1}]\}$.
- ii) if $e \geq 2$, $Q(R) = \{[R, \bar{0}, \bar{a}_i]; i=1, 2, \dots, r\} \cup \{[R, \bar{1}, \bar{0}], [R, \bar{1}, \bar{1}]\}$, (disjoint sum), where $\{\bar{a}_1, \bar{a}_2, \dots, \bar{a}_r\}$ is the representatives of $R/U^2(R)$.

Proof. i) is a special case of Theorem 5.

ii) $(R, \bar{0}, \bar{a}) \cong (R, \bar{0}, \bar{b})$ if and only if there exist an odd integer α and an integer β such that $2\beta \equiv 0$ and $b \equiv \alpha^2(a - \beta^2) \pmod{2^e}$. Put $\beta \equiv 2^{e-1}n \pmod{2^e}$ and $2 \nmid n$, then we have $\beta^2 \equiv 0 \pmod{2^e}$. Therefore, $(R, \bar{0}, \bar{a}) \cong (R, \bar{0}, \bar{b})$ if and only if $\bar{b} = \bar{\alpha}^2 \bar{a}$ for some $\bar{\alpha}$ in $U(R)$, namely, $[\bar{a}] = [\bar{b}]$ in $R/U^2(R)$.

REMARK 6. There is a commutative ring R with the homomorphism $D: Q_f(R) \rightarrow R/U^2(R)$ which is not a monomorphism but the restriction $D|_{Q_{fs}(R)}$ is a monomorphism. For example, if $R = \mathbf{Z}/(2^e)$, ($e \geq 3$), then we have $D([R, \bar{1}, \bar{0}]) = [\bar{1}]$, $D([R, \bar{1}, \bar{1}]) = [\bar{5}]$ and $[\bar{1}] \neq [\bar{5}]$ in $U(R)/U^2(R)$. Thus, the restriction $D|_{Q_{fs}(R)}$ is a monomorphism. But, we have $[R, \bar{0}, \bar{0}] \neq [R, \bar{0}, \bar{2}^{e-2}]$ and $D([R, \bar{0}, \bar{0}]) = D([R, \bar{0}, \bar{2}^{e-2}]) = [\bar{0}]$, Then D is not a monomorphism.

OSAKA KYOIKU UNIVERSITY

References

- [1] H. Bass: *Lectures on Topics in Algebraic K-theory*, Tata Inst. Fund. Research, Bombay, 1967.
- [2] T. Kanzaki: *On the quadratic extensions and the extended Witt ring of a commutative ring*, Nagoya Math. J. **49** (1973), 127–141.
- [3] A. Micali et E. Villamayor: *Sur les algèbres de Clifford. II.*, J. Reine Angew. Math. **242** (1970), 61–90.
- [4] A. Micali et E. Villamayor: *Algèbres de Clifford et groupe de Brauer*, Ann. Sci. Ecole Norm. Sup. 4^e ser. **4** (1971), 285–310.
- [5] P. Revoy: *Sur les deux premiers invariants d'une forme quadratique*, Ann. Sci. Ecole Norm. Sup. 4^e ser. **4** (1971), 311–319.