Kanzaki, T.
Osaka J. Math.
8 (1971), 485-496

ON BILINEAR MODULE AND WITT RING OVER A COMMUTATIVE RING

Dedicated to Professor Keizo Asano on his 60th birthday

TERUO KANZAKI

(Received March 2, 1971)

Let R be any commutative ring, U and M arbitrary R-modules. We call that (M, B, U) is a bilinear R-module if $B: M\times M\to U$: $(x, y) \rightsquigarrow B(x, y)$ is a bilinear form, i.e. $B(x, -)$ and $B(-, y)$ are in $\mathrm{Hom}_R(M, U)$ for every x and y in M. Furthermore, we call that (M, q, U) is quadratic R-module if $q: M\to U$ is a quadratic form, i.e. $q(rx)=r^2q(x)$ for all $r\in R$, $x\in M$, and $B_q: M\times M\to U$ defined by $B_q(x, y)=q(x+y)-q(x)-q(y)$ for $x, y\in M$ is a bilinear form. In this paper, we study about automorphisms ρ of (M, B, U) which satisfy $B(\rho(x), \rho(y))=B(x, y)$ for all x, y in M, for some commutative ring R and some R-module U, and study about Witt ring $W(R)$ and $W(R)$-module $W(U)$ for a finitely generated projective rank one R-module U.

In §1, for non-degenerated symmetric bilinear R-module (M, B, U) we define a non-singular element and a symmetry which are generalizations of ordinary senses. Under some condition on U, we give some generalization of the classical theorem that the orthogonal group is generated by symmetries, if 2 is inversible in R and M is generated by orthogonal non-singular elements. In §2, analogously to [2], we can construct the theory of quadratic modules (M, q, U) and Witt group $W(U)$ for U in $Pic(R)$, where $Pic(R)$ is a category whose objects consist of finitly generated projective rank one R-modules and whose morphisms are R-isomorphisms. Then we shall show that $W(U)$ is a $W(R)$-module, and if there exists V in $Pic(R)$ such that $V\otimes_R V\approx U$ then $W(U)$ is a free $W(R)$-module with rank one. In §3, as supplementary result of [3], we study the structure of $W(R)$ over a complete Noetherian local ring with finite residue field of characteristic $\neq 2$. Throughout this paper, we assume that every ring is commutative ring with unit element and every module is unitary.

1. Automorphism of bilinear module

Let R be any commutative ring and U an arbitrary R-module. A bilinear R-module $M=(M, B, U)$ is called non-degenerated if the homomorphism $M\to$

$\mathrm{Hom}_R(M, U)$; $x \rightsquigarrow B(x, -)$ is R-isomorphism, where $B(x, -)$ is the R-homomorphism $M \to U$; $y \rightsquigarrow B(x, y)$. And, if $B(x, y)=B(y, x)$ for every x y in M, then we call it symmetric bilinear R-module.

Proposition 1.1. *Let $M=(M, B, U)$ be any bilinear R-module, and x an element in M. A cyclic sub-bilinear R-module $(Rx, B|Rx, U)$ is non-degenerated if and only if it satisfies that $(0\colon x)_R=(0\colon B(x, x))_R$ and $(0\colon (0\colon B(x, x))_R)_U=RB(x, x)$, where $(0\colon x)_R=\{r\in R\colon rx=0\}$ and $(0\colon \mathfrak{a})_U=\{y\in U\colon \mathfrak{a}y=0\}$ for x in M or U and ideal $\mathfrak{a}$ of R.*

Proof. Let $\theta\colon Rx \to \mathrm{Hom}_R(Rx, U)$ be the homomorphism defined by $rx \rightsquigarrow B(rx, -)|Rx$. We can show easily that θ is a monomorphism if and only if $(0\colon B(x, x))_R \subset (0\colon x)_R$, and θ is an epimorphism if and only if $(0\colon (0\colon x)_R)_U \subset RB(x, x)$.[1] Since, in general, $(0\colon B(x, x)_R)_R \supset (0\colon x)_R$ and $(0\colon (0\colon B(x, x)_R)_U \supset RB(x, x)$, therefore we have that θ is isomorphism if and only if $(0\colon B(x, x))_R=(0\colon x)_R$ and $(0\colon (0\colon B(x, x))_R)_U=RB(x, x)$.

Definition. Let $M=(M, B, U)$ be any bilinear R-module. An element x in M is called a non-singular element if it satisfies $B(x, M)=RB(x, x)$, where $B(x, M)=\{B(x, y)\colon y\in M\}$.

Remark 1.1. If $M=(M, B, U)$ is an arbitrary bilinear R-module, then an element x of M is non-singular if and only if $M=Rx+(Rx)^{\perp}$, where $(Rx)^{\perp}=\{y\in M\colon B(x, y)=0\}$. If (M, B, U) is non-degenerated, then non-singular element x satisfies $(0\colon x)_R=(0\colon (B(x, x))_R$. Furthermore, if (M, B, U) is non-degenerated symmetric bilinear R-module, then the following conditions are equivalent:

1) x is a non-singular element.
2) $M=Rx\oplus(Rx)^{\perp}$.
3) $(Rx, B|Rx, U)$ is non-degenerated.

Lemma 1.1. *Let (M, B, U) be a non-degenerated symmetric bilinear R-module. If x is a non-singular element, then it satisfies $(0\colon (0\colon B(x, M))_R)_U=B(x, M)$.*

Proof. It is easy from Proposition 1.1. and Remark 1.1.

Definition. Let $M=(M, B, U)$ be a non-degenerated symmetric bilinear R-module. For any non-singular element x in M, we can define an R-automorphism ρ_x of (M, B, U) as follows: For every element y in M, $\rho_x(y)=y-2r_y x$,

---

1) θ is monomorphism $\rightleftarrows$ $B(rx, Rx)=0$ implies $r\in(0\colon x)_R \rightleftarrows (0\colon B(x, x))_R\subset(0\colon x)_R$.

θ is epimoprhism $\rightleftarrows$ for any $f\in\mathrm{Hom}_R(Rx, U)$ $(\approx\mathrm{Hom}_R(R/(\theta\colon x)_R, U))$, there exists $rx\in Rx$ such that $f(sx)=B(rx, sx)$ for all $s\in R$ $\rightleftarrows$ for any $u\notin U(\approx\mathrm{Hom}_R(R. U))$ such that $(0\colon x)_R\, u=0$, there exists $r\in R$ such that $u=B(rx, x)=rB(x, x) \rightleftarrows (0\colon (0\colon x)_R)_U\subset RB(x, x)$.

where r_y is an element of R such that $B(x, y)=r_yB(x, x)$ in $B(x, M)=RB(x, x)$. It is well defined, because we have $(0: x)_R=(0: B(x, x))_R$ from Remark 1.1, therefore r_yx is determined by y. ρ_x is called symmetry. Then it is easy to see that

1) ρ_x is an R-automorphism of M such that $B(\rho_x(y), \rho_x(z))=B(y, z)$ for every y,z in M,

2) $\rho_x^2=I$, $\rho_x(x)=-x$ and $\rho_x|(Rx)^\perp=I$.

Lemma 1.2. *Let $M=(M, B, U)$ be a non-degenerated symmetric bilinear R-module, and suppose 2 is inversible in R. If x and y are non-singular elements such that $B(x, x)=B(y, y)$ and $B(x+y, x+y)=0$, then there exists a symmetry ρ such that $\rho(y)=x$.*

Proof. Since $B(x, x)=B(y, y)$ and $B(x+y, x+y)=0$, we have $0=B(x+y, x+y)=2(B(x, x)+B(x, y))$, that is, $B(x, x)=-B(x, y)$. On the other hand, $B(x-y, x-y)=2(B(x, x)-B(x, y))=4B(x, x)$, and $B(y, M)=RB(y, y)=RB(x, x)=B(x, M)$, hence $B(x-y, M)\subset B(x, M)+B(y, M)=B(x, M)=RB(x, x)=RB(x-y, x-y)$. Therefore, $x-y$ is a non-singular element, and we can define a symmetry $\rho=\rho_{x-y}$, which satisfies $\rho_{x-y}(y)=y-2r_y(x-y)=y-2\left(\frac{-1}{2}\right)(x-y)=x$, where $r_yB(x-y, x-y)=B(x-y, y)=B(x, y)-B(y, y)=-\frac{1}{2}B(x-y, x-y)$.

Now, we assume the following condition:

(*) *For every non zero element u in U, there exists an idempotent e in R such that $Ru\supset eU\neq 0$.*

Lemma 1.3. *Let $M=(M, B, U)$ be a non-degenerated symmetric bilinear R-module satisfying the condition (*), and suppose 2 is inversible in R. Then there exists a non zero non-singular element.*

Proof. Since (M, B, U) is non-degenerated, there exists an element $x\neq 0$ such that $B(x, x)\neq 0$. By the condition (*) there exists an idempotent e in R such that $RB(x, x)\supset eU\neq 0$. Put $x'=ex$, then we have $RB(x', x')=B(x', M)=eU$, therefore x' is a non zero non-singular element in M.

We suppose the following stronger condition in the next proposition:

(**) *For every non zero element u in U, there exists an idempotent e in R such that $Ru=eU$.*

Lemma 1.4. *Let $M=(M, B, U)$ be a non-degenerated symmetric bilinear R-module, and suppose 2 is inversible in R. If x and y are non-singular elements of M such that $B(x, x)=B(y, y)$ and $RB(x+y, x+y)=eU\neq 0$ for some idempotent e in R, then there exists an automorphism π of (M, B, U) such that $\pi(y)=x$ and π is a product of symmetries.*

Proof. By the assumption, there exists an idempotent $e\neq 0$ in R such that R

$B(x+y, x+y)=eU\neq 0$. We put $x'=ex$, $y'=ey$, and $x''=(1-e)x$, $y''=(1-e)y$. Then $x'\neq 0$ and $y'\neq 0$ are non-singular elements, and $RB(x'+y', x'+y')=eU\neq 0$. If $x''\neq 0$ (so that $y''\neq 0$), then x'' and y'' are also non-singular elements and $B(x''+y'', x''+y'')=(1-e)B(x+y, x+y)=0$. By Lemma 1.2, $x''-y''$ is anon-singular element and the symmetry $\rho_{x''-y''}$ satisfies $\rho_{x''-y''}(y'')=x''$. Since y' is in $(R(x''-y''))^{\perp}$, we have $\rho_{x''-y''}(y')=y'$. On the other hand, $R\,B(x'+y', x'+y')=eU=B(x'+y', M)$, therefore $x'+y'$ is non-singular and $\rho_{x'+y'}(y')=y'-2r'_{y'}(x'+y')=y'-(x'+y')=-x'$. Therefore $\rho_{x'}\circ\rho_{x'+y'}(y')=x'$. Since x'' is in $(Rx)^{\perp}$ and in $(R(x'+y'))^{\perp}$, $\rho_{x'}\circ\rho_{x'+y'}(x'')=x''$. Therefore $\rho_{x'}\circ\rho_{x'+y'}\circ\rho_{x''-y''}(y)=\rho_{x'}\circ\rho_{x'+y'}\circ\rho_{x''-y''}(y)'+\rho_{x'}\circ\rho_{x'+y'}\circ\rho_{x''-y''}(y'')=\rho_{x'}\circ\rho_{x'+y'}(y')+\rho_{x'}\circ\rho_{x'+y'}(x'')=x'+x''=x$. Accordingly, $\pi=\rho_{x'}\circ\rho_{x'+y'}\circ\rho_{x''-y''}$ is the automrphism demanded in this lemma.

Proposition 1.2. *Let $M=(M, B, U)$ be a non-degenerated symmetric bilinear R-module satisfying the condition (**), and suppose 2 is inversible in R. If x and y are non-singular elements in M such that $B(x, x)=B(y, y)$, then there exists an automorphism π of (M, B, U) such that $\pi(y)=x$ and π is a product of symmetries. Furthermore, if M is generated by a finite number of orthogonal elements, i.e. $M=\sum_{i=1}^{m}Rx_i$, $B(x_i, x_j)=0$ for $i\neq j$, then the group of all automorphism of (M, B, U), (it is denoted by $O(M, B, U)=\{\pi\in Aut_R(M)$: $B(\pi(x)\pi, (y))=B(x, y)$ for all $x, y\in M\}$), is generated by symmetries of (M, B, U).*

Proof. The first part is obtained by Lemma 1.2 and Lemma 1.4. We suppose that $M=\sum_{i=1}^{m}Rx_i$, $B(x_i, x_j)=0$ for $i\neq j$, and hence, $x_1, \cdots x_n$ are non-singular elements. Let π be any element in $O(M, B, U)$. Using the first part of this proposition for x_1 and $\pi(x_1)$, we have an automorphism π_1 of (M, B, U) such that $\pi_1\circ\pi(x_1)=x_1$ and π_1 is a product of symmetries. Repeating for x_2 and $\pi_1\circ\pi(x_2)$, we have π_2 such that $\pi_2\circ\pi_1\circ\pi(x_2)=x_2$ and π_2 is a product of symmetries. Furthermore, since $0=B(x_1, x_2)=B(\pi_1\circ\pi(x_1), \pi_1\circ\pi(x_2))=B(x_1, \pi_1\circ\pi(x_2))$, form the construction of π_2 we have $\pi_2(x_1)=x_1$, therefore $\pi_2\circ\pi_1\circ\pi(x_1)=x_1$, Thus, repeating these, we obtain automorphisms $\pi_1, \pi_2, \cdots, \pi_n$ of (M, B, U) such that $\pi_n\circ\pi_{n-1}\circ\cdots\pi_1\circ\pi(x_i)=x_i$ for $i=1, 2, \cdots, n$, and $\pi_1, \cdots, \pi_n$ are products of symmetries, Therefore $\pi=\pi_1^{-1}\circ\pi_1^{-1}\circ\cdots\circ\pi_n^{-1}$ is a product of symmetries of (M, B, U).

We consider the specisl case that R is a commutative Von Neumann regular ring, i.e. every principal ideal is generated by an idempotent, and $U=R$. Then form Proposition 1.2 we have easily

Theorem 1.1. *Let R be a commutative Von Neumann regular ring, and $(M, B)=(M, B, R)$ a non-degenerated symmetric bilinear R-module, and suppose 2 is inversible in R. If x and y are non-singular elements in (M, B, R) such that $B(x, x)=B(y, y)$, then there exists an automorphism π of (M, B, U) such that $\pi(y)=x$, and π is a product of symmetries. Furthermore, if M is generated by a* *finite number of orthogonal elements, then the group $O(M, B)$ is generated by symmetries.*

Proposition 1.3. *Let (M, B, U) be a non-degenerated symmetric bilinear R-module satisfying the condition $(*)$, and suppose 2 is inversible. If (M, B, U) has maximum (or minimum) condition for non-degenerated sub-bilinear R-modules, then M is generated by a finite number of orthogonal non-singular elements and $O(M, B, U)$ is generated by symmetries.*

To prove the proposition we are necessary the following lemma:

Lemma 1.5. *Let (M, B, U) be a non-degenerated bilinear R-module. If N is an R-submodule of M such that N is a direct summand of M, then $N^{\perp}=\{y \in M: B(y, N)=0\}$ is also direct summand of M. If $(N, B|N, U)$ is non-degenerated sub-bilinear R-module, then $M=N \oplus N^{\perp}$, and $(N^{\perp}, B|N^{\perp}, U)$ is also non-degenerated.*

Proof. The proof is obtained similarly to the proofs of Lemma (2.1) and Lemma (2.2) in [1].

Proof of Proposition 1.3. By Lemma 1.3, there exists a non zero non-singular element x_1, and by Renark 1.1 $(Rx_1, B|Rx_1, U)$ is non-degenerate. Therefore, by Lemma 1.5 we have $M=Rx_1 \oplus (Rx_1)^{\perp}$ and $((Rx_1)^{\perp}, B|(Rx_1)^{\perp}, U)$ is also non-degenerated, and inductively we have orthogonal non-singular elements $x_1, x_2, \cdots$, but by the maximum (or minimum) condition for non-degenerated sub-bilinear R-modules we have a finite number of orthogonal non-singular elements $x_1, x_2, \cdots, x_n$ such that $M=Rx_1+Rx_2+\cdots+Rx_n$. Thus, we have the proof of the first part. We shall show the second part. Let π be any element of $O(M, B, U)$. By Lemma 1.3, there is a non-singular element x_1, then $M=Rx_1 \oplus (Rx_1)^{\perp}$, and Rx_1 and $(Rx_1)^{\perp}$ are non-degenerate. If $B(x_1+\pi(x_1), x_1+\pi(x_1))=0$, then by Lemma 1.2 there exists symmetry π_1 such that $\pi_1(\pi(x_1))=x_1$, therefore $\pi_1 \circ \pi((Rx_1)^{\perp})=(Rx_1)^{\perp}$ and $\pi_1 \circ \pi | Rx_1=I$. If $B(x_1+\pi(x_1), x_1+\pi(x_1)) \neq 0$, then by the condition $(*)$ there exists an idempotent e in R such that $RB(x_1+\pi(x_1), x_1+\pi(x_1)) \supset eU \neq 0$. We put $x_1'=ex_1$, then we have $R B(x_1'+\pi(x_1'), x_1'+\pi(x_1'))=eU \neq 0$, and x_1' is also non zero non-singular element in M. Therefore, $M=Rx_1' \oplus (Rx_1')^{\perp}$ and by Lemma 1.4 there exists an automorphism π_1 of (M, B, U) such that $\pi_1(\pi(x_1'))=x_1'$ and π_1 is a product of symmetries. Accordingly, for non-degenerated sub-module $((Rx_1')^{\perp}, B|(Rx_1')^{\perp}, U)$ we have $\pi_1 \circ \pi((Rx_1')^{\perp})=(Rx_1')^{\perp}$, and $\pi_1 \circ \pi | Rx_1'=I$. Since (M, B, U) has maximum (or mnimum) condition for non-degenerated sub-bilinear R-modules, we have a finite number of automorphisms $\pi_1, \pi_2, \cdots, \pi_m$ of (M, B, U) such that $\pi_m \circ \pi_{m-1} \circ \cdots \circ \pi_1 \circ \pi=I$, that is, $\pi=\pi_1^{-1} \circ, \cdots \circ \pi_m^{-1}$, and π_i is a product of symmetries for every i. We copmlete the proof.

2. Witt group and Witt ring

Let R be any commutative ring, and U an arbirtary R-module. Then we can construct the Witt group $W(U)$ which is a module over the Witt ring $W(R)$. In this section, we shall study about $W(R)$-module $W(U)$. For an R-module M, (M, q, U) is called quadratic R-module, if q: $M\rightarrow U$ is a map satisfying the following conditions:

1) $q(rx)=r^2q(x)$ for every $r\in R$ and $x\in M$, and
2) B_q: $M\times M\rightarrow U$; $B_q(x, y)=q(x+y)-q(x)-q(y)$, $x, y\in M$, is a bilinear form.

It is called that (M, q, U) is non-degenerated if (M, B_q, U) is non-degenerated.

Lemma 2.1. *If (P, q, U) is non-degenerated quadratic R-module such that P is a finitely generated projective faithful R-module, then U is a finitely generated projective rank one R-module.*

Proof. Since (P, q, U) is non-degenerated and P is finitely generated projective, we have $P\approx\mathrm{Hom}_R(P, U)\approx\mathrm{Hom}_R(P, R)\otimes_R U$ as R-module. Furthermore, since P is finitely generated projective and faithful, by Propostion 6.1. in p. 37, [2], so is also U. Since $\mathrm{rank}(P)=\mathrm{rank}(\mathrm{Hom}_R(P, R))$, we have $\mathrm{rank}(U)=1$.

From now, we consider all non-degenerated quadratic R-module (P, q, U) such that P is finitely generated projective R-module. By Lemma 2.1. we may assume that U is finitely generated projective rank one R-module. We denote by $Pic(U)$ a category whcih object is finitely generaged projective rank one R-moduee and morphism is R-isomprphism.

We shall give analogous definitions and lemmas to [2] for quadratic R-module (M, q, U) with U in $Pic(R)$.[2)]

(2.1) Definition, $H(M, U)=(M\oplus\mathrm{Hom}_R(M, U), q_h, U)$ is called hyperbolic quadratic R-module, if q_h: $M\oplus\mathrm{Hom}_R(M, U)\rightarrow U$ is defined by $q_h(x+f)=f(x)$ for $x\in M$ and $f\in\mathrm{Hom}_R(M, U)$.

If U is in $Pic(R)$, then the following lemmas are proved similarly to ones in [2].

(2.2) $H(M, U)$ is non-degenerated if and only if M is U-reflexive, i.e. Ψ: $M\rightarrow\mathrm{Hom}_R(\mathrm{Hom}_R(M, U), U)$ defined by $\Psi(x)(f)=f(x)$ for $f\in\mathrm{Hom}_R(M, U)$, $x\in M$, is isomorphism.

(2.3) Let (M, q, U) be a quadratic R-module. If M is a projective R-module, then there exists a bilinear form B: $M\times M\rightarrow U$ such that $B(x, x)=q(x)$ for every x in M.

(2.4) If (M, q, U) is a non-degenerated quadratic R-module, then M is U-refl-

2) A part of these definitions and lemmas is due to Prof. A. Micali, I studied from his seminar at Universidad de Rosario. I should like to express here my thanks to him.

exive, and so is also direct summand of M. If P is a finitely generated projective R-module, then P is U-reflexive for every U in $Pic(R)$.

(2.5) Definition. For quadratic R-modules (M, q, U) and (M', q, U'), (f, g): $(M, q, U) \to (M', q', U')$ is called homomorphism of quadratic R-module (M, q, U) to (M', q', U'), if f: $M \to M'$ and g: $U \to U'$ are R-homomorphism such that the following diagram is commutative;

$$\begin{array}{ccc} M\times M & \xrightarrow{f\times f} & M'\times M' \\ \downarrow q & & \downarrow q' \\ U & \xrightarrow{g} & U' \end{array}$$

If f is an isomomorphism and $g=I$, $(U=U')$, then (f, I): $(M, q, U) \to (M', q', U)$ is called *isomorphism*, and denote it by $(M, q, U) \approx (M', q', U)$.

(2.6) Let (M, q, U) be a non-degenerated quadratic R-module, and M_0 a total isotropic R-submodule, i.e. $q(M_0)=0$, such that M_0 is a direct summand of M. Put $\Delta = \{N$: R-submodule such that $M=N \oplus M_0^{\perp}\}$, then we have that the map $N \to \mathrm{Hom}_R(M_0, U)$; $x \rightsquigarrow B_q(x, -)|M_0$ is an R-isomorphism for every N in Δ. If M is a projective R-module, then there exists a total isotropic R-submodule N_0, i.e. $q(N_0)=0$, in Δ, and we have $(M_0 \oplus N_0,\ q|M_0 \oplus N_0,\ U) \approx H(M_0, U)$. Therefore, if (M, q, U) is a non-degenerated quadratic R-module such that M is projective R-module and there exists a total isotropic R-submodule M_0 such that $M_0^{\perp}=M$ and M_0 is a direct summand of M, then (M, q, U) is hyperbolic and $(M, q, U) \approx H(M_0, U)$.

(2.7) If (P, q, U) is a non-degenerated quadratic R-module such that P is projective R-module, then we have $(P, q, U) \perp (P, -q, U) \approx H(P, U)$, where $(P, q, U) \perp (P', q', U) = (P \oplus P', (q \perp q'), U)$ and $(q \perp q')(x \oplus y) = q(x) + q'(y)$ for $x \oplus y \in P \oplus P'$.

(2.8) Definition. Let U and U' be in $Pic(R)$, and (P, q, U) and (P', q', U') any quadratic R-modules. We can define the product $(P, q, U) \otimes (P', q', U') = (P \otimes_R P', q \otimes q', U \otimes_R U')$ as follows;

$$\begin{aligned} &q\otimes q'\colon P\otimes_R P' \to U\otimes_R U';\ q\otimes q'(\textstyle\sum_{i=1}^n x_i\otimes x_i') = 2\sum_{i=1}^n q(x_i)\otimes q'(x_i') \\ &\qquad + \textstyle\sum_{i>j} B_{q\otimes q'}(x_i\otimes x_i',\ x_j\otimes x_j') \qquad \text{for } \sum_{i=1}^n x_i\otimes x_i' \text{ in } P\otimes P', \text{ where} \\ &B_{q\otimes q'} = B_q\otimes B_{q'};\ (P\otimes_R P)\times(P'\otimes_R P') \to U\otimes_R U'. \end{aligned}$$

(2.9) Let U and U' be in $Pic(R)$. If (P, q, U) and (P', q', U') are non-degenerated quadratic R-module such that P and P' are finitely generated projective R-modules, then $(P, q, U) \otimes (P', q', U')$ is also non-degenerated quadratic R-module. Furthermore, if P'' is a finitely generated projective R-module and U'' in $Pic(R)$, then we have $(P, q, U) \otimes H(P'', U'') \approx H(P \otimes_R P'', U \otimes_R U'')$.

Now, we suppose that the following natural isomorphisms in $Pic(R)$ regard as identies I: $U\otimes_R U'\to U'\otimes_R U$; $x\otimes y \rightsquigarrow y\otimes x$, $(U\otimes_R U')\otimes_R U''\to U\otimes_R(U'\otimes_R U'')$; $(x\otimes y)\otimes z \rightsquigarrow x\otimes(y\otimes z)$, $U\otimes_R R\to U$; $x\otimes r\rightsquigarrow xr$, $R\otimes_R R\to R$; $r\otimes s\rightsquigarrow rs$, $U\otimes_R U^*\to R$; $x\otimes f\rightsquigarrow f(x)$, $\cdots$ etc., where $U^*=\mathrm{Hom}_R(U,R)$. Then, for each U in $Pic(R)$ we can construct an abelian group $W(U)$ as follows: Let $Qua(U)$ be the set of all isomorphic classes of non-degenerated quadratic R-modules (P, q, U) such that P is finitely generated projective R-module. $Qua(U)$ makes an abelian semigroup with peration $\perp$ such that, $[(P, q, U)]\perp[(P', q', U')]=[(P, q, U)\perp(P', q', U')]$, where [ ] denotes an isomorphic class. Let $\mathrm{H}(U)=\{[H(P, U)]$ in $Qua(U)$: P is finitely generated projective R-module$\}$. Then $\mathrm{H}(U)$ is a sub semi-group of $Qua(U)$, and $Qua(U)$ has an equivalence relation $\sim$ defined by $\alpha\sim\beta\Leftrightarrow\exists\gamma$, $\delta\in\mathrm{H}(U)$, $\gamma\perp\alpha=\delta\perp\beta$. We denote the quotient $Qua(U)/\sim$ by $W(U)$, then $W(U)$ is also abelian semi-group with operation $+$induced by $\perp$. But, by (2.7), $W(U)$ makes an additive group. $W(U)$ is called Witt group over U. On the other hand, the product $\otimes$ of quadratic R-modules induces a product, that is, for U, U' in $Pic(R)$, $Qua(U)\times Qua(U')\to Qua(U\otimes_R U')$; $([P, q, U)], [(P', q', U')])\to[(P, q, U)\otimes(P', q', U')]$ induces a product $W(U)\times W(U')\to W(U\otimes_R U')$ by (2.9). We denote this product by$\cdot$, then for $\alpha\in W(U)$, $\beta\in W(U')$ and $\gamma\in W(U'')$, we have $\alpha\cdot\beta\in W(U\otimes_R U')$ and $(\alpha\cdot\beta)\cdot\gamma=\alpha\cdot(\beta\cdot\gamma)$ in $W(U\otimes_R U'\otimes_R U'')$.

Therefore, we have that $W(R)$ is a commutative ring, it is called Witt ring, and we have easily

Lemma 2.1. *Let U and U' be in $Pic(R)$. Then, $W(U)$ is $W(R)$-module, $W(U)\cdot W(U')\subset W(U\otimes_R U')$, and $W(U)\cdot W(U^*)$ is an ideal of $W(R)$, where $U^*=Hom_R(U, R)$. If f: $U\to U'$ is isomorphism in $Pic(R)$, then f induces an $W(R)$-isomorphism $W(f)$: $W(U)\to W(U')$ defined by $[(P, q, U)]\to[(P, f\circ q, U')]$.*

From now, we assume that the commutative ring R has inverse element of 2. Then $W(R)$ has unit element $[(R, q_I, R)]$ defined by $q_I(x)=\frac{1}{2}x^2$ for every x in R, and $W(U)$ is unitary $W(R)$-module for every U in $Pic(R)$.

Lemma 2.2. *Let U and V be in $Pic(R)$ such that $V\otimes_R V\approx U$ in $Pic(R)$. Then, any R-isomorphism Φ: $V\otimes_R V\to U$ satisfies $\Phi(x\otimes y)=\Phi(y\otimes x)$ for every x, y in V.*

Proof. We can easily check that homomorphism h: $V\otimes_R V\to U$ is well defined by $h(x\otimes y)=\Phi(x\otimes y)-\Phi(y\otimes x)$ for $x\otimes y$ in $V\otimes_R V$. For any maximal ideal $\mathfrak{p}$ of R, we consider localization by $\mathfrak{p}$ $h_{\mathfrak{p}}$: $(V\otimes_R V)_{\mathfrak{p}}\to U_{\mathfrak{p}}$. But, $(V\otimes_R V)_{\mathfrak{p}}=V_{\mathfrak{p}}\otimes_{R_{\mathfrak{p}}}V_{\mathfrak{p}}=R_{\mathfrak{p}}v\otimes_{R_{\mathfrak{p}}}R_{\mathfrak{p}}v$ for some $v\in V_{\mathfrak{p}}$, therefore $h_{\mathfrak{p}}(x\otimes y)=h_{\mathfrak{p}}(rv\otimes r'v)=\Phi_{\mathfrak{p}}(rv\otimes r'v)-\Phi_{\mathfrak{p}}(r'v\otimes r)=0$ for every $x=rv$, $y=r'v$ in $V_{\mathfrak{p}}=R_{\mathfrak{p}}v$. Accordingly, since $h_{\mathfrak{p}}=0$ for every maximal ideal $\mathfrak{p}$ of R, we have $h=0$.

Theorem 2.1. *If U is in $Pic(R)$ such that there exists V in $Pic(R)$ and*

$V\otimes_R V\approx U$ in Pic(R), then Witt group $W(U)$ is a free $W(R)$-module with rank one.

Proof. Let Φ: $V\otimes_R V\to U$ be an R-isomorphism, and (V, q, U) a quadratic R-module defined by $q(x)=\frac{1}{2}\Phi(x\otimes x)$ for x in V. By Lemma 2.1, $B_q(x, y)=q(x+y)-q(x)-q(y)=\frac{1}{2}(\Phi(x\otimes y)+\Phi(y\otimes x))=\Phi(x\otimes y)$. We shall show that (V, q, U) is non-degenerated. Let θ: $V\to\mathrm{Hom}_R(V, U)$ be a homomorphism defined by $\theta(x)=B_q(x, -)=\Phi(x\otimes -)$. Then, we have the following commutative diagram;

$$\begin{array}{ccc} V^*\otimes_R V\otimes_R V & \xrightarrow{I\otimes\Phi} & V^*\otimes_R U \\ \downarrow{\scriptstyle \mu\otimes I} & & \downarrow{\scriptstyle \nu} \\ R\otimes_R V=V & \xrightarrow{\theta} & \mathrm{Hom}_R(V, U)\,, \end{array}$$

where μ: $V^*\otimes_R V\underset{\approx}{\to} R; f\otimes x\to f(x)$, and ν: $V^*\otimes_R U\underset{\approx}{\to}\mathrm{Hom}_R(V, U); \nu(f\otimes y)(x)=f(x)y$ for $x\in V$, $y\in U$ and $f\in V^*$. Because, since V is a finitely generated projective rank one R-module, there exist $f_1, f_2, \cdots f_n$ in $V^*=\mathrm{Hom}_R(V, R)$ and $x_1, x_2, \cdots x_n$ in V such that $x=\sum_{i=1}^n f_i(x)x_i$ for all x in V, and by [4] we have $\sum_{i=1}^n f_i(x_i)=\mathrm{rank}(V)=1$. Therefore, for any x in V, in we have $\nu\circ(I\otimes\Phi)\circ(\mu^{-1}\otimes I)(x)=\nu\circ(I\otimes\Phi)\circ(\mu^{-1}\otimes I)(\sum_{i=1}^n f_i(x_i)\otimes x)=\nu\circ(I\otimes\Phi)(\sum_{i=1}^n f_i\otimes x_i\otimes x)=\nu(\sum_{i=1}^n f_i\otimes\Phi(x_i\otimes x))$. But for any y in V, $\nu(\sum_{i=1}^n f_i\otimes\Phi(x_i\otimes x)(y)=\sum_{i=1}^n f_i(y)\Phi(x_i\otimes x)=\Phi(\sum_{i=1}^n f_i(y)x_i\otimes x)=\Phi(y\otimes x)$, therefore we have $\nu\circ(I\otimes\Phi)\circ(\mu^{-1}\otimes I)=\theta$. Since, ν, $I\otimes\Phi$, and $\mu\otimes I$ are R-isomorphisms, therefore θ is an isomorphism, that is, (V, q, U) is non-degenerated. Siminarly, we have a non-degenerated quadratic R-module (V^*, q^*, U^*) defined by $q^*(z)=\frac{1}{2}\Phi^{-1*}(z\otimes z)$ for $z\in V^*=\mathrm{Hom}_R(V, R)$, where Φ^{-1*}: $V^*\otimes_R V^*\to U^*$ is dual of Φ^{-1}: $U\to V\otimes_R V$, i.e. $\Phi^{-1*}(f\otimes g)=f\otimes g\circ\Phi^{-1}$ for $f\otimes g\in V^*\otimes_R V^*$. Then we have $(V, q, U)\otimes(V^*, q^*, U^*)\approx(R, q_I, R)$, by the identification $U\otimes_R U^*=R$; $x\otimes f=f(x)$, that is, for $(V, q, U)\otimes(V^*, q^*, U^*)=(V\otimes_R V^*, q\otimes q^*, U\otimes_R U^*)$, we have commutative diagram

$$\begin{array}{ccc} V\otimes_R V^* & \xrightarrow{q\otimes q^*} & U\otimes_R U^* \\ \downarrow\wr & & \| \\ R & \xrightarrow{q_I} & R\,. \end{array}$$

Because, $q\otimes q^*(\sum_i y_i\otimes g_i)=2\sum_i q(y_i)\otimes q^*(g_i)+\sum_{i<j}B_q(y_i, y_j)\otimes B_q^*(g_i, g_j)=2\sum_i\frac{1}{2}\Phi(y_i\otimes y_i)\otimes\frac{1}{2}\Phi^{-1*}(g_i\otimes g_i)+\sum_{i<j}\Phi(y_i\otimes y_j)\otimes\Phi^{-1*}(g_i\otimes g_j)=\sum_i\frac{1}{2}\Phi^{-1*}(g_i\otimes g_i)(\Phi(y_i\otimes y_i))+\sum_{i<j}\Phi^{-1*}(g_i\otimes g_j)(\Phi(y_i\otimes y_j))=\sum_i\frac{1}{2}(g_i(y_i))^2+\sum_{i<j}g_i(y_i)g_j(y_i)=\frac{1}{2}(\sum_i g_i(y_i))^2=q_I(\sum_i g_i(y_i))$ for $\sum_i y_i\otimes g_i$ in $V\otimes V^*$. Therefore we have $[[V^*, q^*, U^*]]\cdot[[V, q, U]]=[[V, q, U]]\cdot[[V^*, q^*, U^*]]$

$=[[R, q_I, R]]=I$ in $W(R)$. Accordingly, $W(U)\cdot W(U^*)=W(R)$ and $W(U)\cdot[[V^*, q^*, U^*]]=W(R)$, therefore $W(U)=W(R)\cdot[[V, q, U]]$ is rank one free $W(R)$-module. We have the proof of Theorem.

We leave here the following question: Is $W(U)$ always a finitely generated projective rank one $W(R)$-module or 0 for every U in $Pic(R)$?

3. Some example of Witt ring

In [3], we studied the structure of Witt rings in the special case over local rings. In this section, we give some supplementary result of [3]. In this section, we suppose that R is commutative ring such that 2 is inversible in R. We denote by $U(R)$ the group of all inversible elements in R, and $U(R)^{(2)}=\{r^2: r\in U(R)\}$. Put $\overline{U(R)}=U(R)/U(R)^{(2)}$. We consider the group ring $Z[\overline{U(R)}]$ of the group $\overline{U(R)}$ over the integers Z. We denote by $H(R)$ the principal ideal of $Z[\overline{U(R)}]$ generated by $\overline{-1}+\bar{1}$ in $Z[\overline{U(R)}]$, where $\bar{a}$ denotes a coset of $U(R)/U(R)^{(2)}$ containing a for $a\in U(R)$. We put $A(R)=Z[\overline{U(R)}]/H(R)$. If R is local ring, the ring $A(R)$ has the following properties (see [3]):

(3.1) There exists a ring epimorphism Θ: $A(R)\rightarrow W(R)$.

(3.2) If -1 is a square element in R, then $A(R)$ is $Z/(2)$-algebra and is local ring with maximal ideal $\mathfrak{m}$ such that $x^2=0$ for every x in $\mathfrak{m}$ and $A(R)/\mathfrak{m}\approx Z/(2)$ as $Z/(2)$-algebra.

(3.3) If -1 is not square element in R, then $A(R)\approx Z[H]$, where H is a sub group of $\overline{U(R)}$ such that $\overline{U(R)}=H\times(\overline{-1})$.

(3.4) If $\overline{U(R)}$ has only two elements, i.e. $\overline{U(R)}=\{\bar{1}, \bar{a}\}$, then we have that

a) if -1 is a square element in R, then Θ: $A(R)\rightarrow W(R)$ is ring isomorphism, and $W(R)\approx A(R)\approx Z/(2)[(\bar{a})]=Z/(2)\cdot\bar{1}+Z/(2)\cdot\bar{a}$, therefore $\bar{1}$ is unit element of $A(R)$ and the maximal ideal is $\mathfrak{m}=\{0, \bar{1}+\bar{a}\}$,

b) if -1 is not square element in R, then $A(R)\approx Z$ and $\ker\Theta\subset 4Z$.

Now, we consider a case where R is complete Noetherian local ring with finite residue field. Let R be a Noetherian local ring with maximal ideal $\mathfrak{p}$ such that $2\notin\mathfrak{p}$ and $R/\mathfrak{p}$ is a finite field.

Lemma 3.1. *Let R be as above. Then the group $\overline{U(R/\mathfrak{p}^n)}=U(R/\mathfrak{p}^n)/U(R/\mathfrak{p}^n)^{(2)}$ has only two elements for every $n=1, 2, \cdots$.*

Proof. We consider the group epimorphism f: $U(R/\mathfrak{p}^n)\rightarrow U(R/\mathfrak{p}^n)^{(2)}$; $\bar{x}\rightarrow\bar{x}^2$. Then we have $\ker f=\{-\bar{1}, \bar{1}\}$. Because, for any $\bar{a}\in\ker f$, $a^2\equiv 1 \pmod{\mathfrak{p}^n}$, hence $a\equiv 1 \pmod{\mathfrak{p}}$ or $a\equiv -1 \pmod{\mathfrak{p}}$, i.e. $a=p_1+1$ or $a=p_2-1$ for some p_i in $\mathfrak{p}$, $i=1, 2$. Therefore $a^2=(p_i\pm 1)^2=p_i^2\pm 2p_i+1\equiv 1 \pmod{\mathfrak{p}^n}$, hence $p_i(p_i\pm 2)\equiv 0 \pmod{\mathfrak{p}^n}$. Since $2\notin\mathfrak{p}$, $p_i\pm 2$ is unit in R, hence $p_i\in\mathfrak{p}^n$, that is, $a=p_i\pm 1\equiv\pm 1 \pmod{\mathfrak{p}^n}$. Since R is Noetherian and $R/\mathfrak{p}$ is finite field, therefore $R/\mathfrak{p}^n$ is

Artinian, and so $R/\mathfrak{p}^n$ is finite ring for every integer $n>0$. Thus, $U(R/\mathfrak{p}^n)$ is finite group and $[U(R/\mathfrak{p}^n): U(R/\mathfrak{p}^n)^{(2)}]=2$.

Proposition 3.1. *Let R be a Noetherian local ring with maximal ideal $\mathfrak{p}$ such that $2\notin\mathfrak{p}$ and $R/\mathfrak{p}$ is a finite field. Then, the completion $\hat{R}$ of R by $\mathfrak{p}$-topology has the following properties;*

1) *$\overline{U(\hat{R})}=U(\hat{R})/U(\hat{R})^{(2)}$ has only two elements, and*
2) *-1 is a square element in $\hat{R}$ if and only if $-\bar{1}$ is a square element in $R/\mathfrak{p}$.*

Proof. Let $f_{n,m}$ be the canonical epimorphism $R/\mathfrak{p}^n \to R/\mathfrak{p}^m$ for $n>m$. Since $\hat{R}=\varprojlim_n R/\mathfrak{p}^n=\{(\bar{a}_1, \bar{a}_2, \cdots, \bar{a}_n, \cdots)\in\Pi_{n=1}^{\infty}R/\mathfrak{p}^n: f_{n,m}(\bar{a}_n)=\bar{a}_m$ for every $n>m\}$, therefore $U(\hat{R})=\varprojlim_n U(R/\mathfrak{p}^n)$, and the product in $U(\hat{R})$ is $\alpha\cdot\beta=(\overline{a_1b_1}, \overline{a_2b_2}, \cdots)$ for $\alpha=(\bar{a}_1, \bar{a}_2, \cdots)$ and $\beta=(\bar{b}_1, \bar{b}_2, \cdots)$ in $U(\hat{R})$. We have that $\alpha=(\bar{a}_1, \bar{a}_2,\cdots)$ is a square element in $U(\hat{R})$ if and only if $\bar{a}_n$ is a square element in $U(R/\mathfrak{p}^n)$ for every $n=1, 2, \cdots$. If $\bar{a}_n$ is square in $U(R/\mathfrak{p}^n)$, then $\bar{a}_i=f_{n,i}(\bar{a}_n)$ is also square in $U(R/\mathfrak{p}^i)$ for every $0<i\leqq n$. Therefore $\alpha=(\bar{a}_1, \bar{a}_2, \cdots)$ is not a square element in $U(\hat{R})$ if and only if there exists a positive integer n such that $\bar{a}_k$ is not a square element in $U(R/\mathfrak{p}^k)$ for every $k\geq n$. If $\alpha=(\bar{a}_1, \bar{a}_2, \cdots)$ and $\beta=(\bar{b}_1, \bar{b}_2, \cdots)$ are not square elements in $U(R)$, then there exists a positive integer m such that $\bar{a}_i$ and $\bar{b}_i$ are not square element in $U(R/\mathfrak{p}^i)$ for every $i\geq m$. But, by Lemma 3.1, $\bar{a}_i\bar{b}_i=\overline{a_ib_i}$ is a square elements in $U(R/\mathfrak{p}^i)$ for every $i\geq m$. Therefore $\alpha\cdot\beta$ must be a square element in $U(\hat{R})$. Accordingly, we have that $\overline{U(\hat{R})}=U(\hat{R})/U(\hat{R})^{(2)}$ has only two elements. Furthermore, if $\alpha=(\bar{a}_1, \bar{a}_2,\cdots)$ is not square element in $U(\hat{R})$, then there exists the minimum positive integer k such that $\bar{a}_i$ is not square element in $U(R/\mathfrak{p}^i)$ for every $i\geqq k$. Let $\beta=(\bar{b}_1, \bar{b}_2, \cdots)$ be not square element in $U(\hat{R})$ such that $\bar{b}_i$ is not square element in $U(R/\mathfrak{p}^i)$ for every $i\geqslant 1$.[3] Then $\alpha\cdot\beta=(\bar{a}_1\bar{b}_1, \bar{a}_2\bar{b}_2, \cdots)$ is a square element in $U(\hat{R})$, therefore $\bar{a}_i\bar{b}_i$ is square element in $U(R/\mathfrak{p}^i)$ for every $i\geq 1$, hence by Lemma 3.1 we have $k=1$. Accordingly, $\alpha=(\bar{a}_1, \bar{a}_2,\cdots)$ is not square element in $U(R)$ if and only if $\bar{a}_1$ is not square element in $U(R/\mathfrak{p})$. Thus, we complete the proof.

From (3.1), $\cdots$, (3.4) and Proposition 3.1, we have easily

Theorem 3.1. *Let R be a Noetherian complete local ring with maximal ideal $\mathfrak{p}$ such that $2\notin\mathfrak{p}$ and $R/\mathfrak{p}$ is a finite field. Then we have that*

1) *if $\overline{-1}$ is a square element in $R/\mathfrak{p}$, then the Witt ring $W(R)$ is a group ring of a cyclic group of order 2 over $Z/(2)$.*

---

3) There exit ts such element β in $U(\hat{R})$. Let b be an element of R such that $\bar{b}$ is not square element in $R/\mathfrak{p}$, and f_i: $R\to R/\mathfrak{p}^i$ the canonical epimorphism $f_i(x)=\bar{x}\in R/\mathfrak{p}^i$ for $x\in R$, $i=1, 2, \cdots$. Put $\bar{b}_i=f_i(b)$. Then $\beta=(\bar{b}_1, \bar{b}_2, \cdots)$ is in $U(\hat{R})$, and $\bar{b}_i$ is not square in $U(R/\mathfrak{p}^i)$ for every $i\geqq 1$.

2) *if* -1 *is not square element in* $R/\mathfrak{p}$, *then the Witt ring* $W(R)$ *is isomorphic to* $Z/(n)$, *where* n *is a multiple of* 4.

UNIVERSIDAD DE ROSARIO AND OSAKA CITY UNIVERSITY

References

[1] H. Bass: *Modules which support nonsingular form*, J. Algebra **13** (1969), 246–262.
[2] ———: Lecture on Topics in Algebraic K-theory, Tata Institute of Fundamental Research, Bombay, 1967.
[3] S. Bruno et T. Kanzaki: *Sur l'anneau de Witt d'un anneau local*, C. R. Acad. Sci. Paris Sér A **272** (1971), 1691–1694.
[4] A. Hattori: *Rank element of a projective module*, Nagoya Math. J. **25** (1965), 113–120.