韓國數學敎育學會誌<數學敎育>
1984. 6. Vol. XXII, No. 3.

Journal of the Korea Society of Mathematical Education
Jun. 1984. Vol. XXII, No. 3.

A Note on Witt Ring over Local Ring

by Myung Jae Kim
Kyong Gi College, Soowon, Korea

In this note, the theorem 1 and 2 will be shown by quite elementary techniques which are immediate generalization of the ones in "field case" to the ones in "local ring case". Throughout this note, we shall asume that A is a local ring with maximal ideal $\mathfrak{M}$, and $2\in A^*=A-\mathfrak{M}$. Let A be a ring and M be an A-module. A quadratic form on M is a map $q: M\rightarrow A$ such that

(i) $q(ax)=a^2q(x)$, $a\in A$, $X\in M$,

(ii) $B_q(x,y)=\frac{1}{2}(q(x+y)-q(x)-q(y))$ is an A-bilinear map from $M\times M$ into A.

B_q in (ii) is called the associated bilinear form of q. For all $x\in M$, $B_q(x,x)=q(x)$. A *quadratic A-module* is a pair (M,q), where M is a unitary *A-module*, and q is a quadratic form on M. A *quadratic A-space* is a quadratic A-module (V,B), where V is a free A-module of finite rank, and $B: V\times V\rightarrow A$ is a symmetric bilinear form on V. Let x be an element of a space (V,B). We define the norm of x to be $n(x)=B(x,x)$. Let $M(A)$ be the set of isometric classes of non-singular quadratic A-spaces. (A is local ring and $2\in A^*$.) $M(A)$, together with operations induced by the orthogonal sum $\perp$ and the tensor product $\otimes$, becomes a commutative semi-ring with identity $\langle 1\rangle$. Let $\hat{W}(A)$ be the set of all formal expressions $E-G$ with E,G in $M(A)$. Two expressions $E-G$, $E'-G'$ are defined to be equal if and only if $E\perp G'\cong E'\perp G$. We define addition and multiplication in $\hat{W}(A)$ as follows:

$$(E_1-G_1)+(E_2-G_2)=(E_1\perp E_2)-(G_1\perp G_2),$$
$$(E_1-G_1)\cdot(E_2-G_2)=((E_1\otimes E_2)\perp(G_1\otimes G_2)-((E_1\otimes G_2)\perp(G_1\otimes E_2)).$$

Then $\hat{W}(A)$ becomes a commutative ring. We call $\hat{W}(A)$ the *Witt-Grothendieck ring of A*. Let H be the free cyclic additive subgroup spanned by $\langle 1\rangle\perp\langle -1\rangle$ in $\hat{W}(A)$. Then H is an ideal in $\hat{W}(A)$, so that $W(A)=\hat{W}(A)/ZH$ is a commutative ring with identity element. $W(A)$ is called the *Witt-ring* over A.

Definition 1. Two orthogonal bases L and L' of a quadratic space are *connectable*, if there are orthogonal bases $L_1,\dots,L_r$ such that $L_1=L$, $L_r=L'$ and L_i and L_{i+1} differ at most in two elements for $i=1,\dots,r-1$.

Definition 2. A local ring A with maximal ideal $\mathfrak{M}$ and identity element 1 is called *quadratically Henselian* if every quadratic monic polynomial $X^2+aX+b\in A[X]$, which splits into coprime linear factors mod $\mathfrak{M}$, has always roots in A.

Theorem 1. *Two orthogonal bases of a quadratic space over A are connectable if A is quadratically Henselian local ring with* $2\in A^*$.

proof. Let $L=\{x_1, ..., x_n\}$ and $L'=\{y_1, ..., y_n\}$ be two orthogonal bases of a space V. We show that L is connectable to a basis containing y_1. Then the theorem follows immediately by induction on n. Renumbering the y_i if necessary we assume $y_1=r_1x_1+...+r_sx_s$ with $s\leq n$ and r_i in A^* for $i=1, ..., s$. Since clearly L and $\{r_1x_1, ..., r_sx_s, ..., x_n\}$ are connectable, we may assume $r_i=1$ for $i=1, ..., s$. We now proceed by induction on s. If $s=1$, we are done. Let $s\geq 2$. We have $n(y_1)=n(x_1)+...+n(x_n)\neq 0$. If we had $n(x_i)+n(x_j)=0$ for all $i\neq j$, $i, j\leq s$, this would imply $2n(x_i)=0$ for $i=1, ..., s$, hence $n(x_i)=0$ for $i=1, ..., s$, since $2\in A^*$. But this is impossible. Thus $n(x_i)+n(x_j)\neq 0$ for some i, j, and we may assume $n(x_1)+n(x_2)\neq 0$. Let $x'_1=x_1+x_2$ and choose x'_2 such that $Ax_1\perp Ax_2\cong Ax'_1\perp Ax'_2$. Thus $\{x'_1, x'_2, x_3, ..., x_n\}$ is connectable to L, and $y_1=x_1'+x_3+...+x_s$ is a shorter presention of y_1. (q.e.d.)

Let A be a commutative quadratically Henselian local ring such that $2\in A^*$. Then the Witt ring $W(A)$ is generated by (a) where $a\in A^*$, and satisfy the following obvious properties;

(i) $(ab^2)=(a)$,

(ii) $(a)+(b)=(a+b)+(ab(a+b))$, if $a+b\in A^*$

(iii) $(a)+(-a)=0$,

(iv) $(a)(b)=(ab)$.

Theorem 2. *Let A be a commutative quadratically Henselian local ring and let k be its residue class field with characteristic not 2. Then $W(A)$ is ring-isomorphic to $W(k)$.*

proof. Denote by $\bar{a}$ the canonical image of $a\in A^*$ in $k=A/\mathfrak{M}$. Let (a) be the similarity class of $\langle\bar{a}\rangle$ (quadratic space over k) in $W(k)$. Above relations (i), (ii), (iii), and (iv) are easily verified for $(a), (b), ..., (a, b, ...\in A^*)$. Thus, there exists a surjective ring-homorphism $\varphi: W(A)\rightarrow W(k)$. To show the injectivity of φ, we must prove that, for $a_1, ..., a_m\in A^*$,

$$\langle\bar{a}_1, ..., \bar{a}_m\rangle\cong\langle\bar{l}, -\bar{l}\rangle\perp...\perp\langle\bar{l}, -\bar{l}\rangle \text{ over } k$$

implies

$$\langle a_1, ..., a_m\rangle\cong\langle l, -l\rangle\perp...\perp\langle l, -l\rangle \text{ over } A.$$

It is sufficient to remark that, for $a, c\in A^*$, $b\in A$, $ax^2+by^2=c$ is solvable in A if, and only if, $\bar{a}\bar{x}^2+\bar{b}\bar{y}^2=\bar{c}$ is solvable in k, since A is quadratically Henselian.

References

1. Knebusch, M. and Kolster, M., *Wittrings*, Vieweg, 1982.
2. Lam, T.Y., *The Algebraic Theory of Quadratic Forms*, W.A. Benjamin, 1973.
3. O'Meara, O.T., *Introduction to Quadratic Forms*, Springer, Berlin-Göttingen-Heidelberg, 1963.