Journal of the Mathematical Society of Japan Vol. 12, No. 2, April, 1960

On Witt ring of quadratic forms.

By Yoshio NAKAMURA

(Received Dec. 23, 1958)
(Revised June 22, 1959)

§ 1. **Introduction.** Witt has proved that the classes of 'ähnlich' forms over a field k, which has characteristic not 2, form a ring (Witt [**2**]). This ring will be called *Witt ring* over k, in this paper. We shall consider the structure of Witt ring. Our results will be shown in theorem 1 for a finite field, in theorem 2 for a complete field with respect to a discrete non-Archimedean valuation, whose residue class field is finite and of characteristic not equal to 2, where Witt ring over that field is related to Witt ring over the residue class field, and in theorem 3 for an algebraic number field of finite degree over the rational number field.

I am quite indebted to Mr. A. Hattori, who has given kind help throughout.

§ 2. **Preliminaries.** In the first place, Eichler's formulation of *Witt group* in terms of metric spaces will be shown as follows (Eichler [**1**]):

Let k be a fixed commutative field of characteristic not 2, then a vector space R over k is made into a metric space by defining the *(inner) product* $\xi\eta$ of two vectors ξ, η, such that $\xi\eta$ is in k and

1. $\xi\eta=\eta\xi$,
2. $(\xi+\eta)\zeta=\xi\zeta+\eta\zeta$,
3. $(x\xi)\eta=x(\xi\eta)$, $x\in k$.

We consider only finite dimensional metric spaces over k. If $\{\iota_1, \cdots, \iota_n\}$ is a basis of R over k (in this case we write $R=k(\iota_1, \cdots, \iota_n)$), the square ξ^2 of $\xi=\sum_{i=1}^{n} x_i\iota_i$, $x_i\in k$, is a quadratic form

$$f=\sum_{i,j=1}^{n} f_{ij}x_ix_j, \qquad (f_{ij}=f_{ji}\in k)$$

in x_i, where $f_{ij}=\iota_i\iota_j$. f is called a *fundamental form* of R, and we denote this by $f\cdots R$. Conversely, every quadratic form f over k is a fundamental form of some space R.

Spaces R are always assumed to be *semi-simple*, namely for every vector $\xi\neq 0$ in R there is a vector η such that $\xi\eta\neq 0$, in other words, if $f\cdots R$, the determinant $|f_{ij}|$ of the matrix (f_{ij}) of coefficients of f is not zero.

Let $f\cdots R$ and $g\cdots S$, then, if R and S are isomorphic spaces over k, f and g are called *equivalent*.

Vectors ξ and η are called *orthogonal* to each other, if $\xi\eta=0$, and spaces R and S are orthogonal to each other, if vectors of R are orthogonal to those of S. If there is a vector $\xi\neq 0$ in a space R such that $\xi^2=0$, then ξ and R are called *isotropic*.

A semi-simple metric space R over k can be decomposed into an *orthogonal sum*

$$R=R_0\oplus N_1\oplus N_2\oplus\cdots$$

of subspaces $R_0, N_1, N_2, \cdots$, namely a direct sum of subspaces which are mutually orthogonal, where R_0 is non-isotropic or the zero space and all the N_i are isomorphic to the space $N=k(\iota_1, \iota_2)$ for which $\iota_1{}^2=\iota_2{}^2=0, \iota_1\iota_2=1$. R_0 is uniquely determined by R up to an isomorphism and is called the *kernel* of R. A form $f(x_1, x_2, \cdots, x_n)$ over k is called *definite*, if $f=0$ or if $f(x_1, \cdots, x_n)=0$ has a unique solution $x_1=x_2=\cdots=x_n=0$ in k. Then a fundamental form of a kernel is definite.

Those spaces over k which have isomorphic kernels are grouped into a class, which is called a *type* over k. A type $\mathfrak{R}$, which has a representative space R, will be denoted by $\mathfrak{R}=\text{Type } R$. For two quadratic forms f and f' such that $f\cdots R$ and $f'\cdots R'$, we denote $f\sim f'$ if both forms are of the same type (or 'ähnlich'), i.e. Type $R=$ Type R'.

The types over k form an abelian group, when we define the sum of two types $\mathfrak{R}$ and $\mathfrak{S}$ as Type$(R\oplus S)$, where $R\in\mathfrak{R}$ and $S\in\mathfrak{S}$. This abelian group is known generally as *Witt group* over k.

We define the product $\mathfrak{R}\mathfrak{S}$ of types $\mathfrak{R}$ and $\mathfrak{S}$ as Type$(R\otimes S)$, where $R\in\mathfrak{R}, S\in\mathfrak{S}$ and $R\otimes S$ is the Kronecker product of two vector spaces R and S over k with the metric such that for any r, r' in R and for any s, s' in S

$$(r\otimes s)(r'\otimes s')=rr'\cdot ss'.$$

Now, the set of the types over k forms a commutative ring, which we shall call *Witt ring* over k.

§3. Witt rings over complete fields with respect to discrete valuations. Let now k be a complete field with respect to a discrete non-Archimedean valutation $|\ |$, whose residue class field $\bar{k}$ is finite and has characteristic not 2. We denote by π a fixed prime element in k with respect to the valuation. Further, we denote by W and $\overline{W}$ Witt rings over k and $\bar{k}$, respectively.

THEOREM 1. *If -1 is a square in $\bar{k}$, then $\overline{W}$ is the two-dimensional algebra over $Z/2Z$ with basiselements $\mathfrak{E}, \mathfrak{U}$ $(\mathfrak{E}^2=\mathfrak{U}^2=\mathfrak{E}, \mathfrak{E}\mathfrak{U}=\mathfrak{U})$, and if -1 is not a square in $\bar{k}$, then $\overline{W}\cong Z/4Z$, where $\mathfrak{E}$ and $\mathfrak{U}$ are types over $\bar{k}$ of forms x^2 and*

εx^2, *ε being a fixed non-square in $\bar{k}$, respectively.*

PROOF. If -1 is a square in $\bar{k}$, then forms

$$0,\ x^2,\ \varepsilon x^2,\ x^2+\varepsilon y^2$$

constitute a complete set of representatives of the equivalence classes of definite forms in $\bar{k}$. So we can see easily the first half of the assertion of the theorem. Further, if -1 is not a square in $\bar{k}$, then we can take the following four forms as a complete set of non-equivalent definite forms:

$$0,\ x^2,\ -x^2,\ x^2+y^2.$$

In fact, any form with more than two variables over a finite field is indefinite. So $x_1^2+\cdots+x_4^2$ is equivalent to a form $x_1^2-x_2^2+f(x_3,x_4)$, and comparing the determinants of the both forms, $f(x_3,x_4)$ can be written as $f(x_3,x_4)=x_3^2-x_4^2$. Hence

$$x_1^2+x_2^2+x_3^2+x_4^2\sim 0,$$

$$x_1^2+x_2^2\sim -x_1^2-x_2^2.$$

We can also see easily the isomorphism of $\overline{W}$ to $Z/4Z$.

LEMMA. *The equivalence classes of the definite forms of the form*

$$(1)\qquad a_1x_1^2+\cdots+a_rx_r^2,$$

where $a_1,\cdots,a_r$ are units of k, together with 0, form a subring V of W isomorphic to $\overline{W}$.

PROOF. We know that if a unit in k is a square then it is also a square modulo the prime ideal (π) and conversely, and that the multiplicative group of units in k is divided into two cosets modulo squares.

Let f be a definite form (1) and $\bar{f}$ be the form f with the coefficients considered modulo (π), then $\bar{f}$ is a definite form over $\bar{k}$.

Now we correspond to f the form $\bar{f}$, then the isomorphism between V and $\overline{W}$ will be naturally induced.

THEOREM 2. *W is isomorphic to the algebra of dimension 2 over the ring $\overline{W}$ with basis elements $\mathfrak{E}$, $\mathfrak{P}$, where $\mathfrak{E}^2=\mathfrak{P}^2=\mathfrak{E}$, $\mathfrak{E}\mathfrak{P}=\mathfrak{P}$.*

PROOF. Every definite form f over k is equivalent to a form such as

$$a_1x_1^2+\cdots+a_rx_r^2+\pi(a_{r+1}x_{r+1}^2+\cdots+a_nx_n^2),$$

where $a_1,\cdots,a_n$ are units in k, and $f_1=a_1x_1^2+\cdots+a_rx_r^2$, $f_2=a_{r+1}x_{r+1}^2+\cdots+a_nx_n^2$ are definite. So we can write the type $\mathfrak{R}$ defined by f as follows:

$$\mathfrak{R}=\mathfrak{R}_1+\mathfrak{P}\mathfrak{R}_2,$$

where $\mathfrak{R}_1$, $\mathfrak{R}_2$ and $\mathfrak{P}$ are types of f_1, f_2 and πx^2, respectively. This representation of $\mathfrak{R}$ is unique, for if $\mathfrak{R}_1+\mathfrak{P}\mathfrak{R}_2=0$, then

$$a_1x_1^2+\cdots+a_rx_r^2\sim -\pi(a_{r+1}x_{r+1}^2+\cdots+a_nx_n^2),$$

so by the above lemma only possible case would be that

$$(2) \qquad a_1x_1^2 + a_2x_2^2 \sim -\pi(a_3x_3^2 + a_4x_4^2)$$

for two definite forms $a_1x_1^2+a_2x_2^2$ and $a_3x_3^2+a_4x_4^2$. But $|a_1x_1^2+a_2x_2^2|$ and $|a_3x_3^2+a_4x_4^2|$ are even powers of $|\pi|$ for any $x_1, \cdots, x_4$ in k. Hence both forms of (2) are never equivalent, which is a contradiction.

Thus W is decomposed, as an additive group, into the direct sum

$$W = V + \mathfrak{P} \cdot V,$$

and the subring V is isomorphic to $\overline{W}$ by the lemma, so this implies the assertion of our theorem.

REMARK. In this proof, if f_1 and f_2 are considered modulo (π), then they are equivalent to the *residue class forms* of f, which are defined implicitly by T. A. Springer (Springer [3]).

§ 4. **Witt rings over algebraic number fields.** In this section, we denote by k an algebraic number field of finite degree over the rational number field. If $\mathfrak{p}$ is a place of k, finite or infinite, then we denote by $k_\mathfrak{p}$ the $\mathfrak{p}$-adic extension of k, and for a type $\mathfrak{R} = \text{Type}(R)$ over k, where $R = k(\iota_1, \cdots, \iota_k)$, we put $R_\mathfrak{p} = k_\mathfrak{p}(\iota_1, \cdots, \iota_n)$ and $\mathfrak{R}_\mathfrak{p} = \text{Type}(R_\mathfrak{p})$, a type over $k_\mathfrak{p}$.

Let G be the ring of rational integers, G_r' be the direct sum $G + \cdots + G$ of r copies of G, and G_r be the subring of G_r', consisting of the elements $(g_1, \cdots, g_r)$ of G_r' such that $g_i \equiv g_j \bmod 2$ for every i, j, specifically $G_1 = G$. For $r = 0$, we put $G_0 = Z/2Z$.

Every type $\mathfrak{R}$ over the field of real numbers is represented by such a form

$$f_r = x_1^2 + \cdots + x_r^2 \quad \text{or} \quad f_{-s} = -x_1^2 - \cdots - x_s^2 .$$

(The zero type is represented by $f_0 = 0$.) r or $-s$ is called the *signature* of the type $\mathfrak{R}$, and denoted by $\sigma(\mathfrak{R}) = r$ or $= -s$. Witt ring over the field of real numbers is isomorphic to the ring of rational integers, if we correspond to a type $\mathfrak{R}$ its signature $\sigma(\mathfrak{R})$.

THEOREM 3. *Let the infinite real places of k be ∞_i $(i = 1, \cdots, r)$, and R be the radical of Witt ring W over k, then, if $r = 0$, R is composed of the types of even-dimensional spaces, and if $r > 0$,*

$$R = \{\mathfrak{R}\,;\ \sigma(\mathfrak{R}_{\infty_i}) = 0, \quad \textit{for } i = 1, \cdots, r\} ,$$

and

$$W/R \cong G_r .$$

PROOF. First, let $r > 0$. If $\sigma(\mathfrak{R}_{\infty_i}) = 0$ for each i, then $\mathfrak{R}$ is of even dimension, and at every finite place $\mathfrak{p}$ of k, $\mathfrak{R}_\mathfrak{p}^3 = 0$ from the fact that in $k_\mathfrak{p}$ a four-dimensional type is determined uniquely (Eichler [1] Satz 7.3). Thus $(\mathfrak{R}^3)_\mathfrak{p} = \mathfrak{R}_\mathfrak{p}^3 = 0$ for every finite or infinite place $\mathfrak{p}$. A type over k, which is zero over every $\mathfrak{p}$-adic extension $k_{\mathfrak{p}}$ of k, is the zero type (Hasse's theorem (Witt [2], Satz 20)). Hence $\mathfrak{R}^3=0$. If $\sigma(\mathfrak{R}_{\infty_i})\neq 0$ for some i, then $\mathfrak{R}^n\neq 0$ for every $n\neq 0$. Therefore the types $\mathfrak{R}$ with $\sigma(\mathfrak{R}_{\infty_i})=0$ $(i=1,\cdots,r)$ form the radical of W.

By the theory of algebraic numbers there is always a number in k whose $\pm$ signs in k_{∞_i} coincide with any given system of signs for each ∞_i. Accordingly, for an element $(g_1,\cdots,g_r)$ of G_r we can build a (diagonal) form f which defines a space S with $\sigma(S_{\infty_i})=g_i$ for every i. Finally, let's put $g_i=\sigma(\mathfrak{R}_{\infty_i})$, $(i=1,\cdots,r)$ for $\mathfrak{R}\in W$, then by the map

$$\mathfrak{R}\rightarrow(g_1,\cdots,g_r)\in G_r\,,$$

the isomorphism between W/R and G_r is easily verified.

Now the assertion for the case of $r=0$ is almost trivial by the beginning part of this proof.

REMARK. If k is an algebraic function field of one variable over a finite field, then $W/R\cong G_0=Z/2Z$, since k has no archimedean places.

References

[1] M. Eichler, Quadratische Formen und orthogonale Gruppen, Berlin, 1952.

[2] E. Witt, Theorie der quadratischen Formen in beliebigen Körpern, C. J., **176** (1937), 31-44.

[3] T. A. Springer, Quadratic forms over fields with a discrete valuation I, Proc. Acad. Amsterdam, **58** (1955), 352-362.