Chapter II
Introduction to Witt Rings

Satya Mandal

University of Kansas, Lawrence KS 66045 USA

May 11 2013

1 Definition of $\widehat{W}(F)$ and $W(F)$

From now on, by a quadratic form, we mean a **nonsingular** quadratic form (see page 27). As always, F will denote a field with $char(F) \neq 2$. We will form two groups out of all isomorphism classes of quadratic forms over F, where the orthogonal sum will be the addition. We need to define a Monoid. In fact, a monoid is like an abelian group, where elements need not have an inverse.

Definition 1.1. A **monoid** is a set M with a binary operation $+$ satisfying the following properties: $\forall\ x, y, x \in M$, we have

1. (Associativity) $(x + y) + z = x + (y + z)$.
2. (Commutativity) $x + y = y + x$
3. (Identity) M has an additive identity (zero) $0 \in M$ such that $0+x = x$.

We define the Grothendieck group of a monoid.

Theorem 1.2. Suppose M is a monoid. Then there is an abelian group G with the following properties:

1. There is a homomorphism $i : M \longrightarrow G$ the binary structurs,
2. G is generated by the image M.
3. G has the following universal property: suppose $\mathcal{G}$ be any abelian group and $\varphi : M \longrightarrow \mathcal{G}$ is a homomorphism of binary structures. Then there is a unique homomorphim $\psi : G \longrightarrow \mathcal{G}$ such that the diagram

$$\begin{tikzcd} M \arrow[r, "i"] \arrow[dr] & G \arrow[d, dashed, "\exists ! \psi"] \\ & \mathcal{G} \end{tikzcd} \qquad \textit{commutes.}$$

Proof. (*The proof is like that of localization. Lam gives a proof when M is cancellative.*) We define an equivalence realtion $\sim$ on $M \times M$ as follows: for $x, y, x', y' \in M$ define

$$(x,y) \sim (x',y') \quad if \quad x + y' + z = x' + y + z \qquad \text{for some} \quad z \in M.$$

(*Think of* $(x,y) = x - y$.) We will denote the equivalence class of (x,y) by $\overline{(x,y)}$. We let G be the set of the equivalence classes. Define "addition" by $\overline{(x,y)} + \overline{(u,v)} := \overline{(x+u, y+v)}$. Then, G is a group. $\overline{(0,0)}$ acts as the zero of G and $-\overline{(x,y)} = \overline{(y,x)}$.

Define $i : M \longrightarrow G$ by $i(x) = \overline{(x,0)}$. It is a homomorphism of binary-structures. It follows it is injective and G is generated by M.

For the universal property, define $\psi(x,y) = \varphi(x) - \varphi(y)$. ∎

Definition. This groups is called the Grothendieck group of M. It is sometimes denoted by $Groth(M)$.

Examples.

1. Let $V(F)$ be the isomorphims classes of finite dimensional vector spaces. Then, $V(F)$ is a (cancellative) monoid, under the operation $\oplus$, direct sum. It follows easily (check or ask me to check) that $Groth(V(F)) \approx \mathbb{Z}$.

2. Let A be a commutative ring. Let $\mathcal{P}(A)$ be the set of all isomorphism classes of finitely generated projective $A-$modules. $\mathcal{P}(A)$ is a monoid under the operation $\oplus$, direct sum. (*Note* $\mathcal{P}(A)$ *not cancellative*). We denote

$$K_0(A) := Groth(\mathcal{P}(A)) \quad \textit{called the Grothendieck group}$$

of projective modules. (*Note, this approach to define Grothendiek Group* $G_0(A)$ *of finitely generated* $A-$*modules does not work.*)

3. Our interest in this course is the monoid $M = M(F)$ of all the isometry classes of quadratic forms. It is a (cancellative) monoid, under the orthogonal sum $\perp$.

Definition 1.3. Let $M = M(F)$ denote the monoid of all nonsingular isometry classes of quadratic spaces over F. Define Grothendieck-Witt Group

$$\widehat{W}(F) := Groth(M(F)). \qquad \textit{By cnacellation} \quad M(F) \hookrightarrow \widehat{W}(F).$$

In deed, $\widehat{W}(F)$ has a ring srtucture. The multiplicative structue is given by tensor product of quadratic forms defined in §1.6. That means,

1. For $x = [(V_1, q_1)], y = [(V_2, q_2))] \in \widehat{W}(F)$ define,

$$xy := [(V_1 \otimes V_2, q_1 \otimes q_2)]$$

2. We can check all the properties of ring for $\perp$ and the tensor product:

   (a) Since tensor product is commutative (up to isomorphim), the multiplication on $\widehat{W}(F)$ is a commutative: i. e. $xy = yx$.

   (b) (Distributivity) $x(y + z) = xy + xz$

   (c) $\langle 1 \rangle$ is the multiplicative identity.

So, $\widehat{W}(F)$ is a commutative ring.

Furhter Comments:

1. Any element $x \in \widehat{W}(F)$ can be written as $x = q_1 - q_2$ where q_1, q_2 are nonsingular quadratic forms.

2. For two quadratic form q_1, q_2 We have $q_1 = q_2 \in \widehat{W}(F) \iff q_1 \cong q_1$.

   Proof. Suppose $q_1 = q_2 \in \widehat{W}(F)$. Then, $(q_1, 0) \sim (q_2, 0)$ and hence, $q_1 + z \cong q_2 + z$ for some quadratic space z. By cancellation $q_1 \cong q_2$. The proof is complete. ■

3. The dimension function induces a homomorphims of binary structures

$$\dim : M(F) \longrightarrow \mathbb{Z} \qquad (V, q) \mapsto \dim V.$$

4. By the universal property, the dimension function induces a homomorphim of groups

$$\dim : \widehat{W}(F) \longrightarrow \mathbb{Z} \qquad q_1 - q_2 \mapsto \dim q_1 - \dim q_2.$$

   In fact, it is a homomorphism of rings.

5. The kernel of the homomorphism is denoted by $\widehat{I}(F)$ is called the Fundamental ideal of $\widehat{W}(F)$.

6. We have,

$$\frac{\widehat{W}(F)}{\widehat{I}(F)} \approx \mathbb{Z}$$

   This ideal is truly fundamental in this theory. Voevodsky received Fields Medal, for proving Milnor's conjecture, concerning these ideals.

Proposition 1.4. The fundamental ideal $\widehat{I}(F)$ is additively generated by

$$\textit{the expressions} \quad \langle a \rangle - \langle 1 \rangle, \quad \textit{with} \quad a \neq 0.$$

Proof. Clearly, for all $a \neq 0$ the elements $\langle a \rangle - \langle 1 \rangle \in \widehat{I}(F)$. Let $z \in \widehat{I}(F)$. Then, $z = q_1 - q_2$ where q_1, q_2 are nonsingualr and $\dim q_1 = \dim q_2 = n$ (*say*). We diagonalize

$$q_1 = \langle a_1, \ldots, a_n \rangle, \quad q_1 = \langle b_1, \ldots, b_n \rangle$$

So,

$$z = q_1 - q_2 = \sum_{i=1}^{n} \langle a_i \rangle - \sum_{i=1}^{n} \langle b_i \rangle = \sum_{i=1}^{n} (\langle a_i \rangle - \langle 1 \rangle) - \sum_{i=1}^{n} (\langle b_i \rangle - \langle 1 \rangle).$$

The proof is complete. ■

The following is a primary object of our study.

Definition 1.5. Define the Witt Ring

$$W(F) := \frac{\widehat{W}(F)}{\mathbb{H} \cdot \mathbb{Z}}$$

Clearly, $W(F)$ inherits the ring structure from $\widehat{W}(F)$.

Proposition 1.6. 1. There is an 1 to 1 correspondence between the

$$\textit{isometry classes of all anisotropic forms} \quad \longleftrightarrow \quad W(F)$$

2. Two (nonsingular) forms q, q' represent the same element in $W(F)$ if and only if $q_a \cong q'_a$. (In this case we say q, q' are "Witt-similar".)

3. If $\dim q = \dim q'$ then q, q' represent the same element in $W(F)$ if and only if $q \cong q'$.

Proof. Suppose $x \in W(F)$. Then, $x = q_1 - q_2 \in W(F)$ for two nongingular forms. Since $\langle a \rangle \perp \langle -a \rangle \cong \mathbb{H}$, we have $\langle -a \rangle = -\langle a \rangle$ for all nonzero $a \in \dot{F}$. With $q_1 \cong \langle a_1 \rangle \perp \cdots \langle a_n \rangle$ and $q_2 \cong \langle b_1 \rangle \perp \cdots \langle b_m \rangle$ we have

$$In \quad W(F) \quad q_1 - q_2 = \langle a_1 \rangle \perp \cdots \perp \langle a_n \rangle \perp (\langle -b_1 \rangle \perp \cdots \langle -b_m \rangle) =: q$$

for some some nonsingualr form q. Now, we can write $q \cong q_h \perp q_a$, by the decomposition theorem. Therefore, $q = q_a \in W(F)$. So, any element $x = q_1 - q_2 \in W(F)$ is represented by an anisotropic form. Now, we show is correspondence is 1-1. Let q, q' be anisotropic and $q = q' \in W(F)$. Then, $q = q' + m\mathbb{H} \in \widehat{W}(F)$. Without loss we assume $m \geq 0$. By the comment above $q \cong q' \perp m\mathbb{H}$. Since q is anisotropic $m = 0$. So, $q \cong q'$.

Now, (2) follows from (1). For (3), write $q = q_h \perp q_a, q' = q'_h \perp q'_a$ where q_a, q'_a are anisotropic and q_h, q'_h are hyperbolic. Suppose $q = q' \in W(F)$. Then $q_a \cong q'_a$, by (2). Comparing dimension, we have $q \cong q'$.

Definition 1.7. Consider the natural homomorphism

$$i : \widehat{W}(F) \longrightarrow W(F)$$

1. The ideal (image) $I(F) := i(\widehat{I}(F))$ is also called the fundamental ideal of $W(F)$.

2. Note that the induced map $i : \widehat{I}(F) \xrightarrow{\sim} I(F)$ is an isomorphism.

   Proof. Suppose $i(x) = 0$. That means $x = m\mathbb{H}$. Considering, dimension, $0 = \dim x = 2m$. So, $m = 0$ and $x = 0$. ∎

Proposition 1.8. A form q represents an element in $I(F) \subseteq W(F)$ if and only if $\dim q$ is even.

Proof. Suppose $x \in I(F)$ is represented by the form q. (*Note, by element in $W(F)$ is represented by a nonsisngular form.*) In any case, $x = q_1 - q_2$ with $\dim q_1 = \dim q_2$. So, $q = q_1 - q_2 + m\mathbb{H} \in \widehat{W}(F)$. The dimension function is defined on $\widehat{W}(F)$. Applying this function, we have $\dim q = 2m$ is even.

Conversely, suppose $\dim q$ is even. In $W(F)$, we have

$$\begin{aligned} q &= \langle a_1, b_1 \rangle \perp \cdots \perp \langle a_n, b_n \rangle \\ &= (\langle a_1 \rangle - \langle -b_1 \rangle) \perp \cdots \perp (\langle a_n \rangle - \langle -b_n \rangle) \in I(F). \end{aligned}$$

∎

Corollary 1.9. Consider the epimorphism

$$\dim : \widehat{W}(F) \twoheadrightarrow \mathbb{Z}.$$

1. dim induces an epimorphism

$$\dim_0 : W(F) \twoheadrightarrow \frac{\mathbb{Z}}{2\mathbb{Z}}.$$

2. Further, $\dim_0$ induces an isomorphism

$$\frac{W(F)}{I(F)} \xrightarrow{\sim} \frac{\mathbb{Z}}{2\mathbb{Z}}.$$

Proof. Consider the commutative diagram

$$\begin{tikzcd}
\widehat{W}(F) \arrow[r] \arrow[d, "\dim"'] & W(F) \arrow[r] \arrow[d, "\dim_0"'] & \frac{W(F)}{I(F)} \arrow[dl, "\sim"] \\
\mathbb{Z} \arrow[r] & \frac{\mathbb{Z}}{2\mathbb{Z}} &
\end{tikzcd}$$

The diagonal map at the end is well defined by the "if" part of (1.8) and it is an isomorphism by the "only if" part of (1.8). ■

2 Group of Square Classes

We exploit the group of square classes $\frac{\dot{F}}{\dot{F}^2}$.

1. The determinant function defines a monoid homomorphism

$$d : M(F) \longrightarrow \frac{\dot{F}}{\dot{F}^2}$$

2. It extends to

$$d : \widehat{W}(F) \longrightarrow \frac{\dot{F}}{\dot{F}^2} \quad by \quad q_1 - q_2 \mapsto d(q_1)d(q_2)^{-1} \in \frac{\dot{F}}{\dot{F}^2}$$

   It does not extend to $W(F)$, because $\det(\mathbb{H}) = -1$ need not be in $\dot{F}^2$.

3. However, for a quadratic form, we define signed determinant

$$d_{\pm}(q) = (-1)^{\frac{n(n-1)}{2}} d(q) \quad where \quad n = \dim q.$$

   Even this fails to extend to a homomorphism on $W(F)$.

4. We define a group structure on

$$Q(F) := \mathbb{Z}_2 \times \frac{\dot{F}}{\dot{F}^2}.$$

$$\forall\ (e,x),(e',x') \in Q(F) \quad define\, product \quad (e,x)\cdot(e',x') := (e+e', (-1)^{ee'}xx').$$

   (a) This defines an abelian group structure on $Q(F)$.
   (b) $(0,1) \in Q(F)$ is the identity.
   (c) Also

$$(e,x)\cdot(e,(-1)^e x) = (0,(-1)^{e^2+e}x^2) = (0,1), \quad which\, describes\, the\, inverse.$$

   (d) We have an exact sequence of groups

$$0 \longrightarrow \frac{\dot{F}}{\dot{F}^2} \longrightarrow Q(F) \longrightarrow \mathbb{Z}_2 \longrightarrow 0 \quad 1st\ homomophism \quad x \mapsto (0,x).$$

Proposition 2.1. *We have the following:*

1. *The map*

$$(\dim_0, d_\pm) : M(F) \longrightarrow Q(F) \quad \textit{is a monoid epimorphism.}$$

2. *This extends to a group epimorphism*

$$(\dim_0, d_\pm) : \widehat{W}(F) \twoheadrightarrow Q(F).$$

3. *This induces an isomorphism*

$$\frac{W(F)}{I(F)^2} \xrightarrow{\sim} Q(F).$$

Proof. To see $(\dim_0, d_\pm)$ is a monoid homomorphism, let q, q' be two non-singular forms, with $\dim q = n, \dim q' = n'$. We compute

$$(\dim_0, d_\pm)(q) \cdot (\dim_0, d_\pm)(q') = \left(n + n', (-1)^{\left(nn' + \frac{(n(n-1)}{2} + \frac{(n'(n'-1)}{2}\right)} d(q)d(q')\right)$$

$$= \left(n + n', (-1)^{\left(\frac{(n+n')(n+n'-1)}{2}\right)} d(q)d(q')\right) = (\dim_0, d_\pm)(q \perp q')$$

To see it is epimorphism, note

$$(\dim_0, d_\pm)(\langle a \rangle) = (1, a \cdot \dot{F}^2), \quad (\dim_0, d_\pm)(\langle 1, -a \rangle) = (0, a \cdot \dot{F}^2).$$

Now, $(\dim_0, d_\pm)$ extends to $\widehat{W}(F)$ from the universal property of $\widehat{W}(F)$. So, (2) is established. To, see (3), note

$$(\dim_0, d_\pm)(\mathbb{H}) = (0, 1). \quad \textit{Hence it factors} \quad \begin{tikzcd} \widehat{W}(F) \arrow[r, two heads] \arrow[d] & Q(F) \\ W(F) \arrow[ur, dashed, "\beta_0"'] & \end{tikzcd}$$

We show that $\beta_0(I(F)^2)$ is trivial. By (1.4) and , $I(F)$ is additively generated by $\langle 1 \rangle - \langle a \rangle = \langle 1, a \rangle$. So, $I(F)^2$ is additively generated by product $\langle 1, a, b, ab \rangle$. we have

$$(\dim_0, d_\pm)(\langle 1, a, b, ab \rangle) = (0, a^2 b^2 \dot{F}^2) = (0, 1).$$

So, β_0 factors through $f : \frac{W(F)}{I(F)^2} \twoheadrightarrow Q(F)$. Now, we will construct an inverse $g : Q(F) \longrightarrow \frac{W(F)}{I(F)^2}$ of f, as follows:

$$g(0, a) = \langle 1, a\rangle \ \ (mod\ I(F)^2), \quad g(1, a) = \langle a\rangle \ \ (mod\ I(F)^2),$$

Routine checking establishes (see textbook) that g is a group homomorphism. It is easy to see that $fg = Id$. So, g is injective. But $g(1, a) = \langle a\rangle \ \ (mod\ I(F)^2)$. So, g is also surjective. ■

Corollary 2.2 (Pfister). *$I(F)^2$ consists of classes of the even dimensional forms q for which $d(q) = (-1)^{\frac{n(n-1)}{2}}$, where $n = \dim q$.*

Proof. It is restatement of (2.1) that the map $f(q) = \left(\dim_0(q), (-1)^{\frac{n(n-1)}{2}} d(q)\right)$ is injective, while the identity of $Q(F)$ is $(0, 1)$. ■

Corollary 2.3 (Pfister). *The map f induces an isomorphim $\frac{I(F)}{I(F)^2} \xrightarrow{\sim} \frac{\dot{F}}{\dot{F}^2}$.*

Proof. We have the diagram

$$\begin{tikzcd}
\frac{I(F)}{I(F)^2} \arrow[r, "d_\pm"] \arrow[d, hook] & \frac{\dot{F}}{\dot{F}^2} \arrow[d, hook] \\
\frac{W(F)}{I(F)^2} \arrow[r, "\sim", "f"'] & Q(F)
\end{tikzcd}$$

We only need to prove that the, restriction of f on the first line lands in $\frac{\dot{F}}{\dot{F}^2}$ It is surjective because $d_\pm(\langle 1, -a\rangle) = a$. It is injective because all the other three maps are. ■

Let $q \in I(F)$, so $\dim q = 2r$. So,

$$f([q]) = \left(2r, (-1)^{\frac{2r(2r-1)}{2}} d(q)\right) = (0, (-1)^r d(q)) .$$

This also shows that the diagram commutes. Now, $f([q]) = (0, 1)$ means $(-1)^r d(q) = 1 \cdot \dot{F}^2$.

$$f([q]) = (0, 1) \Longleftrightarrow (-1)^r d(q) = 1 \cdot \dot{F}^2 \Longleftrightarrow d(q) = \begin{cases} 1 & if\ r\ even \\ -1 & if\ r\ odd. \end{cases}$$

■

Corollary 2.4. *For $q \in I(F)$, we have* $\dim q = 2r$. *Then,*

$$q \in I(F)^2 \Longleftrightarrow d(q) = \begin{cases} 1 & if\ r\ even \\ -1 & if\ r\ odd. \end{cases}$$

Corollary 2.5. *The following are equivalent:*

1. $\widehat{W}(F)$ *is noetherian.*

2. $W(F)$ *is noetherian.*

3. $\frac{\dot{F}}{\dot{F}^2}$ *is finite.*

Proof. (1) $\Longrightarrow$ (2) is obvious.
((2) $\Longrightarrow$ (3)): Note $\frac{I(F)}{I(F)^2}$ is noetherian, over the noetherian ring $\frac{W(F)}{I(F)}$. Also, by (1.9) $\frac{W(F)}{I(F)} \approx \mathbb{Z}_2$. So, $\frac{I(F)}{I(F)^2}$ is finite and hence, by (2.3), $\frac{\dot{F}}{\dot{F}^2}$ is finite.

((3) $\Longrightarrow$ (1)): By diagonalization, $\widehat{W}(F)$ is additively generated by $\langle a \rangle$, with $a \in \frac{\dot{F}}{\dot{F}^2}$. Since, $\frac{\dot{F}}{\dot{F}^2}$ is finite, $\widehat{W}(F)$ is finitely generated commutative ring over $\mathbb{Z}$. So, $\widehat{W}(F)$ is noetherian. ∎

Remark 2.6. *The map* $f : \frac{W(F)}{I(F)^2} \xrightarrow{\sim} Q(F)$ *in (2.1) is an isomorphism of groups. Since,* $\frac{W(F)}{I(F)^2}$ *is ring,* f *induces a ring structure on* $Q(F)$. *Further comments:*

1. *The multiplication is given by*

$$(0, a)o(0, b) = (0, 1),\ (0, a)o(1, b) = (0, a),\ (1, a)o(1, b) = (1, ab).$$

2. *For two fields* F, K *if there is an isomorphism* $\theta : \frac{\dot{F}}{\dot{F}^2} \xrightarrow{\sim} \frac{\dot{K}}{\dot{K}^2}$, *with* $\theta(-1) = -1$ *then* $Q(F) \xrightarrow{\sim} Q(K)$.

3 Some Elementary Computations

Definition 3.1. A field k is said to be quadratically closed, if $\sqrt{a} \in k$ for all $0 \neq a \in k$.

Theorem 3.2. *F is quadratrically closed if and only if* $\dim : \widehat{W}(F) \longrightarrow \mathbb{Z}$ *is an isomprphism. In this case* $W(F) \xrightarrow{\sim} \mathbb{Z}_2$.

Proof. Suppose q is a form. We have

$$q = \langle a_1, \rangle \perp \langle a_2 \rangle \cdots \langle a_n \rangle = \langle b_1^2 \rangle \perp \langle b_2^2 \rangle \cdots \langle b_n^2 \rangle = n\langle 1 \rangle.$$

So, the map dim is an isomorphism. Also $q - q' = (\dim q - \dim q')\langle 1 \rangle \in \widehat{W}(F)$. So, dim is also injective. Note $\mathbb{H} \mapsto 2$. ■

We define signature of the form.

Definition 3.3. Let $F = \mathbb{R}$ and q is a nonsingular form with $\dim q = n$. Use diagonalization, we have $q \cong r\langle 1 \rangle \perp (n-r)\langle -1 \rangle$ for some $n, m > 0$. We define signature of q; as

$$Sig(q) = 2r - n = (number\ of\ \langle 1 \rangle) - (number\ of\ \langle -1 \rangle).$$

We need to justify that this is well defined. Suppose $q \cong s\langle 1 \rangle \perp (n-s)\langle -1 \rangle$. Passing to Witt group

$$[q] = r[\langle 1 \rangle] - (n-r)[\langle 1 \rangle] = (2r-n)[\langle 1 \rangle].$$

Similarly, $[q] = (2s-n)[\langle 1 \rangle]$. So, $(2r-n)[\langle 1 \rangle] = (2s-n)[\langle 1 \rangle]$. It follows from (2) on (3.4 below) that $r = s$

So, $Sig(q)$ is well defined.

Proposition 3.4 (3.2)**.** *Let $F = \mathbb{R}$. Then:*

1. *There are exactly two anisotropic form at each (positive) dimesions, namely $n\langle 1 \rangle, n\langle -1 \rangle$.*

2. $W(\mathbb{R}) \xrightarrow{\sim} \mathbb{Z}$ *is an isomorphism.* (This is not induced by the dimension map.)

3. **(Sylvester's Law of Inertia)** *Two (nonsingular) forms over F are quivalent if and only is they have same dimension and same signature.*

4. $\widehat{W}(\mathbb{R}) \xrightarrow{\sim} \mathbb{Z}(G)$ *where G is a 2−element group.*

Proof. We have $\frac{\dot{F}}{\dot{F}^2} = \{\pm 1\}$. So, a form $q \cong n\langle 1\rangle \perp m\langle -1\rangle$ Clearly, q is anisotropic if and only if either $n = 0$ or $m = 0$. So, (1) is established.

We prove (2). Suppose $x \in W(\mathbb{R})$. There is an anisotropic form q such that $x = [q]$. By (1) $q = n\langle 1\rangle$ for some $n \in \mathbb{Z}$. Define $\psi : W(\mathbb{R}) \longrightarrow \mathbb{Z}$ by $\psi(x) := n$. We need to ensure that ψ is well defined. So, suppose $x = [n\langle 1\rangle] = [m\langle 1\rangle]$. Assume $n \geq m$. So, in $\widehat{W}(F)$ we have $(n\langle 1\rangle) = (m\langle 1\rangle) + u(\mathbb{H})$. Since, q is anisotropic, $u = 0$ and $n = m$. So, ψ is well defined. It is clear that ψ is surjective. Now suppose $x = [n\langle 1\rangle]$ and $\psi(x) = 0$. By definition $n = 0$. So, (2) is established.

We prove (3). Suppose $q \cong q'$. It is established that they have same dimesion and signature. Now suppose q, q' have same signature and dimension. We can write

$$q = m\langle 1\rangle \perp n\langle -1\rangle, \quad r\langle 1\rangle \perp s\langle -1\rangle$$

So, $\dim q = m+n = r+s = \dim q'$, $2n - \dim q = 2r - \dim q'$. So, $m = r, n = s$. So, (3) is established.

We prove (4). The determiant $d : \widehat{W}(\mathbb{R}) \longrightarrow \frac{\dot{\mathbb{R}}}{\dot{\mathbb{R}}^2}$ is defined. We can use this to see $e_1 := \langle 1\rangle \neq \langle -1\rangle =: e_2$. e_1, e_2 are linealry independent over $\mathbb{Z}$. To, see this let $m\langle 1\rangle + n\langle -1\rangle = 0 \in \widehat{\mathbb{R}}$. Taking the image in $W(\mathbb{R})$, we have $(m - n)\langle 1\rangle = 0 \in W(\mathbb{R})$. By (2), $m = n$.

It is also clear that $\widehat{W}\mathbb{R}$ is generated by e_1, e_2, as a ring. So, we have $\widehat{W}\mathbb{R} \approx \mathbb{Z}e_1 \oplus \mathbb{Z}e_2$. The proof is complete. ∎

Remark 3.5 (Skip?)**.** We have the following, when $F = \mathbb{R}$.

1. $\widehat{I}(F)$ a free abelian group generated by $\langle 1\rangle - \langle -1\rangle$. (*Obvious from (4) of (3.4)*)

2. $Sig : M(F) \longrightarrow \mathbb{Z}$ is a monoid homomorphism.

3. Discuss method of "completion of square" for diagonalization.

3.1 Over the filed $F = \mathbb{F}_q$ with $q \neq 2$

Let $q = p^m$ for some prime $p \neq 2$ and $F = \mathbb{F}_q$.

1. $\dot{F}$ is cyclic group of even order $q-1$. (See field theory.)

2. So, $\dot{F} \approx G \times \mathbb{Z}_2$ where $o(G)$ is odd.

3. So, $o\left(\frac{\dot{F}}{\dot{F}^2}\right) = 2$ (*because everything has order 1 or 2.*)

Proposition 3.6 (3.4)**.** *Let $F = \mathbb{F}_q$ and $\frac{\dot{F}}{\dot{F}^2} = \{1, s\}$. Then,*

1. s is a sum of two squares, and

2. every (nonsingular) binary form is universal.

Proof. In fact, $(1) \Longrightarrow (2)$: Since $1, s$ are the only two square classes, there are at most three non-equivalent binary forms

$$f_1 = \langle 1, 1\rangle = x^2 + y^2, \quad f_2 = \langle 1, s\rangle = x^2 + sy^2, \quad f_3 = \langle s, s\rangle = sx^2 + sy^2.$$

We need to check, $1, s \in D(f_i)$. Clealry, $1, s \in D(f_2)$. By (1) $s = a^2 + b^2$. So, $s = f_1(a, b), 1 = f_1(1, 0) \in D(f_1)$. Then, $s = f_3(1, 0), s^2 = f_3(a, b) \in D(f_3)$. So, $(1) \Longrightarrow (2)$.

We will prove (1). Two cases:

1. $-1 \in \dot{F}^2$. Then, $\langle 1, 1\rangle \cong \langle 1, -1\rangle$, which is universal (because $\mathbb{H} = X_1X_2$. So, $s \in D(\langle 1, 1\rangle$.

2. Suppose $-1 \notin \dot{F}^2$. Consider two (finite) sets $\dot{F}^2, 1 + \dot{F}^2$. They are not equal, because $1 \in \dot{F}^2$ and $1 \notin 1 + \dot{F}^2$. In particular, there is a $z \in \dot{F}$ such that $1 + z^2 \notin \dot{F}^2$. Now by hypothesis, $1 + z^2 \neq 0$. Since $\frac{\dot{F}}{\dot{F}^2} = \{1, s\}$, $s\dot{F}^2 = (1 + z^2)\dot{F}^2$. So, $s = (1 + z^2)\lambda^2$ is a sum of two squares. ■

4 Presentation of Witt Rings

We describe $\widehat{W}(F)$ in terms of generators and relations/

Lemma 4.1. *Let F be a field, with $char(F) \neq 2$. Then, $\widehat{W}(F)$ is generated,* **as a commutative ring***), by the set $\{\langle a \rangle : a \in \dot{F}\}$. Further, for $a, b \in \dot{F}$, we have*

1. *($R_0 1$): $\langle 1 \rangle = 1$(= the identity of the ring).*
2. *($R_0 2$): $\langle a \rangle \cdot \langle b \rangle = \langle ab \rangle$*
3. *($R_0 3$): $\langle a \rangle + \langle b \rangle = \langle a+b \rangle \cdot (1 + \langle ab \rangle)$, whenever $a + b \in \dot{F}$.*

Proof. $R_0 1, R_0 2$ follows from definition of product. We have

$$d(\langle a \rangle + \langle b \rangle) = ab\dot{F}^2,$$

and

$$d((\langle a+b \rangle \cdot (1+\langle ab \rangle)) = d(\langle a+b \rangle + \langle a^b + ab^2 \rangle) = (a+b)(a^2b+ab^2)\dot{F}^2 = (a+b)\dot{F}^2.$$

Also, $a + b$ is represented by both sides. Now $R_0 3$ follows from I.5.1. ∎

Theorem 4.2 (4.1)**.** *Let $R = \mathbb{Z}[X_a : a \in \dot{F}]$ be the polynomial ring over $\mathbb{Z}$, where X_a are indeterminates* (possibly, infinitely many)*. Let I be the ideal generated by the set $R1 \cup R2 \cup R3$ where*

1. *$R1 = \{X_1 - 1\}$*
2. *$R2 = \{X_{ab} - X_a X_b : a, b \in \dot{F}\}$*
3. *$R3 = \{X_a + X_b - X_{a+b}(1 + X_{ab}) : a, b \in \dot{F}$ with $a + b \in \dot{F}\}$*

Then $\frac{R}{I} \approx \widehat{W}(F)$.

Proof. As usual define a ring homomorphism

$$f_0 : R \longrightarrow \widehat{W}(F) \quad by \quad \varphi_0(X_a) = \langle a \rangle$$

By lemma 4.1, $f_0(I) = 0$. So, f_0 induces a homomorphims φ, such that

$$\textit{the diagram} \quad \begin{tikzcd} R \arrow[r] \arrow[dr, "f_0"'] & \frac{R}{I} \arrow[d, "f"] \\ & \widehat{W}(F) \end{tikzcd} \quad \textit{commutes.}$$

We will define an inverse of f. We define a monoid homomorphism $\varphi : M(F) \longrightarrow \frac{R}{I}$ as follows:

Suppose q is a quadratic form. Take any diagonalization $q = \langle a_1, \cdots, a_n \rangle$. Define

$$\varphi(q) = X_{a_1} + \cdots + X_{a_n}$$

We need to check that this is well defined. Suppose

$$q = \langle b_1, \cdots, b_n \rangle \quad \textit{be another diagonalization.}$$

By Witt's chain equivalence theorem, we may assume that $\langle a_1, \cdots, a_n \rangle$ and $\langle b_1, \cdots, b_n \rangle$ are simply-equivalent. Without loss of generality, we can assume $a_i = b_i \ \ \forall \ i \geq 3$ and

$$\langle a_1, a_2 \rangle \equiv \langle b_1, b_2 \rangle.$$

Now on the image of X_a will be denoted by x_a. We have the following observation:

1. For all $a \in \dot{F}$, we have $x_{a^2} = 1$.

   Proof. First, by $R1, R2$ we have $1 = x_1 = x_a x_{a^{-1}}$. So, x_a is a unit for all $a \in \dot{F}$.

   (a) (A) Since $a + a = 2a \neq 0$, by $R3$ we have

   $$x_a + x_a = x_{2a}(1 + x_{a^2})$$

   (b) (B) By $R2$, we have $x_a = x_a x_1$. Now

   $$\begin{aligned} x_a + x_a = x_a x_1 + x_a x_1 = x_a[x_1 + x_1] &= x_a[x_2(1 + x_1)] \quad \textit{by } R3 \\ = x_{2a}(1 + x_1) & \qquad \textit{by} \ \ R2 \end{aligned}$$

Comparing (A), (B) and cancelling, we have $x_{a^2} = x_1 = 1$.

Now, we have

$$\begin{pmatrix} b_1 & 0 \\ 0 & b_2 \end{pmatrix} = \begin{pmatrix} x & y \\ z & w \end{pmatrix} \begin{pmatrix} a_1 & 0 \\ 0 & a_2 \end{pmatrix} \begin{pmatrix} x & z \\ y & w \end{pmatrix}.$$

It follows, $b_1 = a_1x^2 + a_2y^2$ and taking determinant $a_1a_2 = b_1b_2c^2$ for some $c \in \dot{F}$.

1. **Case 1.** $x = 0$ or $y = 0$. Without loss of generality $x = 0$. So, $b_1 = a_2y^2$. By $R2$ we have $x_{b_1} = x_{a_2y^2} = x_{a_2}x_{y^2} = x_{a_2}$. Also,

$$x_{a_1} = x_{b_2\frac{b_1}{a_1}c^2} = x_{b_2y^2c^2} = x_{b_2}$$

   Therefore

$$x_{a_1} + x_{a_2} = x_{b_1} + x_{b_2}.$$

2. **Case 2.** $x \neq 0, y \neq 0$. In this case,

$$x_{a_1} + x_{a_2} = x_{a_1x^2} + x_{a_2y^2} = x_{a_1x^2+a_2y^2}(1 + x_{a_1a_2(xy)^2})$$

$$= x_{b_1}(1 + x_{a_1a_2}) = x_{b_1}(1 + x_{b_1b_2}) = x_{b_1} + x_{b_2}$$

So, φ is well defined. It is clearly a monoid homomorphism.

By defintion of Grothendieck group, φ extends to a group homomorphism $\varphi : \widehat{\widetilde{W}}(F) \longrightarrow \frac{R}{I}$. Clearly, φ is the inverse of f.

5 Classification of Small Witt Rings

SKIP.