3. WITT'S CANCELLATION THEOREM

§3.1. Reflections

If V is a quadratic space and $\mathbf{a} \in V$ has non-zero length, the **hyperplane reflection** $\rho_{\mathbf{a}}: V \to V$ is defined by

$$\rho_{\mathbf{a}}(\mathbf{v}) = \mathbf{v} - \frac{2\langle \mathbf{v} \mid \mathbf{a} \rangle}{\langle \mathbf{a} \mid \mathbf{a} \rangle} \mathbf{a}.$$

One easily verifies that ρ_a is an isometry (ie is linear, 1–1, onto and preserves inner products) and that $\rho_{\mathbf{a}}(\mathbf{a}) = -\mathbf{a}$ and vectors orthogonal to a are fixed.

Theorem 1: If $\langle \mathbf{u} \mid \mathbf{u} \rangle = \langle \mathbf{v} \mid \mathbf{v} \rangle$ and $\langle \mathbf{u} - \mathbf{v} \mid \mathbf{u} - \mathbf{v} \rangle \neq 0$ then

$$\rho_{\mathbf{u}-\mathbf{v}}(\mathbf{u}) = \mathbf{v}.$$

Proof: $\langle \mathbf{u} - \mathbf{v} \mid \mathbf{u} + \mathbf{v} \rangle = \langle \mathbf{u} \mid \mathbf{u} \rangle - \langle \mathbf{v} \mid \mathbf{v} \rangle = 0$ so $\mathbf{u} + \mathbf{v}$ is orthogonal to $\mathbf{u} - \mathbf{v}$.

So $\rho_{\mathbf{u}-\mathbf{v}}(\mathbf{u} + \mathbf{v}) = \mathbf{u} + \mathbf{v}$ and

$\rho_{\mathbf{u}-\mathbf{v}}(\mathbf{u} - \mathbf{v}) = \mathbf{v} - \mathbf{u}$ and so

$\rho_{\mathbf{u}}(\mathbf{u}) = \mathbf{v}$. ✋☺

Theorem 2: If $\langle \mathbf{u} \mid \mathbf{u} \rangle = \langle \mathbf{v} \mid \mathbf{v} \rangle \neq 0$ there exists an isometry $\rho: V \to V$ such that $\rho(\mathbf{u}) = \mathbf{v}$.

Proof: If $\langle \mathbf{u} - \mathbf{v} \mid \mathbf{u} - \mathbf{v} \rangle \neq 0$ use Theorem 5 in Chapter 2.

Suppose now that $\langle \mathbf{u} - \mathbf{v} \mid \mathbf{u} - \mathbf{v} \rangle = 0$.

Then $\langle \mathbf{u} \mid \mathbf{u} \rangle = \langle \mathbf{v} \mid \mathbf{v} \rangle = \langle \mathbf{u} \mid \mathbf{v} \rangle$.

Hence $\langle \mathbf{u} + \mathbf{v} \mid \mathbf{u} + \mathbf{v} \rangle = 4\langle \mathbf{u} \mid \mathbf{u} \rangle \neq 0$.
Then $\rho_{\mathbf{u}+\mathbf{v}}(\mathbf{u}) = -\mathbf{v}$ by Theorem 5 in Chapter 2, and so $(\rho_{\mathbf{u}+\mathbf{v}}\rho_{\mathbf{v}})(\mathbf{u}) = \rho_{\mathbf{v}}(-\mathbf{v}) = \mathbf{v}$. ✋☺

A theorem by Cartan and Dieudonné shows that if V is a regular quadratic space of dimension n then every isometry is a product of at most n hyperplane reflections.

§3.2. The Cancellation Theorem

Theorem 3: If $V = \text{rad } V \oplus K_1 = \text{rad } V \oplus K_2$ then

$$K_1 \cong K_2.$$

Proof: If $\mathbf{k} \in K_1$ then $\mathbf{k} = \mathbf{r} + \mathbf{k}'$ for some $\mathbf{k}' \in K_2$.
Define $\rho(\mathbf{k}) = \mathbf{k}'$. ρ is clearly linear (restriction to K_1 of the projection onto K_2). ✋☺

Exercise 1: Show that ρ preserves inner products and hence is an isometry.

Theorem 4: (WITT) If $\langle a_1, \ldots, a_n \rangle \cong \langle b_1, \ldots, b_n \rangle$ and $a_1 = b_1$ then $\langle a_2, \ldots, a_n \rangle \cong \langle b_2, \ldots, b_n \rangle$.

Proof: Case I: $a_1 = b_1 = 0$. The conclusion follows from Theorem 7 in Chapter 2.

Case II: $a_1 = b_1 \neq 0$. Let V by a quadratic space corresponding to $\langle a_1, \ldots, a_n \rangle$.
Then there exists an orthogonal basis $\mathbf{e}_1, \ldots, \mathbf{e}_n$ such that $\langle \mathbf{e}_i \mid \mathbf{e}_i \rangle = \mathbf{a}_i$ and there exists an orthogonal basis $\mathbf{f}_1, \ldots, \mathbf{f}_n$ such that $\langle \mathbf{f}_i \mid \mathbf{f}_i \rangle = \mathbf{b}_i$.

Since $a_1 = b_1 \neq 0$, then by Theorem 2, there exists an isometry $\rho: V \to V$ such that $\rho(\mathbf{e}_1) = \mathbf{f}_1$.

For $i > 1$, $\langle \rho(\mathbf{e}_i) \mid \mathbf{f}_1 \rangle = \langle \rho(\mathbf{e}_i) \mid \rho(\mathbf{e}_1) \rangle = \langle \mathbf{e}_i \mid \mathbf{e}_1 \rangle = 0$,
so $\rho(\mathbf{e}_2), \ldots, \rho(\mathbf{e}_n) \in \langle \mathbf{f}_1 \rangle^{\perp}$.
Now, since $\langle \mathbf{f}_1 \mid \mathbf{f}_1 \rangle \neq 0$, $\langle \mathbf{f}_1 \rangle^{\perp} = \langle \mathbf{f}_2, \ldots, \mathbf{f}_n \rangle$ and so
$\dim \langle \mathbf{f}_1 \rangle^{\perp} = n - 1$.
Since $\rho(\mathbf{e}_2), \ldots, \rho(\mathbf{e}_n)$ are linearly independent (ρ is 1-1) they form a basis (in fact an orthogonal basis) for $\langle \mathbf{f}_1 \rangle^{\perp}$.

Relative to this orthogonal basis the quadratic form for $\langle \mathbf{f}_1 \rangle^{\perp}$ is $\langle a_2, \ldots, a_n \rangle$. But relative to the orthogonal basis $\mathbf{f}_2, \ldots, \mathbf{f}_n$ it is $\langle b_2, \ldots, b_n \rangle$.
Hence $\langle a_2, \ldots, a_n \rangle \cong \langle b_2, \ldots, b_n \rangle$. ☟☺
Corollary: In the decomposition $V \cong m\mathbb{Z} \oplus n\mathcal{H} \oplus W$, where W is non-isotropic, m, n are unique and W is unique, up to isomorphism.

Define the **nullity** of V to be m (this is the nullity of the corresponding matrix). Define the **Witt-index** of V to be n. Define the **core** of V to be W.

§3.3. The Witt Ring

The **Witt Ring** of a quadratic space V is the set of non-isotropic quadratic forms over F with addition and multiplication defined as follows:
If $\mathbf{x} = (x_1, \ldots, x_m)$ and $\mathbf{y} = (y_1, \ldots, y_n)$ are vectors involving $m + n$ distinct variables then

$$a(\mathbf{x}) + b(\mathbf{y}) = \text{core}\,[a(\mathbf{x}) + b(\mathbf{y})] \text{ and}$$
$$a(\mathbf{x}).b(\mathbf{y}) = \text{core}\,[a(\mathbf{x})b(\mathbf{y})].$$

Since every quadratic form can be expressed as a diagonal one, we can write these definitions as:

$$\langle a_1, \ldots, a_m\rangle + \langle b_1, \ldots, b_n\rangle = \text{core}\,\langle a_1, \ldots, a_m, b_1, \ldots, b_n\rangle$$
and
$$\langle a_1, \ldots, a_m\rangle.\langle b_1, \ldots, b_n\rangle$$
$$= \text{core}\,\langle a_1b_1, ..., a_1b_n, a_2b_1, ..., a_2b_n, \ldots, a_mb_1, \ldots, a_mb_n\rangle.$$

Note, to show that addition and multiplication are well-defined one must show that they are compatible with equivalence. This is obvious for addition since the sum of two quadratic forms is defined to be the core of the direct sum. For multiplication we must put a quadratic structure on the tensor product of the two quadratic spaces.

One may easily verify that under these operations, W(F) is a ring. The zero element is the 0-dimensional non-isotropic quadratic form $\langle\ \rangle$, or 0. The additive identity of $\langle a_1, \ldots, a_m\rangle$ is $\langle -a_1, \ldots, -a_m\rangle$ since

$$\langle a_1, \ldots, a_m, -a_1, \ldots, -a_m\rangle$$
$$= \langle a_1, -a_1\rangle \oplus \langle a_2, -a_2\rangle \oplus \ldots \oplus \langle a_m, -a_m\rangle$$

which is hyperbolic.
The multiplicative identity is $\langle 1\rangle = x^2$.

Example 2: $W(\mathbb{C}) \cong \mathbb{Z}_2$.
The elements are $\langle\ \rangle$ and $\langle 1\rangle$.
$\langle 1\rangle + \langle 1\rangle = \text{core}\,\langle 1, 1\rangle = \langle\ \rangle$.

Example 3: $W(\mathbb{R}) \cong \mathbb{Z}$.
The elements are $m\langle 1\rangle$ for $m \in \mathbb{Z}$.

Example 4: $W(\mathbb{Z}_3) \cong \mathbb{Z}_4$.
As for $\mathbb{R}$, non-isotropic quadratic forms have the form $m\langle 1\rangle$ for $m \in \mathbb{Z}$.
However $m\langle 1\rangle$ is isotropic if $m \geq 3$ or $m \leq -3$ since $\langle 1, 1, 1\rangle$ is isotropic.
So we need only consider $\langle -1, -1\rangle$, $\langle -1\rangle$, $\langle\ \rangle$, $\langle 1\rangle$ and $\langle 1, 1\rangle$.
Now $\langle 1, 1, 1\rangle$ being isotropic it is $\mathcal{H} \oplus \langle k\rangle$ for some k.
Equating determinants we see that $k = -1$.
Hence $\langle 1, 1, 1\rangle \cong \langle 1, -1, -1\rangle$.
By the Cancellation Theorem this gives $\langle 1, 1\rangle \cong \langle -1, -1\rangle$.
Or, we can prove this directly:

$$\langle -1, -1\rangle = \langle 2, 2\rangle$$
$$= 2x^2 + 2y^2 = (x + y)^2 + (x - y)^2 \cong \langle 1, 1\rangle.$$

Hence $W(\mathbb{Z}_3) = \{\langle\ \rangle, \langle 1\rangle, \langle -1\rangle, \langle 1, 1\rangle\}$.
It is easy to show that this ring is isomorphic to $\mathbb{Z}_4$.

Example 5: $W(\mathbb{Z}_5) \cong \mathbb{Z}_2(C_2)$
$$= \{a + bx \mid a, b \in \mathbb{Z}_2, x^2 = 1\}$$
the group ring of the cyclic group of order 2 over $\mathbb{Z}_2$,.

$\langle 1, 1\rangle$ is isotropic and hence so is $\langle 2, 2\rangle$ and any higher dimensional quadratic form containing either of them.
Hence $W(\mathbb{Z}_5) = \{\langle\ \rangle, \langle 1\rangle, \langle 2\rangle, \langle 1, 2\rangle\}$.

It can be shown that:

$$W(\mathbb{Z}_p) \cong \begin{cases} \mathbb{Z}_2(C_2) \text{ if } p \equiv 1 \pmod 4 \\ \mathbb{Z}_4 \text{ if } p \equiv 3 \pmod 4 \end{cases}.$$

Example 6: $W(\mathbb{Q})$ is infinite.