Chapter I
Foundations of Quadratic Forms

Satya Mandal

University of Kansas, Lawrence KS 66045 USA

Fall 2013

1 Quadratic Forms and Quadratic Spaces

In this course we assume all fields F have $char(F) \neq 2$.

Definition 1.1. *Let F be a field.*

1. A **quadratic form** over F is a homogeneous polynomial

$$f(X_1, X_2, \ldots, X_n) = \sum_{i,j=1}^{n} \alpha_{ij} X_i X_j \qquad \alpha_{ij} \in F.$$

This is a form in n variables and may also be called an $n-$ary quadratic form.

With $a_{ij} = \frac{\alpha_{ij}+\alpha_{ji}}{2}$ we have

$$f = \sum_{i,j=1}^{n} a_{ij} X_i X_j = \begin{pmatrix} X_1 & X_2 & \cdots & X_n \end{pmatrix} \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix} \begin{pmatrix} X_1 \\ X_2 \\ \cdots \\ X_n \end{pmatrix}$$

$$= X^t M_f X \quad where \quad X = \begin{pmatrix} X_1 \\ X_2 \\ \cdots \\ X_n \end{pmatrix}, \quad M_f = (a_{ij}) \quad is\ symmetric.$$

2. This association

$$f \longleftrightarrow M_f \ establises\ a\ bijection$$

between the set of all quadratic forms over F and the set of all symmetric $n \times n$ matrices.

3. Suppose f, g are two $n-$ary quadratic forms over F. We say f is equivalent to g (write $f \simeq g$), if there is a change of varaibles

$$\begin{pmatrix} Y_1 \\ Y_2 \\ \cdot \\ \cdot \\ \cdot \\ Y_n \end{pmatrix} = C \begin{pmatrix} X_1 \\ X_2 \\ \cdot \\ \cdot \\ \cdot \\ X_n \end{pmatrix} \qquad with \quad C \in GL_n(F)$$

such that $f(X) = g(CX) = g(Y)$. In the matrix form it means,

$$f \simeq g \Longleftrightarrow M_f = C^t M_g C$$

4. This relation $\simeq$ is an equivalence relation.

5. Example: We have

$$f = X_1^2 - X_2^2 \simeq g = X_1 X_2.$$

Proof. We do the change of variables:

$$X_1 \mapsto X_1 + X_2, \quad X_2 \mapsto X_1 - X_2 \qquad or \quad \begin{pmatrix} Y_1 \\ Y_2 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} X_1 \\ X_2 \end{pmatrix}.$$

6. Consider the vector space F^n and denote the standard basis by $e_1, e_2, \dots, e_n$. Given a quadratic form f, define

$$Q_f : F^n \longrightarrow F \qquad by \quad Q_f\left(\sum_{i=1}^{n} x_i e_i\right) = x^t M_f x \quad where \quad x = \begin{pmatrix} x_1 \\ x_2 \\ \cdots \\ x_n \end{pmatrix}.$$

This map Q_f is called the qudratic map of f.

Lemma 1.2. *Assume char$(F) \neq 2$ (as always).*

$$Q_f = Q_g \Longleftrightarrow f = g.$$

Proof. Write $M_f = (a_{ij})$, $M_g = (b_{ij})$. Suppose $Q_f = Q_g$. Then

$$a_{ii} = Q_f(e_i) = Q_g(e_i) = b_{ii}, \qquad and$$

$$\forall\ i \neq j \quad Q_f(e_i + e_j) = (1,1)\begin{pmatrix} a_{ii} & a_{ij} \\ a_{ij} & a_{jj} \end{pmatrix}\begin{pmatrix} 1 \\ 1 \end{pmatrix} = a_{ii} + a_{jj} + 2a_{ij}$$

which is

$$= Q_g(e_i + e_j) = b_{ii} + b_{jj} + 2b_{ij}. \qquad Hence \quad a_{ij} = b_{ij} \quad and \quad f = g.$$

There other way is obvious. The proof is complete. ■

Lemma 1.3. Let f be a quadratic form. Then the quadratic map has the following properties:

1. Q_f is "quadratatic" in the following sense:

$$Q_f(ax) = a^2 Q_f(x) \qquad \forall \quad x \in F^n.$$

2. Define (polarize)

$$B_f : F^n \times F^n \longrightarrow F \quad by \quad B_f(x,y) = \frac{Q_f(x+y) - Q_f(x) - Q_f(y)}{2} \quad \forall \ \ x,y \in F^n.$$

Then, B_f is a symmetric and bilinear pairing, meaning

(a) It is symmetric: $B_f(x,y) = B_f(y,x)$ for all $x, y \in F^n$.

(b) It is bilinear:

$$B_f(ax_1 + bx_1, y) = aB_f(x_1, y) + bB_f(x_2, y)$$

$$and \quad B_f(x, cy_1 + dy_2) = cB_f(x, y_1) + dB_f(x, y_2).$$

Equivalently:

$$y \mapsto B_f(*, y) \quad \text{is linear transformation from} \quad F^n \longrightarrow Hom(F^n, F).$$

3. We have ("depolarization")

$$Q_f(x) = B_f(x,x) \qquad \forall \quad x \in F^n.$$

Proof. (1) is obvious. Clearly, $B(x,y) = B(y,x)$ for all $x, y \in F^n$. Now

$$B(x,y) = \frac{(x+y)^t M_f (x+y) - x^t M_f x - y^t M_f y}{2} = x^t M_f y.$$

Rest follows. The proof is complete. ■

Remark. Four items f, M_f, Q_f, B_f are retrievable fmom each other.

1.1 Coordiante free Approach

Definition 1.4. Let V be a finite dimensional vector spave over a field F.

1. A map $B : V \times V \longrightarrow F$ is called a **symmetric bilinear pairing**, if

   (a) $B(x, y) = B(y, x) \quad \forall\ x, y \in V$,

   (b) For any fixed $x \in V$ the map

   $$B(x, *) : V \longrightarrow V \quad \textit{is linear.}$$

   Equivalently:

   $y \mapsto B(*, y)$ is linear transformation from $F^n \longrightarrow Hom(F^n, F)$.

2. A **quadratic space** is an ordered pair (V, B) where V is as above and B is a symmetric bilinear pairing.

3. Associated to a quadratic space (V, B) we define a **quadratic map**

   $$q = q_b : V \longrightarrow F \qquad \textit{by} \quad q(x) = B(x, x) \quad \forall\ x \in V.$$

   We have the following properties:

   (a) $q(ax) = a^2 q(x)$ for all $x \in V$,

   (b)
   $$2B(x, y) = q(x + y) - q(x) - q(y) \qquad \forall \quad x, y \in V.$$

   Therefore, q and B determine each other. So, we say (V, q) represents the quadratic space (V, B).

4. Given a basis $e_1, \ldots, e_n$ of V, there is a quadratic form

   $$f(X_1, \ldots, X_n) = \sum_{i,j=1}^{n} B(e_i, e_j) X_i X_j. \qquad So, \quad M_f = (B(e_i, e_j)).$$

Lemma 1.5. Suppose $e'_1, \dots, e'_n$ is another basis of V and f' be the corresponding quadratic form

$$f'(X_1, \dots, X_n) = \sum_{i,j=1}^{n} B(e'_i, e'_j) X_i X_j.$$

Then

$$M_{f'} = C^t M_f C \quad where \quad \begin{pmatrix} e'_1 \\ e'_2 \\ \cdots \\ e'_n \end{pmatrix} = C \begin{pmatrix} e_1 \\ e_2 \\ \cdots \\ e_n \end{pmatrix}$$

In particular,

$$f \simeq f' \ \ determines\ an\ equivalence\ class\ of\ quadratic\ form \quad (f_B).$$

Proof. We have

$$X^t(B(e'_i e'_j))X = X^t \left(B \left(\sum_{k=1}^{n} c_{ki} e_k, \sum_{l=1}^{n} c_{jl} e_l \right) \right) X$$

$$= X^t \left(\sum_{k,l=1}^{n} c_{ki} B\left(e_k, e_l\right) c_{lk} \right) X = X^t C^t \left(B\left(e_k, e_l\right)\right) C X$$

The proof is complete. ∎

Definition 1.6. *Suppose $(V, B), (V', B')$ are two quadratic spaces. We say they are isometric ($\simeq$), if there is a linear isomorphism*

$$\tau : V \xrightarrow{\sim} V' \quad \ni \quad B(x, y) = B'(\tau(x), \tau(y)) \quad \forall \ \ x, y \in V.$$

1. Isometry is an equivalence relation.

2. It follows,
$$(V, B) \simeq (V', B') \quad \iff \quad (f_B) \simeq (f_{B'}).$$

3. So, the association $[(V, B)] \mapsto [f_B]$ establishes an $1-1$ correspondence between the isometry classes of $n-$dimensional quadratic spaces and (to) the equivalence classes of $n-$ary quadratic forms.

Suppose (V, B) is a quadratic space (*I said some of the following before*).

1. **Notation:** We denote $V^* := Hom_F(V, F)$.

2. For any fixed x then map $B(x, *) : V \longrightarrow F$ is linear,

$$That\ means \quad B(x,*), B(*, y) \in V^* \quad \forall \quad x, y \in V.$$

3. Further, the map

$$V \longrightarrow V^* \quad sending \quad y \mapsto B(*, y) \quad is\ a\ linear\ map.$$

Proposition 1.7. Suppose (V, B) is a quadratic space and $\{e_1, \ldots, e_n\}$ is a basis of V. Let $M = (B(e_i, e_j))$ ne the associateda symmetric matrix. Then the following are equivalent:

1. M is a nonsingular matrix.

2. The map

$$V \longrightarrow V^* \quad given\ by \quad y \mapsto B(*, y) \quad is\ an\ isomorphism.$$

3. For $x \in V$,
$$B(x, y) = 0 \quad \forall\ y \in V \quad \Longrightarrow x = 0.$$

Proof. Since $\dim V = n < \infty$, we have (2) $\Longleftrightarrow$ (3). Suppose M is non-singualr. Fix $x \in V$ and assume $B(x, y) = 0 \quad \forall\ y \in V$. In particular, $B(x, e_j) = 0$ for all j. Write $x = \sum_{i=1}^n x_i e_i$. So,

$$\forall\ j \quad 0 = B(x, e_j) = \sum_{i=1}^n x_i B(e_i, e_j). \quad So, \qquad M \begin{pmatrix} x_1 \\ x_2 \\ \cdots \\ x_n \end{pmatrix} = \mathbf{0}.$$

So, $x_i = 0$ and hence $x = 0$. So, (3) is established. Now assume (3).

$$\textit{Assume} \qquad M \begin{pmatrix} x_1 \\ x_2 \\ \cdots \\ x_n \end{pmatrix} = \mathbf{0}. \qquad \textit{We prove} \qquad \begin{pmatrix} x_1 \\ x_2 \\ \cdots \\ x_n \end{pmatrix} = \mathbf{0}.$$

Write $x = \sum_{i=1}^n x_i e_i$. We have

$$\begin{pmatrix} B(x, e_1) \\ B(x, e_2) \\ \cdots \\ B(x, e_n) \end{pmatrix} = M \begin{pmatrix} x_1 \\ x_2 \\ \cdots \\ x_n \end{pmatrix} = \mathbf{0}.$$

So,

$$\forall \ \ y = \sum_{j=1}^n y_i e_i \in V \quad \textit{we have} \quad B(x, y) = \sum_{j=1}^n y_i B(x, e_j) = 0.$$

By (3), $x = 0$. The proof is complete. ∎

Definition 1.8. Suppose (V, B) is a quadratic space, satisfying (1.7), then we say (V, B) is said to be regular or nonsingular and $q_B : V \longrightarrow F$ is said to be regular or nonsingular quadratic map.

The vector space $\{0\}$ is also considered a regular quadratic space.

1.2 Sub-Quadratic Spaces

Definition 1.9. Suppose (V, B) is a quadratic space and S be a subspace.

1. Then $(S, B_{|S\times S})$ is a quadratic space.
2. The orthogonal complement of S is defined as
$$S^{\perp} = \{x \in V : B(x, S) = 0\}$$
3. The radical of (V, B) is defined to be $rad(V) = V^{\perp}$. So,
$$(V, B) \ \ is\ regular \quad \Longleftrightarrow \quad rad(V) = 0.$$

Proposition 1.10. Suppose (V, B) is a regular quadratic space and S be subspace of V. Then,

1. (Dimension formula) We have
$$\dim S + \dim S^{\perp} = \dim V.$$
2. $(S^{\perp})^{\perp} = S$.

Proof. Consider the linear isomorphism
$$\varphi : V \xrightarrow{\sim} V^* \quad \varphi(x) = B(*, x).$$
We have an exact sequence
$$0 \longrightarrow \varphi(S^{\perp}) \longrightarrow V^* \xrightarrow{\eta} S^* \longrightarrow 0 \quad where \quad \eta \quad is\ the\ restriction.$$
So,
$$\dim \varphi(S^{\perp}) + \dim S^* = \dim V^* \qquad or \quad \dim S^{\perp} + \dim S = \dim V.$$
Apply (1) twice
$$\dim (S^{\perp})^{\perp} = \dim V - \dim S^{\perp} = \dim V - (\dim V - \dim S) = \dim S.$$
Since $S \subseteq (S^{\perp})^{\perp}$ we have $S = (S^{\perp})^{\perp}$. So, (2) is established. The proof is complete. ∎

2 Diagonalization

$\dot{F}$ will denote the unitis of F.

Definition 2.1. *Suppose f is a quadratic form over F and $d \in \dot{F}$. We say f represents d is $f(x_1, \ldots, x_n) = d$ for some $(x_1, \ldots, x_n) \in F^n$. We denote*

$$D(f) = \{d \in \dot{F} : f \text{ represents } d\}.$$

Similarly, suppose (V, B) is a quadratic space, we say V **represents** *d if $q_B(v) = d$ for some $v \in V$. We denote*

$$D(f) = \{d \in \dot{F} : V \text{ represents } d\}.$$

1. Suppose $a, d \in \dot{F}$. Then,
$$d \in D(f) \iff a^2 d \in D(f), \qquad \text{because} \quad f(ax) = a^2 f(x).$$
2. So, $D(f)$ consists of union of (some) cosets of $\dot{F}$ modulo $\dot{F}^2$.
3. The group $\frac{\dot{F}}{\dot{F}^2}$ is called the group of square classes.
4. Also,
$$d \in D(f) \iff d^{-1} \in D(f); \quad \text{because} \quad d = d^2(d^{-1}).$$
5. In general, $D(f)$ may not be a group and 1 need not be in $D(f)$.
   Example: Consider $f = X_1^2 + X_2^2 + X_3^2$ over $\mathbb{Q}$. Then $1, 2, 14 \in D(f)$. But $7 = 14/2 \notin D(f)$, which is known.
6. If $D(f)$ is closed under multiplication, then $1 \in D(f)$.
   Example: Consider $f_r = \sum_{i=1}^{r} X_i^2$, over any field F. For $r = 1, 2, 3, 8$ we have $D(f_r)$ are groups.

Definition 2.2. *Let* $(V_1, B_1), (V_2, B_2)$ *be two quadratic spaces over* F*. The* **orthogonal sum** *of* $(V_1, B_1), (V_2, B_2)$ *is defined as*

$$V_1 \perp V_2 := (V, B) \quad where \quad V = V_1 \oplus V_2$$

B *is defned on* $V \times V$ *as folows:*

$$B(x_1+x_2, y_1+y_2) = B_1(x_1, y_1)+B_2(x_2, y_2) \qquad where \quad x_1, y_1 \in V_1; x_2, y_2 \in V_2.$$

1. Clearly, $B(V_1, V_2) = 0$.
2. Also,

$$q_B(x_1 + x_2) = q_{B_1}(x_1) + q_{B_2}(x_2) \qquad where \quad x_i \in V_i.$$

3. We also write $q_B = q_{B_1} \perp q_{B_2}$.
4. Example: Let $q_1(X, Y) = X^2 + XY, q_2(X, Y, Z) = XZ + YX$. Then,

$$q_1 \perp q_2(X, Y, U, V, W) = X^2 + XY + UW + VU$$

(*Note, we switch between the bilinear pairing* B *and the form* q_B*. However, we need to view* $q_B : V \longrightarrow V^*$*.*)

Definition 2.3. *For* $d \in F$ *define* $\langle d \rangle$ *to be the one dimensional quadratic space, corresponding to the quadratic form*

$$q(X) = dX^2 \quad So, \quad 2B(X, X) = q(X + X) - q(X) - q(X) = 2dX^2$$

The Representation Criteria:

Theorem 2.4. *Let* (V, B) *be a quadratic space and* $d \in \dot{F}$*. Then,*

$$d \in D(V) \Longleftrightarrow V \cong \langle d \rangle \perp (V', B') \quad \text{for some quadratic space} \quad (V', B').$$

Proof. Suppose $V \cong \langle d \rangle \perp (V', B')$. Then, $q_V(e \oplus 0) = d$, where e is the basis of $\langle d \rangle$.

Conversely, Let $d \in D(V)$. Then, $q(v) = d$ for some $v \in V$. Recall $rad(V) = V^\perp = \{y \in V : B(V, y) = 0\}$. There is a subspace W $V = V^\perp \oplus W$. It follows, $V = V^\perp \perp W$. Also, $D(V) = D(W)$ and $W^\perp = 0$. So, we assume V is regular, by replacing V by W.

Now, Fv is isometric to $\langle d \rangle$. And $Fv^\perp \cap Fv = 0$. Since $\dim Fv + \dim Fv^\perp$, we have $V = Fv \oplus Fv^\perp$. It follows $V \cong Fv \perp Fv^\perp$. The proof is complete. ■

Corollary 2.5 (2.4)**.** *Let (V, B) be a quadratic space. Then,*

$$V \cong \langle d_1 \rangle \perp \langle d_2 \rangle \perp \cdots \perp \langle d_n \rangle \quad \text{where} \quad d_i \in \dot{F}.$$

Proof. Follows by induction. ■

Notation: $\langle d_1, d_2, \ldots, d_n \rangle := \langle d_1 \rangle \perp \langle d_2 \rangle \perp \cdots \perp \langle d_n \rangle$. Also,

$$n\langle d \rangle := \langle d \rangle \perp \langle d \rangle \perp \cdots \perp \langle d \rangle$$

the orthogonal sum of n copies of $\langle d \rangle$.

Corollary 2.6 (2.5)**.** *Suppose (V, B) is a quadratic space and S is a regular subspace. Then*

1. *$V = S \perp S^\perp$*
2. *If T is a subspace of V and $V = S \perp T$ then $T = S^\perp$.*

Proof. (2) follows from (1) because $T \subseteq S^\perp$ and $\dim T = \dim S^\perp$.

Since S is regular, $0 = rad(S) = \{v \in S : B(v, S) = 0\}$. So, $S \cap S^\perp = 0$. So, we show $V = S + S^\perp$. By (2.5), S has an orthogonal basis $e_1, \ldots, e_p$. Again, by regularity (or the decomposition) $B(e_i, e_i) \neq 0$. Now for $z \in V$ write

$$y = z - \sum_{i=1}^{p} \frac{B(z, e_i)}{B(e_i, e_i)} e_i.$$

Then, $B(y, e_k) = 0$ and hence $y \in S^\perp$. So,

$$z = \sum_{i=1}^{p} \frac{B(z, e_i)}{B(e_i, e_i)} e_i + y \in S + S^\perp.$$

The proof is complete. ■

Corollary 2.7 (2.6)**.** *Suppose* (V, B) *is a regular quadratic space and* S *is a subspace. Then,* S *is regular if and only if* $V = S \perp T$ *for some subspace* T *of* V*.*

Proof. One way follows from (2.6). Suppose $V = S \perp T$. Then,

$$\forall\ v \in S, \qquad v \in rad(S) \Longrightarrow v \in rad(V) \Longrightarrow v = 0.$$

So, S is regular. The proof is complete. ∎

2.1 Determinant

Definition 2.8. *Suppose* f *is a nonsingular quadratic form. We define* **determinant** *of* f *as*

$$d(f) := \det(M_f)\dot{F}^2 \in \frac{\dot{F}}{\dot{F}^2}.$$

Caution: Do not mix up $D(f)$ and $d(f)$.

1. *Note* $f \simeq g \Longrightarrow d(f) = d(g)$*, because* $f \simeq g \Longrightarrow M_f = C^t M_g C$*.*
2. *Also,*
$$d(f_1 \perp f_2) = d(f_1)d(f_2).$$
3. *Suppose* (V, B) *is a regualr quadratic space. Then, define*
$$d(V) = d(f) \quad \textit{where } f \ \textit{ is the form wrt a basis.}$$
So, if
$$V = \langle d_1 \rangle \perp \langle d_2 \rangle \perp \cdots \langle d_n \rangle \quad \textit{then} \quad d(V) = d_1 d_2 \cdots d_n.$$

3 Hyperbolic Plane and Hyperbolic Spaces

Definition 3.1. Suppose (V, B) is a quadratic space (*and* q *be the "quadratic" map*).

1. A nonzero element $v \in V$ is said to be an isotropic vector, if $B(v, v) = 0$ (i.e. $q(v) = 0$). Otherwise v is called anisotropic.

2. A quadratic space (V, B) is called isotropic if it contains an (nonzero) isotropic vector.

3. (V, B) said to be anisotropic, if V contains no isotropic element.

4. (V, B) is called totally isotropic, if all its nonzero vectors are isotropic. contains an (nonzero) isotropic vector.

5. *The author avoids defining the zero vector as one of them, he calls it "fruitless debate".*

6. *The zero dimensional space is "technically"* **anisotropic** *space.*

Lemma 3.2. Suppose (V, B) is an anisotropic quadratic space. Then, V is regular.

Proof. We prove $V^{\perp} = 0$. Suppose $v \in V^{\perp}$. Then, $B(v, v) = 0$. So, $v = 0$. ■

Theorem 3.3 (3.2)**.** Suppose (V, B) is two dimensional space. The following are equivalent:

1. V is regular and isotropic.

2. V is regular, with $d(V) = -1\dot{F}^2$.

3. V is isotrometric to $\langle 1, -1\rangle$.

4. V corresponds to the equivalence class of binary quadratic form X_1X_2.

Proof. (3) $\iff$ (4) was established in §1.

((1) $\implies$ (2)): By (2.5) $V = \langle d_1 \rangle \perp \langle d_2 \rangle$. Write $V = Fe_1 + Fe_2$, with $q(e_i) = d_i$ for some $e_1, e_2 \in V$. Since V is regular, $d_1 \neq 0, d_2 \neq 0$. Let $v = ae_1 + be_2$ be isotropic. We assume $a \neq 0$. Then,

$$0 = \langle v, v \rangle = a^2 d_1 + b^2 d_2. \quad \textit{The determinant,} \quad d(V) = d_1 d_2 = -a^{-2} b^2 d_2^2 \dot{F}^2 = -1\dot{F}^2.$$

((2) $\implies$ (3)): We have a diagonalization

$$V = \langle (Fe_1, d_1) \rangle \perp \langle (Fe_2, d_2) \rangle = \langle d_1 \rangle \perp \langle d_2 \rangle, \quad \textit{where} \quad V = Fe_1 + Fe_2.$$

By hypothesis, $d_1 d_2 = -u^2$. Define

$$\tau : (V, B) \xrightarrow{\sim} \langle (Fe_1, d_1) \rangle \perp \langle (Fe_2, -d_1) \rangle \quad \textit{by} \quad \begin{cases} \tau(e_1) & = e_1 \\ \tau(e_2) & = \frac{d_1^2 e_2}{u^2}. \end{cases}$$

Then $B(\tau(e_i), \tau(e_j)) = B(e_i, e_j)$. So, we will write

$(V, B) = \langle (Fe_1, a) \rangle \perp \langle (Fe_2, -a) \rangle$.

Claim: $D(V, B) = F$. To see this, let $\alpha \in F$, the system

$$\begin{cases} x & +y & = a^{-1}\alpha \\ x & -y & = 1 \end{cases} \quad \textit{has solutions} \quad x = b, \ y = c.$$

Then,

$$\langle be_1 + ce_2, be_1 + ce_2 \rangle = a(b^2 - c^2) = a(b + c)(b - c) = \alpha.$$

So, $\alpha \in D(V, B)$. In particular, (V, B) represents 1. By the representation criteria 2.4,

$$(V, B) \cong \langle (Fv, 1) \rangle \perp \langle (Fw, -u^2) \rangle \cong \langle (Fv, 1) \rangle \perp \langle (Fw, -1) \rangle.$$

((3) $\implies$ (1)): Obvious.

Remark. Note $\langle Fv, a \rangle \ncong \langle Fv, 1 \rangle$, unless $a \in \dot{F}^2$.

Definition 3.4. The isometry class of two dimensional quadratic spaces satifying (3.3) is called the **Hyperbolic form** or plane. With respect to the standard basis the symmetric matrix is:

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

1. The Hyperbolic plane is denoted by $\mathbb{H}$.

2. The Hyperbolic plane is considered very basic. It is "trivial" (*loosely speaking*) in the category of quadratic spaces over F, in the sense the one dimensional space is, in the category of vector spaces over F.

3. An orthogonal sum $\mathbb{H} \perp \mathbb{H} \perp \cdots \perp \mathbb{H}$ of hyperbolic planes will be called a Hyperbolic space. The corresponding quadratic space can be written as (*i. e. with respect to some choice of basis*)

$$q = \sum_{i=1}^{m} (X_{2m-1}^2 - X_{2m}^2) \quad or \quad q = \sum_{i=1}^{m} X_{2m-1} X_{2m}.$$

4. **Looking Forward:** We will define the Witt group $W(F)$, in Chapter II. $W(F)$ is generated by all the isometry classes of quadratic spaces, where the hyperbolic spaces would represent the zero of $W(F)$.

Definition 3.5. A quadratic form (or space) is called **universal**, if it represents all the nonzero elements of F.

Theorem 3.6. Let (V, B) be a regular quadratic space. Then,

1. Every totally isotropic subspace $U \subseteq V$ with $\dim U = r > 0$ is contained in a hyperbolic subspace $T \subseteq V$ with $\dim T = 2r$.

2. V is isotropic if and only if V contains a hyperbolic plane (necessarily as an orthogonal sum by (2.6)).

3. V is isotropic $\Longrightarrow \quad V$ is universal.

Proof. (3) is obvious, because $\mathbb{H}$ is given by $q = X_1X_2$. Also, (2) follows from (1) with $r = 1$.

Now we prove (1). Let $v_1, \ldots, v_r$ be a basis of U and $S = \sum_{j=2}^{r} Fv_j$. We have $U^\perp \subseteq S^\perp$. Also, since V is regular, by the dimension formula (1.10),

$$\dim S^\perp = \dim V - \dim S > \dim V - \dim U = \dim U^\perp.$$

So, we pick $y \in \dim S^\perp \setminus U^\perp$. So, $B(v_1, y) \neq 0$. Write $H_1 = Fv_1 + Fy$. The determinant

$$d(H_1) = \begin{vmatrix} 0 & B(v_1, y) \\ B(v_1, y) & B(y, y) \end{vmatrix} \cdot \dot{F}^2 = -B(v_1, y)^2 \cdot \dot{F}^2 = -1 \cdot \dot{F}^2.$$

By (3.3), $H_1 \cong \mathbb{H}$. By (2.6), $V \cong H_1 \perp H_1^\perp$. In fact, $B(v_i, v_j) = 0$ for all i, j, by lemma 3.7. Hence, if follows $S \subseteq H_1^\perp$. Now, the proof is complete by induction. The proof is complete. ∎

Lemma 3.7. *Let (T, B) be a totally isotopic quadratatic space. Then $B(u, v) = 0$ for all $u, v \in T$.*

Proof. It follows from

$$0 = B(u + v, u + v) = B(u, u) + B(v, v) + 2B(u, v).$$

The proof is complete. ∎

Exercise.

1. Prove any element in F is difference of two squares (*assume* $1/2 \in F$, *as always*).

Corollary 3.8 (First Representation Theorem). *Let q be a regular quadratic form, and $d \in \dot{F}$. Then,*

$$d \in D(q) \Longleftrightarrow q \perp \langle -d \rangle \quad \textit{is isotropic.}$$

Proof. Assume $d \in D(q)$. So, there is a $v \in V$ such that $q(v) = d$. So, denote $Q = q \perp \langle -d \rangle$. So, $Q(v, 1) = d - d = 0$. Conversely, assume $Q = q \perp \langle -d \rangle$ is isotropic. Then, by hypothesis, $Q(v) = 0$. Write $v = (v_0, \lambda)$. This means

$$Q(v) = q(v_0) - \lambda^2 d = 0. \quad So, \quad q\left(\frac{v_0}{\lambda}\right) = d.$$

The proof is complete. ∎

Corollary 3.9. *Let q_1, q_2 be regular forms of positive dimension. Then,*

$$q_1 \perp q_2 \quad \textit{is isotropic} \quad \Longleftrightarrow \quad D(q_1) \cap -D(q_2) \neq \phi.$$

Proof. Suppose $q_1 \perp q_2$ is isotropic. If q_1 is isotropic, then $D(q_1) = \dot{F}$ and we are done. So, we assume q_1, q_2 are anisotropic. We have, $q_1(v_1) + q_2(v_2) = 0$ for some nonzero $v_1 \in V_1, v_2 \in V_2$. Since $q_1(v_1) \neq 0, q_2(v_2) \neq 0$, $q_1(v_1) = -q_2(v_2) \in D(q_1) \cap -D(q_2)$.

Conversely, suppose $\lambda \in D(q_1) \cap -D(q_2)$. If q_1 q_2 is isotropic, we are done. Assume they are anisotropic and $q_1(v_1) = -q_2(v_2) = \lambda \neq 0$ for some $v_1 \in V_1, v_2 \in V_2$. So, $q_1(v_1) + q_2(v_2) = 0$. So, $q_1 \perp q_2$ is isotropic. The proof is complete. ∎

Corollary 3.10. *Let $r > 0$ be an integer. Then, the following are equivalent.*

1. *Any regular form of dimension r, over F is universal.*
2. *Any regular form of dimension $r + 1$, over F is isotropic.*

Proof. Supose (1) holds and q be a quadratic form of dimension $r + 1$. We can assume q is anisotropic. By diagonalization, we can assume $q = q_0 \perp \langle d \rangle$, for some $d \neq 0$. Since, q_0 is universal, $q_0(v) = -d$ for some $v \in V(q_0)$. So, $q(v, 1) = 0$. Conversely, assume (2) holds and q is a regular a quadratic form of dimension r. Let $d \in \dot{F}$. By hypothesis $q \perp \langle -d \rangle$ is isotropic. By (3.10) $d \in D(q)$. The proof is complete. ∎

4 Decomposition and Cancellation

We prove some fundamental theorem - namely Decompostion and the Cancellation. Much of it is due to Witt (1937).

Theorem 4.1 (Witt's Decompostion). *Suppose (V,q) is a quadratic space. Then,*

$$(V,q) \cong (V_t, q_t) \perp (V_h, q_h) \perp (V_a, q_a) \quad \textit{is an isometry},$$

where V_t is totally isotropic, V_h is hyperbolic sspace, V_a is anisotropic and q_t, q_h, q_a are restrictions of q. Furhter, isometry types of V_t, V_h, V_a are all uniquely determined.

Proof. Let V_0 be a subspace of V such that

$$V = V_0 \oplus rad(V). \quad It\ follows \quad V = V_0 \perp rad(V)$$

Take $V_t = rad(V)$. It also follows V_t is totally isotropic.

Since $V_0^{\perp} = V^{\perp}$, V_0 is regular. If V_0 contains an isotropic vector we can write $V_0 = \mathbb{H} \perp V_1$. Inductively, we have

$$V_0 = (\mathbb{H} \perp \mathbb{H} \perp \cdots \perp \mathbb{H}) \perp V_a.$$

where V_a is anisotropic. With $V_h = (\mathbb{H} \perp \mathbb{H} \perp \cdots \perp \mathbb{H})$, we have

$$V = V_t \perp V_h \perp V_a \qquad \textit{as required}.$$

To prove the uniqueness part, we use the Cancellation theorem 4.2.

Proof of uniqueness: Suppose

$$V \cong V_t \perp V_h \perp V_a \cong V_t' \perp V_h' \perp V_a',$$

where V_t, V_t' are totally isotropic, V_h, V_h' are hyperbolic spaces and V_a, V_a' are anisotropic. Taking the radical on both sides, we get

$$V_t \cong rad(V_t \perp V_h \perp V_a) \cong rad(V_t' \perp V_h' \perp V_a') \cong V_t'.$$

So, by (4.2), $V_h \perp V_a \cong V_h' \perp V_a'$.

Now let $V_h = m\mathbb{H}, V_h' = n\mathbb{H}$ (*direct sum of m or n copies of* $\mathbb{H}$). So, we have $m\mathbb{H} \perp V_a \cong n\mathbb{H} \perp V_a'$. Assume $m \leq n$. By (4.2), cancelling $\mathbb{H}$, one by one, we get $V_a \cong V_a' \perp (n-m)\mathbb{H}$. Since left side in anisotropic, $m = n$ and $V_a \cong V_a'$. So, the uniqueness is established.

The proof is complete. ■

Theorem 4.2 (Cancellation). *Let q, q_1, q_2 be three quadratic forms. Then,*

$$q_1 \perp q \cong q_2 \perp q \quad \Longrightarrow \quad q_1 \cong q_2.$$

Proof. Comes later. ■

Definition 4.3. Given a quadratic form (V, q), by (4.1), we have $(V, q) \cong V_t \perp V_a \perp m\mathbb{H}$. Here $m = \frac{\dim V_h}{2}$ is uniquely determined. Define

1. Define Witt index of $V := m = \frac{\dim V_h}{2}$.

2. V_a is called the **anisotropic** part of V.

Corollary 4.4. *Suppose (V, q) is a regular quadratic space. The Witt index of V is equals the dimension of any maximal totally isotopic subspace of V.*

Proof. Since it is regular, $V_t = 0$ and $V \cong V_h \perp V_a$. Suppose U is a maximal totally isotopic subspace of V and $\dim U = r$. By theorem 3.6, there is a hyperbolic space $T \supseteq U$ with $\dim T = 2r$. Since T is also regular, by (2.6) we have, $V = T \perp T^{\perp}$. By maximality of U, $T^{\perp}$ is anisotropic. By uniqueness, we have $T \cong V_h$. So,

$$m = \frac{\dim V_h}{2} = \frac{2r}{2} = r.$$

The proof is complete. ■

4.1 Reflection

We consider reflections and projections in any inner product spaces. However, now the field F need not be $\mathbb{R}$ *or* $\mathbb{C}$. In any case, we define reflection in the the same way for quadratic spaces.

Suppose (V, B, q) be any quadratic space.

1. The group (is it so?!) of isomaries of V will be denoted by $O_q(V) = O(V)$. This is also called the orthogonal group.

2. Fix an anisotropic vector $y \in V$. Define

$$\tau_y : V \longrightarrow V \quad by \quad \tau_y(x) = x - \frac{2B(x,y)}{B(y,y)}y$$

Then τ_y is a linear transformation. More interestigly, it has the folwoing properties:

   (a) $\tau_y(y) = -y$.
   (b) For all $x \in (Fy)^\perp$ we have $\tau_y(x) = x$.
   (c) Verbally, τ_y leaves $(Fy)^\perp$ pointwise fixed and sends $y \mapsto -y$.
   (d) So, for $y \in V_a$it follows $\tau_y^2 = id$. We say τ_y is an involution.
   (e) In fact, $\tau_y \in O_q(V)$, which follows from the calculation:

$$B(\tau_y(x), \tau_y(x')) = B\left(x - \frac{2B(x,y)}{B(y,y)}y, x' - \frac{2B(x',y)}{B(y,y)}y\right)$$

$$= B(x,x') - \frac{4B(x,y)B(x',y)}{B(y,y)} + \frac{4B(x,y)B(x',y)}{B(y,y)}B(y,y) = B(x,x').$$

   (f) $\det(\tau_y) = -1$. To see this let $e_1 = y, e_2, \ldots, e_N$ of V with $e_i \in (Fy)^\perp$ for all $i \neq 2$. By diagonalizing, $(Fy)^\perp$ we can assume $B(e_i, e_j) = 0$ for all $i \neq j$. The matrix of q with respect tothis basis is:

$$\begin{pmatrix} -1 & \mathbf{0} \\ \mathbf{0}^t & I_{N-1} \end{pmatrix}. \qquad So, \quad \det(\tau_y) = -1.$$

   This is not to be confused with $\det(V)$.

   (g) τ_y is called a **hyperplane reflection**. It is a reflection against $(Fy)^\perp$.

3. **Remark:** For

$$\sigma \in O(V), \quad we\ have \quad \sigma\tau_y\sigma^{-1} = \tau_{\sigma(y)}.$$

So, set of hyperplane reflections $\{\tau_y : q(y) \neq 0\}$ is closed under conjugation in $O(V)$. **Proof.** Easy checking. ∎

Proof of Cancellation Theorem 4.2: Suppose $q \perp q_1 \cong q \perp q_2$.

1. **Case q is totally isotopic and q_1 is regular:** Let M_i be the symmetric matrices of q_i, for $i = 1, 2$. Then, the symmetrices of $q \perp q_i$ are
$$\begin{pmatrix} 0 & 0 \\ 0 & M_i \end{pmatrix}.$$
Since $q \perp q_1 \cong q \perp q_2$
$$\exists\, E = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \quad \ni \quad \begin{pmatrix} 0 & 0 \\ 0 & M_1 \end{pmatrix} = E^t \begin{pmatrix} 0 & 0 \\ 0 & M_2 \end{pmatrix} E = \begin{pmatrix} 0 & 0 \\ 0 & D^t M_2 D \end{pmatrix}.$$
Since M_1 is nonsingular, so is D and $q_1 \cong q_2$.

2. **Cancellation holds when q is totally isotopic:** Diagolalize q_1, q_2. Since the symmetric matrix of q is zero, using $q \perp q_1 \cong q \perp q_2$, we see both q_1, q_2 has same number of zeros, say r, in their diagonalization. So, $q_1 = r\langle 0\rangle \perp q_1'$, $q_2 = r\langle 0\rangle \perp q_2'$. So, we have
$$q \perp r\langle 0\rangle \perp q_1' \cong q \perp r\langle 0\rangle \perp q_2'.$$
Since, q_1 is reqular, by the first case, $q_1' \cong q_2'$. So, $q_1 \cong q_2$.

3. **The General case:** In this case q is not necessarily totlally isotopic. By diagonalization $q \cong \langle a_1, \ldots, a_n\rangle$. Using induction, we canassume $n = 1$. If $a_1 = 0$, the theorem follows from above. So, we assume $a_1 \neq 0$. We have $\langle a_1\rangle \perp q_1 \cong \langle a_1\rangle \perp q_2$. Let $\varphi : \langle a_1\rangle \perp q_1 \xrightarrow{\sim} \langle a_1\rangle \perp q_2$ be an isometry. Write $\varphi : \langle a_1\rangle = Fe_0$ and $z = \varphi(e_0)$ By theorem 4.5 there is an isometry $\psi \in O(V)$ such that $\psi(z) = e_0$. Let $\tau = \psi\varphi$. Then $\tau(e_0) = e_0$. In fact
$$\tau = \begin{pmatrix} 1 & 0 \\ \lambda e_0 & \eta \end{pmatrix} \quad where \quad \lambda \in V^*, \quad \eta \in End(V).$$
Claim: $\lambda = 0$. To see this let $x \in V$. Then,
$$0 = B(e_0, x) = B(\psi(e_0), \psi(x)) = B(e_0, \lambda(x)e_0 + x) = \lambda(x)a_1.$$
Since $a_1 \neq 0$, we have $\lambda(x) = 0$. So, the claim is established. Therefore,
$$\tau = \begin{pmatrix} 1 & 0 \\ 0 & \eta \end{pmatrix}.$$

For $x, y \in V$, we have

$$B_1(x, y) = B(\tau(x), \tau(y)) = B(\eta(x), \eta(y))$$

So, η is isometry.

Theorem 4.5. *Let (V, q) be a quadratic space and $x.y \in V$ be such that $q(x) = q(y) \neq 0$. Then, ther is an isomtry such that $\tau(x) = y$.*

Proof. Geometrically, reflection around $F(x-y)^{\perp}$ would do. But we need $q(x-y) \neq 0$. We compute

$$q(x+y)+q(x-y) = B(x+y, x+y)+B(x-y, x-y) = 2B(x, x)+2B(y, y) = 4q(x) \neq 0.$$

So, either $q(x+y) \neq 0$ or $q(x-y) \neq 0$. If needed, we replace y be $-y$ and assume $q(x-y) \neq 0$. Also,

$$q(x-y) = B(x-y, x-y) = B(x, x) - 2B(x, y) + B(y, y)$$

$$= 2(B(x, x) - B(x, y)) = 2B(x, x-y).$$

So, we have

$$\tau_{x-y}(x) = x - \frac{2B(x, x-y)}{q(x-y)}(x-y) = x - (x-y) = y.$$

The proof is complete. ∎

5 Witt's Chain Equivalence Theorem

In this section we exploit binary forms.

Proposition 5.1. *Let $q = \langle a, b \rangle$, $q' = \langle c, d \rangle$, be two binary regular forms. Then, $q \cong q'$ if and only if $d(q) = d(q')$ and q, q' represent a common element $e \in \dot{F}$.*

Proof. Suppose $q \cong q'$. Let $A = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$ be the symmetric matrix of q and $B = \begin{pmatrix} c & 0 \\ 0 & d \end{pmatrix}$ be the symmetric matrix of q'. So, $A = E^t B E$ and $\det A = \det E^2 \det B$. So, $d(q) = d(q')$. Write $E = \begin{pmatrix} x & y \\ z & w \end{pmatrix}$. Then,

$$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} = \begin{pmatrix} x & z \\ y & w \end{pmatrix} \begin{pmatrix} c & 0 \\ 0 & d \end{pmatrix} \begin{pmatrix} x & y \\ z & w \end{pmatrix} = \begin{pmatrix} cx^2 + dz^2 & * \\ * & cy^2 + dw^2 \end{pmatrix}$$

So,

$$e := a = q(1, 0) = cx^2 + dz^2 = q'(x^2, z^2).$$

is the common element represented.

Conversely, let $e \in D(q) \cap D(q')$. By Representation criteria $q \cong \langle e, e' \rangle$. Taking determinants $ee' = abt^2$. So,

$$q \cong \langle e, e' \rangle \cong \langle e, \frac{abt^2}{e} \rangle \cong \langle e, abe \rangle. \quad Similarly, \quad q' \cong \langle e, cde \rangle.$$

Again, $ab = cdu^2$. The proof is complete. ∎

Definition 5.2. Suppose $q = \langle a_1, \ldots, a_n \rangle$, $q' = \langle b_1, \ldots, b_n \rangle$ two diagonal forms of dimension n.

1. We say q, q' are simply-equivalent, if there is i, j (possibly equal) such that
   (a) $\langle a_i, a_j \rangle \cong \langle b_i, b_j \rangle$,
   (b) and $a_k = b_k$ for all $k \neq i, j$.

2. We say q, q' are chain equivalent, if there exists a sequence

$$q_0 = q, q_1, \ldots, q_{m-1}, q_m = q' \quad \ni \quad q_i, q_{i+1} \quad \textit{are simply equivalent.}$$

In this case, we write $q \approx q'$.

3. Clearly, $q \approx q' \Longrightarrow q \cong q'$.

The converse:

Theorem 5.3 (Chain Equivalence Theorem)**.** *Suppose $f = \langle a_1, \ldots, a_n \rangle$, $g = \langle b_1, \ldots, b_n \rangle$ two diagonal forms of dimension n. Then,*

$$f \cong g \Longleftrightarrow f \approx g.$$

Proof. We only prove $\Longrightarrow$: For a permuation $\sigma \in S_n$, define $f^\sigma = \langle a_{\sigma(1)}, \ldots, a_{\sigma(n)} \rangle$. Since S_n is generated by transpostions, we have $f^\sigma \approx f$, because

$$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} b & 0 \\ 0 & a \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Using this we can assume all the zero entries in f, g are at the end. Since $f \cong g$, it follows they have same number of zeros. By cancellation, we can assume both f, g are regular. So, $a_i \neq 0, b \neq 0$ for all i.

Without loss we assume $n \geq 3$ and we will use induction. Since $f \approx g$, we have $D(f) = D(g)$. So, $b_1 \in D(f)$.

Claim: $f \approx \langle b_1, c_2, \ldots, c_n \rangle$ for some $c_i \neq 0$. To see this consider the set

$$\mathcal{F} = \{f' = \langle c_1, c_2, \ldots, c_n \rangle : f \approx f'\}$$

Let $h = \langle c_1, c_2, \ldots, c_n \rangle \in \mathcal{F}$ the subform $\langle c_1, c_2, \ldots, c_p \rangle$ represent b_1, with $p \leq n$ minimum. We will prove $p = 1$. Suppose $p \geq 2$. We have

$$b_1 = \sum_{i=1}^{p} c_i x_i^2.$$

Since p is minimal, $d = c_1 x_1^2 + c_2 x_2^2 \neq 0$. By Representation theorem 2.4, $\langle c_1, c_2 \rangle \cong \langle d, c_1 c_2 d \rangle$ (*the 2nd coordiante is obtained by adjusting determinant*). Therefore,

$$f \approx h = \langle c_1, c_2, c_3 \ldots, c_n \rangle \approx \langle d, c_1 c_2 d, c_3, \ldots, c_n \rangle \approx \langle d, c_3, \ldots, c_n, c_1 c_2 d \rangle.$$

Now, first $p-1$ terms represents b_1. Which is a contradiction and $p=1$.

So, $h = \langle b_1, c_2, \dots, c_n \rangle$ for some c_i. It follows

$\langle b_1, c_2, \dots, c_n \rangle \cong \langle b_1, b_2, \dots, b_n \rangle$. *By cancellation* $\langle c_2, \dots, c_n \rangle \cong \langle b_2, \dots, b_n \rangle$.

By induction

$$\langle c_2, \dots, c_n \rangle \approx \langle b_2, \dots, b_n \rangle.$$

Therefore,

$$f \approx \langle b_1, c_2, \dots, c_n \rangle \approx \langle b_1, b_2, \dots, b_n \rangle = g.$$

The proof is complete. ■

6 Tensor Product of Quadratic Spaces

Lam call it Kronecker Tensor Product of Quadratic Spaces.

Definition 6.1. Let $(V_1, B_1, q_1), (V_2, B_2, q_2)$ be quadratic forms over F, with $\dim V_1 = m, \dim V_2 = n$. Write $V = V_1 \otimes V_2$. Define

$$B : V \times V \longrightarrow F \qquad by \quad B(v_1 \otimes v_2, v_1' \otimes v_2') = B_1(v_1, v_1')B_2(v_2, v_2') \quad \forall vi, v_i' \in V_i.$$

It is easy to see that B extends to a symmetric bilinear pairing on $V \times V$.

Method: To do this check it extends to a map $V \longrightarrow V^*$, which I skip (Exercise.

So, (V, B) is a quadratic space with $\dim V = mn$. Let $q = q_B$. Obviously,

$$q(v_1 \otimes v_2) = q_1(v_1)q_2(v_2). \qquad We\ denote \quad q = q_1 \otimes q_2 \quad or \quad = q_1 q_2.$$

Now we coordinatize. Suppose $\{e_1, \ldots, e_m\}$ is a basis of V_1 and $\{\epsilon_1, \ldots, \epsilon_n\}$ is a basis of V_1,. Let $a_{ij} = B_1(e_i, e_j)$ and $M = (a_{ij})$. Also, let $b_{lk} = B_2(\epsilon_l, \epsilon_k)$ and $N = (a_{lk})$. We have

$$\{e_1 \otimes \epsilon_1, \ldots, e_1 \otimes \epsilon_n; \ldots; e_m \otimes \epsilon_1, \ldots, e_m \otimes \epsilon_n\} \quad is\ a\ basis\ of \quad V.$$

With respect this basis, the symmetric matrix of B is

$$\begin{pmatrix} a_{11}N & a_{12}N & \cdots & a_{1m}N \\ a_{21}N & a_{22}N & \cdots & a_{2m}N \\ a_{31}N & a_{32}N & \cdots & a_{3m}N \\ \cdots & \cdots & \cdots & \cdots \\ a_{m1}N & a_{m2}N & \cdots & a_{mm}N \end{pmatrix}.$$ This is also called the Kronecker product.

This Kronecker product of quadratatic forms satifies the following:

1. (Commutativity): $q_1 \otimes q_2 \cong q_2 \otimes q_1$.
2. (Associativity) $(q_1 \otimes q_2) \otimes q_3 \cong q_1 \otimes (q_2 \otimes q_3)$.
3. (Distributivity): $(q \otimes (q_1 \perp q_2) \cong (q \otimes q_1) \perp (q \otimes q_2)$.

4. For diagonal forms, distributivity takes the shape:

$$\langle a_1, \ldots, a_m\rangle \otimes \langle b_1, \ldots, b_n\rangle \cong \langle a_1b_1, \ldots, a_1b_n; \ldots; a_mb_1, \ldots, a_mb_n\rangle$$

Notation: For a nonnegetative integer r and a quadratic form, denote

$$r \cdot f = rf := f \perp \ldots \perp f \qquad\qquad (r\ copies).$$

Corollary 6.2. *Suppose q is a regular quadratic form. Then, $q \otimes \mathbb{H} \cong (\dim q)\mathbb{H}$.*

Proof. We diagonalize $q = \langle a_1, \ldots, a_m\rangle$, with $a_i \neq 0$. Then,

$$q \otimes \mathbb{H} = \langle a_1, \ldots, a_m\rangle \otimes \mathbb{H} \cong (\langle a_1\rangle\mathbb{H}) \perp \cdots \perp (\langle a_m\rangle\mathbb{H}) \cong m\mathbb{H}$$

The proof is complete. ∎

7 Generation of $O(V)$ by reflections

Recall, the group $O(V)$ of all isometries $\sigma : V \xrightarrow{\sim} V$ is called orthogonal group. We will prove that the orthogonal group $O(V)$ of a regular quadratic space is generated by reflections.

Theorem 7.1 (Cartan-Dieudonné). *Suppose (V, B, q) is regular quadratic space, with $\dim V = n$. Then, every isometry $\sigma \in O_q(V)$ is a product of at most n hyperplane reflections.*

The proof comes after a few consequences.

Corollary 7.2. *Use the notations as in (7.1). Suppose $\sigma \in O_q(V)$ is product of n hyperplane reflections. Then, the first (or similarly the last) reflection in the product can be choosen arbitrarily.*

Proof. Suppose $\sigma = \tau_1\tau_2 \cdots \tau_n$ where τ_i are hyperplane reflections. Let τ be any hyperplane reflection. By (7.1), $\tau\sigma = \tau_2' \cdots \tau_r'$ where $r \leq n+1$. We have $\det(\sigma) = (-1)^n = -\det(\tau\sigma) = (-1)^r$. So, $n - r = 2k$ for some k. Since $r \leq n+1$, we have $r \leq n$. We have $\tau^2 = 1$. So,

$$\sigma = \tau^2\sigma = \tau(\tau_2' \cdots \tau_r') \quad \textit{as desired.}$$

The proof is complete. ■

Notation. Denote $SO(V) = \{\sigma \in O(V) : \det\sigma = 1\}$. Here "S" is for "Special". Recall the analogy: $GL_n(F)$ and $SL_n(F)$. Here "GL" abbreviates "General Linear".

Corollary 7.3. *If $\dim V = 2$, then every isometry with determinant -1 is a reflection. If $\dim V \leq 3$, then every $\sigma \in SO(V)$ is product of two reflections.*

Proof. It follows immediately from (7.1), by comparing determinants. ■

Corollary 7.4. *($\dim V = n$). Let $\sigma \in O(V)$. Define*

$$L(\sigma) = \{v \in V : \sigma(v) = v\}$$

the **fixed subspace** *of σ.*

1. *If σ is product of r reflections ($r \leq n$), then $\dim L(\sigma) \geq n - r$.*

2. *If $L(\sigma) = 0$, then σ cannot be written as product of less than n reflections.*

Proof. (2) follows from (1). Now suppose, $\sigma = \tau_1 \cdots \tau_r$, where τ_i are reflections. Recall $\dim L(\tau_i) = n - 1$. Then, $L(\tau_1) \cap \cdots \cap L(\tau_r) \subseteq L(\sigma)$. But $\dim(L(\tau_1) \cap \cdots \cap L(\tau_r)) \geq n - r$. The proof is complete. ∎

Exercise. Give a proof of $\dim(L(\tau_1) \cap \cdots \cap L(\tau_r)) \geq n - r$. Follwing exact sequence helps:

$$0 \longrightarrow V \cap W \longrightarrow V \oplus W \longrightarrow V + W \longrightarrow 0 \quad \text{where V, W are subspaces of U.}$$

Notations. For $\sigma \in O(V)$ define

1. $\tilde{\sigma} = \sigma - 1_V$.

7.1 Proof of theorem 7.1

We proceed to prove theorem 7.1.

Lemma 7.5. *We have $L(\sigma) = Im(\tilde{\sigma})^{\perp}$.*

Proof. Let $v \in L(\sigma)$. So, $\sigma(v) = v$. For $w \in V$, we have

$$B(v, \tilde{\sigma}(w)) = B(v, \sigma(w) - w) = B(v, \sigma(w)) - B(v, w) = B(\sigma(v), \sigma(w)) - B(v, w) = 0.$$

So, $L(\sigma) \subseteq Im(\tilde{\sigma})^{\perp}$. Now, let $v \in Im(\tilde{\sigma})^{\perp}$. For $w \in V$ we have

$$B(\sigma(v) - v, \sigma(w)) = B(\sigma(v), \sigma(w)) - B(v, \sigma(w)) = B(v, w) - B(v, \sigma(w)) = -B(v, \tilde{\sigma}(w)) = 0.$$

Replacing $\sigma(w)$ by w, we get $\sigma(v) - v \in rad(V) = 0$. So, $v \in L(\sigma)$. So, $Im(\tilde{\sigma})^{\perp} \subseteq L(\sigma)$. The proof is complete. ∎

Remark. It is easy to see, for a subspace W of a quadratic space, (W, B) is totally isotropic if and only if $W \subseteq W^{\perp}$.

Corollary 7.6. *Two things:*

1. $(L(\sigma))^{\perp} = Im(\tilde{\sigma})$.

2. *Also,*
$$\tilde{\sigma}^2 = 0 \Longleftrightarrow Im(\tilde{\sigma}) \quad \textit{is totally isotropic.}$$

Proof. By (7.5), (1) follows by taking $\perp$. Now, suppose $\tilde{\sigma}^2 = 0$. We have $Im(\tilde{\sigma})$ is totally isotropic if and only if
$$Im(\tilde{\sigma}) \subseteq Im(\tilde{\sigma})^{\perp} = L(\sigma) := \ker(\tilde{\sigma}) \quad \textit{by } (7.5) \Longleftrightarrow \tilde{\sigma}^2 = 0.$$
The proof is complete. ■

Corollary 7.7. *Let $w \in V$. Then,*
$$\tilde{\sigma}(w) \perp \tilde{\sigma}(w) \Longleftrightarrow \tilde{\sigma}(w) \perp w.$$

Proof. We have
$$B(\tilde{\sigma}(w), \tilde{\sigma}(w)) = B(\sigma(w)-w, \sigma(w)-w) = B(\sigma(w), \sigma(w)) - 2B(\sigma(w), w) + B(w, w)$$
$$= 2B(w, w) - 2B(\sigma(w), w) = 2B(w - \sigma(w), w) = -2B(\tilde{\sigma}(w), w).$$
The proof is complete. ■.

Corollary 7.8. *Suppose $\tilde{\sigma}^2 \neq 0$. Then,*

1. *$\exists$ an anisotropic vector $w \neq 0$ such that $z = \tilde{\sigma}(w)$ is anisotropic or zero.*

2. *In case $z \neq 0$, and $\sigma_1 = \tau_z \sigma$, then $w \in L(\sigma_1)$.*

Proof. Will come later, because it is technical. ■

Proof of (7.1): We use induction on $n = \dim V$. If $n = 1$ then $O(V) = \{\pm 1\}$, where -1 represents the reflection $x \mapsto -x$. (Prove it). So, assume $n > 1$ and the theorem holds for all regular forms of dimension less than n. Now suppose $\sigma \in O(V)$. We prove by contrapositive. So, assume σ does not satisfy the theorem: this means either it is not product of reflections or it is a product of more than n reflections. We claim $\tilde{\sigma}^2 = 0$. If not, by (7.8), there is a $w \in V$ as stated.

1. Assume $z = \tilde{\sigma}(w) = 0$. Then, $\sigma(w) = w$. It follows $\sigma((Fw)^{\perp}) \subseteq (Fw)^{\perp}$. So, σ induces an isometry on $(Fw)^{\perp}$. So, $\sigma|_{(Fw)^{\perp}} = \tau_1 \cdots \tau_r$ with $r \leq n-1$ and $\tau_i \in O((Fw)^{\perp})$ are reflections. Extend τ_i to V by sending $w \mapsto w$, which we continute to denote by τ_i. The extensions are also reflections. So, σ itself is product of $r \leq n-1$ reflections. This is a contradiction.

2. Now, assume $z = \tilde{(\sigma)}(w) \neq 0$. In this case, with $\sigma_1 = \tau_z \sigma$, we have $\sigma_1(w) = w$. Arguing same way as σ_1 is is product of $r \leq n-1$ reflections. So, $\sigma = \tau_z \sigma_1$ is is product of $r \leq n$ reflections. This is also a contradiction.

3. **Remark.** Note we used w is anisotropic, otherwise there would be no guarantee that $\dim Fw^{\perp} < n$, which is needed to apply induction.

So, it follows $\tilde{\sigma}^2 = 0$, as was claimed. So, $Im(\tilde{\sigma}) \subseteq \ker(\tilde{\sigma}) = L(\sigma)$.

1. Suppose $L(\sigma)$ is not totally isotropic. Then, $\exists\ w \in L(\sigma)$ that is anisotropic. So, the the same argument above σ would be product of $r \leq n$ reflections, which would be a contradiction. So, $L(\sigma)$ is totally isotropic. So,
$$L(\sigma) \subseteq L(\sigma)^{\perp} = Im(\tilde{\sigma}) \quad by \quad (7.6). \quad So, \quad L(\sigma) = Im(\tilde{\sigma}).$$

2. By dimension formula
$$n = \dim L(\sigma) + \dim Im(\tilde{\sigma}) = 2 \dim L(\sigma) \quad \text{is even}.$$

3. σ acts as identity of $L(\sigma)$ and also acts as identity on
$$\frac{V}{L(\sigma)} = \frac{V}{(\sigma - 1_V)(V)}.$$
So, $\det \sigma = 1$ i. e. $\sigma \in SO(V)$.

4. So, we have established, if
$$\sigma \quad does\ not\ satisfy\ the\ theorem \quad \Longrightarrow \det \sigma = 1.$$

5. Now, τ be any reflection. Then $\det(\tau\sigma) = -1$. By (4), $\tau\sigma$ satisfy the theorem and hence product of $r \leq n$ reflection. So, $\sigma = \tau(\tau\sigma)$ is product of $r+1 \leq n+1$ reflection. Since $n = \dim V$ is even, and $\det\sigma = 1$, σ is not product of $n+1$ reflections. So, σ is product of $\leq n$ reflections. The proof is complete. ■

Proof of (7.8): Assume (1) of lemma 7.8 is false. We will prove $\tilde{\sigma}^2 = 0$. The assumption means

$$w \neq 0 \in V \quad \textit{anisotropic} \Longrightarrow \tilde{\sigma}(w) \neq 0 \quad \textit{and is isotropic.}$$

This means

$$\tilde{\sigma}(w) \perp \tilde{\sigma}(w) \quad \textit{By } (7.7) \quad \tilde{\sigma}(w) \perp w.$$

The binary form $Fw \oplus F\tilde{\sigma}(w)$ is not regular, because its matrix is

$$\begin{pmatrix} q(w) & 0 \\ 0 & 0 \end{pmatrix}. \qquad \textit{Since } V \quad \textit{is regular} \quad \dim V \geq 3.$$

$$\textbf{Claim}: \quad \forall \quad y \in V \quad y \perp \tilde{\sigma}(y).$$

If $y = 0$ the claim is obvious and if $y \neq 0$ and is anisotropic, it is observed above. So, assume $y \neq 0$ is isotropic. Then, by (3.6) $Fy \oplus Fv \cong \mathbb{H}$ for some v. Now, by decomposition theorem, we write $V = ((Fy \oplus Fv) \perp r\mathbb{H} \perp V_a$. Since $\dim V \geq 3$, there is a anisotropic w such that $y \perp w$. Write $u = y + \epsilon w$ with $\epsilon \in \dot{F}$.

$$B(u,u) = B(y+\epsilon w, y+\epsilon w) = \epsilon^2 B(w,w) \neq 0.$$

So, $u = y + \epsilon w$ is anisotropic and nonzero $\forall \epsilon \in \dot{F}$. So, by the contrary hypothesis, $u \perp \tilde{\sigma}(u)$ for all $\epsilon \in \dot{F}$. That means,

$$0 = B(\tilde{\sigma}(u), u) = B(\tilde{\sigma}(y+\epsilon w), y+\epsilon w)$$

$$= B(\tilde{\sigma}(y), y) + \epsilon[B(\tilde{\sigma}(w), y) + B(\tilde{\sigma}(y), w)] + \epsilon^2 B(\tilde{\sigma}(w), w)$$

Since the last term is zero, we have,

$$0 = B(\tilde{\sigma}(y), y) + \epsilon[B(\tilde{\sigma}(w), y) + B(\tilde{\sigma}(y), w)] \qquad \forall\, \epsilon \in \dot{F}..$$

So, $B(\tilde{\sigma}(y), y) = 0$. This establishes the claim.

By (7.7), we have $Im(\tilde{\sigma})$ is totally isotopic. By (7.6(2)), $\tilde{\sigma}^2 = 0$. This establishes (1) of the lemma.

To prove (2), we compute

$$\sigma_1(w) = \tau_z(\sigma(w)) = \sigma(w) - \frac{2B(\sigma(w), z)}{q(z)} z = \sigma(w) - \frac{2B(\sigma(w), \tilde{\sigma}(w))}{q(\tilde{\sigma}(w))} \tilde{\sigma}(w)$$

$$= \sigma(w) - \frac{2(B(w,w) - B(\sigma(w), w))}{2(B(w,w) - B(\sigma(w), w))} \tilde{\sigma}(w) = w.$$

The proof is complete. Lam gives a geometric argument. ■