1. DEFINITION AND BASIC PROPERTIES

§1.1. Quadratic Forms

An n-ary **quadratic form** over a field F is a polynomial in n variables with coefficients in F, of the form $a(\mathbf{x}) = \Sigma a_{ij}x_ix_j = \mathbf{x}^T A\mathbf{x}$ where $A = (a_{ij})$ is a symmetric matrix and $\mathbf{x}^T = (x_1, x_2, \ldots, x_n)$. Throughout we assume that the characteristic of F is not 2. In other words, $1 + 1 \neq 2$ in F.

Quadratic forms a, b are **equivalent** if there exists an invertible matrix P such that $a(P\mathbf{x}) = b(\mathbf{x})$.
We write this as $\mathbf{a} \approx \mathbf{b}$.
Clearly $\approx$ is an equivalence relation.

Example 1: $x_1^2 - x_2^2 \approx x_1x_2$ since

$$x_1^2 - x_2^2 = (x_1 - x_2)(x_1 + x_2).$$

The matrix here is $\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}$

Theorem 1: If $a(\mathbf{x}) = \mathbf{x}^T A\mathbf{x}$ and $b(\mathbf{x}) = \mathbf{x}^T B\mathbf{x}$ then $a \approx b$ if and only if A, B are congruent, that is $P^TAP = B$ for some invertible matrix P. ✋☺

§1.2. Quadratic Spaces

A **quadratic space** V is a finite dimensional vector space over a field F together with an inner product $\langle \mathbf{u} \mid \mathbf{v} \rangle$ such that:

(1) $\langle \mathbf{u} \mid \mathbf{v} \rangle \in F$ for all $\mathbf{u}, \mathbf{v} \in V$;
(2) $\langle \mathbf{u} \mid \mathbf{v} \rangle = \langle \mathbf{v} \mid \mathbf{u} \rangle$ for all $\mathbf{u}, \mathbf{v} \in V$;
(3) $\langle k\mathbf{u} \mid \mathbf{v} \rangle = k\langle \mathbf{u} \mid \mathbf{v} \rangle$ for all $k \in F$, $\mathbf{u}, \mathbf{v} \in V$;
(4) $\langle \mathbf{u} + \mathbf{v} \mid \mathbf{w} \rangle = \langle \mathbf{u} \mid \mathbf{w} \rangle + \langle \mathbf{v} \mid \mathbf{w} \rangle$ for all $\mathbf{u}, \mathbf{v}, \mathbf{w} \in V$.

A quadratic space is a **Euclidean space** if the zero element is the only one where $\langle \mathbf{v} \mid \mathbf{v} \rangle = 0$.

Examples 2:
(1) $\mathbb{R}^3$ with $\langle \mathbf{u} \mid \mathbf{v} \rangle = \mathbf{u} \cdot \mathbf{v}$, the usual dot product.
(2) $\mathbb{C}$ as a vector space of dimension 2 over $\mathbb{R}$ with $\langle \mathbf{z}_1 \mid \mathbf{z}_2 \rangle$ defined to be $\mathrm{Im}(\mathbf{z}_1\mathbf{z}_2)$.
Note that $\langle 1 \mid 1 \rangle = 0$, so this is not Euclidean.
Denote this by $\mathbb{C}_{\mathbf{I}}$.
(3) $\mathbb{C}$ as a vector space of dimension 2 over $\mathbb{R}$ with $\langle \mathbf{z}_1 \mid \mathbf{z}_2 \rangle$ defined to be $\mathrm{Re}(\mathbf{z}_1\mathbf{z}_2)$. This is also not Euclidean since $\langle e^{\pi i/4} \mid e^{\pi i/4} \rangle = 0$. Denote this by $\mathbb{C}_{\mathbf{R}}$.

Theorem 2: In a quadratic space

$$\langle \mathbf{x} \mid \mathbf{y} \rangle = \frac{1}{2} [\langle \mathbf{x} + \mathbf{y} \mid \mathbf{x} + \mathbf{y} \rangle - \langle \mathbf{x} \mid \mathbf{x} \rangle - \langle \mathbf{y} \mid \mathbf{y} \rangle] \text{ for all } \mathbf{x}, \mathbf{y}.$$

Proof: By (2) and (4),

$$\langle \mathbf{x} + \mathbf{y} \mid \mathbf{x} + \mathbf{y} \rangle = \langle \mathbf{x} \mid \mathbf{x} \rangle + \langle \mathbf{y} \mid \mathbf{y} \rangle + 2\langle \mathbf{x} \mid \mathbf{y} \rangle. \text{ ✋☺}$$

Two quadratic spaces are **isometric** if there is a linear transformation $\tau: V \to W$ such that $\langle \tau(\mathbf{u}) \mid \tau(\mathbf{v}) \rangle = \langle \mathbf{u} \mid \mathbf{v} \rangle$ for all $\mathbf{u}, \mathbf{v} \in V$. We denote this by $V \cong W$. Note that because of Theorem 2 it is sufficient to show that $\langle \tau(\mathbf{v}) \mid \tau(\mathbf{v}) \rangle = \langle \mathbf{v} \mid \mathbf{v} \rangle$ for all $\mathbf{v} \in V$.

Example 3: Show that $\mathbb{C}_R \cong \mathbb{C}_I$.
Solution:
$\langle a + bi \mid a + bi \rangle_R = \mathrm{Re}(a + bi)^2 = a^2 - b^2$.
$\langle a + bi \mid a + bi \rangle_I = \mathrm{Im}(a + bi)^2 = 2ab$.
Now use example 1.

Associated with every *n*-ary quadratic form $a(\mathbf{x})$ there is a quadratic space F^n with

$$\langle \mathbf{x} \mid \mathbf{y} \rangle = \frac{1}{2} [a(\mathbf{x} + \mathbf{y}) - a(\mathbf{x}) - a(\mathbf{y})].$$

In any quadratic space we may construct a quadratic form as follows:
Take a basis $\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_n$ of V and define $a(\mathbf{x}) = \Sigma \langle \mathbf{e}_i | \mathbf{e}_j \rangle x_i x_j$. The resulting quadratic form is not unique, but choosing a different basis results in an equivalent quadratic form.

We thus have the following 1-1 correspondences.

congruence class of SYMMETRIC MATRICES	$\leftrightarrow$	equivalence class of QUADRATIC FORMS	$\leftrightarrow$	isometry class of QUADRATIC SPACES

Example 4:

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad \leftrightarrow \quad x_1^2 - y^2 \quad \leftrightarrow \quad \mathbb{C}_R$$

$$\begin{pmatrix} 0 & ½ \\ ½ & 0 \end{pmatrix} \quad \leftrightarrow \quad x_1x_2 \quad \leftrightarrow \quad \mathbb{C}_I$$

Note that over $\mathbb{R}$:

Positive definite matrices	$\leftrightarrow$	Positive definite quadratic forms	$\leftrightarrow$	Euclidean spaces

§1.3. Diagonalization of Quadratic Forms

Theorem 2: Every quadratic space has an orthogonal basis.

Proof: We prove this by induction on $n = \dim V$.

It's trivial if $n = 1$.

Case I: $V^\perp \neq 0$. Choose $0 \neq \mathbf{v} \in V^\perp$. Then $V = \langle \mathbf{v} \rangle \oplus W$ for some W. By the induction hypothesis W has an orthogonal basis, which together with $\mathbf{v}$ gives an orthogonal basis for V.

Case II: $V^\perp = 0$. By Theorem 1, there exists $\mathbf{v} \in V$ such that $\langle \mathbf{v} \mid \mathbf{v} \rangle \neq 0$.

Let $W = \langle \mathbf{v} \rangle^\perp$. Since $\langle \mathbf{v} \mid \mathbf{v} \rangle \neq 0$, $\mathbf{v} \notin W$.

Now $\sigma: V \to F$, defined by $\sigma(\mathbf{x}) = \langle \mathbf{x} | \mathbf{v} \rangle$, is a linear transformation and rank $\sigma = 1$.

(If it was 0 then $\mathbf{v} \in V^\perp$.)

Hence nullity $\sigma = \dim W = n - 1$.

Thus $V = \langle \mathbf{v} \rangle \oplus W$ and so, as in Case I, V has an orthogonal basis. ✋☺

NOTES:
(1) A quadratic space need not have an orthonormal basis since there could be non-zero vectors of zero length.
(2) If char F = 2 it need not be true.

§1.4. Classification of Quadratic Forms

Notation: $\langle d_1, \ldots, d_n \rangle$ denotes $d_1x_1^2 + \ldots + d_nx_n^2$.
This is called a diagonal form.

Theorem 3: Every quadratic form is equivalent to a diagonal form.
Proof: Put an orthogonal basis $e_1, \ldots, e_n$ into the quadratic space. The quadratic form becomes $\Sigma \langle \mathbf{e_i} \mid \mathbf{e_i} \rangle x_i^2$. ✋☺

Question: When is $\langle a_1, \ldots, a_n \rangle \cong \langle b_1, \ldots, b_n \rangle$?

Examples 4:
(1) Over $\mathbb{R}$: If $a, b > 0$ then $\langle a \mid b \rangle \cong \langle 1, 1 \rangle$ since

$$ax_1^2 + bx_2^2 = (\sqrt{a}\, x_1)^2 + (\sqrt{b}\, x_2)^2.$$

So the following are representatives of the 5 equivalence classes of binary quadratic forms over $\mathbb{R}$:
$\langle 0 \mid 0 \rangle$, $\langle 1 \mid 0 \rangle$, $\langle -1 \mid 0 \rangle$, $\langle 1 \mid 1 \rangle$, $\langle 1 \mid -1 \rangle$, $\langle -1 \mid -1 \rangle$.

(2) Over $\mathbb{C}$: These reduce to 3 equivalence classes, with representatives: $\langle 0 \mid 0 \rangle$, $\langle 1 \mid 0 \rangle$, $\langle 1 \mid 1 \rangle$.

NOTES:
(1) $\langle 1 \mid 1\rangle \cong \langle 1 \mid -1\rangle$ since $x^2 + y^2 = x^2 - (iy)^2$.
(2) $\langle a_1, \ldots, a_n\rangle$ is independent (up to equivalence) of the order of the vectors
(3) $\langle k^2 a_1, a_2, \ldots, a_n\rangle \cong \langle a_1, \ldots, a_n\rangle$. Square factors can be removed in any position.

A **square class** of F is an equivalence class of $F^{\#}$ under the equivalence relation $x \sim y$ if and only if $\frac{x}{y} \in F^{\#2}$ (non-zero squares).
We denote the square class containing *x* by $\mathbf{xF^{\#2}}$.

Examples 5:
(1) $\mathbb{R}$ has 2 equivalence classes, $\mathbb{R}^{\#2}$ (positive reals) and $-\mathbb{R}^{\#2}$ (negative reals).
(2) $\mathbb{C}$ has a single square class.
(3) $\mathbb{Z}_5$ has two square classes viz.

$$\mathbb{Z}_5^{\#2} = \{1, 4\} \text{ and } 2\,\mathbb{Z}_5^{\#2} = \{2, 3\}.$$

Hence every binary quadratic form over $\mathbb{Z}_5$ is equivalent to one of the following:

$$\langle 0 \mid 0\rangle, \quad \langle 1 \mid 0\rangle, \quad \langle 2 \mid 0\rangle, \quad \langle 1 \mid 1\rangle, \quad \langle 1 \mid 2\rangle, \quad \langle 2 \mid 2\rangle.$$

However $\langle 1 \mid 1\rangle \cong \langle 2 \mid 2\rangle$ since

$$2x^2 + 2y^2 = (x + y)^2 + (x - y)^2.$$

(4) $\mathbb{Q}$ has infinitely many square classes.

§1.5. Determinant of a Quadratic Form

The **determinant** of the quadratic form $\mathbf{x}^T A\mathbf{x}$ is defined to be the determinant of A. Since $|P^T AP| = |A|.|P|^2$, the determinant of equivalent quadratic forms are equivalent, that is, they belong to the same square class.

Examples 6: Over $\mathbb{Q}$:

(1) $\langle 3, 2\rangle$ is not equivalent to $\langle 6, 5\rangle$ since $\frac{30}{6} = 5 \notin \mathbb{Q}^{\#2}$.

(2) $\langle 3, 2\rangle \cong \langle 5, 30\rangle$ since:

$$5x^2 + 30y^2 = 3(x + 2y)^2 + 2(x - 3y)^2.$$

(3) $\langle 3, 2\rangle$ is not equivalent to $\langle 1, 6\rangle$ even though they have the same determinant.

For if so, $3x^2 + 2y^2 = 1$ for some $x, y \in \mathbb{Q}$ and hence $3m^2 + 2n^2 = d^2$ for some $m, n, d \in \mathbb{Z}$.

We can assume that the GCD of $m, n, d = 1$ and hence 3 doesn't divide d.

Thus $\left(\frac{d}{n}\right)^2 = 2$ in $\mathbb{Z}_3$, a contradiction as $2 \notin \mathbb{Z}_3^{\#2}$.