Theorem (Lagrange):
Any positive integer is the sum of four squares.

Theorem (Legendre): A positive integer not divisible by 4 is a sum of three squares $\iff$ it is not $\equiv 7 \bmod 8$.

Theorem (Fermat): A positive integer is a sum of two squares $\iff$ any prime factor which is $\equiv 3 \bmod 4$ occurs w/ even multiplicity.

Theorem (Artin): Let f be a rational function over $\mathbb{R}$ in n variables.
Then f is a sum of squares in $\mathbb{R}(x_1, \dots, x_n)$
$\iff f \geq 0$ where defined.
(Pfister: f is a sum of 2^n squares)

Let F be a field of $\mathrm{char} \neq 2$.

Pre-defn: A quadratic form over F is a fn $q: F^n \to F$ s.t.

$$q(\vec{x}) = \sum a_{ij} x_i x_j \quad \text{(e.g. } x_1^2 + \cdots + x_n^2\text{)}$$

Def Let V be a f.d. vector space over F. A symmetric bilinear form on V is a fn

$$B: V \times V \to F \quad \text{s.t.}$$

1) B is bilinear, i.e. $B(\cdot, v)$ & $B(v, \cdot)$ are linear $V \to F$ (for each $v \in V$).

2) $B(v, w) = B(w, v)$

E.g. inner product on $\mathbb{R}^n$.

Say B is <u>nondegenerate</u> or an <u>inner product</u> if

$\forall v \in V$ s.t. $v \neq 0$, then $\exists w$ s.t. $B(v,w) \neq 0$.

Equivalently

$B: V \xrightarrow{\sim} V^\vee$.

An <u>inner product space</u> is a vector space w/ inner product often written $\langle \cdot, \cdot \rangle$.

Ex) Let $e_1, \dots, e_n$ be a basis for V. Then obtain an n-by-n symetric matrix

$a_{ij} = e_i \cdot e_j$.

By bilinearity, this symmetric matrix determines $\cdot$.

Nondegeneracy $\Rightarrow$ (a_{ij}) nonsingular.

For a fixed basis, an inner product $\Longleftrightarrow$ n-by-n nonsingular symmetric matrix.

Ex) Given an inner product space $(V, \cdot)$, define

$q : V \to F$ by

$q(v) = v \cdot v$

"associated quadratic form"

(has the form earlier in a basis.)

Note that the inner product is determined by q

b/c

$$x \cdot y = \frac{1}{2}(q(x+y) - q(x) - q(y)).$$

Will use "quadratic space" & "inner product space" interchangeably.

Questions

1) When are two quadratic spaces isomorphic?

(An isomorphism is a linear iso which preserves the inner product.)

2) Given $(V, \cdot)$, when is there a vector $v \in V$, $v \neq 0$, s/t $v \cdot v = 0$?

(Such V are called isotropic.)

3) Which elements of F occur as $v \cdot v$ for $v \neq 0$?

Goal: Answer all these questions when $F = \mathbb{Q}$ (Hasse–Minkowski).

These questions are much harder for higher degree forms.

Two reasons:

1) Quadratic forms have lots of symmetry.
2) Notion of orthogonality

Orthogonality

Vectors $v, w \in V$ are <u>orthogonal</u> if $v \cdot w = 0$.

Given a subspace $W \subseteq V$, define

$$W^{\perp} = \{ v \in V \text{ s.t. } v \cdot w = 0 \ \forall w \in W \}$$

Have always $\dim W + \dim W^{\perp} = \dim V$.

Note that $W \cap W^\perp \neq 0$ in general.

Fact: if the inner product on V restricts to an inner product on W, then in fact

$$W \oplus W^\perp \cong V.$$

Gives a way of breaking down an inner product space into smaller pieces.

Construction: If (V_1, q_1) & (V_2, q_2) are quadratic spaces, then form

direct sum $(V_1 \oplus V_2, q_1 + q_2)$

(s.t. V_1, V_2 sit inside orthogonally).

("external direct sum").

Diagonalization

Notation: given $a \in F^\times$,

write $\langle a \rangle = \{$ 1-dim inner prod space $Fe_1 \quad e_1 \cdot e_1 = a$.

"quadratic form ax^2"

$(V, \cdot)$

Any inner product space is a direct sum of one-dimensional spaces $\langle a \rangle$ $\quad a \in F^\times$.

(Alternatively, can choose a basis s.t. symmetric matrix of inner product is diagonal.).

Pf: Choose $v \in V$ s.t. $v \cdot v \neq 0$.

Then $V \cong Fv \oplus (Fv)^{\perp}$.

Conclude by induction (to $(Fv)^{\perp}$).

Can always write $(V, \cdot)$

$\cong \langle a_1 \rangle + \langle a_2 \rangle + \cdots + \langle a_n \rangle$

some $a_i \in F^{\times}$

Not unique:

$\langle a_1, \ldots, a_n \rangle \cong \langle a_1 u_1^2, a_2 u_2^2, \ldots, a_n u_n^2 \rangle$

any $u_1, \ldots u_n \in F^{\times}$.

Cor If every element of F is a square (e.g. F algebraically closed), then any quadratic form $\simeq$ $\langle 1, \ldots, 1 \rangle$ i.e.

$$x_1^2 + \cdots + x_n^2.$$

Cor: Any quadratic form over $\mathbb{R}$ is isomorphic to

$$\langle 1 \rangle^{\oplus r} \oplus \langle -1 \rangle^{\oplus s}$$ for some r, s.

(Sylvester: r, s are uniquely determined by the quadratic space. Defines r − s to be the signature of quadratic form.)

Orthogonal group

Def Given a quadratic space (V, q), defines the

$$O(V,q) = \left\{ f : V \xrightarrow{\sim} V \text{ s.t. } q \circ f = q \right\},$$

$= Aut(V, Q)$.

"orthogonal group"

Ex) Given a vector $v \in V$ s.t. $v \cdot v \neq 0$,

define

$R_v : V \to V$ s.t.

$$R_v(x) = x - \frac{2(x \cdot v)}{(v \cdot v)} v$$

("reflection through v")

has the property

$$R_v|_{Fv} = -1.$$

$$R_v|_{(Fv)^\perp} = 1$$

In fact, (Cartan-Dieudonné) $O(V,q)$ generated by reflections