Quadratic Forms and the local global principle

Lecture 4: Quadratic Forms over $\mathbb{Q}$

Part 1. Hasse–Minkowski

Part 2. Classification of quad forms / $\mathbb{R}$

Part 3. Classification of quad forms / $\mathbb{Q}$

Part 1. Hasse–Minkowski

local-global principle: $(\mathbb{Q}_\infty = \mathbb{R})$

If we can understand $\rule{2em}{0.4pt}$ over $\mathbb{Q}_p$ $\forall p \leq \infty$,

can we understand $\rule{2em}{0.4pt}$ over $\mathbb{Q}$?

Example. Say $a \in \mathbb{Q}$.

Q: If $X^2 - a = 0$ has a soln in $\mathbb{Q}_p$ $\forall p \leq \infty$,

does $X^2 - a = 0$ has ~~a~~ soln in $\mathbb{Q}$?

By prime factorization:

valuation of a at p

$$a = \pm \prod_{p<\infty} p^{n_p} = \pm \prod_{p<\infty} p^{v_p(a)}$$

- If $X^2-a=0$ has a soln over $\mathbb{R}$

$$\Rightarrow +$$

- If $X^2-a=0$ is solvable over $\mathbb{Q}_p$

$$\Rightarrow v_p(X^2) = v_p(a)$$

$$\Rightarrow 2v_p(X) = v_p(a)$$

$$\Rightarrow v_p(a) \text{ is even}$$

$$\Rightarrow \underbrace{\frac{v_p(a)}{2}}_{} \text{ is an integer.}$$

applies to <u>all</u> $p<\infty$.

$$\Rightarrow \prod_{p<\infty} p^{\frac{v_p(a)}{2}} \in \mathbb{Q}$$

Further: $\left(\prod_{p<\infty} p^{\frac{v_p(a)}{2}}\right)^2 - a = \underbrace{\prod_{p<\infty} p^{v_p(a)}}_{} - a = 0$

So we've shown: $X^2-a=0$ solvable in $\mathbb{Q}_p$ $\forall p \leq \infty$

$\Rightarrow X^2-a=0$ solvable in $\mathbb{Q}$!

"$X^2-a=0$ satisfies the Hasse Principle"

Rephrase:

$X^2 - a = 0$ is solvable over k

$\Leftrightarrow$ $X^2 - aZ^2 = 0$ has a nontriv soln over k

$\Leftrightarrow$ the quad form $X^2 - aZ^2$ reps 0 over k.

Therefore: Example proves:

f = quad form $/\mathbb{Q}$ dim 2

f_p = quad form $/\mathbb{Q}_p$ $p \leq \infty$

view f as

f represents 0 over $\mathbb{Q}$

if and only if f reps 0 over $\mathbb{Q}_p$ $\forall p \leq \infty$.

Pf: "if": argument in Example

"only if" f reps 0 over $\mathbb{Q} \Rightarrow f_p$ reps 0 over $\mathbb{Q}_p$ obvious $\square$.

Thm (Hasse-Minkowski) f any quad form $/\mathbb{Q}$.

Then f represents $0 \Leftrightarrow f_p$ represents 0 $\forall p \leq \infty$.

Cor. f any quad form $/\mathbb{Q}$; $a \in \mathbb{Q}$ arb.

Then f rep $a \iff f_p$ reps a $\forall p \leq \infty$.

Part 2. Classification of quad forms $/\mathbb{R}$

$$\mathbb{R}^\times / (\mathbb{R}^\times)^2 = \mathbb{R}^\times / (\mathbb{R}_{>0}) = \text{rep by } \pm 1$$

By orthogonality + $(\mathbb{R}^\times)^2 = \mathbb{R}_{>0}$, we know that every quad form f is s.t.

$$f \sim X_1^2 + \dots + X_{n-s}^2 - Y_1^2 - \dots - Y_s^2$$

for some integer $0 \leq s \leq n$.

Claim. The integer s only dep on f. Call $s = s(f)$.

The pair $(n-s, s)$ is called the signature of f.

- f is definite if $s=0$ or $s=n$ (f anisotropic)
- f is indefinite if $s \neq 0, n$

Thm (Classification over $\mathbb{R}$).

f, f' quad forms over $\mathbb{R}$. $f \sim f' \iff n(f) = n(f')$, $s(f) = s(f')$

Can define discriminant in the usual way:

$$d(f) = (-1)^s \in \mathbb{R}^\times/(\mathbb{R}^\times)^2 = \mathbb{R}^\times/\mathbb{R}_{>0} = \{\pm 1\}.$$

Hasse invariant for $\mathbb{R}$ can be def in the same way as over $\mathbb{Q}_p$:

Hilbert symbol

$$(a,b)_\infty := \begin{cases} 1 & \text{if } aX^2+bY^2=Z^2 \text{ has a nontriv soln over } \mathbb{R} \\ -1 & \text{otherwise} \end{cases}$$

Then

$$\varepsilon_\infty(f) := \prod_{i<j} (a_i, a_j)_\infty$$

where: $a_i = \begin{cases} 1 & \text{if } 1 \leq i \leq n-s \\ -1 & \text{if } n-s+1 \leq i \leq n \end{cases}$

Note: $(1,a)_\infty = 1.$

$(-1,-1)_\infty = -1.$

$$\frac{(s)(s-1)}{2}$$

$$= (-1)^{\frac{s(s-1)}{2}}.$$

So: $s(f)$ recovers $d_\infty(f) = (-1)^s$

and $\varepsilon_\infty(f) = (-1)^{s(s-1)/2}$

Part 3. Classificat. of quad forms / $\mathbb{Q}$

Thm. f, f' quad. forms over $\mathbb{Q}$.

$$f \sim f' \iff f_p \sim f_p' \quad \forall\, p \leq \infty.$$

Comment: $\Rightarrow$ is obv. $\Leftarrow$ require work.

Pf. $n = 1$ ✓

We'll prove this by induction.

Let $n = n(f) = n(f')$.

Let $a \in \mathbb{Q}$ be any elt represented by f.

$\Rightarrow$ a is represented by f_p

$\Rightarrow$ a is represented by f_p'

By Lemma 3.10 of the notes,

$$\rightarrow \quad f \sim aZ^2 + g$$

$$f' \sim aZ^2 + g'$$

for quad forms g, g' of rank $n-1$.

In terms of quad spaces: for $k = \mathbb{Q}$ or $\mathbb{Q}_p$, $p \leq \infty$

$$(\underline{k^n}, f) \cong (k, \underline{aZ^2}) \oplus (\underline{k^{n-1}}, g)$$

$$(\underline{k^n}, f') \cong (k, aZ^2) \oplus (\underline{k^{n-1}}, g')$$

Our assumption:

$$(\mathbb{Q}_p^n, f_p) \cong (\mathbb{Q}_p^n, f_p')$$
$$\cup \qquad\qquad \cup$$

Obv: $(\mathbb{Q}_p, az^2) = (\mathbb{Q}_p, az^2)$

Witt's theorem $\Rightarrow$ Given any $W \subseteq V$ quad spaces, and any U_1, U_2 s.t.

$$W \oplus U_1 = W \oplus U_2 = V.$$

Then $U_1 \cong U_2$

$$\Rightarrow (\mathbb{Q}_p^{n-1}, g_p) \cong (\mathbb{Q}_p^{n-1}, g_p'). \quad \forall p \leq \infty$$

$$\Rightarrow (\mathbb{Q}^{n-1}, g) \cong (\mathbb{Q}^{n-1}, g')$$

Ind hyp

$$\Rightarrow (\mathbb{Q}^n, f) \cong (\mathbb{Q}, az^2) \oplus (\mathbb{Q}^{n-1}, g)$$
$$\cong (\mathbb{Q}, az^2) \oplus (\mathbb{Q}^{n-1}, g')$$
$$\cong (\mathbb{Q}^n, f') \qquad \square.$$

Thm $\Rightarrow$ any quad form f over $\mathbb{Q}$ is characterized by:

- rank — $n(f)$
- discriminant — $d(f)$ $\leftarrow$ recovers $d_p(f_p)$ $\forall p$
- local Hasse invt — $\varepsilon_p(f_p)$, $p < \infty$
- signature — $(n-s, s)$ $\leftarrow$ $p = \infty$ invariant.

Prop. Let $n \in \mathbb{Z}_{>0}$, $d \in \underline{\mathbb{Q}^\times/(\mathbb{Q}^\times)^2}$, $(\varepsilon_p)_{p \le \infty}$, $s \in \mathbb{Z}_{\ge 0}$

each ± 1

satisfy:

① $\varepsilon_p = 1$ for all but f many p

and $\prod_{p \le \infty} \varepsilon_p = 1$

② $0 \le s \le n$

③ $d_\infty = (-1)^s$

④ $\varepsilon_\infty = (-1)^{s(s-1)/2}$

Assume further:

- If $n=1$, then $\varepsilon_p = 1 \quad \forall\, p \le \infty$.
- If $n=2$, then $(d_p, \varepsilon_p) \ne (-1,-1)$

im of d in $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2$

__THEN:__ $\exists$ f quad form over $\mathbb{Q}$ with the above invariants.

Pf (n=2 case)

Assume $(d_p, \varepsilon_p) \neq (-1,-1)$ $\forall\, p \leq \infty$ (treat ∞ case separately)

By last week's arg, for each $p \leq \infty$,

$\exists\, a_p \in \mathbb{Q}_p^\times$ s.t. $(a_p, -d_p) = \varepsilon_p$. (*)

Since $\prod_{p \leq \infty} (a_p, -d_p) = \prod_{p \leq \infty} \varepsilon_p = 1$

then the "global Hilbert symbol thm" (Thm 4.5)

$\Rightarrow \exists\, a \in \mathbb{Q}^\times$ s.t. $(a, -d)_p = (a_p, -d_p)_p$
$= \varepsilon_p \;\; \forall\, p \leq \infty$

In other words: $a \in \mathbb{Q}^\times$ (global) realizes all these local Hilb. symbols simultaneously.

Now try: $f = aX^2 + adY^2$

Check: $n(f) = 2 = n$ ✓

$d(f) = a^2 d = d \in \mathbb{Q}^\times / (\mathbb{Q}^\times)^2$ ✓

$\varepsilon_p(f) = (a, ad)_p = \underbrace{(a,-a)_p}_{=1} \cdot (a,-d)_p = \varepsilon_p$ ✓

□

Ex. If $s=0,1,2$: What are d_∞, ε_∞ ?

$(n=2)$

Note $f = aX^2 + adY^2$

$$\|$$

$$(\mathbb{Q}\sqrt{-d},\ a\cdot Nm_{\mathbb{Q}(\sqrt{-d})/\mathbb{Q}})$$