Quadratic Forms and the local-global principle

Lecture 3: Quadratic forms over $\mathbb{Q}_p$

Part 1. $\mathbb{Q}_p$ is harder than $\mathbb{F}_p$

Part 2. Hilbert symbols

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

From now on: all quad spaces are assumed to be <u>nondegenerate</u>.

<u>Part 1: $\mathbb{Q}_p$ is harder than $\mathbb{F}_p$</u>

Week 2: quad spaces over $\mathbb{F}_q$ are classified by: $\left\{ \begin{array}{l} \text{rank}, \ n \\ \underset{\sim}{\text{disc}}, \ d \end{array} \right.$

Recall: $k^\times/(k^\times)^2$ = equiv classes of elts in $k^\times$ under:
$a \sim b \iff a = bx^2$ for some $x \in k^\times$

$$= k^\times/\sim$$

$$\mathbb{F}_q^\times/(\mathbb{F}_q^\times)^2 = \langle \zeta \rangle / \langle \zeta^2 \rangle = 2 \text{ elements}$$

$$= 2 \text{ cosets}: \ (\mathbb{F}_q^\times)^2, \ \zeta(\mathbb{F}_q^\times)^2.$$

$$\begin{array}{cc} \text{w} \Updownarrow & \Updownarrow \\ +1 & -1 \end{array}$$

So: $\text{quad sp}/\mathbb{F}_q \overset{1-1}{\longleftrightarrow} \left\{ (n,d) : \begin{array}{l} n \in \mathbb{Z}_{>0} \quad \text{w} \\ d \in \{\pm 1\} \cong \mathbb{F}_q^\times/(\mathbb{F}_q^\times)^2 \end{array} \right\}$

In part: there are exactly 2 quad sp / $\mathbb{F}_q$ of any given dim n.

Q: What if $k = \mathbb{Q}_p$? $p \neq 2$

First: What does $\mathbb{Q}_p^\times / (\mathbb{Q}_p^\times)^2$ look like?

Fix an integer a which is:
- coprime to p
- not a square in $\mathbb{Q}_p^\times$

(Comment: Hensel's lemma (Prof Bell's course this week)

$\Downarrow$

to find such an a, it suffices to find an a which is not a square mod p (in $\mathbb{F}_p$).)

- By constr: $\underbrace{a(\mathbb{Q}_p^\times)^2} \neq (\mathbb{Q}_p^\times)^2$

  ($a \neq 1$ in $\underbrace{\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2}$)

- p does not have a square root in $\mathbb{Q}_p^\times$

  If it was, then $p = x^2$ for some $x \in \mathbb{Q}_p^\times$

$$\Rightarrow \underbrace{v_p(p)}_{= 1} = v_p(x^2) = 2v_p(x) = \text{even} \quad \divideontimes$$

$\Rightarrow \underbrace{p(\mathbb{Q}_p^\times)^2} \neq (\mathbb{Q}_p^\times)^2$

Q. $p = a$ in $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2$?

$v_p(p) = 1$, $v_p(a) = 0$ $\divideontimes$

$\Rightarrow p(\mathbb{Q}_p^\times)^2 \neq a(\mathbb{Q}_p^\times)^2$

- ap also does not have a square root in $\mathbb{Q}_p^\times$

  Check: $ap \neq a, p, 1$ in $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2$.

So: $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2$ has at least 4 elements $\begin{pmatrix} 1, a, \\ p, ap \end{pmatrix}$

Fact: ——— " — exactly — " ———.

<u>Important Example.</u>

Fact: $\mathbb{Q}_p$ has exactly 3 nonisomorphic quad extn:

space	form	disc $\in \mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2$
① $\mathbb{Q}_p(\sqrt{a})$	$Nm_{\mathbb{Q}_p(\sqrt{a})/\mathbb{Q}_p} = X^2 - aY^2$	$-a$
② $\mathbb{Q}_p(\sqrt{p})$	$Nm = X^2 - pY^2$	$-p$
③ $\mathbb{Q}_p(\sqrt{ap})$	$Nm = X^2 - apY^2$	$-ap$

Note: If $-1 \in (\mathbb{Q}_p^\times)^2$, then

$$-a = a, \quad -p = p, \quad -ap = ap \quad \text{in } \mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2$$

If $-1 \notin (\mathbb{Q}_p^\times)^2$, the

$$-a = 1, \quad -p = ap, \quad -ap = p \quad \text{in } \mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2$$

Recall: general fact from Wk 2: Any anisotropic quad sp of dim 2 / k is of the form $(L, a\,Nm_{L/k})$

L/k quad extn, $a \in k^\times$.

Apply thm to ①, ②, ③ to get 3 more nonisom

space	form	disc $\in \mathbb{Q}_p^\times / (\mathbb{Q}_p^\times)^2$
①' $\mathbb{Q}_p(\sqrt{a})$	$p\,Nm_{\mathbb{Q}_p(\sqrt{a})/\mathbb{Q}_p} = pX^2 - apY^2$	$-ap^2 = -a$
②' $\mathbb{Q}_p(\sqrt{p})$	$a\,Nm = aX^2 - apY^2$	$-a^2p = -p$
③' $\mathbb{Q}_p(\sqrt{ap})$	$a\,Nm = aX^2 - a^2pY^2$	$-a^3p = -ap$

Issue: disc cannot distinguish between

① \& ①', ② \& ②', ③ \& ③'.

Turns out: there's only one other quad space of dim 2 / $\mathbb{Q}_p$:

7th one:

$\mathbb{Q}_p^{\oplus 2}$	$H_2 = XY$	-1

Part 2: Hilbert symbol

Def. For $a, b \in \mathbb{Q}_p^\times$, the Hilbert symbol of a, b is:

$$(a,b) := \begin{cases} +1 & \text{if } aX^2 + bY^2 = Z^2 \text{ has a soln } (X,Y,Z) \in \mathbb{Q}_p^{\oplus 3} \setminus \{(0,0,0)\} \\ -1 & \text{otherwise} \end{cases}$$

$$\mathbb{Q}_p^\times \times \mathbb{Q}_p^\times \to \{\pm 1\}$$

Ex. $a \in \mathbb{Q}_p^\times$

(i) $(a,-a) = 1$

$aX^2 - aY^2 = Z^2$ always has a nontriv soln

e.g. $(1,1,0)$

[(ii) (a^2, b) for any $b \in \mathbb{Q}_p^\times$
$= 1$

$a^2X^2 + bY^2 = Z^2$ always has a nontri soln

e.g. $(1,0,a)$.

(iii) (a,p), ~~assume a is an int. coprime to p.~~

$(a,p) = 1 \Leftrightarrow \underline{aX^2} + \underline{pY^2} = \underline{Z^2}$ has an ntrivtri soln

v_p: ~~even~~ odd even

$\Leftrightarrow X \neq 0$ and

$$a = \frac{1}{X^2}(Z^2 - pY^2)$$

$$= Nm_{\mathbb{Q}_p(\sqrt{p})/\mathbb{Q}_p}\left(\frac{1}{X}(Z + \sqrt{p}Y)\right)$$

so $(a,p) = 1 \Leftrightarrow a$ is the norm of an elt of $\mathbb{Q}_p(\sqrt{p})$

Properties of Hilbert symbol.

- $(a,b)(a,c) = (a,bc)$, $(a,c)(b,c) = (ab,c)$ (bimultiplication)
- $(a,b) = (b,a)$
- $(ax^2, b) = (a,b)$

3rd Prop $\Rightarrow$ Hilbert symbol descends to a map

$$\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2 \times \mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2 \to \{\pm 1\}.$$

<u>Def.</u> (V, Q) quad space over $\mathbb{Q}_p$ wrt some <u>orthog basis</u>, we have

$$Q(X) = a_1 X_1^2 + a_2 X_2^2 + \dots + a_n X_n^2 \; ; \quad a_i \in \mathbb{Q}_p^\times$$

The <u>Hasse invariant</u> is

$$\varepsilon(Q) := \prod_{i<j} (a_i, a_j) \qquad \in \{\pm 1\}$$

<u>Note:</u> $\varepsilon(Q)$ depends only on (V, Q) and not on
(Thm!) the choice of orthog basis.

<u>Ex.</u> Revisit our 7 quad spaces of dim 2 $(p \neq 2)$

① $(\mathbb{Q}_p(\sqrt{a}), Nm) \Leftrightarrow f = X^2 - aY^2$

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

$$\varepsilon(f) = (1, -a) = (1^2, -a) = 1$$

①' $(\mathbb{Q}_p(\sqrt{a}), pNm) \Leftrightarrow f = pX^2 - apY^2$

$$\Rightarrow d(f) = -ap^2 = -a \in \mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2$$

$$\varepsilon(f) = ??$$

$$\varepsilon(f) = (p, -ap) = (p,-p)(p,a)$$
$$= (p,a) = (a,p)$$

So $\varepsilon(f) = 1 \Leftrightarrow$ a is the norm of an elt of $\mathbb{Q}_p(\sqrt{p})$.

$$aX^2 + pY^2 = Z^2$$

Recall: a is not a square mod p.

$\Leftrightarrow$ $aX^2 = Z^2$ has no soln mod p

$\Updownarrow$

$aX^2 + pY^2 = Z^2$

$\Leftrightarrow$ $aX^2 + pY^2 = Z^2$ has no soln in $\mathbb{Q}_p$.

Part 3. Classificatn of quad spaces over $\mathbb{Q}_p$

General.

A quad form is a fn of the form

$$f(X_1, \dots, X_n) = \sum_{i=1}^{n} a_{ii} X_i^2 + 2 \sum_{i=1}^{n} a_{ij} X_i X_j \quad \text{for } a_{ij} \in k.$$

We say that $(k^{\oplus n}, f)$ is the quad space assoc. to f.

We say f, f' are equivalent ($f \sim f'$) if their assoc. quad spaces are isom.

We say f represents $a \in k$ if $\exists$ a nontriv soln to $f(X) = a$.

$k = \mathbb{Q}_p$

Thm (Classificatn over $\mathbb{Q}_p$)

f, g are quad forms over $\mathbb{Q}_p$

Then $f \sim g \iff$

$$n(f) = n(g) \quad \text{(rank)}$$
$$d(f) = d(g) \quad \text{(disc)}$$
$$\varepsilon(f) = \varepsilon(g) \quad \text{(Hasse invt)}$$

Q: For which triples (n, d, ε) does there exist a quad form f with

$$n(f) = n$$
$$d(f) = d$$
$$\varepsilon(f) = \varepsilon$$

?

$$\left(\begin{array}{l} n \in \mathbb{Z}_{>0} \\ d \in \mathbb{Q}_p^\times / (\mathbb{Q}_p^\times)^2 \\ \varepsilon \in \{\pm 1\} \end{array} \right.$$

Prop. $\exists$ a quad fm f with $(n(f), d(f), \varepsilon(f)) = (n, d, \varepsilon)$ iff one of the following holds:

- $n = 1$ & $\varepsilon = 1$
- $n = 2$ & $(d, \varepsilon) \neq (-1, -1)$]
- $n \geq 3$

pf. $n=1$ $\quad f \sim dX^2 \Rightarrow d(f)=d,\ \varepsilon(f)=1$

$n=2$ • Claim 1. $(d,\varepsilon)=(-1,-1)$ is not realizable.

pf. write $f \sim aX^2+bY^2$

then $d(f)=ab$, $\varepsilon(f)=(a,b)$.

If $d(f)=-1$, then $ab=-1$

$$\Rightarrow \varepsilon(f)=(a,b)=(a,b)(-b,b)$$
$$=(-ab,b)=(1,b)=1. \checkmark$$

• Claim 2. If $d\neq -1$, ε arb, then (d,ε) is realizable.

pf. $d\neq -1 \Leftrightarrow -d \notin (\mathbb{Q}_p^\times)^2$.

$\Rightarrow$ for any ε, $\exists\ a\in\mathbb{Q}_p^\times$ s.t.

$$(a,-d)=\varepsilon.$$

(since norm maps for extns of $\mathbb{Q}_p$ are never surj.)

Consider $f\sim aX^2+adY^2$

Then $d(f)=a^2d=d$ ✓

$$\varepsilon(f)=(a,ad)=(a,-a)(a,-d)$$
$$=(a,-d)=\varepsilon \checkmark$$

✓

• Claim 3: $(-1,1)$ is realizable.

Pf: $f \sim X^2 - Y^2$

then $d(f) = -1$ ✓

$\varepsilon(f) = (1,-1) = 1$ ✓

(d,ε) chosen.

$n=3$ we want to constr. f rank 3 s.t.

$$d(f) = d, \quad \varepsilon(f) = \varepsilon$$

Let $a \in k^\times$ be any elts s.t. $a \neq -d$ in $\mathbb{Q}_p^\times / (\mathbb{Q}_p^\times)^2$.

Consider g a quad form of rk 2 s.t.

$$d(g) = ad \neq -1$$

$$\varepsilon(g) = (a,-d)\,\varepsilon$$

Note: g exists by the $n=2$ case above!

Set $f \sim aZ^2 + g$

Compute: $d(f) = a \cdot d(g) = a^2 d = d$ ✓

$$\begin{aligned}\varepsilon(f) &= (a, d(g)) \cdot \varepsilon(g) \\ &= (a, ad) \cdot (a,-d) \cdot \varepsilon \\ &= \underbrace{(a,-a)}_{=1}\underbrace{(a,-d)(a,-d)}_{=1} \cdot \varepsilon \\ &= \varepsilon\end{aligned}$$

$\square$

Cor. Over $\mathbb{Q}_p$, p odd, there are:

- 4 quad forms of rk 1
- $8-1=7$ quad forms of rk 2
- 8 quad forms of rk n for any $n \geq 3$

Fact. $\left|\mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2\right| = 8$

Cor. Over $\mathbb{Q}_2$, there are:

- 8 quad forms of rk 1
- $16-1=15$ quad forms of rk 2
- 16 quad forms of rk n for any $n \geq 3$