Lecture 32: Hilbert Symbol; Forms over $\mathbb{Q}_p$

Last time:

Hasse-Minkowski Thm: q a quad form on $\mathbb{Q}^n$.
Then $\exists x \in \mathbb{Q}^n$ with $q(x)=0 \iff$ For every place v, $\exists x_v \in \mathbb{Q}_v^n$ with $q(x_v)=0$. [*Note:* gen to any number field K.]

Note: Following Serre, "A course in arithmetic."

Goal: Classify quadratic forms over $\mathbb{Q}_p$.

Hilbert Symbol:

K field of char 0. For $a, b \in K^\times$, define

$$(a,b) = \begin{cases} 1 & \text{if } z^2 - ax^2 - by^2 = 0 \text{ has a nontrivial solution in } K^3. \\ -1 & \text{otherwise.} \end{cases}$$

Note this doesn't change if we replace a by ak^2 for $k \in K^\times$, so $(\ ,\ ): K^\times/(K^\times)^2 \times K^\times/(K^\times)^2 \longrightarrow \{\pm 1\}$.

Ex: $K = \mathbb{R}$
$(1,1) = 1$
$(1,-1) = 1$
$(-1,-1) = -1$

Prop: $a, b \in K^\times$. Set $L = K(\sqrt{b})$.
Then $(a,b) = 1 \iff a \in N_{L/K}(L^\times)$.

Proof: If $L = K$, i.e. $b = c^2$ for c in K, then $(a,b) = 1$ since $c^2 - a\cdot 0^2 - b\cdot 1^2 = 0$ and $a \in N_{L/K}(L) = K$.

do assume $L \neq K$.

($\Leftarrow$) Suppose $a = N_{L/K}(\alpha)$ where $\alpha = z + y\sqrt{b}$ with $z, y \in K$

Thus $a = z^2 - y^2 b \Rightarrow z^2 - a \cdot 1^2 - b y^2 \Rightarrow (a,b) = 1$.

($\Rightarrow$) Conversely, suppose $(a,b) = 1$. Then

$$a = \frac{z^2}{x^2} - \frac{y^2}{x^2} b = N_{L/K}\left(\frac{z}{x} + \frac{y}{x}\sqrt{b}\right).$$ ▨

Basic props: (i) $(a,b) = (b,a)$ and $(a, c^2) = 1$.

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

(iii) $(a,b) = 1 \Rightarrow (aa', b) = (a', b)$ for all $a' \in K^\times$.

(iv) $(a,b) = (a, -ab) = (a, (1-a)b)$

Pf: (i) and (ii) are clear; (iv) follows from rest.

(iii) Have $a \in \underbrace{N_{L/K}(L^\times)}_{\text{subgroup of } K^\times}$. Then $aa' \in N_{L/K}(L^\times) \Leftrightarrow a' \in N_{L/K}(L^\times)$ ▨

For $K = \mathbb{R}$ or $K = \mathbb{Q}_p$, there are *explicit* formulas for (a,b). E.g. if $p \neq 2$

$$(a,b) = (-1)^{\alpha\beta\varepsilon(p)} \left(\frac{u}{p}\right)^{\beta} \left(\frac{v}{p}\right)^{\alpha} \quad \text{where} \quad \begin{aligned} a &= p^\alpha u \quad u \in \mathbb{Z}_p^\times \\ b &= p^\beta v \quad v \in \mathbb{Z}_p^\times \end{aligned}$$

and $\varepsilon(p) = \frac{p-1}{2}$.

Cor: Bilinearity $(aa', b) = (a,b)(a',b)$

Suppose $a, b \in \mathbb{Q}^\times$, v a place of $\mathbb{Q}$.

Let $(a,b)_v = (a,b)$ where a, b are regarded as elts of $\mathbb{Q}_p$.

Then Quadratic Reciprocity is equivalent to

Product Formula: Only finitely many $(a,b)_v \neq 1$, and

$$\prod_{v \text{ place of } \mathbb{Q}} (a,b)_v = 1.$$

Fact: Still true if we replace $\mathbb{Q}$ by a number field.

Quadratic forms over $\mathbb{Q}_p$: (V, q) nondegenerate

Choose a basis where $q(x) = \sum_{i=1}^{n} a_i x_i^2$.

$$\text{disc}(q) = \prod a_i \quad (\text{in } \mathbb{Q}_p^\times / (\mathbb{Q}_p^\times)^2)$$

$$\varepsilon(q) = \prod_{i<j} (a_i, a_j)$$

Prop: ε doesn't depend on the choice of diagonalizing basis.

Pf: See Serre.

Thm: Two nondegenerate quad forms on $\mathbb{Q}_p^n$ are isometric iff they have the same disc and ε.

Cor: For p odd, there are 8 quad forms on $\mathbb{Q}_p^n$.

Prop: If p is odd, then $\mathbb{Q}_p^\times / (\mathbb{Q}_p^\times)^2 \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$

Pf: Suppose $x \in \mathbb{Q}_p$. Then $x = p^k u$ with $u \in \mathbb{Z}_p^\times$. Since this expression is unique, x is a square iff k is even and $u \in (\mathbb{Z}_p^\times)^2$. Now u is a square iff $\bar{u}$ is a square in $\mathbb{F}_p$.
Let $v \in \mathbb{Z}$ be a non-square mod p.

Claim: $\mathbb{Q}_p^\times / (\mathbb{Q}_p^\times)^2 = \{1, v, p, vp\}$

First note the RHS is a subgp of the LHS.
Given $x = p^k u \in \mathbb{Q}^p$, mod the RHS we have

$$x \sim u \sim \begin{cases} 1 & \text{if } \bar{u} \text{ is a square mod } p \\ v & \text{otherwise.} \end{cases}$$