Lecture 8: Hilbert Reciprocity

Up to now: 1. Quadratic forms over general fields F (Witt's theorems, ...)

2. $F = \mathbb{F}_p$ classification

3. $F = \mathbb{Q}_p, \mathbb{R}$ (local fields) classification.

From now on: Number theory.

$F = \mathbb{Q}$.

"$F = \mathbb{Z}$"

General principle: To study $\mathbb{Q}$, first study $\mathbb{Q}_p$, $\mathbb{R}$, then see how they fit together.

Recall Hilbert symbols: $a, b \in \mathbb{Q}_p^\times$

$$\rightsquigarrow (a,b)_{\mathbb{Q}_p} \in \{\pm 1\}$$

$$:= \begin{cases} +1 & \text{if } aX^2 + bY^2 = Z^2 \text{ has a sol'n } \neq (0,0,0) \\ -1 & \text{otherwise.} \end{cases}$$

Same thing for $\mathbb{R}$ replacing $\mathbb{Q}_p$.

p odd:

$$(a,b)_{\mathbb{Q}_p} = (-1)^{v(a)v(b)} \cdot \frac{a^{v(b)} / b^{v(a)}}{p} \quad \left(\in \mathbb{Z}_p^\times\right)$$

$v(x) =$ p-adic valuation of x $\in \mathbb{Z}$

$x = p^{v(x)} \cdot u$

$u \in \mathbb{Z}_p^\times$

Ex:

- If $a, b \in \mathbb{Q}_p^\times$, then $(a,b)_{\mathbb{Q}_p} = +1$.
  ($\iff v(a) = v(b) = 0$)

- If $a \in \mathbb{Q}_p^\times$, $b = p$

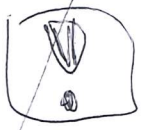
$$(a, p)_{\mathbb{Q}_p} = \left(\frac{a}{p}\right)$$

$\frac{x-1}{2} \in \mathbb{Z}_2 \downarrow \mathbb{Z}/2\mathbb{Z}$

$\equiv 1 \pmod 2$

$\mathbb{Q}_2^\times \to (\mathbb{Z}/2\mathbb{Z})^\times$

$\mathbb{Z}_2^\times \to 1$



not true for $p=2$. In fact, if $a, b \in \mathbb{Z}_2^\times$,

then $(a,b)_{\mathbb{Q}_2} = (-1)^{\frac{a-1}{2}\cdot\frac{b-1}{2}}$.

$$(a, 2)_{\mathbb{Q}_2} = (-1)^{\frac{a^2-1}{8}}$$

- $(a,b)_{\mathbb{R}} = -1 \iff b, a < 0$.

$x \in \mathbb{Q}^\times \Rightarrow v_p(x) = 0$ for all but finitely many p.

Cor: If $a, b \in \mathbb{Q}^\times$, then $(a,b)_{\mathbb{Q}_p} = +1$ for all but finitely many p.

Thm (Hilbert reciprocity): Let $a, b \in \mathbb{Q}$. Then

$$(a,b)_{\mathbb{R}} \cdot \prod_p (a,b)_{\mathbb{Q}_p} = +1$$

(infinite product reduces to a finite product by previous corollary)

Concretely: $aX^2 + bY^2 = Z^2$ does not have a nontrivial sol'n in $\mathbb{Q}$ is the set of places of $\mathbb{Q}$ in which finite & even.

$$\prod_v (a,b)_{\mathbb{Q}_v} = +1$$

$v = "\infty"$ $\quad \mathbb{Q}_v = \mathbb{R}$

Specialize to $a=p$, $b=q$ $\quad p, q$ distinct odd primes.

$$(p,q)_v = +1 \quad \text{if} \quad v \notin \{p, q, 2, \infty\}$$

$$(p,q)_{\mathbb{R}} = +1 \quad (p>0)$$

$$(p,q)_{\mathbb{Q}_2} = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

$$(p,q)_{\mathbb{Q}_p} = \left(\frac{q}{p}\right)$$

$$(p,q)_{\mathbb{Q}_q} = \left(\frac{p}{q}\right)$$

$\{+1$ unless $p \equiv 3 \pmod 4$ and $q \equiv 3 \pmod 4$, in which case -1

$\Rightarrow$ $\cancel{(-1)^{\frac{p-1}{2}\frac{q-1}{2}}} \cdot \left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$

$\left(\frac{13}{p}\right) = 1$

Hilbert reciprocity also gives (p odd prime)

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} \qquad a=-1 \quad b=p$$

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} \qquad a=2 \quad b=p$$

Tate's proof of Hilbert reciprocity

Step 1: Classify all symbols for $F=\mathbb{Q}_v$

Step 1.5: Deduce some relation of the form

$$\prod_v (a,b)_{a_v}^{\varepsilon_v} = +1$$

$$\varepsilon_v \in \{0,1\}$$

Step 2: Prove that the only possible such relation has $\varepsilon_v = +1$.

$\Rightarrow$ Hilbert reciprocity.

Recall: F field, A ab gp (written multiplicatively)

A <u>symbol</u> on F w/ values in A is a function

$$\varphi : F^\times \times F^\times \longrightarrow A$$

such that: $\varphi(a,b) = \varphi(b,a)^{-1}$

1) $\varphi(ab, c) = \varphi(a,c) \cdot \varphi(b,c)$

$\varphi(a, bc) = \varphi(a,b) \cdot \varphi(a,c)$

2) $\varphi(a,b) = 1$ if $a+b = 1$ $\quad (a,b \in F^\times)$

<u>Ex:</u> On $\mathbb{Q}_p$, the Hilbert symbol $(\cdot,\cdot)_{\mathbb{Q}_p}$ is a symbol w/ values in $\{\pm 1\}$.

Rk: If $E \xrightarrow{f} E$ is a homomorphism of fields & φ is a symbol on E, then $\varphi \circ f$ is a symbol on F.

$\Rightarrow$ $(\ ,\ )_{\mathbb{Q}_p}$ restricts to a symbol on $\mathbb{Q}$.

Ex: For p prime, $\exists$ tame symbol on $\mathbb{Q}$

$$(a,b)_p := (-1)^{v_p(a)\cdot v_p(b)} \cdot \left(a^{v_p(b)} / b^{v_p(a)} \right)$$

$\mathbb{F}_p^\times$

$p=2$ trivial

Universal symbol: Set A to be the free abelian gp on set $F^\times \times F^\times$

~~subject to follow~~

modulo subgp generated by

(ab, c)

$(a, c)^{-1} (b, c)^{-1}$

$(a, bc) \cdot (a, b)^{-1} (a, c)^{-1}$

$(a, 1)$ for $a \neq 1$.

~~(A)~~ The A is denoted $K_2(F)$.

($K_1(F)$ the all is to exist)

∃ symbol on F w/ values in $K_2(F)$

defined by

$(a,b) \mapsto$ image of (a,b) in $K_2(F)$

$(=: \{a,b\})$

Moreover, bijection

$$\left\{\begin{array}{c}\text{symbols on } F \\ \text{w/ values in } A\end{array}\right\} \longleftrightarrow \left\{\text{homomorphisms } K_2(F) \to A\right\}$$

$F^\times \times F^\times$

Thm (Tate): $K_2(\mathbb{Q}) \cong A_2 \oplus A_3 \oplus A_5 \oplus \cdots$

$A_2 = \{\pm 1\}$

$A_p = (\mathbb{Z}/p\mathbb{Z})^\times$ p odd.

$\{a,b\} \mapsto \left((a,b)_{\mathbb{Q}_2}, (a,b)_3, (a,b)_5, \ldots \right)$

A_2