Lecture 5

Recap: In lecture 4, we learned

$$\mathbb{Z}_p = \left\{ \sum_{n\geq 0} b_n p^n : b_n \in \{0,\dots,p-1\} \right\}$$

$$= \left\{ (a_n) \in \prod_{n\geq 1} \mathbb{Z}/p^n\mathbb{Z} : a_{n+1} \equiv a_n \bmod p^n \right\}$$

$$(a_n)_{n\geq 1} \longleftrightarrow \sum_{n\geq 0} b_n p^n$$

$$a_n \equiv \sum_{i=0}^{n-1} b_i p^i \bmod p^n \qquad b_0 = a_1,\ b_n = (a_{n+1} - a_n)/p^n$$

$$\mathbb{Q}_p = \mathrm{Frac}(\mathbb{Z}_p) = \left\{ \sum_{n\geq k} b_n p^n : b_n \in \{0,\dots,p-1\},\ k \in \mathbb{Z} \right\}$$

Q: When does a quaternion algebra $(a,b)_{\mathbb{Q}}$ split over $\mathbb{Q}$? (i.e., when does $ax^2+by^2=1$ have a $\mathbb{Q}$-pt?

Rmk: Since $\mathbb{Q} \subseteq \mathbb{R}, \mathbb{Q}_p$ $\forall p$ splitting over $\mathbb{Q}$ $\Rightarrow$ splitting over $\mathbb{R}, \mathbb{Q}_p$.

Today: The converse! We need a bookkeeping tool.

Def Let v denote either a prime p or ∞. For $a,b \in \mathbb{Q}^\times$ the Hilbert symbol $(a,b)_v \in \{-1,1\}$ is defined by

$$(a,b)_v = \begin{cases} +1 & \text{if } ax^2+by^2=1 \text{ has a soln in } \mathbb{Q}_v \\ -1 & \text{if } ax^2+by^2=1 \text{ has No soln in } \mathbb{Q}_v \end{cases}$$

Where $\mathbb{Q}_\infty := \mathbb{R}$.

Made with Goodnotes

Recall that over $\mathbb{R}$, this amounts to checking whether a or b are >0, i.e.

$$(a,b)_\infty = \begin{cases} -1 & \text{if } a,b<0 \\ 1 & \text{otherwise} \end{cases}$$

It turns out that for odd primes p, there is also a straightforward condition to check.

Computational rules for $(a,b)_p$:

Let p be an odd prime and a,b be nonzero integers.

1. If $p \nmid a$ and $p \nmid b$ then $(a,b)_p = +1$

2. If $p \mid a$ and $p \nmid b$, write $a = p^k a'$ where $k = v_p(a)$ (and $p \nmid a'$). Then $(a,b)_p = \left(\frac{b}{p}\right)^k$, where $\left(\frac{b}{p}\right)$ is the Legendre symbol.

Note: If $p \mid a$ and $p \mid b$, we can reduce to one of the cases above. Lecture 2 tells us $(a,b)_p$ depends only on a,b up to squares. So we can reduce to $a = pa'$, $b = pb'$ w/ $p \nmid a', b'$. Then Lecture 2 tells us that $(pa', pb')_{\mathbb{Q}} \simeq (-a'b', pa')_{\mathbb{Q}}$.

not divisible by p.

Why does this work? One needs to understand square classes in $\mathbb{Q}_p^\times$.

Note that for $\mathbb{R}^\times/(\mathbb{R}^\times)^2$ the coset reps are $\{1,-1\}$.

Made with Goodnotes

Some of the ingredients involved:

(1) Let $u \in \mathbb{Z}_p^\times$. Recall this means $u = \sum_{n \geq 0} b_n p^n$ w/ $b_0 \neq 0$, i.e., $p \nmid u$.

Then in the exercises you'll show that u is a square in $\mathbb{Z}_p$ iff its reduction mod p is a square in $\mathbb{Z}/p\mathbb{Z}$.

(2) Square classes in $\mathbb{Q}_p^\times$ (for odd p):

$\mathbb{Q}_p^\times / (\mathbb{Q}_p^\times)^2$ has only 4 elements: coset reps are $\{1, u, p, pu\}$ where u is a nonsquare unit in $\mathbb{Z}_p^\times$.

(3) The Hilbert symbol $(a,b)_p$ depends only on the square classes of a, b in $\mathbb{Q}_p^\times$. So need only to determine the Hilbert symbol for pairs from the finite list $\{1, u, p, pu\}$.

Ex: $(p,p)_{\mathbb{Q}_p} \simeq (p,-1)_{\mathbb{Q}_p}$ by Lecture 2.

Let's consider $px^2 - y^2 = 1$ over $\mathbb{Q}_p$.

If -1 is a square mod p, then by (1), -1 is a square in $\mathbb{Z}_p^\times$, say $y^2 = -1$. So $(0, y)$ is a soln.

Conversely, if (x, y) is a solution in $\mathbb{Q}_p$, then by computing valuations, one finds $x, y \in \mathbb{Z}_p$.
Reducing mod p gives $y^2 \equiv -1 \bmod p$. So by (1), -1 is a square in $\mathbb{Z}_p^\times$.

Thus $(p,p)_p = (p,-1)_p = \left(\frac{-1}{p}\right)$.

$v_p(1) = 0$
$v_p(px^2 - y^2) = \min\{1 + 2v_p(x), 2v_p(y)\}$
so $v_p(x), v_p(y) \geq 0$.

Made with Goodnotes

Back to our main goal...

Theorem (Hasse-Minkowski for conics)
Let $a, b \in \mathbb{Q}^\times$. A conic defined by $ax^2+by^2=1$ has a solution over $\mathbb{Q}$ iff it has a solution over $\mathbb{R}$ and over $\mathbb{Q}_p$ for every prime p.

($\Rightarrow$) is immediate since $\mathbb{Q} \subseteq \mathbb{R}, \mathbb{Q}_p$. The converse is a deep result!

In other words $(a,b)_{\mathbb{Q}}$ splits iff $(a,b)_{\mathbb{R}}$ and $(a,b)_{\mathbb{Q}_p}$ splits for all p.

Let's apply this result to an example:

Does the equation $3x^2+5y^2=1$ have any solutions in $\mathbb{Q}$?

We now know we can study the quaternion algebra $(3,5)_{\mathbb{Q}}$. We'll start computing Hilbert symbols.

Recall that we need only to check $\mathbb{R}$, $\mathbb{Q}_2$, and $\mathbb{Q}_p$ for p dividing a or b.

- $v=\infty$: $(3,5)_\infty = 1$ since $3,5>0$. There are lots of solutions over $\mathbb{R}$.

Made with Goodnotes

- $p=3$: We have $3 \nmid 5$ but $3 \mid 3$, and $v_3(3)=1$.

So $(3,5)_3 = \left(\frac{5}{3}\right)^1 = \left(\frac{2}{3}\right)^1$ by rules of Hilbert symbol.

Since 2 is not a square mod 3, this tells us

$(3,5)_3 = -1$, ie., $3x^2+5y^2=1$ has NO $\mathbb{Q}_3$ solns.

This tells us that $3x^2+5y^2=1$ cannot have any solutions over $\mathbb{Q}$!

Lemma: If A, A' are isomorphic quaternion algebras over $\mathbb{Q}$, then they are also isomorphic over $\mathbb{R}$ and $\mathbb{Q}_p$ for all primes p.

The contrapositive says that if A, A' have different splitting behavior for even just one prime p, then they cannot be isomorphic over $\mathbb{Q}$.

Theorem: There exist infinitely many mutually non-isomorphic quaternion algebras over $\mathbb{Q}$.

Proof idea: Consider the family of algebras $A_p = (-1,p)_{\mathbb{Q}}$ for $p \equiv 3 \bmod 4$.

Made with Goodnotes

- $(-1, p)_p = \left(\frac{-1}{p}\right) = -1$ so A_p is nonsplit over $\mathbb{Q}_p$
- If $q \neq p$ is a prime w/ $q \equiv 3 \bmod 4$, then Exercise 5.19 asks you to show that A_p splits over $\mathbb{Q}_q$.
- Conclude that A_p and A_q are not isom over $\mathbb{Q}$ when $p \neq q$. ∎

Made with Goodnotes