Talk 6: Forms over $\mathbb{Q}_p$ & the Hasse principle

1 Recap of previous talks

- **Talk 1 & 2.** A quadratic form $\mathbf{f}(x_1, ..., x_n) = \sum_{i,j=1}^{n} a_{ij}x_ix_j (a_{ij} \in k)$ is said to *regular* if $d(\mathbf{f}) := det(a_{ij}) \neq 0$ and hence lies in $k^*/(k^*)^2$. It is moreover called *isotropic* if it admits a non-trivial solution in k^n.
  For two regular quadratic forms $\mathbf{f}(x_1, ..., x_n), \mathbf{g}(y_1, ..., y_m)$, if $\mathbf{f}(\underline{x}) - \mathbf{g}(\underline{y})$ is isotropic, then there is a $b \neq 0$, represented by both $\mathbf{f}, \mathbf{g}$.
  (*Witt's lemma*) If $f_i(\underline{x}), g_i(\underline{y})$(i=1,2), are quadratic forms(f_i regular) s.t. $f_1(\underline{x})+g_1(\underline{y}) \sim_k f_2(\underline{x})+g_2(\underline{y})$ and $f_1(\underline{x}) \sim_k f_2(\underline{x})$. Then $g_1 \sim_k g_2$.

- **Talk 3.** Here we learnt about the field of $p-$adic numbers $\mathbb{Q}_p(p$ a prime). It is the completion of $\mathbb{Q}$ w.r.t. the non-Archimedean valuation $|.|_p$. The *unit ball*(which is also a ring) $\mathbb{Z}_p := \{|x|_p \leq 1\}$ is called the ring of *$p-$adic integers*.

- **Talk 4.** Here we studied *Hensel's lemma* which gives sufficient conditions to lift a solution of $f(T) \in \mathbb{Z}_p[T]$ over $\mathbb{F}_p \simeq \mathbb{Z}_p/p\mathbb{Z}_p$ to $\mathbb{Z}_p$. Moreover if $f(T_1, ..., T_n) \in \mathbb{Z}[T_1, ..., T_n]$ has a solution in each $\mathbb{Z}/p^n\mathbb{Z}(\forall n > 0)$, then it has a solution in $\mathbb{Z}$.

- **Talk 5.** For p, a prime number or ∞, the *Hilbert norm residue symbol*, $\left(\frac{a,b}{p}\right)(a, b \in \mathbb{Q}_p^*)$,

$$\left(\frac{a,b}{p}\right) = \begin{cases} 1, & P(a,b) \text{ is isotropic;} \\ -1, & \text{otherwise} \end{cases}$$

where $P(a, b) = aX^2 + bY^2 - Z^2$ It satisfies among many other properties, $\left(\frac{a_1,b}{p}\right)\left(\frac{a_2,b}{p}\right) = \left(\frac{a_1a_2,b}{p}\right)$. Also we have the *product formula*

$$\prod_{p \in \text{primes} \cup \infty} \left(\frac{a,b}{p}\right) = 1$$

2 Equivalence of forms over $\mathbb{Q}_p$

We can give a purely arithmetic characterization of equivalent regular quadratic forms over $\mathbb{Q}_p(p$ a prime number).

Definition 2.1. The form $f(\underline{x})$ over $\mathbb{Q}_p$ be equivalent to a diagonal form $a_1x_1^2+..., a_nx_n^2$.

1. $n(f) := n$ is the rank of the form f.
2. $d(f)$ is the class of determinant $det(f) \in \mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2$.
3. $c(f) := \prod_{i<j} \left(\frac{a_i,a_j}{p}\right)$

All the three numbers defined above are invariant under the equivalence of forms.

Theorem 2.2.
- *For two regular quadratic forms f_1, f_2 over $\mathbb{Q}_p$, $(n(f_1), d(f_1), c(f_1)) = (n(f_2), d(f_2), c(f_2)) \iff f_1 \sim_{\mathbb{Q}_p} f_2$.*
- *Analogously, for a form over $\mathbb{Q}_\infty = \mathbb{R}$, the pair $(n(f), s(f))$ determine the equivalence class of f, where $s(f)$ is the number of negative coefficients in a diagonalization of f.*

3 Hasse principle

Also known as the *local-global principle*, this is a philosophical statement of the form
Hasse principle. *A property or theorem* ***P*** *holds true over* $\mathbb{Q} \iff$ *the property or theorem* ***P*** *holds true over* $\mathbb{Q}_p$ *and over* $\mathbb{Q}_\infty = \mathbb{R}$.

This principle first formulated in its present day form by *Helmut Hasse*(1898-1979) in the context of *H. Minkowski's*(1864-1909) theorem on existence of integral solutions of a form over $\mathbb{Z}$ from its solutions in each residue ring $\mathbb{Z}/N\mathbb{Z}$.

Theorem 3.1 (Strong Hasse principle)**.** *A (regular) quadratic form on* $n-$*variables over* $\mathbb{Q}$ *is isotropic* $\iff$ *it is isotropic over all* $\mathbb{Q}_p$ *(p a prime) and over* $\mathbb{R}$.

Consequently, we obtain

Corollary 3.2 (Weak Hasse principle)**.** *If two regular quadratic forms* $f \sim_{\mathbb{Q}} g \iff f \sim_{\mathbb{Q}_p} g\ \forall p$*(including* $p = \infty$*).*

4 Counterexample(s)

When one goes beyond the setup of degree 2 homogeneous forms, one encounters a lot of counterexamples to the Hasse principle.

- (Lind-Reichardt(1940's)) They (independently) showed that the equation $X^4 - 17Y^4 = Z^2W^2$ has local solutions(i.e. in all $\mathbb{Q}_p$ and $\mathbb{R}$) but it has no solution in $\mathbb{Q}$.

•(Selmer(1951)) The equation $F(X, Y, Z) := 3X^3 + 4Y^3 + 5Z^3$ has solutions in each $\mathbb{Q}_p$(inc. $p = \infty$) but no solution in $\mathbb{Q}$.

We'll focus our attention on the counterexample of Selmer(cf. [Con, §2]). We'll use Hensel's lemma to show that it has solution in each $\mathbb{Q}_p$(inc. $\mathbb{R}$). Showing that it has no solution in $\mathbb{Q}$ requires techniques from the theory of *elliptic curves* and goes well beyond our scope(cf. [Cas2, pg.86-87])[a].

Example 4.1.
- (in $\mathbb{Q}_3$) Setting $(X, Z) = (0, -1)$, $F(0, Y, -1) = 4Y^3 - 5$ has a solution $Y = 2$ in $\mathbb{Z}/3\mathbb{Z}$. Using Hensel's lemma lift to $\beta \in \mathbb{Z}_3$(using $|f(2)|_3 < |f'(2)|_3^2$). $(0, \beta, -1)$ is a solution.
- (in $\mathbb{Q}_5$) Setting $(Y, Z) = (0, 1)$, the equation $g(X) := 3X^3 + 5$ has a solution $X = 2$ in $\mathbb{Z}/5\mathbb{Z}$ which is a cube there(exercise!), so it can be lifted using Hensel's lemma.
- (in $\mathbb{Q}_p, p \neq 3, 5$) Here one separately analyzes
  - 3 mod p is a cube, then $X^3 + 3$ has a root in $\mathbb{Z}/p\mathbb{Z}$, hence can be lifted to $\mathbb{Z}_p$.
  - 3 mod p is not a cube, then $p \equiv 1(\mod 3)$ and any $a \in (\mathbb{Z}/p\mathbb{Z})^*$ can be written $b^3, 3b^3$ or $9b^3$. One chooses $a = 5$ and uses Hensel's lemma.
- (in $\mathbb{R}$) Obvious.

[a] One can alternately prove it using the arithmetic of *cubic field extensions* cf. [Con, §3]

References

[Con] Keith Conrad: *Selmer's example.*

[Cas1] J.W.S. Cassels: Rational quadratic forms.

[Cas2] J.W.S. Cassels: Lectures on elliptic curves.