DESCENT AND BRAUER-MANIN OBSTRUCTION

David Harari
Université de Paris-Sud

GOALS:

- Give necessary conditions (if possible "computable"!) for the set of rational points of a variety X being $\neq \emptyset$.
- Find families of varieties for which those conditions are sufficient.
- Describe the closure of $X(\mathbb{Q})$ in $X(\mathbb{A}_{\mathbb{Q}})$.

I. Some reciprocity laws in arithmetic

k number field ($[k:\mathbb{Q}] < \infty$)

For each place v of k, set

$k_v :=$ completion of k at v

__ex__: $k = \mathbb{Q}$, we have the p-adic fields $\mathbb{Q}_p$ (p prime) and the field $\mathbb{Q}_\infty = \mathbb{R}$ of real numbers.

I.1. The "simplest" reciprocity law: product formula

Let $r \in \mathbb{Q}^*$, $r = \pm p_1^{\alpha_1} \cdots p_r^{\alpha_r}$

(p_i prime, $\alpha_i \in \mathbb{Z}$).

For any completion $\mathbb{Q}_v$ of $\mathbb{Q}$ and any $x_v \in \mathbb{Q}_v$, set $|x_v|_v := p^{-v(x_v)}$

if $\mathbb{Q}_v = \mathbb{Q}_p$ for p prime number

($v(x_v)$ = p-adic valuation of x_v);

$|x_v|_v$ is the normalized absolute value of x_v.

If $v = \infty$, $\mathbb{Q}_v = \mathbb{R}$, define $|x_v|_v$ = usual absolute value of $x_v \in \mathbb{R}$.

Let Ω_φ be the set of all places of φ. Then for any $r \in \varphi$, we have:

$$\boxed{\prod_{v \in \Omega_\varphi} |r|_v = 1 \quad \text{(product formula)}}$$

indeed $|r|_\infty = p_1^{d_1} \cdots p_r^{d_r}$

$|r|_v = p_i^{-d_i}$ if v corresponds to p

$|r|_v = 1$ for other v.

<u>Corollary</u>: Let $(r_v) \in \prod_{v \in \Omega_{\mathbb{Q}}} \mathbb{Q}_v^*$.

If the "local" (r_v) comes from a "global" $r \in \mathbb{Q}^*$, then:

i) $v(r_v) = 0$ for almost all v (i.e. (r_v) is an idele).

ii) The product formula $\prod_{v \in \Omega_{\mathbb{Q}}} |r_v|_v = 1$ must be satisfied.

$\to$ first example of reciprocity law.

This extends to any number field k (with the right normalizations for $|\cdot|$).

I.2. The quadratic reciprocity law: classical formulation.

$p \neq 2$ prime number, $x \in (\mathbb{Z}/p\mathbb{Z})^*$,

define $\left(\frac{x}{p}\right) = x^{\frac{p-1}{2}} \in \{\pm 1\}$

(Legendre symbol).

set $\left(\frac{0}{p}\right) = 0$ and $\left(\frac{x}{p}\right) := \left(\frac{\bar{x}}{p}\right)$ for $x \in \mathbb{Z}$.

Then $\left(\frac{x}{p}\right) = 1 \iff x$ is a square mod. p

Properties: $\left(\frac{xy}{p}\right) = \left(\frac{x}{p}\right)\left(\frac{y}{p}\right)$

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

Th [Gauss] (Quadratic reciprocity law).

Let l, p be distinct prime numbers. Then:

$$\boxed{\left(\frac{l}{p}\right) = \left(\frac{p}{l}\right) \cdot (-1)^{\frac{(p-1)(l-1)}{4}}}$$

very useful to compute Legendre symbols, e.g. $\left(\frac{29}{43}\right) = \left(\frac{43}{29}\right) = \left(\frac{14}{29}\right) = \left(\frac{2}{29}\right) \cdot \left(\frac{7}{29}\right)$

$$= -\left(\frac{7}{29}\right) = -\left(\frac{29}{7}\right) = -\left(\frac{1}{7}\right) = -1$$

The link to a "local-global" statement is not obvious for the moment → have to use Hilbert's symbo

I.3. The quadratic reciprocity law via Hilbert symbols

Let $K = \mathbb{R}$, $\mathbb{C}$, or a p-adic field := finite extension of $\mathbb{Q}_p$.

(typically K := completion of a number field at some place).

For $a, b \in K^*$, define the Hilbert symbol $(a,b) \in \mathbb{Z}/2$ by:

$(a,b) = 0$ if $z^2 - ax^2 - by^2 = 0$ has a non-trivial solution in K.

$(a,b) = 1$ else.

(of course if $K = \mathbb{C}$, the (a,b) is always 0).

<u>Properties</u>: • $(a,b)=0 \iff a$ is a norm of $K(\sqrt{b})/K$.

• $(a,b)=(b,a)$ $\quad (a,c^2)=0$

• $(a,-a)=0$ $\quad (a,1-a)=0$.

<u>Th</u>: The Hilbert symbol is bilinear, that is: $(aa',b) = (a,b)+(a',b)$

Can be proved over $\mathbb{Q}_p$ using explicit computations with Legendre symbols. More complicated in general (see next talk).

We can now state the reciprocity law for Hilbert symbol:

Th: let k be a number field

$(a,b) \in k^* \times k^*$, $(a,b)_v :=$ Hilbert symbol of a,b in k_v, $\Omega_k :=$ set of all places of k. Then:

i) $(a,b)_v = 0$ for almost all places v of k.

ii) $$\sum_{v \in \Omega_k} (a,b)_v = 0$$

i) is easy using Hensel's lemma (implies that if $v \nmid 2ab$, then $z^2 - ay^2 - bx^2 = 0$ has a non trivial solution in k_v).

Let us explain ii) when $k = \mathbb{Q}$.

Using bilinearity, the significant case is $a = \ell$, $b = \ell'$ distinct odd prime numbers. Then:

$$(\ell, \ell')_2 = (-1)^{\frac{(\ell-1)}{2}\frac{(\ell'-1)}{2}}$$

$$(\ell, \ell')_\ell = \left(\frac{\ell'}{\ell}\right) \qquad (\ell, \ell')_{\ell'} = \left(\frac{\ell}{\ell'}\right)$$

$(\ell, \ell')_v = 0$ else, hence the result follows from the quadratic reciprocity law.

(But the statement with Hilbert symbols is the same for all number fields).

Reformulation:

Set $K = k(\sqrt{a})$, $K_v = K \otimes_k k_v$,

then the reciprocity law says that there is a complex:

$$k^*/NK^* \longrightarrow \bigoplus_{\text{all } v} k_v^*/NK_v^* \xrightarrow{j} \mathbb{Z}/2$$

(each k_v^*/NK_v^* is 0 or $\mathbb{Z}/2$, so it is naturally embedded in $\mathbb{Z}/2$; the map j is the sum of those embeddings).

Actually the sequence above is exact (uses Dirichlet's theorem about primes in arithmetic progression)

Class field theory yields the exact sequence as above for any cyclic extension K/k;

For every K/k cyclic, the first map is injective, but not in general!

(ex: -1 is a local norm everywhere but not a global norm for $k = \mathbb{Q}$, $K = \mathbb{Q}(\sqrt{13}, \sqrt{17})$).

I.4. An application to rational points of algebraic varieties

Consider the surface

$$V: \quad y^2 + z^2 = (x^2-2)(3-x^2) \neq 0 \text{ over } \mathbb{Q}.$$

Th [Iskovskih] V is a counter-example to the Hasse principle.

Namely $V(\mathbb{Q}_p) \neq \phi$ for all p prime and $p = \infty$

But $V(\mathbb{Q}) = \phi$.

Idea of the proof:

i) $V(\varphi_p) \neq \emptyset$ is easy using Hensel's lemma.

ii) Let (x_p, y_p, z_p) be a solution of φ_p.

The local computations show that:

If $p \neq 2$, $(-1, x_p^2 - 2)$ must be zero.

If $p = 2$, $(-1, x_2^2 - 2)$ must be $\neq 0$.

Hence a rational solution (x, y, z) would not satisfy $\sum_{v \in \Omega_\varphi} (-1, x^2 - 2)_v = 0$ IMPOSSIBLE.

This is an example of Brauer-Manin obstruction $\rightsquigarrow$ next talk...