Rational Points Talk 1

Adèle Ring

Let K be a global field, let Ω_K denote the set of places of K. Let S be a finite set $S \subseteq \Omega_K$ containing all archemedian places

$$\mathcal{O}_{K,S} = \{a \in K \mid v(a) \geq a \quad \forall v \notin S\}$$

the ring of S-integers

Def Given k global field the adèle ring of k $\mathbb{A}_k$ is

$$\mathbb{A}_k = \prod_{v \in \Omega_K}{}' (k_v, \mathcal{O}_{k_v})$$

i.e

$$\mathbb{A}_k = \left\{ (x_v) \in \prod_v k_v \;\middle|\; x_v \in \mathcal{O}_{k_v} \text{ for all but finitely many } v \right\}$$

We equip $\mathbb{A}_k$ with the unique topology s.t.

- $\mathbb{A}_k$ is a topological group (topological space, $\cdot$, $\cdot^{-1}$ continuous)
- $\prod_{v \in \Omega_K} \mathcal{O}_{k_v}$ is open
- the subspace topology on $\prod_{v \in \Omega_K} \mathcal{O}_v$ agrees w/ product topology.

KEY QUESTIONS

Let k be a field and X a variety over k.

- Does X have a k-rational pt?

↳ To answer over arbitrary X is equivalent to Hilbert's 10^{th} problem over k:
Does there exist an algorithm taking in $f(x_1, \ldots, x_n) \in k[x_1, \ldots, x_n]$ & puts out YES or NO according to if $\exists\, a \in k^n$ s.t $f(a) = 0$

- Is $X(k)$ finite? If so can we list all the points?

- Is $X(k)$ Zariski dense in X?
- OR does there exist finite L/k s.t. $X(L)$ is Zariski dense in X?

Hasse Principle — ~~Does~~ For k global, does
$$X(k_v) \neq \emptyset \ \forall v \in \Omega_k \Rightarrow X(k) \neq \emptyset$$

Counter-Ex. $(x^2-2)(x^2-17)(x^2-34)$ $/\mathbb{Q}$

For v archemedian k_v has $\sqrt{2}$ $\sqrt{7}$ $\sqrt{34}$ ✓

- For $v=2$ has solution. - indeed
$$1^2 - 17 \equiv 0 \bmod 8$$
so Hensel's Lemma gives soln in $\mathbb{Q}_2$
- For $v=7$ we have
$$3^2 - 2 \equiv 0 \bmod 7$$
so Hensel's lemma gives soln in $\mathbb{Q}_7$
- For finite $p \neq 2,7$ either 2 or 7 is a square mod p so Hensel gives soln. OR neither 2 nor 7 is a square mod p so 34 is giving soln. via Hensel.
- Clearly $(x^2-2)(x^2-17)(x^2-34)$ has no $\mathbb{Q}$ soln.

- For k global, $v \in \Omega_k$ is $X(k)$ dense in $X(k_v)$? (wrt v-adic topology)

Weak Approx. — Is $X(k) \to \prod_v X(k_v)$ dense wrt product topology of v adic topologies?

Weak Weak Approx. — Is $X(k) \to \prod_{v \notin S} X(k_v)$ dense where S is a finite set?

Strong Approx. - Is $X(k) \to X(\mathbb{A}_k)$ dense wrt adelic topology?

- Is $X(k) \to X(\mathbb{A}_k^S)$ dense wrt adelic topology where $S \subseteq \Omega_k$ is finite?

- Given H a height function on $\mathbb{P}^n(k)$ for $X \subseteq \mathbb{P}^n_k$
$$N_X(B) = \#\{x \in X(\cancel{k}) \mid H(x) \leq B\}$$
$\Rightarrow$ Can one predict growth of $N_X(B)$ as $B \to \infty$ (Manin's conjecture).

What is known

Let X be a nice curve over a global field k of genus g

$g=0$ Either $X(k) = \emptyset$ or $X(k) \cong \mathbb{P}_k$

$g=1$ w/ specified rat. pt. we have ell. curve. Mordell-Weil tells us
$X(k)$ is fin. gen. abelian group.
~~Torsion is one of~~ For $k=\mathbb{Q}$ the torsion is one of

(Mazur) 15 groups. Rank hard to calculate.

$g \geq 2$ (Faltings) $X(k)$ is finite.
(~~Note~~ Not effective i.e can't find the points).

For X abelian variety we have Mordell-Weil.

Thrm (Hasse-Minkowski) The Hasse principle holds for quadratic forms (i.e. degree 2 homogeneous polynomials).

· Hilbert's 10^{th} problem is known not to hold for global function fields.

Aims of reading group

Faithfully Flat ~~Desc~~ Descent:

To describe a scheme X/S it is enough to describe a scheme Y/T - where $T \to S$ is faithfully flat - along with 'descent data'. For us this may mean describing a scheme over a finite ext. L/k instead ~~of~~ over k.

Why? If X/S is descended from Y/T, X inherits properties from Y.

Brauer Manin Obstruction:

This is a cohomological obstruction to the Hasse principle.

For given variety X/k we construct a set

$$X(\mathbb{A}_k)^{Br}$$

such that $X(k) \hookrightarrow X(\mathbb{A}_k)^{Br} \hookrightarrow X(\mathbb{A}_k)$.

It is possible $X(\mathbb{A}_k) \neq \emptyset$ but ~~$X(\mathbb{A}_k)$~~ $X(\mathbb{A}_k)^{Br} = \emptyset$ - we call this the Brauer Manin obstruction.

Descent

Another cohomological obstruction to the Hasse principle. Again we construct set

$$X(\mathbb{A}_k)^{descent}$$

such that ~~$X(\mathbb{A}_k)^{descent}$~~ $X(k) \hookrightarrow X(\mathbb{A}_k)^{descent}$.

This is done via the theory of Selmer groups.

STRONGER Than Brauer-Manin.

- the subspace toplogy on $\prod_{v \in \Omega_K} \mathcal{O}_v$ agrees w/ product toplogy.

Étale Algebras

This is the generalised notation of finite sep. field ext.

Problem: L/K field ext. K'/K field ext.
$L \otimes_K K'$ might not be a field!

Ex $K = \mathbb{Q}$. $\mathbb{Q}(\sqrt{5}) \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{7}) \cong \mathbb{Q}(\sqrt{5}, \sqrt{7})$ sep. field ext.
But! $\mathbb{Q}(\sqrt{5}) \otimes \mathbb{Q}(\sqrt{5}) \ncong \cancel{\mathbb{Q}(\sqrt{5})}$ not a field!

Def A K-algebra L is étale if one of the following equivalent conditions hold

- L direct prod. of fin. sep. ext. of K
- $L \otimes_K K_s$ is a finite product of copies of K_s
- $\operatorname{Spec} L \to \operatorname{spec} K$ is finite & étale.

A morphism of étale algebras is a morphism of K-alg.

Grothendieck generalised Galois theory to étale algebras:

Thm The functors

i.e set G_K acts on

$$\{\text{finite } G_K\text{-sets}\}^{op} \longleftrightarrow \{\text{étale } k\text{-algebras}\}$$

$$S \longmapsto \operatorname{Hom}_{G_K\text{-sets}}(S, K_s) = \operatorname{Hom}_{sets}(S, K_s)^{G_K}$$

$$\operatorname{Hom}_{K\text{-alg}}(L, K_s) \longleftarrow L$$

are inverse equivalences of categories.

Recall C^{opp}. $Ob(C^{op}) := Ob(C)$
$\operatorname{Hom}_{C^{op}}(a, b) = \operatorname{Hom}_C(b, a)$

ex. Let S be transitive G_K set, i.e $S = G_K/H$ for H open subgroup of G_K the corr. étale algebra is $\mathrm{Hom}_{G_K\text{-sets}}(G_K/H, k_s) = (k_s)^H$.

In general finite G_K set S is finite disjoint union $\coprod_i S_i$ of transitive G_K sets.
If S_i corr to the finite sep. ext. L_i then S corr to $\prod L_i$.

Def Let L be an étale alg w/ left action by a finite group G. If ~~Ω~~ Ω/k is a field ext. then $L \otimes_k \Omega$ is an étale Ω-alg. w/ left G action & so is $\prod_{g\in G} \Omega = \mathrm{Hom}_{\text{sets}}(G, \Omega)$ via the right translation G-action on G.
We call L a Galois étale k-algebra w/ Galois group G if for some field ext. Ω/k $L \otimes_k \Omega \simeq \prod_{g \in G} \Omega$ as étale Ω-algebras.

Why must we specify G?

Ex $L = k \times k \times k \times k$
S_4, $\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ all act on L
W/ $\mathbb{Z}/4\mathbb{Z} \curvearrowright L$ we ~~set~~ see
L is a Galois étale k-alg w/ Galois group $\mathbb{Z}/4\mathbb{Z}$
Since $L \otimes_k k \cong \prod_{g \in \mathbb{Z}/4\mathbb{Z}} k$

equally w/ $\mathbb{Z}/2\mathbb{Z} \circ \mathbb{Z}/2\mathbb{Z}$. But $\mathrm{Aut}(L/k) = S_4$
i.e Gal $\neq$ Aut.

Galois descent:

L/k finite Galois ext. w/ G.G. G. An action of G on an L-vector space is semilinear if $\forall \sigma \in G$ $l \in L$, $w \in W$

$$\sigma(lw) = \sigma(l)\sigma(w)$$

Ex. $W = L^n$
define $G \circlearrowright W$ by
$$\sigma(\omega_1, \dots, \omega_n) = (\sigma(\omega_1), \dots \sigma(\omega_n))$$

Let $W^G = \{w \in W \mid gw = w \ \forall g \in G\}$

Lemma Let V be a k-v.s.
$$V \mapsto (V \otimes_k L)^G$$
$$v \longmapsto v \otimes 1$$
is an isomorphism

Lemma. Let W be an L-v.s. with semilinear G-action then
$$W^G \otimes_k L \longrightarrow W$$
$$w \otimes l \rightarrow lw$$
is an isomorphism.

Thm Let L/k be a finite Galois ext. of fields w/ Galois group G. The functors
$$\{k\text{-v.s}\} \underset{G\text{-invariants}}{\overset{\otimes_k L}{\rightleftarrows}} \{L\text{-v.s. w/ semilinear } G\text{-action}\}$$
are inverse equivalences of categories

Cor L/k finite Galois ext. of fields w/ galois group G
For each $r \in \mathbb{Z}_{\geq 0}$ $\exists$ only one r-dim L-v.s w/ semilinear G action up to isomorphism

Group / Galois Cohomology

Let G be a finite group
$$\mathbb{Z}G = \{ \sum_{g\in G} n_g g \mid n_g \in \mathbb{Z}\}$$
the integral group ring.

Let M be a $\mathbb{Z}G$-module.
For all $i \in \mathbb{Z}_{\geq 0}$ $\exists$ a unique group
$$H^i(G, M)$$
the ith cohomology group of G by M.

Ex. - $H^0(G,M) = M^G = \{ m\in M \mid gm = m \ \forall g \in G\}$
the invariants.

- $$H^1(G,M) = \frac{\{\varphi : G \to M \mid \varphi(gh) = g\varphi(h) + \varphi(g) \ \forall g,h\}}{\{\varphi : G \to M \mid \exists m \ \varphi(g) = gm - m\} \ \forall g}$$

the set on the top are called the derivations of G w/ coefficients in M, on the bottom we have the inner derivations.

Note. If G acts trivially on M $H^1(G,M) = \mathrm{Hom}(G, M)$

- $$H^2(G,M) = \frac{\{\varphi : G\times G \to M \mid g\varphi(h,k) - \varphi(gh,k) + \varphi(g,hk) - \varphi(g,h) = 0\}}{\{\varphi : G\times G \to M \mid \varphi(g,h) = g\sigma(h) - \sigma(gh) + \sigma(g)\}}$$

where σ is ~~an~~ derivation of G w/ coeff in M.

Let k be a global field. We let
$H^i(k, M)$ denote $H^i(\mathrm{Gal}(\bar{k}/k), M)$.

Ex. For $n \in \mathbb{N}$ $H^1(k, \mu_n) = k^\times/(k^\times)^n$.

Prop. ~~We have a long exact sequence~~ Let
$0 \to M_1 \to M_2 \to M_3 \to 0$ be an exact sequence of G-modules. Then we have a long exact sequence

$$\cdots \to H^n(G, M_2) \to H^n(G, M_3) \xrightarrow{\delta} H^{n+1}(G, M_1) \to H^{n+1}(G, M_2).$$

Thrm (H90) Let L/k be Galois ext of fields
$$H^1(\mathrm{Gal}(L/k), L^\times) = 0.$$

Def. Given a field k $Br(k)$, the Brauer group of k is
$$H^2(~~G_k~~\ G_k, K_{sep}^\times)$$

Note - You can also describe the Brauer group as central simple k-algebras up to equivalence w/ group operation $\otimes$.

Ex. If K is alg. closed $Br(K) = 0$.

$$1 \to \mu_n \cancel{\mathbb{Z}/\mathbb{Z}} \to K_{sep}^\times \xrightarrow{\times n} K_{sep}^\times \to 1$$

gives

~~$\to K^\times \to K^\times \to H^1(K, \mu_n) \to H^1(K, K^\times) \to H^1(K, K^\times)$~~

$$\mu_n^G \to K^\times \xrightarrow{n} K^\times \to H^1(k, \mu_n) \to 0.$$

$$\Rightarrow \quad H^1(k, \mu_n) = k^\times/(k^\times)^n.$$

This also gives us
$$H^2(K, \mu_n) = Br(k)[n]$$

Thrm Let K be local field.

i) $\exists$ an injection $\mathrm{inv}: Br\,k \to \mathbb{Q}/\mathbb{Z}$ whose image is
$$\begin{cases} \frac{1}{2}\mathbb{Z}/\mathbb{Z} & k = \mathbb{R} \\ 0 & k = \mathbb{C} \\ \mathbb{Q}/\mathbb{Z} & k \text{ non-arch} \end{cases}$$

ii) If L/k finite
$$\begin{array}{ccc} Br\,k & \xrightarrow{\mathrm{inv}} & \mathbb{Q}/\mathbb{Z} \\ \downarrow & & \downarrow \times [L:k] \\ Br\,L & \xrightarrow[\mathrm{inv}]{} & \mathbb{Q}/\mathbb{Z} \end{array}$$
commutes

Thm Let K be a global field. For each $v \in \Omega_K$ let K_v be its completion at v. Let $\mathrm{inv}_v : \mathrm{Br}\, K_v \to \mathbb{Q}/\mathbb{Z}$ be as above. Then we have the exact sequence

$$1 \longrightarrow \mathrm{Br}\, K \to \bigoplus_v \mathrm{Br}\, K_v \xrightarrow{\sum_v \mathrm{inv}_v} \mathbb{Q}/\mathbb{Z} \to 1.$$