Introduction to elliptic curves and selmer groups

ICTS Lectures

Content

- Group cohomology
- Principal homogeneous spaces.
- Tate shafarevich group of elliptic curves
- Selmer group of elliptic curves
  - Finiteness of n-selmer groups.
  - Weak Mordell-Weil theorem.
  - Kummer pairing
- Selmer groups of p-adic representations.

Main referenie Books

- The Arithmetic of Elliptic curves - Joseph H. Silverman.
- Elliptic curves — J. S. Milne.

Group cohomology

cohomology of finite groups.

Let G be a finite group. A G-module is an abelian group M together with an action of G, i.e. a map

$$G \times M \longrightarrow M$$
$$(\sigma, m) \longrightarrow \sigma m$$

such that

(a) $\sigma(m+m') = \sigma m + \sigma m'$

(b) $(\sigma\tau)(m) = \sigma(\tau m)$ for all $\sigma, \tau \in G$, $m \in M$;

(c) $1m = m$ for all m.

equivalently, $G \longrightarrow \mathrm{Aut}(M)$

$\sigma \longrightarrow \phi_\sigma$

with $\phi_\sigma(m) = \sigma m$ is a group homomorphism.

Example 1

Let L be a finite Galois extension of a field K with Galois group G. Let E be an elliptic curve over K. Then $E(L)$ is a G-module via the co-ordinate wise action.

Let M be a G-module, we define,

$$H^0(G, M) = M^G = \{m \in M \mid \sigma m = m \ \forall\ \sigma \in G\}.$$

In particular, for the G-module $E(L)$ in Example 1, $H^0(G, E(L)) = E(K)$.

- $H^0(G, M)$ is called the zeroth cohomology group of G-module M.

A cross homomorphism is a function $f: G_1 \to M$ such that $f(\sigma\tau) = f(\sigma) + \sigma f(\tau)$, for all $\sigma, \tau \in G_1$.

For any $m \in M$, $f(\sigma) = \sigma m - m$ for all $\sigma \in G_1$ is a cross homomorphism called as principal cross homomorphism.

The set of cross homomorphism is a group under pointwise addition of functions and principal cross homomorphisms form a subgroup.

— The 1st cohomology group $H^1(G, M)$ of G_1-module M is defined as

$$H^1(G_1, M) := \frac{\{\text{cross homomorphisms}\}}{\{\text{principal cross homomorphism}\}}$$

— Note that when G acts trivially on M then

$$H^1(G, M) = \text{Hom}(G, M)$$

— Connecting homomorphism

Let $0 \to M \xrightarrow{\phi} N \xrightarrow{\psi} P \to 0$ be an exact sequence of G_1-modules. Let $p \in P^{G_1} \subseteq P$. Let $n \in N$ such that $\psi(n) = p$. Since $\psi(\sigma n - n) = \sigma p - p = 0 \ \forall \ \sigma \in G_1$, $\sigma n - n = \phi(m_\sigma)$ for some $m_\sigma \in M$.

we define, $\delta(p)(\sigma) = m_\sigma$. $\quad p \in H^0(G_1, P) \to H^1(G_1, M)$

Then $\delta(p)$ is a cross homomorphism. Further, modulo principal cross homomorphisms, $\delta(p)$ is independent of choice of n such that $\psi(n) = p$.

Proposition 1

For an exact sequence

$$0 \longrightarrow M \longrightarrow N \longrightarrow P \longrightarrow 0,$$

there is a canonical exact sequence

$$0 \longrightarrow H^0(G, M) \longrightarrow H^0(G, N) \longrightarrow H^0(G, P) \xrightarrow{\delta} H^1(G, M) \longrightarrow H^1(G, N) \longrightarrow H^1(G, P).$$

Here δ is the connecting homomorphism.

Inflation-restriction

Let $H \leq G$ be a subgroup.

The restriction map

$$\text{Res} : H^1(G, M) \longrightarrow H^1(H, M)$$
$$f \longrightarrow f|_H$$

is a group homomorphism.

Suppose that $H \trianglelefteq G$ be a normal subgroup, and let M be a G-module. Then M^H is a G/H-module. A cross homomorphism $f : G/H \longrightarrow M^H$ defines a crossed homomorphism $f : G \longrightarrow M$ via $f : G \longrightarrow G/H \longrightarrow M^H \subseteq M$, which further induces a homomorphism

$$\text{Inf} : H^1(G/H, M^H) \longrightarrow H^1(G, M)$$ called Inflation homomorphism.

Proposition 2: For a G-module M and a normal subgroup $H \trianglelefteq G$, the sequence

$$0 \longrightarrow H^1(G/H, M^H) \xrightarrow{\text{Inf}} H^1(G, M) \xrightarrow{\text{Res}} H^1(H, M)^{G/H}$$ is exact.

Cohomology of infinite Galois groups.

Let K be a perfect field, and let $\overline{K}$ be an algebraic closure of K.
Let $J \subseteq \overline{K}$ be a normal extension of K, non necessarily finite over K.
Let $Gal(J/K)$ be the Galois group of J/K, i.e. the group of automorphisms of J fixing K.

The group $Gal(J/K)$ is a topological group for which open subgroups are those fixing some finite extension of K. we have,

$$Gal(J/K) = \varprojlim_{L \subseteq J} Gal(L/K)$$

where, L varies over finite normal extensions of K and limit is taken with respect to the natural projection maps of quotient group.

Let M be a discrete $Gal(J/K)$-module, i.e. the corresponding map $Gal(J/K) \times M \to M$ is continuous when M is given discrete topology.

Equivalently, $M = \bigcup_H M^H$, H open in $Gal(J/K)$.

Or Equivalently, stabilizer of every element in M is an open subgroup of $Gal(J/K)$.

Example

- For an Elliptic curve E over over K, $E(J)$ is a discrete $Gal(J/K)$-module.
- The torsion subgroup $E(J)_{tor} \leq E(J)$ is a discrete submodule.

$E(J) = \bigcup E(L)$

For an infinite Galois group $Gal(J/K)$ and a discrete $G_1(J/K)$-module M, $H^1(G_1, M)$ is defined as the group of all continuous crossed product homomorphisms $f: G_1 \to M$ modulo the subgroup of principal crossed homomorphisms. Equivalently,

$$H^1(G_1(J/K), M) := \varinjlim_{L \subseteq J} H^1(Gal(L/K), M^{G_1(J/L)})$$

where, L varies over finite Galois extensions of K and direct limit is taken with respect to the inflation maps.

Note that since $stab(m)$ is an open subgroup of $G_1(J/K)$ for every $m \in M$, the principal cross homomorphism $f(\sigma) = \sigma m - m$ is continuous

Notation: For the sep closure K^{sep} in an alg closure $\overline{K}$, $H^i(K, M) := H^i(Gal(K^{sep}/K), M)$.

Proposition 3 For a continuous discrete $G_1(J/M)$-module M, $H^1(G_1(J/K), M)$ is torsion.

Proof: Let $f \in H^1(G_1(J/K), M)$. Then $\exists$ a finite Galois extension L/K such that $f \in H^1(G_1(L/K), M^{G_1(L/K)}) \subseteq H^1(G_1(J/K), M)$. Let $n = |G_1(L/K)|$.

For a $g \in G_1$,

$$\sum_{h \in G_1(L/K)} f(h) = \sum_{h \in G_1(L/K)} f(gh) = g \sum_{h \in G_1(L/K)} f(h) + n f(g)$$

$$\Rightarrow \quad n f(g) = gm - m \quad \text{for} \quad m = \sum_{h \in G_1(L/K)} f(h)$$

$$\Rightarrow \quad nf = 0 \quad \text{in} \quad H^1(G_1(J/K), M).$$

□

Principal homogeneous space.

(of set)

Let A be an abelian group. A right A-set

$$W \times A \longrightarrow W$$
$$(w, a) \longrightarrow w + a$$

is called a principal homogeneous space for A if $W \neq \emptyset$ and the map

$$W \times A \longrightarrow W \times W$$
$$(w, a) \longrightarrow (w, w + a)$$

is bijective, i.e. given $w_1, w_2 \in W$, there is a unique $a \in A$ such that $w_1 + a = w_2$.

A morphism of principal homogeneous spaces is a map of A-sets.

Examples: 1) Addition $A \times A \longrightarrow A$ makes A into a principal homogeneous space.

2. For a field K, the affine line $\mathbb{A}^1_K$ is a principal homogeneous space for K.

Proposition 4

Let W and W' be two principal homogeneous space for A. Then for every $w_1 \in W$ and $w_2 \in W'$, there exists a unique morphism $\varphi : W \longrightarrow W'$ such that $\varphi(w_1) = w_2$. Moreover, every morphism from $W \longrightarrow W'$ is an isomorphism.

Proof $\varphi(w) = w_2 + a$ for $w = w_1 + a$ satisfy $\varphi(w_1) = w_2$.

Let $\psi : W \longrightarrow W'$ be a morphism with $\psi(w_1) = w_2$. Since ψ is a morphism

$$\psi(w) = \psi(w_1 + a) = \psi(w_1) + a = w_2 + a \quad \forall\, w \in W.$$

This proves uniqueness of φ.

There is a unique morphism $\psi : W' \to W$ with $\psi(w_2) = w_1$. Again uniqueness implies $\phi \circ \psi = Id_{W'}$ and $\psi \circ \phi = Id_W$.

$\Rightarrow$ ϕ & ψ are isomorphisms. $\square$

— As a consequence, for a principal homogeneous space W and $w \in W$, there is a unique isomorphism $\phi : A \to W$ such that $\phi(0) = w$.

— we have,

$A = Aut(W)$

$a \longrightarrow (w \longrightarrow w + a)$

Principal homogeneous space of curves

Let E be an elliptic curve over a field K. A principal homogeneous space for E is a curve W over K together with a right action of E given by a map of varieties

$$W \times E \to W$$
$$(w, P) \longrightarrow w + P$$

such that

$$W \times E \to W \times W$$
$$(w, P) \longrightarrow (w, w + P)$$

is an isomorphism of algebraic varieties.

— If W is a principal homogeneous space of E then for every field extension L/K, $W(L)$ is either empty or a principal homogeneous space of $E(L)$ as sets.

A morphism $\varphi : W \to W'$ of principal homogeneous spaces over E is a morphism of algebraic varieties such that,

$$\begin{array}{ccc} W \times E & \longrightarrow & W \\ \downarrow & & \downarrow \\ W' \times E & \longrightarrow & W' \end{array}$$

commutes.

Proposition 4 and its consequences applies to principal homogeneous spaces over elliptic curves. In particular, we have

- Addition $E \times E \to E$ makes E into a principal homogeneous space called trivial principal homogeneous space.
- Let W & W' be principal homogeneous spaces fo E. For any $w \in W(K)$ and $w' \in W'(K)$ there exist a unique morphism $W \to W'$ of principal homogeneous spaces sending w to w'. Further, such a morphism is in fact an isomorphism.
- Since $W(L) \neq \emptyset$ for a finite extension L/K, there is an isomorphism from $W \to E$ over L. In particular W is trivial over a finite extension of K.
- For a point $P \in E(K)$, $w \mapsto w + P$ is an automorphism of W, and every automorphism of W over K is of this form for a unique $P \in E(K)$.

Classification of principal homogeneous spaces.

Let W be a principal homogeneous space for E, and $w \in W(\bar{K})$. For any $\sigma \in Gal(\bar{K}/K)$, $\sigma w \in W(\bar{K})$. There is a unique $f_w(\sigma) \in E(\bar{K})$, such that $\sigma w = w + f_w(\sigma)$. We have

$$(\sigma\tau)(w) = \sigma(\tau w) = \sigma(w + f_w(\tau)) = \sigma w + \sigma f_w(\tau) = w + f_w(\sigma) + \sigma f_w(\tau)$$

$$\Rightarrow \quad f_w(\sigma\tau) = f_w(\sigma) + \sigma f_w(\tau).$$

Hence $f_w : Gal(\bar{K}/K) \to E(\bar{K})$ is a cross homomorphism.

Since $w \in W(L) \cong E(L)$ for a finite extension L/K, $f_w(\sigma) = 0$ $\forall\, \sigma \in Gal(\bar{K}/L)$. This implies that f_w is continuous.

Let $w, w' \in W(\bar{K})$ and $f_w, f_{w'}$ be corresponding cross homomorphism respectevely.

Let $w = w' + P$ for some $P \in E(\bar{K})$.

$\Rightarrow \sigma(w) = \sigma(w') + \sigma(P)$

$\Rightarrow w + f_w(\sigma) = w' + f_{w'}(\sigma) + \sigma(P)$

$\Rightarrow w' + P + f_w(\sigma) = w' + f_{w'}(\sigma) + \sigma(P)$

$f_{w'}(\sigma) - f_w(\sigma) = \sigma(P) - P \quad \forall \ \sigma$.

Cross homomorphism f_w modulo principal cross holomorphism associated to a point w is independent of w.

Now suppose that W & W' be principal homogeneous of E with an isomorphism $\varphi : W \longrightarrow W'$ over K. Let $w \in W(\bar{K})$ and $w' = \varphi(w)$.

Then $\sigma w = w + f_w(\sigma) \Rightarrow \varphi(\sigma w) = \varphi(w) + f_w(\sigma)$

$\Rightarrow \sigma[\varphi(w)] = \varphi(w) + f_w(\sigma) \Rightarrow \sigma w' = w' + f_w(\sigma)$.

$\Rightarrow f_w(\sigma) = f_{w'}(\sigma) \quad \forall \ \sigma \in Gal(\bar{K}/K)$.

$\Rightarrow w \longmapsto f_w$ is a well defined function from

$\{$ Principal homogeneous spaces for $E\}/_{\sim} \xrightarrow{\phi} H^1(K, E)$

Suppose that $f_w(\sigma) = \sigma(P) - P$ for some $P \in E(\bar{K})$.

Then $\sigma(w - P) = \sigma w - \sigma P = w + \sigma(P) - P - \sigma P = w - P$.

$\Rightarrow w - P \in W(K)$.

This shows that if the cohomology class of f_w is zero then W is trivial over K.

Theorem 5

The function ϕ defined above is a bijection.

Proof: Let W and W' be principal homogeneous space of E over K. Let $w \in W(\bar{K})$ and $w' \in W(\bar{K})$.

Suppose that $f_W = f_{W'}$ in $H^1(K, E)$.

$\Rightarrow$ There is $P \in E(\bar{K})$ such that

$$f_{W'}(\sigma) = f_{cW}(\sigma) + \sigma P - P \quad \forall \ \sigma.$$

$$\sigma(W' - P) = W' - P + f_{W'-P}(\sigma)$$

$$\Rightarrow \quad \sigma(W') - \sigma(P) = W' - P + f_{W'-P}(\sigma)$$

$$\Rightarrow \quad W' + f_{W'}(\sigma) - \sigma(P) = W' - P + f_{W'-P}(\sigma)$$

$$\Rightarrow \quad f_{W'-P}(\sigma) = f_{W'}(\sigma) - \sigma(P) + P \quad \Rightarrow \quad f_{W'-P} = f_W$$

by replacing W' by $W'-P$ we assume $f_W(\sigma) = f_{W'}(\sigma) \ \forall \ \sigma$.

There is a unique isomorphism $\varphi : W \longrightarrow W'$ over $\bar{K}$ with $\varphi(W) = W'$.

Let $x \in W$ and write $x = W + Q$

$$\varphi(\sigma x) = \varphi(\sigma(W + Q)) = \varphi(W + f_W(\sigma) + \sigma Q) = W' + f_W(\sigma) + \sigma Q$$

$$= W' + f_{W'}(\sigma) + \sigma Q$$

$$= \sigma W' + \sigma Q$$

$$= \sigma(W' + Q)$$

$$= \sigma \varphi(x).$$

$\Rightarrow$ $\varphi : W \longrightarrow W$ is defined over K.

$\Rightarrow$ ϕ is injective.

Surjective (a brief sketch)

objects: Smooth curves defined over K	objects: finitely generated extensions J/K of transcendence degree one with $J \cap \bar{K} = K$.
maps: non constant rational maps defined over K.	$\longleftrightarrow$ Maps: field homomorphisms fixing K

Let $f \in H^1(K, E)$. Let $\bar{K}(E)$ be the function field of E over $\bar{K}$. For every $\sigma \in Gal(\bar{K}/K)$, we have an automorphism $T_{f(\sigma)} : E \longrightarrow E$

$$x \longrightarrow x + f(\sigma)$$

which in turn induces an automorphism of the function field $\bar{K}(E)$ of E over $\bar{K}$.

Let $F := \bar{K}(E)^{Gal(\bar{K}/K)}$.

As a consequence of <u>speiser's lemma</u> (theory of Galois descent), we have an isomorphism

$$\bar{K}F \simeq \bar{K} \underset{K}{\otimes} F \longrightarrow \bar{K}(E)$$

$$m \otimes x \longrightarrow mx$$

This implies that F has transcendence degree one over K. Let W be the curve corresponding to the field F.
From the fact that $\bar{K}F = \bar{K}(E)$, we get that there is an isomorphism

$$\varphi : W \longrightarrow E \quad \text{over } \bar{K}.$$

Then by construction $\varphi^\sigma \circ \varphi^{-1} : E \longrightarrow E$ is given by $T_{f(\sigma)}^{-1} = T_{-f(\sigma)}$, where $\varphi^\sigma = \sigma \circ \varphi \circ \sigma^{-1}$.

We define

$$\mu : W \times E \longrightarrow W$$

$$(w, P) \longrightarrow \varphi^{-1}(\varphi(w) + P) \qquad [\mu(w, p) := w + P]$$

μ induces an structure of principal homogeneous space of E over K.

Let $\omega_0 \in W$ such that,

$$\psi(\omega_0) = 0 \in E.$$

Then $\sigma\omega_0 = (\psi^\sigma)^{-1}(0)$

$$= \psi^{-1} \circ T_{f(\sigma)}^{-1}(0) = \psi^{-1}(0 + f(\sigma))$$

$$= \psi^{-1}(\psi(\omega_0) + f(\sigma))$$

$$= \mu(\omega_0, f(\sigma)) = \omega_0 + f(\sigma)$$

$$\Rightarrow \quad \phi(W) = f$$

$\therefore$ ϕ is surjective.

Tate Shafarevich group

Let K be a number field. For a prime v of K let K_v denote the completion of K at v.

Let E be an elliptic curve defined over K. Then E is also a curve over K_v

The Tate shafarevich group $Ш(E/K)$ of E over K is defined as

$$Ш(E/K) := \ker\left(H^1(K, E) \xrightarrow{\text{res}} \prod_v H^1(K_v, E) \right)$$

Equivalently, $Ш(E/K)$ is the set of all principal homogeneous spaces of E over K which are trivial over over K_v $\forall$ v.

Thus $Ш(E/K)$ measures the failure of Hasse principle for principal homogeneous spaces of E.

Conjecture (BSD)

$Ш(E/K)$ is finite for every number field K.

— It is know that if $Ш(E/K)$ is finite then it is a perfect square (Cassels).

$H^1(K, E[n])$

Let K be a perfect field of characteristic p coprime to an integer n. Let E be an elliptic curve over K. Being an isogeny multiplication by n map, $E \xrightarrow{n} E$ is a a surjective map.

Consider the exact sequence

$$0 \to E[n] \longrightarrow E \xrightarrow{n} E \to 0$$

where $E[n]$ denotes the n-torsion points of E.

we get the following associated exact sequence

$$0 \to E(K)[n] \longrightarrow E(K) \xrightarrow{n} E(K) \longrightarrow H^1(K, E[n]) \longrightarrow H^1(K, E) \xrightarrow{n} H^1(K, E)$$

$$\Rightarrow \quad 0 \to \frac{E(K)}{nE(K)} \longrightarrow H^1(K, E[n]) \longrightarrow H^1(K, E)[n] \to 0.$$

Geometric interpretation of $H^1(K, E[n])$

n-covering: An n-covering is a pair (W, α) consisting of a principal homogeneous space W for E and a morphism of varieties $\alpha : W \to E$ over K such that for some $w \in W(\bar{K})$, $\alpha(w + P) = nP$ for all $P \in E(\bar{K})$.

— A morphism $(W, \alpha) \to (W', \alpha')$ of n-coverings is a morphism $\varphi : W \to W'$ of principal homogeneous spaces such that $\alpha = \alpha' \circ \varphi$.

Let (W, α) be a n-covering of E. Let $w \in W(\bar{K})$.
For $\sigma \in Gal(\bar{K}/K)$, let $\sigma w = w + f(\sigma)$.
The equation $\sigma\alpha(w) = \alpha(\sigma w)$ implies that $nf(\sigma) = 0$.

we get a map

$$f_w : Gal(\bar{K}/K) \to E[n]$$
$$\sigma \longmapsto f(\sigma)$$

As before, f_w is a cross homomorphism.
This induces a map

$$\phi_n : \{ n\text{-coverings} \} \to H^1(K, E[n])$$

Theorem 6: ϕ_n is a bijection.

Proof of Theorem 6 is similar to the proof of Theorem 5.

Selmer group

Let K be a number field and E/K be an elliptic curve. Let $n>1$ be an integer. Consider the exact sequence

$$0 \longrightarrow E(K)/nE(K) \xrightarrow{\delta} H^1(K, E[n]) \longrightarrow H^1(K, E)[n] \longrightarrow 0.$$

The group $H^1(K, E[n])$ is always infinite for any elliptic curve E/K and integer $n>1$.

We next define a smaller subgroup in $H^1(K, E[n])$ called n-Selmer group which is always finite and also contains $E(K)/nE(K)$.

Definition: The n-Selmer group of E over a number field K is defined as

$$Sel_n(E/K) := \ker\left(H^1(K, E[n]) \xrightarrow{res} \prod_v H^1(K_v, E)\right)$$

where v varies over the set of primes of K.

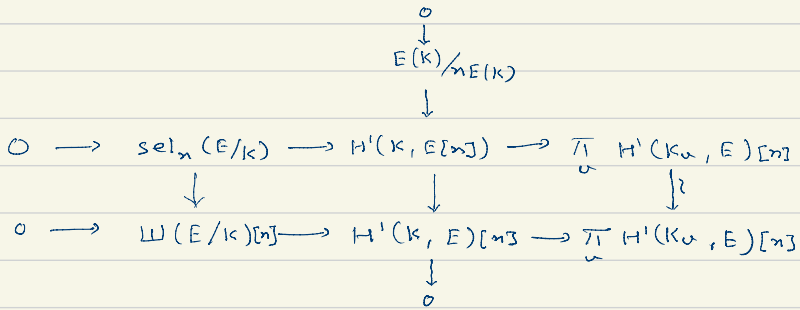
Thus n-selmer group is the set of n-coverings which fails to satisfy Hasse principal.

Proposition 7

We have an exact sequence

$$0 \longrightarrow E(K)/nE(K) \longrightarrow Sel_n(E/K) \longrightarrow Ш(E/K)[n] \longrightarrow 0.$$

Proof: Proposition is an immediate consequence of the following commutative diagram and snake lemma.



□

Lemma 8 - Let v be a discrete valuation of K with $v(n) = 0$. Suppose that E has good reduction at v. Let $\tilde{E}_v$ be the reduced curve modulo v. Then the reduction map induces an injection $E(K)[n] \longrightarrow \tilde{E}_v(\mathbb{F}_v)[n]$, where $\mathbb{F}_v$ is the residue field at v.

proof:

From the structure of structure of rational points of elliptic curves over local fields, and using the assumption that E has good reduction at v, we have an exact sequence,

$$0 \longrightarrow E_1(K) \longrightarrow E(K) \longrightarrow \tilde{E}_v(\mathbb{F}_v) \longrightarrow 0$$

Here $E_1(K) \cong \hat{E}(m)$ where $\hat{E}$ is the formal group of E and $m = \{a \in K_v \mid v(a) > 0\}$.

From the assumption that $v(n) = 0$ and general theory of formal group, we have $\hat{E}(m)[n] = 0$.

This proves the lemma.

Definition Let K be a number field, v be a prime of K and I_v be the inertia subgroup at v.

We say an element $f \in H^1(K_v, M)$ is unramified if $f|_{I_v} \in H^1(I_v, M)$ is trivial.

Consider the exact sequence

$$0 \to E(K_v)/nE(K_v) \xrightarrow{\delta_v} H^1(K_v, E[n]) \to H^1(K_v, E)[n] \to 0$$

Here δ_v be the connecting homomorphism defined as $\delta_v(P)(\sigma) = Q^\sigma - Q$ where $nQ = P$, $P \in E(K_v)$, $Q \in E(\overline{K}_v)$.

Lemma 9: Suppose that E has good reduction at v and $v(n) = 0$. Then for every $P \in E(K_v)$, $\delta_v(P)$ is unramified.

Proof: Let $\sigma \in I_v$. Let $Q \in E(\overline{K}_v)$ such that $nQ = P$. Then $Q^\sigma - Q \in E[n]$.

Let $\overline{Q}$ be the image of Q in $\tilde{E}(\overline{k}_v)$.

Then $\overline{Q}^\sigma = \overline{Q}$.

$\Rightarrow$ $\overline{Q}^\sigma - \overline{Q} = 0$ in $E(\overline{k}_v)$.

From Lemma 8, $Q^\sigma - Q = 0$.

$\Rightarrow$ $\delta_v(P)|_{I_v} = 0$

$\Rightarrow$ $\delta_v(P)$ is unramified. $\square$

We have $f \in Sel_n(E/K)$ iff $f|_{Gal(\overline{K}_v/K_v)} = 0$ for every prime v. This implies that $f \in Sel_n(E/K)$ iff $f \in \operatorname{Im} \delta_v$.

As a consequence, we have an equivalent definition of n-selmer group:

$$0 \longrightarrow Sel_n(E/K) \longrightarrow H^1(K, E[n]) \longrightarrow \prod_v \frac{H^1(K_v, E[n])}{\text{Im } \delta_v}$$

— δ_v is also called local kummer map at v.

Theorem 10

$Sel_n(E/K)$ is finite.

Proof: Let S be a finite set of primes of K containing the set of bad primes of E, primes dividing n and infinite primes. Let K_S be the maximal extension of K unramified outside S. Then K_S/K is a Galois extension of K.

From Lemma 9, we get that,

$$Sel_n(E/K) \subseteq Ker\left(H^1(K, E[n]) \xrightarrow{res} \prod_{v \notin S} H^1(I_v, E[n]) \prod_{v \in S} \frac{H^1(K_v, E[n])}{\text{Im } \delta_v} \right)$$

This implies that $Sel_n(E/K) \subseteq Ker\left(H^1(K, E[n]) \xrightarrow{res} H^1(K_S, E[n])\right)$

$$= H^1(Gal(K_S/K), E[n]).$$

From Lemma 8, I_v acts trivially on $E[n]$ $\forall$ $v \notin S$.

$\Rightarrow K_S(E[n]) = K_S \Rightarrow Gal(\overline{K}/K_S)$ acts trivially on $E[n]$.

Let $L = K(E[n])$ be the field extension of K obtained by adjoining co-ordinates of $E[n]$ in K.

Then $L \subseteq K_S$ as $Gal(\overline{K}/K_S)$ acts trivially on $E[n]$. Further since $Gal(K_S/L)$ is Kernel of the action of $Gal(K_S/K)$ on $E[n]$, L/K is a Galois extension.

Consider the exact sequence

$$0 \to H^1(\mathrm{Gal}(L/K), E[n]) \to H^1(\mathrm{Gal}(K_s/K), E[n]) \to H^1(\mathrm{Gal}(K_s/L), E[n])$$

since $\mathrm{Gal}(L/K)$ is finite, $H^1(\mathrm{Gal}(L/K), E[n])$ is also finite.

Let $f \in H^1(\mathrm{Gal}(K_s/L), E[n])$. Let T be the fixed field of $\ker(f)$. Then T is unramified outside a finite set of primes S and $[T:L] \leq n^2$.

From Hermite-Minkowski theorem bounding degree of extensions by discriminant in algebraic number theory), we get that there are finitely many such extensions.

$\Rightarrow$ $H^1(\mathrm{Gal}(K_s/L), E[n])$ is a finite group.

$\Rightarrow$ $\mathrm{Sel}_n(E/K)$ is finite. □

Corollary (Weak Mordell-Weil theorem).
For a number field K and and elliptic curve E over K, $E(K)/nE(K)$ is finite.

□

Kummer pairing

Let K be a number field and E/K be an elliptic curve with $K = K(E[n])$. The Kummer pairing

$$\kappa : E(K) \times \mathrm{Gal}(\bar{K}/K) \to E[n]$$

is defined as follows.
Let $P \in E(K)$ and choose any point $Q \in E(\bar{K})$ satisfying $nQ = P$. Then

$$\kappa(P, \sigma) = Q^{\sigma} - Q.$$

i.e. $\chi(P,\sigma) = \delta(P)(\sigma)$ where δ is the connecting homomorphism

$E(K) \xrightarrow{\delta} H^1(K, E[n])$.

We have the following:

- The kummer pairing is bilinear.
- kernel of χ on left is $nE(K)$.
- kernel of χ on right is $Gal(\bar{K}/L)$ where $L = K(n^{-1}E(K)) \subseteq K_s$.

As a consequence χ induces a perfect pairing.

$$E(K)/nE(K) \times Gal(L/K) \longrightarrow E[n]$$

In particular, this also implies that $E(K)/nE(K)$ is finite.

(Full) Selmer group.

We have so far only discussed n-selmer group. The selmer group of E over K is defined as

$Sel(E/K) := \varinjlim Sel_n(E/K)$ where

Limit is taken with respect to multiplication by n-maps.

We again have

$0 \to Sel(E/K) \longrightarrow H^1(K, E(\bar{K})_{tor}) \longrightarrow \prod H^1(K_v, E)$

and

$$0 \longrightarrow E(K) \otimes \mathbb{Q}/\mathbb{Z} \longrightarrow Sel(E/K) \longrightarrow Ш(E/K) \longrightarrow 0$$

Conjecture (BSD)

$$Sel(E/K) \cong (\mathbb{Q}/\mathbb{Z})^{r(E/K)}$$

where $E(K) \otimes \mathbb{Q} \cong \mathbb{Q}^{r(E/K)}$

Also recall the exact sequence

$$0 \longrightarrow Sel_n(E/K) \longrightarrow H^1(K, E[n]) \longrightarrow \prod_v H^1(K_v, E[n]) / Im(\delta_v)$$

where

$$\delta_v : E(K_v)/nE(K_v) \longrightarrow H^1(K_v, E[n])$$

Taking direct limit over n, we get an injective map

$$\delta_v : E(K_v) \otimes \mathbb{Q}/\mathbb{Z} \longrightarrow H^1(K, E(\bar{K}_v)_{tor})$$

δ_v is also called local kummer maps.

As a consequence, we have

$$0 \longrightarrow Sel(E/\mathbb{Q}) \longrightarrow H^1(K, E(\bar{K})_{tor}) \longrightarrow \prod_v H^1(K, E(\bar{K}_v)_{tor}) / Im(\delta_v).$$

Selmer group of p-adic Galois representation (brief sketch)

Let p be a prime number and E be an elliptic curve defined over a number field K.

We have $E_{p^\infty} := E(\bar{K})$ (p-primary part)

$$\cong \mathbb{Q}_p/\mathbb{Z}_p \oplus \mathbb{Q}_p/\mathbb{Z}_p$$

The Tate-module

$$T_p E := \varprojlim_r E[p^r] \cong \mathbb{Z}_p \oplus \mathbb{Z}_p$$

where inverse limit is taken with respect to multiplication by p-maps.

Then $V_p E := T_p E \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ is a rank two continuous representation of $Gal(\bar{K}/K)$ and $E_{p^\infty} \cong V_p E / T_p E$.

The p-primary selmer group $Sel_{p^\infty}(E/K)$ of E/K is defined as the p-primary subgroup of $Sel(E/K)$. We have an exact sequence

$$0 \longrightarrow Sel_{p^\infty}(E/K) \longrightarrow H^1(K, E_{p^\infty}) \longrightarrow \prod_v H^1(K_v, E)$$

Equivalently,

$$0 \to Sel_{p^\infty}(E/K) \longrightarrow H^1(K, E_{p^\infty}) \longrightarrow \prod_v \frac{H^1(K_v, E_{p^\infty})}{\operatorname{Im} \delta_v}$$

where δ_v is the connecting homomorphism

$$\delta_v : E(K_v) \otimes \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow H^1(K_v, E_{p^\infty})$$

Remark: As a consequence of Faltings isogeny theorem isogeny class of E is determined by V_pE. Therefore Mordell-Weil rank is also determined by T_pE.

Remark: From the structure of rational point of elliptic curves over local fields, if v is a finite prime of K then $E(K_v)$ is a finitely generated G_v-module, where $\mathcal{O}_v$ is the ring of integers of K_v. As a consequence $E(K_v) \otimes \mathbb{Q}_p/\mathbb{Z}_p = 0 \quad \forall\, v \nmid p$. If v is an infinite prime then either $E(K_v)$ is divisible or a product of a $\mathbb{Z}/2\mathbb{Z}$ with a divisible group.

Hence, p-primary selmer group of E over K is defined as.

$$0 \longrightarrow Sel_{p^\infty}(E/K) \longrightarrow H^1(K, E_{p^\infty}) \longrightarrow \prod_{v \nmid p} H^1(K_v, E_{p^\infty}) \prod_{v \mid p} \frac{H^1(K_v, E_{p^\infty})}{\operatorname{Im} \delta_v}$$

Problem: To describe $S_{p^\infty}(E/K)$ purely in terms of V_pE.

A solution to this problem lies in the notion of Bloch-Kato Selmer group. We shall only briefly sketch the definition For more details readers are refered to the orignal article of Bloch and Kato.

For a finite prime v, Let K_v^{ur} be the maximal unramified extension of K_v. Let V be a finite dimensional p-adic representation of $Gal(\overline{K}/K)$, unramified outside a finite set of primes S of K containing primes dividing p and unramified primes.

$v \nmid p$ case

Suppose that $v \nmid p$. Let I_v denote the inertia subgroup at v. Consider the subgroup $H^1_{ur}(K_v, V) \leq H^1(K_v, V)$ defined as

$$H^1_{ur}(K_v, V) := \ker\left(H^1(K_v, V) \xrightarrow{\text{res}} H^1(K_v^{ur}, V)\right).$$

Here, $H^1(K_v, V)$ consists of classes of continuous cross homomorphisms from $\mathrm{Gal}(\overline{K_v}/K_v) \longrightarrow V$.

Let $T \leq V$ be a $\mathrm{Gal}(\overline{K}/K)$-invariant lattice. Put $A = V/T$.

We define,

$$H^1_{ur}(K_v, A) := \pi_v\left(H^1_{ur}(K_v, V)\right) \leq H^1(K_v, A)$$

Here $\pi_v : H^1(K_v, V) \longrightarrow H^1(K_v, A)$ is induced by $\pi_v : V \longrightarrow A$.

Note that Image of π_v is divisible.

Example: Let $V = V_p E$ for an elliptic curve E defined over K. Then using the fact that $H^0(K_v, E_{p^\infty})$ is finite and Tate duality it can be shown that $H^1(K_v, V_p E) = 0 \quad \forall \quad v \nmid p$. As a consequence $H^1_{ur}(K_v, E_{p^\infty}) = 0$.

Remark: $H^1(K_v, V_p E) = 0$ is equivalent to the assertion that $H^1(K_v, E_{p^\infty})$ is finite.

In fact, for a finite prime $v \nmid p$ of good reduction of E,

$$\# H^1(K_v, E_{p^\infty}) = |L_v(E,1)|_p$$

where $L_v(E,s)$ is the local L-factor of E at v and $|\cdot|$ denote the p-adic norm with $|p|_p = \frac{1}{p}$.

If E has bad reduction at $v \nmid p$ then

$$\# H^1(K_v, E_{p^\infty}) = \left| \frac{L_v(E,1)}{c_v} \right|_p$$

where c_v denote the tamagawa number of E at v.

$v|p$ case

Local condition for Bloch Kato selmer group at primes dividing p is defined using the crystalline p-adic period ring B_{crys} by Fontaine. We omit details here and refer the readers to the original article of Fontaine on p-adic periods.

For primes $v|p$ of K, the local Bloch-Kato conditions are defined as

$$H^1_{BK}(K_v, V) := \ker\left(H^1(K_v, V) \longrightarrow H^1(K_v, V \otimes_{\mathbb{Q}_p} B_{crys})\right)$$

$$H^1_{BK}(K_v, A) := \pi_v\left(H^1_{BK}(K_v, V)\right)$$

Example: Let E be an elliptic curve defined over K. Then for every $v \mid p$, $H^1_{BK}(K_v, E_{p^\infty}) = \text{Image}(\delta_v) = E(K_v) \otimes \mathbb{Q}_p/\mathbb{Z}_p$.

The Bloch-Kato selmer group of V over K is defined as

$$H^1_{BK}(K, V) := \ker\left(H^1(K, V) \longrightarrow \prod_{v \nmid p} \frac{H^1(K_v, V)}{H^1_{ur}(K_v, V)} \prod_{v \mid p} \frac{H^1(K_v, V)}{H^1_{BK}(K_v, V)} \right)$$

and

$$H^1_{BK}(K, A) = \ker\left(H^1(K, A) \longrightarrow \prod_{v \nmid p} \frac{H^1(K_v, A)}{H^1_{ur}(K_v, A)} \prod_{v \mid p} \frac{H^1(K_v, A)}{H^1_{BK}(K_v, A)} \right)$$

Example. For an elliptic curve E/K comparing the local conditions we see that $H^1_{BK}(K, E_{p^\infty}) = Sel_{p^\infty}(E/K)$.

— We have a natural homomorphism

$$H^1_{BK}(K, V) \xrightarrow{\pi} H^1_{BK}(K, A) \quad \text{induced by} \quad V \xrightarrow{\pi} A$$

and $\text{Im}(\pi) =$ divisible part of $H^1_{BK}(K, A)$.

BSD conjecture

$\text{rank}_{\mathbb{Q}_p} H^1_{BK}(K, V_p E) =$ Mordell-Weil rank of E.

Relation with BSD formula

(Ref: Greenberg's Notes on Iwasawa Theory of elliptic curves)

Let K be a number field, E/K be an elliptic curve over K and p be an odd prime.

We have already seen

$$\#\, H^1(K_v, E_{p^\infty}) = \left| \frac{L_v(E,1)}{c_v} \right|_p \quad \text{for every finite prime } v \nmid p.$$

If $E(K)$ is finite then BSD predicts

$$\#\, Ш(E/K) = \sqrt{|disc_K|} \times \#(E(K)_{tor})^2 \times \frac{1}{\Omega_{E/K}} \times \frac{1}{\prod_{v<\infty} c_v} \times L(E/K, 1)$$

$|disc_K|$:= modulus of discriminant of E/K.

$\Omega_{E/K}$:= global period of E/K.

Finiteness of $E(K)$ + BSD $\Rightarrow Ш(E/K)(p) = Sel_{p^\infty}(E/K)$.

Suppose that E has good and ordinary reduction at primes of K dividing p.

This assumptions implies that there is an exact sequence

$$0 \longrightarrow E_{p^\infty}^+ \longrightarrow E_{p^\infty} \longrightarrow \tilde{E}_{p^\infty} \longrightarrow 0$$

of $Gal(\bar{K}_v/K_v)$ module for every $v \mid p$.

$\tilde{E}_{p^\infty} = E(\bar{f}_v)_{p^\infty}$ where f_v is the residue field at v.

Let $K_\infty \subseteq K(\mu_{p^\infty})$ be the unique extension of K with $\Gamma := Gal(K_\infty/K) \cong \mathbb{Z}_p$. Here μ_{p^∞} denote the union of p-power roots of unity. There is a tower of extensions of number fields

$$K = K_0 \subseteq K_1 \subseteq K_2 \subseteq \cdots \subseteq K_n \subseteq \cdots K_\infty$$

with $Gal(K_n/K) \cong \mathbb{Z}/p^n\mathbb{Z}$.

For every $n \geq 0$ $Gal(K_n/K)$ acts on $Sel_{p^\infty}(E/K_n)$ continuously

As a consequence Γ acts continuously on

$$Sel_{p^\infty}(E/K_\infty) := \varinjlim Sel_{p^\infty}(E/K_n).$$

Control theorem (Mazur)

kernel and co-kernel of $Sel_{p^\infty}(E/K_n) \xrightarrow{res} Sel_{p^\infty}(E/K_\infty)^{\Gamma_n}$ is bounded independent of n for $\Gamma_n := Gal(K_\infty/K_n)$.

In particular control theorem + finiteness of $Sel_{p^\infty}(E/K)$ $\Rightarrow$ $Sel_{p^\infty}(E/K_\infty)^\Gamma$ is finite.

From the fact that Γ is procyclic, we get that $Sel_{p^\infty}(E/K_\infty)_\Gamma$ (co-invariance) is also finite.

A precise version of control theorem implies that the Euler characteristic

$$\chi(E/K_\infty) := \frac{\#Sel_{p^\infty}(E/K_\infty)^\Gamma}{\#Sel_{p^\infty}(E/K_\infty)_\Gamma}$$

$$= \frac{\#Ш(E/K)(p)}{\#(E(K)_{p^\infty})^2} \times \frac{1}{\prod_v |c_v|_p} \times \prod_{v|p} (\#\tilde{E}_v(f_v)_{p^\infty})^2$$

(BSD or Iwasawa main conj. for elliptic curves $\Rightarrow$)

$$\chi(E/K_\infty) =_p \frac{L(E/K,1)}{\Omega_E} \times \sqrt{|Disc|_K} \prod_{v\nmid\infty} (\#\tilde{E}_v(f_v)_{p^\infty})^2$$