Introduction to Galois Cohomology

Hwajong Yoo

Seoul National University

February 10th, 2025
2025 (SNU) Algebra Camp

Q: What is Galois cohomology?

Q: What is Galois cohomology?

A: Galois (Group) cohomology, i.e., group cohomology for certain Galois group.

Q: What is Galois cohomology?

A: Galois (Group) cohomology, i.e., group cohomology for certain Galois group.

Q: What is Group cohomology?

Q: What is Galois cohomology?

A: Galois (Group) cohomology, i.e., group cohomology for certain Galois group.

Q: What is Group cohomology?

A: Cohomology theory for G-modules...

Q: What is Galois cohomology?

A: Galois (Group) cohomology, i.e., group cohomology for certain Galois group.

Q: What is Group cohomology?

A: Cohomology theory for G-modules...

Q: What is Cohomology theory...?

Goals of this talk

Introduce Galois cohomology and provide two applications for Prof. Kim's talk.

Goals of this talk

Introduce Galois cohomology and provide two applications for Prof. Kim's talk.

Theorem A (Kummer Theory)

Let K be a number field and suppose that $\mu_n \subset K$. Then we have an isomorphism:

$$\Phi : K^\times/(K^\times)^n \to \mathrm{Hom}(G_K, \mu_n),$$

where $G_K := \mathrm{Gal}(\overline{K}/K)$ is the absolute Galois group of K.

Goals of this talk

Introduce Galois cohomology and provide two applications for Prof. Kim's talk.

Theorem A (Kummer Theory)

Let K be a number field and suppose that $\mu_n \subset K$. Then we have an isomorphism:

$$\Phi : K^\times/(K^\times)^n \to \mathrm{Hom}(G_K, \mu_n),$$

where $G_K := \mathrm{Gal}(\overline{K}/K)$ is the absolute Galois group of K.

Theorem B (Weak Mordell–Weil Theorem)

Let E be an elliptic curve over a number field K. Then $E(K)/nE(K)$ is finite for any $n \geq 2$.

Part I: Galois cohomology

étale cohomology $\longrightarrow$ Galois cohomology $\longrightarrow$ Group cohomology

étale cohomology $\longrightarrow$ Galois cohomology $\longrightarrow$ Group cohomology

Q: What do we expect about cohomology theory?

étale cohomology $\longrightarrow$ Galois cohomology $\longrightarrow$ Group cohomology

Q: What do we expect about cohomology theory?

G a group, M a G-module $\longmapsto$ $\boxed{H^i(G,M)}$ an abelian group.

$\forall$ a short exact sequence of G-modules:

$$0 \longrightarrow L \longrightarrow M \longrightarrow N \longrightarrow 0,$$

$\forall$ a short exact sequence of G-modules:

$$0 \longrightarrow L \longrightarrow M \longrightarrow N \longrightarrow 0,$$

$\exists$ a long exact sequence of G-modules:

$$0 \longrightarrow H^0(G,L) \longrightarrow H^0(G,M) \longrightarrow H^0(G,N) \longrightarrow$$
$$\longrightarrow H^1(G,L) \longrightarrow H^1(G,M) \longrightarrow H^1(G,N) \longrightarrow$$
$$\longrightarrow H^2(G,L) \longrightarrow H^2(G,M) \longrightarrow H^2(G,N) \longrightarrow$$
$$\longrightarrow H^3(G,L) \longrightarrow \cdots$$

G-modules: abelian groups having an action of a group G.

e.g. μ_n the group of n-th roots of unity, action of $G_{\mathbf{Q}} = \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ or $G = \mathrm{Gal}(\mathbf{Q}(\mu_n)/\mathbf{Q})$.

$$\zeta_n \text{ a primitive } n\text{-th root of unity} \longmapsto \langle \zeta_n \rangle \simeq \mu_n.$$

$$\forall \sigma \in G_{\mathbf{Q}}, \quad \sigma(\zeta_n) = \zeta_n^k \quad \text{for some integer } k.$$

The action of $G_{\mathbf{Q}}$ on μ_n factors through G and so $H^i(G_{\mathbf{Q}}, \mu_n) = H^i(G, \mu_n)$.

G-modules: abelian groups having an action of a group G.

e.g. μ_n the group of n-th roots of unity, action of $G_{\mathbf{Q}} = \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ or $G = \mathrm{Gal}(\mathbf{Q}(\mu_n)/\mathbf{Q})$.

$$\zeta_n \text{ a primitive } n\text{-th root of unity} \longmapsto \langle \zeta_n \rangle \simeq \mu_n.$$

$$\forall \sigma \in G_{\mathbf{Q}}, \quad \sigma(\zeta_n) = \zeta_n^k \quad \text{for some integer } k.$$

The action of $G_{\mathbf{Q}}$ on μ_n factors through G and so $H^i(G_{\mathbf{Q}}, \mu_n) = H^i(G, \mu_n)$.

> Q: Can we compute $H^i(G_{\mathbf{Q}}, \mu_n)$?

We didn't define these groups yet....

Let $\mathscr{A}$ and $\mathscr{B}$ be two abelian categories. Suppose that $\mathscr{A}$ has enough injectives. Then for a left exact functor $F : \mathscr{A} \to \mathscr{B}$, there is a functor

$$R^i F : \mathscr{A} \to \mathscr{B}$$

such that $\forall$ a short exact sequence in $\mathscr{A}$

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0,$$

Let $\mathscr{A}$ and $\mathscr{B}$ be two abelian categories. Suppose that $\mathscr{A}$ has enough injectives. Then for a left exact functor $F : \mathscr{A} \to \mathscr{B}$, there is a functor

$$R^i F : \mathscr{A} \to \mathscr{B}$$

such that $\forall$ a short exact sequence in $\mathscr{A}$

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0,$$

$\exists$ a long exact sequence in $\mathscr{B}$

$$\begin{aligned}
0 \longrightarrow F(A) \longrightarrow F(B) \longrightarrow F(C) &\longrightarrow \\
\longrightarrow R^1F(A) \longrightarrow R^1F(B) \longrightarrow R^1F(C) &\longrightarrow \\
\longrightarrow R^2F(A) \longrightarrow R^2F(B) \longrightarrow \cdots &
\end{aligned}$$

Construction

Choose an injective resolution of an object $A \in \mathscr{A}$

$$0 \longrightarrow A \longrightarrow I^0 \longrightarrow I^1 \longrightarrow I^2 \longrightarrow I^3 \longrightarrow \cdots$$

We then obtain a cochain complex

$$0 \longrightarrow F(I^0) \longrightarrow F(I^1) \longrightarrow F(I^2) \longrightarrow F(I^3) \longrightarrow \cdots$$

Finally, $\boxed{R^i F(A)}$ is defined as its cohomology at the i-th spot.

Construction

Choose an injective resolution of an object $A \in \mathscr{A}$

$$0 \longrightarrow A \longrightarrow I^0 \longrightarrow I^1 \longrightarrow I^2 \longrightarrow I^3 \longrightarrow \cdots$$

We then obtain a cochain complex

$$0 \longrightarrow F(I^0) \longrightarrow F(I^1) \longrightarrow F(I^2) \longrightarrow F(I^3) \longrightarrow \cdots$$

Finally, $\boxed{R^i F(A)}$ is defined as its cohomology at the i-th spot.

This construction does not depend on the choice of a resolution!

Group cohomology

Let Mod(G) be the category of G-modules, or equivalently $\mathbf{Z}[G]$-modules.

Also, let Mod$(\mathbf{Z})$ be the category of abelian groups, or equivalently $\mathbf{Z}$-modules.

Consider the functor $F = (-)^G$: Mod$(G) \to$ Mod$(\mathbf{Z})$.

Group cohomology

Let Mod(G) be the category of G-modules, or equivalently $\mathbf{Z}[G]$-modules.

Also, let Mod$(\mathbf{Z})$ be the category of abelian groups, or equivalently $\mathbf{Z}$-modules.

Consider the functor $F = (-)^G$: Mod$(G) \to$ Mod$(\mathbf{Z})$.

Exercise

Prove that F is left exact.

Group cohomology

Let Mod(G) be the category of G-modules, or equivalently $\mathbf{Z}[G]$-modules.

Also, let Mod$(\mathbf{Z})$ be the category of abelian groups, or equivalently $\mathbf{Z}$-modules.

Consider the functor $F = (-)^G$: Mod$(G) \to$ Mod$(\mathbf{Z})$.

Exercise

Prove that F is left exact.

Definition

For a G-module M, the i-th cohomology group $H^i(G, M)$ is defined as

$$H^i(G, M) := R^i F(M).$$

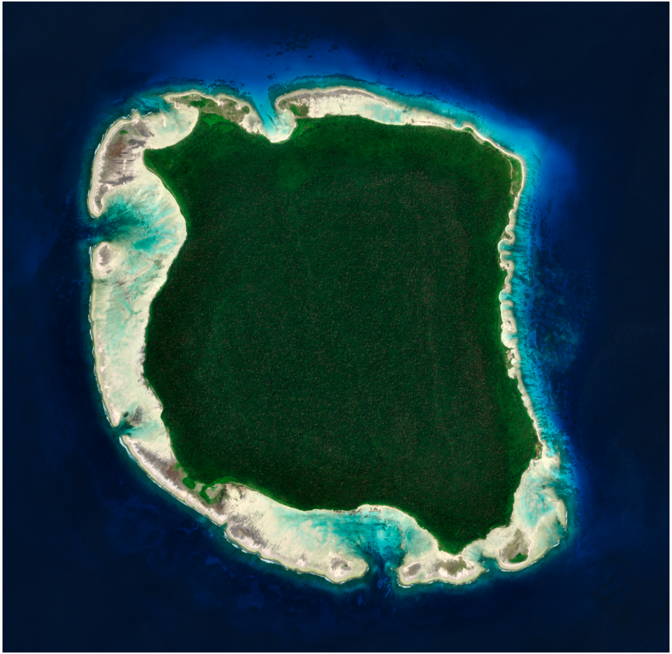
Real life: How to compute it?

$$H^0(G_{\mathbf{Q}}, \mu_n) = \mu_n^{G_{\mathbf{Q}}} = 1 \text{``}={\text{''}} 0$$

Real life: How to compute it?

$$H^0(G_{\mathbf{Q}},\mu_n)=\mu_n^{G_{\mathbf{Q}}}=1\text{``}=\text{''}0$$

$$H^1(G_{\mathbf{Q}},\mu_n)=? \quad H^2(G_{\mathbf{Q}},\mu_n)=?$$



Another look

Q: What is the functor $(-)^G$?

Another look

Q: What is the functor $(-)^G$?

A: $M^G = \mathsf{Hom}_{\mathbf{Z}[G]}(\mathbf{Z}, M)$

Another look

Q: What is the functor $(-)^G$?

A: $M^G = \mathrm{Hom}_{\mathbf{Z}[G]}(\mathbf{Z}, M)$

Theorem

Let

$$\cdots \longrightarrow P^3 \longrightarrow P^2 \longrightarrow P^1 \longrightarrow P^0 \longrightarrow \mathbf{Z} \longrightarrow 0$$

be a projective resolution of $\mathbf{Z}$. Then $H^i(G, M)$ is equal to the i-th cohomology of the cochain complex

$$\cdots \longrightarrow \mathrm{Hom}_{\mathbf{Z}[G]}(P^2, M) \longrightarrow \mathrm{Hom}_{\mathbf{Z}[G]}(P^1, M) \longrightarrow \mathrm{Hom}_{\mathbf{Z}[G]}(P^0, M) \longrightarrow 0.$$

Namely, if

$$P^\bullet \to \mathbf{Z} \to 0 \quad \text{and} \quad 0 \to M \to I^\bullet$$

are two (projective and injective) resolutions, then the i-th cohomologies of the following two cochain complexes are equal:

$$\mathsf{Hom}_{\mathbf{Z}[G]}(P^\bullet, M) \quad \text{and} \quad \mathsf{Hom}_{\mathbf{Z}[G]}(\mathbf{Z}, I^\bullet).$$

Namely, if

$$P^\bullet \to \mathbf{Z} \to 0 \quad \text{and} \quad 0 \to M \to I^\bullet$$

are two (projective and injective) resolutions, then the i-th cohomologies of the following two cochain complexes are equal:

$$\mathrm{Hom}_{\mathbf{Z}[G]}(P^\bullet, M) \quad \text{and} \quad \mathrm{Hom}_{\mathbf{Z}[G]}(\mathbf{Z}, I^\bullet).$$

There is a very good free resolution of $\mathbf{Z}$!

Namely, if

$$P^\bullet \to \mathbf{Z} \to 0 \quad \text{and} \quad 0 \to M \to I^\bullet$$

are two (projective and injective) resolutions, then the i-th cohomologies of the following two cochain complexes are equal:

$$\mathrm{Hom}_{\mathbf{Z}[G]}(P^\bullet, M) \quad \text{and} \quad \mathrm{Hom}_{\mathbf{Z}[G]}(\mathbf{Z}, I^\bullet).$$

There is a very good free resolution of $\mathbf{Z}$!

Exercise

Study the standard complex or bar resolution.

Alternative definition of H^1

Let G be a finite group acting on an abelian group M. A crossed homomorphism is a map $f : G \to M$ such that

$$f(\sigma\tau) = f(\sigma) + \sigma \cdot f(\tau) \quad \text{for all } \sigma, \tau \in G$$

and it is said to be principal if there is an element $m \in M$ such that

$$f(\sigma) = \sigma \cdot m - m \quad \text{for all } \sigma in G.$$

We then have

$$H^1(G, M) = \frac{\text{crossed homomorphisms}}{\text{principal crossed homomorphisms}}.$$

Alternative definition of H^1

Let G be a finite group acting on an abelian group M. A crossed homomorphism is a map $f : G \to M$ such that

$$f(\sigma\tau) = f(\sigma) + \sigma \cdot f(\tau) \quad \text{for all } \sigma, \tau \in G$$

and it is said to be principal if there is an element $m \in M$ such that

$$f(\sigma) = \sigma \cdot m - m \quad \text{for all } \sigma in G.$$

We then have

$$H^1(G, M) = \frac{\text{crossed homomorphisms}}{\text{principal crossed homomorphisms}}.$$

By definition, if G acts trivially on M, then we have

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

Change the group

Let $\lambda : H \to G$ be a group homomorphism. Then λ gives rise to an exact functor

$$\Phi_\lambda : \mathsf{Mod}(G) \to \mathsf{Mod}(H)$$

because every G-module can be considered as a H-module via λ. In particular, if H is a subgroup of G, then we have

$$\mathsf{res}_H^G : H^i(G, M) \to H^i(H, M).$$

Change the group

Let $\lambda : H \to G$ be a group homomorphism. Then λ gives rise to an exact functor

$$\Phi_\lambda : \mathsf{Mod}(G) \to \mathsf{Mod}(H)$$

because every G-module can be considered as a H-module via λ. In particular, if H is a subgroup of G, then we have

$$\mathsf{res}^G_H : H^i(G, M) \to H^i(H, M).$$

Also, if N is a normal subgroup of G, then we may take $(G, H) = (G/N, G)$ (and λ is the quotient map), and hence we obtain

$$\mathsf{inf}^{G/N}_G : H^i(G/N, M^N) \to H^i(G, M^N) \to H^i(G, M).$$

Inflation and Restriction

Theorem

Let G be a group and N a normal subgroup. Then for $M \in \text{Mod}(G)$ we have an exact sequence

$$0 \longrightarrow H^1(G/N, M^N) \xrightarrow{\text{inf}} H^1(G, M) \xrightarrow{\text{res}} H^1(N, M)^{G/N} \longrightarrow H^2(G/N, M^N) \xrightarrow{\text{inf}} H^2(G, M).$$

Inflation and Restriction

Theorem

Let G be a group and N a normal subgroup. Then for $M \in \mathrm{Mod}(G)$ we have an exact sequence

$$0 \longrightarrow H^1(G/N, M^N) \xrightarrow{\text{inf}} H^1(G,M) \xrightarrow{\text{res}} H^1(N,M)^{G/N} \longrightarrow H^2(G/N, M^N) \xrightarrow{\text{inf}} H^2(G,M).$$

Exercise

Study the Grothendieck spectral sequence.

Part II: Applications

Hilbert's Theorem 90

Theorem (Kummer, Hilbert, Noether)

Let L/K be a finite Galois extension with Galois group G. Then $H^1(G, L^\times) = 0$.

Hilbert's Theorem 90

Theorem (Kummer, Hilbert, Noether)

Let L/K be a finite Galois extension with Galois group G. Then $H^1(G, L^\times) = 0$.

Proof. Let $f : G \to L^\times$ be a crossed homomorphism. In multiplicative notation, this means that for any $\sigma, \tau \in G$, we have $f(\sigma\tau) = f(\sigma)\sigma(f(\tau))$ or equivalently

$$\boxed{\sigma(f(\tau)) = f(\sigma)^{-1} f(\sigma\tau)},$$

and we have to find $\boxed{m \in L^\times}$ such that $f(\sigma) = \sigma(m)/m$ for all $\sigma \in G$.

Hilbert's Theorem 90

Theorem (Kummer, Hilbert, Noether)

Let L/K be a finite Galois extension with Galois group G. Then $H^1(G, L^\times) = 0$.

Proof. Let $f : G \to L^\times$ be a crossed homomorphism. In multiplicative notation, this means that for any $\sigma, \tau \in G$, we have $f(\sigma\tau) = f(\sigma)\sigma(f(\tau))$ or equivalently

$$\boxed{\sigma(f(\tau)) = f(\sigma)^{-1} f(\sigma\tau)},$$

and we have to find $\boxed{m \in L^\times}$ such that $f(\sigma) = \sigma(m)/m$ for all $\sigma \in G$.

Lemma (Dedekind)

Let L/K be a finite Galois extension. Then distinct elements of $\mathrm{Gal}(L/K)$ are linear independent over L.

As $f(\tau) \in L^\times$ is nonzero, the above lemma implies that

$$\sum_{\tau \in G} f(\tau) \cdot \tau : L \to L$$

is not a zero map, i.e., there exists an $\alpha \in L$ such that

$$\beta := \sum_{\tau \in G} f(\tau) \cdot \tau(\alpha) \neq 0.$$

But then, for $\sigma \in G$, we have

$$\begin{aligned}\sigma(\beta) &= \sum_{\tau \in G} \sigma(f(\tau)) \cdot \sigma\tau(\alpha) \\ &= \sum_{\tau \in G} f(\sigma)^{-1} f(\sigma\tau) \cdot \sigma\tau(\alpha) \\ &= f(\sigma)^{-1} \sum_{\tau \in G} f(\sigma\tau) \cdot \sigma\tau(\alpha) = f(\sigma)^{-1}\beta\end{aligned}$$

as τ runs over G, so also does $\sigma\tau$. Thus, we have $f(\sigma) = \beta/\sigma(\beta) = \sigma(\beta^{-1})/\beta^{-1}$. $\square$

Infinite Galois theory

Let L/K be a Galois extension with infinite Galois group G and M a G-module. The group G has natural profinite topology, i.e., basic open sets of G are those subgroups $H < G$ which have finite index in G. We then define the cohomology groups of G with coefficients in A as

$$H^i(G, M) := \varinjlim H^i(G/H, M^H),$$

where H runs through all open subgroups of G. (Use the inflation maps!)

Infinite Galois theory

Let L/K be a Galois extension with infinite Galois group G and M a G-module. The group G has natural profinite topology, i.e., basic open sets of G are those subgroups $H < G$ which have finite index in G. We then define the cohomology groups of G with coefficients in A as

$$H^i(G, M) := \varinjlim H^i(G/H, M^H),$$

where H runs through all open subgroups of G. (Use the inflation maps!)

Theorem

Let L/K be an infinite Galois extension with Galois group G. Then $H^1(G, L^\times) = 0$.

Proof.

Exercise! □

Classification of quadratic / cubic extensions

Question

Can we classify all the quadratic extensions of $\mathbb{Q}$?

Classification of quadratic / cubic extensions

Question

Can we classify all the quadratic extensions of $\mathbb{Q}$?

Question

Can we classify all the cubic extensions of $\mathbb{Q}$?

Kummer theory

Suppose that K is a number field containing a primitive n-th root of unity ζ_n, or equivalently $\mu_n \subset K$ for a given integer $n \geq 2$. Then we can easily classify abelian extensions of exponent n in terms of some data related to $K^\times$ (cf. CFT).

More precisely, for any $a \in K^\times$, the field $L = K(\sqrt[n]{a})$ is the splitting field of $f(x) = x^n - a$ over K; the notation $\sqrt[n]{a}$ denotes a particular primitive n-th root of a, but it does not matter which root we pick because $\mu_n \subset K$ (and so all the n-th roots of a are of the form $\zeta_n^k \sqrt[n]{a}$). Note that L is a Galois extension of K, and $\mathrm{Gal}(L/K)$ is cyclic as we have an injective homomorphism:

$$\begin{array}{ccc} \mathrm{Gal}(L/K) & \hookrightarrow & \mu_n \simeq \mathbf{Z}/n\mathbf{Z} \\ \sigma & \longmapsto & \frac{\sigma(\sqrt[n]{a})}{\sqrt[n]{a}} \end{array}$$

This homomorphism is an isomorphism if and only if $x^n - a$ is irreducible.

Lemma

Let L/K be a cyclic field extension of degree n with Galois group $\langle\sigma\rangle$ and suppose that L contains a primitive n-th root of unity ζ_n. Then $\sigma(\alpha) = \zeta_n \alpha$ for some $\alpha \in L$.

Proof.

The automorphism σ is a linear transformation of L with characteristic polynomial $x^n - 1$; by the above lemma by Dedekind it must be its minimal polynomial, since $\{1, \sigma, \sigma^2, \ldots, \sigma^{n-1}\}$ is linearly independent. Thus, ζ_n is an eigenvalue of σ. $\square$

Classification of cyclic extensions

Theorem (classification)

Let K be a number field containing a primitive n-th root of unity ζ_n. If L/K is a cyclic extension of degree n, then $L = K(\sqrt[n]{a})$ for some $a \in K^\times$.

Proof.

By the above lemma, there is an element $\alpha \in L$ for which $\sigma(\alpha) = \zeta_n \alpha$. We have

$$\sigma(\alpha^n) = \sigma(\alpha)^n = (\zeta_n \alpha)^n = \alpha^n,$$

thus $a = \alpha^n$ is invariant under the action of $\langle \sigma \rangle = \mathrm{Gal}(L/K)$ and thus lies in K. Moreover, the orbit $\{\alpha, \zeta\alpha, \ldots, \zeta^{n-1}\alpha\}$ of α under the action of $\mathrm{Gal}(L/K)$ has order n, so

$$L = K(\alpha) = K(\sqrt[n]{a}).$$

□

Kummer pairing

Definition

Let K be a number field and assume that $\zeta_n \in K$. The Kummer pairing is the map

$$\langle -,-\rangle : \mathrm{Gal}(\overline{K}/K) \times K^\times \longrightarrow \langle \zeta_n \rangle = \mu_n$$

$$\langle \sigma, a \rangle \longmapsto \frac{\sigma(\sqrt[n]{a})}{\sqrt[n]{a}}$$

which is well-defined. Indeed, if α and β are two n-th roots of a, then $(\alpha/\beta)^n = 1$ and so $\alpha/\beta \in \langle \zeta_n \rangle \subset K$ is fixed by σ. Thus,

$$\sigma(\beta)/\beta = \sigma(\beta)/\beta \cdot \sigma(\alpha/\beta)/(\alpha/\beta) = \sigma(\alpha)/\alpha$$

and the value of $\langle \sigma, a \rangle$ does not depend on the choice of $\sqrt[n]{a}$.

First Proof of Theorem A

From the Kummer pairing, we have a natural map sending $a \in K^\times$ to $(\sigma \mapsto \langle \sigma, a \rangle)$:

$$\Phi : K^\times \to \mathrm{Hom}(G_K, \mu_n)$$

It suffices to show that $\ker(\Phi) = (K^\times)^n$ and Φ is surjective.

1) For each $a \in K^\times \setminus (K^\times)^n$, if we pick an n-th root $\alpha \in \overline{K}$, then the extension $K(\alpha)/K$ is non-trivial and some $\sigma \in G_K$ must act nontrivially on α. For this σ, we have $\langle \sigma, a \rangle \neq 1$ and so $a \notin \ker(\Phi)$. Note that $(K^\times)^n \subset \ker(\Phi)$ is obvious.

2) Surjectivity is an exercise. Use the classification theorem.

Another proof of Theorem A

The multiplicative group $\overline{K}^{\times}$ is a G_K-module and there is an exact sequence of G_K-modules:

$$0 \longrightarrow \mu_n \longrightarrow \overline{K}^{\times} \xrightarrow{(-)^n} \overline{K}^{\times} \longrightarrow 0.$$

Taking a long exact sequence of cohomology yields:

$$\begin{array}{ccccccccc}
0 \longrightarrow & \mu_n^{G_K} & \longrightarrow & (\overline{K}^{\times})^{G_K} & \xrightarrow{(-)^n} & (\overline{K}^{\times})^{G_K} & \longrightarrow & H^1(G_K, \mu_n) & \longrightarrow & H^1(G_K, \overline{K}^{\times}) \\
& \| (a) & & \| (b) & & \| (c) & & \| (d) & & \| (e) \\
& \mu_n & \longrightarrow & K^{\times} & \xrightarrow{(-)^n} & K^{\times} & \longrightarrow & \mathrm{Hom}(G_K, \mu_n) & \longrightarrow & 0
\end{array}$$

Another proof of Theorem A

The multiplicative group $\overline{K}^\times$ is a G_K-module and there is an exact sequence of G_K-modules:

$$0 \longrightarrow \mu_n \longrightarrow \overline{K}^\times \xrightarrow{(-)^n} \overline{K}^\times \longrightarrow 0.$$

Taking a long exact sequence of cohomology yields:

$$\begin{array}{ccccccccc}
0 \longrightarrow \mu_n^{G_K} & \longrightarrow & (\overline{K}^\times)^{G_K} & \xrightarrow{(-)^n} & (\overline{K}^\times)^{G_K} & \longrightarrow & H^1(G_K, \mu_n) & \longrightarrow & H^1(G_K, \overline{K}^\times) \\
\| (a) & & \| (b) & & \| (c) & & \| (d) & & \| (e) \\
\mu_n & \longrightarrow & K^\times & \xrightarrow{(-)^n} & K^\times & \longrightarrow & \mathrm{Hom}(G_K, \mu_n) & \longrightarrow & 0
\end{array}$$

Why? $(a), (d)$: Note that we assume that $\mu_n \subset K$, and so G_K acts trivially on μ_n.

$(b), (c)$: Galois theory. (e) : Hilbert's theorem 90. □

Elliptic curves

Note that the group scheme $\mathbf{G}_m$ is used in the previous discussion. A bit more specifically,

$$\mathbf{G}_m(L) = L^\times \quad \text{and} \quad \mathbf{G}_m(\overline{K}) = \overline{K}^\times.$$

Elliptic curves

Note that the group scheme $\mathbf{G}_m$ is used in the previous discussion. A bit more specifically,

$$\mathbf{G}_m(L) = L^\times \quad \text{and} \quad \mathbf{G}_m(\overline{K}) = \overline{K}^\times.$$

Other type of group schemes can be used in a similar manner: Let E be an elliptic curve over a number field K. As above, there is an exact sequence of G_K-modules:

$$0 \longrightarrow E[n] \longrightarrow E(\overline{K}) \xrightarrow{\times n} E(\overline{K}) \longrightarrow 0.$$

Here, $E[n] := \{P \in E(\overline{K}) : nP = 0\}$ is the group of n-torsion points.

Taking a long exact sequence of cohomology gives rise to:

$$0 \longrightarrow E[n]^{G_K} \longrightarrow E(\overline{K})^{G_K} \xrightarrow{\times n} E(\overline{K})^{G_K} = E(K)$$

$$\longrightarrow H^1(G_K, E[n]) \longrightarrow H^1(G_K, E(\overline{K})) \xrightarrow{\times n} H^1(G_K, E(\overline{K})).$$

Taking a long exact sequence of cohomology gives rise to:

$$0 \longrightarrow E[n]^{G_K} \longrightarrow E(\overline{K})^{G_K} \xrightarrow{\times n} E(\overline{K})^{G_K} = E(K)$$

$$\longrightarrow H^1(G_K, E[n]) \longrightarrow H^1(G_K, E(\overline{K})) \xrightarrow{\times n} H^1(G_K, E(\overline{K})).$$

Thus, we obtain a short exact sequence:

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

If $H^1(G_K, E[n])$ were **finite**, we would be very happy. But unfortunately, it is NOT...

Local picture

For a prime v, we fix an extension of v to $\overline{K}$. We then have a commutative diagram:

$$\begin{array}{ccc} \overline{K} & \hookrightarrow & \overline{K}_v \\ | & & | \\ K & \overset{\iota_v}{\hookrightarrow} & K_v \end{array}$$

and so a decomposition group $G_v = \mathrm{Gal}(\overline{K}_v/K_v) \subset G_K$. Now G_v acts on $E(\overline{K}_v)$ and similarly as above we get:

$$0 \longrightarrow E(K_v)/nE(K_v) \longrightarrow H^1(G_v, E[n]) \longrightarrow H^1(G_v, E(\overline{K}_v))[n] \longrightarrow 0.$$

Via the maps $E(K) \hookrightarrow E(K_v)$ and $G_v \subset G_K$, we get commutative short exact sequences:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & E(K)/nE(K) & \xrightarrow{\iota} & H^1(G_K, E[n]) & \longrightarrow & H^1(G_K, E(\overline{K}))[n] & \longrightarrow & 0,\\
 & & \downarrow & \searrow^{f_v} & \downarrow{\scriptstyle \mathrm{res}} & \searrow^{g_v} & \downarrow{\scriptstyle \mathrm{res}} & & \\
0 & \longrightarrow & E(K_v)/nE(K_v) & \longrightarrow & \boxed{H^1(G_v, E[n])} & \longrightarrow & H^1(G_v, E(\overline{K}_v))[n] & \longrightarrow & 0.
\end{array}$$

If E has good reduction at v and $v \nmid n$, then the action of G_v on $E[n]$ is unramified (Néron–Ogg–Shafarevich criterion) so it factors through the quotient $G_v/I_v \simeq \langle \mathrm{Frob}_v \rangle \simeq \widehat{\mathbf{Z}}$. Furthermore, if $E[n] = E(K_v)[n]$, then

$$H^1(G_v, E[n]) = \mathrm{Hom}(\widehat{\mathbf{Z}}, (\mathbf{Z}/n\mathbf{Z})^2) \simeq (\mathbf{Z}/n\mathbf{Z})^2$$

is obviously finite. If f_v were **injective**, we would be very happy. But it is NOT...

Selmer groups (and TS)

$$
\begin{array}{ccccccccc}
0 & \longrightarrow & E(K)/nE(K) & \xrightarrow{\iota} & H^1(G_K, E[n]) & \longrightarrow & H^1(G_K, E(\overline{K}))[n] & \longrightarrow & 0, \\
 & & \downarrow & \overset{f_v}{\searrow} & \downarrow & \overset{g_v}{\searrow} & \downarrow & & \\
0 & \longrightarrow & E(K_v)/nE(K_v) & \longrightarrow & \boxed{H^1(G_v, E[n])} & \longrightarrow & H^1(G_v, E(\overline{K}_v))[n] & \longrightarrow & 0.
\end{array}
$$

However, since the diagram is commutative any element in the image of ι maps to 0 by g_v.
This motivates the following definition...

Selmer groups (and TS)

Definition

The n-Selmer group of E/K is the group

$$\mathrm{Sel}^{(n)}(E/K) := \ker\left(H^1(G_K, E[n]) \to \prod_{\text{all } v} H^1(G_v, E(\overline{K}_v))\right)$$

and the Tate–Shafarevich group of E/K is the group

$$\text{Ш}(E/K) := \ker\left(H^1(G_K, E(\overline{K})) \to \prod_{\text{all } v} H^1(G_v, E(\overline{K}_v))\right).$$

Proof of Theorem B

From the discussion above, we obtain a short exact sequence:

$$0 \longrightarrow E(K)/nE(K) \longrightarrow \boxed{\mathrm{Sel}^{(n)}(E/K)} \longrightarrow \text{Ш}(E/K)[n] \longrightarrow 0.$$

Theorem C

The group $\mathrm{Sel}^{(n)}(E/K)$ is finite. Hence $E(K)/nE(K)$ and $\text{Ш}(E/K)[n]$ are also finite.

Conjecture

The group $\text{Ш}(E/K)$ is finite.

Sketch of the proof

First, we may consider the finite extension $L = K(E[n])$ of K. Then it is not hard to prove that $E(K)/nE(K)$ is finite if $E(L)/nE(L)$ is finite.

Then we construct the same exact sequences for L instead of K. Note that $H^1(G_L, E[n]) = \mathrm{Hom}(G_L, E[n])$ as G_L acts trivally on $E[n]$. It turns out that an element of $\mathrm{Sel}^{(n)}(E/L)$ (as a subgroup of $\mathrm{Hom}(G_L, E[n])$) is a special map from G_L to $E[n]$. Furthermore, such a map corresponds to a finite extension of exponent n of L unramified outside a finite set S.

Finally, the number of such “unramified” extensions is finite.

Sketch of the proof

First, we may consider the finite extension $L = K(E[n])$ of K. Then it is not hard to prove that $E(K)/nE(K)$ is finite if $E(L)/nE(L)$ is finite.

Then we construct the same exact sequences for L instead of K. Note that $H^1(G_L, E[n]) = \mathrm{Hom}(G_L, E[n])$ as G_L acts trivally on $E[n]$. It turns out that an element of $\mathrm{Sel}^{(n)}(E/L)$ (as a subgroup of $\mathrm{Hom}(G_L, E[n])$) is a special map from G_L to $E[n]$. Furthermore, such a map corresponds to a finite extension of exponent n of L unramified outside a finite set S.

Finally, the number of such "unramified" extensions is finite.

Remark

We can directly prove that $\mathrm{Sel}^{(n)}(E/K)$ is finite by a similar argument.

References

Kummer theory

- Birch's article in ANT book by Cassels and Frohlich.
- Borcherd's youtube: https://www.youtube.com/watch?v=UaeJNQ5x17g
- Wake's student REU: https://www.math.uchicago.edu/~may/VIGRE/VIGRE2010/REUPapers/Harper.pdf
- Sutherland's LN: https://math.mit.edu/classes/18.785/2018fa/LectureNotes20.pdf

Weak Mordell–Weil Theorem

- Silverman's book: The arithmetic of elliptic curves
- Li's article: https://arxiv.org/pdf/1912.04401

Thank you very much
for your attention!