GALOIS COHOMOLOGY

1. Group Cohmology

Let G be a finite group. We say an abelian group A is a G-module if A is a module for the group ring $\mathbb{Z}[G] = \{\sum_{i=1}^{n} x_i g_i | x_i \in \mathbb{Z}, g_i \in G, n\,\text{finite}\}$. We define the first and second cohomology groups of A by

$$H^0(G, A) = \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, A)$$

and

$$H^1(G, A) = \mathrm{Ext}^1_{\mathbb{Z}[G]}(\mathbb{Z}, A)$$

where $\mathbb{Z}$ is considered the trivial G-module where $gx = x$ for every $x \in \mathbb{Z}, g \in G$. Let $\phi : \mathbb{Z} \to A$ be a module homomorphism. Then

$$\begin{aligned} \phi(1) &= \phi(g \cdot 1) \quad \forall g \in G \\ &= g \cdot \phi(1), \end{aligned}$$

so $\phi(1) \in A^G = \{x \in A \,|\, gx = x, \forall g \in G\}$, the set of elements at which G acts trivially. Since a $\mathbb{Z}$ homomorphism is completely determined by the image of 1, we can set

$$H^0(G, A) = \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, A) = A^G.$$

We can also define the first cohomology group as

$$H^1(G, A) = \frac{Z^1(G, A)}{B^1(G, A)}$$

where

$$Z^1(G, A) = \{\phi : G \to A \,|\, \phi(gh) = \phi(g) + g\phi(h)\}$$
$$B^1(G, A) = \{\delta \in Z^1 \,|\, \exists a \in A \text{ such that } \delta(g) = ga - a, \forall g \in G\}$$

Proposition 1.1. *With this setup, we can take a short exact sequence of G-modules*

$$0 \to A \to B \to C \to 0$$

and form the long exact sequence

$$0 \to H^0(G, A) \to H^0(G, B) \to H^0(G, C) \to H^1(G, A) \to H^1(G, B) \to H^1(G, C)$$

2. Galois Cohomology

We can now use the machinery of group cohomology to study number fields. Let L, K be number fields and $L : K$ a finite degree Galois extension with Galois group $G_{L:K}$. A Galois module A is a module over $G_{L:K}$.

Example 2.1. We can consider the Galois modules $A = L \simeq K[G]$, or $A = L^\times$ where $L^\times$ is the multiplicative group of L.

Example 2.2. If E is an elliptic curve over K then $A = E(L)$ is a Galois module, since the addition formulas are rational in $\mathbb{Q}$.

Definition 2.3. The first Galois cohomology group is $H^1(L : K, A) = H^1(G_{L:K}, A)$.

The following result gives an important terminating condition for the long exact sequences:

Theorem 2.4 (Hilbert's Theorem 90)**.** $H^1(L : K, L^\times) = 0$

Proof: Serre

In what follows we will take $L = \bar{K}$, the algebraic closure of K and $G_K = G_{\bar{K}:K}$ its Galois group. This extension is usually infinite, so it will be necessary to make amendmends to the previous defintions.

Definition 2.5. A G_K-module A is called a continuous G_K-module if for all $g \in G_K, a \in A$, there exists a finite Galois extension $L : K$ such that $g(a)$ depends only on the image of g in $G_{L:K}$.

Example 2.6. $\bar{K}, \bar{K}^\times$ and $E(\bar{K})$ are all continuous G_K-modules.

To form homology groups, set

$$H^1(K, A) = \frac{Z^1_{\text{cts}}(K, A)}{B^1(K, A)}$$

where

$$Z^1_{\text{cts}} = \{\phi : G_K \to A \,|\, \exists L : K \text{ such that } \phi(g) \text{ depends only on } g/L\}.$$

If we have a short exact sequence of continuous G_K-modules

$$0 \to A \to B \to C \to 0$$

this gives a long exact sequence of Galois cohomology groups

$$0- > A^{G_K} \to B^{G_K} \to C^{G_K} \to H^1(K, A) \to H^1(K, B) \to H^1(K, C).$$

3. Applications to Elliptic Curves

A crucial step in the proof of the Mordell-Weil theorem, enough to show that the rank of an elliptic curve over $\mathbb{Q}$ is finite, is the study of the size of the quotient $E(\mathbb{Q})/2E(\mathbb{Q})$. In curves with at least one 2-torsion point, this can be done with the help of an isogeny.

Let

$$E : y^2 = x^3 + ax^2 + bx$$

be an elliptic curve over $\mathbb{Q}$. We know E has the rational points $\mathcal{O}, T = (0, 0)$.

We also consider the curve

$$\bar{E} : y^2 = x^3 + \bar{a}x^2 + \bar{b}x$$

where $\bar{a} = -2a$ and $\bar{b} = a^2 - 4b$. Repeating this process yields the curve

$$\bar{\bar{E}} : y^2 = x^3 + 4ax^2 + 16bx$$

which is birationally equivalent to E by the transformation $y \mapsto 8y, x \mapsto 4x$.

Proposition 3.1. *Let $E, \bar{E}$ be as above. The maps $\phi : E \to \bar{E}$ and $\psi : \bar{E} \to E$ defined by*

$$\phi(P) = \begin{cases} (\frac{y^2}{x^2}, \frac{y(x^2-b)}{x^2}), & \text{if } P \neq \mathcal{O}, T \\ \bar{\mathcal{O}}, & \text{if } P = \mathcal{O} \text{ or } P = T \end{cases}$$

and

$$\psi(P) = \begin{cases} (\frac{\bar{y}^2}{4\bar{x}^2}, \frac{\bar{y}(\bar{x}^2-\bar{b})}{8\bar{x}^2}), & \text{if } P \neq \bar{\mathcal{O}}, \bar{T} \\ \bar{\mathcal{O}}, & \text{if } \bar{P} = \bar{\mathcal{O}} \text{ or } \bar{P} = \bar{T} \end{cases}$$

are elliptic curve homomorphisms, $Ker(\phi) = \{\mathcal{O}, T\}$ and

$$\psi \circ \phi(P) = 2P, \text{ for all points } P \in E.$$

Proof: Silverman and Tate

Lemma 3.2. *If $E/\psi(\bar{E}))$ and $\bar{E}/\phi(E)$ are finite, then so is $E/2E$*

Proof: Silverman and Tate.

We are thus led to consider the quotient $E(\mathbb{Q})/\psi(\bar{E}(\mathbb{Q}))$ (the other one can be treated identically).

By the proposition, we have a short exact sequence of $G_{\mathbb{Q}}$-modules

$$0 \to \{\mathcal{O}, T\} \to \bar{E}(\bar{\mathbb{Q}}) \xrightarrow{\psi} E(\mathbb{Q}) \to 0$$

and $\{\mathcal{O}, T\} \simeq \mathbb{Z}/2\mathbb{Z}$. Taking Galois cohomology we get the long exact sequence

$$0 \to \mathbb{Z}/2\mathbb{Z} \to \bar{E}(\mathbb{Q}) \xrightarrow{\psi} E(\mathbb{Q}) \to H^1(\mathbb{Q}, \mathbb{Z}/2\mathbb{Z}) \to H^1(\mathbb{Q}, \bar{E}) \xrightarrow{H^1(\psi)} H^1(\mathbb{Q}, E)$$

This in turn gives us the short exact sequence

$$0 \to \frac{E(\mathbb{Q})}{\psi(\bar{E}(\mathbb{Q}))} \to H^1(\mathbb{Q}, \mathbb{Z}/2\mathbb{Z}) \to H^1(\mathbb{Q}, \bar{E}(\mathbb{Q}))[\psi] \to 0$$

where $H^1(\mathbb{Q}, \bar{E}(\mathbb{Q}))[\psi] = (H^1(\psi))^{-1}$.

To get the order of $E(\mathbb{Q})/\psi(\bar{E}(\mathbb{Q}))$ we need to know the order of $H^1(\mathbb{Q}, \mathbb{Z}/2\mathbb{Z})$.

Proposition 3.3. $H^1(\mathbb{Q}, \mathbb{Z}/2\mathbb{Z}) \simeq \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$

Proof: Consider the exact sequence of Galois modules

$$0 \to \mu_2 \to \bar{\mathbb{Q}}^\times \xrightarrow{2} \bar{\mathbb{Q}}^\times \to 0$$

where $\mu_2 = \mathrm{Gal}(\mathbb{Q}(i) : \mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z}$.

Taking cohomology gives the long exact sequence

$$0 \to \mu_2 \to \bar{\mathbb{Q}}^\times \xrightarrow{2} \bar{\mathbb{Q}}^\times \to H^1(\mathbb{Q}, \mathbb{Z}/2\mathbb{Z}) \to H^1(\mathbb{Q}, \bar{\mathbb{Q}}^\times)$$

and $H^1(\mathbb{Q}, \bar{\mathbb{Q}}^\times) \simeq 0$ by Hilbert's Theorem 90. Thus,

$$H^1(\mathbb{Q}, \mathbb{Z}/2\mathbb{Z}) \simeq \mathbb{Q}^\times/(\mathbb{Q}^\times)^2.$$

4. The Selmer and Tate-Shafarevich Groups

In the effort to understand $E/2E$, we were led to consider the quotient $E(\mathbb{Q})/\psi(E(\mathbb{Q}))$. Our application of Galois cohomology showed that this group is closed related to the multiplicative group of rationals modulo squares $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$. This group, in turn, can be studied by means of local method.

Definition 4.1. A place ν is either a prime number p or ∞. $\mathbb{Q}_\nu$ then is either the field of p-adic numbers if $\nu = p$ or $\mathbb{R}$ if $\nu = \infty$.

There is then a natural inclusion $\mathbb{Q} \to \prod_\nu \mathbb{Q}_\nu, x \mapsto (x \mod 2, x \mod 3, \dots, x)$. This extends to the commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E(\mathbb{Q})/\psi(E(\mathbb{Q})) & \longrightarrow & \mathbb{Q}^\times/(\mathbb{Q}^\times)^2 & \longrightarrow & H^1(\mathbb{Q}, \bar{E})[\psi] & \longrightarrow & 0 \\ & & & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \prod_\nu E(\mathbb{Q}_\nu)/\psi(E(\mathbb{Q}_\nu)) & \longrightarrow & \prod_\nu (\mathbb{Q}_\nu^\times/(\mathbb{Q}_\nu)^\times)^2 & \longrightarrow & \prod_\nu H^1(\mathbb{Q}_\nu, \bar{E})[\psi] & \longrightarrow & 0 \end{array}$$

We are now ready to make the following definition

Definition 4.2 (Selmer Group)**.** The Selmer group of the elliptic curve E is defined

$$\mathrm{Sel}(E) = \mathrm{Ker}\big((\mathbb{Q}^\times/(\mathbb{Q}^\times)^2 \to \prod_\nu H^1(\mathbb{Q}_\nu, \bar{E})[\psi]\big)$$

This group is important in rank computations primarily because it is effectively computable.

Theorem 4.3. *Let $E : y^2 = x^3 + ax^2 + bx$ and write $b = p_1^{e_1} \cdots p_t^{e_t}$. Then Sel $\simeq \{b_1 = \pm p_1^{a_1} \cdots p_t^{a_t} \,|\, a_i = 0$ or 1 and the equation $N^2 = b_1 M^4 + \frac{b}{b_1} e^4$ has a solution.$\}$*

Definition 4.4 (Tate-Shafarevich Group)**.** The Tate-Shafarevich group of the elliptic curve E is defined

$$\mathrm{TS}(E/\mathbb{Q}) = \mathrm{Ker}\big((H^1(\mathbb{Q}, \bar{E}) \to \prod_\nu H^1(\mathbb{Q}_\nu, \bar{E})[\psi]\big)$$