Galois cohomology and weak Mordell–Weil theorem

Yunhai Xiang

August 15, 2021

Abstract

This is my final project for the Spring 2021 reading course *Introduction to Arithmetic Geometry* at University of Waterloo, taught by Faisal Al-Faisal. In this write-up, we discuss an important tool in arithmetic geometry called Galois cohomology. In particular, we give an application of Galois cohomology by proving the weak Mordell–Weil theorem.

Contents

1 Introduction

Recall the basic fact from Galois theory that for some perfect field k with algebraic closure K, the Galois group $G = \mathrm{Gal}(K/k)$ is isomorphic to an inverse limit

$$G \cong \varprojlim \mathrm{Gal}(L/k)$$

ranging over the finite Galois extensions L/k with the natural projections. The inverse limits of finite groups, such as the example above, are called *profinite* groups. By viewing each of the Galois group $\mathrm{Gal}(L/k)$ as a topological group with the discrete topology, the resulting inverse limit G is endowed with the *Krull topology* in which a basis for the neighborhood at the identity is the collection of normal subgroups having finite index in G. This motivates us to apply tools in homological algebra to solve number theory problems. In particular, Galois cohomology is the study of group cohomology on Galois modules [1].

2 Group cohomology and Galois cohomology

We begin by revisiting the machinery of group cohomology.

Definition 2.1. Let G be a (multiplicative) group, a *G-module* is an (additive) abelian group M along with a group action $G \times M \to M$ compatible with addition, i.e. $g(a+b) = ga + gb$ for all $g \in G$ and $a, b \in M$. Equivalently, we can think of a G-module as a $\mathbf{Z}[G]$-module, where $\mathbf{Z}[G]$ is the group ring of G over the ring of integers $\mathbf{Z}$.

We write $\mathbf{Mod}_G$ for the category of G-modules, that is, the category whose objects are G-modules and morphisms are group homomorphisms that commute with scalar multiplication i.e. the group homomorphism $\varphi : M \to M$ such that $\varphi(gm) = g\varphi(m)$ for $m \in M$ and $g \in G$. In fact, the category $\mathbf{Mod}_G$ can be identified as the category of $\mathbf{Z}[G]$-modules.

Definition 2.2. For group G and G-module M, define the *group cochain complex* of G as

$$\cdots \xleftarrow{d^3} C^2(G;M) \xleftarrow{d^2} C^1(G;M) \xleftarrow{d^1} C^0(G;M) \xleftarrow{d^0} \mathbf{0}$$

where, for each $i \geq 0$, the group of i-cochains $C^i(G;M)$ is the group of maps $f : G^i \to M$ with pointwise addition (viewing $G^0 = \mathbf{1} = \{1\}$), and the differential $d^{i+1} : C^i(G;M) \to C^{i+1}(G;M)$ is such that $d^{i+1}f : G^{i+1} \to M$ is the function that maps $(g_1, \ldots, g_{i+1})$ to

$$g_1 f(g_2, \ldots, g_{i+1}) + \sum_{j=1}^{i} (-1)^j f(g_1, \ldots, g_{j-1}, g_j g_{j+1}, g_{j+2}, \ldots, g_{i+1}) + (-1)^{i+1} f(g_1, \ldots, g_i)$$

and $d^0 : \mathbf{0} \to C^0(G;M)$ is the trivial map $0 \mapsto [1 \mapsto 0]$ where $\mathbf{0} = \{0\}$. The *i-th cohomology group* of G is $H^i(G;M) = \mathrm{Ker}(d^{i+1})/\mathrm{Im}(d^i)$ for $i \geq 0$. This is well defined as $d^{i+1} \circ d^i = 0$ for $i \geq 0$.

Example 2.3. For $i = 0, 1$, the map $d^{i+1}f$ is defined as

$$(d^1 f)(g) = gf(1) - f(1)$$
$$(d^2 f)(g,h) = gf(h) - f(gh) + f(g)$$

and therefore the first two cohomology groups are

$$H^0(G;M) = \{f \in C^0(G;M) : \forall g \in G,\ gf(1) = f(1)\}$$
$$H^1(G;M) = \frac{\{f \in C^1(G;M) : \forall g,h \in G,\ f(gh) = gf(h) + f(g)\}}{\{f \in C^1(G;M) : \exists m \in M, \forall g \in G,\ f(g) = gm - m\}}$$

Note that $H^0(G;M)$ can be identified as the stabilizer $M^G = \{m \in M : \forall g \in G,\ gm = m\}$. Let $f \in C^1(G;M)$. If $f(gh) = gf(h) + f(g)$ for all $g, h \in G$, then f is called a *crossed homomorphism*; and if there exists $m \in M$ with $f(g) = gm - m$ for all $g \in G$, then f is called a *principal crossed homomorphism*. So $H^1(G;M)$ is the crossed homomorphisms modulo the principal ones.

Let A, B be G-modules and $\alpha : A \to B$ a morphism of G-modules, we remark that α induces group homomorphisms $\alpha^i : C^i(G; A) \to C^i(G; B)$ mapping $f \mapsto \alpha \circ f$ for each $i \geq 0$. The maps α^i for $i \geq 0$ are viewed collectively as a morphism of the cochain complexes $\alpha^\bullet : C^\bullet(G; A) \to C^\bullet(G; B)$. We denote the differential of the complex $C^\bullet(G; A)$ as d_A, and that of $C^\bullet(G; B)$ as d_B, then the differentials are compatible with $\alpha^\bullet$ in the sense of the following lemma.

Lemma 2.4. $d^i_B \circ \alpha^i = \alpha^{i+1} \circ d^i_A$ for all $i \geq 0$.

Proof. This can be proved via a routine check on the related definitions. □

By Lemma 2.4, we see that a G-module morphism α induces a well defined homomorphism on the cohomology groups $\alpha^* : H^i(G; A) \to H^i(G; B)$ for each $i \geq 0$, which is the obvious map i.e. the map that sends the equivalence class of f to the equivalence class of $\alpha^i(f)$. We omit the superscript of α^* for sake of clarity, as it does not cause confusion. The reason we need this induced homomorphism is because we want to show the existance of long exact sequences in the cohomology groups. But before we can prove this, we need two more lemmas.

Lemma 2.5. Let G be a group. Suppose we have a short exact sequence of G-modules

$$\mathbf{0} \longrightarrow A \xrightarrow{\alpha} B \xrightarrow{\beta} C \longrightarrow \mathbf{0}$$

then the induced sequence on the group cochain complex of G

$$\mathbf{0} \longrightarrow C^\bullet(G; A) \xrightarrow{\alpha^\bullet} C^\bullet(G; B) \xrightarrow{\beta^\bullet} C^\bullet(G, C) \longrightarrow \mathbf{0}$$

is exact.

Proof. Fix some $i \geq 0$. Let $f \in C^i(G; A)$ such that $\alpha \circ f = 0$, then since α is injective, $f = 0$. Hence α^i is injective. Let $f \in C^i(G; C)$, since β is surjective, $f = \beta \circ g$ for some $g \in C^i(G; B)$. Hence β^i is surjective. Next, for each $f \in C^i(G; B)$ with $\beta \circ f = 0$, since $\operatorname{Ker}(\beta) = \operatorname{Im}(\alpha)$, there exists $g \in C^i(G; A)$ with $\alpha \circ g = f$. Conversely, for each $g \in C^i(G; A)$, we have $\beta \circ (\alpha \circ g) = (\beta \circ \alpha) \circ g = 0$, since $\operatorname{Ker}(\beta) = \operatorname{Im}(\alpha)$. Thus $\operatorname{Ker}(\beta^i) = \operatorname{Im}(\alpha^i)$. Hence the sequence

$$\mathbf{0} \longrightarrow C^i(G; A) \xrightarrow{\alpha^i} C^i(G; B) \xrightarrow{\beta^i} C^i(G, C) \longrightarrow \mathbf{0}$$

is exact, and therefore the induced sequence on the group cochain complexes is exact. □

Moreover, the construction in Lemma 2.5 is natural in the sense of natural transformations, i.e., given a morphism between short exact sequences of G-modules, there is a corresponding morphism between the long exact sequences given by the induced homomorphisms between cohomology groups, which we will not explain in detail. Next, we need the following lemma.

Lemma 2.6 (Snake lemma)**.** In an abelian category, given a commutative diagram

$$\begin{tikzcd}
 & A \arrow[r, "a"] \arrow[d, "f"] & B \arrow[r, "b"] \arrow[d, "g"] & C \arrow[r] \arrow[d, "h"] & \mathbf{0} \\
\mathbf{0} \arrow[r] & D \arrow[r, "c"] & E \arrow[r, "d"] & F &
\end{tikzcd}$$

where the rows are exact and $\mathbf{0}$ is the zero object, then there exists an exact sequence

$$\operatorname{Ker}(f) \longrightarrow \operatorname{Ker}(g) \longrightarrow \operatorname{Ker}(h) \xrightarrow{\delta} \operatorname{Coker}(f) \longrightarrow \operatorname{Coker}(g) \longrightarrow \operatorname{Coker}(h)$$

where δ is known as the *connecting morphism*.

Proof. This is a familiar lemma in homological algebra. □

Now, we can finally prove the main theorem of this section.

Theorem 2.7. Let G be a group. Suppose we have a short exact sequence of G-modules

$$\begin{tikzcd} \mathbf{0} \arrow[r] & A \arrow[r, "\alpha"] & B \arrow[r, "\beta"] & C \arrow[r] & \mathbf{0} \end{tikzcd}$$

then there exists a long exact sequence of abelian groups

$$\begin{tikzcd} \mathbf{0} \arrow[r] & H^0(G;A) \arrow[r, "\alpha^*"] & H^0(G;B) \arrow[r, "\beta^*"] & H^0(G;C) \arrow[r, "\delta^0"] & H^1(G;A) \arrow[r, "\alpha^*"] & \cdots \end{tikzcd}$$

for some homomorphisms $\delta^i : H^i(G;C) \to H^{i+1}(G;A)$ for $i \geq 0$.

Proof. Fix some $j \geq 0$, and consider the diagram

$$\begin{tikzcd} \mathbf{0} \arrow[r] & C^j(G;A) \arrow[r, "\alpha^j"] \arrow[d, "d_A^{j+1}"] & C^j(G;B) \arrow[r, "\beta^j"] \arrow[d, "d_B^{j+1}"] & C^j(G;C) \arrow[r] \arrow[d, "d_C^{j+1}"] & \mathbf{0} \\ \mathbf{0} \arrow[r] & C^{j+1}(G;A) \arrow[r, "\alpha^{j+1}"] & C^{j+1}(G;B) \arrow[r, "\beta^{j+1}"] & C^{j+1}(G;C) \arrow[r] & \mathbf{0} \end{tikzcd}$$

then the rows are exact by Lemma 2.5. The exact sequence of cokernels $j = i - 1$ and kernels $j = i + 1$ can be placed in a second diagram

$$\begin{tikzcd} & C^i(G;A)/\mathrm{Im}(d_A^i) \arrow[r, "\alpha^i"] \arrow[d, "d_A^i"] & C^i(G;B)/\mathrm{Im}(d_B^i) \arrow[r, "\beta^i"] \arrow[d, "d_B^i"] & C^i(G;C)/\mathrm{Im}(d_C^i) \arrow[r] \arrow[d, "d_C^i"] & \mathbf{0} \\ \mathbf{0} \arrow[r] & \mathrm{Ker}(d_A^{i+1}) \arrow[r, "\alpha^{i+1}"] & \mathrm{Ker}(d_B^{i+1}) \arrow[r, "\beta^{i+1}"] & \mathrm{Ker}(d_C^{i+1}) & \end{tikzcd}$$

and so by the snake lemma, we have an exact sequence

$$\begin{tikzcd} \cdots \arrow[r, "\alpha^*"] & H^i(G;B) \arrow[r, "\beta^*"] & H^i(G;C) \arrow[r, "\delta^i"] & H^{i+1}(G;A) \arrow[r, "\alpha^*"] & H^{i+1}(G;B) \arrow[r, "\beta^*"] & \cdots \end{tikzcd}$$

by concatonation. □

Let A be a subgroup of G, then the inclusion $A \hookrightarrow G$ induces $\mathrm{Res} : H^i(G;M) \to H^i(A;M)$, the *restriction map* on the cohomologies, and if further that A is normal in G, then the quotient map $G \to G/A$ and inclusion $M^A \hookrightarrow M$ induces $\mathrm{Inf} : H^i(G/H;M^A) \to H^i(G;M)$, the *inflation map* on the cohomologies. We then have the following theorem.

Theorem 2.8. Let G be a group with normal subgroup A and M a G-module, then the sequence

$$\begin{tikzcd} \mathbf{0} \arrow[r] & H^1(G/A;M^A) \arrow[r, "\mathrm{Inf}"] & H^1(G;M) \arrow[r, "\mathrm{Res}"] & H^1(A;M) \end{tikzcd}$$

is exact.

Proof. The injectivity of inflation is obvious. Let f be a principal crossed homomorphism in the sense that f is zero in $H^1(G/A;M^A)$. Suppose that $f(\overline{g}) = (g-1)a$ for some $a \in M$ and $g \in G$, then $a \in M^A$ and $f(\overline{1}) = 0$, so Inf is injective. Also, note that $\mathrm{Res} \circ \mathrm{Inf}(f)(n) = f(\overline{n}) = 0$ for all $n \in A$. Next, let f be a principal crossed homomorphism in the sense that f is zero in $H^1(G;A)$ and suppose $\mathrm{Res}(f) = 0$. Then there exists $a \in M$ with $f(n) = (n-1)a$ for all $n \in A$. Define k as another principal crossed homomorphism by $k(g) = f(g) - (g-1)a$, then $k(n) = 0$ for all $n \in A$. Thus $k(gn) = gk(n) + k(g)$ for all $g \in G$ and $n \in A$, so k factors through G/A. Moreover, $k(g) = k(gg^{-1}ng) = k(ng) = nk(g) + k(n) = nk(g)$, thus k has image in M^A. Thus k is the inflation of a principal crossed homomorphism, proving the exactness. □

The exact sequence in Theorem 2.8 is the *inflation-restriction sequence*. In fact, under certain conditions, we have an inflation-restriction sequence on the higher cohomology groups.

Proposition 2.9. Let G be a group with normal subgroup A, and let M be a G-module. Suppose that $i \geq 1$, and that $H^j(A; M)$ is trivial for all $1 \leq j \leq i-1$, then the sequence

$$\mathbf{0} \longrightarrow H^i(G/A; M^A) \xrightarrow{\text{Inf}} H^i(G; M) \xrightarrow{\text{Res}} H^i(A; M)$$

is exact.

We will not give a proof of Proposition 2.9 in this write-up, and we will proceed to discuss Galois cohomology, i.e. group cohomology on the profinite Galois group. Recall once more that for some perfect field k with algebraic closure K, the Galois group $G = \text{Gal}(K/k)$ is isomorphic to an inverse limit

$$G \cong \varprojlim \text{Gal}(L/k)$$

ranging over the finite Galois extensions L/k with the natural projections. This fact makes G a profinite group, and the Krull topology is a topology on G where a basis for the neighborhood at the identity is the collection of normal subgroups having finite index in G. Next, a *topological G-module* is a topological abelian group M where the action $G \times M \to M$ is continuous. By restricting $C^i(G; M)$ to the continuous functions $f : G^i \to M$, we can check that all theorems and lemmas we have proved so far still holds after slight modifications.

3 Kummer sequence and weak Mordell–Weil theorem

Let k be a perfect field with algebraic closure K. Fix an elliptic curve E over k. There is a well known structure theorem for the elliptic curve group $E(k)$, the Mordell–Weil theorem.

Proposition 3.1 (Mordell–Weil)**.** The elliptic curve group $E(k)$ is finitely generated.

Since $E(k)$ is an abelian group, Mordell–Weil tells us that $E(k) \cong E(k)_{\text{tors}} \oplus \mathbf{Z}^{\oplus r}$ where $r \in \mathbf{N}$ is the *rank* of the elliptic curve and $E(k)_{\text{tors}}$ is a finite group, i.e. the torsion component. The proof of this theorem consists of two parts. The first part is the weak Mordell–Weil theorem, and the second part is an infinite descent argument using height functions [2]. We will not discuss the second part, and we will focus on discussing the first part.

Proposition 3.2 (weak Mordell–Weil)**.** The group $E(k)/nE(k)$ is finite for all $n \geq 2$.

To show the weak Mordell–Weil theorem, we first make the important observation that for $n \geq 2$, the following sequence of topological $\text{Gal}(K/k)$-modules

$$\mathbf{0} \longrightarrow E(K)[n] \longrightarrow E(K) \xrightarrow{n} E(K) \longrightarrow \mathbf{0} \qquad (\star)$$

is exact. Next, we deduce an exact sequence of abelian groups from $(\star)$.

Lemma 3.3. For $n \geq 2$, the sequnce of abelian groups

$$\mathbf{0} \to E(k)/nE(k) \to H^1(\text{Gal}(K/k), E(K)[n]) \to H^1(\text{Gal}(K/k), E(K))[n] \to \mathbf{0}$$

is exact.

Proof. By applying Theorem 2.7 to $(\star)$, we have a long exact sequence

$$\begin{tikzcd}
\mathbf{0} \arrow[r] & E(k)[n] \arrow[r] & E(k) \arrow[r, "n"] & E(k) \arrow[d, "\delta"] \\
& H^1(\text{Gal}(K/k); E(K)) & H^1(\text{Gal}(K/k); E(K)) \arrow[l, "n"'] & H^1(\text{Gal}(K/k); E(K)[n]) \arrow[l]
\end{tikzcd}$$

where the rest of the long exact sequence is omitted as we don't need them. We can then deduce the short exact sequence by modifying this long exact sequence in the obvious way. □

If the abelian group $H^1(\mathrm{Gal}(K/k), E(K)[n])$ is finite then life is easy. Unfortunately, this is not true in general. Thus, we aim to find a smaller group such that it also contains the image of $E(k)/nE(k)$. We observe that for a place v of k, by considering E/k_v, we obtain a diagram.

$$\begin{tikzcd}
\mathbf{0} \arrow[r] & E(k)/nE(k) \arrow[r] \arrow[d] & H^1(\mathrm{Gal}(K/k), E(K)[n]) \arrow[r] \arrow[d] & H^1(\mathrm{Gal}(K/k), E(K))[n] \arrow[r] \arrow[d] & \mathbf{0} \\
\mathbf{0} \arrow[r] & E(k_v)/nE(k_v) \arrow[r] & H^1(\mathrm{Gal}(K_v/k_v), E(K_v)[n]) \arrow[r] & H^1(\mathrm{Gal}(K_v/k_v), E(K_v))[n] \arrow[r] & \mathbf{0}
\end{tikzcd}$$

where $K_v = \overline{k_v}$. This motivates us the define the Selmer groups and Tate–Shafarevich groups.

Definition 3.4. For an elliptic curve E/k and $n \geq 2$, define the n-Selmer group of E as

$$\mathrm{Sel}_n(E/k) = \mathrm{Ker}\left(H^1(\mathrm{Gal}(K/k); E(K)[n]) \longrightarrow \prod_v H^1(\mathrm{Gal}(K_v/k_v); E(K_v))\right)$$

and similarly, we define the group

$$\mathrm{Sha}(E/k) = \mathrm{Ker}\left(H^1(\mathrm{Gal}(K/k); E(K)) \longrightarrow \prod_v H^1(\mathrm{Gal}(K_v/k_v); E(K_v))\right)$$

as the Tate–Shafarevich group of E.

Lemma 3.5 (Kummer sequence)**.** For $n \geq 2$, the sequence of abelian groups

$$\mathbf{0} \longrightarrow E(k)/nE(k) \longrightarrow \mathrm{Sel}_n(E/k) \longrightarrow \mathrm{Sha}(E/k)[n] \longrightarrow \mathbf{0}$$

is exact.

Proof. We can deduce this from Lemma 3.3 with kernel-cokernel exact sequence. □

The Tate-Shafarevich has a geometric interpretation that it measures the failure of the local-global principle. In general, it is conjectured that $\mathrm{Sha}(E/k)$ is finite. However, we know that the n-Selmer group for an elliptic curve is finite. Thus, we can finally finish the proof.

Theorem 3.6 (weak Mordell–Weil)**.** The group $E(k)/nE(k)$ is finite for all $n \geq 2$.

Proof. By Lemma 3.5, $E(k)/nE(k)$ injects into the n-Selmer group of E, which is finite. □

References

[1] J.-P. Serre, *Galois Cohomology*. Springer.

[2] J. Silverman, *The Arithmetic of Elliptic Curves*. Graduate Texts in Mathematics, Springer.