18.787: Selmer Groups and Euler Systems

Nir Elber

Fall 2025

Contents

How strange to actually have to see the path of your journey in order to make it.

—Neal Shusterman, [Shu16]

Theme 1
2-Selmer Groups

1.1 September 4

Here are some administrative notes.

- There are no exams. Half of the grade will be based on problem sets (there will be two or three), all posted before November. The other half will be based on note-taking; currently, one must take notes for at least one lecture.
- There is a Canvas, which contains information about the course.
- There will be office hours from 11AM to 12PM on Tuesday and Thursday in 2-476. There should also be availability by appointment if desired.

There is no class next week, so the next class is September 16th.

1.1.1 Algebraic Rank

We will overview the course today. This course will be interested in Selmer groups and Euler systems. The relationship between these two notions is that Euler systems are a popular way to bound the size of Selmer groups.

To explain these notions, fix an elliptic curve E over a field k. (For us, an elliptic curve is a smooth, proper, connected curve of genus 1 with a distinguished point $\mathcal{O} \in E(k)$.) We will frequently take k to be a global, local, or finite field.

Remark 1.1. If the characteristic of k is not 2 or 3, then E admits an affine model

$$E\colon Y^2Z = X^3 + aXZ^2 + bZ^3,$$

where $a, b \in k$. The distinguished point is $[0:1:0]$.

We also recall that E is identified with its Jacobian by the isomorphism $E \to \operatorname{Jac} E$ defined by $x \mapsto (x) - (\mathcal{O})$, which gives E a group law.

This group law can be seen to be commutative, so $E(k)$ is an abelian group.

Theorem 1.2 (Mordell–Weil). For any elliptic curve E over a number field k, the abelian group $E(k)$ is finitely generated.

Thus, $E(k)$ can be understood by its torsion subgroup $E(k)_{\mathrm{tors}}$ and its rank $\operatorname{rank} E(k)$. This rank is important enough to be given a name.

Definition 1.3 (algebraic rank)**.** For any elliptic curve E over a number field k. Then the *algebraic rank* $r_{\text{alg}}(E)$ equals $\operatorname{rank} E(k)$.

There is another notion of rank. For this, we recall the definition of the L-function.

Definition 1.4. Fix an elliptic curve E defined over a number field k. Then its *L-function* is defined as

$$L(E,s) \doteq \prod_p \frac{1}{1-a_p p^{-s}+p^{1-2s}},$$

where $a_p := (p+1) - \#E(\mathbb{F}_p)$ and $\doteq$ means that this is an equality up to some finite number of factors.

Remark 1.5. If E is defined over $\mathbb{Q}$, it is known that $L(E,s) = L(f,s)$ for some modular Hecke eigenform f with weight 2. Thus, $L(E,s)$ admits a holomorphic continuation to $\mathbb{C}$, and there is a functional equation relating $L(E,s)$ and $L(E,2-s)$.

Once we know $L(E,s)$ admits a continuation, we can make sense of the Birch and Swinnerton-Dyer conjecture.

Definition 1.6 (analytic rank)**.** The *analytic rank* $r_{\text{an}}(E)$ of an elliptic curve E defined over $\mathbb{Q}$ is defined as the order of vanishing of $L(E,s)$ at $s=1$.

Conjecture 1.7 (Birch–Swinnerton-Dyer)**.** Fix an elliptic curve E defined over $\mathbb{Q}$. Then

$$r_{\text{an}}(E) = \operatorname{rank} E(\mathbb{Q}).$$

While this is still a conjecture, there is a lot of evidence nowadays.

Theorem 1.8 (Gross–Zagier–Kolyvagin)**.** Fix an elliptic curve E defined over $\mathbb{Q}$. If $r_{\text{an}}(E) \le 1$, then $r_{\text{an}} = \operatorname{rank} E(\mathbb{Q})$.

1.1.2 The Tate–Shafarevich Group

In fact, Gross–Zagier–Kolyvagin know more: one can prove "finiteness of Ш."

Definition 1.9 (Tate–Shafarevich group)**.** Fix an elliptic curve E defined over a global field k. Then we define the *Tate–Shafarevich group* $Ш(E/k)$ as the kernel

$$Ш(E/k) := \ker\left(\mathrm{H}^1(k,E) \to \prod_v \mathrm{H}^1(k_v,E)\right),$$

where the right-hand product is taken over the places v of k.

Remark 1.10. Roughly speaking, $\mathrm{H}^1(k,E)$ classifies torsors of E, which amount to curves C with Jacobian isomorphic to E. Being in the kernel means that C is isomorphic to E over each local field k_v, which amounts to $C(k_v)$ being nonempty. Thus, we see that $Ш(E/k)$ being nontrivial amounts to the existence of certain genus-1 curves admitting points locally but not globally.

It may seem strange to have points locally but not globally, but such things do happen.

Example 1.11. The projective cubic curve $C\colon 3X^3+4Y^3+5Z^3=0$ has points over every local completion over $\mathbb{Q}$, but C turns out to not admit rational points. Note that it is not so easy to actually prove that C does not admit rational points. Also, this example is not so pathological: C is a torsor for the elliptic curve $E\colon X^3+Y^3+60Z^3=0$, so it provides a nontrivial element of $\text{Ш}(E/\mathbb{Q})$.

Remark 1.12. It turns out that $[C]$ has order 3. Professor Zhang explained that this can be seen because C has an effective divisor of degree 3.

However, these bizarre things should not happen so frequently.

Conjecture 1.13. Fix an elliptic curve E over a global field k. Then $\text{Ш}(E/k)$ is finite.

Remark 1.14. When trying to prove this conjecture, one frequently just wants to know $\text{Ш}(E/k)[p^\infty]$ is finite for all primes p. (Of course, one also wants to know that $\text{Ш}(E/k)$ vanishes for primes p large enough.) It is often possible to verify that $\text{Ш}(E/k)[p^\infty]$ is finite for a given prime p, but it is difficult to actually show that $\text{Ш}(E/k)$ is then finite! One does not even know if the dimensions $\dim_{\mathbb{F}_p}\text{Ш}(E/k)[p]$ are bounded.

Let's now add to our previous theorem.

Theorem 1.15 (Gross–Zagier–Kolyvagin)**.** Fix an elliptic curve E defined over $\mathbb{Q}$. If $r_{\text{an}}(E)\le 1$, then $r_{\text{an}}=\operatorname{rank}E(\mathbb{Q})$ and $\#\text{Ш}(E/\mathbb{Q})<\infty$.

This theorem is more or less the only way one can know that $\text{Ш}(E/k)$ is finite. In particular, we do not have a single example of an elliptic curve E with analytic rank at least 2 and $\text{Ш}(E/k)$ known to be finite.[1]

Remark 1.16. Professor Zhang does not know the answer to the following question: for each prime p, does there exist an elliptic curve E with $\text{Ш}(E/\mathbb{Q})[p]\neq 0$?

1.1.3 Selmer Groups

Even though r_{alg} and Ш appear to be difficult invariants, one can combine them into the Selmer group, and then they seem to be controlled.

For the moment, it is enough to know that these Selmer groups $\operatorname{Sel}_m(E)$ are indexed by integers $m\in\mathbb{Z}$ and sit in a short exact sequence

$$0\to E(k)/mE(k)\to\operatorname{Sel}_m(E/k)\to\text{Ш}(E)[m]\to 0.$$

For example, it follows that

$$\dim_{\mathbb{F}_p}\operatorname{Sel}_p(E/k)=r_{\text{alg}}(E)+\dim_{\mathbb{F}_p}\#\text{Ш}(E)[p]+\dim_{\mathbb{F}_p}E[p].$$

This last term is easy to compute, so we may ignore it; for example, it is known to vanish when $k=\mathbb{Q}$ and p is large. Anyway, the point is that the Selmer group has managed to combine information about the algebraic rank and Ш.

But now we have a miracle: Selmer groups are rather computable. In particular, $\operatorname{Sel}_2(E)$ is pretty well-understood, using quadratic twists. Working concretely, an elliptic curve $E\colon Y^2=f(X,Z)$ admits a quadratic twist $E^{(d)}\colon dY^2=f(X,Z)$; this is called a quadratic twist because E and $E^{(d)}$ become isomorphic after base-changing from $\mathbb{Q}$ to $\mathbb{Q}(\sqrt{d})$. It now turns out that

$$\operatorname{Sel}_m(E)\subseteq\mathrm{H}^1(\mathbb{Q},E[m]),$$

[1] Gross–Zagier have also proven that there exist elliptic curves with analytic rank larger than 1.

cut out by some local conditions; the point is that this right-hand group can frequently be computed by hand. For example, if $m = 2$, then $E[2]$ is found as from the roots of $f(X, 1)$. Notably, $E[2]$ won't change when taking quadratic twists, but the Selmer group may get smaller.

Here is the sort of thing we are recently (!) able to prove, using 2-Selmer groups.

Theorem 1.17 (Zywina)**.** Let K/F be a quadratic extension of number fields. Then there is an elliptic curve E over F such that

$$r_{\text{alg}}(E/K) = r_{\text{alg}}(E/F) = 1.$$

Remark 1.18. Zywina's argument follows an idea of Koymans–Pagano. The idea is to compute the 2-Selmer groups by hand to upper-bound the rank, and then one can do some tricks to lower-bound the rank.

If we have time, we may also get to the following result about distribution of ranks.

Theorem 1.19 (Smith)**.** Fix an elliptic curve E over $\mathbb{Q}$. As d varies, $\operatorname{Sel}_{2^\infty}\left(E^{(d)}/\mathbb{Q}\right)$ has rank 0 half of the time and 1 half of the time.

Let's see what we can say for higher dimensions, so throughout X is smooth proper variety over $\mathbb{Q}$. It turns out that a Selmer group can be defined for any Galois representation, so the following conjecture makes sense.

Conjecture 1.20 (Bloch–Kato)**.** Let X be a smooth proper variety over $\mathbb{Q}$. Then for any integer i, we have

$$\operatorname{Sel}_{p^\infty}\left(\mathrm{H}^{2i-1}_{\text{ét}}(X_{\overline{\mathbb{Q}}};\mathbb{Q}_\ell)(i)\right) = \operatorname{ord}_{s=0} L\left(\mathrm{H}^{2i-1}_{\text{ét}}(X_{\overline{\mathbb{Q}}};\mathbb{Q}_\ell)(i), s\right).$$

There is some evidence for this conjecture in higher dimensions, but they largely arise from Shimura varieties. Most of what is known is for when the order of vanishing is zero.

Let's end class by actually defining a Selmer group.

Definition 1.21 (group cohomology)**.** Fix a group G. The *group cohomology groups* $\mathrm{H}^\bullet(G;-)$ are the right-derived functors for the invariants functor $(\cdot)^G\colon \operatorname{Mod}_{\mathbb{Z}[G]} \to \operatorname{Ab}$. When G is profinite, we define the group cohomology as the limit of the group cohomology of the finite quotients. When G is an absolute Galois group of a field k, we may write $\mathrm{H}^\bullet(k;-)$ for the group cohomology.

To define the Selmer groups, we recall the short exact sequence

$$0 \to E[m] \to E \overset{m}{\to} E \to 0$$

of group schemes (and also over $\overline{k}$-points). Taking Galois cohomology produces a long exact sequence

$$E(k) \overset{m}{\to} E(k) \to \mathrm{H}^1(k;E[m]) \to \mathrm{H}^1(k;E) \overset{m}{\to} \mathrm{H}^1(k;E),$$

so there is a short exact sequence

$$0 \to E(k)/mE(k) \to \mathrm{H}^1(k;E[m]) \to \mathrm{H}^1(k;E)[m] \to 0.$$

If k is global, there is also a short exact sequence at each completion for each finite place v.

Definition 1.22 (Selmer group)**.** We define the m-Selmer group is defined as the fiber product in the following diagram.

$$\begin{tikzcd}
\operatorname{Sel}_m(E/k) \arrow[r] \arrow[d] \arrow[dr, phantom, "\lrcorner", very near start] & \mathrm{H}^1(\mathbb{Q};E[m]) \arrow[d] \\
\prod_v E(\mathbb{Q}_v)/mE(\mathbb{Q}_v) \arrow[r] & \prod_v \mathrm{H}^1(\mathbb{Q}_v;E[m])
\end{tikzcd}$$

1.2 September 16

Welcome to the second class of the semester. The note-taker is furiously eating lunch.

1.2.1 Construction of Group Cohomology

For the next few weeks, we are going to focus on proving Theorem 1.17. This will be done using Selmer groups.

We begin by recalling the definition of group cohomology.

Definition 1.23 (module)**.** Fix a group G. Then a G-*module* is an abelian group M equipped with an action by G for which $1m = m$ for all $m \in M$ and $g(m+n) = gm + gn$ for all $g \in G$ and $m, n \in M$.

Remark 1.24. Equivalently, a G-module is a module for the ring $\mathbb{Z}[G]$.

Definition 1.25 (invariants)**.** Fix a group G. Then there is a functor $(-)^G \colon \mathrm{Mod}_{\mathbb{Z}[G]} \to \mathrm{Ab}$ given on objects by sending a G-module M to the subset

$$M^G := \{m \in M : gm = m \text{ for all } g \in G\}.$$

On morphisms, it sends $f \colon M \to N$ to the restriction $f \colon M^G \to N^G$.

Remark 1.26. One can show that there is a natural isomorphism

$$\mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, -) \Rightarrow (-)^G.$$

It sends a map $f \colon \mathbb{Z} \to M$ to $f(1)$; the inverse sends $m \in M^G$ to the map $f \colon \mathbb{Z} \to M$ given by $k \mapsto km$.

Definition 1.27 (group cohomology)**.** Fix a group G. The *group cohomology groups* $\mathrm{H}^\bullet(G; -)$ are the right-derived functors for the invariants functor $(\cdot)^G \colon \mathrm{Mod}_{\mathbb{Z}[G]} \to \mathrm{Ab}$.

Remark 1.28. In light of the natural isomorphism $(-)^G = \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, -)$, we see that

$$\mathrm{H}^\bullet(G, -) = \mathrm{Ext}^\bullet_{\mathbb{Z}[G]}(\mathbb{Z}, -).$$

1.2.2 Some Calculations

Because we are now dealing with Ext groups, there are two ways to compute $\mathrm{H}^\bullet(G, M)$.

- We can build an injective resolution of M, apply $(-)^G$, and take cohomology.
- We can build a projective resolution of $\mathbb{Z}$, apply $\mathrm{Hom}_{\mathbb{Z}[G]}(-, M)$, and take cohomology.

The second is easier for the purposes of calculation.

Example 1.29. It turns out that there is a free resolution

$$\cdots \to \mathbb{Z}\left[G^3\right] \to \mathbb{Z}\left[G^2\right] \to \mathbb{Z}[G] \to \mathbb{Z} \to 0.$$

Here, the map $\mathbb{Z}[G] \to \mathbb{Z}$ sends $\sum_g a_g g$ to $\sum_g a_g$. In general, the map $d_{n+1}\colon \mathbb{Z}\left[G^{n+1}\right] \to \mathbb{Z}\left[G^n\right]$ is given by $\mathbb{Z}$-linearly extending

$$d_{n+1}(g_0, \ldots, g_n) := \sum_{i=0}^{n} (-1)^i (g_0, \ldots, g_{i-1}, g_{i+1}, \ldots, g_n).$$

One can check that this is a free resolution of $\mathbb{Z}$. We let $\mathcal{P}_\bullet$ be the above complex where we have truncated off $\mathbb{Z}$, so we see that $\mathrm{H}^i(G; M)$ is

$$\operatorname{Ext}^i_{\mathbb{Z}[G]}(\mathbb{Z}, M) = \mathrm{H}^i(\operatorname{Hom}_G(\mathcal{P}_\bullet, M)).$$

Remark 1.30. If G is finite and M is finite, then a direct calculation of the cohomology via the resolution in Example 1.29 implies that $\mathrm{H}^i(G; M)$ is finite in all degrees.

While the combinatorics in Example 1.29 becomes difficult for large n, we can be fairly explicit about $n = 1$. In this case, one can show that $\mathrm{H}^1(G; M)$ is isomorphic to the quotient of the crossed homomorphisms by the principal crossed homomorphisms.

Definition 1.31 (crossed homomorphism)**.** Fix a group G and a G-module M. Then a *crossed homomorphism* is a function $f\colon G \to M$ for which

$$f(gh) = gf(h) + f(g)$$

for all $g, h \in G$.

Example 1.32 (principal crossed homomorphism)**.** For any $m \in M$, we can define a map $f\colon G \to M$ by

$$f(g) := (g - 1)m.$$

This is a crossed homomorphism, which amounts to checking

$$(gh - 1)m \stackrel{?}{=} g(h - 1)m + (g - 1)m.$$

We call such a crossed homomorphism "principal."

Example 1.33. If the action of G on M is trivial, then a crossed homomorphism is just a group homomorphism. Additionally, all the principal crossed homomorphisms vanish, so we see that

$$\mathrm{H}^1(G; M) = \operatorname{Hom}_{\mathbb{Z}}(G, M).$$

For example, $\mathrm{H}^1(1; \mathbb{Z}) = \mathbb{Z}$ is infinite.

In the case where G is cyclic, there is an easier resolution than the one in Example 1.29.

Proposition 1.34. Fix a finite cyclic group G. Then for any G-module M and index $i > 0$, we have

$$\mathrm{H}^i(G; M) = \begin{cases} M^G / \operatorname{im} \mathrm{N}_G & \text{if } i \text{ is even,} \\ \ker \mathrm{N}_G / \operatorname{im}(\sigma - 1) & \text{if } i \text{ is odd.} \end{cases}$$

In particular, $\{\mathrm{H}^i(G; M)\}_{i>0}$ is 2-periodic.

Proof. Suppose that G is finite cyclic of order n and generated by some σ. We will build an explicit resolution for $\mathbb{Z}$. We start with the degree map $\mathbb{Z}[G] \twoheadrightarrow \mathbb{Z}$ has kernel generated by $(\sigma - 1)$, so we can surject onto its kernel via the map $(\sigma - 1)\colon \mathbb{Z}[G] \to \mathbb{Z}[G]$. On the other hand, the kernel of $(\sigma - 1)$ is exactly isomorphic to $\mathbb{Z}$, given by the elements of the form $k \sum_{i=0}^{n-1} \sigma^i$ where k is some integer. In other words, the kernel of $(\sigma - 1)$ is given by the norm map $\mathrm{N}_G\colon \mathbb{Z}[G] \to \mathbb{Z}[G]$, where $\mathrm{N}_G(x) := \sum_{g \in G} gx$. Because we are back at $\mathbb{Z}$, we see that we can iterate to produce a resolution

$$\cdots \xrightarrow{(\sigma-1)} \mathbb{Z}[G] \xrightarrow{\mathrm{N}_G} \mathbb{Z}[G] \xrightarrow{(\sigma-1)} \mathbb{Z}[G] \xrightarrow{\deg} \mathbb{Z} \to 0.$$

We now compute cohomology. After truncating and applying $\operatorname{Hom}_{\mathbb{Z}[G]}(-, M)$, we receive the complex

$$0 \to M \xrightarrow{\sigma-1} M \xrightarrow{\mathrm{N}_G} M \overset{\sigma-1}{M} \to \cdots,$$

where the leftmost M lives in degree 0. For example, we can see that $\mathrm{H}^0(G; M)$ is $\ker(\sigma - 1)$, which is $\{m \in M : \sigma m = m\}$, which is M^G. Continuing, for $i > 0$, we see that

$$\mathrm{H}^i(G; M) = \begin{cases} M^G / \operatorname{im} \mathrm{N}_G & \text{if } i \text{ is even,} \\ \ker \mathrm{N}_G / \operatorname{im}(\sigma - 1) & \text{if } i \text{ is odd,} \end{cases}$$

as desired. ■

1.2.3 Change of Group

We will get some utility out of having more functors.

Definition 1.35 (induction)**.** Fix a subgroup $H \subseteq G$. Then there is an *induction* functor $\operatorname{Ind}_H^G\colon \operatorname{Mod}_H \to \operatorname{Mod}_G$ given on objects by sending any H-module N to $\operatorname{Ind}_H^G N$, defined as the module of functions $f\colon G \to N$ for which $f(hx) = hf(x)$ for any $h \in H$. This is a G-module with action given by

$$(gf)(x) := f(xg).$$

With an induction, we also have a restriction.

Definition 1.36 (restriction)**.** Fix a subgroup $H \subseteq G$. Then there is a *restriction* functor $\operatorname{Res}_H^G\colon \operatorname{Mod}_G \to \operatorname{Mod}_H$ given on objects by sending any G-module M to the same abelian group equipped with an H-action via the inclusion $H \subseteq G$. This functor is the identity on morphisms.

Remark 1.37. We can define a map $M \to \operatorname{Ind}_H^G \operatorname{Res}_H^G M$ given by sending $m \in M$ to the map $f\colon G \to M$ defined by $f(g) := gm$. This gives part of the adjunction.

Here are the results on induction and restriction.

Proposition 1.38 (Frobenius reciprocity)**.** Fix a subgroup H of a finite group G. Then Ind_H^G and Res_H^G are adjoints of each other. In particular, $\operatorname{Ind}_H^G\colon \operatorname{Mod}_H \to \operatorname{Mod}_G$ is an exact functor.

Proposition 1.39 (Shapiro's lemma). Fix a subgroup H of a finite group G. Then there is a natural isomorphism

$$\mathrm{H}^\bullet\left(G;\operatorname{Ind}_H^G(-)\right)\simeq\mathrm{H}^i(H;-).$$

It turns out that restriction has a sort of dual.

Definition 1.40 (corestriction). Fix a finite-index subgroup H of a group G. Then we define the *corestriction* $\operatorname{Cores}\colon \mathrm{H}^i(H;M)\to\mathrm{H}^i(G;M)$ map by extending the map $M^H\to M^G$ in degree 0 defined by

$$m\mapsto\sum_{gH\in G/H}gm.$$

Remark 1.41. It turns out that the composite

$$\mathrm{H}^i(G;M)\overset{\mathrm{Res}}{\to}\mathrm{H}^i(H;M)\overset{\mathrm{Cores}}{\to}\mathrm{H}^i(G;M)$$

is multiplication by $[G:H]$. For example, if G is finite, we can set H to be the trivial group so that the middle term vanishes in positive degree; thus, we see that $\mathrm{H}^i(G;M)$ is $|G|$-torsion for $i>0$.

Our last functor allows us to take quotients.

Definition 1.42 (inflation). Fix a normal subgroup H of a group G. Then for any G-module M, there is an inflation map $\mathrm{H}^\bullet\left(G/H;M^H\right)\to\mathrm{H}^\bullet(G;M)$ defined as the composite

$$\mathrm{H}^\bullet\left(G/H,M^H\right)\to\mathrm{H}^\bullet\left(G;M^H\right)\to\mathrm{H}^\bullet(G;M).$$

The left map exists via the forgetful functor $\operatorname{Mod}_{G/H}\to\operatorname{Mod}_G$ induced by the quotient $G\twoheadrightarrow G/H$. The right map exists by functoriality of $\mathrm{H}^\bullet(G;-)$.

Here is the result we need on inflation.

Proposition 1.43 (Inflation–restriction). Fix a G-module M. Then there is an exact sequence

$$0\to\mathrm{H}^1(G/H;M^H)\overset{\mathrm{Inf}}{\to}\mathrm{H}^1(G;M)\overset{\mathrm{Res}}{\to}\mathrm{H}^1(H;M)^{G/H}.$$

1.2.4 Galois Cohomology

We quickly explain how to take cohomology for profinite groups.

Example 1.44. Fix a finite field k with q elements. Then $\operatorname{Gal}(\overline{k}/k)$ is a profinite group with topological generator given by the Frobenius. Explicitly,

$$\operatorname{Gal}(\overline{k}/k)=\lim_n\operatorname{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)=\lim_n\mathbb{Z}/n\mathbb{Z}=\widehat{\mathbb{Z}}.$$

Definition 1.45 (discrete). Fix a profinite group G. Then a G-module M is *discrete* if and only if the stabilizer $\operatorname{Stab}_G(m)$ is open for all $m\in M$.

Remark 1.46. Equivalently, we are asking for the action map $G\times M\to M$ to be continuous, where M has been given the discrete topology: the fiber over the open set $\{m\}$ of M contains the open subset $\operatorname{Stab}_G(m)\times\{m\}$.

Definition 1.47 (continuous group cohomology)**.** Fix a profinite group G, and write $G = \lim_H G/H$, where the limit varies over open normal subgroups. Then we define

$$\mathrm{H}^i_{\mathrm{cts}}(G;M) := \operatorname*{colim}_{\text{open normal } H\subseteq G} \mathrm{H}^i\left(G/H; M^H\right).$$

We will frequently write $\mathrm{H}^i(G;M)$ for $\mathrm{H}^i_{\mathrm{cts}}(G;M)$ whenever G is profinite. In particular, we will never use ordinary group cohomology for profinite groups G.

Remark 1.48. Equivalently, following Example 1.29, we can define $\mathrm{H}^i_{\mathrm{cts}}(G;M)$ as

$$\mathrm{H}^i(\mathrm{Hom}_{\mathrm{cont}}(\mathcal{P}_\bullet, M)),$$

where we are now requiring that the maps from $\mathcal{P}_j \to M$ be continuous.

We can now upgrade our calculation for cyclic groups to procyclic groups.

Proposition 1.49. Fix a procyclic group G with generator σ. Fix a finite discrete G-module M. Then

$$\mathrm{H}^i\left(G;M\right) = \begin{cases} M^G & \text{if } i = 0, \\ M/(\sigma - 1) & \text{if } i = 1, \\ 0 & \text{if } i \geq 2. \end{cases}$$

Remark 1.50. Equivalently, the cohomology of M is computed via the two-term complex

$$0 \to M \overset{\sigma-1}{\to} M \to 0.$$

This allows us to say something about Galois cohomology.

Notation 1.51. Fix a field k and a commutative group scheme X over k. Then we set the notation

$$\mathrm{H}^i(k;X) := \mathrm{H}^i\left(\mathrm{Gal}(\overline{k}/k); X(\overline{k})\right).$$

Example 1.52. Fix a finite field k. From Proposition 1.49, we see that $\mathrm{H}^i(k;M) = 0$ for $i \geq 2$ for any finite discrete $\mathrm{Gal}(\overline{k}/k)$-module M.

1.3 September 18

Today, we will continue to review Galois cohomology.

1.3.1 Local Duality

Akin to Proposition 1.49, we have the following duality statement for local fields.

Theorem 1.53 (Tate)**.** Fix a finite extension K of $\mathbb{Q}_p$, set $G := \operatorname{Gal}(\overline{K}/K)$ for brevity, and let M be a finite discrete G-module.

(a) Finiteness: the modules $\mathrm{H}^i(K; M)$ are finite for all i and vanishes for $i \geq 3$.

(b) Duality: for a G-module M, we define the G-module $M^* := \operatorname{Hom}_{\mathbb{Z}}(M, \mu_\infty(\overline{K}))$. Then there is a perfect pairing
$$\mathrm{H}^i(K; M) \times \mathrm{H}^{2-i}(K; M^*) \to \mathbb{Q}/\mathbb{Z}.$$

(c) Euler characteristic formula: one has
$$\frac{\#\mathrm{H}^0(K; M) \cdot \#\mathrm{H}^2(K; M)}{\#\mathrm{H}^1(K; M)} = \frac{1}{\#(\mathcal{O}_K/(\#M)\mathcal{O}_K)}.$$

Remark 1.54. One can define the pairing via a cup product
$$\cup\colon \mathrm{H}^i(K; M) \times \mathrm{H}^{2-i}(K; M^*) \to \mathrm{H}^2(K; \mu_\infty),$$
and it turns out that the target is isomorphic to $\mathbb{Q}/\mathbb{Z}$ (via the "local invariant" map of local class field theory).

Remark 1.55. One calls (c) an Euler characteristic formula because the invariant
$$\chi(M) := \frac{\#\mathrm{H}^0(K; M) \cdot \#\mathrm{H}^2(K; M)}{\#\mathrm{H}^1(K; M)}$$
behaves like an Euler characteristic. Indeed, it is like an alternating sum of cohomology groups.

Remark 1.56. It is possible to check Theorem 1.53 explicitly for $M \in \{\mathbb{Z}/m\mathbb{Z}, \mu_m\}$.

In order to relate local fields with finite fields, we should explain how one can recover an unramified cohomology.

Definition 1.57 (inertia group)**.** Fix a local field K with finite residue field k. Then the Galois action on K preserves the absolute value and therefore descends to $\mathcal{O}_K/\mathfrak{p}_K = k$. We define the *inertia subgroup* I_K of $\operatorname{Gal}(\overline{K}/K)$ to fit in the short exact sequence
$$1 \to I_K \subseteq \operatorname{Gal}(\overline{K}/K) \to \operatorname{Gal}(\overline{k}/k) \to 1.$$

Remark 1.58. Let K^{ur} be the maximal unramified extension of K. Then we see that $\operatorname{Gal}(K^{\mathrm{ur}}/K)$ is simply $\operatorname{Gal}(\overline{K}/K)/I_K$.

Definition 1.59 (unramified)**.** Fix a local field K. Then a $\operatorname{Gal}(\overline{K}/K)$-module M is *unramified* if and only if I_K acts trivially on M. In this case, we define the *unramified cohomology* $\mathrm{H}^i_{\mathrm{ur}}(K; M)$ as the image of
$$\operatorname{Inf}\colon \mathrm{H}^i(\operatorname{Gal}(K^{\mathrm{ur}}/K); M) \to \mathrm{H}^i(\operatorname{Gal}(\overline{K}/K); M).$$

Remark 1.60. By Proposition 1.49, we see that only the unramified cohomology which has a chance of being nonzero is indices 0 and 1.

We are now able to relate our two dualities.

Theorem 1.61. Fix a finite extension K of $\mathbb{Q}_p$. Let M be a discrete Galois module, and suppose further that M is unramified and that $\#M$ is coprime to p. Then M^* is still unramified, and under the duality pairing

$$\mathrm{H}^i(K;M)\times\mathrm{H}^{2-i}(K;M^*)\to\mathbb{Q}/\mathbb{Z},$$

the two subgroups $\mathrm{H}^1_{\mathrm{ur}}(K;M)$ and $\mathrm{H}^1_{\mathrm{ur}}(K;M^*)$ are annihilators of each other.

Proof. One can check directly that $\mathrm{H}^1_{\mathrm{ur}}(K;M)$ and $\mathrm{H}^1_{\mathrm{ur}}(K;M^*)$ annihilate each other because the cup product lands in $\mathrm{H}^2_{\mathrm{ur}}(K;\mathbb{Z}/(\#M)\mathbb{Z})$, which automatically vanishes by Proposition 1.49. Because we have a perfect pairing, it now remains to show that these two groups have the same size.

By Proposition 1.49, we see that $\mathrm{H}^1_{\mathrm{ur}}(K;M)$ is

$$\mathrm{H}^1\left(M\overset{\sigma-1}{\to}M\right)=\operatorname{coker}\left(M\overset{\sigma-1}{\to}M\right).$$

But because M is finite, we see that the size of this cokernel equals the size of this kernel, so we conclude that $\#\mathrm{H}^1_{\mathrm{ur}}(K;M)=\#\mathrm{H}^0_{\mathrm{ur}}(K;M)$, but this is just $\#\mathrm{H}^0(K;M)$ because M is unramified. One similarly deduces that $\#\mathrm{H}^1_{\mathrm{ur}}(K;M^*)=\#\mathrm{H}^0(K;M^*)$, which is $\#\mathrm{H}^2(K;M)$ by Theorem 1.53. We now complete the proof with an Euler characteristic calculation because we know $\chi(M)=1$ by Theorem 1.53. ■

Here is why unramified cohomology will be relevant to our story.

Lemma 1.62. Fix a finite extension K of $\mathbb{Q}_p$, and fix an elliptic curve E of good reduction. Further, choose an integer m coprime to p. Then the image of the map

$$0\to E(K)/mE(K)\to\mathrm{H}^1(K;E[m])$$

coincides with $\mathrm{H}^1_{\mathrm{ur}}(K;E[m])$.

Remark 1.63. The map $E(K)/mE(K)\to\mathrm{H}^1(K;E[m])$ is induced by the "Kummer" exact sequence

$$0\to E[m]\to E\overset{m}{\to}E\to 0.$$

Indeed, taking Galois cohomology produces an exact sequence

$$E(K)\overset{m}{\to}E(K)\to\mathrm{H}^1(K;E[m]).$$

The point of this lemma is that we are interested in $E(K)/mE(K)$, which appears to be some difficult invariant including the rank of E. However, $E[m]$ is just some explicitly computable torsion, so we find that we are actually able to handle $E(K)/mE(K)$ over local fields! For example, it turns out that $E[m](K)$ descends to the residue field in $E[m](k)$, which is contained in $E(k)$.

1.3.2 Selmer Groups

We are now allowed to make the following global definition.

Definition 1.64. Fix a number field K, and fix a finite discrete Galois module M. Furthermore, for each place v of K, choose a subset $\mathcal{L}_v \subseteq \mathrm{H}^1(K_v; M)$, and we require that $\mathcal{L}_v = \mathrm{H}^1_{\mathrm{ur}}(K_v; M)$ for all but finitely many v. Then we define the *Selmer group* with respect to $\mathcal{L}$ to be the pullback in the following square.

$$\begin{tikzcd}
\mathrm{Sel}_{\mathcal{L}}(M) \arrow[r] \arrow[d] \arrow[dr, phantom, "\lrcorner", very near start] & \mathrm{H}^1(K; M) \arrow[d] \\
\prod_v \mathcal{L}_v \arrow[r] & \prod_v \mathrm{H}^1(K_v; M)
\end{tikzcd}$$

The vertical maps are induced by the maps $\mathrm{Gal}(\overline{K_v}/K_v) \to \mathrm{Gal}(\overline{K}/K)$ given restricting an automorphism.

Example 1.65. If E is an elliptic curve over a global field K, we can define $M := E[m]$ and choose $\mathcal{L}_v$ to be the image of the map

$$0 \to E(K_v)/mE(K_v) \to \mathrm{H}^1(K; E[m])$$

for each place v. We may write $\mathrm{Sel}_m(E)$ for $\mathrm{Sel}_{\mathcal{L}}(E[m])$ in this situation.

Remark 1.66. It is undesirable to require that $\mathcal{L}_v = \mathrm{H}^1_{\mathrm{ur}}(K_v; M)$ for all places of v because we do not expect M to be unramified at all v.

Remark 1.67. One expects $\prod_v \mathcal{L}_v$ and $\mathrm{H}^1(K; M)$ to be very large, but they tend to be rather transverse. For example, in the elliptic curve case, the Weil pairing makes $\prod_v \mathrm{H}^1(K_v; E[m])$ into a quadratic space, and it turns out that both of our input spaces are in some sense Lagrangian with respect to this pairing.

Here is our finiteness result.

Theorem 1.68. Fix a number field K, and fix a finite discrete Galois module M. Furthermore, for each place v of K, choose a subset $\mathcal{L}_v \subseteq \mathrm{H}^1(K_v; M)$, and we require that $\mathcal{L}_v = \mathrm{H}^1_{\mathrm{ur}}(K_v; M)$ for all but finitely many v. Then $\mathrm{Sel}_{\mathcal{L}}(M)$ is finite.

Proof. We proceed in steps. The point is to reduce the case to where M has a trivial Galois action, from which we will be able to apply class field theory.

1. We note that making $\mathcal{L}$ larger cannot help us, so we may assume that either $\mathcal{L}_v = \mathrm{H}^1(K_v; M)$ or $\mathcal{L}_v = \mathrm{H}^1_{\mathrm{ur}}(K_v; M)$ for all places v, and we let S to be the finite set in which the former occurs. We also may as well enlarge S so that M is unramified outside S. From now one, we will abbreviate $\mathrm{Sel}_{\mathcal{L}}(M)$ to $\mathrm{Sel}_S(M)$.

2. We reduce to the case where M has the trivial Galois action. Indeed, because M is finite and discrete, the continuity of the action provides a finite extension L of K for which $\mathrm{Gal}(\overline{K}/L)$ acts trivially on M. We now sit in the following diagram.

$$\begin{tikzcd}
 & & \mathrm{Sel}_S(M) \arrow[r] \arrow[d] & \mathrm{Sel}_T\left(\mathrm{Res}^{\mathrm{Gal}(\overline{K}/K)}_{\mathrm{Gal}(\overline{K}/L)} M\right) \arrow[d] \\
0 \arrow[r] & \mathrm{H}^1(\mathrm{Gal}(L/K); M) \arrow[r, "\mathrm{Inf}"] & \mathrm{H}^1(K; M) \arrow[r, "\mathrm{Res}"] & \mathrm{H}^1(L; M)
\end{tikzcd}$$

   Here, T is the collection of primes of L sitting above S. By definition of the Selmer group, the square is a pullback square, and the horizontal line is exact by the Inflation–Restriction exact sequence. Thus, finiteness for the restricted module implies finiteness for $\mathrm{Sel}_S(M)$ because $\mathrm{H}^1(\mathrm{Gal}(L/K); M)$ is finite (as the cohomology group of a finite module over a finite group).

3. It remains to show finiteness when the Galois action is trivial. Because M is a finite abelian group, it is a sum of cyclic groups (with trivial action), so we may assume that M is some cyclic group $\mathbb{Z}/m\mathbb{Z}$. Thus, we see that $\operatorname{Sel}_S(\mathbb{Z}/m\mathbb{Z})$ now embeds into $\mathrm{H}^1(K;\mathbb{Z}/m\mathbb{Z})$, which is the same as

$$\operatorname{Hom}(\operatorname{Gal}(\overline{K}/K),\mathbb{Z}/m\mathbb{Z}).$$

It turns out that a given character χ is unramified at some place $v \in S$ if and only if $\chi|_{I_v} = 1$. Thus, we want to show that there are only finitely many Galois characters which are unramified outside S. For this, we see that χ factors through an extension L of K which is of degree at most m over K and unramified outside S, of which there are only finitely many by the Hermite–Minkowski theorem.[2] ■

1.3.3 An Extended Example

Fix a nonzero integer n and consider the "congruent number" elliptic curve

$$E_n \colon y^2 = x(x-n)(x+n).$$

One can show by some rearrangement that E_n is a quadratic twist of the elliptic curve $y^2 = x^3 - x$. One can show that $E(\mathbb{Q})_{\text{tors}} = E[2]$, which is precisely the set

$$E_n[2] = \{\infty, (0,0), (n,0), (-n,0)\}.$$

We are going to prove the following.

Theorem 1.69. We have

$$\dim_{\mathbb{F}_2} \operatorname{Sel}_2(E_p) = 2 + \begin{cases} 0 & \text{if } p \equiv 1,3 \pmod 8, \\ 1 & \text{if } p \equiv 5,7 \pmod 8. \end{cases}$$

Example 1.70. For any elliptic curve E over $\mathbb{Q}$, one has

$$\dim_{\mathbb{F}_2} \operatorname{Sel}_2(E) = \dim_{\mathbb{F}_2} E[2](\overline{\mathbb{Q}}) + \operatorname{rank} E(\mathbb{Q}) + \dim_{\mathbb{F}_2} Ш(E)[2].$$

Thus, one sees that $p \equiv 1,3 \pmod 8$ must have rank 0 and trivial $Ш(E)[2]$. If $Ш$ is finite, then the fact that it should be square further implies that the rank is 1 and $Ш(E)[2]$ is trivial.

Let's spend some time setting up the calculation. We work with a general elliptic curve E over a number field K. Because $E[2]$ is defined over K, the Galois action is trivial. Thus, we see that $\mathrm{H}^1(K;E[2])$ is simply $\mathrm{H}^1(K;\mu_2)^2$, and we can compute this cohomology using the "Kummer" exact sequence

$$1 \to \mu_2 \to \overline{K}^\times \overset{2}{\to} \overline{K}^\times \to 1,$$

which in Galois cohomology produces an isomorphism $\mathrm{H}^1(K;\mu_2) \cong K^\times/K^{\times 2}$ by Hilbert's theorem 90. We may now identify $\mathrm{H}^1(K;E[2])$ with

$$\left\{(\alpha,\beta,\gamma) \in (K^\times/K^{\times 2})^3 : \alpha\beta\gamma = 1\right\}.$$

It turns out that this map (approximately) sends some point (x,y) of $E(K)/2E(K)$ to the triple $(x-a_1, x-a_2, x-a_3)$ when E has the form $y^2 = (x-a_1)(x-a_2)(x-a_3)$. Technically speaking, we should note that we send ∞ to the identity $(1,1,1)$, and we send any two-torsion point like $(a_1,0)$ to the triple whose last two coordinates are $a_1 - a_2$ and $a_3 - a_2$.

Of course, we would like a way to know if an interesting triple (α,β,γ) is in the image without having to find points in $E(K)$ first. Here is one such test.

[2] Technically speaking, Hermite–Minkowski only bounds the number of fields with bounded discriminant, but the discriminant is supported in S and the primes have exponent bounded by the degree.

Lemma 1.71. Fix an elliptic curve $E\colon y^2 = (x-a_1)(x-a_2)(x-a_3)$ over a finite extension K of $\mathbb{Q}_p$. Then a triple (α, β, γ) lies in the image of the above map if and only if the system of equations

$$\begin{cases} \alpha u^2 = x - a_1, \\ \beta v^2 = x - a_2, \\ \gamma w^2 = x - a_3 \end{cases}$$

admits a solution.

BIBLIOGRAPHY

[Shu16] Neal Shusterman. *Scythe*. Arc of a Scythe. Simon & Schuster, 2016.

List of Definitions