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* $\text{Ш}(E/k)$ as the kernel

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

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 $\text{Ш}(E/k)$ 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 $Ш(E/\mathbb{Q})$.

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 $Ш(E/k)$ is finite.

Remark 1.14. When trying to prove this conjecture, one frequently just wants to know $Ш(E/k)[p^\infty]$ is finite for all primes p. (Of course, one also wants to know that $Ш(E/k)$ vanishes for primes p large enough.) It is often possible to verify that $Ш(E/k)[p^\infty]$ is finite for a given prime p, but it is difficult to actually show that $Ш(E/k)$ is then finite! One does not even know if the dimensions $\dim_{\mathbb{F}_p} Ш(E/k)[p]$ 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 $r_{\mathrm{an}}(E)\le 1$, then $r_{\mathrm{an}}=\operatorname{rank} E(\mathbb{Q})$ and $\#Ш(E/\mathbb{Q})<\infty$.

This theorem is more or less the only way one can know that $Ш(E/k)$ is finite. In particular, we do not have a single example of an elliptic curve E with analytic rank at least 2 and $Ш(E/k)$ 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 $Ш(E/\mathbb{Q})[p]\ne 0$?

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 $\mathrm{Sel}_m(E)$ are indexed by integers $m\in\mathbb{Z}$ and sit in a short exact sequence

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

For example, it follows that

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

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, $\mathrm{Sel}_2(E)$ 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

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

[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, $\mathrm{Sel}_{2^\infty}\left(E^{(d)}/\mathbb{Q}\right)$ 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

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

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 $(\cdot)^G \colon \mathrm{Mod}_{\mathbb{Z}[G]} \to \mathrm{Ab}$. 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

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

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

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

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.

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

1.2 September 16

Welcome to the second class of the semester. The note-taker is furiously eating lunch. For today's class, we will review group cohomology, but we will freely assume standard facts about derived functors in order to not be bogged down in commutative algebra.

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 $(-)^G \colon \operatorname{Mod}_{\mathbb{Z}[G]} \to \operatorname{Ab}$ 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

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

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 $(-)^G \colon \operatorname{Mod}_{\mathbb{Z}[G]} \to \operatorname{Ab}$.

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

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

Remark 1.29. It is worthwhile to remember that we actually expect the groups $\mathrm{H}^\bullet(G; M)$ to exhibit two kinds of functoriality: there is a functoriality in M, and if we have a group homomorphism $G' \to G$, then we expect the induced "forgetful" functor $\operatorname{Mod}_G \to \operatorname{Mod}_{G'}$ to also induce a natural transformation $\mathrm{H}^\bullet(G; -) \to \mathrm{H}^\bullet(G'; -)$. Such a map will be made explicit shortly in Remark 1.31.

1.2.2 Tools for 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 $\operatorname{Hom}_{\mathbb{Z}[G]}(-, M)$, and take cohomology.

The second is easier for the purposes of calculation.

Example 1.30. 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

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

Remark 1.31. This construction of group cohomology even has good functoriality properties: given a group homomorphism $g \colon G' \to G$ and a morphism $f \colon M \to M'$ of abelian groups for which M is a G-module and M' has the induced G'-module structure, we get an induced map of the associated complexes $\mathcal{P}(G')_\bullet \to \mathcal{P}(G)_\bullet$ (of Example 1.30) and thus of the complexes $\mathrm{Hom}_G(\mathcal{P}(G)_\bullet, M) \to \mathrm{Hom}_{G'}(\mathcal{P}(G')_\bullet, M')$ and thus of cohomology groups

$$\mathrm{H}^i(\mathrm{Hom}_{G'}(\mathcal{P}(G')_\bullet, M')) \to \mathrm{H}^i(\mathrm{Hom}_G(\mathcal{P}(G)_\bullet, M)).$$

On cocycles, we can see that this map sends the class of some cocycle $c \colon \mathbb{Z}[G^n] \to M$ to the class of the induced composite $\mathbb{Z}[(G')^n] \to \mathbb{Z}[G^n] \to M \to M'$.

Remark 1.32. If G is finite and M is finite, then a direct calculation of the cohomology via the resolution in Example 1.30 implies that $\mathrm{H}^i(G; M)$ is finite in all degrees.

While the combinatorics in Example 1.30 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 1.33 (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 1.34 (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."

Lemma 1.35. Fix a group G and a G-module M. Then $\mathrm{H}^1(G;M)$ is isomorphic to the group of crossed homomorphisms modulo the subgroup of principal crossed homomorphisms.

Proof. We use Example 1.30, which splits the calculation as follows.

- We claim that the group of 1-cocycles of M is isomorphic to the group of crossed homomorphisms. Indeed, a 1-cocycle is simply an element in the kernel of the map
$$\operatorname{Hom}_G\left(\mathbb{Z}\left[G^2\right], M\right) \stackrel{d_3}{\to} \operatorname{Hom}_G\left(\mathbb{Z}\left[G^3\right], M\right).$$
In other words, by considering $\mathbb{Z}$-linear extensions, we are looking at a map $c\colon G^2 \to M$ such that $c(gx_1, gx_2) = gc(x_1, x_2)$ and for which $d_3c(g_0, g_1, g_2) = 0$ always, which amounts to the condition
$$c(g_1, g_2) - c(g_0, g_2) + c(g_0, g_1) = 0$$
for all $g_0, g_1, g_2 \in G$. Now, the condition $c(gx_1, gx_2) = gc(x_1, x_2)$ implies that c is uniquely determined by its restriction $f\colon G \to M$ given by $f(g) := c(e, g)$; indeed, then $c(g_1, g_2) = g_1 f\left(g_1^{-1} g_2\right)$. Then the condition that c is a 1-cocycle is translates into the condition
$$g_1 f\left(g_1^{-1} g_2\right) + g_0 f\left(g_0^{-1} g_1\right) = g_0 f\left(g_0^{-1} g_2\right)$$
for all $g_0, g_1, g_2 \in G$. By dividing out by g_0 and setting $g := g_0^{-1} g_1$ and $h := g_1^{-1} g_2$, this condition becomes equivalent to
$$f(gh) = gf(h) + f(g)$$
for all $g, h \in G$. Thus, we see that the map taking a 1-cocyle c of M to the map $f\colon G \to M$ given by $f(g) := c(e, g)$ is a bijection, and one can see that is $\mathbb{Z}$-linear, so it is an isomorphism.
- We claim that the subgroup of 1-coboundaries of M is isomorphic to the subgroup of principal crossed homomorphisms. Indeed, a 1-coboundary is simply an element in the image of the map
$$\operatorname{Hom}_G\left(\mathbb{Z}\left[G\right], M\right) \stackrel{d_2}{\to} \operatorname{Hom}_G\left(\mathbb{Z}\left[G^2\right], M\right).$$
A G-linear map $b\colon \mathbb{Z}[G] \to M$ amounts to the data of a single element $b(1) \in M$, so we will identify the left group with M. Then the corresponding 1-coboundary is defined by
$$d_2 b(g_0, g_1) = g_0 b - g_1 b.$$
The algorithm described in the previous point translates this into the crossed homomorphism $f\colon G \to M$ defined by $f(g) = b(e, g) = (1-g)b$, which is a principal crossed homomorphism. This mapping is now seen to be bijective and $\mathbb{Z}$-linear, so the result follows. ■

Remark 1.36. This "restriction" map taking a 1-cocycle to a crossed homomorphism has all the functoriality one could ask for: for a homomorphism $g\colon G' \to G$ and a morphism $f\colon M \to M'$ of abelian groups, we can compute that the functoriality map of Remark 1.31 sends a crossed homomorphism $G \to M$ to the composite $G' \to G \to M \to M'$. Indeed, this is just a matter of appropriately restricting everywhere.

Example 1.37. 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 1.30.

Proposition 1.38. Fix a finite cyclic group G generated by σ. 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 $\mathrm{N}_G(x) := \sum_{g\in G} gx$; equivalently, we can view N_G as multiplication by the norm element $\mathrm{N}_G := \sum_{g\in G} g$. Because we are back at $\mathbb{Z}$, we see that we can iterate to produce a resolution

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

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

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

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. ■

Remark 1.39. The result Proposition 1.38 has rather poor functoriality properties. Fix cyclic groups $G = \langle\sigma\rangle$ and $G' = \langle\sigma'\rangle$, and suppose we have a surjection $g\colon G' \to G$, which up to changing generators must be given by $g(\sigma') = \sigma$. Set $m := \#G'/\#G$ for brevity. Now, the identities $g(\sigma'-1) = (\sigma-1)$ and $g(\mathrm{N}_{G'}) = m\,\mathrm{N}_G$ produce the morphism

$$\begin{tikzcd} \cdots \arrow[r] & \mathbb{Z}[G'] \arrow[r, "\mathrm{N}_{G'}"] \arrow[d, "m^2 g"] & \mathbb{Z}[G'] \arrow[r, "(\sigma'-1)"] \arrow[d, "mg"] & \mathbb{Z}[G'] \arrow[r, "\mathrm{N}_{G'}"] \arrow[d, "mg"] & \mathbb{Z}[G'] \arrow[r, "(\sigma'-1)"] \arrow[d, "g"] & \mathbb{Z}[G'] \arrow[r, "\deg"] \arrow[d, "g"] & \mathbb{Z} \arrow[r] \arrow[d, equal] & 0 \\ \cdots \arrow[r] & \mathbb{Z}[G] \arrow[r, "\mathrm{N}_G"'] & \mathbb{Z}[G] \arrow[r, "(\sigma-1)"'] & \mathbb{Z}[G] \arrow[r, "\mathrm{N}_G"'] & \mathbb{Z}[G] \arrow[r, "(\sigma-1)"'] & \mathbb{Z}[G] \arrow[r, "\deg"'] & \mathbb{Z} \arrow[r] & 0 \end{tikzcd}$$

of chain complexes. Now, given a morphism $f\colon M \to M'$ where M is a G-module, and M' has the induced G'-module structure, we may apply $\operatorname{Hom}_G(-,M)$ and $\operatorname{Hom}_{G'}(-,M')$ to get another morphism of chain complexes induced by f and the above morphism. It follows that the induced map $\mathrm{H}^i(G;M) \to \mathrm{H}^i(G';M')$ is given by $m^{\lfloor i/2\rfloor}f$ by a computation on the corresponding cocycles.

1.2.3 Change of Group

We will get some utility out of having more functors.

Definition 1.40 (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

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

Remark 1.41. A function $f\colon G\to N$ has equivalent data to a homomorphism $f\colon \mathbb{Z}[G]\to N$ of abelian groups by extending $\mathbb{Z}$-linearly. The condition that $f(hx)=hf(x)$ then amounts to requiring that the map $\mathbb{Z}[G]\to N$ is $\mathbb{Z}[H]$-linear. Thus, we see that $\operatorname{Ind}_H^G N$ is bijection with $\operatorname{Hom}_{\mathbb{Z}[H]}(\mathbb{Z}[G],N)$, and one can see that this bijection is $\mathbb{Z}[G]$-linear and natural in N.

With an induction, we also have a restriction.

Definition 1.42 (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.

Here are the results on induction and restriction.

Proposition 1.43 (Frobenius reciprocity)**.** Fix a finite-index subgroup H of a 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.

Sketch. This reduces to the $\otimes$-Hom adjunction, for both claims. ∎

Remark 1.44. 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.

Proposition 1.45 (Shapiro's lemma)**.** Fix a subgroup H of a finite group G. Then there is a natural isomorphism

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

Sketch. Fix an H-module N. Then $\mathrm{H}^i(H;N)$ is computed by taking $(-)^H$ on an injective resolution of N and then calculating cohomology. Alternatively, one can apply the exact functor Ind_H^G to this injective resolution to produce an injective resolution of $\operatorname{Ind}_H^G N$ and then take $(-)^G$ to compute the cohomology $\mathrm{H}^i\left(G;\operatorname{Ind}_H^G N\right)$. One then checks that these produce the same answer. ∎

It turns out that restriction has a sort of dual.

Definition 1.46 (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 1.47. It turns out that the composite

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

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 1.48 (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 $\mathrm{Mod}_{G/H}\to\mathrm{Mod}_G$ 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 1.49 (Inflation–restriction)**.** Fix a G-module M. Then there is an exact sequence

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

Sketch. One can explicitly compute this on the level of 1-cocycles. ■

1.2.4 Profinite Cohomology

We quickly explain how to take cohomology for profinite groups.

Example 1.50. Fix a finite field k with q elements. Then $\mathrm{Gal}(\overline{k}/k)$ is a profinite group with topological generator given by the Frobenius. Explicitly,

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

Definition 1.51 (discrete)**.** Fix a profinite group G. Then a G-module M is *discrete* if and only if the stabilizer $\mathrm{Stab}_G(m)$ is open for all $m\in M$.

Remark 1.52. 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 $\mathrm{Stab}_G(m)\times\{m\}$.

Definition 1.53 (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

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

Here, we are taking the colimit of the maps $\mathrm{H}^i\left(G/H;M^H\right)\to\mathrm{H}^i\left(G/H';M^{H'}\right)$ produced whenever $H'\subseteq H$ via Remark 1.31, in which case we have a surjection $G/H'\twoheadrightarrow G/H$ and an inclusion $M^H\hookrightarrow M^{H'}$. We will frequently write $\mathrm{H}^i(G;M)$ for $\mathrm{H}^i_{\text{cts}}(G;M)$ whenever G is profinite. In particular, we will never use ordinary group cohomology for profinite groups G.

Remark 1.54. Equivalently, following Example 1.30, we can define $\mathrm{H}^i_{\text{cts}}(G;M)$ as

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

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 1.55. Fix a procyclic group G isomorphic to $\widehat{\mathbb{Z}}$ with generator σ. Fix a finite discrete G-module M. Then

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

Proof. Set $H_m:=\overline{\langle\sigma^m\rangle}$ for brevity, which we note is the kernel of the map $G\to\mathbb{Z}/m\mathbb{Z}$ defined by $\sigma\mapsto 1$, so H_m is a closed and normal subgroup of finite index, so H_m is also open because G is compact. In fact, every open normal subgroup $H\subseteq G$ takes this form: being open, we see that H is finite index because G is compact, and being normal, we see that H must be then be the kernel of some map $G\to A$ where A is a finite group. Replacing A with the (cyclic!) image of G, we may find an $m\geq 1$ for which $A=\mathbb{Z}/m\mathbb{Z}$ where $\sigma\in G$ is sent to 1, so we see that $H=H_m$.

Now, by plugging in the definitions, we see that

$$\mathrm{H}^i(G;M)=\operatorname*{colim}_{m\geq 1}\mathrm{H}^i\left(G/H_m;M^{\sigma^m}\right),$$

where $M^{\sigma^m}=M^{\overline{\langle\sigma^m\rangle}}$ by continuity. We now see that we have to use Remark 1.39 to compute the internal maps. Setting $M_m:=M^{\sigma^m}$ for brevity, Remark 1.39 tells us that the inclusion $H_{m'}\subseteq H_m$ (which exists whenever $m\mid m'$) induces a map

$$\mathrm{H}^i\left(G/H_m;M_m\right)\to\mathrm{H}^i\left(G/H_{m'};M_{m'}\right)$$

given by $(m'/m)^{\lfloor i/2\rfloor}$ times the natural inclusion. For example, we see that $i\geq 2$ allows us to make this map zero simply by making m'/m divisible by $\#M$, so we conclude that the entire colimit $\mathrm{H}^i(G;M)$ vanishes.

However, for $i\in\{0,1\}$, we see that these maps are given by the natural inclusions. Because M is finite and discrete, there is an open normal subgroup $H\subseteq G$ fixing M, so as soon as H_m is small enough to be contained in H (say, if $H=H_n$, then this happens as soon as $n\mid m$), we find that

$$\mathrm{H}^i(G/H_m;M_m)=\mathrm{H}^i(G/H_m;M)=\begin{cases}M^\sigma & \text{if } i=0,\\ \ker \mathrm{N}_{G/H_m}|_M/(\sigma-1)M & \text{if } i=1,\end{cases}$$

where the last equality follows from Proposition 1.38. Additionally, once m is sufficiently divisible, the calculations of Remark 1.39 show that N_{G/H_m} will multiply by a large scalar, so all M will be in the kernel (e.g., this should happen as soon as $n\cdot\#M\mid m$ so that N_{G/H_m} has a factor of $\#M$). The natural inclusions in our colimit are now identities on these modules, so it follows that $\mathrm{H}^i(G;M)$ is given as claimed. ∎

Remark 1.56. 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 1.57. Fix a field k and a commutative group scheme X over k. Then we set the notation

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

For any Galois extension L of k, we may also write $\mathrm{H}^i(L/k;X):=\mathrm{H}^i(\mathrm{Gal}(L/k);X(L))$.

Remark 1.58. Open normal subgroups of $\mathrm{Gal}(k^{\mathrm{sep}}/k)$ are in bijection with finite Galois extensions L of k by (infinite) Galois theory, so

$$\mathrm{H}^i(k;X)=\operatorname*{colim}_{\text{finite, Galois } L\supseteq k}\mathrm{H}^i\left(\mathrm{Gal}(L/k);\mathrm{H}^0(L;X_L\right).$$

Example 1.59. If X is quasiprojective, then we have an embedding $X \hookrightarrow \mathbb{P}_k^n$ for some $n \geq 0$, so we have a Galois-invariant map $X(k^{\mathrm{sep}}) \subseteq \mathbb{P}^n(k^{\mathrm{sep}})$. Taking Galois invariants on the right simply produces $\mathbb{P}^n(k)$, so we find that $\mathrm{H}^0(k, X) = X(k)$.

Example 1.60. Fix a finite field k. From Proposition 1.55, we see that $\mathrm{H}^i(k; M) = 0$ for $i \geq 2$ for any finite discrete $\mathrm{Gal}(\overline{k}/k)$-module M.

Example 1.61. If M has the trivial action, then Example 1.37 induces a commutative square

$$\begin{tikzcd}
\mathrm{H}^1\left(G/H; M\right) \arrow[r] \arrow[d] & \mathrm{Hom}\left(G/H, M\right) \arrow[d] \\
\mathrm{H}^1\left(G/H'; M\right) \arrow[r] & \mathrm{Hom}\left(G/H', M\right)
\end{tikzcd}$$

for any inclusion $H' \subseteq H$ of open normal subgroups. Taking the colimit reveals that $\mathrm{H}^1(G; M) = \mathrm{Hom}_{\mathrm{cts}}(G, M)$.

1.3 September 18

Today, we will continue to review Galois cohomology.

1.3.1 Local Duality

Akin to Proposition 1.55, we have the following duality statement for local fields.

Theorem 1.62 (Tate)**.** Fix a finite extension K of $\mathbb{Q}_p$, set $G := \mathrm{Gal}(\overline{K}/K)$ 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 $M^* := \mathrm{Hom}_{\mathbb{Z}}(M, \mu_\infty(\overline{K}))$. 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 1.63. 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 1.64. 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 1.65. It is possible to check Theorem 1.62 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 1.66 (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 $\mathrm{Gal}(\overline{K}/K)$ to fit in the short exact sequence

$$1 \to I_K \subseteq \mathrm{Gal}(\overline{K}/K) \to \mathrm{Gal}(\overline{k}/k) \to 1.$$

Remark 1.67. Let K^{ur} be the maximal unramified extension of K. Then we see that $\mathrm{Gal}(K^{\mathrm{ur}}/K)$ is simply $\mathrm{Gal}(\overline{K}/K)/I_K$, which is $\mathrm{Gal}(\overline{k}/k)$.

Definition 1.68 (unramified)**.** Fix a local field K. Then a $\mathrm{Gal}(\overline{K}/K)$-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

$$\mathrm{Inf}\colon \mathrm{H}^i(\mathrm{Gal}(K^{\mathrm{ur}}/K);M) \to \mathrm{H}^i(\mathrm{Gal}(\overline{K}/K);M).$$

Remark 1.69. By Proposition 1.55 (which applies by Remark 1.67), we see that only the unramified cohomology which has a chance of being nonzero is indices 0 and 1.

Example 1.70. Suppose that M is a trivial Galois module, and consider the commutative diagram

$$\begin{tikzcd}
\mathrm{H}^1\left(\mathrm{Gal}(K^{\mathrm{ur}}/K);M\right) \arrow[r] \arrow[d] & \mathrm{Hom}\left(\mathrm{Gal}(K^{\mathrm{ur}}/K),M\right) \arrow[d] \\
\mathrm{H}^1\left(\mathrm{Gal}(K^{\mathrm{sep}}/K);M\right) \arrow[r] & \mathrm{Hom}\left(\mathrm{Gal}(K^{\mathrm{sep}}/K),M\right)
\end{tikzcd}$$

induced by the commutative squares of Example 1.61. In particular, the rightward map is induced by the quotient $\mathrm{Gal}(K^{\mathrm{sep}}/K) \twoheadrightarrow \mathrm{Gal}(K^{\mathrm{ur}}/K)$. Thus, an element $\chi \in \mathrm{H}^1(K;M)$ viewed as a Galois character is unramified if and only if it factors through $\mathrm{Gal}(K^{\mathrm{ur}}/K)$, which is equivalent to vanishing on the (closed) inertia subgroup I_K.

We are now able to relate our two dualities.

Theorem 1.71. 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 1.55. Because we have a perfect pairing, it now remains to show that these two groups have the same size.

By Proposition 1.55, 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 1.62. We now complete the proof with an Euler characteristic calculation because we know $\chi(M) = 1$ by Theorem 1.62. ■

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

Lemma 1.72. Fix a finite extension K of $\mathbb{Q}_p$, and fix an elliptic curve E of good reduction. For any positive integer m coprime to p, the image of the map

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

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

Sketch. The given map is induced from the long exact sequence of the map

$$0 \to E[m](\overline{K}) \to E(\overline{K}) \overset{m}{\to} E(\overline{K}) \to 0$$

by taking Galois invariants. Indeed, the long exact sequence includes the maps

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

Now, to show the claim, we note that there is a morphism

$$\begin{tikzcd} 0 \arrow[r] & E[m](K^{\mathrm{unr}}) \arrow[r] \arrow[d, hook] & E(K^{\mathrm{unr}}) \arrow[r] \arrow[d, hook] & E(K^{\mathrm{unr}}) \arrow[r] \arrow[d, hook] & 0 \\ 0 \arrow[r] & E[m](\overline{K}) \arrow[r] & E(\overline{K}) \arrow[r] & E(\overline{K}) \arrow[r] & 0 \end{tikzcd}$$

of short exact sequences. Because E has good reduction over $\mathbb{Q}_p$ and $p \nmid m$, it follows that the left map is actually surjective and hence the identity. Now, taking Galois invariants shows that the square

$$\begin{tikzcd} E(K)/mE(K) \arrow[r] \arrow[d, equal] & \mathrm{H}^1(K^{\mathrm{unr}}/K; E[m]) \arrow[d] \\ E(K)/mE(K) \arrow[r] & \mathrm{H}^1(\overline{K}/K; E[m]) \end{tikzcd}$$

commutes. Now, $\mathrm{H}^1_{\mathrm{ur}}(K; E[m])$ is the image of the right vertical map by definition, so it is enough to show that the top horizontal map is surjective. This amounts to noting that the next term $\mathrm{H}^1(K^{\mathrm{unr}}/K; E)$ vanishes: indeed, it is the colimit of the Galois cohomology groups $\mathrm{H}^1(L/K; E)$ where L/K is finite and unramified, but this group is trivial because $E(L)$ is divisible for all finite extensions L of $\mathbb{Q}_p$. ■

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 1.73. 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.

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

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 1.74. 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 1.75. 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 1.76. One expects $\prod_v \mathcal{L}_v$ and $\mathrm{H}^1(K; M)$ to be very large, but they tend to be rather transverse in $\prod_v \mathrm{H}^1(K_v; M)$. 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 $\prod_v \mathcal{L}_v$ is isotropic (by Theorem 1.62), and the image of $\mathrm{H}^1(K; E[m])$ is isotropic by some global duality.

Remark 1.77. While the map $\prod_v \mathcal{L}_v \to \prod_v \mathrm{H}^1(K_v; M)$ is certainly injective, the vertical map is not always expected to be. In short, it is injective in the case $E[p]$ when p is prime by combining the Chebotarev density theorem and the fact that p-Sylow subgroups of $\mathrm{GL}(E[p])$ are cyclic [PR12, Theorem 4.16]. However, it will frequently fail to be injective outside this case due to Ш problems.

Here is our finiteness result.

Theorem 1.78. 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 start by noting that we have two legal reductions: we are allowed to make $\mathcal{L}$ and K larger.

- 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. For example, S includes the places where M is ramified. From now on, we will abbreviate $\mathrm{Sel}_{\mathcal{L}}(M)$ to $\mathrm{Sel}_S(M)$. As noted previously with $\mathcal{L}$, we remark that we may enlarge S, and it will not make the problem any easier.
- We show that we may reduce the question to any finite extension K' of K. For this, we let M' be the module M with the restricted Galois action, and we let S' be the set of primes of K' lying over a prime

of S. We then draw the following diagram.

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

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 $\mathrm{H}^1(\mathrm{Gal}(K'/K);M)$ is finite (as the cohomology group of a finite module over a finite group).

We now complete the proof. To start, we remark that we may extend K to an extension in which M has the trivial Galois action. Indeed, because M is finite and discrete, the continuity of the action provides a finite extension K' of K for which $\mathrm{Gal}(\overline{K}/K')$ acts trivially on M.

Now, it remains to show finiteness when the Galois action is trivial and where the ground field is large. 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 $\mathrm{Sel}_S(\mathbb{Z}/m\mathbb{Z})$ now embeds into $\mathrm{H}^1(K;\mathbb{Z}/m\mathbb{Z})$, which is the same as

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

By Example 1.70, we see that a given character χ represents an unramified class 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. Indeed, the discriminant of L over $\mathbb{Q}$ is finitely supported (inside S and whatever primes of $\mathbb{Q}$ ramify in K), and the exponents of these primes are also upper-bounded because the order of a prime p dividing the discriminant is upper-bounded as a function of the ramification index,[2] which is upper-bounded by the degree. ■

Remark 1.79. Here is another way to conclude at the end, which uses Kummer theory. For technical reasons, we extend K to be Galois over $\mathbb{Q}$, and we go ahead and enlarge S to be Galois-invariant and include the primes dividing m; let $S_\mathbb{Q}$ be the corresponding primes in $\mathbb{Q}$ lying under a prime in S.

Note that any such Galois character χ factors through $\mathrm{Gal}(L/k)$ where L is finite abelian over k of exponent dividing m and unramified outside S. Thus, it is enough to show that there are only finitely many such fields L. But Kummer theory (via Theorem A.8) tells us that abelian extensions L/k of exponent dividing m are in bijection with subgroups $B\subseteq K^\times/K^{\times m}$. To check that L is unramified outside S translates, Remark A.9 explains that we may check that B is generated by elements whose norms are supported in $S_\mathbb{Q}$. Thus, the prime factorizations of the generators of B are limited in exponent (by m) and support (by S) and unit (because $\mathcal{O}_K^\times/\mathcal{O}_K^{\times m}$ is finite), so there are only finitely many available subgroups B, and we are done.

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 $E(\mathbb{Q})_{\mathrm{tors}}=E[2]$, which is precisely the set

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

We are going to prove the following.

[2] This follows from the theory of higher ramification groups.

Theorem 1.80. We have

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

Example 1.81. For any elliptic curve E over $\mathbb{Q}$, one has

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

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

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

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.

Lemma 1.82. 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.

Appendix A
Galois Cohomology

In this chapter, we run through some recollections of Galois cohomology which did not appear in class.

A.1 Hilbert's Theorem 90

Hilbert's theorem 90 is a tool frequently used in order to get Kummer theory off of the ground. We will require the following algebraic input.

Proposition A.1 (Dedekind)**.** Fix a group G and a field k and some distinct characters $\chi_1, \ldots, \chi_n \colon G \to k^\times$. Then the characters $\{\chi_1, \ldots, \chi_n\}$ are linearly independent.

Proof. This proof is tricky. Suppose for the sake of contradiction that there is a nonempty set $\{\chi_1, \ldots, \chi_n\}$ of distinct characters $k^\times \to A$ which fails to be linearly independent. We may as well assume that n is as small as possible; we will derive contradiction by showing that some strict subset of these characters continues to not be linearly independent.

Now, we are given a relation

$$a_1\chi_1 + a_2\chi_2 + \cdots + a_n\chi_n = 0$$

for some $a_1, \ldots, a_n \in k$; the minimality of our set of characters implies that all these coefficients are nonzero. The point is that there are two ways to produce a new relation.

- On one hand, we can multiply this entire relation by some $a \in k^\times$ to produce the relation

$$aa_1\chi_1 + aa_2\chi_2 + \cdots + aa_n\chi_n = 0.$$

- On the other hand, we note that any $g, h \in G$ has

$$a_1\chi_1(g)\chi_1(h) + a_2\chi_2(g)\chi_2(h) + \cdots + a_n\chi_n(g)\chi_n(h) = 0$$

  because the $\chi_\bullet$s are multiplicative. Thus, for any $g \in G$, we produce a new relation

$$a_1\chi_1(g)\chi_1 + a_2\chi_2(g)\chi_2 + \cdots + a_n\chi_n(g)\chi_n = 0.$$

To complete the proof, we play these two relations against each other. Our characters are all distinct, so we may find some $g \in G$ for which $\chi_1(g) \neq \chi_2(g)$. Now, subtracting the relations

$$a_1\chi_1(g)\chi_1 + a_2\chi_1(g)\chi_2 + \cdots + a_n\chi_1(g)\chi_n = 0$$

and

$$a_1\chi_1(g)\chi_1 + a_2\chi_2(g)\chi_2 + \cdots + a_n\chi_n(g)\chi_n = 0$$

produces the relation

$$a_1(\chi_1(g) - \chi_2(g))\chi_2 + \cdots + a_n(\chi_1(g) - \chi_n(g))\chi_n = 0.$$

This is a nonzero relation because $a_1(\chi_1(g) - \chi_2(g)) \neq 0$, so we conclude that the characters $\{\chi_2, \ldots, \chi_n\}$ fail to be linearly independent, which is our desired contradiction. ■

Theorem A.2 (Hilbert 90)**.** Fix a field k.

(a) For any finite Galois extension L of k, we have $\mathrm{H}^1(L/k, \mathbb{G}_m) = 0$.

(b) We have $\mathrm{H}^1(k, \mathbb{G}_m) = 0$.

Proof. Note that (a) implies (b) by taking the colimit over all L via Remark 1.58 (where we are silently using Example 1.59). It remains to show (a), for which we use Lemma 1.35.

Set $G := \mathrm{Gal}(L/k)$, and we fix a crossed homomorphism $f\colon G \to L^\times$, which we want to show is actually principal. Well, we are given that $f(gh) = f(g)\cdot g(f(h))$ for any $g, h \in G$. We are on the hunt for some $b \in L^\times$ for which $f(g) = g(b)/b$ for all $g \in G$; provided that b is nonzero, this is equivalent to $g(b) = f(g)^{-1}b$, so b is more or less an eigenvector for the G-action with eigenvalue given by f^{-1}. Thus, a natural candidate would be to take some $a \in L$ and produce the "average" of the G-action defined by

$$b := \sum_{g\in G} f(g)g(a).$$

Indeed, for any $h \in G$, we see that $h(b)$ is

$$\sum_{g\in G} hf(g)hg(a) = \frac{1}{f(h)}\sum_{g\in G} f(hg)hg(a) = \frac{1}{f(h)}\sum_{g\in G} f(g)g,$$

so $h(b) = f(h)^{-1}b$. It remains to see that we can find some $a \in L$ for which the resulting b is nonzero, which follows from Proposition A.1. ■

Here are a couple applications.

Corollary A.3. Fix a cyclic extension L/k where $\mathrm{Gal}(L/k)$ has generator σ. For $\alpha \in L^\times$, if $\mathrm{N}_{L/k}(\alpha) = 1$, then there is β such that $\alpha = \sigma(\beta)/\beta$.

Proof. By Proposition 1.38, we see that

$$\mathrm{H}^1(L/k, L^\times) = \frac{\ker\left(\mathrm{N}\colon L^\times \to K^\times\right)}{\mathrm{im}\left((\sigma-1)\colon L^\times \to L^\times\right)},$$

so the result follows by Theorem A.2. ■

Example A.4. Fix a base field k and a positive integer m not divisible by $\operatorname{char} k$. Consider the finite commutative group scheme $\mu_m \subseteq \mathbb{G}_m$ given by the mth roots of unity. Then the long exact sequence of Galois modules

$$1 \to \mu_m(k^{\mathrm{sep}}) \to k^{\mathrm{sep}\times} \stackrel{m}{\to} k^{\mathrm{sep}\times} \to 1$$

induces an exact sequence

$$k^\times \stackrel{m}{\to} k^\times \to \mathrm{H}^1(k; \mu_m) \to \mathrm{H}^1(k; \mathbb{G}_m).$$

But the last term vanishes by Theorem A.2, so we conclude that $\mathrm{H}^1(k; \mu_m) \cong k^\times/k^{\times m}$.

A.2 Kummer Theory

Kummer theory classifies abelian extensions a given field k of exponent m, provided that $\mu_m \subseteq k^\times$ and $\operatorname{char} k \nmid m$. Let's start with the most basic case.

Lemma A.5. Fix a field k and a positive integer m such that $\mu_m \subseteq k$ and $\operatorname{char} k \nmid m$. For any cyclic extension K/k of degree m, there is $\alpha \in K$ such that $K = k(\alpha)$ and $\alpha^m \in k$.

Proof. Choose a generator σ of $\operatorname{Gal}(K/k)$. We use Theorem A.2 to construct the needed α. Well, choose a generator ζ of μ_m, and then $\zeta \in k$ implies that $\mathrm{N}_{K/k}(\zeta) = \zeta^m = 1$. Thus, there is $\alpha \in K$ such that $\zeta = \sigma(\alpha)/\alpha$, so $\sigma(\alpha) = \zeta\alpha$, and a quick induction shows that $\sigma^i(\alpha) = \zeta^i\alpha$ for all i. Thus, α has m distinct Galois conjugates, so $k(\alpha)$ is a degree m extension of k, so $k(\alpha) = K$ follows for degree reasons. Lastly, we should check that $\alpha^m \in k$, which follows because

$$\sigma^i\left(\alpha^m\right) = \zeta^{mi}\alpha^m = \alpha^m$$

for all σ^i. ■

For our main result, we should define a "Kummer pairing."

Definition A.6 (Kummer pairing)**.** Fix a field k and a positive integer m such that $\operatorname{char} k \nmid m$ and $\mu_m \subseteq k$. Then we define the *Kummer pairing*

$$\langle -, - \rangle \colon \operatorname{Gal}(k^{\text{sep}}/k) \times k^\times/k^{\times m} \to \mu_m$$

as follows: for any $\sigma \in \operatorname{Gal}(k^{\text{sep}}/k)$ and $a \in k^\times$, select some $\alpha \in k^{\text{sep}} \times$ which is a root of the polynomial $X^m - a$. Then we define $\langle \sigma, a \rangle := \sigma(\alpha)/\alpha$.

Remark A.7. Let's check that this pairing is well-defined.

- We see that any root of $X^m - a$ is separable because this polynomial is separable: its derivative is mX^{m-1} because $\operatorname{char} k \nmid m$.
- Independent of α: the other roots of this polynomial take the form $\zeta\alpha$ for some $\zeta \in \mu_m \subseteq k$, so $\sigma(\zeta\alpha)/(\zeta\alpha) = \sigma(\alpha)/\alpha$, so $\langle \sigma, a \rangle$ does not depend on the choice of α.
- Image in μ_m: note $\langle \sigma, a \rangle \in \mu_m$ because $(\sigma(\alpha)/\alpha)^m = \sigma(a)/a = 1$.
- Independent of $k^{\times m}$: if we replace a with some $a' := ab^m$ where $b \in k^\times$, then we may select $\alpha' := \alpha b$, which shows $\sigma(\alpha')/\alpha' = \sigma(\alpha)/\alpha$, so $\langle \sigma, a \rangle = \langle \sigma, ab \rangle$.

Theorem A.8 (Kummer)**.** Fix a field k and a positive integer m. Suppose that $\operatorname{char} k \nmid m$ and $\mu_m \subseteq k$.

(a) There is a map sending subgroups B between $k^{\times m}$ and $k^\times$ to abelian extensions K/k of exponent m. This map sends B to the extension $K_B := k(B^{1/m})$ of k generated by the mth roots of B.

(b) Given some such B, the pairing restricted Kummer pairing

$$\operatorname{Gal}(K_B/k) \times B \to \mu_m$$

is perfect.

(c) The map in (a) is an inclusion-preserving bijection.

Proof. We use the Kummer pairing to show the parts in sequence. Everything is rather formal except for the surjectivity check in (c), for which we must use Lemma A.5.

(a) We must check that K_B/k is an abelian Galois extension of exponent m.

- To see that it is Galois, it is enough to check that it is generated by Galois elements, so it is enough to check that all Galois conjugates of $\alpha \in B^{1/m}$ live in K_B. Well, $a \coloneqq \alpha^m$ is an element of k by construction, so α is the root of the polynomial $X^m - a$. Because $\mu_m \subseteq k$, we see that the set
$$\{\zeta\alpha : \zeta \in \mu_m\}$$
of roots of $X^m - a$ is therefore contained in K_B.
- To see that it is abelian, choose two automorphisms $\sigma, \tau \in \operatorname{Gal}(K_B/k)$. We would like to check that $\sigma\tau = \tau\sigma$. It is enough to check this equality on generating elements of K_B/k, so we once again choose some $\alpha \in B^{1/m}$ and set $a \coloneqq \alpha^m$. Then we see that
$$\sigma\tau(\alpha) = \langle\sigma, a\rangle\langle\tau, a\rangle = \tau\sigma(\alpha).$$

(b) Here are our checks.

- Injective on $\operatorname{Gal}(K_B/k)$: suppose that $\sigma \in \operatorname{Gal}(K_B/k)$ makes $\langle\sigma, \cdot\rangle$ the trivial function, and we must show that σ is trivial. Well, it is enough to show that σ is trivial on $B^{1/m}$, so we choose some $\alpha \in B^{1/m}$ and set $a \coloneqq \alpha^m$. Then
$$\frac{\sigma(\alpha)}{\alpha} = \langle\sigma, a\rangle = 1,$$
so σ is the identity on α.
- Injective on $B/k^{\times m}$: suppose that $a \in B$ makes $\langle\cdot, a\rangle$ is trivial, and we would like to show that $a \in k^{\times m}$. Well, choose a root $\alpha \in K_B$ of $X^m - a$, and we would like to show that $\alpha \in k$. For this, we note that $\langle\sigma, \alpha\rangle = 1$ implies that $\sigma(\alpha) = \alpha$ for all $\sigma \in \operatorname{Gal}(K_B/k)$, so the result follows.

(c) This will require some effort. Here are our checks.

- Inclusion-preserving: if $B_1 \subseteq B_2$, then we see $B_1^{1/m} \subseteq B_2^{1/m}$, so $K_{B_1} \subseteq K_{B_2}$.
- Injective: in light of the previous check, it's enough to see that $K_{B_1} \subseteq K_{B_2}$ implies that $B_1 \subseteq B_2$. For this, we reduce to the finite case. Choose $b \in B_1$, and it is enough to check that $b \in B_2$ given that $K_{\langle b\rangle} \subseteq K_{B_2}$. However, $b \in K_{B_2}$ implies that b can be written as a finite polynomial in terms of finitely many elements in $B_2^{1/m}$, so we may as well replace B_2 by this finitely generated subgroup to check that $b \in B_2$. In total, we are reduced to the case where B_1 is generated by b and B_2 is finitely generated.

  Now, define $B_3 \subseteq k^\times$ as being generated by B_2 and b. Because $b \in K_{B_2}$ already, we know $K_{B_2} = K_{B_3}$, so the duality of (b) implies
$$[B_2 : k^{\times m}] = [B_3 : k^{\times m}].$$
  Because $B_2/k^{\times m} \subseteq B_3/k^{\times m}$ already, we see that equality must follow, so $b \in B_2$ is forced.
- Surjective: Choose an extension K/k which is abelian of exponent m. It is enough to check that K can be generated by the mth roots of some subset $S \subseteq k^{\times m}$, from which we find $K = K_B$ where B is the multiplicative subgroup generated by S. By writing K as a composite of finite extensions of k, we note that each of these finite extensions must be abelian, so it is enough to generate such a finite abelian extension by mth roots. Well, a finite abelian group can be written as a product of cyclic groups, so we may write a finite abelian extension as a composite of cyclic ones, so it is enough to generate such finite cyclic extensions by mth roots. This is possible by Lemma A.5. ■

Remark A.9. It will be worthwhile to know something about ramification in the case where k is a number field. Given a finitely generated subgroup $B = \langle b_1, \ldots, b_n \rangle$ of $k^\times / k^{\times m}$, we claim that K_B/k can only be ramified at primes $\mathfrak{p}$ lying over rational primes dividing

$$m \prod_{i=1}^{n} \mathrm{N}_{k/\mathbb{Q}}(b_i).$$

Because the composite of unramified extensions is unramified, we may assume that $n = 1$ so that $B = \langle b \rangle$. Now, a prime $\mathfrak{p}$ of k ramifies in K_B if and only if $\mathfrak{p}$ divides the relative discriminant of K_B/k. But this relative discriminant divides the discriminant of the generating polynomial $f(X) \coloneqq X^m - b$, which can be computed (up to sign) to be $\mathrm{N}_{K_B/k} f'(\beta)$, where $\beta^m = b$. The result follows because $f'(X) = mX^{m-1}$.

Bibliography

[PR12] Bjorn Poonen and Eric Rains. "Random maximal isotropic subspaces and Selmer groups". In: *J. Amer. Math. Soc.* 25.1 (2012), pp. 245–269. ISSN: 0894-0347. DOI: 10.1090/S0894-0347-2011-00710-8. URL: https://doi.org/10.1090/S0894-0347-2011-00710-8.

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

List of Definitions