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 $Ш(E/\mathbb{Q})$.

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

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

For example, it follows that

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

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

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

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.

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

1.2 September 16

Welcome to the second class of the semester. The note-taker is furiously eating lunch. 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 $(-)^G \colon \mathrm{Mod}_{\mathbb{Z}[G]} \to \mathrm{Ab}$ 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 $(-)^G \colon \mathrm{Mod}_{\mathbb{Z}[G]} \to \mathrm{Ab}$.

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

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

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 $\mathrm{Mod}_G \to \mathrm{Mod}_{G'}$ 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 $\mathrm{Hom}_{\mathbb{Z}[G]}(-, M)$, 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

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

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

$$f(g) \coloneqq (g-1)m.$$

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. The point is that a 1-cocycle $c\colon \mathbb{Z}\left[G^2\right] \to M$ should be sent to the "restriction" $f(g) := c(e, g)$, which turns out to be a crossed homomorphism.

- 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

$$\mathrm{Hom}_G\left(\mathbb{Z}\left[G^2\right], M\right) \stackrel{d_3}{\to} \mathrm{Hom}_G\left(\mathbb{Z}\left[G^3\right], M\right).$$

  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

$$\mathrm{Hom}_G\left(\mathbb{Z}\left[G\right], M\right) \stackrel{d_2}{\to} \mathrm{Hom}_G\left(\mathbb{Z}\left[G^2\right], M\right).$$

  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

$$d_2b(g_0, g_1) = g_0b - g_1b.$$

  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

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

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 $\mathrm{N}_G(x)\coloneqq\sum_{g\in G}gx$; equivalently, we can view N_G as multiplication by the norm element $\mathrm{N}_G\coloneqq\sum_{g\in G}g$. Because we are back at $\mathbb{Z}$, we see that we can iterate to produce a resolution

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

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

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

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 $m\coloneqq\#G'/\#G$ for brevity. Now, the identities $g(\sigma'-1)=(\sigma-1)$ and $g(\mathrm{N}_{G'})=m\,\mathrm{N}_G$ produce the morphism

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

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

$$(gf)(x)\coloneqq f(xg).$$

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 $f(g) \coloneqq gm$. 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

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

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

Fix.

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

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

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

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 $X \hookrightarrow \mathbb{P}^n_k$ 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

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

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 $G := \operatorname{Gal}(\overline{K}/K)$ 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 1.63. 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 $\operatorname{Gal}(\overline{K}/K)$ 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 1.67. Let K^{ur} be the maximal unramified extension of K. Then we see that $\operatorname{Gal}(K^{\mathrm{ur}}/K)$ is simply $\operatorname{Gal}(\overline{K}/K)/I_K$, which is $\operatorname{Gal}(\overline{k}/k)$.

Definition 1.68 (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 1.69. 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.

Example 1.71. Suppose that m is a positive integer nonzero in K. Then Example A.4 provides an isomorphism

$$\delta\colon K^\times/K^{\times m} \to \mathrm{H}^1(K; \mu_m)$$

given by $\delta(a)\colon \sigma \mapsto \sigma\sqrt[m]{a}/\sqrt[m]{a}$. We claim that $\delta(a) \in \mathrm{H}^1_{\mathrm{ur}}(K; \mu_m)$ if and only if $v(a) \equiv 0 \pmod m$. Indeed, $\delta(a)$ is unramified if and only if I_K fixes $K(\sqrt[m]{a})$, which is equivalent to the extension $K(\sqrt[m]{a})/K$ being unramified. We can see that this extension is unramified if and only if $\sqrt[m]{a}$ succeeds at having integer valuation, which is equivalent to $v(a) \equiv 0 \pmod m$.

We are now able to relate our two dualities.

Proposition 1.72. 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. The fact that M^* is unramified is direct because both M and $\mu_{\#M}$ are unramified. 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 $\mathrm{H}^2_{\mathrm{ur}}(K; \mu_{\#M})$, 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 1.73. 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

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

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 can be checked by passing to finite fields and then counting! ■

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 1.74 (Selmer group)**.** 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 the *local conditions* $\mathcal{L}$ to be the pullback in the following square.

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

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

We will primarily be interested in the following example; we will say more about Selmer groups of elliptic curves next class.

Example 1.75. 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. This assembles into a local condition by Lemma 1.73, so we receive a Selmer group $\mathrm{Sel}_{\mathcal{L}}(E[m])$. We may write $\mathrm{Sel}_m(E)$ for $\mathrm{Sel}_{\mathcal{L}}(E[m])$ in this situation.

This definition is slightly complicated, so here are many remarks.

Remark 1.76. To unravel the pullback, we note that the bottom arrow is an inclusion (of abelian groups), so the top arrow must be as well, allowing us to write

$$\operatorname{Sel}_{\mathcal{L}}(M) = \left\{c \in \mathrm{H}^1(K;M) : \operatorname{Res}_v c \in \mathcal{L}_v \text{ for all places } v\right\}.$$

Remark 1.77. 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, which means that $\mathrm{H}^1_{\mathrm{ur}}(K_v;M)$ is not expected to make sense at all places v. On the other hand, the requirement $\mathcal{L}_v = \mathrm{H}^1_{\mathrm{ur}}(K_v;M)$ does make sense because M is unramified at all but finitely many places v: the Galois action on M factors through $\operatorname{Gal}(L/K)$ for some finite extension L of K, so for any place v unramified in L has its inertia group I_v have trivial image in $\operatorname{Gal}(L/K)$ and thus acts trivially on M.

Remark 1.78. The power of $\operatorname{Sel}_{\mathcal{L}}(M)$ is that it requires the cocycles to be unramified outside a fixed set of places. For comparison, the image of $\mathrm{H}^1(K;M)$ maps to the restricted direct product

$$\prod_v \left(\mathrm{H}^1(K_v;M), \mathrm{H}^1_{\mathrm{ur}}(K_v;M)\right).$$

This amounts to saying that a given cocycle class $c \in \mathrm{H}^1(K;M)$ is unramified at all but finitely many places v. To see this, the definition of $\mathrm{H}^1(K;M)$ as a colimit means that there is a finite extension L of K for which c is the inflation of an element in $\mathrm{H}^1(L/K;M)$. Thus, for any place v unramified in L, the inertia group I_v has trivial image in $\operatorname{Gal}(L/K)$, so $c|_{I_v}$ is trivial, so $\operatorname{Res}_v c$ is unramified.

Inspired by Remark 1.78, we make the following notation.

Notation 1.79. Fix a number field K and a finite discrete Galois module M. For each index i, we define $\mathrm{H}^i(\mathbb{A}_K;M)$ as the restricted direct product

$$\mathrm{H}^i(\mathbb{A}_K;M) \coloneqq \prod_v \left(\mathrm{H}^i(K_v;M), \mathrm{H}^i_{\mathrm{ur}}(K_v;M)\right).$$

Here, the restricted direct product makes sense because M is unramified at all but finitely many places v of K (as discussed in Remark 1.77).

Here is our finiteness result.

Theorem 1.80. 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 $\operatorname{Sel}_{\mathcal{L}}(M)$ 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 $\operatorname{Sel}_{\mathcal{L}}(M)$ to $\operatorname{Sel}_S(M)$. 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.

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

By definition of the Selmer group, the square is a pullback square, and the horizontal line is exact by the Inflation–Restriction exact sequence (Proposition 1.49). Thus, finiteness for the restricted module implies finiteness for $\operatorname{Sel}_S(M)$ because $\mathrm{H}^1(\operatorname{Gal}(K'/K); M)$ 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 $\operatorname{Gal}(\overline{K}/K')$ 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 $\operatorname{Sel}_S(\mathbb{Z}/m\mathbb{Z})$ now embeds into $\mathrm{H}^1(K; \mathbb{Z}/m\mathbb{Z})$, which is the same as

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

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 1.81. 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 $\operatorname{Gal}(L/k)$ 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.

1.4 September 23

Today, we compute some Selmer groups of the congruent number of elliptic curve.

1.4.1 The Weil Pairing

Even though we are not going to use many of the results in this subsection in the future, it is useful to give some general facts and conjectures in order to build intuition about Selmer groups of elliptic curves, following [PR12]. For later use, we begin with a discussion of the Weil pairing, following [Sil09, Section III.3], though we remark that one can generalize everything to abelian varieties without too much trouble.

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

Definition 1.82 (Weil pairing)**.** Fix an elliptic curve E over a field K. For each positive integer m, we define the *Weil pairing*

$$e_m \colon E[m] \times E[m] \to \mu_m$$

as follows. Fix $S, T \in E[m]$. Choose functions f and g in $K(E)$ for which $\operatorname{div} f = m[T] - m[\infty]$ and $f \circ [m] = g^m$. Now, the function $E \to \mathbb{P}^1$ defined by $X \mapsto g(X+S)/g(X)$ turns out to be constant, so we define $e_m(S,T)$ to be this constant value.

Remark 1.83. Let's explain why the functions f and g exist. The isomorphism $\operatorname{Pic}^0(E) \to E$ of group schemes shows that a divisor $\sum_i n_i[P_i]$ in $\operatorname{Pic}^0(E)$ vanishes (i.e., arises from a function unique up to $\overline{K}^\times$) if and only if the associated sum $\sum_i n_i P_i$ is 0 in E. This explains why there is some f for which $\operatorname{div} f = m[T] - m[\infty]$. Furthermore, we can select g for which $\operatorname{div} g = [m]^*[T] - [m]^*[\infty]$, which can be computed as $\sum_{T' \in E[m]}([T+T'] - [T'])$. As such, $f \circ [m]$ and g^m have the same divisor, so we can force an equality by multiplying by a suitable scalar.

Remark 1.84. Let's explain why $X \mapsto g(X+S)/g(X)$ is constant and outputs to μ_m. For the constancy, we note that this is a function between two connected curves, so it is enough to check that it fails to be surjective. Well, $g(X+S)^m = f(mX+mS) = f(mX)$ is also equal to $g(X)^m = f(mX)$, so $g(X+S)/g(X)$ must output to the finite set of roots of unity (or ∞). Thus, this function is indeed not surjective. Lastly, the output is to μ_m because there must be some X for which $g(X+S) \neq \infty$ and $g(X) \neq 0$ (after all, g has only finitely many zeroes and poles).

Remark 1.85. The value $e_m(S,T)$ does not depend on the choices f and g: we know f is unique up to scalar, so g is also unique up to scalar, so the quotient $g(X+S)/g(X)$ is well-defined.

Remark 1.86. When generalizing to abelian varieties, the correct Weil pairing is defined between an abelian variety A and its "dual" $\operatorname{Pic}^0 A$.

Example 1.87. Here is basically the only example that can be done by hand: take $m = 2$, and suppose that E is the projective closure of $y^2 = (x-a)(x-b)(x-c) = x^3 - s_1x^2 + s_2x - s_3$. We will compute f and g for the 2-torsion point $T \coloneqq (a,0)$. Indeed, take $f(x) \coloneqq x - a$; this only can have a root at T, and it has a double root there because the tangent line is vertical. Thus, $\operatorname{div} f = 2[T] - 2[\infty]$. Continuing, with the help of a computer algebra system and the doubling formula for an elliptic curve, one can check that

$$f \circ [2] = \left(\frac{x^2 - 2ax - 2a^2 + 2s_1a - s_2}{2y} \right)^2,$$

so we may take g to be the function $\left(x^2 - 2ax - 2a^2 + 2s_1a - s_2\right)/2y$. We will not bother to compute $g(X+S)/g(X)$ for various points X and S.

Here are our checks on this pairing.

Lemma 1.88. Fix an elliptic curve E over a field K. For each positive integer m, the Weil pairing e_m is bilinear, alternating, non-degenerate, and Galois-invariant. Furthermore, given two positive integers m and k, we have that

$$e_{mk} = e_m \circ ([k], \mathrm{id}).$$

Proof. We run our checks one at a time. Whenever torsion points, we will silently produce f and g as in the Weil pairing.

- Linear on the left: given $T \in E[m]$, we produce f and g as usual. Then for $S_1, S_2 \in E[m]$, the identity $e_m(S_1 + S_2, T) = e_m(S_1, T)e_m(S_2, T)$ can be expanded into the equality
$$\frac{g(X+S_1+S_2)}{g(X)} = \frac{g(X+S_1+S_2)}{g(X+S_2)} \cdot \frac{g(X+S_2)}{g(X)}.$$
- Linear on the right: given $T_1, T_2 \in E[m]$, we produce the functions f_1, f_2, f_3, g_1, g_2, and g_3, where the pair (f_1, g_1) is for the torsion point $T \coloneqq T_1 + T_2$. We need a way to relate these functions, so we remark that
$$\operatorname{div} \frac{f_3}{f_1 f_2} = m([T_1 + T_2] - [T_1] - [T_2] + [\infty]),$$
so as discussed in Remark 1.83, we may produce a function h with $\operatorname{div} h = [T_1 + T_2] - [T_1] - [T_2] + [\infty]$. Adjusting h by a scalar, we can achieve the equality $f_3 = f_1 f_2 h^m$, so taking mth powers gives $g_3 = g_1 g_2 (h \circ [m])^m$.
Now, for any $S \in E[m]$, we see that $e_m(S, T_1 + T_2)$ equals $g_3(X + S)/g_3(X)$, which now expands into
$$\underbrace{\frac{g_1(X+S)}{g_1(X)}}_{e_m(S,T_1)} \cdot \underbrace{\frac{g_2(X+S)}{g_2(X)}}_{e_m(S,T_2)} \cdot \underbrace{\frac{h(mX+mS)^m}{h(mX)^m}}_{1}.$$
- Alternating: we need to check that $e_m(T, T) = 1$ for $T \in E[m]$. Producing f and g as usual, we would like to show that $g(X + T) = g(X)$. The trick is to consider the function
$$\prod_{i=0}^{m-1} f \circ \tau_{iT},$$
where iT is translation by T. A direct expansion with $\operatorname{div} f = m[T] - m[\infty]$ shows that the divisor of the above function vanishes (it is $\sum_i m([(i+1)T] - m[iT])$, which telescopes), so it is constant. Composing with $[m]$ and taking mth roots, we see that
$$\prod_{i=0}^{m-1} g \circ \tau_{iT'}$$
is also constant, where T' has been chosen so that $mT' = T$. For example, we should get the same value plugging in X and $X + T'$. Taking the quotient causes the terms $0 < i < m-1$ to vanish from both products, leaving us with $g(X + T)/g(X) = 1$.
- Non-degenerate: because the pairing is already alternating, it is enough to show that $e_m(-, T) = 1$ implies that $T = \infty$. Well, choose f and g as usual, and we are given that $g(X + S) = g(X)$ for any $S \in E[m]$. Thus, E factors through the elliptic curve $E/E[m]$, so we receive a function h for which $g = h \circ [m]$. But now $h^m = f$, so $\operatorname{div} h = [T] - [\infty]$. Because $E \neq \mathbb{P}^1$, we are forced to have $T = \infty$.
- Galois-invariant: fix $S, T \in E[m]$, and choose $\sigma \in \operatorname{Gal}(K^{\text{sep}}/K)$. Picking up functions f and g as usual, we note that $(\sigma f) \circ [m] = (\sigma g)^m$ and $\operatorname{div} \sigma f = m[\sigma T] - m[\infty]$, so $e_m(\sigma S, \sigma T)$ is
$$\frac{\sigma g(\sigma X + \sigma S)}{\sigma g(\sigma X)} = \sigma\left(\frac{g(X+S)}{g(X)}\right),$$
which of course is $\sigma e_m(S, T)$.
- Lastly, we need to check that $e_{mk}(S, T) = e_m(kS, T)$ for $S \in E[mk]$ and $T \in E[m]$. Well, choose f and g as usual, and then we note that f^k and $g \circ [k]$ work to define e_{mk}, so $e_{mk}(S, T)$ equals
$$\frac{g(kX+kS)}{g(kX)},$$
which is $e_m(kS, T)$. ■

In the sequel, it will be helpful to have another presentation of the Weil pairing.

Notation 1.89. Fix a smooth proper curve C over a field K. For each function $f \in C(K)$ and divisor D on K such that $\operatorname{supp} D$ and $\operatorname{supp} \operatorname{div} f$ are disjoint, we write $D = \sum_i n_i[P_i]$ and define

$$f(D) = \prod_i f(P_i)^{n_i}.$$

Definition 1.90 (Weil pairing)**.** Fix an elliptic curve E over a field K. For each positive integer m, we define the *Weil pairing*

$$\widetilde{e}_m \colon E[m] \times E[m] \to \mu_m$$

as follows. Given $S, T \in E[m]$, choose divisors D_S and D_T of disjoint support such that $D_S \equiv [S] - [\infty]$ and $D_T \equiv [T] - [\infty]$. Then choose functions f_S and f_T for which $\operatorname{div} f_S = mD_S$ and $\operatorname{div} f_T = mD_T$, and we define $\widetilde{e}_m(S,T) := f_S(D_T)/f_T(D_S)$.

Remark 1.91. It is possible to find divisors D_S and D_T by (say) taking $D_S := [S] - [\infty]$ and $D_T := [R+S] - [R]$ for some auxiliary torsion point $R \in E(\overline{K})$ of order larger than m. Then f_S and f_T are uniquely defined up to scalars (see Remark 1.83), and the values $f_S(D_T)$ and $f_T(D_S)$ are well-defined because the supports are disjoint, and $\deg D_T = \deg D_S = 0$. Note that we have not yet shown that $\widetilde{e}$ is independent of the choice of divisors D_S and D_T!

To see that this definition is well-defined (and agrees with the one provided earlier), we need the following tool.

Theorem 1.92 (Weil reciprocity)**.** Fix a smooth proper curve C over an algebraically closed field K. For any $f, g \in K(C)$ with disjoint supports, we have

$$f(\operatorname{div} g) = g(\operatorname{div} f).$$

Proof. We have two steps.

1. We handle the case where $C = \mathbb{P}^1$. Here, f and g are just some rational functions in the coordinate x. By changing coordinates (and using the fact that $\overline{K}$ is infinite while $\operatorname{supp} f$ and $\operatorname{supp} g$ are finite), we may assume that neither f nor g have neither a root nor pole at ∞. After adjusting by scalars (which does not change the validity of the conclusion), we may now set

$$f(x) = \prod_{i=1}^{M} (x - a_i)^{m_i} \qquad \text{and} \qquad g(x) = \prod_{j=1}^{N} (x - b_j)^{n_j}$$

for some $a_1, \ldots, a_M, b_1, \ldots, b_N \in K$ and $m_1, \ldots, m_M, n_1, \ldots, n_N \in \mathbb{Z}$. Because $\operatorname{supp} f$ and $\operatorname{supp} g$ avoid ∞, we have $\operatorname{div} f = \sum_i m_i[a_i]$ and $\operatorname{div} g = \sum_j n_j[b_j]$. Now, on one hand $f(\operatorname{div} g)$ equals

$$\prod_{j=1}^{N} f(b_j)^{n_j} = \prod_{j=1}^{N} \prod_{i=1}^{M} (b_j - a_i)^{m_i n_j}.$$

Similarly, we find that $g(\operatorname{div} f)$ equals

$$\prod_{i=1}^{M} \prod_{j=1}^{N} (a_i - b_j)^{m_i n_j}.$$

Now, these two values differ by (-1) to the power of $\sum_{i,j} m_i n_j$, which of course is zero because $\sum_i m_i = \sum_j n_j = 0$.

2. We handle the general case. View g as a rational map $C \to \mathbb{A}^1$, which can then be extended to a regular map $g\colon C \to \mathbb{P}^1$ because C is proper. We now formally manipulate divisors. Note that $\operatorname{div} g = g^* \operatorname{div} \operatorname{id}_{\mathbb{P}^1}$ by definition, so $f(\operatorname{div} g)$ equals
$$f(g^* \operatorname{div} \operatorname{id}_{\mathbb{P}^1}) = (g_* f)(\operatorname{div} \operatorname{id}_{\mathbb{P}^1}).$$
Now, by the first step, this is
$$\operatorname{id}_{\mathbb{P}^1}(\operatorname{div} g_* f) = \operatorname{id}_{\mathbb{P}^1}(g_* \operatorname{div} f).$$
This right-hand side collapses to $g(\operatorname{div} f)$, so we are done. ∎

We now give a few remarks about our definition of $\widetilde{e}$.

Remark 1.93. We show that $\widetilde{e}$ is independent of the choices of D_S and D_T. By symmetry, it will be enough to show that it is independent of the choice of D_S. Accordingly, suppose we choose another divisor D_S' linearly equivalent to D_S, and then we choose another function f_S' with divisor equal to mD_S'. Then we want to show that
$$\frac{f_S(D_T)}{f_T(D_S)} \stackrel{?}{=} \frac{f_S'(D_T)}{f_T(D_S')}.$$
Well, $D_S \equiv D_S'$ implies that there is a function g with $\operatorname{div} g = D_S' - D_S$. Then we see $\operatorname{div} f_S' = \operatorname{div} f_S g^m$, so after adjusting by a scalar, we may assume that $f_S' = f_S g^m$. The above equality then rearranges into $f_T(\operatorname{div} g) = g(D_T)^m$, which follows from Theorem 1.92.

Remark 1.94. We note that we can directly check that $\widetilde{e}(S,T)^m = 1$. Indeed, this quotient is
$$\frac{f_S(mD_T)}{f_T(mD_S)} = \frac{f_S(\operatorname{div} f_T)}{f_T(\operatorname{div} f_S)},$$
which is 1 by Theorem 1.92.

Proposition 1.95. Fix an elliptic curve E over a field K and a positive integer m. For any $S, T \in E[m]$, we have
$$\widetilde{e}(S,T) = e(T,S).$$

Proof. We follow [Sil09, Exercise 3.16]; note that an argument for this exercise is provided in the back matter. For $m = 1$ or $S = T$, everything is trivial, so there is nothing to do. Otherwise, we proceed in steps.

1. We set up notation. Choose points S' and T' with $mS' = S$ and $mT' = T$. Further, by adjusting T' by an element of $E[m]$, we may assume that $S' \neq T'$ (which we do for technical reasons), and we let R be an auxiliary point so that $2R = S' - T'$; note then that the divisors $D_S := [S] - [\infty]$ and $D_T := [T + mR] - [mR]$ have disjoint support. Then mD_S and mD_T are linearly equivalent to 0, so we may find functions f_S and f_T with $\operatorname{div} f_S = mD_S$ and $\operatorname{div} f_T = mD_T$, and as in Remark 1.83, we may find functions g_S and g_T for which $f_S \circ [m] = g_S^m$ and $f_T \circ [m] = g_T^m$. Before going further, we note that, as in Remark 1.83, we have
$$\operatorname{div} g_S = \sum_{P \in E[m]} ([P + S'] - [P]) \qquad \text{and} \qquad \operatorname{div} g_T = \sum_{P \in E[m]} ([P + T' + R] - [P + R]).$$

2. By plugging in our various pairings, we see that we are interested in showing
$$\frac{f_S(D_T)}{f_T(D_S)} \stackrel{?}{=} \frac{g_S(X + S)}{g_S(X)}.$$

To start, a direct calculation shows that the left-hand side is

$$\frac{f_S(mT'+mR)/f_S(mR)}{f_T(mS')/f_T(\infty)} = \left(\frac{g_S(T'+R)/g_S(R)}{g_T(S')/g_T(\infty)}\right)^m.$$

The trick is that the function

$$\frac{g_S(X+T'+R)/g_S(X+R)}{g_T(X+S')/g_T(X)}$$

is a constant function. This will use the fact that $2R = S' - T'$. Indeed, it is enough to show that the divisor of this function vanishes, so we calculate its divisor to be

$$\begin{aligned}\sum_{P\in E[m]} &([P+S'-T'-R]-[P-T'-R]) - ([P+S'-R]-[P-R]) \\ &- ([P+T'-S'+R]-[P-S'+R]) + ([P+T'+R]-[P+R]).\end{aligned}$$

Plugging in $S' = T' + 2R$, we get

$$\begin{aligned}\sum_{P\in E[m]} &([P+R]-[P-T'-R]) - ([P+T'+R]-[P-R]) \\ &- ([P-R]-[P-T'-R]) + ([P+T'+R]-[P+R]),\end{aligned}$$

which vanishes term-wise.

3. Continuing, we see that $\widetilde{e}(S,T)$ is

$$\prod_{i=0}^{m-1} \frac{g_S((i+1)T'+R)/g_S(iT'+R)}{g_T(iT'+S')/g_T(iT')}$$

by the constancy of the preceding paragraph, which collapses to

$$\frac{g_S(T+R)}{g_S(R)} \prod_{i=0}^{m-1} \frac{g_T(iT')}{g_T(iT'+S)}.$$

The left-hand term is simply $e(T,S)$ by its construction, so it remains to show that the right-hand product is 1. For this, we see that we have to show that the function

$$\prod_{i=0}^{m-1} g_T(iT'+X)$$

is constant, which we achieve with another divisor calculation: the divisor of this function is

$$\sum_{P\in E[m]} \left(\sum_{i=0}^{m-1}[P+T'+R-iT'] - [P+R-iT']\right),$$

which collapses to

$$\sum_{P\in E[m]} ([P+mT'+R]-[P+R]),$$

which now vanishes because $mT' \in E[m]$. ■

1.4.2 The Weil Pairing for Selmer Groups

The Weil pairing now interacts with cohomology as follows.

Proposition 1.96. Fix a field K of characteristic 0 and a positive integer m.

(a) The Weil pairing induces a symmetric cup-product pairing

$$\mathrm{H}^1(K; E[m]) \times \mathrm{H}^1(K; E[m]) \to \mathrm{H}^2(E; \mu_m).$$

(b) If K is local, then the pairing in (a) is perfect.

(c) The subspace $E(K)/mE(K)$ of $\mathrm{H}^1(K; E[m])$ is isotropic.

(d) If K is local and m is prime, then the subspace $E(K)/mE(K)$ of $\mathrm{H}^1(K; E[m])$ is maximal isotropic.

Proof. We show the parts separately.

(a) This pairing is defined by
$$(c_1, c_2) \mapsto \mathrm{H}^2(e_m)(c_1 \cup c_2),$$
which is symmetric because $\cup$ and e_m are both alternating.

(b) This follows from local duality. Indeed, the Weil pairing on $E[m]$ is perfect and Galois-invariant, so it induces an isomorphism $E[m] \cong \mathrm{Hom}(E[m], \mu_m)$ of (finite discrete) Galois modules. The cup-product pairing in the statement is now exactly the pairing of Theorem 1.62.

(c) We will show this directly on the level of cocycles. Fix $P, Q \in E(K)/mE(K)$, and we want to show that the 2-cocycle $\mathrm{H}^2(e_m)(\delta_P \cup \delta_Q)$ is a 2-coboundary. Expanding out the definitions, we see that we should choose P' and Q' with $P = mP'$ and $Q = mQ'$, and then we want to show the map

$$(\sigma, \tau) \mapsto e_m(\sigma P' - P', \sigma\tau Q' - \sigma Q')$$

is a 2-coboundary. For this, we will use Proposition 1.95, which allows us to instead show that the 2-cocycle
$$c\colon (\sigma, \tau) \mapsto \widetilde{e}_m(\sigma P' - P', \sigma\tau Q' - \sigma Q')^{-1}$$
is a 2-coboundary.

Accordingly, we now set up some notation. If $P = Q$, then there is nothing to do, so we omit this case. For each $\sigma \in \mathrm{Gal}(K^{\mathrm{sep}}/K)$, we define the divisors $D_{P,\sigma} := [\sigma P'] - [P']$ and $D_{Q,\sigma} := [\sigma Q'] - [Q']$. Note that any $D_{P,\sigma}$ and any $D_{Q,\tau}$ have disjoint support: $P \neq Q$ forces $\sigma P' \neq \tau Q'$ for any σ or τ because $m\sigma P' = P$ and $m\tau Q' = Q$. We also note that $D_{P,\sigma\tau} = \sigma D_{P,\tau} + D_{P,\sigma}$ and similarly for Q. Continuing, we select functions $f_{P,\sigma}$ and $f_{Q,\sigma}$ so that $\operatorname{div} f_{P,\sigma} = mD_{p,\sigma}$ and $\operatorname{div} f_{Q,\sigma} =$. By choosing another point S not in the Galois orbit of the previously defined points, we may normalize the functions $f_\bullet$ so that they evaluate to 1 on S. Then we see that

$$f_{P,\sigma\tau} = \sigma f_{P,\tau} \cdot f_{P,\sigma}$$

because they have the same divisor and the same nonzero value at S; a similar statement holds for Q.

We are now ready to calculate. To begin, note $c(\sigma, \tau)$ is

$$\widetilde{e}_m(\sigma P' - P', \sigma\tau Q' - Q')\widetilde{e}_m(\sigma P' - P', \sigma Q' - Q')^{-1} = \frac{f_{Q,\sigma\tau}(D_{P,\sigma})}{f_{P,\sigma}(D_{Q,\sigma\tau})} \cdot \frac{f_{P,\sigma}(D_{Q,\sigma})}{f_{Q,\sigma}(D_{P,\sigma})}.$$

We now recall $f_{Q,\sigma\tau} = \sigma f_\tau \cdot f_\sigma$ and $D_{Q,\sigma\tau} = \sigma D_\tau + D_\sigma$, so $c(\sigma, \tau)$ equals

$$\frac{(\sigma f_{Q,\tau})(D_{P,\sigma})}{f_{P,\sigma}(\sigma D_{Q,\tau})} = \frac{\sigma f_{Q,\tau}(P')}{\sigma f_{Q,\tau}(\sigma^{-1}P')} \cdot \frac{f_{P,\sigma}(\sigma Q)}{f_{P,\sigma}(\sigma\tau Q)}.$$

We will complete the proof by showing that each factor of the right-hand side is a 2-coboundary. For example, the 1-cochain $\sigma \mapsto f_{Q,\sigma}(P')$ produces the 1-coboundary sending (σ, τ) to

$$\frac{\sigma f_{Q,\tau}(P') \cdot f_{Q,\sigma}(P')}{f_{Q,\sigma\tau}(P')} = \frac{\sigma f_{Q,\tau}(P')}{\sigma f_{Q,\tau}(\sigma^{-1}P')}.$$

Similarly, the 1-cochain $\sigma \mapsto f_{P,\sigma}(\sigma Q')$ produces the 2-coboundary sending (σ, τ) to

$$\frac{\sigma f_{P,\tau}(\tau Q') \cdot f_{P,\sigma}(\sigma Q')}{f_{P,\sigma\tau}(\sigma\tau Q')} = \frac{\sigma f_{P,\tau}(\tau Q') \cdot f_{P,\sigma}(\sigma Q')}{\sigma f_{P,\tau}(\sigma^{-1}\sigma\tau Q) \cdot f_{P,\sigma}(\sigma\tau Q)}.$$

Multiplying these two 2-coboundaries together completes the proof.

(d) You may show this on the homework! ■

Let's apply the Weil pairing to our Selmer groups.

Remark 1.97. For any local field K_v, we note that $E(K_v) = E(\mathcal{O}_v)$ if E has good reduction at v. At a high level, this follows from the valuative criterion of properness or the theory of Néron models. More directly, one can see that a point $[X : Y : Z] \in \mathbb{P}^2(K_v)$ satisfying the equation defining E may have its coordinates adjusted until all coordinates are in $\mathcal{O}_v$ by homogeneity.

Theorem 1.98. Fix an elliptic curve E over a number field K, and choose a positive integer m. Then $\operatorname{Sel}_m(E/K)$ sits in the following pullback square.

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

(a) If m is prime, then the right vertical arrow is injective.

(b) The images of the bottom and right arrows are maximal isotropic subspaces with respect to the pairing induced by the Weil pairing.

Proof. The pullback square is exactly the one in the definition of the Selmer group by Remarks 1.78 and 1.97. The rest of the statement is [PR12, Theorem 4.14]. In particular, see [PR12, Example 4.18]. ■

Remark 1.99. The moral is that we may view $\operatorname{Sel}_p(E/K)$ may be viewed as an intersection of two maximal isotropic subspaces. Such a "random" intersection is expected to be rather transverse, which perhaps explains why $\operatorname{Sel}_p(E/K)$ is finite-dimensional.

Remark 1.100. Part (a) is a rather sensitive result because it depends on a certain vanishing of Ш result [PR12, Proposition 3.3(e)]. It is not expected to be true if E is replaced by a different module or if m is no longer prime. For example, on the homework, you may show that the map

$$\mathrm{H}^1\left(\mathbb{Q}(\sqrt{7}); \mu_8\right) \to \mathrm{H}^1\left(\mathbb{A}_{\mathbb{Q}(\sqrt{7})}; \mu_8\right)$$

fails to be injective.

1.4.3 Conjectures on the Selmer Group

While we're here, we acknowledge that now is as good as time as any to recall/give the definition of the Tate–Shafarevich group.

Definition 1.101 (Tate–Shafarevich group)**.** Fix a number field K and a discrete Galois module M. Then we define the *Tate–Shafarevich group* $Ш(M/K)$ as

$$Ш(M/K) := \ker\left(\mathrm{H}^1(K;M) \to \prod_v \mathrm{H}^1(K_v;M)\right).$$

Lemma 1.102. Fix an elliptic curve E over a number field K. For each positive integer m, there is an exact sequence

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

Proof. Functoriality of evaluating E on a field yields a morphism

$$\begin{tikzcd} 0 \arrow[r] & E[m](\overline{K}) \arrow[r] \arrow[d, hook] & E(\overline{K}) \arrow[r, "m"] \arrow[d, hook] & E(\overline{K}) \arrow[r] \arrow[d, hook] & 0 \\ 0 \arrow[r] & \prod_v E[m](\overline{K_v}) \arrow[r] & \prod_v E(\overline{K_v}) \arrow[r, "m"] & \prod_v E(\overline{K_v}) \arrow[r] & 0 \end{tikzcd}$$

of short exact sequences, where everything in sight is a continuous Galois module. Taking Galois cohomology thus produces another morphism

$$\begin{tikzcd} 0 \arrow[r] & E(K)/mE(K) \arrow[r] \arrow[d] & \mathrm{H}^1(K;E[m]) \arrow[r] \arrow[d] & \mathrm{H}^1(K;E)[m] \arrow[r] \arrow[d] & 0 \\ 0 \arrow[r] & \prod_v E(K_v)/mE(K_v) \arrow[r] & \prod_v \mathrm{H}^1(K_v;E[m]) \arrow[r] & \prod_v \mathrm{H}^1(K_v;E)[m] \arrow[r] & 0 \end{tikzcd}$$

of short exact sequences. Now, the kernel of the rightmost vertical arrow is $Ш(E/K)[m]$ by definition of $Ш(E/K)$. Accordingly, we claim that we may take a pullback of the top short exact sequence to produce yet another morphism

$$\begin{tikzcd} 0 \arrow[r] & E(K)/mE(K) \arrow[r] \arrow[d, equal] & \mathrm{Sel}_m(E/K) \arrow[r] \arrow[d, hook] \arrow[dr, phantom, "\lrcorner", very near start] & Ш(E/K)[m] \arrow[r] \arrow[d, hook] & 0 \\ 0 \arrow[r] & E(K)/mE(K) \arrow[r] & \mathrm{H}^1(K;E[m]) \arrow[r] & \mathrm{H}^1(K;E)[m] \arrow[r] & 0 \end{tikzcd}$$

of short exact sequences. Here, the middle term of the top short exact sequence is in fact $\mathrm{Sel}_m(E/K)$: this fiber product should consist of the elements of $\mathrm{H}^1(K;E[m])$ which vanish in $\prod_v \mathrm{H}^1(K_v;E)$, which by exactness is equivalent to their image along $\mathrm{H}^1(K;E[m]) \to \prod_v \mathrm{H}^1(K_v;E[m])$ coming from $\prod_v E(K_v)/mE(K_v)$.

It is now totally formal that the top row is exact: exactness on the right follows because the pullback of an epimorphism is an epimorphism. Further, exactness elsewhere amounts to saying that $E(K)/mE(K)$ is the kernel of $\mathrm{Sel}_m(E/K) \to Ш(E/K)[m]$, which follows because pullbacks commute with kernels (recall limits commute with limits). ■

Thus, we see that $\mathrm{Sel}_m(E/K)$ contains contributions from three interesting invariants of E: the m-torsion $E[m]$, the algebraic rank $\mathrm{rank}_{\mathbb{Z}} E(K)$, and $Ш(E/K)$. Of course, the m-torsion is the least interesting, so we introduce some notation to get rid of it.

Notation 1.103. Fix an elliptic curve E over a number field K. For each prime p, we define

$$S_p(E/K) := \dim_{\mathbb{F}_p} \mathrm{Sel}_p(E/K) - \dim_{\mathbb{F}_p} E(K)[p].$$

Remark 1.104. Let r be the algebraic rank of E over K so that $E(K) \cong E(K)_{\text{tors}} \oplus \mathbb{Z}^{\oplus r}$. Thus, for any prime p,

$$\frac{E(K)}{pE(K)} \cong \frac{E(K)_{\text{tors}}}{pE(K)_{\text{tors}}} \oplus \left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^{\oplus r}$$

Note $E(K)_{\text{tors}}$ is some finite abelian group, so the kernel and cokernel of $p\colon E(K)_{\text{tors}} \to E(K)_{\text{tors}}$ have the same size by an Euler characteristic argument. Thus,

$$\dim_{\mathbb{F}_p} E(K)/pE(K) = \dim_{\mathbb{F}_p} E(K)[p] + \operatorname{rank}_{\mathbb{Z}} E(K).$$

Lemma 1.102 now implies that $\operatorname{rank}_{\mathbb{Z}} E(K) + \dim_{\mathbb{F}_p} Ш(E/K)[p] = S_p(E/K)$.

Let's make some "parity conjectures." Fix an elliptic curve E over a number field K.

- Note that $Ш(E/K)$ is known to have an alternating "Cassels–Tate" pairing and is expected to be finite, so its size is conjectured to be a square.
- Similarly, $E[m](K)$ has a Weil pairing, which is a perfect alternating pairing on it, so it similarly follows that the size is a square.

For example, for taking m to be a prime p, this produces the following conjecture via Remark 1.104.

Conjecture 1.105 (Partity for Mordell–Weil rank). Fix an elliptic curve E over a number field K. Then for each prime p,

$$S_p(E/K) \stackrel{?}{\equiv} \operatorname{rank} E(K) \pmod 2.$$

By comparing with the Birch and Swinnerton-Dyer conjecture, we can make a parity conjecture comparing to modular forms.

Conjecture 1.106 (Parity for global root number). Fix an elliptic curve E over a number field K with an attached modular form f_E. Then

$$(-1)^{S_p(E/K)} = \varepsilon(f_E/K),$$

where $\varepsilon(f_E/K)$ is the sign of the L-function's functional equation.

Remark 1.107. There is a purely local definition of $\varepsilon(f_E/K)$ which does not require us to know that there is an attached modular form.

Remark 1.108. Conjecture 1.106 is known if $K = \mathbb{Q}$ by Nekovář and Dokchitser–Dokchitser. If $E[p](K)$ is nontrivial, it is still known by Dokchitser–Dokchitser again. There are other results by Česnavičius.

1.4.4 2-Descent

In this subsection, we explain how to compute 2-Selmer groups of elliptic curves E over a number field K for which $E[2](K) = E[2](\overline{K})$.

To begin, suppose that K is an arbitrary field of characteristic 0, to be set to be a number field shortly. Writing E into Weierstrass form $y^2 = f(x)$ for a cubic x, one sees that the roots of f produce the nontrivial 2-torsion points of f. (This follows from the usual group law of E.) Thus, f is required to fully factor over K, allowing us to write E as the projective closure of the affine curve cut out by

$$y^2 = (x-a_1)(x-a_2)(x-a_3)$$

for some $a_1, a_2, a_3 \in K$. In this situation, we see that

$$E[2] = \{\infty, (a_1, 0), (a_2, 0), (a_3, 0)\}.$$

Now, $E[2]$ has trivial Galois action, so we may identify it with the isomorphic Galois module $\mu_2^{\oplus 2}$. For symmetry reasons, it will in fact be easier to identify it with the "trace zero" hyperplane H of $\mu_2^{\oplus 3}$: namely, we embed $E[2]$ into $\mu_2^{\oplus 3}$ by

$$\begin{cases} \infty \mapsto (+1,+1,+1), \\ (a_1,0) \mapsto (+1,-1,-1), \\ (a_2,0) \mapsto (-1,+1,-1), \\ (a_3,0) \mapsto (-1,-1,+1). \end{cases}$$

Namely, the image of this embedding is $H = \{(\varepsilon_1,\varepsilon_2,\varepsilon_3) \in \mu_2^{\oplus 3} : \varepsilon_1\varepsilon_2\varepsilon_3 = 1\}$, which is the kernel of the product map $H \to \mu_2$.

Remark 1.109. This embedding can be explained by the Weil pairing: it is given by

$$S \mapsto \big(e_2(S,(a_1,0)), e_2(S,(a_2,0)), e_2(S,(a_3,0))\big).$$

Indeed, note that e_2 is linear and alternating by Lemma 1.88, so it must have $e_2(\infty,T) = e_2(T,T) = 1$ for each $T \in E[2]$. However, because $E[2] \cong (\mathbb{Z}/2\mathbb{Z})^2$, if $e_2(S,T) = 1$ for any $S \notin \{\infty, T\}$, then $e_2(-,T)$ is trivial, violating the non-degeneracy of Lemma 1.88.

Thus, we may identify $\mathrm{H}^1(K;E[2]) = \mathrm{H}^1(K;H)$, which tracking through the functoriality of Example A.4 gives

$$\mathrm{H}^1(K;H) \cong \left\{(\alpha,\beta,\gamma) : K^\times/K^{\times 2} : \alpha\beta\gamma \in K^{\times 2}\right\}.$$

In order to compute the 2-Selmer group, we need to understand the image of the map $E(K)/2E(K) \to \mathrm{H}^1(K;E[2]) = \mathrm{H}^1(K;H)$.

Proposition 1.110. Fix an elliptic curve E over a field K which is the projective closure of $y^2 = (x-a_1)(x-a_2)(x-a_3)$. Identifying $E[2]$ with the trace-zero hyperplane $H \subseteq \mu_2^{\oplus 3}$, the boundary map $\delta\colon E(K)/2E(K) \to \mathrm{H}^1(K;H)$ is the map

$$\delta\colon \begin{cases} (x,y) \mapsto (x-a_1, x-a_2, x-a_3) & \text{if } y \neq 0, \\ \infty \mapsto (1,1,1), \\ (a_1,0) \mapsto ((a_1-a_2)(a_1-a_3), a_1-a_2, a_1-a_3), \\ (a_2,0) \mapsto (a_2-a_1, (a_2-a_1)(a_2-a_3), a_2-a_3), \\ (a_3,0) \mapsto (a_3-a_1, a_3-a_2, (a_3-a_1)(a_3-a_2)). \end{cases}$$

Proof. Our exposition is taken from [Sil09, Theorem X.1.1] and the discussion after it. To be explicit, let δ_K be the isomorphism identifying $K^\times/K^{\times 2} \to \mathrm{H}^1(K;\mu_2)$; it sends $\alpha \in K^\times/K^{\times 2}$ to the 1-cocycle $\sigma \mapsto \sigma\sqrt{\alpha}/\sqrt{\alpha}$.

The idea is to compute δ using the Weil pairing, via Remark 1.109. Because e_2 is linear and Galois-invariant, we any $T \in E[2]$ produces a map $e_2(-,T)\colon E[2] \to \mu_2$, so any $P \in E(K)/2E(K)$ functorially produces a 1-cocycle

$$\sigma \mapsto e_2(\delta(P)(\sigma),T)$$

in $\mathrm{H}^1(K;\mu_2)$, which must be identified with $\delta_K(b(P,T))$ for some uniquely defined $b(P,T) \in K^\times/K^{\times 2}$. In fact, by Remark 1.109, we see that $e_2(-,(a_i,0))\colon E[2] \to \mu_2$ is projection onto the ith coordinate of $E[2] \hookrightarrow H$. Thus, $b(P,(a_i,0))$ will continue to be the ith coordinate in $\mathrm{H}^1(K;H) \hookrightarrow \left(K^\times/K^{\times 2}\right)^3$.

We thus see that we will be content with computing $b(P,T)$ for $T \in E[2] \setminus \{\infty\}$; say $T := (a_i,0)$. To begin, fix some $Q \in E(K^{\mathrm{sep}})$ with $2Q = P$, and fix some $\beta \in \overline{K}$ with $\beta^2 = b(P,T)$. On one hand, we see that $\delta_K(b(P,T))(\sigma) = \sigma\beta/\beta$. On the other hand, choosing f and g as in Example 1.87, we see that

$$e_2(\delta(P)(\sigma),T) = \frac{g(X+\sigma Q - Q)}{g(X)}.$$

Now, provided that $g(Q) \neq 0$, which is equivalent to $g(Q)^2 = f(2Q) = f(P) \neq 0$, we may plug in Q to see $e_2(\delta(P)(\sigma), T) = g(\sigma Q)/g(Q)$, so

$$\frac{\sigma g(Q)}{g(Q)} = \frac{\sigma\beta}{\beta}.$$

Thus, $\delta_K(g(Q)) = \delta_K(\beta)$, so $g(Q)$ and β represent the same class in $K^\times/K^{\times 2}$. Accordingly, up to squares, we can compute $b(P,T)$ as $\beta^2 = g(Q)^2$, which is $f(2Q)$ by construction of the Weil pairing, which is $f(P)$ (as usual, provided this makes sense).

We now recall that $f(x) = x - a_i$, so we find that the ith coordinate of $\delta(x,y)$ will be $x - a_i$ whenever $a_i \neq 0$. To finish up the calculation, we note that $\delta(\infty) = (1,1,1)$ because identities go to identities, and the remaining ith coordinate of $\delta(a_i, 0)$ can be computed from the other two because all three coordinates must multiply to be a square. ■

Corollary 1.111. Fix an elliptic curve E over a field K which is the projective closure of $y^2 = (x-a_1)(x-a_2)(x-a_3)$. Identifying $E[2]$ with the trace-zero hyperplane $H \subseteq \mu_2^{\oplus 3}$, a triple $(\alpha,\beta,\gamma) \in \mathrm{H}^1(K; H)$ is in the image of the boundary map from $E(K)/2E(K)$ if and only if the conic $T_{(\alpha,\beta,\gamma)} \subseteq \mathbb{P}(1,1,1,2,1)$ cut out by the affine 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. (Namely, the coordinates u, v, and w have weight 1, and x has weight 2.)

Proof. Let's begin by showing that admitting a solution implies being in the image of δ. In projective coordinates $[U : V : W : X : Z]$, the equations are

$$\begin{cases} \alpha U^2 = X - a_1 Z^2, \\ \beta V^2 = X - a_2 Z^2, \\ \gamma W^2 = X - a_3 Z^2. \end{cases}$$

The points at infinity occur with $Z = 0$, where we see that we have a point if and only if $\alpha U^2 = \beta V^2 = \gamma W^2$, which amounts to requiring that $(\alpha,\beta,\gamma) = (1,1,1)$ in $\left(K^\times/K^{\times 2}\right)^3$.

Otherwise, we are allowed to work in affine coordinates, setting $Z = 1$. The idea is to use a solution to construct an explicit pre-image, using the calculation of Proposition 1.110. The presence of a solution means that $\alpha(x-a_1)$, $\beta(x-a_2)$, and $\gamma(x-a_3)$ are all squares, which in turn means that we can find y for which

$$y^2 = (x-a_1)(x-a_2)(x-a_3).$$

We now see that (α,β,γ) is the image of (x,y) along δ: this is immediately apparent if $y \neq 0$ (i.e., $x \notin \{a_1, a_2, a_3\}$), but even if (say) $(x,y) = (a_1, 0)$, then $\beta(x-a_2)$ and $\gamma(x-a_3)$ are nonzero squares and thus uniquely determine $\alpha \in K^\times/K^{\times 2}$, so we still find that $(\alpha,\beta,\gamma) = \delta(a_1, 0)$. (A similar argument works for $(x,y) = (a_2, 0)$ and $(x,y) = (a_3, 0)$—one just has to rearrange the indices.)

This argument also tells us how to show that being in the image of δ implies that we admit a solution.

- We handled $\delta(\infty)$ in the first paragraph.
- For $(x,y) \in E(K)$ with $y \neq 0$, we see that $\delta(x,y) = (x-a_1, x-a_2, x-a_3)$, so $T_{\delta(x,y)}$ admits the solution $(u,v,w,x) = (1,1,1,x)$.
- For the remaining points (x,y) with $y = 0$, it is by symmetry enough to only handle $(x,y) = (a_1, 0)$. Then $\delta(x,y) = (\alpha,\beta,\gamma)$ has $\beta = a_1 - a_2$ and $\gamma = a_1 - a_3$, so $T_{\delta(x,y)}$ admits the solution $(u,v,w,x) = (0,1,1,a_1)$. ■

Remark 1.112. Here is a more geometric argument for Corollary 1.111. To understand the image of this map δ, it is equivalent to understand the kernel of the next map in the long exact sequence, which is

$$\mathrm{H}^1(K; E[2]) \to \mathrm{H}^1(K; E)[2].$$

Now, $\mathrm{H}^1(K; E)$ classifies principal homogeneous spaces [Sil09, Section X.3], which are trivial if and only if they admit a K-rational point (after all, principal homogeneous spaces for E are twists of E). Thus, it is enough to check that the principal homogeneous space associated to the triple (α, β, γ) admits a K-rational point, but one can check that this principal homogeneous space is exactly the conic $T_{(\alpha,\beta,\gamma)}$!

While we're here, we give some general remarks for how big these groups should be. In the case of 2-descent, one can get away with just doing Kummer theory.

Example 1.113. Fix an elliptic curve E over a number field K which is the projective closure of $y^2 = (x-a_1)(x-a_2)(x-a_3)$. Then

$$\dim_{\mathbb{F}_2} E(K_v)/2E(K_v) = \begin{cases} 0 & \text{if } K_v = \mathbb{C}, \\ 1 & \text{if } K_v = \mathbb{R}, \\ 2 & \text{if } v \text{ is odd}, \\ 2 + [K_v : \mathbb{Q}_2] & \text{if } v \text{ is even.} \end{cases}$$

Proof. By Theorem 1.98, the image of $E(K_v)/2E(K_v) \to \mathrm{H}^1(K_v; E[2])$ should have dimension equal to

$$\frac{1}{2} \dim_{\mathbb{F}_2} \mathrm{H}^1(K_v; E[2]) = \dim_{\mathbb{F}_2} \mathrm{H}^1(K_v; \mu_2).$$

By Example A.4, we are left to compute $K_v^\times / K_v^{\times 2}$. In the archimedean cases, we directly see that $\mathbb{C}^\times/\mathbb{C}^{\times 2} = 1$ (because $\mathbb{C}$ is algebraically closed) and $\mathbb{R}^\times/\mathbb{R}^{\times 2} = \mathbb{R}^\times/\mathbb{R}^+ = \{\pm 1\}$.

Otherwise, we suppose that K is a finite extension of $\mathbb{Q}_p$, and we claim that

$$K_v^\times \cong \mathbb{Z} \times \mathbb{F}_v \times \mu_{p^\infty}(K_v) \times \mathcal{O}_v$$

as abelian groups. To begin, note $K_v^\times \cong \mathbb{Z} \times \mathcal{O}_v^\times$ by using the valuation; additionally, by modding out by $\mathfrak{p}_v$, we find that $\mathcal{O}_v^\times \cong \mathbb{F}_v \times (1 + \mathfrak{p}_v)$.

Now, recall that the exponential map $\exp\colon \mathfrak{p}_v \to (1+\mathfrak{p}_v)$ identifies open neighborhoods of the identity of K_v and $K_v^\times$, so it follows that $\mathcal{O}_v^\times$ is a finitely generated $\mathcal{O}_v$-module. Because $\mathcal{O}_v$ is a principal ideal domain, it follows that $\mathcal{O}_v^\times$ is isomorphic to its torsion times its free part. The free part of $\mathcal{O}_v^\times$ has rank 1 because the exponential map identifies a finite-index open subgroup with $\mathcal{O}_v$. Lastly, the torsion of $(1 + \mathfrak{p}_v)$ must be p-power (because $(1+\varpi)^n \equiv 1 + n\varpi \pmod{\mathfrak{p}_v^{2m}}$ for any $\varpi \in \mathfrak{p}^m$), and conversely, the p-power torsion of $K_v^\times$ all lives in $\mathcal{O}_v^\times$ by looking at the valuation and is in fact $1 \pmod{\mathfrak{p}_v}$ by looking $\pmod{\mathfrak{p}_v}$. The claim follows.

To complete the calculation, we write

$$\frac{K_v^\times}{K_v^{\times 2}} \cong \frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{F}_v^\times}{\mathbb{F}_v^{\times 2}} \times \frac{\mu_{p^\infty}(K_v)}{\mu_{p^\infty}(K_v)^2} \times \frac{\mathcal{O}_v}{2\mathcal{O}_v}.$$

Continuing, we note that the kernel and cokernel of the endomorphisms $2\colon \mathbb{F}_v^\times \to \mathbb{F}_v^\times$ and $2\colon \mu_{2^\infty}(K_v) \to \mu_{2^\infty}(K_v)$ have the same size, so we see

$$\dim_{\mathbb{F}_2} \frac{K_v^\times}{K_v^{\times 2}} \cong 1 + \dim_{\mathbb{F}_2} \mathbb{F}_v^\times[2] + \dim_{\mathbb{F}_2} \mu_{p^\infty}(K_v)[2] + \dim_{\mathbb{F}_2} \frac{\mathcal{O}_v}{2\mathcal{O}_v}.$$

We now have two cases.

- If v is odd, then $\mathbb{F}_v^\times[2] \cong \mathbb{Z}/2\mathbb{Z}$ and $\mu_{p^\infty}(K_v)[2] = 0$ and $\mathcal{O}_v/2\mathcal{O}_v = 0$. In total, we get 2 dimensions.
- If v is even, then $\mathbb{F}_v^\times[2] = 0$ and $\mu_{p^\infty}(K_v)[2] = \mu_2(K_v) = \{\pm 1\}$ and $\mathcal{O}_v/2\mathcal{O}_v \cong (\mathbb{Z}/2\mathbb{Z})^{[K_v:\mathbb{Q}_2]}$. In total, we get $2 + [K_v : \mathbb{Q}_2]$ dimensions. ∎

1.4.5 Congruent Number Elliptic Curves

We now return to the congruent number elliptic curves $E_d\colon y^2 = x(x-d)(x+d)$, where $d \in \mathbb{Z}$ is some squarefree positive integer. It turns out that E_d is a quadratic twist of $E_1\colon y^2 = x^3 - x$, and these elliptic curves have complex multiplication by $\mathbb{Z}[i]$. Importantly, the 2-torsion

$$E[2] = \{\infty, (0,0), (+d,0), (-d,0)\}$$

is fully defined over $\mathbb{Q}$. Here is a bit more about what is known.

Remark 1.114 (Birch–Stephens)**.** Fix a squarefree positive integer d. It is known that

$$\varepsilon(E_d/\mathbb{Q}) = \begin{cases} +1 & \text{if } d \equiv 1,2,3 \pmod 8, \\ -1 & \text{if } d \equiv 5,6,7 \pmod 8. \end{cases}$$

Furthermore, they computed

$$S_2(E_d/\mathbb{Q}) \equiv \begin{cases} 0 \pmod 2 & \text{if } d \equiv 1,2,3 \pmod 8, \\ 1 \pmod 2 & \text{if } d \equiv 5,6,7 \pmod 8. \end{cases}$$

They proved this using calculations of Selmer groups. We will show the following.

Theorem 1.115. Fix an odd positive prime integer $d = p$, and let E_p be the projective closure of $y^2 = x(x-p)(x+p)$. Then

$$S_2(E_p/\mathbb{Q}) = \begin{cases} 2 & \text{if } p \equiv 1 \pmod 8, \\ 0 & \text{if } p \equiv 3 \pmod 8, \\ 1 & \text{if } p \equiv 5,7 \pmod 8. \end{cases}$$

Remark 1.116. In the first case $p \equiv 1 \pmod 8$, it is possible to get both 0 and 2 for the Mordell–Weil rank. Indeed, for many small primes p, $\operatorname{rank} E_p(\mathbb{Q}) = 0$, but $\operatorname{rank} E_{41}(\mathbb{Q}) = 2$.

Remark 1.117. It has been verified by Heegner–Monsky that $p \equiv 5,7 \pmod 8$ implies $\operatorname{rank} E_p(\mathbb{Q}) = 1$. This requires the construction of non-torsion points, which uses Heegner points.

We are going to use 2-descent. As in Section 1.4.4, we identify $\mathrm{H}^1(K; E_d)$ with $\mathrm{H}^1(K; H)$. We begin with two technical calculations.

Lemma 1.118. Fix an odd positive squarefree integer d, and let E_d be the elliptic curve over $\mathbb{Q}$ which is the projective closure of $y^2 = x(x-d)(x+d)$. We will compute the image of $\delta_v\colon E_d(K_v)/2E_d(K_v) \to \mathrm{H}^1(K_v; H)$ for each place v.

(a) If $v \nmid 2d\infty$, then the image of δ_v consists of the triples (α, β, γ) such that $v(\alpha) = v(\beta) = v(\gamma) = 0$.

(b) The image of δ_v contains the triples

$$S := \{(1,1,1), (-1,-d,d), (d,2,2d), (-d,-2d,2)\}.$$

(c) If $v \mid d\infty$, then the image of δ_v is S.

(d) If $v = 2$, the image of δ_v is $\operatorname{span}(S \cup \{(1,5,5)\})$.

Proof. We show the parts in sequence.

(a) If $v \nmid 2d\infty$, then E_d has good reduction at the finite place v, so by Lemma 1.73, the image of δ_v is $\mathrm{H}^1_{\mathrm{ur}}(K_v; H)$. The result now follows by looking coordinate-wise via Example 1.71.

(b) The given set S is precisely the image of $E_d[2]$. Indeed,

$$\begin{aligned}\delta_v(\infty) &= (1,1,1),\\ \delta_v(0,0) &= (-1,-d,d),\\ \delta_v(d,0) &= (d,2,2d),\\ \delta_v(-d,0) &= (-d,-2d,2).\end{aligned}$$

(c) If $v = \infty$, then we have a linearly independent set $\{(-1,-1,+1)\}$, which spans the image of δ_v by Example 1.113. Similarly, if $v \mid d$, then we have a linearly independent set $\{(-1,-d,d),(d,2,2d)\}$ (because d is squarefree), which spans the image of δ_v by Example 1.113.

(d) You may do this for the homework! ■

We will also need the following technical result.

> **Lemma 1.119.** Let $T \subseteq \mathbb{P}^n_{\mathbb{Z}}$ be a smooth projective conic. If T admits solutions in $\mathbb{Q}_v$ for all but one place v_0, then T admits solutions in $\mathbb{Q}_{v_0}$ as well.

Proof. You may show this for the homework! ■

We now proceed with the proof of Theorem 1.115.

Proof of Theorem 1.115. We have identified $\mathrm{H}^1(K; E_d[2])$ with the trace-zero hyperplane of $\left(K^\times/K^{\times 2}\right)^3$. Now, let $\mathcal{L}_v \subseteq \left(K^\times/K^{\times 2}\right)^3$ be the corresponding local condition of the Selmer group at the place v, as computed in Lemma 1.118. Thus,

$$\mathrm{Sel}_2(E_d/\mathbb{Q}) \cong \{(\alpha,\beta,\gamma) : (\alpha,\beta,\gamma) \in \mathcal{L}_v \text{ for all } v\}.$$

The local conditions $v \nmid 2d\infty$ show that α, β, and γ should (up to squares) be supported on primes dividing $2d$; adjusting these rationals up to squares, we may assume that they are all integers dividing $2d$.

Now, we are not actually interested in computing the Selmer group on the nose. Instead, we would like to compute the (dimension of the) quotient by $E[2]$. Well, examining the local condition at ∞, we see that taking a quotient by the subgroup generated by $\delta(0,0) = (-1,-d,d)$ corresponds exactly to assuming (α,β,γ) are all positive—a priori, none are negative or exactly α and β are negative. Similarly, examining the local condition at 2, we see that taking a quotient by the subgroup generated by $\delta(d,0) = (d,2,2d)$ corresponds exactly to assuming that (α,β,γ) are all odd. Thus,

$$\frac{\mathrm{Sel}_2(E_d/\mathbb{Q})}{E[2]} \subseteq \left\{(\alpha,\beta,\gamma) \in \mathbb{Z}^3_{>0} : \alpha,\beta,\gamma \mid d, \alpha\beta\gamma \text{ is square}\right\}.$$

By Lemma 1.118, all triples (α,β,γ) in the above set are automatically in the local condition at a place $v \nmid 2d$, so there are only finitely many more places to check.

Only now do we use the fact that $d = p$ is prime. By Lemma 1.119 combined with Corollary 1.111, we are allowed to avoid checking $(\alpha,\beta,\gamma) \in \mathcal{L}_{v_0}$ for a single place v_0; we choose $v_0 = 2$, so it only remains to check the place at the prime p. In other words, we are interested in which of the triples

$$\{(1,1,1),(1,p,p),(p,1,p),(p,p,1)\}$$

live in $\mathcal{L}_p = \{(1,1,1),(-1,-p,p),(p,2,2p),(-p,-2p,2)\}$. (Note that the elements of $\mathcal{L}_p$ are only defined up to squares!) We handle these one at a time.

- We see that $(1,1,1) \in \mathcal{L}_p$ always.

- By examining valuations (even $\pmod 2$), we see that $(1, p, p) \in \mathcal{L}_p$ if and only if it is $(-1, -p, p)$ up to squares, which is equivalent to -1 being square, which is equivalent to $p \equiv 1 \pmod 4$.
- By examining valuations, we see that $(p, 1, p) \in \mathcal{L}_p$ if and only if it is $(p, 2, 2p)$ up to squares, which is equivalent to 2 being square, which is equivalent to $p \equiv \pm 1 \pmod 8$.
- Lastly, we similarly find that $(p, p, 1) \in \mathcal{L}_p$ if and only if it is $(-p, -2p, p)$ up to squares, which is equivalent to -1 and 2 being squares, which is equivalent to $p \equiv 1 \pmod 8$.

Totaling the above cases completes the proof. ■

Corollary 1.120. Fix an odd positive squarefree integer d, and let E_d be the projective closure of $y^2 = x(x-d)(x+d)$. Let $\nu(d)$ be the number of positive integers of d. Then

$$S_2(E_d) \le 2\nu(d).$$

Proof. The proof of Theorem 1.115 shows that

$$\frac{\operatorname{Sel}_2(E_d/\mathbb{Q})}{E[2]} \subseteq \left\{(\alpha, \beta, \gamma) \in \mathbb{Z}^3_{>0} : \alpha, \beta, \gamma \mid d, \alpha\beta\gamma \text{ is square}\right\}.$$

The right-hand side has a basis over $\mathbb{F}_2$ given by (p, q, pq) where p and q are primes dividing d, so this space has dimension $2\nu(n)$. ■

1.5 September 25

Today we continue. We began class by saying a bit more about Theorem 1.115, which I have placed in yesterday's notes.

1.5.1 The Selmer Group of the Dual

As usual, fix a number field K, and let M be a Galois module. We would like to compare the Selmer group of M and its dual M^*.

Notation 1.121. Fix a number field K and a finite discrete Galois module M with local conditions $\mathcal{L}$. Then the dual module M^* admits dual local conditions $\mathcal{L}^* := \{\mathcal{L}_v^*\}_v$ defined by taking the annihilator along the duality of Theorem 1.62.

Remark 1.122. To check that $\mathcal{L}^*$ actually assembles into a local condition, we need to check that $\mathcal{L}_v^* = \mathrm{H}^1_{\mathrm{ur}}(K_v; M^*)$ for all but finitely many places v. Well, M is unramified at all but finitely places v (by Remark 1.77), so M^* is as well, and whenever $\mathcal{L}_v = \mathrm{H}^1_{\mathrm{ur}}(K_v; M)$, Proposition 1.72 tells us that the annihilator of $\mathcal{L}_v$ is

$$\mathcal{L}_v^* = \mathrm{H}^1_{\mathrm{ur}}(K_v; M^*).$$

Remark 1.123. Taking annihilators is inclusion-reversing: if $\mathcal{L} \subseteq \mathcal{L}'$, then we can see place-by-place that $(\mathcal{L}')^* \subseteq \mathcal{L}^*$.

Example 1.124. Fix an elliptic curve E over a number field K. Given a prime p, we let $\mathcal{L}_v \subseteq \mathrm{H}^1(K_v; E[p])$ be the image of $E(K_v)/mE(K_v)$. Then the Weil pairing provides an isomorphism $E[p] \cong E[m]^*$ of Galois modules (see Lemma 1.88). Furthermore, this isomorphism makes $\mathcal{L}_v$ a maximal isotropic subspace by Proposition 1.96, so $\mathcal{L}_v$ is its own orthogonal complement; we conclude $\mathcal{L}$ is identified with $\mathcal{L}^*$.

For our main result, we will want to compare the Selmer group of M and M^*. To state this appropriately, we will want the following exact sequence.

Remark 1.125. For any inclusion of $\mathcal{L} \subseteq \mathcal{L}'$ of local conditions, we claim that there is a left-exact sequence

$$0 \to \mathrm{Sel}_{\mathcal{L}}(M) \to \mathrm{Sel}_{\mathcal{L}'}(M) \to \prod_v \frac{\mathcal{L}'_v}{\mathcal{L}_v}.$$

The left map is induced by pulling back the inclusion $\prod_v \mathcal{L}_v \hookrightarrow \prod_v \mathcal{L}'_v$ along $\mathrm{H}^1(K; M) \to \mathrm{H}^1(\mathbb{A}_K; M)$, and the right map is the canonical projection. The left map is injective by construction, and we are exact in the middle by definition of these Selmer groups: a class $c \in \mathrm{Sel}_{\mathcal{L}'}(M)$ lives in $\mathrm{Sel}_{\mathcal{L}}(M)$ if and only if $\mathrm{loc}_v\, c \in \mathcal{L}_v$ for each place v.

Remark 1.126. An equivalent way to view Remark 1.125 is to say that the square

$$\begin{tikzcd} \mathrm{Sel}_{\mathcal{L}}(M) \arrow[r] \arrow[d] & \mathrm{Sel}_{\mathcal{L}'}(M) \arrow[d] \\ \prod_v \mathcal{L}_v \arrow[r] & \prod_v \mathcal{L}'_v \end{tikzcd}$$

is a pullback square. Indeed, this is also equivalent to saying that an element $c \in \mathrm{Sel}_{\mathcal{L}'}(M)$ in fact comes from $\mathrm{Sel}_{\mathcal{L}}(M)$ if and only if $\mathrm{loc}_v\, c \in \mathcal{L}_v$ for each place v.

Theorem 1.127. Fix a number field K and a Galois module M with local conditions $\mathcal{L} \subseteq \mathcal{L}'$. Then the image of the two canonical maps

$$\mathrm{Sel}_{\mathcal{L}'}(M) \to \prod_v \frac{\mathcal{L}'_v}{\mathcal{L}_v} \qquad \text{and} \qquad \mathrm{Sel}_{\mathcal{L}^*}(M^*) \to \prod_v \frac{\mathcal{L}^*_v}{(\mathcal{L}')^*_v}$$

are orthogonal complements of each other with respect to the pairing $\langle -, - \rangle := \sum_v \langle -, - \rangle_v$, where $\langle -, - \rangle_v$ is induced by local Tate duality (Theorem 1.62).

Remark 1.128. Let's explain why the given pairing is even well-defined. By Theorem 1.62, we see that $\mathcal{L}_v$ and $\mathcal{L}^*_v$ are annihilators of each other (and similar for $(\mathcal{L}')^*$), so we can descend the local pairing to a well-defined perfect pairing

$$\frac{\mathcal{L}'_v}{\mathcal{L}_v} \times \frac{\mathcal{L}^*_v}{(\mathcal{L}')^*_v} \to \mathbb{Q}/\mathbb{Z}.$$

In order to be able to sum this pairing over all v, we note that $\mathcal{L}_v = \mathcal{L}'_v = \mathrm{H}^1_{\mathrm{ur}}(K_v; M)$ for all but finitely many places v, so the product $\prod_v \mathcal{L}'_v/\mathcal{L}_v$ is actually a finite product; similarly, the product $\prod_v \mathcal{L}^*_v/(\mathcal{L}')^*_v$ is also finite.

Proof. Our exposition follows [Rub00, Theorem 1.7.3]. We will use the middle three terms of the nine-term exact sequence arising from Pitou–Tate global duality, which asserts the following.

Theorem 1.129 (Pitou–Tate)**.** Fix a number field K and a finite set of places Σ, and let K_Σ be the maximal Galois extension unramified at Σ. For any finite discrete Galois module M, there is an exact sequence

$$\mathrm{H}^1(K_\Sigma/K; M) \overset{\mathrm{loc}}{\to} \bigoplus_{v \in \Sigma} \mathrm{H}^1(K_v; M) \overset{\mathrm{loc}^\vee}{\to} \mathrm{H}^1(K_\Sigma/K; M^*)^\vee,$$

where $(-)^\vee := \mathrm{Hom}(-, \mathbb{Q}/\mathbb{Z})$.

For a proof of this (difficult!) theorem, we refer to [Mil06, Theorem I.4.10], but the reader is warned that the notation is rather dense there.

We now proceed with our argument. For brevity, let π_M denote the map $\operatorname{Sel}_{\mathcal{L}^\Sigma}(M) \to \prod_v \mathcal{L}'_v/\mathcal{L}_v$, and we define π_{M^*} analogously. By symmetry of the situation (namely, we may replace M with M^*), it is enough to show that

$$(\operatorname{im}\pi_{M^*})^\perp \stackrel{?}{=} \operatorname{im}\pi_M.$$

In other words, we would like to show that any $c \in \prod_v \mathcal{L}'_v/\mathcal{L}_v$ has $c \in \operatorname{im}\pi_M$ if and only if $\langle c, \pi_{M*}\widetilde{c}^*\rangle = 0$ for all $\widetilde{c}' \in \operatorname{Sel}_{\mathcal{L}^*}(M^*)$. This is then equivalent to saying that the sequence

$$\operatorname{Sel}_{\mathcal{L}'}(M) \stackrel{\pi_M}{\to} \prod_v \frac{\mathcal{L}'_v}{\mathcal{L}_v} \stackrel{\pi_{M^*}^\vee}{\to} \operatorname{Sel}_{\mathcal{L}^*}(M^*)^\vee$$

is exact, where $(-)^\vee := \operatorname{Hom}_{\mathbb{Z}}(-, \mathbb{Q}/\mathbb{Z})$ is the Pontryagin dual; here, the right map has identified $\mathcal{L}'_v/\mathcal{L}_v$ with $(\mathcal{L}^*_v/(\mathcal{L}')^*_v)^\vee$ via Theorem 1.62.

We now focus on the exactness of this sequence directly. We will have two cases: we start by handling large $\mathcal{L}'$ and small $\mathcal{L}$, and then we make a reduction to the general case. Let's begin with large $\mathcal{L}'$. Let Σ be a finite set of places where $\mathcal{L}'_v \neq \mathrm{H}^1_{\mathrm{ur}}(K_v; M)$; for example, Σ includes all archimedean places and all places where M fails to be unramified. By enlarging $\mathcal{L}$, we are allowed to assume that $\mathcal{L}'_v = \mathrm{H}^1(K_v; M)$ for $v \in \Sigma$. Dually, we possibly expand Σ (and so expand $\mathcal{L}'$) so that $\mathcal{L}_v = \mathrm{H}^1_{\mathrm{ur}}(K_v; M)$ for $v \notin \Sigma$ and $\mathcal{L}_v = 0$ for $v \in \Sigma$. We now have two steps.

1. The key claim is that

$$\operatorname{Sel}_{\mathcal{L}'}(M) \stackrel{?}{=} \mathrm{H}^1(K_\Sigma/K; M) \qquad \text{and} \qquad \operatorname{Sel}_{\mathcal{L}^*}(M^*) = \mathrm{H}^1(K_\Sigma/K; M^*).$$

   By symmetry, it is enough to just handle the left equality. Well, $\operatorname{Sel}_{\mathcal{L}'}(M)$ consists of the classes c in $\mathrm{H}^1(K; M)$ which localize to unramified classes outside Σ. By the Inflation–Restriction exact sequence (Proposition 1.49), this is equivalent to asking for c to vanish in $\mathrm{H}^1(I_v; M)$ for each inertia subgroup I_v for $v \notin \Sigma$. Taking the union of these I_vs, it is equivalent to ask for c to vanish in $\mathrm{H}^1(K_\Sigma; M)$, which by Proposition 1.49 (again!) is equivalent to c coming from $\mathrm{H}^1(K_\Sigma/K; M)$.

2. We now apply Theorem 1.129, which provides us with an exact sequence

$$\operatorname{Sel}_{\mathcal{L}'}(M) \stackrel{\pi_M}{\to} \bigoplus_{v\in\Sigma} \mathrm{H}^1(K_v; M) \stackrel{\pi_{M^*}^\vee}{\to} \operatorname{Sel}_{\mathcal{L}^*}(M^*)^\vee.$$

   This is the desired exact sequence after replacing $\bigoplus_{v\in\Sigma} \mathrm{H}^1(K_v; M)$ with $\prod_v \mathcal{L}'_v/\mathcal{L}_v$, which is legal because

$$\frac{\mathcal{L}'_v}{\mathcal{L}_v} = \begin{cases} \mathrm{H}^1(K_v; M) & \text{if } v \in \Sigma, \\ 0 & \text{otherwise.} \end{cases}$$

We now turn to smaller $\mathcal{L}'$ and larger $\mathcal{L}$.

1. We handle smaller $\mathcal{L}'$. Namely, suppose we have proven the statement for local conditions $\mathcal{L} \subseteq \mathcal{L}'_0$ (with $\mathcal{L}$ small and $\mathcal{L}'_0$ large), and we would like to show it for $\mathcal{L} \subseteq \mathcal{L}'$, where $\mathcal{L}'$ is between $\mathcal{L}$ and $\mathcal{L}'_0$. We note that we have a commutative diagram

$$\begin{tikzcd} \operatorname{Sel}_{\mathcal{L}'}(M) \arrow[r] \arrow[d, hook] & \prod_v \frac{\mathcal{L}'_v}{\mathcal{L}_v} \arrow[r] \arrow[d, hook] & \operatorname{Sel}_{\mathcal{L}^*}(M^*)^\vee \arrow[d, equal] \\ \operatorname{Sel}_{\mathcal{L}'_0}(M) \arrow[r] & \prod_v \frac{\mathcal{L}'_{0v}}{\mathcal{L}_v} \arrow[r] & \operatorname{Sel}_{\mathcal{L}^*}(M^*)^\vee \end{tikzcd}$$

   where all vertical arrows are injective, and the bottom row is exact. By noting that limits commute with limits (or a direct diagram chase), it is enough to note that the left square is a pullback square, which follows from Remark 1.126.

2. We handle larger $\mathcal{L}$. Namely, suppose we have proven the statement for local conditions $\mathcal{L}_0 \subseteq \mathcal{L}'$ (with $\mathcal{L}_0$ small), and we would like to show it for $\mathcal{L} \subseteq \mathcal{L}'$, where $\mathcal{L}$ is between $\mathcal{L}_0$ and $\mathcal{L}'$. Well, replacing M with M^* and dualizing all local conditions (and taking the Pontryagin dual of the desired exact sequence) allows us to repeat the argument of the previous case. ■

Example 1.130. Given local conditions $\mathcal{L} \subseteq \mathcal{L}'$ of M, then Theorem 1.127 shows that one of the two maps

$$\operatorname{Sel}_{\mathcal{L}'}(M) \to \prod_v \frac{\mathcal{L}'_v}{\mathcal{L}_v} \qquad \text{and} \qquad \operatorname{Sel}_{\mathcal{L}^*}(M^*) \to \prod_v \frac{\mathcal{L}^*_v}{(\mathcal{L}')^*_v}$$

being surjective implies that the other one is zero. Indeed, the pairing between these two groups is the (finite) sum of perfect pairings and hence perfect (see Remark 1.128), so the orthogonal complement of a full space is zero.

1.5.2 Modifying the Local Condition

For our application, we will want some way to build inclusions of local conditions.

Definition 1.131 (strict, relaxed)**.** Fix a number field K and a finite discrete Galois module M with local conditions $\mathcal{L}$. For a finite set of places Σ, we define the *strict local conditions* $\mathcal{L}_\Sigma$ and the *relaxed local conditions* $\mathcal{L}^\Sigma_v$ by

$$(\mathcal{L}_\Sigma)_v := \begin{cases} \mathcal{L}_v & \text{if } v \notin \Sigma, \\ 0 & \text{if } v \in \Sigma, \end{cases} \qquad \text{and} \qquad \left(\mathcal{L}^\Sigma\right)_v := \begin{cases} \mathcal{L}_v & \text{if } v \notin \Sigma, \\ \mathrm{H}^1(K_v; M) & \text{if } v \in \Sigma. \end{cases}$$

If Σ is a singleton $\{v_0\}$, we may abuse notation and write $\mathcal{L}_{v_0}$ and $\mathcal{L}^{v_0}$ for the strict and local conditions, respectively.

Remark 1.132. Of course, $\mathcal{L}^\Sigma$ and $\mathcal{L}_\Sigma$ continue to be local conditions because all but finitely many v have $v \notin \Sigma$ and also $\mathcal{L}_v = \mathrm{H}^1_{\mathrm{ur}}(K_v; M)$.

Example 1.133. We claim that $(\mathcal{L}_\Sigma)^* = (\mathcal{L}^*)^\Sigma$. Indeed, for any $v \notin \Sigma$, both sides are $\mathcal{L}^*_v$; and for any $v \in \Sigma$, both sides are $\{0\}^* = \mathrm{H}^1(K_v; M^*)$. Similarly, we see that $(\mathcal{L}^\Sigma)^* = (\mathcal{L}^*)_\Sigma$.

Example 1.134. Fix a finite set of places Σ. If the map $\operatorname{Sel}_{\mathcal{L}}(M) \to \bigoplus_{v\in\Sigma} \mathcal{L}_v$ is surjective, then we claim that the map

$$\operatorname{Sel}_{(\mathcal{L}^*)^\Sigma}(M^*) \to \bigoplus_{v\in\Sigma} \frac{\mathrm{H}^1(K_v; M^*)}{\mathcal{L}^*_v}$$

vanishes. Indeed, this follows from Example 1.130 (and Example 1.133) using the local conditions $\mathcal{L}_\Sigma \subseteq \mathcal{L}$.

For our application, we will explain how a Selmer rank changes as we modify the local condition "one place at a time." For later use, we pick up two technical lemmas, which find their application in the next subsection.

Lemma 1.135. Fix an elliptic curve E over a number field K. Choose a prime p, and set $\mathcal{L}$ to be a local condition on $E[p]$ with $\mathcal{L} = \mathcal{L}^*$. Letting Σ be the singleton of a place v_0, we have

$$\dim_{\mathbb{F}_p} \operatorname{Sel}_{\mathcal{L}^\Sigma}(E[p]) - \dim_{\mathbb{F}_p} \operatorname{Sel}_{\mathcal{L}_\Sigma}(E[p]) = \frac{1}{2} \dim_{\mathbb{F}_p} \mathrm{H}^1(K_{v_0}; E[p]).$$

Proof. Set $M := E[p]$ to avoid distraction. The point is to use Example 1.124, which explains that the Weil pairing provides an isomorphism $M \cong M^*$ of Galois modules, and we are given that it also induces an identification $\mathcal{L} \cong \mathcal{L}^*$ of local conditions.

Remark 1.125 provides us with the exact sequences

$$0 \to \operatorname{Sel}_{\mathcal{L}_\Sigma}(M) \to \operatorname{Sel}_{\mathcal{L}^\Sigma}(M) \to \mathrm{H}^1(K_{v_0}; M),$$

and

$$0 \to \operatorname{Sel}_{(\mathcal{L}^*)_\Sigma}(M^*) \to \operatorname{Sel}_{(\mathcal{L}^*)^\Sigma}(M^*) \to \mathrm{H}^1(K_{v_0}; M^*),$$

and Theorem 1.127 tells us that the images in the rightmost terms are orthogonal complements (where we have silently used Example 1.133). Now, via the duality $M \cong M^*$ discussed in the previous paragraph, the second exact sequence is identified with the first one. We conclude that

$$\frac{\operatorname{Sel}_{\mathcal{L}^\Sigma}(M)}{\operatorname{Sel}_{\mathcal{L}_\Sigma}(M)} \subseteq \mathrm{H}^1(K_{v_0}; M)$$

is the orthogonal complement of itself, so the result follows. ■

Example 1.136. In the sequel, we will typically take $\mathcal{L}$ to be the local condition $\mathcal{L}_v := E(K_v)/pE(K_v)$, which is self-dual as discussed in Proposition 1.96.

Lemma 1.137. Fix an elliptic curve E over a number field K. Choose a prime P, and set $\mathcal{L}$ to be a local condition on $E[p]$ with $\mathcal{L} = \mathcal{L}^*$. Further, for a given place v_0, let $\mathcal{L}'_{v_0} \subseteq \mathrm{H}^1(K_{v_0}; E[p])$ be some self-dual subspace disjoint from $\mathcal{L}_{v_0}$, and extend it to the local condition $\mathcal{L}'$ given by $\mathcal{L}'_v = \mathcal{L}_v$ for $v \neq v_0$.

(a) If $\operatorname{Sel}_{\mathcal{L}}(E[p]) \to \mathrm{H}^1(K_{v_0}; E[2])$ vanishes, then

$$\dim_{\mathbb{F}_p} \operatorname{Sel}_{\mathcal{L}'}(E[p]) = \dim_{\mathbb{F}_p} \operatorname{Sel}_{\mathcal{L}}(E[p]) + \frac{1}{2} \dim_{\mathbb{F}_2} \mathrm{H}^1(K_{v_0}; E[p]).$$

(b) If $\operatorname{Sel}_{\mathcal{L}}(E[p]) \to \mathrm{H}^1(K_{v_0}; E[2])$ surjects onto $\mathcal{L}_{v_0}$, then

$$\dim_{\mathbb{F}_p} \operatorname{Sel}_{\mathcal{L}}(E[p]) = \dim_{\mathbb{F}_p} \operatorname{Sel}_{\mathcal{L}'}(E[p]) - \frac{1}{2} \dim_{\mathbb{F}_2} \mathrm{H}^1(K_{v_0}; E[p]).$$

Proof. All the hypotheses will be used, though much care will be required. Set $M := E[p]$ and $\Sigma := \{v_0\}$ for brevity. The main point is to chase around a pullback square. Because $\mathcal{L}_{v_0}$ and $\mathcal{L}'_{v_0}$ are disjoint maximal isotropic subspaces, we see that $\mathcal{L} + \mathcal{L}' = \mathcal{L}^\Sigma$ and $\mathcal{L} \cap \mathcal{L}' = \mathcal{L}_\Sigma$. Pulling back the intersection along $\mathrm{H}^1(K; M) \to \mathrm{H}^1(\mathbb{A}_K; M)$ produces the pullback square

$$\begin{tikzcd} \operatorname{Sel}_{\mathcal{L}_\Sigma}(M) \arrow[r] \arrow[d] \arrow[dr, phantom, "\lrcorner", very near start] & \operatorname{Sel}_{\mathcal{L}'}(M) \arrow[d] \\ \operatorname{Sel}_{\mathcal{L}}(M) \arrow[r] & \operatorname{Sel}_{\mathcal{L}^\Sigma}(M) \end{tikzcd} \tag{1.1}$$

of intersections inside $\mathrm{H}^1(K; M)$. We now show (a) and (b) separately.

(a) The exactness of

$$0 \to \operatorname{Sel}_{\mathcal{L}_\Sigma}(M) \to \operatorname{Sel}_{\mathcal{L}}(M) \to \mathcal{L}_\ell$$

from Remark 1.125 implies that the inclusion $\operatorname{Sel}_{\mathcal{L}_\Sigma}(M) \to \operatorname{Sel}_{\mathcal{L}}(M)$ is an isomorphism. Thus, the left arrow of (1.1) is an isomorphism, so the right arrow is also an isomorphism, and the result follows from Lemma 1.135.

(b) We are given that $\operatorname{Sel}_{\mathcal{L}}(M) \to \mathcal{L}_\ell$ is surjective, so Example 1.134 implies that the exact sequence

$$0 \to \operatorname{Sel}_{\mathcal{L}}(M) \to \operatorname{Sel}_{\mathcal{L}^\Sigma}(M) \to \frac{\mathrm{H}^1(K_{v_0}; M)}{\mathcal{L}_{v_0}}$$

of Remark 1.125 maps to 0 at the end, so the inclusion $\operatorname{Sel}_{\mathcal{L}}(M) \to \operatorname{Sel}_{\mathcal{L}^\Sigma}(M)$ is an isomorphism. (We are silently using $\mathcal{L} = \mathcal{L}^*$ and Example 1.133.) Thus, the bottom arrow of (1.1) is an isomorphism, so the top arrow is also an isomorphism. The claim now follows from Lemma 1.135. ∎

1.5.3 Application to Congruent Number Elliptic Curves

As an application, we compare 2-Selmer ranks of congruent number elliptic curves.

Lemma 1.138. Fix an odd positive squarefree integer d and an odd prime ℓ not dividing d, and let E and E' be the projective closures of $y^2 = x(x-d)(x+d)$ and $y^2 = x(x-d\ell)(x+d\ell)$, respectively. Further, let $\mathcal{L}$ and $\mathcal{L}'$ be the associated local conditions on $\mathrm{H}^1(\mathbb{Q}; H)$, where $H \subseteq \mu_2^{\oplus 3}$ is the trace-zero hyperplane.

(a) The local conditions $\mathcal{L}$ and $\mathcal{L}'$ are self-dual.

(b) The group $\mathcal{L}_\ell \cap \mathcal{L}'_\ell$ is trivial.

(c) We have $\mathcal{L}_v = \mathcal{L}'_v$ for all $v \neq \ell$ if and only if $\ell \equiv 1 \pmod 8$ and $\ell \in \mathbb{Q}_p^{\times 2}$ for each prime $p \mid d$.

Proof. Quickly, (a) follows from Proposition 1.96. For (b), we use Lemma 1.118. Indeed, every nontrivial triple (α, β, γ) in $\mathcal{L}'_\ell$ has $1 \in \{v(\alpha), v(\beta), v(\gamma)\}$ while $\mathcal{L}_\ell$ exclusively has triples (α, β, γ) for which $v(\alpha) = v(\beta) = v(\gamma) = 0$. Thus, the only triple in the intersection is the trivial one. While we're here, we remark that we also have $\mathcal{L}_\ell + \mathcal{L}'_\ell = \mathrm{H}^1(\mathbb{Q}_\ell; H)$ because each subspace has half the dimension of the total (by Proposition 1.96).

We now show (c) by casework, going place-by-place; we will use Lemma 1.118 freely throughout.

- For $v \nmid 2d\ell\infty$, we see that $\mathcal{L}_v$ and $\mathcal{L}'_v$ both contain the triples (α, β, γ) with $v(\alpha) = v(\beta) = v(\gamma) = 0$.
- For $v = \infty$, both are the same.
- For finite $v = p$ with $p \mid d$, we note that we certainly have $\#\mathcal{L}_v = \#\mathcal{L}'_v$, so it is enough to just get an inclusion. Comparing the two $\mathbb{F}_2$-subspaces, it is enough to check $\{(-1, -d\ell, d\ell), (d\ell, 2, 2d\ell)\} \subseteq \mathcal{L}_p$, which is equivalent to having $\{(1, \ell, \ell), (\ell, 1, \ell)\} \subseteq \mathcal{L}_p$. This inclusion forces $(1, \ell, \ell) = (1, 1, 1)$ by considering valuations, so ℓ must be a square in $\mathbb{Q}_p^\times$; conversely, if ℓ is a square, then $(1, \ell, \ell) = (\ell, 1, \ell) = (1, 1, 1)$.
- Lastly, for $v = 2$, it is once again enough to achieve the inclusion $\{(1, \ell, \ell), (\ell, 1, \ell)\} \subseteq \mathcal{L}_2$. This time, considering valuations (and the fact that -1 is not a square) implies that $(1, \ell, \ell)$ is either $(1, 1, 1)$ or $(1, 5, 5)$, which means that either ℓ or 5ℓ is a square in $\mathbb{Q}_2$. But if 5ℓ is a square, then $(\ell, 1, \ell) \notin \mathcal{L}_2$, so we must instead have ℓ be a square. Of course, having ℓ be a square is also sufficient.

Combining the above cases completes the argument. ∎

Example 1.139. Let E' be the projective closure of $y^2 = x(x-\ell)(x+\ell)$, where ℓ is a prime equivalent to $1 \pmod 8$. Then we claim that $S_2(E') = 2$, thereby recovering some of Theorem 1.115. Indeed, let E be the projective closure of $y^2 = x(x-1)(x+1)$, and we know that $S_2(E) = 0$ by Corollary 1.120. In particular, it follows that $\operatorname{Sel}_2(E)$ is represented by the triples coming from $E[2]$, which are

$$\{(1,1,1), (-1,-1,1), (1,2,2), (-1,-2,2)\}.$$

Because $\ell \equiv 1 \pmod 8$, these all give the trivial class in $\mathrm{H}^1(\mathbb{Q}_\ell; H)$, so all parts of Lemma 1.138 are satisfied, so Lemma 1.137 kicks in and yields $S_2(E') = S_2(E) + 2 = 2$.

Remark 1.140. Many of these techniques can be made to work in more generality. For example, we refer to [MR10, Sections 2 and 3] for a taste of such results.

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*

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

as follows: for any $\sigma \in \operatorname{Gal}(k^{\mathrm{sep}}/k)$ and $a \in k^\times$, select some $\alpha \in k^{\mathrm{sep}}\times$ 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, $a := \alpha^m$ 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 $a := \alpha^m$. 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 $a := \alpha^m$. 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 $B = \langle b_1, \dots, b_n \rangle$ 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 $f(X) := X^m - b$, 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

[Rub00] Karl Rubin. *Euler systems*. Vol. 147. Annals of Mathematics Studies. Hermann Weyl Lectures. The Institute for Advanced Study. Princeton University Press, Princeton, NJ, 2000, pp. xii+227. ISBN: 0-691-05075-9; 0-691-05076-7. DOI: 10.1515/9781400865208. URL: https://doi.org/10.1515/9781400865208.

[Mil06] J.S. Milne. *Arithmetic Duality Theorems*. Second. BookSurge, LLC, 2006, pp. viii+339. ISBN: 1-4196-4274-X.

[Sil09] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*. 2nd ed. Graduate Texts in Mathematics. Springer New York, NY, 2009. DOI: https://doi.org/10.1007/978-0-387-09494-6.

[MR10] B. Mazur and K. Rubin. "Ranks of twists of elliptic curves and Hilbert's tenth problem". In: *Invent. Math.* 181.3 (2010), pp. 541–575. ISSN: 0020-9910. DOI: 10.1007/s00222-010-0252-0. URL: https://doi.org/10.1007/s00222-010-0252-0.

[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