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

Our main new insight is to bring additive combinatorics into this field.

—Peter Koymans and Carlo Pagano [KP25]

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 $E(k)_{\text{tors}}$ 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 $a_p \coloneqq (p+1) - \#E(\mathbb{F}_p)$ 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 $r_{\text{an}}(E) \leq 1$, 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

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

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 $Ш(E/\mathbb{Q})[p]\neq 0$?

1.1.3 Selmer Groups

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

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

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

For example, it follows that

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

so there is a short exact sequence

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

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

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

$$\begin{array}{ccc} \mathrm{Sel}_m(E/k) & \longrightarrow & \mathrm{H}^1(\mathbb{Q}; E[m]) \\ \downarrow & \lrcorner & \downarrow \\ \prod_v E(\mathbb{Q}_v)/mE(\mathbb{Q}_v) & \longrightarrow & \prod_v \mathrm{H}^1(\mathbb{Q}_v; E[m]) \end{array}$$

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

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

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

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

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" $f(g) \coloneqq c(e,g)$, 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
$$\mathrm{Hom}_G\left(\mathbb{Z}\left[G^2\right], M\right) \xrightarrow{d_3} \mathrm{Hom}_G\left(\mathbb{Z}\left[G^3\right], M\right).$$
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 $f(g) \coloneqq c(e,g)$; 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 $g \coloneqq g_0^{-1}g_1$ and $h \coloneqq g_1^{-1}g_2$, 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 $f(g) \coloneqq c(e,g)$ 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
$$\mathrm{Hom}_G\left(\mathbb{Z}\left[G\right], M\right) \xrightarrow{d_2} \mathrm{Hom}_G\left(\mathbb{Z}\left[G^2\right], M\right).$$
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, $\left\{\mathrm{H}^i(G; M)\right\}_{i>0}$ 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 $\mathrm{N}_G \coloneqq \sum_{g \in G} g$. The kernel of N_G can be calculated as the image of $(\sigma - 1)$ again, so 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 $\mathrm{Hom}_{\mathbb{Z}[G]}(-, M)$, 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. ∎

It is worthwhile to explain the functoriality properties of Proposition 1.38, which are rather bizarre.

Corollary 1.39. Fix a surjection $G' \to G$ of cyclic groups. Then given a morphism $f\colon M \to M'$ where M is a G-module, and M' has the induced G'-module structure, the induced map

$$f\colon \mathrm{H}^i(G; M) \to \mathrm{H}^i(G'; M')$$

is $(\#G'/\#G)^{\lfloor i/2 \rfloor} f$ once these groups have been identified with subquotients of M and M' via Proposition 1.38.

Proof. Denote the surjection $G' \to G$ by g, and we choose a generator σ' for G', and then we define $\sigma \coloneqq g(\sigma')$, which we see must generate G. We also 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

$$\begin{array}{ccccccccccccccc}
\cdots & \longrightarrow & \mathbb{Z}[G'] & \xrightarrow{\mathrm{N}_{G'}} & \mathbb{Z}[G'] & \xrightarrow{(\sigma'-1)} & \mathbb{Z}[G'] & \xrightarrow{\mathrm{N}_{G'}} & \mathbb{Z}[G'] & \xrightarrow{(\sigma'-1)} & \mathbb{Z}[G'] & \xrightarrow{\deg} & \mathbb{Z} & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle m^2 g} & & \downarrow{\scriptstyle mg} & & \downarrow{\scriptstyle mg} & & \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle g} & & \| & & \\
\cdots & \longrightarrow & \mathbb{Z}[G] & \xrightarrow[\mathrm{N}_G]{} & \mathbb{Z}[G] & \xrightarrow[(\sigma-1)]{} & \mathbb{Z}[G] & \xrightarrow[\mathrm{N}_G]{} & \mathbb{Z}[G] & \xrightarrow[(\sigma-1)]{} & \mathbb{Z}[G] & \xrightarrow[\deg]{} & \mathbb{Z} & \longrightarrow & 0
\end{array}$$

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 $\mathrm{Hom}_G(-, M)$ and $\mathrm{Hom}_{G'}(-, M')$ to get another morphism of chain complexes

$$\begin{array}{ccccccccccccc}
0 & \longrightarrow & M & \xrightarrow{(\sigma-1)} & M & \xrightarrow{\mathrm{N}_G} & M & \xrightarrow{(\sigma-1)} & M & \xrightarrow{\mathrm{N}_G} & M & \longrightarrow & \cdots \\
 & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle mf} & & \downarrow{\scriptstyle mf} & & \downarrow{\scriptstyle m^2 f} & & \\
0 & \longrightarrow & M' & \xrightarrow[(\sigma'-1)]{} & M' & \xrightarrow[\mathrm{N}_{G'}]{} & M' & \xrightarrow[(\sigma'-1)]{} & M' & \xrightarrow[\mathrm{N}_{G'}]{} & M' & \longrightarrow & \cdots
\end{array}$$

induced by f and the above morphism. Taking cohomology, 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 $\mathrm{Ind}_H^G\colon \mathrm{Mod}_H \to \mathrm{Mod}_G$ given on objects by sending any H-module N to $\mathrm{Ind}_H^G N$, 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 $\mathrm{Ind}_H^G N$ is bijection with $\mathrm{Hom}_{\mathbb{Z}[H]}(\mathbb{Z}[G], N)$, 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 $\mathrm{Res}_H^G\colon \mathrm{Mod}_G \to \mathrm{Mod}_H$ 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, $\mathrm{Ind}_H^G\colon \mathrm{Mod}_H \to \mathrm{Mod}_G$ is an exact functor.

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

Remark 1.44. We can define a map $M \to \mathrm{Ind}_H^G \mathrm{Res}_H^G M$ 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

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

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 $\mathrm{Ind}_H^G N$ and then take $(-)^G$ to compute the cohomology $\mathrm{H}^i\left(G; \mathrm{Ind}_H^G N\right)$. 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* $\mathrm{Cores}\colon \mathrm{H}^i(H;M) \to \mathrm{H}^i(G;M)$ 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

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

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

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

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. For any discrete topological module M, we define

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

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 $\mathrm{H}^i_{\mathrm{cts}}(G; M)$ 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 $\mathrm{H}^i_{\mathrm{cts}}(G; M)$ as

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

where we are now requiring that the maps from $\mathcal{P}_j \to M$ be continuous. This definition generalizes to arbitrary topological groups G.

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 discrete G-module M. Then

$$\mathrm{H}^i(G; M) = \begin{cases} M^G & \text{if } i = 0, \\ M'/(\sigma - 1)M & \text{if } i = 1, \\ 0 & \text{if } i \geq 3, \end{cases}$$

where M' is the subset of elements annihilated by $1 + \sigma + \cdots + \sigma^n$ for some n. Furthermore, if M is divisible or torsion as a group, then $\mathrm{H}^2(G; M) = 0$.

Proof. We proceed in steps, following [GS13, Section XIII.1].

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

2. We apply the cohomology of cyclic groups. By plugging in the definitions, we see that

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

where $M^{\sigma^m} = M^{\overline{\langle \sigma^m \rangle}}$ by continuity. Because G/H_m is cyclic, Proposition 1.38 tells us that $i > 0$ has

$$\mathrm{H}^i(G; M) = \begin{cases} \operatorname{colim}_{m \geq 1} M^G / \mathrm{N}_{G/H_m}\left(M^{\sigma^m}\right) & \text{if } i \text{ is even}, \\ \operatorname{colim}_{m \geq 1} \ker \mathrm{N}_{G/H_m} / (1 - \sigma) M^{\sigma^m} & \text{if } i \text{ is odd}. \end{cases}$$

We now see that we have to use Corollary 1.39 to compute the internal maps: the map between the mth term and the m'th term (where $m \mid m'$) is given by multiplication by $(m'/m)^{\lfloor i/2 \rfloor}$.

3. We compute at $i = 0$ and $i = 1$. At $i = 0$, there is nothing to do because the colimit is just M^G at all stages. At $i = 1$, we claim that the natural inclusions $\ker \mathrm{N}_{G/H_m} \to M'$ induce an isomorphism

$$\operatorname*{colim}_{m \geq 1} \frac{\ker \mathrm{N}_{G/H_m}}{(1-\sigma)M^{\sigma^m}} \to \frac{M'}{(1-\sigma)M}.$$

Here are the checks on this map.

- Well-defined: the inclusions assemble into a well-defined map because the internal maps in the colimit are simply induced by inclusion. Indeed, there is no multiplication present because $i = 1$.
- Surjective: any class $a \in M'$ will be annihilated by some $1+\sigma+\cdots+\sigma^{m-1}$. But then $(\sigma^m - 1)\, a = 0$ as well, so $a \in \ker \mathrm{N}_{G/H_m}$.
- Injective: suppose a class a coming from $\ker \mathrm{N}_{G/H_m}/(1-\sigma)M^{\sigma^m}$ in the colimit goes to 0 in $M'/(1-\sigma)M$. In particular, we are given that a is annihilated by some $1 + \sigma + \cdots + \sigma^{m-1}$ and also takes the form $(1-\sigma)b$. It follows that $\sigma^m b = b$ as well, so $a \in (1-\sigma)M^{\sigma^m}$, so a vanishes in the colimit already.

4. We show $\mathrm{H}^2(G; M) = 0$ when M is torsion. Indeed, in this case, we are computing the colimit of $M^G/\mathrm{N}_{G/H_m}\left(M^{\sigma^m}\right)$, where the transition map between the mth and m'th term is given by multiplication by m'/m. Because M is torsion, for any given class in the mth term $M^G/\mathrm{N}_{G/H_m}\left(M^{\sigma^m}\right)$, we can select m' sufficiently large so that the multiplication map will kill it. We conclude that the entire colimit must vanish.

5. We show $\mathrm{H}^2(G; M) = 0$ when M is divisible. We will show that the multiplication-by-n endomorphism on $\mathrm{H}^2(G; M)$ is injective for all positive integers $n > 0$, which will complete the proof because $\mathrm{H}^2(G; M)$ is a torsion group (because it is the colimit of torsion groups). To see the claim, we note that $n \colon M \to M$ is surjective, so we have a short exact sequence

$$0 \to M[n] \to M \xrightarrow{n} M \to 0$$

of discrete G-modules. The long exact sequence (which holds even after the colimit because the colimit is filtered) then shows that

$$\mathrm{H}^2(G; M[n]) \to \mathrm{H}^2(G; M) \xrightarrow{n} \mathrm{H}^2(G; M)$$

is exact, so the claim follows from the previous step.

6. We show $\mathrm{H}^i(G; M) = 0$ when i is odd and $i \geq 3$. Write $i = 2j + 1$ for $j \geq 1$ so that $\lfloor i/2 \rfloor = j$. Then

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

and the transition maps are given by multiplication by $(m'/m)^j$. It is enough to show that any class $a \in \ker \mathrm{N}_{G/H_m}$ vanishes in the colimit. Well, $m\mathrm{H}^1(G/H_m; M^{\sigma^m}) = 0$, so we see that ma must vanish in this cohomology group, so $ma = (1-\sigma)b$ for some $b \in M^{\sigma^m}$. Thus, we see that a vanishes along the transition map

$$\frac{\ker \mathrm{N}_{G/H_m}}{(1-\sigma)M^{\sigma^m}} \xrightarrow{m^j} \frac{\ker \mathrm{N}_{G/H_{m^2}}}{(1-\sigma)M^{\sigma^{m^2}}}$$

because $m^j a = (1-\sigma)m^{j-1}b$.

7. We show $\mathrm{H}^i(G; M) = 0$ when i is even and $i \geq 4$. Instead of proceeding by dimension-shifting (which is mildly technical because G is infinite), we will argue directly as in the previous step. Write $i = 2j$ for $j \geq 2$ so that $\lfloor i/2 \rfloor = j$. Then

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

and the transition maps are given by multiplication by $(m'/m)^j$. Once again, it is enough to show that any class $a \in M^G$ vanishes in the colimit. Well, find m for which $\sigma^m a = a$, so $m\mathrm{H}^2(G/H_m; M^{\sigma^m}) = 0$ implies that $ma = \mathrm{N}_{G/H_m}(b)$ for some $b \in M^{\sigma^m}$. Then $\mathrm{N}_{G/H_{mk}}(b) = \mathrm{N}_{G/H_k}\mathrm{N}_{G/H_m}(b) = kma$, so a vanishes along the transition map

$$\frac{M^G}{\mathrm{N}_{G/H_m}(M^{\sigma^m})} \to \frac{M^G}{\mathrm{N}_{G/H_{m^2}}(M^{\sigma^{m^2}})}$$

because $m^j a = m^{j-2}\mathrm{N}_{G/H_{m^2}}(b)$. ∎

Remark 1.56. Equivalently, when M is torsion, the cohomology of M is computed via the two-term complex

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

Remark 1.57. If M is torsion, then we claim that $M' = M$. Indeed, any given element $a \in M$ is stabilized by some open subgroup H_m, meaning $\sigma^m a = a$. Thus,

$$\left(1 + \sigma + \cdots + \sigma^{mn-1}\right) a = n\left(1 + \sigma + \cdots + \sigma^{m-1}\right) a$$

vanishes for some n because a is torsion.

Example 1.58. Set $G \coloneqq \widehat{\mathbb{Z}}$ with generator σ, and give $\mathbb{Q}$ the trivial action. Because $\mathbb{Q}$ is divisible, Proposition 1.55 tells us that $\mathrm{H}^i(G;\mathbb{Q}) = 0$ for $i \geq 2$ automatically. Further, we see that no nonzero element $\mathbb{Q}$ is not annihilated by $1 + \sigma + \cdots + \sigma^n$ for any n, so $\mathrm{H}^1(G;\mathbb{Q}) = 0$ as well. We conclude that

$$\mathrm{H}^i(G;\mathbb{Q}) = \begin{cases} \mathbb{Q} & \text{if } i = 0, \\ 0 & \text{if } i \geq 1. \end{cases}$$

Example 1.59. Set $G \coloneqq \widehat{\mathbb{Z}}$ with generator σ,and give the finite abelian group A the trivial action. By Proposition 1.38, we know that $\mathrm{H}^i(G;A) = 0$ for $i \geq 2$ automatically. Continuing, by Remark 1.57, we see further that $\mathrm{H}^1(G;A) = A$. We conclude that

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

Example 1.60. Set $G \coloneqq \widehat{\mathbb{Z}}$ with generator σ,and give the abelian group $\mathbb{Z}$ the trivial action. By Proposition 1.38, we know that $\mathrm{H}^i(G;A) = 0$ for $i \geq 3$ automatically; similarly, we see that no nonzero element is annihilated by $1+\sigma+\cdots+\sigma^n$ for any n, so $\mathrm{H}^1(G;\mathbb{Z}) = 0$. Continuing, as in the proof of Proposition 1.38, we see that $\mathrm{H}^2(G;\mathbb{Z})$ is the colimit of the quotients $\mathbb{Z}/m\mathbb{Z}$, where the transition maps $\mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/m'\mathbb{Z}$ are given by multiplication by m'/m; equivalently, this is the inclusion $\frac{1}{m}\mathbb{Z}/\mathbb{Z} \to \frac{1}{m'}\mathbb{Z}/\mathbb{Z}$. We conclude that

$$\mathrm{H}^i(G;A) = \begin{cases} \mathbb{Z} & \text{if } i = 0, \\ \mathbb{Q}/\mathbb{Z} & \text{if } i = 2, \\ 0 & \text{otherwise.} \end{cases}$$

This allows us to say something about Galois cohomology.

Notation 1.61. Fix a field k and a commutative group scheme X over k. Then we set the notation

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

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

Remark 1.62. 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 1.63. 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 1.64. 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 1.65. If M has the trivial action, then Example 1.37 induces a commutative square

$$\begin{array}{ccc} \mathrm{H}^1\left(G/H;M\right) & \longrightarrow & \mathrm{Hom}\left(G/H,M\right) \\ \downarrow & & \downarrow \\ \mathrm{H}^1\left(G/H';M\right) & \longrightarrow & \mathrm{Hom}\left(G/H',M\right) \end{array}$$

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 and Global Duality

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

Theorem 1.66 (Tate)**.** Fix a finite extension K of $\mathbb{Q}_p$, set $G \coloneqq \mathrm{Gal}(\overline{K}/K)$ for brevity, and let M be a finite discrete G-module.

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

(b) Duality: for a G-module M, we define the G-module $M^* \coloneqq \mathrm{Hom}_{\mathbb{Z}}(M, \mu_\infty(\overline{K}))$. Then there is a perfect pairing

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

(c) Euler characteristic formula: one has

$$\frac{\#\mathrm{H}^0(K;M)\cdot\#\mathrm{H}^2(K;M)}{\#\mathrm{H}^1(K;M)} = \frac{1}{\#(\mathcal{O}_K/(\#M)\mathcal{O}_K)}.$$

Remark 1.67. 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 1.68. One calls (c) an Euler characteristic formula because the invariant

$$\chi(M) \coloneqq \frac{\#\mathrm{H}^0(K;M)\cdot \#\mathrm{H}^2(K;M)}{\#\mathrm{H}^1(K;M)}$$

behaves like an Euler characteristic. Indeed, it is like an alternating sum of cohomology groups.

Remark 1.69. It is possible to check Theorem 1.66 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 1.70 (inertia group)**.** Fix a local field K with finite residue field k. Then the Galois action on K preserves the absolute value and therefore descends to $\mathcal{O}_K/\mathfrak{p}_K=k$. We define the *inertia subgroup* I_K of $\mathrm{Gal}(\overline{K}/K)$ to fit in the short exact sequence

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

Remark 1.71. Let K^{ur} be the maximal unramified extension of K. Then we see that $\mathrm{Gal}(K^{\mathrm{ur}}/K)$ is simply $\mathrm{Gal}(\overline{K}/K)/I_K$, which is $\mathrm{Gal}(\overline{k}/k)$.

Definition 1.72 (unramified)**.** Fix a local field K. Then a $\mathrm{Gal}(\overline{K}/K)$-module M is *unramified* if and only if I_K acts trivially on M. In this case, we define the *unramified cohomology* $\mathrm{H}^i_{\mathrm{ur}}(K;M)$ as the image of

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

Remark 1.73. By Proposition 1.55 (which applies by Remark 1.71), we see that only the unramified cohomology which has a chance of being nonzero is indices 0 and 1.

Example 1.74. Suppose that M is a trivial Galois module, and consider the commutative diagram

$$\begin{array}{ccc}
\mathrm{H}^1\left(\mathrm{Gal}(K^{\mathrm{ur}}/K);M\right) & \longrightarrow & \mathrm{Hom}\left(\mathrm{Gal}(K^{\mathrm{ur}}/K),M\right)\\
\downarrow & & \downarrow\\
\mathrm{H}^1\left(\mathrm{Gal}(K^{\mathrm{sep}}/K);M\right) & \longrightarrow & \mathrm{Hom}\left(\mathrm{Gal}(K^{\mathrm{sep}}/K),M\right)
\end{array}$$

induced by the commutative squares of Example 1.65. 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 1.75. 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 1.76. 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

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

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 1.66. We now complete the proof with an Euler characteristic calculation because we know $\chi(M) = 1$ by Theorem 1.66. ∎

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

Lemma 1.77. 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

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

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

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

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

$$\begin{array}{ccccccccc}
0 & \longrightarrow & E[m](K^{\mathrm{unr}}) & \longrightarrow & E(K^{\mathrm{unr}}) & \longrightarrow & E(K^{\mathrm{unr}}) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & E[m](\overline{K}) & \longrightarrow & E(\overline{K}) & \longrightarrow & E(\overline{K}) & \longrightarrow & 0
\end{array}$$

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

$$\begin{array}{ccc} E(K)/mE(K) & \longrightarrow & \mathrm{H}^1(K^{\mathrm{unr}}/K; E[m]) \\ \| & & \downarrow \\ E(K)/mE(K) & \longrightarrow & \mathrm{H}^1(\overline{K}/K; E[m]) \end{array}$$

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 $E(k)$.

While we're here, even though we will not use it for some time, now is as good a time as any to note that there is a global duality statement.

Theorem 1.78 (Pitou–Tate)**.** Fix a number field K and a set of places Σ of K, and let K_Σ be the maximal Galois extension ramified only at Σ. For any finite discrete Galois module M, there is an exact sequence

$$\mathrm{H}^1(K_\Sigma/K; M) \xrightarrow{\mathrm{loc}} \prod_{v \in \Sigma} \left(\mathrm{H}^1(K_v; M), \mathrm{H}^1_{\mathrm{ur}}(K_v; M)\right) \xrightarrow{\mathrm{loc}^\vee} \mathrm{H}^1(K_\Sigma/K; M^*)^\vee,$$

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

Remark 1.79. The restricted product makes sense because M will be unramified at all but finitely many places v: the Galois action on M factors through $\mathrm{Gal}(L/K)$ 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 $\mathrm{Gal}(L/K)$ and thus acts trivially on M.

Remark 1.80. Let's define the right-hand map. It is enough to define a pairing on

$$\prod_{v \in \Sigma} \left(\mathrm{H}^1(K_v; M), \mathrm{H}^1_{\mathrm{ur}}(K_v; M)\right) \times \prod_{v \in \Sigma} \left(\mathrm{H}^1(K_v; M^*), \mathrm{H}^1_{\mathrm{ur}}(K_v; M^*)\right).$$

For this, we simply sum the local pairings of Theorem 1.66. These sums are finite (and so converge) because all but finitely many places $v \in \Sigma$ compute a pairing from $\mathrm{H}^1_{\mathrm{ur}}(K_v; M) \times \mathrm{H}^1_{\mathrm{ur}}(K_v; M^*)$, which vanishes by Proposition 1.76.

The given exact sequence is in fact the middle three terms of a nine-term exact sequence. 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.

Remark 1.81. In [Mil06, Theorem I.4.10], Σ is required to be nonempty. However, the statement of Theorem 1.78 has no content if Σ is empty because then the middle term vanishes.

1.3.2 Selmer Groups

We are now allowed to make the following global definition.

Definition 1.82 (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.

$$\begin{array}{ccc} \mathrm{Sel}_{\mathcal{L}}(M) & \longrightarrow & \mathrm{H}^1(K; M) \\ \downarrow & \lrcorner & \downarrow \\ \prod_v \mathcal{L}_v & \hookrightarrow & \prod_v \mathrm{H}^1(K_v; M) \end{array}$$

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 1.83. If E is an elliptic curve over a global field K, we can define $M \coloneqq E[m]$ 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 1.77, 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 1.84. 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

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

Remark 1.85. 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 by Remark 1.79.

Remark 1.86. The power of $\mathrm{Sel}_{\mathcal{L}}(M)$ 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 $\mathrm{Gal}(L/K)$, so $c|_{I_v}$ is trivial, so $\mathrm{Res}_v\, c$ is unramified.

Inspired by Remark 1.86, we make the following notation.

Notation 1.87. 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 1.79).

Here is our finiteness result.

Theorem 1.88. Fix a number field K, and fix a finite discrete Galois module M. Furthermore, for each place v of K, choose a subset $\mathcal{L}_v \subseteq \mathrm{H}^1(K_v; M)$, and we require that $\mathcal{L}_v = \mathrm{H}^1_{\mathrm{ur}}(K_v; M)$ for all but finitely many v. Then $\mathrm{Sel}_{\mathcal{L}}(M)$ is finite.

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

- We note that making $\mathcal{L}$ larger cannot help us, so we may assume that either $\mathcal{L}_v = \mathrm{H}^1(K_v; M)$ or $\mathcal{L}_v = \mathrm{H}^1_{\mathrm{ur}}(K_v; M)$ for all places v, and we let S to be the finite set in which the former occurs. For example, S includes the places where M is ramified. From now on, we will abbreviate $\mathrm{Sel}_{\mathcal{L}}(M)$ to $\mathrm{Sel}_S(M)$. As noted previously with $\mathcal{L}$, we remark that we may enlarge S, and it will not make the problem any easier.
- We show that we may reduce the question to any finite extension K' of K. For this, we let M' be the module M with the restricted Galois action, and we let S' be the set of primes of K' lying over a prime of S. We then draw the following diagram.

$$\begin{array}{ccccccc} & & & & \mathrm{Sel}_S(M) & \longrightarrow & \mathrm{Sel}_{S'}(M') \\ & & & & \downarrow & & \downarrow \\ 0 & \longrightarrow & \mathrm{H}^1(\mathrm{Gal}(K'/K); M) & \xrightarrow{\mathrm{Inf}} & \mathrm{H}^1(K; M) & \xrightarrow{\mathrm{Res}} & \mathrm{H}^1(K'; M) \end{array}$$

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

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

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

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

By Example 1.74, 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. ∎

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

Remark 1.89. Here is another way to conclude at the end, which uses Kummer theory. For technical reasons, we extend K to be Galois over $\mathbb{Q}$, and we go ahead and enlarge S to be Galois-invariant and include the primes dividing m; let $S_{\mathbb{Q}}$ be the corresponding primes in $\mathbb{Q}$ lying under a prime in S.

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

1.4 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.

Definition 1.90 (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 1.91. Let's explain why the functions f and g exist. The isomorphism $\mathrm{Pic}^0(E) \to E$ of group schemes shows that a divisor $\sum_i n_i[P_i]$ in $\mathrm{Pic}^0(E)$ 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 1.92. 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 1.93. 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 1.94. When generalizing to abelian varieties, the correct Weil pairing is defined between an abelian variety A and its "dual" $\operatorname{Pic}^0 A$.

Example 1.95. 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 1.96. 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 1.91, 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 $\sigma \in \operatorname{Gal}(K^{\mathrm{sep}}/K)$. 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 1.97. 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 1.98 (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 $\widetilde{e}_m(S, T) \coloneqq f_S(D_T)/f_T(D_S)$.

Remark 1.99. It is possible to find divisors D_S and D_T by (say) taking $D_S \coloneqq [S] - [\infty]$ and $D_T \coloneqq [R + S] - [R]$ 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 1.91), 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 1.100 (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 $a_1, \dots, a_M, b_1, \dots, b_N \in K$ and $m_1, \dots, m_M, n_1, \dots, n_N \in \mathbb{Z}$. 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 $\operatorname{div} g = g^* \operatorname{div} \mathrm{id}_{\mathbb{P}^1}$ by definition, so $f(\operatorname{div} g)$ equals

$$f(g^* \operatorname{div} \mathrm{id}_{\mathbb{P}^1}) = (g_* f)(\operatorname{div} \mathrm{id}_{\mathbb{P}^1}).$$

Now, by the first step, this is

$$\mathrm{id}_{\mathbb{P}^1}(\operatorname{div} g_* f) = \mathrm{id}_{\mathbb{P}^1}(g_* \operatorname{div} f).$$

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 1.101. 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 1.100.

Remark 1.102. 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 1.100.

Proposition 1.103. 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 1.91, 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 1.91, 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 $mT' \in E[m]$. ∎

This last interpretation of the Weil pairing can also be viewed as a commutator pairing (as in Proposition A.14).

Definition 1.104 (Heisenberg group)**.** Fix an elliptic curve E over a field K and an integer m. For an extension L/K, we define the *Heisenberg group* $\mathcal{H}_m(L)$ to consist of pairs (x,f) where $x \in E(L)$ and f is a rational function in $L(E)$ for which $\operatorname{div} f = m[x] - m[\infty]$. The group operation is given by

$$(x,f)\cdot(y,g) \coloneqq (x+y, \tau_y f \cdot g),$$

where τ_y denotes the translation action $\tau_y f(t) \coloneqq f(t-y)$.

Remark 1.105. Note that $\mathcal{H}_m(L)$ is a subgroup of $E(L) \ltimes L(E)^\times$, where $E(L)$ acts on $L(E)^\times$ by translation. Indeed, we just have to check closure under the group operation (and inversion), for which we note that $(x,f),(y,g) \in \mathcal{H}_m$ have

$$\operatorname{div}(\tau_y f \cdot g) = m[x+y] - m[y] + m[y] - m[\infty].$$

Similarly, $(x,f)^{-1} = \left(-x, \tau_{-x} f^{-1}\right)$ has $\operatorname{div} \tau_{-x} f^{-1} = m[-x] - m[\infty]$.

Remark 1.106. Note that having some f with $\operatorname{div} f = m[x] - m[\infty]$ implies that $m \cdot x = \infty$ in $E(L)$; conversely, any such $x \in E(L)[m]$ has some $f \in L(E)$ with $\operatorname{div} f = m[x] - m[\infty]$, and this f is unique up to scalar. Thus, there is a short exact sequence

$$1 \to L^\times \to \mathcal{H}_m(L) \to E[m](L) \to 0,$$

where $L^\times \to \mathcal{H}_m(L)$ is given by sending $\alpha \in L^\times$ to the constant function α. Note that $L^\times$ embeds into the center of $\mathcal{H}_m(L)$!

Lemma 1.107. Fix an elliptic curve E over a field K. For each positive integer m and $S, T \in E[m]$, we have

$$\widetilde{e}_m(S,T) = \varphi(S,T)^{-1},$$

where $\varphi\colon E[m] \otimes E[m] \to \overline{K}^\times$ is the commutator pairing induced by the short exact sequence of Remark 1.106.

Proof. This is a direct calculation. Choose functions f_S and f_T for which $\operatorname{div} f_S = m[S] - m[\infty]$ and $\operatorname{div} f_T = m[T] - m[\infty]$. Then the commutator pairing $\varphi(S,T)$ is simply

$$\begin{aligned}(S, f_S)(T, f_T)(S, f_S)^{-1}(T, f_T)^{-1} &= (S+T, \tau_T f_S \cdot f_T)(S+T, \tau_S f_T \cdot f_S)^{-1} \\ &= (S+T, \tau_T f_S \cdot f_T)\left(-S-T, \tau_{-T} f_T^{-1} \cdot \tau_{-S-T} f_S^{-1}\right) \\ &= (0, \tau_{-S} f_S \cdot \tau_{-S-T} f_T \cdot \tau_{-T} f_T^{-1} \cdot \tau_{-S-T} f_S^{-1}).\end{aligned}$$

Thus, the commutator pairing outputs the value of the constant function

$$X \mapsto \frac{f_S(X+S) f_T(X+S+T)}{f_T(X+T) f_S(X+S+T)}.$$

In order to make $\widetilde{e}$ appear, we need to take quotients by rational functions with disjoint support. Choose an auxiliary point $P \in E(\overline{K})$ which is not m-torsion. We would like to compute the quotient

$$\frac{f_T([P+S+T]-[P+T])}{f_S([P+S+T]-[P+S])}.$$

Well, the function $\tau_{P+T} f_S$ has $\operatorname{div} \tau_{P+T} f_S = m[P+S+T] - m[P+T]$, so this quotient is

$$\frac{f_T([P+S+T]-[P+T]}{\tau_{P+T} f_S([T]-[\infty])} \cdot \frac{f_S([-P]+[-P-T])}{f_S([P+S+T]-[P+S])}.$$

The left term is $\widetilde{e}(T,S)$, so we are left to show that

$$\frac{f_S(-P) f_S(P+S)}{f_S(-P-T) f_S(P+T+S)} \stackrel{?}{=} 1.$$

We now claim that the function $X \mapsto f_S(-X) f_S(X+S)$ is constant, which will complete the proof. Indeed, the divisor of this function is $m[-S] - m[\infty] + m[\infty] - m[-S] = 0$. ∎

1.4.2 Some Maximal Isotropic Subspaces

The Weil pairing now interacts with cohomology as follows.

Lemma 1.108. Fix a field K of characteristic 0 and a positive integer m.

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

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

In fact, this pairing on $\mathrm{H}^1(K; E[m])$ is induced by a quadratic function $\mathrm{H}^1(K; E[m]) \to \mathrm{H}^2(K; \mathbb{G}_m)$.

(b) The boundary map $\mathrm{H}^1(K; E[m]) \to \mathrm{H}^2(K; \mathbb{G}_m)$ vanishes on $E(K)/mE(K)$. Thus, the subspace $E(K)/mE(K)$ of $\mathrm{H}^1(K; E[m])$ is isotropic.

Proof. We handle 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.

It remains to produce the desired quadratic function. We follow [PR12, Corollary 4.7]. To begin, note Lemma 1.107 tells us that the Weil pairing e_m is induced by a commutator pairing, so Proposition A.14 implies that the pairing on $\mathrm{H}^1(K; E[m])$ is induced by the boundary map $q\colon \mathrm{H}^1(K; E[m]) \to \mathrm{H}^2(K; \mathbb{G}_m)$. To show that q is a quadratic function, we note that $\langle m, n\rangle_q = q(m+n)q(m)^{-1}q(n)^{-1}$ is already understood to be symmetric and bilinear, so we only have to check that $q(km) = k^2 q(m)$ for all m and $k \in \mathbb{Z}$. By the bilinearity we already have, it is enough to just check that $q(-m) = q(m)$ for all m. To this end, we note that there is a morphism

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathbb{G}_m & \longrightarrow & \mathcal{H}_m & \longrightarrow & E[m] & \longrightarrow & 0 \\ & & \| & & \downarrow & & \downarrow{\scriptstyle -1} & & \\ 1 & \longrightarrow & \mathbb{G}_m & \longrightarrow & \mathcal{H}_m & \longrightarrow & E[m] & \longrightarrow & 0 \end{array}$$

of short exact sequence, where the map $\mathcal{H}_m \to \mathcal{H}_m$ is given by $(x, f) \mapsto (-x, \iota f)$; here, $\iota\colon \overline{K}(E) \to \overline{K}(E)$ is defined by $\iota g(p) \coloneqq g(-p)$. Certainly this map is well-defined, and it is a group homomorphism because $(x, f)(y, g) = (x + y, \tau_y f \cdot g)$ goes to $(-x, \iota f)(-y, \iota g) = (-x - y, \tau_{-y}\iota f \cdot \iota g)$. Functoriality of the boundary now gives us a commuting square

$$\begin{array}{ccc} \mathrm{H}^1(K; E[m]) & \xrightarrow{q} & \mathrm{H}^2(K; \mathbb{G}_m) \\ {\scriptstyle -1}\downarrow & & \| \\ \mathrm{H}^1(K; E[m]) & \xrightarrow{q} & \mathrm{H}^2(K; \mathbb{G}_m) \end{array}$$

which is exactly what we wanted to show.

(b) We will show this directly on the level of cocycles, following [PR12, Proposition 4.9]. Note that the first sentence implies the second one: Proposition A.14 combined with Lemma 1.107 tells us that the pairing on $\mathrm{H}^1(K; E[m])$ is given by the boundary map.

We now show the first sentence. It is enough to show the boundary $\delta\colon \mathrm{H}^0(K; E) \to \mathrm{H}^1(K; E[m])$ factors through $\mathrm{H}^1(K; \mathcal{H}_m)$ because then the composite

$$\mathrm{H}^1(K; \mathcal{H}_m) \to \mathrm{H}^1(K; E[m]) \to \mathrm{H}^2(K; \mathbb{G}_m)$$

vanishes by Lemma A.13. We will show this factoring directly on the level of cocycles.

Fix some $x \in E(K)$ and choose some $y \in E(\overline{K})$ with $y = mx$ so that $\delta(g) \coloneqq gy - y$. We are tasked with finding some 1-cocycle c of $\mathcal{H}_m$ such that $\delta = \mathrm{pr}_1(c)$, where $\mathrm{pr}_1\colon \mathcal{H}_m \to E[m]$ is the canonical projection. Thus, we need to find functions $f_g \in \overline{K}(E)$ such that $\operatorname{div} f_g = m[\delta(g)] - m[\infty]$ so that $c(g) \coloneqq (\delta(g), f_g)$ is a 1-cocycle of $\mathcal{H}_m$. Note that such functions certainly exist because $\delta(g) \in E[m]$, and they are unique up to scalar.

Now, checking that c is a 1-cocycle amounts to verifying the equality $c(gh) = gc(h) \cdot c(g)$. This is equivalent to

$$(\delta(gh), f_{gh}) \overset{?}{=} \left(g\delta(h) + \delta(g), \tau_{\delta(g)} g f_h \cdot f_g\right).$$

The left coordinates are equal because δ is a 1-cocycle, so it remains to produce the functions $f_\bullet$ achieving $f_{gh} = \tau_{gy-y} g f_h \cdot f_g$; equivalently, we need to achieve $\tau_y f_{gh} = g\tau_y f_h \cdot \tau_y f_g$. Well, note that the divisors of both sides are

$$m[ghy] - m[y] = m[ghy] - m[gy] + m[gy] - m[y],$$

so these functions are certainly the same up to a scalar. To fix the scalar, note that we may assume $y \neq \infty$ (otherwise, $x = \infty$, and we can choose all the functions $f_\bullet$ to be constants), so we may normalize all functions so that $\tau_y f_g(\infty) = 1$ for all g. Then the equality $\tau_y f_{gh} = g\tau_y f_h \cdot \tau_y f_g$ follows from the equality at the point ∞. ∎

We now produce some local and global isotropy results. Here is the local one.

Proposition 1.109. Fix a local field K of characteristic 0 and a positive integer m.

(a) The Weil pairing makes $\mathrm{H}^1(K; E[m])$ a non-degenerate quadratic space. Explicitly, this is a quadratic space over $\mathbb{Z}/m\mathbb{Z}$ if K is nonarchimedean and over $\mathbb{Z}/\gcd(m,2)\mathbb{Z}$ if K is archimedean.

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

Proof. These claims follow from local duality. For (a), note the Weil pairing on $E[m]$ is perfect and Galois-invariant (by Lemma 1.96), so it induces an isomorphism $E[m] \cong \mathrm{Hom}(E[m], \mu_m)$ of (finite discrete) Galois modules. Thus, we can think of the pairing on $\mathrm{H}^1(K; E[m])$ as fitting into the commutative diagram

$$\begin{array}{ccccc} \mathrm{H}^1(K;E[m]) & \times & \mathrm{H}^1(K;E[m]) & \xrightarrow{\cup} & \mathrm{H}^2(K;\mu_m) \\ \downarrow{\scriptstyle e_m} & & \| & & \| \\ \mathrm{H}^1(K;E[m]^*) & \times & \mathrm{H}^1(K;E[m]) & \xrightarrow{\cup} & \mathrm{H}^2(K;\mu_m) \end{array} \qquad \begin{array}{ccc} (c_1,c_2) & \longmapsto & e_m(c_1 \cup c_2) \\ \downarrow & & \downarrow \\ (g \mapsto e_m(c_1(g),-),c_2) & \longmapsto & (g,h) \mapsto e_m(c_1(g), gc_2(h)) \end{array}$$

where the bottom row is perfect by Theorem 1.66. Thus, the induced pairing is perfect, and we see that we actually have a quadratic space over $\mathbb{Z}/m\mathbb{Z}$ because the target of the pairing is $\mathrm{H}^2(K;\mu_m) \cong \mathbb{Z}/m\mathbb{Z}$ by local class field theory.

We now move on to (b), following [Tat01, Theorem 8.2]. We begin by recalling the Kummer short exact sequence

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

which is induced by the short exact sequence $0 \to E[m] \to E \to E \to 0$. Roughly speaking, the result will follow by comparing this short exact sequence with its dual. By Lemma 1.108, we see that $E(K)/mE(K)$ is an isotropic subspace of $\mathrm{H}^1(K; E[m])$, so the Weil pairing descends to a pairing

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

where we are viewing $\mathrm{H}^1(K; E)[m]$ as the quotient of $\mathrm{H}^1(K; E[m])$ by $E(K)/mE(K)$.

The main claim is that this last Weil pairing is perfect. For now, let's content ourselves with explaining why this completes the proof. We would like to show that a class $c \in \mathrm{H}^1(K; E[m])$ has $x \cup c = 0$ for all $x \in E(K)/mE(K)$ if and only if $c \in E(K)/mE(K)$. In other words, the functional $- \cup c$ on $E(K)/mE(K)$ vanishes if and only if c vanishes in the quotient $\mathrm{H}^1(K; E)[m]$, which is exactly the main claim.

We now show the main claim. Let $(-)^\vee := \mathrm{Hom}_{\mathbb{Z}}(-, \mathbb{Q}/\mathbb{Z})$ denote the Pontryagin dual. Then we note that the Weil pairing induces a morphism

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \dfrac{E(K)}{mE(K)} & \longrightarrow & \mathrm{H}^1(K;E[m]) & \longrightarrow & \mathrm{H}^1(K;E)[m] & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \mathrm{H}^1(K;E)[m]^\vee & \longrightarrow & \mathrm{H}^1(K;E[m])^\vee & \longrightarrow & \left(\dfrac{E(K)}{mE(K)}\right)^\vee & \longrightarrow & 0 \end{array}$$

of short exact sequences. We showed in (a) that the middle morphism is an isomorphism, so it follows that the left morphism is injective, and the right morphism is surjective. But the size of a finite abelian group and its Pontryagin dual are the same, so it follows that the left and right morphisms are isomorphisms, which is what we wanted to show! ∎

Here is the global isotropy result.

Remark 1.110. 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.

Proposition 1.111. Fix a number field K and a positive integer m.

(a) The Weil pairing makes $\mathrm{H}^1(\mathbb{A}_K; E[m])$ a non-degenerate quadratic space over $\mathbb{Z}/m\mathbb{Z}$.

(b) The image of $E(\mathbb{A}_K)/mE(\mathbb{A}_K)$ in $\mathrm{H}^1(\mathbb{A}_K; E[m])$ is maximal isotropic.

(c) The image of $\mathrm{H}^1(K; E[m])$ in $\mathrm{H}^1(\mathbb{A}_K; E[m])$ is maximal isotropic.

Proof. Before we do anything, let's describe the pairing on $\mathrm{H}^1(\mathbb{A}_K; E[m])$. It is the one induced from Remark 1.80 and the Weil pairing (see also the diagram in Proposition 1.109). More explicitly, for two classes c and c', the pairing is

$$\langle c, c' \rangle \coloneqq \sum_v \langle \mathrm{loc}_v\, c, \mathrm{loc}_v\, c' \rangle_v,$$

where $\langle -, - \rangle_v$ is the (local) Weil pairing on $\mathrm{H}^1(K_v; E[m])$ of Proposition 1.109 (and Theorem 1.66). In particular, the fact that the Weil pairing is antisymmetric implies that the pairing on $\mathrm{H}^1(\mathbb{A}_K; E[m])$ is symmetric. Furthermore, because all the local pairings output to $\mathrm{H}^2(K_v; \mu_m) \hookrightarrow \mathbb{Z}/m\mathbb{Z}$, we see that we receive a quadratic space over $\mathbb{Z}/m\mathbb{Z}$.

(a) This is a local statement; in particular, it is just a "sum" of local results. In light of the above remarks, it only remains to show the non-degeneracy. For this, suppose that $c \in \mathrm{H}^1(\mathbb{A}_K; E[m])$ has $\langle c, c' \rangle = 0$ for all $c' \in \mathrm{H}^1(\mathbb{A}_K; E[m])$, so we want to show that $c = 0$. By definition of $\mathrm{H}^1(\mathbb{A}_K; E[m])$, it is enough to show that $\mathrm{loc}_v\, c = 0$ for all places v. Well, for each v_0, and class $c'_{v_0} \in \mathrm{H}^1(K_v; E[m])$, we can define a class $c' \in \mathrm{H}^1(\mathbb{A}_K; E[m])$ by

$$\mathrm{loc}_v\, c' \coloneqq \begin{cases} c'_{v_0} & \text{if } v = v_0, \\ 0 & \text{otherwise.} \end{cases}$$

Then $c' \in \mathrm{H}^1(\mathbb{A}_K; E[m])$ and $\langle c, c' \rangle = \langle \mathrm{loc}_{v_0}\, c, c'_{v_0} \rangle_{v_0}$ must vanish for all c'_{v_0}, so it follows that $\mathrm{loc}_{v_0}\, c = 0$ by Proposition 1.109.

(b) This is also a local statement. Indeed, given $c \in \mathrm{H}^1(\mathbb{A}_K; E[m])$, we have to show $c \in E(\mathbb{A}_K)/mE(\mathbb{A}_K)$ if and only if c annihilates $E(\mathbb{A}_K)/mE(\mathbb{A}_K)$. Certainly if c is in $E(\mathbb{A}_K)/mE(\mathbb{A}_K)$, then summing Proposition 1.109 shows that c annihilates $E(\mathbb{A}_K)/mE(\mathbb{A}_K)$.

Conversely, suppose c annihilates $E(\mathbb{A}_K)/mE(\mathbb{A}_K)$, and we will show $\mathrm{loc}_{v_0}\, c \in E(K_{v_0})/mE(K_{v_0})$ for all v_0. Well, by Proposition 1.109, it is enough to show that

$$\langle \mathrm{loc}_{v_0}\, c, c'_{v_0} \rangle_{v_0} = 0$$

for all $c'_{v_0} \in \mathrm{H}^1(K_{v_0}; E[m])$, but this follows by using c'_{v_0} to construct a class $c' \in \mathrm{H}^1(\mathbb{A}_K; E[m])$ exactly as in (a).

(c) This is a global statement. Indeed, we will use Pitou–Tate duality in the form of Theorem 1.78. Let's explain what we can show without global duality: we can show that $\mathrm{H}^1(K; E[m])$ is isotropic. In fact, the quadratic form $\mathrm{H}^1(\mathbb{A}_K; E[m]) \to \mathbb{Z}/m\mathbb{Z}$ vanishes on $\mathrm{H}^1(K; E[m])$. To see this, note the commutativity of the diagram

$$\begin{array}{ccc} \mathrm{H}^1(K; E[m]) & \longrightarrow & \mathrm{H}^2(K; \mathbb{G}_m) \\ \downarrow & & \downarrow \\ \mathrm{H}^1(\mathbb{A}_K; E[m]) & \longrightarrow & \mathrm{H}^2(\mathbb{A}_K; \mathbb{G}_m) \end{array}$$

causes the composite $\mathrm{H}^1(K; E[m]) \to \mathbb{Z}/m\mathbb{Z}$ to factor through

$$\mathrm{H}^2(K; \mathbb{G}_m) \to \mathrm{H}^2(\mathbb{A}_K; \mathbb{G}_m) \to \mathbb{Q}/\mathbb{Z}.$$

This last composite vanishes because it is part of the fundamental exact sequence of global class field theory.

It remains to show that $\mathrm{H}^1(K; E[m])$ is maximal isotropic. Well, suppose that we have a class $c \in \mathrm{H}^1(\mathbb{A}_K; E[m])$ such that $c \cup c' = 0$ for all $c' \in \mathrm{H}^1(K; E[m])$, and we would like to show that $c \in \mathrm{H}^1(K; E[m])$. Well, Theorem 1.78 applied with Σ equal to the set of all places shows that we have an exact sequence

$$\mathrm{H}^1(K; E[m]) \to \mathrm{H}^1(\mathbb{A}_K; E[m]) \to \mathrm{H}^1(K; E[m]^*)^\vee.$$

Identifying $\mathrm{H}^1(K; E[m]^*)$ with $\mathrm{H}^1(K; E[m])$ via the Weil pairing, we see that $c \in \mathrm{H}^1(\mathbb{A}_K; E[m])$ vanishes in $\mathrm{H}^1(K; E[m])^\vee$ by hypothesis! Thus, c must come from a class in $\mathrm{H}^1(K; E[m])$. ■

We now summarize our results as follows.

Theorem 1.112. Fix an elliptic curve E over a number field K, and choose a positive integer m. Then $\mathrm{Sel}_m(E/K)$ sits in the following pullback square.

$$\begin{array}{ccc} \mathrm{Sel}_m(E/K) & \longrightarrow & \mathrm{H}^1(K; E[m]) \\ \downarrow & \lrcorner & \downarrow \\ E(\mathbb{A}_K)/mE(\mathbb{A}_K) & \hookrightarrow & \mathrm{H}^1(\mathbb{A}_K; E[m]) \end{array}$$

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 the one in the definition of the Selmer group by Remarks 1.86 and 1.110. The rest of the result is a combination of Propositions 1.109 and 1.111. ■

Remark 1.113. The moral is that we may view $\mathrm{Sel}_p(E/K)$ 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 $\mathrm{Sel}_p(E/K)$ is finite-dimensional.

Remark 1.114. If m is prime, then the right vertical arrow in Theorem 1.112 is injective; see [PR12, Theorem 4.14] for a proof. This 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 $E[m]$ is replaced by a different module; see Remark 1.116 below for an example.

Example 1.115 (Counterexamples to Grunwald–Wang)**.** We have the following.

(a) The positive integer 16 is an eighth power in $\mathbb{Q}_v$ for all places v except $v = 2$. However, 16 is not an eighth power in $\mathbb{Q}_2$.

(b) The positive integer 16 is an eighth power in $\mathbb{Q}(\sqrt{7})_v$ for all places v. However, 16 is not an eighth power in $\mathbb{Q}(\sqrt{7})$.

Proof. Before showing either of the parts, we claim that 16 is an eighth power in a field K if and only if $\sqrt{2} \in K$ or $\sqrt{-2} \in K$ or $\sqrt{-1} \in K$. Certainly the reverse direction holds because

$$\left(\sqrt{2}\right)^8 = \left(\sqrt{-2}\right)^8 = (1+i)^8 = 16.$$

In the forward direction, if 16 is an eighth power, then we see that one of 4 or -4 is a fourth power. If -4 is a fourth power, then -4 is a square, so either $2 = 0$ (in which case $\sqrt{2} \in K$) or -1 is a square. Otherwise, 4 is a fourth power, so one of 2 or -2 is a square, as desired.

(a) We do this by casework on the place v. For example, if v is archimedean, the result follows because $\sqrt{2} \in \mathbb{R}$. Additionally, for $v = 2$, we see that $v_2(16) = 4$ is not divisible by 8, so 16 cannot possibly be an eighth power.

It remains to handle places v given by odd primes p. It is enough to show that $\{\sqrt{2}, \sqrt{-2}, i\} \cap \mathbb{Q}_p \neq \varnothing$ for each odd prime p. In other words, we are asking for one of the quadratics to $x^2 - 2$ or $x^2 + 2$ or $x^2 - 1$ to admit a root. By Hensel's lemma, it is equivalent for one of these quadratics to admit a root over $\mathbb{F}_p$, which in turn is equivalent to having

$$1 \overset{?}{\in} \left\{ \left(\frac{2}{p}\right), \left(\frac{-2}{p}\right), \left(\frac{-1}{p}\right) \right\}.$$

To see this, we note that

$$\left(\frac{2}{p}\right)\left(\frac{-2}{p}\right)\left(\frac{-1}{p}\right) = 1,$$

so it is not possible for all three Legendre symbols to equal -1!

(b) Set $K \coloneqq \mathbb{Q}(\sqrt{7})$ for brevity. By (a), to show that 16 is an eighth power in all K_v, we only have to handle places v above 2. Note that 7 is not a square in $\mathbb{Q}_2$ (indeed, it is not a square $\pmod 4$), so there is only one place $\mathbb{Q}_2(\sqrt{7})$ above 2. It remains to show that 16 is an eighth power in $\mathbb{Q}_2(\sqrt{7})$, which is true because $\sqrt{-1} \in \mathbb{Q}_2(\sqrt{7})$ (indeed, $-7 \in \mathbb{Q}_2^{\times 2}$).

Lastly, we should show that 16 is not an eighth power in K. It is enough to show that none of $\sqrt{-1}$ or $\sqrt{2}$ or $\sqrt{-2}$ are in K, which holds because $K = \mathbb{Q}(\sqrt{7})$ is a quadratic extension avoiding all those elements. Explicitly, K is totally real, so -1 and -2 cannot be squares, and we can see that there is no $a, b \in \mathbb{Z}$ for which

$$\left(a + b\sqrt{7}\right)^2 = a^2 + 7b^2 + 14ab\sqrt{7}$$

can equal 2: this would require $a = 0$ or $b = 0$, but certainly neither 2 nor $7/2$ is a square in $\mathbb{Z}$. ∎

Remark 1.116. Example A.4 identifies $\mathrm{H}^1(K; \mu_8)$ with $K^\times / K^{\times 8}$, so the second part of Example 1.115 shows that the map

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

fails to be injective because the nontrivial class $16 \in K^\times / K^{\times 8}$ vanishes in $\mathrm{H}^1\left(\mathbb{A}_{\mathbb{Q}(\sqrt{7})}; \mu_8\right)$.

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 1.117 (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

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

Lemma 1.118. 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

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E[m](\overline{K}) & \longrightarrow & E(\overline{K}) & \xrightarrow{m} & E(\overline{K}) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \prod_v E[m](\overline{K_v}) & \longrightarrow & \prod_v E(\overline{K_v}) & \xrightarrow{m} & \prod_v E(\overline{K_v}) & \longrightarrow & 0 \end{array}$$

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

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E(K)/mE(K) & \longrightarrow & \mathrm{H}^1(K; E[m]) & \longrightarrow & \mathrm{H}^1(K; E)[m] & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \prod_v E(K_v)/mE(K_v) & \longrightarrow & \prod_v \mathrm{H}^1(K_v; E[m]) & \longrightarrow & \prod_v \mathrm{H}^1(K_v; E)[m] & \longrightarrow & 0 \end{array}$$

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

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E(K)/mE(K) & \longrightarrow & \mathrm{Sel}_m(E/K) & \longrightarrow & Ш(E/K)[m] & \longrightarrow & 0 \\ & & \| & & \downarrow & \lrcorner & \downarrow & & \\ 0 & \longrightarrow & E(K)/mE(K) & \longrightarrow & \mathrm{H}^1(K; E[m]) & \longrightarrow & \mathrm{H}^1(K; E)[m] & \longrightarrow & 0 \end{array}$$

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

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

Remark 1.120. Let r be the algebraic rank of E over K so that $E(K) \cong E(K)_{\mathrm{tors}} \oplus \mathbb{Z}^{\oplus r}$. Thus, for any prime p,

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

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

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

Lemma 1.118 now implies that $\mathrm{rank}_{\mathbb{Z}} E(K) + \dim_{\mathbb{F}_p} Ш(E/K)[p] = S_p(E/K)$.

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 1.120.

Conjecture 1.121 (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 1.122 (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 1.123. 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 1.124. Conjecture 1.122 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 1.125. 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 1.96, 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 1.96.

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 1.126. 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 1.125. 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 1.125, 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 $T \coloneqq (a_i,0)$. 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 1.95, 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 1.127. 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 1.126. 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 1.128. Here is a more geometric argument for Corollary 1.127. 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 $T_{(\alpha,\beta,\gamma)}$!

Remark 1.129. After rearranging, solving the system in Corollary 1.127 is equivalent to solving the (projective closure of the) system

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

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 1.130. 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 1.112, 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. ∎

Remark 1.131. For an odd prime ℓ, we see that $K_v^\times/K_v^{\times\ell}$ is always $\{1\}$ when $K_v \in \{\mathbb{R}, \mathbb{C}\}$. When v is finite and p-adic, we similarly find that

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

Here are our two cases.

- If $v \nmid \ell$, then the dimension is $1 + 1_{\ell|\#\mathbb{F}_v - 1} + 0 + 0$.
- If $v \mid \ell$, then the dimension is $1 + 0 + 1_{\zeta_p \in K_v} + [K_v : \mathbb{Q}_p]$.

However, with a little more theory, one can say more.

Lemma 1.132. Fix an elliptic curve E over a nonarchimedean local field K_v. Then $E(K_v)$ admits a finite-index subgroup isomorphic to $\mathcal{O}_v$.

Proof. The proof of this result is fairly involved, so we will be sketchy; we refer to [Sil09, Proposition VII.6.3] for more details. Let $E_0(K_v) \subseteq E(K)$ denote the collection of points which reduce to a non-singular point in $E(\mathbb{F}_v)$, and we let $E_1(K_v) \subseteq E(K)$ denote the collection of points which reduce to the identity of $E(\mathbb{F}_v)$.

The main point is to show that $E(K_v)/E_0(K_v)$ is finite, but for now let's explain why it completes the proof. It turns out that the canonical maps

$$0 \to E_1(K_v) \to E_0(K_v) \to E(\mathbb{F}_v) \to 0$$

assemble into a short exact sequence [Sil09, Proposition VII.2.1]. Thus, it is enough to show that $E_1(K_v)$ admits a finite-index subgroup isomorphic to $\mathcal{O}_v$. Well, $E_1(K_v)$ is isomorphic to $G_E(\mathfrak{m}_v)$, where G_E is the one-dimensional formal group of E [Sil09, Proposition VII.2.2]. Then the canonical filtration $G_E(\mathfrak{m}_v^\bullet)$ shows that $G_E(\mathfrak{m}_v^i)/G_E\left(\mathfrak{m}_v^{i+1}\right)$ is finite for all i, and for i large enough, there is a logarithm map establishing that $G_E(\mathfrak{m}_v^i)$ is isomorphic to $\mathcal{O}_v$. This completes the proof modulo the finiteness of $E(K_v)/E_0(K_v)$.

It remains to show that $E(K_v)/E_0(K_v)$, for which we follow [Sil09, Exercise 7.6]. Because K_v is a topological field, we see that $E(K_v) \subseteq \mathbb{P}^2(K_v)$ is a topological group. In fact, $E(K_v) \subseteq \mathbb{P}^2(K_v)$ is a closed subset of the compact space $\mathbb{P}^2(K_v)$, so $E(K_v)$ is compact. The reduction map $\mathbb{P}^2(K_v) \to \mathbb{P}^2(\mathbb{F}_v)$ is a continuous map to a finite discrete space, so $E_0(K_v) \subseteq E(K_v)$ is an open subgroup. Compactness then forces $E_0(K_v)$ to be finite-index in $E(K_v)$. ∎

Proposition 1.133. Fix an elliptic curve E over field $\mathbb{Q}_p$. For any prime ℓ,

$$\dim_{\mathbb{F}_\ell} E(\mathbb{Q}_p)/\ell E(\mathbb{Q}_p) = \dim_{\mathbb{F}_\ell} E(\mathbb{Q}_p)[\ell] + \begin{cases} 1 & \text{if } p = \ell, \\ 0 & \text{if } p \neq \ell. \end{cases}$$

Thus, $\dim_{\mathbb{F}_\ell} E(\mathbb{Q}_p)/\ell E(\mathbb{Q}_p) \in \{0, 1, 2, 3\}$, where 3 is only possible when $p = \ell$.

Proof. Set $K_v \coloneqq \mathbb{Q}_\ell$ for brevity. We will use Lemma 1.132, which grants us an exact sequence

$$0 \to \mathcal{O}_v \to E(K_v) \to C \to 0,$$

where C is some finite abelian group. This exact sequence has an endomorphism given by multiplication by ℓ. Applying the Snake lemma to this endomorphism yields the exact sequence

$$0 \to \mathcal{O}_v[\ell] \to E(K_v)[\ell] \to C[\ell] \to \frac{\mathcal{O}_v}{\ell\mathcal{O}_v} \to \frac{E(K_v)}{\ell E(K_v)} \to \frac{C}{\ell C} \to 0.$$

The result will follow by taking dimensions of this exact sequence; for example, just the right-exact part of this sequence immediately shows us that $E(K_v)/\ell E(K_v)$ is finite. We thus have

$$\dim_{\mathbb{F}_\ell} \frac{E(K_v)}{\ell E(K_v)} - \dim_{\mathbb{F}_\ell} E(K_v)[\ell] = \dim_{\mathbb{F}_\ell} \frac{\mathcal{O}_v}{\ell\mathcal{O}_v} - \dim_{\mathbb{F}_\ell} \mathcal{O}_v[\ell] + \dim_{\mathbb{F}_\ell} \frac{C}{\ell C} - \dim_{\mathbb{F}_\ell} C[\ell].$$

Now, we note that $\mathcal{O}_v[\ell] = 0$ because K_v has characteristic 0. Continuing, and $\#C_\ell = \#(C/\ell C)$ because the kernel and cokernel of the endomorphism $\ell\colon C \to C$ should have the same size. We are left with

$$\dim_{\mathbb{F}_\ell} \frac{E(K_v)}{\ell E(K_v)} = \dim_{\mathbb{F}_\ell} \frac{\mathcal{O}_v}{\ell\mathcal{O}_v} + \dim_{\mathbb{F}_\ell} E(K_v)[\ell].$$

We now note that $\ell = p$ implies that $\mathcal{O}_v/\ell\mathcal{O}_v \cong \mathbb{Z}/\ell\mathbb{Z}$; otherwise, $\mathcal{O}_v/\ell\mathcal{O}_v = 0$. ∎

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 1.134 (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 1.135. 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 1.136. 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 1.137. 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 $\mathrm{H}^1(\mathbb{Q}; E_d)$ with $\mathrm{H}^1(\mathbb{Q}; H)$. We begin with two technical calculations.

Lemma 1.138. 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 $\delta_v \colon E_d(\mathbb{Q}_v)/2E_d(\mathbb{Q}_v) \to \mathrm{H}^1(\mathbb{Q}_v; H)$ 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

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

(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 1.77, the image of δ_v is $\mathrm{H}^1_{\mathrm{ur}}(\mathbb{Q}_v; H)$. The result now follows by looking coordinate-wise via Example 1.75.

(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 1.130. 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 1.130.

(d) Because -1, 2, and 5 are linearly independent in $\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2}$, we see that the triples $(1,5,5)$, $(-1,-d,d)$, and $(d,2,2d)$ are linearly independent triples. Thus,

$$\dim_{\mathbb{F}_2} \operatorname{span}(S \cup \{1,5,5\}) = 3,$$

which also equals $\dim_{\mathbb{F}_2} \operatorname{im} \delta_v$ by Example 1.130. Thus, it suffices to show that $\operatorname{span}(S \cup \{1,5,5\}) \subseteq \operatorname{im} \delta_v$.

By (b), it is enough to check that $(1,5,5) \in \operatorname{im} \delta_v$. For this, we will use Remark 1.129, which tells us that we need to produce a nonzero solution to the system

$$\begin{cases} x^2 - 5y^2 = +dw^2, \\ x^2 - 5z^2 = -dw^2, \end{cases}$$

in $\mathbb{Q}_2$. The solubility of this system does not change if we change d by an element of $\mathbb{Q}_2^{\times 2}$, so we may assume $d \in \{\pm 1, \pm 5\}$. Similarly, by symmetry, we may adjust the sign of d, so we may assume that $d \in \{1,5\}$. In these cases, we may set $(x,w) = (1,2)$ so that we need $5y^2 \in \{-3,-19\}$ and $5z^2 \in \{5,21\}$, both of which are possible. ∎

We will also need the following technical result.

Lemma 1.139. Fix an odd positive squarefree integer d, and let E be the elliptic curve over $\mathbb{Q}$ which is the projective closure of $y^2 = x(x-d)(x+d)$. Further, fix some triple $(\alpha, \beta, \gamma) \in \mathrm{H}^1(\mathbb{Q}; H)$. If (α, β, γ) is in the image of $\delta_v \colon E_d(\mathbb{Q}_v)/2E_d(\mathbb{Q}_v) \to \mathrm{H}^1(\mathbb{Q}_v; H)$ for each place $v \neq 2$, then it is also in the image of δ_2.

Proof. We use Corollary 1.127, freely using the calculations of Lemma 1.138. Fix a triple (α, β, γ) which is in the image of δ_v for each place $v \neq 2$; we may as well represent (α, β, γ) as a triple of squarefree integers. We will show that $(\alpha, \beta, \gamma) \in \operatorname{im} \delta_2$.

1. Quickly, note that α is odd (modulo squares). Surely this is the case for $(\alpha, \beta, \gamma) \notin \delta_2(E[2])$. Otherwise, by Proposition 1.126, we know α equals the x-coordinate of some $(x, y) \in E(\mathbb{Q}_2)$, meaning

$$y^2 = x\left(x^2 - d^2\right).$$

   We now compute some valuations to show that $\nu_2(x)$ is even, which means α is odd.

   - There is nothing to do if $\nu_2(x) = 0$.
   - If $\nu_2(x) > 0$, then the valuations are $2\nu_2(y) = \nu_2(x)$, so $\nu_2(x)$ is even.
   - If $\nu_2(x) < 0$, then the valuations are $2\nu_2(y) = -3\nu_2(x)$, so $\nu_2(x)$ is still even.

2. We make some reductions. By Lemma 1.138, we know that (α, β, γ) is unramified for $v \nmid 2d\infty$, so the prime factorizations of α, β, and γ are supported in the prime factors of $2d$.

   For our next few reductions, we note that multiplying any triple by the image of $\delta(E[2])$ will not change whether it is in the image of δ_2. For example, with α odd, we see that we may multiply by the triple $(d, 2, 2d)$ to force β to be odd, which in turn forces γ to be odd too. Multiplying by the triple $(-1, -d, d)$, we may assume that $\alpha \pmod 8$ is in $\{1, 5\}$. Similarly, multiplying by the triple $(1, 5, 5)$, we may assume that $\beta \pmod 8$ is in $\{1, 3\}$.

3. We complete the proof using Hilbert symbols. By Remark 1.129, we know that the equations

$$\begin{cases} \alpha x^2 - \beta y^2 = -dw^2, \\ \alpha x^2 - \gamma z^2 = +dw^2 \end{cases}$$

   has solutions in each $\mathbb{Q}_v$ for $v \neq 2$. Thus, $(-d\alpha, d\beta)_v = (d\alpha, -d\gamma)_v = (2d\beta, -2d\gamma)_v = 1$ for each $v \neq 2$, so Hilbert reciprocity[3] implies that

$$(-d\alpha, d\beta)_2 = (d\alpha, -d\gamma)_2 = (2d\beta, -2d\gamma)_2 = 1.$$

   We now show that $(\alpha, \beta, \gamma) \in \operatorname{im} \delta_2$ directly. We may consider this triple up to $\mathbb{Q}_2^{\times 2}$, meaning that we may assume $\alpha \in \{1, 5\}$ and $\beta \in \{1, 3\}$. For example, because everything is odd and $\alpha \in \{1, 5\}$, we see that $(\alpha, d)_2 = (\alpha, \beta)_2 = (\alpha, \gamma)_2 = 1$.[4] As such, $(-d\alpha, d\beta)_2 = (-d, \beta)_2$ and $(d\alpha, -d\gamma)_2 = (d, \beta)_2$, so $(-1, \beta)_2 = 1$. Thus, $\beta \neq 3$ is forced,[5] so $\gamma = 1$ follows. ∎

We now proceed with the proof of Theorem 1.135.

Proof of Theorem 1.135. We have identified $\mathrm{H}^1(\mathbb{Q}; E_d[2])$ with the trace-zero hyperplane of $\left(\mathbb{Q}^\times/\mathbb{Q}^{\times 2}\right)^3$. Now, let $\mathcal{L}_v \subseteq \left(\mathbb{Q}^\times/\mathbb{Q}^{\times 2}\right)^3$ be the corresponding local condition of the Selmer group at the place v, as computed in Lemma 1.138. 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

[3] In this case, it is possible to unwind the application of Hilbert reciprocity into merely applications of Quadratic reciprocity, but this language is convenient anyway.

[4] In particular, $(5, -)_2$ vanishes on odds. It is not hard to show $(5, -5)_2 = 1$ (because $5 \cdot 1^2 - 5 \cdot 1^2 = 0^2$), and $(5, -1)_2 = 1$ because $5 \cdot 1^2 - 1 \cdot 1^2 = 2^2$.

[5] We need to show that $(-1, 3)_2 = -1$, which holds because $3x^2 - y^2 = z^2$ has no nontrivial solutions by $\pmod 8$ considerations.

(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 1.138, 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 1.139 combined with Corollary 1.127, 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 1.140. 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

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

Proof. The proof of Theorem 1.135 shows that

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

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 1.135, 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 1.141. 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 1.66. We say that $\mathcal{L}$ is *self-dual* if and only if there is a choice of isomorphism $M \to M^*$ sending $\mathcal{L}$ to $\mathcal{L}^*$.

Remark 1.142. 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 1.79), so M^* is as well, and whenever $\mathcal{L}_v = \mathrm{H}^1_{\mathrm{ur}}(K_v; M)$, Proposition 1.76 tells us that the annihilator of $\mathcal{L}_v$ is

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

Remark 1.143. 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 1.144. 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 1.96). Furthermore, this isomorphism makes $\mathcal{L}_v$ a maximal isotropic subspace by Proposition 1.109, 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 1.145. 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 1.146. An equivalent way to view Remark 1.145 is to say that the square

$$\begin{array}{ccc} \mathrm{Sel}_{\mathcal{L}}(M) & \longrightarrow & \mathrm{Sel}_{\mathcal{L}'}(M) \\ \downarrow & & \downarrow \\ \prod_v \mathcal{L}_v & \longrightarrow & \prod_v \mathcal{L}'_v \end{array}$$

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 1.147. 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 1.66).

Remark 1.148. Let's explain why the given pairing is even well-defined. By Theorem 1.66, 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, as stated in Theorem 1.78.

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

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

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 $\widetilde{c}' \in \mathrm{Sel}_{\mathcal{L}^*}(M^*)$. This is then equivalent to saying that the sequence

$$\mathrm{Sel}_{\mathcal{L}'}(M) \overset{\pi_M}{\to} \prod_v \frac{\mathcal{L}'_v}{\mathcal{L}_v} \overset{\pi^\vee_{M^*}}{\to} \mathrm{Sel}_{\mathcal{L}^*}(M^*)^\vee$$

is exact, where $(-)^\vee := \mathrm{Hom}_{\mathbb{Z}}(-, \mathbb{Q}/\mathbb{Z})$ 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 1.66.

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

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

   By symmetry, it is enough to just handle the left equality. Well, $\mathrm{Sel}_{\mathcal{L}'}(M)$ 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 1.78, which provides us with an exact sequence

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

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

$$\begin{array}{ccccc} \mathrm{Sel}_{\mathcal{L}'}(M) & \longrightarrow & \prod_v \frac{\mathcal{L}'_v}{\mathcal{L}_v} & \longrightarrow & \mathrm{Sel}_{\mathcal{L}^*}(M^*)^\vee \\ \downarrow & & \downarrow & & \| \\ \mathrm{Sel}_{\mathcal{L}'_0}(M) & \longrightarrow & \prod_v \frac{\mathcal{L}'_{0v}}{\mathcal{L}_v} & \longrightarrow & \mathrm{Sel}_{\mathcal{L}^*}(M^*)^\vee \end{array}$$

   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 1.146.

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 1.149. Given local conditions $\mathcal{L} \subseteq \mathcal{L}'$ of M, then Theorem 1.147 shows that one of the two maps

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

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 1.148), 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 1.150 (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

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

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 1.151. 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 1.152. 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 1.153. Fix a finite set of places Σ. If the map $\mathrm{Sel}_\mathcal{L}(M) \to \bigoplus_{v\in\Sigma} \mathcal{L}_v$ is surjective, then we claim that the map

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

vanishes. Indeed, this follows from Example 1.149 (and Example 1.152) 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 a technical result, which finds its application in the next subsection.

Lemma 1.154. Fix a number field K and a finite self-dual Galois module M which is a vector space over $\mathbb{F}_p$. Let $\mathcal{L}$ be a self-dual local condition. Letting Σ be the singleton of a place v_0, we have

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

Proof. Remark 1.145 provides us with the exact sequences

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

and

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

and Theorem 1.147 tells us that the images in the rightmost terms are orthogonal complements (where we have silently used Example 1.152). 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

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

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

Example 1.155. 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 1.109.

Lemma 1.156. 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 $\mathrm{Sel}_\mathcal{L}(E[p]) \to \mathrm{H}^1(K_{v_0}; E[p])$ vanishes, then

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

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

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

Proof. All the hypotheses will be used, though much care will be required. Set $M \coloneqq E[p]$ and $\Sigma \coloneqq \{v_0\}$ 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

$$\begin{array}{ccc} \mathrm{Sel}_{\mathcal{L}_\Sigma}(M) & \longrightarrow & \mathrm{Sel}_{\mathcal{L}'}(M) \\ \downarrow & \lrcorner & \downarrow \\ \mathrm{Sel}_{\mathcal{L}}(M) & \longrightarrow & \mathrm{Sel}_{\mathcal{L}^\Sigma}(M) \end{array} \tag{1.1}$$

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

(a) The exactness of

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

from Remark 1.145 implies that the inclusion $\mathrm{Sel}_{\mathcal{L}_\Sigma}(M) \to \mathrm{Sel}_{\mathcal{L}}(M)$ 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 1.154.

(b) We are given that $\mathrm{Sel}_{\mathcal{L}}(M) \to \mathcal{L}_\ell$ is surjective, so Example 1.153 implies that the exact sequence

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

of Remark 1.145 maps to 0 at the end, so the inclusion $\mathrm{Sel}_{\mathcal{L}}(M) \to \mathrm{Sel}_{\mathcal{L}^\Sigma}(M)$ is an isomorphism. (We are silently using $\mathcal{L} = \mathcal{L}^*$ and Example 1.152.) Thus, the bottom arrow of (1.1) is an isomorphism, so the top arrow is also an isomorphism. The claim now follows from Lemma 1.154. ∎

1.5.3 Application to Congruent Number Elliptic Curves

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

Lemma 1.157. 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 1.109. For (b), we use Lemma 1.138. 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 1.109).

We now show (c) by casework, going place-by-place; we will use Lemma 1.138 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 1.158. 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 1.135. 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 1.140. In particular, it follows that $\mathrm{Sel}_2(E)$ 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 1.157 are satisfied, so Lemma 1.156 kicks in and yields $S_2(E') = S_2(E) + 2 = 2$.

In fact, we can upgrade this argument as follows.

Proposition 1.159. Fix a set S of primes such that each pair (ℓ_1,ℓ_2) of primes in S have $\ell_1,\ell_2 \equiv 1 \pmod 8$ and $\ell_1 \in \mathbb{Q}_{\ell_2}^{\times 2}$. Further, let d be the product of the primes in S, and let E be the projective closure of $y^2 = x(x-d)(x+d)$. Then

$$\dim_{\mathbb{F}_2} \mathrm{Sel}_2(E) = 2\#S + 2.$$

Proof. We induct on $\#S$. For $\#S = 0$, this follows from Corollary 1.140 because $\dim_{\mathbb{F}_2} E[2](\mathbb{Q}) = 2$ already.

For the induction, suppose we have the statement for S and d, and we would like to show it for $S \cup \{\ell\}$ for some prime $\ell \notin S$ which is $1 \pmod 8$ and a square modulo every prime of S. Accordingly, let E and E' be the projective closures of $y^2 = x(x-d)(x+d)$ and $y^2 = x(x-d\ell)(x+d\ell)$. We would like to show that

$$\dim_{\mathbb{F}_2} \mathrm{Sel}_2(E') \stackrel{?}{=} \dim_{\mathbb{F}_2} \mathrm{Sel}_2(E) + 2.$$

Note that all parts of Lemma 1.157 are satisfied, so Lemma 1.156 applies, so it remains to show that the map $\mathrm{Sel}_2(E) \to \mathrm{H}^1(\mathbb{Q}_\ell; E[2])$ vanishes. Well, the calculation of Theorem 1.135 shows that each class in $\mathrm{Sel}_2(E)/E[2]$ is represented by a triple in

$$\{(\alpha,\beta,\gamma) \in \mathbb{Z} : \alpha,\beta,\gamma \mid 2d, \alpha\beta\gamma \text{ is square}\}.$$

We now claim that each triple (α,β,γ) in the larger right-hand set is trivial in $\mathrm{H}^1(\mathbb{Q}_\ell; H)$, which will complete the proof. To show the claim, it is enough to see that -1, 2, and every prime dividing d are all squares in $\mathbb{Q}_\ell$. The first two arise because $\ell \equiv 1 \pmod 8$, and the last is true by quadratic reciprocity. ■

Here is a more involved application.

Proposition 1.160. Fix a set S of primes such that each pair (ℓ_1,ℓ_2) of primes in S have $\ell_1,\ell_2 \equiv 5 \pmod 8$ and $\ell_1 \notin \mathbb{Q}_{\ell_2}^{\times 2}$. Further, suppose that $\#S$ is odd, and let d be the product of the primes in S. Letting E denote the projective closure of $y^2 = x(x-d)(x+d)$, we have

$$\dim_{\mathbb{F}_2} \mathrm{Sel}_2(E) = 3.$$

Proof. Using the notation of Theorem 1.135, we will show the stronger statement that

$$\mathrm{Sel}_2(E) \stackrel{?}{=} \mathrm{span}(E[2] \cup \{(1,d,d)\}).$$

The rank claim then follows because the triples $\{(-1,-d,d),(d,2,2d),(1,d,d)\}$ form a basis. For this, we induct on $\#S$, where $\#S=1$ follows from Theorem 1.135.

For the induction, suppose we have the statement for S and d, and we would like to show it for some set $S\cup\{\ell_1,\ell_2\}$ still satisfying the list of conditions; set $\ell\coloneqq\ell_1\ell_2$ for brevity. Accordingly, let E and E' be the projective closures of $y^2=x(x-d)(x+d)$ and $y^2=(x-d\ell)(x+d\ell)$. Let $\mathcal{L}$ and $\mathcal{L}'$ be the associated local conditions of $\mathrm{H}^1(\mathbb{A}_K;H)$, where $E[2]$ and $E'[2]$ are identified with H as in Theorem 1.135.

Quickly, let's compare our local conditions $\mathcal{L}$ and $\mathcal{L}'$, freely using Lemma 1.138.

- For $v\nmid 2d\ell\infty$, we see that $\mathcal{L}_v$ and $\mathcal{L}'_v$ both contain the unramified triples.
- For $v=\infty$, both are the same.
- For finite $v=p$ with $p\mid d$, we claim that $\mathcal{L}_v=\mathcal{L}'_v$. Well, the sizes are the same, so it is enough to just get an inclusion, so it is enough to check $\{(-1,-d\ell,d\ell),(d\ell,2,2d\ell)\}\subseteq\mathcal{L}_p$, which is equivalent to having $\{(1,\ell,\ell),(\ell,1,\ell)\}\subseteq\mathcal{L}_p$. But this is true because $\ell=\ell_1\ell_2$ is a square in $\mathbb{Q}_p^\times$.
- For $v=2$, it is once again enough to achieve the inclusion $\{(1,\ell,\ell),(\ell,1,\ell)\}\subseteq\mathcal{L}_2$. This is true because $\ell\equiv 1\pmod 8$, so $\ell\in\mathbb{Q}_2^{\times 2}$.
- Lastly, for $v\in\{\ell_1,\ell_2\}$, we see that $\mathcal{L}_v$ contains unramified triples, but the only unramified triple in $\mathcal{L}'_v$ is the trivial one, so $\mathcal{L}_v\cap\mathcal{L}'_v$ is trivial.

Thus, we see that we are going to use Lemma 1.156 twice. Accordingly, let $\mathcal{L}''$ be an "intermediate" local condition given by

$$\mathcal{L}''_v\coloneqq\begin{cases}\mathcal{L}_v & \text{if } v\neq\ell_1,\\ \mathcal{L}'_v & \text{if } v=\ell_1.\end{cases}$$

Thus, $\mathcal{L}$ and $\mathcal{L}''$ differ only at the place $v=\ell_1$, and $\mathcal{L}''$ and $\mathcal{L}'$ differ only at the place $v=\ell_2$. We now have two steps.

1. We claim that $\mathrm{Sel}_{\mathcal{L}''}(H)=\{(1,1,1),(-1,-1,1)\}$. One inclusion is not so bad: certainly $(1,1,1)\in\mathrm{Sel}_{\mathcal{L}''}(H)$. Additionally, $(1,-1,-1)\in\mathrm{Sel}_{\mathcal{L}''}(H)$ because it is already in $\mathcal{L}_v$ for all v, and $(1,-1,-1)\in\mathcal{L}_{\ell_1}$ because $(-1,-1,1)$ equals $(1,1,1)$ up to squares in $\mathbb{Q}_{\ell_1}^\times$.

   For the other inclusion, it is enough to check that

   $$\dim_{\mathbb{F}_2}\mathrm{Sel}_{\mathcal{L}''}(H)=\mathrm{Sel}_{\mathcal{L}}(H)-2.$$

   For this, we use Lemma 1.156(b) at the place $v_0=\ell_1$. The hypotheses on the local conditions were checked above, so it remains to check that the map $\mathrm{Sel}_{\mathcal{L}}(H)\to\mathcal{L}_{\ell_1}$ is surjective. This holds by the calculation of Lemma 1.138 by using the global triples coming from $E[2]$.

2. We claim that $\mathrm{Sel}_{\mathcal{L}'}(H)=\mathrm{span}(E'[2]\cup\{(1,d\ell,d\ell)\}$, which will complete the proof. Again, one inclusion is not so bad: certainly $E'[2]$ provides elements of the Selmer group. Additionally, we once again see that $(1,d\ell,d\ell)\in\mathrm{Sel}_{\mathcal{L}'}(H)$ by checking place-by-place: along with the checks from the previous step, we merely have to check that $(1,d\ell,d\ell)\in\mathcal{L}'_{\ell_2}$, which is true because this triple is equivalent to $(-1,-d\ell,d\ell)$ up to squares.

   For the other inclusion, we will again use ranks, noting that it is enough to check that

   $$\dim_{\mathbb{F}_2}\mathrm{Sel}_{\mathcal{L}'}(H)=\mathrm{Sel}_{\mathcal{L}''}(H)+2,$$

   which will follow from Lemma 1.156(b) at the place $v_0=\ell_2$. Again, the hypotheses on the local conditions are satisfied, so it remains to check that the map $\mathrm{Sel}_{\mathcal{L}''}(H)\to\mathcal{L}''_{\ell_2}$ is trivial. Well, from the calculation in the previous step, we know that $\mathrm{Sel}_{\mathcal{L}''}(H)=\{(1,1,1),(-1,-1,1)\}$, and both of these elements are trivial up to squares in $\mathbb{Q}_{\ell_2}^\times$. ∎

Remark 1.161. 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.

1.6 September 30

This week, we will prove Koymans–Pagano's theorem.

1.6.1 The Theorem and Its Application

Quickly, let's recall the statement that we are going to sketch, which is [KP25, Theorem 2.4].

Theorem 1.162 (Koymans–Pagano)**.** Fix a quadratic extension $K(i)/K$ of number fields, and further assume that K has at least 32 real places. Then there is an elliptic curve E over K such that

$$\operatorname{rank} E(K) = \operatorname{rank} E(K(i)) > 0.$$

Let's say something about the application of Theorem 1.162, which is to Hilbert's 10th problem.

Definition 1.163 (Diophantine)**.** Fix a number field K. Then a subset $S \subseteq \mathcal{O}_K$ is *Diophantine* if and only if there is an affine scheme X of finite type over $\mathcal{O}_K$ and a morphism $\pi\colon X \to \mathbb{A}^1_{\mathcal{O}_L}$ such that $S = \pi(X(\mathcal{O}_K))$.

Remark 1.164. In other words, there are polynomials $f_1, \dots, f_m \in \mathcal{O}_K[t, x_1, \dots, x_n]$ such that S consists of the values $t \in \mathcal{O}_L$ for which

$$\begin{cases} f_1(t, x_1, \dots, x_n) = 0, \\ \quad \vdots \\ f_m(t, x_1, \dots, x_n) = 0 \end{cases}$$

admits a solution in $\mathcal{O}_L$. Indeed, the above is equivalent to asserting that S is the image of the map

$$\operatorname{Spec} \frac{\mathcal{O}_K[t, x_1, \dots, x_n]}{(f_1, \dots, f_m)} \to \mathbb{A}^1_{\mathcal{O}_K}$$

given by projecting onto the t coordinate.

Remark 1.165. One can remove the "affine" hypothesis from X. Indeed, it is enough to show that the collection of Diophantine subsets is closed under finite unions. Well, one simply has to note that t satisfies one of two systems of equations $\{f_i(t, \overline{x})\}_i$ or $\{g_j(t, \overline{y})\}_j$ if and only if it satisfies the single system of equations

$$\{f_i(t, \overline{x}) g_j(t, \overline{y})\}_{i,j}.$$

Remark 1.166. One can reduce to a system of equations having a single equation, possibly in many variables. It is enough to explain how to take a system of two equations $f(t, \overline{x})$ and $g(t, \overline{y})$ and produce a single equation. Well, choose a homogeneous polynomial $h \in \mathcal{O}_L[x, y]$ with no nonzero solution. Then t satisfies both $f(t, \overline{x})$ and $g(t, \overline{y})$ if and only if t satisfies the composite polynomial $h(f(t, \overline{x}), g(t, \overline{x}))$.

Then Theorem 1.162 is the key input in the following result.

Theorem 1.167 (Koymans–Pagano)**.** Fix a number field K. Then $\mathbb{Z} \subseteq \mathcal{O}_K$ is Diophantine.

Remark 1.168. Let's explain the significance of this result. Building on work of Davis, Putnam, and Robinson, Matiyasevich used Pell equations to show that there is no algorithm which can determine if a subset of $\mathbb{Z}$ is Diophantine [Mat70]. Theorem 1.167 then shows that there is no algorithm which can determine if a subset of $\mathcal{O}_K$ is Diophantine: indeed, because $\mathbb{Z} \subseteq \mathcal{O}_K$ is Diophantine, every subset Diophantine subset of $\mathbb{Z}$ is now a Diophantine subset of $\mathcal{O}_K$.

Theorem 1.167 is proven thanks to the following reduction of [Shl08].

Theorem 1.169. Fix a finite extension L/K of number fields. If there is an abelian variety A over K such that

$$\operatorname{rank} A(L) = \operatorname{rank} A(K) > 0,$$

then $\mathcal{O}_K \subseteq \mathcal{O}_K$ is a Diophantine subset.

In order to explain how this applies, we need the following "base case" of [Den80].

Theorem 1.170 (Denef)**.** Fix a totally real number field K. Then $\mathbb{Z} \subseteq \mathcal{O}_K$ is Diophantine.

We will also need some flexibility to make our reductions.

Proposition 1.171. Fix an extension L/K of number fields.

(a) Diophantine subsets of $\mathcal{O}_K$ are closed under finite intersection.

(b) If $\mathbb{Z} \subseteq \mathcal{O}_K$ is Diophantine, and $\mathcal{O}_K \subseteq \mathcal{O}_L$ is Diophantine, then $\mathbb{Z} \subseteq \mathcal{O}_L$ is Diophantine.

(c) If $\mathbb{Z} \subseteq \mathcal{O}_L$ is Diophantine, then $\mathbb{Z} \subseteq \mathcal{O}_K$ is Diophantine.

Proof. We show the parts separately, following [DL78, Proposition 1].

(a) Take the fiber product of the schemes whose image are giving the provided Diophantine subsets.

(b) We may cut out $\mathbb{Z} \subseteq \mathcal{O}_L$ by first cutting out $\mathcal{O}_K \subseteq \mathcal{O}_L$ by polynomials and then appending the polynomials which cut out $\mathbb{Z} \subseteq \mathcal{O}_K$.

(c) This follows because $\mathcal{O}_L$ is a finitely presented $\mathcal{O}_K$-module. Indeed, one can simply replace all coefficients in $\mathcal{O}_L$ with formal sums of a generating set from $\mathcal{O}_K$ subject to certain relations. ∎

Proof that Theorem 1.162 implies Theorem 1.167. We follow [KP25, Theorem 2.6]. To match our application, we change variables somewhat. Let F be a number field so that we want to show $\mathbb{Z} \subseteq \mathcal{O}_F$ is Diophantine. We let E be some totally real multiquadratic field of degree 64, and we set L to be the normal closure of $EF(i)$. By Proposition 1.171, it is enough to $\mathbb{Z} \subseteq \mathcal{O}_L$ is Diophantine. We now proceed in steps.

1. Suppose $L = K(i)$ for some field K containing E with at least one real place. Then we claim that $\mathcal{O}_K \subseteq \mathcal{O}_L$ is Diophantine. By Theorem 1.169, it is enough to find an elliptic curve E with $\operatorname{rank} E(L) = \operatorname{rank} E(K) > 0$, which is what we will use Theorem 1.162 for. For this, it remains to show that K has at least 32 real places. In fact, we will show that the number of real embeddings is

$$\frac{1}{2}\#C_{\mathrm{Gal}(L/\mathbb{Q})}(\mathrm{Gal}(L/K)).$$

To see why this completes the proof, note that this centralizer equals $[L : \mathbb{Q}]$ divided by the number of elements conjugate to an element in $\mathrm{Gal}(L/K)$, but $E \subseteq K$ means that being conjugate to an element in $\mathrm{Gal}(L/K)$ requires being conjugate to an element in $\mathrm{Gal}(L/E)$ (because $E/\mathbb{Q}$ is Galois). So the size of the centralizer is lower-bounded by $[E : \mathbb{Q}] = 64$.

It remains to count these real embeddings. Fix some real embedding $\sigma\colon K \hookrightarrow \mathbb{R}$, which we extend to some embedding $\widetilde{\sigma}\colon L \hookrightarrow \mathbb{C}$. Then the other archimedean embeddings of K look like $\widetilde{\sigma} \circ \tau$ for

$\tau \in \mathrm{Gal}(L/\mathbb{Q})$. Now, we note that $\widetilde{\sigma} \circ \tau$ is a real embedding of K if and only if it is equal to its conjugate, which one can check is equivalent to commuting with $\mathrm{Gal}(L/K)$. Pairing off the (complex!) embeddings τ of L completes the counting.

2. We now let M be the intersection of all fields K containing E with at least one real place and for which $L = K(i)$. By the previous step and Proposition 1.171, we see that $\mathcal{O}_M \subseteq \mathcal{O}_L$ is Diophantine, so by Proposition 1.171 again, it is enough to show that $\mathbb{Z} \subseteq \mathcal{O}_M$ is Diophantine. In fact, we claim that M is totally real, from which the claim follows by Theorem 1.170. Indeed, to see that M is totally real, we note that M is Galois over $\mathbb{Q}$ because it is an intersection of a Galois-invariant collection of fields. Further, M has at least one real places, so it follows that M is totally real! ■

1.6.2 Reduction to Selmer Groups

We now outline the proof of Theorem 1.162, which will be done by controlling some quadratic twists.

Definition 1.172 (quadratic twist)**.** For an elliptic curve E over a field K (not of characteristic two) cut out by the equation $y^2 = x^3 + ax^2 + bc + c$, the *quadratic twist* E^t by some $t \in K^\times/K^{\times 2}$ is the elliptic curve cut out by the equation.

$$ty^2 = x^3 + ax^2 + bx + c.$$

Remark 1.173. There is an isomorphism from E to E^t over the quadratic extension $\mathbb{Q}(\sqrt{t})$ given by $(x, y) \mapsto (x, y/\sqrt{t})$. Note that this isomorphism is not defined over K!

Remark 1.174. Note that the given equation for E^t is equivalent to

$$\left(t^2 y\right)^2 = (tx)^3 + at(tx)^2 + bt^2(tx) + ct^3,$$

so E^t could also be cut out by the equation

$$y^2 = x^3 + atx^2 + bt^2 x + c.$$

For example, in the case where E is cut out by $y^2 = (x-a_1)(x-a_2)(x-a_3)$, this latter equation becomes the convenient equation $y^2 = (x - a_1 t)(x - a_2 t)(x - a_3 t)$.

Remark 1.175. Here is the important point of quadratic twists: the isomorphism $E_L^t \cong E_L$ given by $(x, y) \mapsto (x, y/\sqrt{t})$ induces an embedding

$$\iota \colon E^t(K) \hookrightarrow E(L).$$

Now, write $\mathrm{Gal}(L/K) = \{1, \sigma\}$, and we claim that the image of ι is exactly the subgroup of $E(L)$ such that σ acts by -1: indeed, $-(x, y) = (x, -y)$, so $\sigma(x, y) = -(x, y)$ if and only if $x \in K$ and $y \in K/\sqrt{t}$. Writing $(x', y') \coloneqq (x, y/\sqrt{t})$, we then see that $(x, y) \in E(L)$ if and only if $(x', y') \in E^t(K)$.

Lemma 1.176. Fix a number field K, and let $L = K(\sqrt{t})$ be a quadratic extension, where $t \in K^\times/K^{\times 2}$ is nontrivial. For any elliptic curve E over K, we have

$$\operatorname{rank} E(L) = \operatorname{rank} E(K) + \operatorname{rank} E^t(K).$$

Proof. For concreteness, we present E and E^t as cut out by the equations $y^2 = x^3 + ax^2 + bx + c$ and $ty^2 = x^3 + ax^2 + bx + c$, respectively. Because $E(K)$ is a finitely generated group, we can compute its rank

as $\dim_{\mathbb{Q}} E(K)_{\mathbb{Q}}$. This applies to the other elliptic curves as well, so we are left to show

$$\dim_{\mathbb{Q}} E(L)_{\mathbb{Q}} = \dim_{\mathbb{Q}} E(K)_{\mathbb{Q}} + \dim_{\mathbb{Q}} E^t(K)_{\mathbb{Q}}.$$

Now, because E is defined over K, the set $E(L)$ admits an action by $\mathrm{Gal}(L/K)$. But $\mathrm{Gal}(L/K)$ has two elements, which we denote $\{1, \sigma\}$. Then $\sigma^2 = 1$ splits over $\mathbb{Q}$ and so implies that the representation $E(L)$ of $\mathrm{Gal}(L/K)$ splits into eigenspaces of σ as $V_+ \oplus V_-$ where σ acts on V_+ by $+1$ and acts on V_- by -1. We now compute these spaces.

- We claim $E(K)_{\mathbb{Q}} = V_+$. Indeed, $(x, y) \otimes q \in E(L) \otimes \mathbb{Q}$ is fixed by σ if and only if $(x, y) \in E(K)$.
- We claim $E^t(K)_{\mathbb{Q}} \cong V_-$. Indeed, $(x, y) \otimes q \in E(L) \otimes \mathbb{Q}$ has eigenvalue -1 if and only if (x, y) comes from $E^t(K)$ via Remark 1.175.

Summing the above two calculations completes the proof. ∎

As such, to show Theorem 1.162, we will instead sketch the following.

Theorem 1.177 (Koymans–Pagano)**.** Fix a quadratic extension $K(i)/K$ of number fields, and further assume that K at least 32 real places. Then there is an elliptic curve E over K and $t \in K^\times/K^{\times 2}$ for which $E[2](\overline{K}) = E[2](K)$ and

$$\dim_{\mathbb{F}_2} \mathrm{Sel}_2(E^t/K) = 2 \qquad \text{and} \qquad \mathrm{rank}\, E^{-t}(K) > 0.$$

Proof that Theorem 1.177 implies Theorem 1.162. We claim that E^{-t} is the elliptic curve we are looking for, so we have to show that $\mathrm{rank}\, E^{-t}(K(i)) = \mathrm{rank}\, E^{-t}(K)$. Well, by Lemma 1.176, it is enough to show that

$$\mathrm{rank}\left(E^{-t}\right)^{-1}(K) = 0.$$

But of course, $(E^{-t})^{-1} = E^t$ (for example, by unwinding our definition of the quadratic twists), so we want to show that $\mathrm{rank}\, E^t(K) = 0$. Now, Lemma 1.118 tells us that

$$\dim_{\mathbb{F}_2} \mathrm{Sel}_2(E^t/K) \geq \dim_{\mathbb{F}_2} \frac{E(K)}{2E(K)}.$$

Because $E[2](K) = E[2](\overline{K})$, this right-hand side is $2 + \mathrm{rank}\, E(K)$, so $\dim_{\mathbb{F}_2} \mathrm{Sel}_2(E^t/K) = 2$ enforces $\mathrm{rank}\, E(K) = 0$. ∎

Remark 1.178. An examination of the inequality at the end produced by Lemma 1.118 shows that this proof has also verified that the elliptic curve constructed in Theorem 1.177 has $Ш(E/K)[2] = 0$. It may be interesting to construct curves with controlled Ш in addition.

1.6.3 Twisting for Rank

We will only manage to sketch Theorem 1.177. Our argument is based on two ideas.

- One can use 2-Selmer groups to control ranks under quadratic twists. Because this is a bound on Selmer groups, this only gives an upper bound of a rank.
- One can sometimes construct explicit non-torsion rational points on elliptic curves. This only gives a lower bound of a rank.

We will return to the first point shortly. For now, let's explain the second. It is fairly explicit: suppose we write E as the projective closure of

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

for $a_1, a_2, a_3 \in \mathcal{O}_K$. If we plug in $x = c/d$, then our right-hand side is

$$\prod_{i=1}^{3}(x-a_i) = \frac{1}{d^4}\cdot d\prod_{i=1}^{3}(c-a_i d).$$

Thus, if we set $t := d\prod_{i=1}^{3}(c-a_i d)$, then E^t is the projective closure by $ty^2 = (x-a_1)(x-a_2)(x-a_3)$, which has the rational point $(c/d, 1/d^2)$ by construction. If c/d is "generic," then this should even provide us with a non-torsion rational point.

Lemma 1.179. Fix an elliptic curve E defined over a number field K. For any positive integer d,

$$\bigcup_{[L:K]<d} E(L)_{\mathrm{tors}}$$

is finite.

Proof. We use the theory of the Néron–Tate height $\hat{h}$, which is summarized in [Sil09, Theorem 9.3]. Indeed, we note that $\hat{h}$ vanishes on $E(\overline{K})_{\mathrm{tors}}$, so the union in question is a set of bounded height and degree, so it is finite by Northcott's property (of heights). ∎

Proposition 1.180. Fix an elliptic curve E defined over a number field K. For all but finitely many $t \in K^\times/K^{\times 2}$, we have $E^t(K)_{\mathrm{tors}} = E^t(K)[2]$.

Proof. We use Lemma 1.179, following [KP25, Lemma 3.2]. It is enough to show that

$$E^t(K(\sqrt{t}))_{\mathrm{tors}} \overset{?}{\subseteq} E^t(K)[2]$$

for all but finitely many t.

We now apply Lemma 1.179: after embedding $E^t(K) \hookrightarrow E(K(\sqrt{t}))$ via Remark 1.175, the union over all $K(\sqrt{t})$ of the left-hand side must be a finite set. Thus, for all but finitely many t, we need to have $E(K)_{\mathrm{tors}} \subseteq E(K)_{\mathrm{tors}}$ for a distinct $s \in K^\times/K^{\times 2}$. But after the embedding of Remark 1.175, we see that the intersection of $E^t(K)$ and $E^s(K)$ in $E(K(\sqrt{s},\sqrt{t}))$ must live in $E(K)$ and thus by fixed by the Galois actions. But the image of $E^t(K)$ is the Galois submodule with eigenvalue -1, so it follows that the intersection is contained in $E(K)[2] = E^t(K)[2]$. ∎

Thus, we will be able to focus on calculating Selmer ranks for twists of specific type.

Theorem 1.181 (Koymans–Pagano)**.** Fix a quadratic extension $K(i)/K$ of number fields, and further assume that K has at least 32 real places. Then there is an elliptic curve E over K cut out by $y^2 = (x-a_1)(x-a_2)(x-a_3)$ for $a_1, a_2, a_3 \in \mathcal{O}_K$ with the following property: there are infinitely many $t \in K^\times/K^{\times 2}$ of the form $d\prod_{i=1}^{3}(c+a_i d)$ (where $m, c, d \in \mathcal{O}_K$) and

$$\dim_{\mathbb{F}_2} \mathrm{Sel}_2(E^t/K) = 2.$$

Proof that Theorem 1.181 implies Theorem 1.177. We only have to check that $\operatorname{rank} E^{-t}(K) > 0$. As argued above Lemma 1.179, when t takes the form $d\prod_{i=1}^{3}(c+a_i d)$, the twist E^{-t} cut out by the equation

$$-d(c+a_1d)(c+a_2d)(c+a_3d)y^2 = (x-a_1)(x-a_2)(x-a_3)$$

contains the K-rational point $\left(-c/d, 1/d^2\right)$. Now, by Proposition 1.180, for all but finitely many t, the only torsion points of $E^{-t}(K)$ are 2-torsion, which are either ∞ or are an affine point (x,y) with $y=0$. This means that the constructed point $\left(-c/d, 1/d^2\right)$ is in fact non-torsion, so $\operatorname{rank} E^{-t}(K) > 0$ follows. ■

1.7 October 2

There is no class next Tuesday. We began class by proving Theorem 1.184; I have moved the proof there.

1.7.1 Twisting for Selmer Rank

As usual, fix some elliptic curve E which is the projective closure $y^2 = (x-a_1)(x-a_2)(x-a_3)$. For any local condition $\mathcal{L} \subseteq \mathrm{H}^1(\mathbb{A}_K; E[2])$, we may form a Selmer group $\mathrm{Sel}_{\mathcal{L}}(E[2])$, which may or may not actually come globally from an elliptic curve.

We now note there is a distinguished element among the Lagrangian subspaces of $\mathrm{H}^1(\mathbb{A}_K; E[2])$, given by the unramified cohomology.

Definition 1.182 (transverse)**.** A Lagrangian subspace $\mathcal{L}_v \subseteq \mathrm{H}^1(K_v; E[2])$ is *transverse* if and only if

$$\mathcal{L}_v \cap \mathrm{H}^1(K_v; E[2]) = 0.$$

Following our calculation from the congruent number elliptic curves, we see that the image of $E[2](K_v) \to \mathrm{H}^1(K_v; E[2])$ is spanned by

$$\{(a_3-a_1, a_3-a_2, (a_3-a_1)(a_3-a_2)), (a_2-a_1, (a_2-a_1)(a_2-a_3), a_2-a_3)\}.$$

On the other hand, if we twist this by some uniformizer ϖ_v of K_v, then the image of $E^{\varpi_v}[2] \to \mathrm{H}^1(K_v; E[2])$ is spanned by

$$\{(\varpi_v(a_3-a_1), \varpi_v(a_3-a_2), (a_3-a_1)(a_3-a_2)), (\varpi_v(a_2-a_1), (a_2-a_1)(a_2-a_3), \varpi_v(a_2-a_3))\}.$$

For example, if $v(a_i - a_j) = 0$, we can immediately see that these vectors are nonzero and linearly independent, so we already have a Lagrangian subspace!

Notation 1.183. We let $\mathcal{L}_{\varpi_v}$ denote the above Lagrangian subspace.

We are thus able to complete our descent via some property akin to a "Markov chain."

Theorem 1.184. Fix some Lagrangian local condition $\mathcal{L} \subseteq \mathrm{H}^1(\mathbb{A}_K; E[2])$. Suppose we are given v_0 for which $\mathcal{L}_{v_0} = \mathrm{H}^1_{\mathrm{ur}}(K_{v_0}; E[2])$, so we set

$$\mathcal{L}' \coloneqq \prod_{v \neq v_0} \mathcal{L}_v \cdot \mathcal{L}_{\varpi_{v_0}}.$$

Then set $r \coloneqq \dim_{\mathbb{F}_2} \mathrm{Sel}_{\mathcal{L}}(E[2])$ and $r' \coloneqq \dim_{\mathbb{F}_2} \mathrm{Sel}_{\mathcal{L}'}(E[2])$. Then $r \equiv r' \pmod 2$, and

$$r' - r = \begin{cases} -2 & \text{if } \mathrm{loc}_{v_0}(\mathrm{Sel}_{\mathcal{L}}(E[2])) = \mathcal{L}_{v_0}, \\ +2 & \text{if } \mathrm{loc}_{v_0}(\mathrm{Sel}_{\mathcal{L}'}(E[2])) = \mathcal{L}'_{v_0}, \\ +0 & \text{otherwise.} \end{cases}$$

Remark 1.185. One input here is the following piece of linear algebra: given an even-dimensional quadratic space V, then there are two families of Lagrangian subspaces $\mathcal{F}_1$ and $\mathcal{F}_2$, and two Lagrangians $\mathcal{L}$ and $\mathcal{L}'$ are in the same family if and only if $\operatorname{codim}(\mathcal{L} \cap \mathcal{L}', \mathcal{L})$ is even-dimensional.

Example 1.186. The subspace $\operatorname{loc}_{v_0}(\operatorname{Sel}_{\mathcal{L}^{v_0}}(E[2]))$ is 2-dimensional by a global duality result, and in fact this space can be seen to be isotropic because they vanish outside a given place because the global inner product is the sum of local inner products.

Remark 1.187. The condition $\operatorname{loc}_{v_0}(\operatorname{Sel}_{\mathcal{L}'}(E[2])) = \mathcal{L}'_{v_0}$ implies that $\operatorname{loc}_{v_0}(\operatorname{Sel}_{\mathcal{L}}) = 0$ because our subspaces are transverse.

Proof. Write $\operatorname{Sel}_{\mathcal{L}}(E[2]) = \mathcal{L} \cap G$, where $G \coloneqq \mathrm{H}^1(K; E[2])$ and the intersection takes place in $\mathrm{H}^1(\mathbb{A}_K; E[2])$. One now has a pullback square

$$\begin{array}{ccc} \operatorname{Sel}_{\mathcal{L}\cap\mathcal{L}'}(E[2]) & \longrightarrow & \operatorname{Sel}_{\mathcal{L}}(E[2]) \\ \downarrow & \lrcorner & \downarrow \\ \operatorname{Sel}_{\mathcal{L}'}(E[2]) & \longrightarrow & \operatorname{Sel}_{\mathcal{L}+\mathcal{L}'}(E[2]) \end{array}$$

because the top-left is the intersection. Upon taking loc_{v_0}, we let the bottom-right image be $\mathcal{M}$, and we receive a pullback diagram

$$\begin{array}{ccc} 0 & \longrightarrow & \mathcal{M} \cap \mathcal{L}_{v_0} \\ \downarrow & \lrcorner & \downarrow \\ \mathcal{M} \cap \mathcal{L}'_{v_0} & \longrightarrow & \mathcal{M} \end{array}$$

again because we are just taking intersections. Here, $\mathcal{M} \subseteq \mathrm{H}^1(K_{v_0}; E[2])$ is just some Lagrangian subspace. Because $\mathcal{M} \cap \mathcal{L}_{v_0}$ and $\mathcal{M} \cap \mathcal{L}'_{v_0}$ are disjoint subspaces of a 2-dimensional space, we conclude that the difference in ranks is in $\{-2, +0, +2\}$. ∎

1.7.2 The Proof in a Special Case

We will prove our main theorem in a special case.

Theorem 1.188. Fix an elliptic curve E with $E[2](K) = (\mathbb{Z}/2\mathbb{Z})^2$. Suppose that $\operatorname{Sel}_2(E/K)$ is six-dimensional with basis $\{c_1, \dots, c_6\}$. Further, suppose that K admits six real archimedean places $\{\tau_1, \dots, \tau_6\}$ with some prescribed local behavior. Then we can find t for which

$$\operatorname{rank} \operatorname{Sel}_2(E^t/K) = 0 \qquad \text{and} \qquad \operatorname{rank} E^{-t}(K) > 0.$$

One can make some local twists described by Theorem 1.184 to achieve this situation. Roughly speaking, we are hoping to twist in the end by some

$$t = \prod_{i=1}^{3} (a_i d - c) \cdot d.$$

Let $q_i = a_i d - c$ for $i \in \{1, 2, 3\}$ and $q_d = 4 \coloneqq d$. We would like for all of these factors to be prime (which we will achieve with additive combinatorics), and we would like some control over how these things are adjusted by Theorem 1.184. In order to get some local control later, we fix some large set T of places (including archimedean places, bad places, 2, and 3, and maybe more), and we choose a large N to be supported on these places and with large enough power (e.g., the class number will be good enough for our purposes).

Let's explain the additive combinatorics which will let us assume that the factors in t are prime. We are going to state a Green–Tao

Definition 1.189 (admissible)**.** Fix a number field K. A *linear form* is a map $\varphi\colon \mathcal{O}_K^m \to \mathcal{O}_K$ of the form $\varphi_i(x) = a\cdot x + b$ where $a \in \mathcal{O}_K^m$ and $b \in \mathcal{O}_K$. We will then define the *homogeneous part* φ° as $\varphi^\circ(x) \coloneqq a\cdot x$.

Definition 1.190 (admissible)**.** Fix a number field K. A collection $\{\varphi_i\}_{i=1}^n$ of linear forms is *admissible* at a finite place v if and only if

$$\prod_{i=1}^n \varphi_i(x) \not\equiv 0 \pmod{\varpi_v}$$

admits a solution x.

Example 1.191. The triple $\{y, x+y, x+2y\}$ is not admissible at 2 because the sum is even.

Definition 1.192 (local density)**.** Fix a number field K and choose linear forms $\{\varphi_i\}_{i=1}^n$. For a finite place v, we define the *local density* as

$$\beta_v \coloneqq \frac{\#\left\{x \in \mathbb{F}_v^m : \prod_i \varphi_i(x) \not\equiv 0 \pmod{\varpi_v}\right\}}{\#\mathbb{F}_v^m}.$$

Definition 1.193 (von Mangoldt)**.** Fix a number field K. Then we define the *von Mangoldt function* Λ_K as

$$\Lambda_K(x) \coloneqq \begin{cases} \log \mathrm{N}\,\mathfrak{p} & \text{if } (x) = \mathfrak{p}^i \text{ for a prime ideal } \mathfrak{p}, \\ 0 & \text{otherwise.} \end{cases}$$

Theorem 1.194 (Kai)**.** Fix a number field K and some d-dimensional linear forms $\{\varphi_i\}_{i=1}^n$ for which the homogeneous parts φ_i° are pairwise linearly independent. Further, choose a convex set Ω with volume growing as

$$\mathrm{vol}\left(\Omega \cap [-N, N]^d\right) = cN^d + o\left(N^d\right)$$

for some fixed $c > 0$. Then

$$\sum_{x \in \Omega \cap [-N,N]^d \cap \mathbb{Z}^d} \prod_i \Lambda_K(\varphi_i(x)) = \frac{cN^d}{\mathrm{Res}_{s=1}\,\zeta_K(s)^n} \prod_p \beta_p + o\left(N^d\right).$$

For our application, we take

$$\varphi_i(x, y) = N^2 x + a_i N^2 \cdot N^2 H y + 1$$

for $i \in \{1, 2, 3\}$ and further define $\varphi_4(x, y) = N^2 y + 1$. This is admissible at every nonarchimedean place, and one can check a volume result at the archimedean places to prescribe some Ω.

We are now able to prove our result. Simply define $\mathcal{L}_i$ inductively by $\mathcal{L}_0$ to be the local condition of E, and we define $\mathcal{L}_i$ for $i > 0$ to be the modification of $\mathcal{L}_{i-1}$ by q_i. We can use Theorem 1.184 to control the rank of the Selmer groups (using the unnamed local conditions on the $\tau_\bullet$s via Hilbert reciprocity), and we conclude by choosing t generically.

Theme 2
Kolyvagin's Euler System

Kolyvagin has proved a great part of Conjecture 1.2.

—Benedict Gross [Gro91]

2.1 October 9

Today, we begin our discussion of Euler systems. We will mostly follow Gross's article [Gro91].

2.1.1 The Main Theorem

We are interested in proving the following result.

Definition 2.1 (analytic rank)**.** Fix a modular elliptic curve E over $\mathbb{Q}$. Then the *analytic rank* $r_{\mathrm{an}}(E/\mathbb{Q})$ equals the order of the vanishing of the L-function $L(E,s)$ at $s=1$.

Definition 2.2 (algebraic rank)**.** Fix an elliptic curve E over a number field K. Then the *algebraic rank* $r_{\mathrm{alg}}(E/K)$ is $\operatorname{rank} E(K)$.

Theorem 2.3 (Gross–Zagier, Kolyvagin)**.** Fix an elliptic curve E over $\mathbb{Q}$ for which $r_{\mathrm{an}}(E/\mathbb{Q}) \le 1$. Then $r_{\mathrm{an}}(E/\mathbb{Q}) = r_{\mathrm{alg}}(E/\mathbb{Q})$ and $Ш(E/\mathbb{Q})$ is finite.

Remark 2.4. For technical reasons, we will only show that $Ш(E/\mathbb{Q})[p^\infty] = 0$ for sufficiently large primes p.

It will be helpful to fix an auxiliary imaginary quadratic extension $K \coloneqq \mathbb{Q}(\sqrt{d})$, which we will choose more carefully at a later time. Then we see that $L(E_K, s) = L(E,s)L\left(E^d, s\right)$.

Remark 2.5. On the automorphic side, suppose that E admits a weight 2 Hecke eigenform f_E for which $L(E,s) = L(f_E,s)$ once appropriately normalized. Letting η be the nontrivial quadratic character of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ with kernel $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$, our identity reads

$$L(E_K,s) = L(f_E,s)L(f_E \otimes \eta, s).$$

After some analytic considerations, we are able to find some K for which $\mathrm{ord}_{s=1} L(E_K,s) = 1$, so we reduce to the following.

Theorem 2.6 (Gross–Zagier, Kolyvagin)**.** Fix a modular elliptic curve E over $\mathbb{Q}$, and choose an imaginary quadratic field K. Suppose the "Heegner hypothesis" that if E has bad reduction at places over a rational prime p, then p is split in K; we also require $K \notin \{\mathbb{Q}(i), \mathbb{Q}(\zeta_3)\}$. If $r_{\mathrm{an}}(E/K) = 1$, then $r_{\mathrm{alg}}(E/K) = 1$ and $Ш(E/K)$ is finite.

Remark 2.7. One needs to do a little work to show that Theorem 2.6 implies Theorem 2.3 because, after all, it is quite possible for $r_{\mathrm{alg}}(E/K) = 1$ while $r_{\mathrm{alg}}(E/\mathbb{Q}) = 1$. This is known due to many people; we mention Waldspurger, Bump–Friedberg–Hoffstein, and Murty–Murty.

Remark 2.8. Theorem 2.6 is still known without the Heegner hypothesis.

2.1.2 Heegner Points

The most striking aspect of Theorem 2.6 is that it is has $r_{\mathrm{alg}}(E/K) = 1$ as a conclusion, which means that we will need to find a non-torsion point on E using the hypothesis $r_{\mathrm{an}}(E/K) = 1$. This is done using the theory of Heegner points.

Definition 2.9 (modular curve)**.** Fix a positive integer N, and define the congruence subgroup $\Gamma_0(N)$ to be

$$\Gamma_0(N) \coloneqq \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : c \equiv 0 \pmod{N} \right\}.$$

Then we define the *modular curve* $Y_0(N)(\mathbb{C})$ as the quotient of $\mathcal{H} \coloneqq \{\tau \in \mathbb{C} : \mathrm{Im}\,\tau > 0\}$ by the action of $\Gamma_0(N)$ by Möbius transformations. We then define $X_0(N)(\mathbb{C})$ as the completion of $Y_0(N)$ as a Riemann surface; concretely, it is the quotient of $\mathcal{H} \cup \mathbb{P}^1(\mathbb{Q})$ by the action of $\Gamma_0(N)$, and the extra points in $\mathbb{P}^1(\mathbb{Q})/\Gamma_0(N)$ are referred to as cusps.

Remark 2.10. There is also a "moduli" description of $Y_0(N)$: it is the (coarse) moduli space of isogenies $E \to E'$ whose kernel (over $\overline{\mathbb{Q}}$) is a cyclic group of degree N, considered up to suitable isomorphism.

Definition 2.11 (geometrically modular)**.** Fix an elliptic curve E over $\mathbb{Q}$. Then E is *geometrically modular* if and only if there is a non-constant map $X_0(N) \to E$.

Remark 2.12. Equivalently, we are saying that $\mathrm{Jac}\, X_0(N)$ has an isogeny factor isomorphic to E.

Definition 2.13 (Heegner point)**.** Fix a positive integer N, and suppose that an imaginary quadratic field $K/\mathbb{Q}$ satisfies the "Heegner hypothesis" that each prime $p \mid N$ splits in K. Then the principal ideal (N) splits into a product $\mathcal{N}\overline{\mathcal{N}} = (N)$ where $\mathcal{O}_K/\mathcal{N} \cong \mathbb{Z}/N\mathbb{Z}$. Then we define the *Heegner point* $x_1 \in Y_0(N)$ as the element of $Y_0(N)$ corresponding to the isogeny

$$\mathbb{C}/\mathcal{O}_K \to \mathbb{C}/\mathcal{N}^{-1}.$$

Note that the kernel of this map is given by $\mathcal{N}^{-1}/\mathcal{O}_K$, which is isomorphic to $\mathcal{O}_K/\mathcal{N} \cong \mathbb{Z}/N\mathbb{Z}$.

Remark 2.14. Let's explain where the construction of $\mathcal{N}$ comes from. By the Chinese remainder theorem, it is enough to consider the case where $N = p^\nu$ for some prime p, and by the Heegner hypothesis, we see $(p) = \mathfrak{p}\overline{\mathfrak{p}}$ in $\mathcal{O}_K$. Then $(p^\nu) = \mathfrak{p}^\nu\overline{\mathfrak{p}}^\nu$, so we can take $\mathcal{N} \coloneqq \mathfrak{p}^\nu$.

Remark 2.15. The elliptic curve $\mathbb{C}/\mathcal{O}_K$ has a natural action by $\mathcal{O}_K$, so its endomorphisms are given by $\mathcal{O}_K$. The same holds for the isogenous elliptic curve $\mathbb{C}/\mathcal{N}^{-1}$.

Remark 2.16. It follows from the theory of complex multiplication of elliptic curve that $\mathbb{C}/\mathcal{O}_K$ descends to an elliptic curve defined over the Hilbert class field H_K of K.

Definition 2.17 (Heegner point)**.** Fix a geometrically modular elliptic curve E of conductor N over an imaginary quadratic field K satisfying the "Heegner hypothesis." Letting $\varphi_E \colon X_0(N) \to E$ be the modularity map. Then we define the *Heegner point* $y_K \in E(K)$ as

$$y_K = \sum_{\sigma \in \mathrm{Gal}(H/K)} \sigma(\varphi_E(x_1)).$$

This construction of y_K is known to have amazing properties.

Theorem 2.18 (Gross–Zagier)**.** Fix a geometrically modular elliptic curve E over $\mathbb{Q}$, and choose an imaginary quadratic field K satisfying the "Heegner hypothesis." Then the sign of the functional equation for $L(E/K, s)$ is -1, and

$$L'(E/K, 1) = c_E \hat{h}(y_K),$$

where c_E is some explicit nonzero constant, and $\hat{h}$ is a non-torsion point.

Corollary 2.19. Fix a geometrically modular elliptic curve E over $\mathbb{Q}$, and choose an imaginary quadratic field K satisfying the "Heegner hypothesis." If $r_{\mathrm{an}}(E/K) = 1$, then $\operatorname{rank} E(K) \geq 1$.

Proof. If $r_{\mathrm{an}}(E/K) = 1$, then $L'(E/K) \neq 0$, so it follows that $\hat{h}(y_K) \neq 0$, so this point is non-torsion by properties of the Néron–Tate height. ∎

Remark 2.20. It is possible but nontrivial to relax the Heegner hypothesis in this situation. Notably, one has to replace the modular curve $X_0(N)$ with a Shimura curve whose quaternion algebra is ramified at the bad primes p.

Remark 2.21. In fact, one can check that y_K has the expected Galois action so that it contributes to the correct $E(\mathbb{Q})$ or $E^d(\mathbb{Q})$.

2.1.3 Kolyvagin's Result

We are now ready to explain what Kolyvagin proved.

Theorem 2.22 (Kolyvagin)**.** Fix a geometrically modular elliptic curve E over $\mathbb{Q}$, and choose an imaginary quadratic field K satisfying the "Heegner hypothesis." If y_K is not a torsion point, then $r_{\mathrm{alg}}(E/K) = 1$, and $Ш(E/K)$ is finite.

Let's explain how this might be done. Suppose y_K is non-torsion. Then for all but finitely many primes p, we see y_K produces a nontrivial class in

$$E(K)/pE(K) \hookrightarrow \mathrm{Sel}_p(E/K).$$

Having a nonzero class like this is surprising!

Theorem 2.23 (Kolyvagin)**.** Fix a geometrically modular elliptic curve E over $\mathbb{Q}$, and choose an imaginary quadratic field K satisfying the "Heegner hypothesis." Choose a prime p such that the Galois representation $\overline{\rho}\colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}(E[p])$ is surjective. If y_K represents a nonzero class $\delta_p(y_K)$ in $\mathrm{H}^1(K; E[p])$, then

$$\mathrm{Sel}_p(E/K) = \mathbb{F}_p \cdot \delta_p(y_K).$$

Remark 2.24. Comparing Theorem 2.18 with the Birch–Swinnerton-Dyer conjecture, one expects that y_K is divisible by p if and only if p divides $\#Ш(E/K)$ multiplied by some bad local Tamagawa numbers.

In particular, it follows that $Ш(E/K)[p] = 0$.

Remark 2.25. One can sharpen the argument of Theorem 2.23 to work with prime-powers of p instead of just p. This allows him to show that $Ш(E/K)$ is finite.

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 $\chi_1, \dots, \chi_n \colon G \to k^\times$. Then the characters $\{\chi_1, \dots, \chi_n\}$ are linearly independent.

Proof. This proof is tricky. Suppose for the sake of contradiction that there is a nonempty set $\{\chi_1, \dots, \chi_n\}$ 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 $a_1, \dots, a_n \in k$; 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 $\{\chi_2, \dots, \chi_n\}$ 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 1.62 (where we are silently using Example 1.63). It remains to show (a), for which we use Lemma 1.35.

Set $G \coloneqq \mathrm{Gal}(L/k)$, 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

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

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

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

so the result follows by Theorem A.2. ∎

Example A.4. Fix a base field k and a positive integer m not divisible by $\mathrm{char}\, k$. 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

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

induces an exact sequence

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

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

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

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 $\langle \sigma, a \rangle \coloneqq \sigma(\alpha)/\alpha$.

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 $a' \coloneqq ab^m$ where $b \in k^\times$, then we may select $\alpha' \coloneqq \alpha b$, 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 $K_B \coloneqq k(B^{1/m})$ of k generated by the mth roots of B.

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

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

is perfect.

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

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

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

- To see that it is Galois, it is enough to check that it is generated by Galois elements, so it is enough to check that all Galois conjugates of $\alpha \in B^{1/m}$ live in K_B. Well, $a \coloneqq \alpha^m$ is an element of k by construction, so α is the root of the polynomial $X^m - a$. Because $\mu_m \subseteq k$, we see that the set

$$\{\zeta\alpha : \zeta \in \mu_m\}$$

of roots of $X^m - a$ is therefore contained in K_B.

- To see that it is abelian, choose two automorphisms $\sigma, \tau \in \mathrm{Gal}(K_B/k)$. We would like to check that $\sigma\tau = \tau\sigma$. It is enough to check this equality on generating elements of K_B/k, so we once again choose some $\alpha \in B^{1/m}$ and set $a \coloneqq \alpha^m$. Then we see that

$$\sigma\tau(\alpha) = \langle\sigma, a\rangle\langle\tau, a\rangle = \tau\sigma(\alpha).$$

(b) Here are our checks.

- Injective on $\mathrm{Gal}(K_B/k)$: suppose that $\sigma \in \mathrm{Gal}(K_B/k)$ makes $\langle\sigma, \cdot\rangle$ the trivial function, and we must show that σ is trivial. Well, it is enough to show that σ is trivial on $B^{1/m}$, so we choose some $\alpha \in B^{1/m}$ and set $a \coloneqq \alpha^m$. Then

$$\frac{\sigma(\alpha)}{\alpha} = \langle\sigma, a\rangle = 1,$$

so σ is the identity on α.

- Injective on $B/k^{\times m}$: suppose that $a \in B$ makes $\langle\cdot, a\rangle$ is trivial, and we would like to show that $a \in k^{\times m}$. Well, choose a root $\alpha \in K_B$ of $X^m - a$, and we would like to show that $\alpha \in k$. For this, we note that $\langle\sigma, \alpha\rangle = 1$ implies that $\sigma(\alpha) = \alpha$ for all $\sigma \in \mathrm{Gal}(K_B/k)$, 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 $f(X) \coloneqq X^m - b$, which can be computed (up to sign) to be $\mathrm{N}_{K_B/k} f'(\beta)$, where $\beta^m = b$. The result follows because $f'(X) = mX^{m-1}$.

A.3 Commutators

We will want to say something brief about nonabelian group cohomology.

Definition A.10. Fix a topological group G, and let M be a topological group with continuous action by G. Then we define $\mathrm{H}^0(G; M) \coloneqq M^G$ and $\mathrm{H}^1(G; M)$ as the pointed set of continuous 1-cocycles modulo continuous 1-coboundaries. Explicitly, a 1-cocycle is a function $f \colon G \to M$ for which

$$f(gh) = gf(h) \cdot f(g),$$

and two 1-cocycles f and f' are equivalent if and only if there is $m \in M$ for which $(gm)f(g) = f'(g)m$ for all $g \in G$.

Remark A.11. A morphism $M \to M'$ of groups with G-action induces (by functoriality) a morphism $\mathrm{H}^1(G; M) \to \mathrm{H}^1(G; M')$ of pointed sets. Indeed, a continuous 1-cocycle $G \to M$ certainly produces a continuous 1-cocycle $G \to M'$ by composition, and the same is true for 1-coboundaries. If M and M' are both abelian, then we can see that $\mathrm{H}^1(G; M)$ and $\mathrm{H}^1(G; M')$ are both groups under pointwise multiplication (indeed, they are the usual group cohomology groups), and the functorial map is a homomorphism.

Lemma A.12. Fix a topological group G and an exact sequence

$$1 \to A \to B \to C \to 1$$

of topological groups with continuous G-action. Then there is an exact sequence

$$0 \longrightarrow \mathrm{H}^0(G; A) \longrightarrow \mathrm{H}^0(G; B) \longrightarrow \mathrm{H}^0(G; C) \longrightarrow \mathrm{H}^1(G; A) \longrightarrow \mathrm{H}^1(G; B) \longrightarrow \mathrm{H}^1(G; C)$$

of pointed sets. If $A \subseteq Z(B)$ and C is abelian, then the last row can be continued by a map $\mathrm{H}^1(G; C) \to \mathrm{H}^2(G; A)$. If B is abelian, then the boundary maps are homomorphisms.

Proof. This proof is exactly the same as the usual one, but we are forced to write things out explicitly because we no longer have access to derived functors. We will still be somewhat brief. For psychological reasons, identify A with its image in B, and label the last map as $\pi \colon B \to C$. We proceed in steps.

1. Exactness of the top row follows because taking G-invariants is a left-exact functor.
2. We define the map $\delta_0 \colon \mathrm{H}^0(G;C) \to \mathrm{H}^1(G;A)$. Indeed, given $c \in C^G$, we can find some $b \in B$ for which $\pi(b) = c$. Then b produces a 1-coboundary given by $f_b(g) \coloneqq (gb)b^{-1}$, which we can quickly check is in fact a 1-cocycle: $(ghb)b^{-1} = g\left((hb)b^{-1}\right) \cdot (gb)b^{-1}$. Now, we note that
$$\pi\left((gb)b^{-1}\right) = gc \cdot c^{-1}$$
is trivial, so f_b actually has values in A, so f_b defines a class in $\mathrm{H}^1(G;A)$. To show that this map $\delta_0(c) \coloneqq f_b$ is well-defined, we need to know that it does not depend on the choice of lifting $b \in B$. Well, any other lift takes the form ab for some $a \in A$, and we see that $f_{ab}(g) = (ga)f(b)a^{-1}$, so f_{ab} and f_b are equivalent.
Lastly, we should show that δ_0 is a homomorphism when B is abelian. Well, given $c, c' \in C^G$, we grant them lifts b and b', and then bb' is a lift of cc', so it is enough to note that $f_{bb'} = f_b f_{b'}$ by the commutativity in B.
3. Exact at $\mathrm{H}^0(G;C)$: an element $c \in C^G$ vanishes in $\mathrm{H}^1(G;A)$ if and only if its lift $b \in B$ is actually an element of A. This is equivalent to saying that $f_a = (ga)a^{-1}$ is equivalent to the identity.
4. Exact at $\mathrm{H}^1(G;A)$: a 1-cocycle $f \in \mathrm{H}^1(G;A)$ vanishes in $\mathrm{H}^1(G;B)$ if and only if there is $b \in B$ for which $f(g) = (gb)b^{-1}$ for all $g \in G$. This is equivalent to saying that $f = \delta_0(\pi(b))$.
5. Exact at $\mathrm{H}^1(G;B)$: a 1-cocycle $f \in \mathrm{H}^1(G;B)$ vanishes in $\mathrm{H}^1(G;C)$ if and only if there is $c \in C$ for which $\pi(f(g)) = (gc)c^{-1}$ for all $g \in G$. Choosing a lift $b \in B$ for c, we see that we may change f to the equivalent 1-cocycle $f'(g) \coloneqq (gb)^{-1}f(g)b$ which now has $\pi(f(g)) = 1$ for all $g \in G$. But now f comes from a class in $\mathrm{H}^1(G;A)$. ∎

Lemma A.13. Fix a topological group G and an exact sequence
$$1 \to A \to B \to C \to 1$$
of topological groups with continuous G-action. If $A \subseteq Z(B)$ and A is abelian, then the long exact sequence of Lemma A.12 can be continued to a map $\delta_1 \colon \mathrm{H}^1(G;C) \to \mathrm{H}^2(G;A)$.

Proof. We define the map $\delta_1 \colon \mathrm{H}^1(G;C) \to \mathrm{H}^2(G;A)$. Choose a 1-cocycle f representing a class in $\mathrm{H}^1(G;C)$. Then we can define a 1-cochain $\widetilde{f} \colon G \to B$ by $\pi\left(\widetilde{f}(g)\right) = f(g)$ for all $g \in G$. We claim that this makes the boundary
$$\partial\widetilde{f}(g,h) \coloneqq g\widetilde{f}(h) \cdot \widetilde{f}(g) \cdot \widetilde{f}(gh)^{-1}$$
into a 2-cocycle of A, which will be $\delta_1 f$. Certainly $\pi\left(\widetilde{f}(g,h)\right) = 1$ for all g and h (because C is abelian), so $\widetilde{f}$ outputs to A. To check the cocycle condition, we note that $A \subseteq Z(B)$, so $\partial\widetilde{f}(g,h) = \widetilde{f}(gh)^{-1} \cdot g\widetilde{f}(h) \cdot \widetilde{f}(g)$ as well (seen by conjugating by $\widetilde{f}(gh)$), so checking the cocycle condition amounts to computing
$$\begin{aligned}
&g_1\partial\widetilde{f}(g_2,g_3) \cdot \partial\widetilde{f}(g_1,g_2g_3) \cdot \left(\partial\widetilde{f}(g_1g_2,g_3) \cdot \partial\widetilde{f}(g_1,g_2)\right)^{-1} \\
&= \frac{g_1g_2\widetilde{f}(g_3) \cdot g_1\widetilde{f}(g_2) \cdot g_1\widetilde{f}(g_2g_3)^{-1} \cdot g_1\widetilde{f}(g_2g_3) \cdot \widetilde{f}(g_1) \cdot \widetilde{f}(g_1g_2g_3)^{-1}}{\widetilde{f}(g_1g_2g_3)^{-1} \cdot g_1g_2\widetilde{f}(g_3) \cdot \widetilde{f}(g_1g_2) \cdot \widetilde{f}(g_1g_2)^{-1} \cdot g_1\widetilde{f}(g_2) \cdot \widetilde{f}(g_1)} \\
&= \frac{g_1g_2\widetilde{f}(g_3) \cdot g_1\widetilde{f}(g_2) \cdot \widetilde{f}(g_1) \cdot \widetilde{f}(g_1g_2g_3)^{-1}}{\widetilde{f}(g_1g_2g_3)^{-1} \cdot g_1g_2\widetilde{f}(g_3) \cdot g_1\widetilde{f}(g_2) \cdot \widetilde{f}(g_1)},
\end{aligned}$$
so everything cancels because it takes the form $b_1b_2^{-1}b_1^{-1}b_2$ where $b_1b_2^{-1} \in A$.

We now check that δ_1 is well-defined, for which we need to check that δ_1 does not depend on the choice of representative f or the choice of lift $\widetilde{f}$. Changing the lift $\widetilde{f}$ to some $\widetilde{f}'$ means that $c(g) \coloneqq \widetilde{f}(g)\widetilde{f}'(g)^{-1}$ is in A

for all $g \in G$, so we find that $\partial\widetilde{f}' = \partial\widetilde{f} \cdot \partial c$ (because A is central), so the 2-coboundary c witnesses that $\partial\widetilde{f}'$ is equivalent to $\widetilde{f}$. Lastly, changing f to some other f' means that there is $c \in C$ for which $f(g) = gc \cdot f'(g) \cdot c^{-1}$. Then lifting $c \in C$ to some $b \in B$ shows that f' can be lifted to

$$(g,h) \mapsto (ghb) \cdot g\widetilde{f}(h) \cdot (gb)^{-1} \cdot (gb) \cdot \widetilde{f}(g) \cdot b^{-1} \cdot b \cdot \widetilde{f}(gh)^{-1} \cdot (ghb)^{-1},$$

which equals the original $\partial\widetilde{f}$ after remarking that A is central in B.

Lastly, we need to check exactness at $\mathrm{H}^1(G;C)$. Well, a 1-cocycle $f : G \to C$ vanishes in $\mathrm{H}^2(G;A)$ if and only if there is a 1-cochain $a : G \to A$ for which $\partial\widetilde{f} = \partial a$, where $\widetilde{f}$ is a chosen lift of f. Because a is central, this is equivalent to $\partial\left(a^{-1}\widetilde{f}\right)$ being a trivial 2-cocycle, which means that $a^{-1}\widetilde{f}$ is a 1-cocycle in $\mathrm{H}^1(G;B)$, and we can see that it has image f in $\mathrm{H}^1(G;C)$. Conversely, any 1-cocycle f in B has $\delta_1(\pi(f))$ trivial because $\pi(f)$ can be lifted to f, and $\partial f = 1$ because f is already a 1-cocycle. ■

In the exact sequence

$$1 \to A \to B \to C \to 1,$$

with $A \subseteq Z(B)$ and C abelian, the boundary map $\delta_1 : \mathrm{H}^1(G;C) \to \mathrm{H}^2(G;A)$ of Lemma A.13 is a homomorphism when B abelian. However, when B is not abelian, it turns out to be quadratic.

Proposition A.14. Fix a topological group G and an exact sequence

$$1 \to A \to B \to C \to 1$$

of topological groups with continuous G-action.

(a) There is an antisymmetric pairing $\varphi : C \otimes C \to A$ given on pure tensors $c \otimes c'$ by lifting c and c' to b and b', respectively, and defining $\varphi(c \otimes c') \coloneqq bb'b^{-1}(b')^{-1}$.

(b) For any $f, f' \in \mathrm{H}^1(G;C)$, we have $\delta_1(ff') = \delta_1(f)\delta_1(f')\varphi(f \cup f')^{-1}$.

Proof. This is [Zar74, Section 1]. As usual, identify A with its image in B, and denote the map $B \to C$ by π. We now quickly dispatch with (a).

- Note that φ outputs to A because $\pi\left(bb'b^{-1}(b')^{-1}\right) = 1$, meaning that $\pi \circ \varphi$ is trivial.
- Well-defined: changing the lifts b or b' will only adjust them by a central element in A, which will not affect the output commutator.
- Antisymmetric: note $[b,b']^{-1} = [b',b]$, so $\varphi(c \otimes c') = \varphi(c' \otimes c)^{-1}$.
- Bilinear: upon lifting $c_1, c_2, c' \in C$ to $b_1, b_2, b' \in B$, respectively, checking $\varphi(c_1c_2, c') = \varphi(c_1,c')\varphi(c_2,c')$ amounts to calculating

$$\begin{aligned}[b_1,b'] \cdot [b_2,b'] \cdot [b_1b_2,b']^{-1} &= b_1b'b_1^{-1}\left[(b')^{-1},b_2\right] b_1 \left[b_2,(b')^{-1}\right] (b')^{-1}b_1^{-1} \\ &= b_1b'b_1^{-1}b_1(b')^{-1}b_1^{-1} \cdot \left[(b')^{-1},b_2\right] \cdot \left[b_2,(b')^{-1}\right], \\ &= 1,\end{aligned}$$

  where we have repeatedly used that the fact that A is central. The other bilinearity check follows from antisymmetry.

We now turn to (b). This is a direct calculation. For $f, f' \in \mathrm{H}^1(G;C)$ and $g, h \in G$, we choose lifts $\widetilde{f}$ and $\widetilde{f}'$ of f and f' respectively, so we can calculate

$$\begin{aligned}\delta_1(ff')(g,h) &= g\widetilde{f}(h) \cdot g\widetilde{f}'(h) \cdot \widetilde{f}(g) \cdot \widetilde{f}'(g) \cdot \widetilde{f}'(gh)^{-1} \cdot \widetilde{f}(gh)^{-1} \\ &= \widetilde{f}(gh)^{-1} \cdot g\widetilde{f}(h) \cdot g\widetilde{f}'(h) \cdot \widetilde{f}(g) \cdot \widetilde{f}'(g) \cdot \widetilde{f}'(gh)^{-1} \\ &= \widetilde{f}(gh)^{-1} \cdot g\widetilde{f}(h) \cdot \widetilde{f}(g) \cdot \left[\widetilde{f}(g)^{-1}, g\widetilde{f}'(h)\right] \cdot g\widetilde{f}'(h) \cdot \widetilde{f}'(g) \cdot \widetilde{f}'(gh)^{-1} \\ &= \partial\widetilde{f}(g,h) \cdot \varphi\left(f^{-1} \cup f'\right)(g,h) \cdot \partial\widetilde{f}'(g,h).\end{aligned}$$

The result follows after rearranging. ■

Definition A.15 (commutator pairing)**.** Given a short exact sequence

$$1 \to A \to B \to C \to 1$$

of groups such that $A \subseteq Z(B)$ and C is abelian, we let $\varphi\colon C \otimes C \to A$ defined in Proposition A.14 be the *commutator pairing*.

Appendix B
Linear Algebra

It is my experience that proofs involving matrices can be shortened by 50% if one throws the matrices out.

—Emil Artin

In this short appendix, we do a little linear algebra. Our exposition mostly follows [Knu91].

B.1 Bilinear Forms

We will be interested in bilinear forms. We will largely focus on the case of free modules over rings, but many of the definitions work with general modules, so we will go ahead and statement as such.

Definition B.1 (bilinear form)**.** Fix a module M over a ring R. Then a *bilinear form* $\langle -, - \rangle$ on M is a bilinear map $M \times M \to R$. An *isometry* of modules equipped with bilinear forms is an isomorphism of modules preserving the bilinear forms.

Example B.2. Suppose M is free of finite rank d with basis $\{e_1, \dots, e_d\}$. Then we define $\langle -, - \rangle$ on M by

$$\left\langle \sum_{i=1}^{d} a_i e_i, \sum_{j=1}^{d} b_i e_i \right\rangle = \sum_{i=1}^{d} a_i b_i.$$

Remark B.3. Suppose M is free of finite rank d. Given an ordered basis $\{e_i\}$ of M, we can represent $\langle -, - \rangle$ by the matrix A whose coefficients are given by

$$A_{ij} \coloneqq \langle e_i, e_j \rangle.$$

Then $\langle v, w \rangle = v^\intercal A w$, where we have implicitly used the ordered basis to identify M with R^d.

Remark B.4. For any bilinear form $\langle -, - \rangle$ on a module M, the bilinear form automatically restricts to any submodule of M. Similarly, we note that it extends to $M \otimes_R S$ for any ring extension $R \to S$.

Definition B.5 (symmetric, alternating)**.** Fix a module M over a ring R. Then a bilinear form $\langle -, - \rangle$ is *symmetric* if and only if

$$\langle m, n \rangle = \langle n, m \rangle$$

for all $m, n \in M$. It is *alternating* if and only if $\langle m, m \rangle = 0$ for all $m \in M$.

Remark B.6. As in Remark B.3, we see that $\langle -, - \rangle$ is symmetric if and only if the matrix A is symmetric.

Remark B.7. If $\langle -, - \rangle$ is alternating, then for any $m, n \in M$, we see that $\langle m+n, m+n \rangle = 0$ implies that

$$\langle m, n \rangle = -\langle n, m \rangle.$$

However, the converse need not be true in characteristic 2. Anyway, as in Remark B.3, we see that $\langle -, - \rangle$ is alternating if and only if $A = -A^\intercal$ and the diagonal entries of A vanish.

Definition B.8 (non-degenerate)**.** Fix a module M over a ring R. Then a bilinear form $\langle -, - \rangle$ is *perfect* if and only if the following two conditions hold.

(a) For any $m \in M$, the map $M \to M^*$ given by $m \mapsto \langle m, - \rangle$ is an isomorphism.

(b) For any $n \in M$, the map $M \to M^*$ given by $m \mapsto \langle -, n \rangle$ is an isomorphism.

Remark B.9. Fixing the matrix A as in Remark B.3, we see that $\langle -, - \rangle$ is non-degenerate if and only if A is invertible. In fact, A being invertible is equivalent to either one of (a) or (b).

Remark B.10. Conversely, given an isomorphism $\varphi_\bullet \colon M \to M^*$, we can produce a bilinear pairing $\langle -, - \rangle$ on M given by

$$\langle m, n \rangle \coloneqq \varphi_m(n).$$

Example B.11. Fix M and $\langle -, - \rangle$ as in Example B.2. Then $\langle -, - \rangle$ is symmetric (by definition), and it is perfect because homomorphisms $\varphi \colon M \to R$ are in bijection with n-tuples R^n by

$$\varphi \mapsto (\varphi(e_1), \dots, \varphi(e_n)).$$

In particular, this defines the isomorphisms $M \to M^*$.

Example B.12 (hyperbolic space)**.** Suppose N is free over R of finite rank d with basis $\{e_1, \dots, e_d\}$. Further, let $\{f_1, \dots, f_d\}$ be the functionals where f_i is the projection onto the ith coordinate. Then set $H(N) \coloneqq N \oplus N^*$, which we call "hyperbolic space." Note $H(N)$ has a canonical bilinear form given by

$$\langle (e, f), (e', f') \rangle \coloneqq f(e') + f'(e).$$

This pairing is symmetric by construction, and it is perfect: the induced morphism $H(N) \to H(N)^*$ simply swaps the factors of $N \oplus N^*$, where N and N^* are being identified via their ordered bases. For example, f_i is sent to the functional $\langle (e, f), (0, f_i) \rangle = f_i(e)$, and e_i is sent to the functional $\langle (e, f), (e_i, 0) \rangle = f(e_i)$.

B.2 Quadratic Forms

It will turn out that quadratic forms are "more fundamental" than bilinear forms.

Definition B.13 (quadratic form)**.** Fix module M and N over a ring R. Then a *quadratic function* is a function $q\colon M \to N$ satisfying the following.

(a) For any $r \in R$ and $m \in M$, we have $q(rm) = r^2 q(m)$.

(b) The function $\langle -, - \rangle_q \colon M \times M \to N$ defined by $\langle m, n \rangle_q \coloneqq q(m+n) - q(m) - q(n)$ is symmetric and bilinear.

If $N = R$, then we call q a *quadratic form*.

Definition B.14 (quadratic space)**.** A *quadratic space* (M, q) is a pair of a finitely generated projective module M and a quadratic form q on M. The quadratic space is *regular* if and only $\langle -, - \rangle_q$ is perfect. A morphism of quadratic spaces is a morphism of the underlying modules preserving the quadratic form. An *isometry* is an isomorphism of quadratic spaces.

Remark B.15. Note that $\langle -, - \rangle_q$ is automatically symmetric.

Remark B.16. If $2 \in R^\times$, then we can recover q from the bilinear form $\langle -, - \rangle_q$ as

$$q(m) \coloneqq \frac{1}{2} \langle m, m \rangle_q.$$

However, in characteristic 2, there is a difference between the notions! It is not unreasonable to think that the bilinear form carries "more" information.

Example B.17 (diagonal form)**.** Fix M as in Example B.2 with basis $\{e_1, \dots, e_d\}$. Then we define the diagonal quadratic form

$$q\left(\sum_{i=1}^{d} a_i e_i \right) = \sum_{i=1}^{d} a_i^2.$$

Then $q(m+n) - q(m) - q(n) = 2\langle m, n \rangle$. In particular, if $\operatorname{char} R = 0$, then $\langle -, - \rangle_q$ vanishes!

Example B.18 (hyperbolic form)**.** Fix N as in Example B.12 with basis $\{e_1, \dots, e_d\}$ so that N^* has dual basis $\{f_1, \dots, f_d\}$. Then we define the quadratic form q on $H(N)$ by

$$q((e, f)) \coloneqq f(e).$$

Then $q(m+n) - q(m) - q(n) = \langle m, n \rangle$. In particular, $H(N)$ is regular.

Remark B.19. Note that the quadratic form q on M will automatically restrict to a quadratic form on any subspace $N \subseteq M$. Additionally, for any ring extension $R \to S$, there is an extension of q to $M \otimes_R S$ by

$$q(m \otimes s) \coloneqq s^2 q(m).$$

Remark B.20. There is a notion of direct sum of quadratic spaces: one can define $(M, q) \oplus (M', q')$ as having the underlying R-module $M \oplus M'$ with the quadratic form given by $(m, m') \mapsto q(m) + q(m')$.

We will want a few ways to simplify a quadratic form.

Lemma B.21. Fix a quadratic space (M, q) over a ring R such that 2 is not a zero-divisor. Then there is an étale ring extension $R \to S$ and a basis $\{e_1, \dots, e_d\}$ of M_S for which q_S takes the form

$$\left\langle \sum_{i=1}^{d} a_i e_i, \sum_{j=1}^{d} b_j e_j \right\rangle = \sum_{i=1}^{n} c_i a_i b_i$$

for some constants $c_1, \dots, c_d \in S$.

Proof. Working (Zariski) locally, we may assume that M is free. The point is to use the Gram–Schmidt process, but it is slightly complicated by the fact that we don't have a positive-definiteness hypothesis.

We will induct on the rank of M, where the case of M having rank 0 has no content. For the induction, choose a rank $d+1$, and start with any basis $\{e_1, \dots, e_{d+1}\}$ of M. By the inductive hypothesis, we may pass to an étale extension of R so that q is diagonal when restricted to $\{e_1, \dots, e_d\}$. By the Gram–Schmidt process, we may as well assume that $\langle e_i, e_{d+1}\rangle_q = 0$ whenever $q(e_i) \neq 0$.[1] We will then not touch such e_i with $q(e_i) \neq 0$, so we may as well assume that $q(e_i) = 0$ for all $i \leq d$.

Now, if $\langle e_i, e_{d+1}\rangle_q = 0$ for any $i \leq d$, then it suffices to diagonalize the lower-dimensional subspace $\operatorname{span}\{e_j : j \neq i\}$, so we are done by the induction. Additionally, if $\langle e_{d+1}, e_{d+1}\rangle \neq 0$, then an étale extension allows us to normalize to $\langle e_{d+1}, e_{d+1}\rangle_q = 1$ and then apply the Gram–Schmidt process to achieve that $\langle e_1, 0\rangle_q = 0$, allowing us to induct again.

As such, we go ahead and assume that $\langle e_1, e_{d+1}\rangle_q \neq 0$ and $\langle e_{d+1}, e_{d+1}\rangle_q = 0$. However, we then see that

$$\langle e_1 + e_{d+1}, e_1 + e_{d+1}\rangle_q = 2\langle e_1, e_{d+1}\rangle_q$$

is nonzero. As such, we may replace e_1 with $e_1 + e_{d+1}$ and induct as in the previous paragraph. ∎

Lemma B.22. Fix a regular quadratic space (M, q) over a ring R of even rank. Then (M, q) is isomorphic to the hyperbolic space of Example B.18 fppf-locally.

Proof. Working Zariski locally, we may assume that M is free of rank $2d$. An examination of Example B.18 shows that our goal is to (fppf-locally) find a basis $\{u_1, \dots, u_d\} \sqcup \{v_1, \dots, v_d\}$ where $q(\operatorname{span}\{u_1, \dots, u_d\}) = \{0\}$ and $q(\operatorname{span}\{v_1, \dots, v_d\}) = \{0\}$ and $\langle u_i, v_j\rangle_q = 1_{i=j}$. We will induct on d, for which we note that the case of $d = 0$ has no content.

For the induction, we assume that M is free of rank $2d+2$, and we go ahead and choose some direct summand $U \oplus V \subseteq M$ where U and V have bases as in the previous paragraph.

1. We claim that we can find $u_{d+1} \in M$ for which $q(\operatorname{span}(U \cup \{u_{d+1}\})) = \{0\}$. Choose any $u, v \in M$ to complete the basis. Ordering the basis as $\{u_1, v_1, u_2, v_2, \dots, u_d, v_d, u, v\}$, we see that the matrix corresponding to $\langle -, -\rangle_q$ looks like

$$\operatorname{diag}\left(1_2, \dots, 1_2, \begin{bmatrix} 2q(u) & \langle u, v\rangle_q \\ \langle u, v\rangle_q & 2q(v) \end{bmatrix}\right).$$

   This matrix must be invertible, so its determinant must be a unit, so we see that q continues to provide a non-degenerate bilinear form on $\operatorname{span}\{u, v\}$. But now we are just trying to find a nontrivial root of a quadratic equation. It is enough to do this on fibers points because geometric points spread out to flat neighborhoods, but this is surely solvable in geometric fibers because solving a homogeneous equation in two variables amounts to solving some quadratic.

[1] We need to use étale ring extensions in order to localize at non-zero-divisors and take square roots of the norms.

2. We now apply a Gram–Schmidt process. We now see that $q(u_{d+1})$ and $q(v)$ must both be units, so an additional covering allows us to grant $q(v) = 0$; we now call this element v_{d+1}. Replacing v_{d+1} with $v_{d+1} - \langle w_i, w_{d+1}\rangle u_i$ allows us to assume that $\langle u_i, v\rangle = 0$ for all $i \neq d+1$. Next, replacing u_{d+1} with $u_{d+1} - \langle w_i, u_{d+1}\rangle u_i$ allows us to assume that $\langle u_{d+1}, w_i\rangle = 0$ for $i \neq d+1$. Lastly, we see that $\langle u_{d+1}, v_{d+1}\rangle \neq 0$ must be a unit by examining the determinant of the previous step, so we may rescale u_{d+1} so that $\langle u_{d+1}, v_{d+1}\rangle = 1$. ■

B.3 The Clifford Algebra

In this section, we pick up exactly as much about the Clifford algebra as we need in order to define the special orthogonal group.

Definition B.23 (Clifford algebra)**.** Fix a quadratic space (M, q) over a ring R. Then we define the *Clifford algebra* $C(M, q)$ as the quotient of the tensor algebra TM by the ideal generated by the elements $x \otimes x - q(x)$. We may abbreviate $C(M, q)$ to $C(M)$ or $C(q)$.

Remark B.24. Note that TM has a natural grading by $\mathbb{Z}$, which projects onto a natural grading by $\mathbb{Z}/2\mathbb{Z}$. With respect to the $\mathbb{Z}/2\mathbb{Z}$-grading, we see that the elements $x \otimes x - q(x)$ are homogeneous of degree 0, so the quotient $C(M, q)$ is also $\mathbb{Z}/2\mathbb{Z}$-graded.

Remark B.25. The formation of $C(M, q)$ is compatible with ring extensions $R \to S$: namely, $C(M)_S = C(M_S)$.

Remark B.26. By construction, $C(M, q)$ has the following universal property: for any (possibly non-commutative) R-algebra A equipped with a map $\varphi\colon M \to A$ for which $\varphi(x)^2 = q(x)$, there is a unique map $C(M, q) \to A$ extending φ. To see this, note that $\varphi\colon M \to A$ extends to a unique map $TM \to A$, so there is certainly only one quotient map down to $C(M, q)$. And of course, this quotient map extends because $\varphi(x)^2 = q(x)$ for all $x \in M$.

Remark B.27. The universal property implies that $C(M, q)$ is functorial in M: any morphism $(M, q) \to (M', q')$ of quadratic spaces induces a map $M \to C(M', q')$ sending $x \in M$ to $x \otimes x = q'(x) = q(x)$, so this extends uniquely to a map $C(M, q) \to C(M', q')$. Functoriality follows from the uniqueness of this construction.

Example B.28. Let's compute $C(M, q)$ when M is free of rank 1, spanned by $\{e\}$. Then $TM = R[e]$, and we are taking the quotient by the principal ideal generated by $e^2 - q(e)$, so

$$C(M, q) \cong \frac{R[e]}{(e^2 - q(e))}.$$

For example, we see that $C(M, q)$ has a basis given by $\{1, e\}$.

Example B.29. If $q = 0$, then $C(M) = \wedge^\bullet M$ because we are just taking the quotient by the tensors $x \otimes x$.

Lemma B.30. Fix quadratic spaces (M, q) and (M', q') over R. Then the canonical map

$$C(M \oplus M') \to C(M) \otimes C(M')$$

is an isomorphism.

Proof. Let's begin by defining the canonical map: the map $\varphi\colon M \oplus M' \to C(M) \otimes C(M')$ defined by sending $(x,0) \mapsto (x \otimes 1)$ and $(0,x') \mapsto (1 \otimes x')$ satisfies that $\varphi(x,x')^2$ equals

$$\left(x^2 \otimes 1\right) + \left(1 \otimes (x')^2\right) = q(x) + q'(x),$$

so we induce a unique map $C(M \oplus M') \to C(M) \otimes C(M')$ extending φ by Remark B.27. On the other hand, the inclusion $M \to M \oplus M'$ functorially provides a map $C(M) \to C(M \oplus M')$, so we can take the tensor product of these two maps to produce a map $C(M) \otimes C(M') \to C(M \oplus M')$. By construction, this latter map definitionally sends $(x \otimes 1) \mapsto (x,0)$ and $(1 \otimes x') \mapsto (0,x')$. Thus, we see that the two maps are inverses on generators, so they are inverse morphisms. ∎

Proposition B.31 (Poincaré–Birkhoff–Witt)**.** Fix a quadratic space (M,q) over R with basis $\{e_1,\dots,e_d\}$. Then $C(M,q)$ is free as an R-module with basis given by the monomials

$$e_{i_1 \dots i_k} \coloneqq e_{i_1} \cdots e_{i_k},$$

where $1 \le i_1 < \cdots < i_k \le d$.

Proof. We proceed in steps, following [Knu91, Theorem IV.1.5.1]. We quickly remark that keeping track of various linear actions explains that the conclusion does not depend on the choice of basis.

1. If $2 \in R^\times$, then we can use Lemma B.21 to diagonalize (M,q). This means that (M,q) is a direct sum of one-dimensional quadratic spaces, so Lemma B.30 allows us to reduce to the case where M is one-dimensional. In this case, the result is just Example B.28.
2. If 2 is not a zero divisor in R, then we may check the basis result after passing to the étale extension $R \to K(R)$, and now $2 \in K(R)^\times$.
3. Fixing generators of R as a $\mathbb{Z}$-algebra, we may construct a $\mathbb{Z}$-algebra R' for which there is a projection $\pi\colon R' \twoheadrightarrow R$, but now we may take R' to not have 2 as a zero divisor. We now lift (M,q) to some quadratic space (M',q') on R': define M' to formally have the basis $\{e_1',\dots,e_d'\}$, and then we may define q' so that $\pi(q'(e_i')) = q(e_i)$ for all i and $\pi(\langle e_i', e_j'\rangle) = \langle e_i, e_j\rangle$ for all i and j. Then the previous step shows that the basis result holds for (M',q'), so it descends to $C(M) = C(M') \otimes_{R'} R$ by Remark B.25. ∎

Example B.32. Let's compute $C(H(N))$ when N is free of rank 1, spanned by $\{e\}$. Let $\{f\} \subseteq N^*$ be the dual basis. Then Proposition B.31 assures us that $C(H(N))$ has basis $\{1,e,f,ef\}$, and we see that the relations are given by $e^2 = f^2 = 0$ and $ef + fe = 1$. On the other hand, we know that $\wedge^\bullet N$ has basis $\{1,e\}$. Thus, we note that there is a map $C(H(N)) \to \mathrm{End}(\wedge^\bullet N)$ given by

$$e \mapsto \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \qquad \text{and} \qquad f \mapsto \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}.$$

In particular, we can see that $ef+fe=1$, so this map of algebras is well-defined. In fact, we can see that it is an isomorphism of modules, and the image of $C^+(H(N))$ is given by matrices of the form $\left[\begin{smallmatrix} * & 0 \\ 0 & * \end{smallmatrix}\right]$ while the image of $C^-(H(N))$ is given by matrices of the form $\left[\begin{smallmatrix} 0 & * \\ * & 0 \end{smallmatrix}\right]$. For example, $Z(C^+(H(N))) \cong R \oplus R$.

Proposition B.33. Fix a finitely generated projective module N of finite rank over R. Then there is an isomorphism

$$C(H(N)) \to \mathrm{End}(\wedge^\bullet N)$$

of $\mathbb{Z}/2\mathbb{Z}$-graded algebras over R.

Proof. This is [Knu91, Proposition IV.2.1.1]. Let's begin by describing the map, which is produced via Remark B.27.

- Given $e \in N$, we define $\varphi_e \colon \wedge^\bullet N \to \wedge^\bullet N$ by $e \wedge -$. More precisely, this is the unique quotient of the alternating map $N^k \to \wedge^\bullet N$ given by $(e_1, \dots, e_k) \mapsto e \wedge e_1 \wedge \cdots \wedge e_k$. While we're here, we note that $e \wedge e = 0$ implies that $\varphi_e^2 = 0$.
- Given $f \in N^*$, we define $\varphi_f \colon \wedge^\bullet N \to \wedge^\bullet N$ on pure tensors by

$$\varphi_f(e_1 \wedge \cdots \wedge e_k) \coloneqq \sum_{i=1}^{k} (-1)^i f(e_i)(e_1 \wedge \cdots \wedge \widehat{e_i} \wedge \cdots \wedge e_k).$$

  Indeed, we see that the left-hand side is alternating in $(e_1, \dots, e_k)$, so this is a well-defined endomorphism. While we're here, we note that $\varphi_f^2 = 0$: for any $i < j$, we see that the sum $\varphi_f^2(e_1 \wedge \cdots \wedge e_k)$ contains the pure tensor $e_1 \wedge \cdots \wedge \widehat{e_i} \wedge \cdots \wedge \widehat{e_j} \wedge \cdots \wedge e_k$ exactly twice with the coefficients $(-1)^i f(e_i) \cdot (-1)^j f(e_j)$ and $(-1)^{j-1} f(e_j) \cdot (-1)^i f(e_i)$; these exactly cancel out!

In order to extend this to a map from $C(H(N))$, we must check that $\varphi(e, f)^2 = q(e, f) \operatorname{id}$. Well, $\varphi_e^2 = \varphi_f^2 = 0$, so we are trying to check that $\varphi_e \varphi_f + \varphi_f \varphi_e = f(e) \operatorname{id}$. We may merely check this on pure tensors: on $(e_1 \wedge \cdots \wedge e_k)$, we get

$$\begin{aligned} &e \wedge \sum_{i=1}^{k} (-1)^i f(e_i)(e_1 \wedge \cdots \wedge \widehat{e_i} \wedge \cdots \wedge e_k) \\ &\quad + f(e)(e_1 \wedge \cdots \wedge e_k) + \sum_{i=1}^{k} (-1)^{i+1} f(e_i)(e \wedge e_1 \wedge \cdots \wedge \widehat{e_i} \wedge \cdots \wedge e_k). \end{aligned}$$

The two sums cancel out, so we are indeed left with the scalar operator $f(e) \operatorname{id}(e_1 \wedge \cdots \wedge e_k)$.

We have thus defined our map $\varphi \colon C(H(N)) \to \operatorname{End}(\wedge^\bullet N)$. We quickly go ahead and explain that it preserves the grading: here, $\wedge^\bullet N$ has a natural $\mathbb{Z}$-grading, which can be turned into a $\mathbb{Z}/2\mathbb{Z}$-grading, which we label by $\wedge^+ N \oplus \wedge^- N$; namely, $\wedge^+ N$ has the even pure tensors, and $\wedge^- N$ has the odd pure tensors. Then $\operatorname{End}(\wedge^\bullet N)$ obtains a natural $\mathbb{Z}/2\mathbb{Z}$-grading, where the degree-0 piece consists of the morphisms preserving the grading $\wedge^+ N \oplus \wedge^- N$, and the degree-$1$ piece swaps the grading. We thus see that any $(e, f) \in H(N)$ has $\varphi_{(e,f)} = \varphi_e + \varphi_f$ in $\operatorname{End}(\wedge^\bullet N)_1$, so because these elements generate $C(H(N))$, we conclude that φ preserves the grading.

While we are here, we also remark that this morphism is additive in N: given a decomposition $N = N_1 \oplus N_2$, the diagram

$$\begin{array}{ccc} C(H(N_1 \oplus N_2)) & \longrightarrow & \operatorname{End}(\wedge^\bullet(N_1 \oplus N_2)) \\ \downarrow & & \uparrow \\ C(H(N_1)) \otimes C(H(N_2)) & \longrightarrow & \operatorname{End}(\wedge^\bullet N_1) \otimes \operatorname{End}(\wedge^\bullet N_2) \end{array} \qquad \begin{array}{ccc} ((e_1, f_1), (e_2, f_2)) & \longmapsto & \operatorname{diag}(\varphi_{(e_1,f_1)}, \varphi_{(e_2,f_2)}) \\ \downarrow & & \uparrow \\ (e_1, f_1) \otimes (e_2, f_2) & \longmapsto & \varphi_{(e_1,f_1)} \otimes \varphi_{(e_2,f_2)} \end{array}$$

commutes. In particular, the left vertical arrow is an isomorphism by Lemma B.30, and the right arrow can be seen to be an isomorphism because N_1 and N_2 continue to be finitely generated and locally free, so locally it amounts to the identity $M_{n_1}(R) \otimes M_{n_2}(R) = M_{n_1}(M_{n_2}(R)) = M_{n_1 n_2}(R)$.

In light of the previous paragraph, we note that it is enough to show that φ is an isomorphism Zariski-locally, so we may assume that N is free, so we may assume that N is free of rank 1 by taking sums. However, a quick inspection of Example B.32 shows that the isomorphism $C(H(N)) \to \operatorname{End}(\wedge^\bullet N)$ constructed there is exactly φ! ∎

Corollary B.34. Fix a regular quadratic space (M, q) over R of even rank. Then $Z(C^+(M))$ is a separable algebra over R of rank 2.

Proof. The conclusion may be checked fppf-locally, so we may assume that $M \cong H(N)$ for some free module N by Lemma B.22. In this case, by Proposition B.33, we see that $C^+(M)$ is identified with

$$\operatorname{End}(\wedge^+ N) \oplus \operatorname{End}(\wedge^- N).$$

However, the center of a matrix algebra is given by the scalars, so the center is $R \oplus R$. ∎

B.4 The Orthogonal Group

We are now allowed to define the special orthogonal group.

Definition B.35 (orthogonal group)**.** Fix a regular quadratic space (M, q) over R of constant rank. Then the *orthogonal group* is

$$\mathrm{O}(M, q) \coloneqq \{g \in \mathrm{Aut}_R(M) : q(g(m)) = q(m) \text{ for all } m \in M\}.$$

We may also write $\mathrm{O}(M)$ or $\mathrm{O}(q)$ for $\mathrm{O}(M, q)$.

Definition B.36 (Dickson invariant)**.** Fix a regular quadratic space (M, q) over R of constant even rank. Then we define the *Dickson invariant* D of $\mathrm{O}(q)$ as follows: a given $g \in \mathrm{O}(q)$ induces an automorphism of $C^+(q)$ and thus an automorphism of the center Z, but $\mathrm{Aut}_R Z$ has two elements by Corollary B.34, so we define $D(g) \in \mathbb{Z}/2\mathbb{Z}$ to correspond to the trivial or nontrivial element of $\mathrm{Aut}_R Z$.

This definition is surprisingly tricky to "sit down and compute," but we must. Here are a couple tricks.

Example B.37. Let N be free of rank 1 spanned by $\{e\}$, and let $\{f\} \subseteq N^*$ be the dual basis. Then define $g \in \mathrm{Aut}_R H(N)$ by $g(e) = f$ and $g(f) = e$, and we can see that $q((ae, bf)) = q((be, af))$, so $g \in \mathrm{O}(H(N))$. Let's compute $D(g)$. By Example B.32, we see that $C^+(H(N))$ is identified with the subset of $\mathrm{End}(\wedge^\bullet H(N))$ given by the matrices $\left[\begin{smallmatrix} * & 0 \\ 0 & * \end{smallmatrix}\right]$ for the ordered basis $\{1, e\}$. Notably, ef goes to $\left[\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right]$, and fe goes to $\left[\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right]$, so

$$Z\left(C^+(H(N))\right) = Ref \oplus Rfe.$$

We now see that g swaps these two factors, so $D(g) = 1$.

Remark B.38. Given a decomposition $M = M_1 \oplus M_2$ of regular quadratic spaces of even rank, we note that there is a composite

$$\mathrm{O}(M_1) \to \mathrm{O}(M) \xrightarrow{D} \mathbb{Z}/2\mathbb{Z},$$

which we claim is just the Dickson invariant on $\mathrm{O}(M_1)$. Indeed, functoriality provides a ring homomorphism $C(M_1) \to C(M)$ (which we in fact know to be injective, for example by Proposition B.31), which then descends to an embedding

$$Z\left(C^+(M_1)\right) \to Z\left(C^+(M)\right)$$

of commutative algebras over R. Both of these are separable algebras of rank 2 over R, so this embedding must be an isomorphism. We conclude that the action of some $g \in \mathrm{O}(H(N_1))$ is nontrivial on the left center if and only if it is trivial on the right center, which is what we needed.

Example B.39. Let N be free with basis $\{e_1, \dots, e_d\}$, and let $\{f_1, \dots, f_d\} \subseteq N^*$ be the dual basis. Then define $g \in \mathrm{Aut}_R H(N)$ by $g(e_1) = f_1$ and $g(f_1) = e_1$ and $g(e_i) = e_i$ and $g(f_i) = f_i$ for $i > 1$. Then $H(N)$ decomposes as in Remark B.38 (namely, g is the identity on the large subspace $H(\mathrm{span}\{e_2, \dots, e_d\})$), so we may compute $D(g) = 1$ directly from Example B.37.

We now define the special orthogonal group.

Definition B.40 (special orthogonal group)**.** Fix a regular quadratic space (M, q) over R of constant rank. We will define the *special orthogonal group* $\mathrm{SO}(M, q)$ depending on the rank.

- If (M, q) is of odd rank, then $\mathrm{SO}(M, q)$ is the kernel of the determinant map on $\mathrm{O}(M, q)$.
- If (M, q) is of even rank, then $\mathrm{SO}(M, q)$ is the kernel of the Dickson invariant on $\mathrm{O}(M, q)$.

Remark B.41. Let's explain why we use the Dickson invariant instead of the determinant in the even rank case. It is in general true that $\langle gm, gn\rangle = \langle m, n\rangle$ for all $m, n \in M$ and so $g^\intercal g = \mathrm{id}$ (where $(-)^\intercal$ is defined with respect to $\langle -, -\rangle$), so $\det g^2 = 1$. But if, for example, $\mathrm{char}\, R = 2$, then this directly implies that $\det g = 1$, so we do not produce an index-2 subgroup!

Remark B.42. In this level of generality, it is not totally obvious that $\mathrm{SO}(M, q)$ has index 2! When $M \cong H(N)$, this follows from Example B.39. When M has odd rank and diagonalizes as in Lemma B.21, this follows by taking $g = \mathrm{diag}(-1, 1, \ldots, 1)$, which has determinant -1. Luckily, we will never stray outside these controlled cases in applications.

B.5 Lagrangian Subspaces

In the sequel, we will get a lot of utility out of orthogonal complements.

Definition B.43 (orthogonal complement)**.** Fix a quadratic space (M, q). For a subset $S \subseteq M$, we define the *orthogonal complement*

$$S^\perp = \{m \in M : \langle m, s\rangle = 0 \text{ for all } s \in S\}.$$

Remark B.44. Bilinearity implies that $S^\perp \subseteq M$ is a submodule: it is the intersection of the kernel of the functionals $m \mapsto \langle m, s\rangle$ as $s \in S$ varies.

Remark B.45. Fix a regular quadratic space (M, q). Given a direct summand $U \subseteq M$, we note that the isomorphism $M \to M^*$ given by q restricts to a surjection $M^* \to U^*$ (given by $m \mapsto \langle m, -\rangle|_U$) with kernel $U^\perp$, meaning that we have a short exact sequence

$$0 \to U^\perp \to M \to U^* \to 0.$$

Note that U^* is finitely generated and projective because U is, so the short exact sequence splits so $U^\perp$ is also finitely generated and projective. In fact, we can see that $\mathrm{rank}\, U + \mathrm{rank}\, U^\perp = \mathrm{rank}\, U^* + \mathrm{rank}\, U^\perp = \mathrm{rank}\, M$ from this short exact sequence.

Definition B.46 (Lagrangian)**.** Fix a regular quadratic space (M, q). Then a submodule $N \subseteq M$ is *Lagrangian* if and only if it is a direct summand and $N^\perp = N$.

Example B.47. Fix N as in Example B.18. Embedding N into $H(N)$, we see that $N^\perp$ consists of the elements $(e, f) \in H(N)$ for which $f = 0$. Thus, $N^\perp = N$, so N is Lagrangian.

The orthogonal groups can be used to parameterize Lagrangian subspaces.

Proposition B.48. Fix a regular quadratic space (V, q) over a field K. Then the natural action of $\mathrm{O}(V)$ on the collection G of Lagrangians is transitive.

Remark B.49. One can weaken the hypothesis that K is a field, but one must be careful. We refer to [Knu91, Section IV.5] for some discussion.

Appendix C
Homework 1

The homework problems have been recorded as propositions.

C.1 The Cohomology of $\widehat{\mathbb{Z}}$

We begin by recalling the cohomology of cyclic groups.

Lemma C.1. 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 $\mathrm{N}_G \coloneqq \sum_{g\in G} g$. The kernel of N_G can be calculated as the image of $(\sigma-1)$ again, so we see that we can iterate to produce a resolution

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

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

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

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

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

as desired. ∎

It is worthwhile to explain the functoriality properties of Lemma C.1, which are rather bizarre.

Lemma C.2. Fix a surjection $G' \to G$ of cyclic groups. Then given a morphism $f\colon M \to M'$ where M is a G-module, and M' has the induced G'-module structure, the induced map

$$f\colon \mathrm{H}^i(G; M) \to \mathrm{H}^i(G'; M')$$

is $(\#G'/\#G)^{\lfloor i/2 \rfloor} f$ once these groups have been identified with subquotients of M and M' via Lemma C.1.

Proof. Denote the surjection $G' \to G$ by g, and we choose a generator σ' for G', and then we define $\sigma := g(\sigma')$, which we see must generate G. We also set $m := \#G'/\#G$ for brevity. Now, the identities $g(\sigma' - 1) = (\sigma - 1)$ and $g(\mathrm{N}_{G'}) = m\,\mathrm{N}_G$ produce the morphism

$$\begin{array}{ccccccccccccccc}
\cdots & \longrightarrow & \mathbb{Z}[G'] & \xrightarrow{\mathrm{N}_{G'}} & \mathbb{Z}[G'] & \xrightarrow{(\sigma'-1)} & \mathbb{Z}[G'] & \xrightarrow{\mathrm{N}_{G'}} & \mathbb{Z}[G'] & \xrightarrow{(\sigma'-1)} & \mathbb{Z}[G'] & \xrightarrow{\deg} & \mathbb{Z} & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle m^2 g} & & \downarrow{\scriptstyle mg} & & \downarrow{\scriptstyle mg} & & \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle g} & & \| & & \\
\cdots & \longrightarrow & \mathbb{Z}[G] & \xrightarrow[\mathrm{N}_G]{} & \mathbb{Z}[G] & \xrightarrow[(\sigma-1)]{} & \mathbb{Z}[G] & \xrightarrow[\mathrm{N}_G]{} & \mathbb{Z}[G] & \xrightarrow[(\sigma-1)]{} & \mathbb{Z}[G] & \xrightarrow[\deg]{} & \mathbb{Z} & \longrightarrow & 0
\end{array}$$

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 $\mathrm{Hom}_G(-, M)$ and $\mathrm{Hom}_{G'}(-, M')$ to get another morphism of chain complexes

$$\begin{array}{ccccccccccccc}
0 & \longrightarrow & M & \xrightarrow{(\sigma-1)} & M & \xrightarrow{\mathrm{N}_G} & M & \xrightarrow{(\sigma-1)} & M & \xrightarrow{\mathrm{N}_G} & M & \longrightarrow & \cdots \\
 & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle mf} & & \downarrow{\scriptstyle mf} & & \downarrow{\scriptstyle m^2 f} & & \\
0 & \longrightarrow & M' & \xrightarrow[(\sigma'-1)]{} & M' & \xrightarrow[\mathrm{N}_{G'}]{} & M' & \xrightarrow[(\sigma'-1)]{} & M' & \xrightarrow[\mathrm{N}_{G'}]{} & M' & \longrightarrow & \cdots
\end{array}$$

induced by f and the above morphism. Taking cohomology, 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. ∎

Proposition C.3. Let $\mathfrak{g} = \widehat{\mathbb{Z}}$, a profinite group (the inverse limit $\lim_n \mathbb{Z}/n\mathbb{Z}$), which is isomorphic to the absolute Galois group of a finite field. Let M be a discrete $\mathfrak{g}$-module (i.e., the stabilizer of ever $m \in M$ is an open subgroup of $\mathfrak{g}$; equivalently, $M = \bigcup_H M^H$ is the union of the invariants of open subgroups of $\mathfrak{g}$). Recall from Milne's notes [Mil20, Section II.4] that the cohomology of a profinite group G acting continuously on G can be computed as the inductive limit, via the inflations, over all open normal subgroups H:

$$\mathrm{H}^i(G; M) = \operatorname*{colim}_H \mathrm{H}^i(G/H; M^H).$$

(a) Denote by σ the topological generator 1 in $\mathfrak{g}$. Let M' be the set of elements annihilated by $1 + \sigma + \sigma^2 + \cdots + \sigma^n$ for some $n \in \mathbb{N}$. Show that $\mathrm{H}^1(\mathfrak{g}; M) = M'/(\sigma - 1)M$. In particular, if M is torsion, we have $\mathrm{H}^1(\mathfrak{g}; M) = M/(\sigma - 1)M$.

(b) If M is divisible (i.e., the multiplication-by-n map is surjective for all $n \geq 1$) or finite torsion, then $\mathrm{H}^2(\mathfrak{g}; M) = 0$.

(c) Show that $\mathrm{H}^i(\mathfrak{g}; \mathbb{Q}) = 0$ for all $i \geq 1$. Here, $\mathbb{Q}$ has the trivial $\mathfrak{g}$-action.

(d) Show that the group $\mathfrak{g}$ has cohomological dimension 1; i.e., for all finite discrete $\mathfrak{g}$-modules M, we have $\mathrm{H}^i(\mathfrak{g}; M) = 0$ for $i > 1$, and there exists M such that $\mathrm{H}^1(\mathfrak{g}; M) \neq 0$.

(e) Show that for any discrete $\mathfrak{g}$-module M, we have $\mathrm{H}^i(\mathfrak{g}; M) = 0$ when $i \geq 3$.

Proof. We proceed in steps, following [GS13, Section XIII.1]. Before doing anything, we set up some notation around the cohomology of (pro)cyclic groups. For example, let's describe the open subgroups of $\mathfrak{g}$. Set $H_m := \overline{\langle \sigma^m \rangle}$ for brevity, which we note is the kernel of the map $\mathfrak{g} \to \mathbb{Z}/m\mathbb{Z}$ defined by $\sigma \mapsto 1$, so H_m is

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

Thus, we see that

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

where $M^{\sigma^m} = M^{\overline{\langle \sigma^m \rangle}}$ by continuity. Because $\mathfrak{g}/H_m$ is cyclic, Lemma C.1 tells us that $i > 0$ has

$$\mathrm{H}^i(\mathfrak{g}; M) = \begin{cases} \operatorname{colim}_{m \geq 1} M^{\mathfrak{g}} / \mathrm{N}_{\mathfrak{g}/H_m}\left(M^{\sigma^m}\right) & \text{if } i \text{ is even,} \\ \operatorname{colim}_{m \geq 1} \ker \mathrm{N}_{\mathfrak{g}/H_m} / (1-\sigma) M^{\sigma^m} & \text{if } i \text{ is odd.} \end{cases}$$

We now see that we have to use Lemma C.2 to compute the internal maps: the map between the mth term and the m'th term (where $m \mid m'$) is given by multiplication by $(m'/m)^{\lfloor i/2 \rfloor}$. The various parts of the problem amount to calculations with this.

(a) We go ahead and compute at $i = 0$ and $i = 1$. At $i = 0$, there is nothing to do because the colimit is just $M^{\mathfrak{g}}$ at all stages. At $i = 1$, we claim that the natural inclusions $\ker \mathrm{N}_{\mathfrak{g}/H_m} \to M'$ induce an isomorphism

$$\operatorname*{colim}_{m \geq 1} \frac{\ker \mathrm{N}_{\mathfrak{g}/H_m}}{(1-\sigma) M^{\sigma^m}} \to \frac{M'}{(1-\sigma) M}.$$

Here are the checks on this map.

- Well-defined: the inclusions assemble into a well-defined map because the internal maps in the colimit are simply induced by inclusion. Indeed, there is no multiplication present because $i = 1$.
- Surjective: any class $a \in M'$ will be annihilated by some $1+\sigma+\cdots+\sigma^{m-1}$. But then $(\sigma^m - 1)\, a = 0$ as well, so $a \in \ker \mathrm{N}_{\mathfrak{g}/H_m}$.
- Injective: suppose a class a coming from $\ker \mathrm{N}_{\mathfrak{g}/H_m}/(1-\sigma)M^{\sigma^m}$ in the colimit goes to 0 in $M'/(1-\sigma)M$. In particular, we are given that a is annihilated by some $1 + \sigma + \cdots + \sigma^{m-1}$ and also takes the form $(1-\sigma)b$. It follows that $\sigma^m b = b$ as well, so $a \in (1-\sigma)M^{\sigma^m}$, so a vanishes in the colimit already.

While we're here, we note that if M is torsion, then $M' = M$. Indeed, any given element $a \in M$ is stabilized by some open subgroup H_m, meaning $\sigma^m a = a$. Thus,

$$\left(1 + \sigma + \cdots + \sigma^{mn-1}\right) a = n \left(1 + \sigma + \cdots + \sigma^{m-1}\right) a$$

vanishes for some n because a is torsion.

(b) We handle torsion and divisibility separately.

- We show $\mathrm{H}^2(\mathfrak{g}; M) = 0$ when M is torsion. Indeed, in this case, we are computing the colimit of $M^{\mathfrak{g}}/\mathrm{N}_{\mathfrak{g}/H_m}\left(M^{\sigma^m}\right)$, where the transition map between the mth and m'th term is given by multiplication by m'/m. Because M is torsion, for any given class in the mth term $M^{\mathfrak{g}}/\mathrm{N}_{\mathfrak{g}/H_m}\left(M^{\sigma^m}\right)$, we can select m' sufficiently large so that the multiplication map will kill it. We conclude that the entire colimit must vanish.
- We show $\mathrm{H}^2(\mathfrak{g}; M) = 0$ when M is divisible. We will show that the multiplication-by-n endomorphism on $\mathrm{H}^2(\mathfrak{g}; M)$ is injective for all positive integers $n > 0$, which will complete the proof because $\mathrm{H}^2(\mathfrak{g}; M)$ is a torsion group (because it is the colimit of torsion groups). To see the claim, we note that $n \colon M \to M$ is surjective, so we have a short exact sequence

$$0 \to M[n] \to M \xrightarrow{n} M \to 0$$

of discrete $\mathfrak{g}$-modules. The long exact sequence (which holds even after the colimit because the colimit is filtered) then shows that

$$\mathrm{H}^2(\mathfrak{g}; M[n]) \to \mathrm{H}^2(\mathfrak{g}; M) \xrightarrow{n} \mathrm{H}^2(\mathfrak{g}; M)$$

is exact, so the claim follows from the previous point.

(c) Because $\mathbb{Q}$ is divisible, we know that $\mathrm{H}^i(\mathfrak{g}; \mathbb{Q}) = 0$ for $i = 2$ automatically, and we show in part (e) below that $\mathrm{H}^i(\mathfrak{g}; \mathbb{Q}) = 0$ for $i \geq 3$ automatically as well. Further, we see that no nonzero element $\mathbb{Q}$ is not annihilated by $1 + \sigma + \cdots + \sigma^n$ for any n, so $\mathrm{H}^1(\mathfrak{g}; \mathbb{Q}) = 0$ as well. We conclude that

$$\mathrm{H}^i(\mathfrak{g}; \mathbb{Q}) = \begin{cases} \mathbb{Q} & \text{if } i = 0, \\ 0 & \text{if } i \geq 1. \end{cases}$$

(d) Given a finite $\mathfrak{g}$-module M, we see that M is torsion, so $\mathrm{H}^2(\mathfrak{g}; M) = 0$ automatically. Additionally, we will show in part (e) below that $\mathrm{H}^i(\mathfrak{g}; M) = 0$ for $i \geq 3$ automatically as well.

It remains to actually find a finite $\mathfrak{g}$-module M with nonzero $\mathrm{H}^1(\mathfrak{g}; M)$. Well, give some finite abelian group A the trivial action. Then $A' = A$ and $(\sigma - 1)A = 0$, so $\mathrm{H}^1(\mathfrak{g}; A) = A$, which is nonzero.

(e) We handle even i and odd i separately, giving the same argument twice. It is possible that one can use dimension-shifting to deduce one case from the other, but this is not a totally trivial matter because $\mathfrak{g}$ is infinite.

- We show $\mathrm{H}^i(\mathfrak{g}; M) = 0$ when i is odd and $i \geq 3$. Write $i = 2j + 1$ for $j \geq 1$ so that $\lfloor i/2 \rfloor = j$. Then

$$\mathrm{H}^i(\mathfrak{g}; M) = \operatorname*{colim}_{m \geq 1} \frac{\ker \mathrm{N}_{\mathfrak{g}/H_m}}{(1-\sigma)M^{\sigma^m}},$$

and the transition maps are given by multiplication by $(m'/m)^j$. It is enough to show that any class $a \in \ker \mathrm{N}_{\mathfrak{g}/H_m}$ vanishes in the colimit. Well, $m\mathrm{H}^1(\mathfrak{g}/H_m; M^{\sigma^m}) = 0$, so we see that ma must vanish in this cohomology group, so $ma = (1-\sigma)b$ for some $b \in M^{\sigma^m}$. Thus, we see that a vanishes along the transition map

$$\frac{\ker \mathrm{N}_{\mathfrak{g}/H_m}}{(1-\sigma)M^{\sigma^m}} \xrightarrow{m^j} \frac{\ker \mathrm{N}_{\mathfrak{g}/H_{m^2}}}{(1-\sigma)M^{\sigma^{m^2}}}$$

because $m^j a = (1-\sigma)m^{j-1}b$.

- We show $\mathrm{H}^i(\mathfrak{g}; M) = 0$ when i is even and $i \geq 4$. Write $i = 2j$ for $j \geq 2$ so that $\lfloor i/2 \rfloor = j$. Then

$$\mathrm{H}^i(\mathfrak{g}; M) = \operatorname*{colim}_{m \geq 1} \frac{M^{\mathfrak{g}}}{\mathrm{N}_{\mathfrak{g}/H_m}(M^{\sigma^m})},$$

and the transition maps are given by multiplication by $(m'/m)^j$. Once again, it is enough to show that any class $a \in M^{\mathfrak{g}}$ vanishes in the colimit. Well, find m with $\sigma^m a = a$, so $m\mathrm{H}^2(\mathfrak{g}/H_m; M^{\sigma^m}) = 0$ implies that $ma = \mathrm{N}_{\mathfrak{g}/H_m}(b)$ for some $b \in M^{\sigma^m}$. Then $\mathrm{N}_{\mathfrak{g}/H_{mk}}(b) = \mathrm{N}_{\mathfrak{g}/H_k}\mathrm{N}_{\mathfrak{g}/H_m}(b) = kma$, so a vanishes along the transition map

$$\frac{M^{\mathfrak{g}}}{\mathrm{N}_{\mathfrak{g}/H_m}(M^{\sigma^m})} \to \frac{M^{\mathfrak{g}}}{\mathrm{N}_{\mathfrak{g}/H_{m^2}}(M^{\sigma^{m^2}})}$$

because $m^j a = m^{j-2}\mathrm{N}_{\mathfrak{g}/H_{m^2}}(b)$. ∎

C.2 Local Cohomology

Proposition C.4. In this question, K is a finite extension of $\mathbb{Q}_p$, $\Gamma_K := \mathrm{Gal}(\overline{K}/K)$, M is a finite Γ_K-module, and we set $\mathrm{H}^i(M) := \mathrm{H}^i(K;M) = \mathrm{H}^i(\Gamma_K;M)$. Then local Tate duality asserts that the cup product induces a perfect pairing between two finite abelian groups

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

where $M^* := \mathrm{Hom}(M, \mu_\infty)$ and $\mu_\infty := \bigcup_n \mu_n$. The Euler–Poincaré characteristic is defined for any finite Γ_K-module M as

$$\chi(M) := \frac{h^0(M)h^2(M)}{h^1(M)},$$

where $h^i := \#\mathrm{H}^i(M)$. Then we have a formula

$$\chi(M) = \frac{1}{\#(\mathcal{O}_K/n\mathcal{O}_K)},$$

where $n := \#M$.

(a) How many elements does $K^\times/K^{\times 2}$ have? How many different quadratic extensions does K have? In general, how many elements does $K^\times/K^{\times \ell}$ have a prime ℓ?

(b) Let E be an elliptic curve over K and ℓ a prime number (we allow $\ell = p$). Then it is known that the Weil pairing induces a Γ_K-isomorphism $E[\ell] \cong E[\ell]^*$. Show that, regardless of the reduction type of E, we always have

$$\dim_{\mathbb{F}_\ell} E(K)/\ell E(K) = \frac{1}{2}\dim_{\mathbb{F}_\ell} \mathrm{H}^1(K;E[\ell]).$$

What are the possible values of $\dim_{\mathbb{F}_\ell} E(K)/\ell E(K)$ if $K = \mathbb{Q}_p$?

Proof of Proposition C.4(a). Let v be the place of K. Let's start by computing the size of $K^\times/K^{\times \ell}$ for primes ℓ. By the Kummer exact sequence

$$0 \to \mu_\ell \to \mathbb{G}_m \xrightarrow{\ell} \mathbb{G}_m \to 0$$

and Hilbert's theorem 90, we conclude that the boundary map $K^\times/K^{\times \ell} \to \mathrm{H}^1(K;\mu_\ell)$ is an isomorphism. Thus, we may focus on computing the size of $\mathrm{H}^1(K;\mu_\ell$, for which we use the Euler characteristic. Indeed, we know that $h^1(\mu_\ell)$ is

$$h^1(\mu_\ell) = h^0(\mu_\ell)h^2(\mu_\ell) \cdot \#(\mathcal{O}_K/\ell\mathcal{O}_K)$$

after plugging in for $\chi(\mu_\ell)$. We will compute each of these terms separately.

- For $h^0(\mu_\ell)$, note $\mathrm{H}^0(K;\mu_\ell) = \mu_\ell(K)$.
- For $h^2(\mu_\ell)$, we claim that $\mu_\ell^* = \mathbb{Z}/\ell\mathbb{Z}$, which implies that $h^2(\mu_\ell^*)$ is

  $$h^0(\mathbb{Z}/\ell\mathbb{Z}) = \ell$$

  by local duality. To show the claim, recall $\mu_\ell^* = \mathrm{Hom}(\mu_\ell, \mu_\infty)$. Any map $\mu_\ell \to \mu_\infty$ factors through $\mu_\infty[\ell] = \mu_\ell$, so $\mu_\ell^* = \mathrm{Hom}(\mu_\ell, \mu_\ell)$. Now, a map $\mu_\ell \to \mu_\ell$ must be of the form $\zeta \mapsto \zeta^k$ for some integer k, so there is a surjection $\mathbb{Z} \to \mu_\ell^*$ with kernel $\ell\mathbb{Z}$. The induced map $\mathbb{Z}/\ell\mathbb{Z} \to \mu_\ell^*$ is also Galois-invariant because all the given homomorphisms $\mu_\ell \to \mu_\ell$ are automatically Galois-invariant.
- For $\#(\mathcal{O}_K/\ell\mathcal{O}_K)$, we have two cases. If $v \nmid \ell$, then ℓ is a unit in $\mathcal{O}_K$, so this quotient is trivial. Otherwise, if $v \mid \ell$, then $\mathcal{O}_K \cong \mathbb{Z}_\ell^{[K:\mathbb{Q}_p]}$ as an abelian group, so this quotient is isomorphic to

In total, we conclude that

$$\#\left(K^\times/K^{\times\ell}\right) = \#\mu_\ell(K)\cdot\ell\cdot\ell^{[K:\mathbb{Q}_p]\cdot 1_{v\mid\ell}}.$$

For example,

$$\#\left(K^\times/K^{\times 2}\right) = \begin{cases} 4 & \text{if } v\nmid 2,\\ 4\cdot 2^{[K:\mathbb{Q}_2]} & \text{if } v\mid 2.\end{cases}$$

Lastly, we note that the number of quadratic extensions of K are in bijection with $K^\times/K^{\times 2}$ by Kummer theory. (Slightly more explicitly, a class $\alpha\in K^\times/K^{\times 2}$ gives rise to a quadratic extension $K(\sqrt{\alpha})$, and these extensions are unique. In characteristic 0, completing the square shows that every quadratic extension arises in this way.) Thus, the preceding equation also computes the number of quadratic extensions of K. ■

For the proof of (b), we will require the following fact. For the subsequent argument, we will need the following fact.

Lemma C.5. Fix an elliptic curve E over a nonarchimedean local field K_v. Then $E(K_v)$ admits a finite-index subgroup isomorphic to $\mathcal{O}_v$.

Proof. The proof of this result is fairly involved, so we will be sketchy; we refer to [Sil09, Proposition VII.6.3] for more details. Let $E_0(K_v)\subseteq E(K)$ denote the collection of points which reduce to a non-singular point in $E(\mathbb{F}_v)$, and we let $E_1(K_v)\subseteq E(K)$ denote the collection of points which reduce to the identity of $E(\mathbb{F}_v)$.

The main point is to show that $E(K_v)/E_0(K_v)$ is finite, but for now let's explain why it completes the proof. It turns out that the canonical maps

$$0\to E_1(K_v)\to E_0(K_v)\to E(\mathbb{F}_v)\to 0$$

assemble into a short exact sequence [Sil09, Proposition VII.2.1]. Thus, it is enough to show that $E_1(K_v)$ admits a finite-index subgroup isomorphic to $\mathcal{O}_v$. Well, $E_1(K_v)$ is isomorphic to $G_E(\mathfrak{m}_v)$, where G_E is the one-dimensional formal group of E [Sil09, Proposition VII.2.2]. Then the canonical filtration $G_E(\mathfrak{m}_v^\bullet)$ shows that $G_E(\mathfrak{m}_v^i)/G_E\left(\mathfrak{m}_v^{i+1}\right)$ is finite for all i, and for i large enough, there is a logarithm map establishing that $G_E(\mathfrak{m}_v^i)$ is isomorphic to $\mathcal{O}_v$. This completes the proof modulo the finiteness of $E(K_v)/E_0(K_v)$.

It remains to show that $E(K_v)/E_0(K_v)$, for which we follow [Sil09, Exercise 7.6]. Because K_v is a topological field, we see that $E(K_v)\subseteq\mathbb{P}^2(K_v)$ is a topological group. In fact, $E(K_v)\subseteq\mathbb{P}^2(K_v)$ is a closed subset of the compact space $\mathbb{P}^2(K_v)$, so $E(K_v)$ is compact. The reduction map $\mathbb{P}^2(K_v)\to\mathbb{P}^2(\mathbb{F}_v)$ is a continuous map to a finite discrete space, so $E_0(K_v)\subseteq E(K_v)$ is an open subgroup. Compactness then forces $E_0(K_v)$ to be finite-index in $E(K_v)$. ■

Proof of Proposition C.4(b). We refer to [Sil09, Proposition III.8.1] (also recorded in the notes) for the fact that the Weil pairing induces a Galois-invariant isomorphism $E[\ell]\to E[\ell]^*$. This follows from the fact that the Weil pairing $E[\ell]\times E[\ell]\to\mu_\ell$ is non-degenerate and Galois-invariant.

We will calculate both sides of the required equality

$$\dim_{\mathbb{F}_\ell} E(K)/\ell E(K)\overset{?}{=}\frac{1}{2}\dim_{\mathbb{F}_\ell}\mathrm{H}^1(K;E[\ell])$$

separately.

- We compute $\dim_{\mathbb{F}_\ell} E(K)/\ell E(K)$, using Lemma C.5, which grants us an exact sequence

  $$0\to\mathcal{O}_v\to E(K)\to C\to 0,$$

  where C is some finite abelian group. This exact sequence has an endomorphism given by multiplication by ℓ. Applying the Snake lemma to this endomorphism yields the exact sequence

  $$0\to\mathcal{O}_v[\ell]\to E(K)[\ell]\to C[\ell]\to\frac{\mathcal{O}_v}{\ell\mathcal{O}_v}\to\frac{E(K)}{\ell E(K)}\to\frac{C}{\ell C}\to 0.$$

The calculation will follow by taking dimensions of this exact sequence; for example, just the right-exact part of this sequence immediately shows us that $E(K)/\ell E(K)$ is finite. We thus have

$$\dim_{\mathbb{F}_\ell} \frac{E(K)}{\ell E(K)} - \dim_{\mathbb{F}_\ell} E(K)[\ell] = \dim_{\mathbb{F}_\ell} \frac{\mathcal{O}_v}{\ell \mathcal{O}_v} - \dim_{\mathbb{F}_\ell} \mathcal{O}_v[\ell] + \dim_{\mathbb{F}_\ell} \frac{C}{\ell C} - \dim_{\mathbb{F}_\ell} C[\ell].$$

Now, we note that $\mathcal{O}_v[\ell] = 0$ because K has characteristic 0. Continuing, and $\#C_\ell = \#(C/\ell C)$ because the kernel and cokernel of the endomorphism $\ell \colon C \to C$ should have the same size. We are left with

$$\dim_{\mathbb{F}_\ell} \frac{E(K)}{\ell E(K)} = \dim_{\mathbb{F}_\ell} \frac{\mathcal{O}_v}{\ell \mathcal{O}_v} + \dim_{\mathbb{F}_\ell} E(K)[\ell].$$

To compute $\mathcal{O}_K/\ell\mathcal{O}_K$, there are two cases: if $v \nmid \ell$, then this is trivial; otherwise, $\mathcal{O}_K \cong \mathbb{Z}_\ell^{[K:\mathbb{Q}_\ell]}$, so in total,

$$\dim_{\mathbb{F}_\ell} \frac{E(K)}{\ell E(K)} = \dim_{\mathbb{F}_\ell} E(K)[\ell] + \begin{cases} 0 & \text{if } v \nmid \ell, \\ [K:\mathbb{Q}_\ell] & \text{if } v \mid \ell. \end{cases}.$$

- We compute $\dim_{\mathbb{F}_\ell} \mathrm{H}^1(K; E[\ell])$, using the Euler characteristic. Indeed, by plugging everything in, we see that
$$h^1(E[\ell]) = h^0(E[\ell])h^2(E[\ell]) \cdot \#\left(\mathcal{O}_K/\ell^2\mathcal{O}_K\right).$$
(Recall $E[\ell]$ has size ℓ^2 over the algebraic closure.) Because $E[\ell] \cong E[\ell]^*$, it follows that $h^0(E[\ell]) = h^2(E[\ell])$ by local duality. Thus, noting $h^0(E[\ell]) = E(K)[\ell]$, we find that
$$h^1(E[\ell]) = \#E(K)[\ell]^2 \cdot \#\left(\mathcal{O}_K/\ell^2\mathcal{O}_K\right).$$
As in the previous point, we can calculate $\mathcal{O}_K/\ell^2\mathcal{O}_K$ by cases for when $v \nmid \ell$ or $v \mid \ell$, finding that
$$\dim_{\mathbb{F}_\ell} \mathrm{H}^1(K; E[\ell]) = 2\dim_{\mathbb{F}_\ell} E(K)[\ell] + \begin{cases} 0 & \text{if } v \nmid \ell, \\ 2[K:\mathbb{Q}_\ell] & \text{if } v \mid \ell. \end{cases}.$$

The equality

$$\dim_{\mathbb{F}_\ell} E(K)/\ell E(K) = \frac{1}{2}\dim_{\mathbb{F}_\ell} \mathrm{H}^1(K; E[\ell])$$

now follows by comparing the above two calculations.

We now move to $K = \mathbb{Q}_p$. The above calculation has showed that

$$\dim_{\mathbb{F}_\ell} E(\mathbb{Q}_p)/\ell E(\mathbb{Q}_p) = \dim_{\mathbb{F}_\ell} E(\mathbb{Q}_p)[\ell] + 1_{p=\ell}.$$

Now, $E(\overline{\mathbb{Q}}_p)[\ell]$ is isomorphic to $(\mathbb{Z}/\ell\mathbb{Z})^2$, so $E(\mathbb{Q}_p)[\ell]$ has dimension in $\{0,1,2\}$. We conclude that

$$\dim_{\mathbb{F}_\ell} E(\mathbb{Q}_p)/\ell E(\mathbb{Q}_p) \in \begin{cases} \{0,1,2\} & \text{if } p \neq \ell, \\ \{1,2,3\} & \text{if } p = \ell, \end{cases}$$

as needed. ∎

Remark C.6. In the notes, we show the stronger statement that $\mathrm{H}^1(K; E[m])$ is a non-degenerate quadratic space (with the pairing induced by the Weil pairing), and $E(K)/mE(K)$ embeds as a maximal isotropic subspace. Note that m is not required to be prime!

C.3 The "Counterexample" to Grunwald–Wang

Proposition C.7.

(a) Show that 16 is an eighth power in $\mathbb{R}$ and all $\mathbb{Q}_p$ for $p \neq 2$, but not an eighth power in $\mathbb{Q}_2$.

(b) Let $K = \mathbb{Q}(\sqrt{7})$. Show that 16 is an eighth power in every completion K_v of K but not an eighth power in K. In particular, the localization map

$$\mathrm{H}^1(K;\mu_8) \to \prod_v \mathrm{H}^1(K_v;\mu_8)$$

is not injective.

Proof. Before showing either of the parts, we claim that 16 is an eighth power in a field K if and only if $\sqrt{2} \in K$ or $\sqrt{-2} \in K$ or $\sqrt{-1} \in K$. Certainly the reverse direction holds because

$$\left(\sqrt{2}\right)^8 = \left(\sqrt{-2}\right)^8 = (1+i)^8 = 16.$$

In the forward direction, if 16 is an eighth power, then we see that one of 4 or -4 is a fourth power. If -4 is a fourth power, then -4 is a square, so either $2 = 0$ (in which case $\sqrt{2} \in K$) or -1 is a square. Otherwise, 4 is a fourth power, so one of 2 or -2 is a square, as desired.

(a) We do this by casework on the place v. For example, if v is archimedean, the result follows because $\sqrt{2} \in \mathbb{R}$. Additionally, for $v = 2$, we see that $v_2(16) = 4$ is not divisible by 8, so 16 cannot possibly be an eighth power.

It remains to handle places v given by odd primes p. It is enough to show that $\{\sqrt{2}, \sqrt{-2}, i\} \cap \mathbb{Q}_p \neq \varnothing$ for each odd prime p. In other words, we are asking for one of the quadratics to $x^2 - 2$ or $x^2 + 2$ or $x^2 - 1$ to admit a root. By Hensel's lemma, it is equivalent for one of these quadratics to admit a root over $\mathbb{F}_p$, which in turn is equivalent to having

$$1 \overset{?}{\in} \left\{ \left(\frac{2}{p}\right), \left(\frac{-2}{p}\right), \left(\frac{-1}{p}\right) \right\}.$$

To see this, we note that

$$\left(\frac{2}{p}\right)\left(\frac{-2}{p}\right)\left(\frac{-1}{p}\right) = 1,$$

so it is not possible for all three Legendre symbols to equal -1!

(b) Set $K \coloneqq \mathbb{Q}(\sqrt{7})$ for brevity. By (a), to show that 16 is an eighth power in all K_v, we only have to handle places v above 2. Note that 7 is not a square in $\mathbb{Q}_2$ (indeed, it is not a square $\pmod 4$), so there is only one place $\mathbb{Q}_2(\sqrt{7})$ above 2. It remains to show that 16 is an eighth power in $\mathbb{Q}_2(\sqrt{7})$, which is true because $\sqrt{-1} \in \mathbb{Q}_2(\sqrt{7})$ (indeed, $-7 \in \mathbb{Q}_2^{\times 2}$).

Next, we should show that 16 is not an eighth power in K. It is enough to show that none of $\sqrt{-1}$ or $\sqrt{2}$ or $\sqrt{-2}$ are in K, which holds because $K = \mathbb{Q}(\sqrt{7})$ is a quadratic extension avoiding all those elements. Explicitly, K is totally real, so -1 and -2 cannot be squares, and we can see that there is no $a, b \in \mathbb{Z}$ for which

$$\left(a + b\sqrt{7}\right)^2 = a^2 + 7b^2 + 14ab\sqrt{7}$$

can equal 2: this would require $a = 0$ or $b = 0$, but certainly neither 2 nor $7/2$ is a square in $\mathbb{Z}$.

It remains to explain the last sentence. Well, we may functorially identify $\mathrm{H}^1(K;\mu_8)$ with $K^\times/K^{\times 8}$ (by the boundary map of the Kummer exact sequence for $\mathbb{G}_{m,K}$), so the map

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

fails to be injective because the nontrivial class $16 \in K^\times/K^{\times 8}$ vanishes in all localizations. ∎

C.4 Congruent Number Elliptic Curves at 2

Consider the congruent number elliptic curve over $\mathbb{Q}$ given on affine coordinates by

$$E_d \colon y^2 = x(x-d)(x+d).$$

The local condition at a place v can be described using the map

$$\begin{array}{ccc} E_d(K_v) & \to & \left\{(\alpha,\beta,\gamma) \in (K_v^\times / K_v^{\times 2})^{\oplus 3} : \alpha\beta\gamma = 1\right\} \\ (x,y) & \mapsto & (x, x-d, x+d) \end{array}$$

for $x \notin \{0, \pm d\}$, and a similar map works for $x \in \{0, \pm d\}$ where the two nonzero coordinates determine the third via $\alpha\beta\gamma = 1$. Assume that d is an odd integer.

Lemma C.8. Fix everything as above. We compute information about image of $\delta_v \colon E_d(\mathbb{Q}_v)/2E_d(\mathbb{Q}_v) \to \mathrm{H}^1(\mathbb{Q}_v; H)$ for each place v, where $H \subseteq \mu_2^{\oplus 3}$ is the trace-zero hyperplane.

(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

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

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

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 the image of δ_v is $\mathrm{H}^1_{\mathrm{ur}}(\mathbb{Q}_v; H)$. The result now follows by looking coordinate-wise.

(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 the dimension calculations of Proposition C.4(a). 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 Proposition C.4(a) again. ∎

Proposition C.9. Fix everything as above.

(a) Show that the local condition at the 2-adic place is the three-dimensional subspace spanned by $\{(1,5,5), (-1,-d,d), (d,2,2d)\}$.

(b) Show that if the following system of equations $T_{\alpha,\beta,\gamma}$ for α,β,γ all positive and odd

$$\begin{cases} \alpha u^2 - \beta v^2 = -d, \\ \alpha u^2 - \gamma w^2 = d \end{cases}$$

has solutions in $\mathbb{Q}_v$ for all $v \neq 2$, then $T_{\alpha,\beta,\gamma}$ has solutions in $\mathbb{Q}_2$.

Proof. We quickly handle (a).

1. Because -1, 2, and 5 are linearly independent in $\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2}$, we see that the triples $(1,5,5)$, $(-1,-d,d)$, and $(d,2,2d)$ are linearly independent triples. Thus,
$$\dim_{\mathbb{F}_2} \operatorname{span}(S \cup \{1,5,5\}) = 3,$$
which also equals $\dim_{\mathbb{F}_2} \operatorname{im} \delta_v$ by Proposition C.4(a). Thus, it suffices to show that $\operatorname{span}(S \cup \{1,5,5\}) \subseteq \operatorname{im} \delta_v$.

2. By Lemma C.8, it is enough to check that $(1,5,5) \in \operatorname{im} \delta_v$. For this, we recall that it is equivalent to produce a nonzero solution to the system
$$\begin{cases} x^2 - 5y^2 = +dw^2, \\ x^2 - 5z^2 = -dw^2, \end{cases}$$
in $\mathbb{Q}_2$. The solubility of this system does not change if we change d by an element of $\mathbb{Q}_2^{\times 2}$, so we may assume $d \in \{\pm 1, \pm 5\}$. Similarly, by symmetry, we may adjust the sign of d, so we may assume that $d \in \{1,5\}$. In these cases, we may set $(x,w) = (1,2)$ so that we need $5y^2 \in \{-3,-19\}$ and $5z^2 \in \{5,21\}$, both of which are possible.

We now move on to (b). We are given a triple (α,β,γ) which is in the image of δ_v for each place $v \neq 2$; we may as well represent (α,β,γ) as a triple of squarefree integers. We must show that $(\alpha,\beta,\gamma) \in \operatorname{im} \delta_2$.

1. Even though it is already given in the problem, we quickly explain that α is odd (modulo squares). Surely this is the case for $(\alpha,\beta,\gamma) \in \delta_2(E_d[2])$. Otherwise, we know α equals the x-coordinate of some $(x,y) \in E_d(\mathbb{Q}_2)$, meaning
$$y^2 = x\left(x^2 - d^2\right).$$
We now compute some valuations to show that $\nu_2(x)$ is even, which means α is odd.
   - There is nothing to do if $\nu_2(x) = 0$.
   - If $\nu_2(x) > 0$, then the valuations are $2\nu_2(y) = \nu_2(x)$, so $\nu_2(x)$ is even.
   - If $\nu_2(x) < 0$, then the valuations are $2\nu_2(y) = -3\nu_2(x)$, so $\nu_2(x)$ is still even.

2. We make some reductions. By Lemma C.8, we know that (α,β,γ) is unramified for $v \nmid 2d\infty$, so the prime factorizations of α, β, and γ are supported in the prime factors of $2d$.

   For our next few reductions, we note that multiplying any triple by the image of $\delta(E[2])$ will not change whether it is in the image of δ_2. For example, with α odd, we see that we may multiply by the triple $(d,2,2d)$ to force β to be odd, which in turn forces γ to be odd too. Multiplying by the triple $(-1,-d,d)$, we may assume that $\alpha \pmod 8$ is in $\{1,5\}$. Similarly, multiplying by the triple $(1,5,5)$, we may assume that $\beta \pmod 8$ is in $\{1,3\}$.

3. We complete the proof using Hilbert symbols. We know that the equations
$$\begin{cases} \alpha x^2 - \beta y^2 = -dw^2, \\ \alpha x^2 - \gamma z^2 = +dw^2 \end{cases}$$
has solutions in each $\mathbb{Q}_v$ for $v \neq 2$. Thus, $(-d\alpha, d\beta)_v = (d\alpha, -d\gamma)_v = (2d\beta, -2d\gamma)_v = 1$ for each $v \neq 2$, so Hilbert reciprocity[1] implies that
$$(-d\alpha, d\beta)_2 = (d\alpha, -d\gamma)_2 = (2d\beta, -2d\gamma)_2 = 1.$$
We now show that $(\alpha,\beta,\gamma) \in \operatorname{im} \delta_2$ directly. We may consider this triple up to $\mathbb{Q}_2^{\times 2}$, meaning that we may assume $\alpha \in \{1,5\}$ and $\beta \in \{1,3\}$. For example, because everything is odd and $\alpha \in \{1,5\}$, we see that $(\alpha,d)_2 = (\alpha,\beta)_2 = (\alpha,\gamma)_2 = 1$.[2] As such, $(-d\alpha, d\beta)_2 = (-d,\beta)_2$ and $(d\alpha,-d\gamma)_2 = (d,\beta)_2$, so $(-1,\beta)_2 = 1$. Thus, $\beta \neq 3$ is forced,[3] so $\gamma = 1$ follows. ∎

[1] In this case, it is possible to unwind the application of Hilbert reciprocity into merely applications of Quadratic reciprocity, but this language is convenient anyway.

[2] In particular, $(5,-)_2$ vanishes on odds. It is not hard to show $(5,-5)_2 = 1$ (because $5 \cdot 1^2 - 5 \cdot 1^2 = 0^2$), and $(5,-1)_2 = 1$ because $5 \cdot 1^2 - 1 \cdot 1^2 = 2^2$.

[3] We need to show that $(-1,3)_2 = -1$, which holds because $3x^2 - y^2 = z^2$ has no nontrivial solutions by $\pmod 8$ considerations.

C.5 A Selmer Calculation

We begin by recalling from class how to change the local condition one place at a time.

Lemma C.10. Fix a number field K and a finite self-dual Galois module M which is a vector space over $\mathbb{F}_p$. Let $\mathcal{L}$ be a self-dual local condition. Letting Σ be the singleton of a place v_0, we have

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

Proof. Recall the exact sequences

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

and

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

Global duality tells us that the images in the rightmost terms are orthogonal complements. 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

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

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

Lemma C.11. 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 $\mathrm{Sel}_{\mathcal{L}}(E[p]) \to \mathrm{H}^1(K_{v_0}; E[p])$ vanishes, then

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

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

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

Proof. All the hypotheses will be used, though much care will be required. Set $M \coloneqq E[p]$ and $\Sigma \coloneqq \{v_0\}$ 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

$$\begin{array}{ccc} \mathrm{Sel}_{\mathcal{L}_\Sigma}(M) & \longrightarrow & \mathrm{Sel}_{\mathcal{L}'}(M) \\ \downarrow & \lrcorner & \downarrow \\ \mathrm{Sel}_{\mathcal{L}}(M) & \longrightarrow & \mathrm{Sel}_{\mathcal{L}^\Sigma}(M) \end{array} \tag{C.1}$$

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

(a) The exactness of

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

implies that the inclusion $\mathrm{Sel}_{\mathcal{L}_\Sigma}(M) \to \mathrm{Sel}_{\mathcal{L}}(M)$ is an isomorphism. Thus, the left arrow of (C.1) is an isomorphism, so the right arrow is also an isomorphism, and the result follows from Lemma C.10.

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

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

of maps to 0 at the end, so the inclusion $\mathrm{Sel}_{\mathcal{L}}(M) \to \mathrm{Sel}_{\mathcal{L}^\Sigma}(M)$ is an isomorphism. Thus, the bottom arrow of (C.1) is an isomorphism, so the top arrow is also an isomorphism. The claim now follows from Lemma C.10. ■

Proposition C.12. Continue to consider the congruent number elliptic curve over $\mathbb{Q}$

$$E_d \colon y^2 = (x-d)(x+d)$$

where d is an odd integer. Let d be the product of an odd number of primes p_i such that all p_i are $5 \pmod 8$ and are mutually non-quadratic residues to each other. Show that

$$\dim_{\mathbb{F}_2} \mathrm{Sel}_2(E_d) = 3.$$

Proof. Fix $E \coloneqq E_d$ for brevity. We will show the stronger statement that

$$\mathrm{Sel}_2(E) \stackrel{?}{=} \mathrm{span}(E[2] \cup \{(1,d,d)\}).$$

The rank claim then follows because the triples $\{(-1,-d,d),(d,2,2d),(1,d,d)\}$ form a basis. For this, we induct on $\#S$, where $\#S = 1$ follows from results in class.

For the induction, suppose we have the statement for S and d, and we would like to show it for some set $S \cup \{\ell_1, \ell_2\}$ still satisfying the list of conditions; set $\ell \coloneqq \ell_1\ell_2$ for brevity. Accordingly, let E and E' be the projective closures of $y^2 = x(x-d)(x+d)$ and $y^2 = (x-d\ell)(x+d\ell)$. Let $\mathcal{L}$ and $\mathcal{L}'$ be the associated local conditions of $\mathrm{H}^1(\mathbb{A}_K; H)$, where $E[2]$ and $E'[2]$ are identified with the trace-zero hyperplane $H \subseteq \mu_2^{\oplus 3}$ as usual.

Quickly, let's compare our local conditions $\mathcal{L}$ and $\mathcal{L}'$, freely using Lemma C.8.

- For $v \nmid 2d\ell\infty$, we see that $\mathcal{L}_v$ and $\mathcal{L}'_v$ both contain the unramified triples.
- For $v = \infty$, both are the same.
- For finite $v = p$ with $p \mid d$, we claim that $\mathcal{L}_v = \mathcal{L}'_v$. Well, the sizes are the same, so it is enough to just get an inclusion, so it is enough to check $\{(-1,-d\ell,d\ell),(d\ell,2,2d\ell)\} \subseteq \mathcal{L}_p$, which is equivalent to having $\{(1,\ell,\ell),(\ell,1,\ell)\} \subseteq \mathcal{L}_p$. But this is true because $\ell = \ell_1\ell_2$ is a square in $\mathbb{Q}_p^\times$.
- For $v = 2$, it is once again enough to achieve the inclusion $\{(1,\ell,\ell),(\ell,1,\ell)\} \subseteq \mathcal{L}_2$. This is true because $\ell \equiv 1 \pmod 8$, so $\ell \in \mathbb{Q}_2^{\times 2}$.
- Lastly, for $v \in \{\ell_1, \ell_2\}$, we see that $\mathcal{L}_v$ contains unramified triples, but the only unramified triple in $\mathcal{L}'_v$ is the trivial one, so $\mathcal{L}_v \cap \mathcal{L}'_v$ is trivial.

Thus, we see that we are going to use Lemma C.11 twice. Accordingly, let $\mathcal{L}''$ be an "intermediate" local condition given by

$$\mathcal{L}''_v \coloneqq \begin{cases} \mathcal{L}_v & \text{if } v \neq \ell_1, \\ \mathcal{L}'_v & \text{if } v = \ell_1. \end{cases}$$

Thus, $\mathcal{L}$ and $\mathcal{L}''$ differ only at the place $v = \ell_1$, and $\mathcal{L}''$ and $\mathcal{L}'$ differ only at the place $v = \ell_2$. We now have two steps.

1. We claim that $\mathrm{Sel}_{\mathcal{L}''}(H) = \{(1,1,1),(-1,-1,1)\}$. One inclusion is not so bad: certainly $(1,1,1) \in \mathrm{Sel}_{\mathcal{L}''}(H)$. Additionally, $(1,-1,-1) \in \mathrm{Sel}_{\mathcal{L}''}(H)$ because it is already in $\mathcal{L}_v$ for all v, and $(1,-1,-1) \in \mathcal{L}_{\ell_1}$ because $(-1,-1,1)$ equals $(1,1,1)$ up to squares in $\mathbb{Q}_{\ell_1}^\times$.

For the other inclusion, it is enough to check that

$$\dim_{\mathbb{F}_2} \mathrm{Sel}_{\mathcal{L}''}(H) = \mathrm{Sel}_{\mathcal{L}}(H) - 2.$$

For this, we use Lemma C.11(b) at the place $v_0 = \ell_1$. The hypotheses on the local conditions were checked above, so it remains to check that the map $\mathrm{Sel}_{\mathcal{L}}(H) \to \mathcal{L}_{\ell_1}$ is surjective. This holds by the calculation of Lemma C.8 by using the global triples coming from $E[2]$.

2. We claim that $\mathrm{Sel}_{\mathcal{L}'}(H) = \mathrm{span}(E'[2] \cup \{(1, d\ell, d\ell)\}$, which will complete the proof. Again, one inclusion is not so bad: certainly $E'[2]$ provides elements of the Selmer group. Additionally, we once again see that $(1, d\ell, d\ell) \in \mathrm{Sel}_{\mathcal{L}'}(H)$ by checking place-by-place: along with the checks from the previous step, we merely have to check that $(1, d\ell, d\ell) \in \mathcal{L}'_{\ell_2}$, which is true because this triple is equivalent to $(-1, -d\ell, d\ell)$ up to squares.

   For the other inclusion, we will again use ranks, noting that it is enough to check that

$$\dim_{\mathbb{F}_2} \mathrm{Sel}_{\mathcal{L}'}(H) = \mathrm{Sel}_{\mathcal{L}''}(H) + 2,$$

   which will follow from Lemma C.11(b) at the place $v_0 = \ell_2$. Again, the hypotheses on the local conditions are satisfied, so it remains to check that the map $\mathrm{Sel}_{\mathcal{L}''}(H) \to \mathcal{L}''_{\ell_2}$ is trivial. Well, from the calculation in the previous step, we know that $\mathrm{Sel}_{\mathcal{L}''}(H) = \{(1,1,1), (-1,-1,1)\}$, and both of these elements are trivial up to squares in $\mathbb{Q}^\times_{\ell_2}$. ■

BIBLIOGRAPHY

[Mat70] Ju. V. Matijasevič. "The Diophantineness of enumerable sets". In: *Dokl. Akad. Nauk SSSR* 191 (1970), pp. 279–282. ISSN: 0002-3264.

[Zar74] Yu. G. Zarkhin. "Noncommutative cohomologies and Mumford groups". In: *Mathematical notes of the Academy of Sciences of the USSR* 15.3 (1974), pp. 241–244. DOI: 10.1007/BF01438377. URL: https://doi.org/10.1007/BF01438377.

[DL78] J. Denef and L. Lipshitz. "Diophantine sets over some rings of algebraic integers". In: *J. London Math. Soc. (2)* 18.3 (1978), pp. 385–391. ISSN: 0024-6107. DOI: 10.1112/jlms/s2-18.3.385. URL: https://doi.org/10.1112/jlms/s2-18.3.385.

[Den80] J. Denef. "Diophantine sets over algebraic integer rings. II". In: *Trans. Amer. Math. Soc.* 257.1 (1980), pp. 227–236. ISSN: 0002-9947. DOI: 10.2307/1998133. URL: https://doi.org/10.2307/1998133.

[Gro91] Benedict H. Gross. "Kolyvagin's work on modular elliptic curves". In: *L-functions and arithmetic (Durham, 1989)*. Vol. 153. London Math. Soc. Lecture Note Ser. Cambridge Univ. Press, Cambridge, 1991, pp. 235–256. DOI: 10.1017/CBO9780511526053.009. URL: https://doi.org/10.1017/CBO9780511526053.009.

[Knu91] Max-Albert Knus. *Quadratic and Hermitian forms over rings*. Vol. 294. Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]. With a foreword by I. Bertuccioni. Springer-Verlag, Berlin, 1991, pp. xii+524. ISBN: 3-540-52117-8. DOI: 10.1007/978-3-642-75401-2. URL: https://doi.org/10.1007/978-3-642-75401-2.

[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.

[Tat01] John Tate. "Galois cohomology". In: *Arithmetic algebraic geometry (Park City, UT, 1999)*. Vol. 9. IAS/Park City Math. Ser. Amer. Math. Soc., Providence, RI, 2001, pp. 465–479. DOI: 10.1090/pcms/009/07. URL: https://doi.org/10.1090/pcms/009/07.

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

[Shl08] Alexandra Shlapentokh. "Elliptic curves retaining their rank in finite extensions and Hilbert's tenth problem for rings of algebraic numbers". In: *Trans. Amer. Math. Soc.* 360.7 (2008), pp. 3541–3555. ISSN: 0002-9947. DOI: 10.1090/S0002-9947-08-04302-X. URL: https://doi.org/10.1090/S0002-9947-08-04302-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.

[GS13] Marvin J Greenberg and Jean-Pierre Serre. *Local Fields*. eng. Vol. 67. Graduate Texts in Mathematics. Springer, 2013. ISBN: 9780387904245.

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

[Mil20] J.S. Milne. *Class Field Theory (v4.03)*. Available at www.jmilne.org/math/. 2020.

[KP25] Peter Koymans and Carlo Pagano. *Hilbert's tenth problem via additive combinatorics*. 2025. URL: https://arxiv.org/abs/2412.01768.

List of Definitions