

THEME 1

HOMEWORK 1

The homework problems have been recorded as propositions.

1.1 The Cohomology of $\widehat{\mathbb{Z}}$

We begin by recalling the cohomology of cyclic groups.

Lemma 1.1. Fix a finite cyclic group G generated by σ . Then for any G -module M and index $i > 0$, we have

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

In particular, $\{H^i(G; M)\}_{i>0}$ 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 $\mathbb{Z}[G] \rightarrow \mathbb{Z}$ has kernel generated by $(\sigma - 1)$, so we can surject onto its kernel via the map $(\sigma - 1): \mathbb{Z}[G] \rightarrow \mathbb{Z}[G]$. 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 $N_G: \mathbb{Z}[G] \rightarrow \mathbb{Z}[G]$, where $N_G(x) := \sum_{g \in G} gx$; equivalently, we can view N_G as multiplication by the norm element $N_G := \sum_{g \in G} g$. 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

$$\cdots \xrightarrow{(\sigma-1)} \mathbb{Z}[G] \xrightarrow{N_G} \mathbb{Z}[G] \xrightarrow{(\sigma-1)} \mathbb{Z}[G] \xrightarrow{\deg} \mathbb{Z} \rightarrow 0.$$

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

$$0 \rightarrow M \xrightarrow{\sigma-1} M \xrightarrow{N_G} M \xrightarrow{\sigma-1} M \rightarrow \cdots,$$

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

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

as desired. ■

It is worthwhile to explain the functoriality properties of Lemma 1.1, which are rather bizarre.

Lemma 1.2. Fix a surjection $G' \rightarrow G$ of cyclic groups. Then given a morphism $f: M \rightarrow M'$ where M is a G -module, and M' has the induced G' -module structure, the induced map

$$f: H^i(G; M) \rightarrow H^i(G'; M')$$

is $(\#G'/\#G)^{[i/2]} f$ once these groups have been identified with subquotients of M and M' via Lemma 1.1.

Proof. Denote the surjection $G' \rightarrow G$ 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 $g(N_{G'}) = m N_G$ produce the morphism

$$\begin{array}{ccccccccccc} \cdots & \longrightarrow & \mathbb{Z}[G'] & \xrightarrow{N_{G'}} & \mathbb{Z}[G'] & \xrightarrow{(\sigma'-1)} & \mathbb{Z}[G'] & \xrightarrow{N_{G'}} & \mathbb{Z}[G'] & \xrightarrow{(\sigma'-1)} & \mathbb{Z}[G'] & \xrightarrow{\deg} & \mathbb{Z} & \longrightarrow & 0 \\ & & \downarrow m^2 g & & \downarrow m g & & \downarrow m g & & \downarrow g & & \downarrow g & & \parallel & & \\ \cdots & \longrightarrow & \mathbb{Z}[G] & \xrightarrow{N_G} & \mathbb{Z}[G] & \xrightarrow{(\sigma-1)} & \mathbb{Z}[G] & \xrightarrow{N_G} & \mathbb{Z}[G] & \xrightarrow{(\sigma-1)} & \mathbb{Z}[G] & \xrightarrow{\deg} & \mathbb{Z} & \longrightarrow & 0 \end{array}$$

of chain complexes. Now, given a morphism $f: M \rightarrow M'$ where M is a G -module, and M' has the induced G' -module structure, we may apply $\text{Hom}_G(-, M)$ and $\text{Hom}_{G'}(-, M')$ to get another morphism of chain complexes

$$\begin{array}{ccccccccccc} 0 & \longrightarrow & M & \xrightarrow{(\sigma-1)} & M & \xrightarrow{N_G} & M & \xrightarrow{(\sigma-1)} & M & \xrightarrow{N_G} & M & \longrightarrow & \cdots \\ & & \downarrow f & & \downarrow f & & \downarrow m f & & \downarrow m f & & \downarrow m^2 f & & \\ 0 & \longrightarrow & M' & \xrightarrow{(\sigma'-1)} & M' & \xrightarrow{N_{G'}} & M' & \xrightarrow{(\sigma'-1)} & M' & \xrightarrow{N_{G'}} & M' & \longrightarrow & \cdots \end{array}$$

induced by f and the above morphism. Taking cohomology, it follows that the induced map $H^i(G; M) \rightarrow H^i(G'; M')$ is given by $m^{[i/2]} f$ by a computation on the corresponding cocycles. ■

Proposition 1.3. 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 every $m \in M$ 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 :

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

- (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 $H^1(\mathfrak{g}; M) = M'/(\sigma - 1)M$. In particular, if M is torsion, we have $H^1(\mathfrak{g}; M) = M/(\sigma - 1)M$.
- (b) If M is divisible (i.e., the multiplication-by- n map is surjective for all $n \geq 1$) or finite torsion, then $H^2(\mathfrak{g}; M) = 0$.
- (c) Show that $H^i(\mathfrak{g}; \mathbb{Q}) = 0$ 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 $H^i(\mathfrak{g}; M) = 0$ for $i > 1$, and there exists M such that $H^1(\mathfrak{g}; M) \neq 0$.
- (e) Show that for any discrete \mathfrak{g} -module M , we have $H^i(\mathfrak{g}; M) = 0$ 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 $H_m := \langle \sigma^m \rangle$ for brevity, which we note is the kernel of the map $\mathfrak{g} \rightarrow \mathbb{Z}/m\mathbb{Z}$ 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 $\mathfrak{g} \rightarrow A$ 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

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

where $M^{\sigma^m} = \overline{M^{\langle \sigma^m \rangle}}$ by continuity. Because \mathfrak{g}/H_m is cyclic, Lemma 1.1 tells us that $i > 0$ has

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

We now see that we have to use Lemma 1.2 to compute the internal maps: the map between the m th 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 $\ker N_{\mathfrak{g}/H_m} \rightarrow M'$ induce an isomorphism

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

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 $1 + \sigma + \dots + \sigma^{m-1}$. But then $(\sigma^m - 1)a = 0$ as well, so $a \in \ker N_{\mathfrak{g}/H_m}$.
- Injective: suppose a class a coming from $\ker N_{\mathfrak{g}/H_m} / (1 - \sigma) M^{\sigma^m}$ in the colimit goes to 0 in $M' / (1 - \sigma) M$. In particular, we are given that a is annihilated by some $1 + \sigma + \dots + \sigma^{m-1}$ 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,

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

vanishes for some n because a is torsion.

- (b) We handle torsion and divisibility separately.

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

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

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

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

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

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

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

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

It remains to actually find a finite \mathfrak{g} -module M with nonzero $H^1(\mathfrak{g}; M)$. Well, give some finite abelian group A the trivial action. Then $A' = A$ and $(\sigma - 1)A = 0$, so $H^1(\mathfrak{g}; A) = A$, 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 $H^i(\mathfrak{g}; M) = 0$ when i is odd and $i \geq 3$. Write $i = 2j + 1$ for $j \geq 1$ so that $\lfloor i/2 \rfloor = j$. Then

$$H^i(\mathfrak{g}; M) = \operatorname{colim}_{m \geq 1} \frac{\ker N_{\mathfrak{g}/H_m}}{(1 - \sigma)M^{\sigma^m}},$$

and the transition maps are given by multiplication by $(m'/m)^j$. It is enough to show that any class $a \in \ker N_{\mathfrak{g}/H_m}$ vanishes in the colimit. Well, $mH^1(\mathfrak{g}/H_m; M^{\sigma^m}) = 0$, 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

$$\frac{\ker N_{\mathfrak{g}/H_m}}{(1 - \sigma)M^{\sigma^m}} \xrightarrow{m^j} \frac{\ker N_{\mathfrak{g}/H_{m^2}}}{(1 - \sigma)M^{\sigma^{m^2}}}$$

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

- We show $H^i(\mathfrak{g}; M) = 0$ when i is even and $i \geq 4$. Write $i = 2j$ for $j \geq 2$ so that $\lfloor i/2 \rfloor = j$. Then

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

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 $mH^2(\mathfrak{g}/H_m; M^{\sigma^m}) = 0$ implies that $ma = N_{\mathfrak{g}/H_m}(b)$ for some $b \in M^{\sigma^m}$. Then $N_{\mathfrak{g}/H_{m^2}}(b) = N_{\mathfrak{g}/H_m} N_{\mathfrak{g}/H_m}(b) = kma$, so a vanishes along the transition map

$$\frac{M^{\mathfrak{g}}}{N_{\mathfrak{g}/H_m}(M^{\sigma^m})} \rightarrow \frac{M^{\mathfrak{g}}}{N_{\mathfrak{g}/H_{m^2}}(M^{\sigma^{m^2}})}$$

because $m^j a = m^{j-2} N_{\mathfrak{g}/H_{m^2}}(b)$. ■

1.2 Local Cohomology

Proposition 1.4. In this question, K is a finite extension of \mathbb{Q}_p , $\Gamma_K := \text{Gal}(\overline{K}/K)$, M is a finite Γ_K -module, and we set $H^i(M) := H^i(K; M) = H^i(\Gamma_K; M)$. Then local Tate duality asserts that the cup product induces a perfect pairing between two finite abelian groups

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

where $M^* := \text{Hom}(M, \mu_\infty)$ 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 $h^i := \#H^i(M)$. Then we have a formula

$$\chi(M) = \frac{1}{\#(\mathcal{O}_K/n\mathcal{O}_K)},$$

where $n := \#M$.

- 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 ?
- 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

$$\dim_{\mathbb{F}_\ell} E(K)/\ell E(K) = \frac{1}{2} \dim_{\mathbb{F}_\ell} H^1(K; E[\ell]).$$

What are the possible values of $\dim_{\mathbb{F}_\ell} E(K)/\ell E(K)$ if $K = \mathbb{Q}_p$?

Proof of Proposition 1.4(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

$$0 \rightarrow \mu_\ell \rightarrow \mathbb{G}_m \xrightarrow{\ell} \mathbb{G}_m \rightarrow 0$$

and Hilbert's theorem 90, we conclude that the boundary map $K^\times/K^{\times \ell} \rightarrow H^1(K; \mu_\ell)$ is an isomorphism. Thus, we may focus on computing the size of $H^1(K; \mu_\ell)$, 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 $H^0(K; \mu_\ell) = \mu_\ell(K)$.
- 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 $\mu_\ell^* = \text{Hom}(\mu_\ell, \mu_\infty)$. Any map $\mu_\ell \rightarrow \mu_\infty$ factors through $\mu_\infty[\ell] = \mu_\ell$, so $\mu_\ell^* = \text{Hom}(\mu_\ell, \mu_\ell)$. Now, a map $\mu_\ell \rightarrow \mu_\ell$ must be of the form $\zeta \mapsto \zeta^k$ for some integer k , so there is a surjection $\mathbb{Z} \rightarrow \mu_\ell^*$ with kernel $\ell\mathbb{Z}$. The induced map $\mathbb{Z}/\ell\mathbb{Z} \rightarrow \mu_\ell^*$ is also Galois-invariant because all the given homomorphisms $\mu_\ell \rightarrow \mu_\ell$ 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

$$\#(K^\times/K^{\times\ell}) = \#\mu_\ell(K) \cdot \ell \cdot \ell^{[K:\mathbb{Q}_p] \cdot 1_{v|\ell}}.$$

For example,

$$\#(K^\times/K^{\times 2}) = \begin{cases} 4 & \text{if } v \nmid 2, \\ 4 \cdot 2^{[K:\mathbb{Q}_2]} & \text{if } v \mid 2. \end{cases}$$

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 1.5. 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

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

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 $G_E(\mathfrak{m}_v^i)/G_E(\mathfrak{m}_v^{i+1})$ 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 $\mathbb{P}^2(K_v) \rightarrow \mathbb{P}^2(\mathbb{F}_v)$ 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 1.4(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 $E[\ell] \rightarrow E[\ell]^*$. This follows from the fact that the Weil pairing $E[\ell] \times E[\ell] \rightarrow \mu_\ell$ is non-degenerate and Galois-invariant.

We will calculate both sides of the required equality

$$\dim_{\mathbb{F}_\ell} E(K)/\ell E(K) \stackrel{?}{=} \frac{1}{2} \dim_{\mathbb{F}_\ell} H^1(K; E[\ell])$$

separately.

- We compute $\dim_{\mathbb{F}_\ell} E(K)/\ell E(K)$, using Lemma 1.5, which grants us an exact sequence

$$0 \rightarrow \mathcal{O}_v \rightarrow E(K) \rightarrow C \rightarrow 0,$$

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

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

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 $\ell: C \rightarrow C$ 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 $\dim_{\mathbb{F}_\ell} H^1(K; E[\ell])$, using the Euler characteristic. Indeed, by plugging everything in, we see that

$$h^1(E[\ell]) = h^0(E[\ell])h^2(E[\ell]) \cdot \#(\mathcal{O}_K/\ell^2 \mathcal{O}_K).$$

(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

$$h^1(E[\ell]) = \#E(K)[\ell]^2 \cdot \#(\mathcal{O}_K/\ell^2 \mathcal{O}_K).$$

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

$$\dim_{\mathbb{F}_\ell} H^1(K; E[\ell]) = 2 \dim_{\mathbb{F}_\ell} E(K)[\ell] + \begin{cases} 0 & \text{if } v \nmid \ell, \\ 2[K:\mathbb{Q}_\ell] & \text{if } v \mid \ell. \end{cases}$$

The equality

$$\dim_{\mathbb{F}_\ell} E(K)/\ell E(K) = \frac{1}{2} \dim_{\mathbb{F}_\ell} H^1(K; E[\ell])$$

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 1.6. In the notes, we show the stronger statement that $H^1(K; E[m])$ 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!

1.3 The “Counterexample” to Grunwald–Wang

Proposition 1.7.

- (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

$$H^1(K; \mu_8) \rightarrow \prod_v H^1(K_v; \mu_8)$$

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

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

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 $\{\sqrt{2}, \sqrt{-2}, i\} \cap \mathbb{Q}_p \neq \emptyset$ 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

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

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 $K := \mathbb{Q}(\sqrt{7})$ 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 $(\bmod 4)$), so there is only one place $\mathbb{Q}_2(\sqrt{7})$ above 2. It remains to show that 16 is an eighth power

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

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

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 $H^1(K; \mu_8)$ with $K^\times / K^{\times 8}$ (by the boundary map of the Kummer exact sequence for $\mathbb{G}_{m,K}$), so the map

$$H^1(\mathbb{Q}(\sqrt{7}); \mu_8) \rightarrow \prod_v H^1(K_v; \mu_8)$$

fails to be injective because the nontrivial class $16 \in K^\times / K^{\times 8}$ vanishes in all localizations. ■

1.4 Congruent Number Elliptic Curves at 2

Consider the congruent number elliptic curve over \mathbb{Q} given on affine coordinates by

$$E_d: y^2 = x(x-d)(x+d).$$

The local condition at a place v can be described using the map

$$\begin{aligned} E_d(K_v) &\rightarrow \{(\alpha, \beta, \gamma) \in (K_v^\times / K_v^{\times 2})^{\oplus 3} : \alpha\beta\gamma = 1\} \\ (x, y) &\mapsto (x, x-d, x+d) \end{aligned}$$

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 1.8. Fix everything as above. We compute information about image of $\delta_v: E_d(\mathbb{Q}_v)/2E_d(\mathbb{Q}_v) \rightarrow H^1(\mathbb{Q}_v; H)$ 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

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

- (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 $H_{\text{ur}}^1(\mathbb{Q}_v; H)$. 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 1.4(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 1.4(a) again. ■

Proposition 1.9. 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,

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

which also equals $\dim_{\mathbb{F}_2} \text{im } \delta_v$ by Proposition 1.4(a). Thus, it suffices to show that $\text{span}(S \cup \{1, 5, 5\}) \subseteq \text{im } \delta_v$.

2. By Lemma 1.8, it is enough to check that $(1, 5, 5) \in \text{im } \delta_v$. 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 $(\alpha, \beta, \gamma) \in \text{im } \delta_2$.

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 $(\alpha, \beta, \gamma) \notin \delta_2(E_d[2])$. Otherwise, we know α equals the x -coordinate of some $(x, y) \in E_d(\mathbb{Q}_2)$, meaning

$$y^2 = x(x^2 - d^2).$$

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 1.8, 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 reciprocity¹ implies that

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

We now show that $(\alpha, \beta, \gamma) \in \text{im } \delta_2$ 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 $(\text{mod } 8)$ considerations.

1.5 A Selmer Calculation

We begin by recalling from class how to change the local condition one place at a time.

Lemma 1.10. 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

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

Proof. Recall the exact sequences

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

and

$$0 \rightarrow \text{Sel}_{(\mathcal{L}^*)_\Sigma}(M^*) \rightarrow \text{Sel}_{(\mathcal{L}^*)}(M^*) \rightarrow H^1(K_{v_0}; M^*).$$

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

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

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

Lemma 1.11. 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 $\mathcal{L}'_{v_0} \subseteq H^1(K_{v_0}; E[p])$ 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 $\text{Sel}_{\mathcal{L}}(E[p]) \rightarrow H^1(K_{v_0}; E[p])$ vanishes, then

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

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

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

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

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

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

(a) The exactness of

$$0 \rightarrow \text{Sel}_{\mathcal{L}_\Sigma}(M) \rightarrow \text{Sel}_{\mathcal{L}}(M) \rightarrow \mathcal{L}_\ell$$

implies that the inclusion $\text{Sel}_{\mathcal{L}_\Sigma}(M) \rightarrow \text{Sel}_{\mathcal{L}}(M)$ 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 1.10.

(b) We are given that $\text{Sel}_{\mathcal{L}}(M) \rightarrow \mathcal{L}_{\ell}$ is surjective, so the exact sequence

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

of maps to 0 at the end, so the inclusion $\text{Sel}_{\mathcal{L}}(M) \rightarrow \text{Sel}_{\mathcal{L}^{\Sigma}}(M)$ is an isomorphism. Thus, the bottom arrow of (1.1) is an isomorphism, so the top arrow is also an isomorphism. The claim now follows from Lemma 1.10. ■

Proposition 1.12. Continue to consider the congruent number elliptic curve over \mathbb{Q}

$$E_d: y^2 = (x - d)(x + d)$$

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 (mod 8) and are mutually non-quadratic residues to each other. Show that

$$\dim_{\mathbb{F}_2} \text{Sel}_2(E_d) = 3.$$

Proof. Fix $E := E_d$ for brevity. We will show the stronger statement that

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

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 $\ell := \ell_1 \ell_2$ 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 $H^1(\mathbb{A}_K; H)$, 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 1.8.

- 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 1.11 twice. Accordingly, let \mathcal{L}'' be an "intermediate" local condition given by

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

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 $\text{Sel}_{\mathcal{L}''}(H) = \{(1, 1, 1), (-1, -1, 1)\}$. One inclusion is not so bad: certainly $(1, 1, 1) \in \text{Sel}_{\mathcal{L}''}(H)$. Additionally, $(1, -1, -1) \in \text{Sel}_{\mathcal{L}''}(H)$ 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

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

For this, we use Lemma 1.11(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 $\text{Sel}_{\mathcal{L}}(H) \rightarrow \mathcal{L}_{\ell_1}$ is surjective. This holds by the calculation of Lemma 1.8 by using the global triples coming from $E[2]$.

2. We claim that $\text{Sel}_{\mathcal{L}'}(H) = \text{span}(E'[2] \cup \{(1, d\ell, d\ell)\})$, 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 $(1, d\ell, d\ell) \in \text{Sel}_{\mathcal{L}'}(H)$ 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

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

which will follow from Lemma 1.11(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 $\text{Sel}_{\mathcal{L}''}(H) \rightarrow \mathcal{L}''_{\ell_2}$ is trivial. Well, from the calculation in the previous step, we know that $\text{Sel}_{\mathcal{L}''}(H) = \{(1, 1, 1), (-1, -1, 1)\}$, and both of these elements are trivial up to squares in $\mathbb{Q}_{\ell_2}^\times$. ■