254B: Rational Points on Varieties

Nir Elber

Spring 2023

Contents

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

—Neal Shusterman, [Shu16]

Theme 1
Quadratic Forms

I guess I'll start with math.

—Martin Olsson

1.1 January 18

Here we go.

1.1.1 House-Keeping

This is a second semester of algebraic number theory, but we are not really learning algebraic number theory. Instead, we will focus on rational points on varieties. Some notes.

- There is a bCourses, which has the syllabus.
- Ideally, we will require a graduate-level first course in algebraic number theory. Notably, we will not assume class field theory. We will also require algebraic geometry, at the level of chapter II of [Har77]. Roughly speaking, the first half of the course will focus on algebraic number theory, and the second half will certainly use scheme theory.

  It might be helpful to know about cohomology in advance. We will need group cohomology to begin and more general derived functors later.
- Homework will be assigned about every two weeks. Don't stress too much about it. However, there will be no homework drops.
- There will be a term paper, about 10 pages. The idea is to pick a topic you like and then talk about it.
- Grades will be fine as long as you don't completely vanish.
- If you are sick, do not come to class.

1.1.2 Course Overview

Here are the topics for the class.

Quadratic Forms

We will begin with quadratic forms, which are essentially genus-0 curves. Explicitly, we are asking the following question.

Question 1.1. Fix a field K and a quadratic form $Q \in K[x_0, \dots, x_n]$, which is a homogeneous polynomial of degree 2; we are interested if Q has nontrivial zeroes. In other words, we want to know if the projective variety $V(Q) \subseteq \mathbb{P}^n_K$ has a K-point.

Example 1.2. Set $K = \mathbb{Q}$ and $Q = x_0^2 + x_1^2 + x_2^2$. Then Q has no nontrivial zeroes. Indeed, it has no nontrivial zeroes over $\mathbb{R}$, and $\mathbb{Q} \subseteq \mathbb{R}$.

Remark 1.3. We are describing these quadratic forms as "genus-0 curves" because the variety $V(Q)$ is isomorphic to $\mathbb{P}^1_{\overline{K}}$ over $\overline{K}$.

We will approach Question 1.1 from the perspective of the local-to-global principle. Indeed, we will show the following.

Theorem 1.4. Let Q be a quadratic form over a number field K. Then $V(Q)$ has a K-point if and only if $V(Q)$ has a K_v point for all places v of K.

The above result Theorem 1.4 is very special to quadratic forms, and the analogous statement fails for, say, elliptic curves.

The reason we are interested in quadratic forms is that these computations lead naturally to class field theory.

Example 1.5. Fix a number field K, and let $Q = x_0^2 - ax_1^2$ be a quadratic form, where $a \in K^\times$. Roughly speaking, Theorem 1.4 now asserts that $a \in K$ is a square if and only if a is a square in each localization K_v, which is tied to the Hasse norm theorem.

Here are some references.

- Serre's [Ser12] is good, though Serre avoids class field theory by focusing on $K = \mathbb{Q}$. We will not want to avoid these ideas, however, because we want to see a need for cohomology.
- Milne's [Mil20] is good, though we will of course not do all of it.
- Lam also has a book [Lam05] on quadratic forms.

References for this portion of the course include

Elliptic Curves

After discussing genus-0 curves, we will say something about elliptic curves. The goal is to prove the following result, which is the Mordell–Weil theorem.

Theorem 1.6. Let E be an elliptic curve over a number field K. Then $E(K)$ is a finitely generated abelian group.

Here are some references.

- Silverman's [Sil09] is the standard resource, but it avoids algebraic geometry.

We might also spend a lecture saying words about higher-dimensional abelian varieties, but it is a lot harder.

Brauer–Manin Obstructions

These refer to special obstructions to the local-to-global principle, as seen in Theorem 1.4. Poonen has a reasonable text on this. All of this is already potentially too much, so we will stop here.

1.1.3 Quadratic Forms

Let's do some math. For most of our discussion here, we fix K to be a field with $\operatorname{char} K \neq 2$.

Definition 1.7 (quadratic form)**.** Fix a field K with $\operatorname{char} K \neq 2$. Then a *quadratic form* Q on a finite-dimensional K-vector space V is a map $Q\colon V \to K$ satisfying the following conditions.

- Quadratic: $Q(av) = a^2 Q(v)$ for all $a \in K$ and $v \in V$.
- Bilinear: the function $B\colon V^2 \to K$ defined by $B(v,w) \coloneqq \frac{1}{2}(Q(v+w) - Q(v) - Q(w))$ is K-bilinear. Note B is symmetric automatically.

Remark 1.8. One can view the quadratic form Q as cutting out a projective variety in $\mathbb{P}V$.

Remark 1.9. Given a quadratic form Q on V giving the bilinear form B, we note

$$B(v,v) = \frac{1}{2}(Q(2v) - 2Q(v)) = Q(v),$$

so we can recover the quadratic form from the bilinear form. This establishes a bijection between quadratic forms and bilinear forms.

We now associate a special symmetric matrix B^* to a bilinear form $B\colon V \times V \to K$. A bilinear form $B\colon V^2 \to K$ gives a map $B\colon V \otimes_K V \to K$, which gives a map $B^*\colon V \to V^\vee$ by the tensor–hom adjunction. (Explicitly, $B^*\colon v \mapsto B(v,\cdot)$.) Giving V a basis $\{e_i\}_{i=1}^n$ and $V^\vee$ the dual basis $\{e_i^\vee\}_{i=1}^n$, we may represent B^* as the matrix $A = (a_{ij})_{1 \le i,j \le n}$. Explicitly, we see

$$B(e_i,\cdot) = B^*(e_i) = \sum_{j=1}^n a_{ij} e_j^\vee,$$

so $B(e_i,e_j) = a_{ij} = e_i^\intercal B^* e_j$. As such, we see that $a_{ij} = a_{ji}$ because B is symmetric, so B^* is symmetric.

More generally, for vectors $v = \sum_i x_i e_i$ and $w = \sum_j y_j e_j$, we see

$$B(v,w) = \sum_{i=1}^n \sum_{j=1}^n x_i y_j B(e_i,e_j) = \sum_{i=1}^n \sum_{j=1}^n (x_i e_i^\intercal) B^*(y_j e_j) = v^\intercal B^* w,$$

and so

$$Q(v) = B(v,v) = v^\intercal B^* v = \sum_{i=1}^n \sum_{j=1}^n a_{ij} x_i x_j.$$

This justifies us viewing Q as being a homogeneous polynomial of degree 2.

Definition 1.10 (non-degenerate)**.** A quadratic form Q on a finite-dimensional K-vector space V is *non-degenerate* if and only if the induced bilinear form $B\colon V \otimes_K V \to K$ induces an isomorphism $B^*\colon V \to V^\vee$.

Remark 1.11. Because $\dim V = \dim V^\vee$, we see Q is non-degenerate if and only if $B^*\colon V \to V^\vee$ is injective, which is equivalent to asserting $B(v,\cdot)\colon V \to K$ is the zero map if and only if $v = 0$.

Given our quadratic form Q on K, we note there is a map

$$\bigwedge^n V \xrightarrow{\det B^*} \bigwedge^n V^\vee = \left(\bigwedge^n V\right)^\vee$$

of 1-dimensional K-vector spaces, where $n = \dim V$. Equivalently, we get a map

$$\left(\bigwedge^n V\right)^{\otimes 2} \to K,$$

which is still of 1-dimensional vector spaces and is essentially given by B^*. This morphism produces an element of K, but we can visually see that adjusting the basis of V adjusts this constant by a square in K.

More directly, letting $\{e_i'\}_{i=1}^n$ be a new basis of V, we can compute the new matrix by computing $B(e_i', e_j')$. Let $e_i' = \sum_{k=1}^n s_{ik} e_k$ so that $S = (s_{ij})_{1 \le i,j \le n}$ is the change-of-basis matrix. Then

$$B(e_i', e_j') = \sum_{k=1}^n \sum_{\ell=1}^n s_{ik} s_{j\ell} B(e_i, e_j) = \sum_{k=1}^n \sum_{\ell=1}^n s_{ik} a_{ij} s_{j\ell} = (S^\intercal A S)_{ij},$$

so $S^\intercal A S$ is our new matrix, meaning we have adjusted or determinant by the square $(\det S)^2$.

So here is our definition.

Definition 1.12 (discriminant)**.** Fix a quadratic form Q on a finite-dimensional K-vector space. Then the *discriminant* is $\det B^* \in K/\left(K^{\times 2}\right)$, where $B^* \colon V \to V^\vee$ is the associated linear transformation. Note that Q is non-degenerate if and only if $\operatorname{disc} Q \neq \{0\}$.

The goal of this part of the course is the following result, which we will write down more precisely.

Theorem 1.13 (Hasse–Minkowski)**.** Let K be a number field, and let Q be a quadratic form on the K-vector space V. Then Q has a nontrivial zero in V if and only if Q has a nontrivial zero in $V \otimes_K K_v$ for all places v of K.

We are going to black-box a few cohomological tools in the course of proving Theorem 1.13. Later we will go back and prove them.

1.2 January 20

We continue. Today we move towards a proof of Theorem 1.13.

1.2.1 Orthogonal Basis

We established a lot of notation last class, so we pick up the following notation.

Definition 1.14 (quadratic space)**.** Fix a field K of characteristic not 2. Then a *quadratic space* is a triple (V, Q, B), where Q is a quadratic form on the finite-dimensional K-vector space V, and B is the corresponding bilinear form. We say that the space (V, Q, B) is *non-degenerate* if Q is.

Bilinear forms tend to behave with special bases.

Definition 1.15 (orthogonal)**.** Fix a field K and a quadratic space (V, Q, B). Then v and w are *orthogonal* if and only if $B(v, w) = 0$.

Here's why we care.

Lemma 1.16. Fix a field K of characteristic not 2. Then a quadratic space (V, Q, B) admits a basis of orthogonal vectors.

Proof. We induct on $\dim V$. If $Q = 0$ (for example, if $\dim V = 0$), then $B(v, w) = \frac{1}{2}(Q(v+w) - Q(v) - Q(w)) = 0$ for all $v, w \in V$, so any basis will work.

Otherwise, $Q \neq 0$. It follows that $Q(e_1) \neq 0$ for some fixed $e_1 \in V$. To induct downwards, we let H denote the kernel of the map $B(e_1, \cdot) \colon V \to K$, which is surjective because $B(e_1, e_1) \neq 0$. As such, we can decompose

$$V \stackrel{?}{=} Ke_1 \oplus H,$$

which is a direct sum as vector spaces. Indeed, for any $v \in V$, we can write $v = \langle e_1, v\rangle e_1 + (v - \langle e_1, v\rangle e_1)$ so that $\langle e_1, v\rangle e_1 \in Ke_1$ while $(v - \langle e_1, v\rangle e_1) \in H$. Because $\dim H = \dim V - \dim K = \dim V - 1$ and $\dim Ke_1 = 1$, we conclude that this must in fact be a direct sum.

We now apply the inductive hypothesis to H to finish. Indeed, $\dim H < \dim V$ grants us an orthogonal basis $\{e_2, \dots, e_n\}$ spanning H, where $n := \dim V$. Thus, $\{e_1, \dots, e_n\}$ spans V and is a basis, and we see $\langle e_i, e_j\rangle = 0$ for any $i < j$ because either $i = 1$ and $e_j \in H$ or by construction of the e_i if $i, j \geq 2$. ∎

Remark 1.17. Note that when Q is given an orthogonal basis $\{e_i\}_{i=1}^n$, we get to compute that $v = \sum_i x_i e_i$ yields

$$Q(v) = B(v, v) = \sum_{i=1}^n \sum_{j=1}^n x_i x_j B(x_i, x_j) = \sum_{i=1}^n a_i x_i^2,$$

where $a_i := B(e_i, e_i)$. The point is that we only need to look at quadratic forms lacking cross terms.

1.2.2 Small Dimensions

We are going to induct on dimension to show Theorem 1.13, so we pick up a few lemmas.

Definition 1.18 (represents)**.** Fix a quadratic space (V, Q, B) over a field K not of characteristic 2. Then we say Q *represents* $c \in K$ if and only if there is a nonzero $v \in V$ such that $Q(v) = c$.

The following lemma explains why we've been focusing on representing 0 thus far (e.g., in the statement of Theorem 1.13).

Lemma 1.19. Fix a non-degenerate quadratic space (V, Q, B) over a field K not of characteristic 2. If Q represents 0, then Q represents c for all $c \in K$.

Proof. To begin, for any $t \in K$ and $v, w \in V$, we compute

$$Q(tv + w) - t^2 Q(v) - Q(w) = Q(tv + w) - Q(tv) - Q(w) = 2B(tv, w) = 2tB(v, w),$$

so

$$Q(tv + w) = t^2 Q(v) + 2tB(v, w) + Q(v).$$

Now, because Q represents 0, we may find $v \neq 0$ such that $Q(v) = 0$. Further, because Q is non-degenerate, we see that $v \neq 0$ requires $w \in V$ such that $B(v, w) \neq 0$ by Remark 1.11. Setting $\alpha := 2B(v, w)$ and $\beta = Q(w)$, we see

$$Q(tv + w) = \alpha t + \beta,$$

where $\alpha \neq 0$, so letting t vary completes the proof. Indeed, for any $c \in K$, set $t := (c - \beta)/\alpha$. ∎

The following lemma will be useful in our induction on variables.

Lemma 1.20. Fix a non-degenerate quadratic space (V, Q, B) over a field K not of characteristic 2. Then Q represents $c \in K$ if and only if $R \coloneqq Q - cy^2$ represents 0, where R is on a vector space of dimension one larger.

Proof. In one direction, if $Q(x_1, \dots, x_n) = c$ for some $(x_1, \dots, x_n) \neq 0$, then $R(x_1, \dots, x_n, 1) = c - c = 0$ with $(x_1, \dots, x_n, 1) \neq 0$.

In the other direction, suppose $R(x_1, \dots, x_n, y) = 0$ for $(x_1, \dots, x_n, y) \neq 0$. Note $Q(x_1, \dots, x_n) = cy^2$, so we have two cases.

- If $y \neq 0$, then we see $Q(x_1/y, \dots, x_n/y) = c$.
- If $y = 0$, then we see $Q(x_1, \dots, x_n) = 0$, but $(x_1, \dots, x_n) \neq 0$, so Lemma 1.19 finishes. ∎

Here is a more basic lemma to deal with small dimensions.

Lemma 1.21. Fix a field K not of characteristic 2. Fix nonzero $a, b, c \in K$.

(a) $Q = x^2$ does not represent 0.

(b) $Q = x^2 - ay^2$ represents 0 if and only if a is a square.

(c) $Q = x^2 - ay^2 - bz^2$ represents 0 if and only if b is in the image of the norm map $\mathrm{N}\colon K(\sqrt{a}) \to K$.

(d) $Q = x^2 - by^2 - cz^2 + acw^2$ represents 0 if and only if c is in the image of the norm map $K(\sqrt{a}, \sqrt{b}) \to K(\sqrt{ab})$.

Note that part (d) really requires expanding our field K in a nontrivial way. In particular, even if one only cared about $\mathbb{Q}$, phrasing part (d) without extending from $\mathbb{Q}$ would require some obfuscation.

Proof. Here we go.

(a) Note $x^2 = 0$ implies $x = 0$.

(b) Applying Lemma 1.20 to (a), we see that Q represents 0 if and only if $Q_1 \coloneqq x^2$ represents a. (Note Q_1 is non-degenerate: it has discriminant 1.)

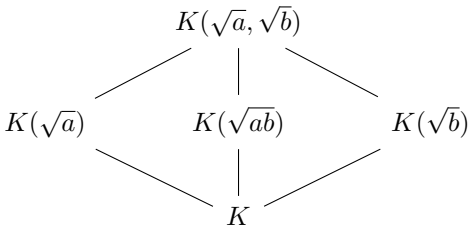
(c) If a is a square, then Q represents 0 (take $(x, y, z) = (\sqrt{a}, 1, 0)$), and b is indeed in the image of the norm map $K \to K$.

Otherwise, $a \neq 0$ is not a square, so $x^2 - ay^2$ is a non-degenerate quadratic form. By Lemma 1.20 we see Q represents 0 if and only if $x^2 - ay^2$ represents b, or

$$b = (x - y\sqrt{a})(x + y\sqrt{a}) = \mathrm{N}_K^{K(\sqrt{a})}(x + y\sqrt{a})$$

for some $x, y \in K$, which is equivalent to $b \in \operatorname{im} \mathrm{N}_K^{K(\sqrt{a})}$.

(d) This is a bit complicated. We will work towards having the following tower of fields.



(1.1)

We quickly deal with degenerate cases.

- If a is a square, recall $a \neq 0$, so Q represents 0 by $(x,y,z,w) = (0,0,1,1/\sqrt{a})$. Further, we see $K(\sqrt{a},\sqrt{b}) = K(\sqrt{ab})$ because $a \neq 0$, so c is of course in the image of the norm map.
- If b is a square, Q represents 0 by $(x,y,z,w) = (\sqrt{b},1,0,0)$. Further, $K(\sqrt{a},\sqrt{b}) = K(\sqrt{ab})$ because $b \neq 0$, so c is again in the image of the norm map.
- If ab is a square but neither nor a nor b are squares, then we see that $\sqrt{a} = \sqrt{ab}/\sqrt{b}$, so $K(\sqrt{a}) = K(\sqrt{b})$. Thus, c is in the image of the norm map $K(\sqrt{a},\sqrt{b}) \to K(\sqrt{ab})$ if and only if c is in the image of the norm map $K(\sqrt{b}) \to K$.

  If c is in the image of the norm map, then $0 = x^2 - by^2 - c \cdot 1^2 + ac \cdot 0^2$ for some $x, y \in K$, so Q represents 0. Conversely, if Q represents 0 by $(x,y,z,w) \neq 0$, then we note $z^2 - aw^2 = 0$ forces $z = w = 0$ by (b) and so $x^2 - by^2 = 0$, which forces $x = y = 0$ by (b) again. Thus, $z^2 - aw^2 \neq 0$, so we can solve
  $$c = \frac{x^2 - by^2}{z^2 - aw^2} = \frac{\mathrm{N}_K^{K(\sqrt{b})}(x + b\sqrt{y})}{\mathrm{N}_K^{K(\sqrt{a})}(z + w\sqrt{a})},$$
  so c is in the image of the map $\mathrm{N}_K^{K(\sqrt{a})} = \mathrm{N}_K^{K(\sqrt{b})}$ because this function is multiplicative.

Lastly, we must deal with the case where all the quadratic fields in (1.1) are not K. Quickly, we note that $K(\sqrt{a}) \neq K(\sqrt{b})$ in this situation. Indeed, if $\sqrt{a} \in K(\sqrt{b})$, then we can write $\sqrt{a} = x + y\sqrt{b}$ for some $x, y \in K$. Applying the Galois action of $K(\sqrt{a}) = K(\sqrt{b})$, we then see
$$-\sqrt{a} = x - y\sqrt{b},$$
so $x = 0$, and we get $\sqrt{a} = y\sqrt{b}$ for some $y \in K$. Thus, $\sqrt{ab} = yb$, implying $K(\sqrt{ab}) = K$, which degenerates this case.

It follows $K(\sqrt{a}) \cap K(\sqrt{b}) = K$ in our case, so $K(\sqrt{a},\sqrt{b})/K$ is in fact a biquadratic extension in our case. Arguing exactly as in the last degenerate case above, we note that Q represents 0 by $(x,y,z,w) \neq 0$ if and only if
$$c = \frac{x^2 - by^2}{z^2 - aw^2} = \frac{\mathrm{N}_K^{K(\sqrt{b})}(x + y\sqrt{b})}{\mathrm{N}_K^{K(\sqrt{a})}(z + w\sqrt{a})},$$
which is equivalent to $c = \mathrm{N}_K^{K(\sqrt{a})}(\alpha) \cdot \mathrm{N}_K^{K(\sqrt{b})}(\beta)$ for some $\alpha \in K(\sqrt{a})$ and $\beta \in K(\sqrt{b})$. We would like this last condition to be equivalent to $c \in \mathrm{N}_K^{K(\sqrt{a},\sqrt{b})}$. Thus, to finish the proof, we outsource to a lemma (Lemma 1.23) we will prove next class. ∎

Remark 1.22. Lemma 1.21 provides the connection to norms, which have a connection to cohomology. So we can see that, indeed, we will be able to use cohomological tools shortly.

1.3 January 20

Last time we were in the middle of showing Lemma 1.21, so we continue where we left off.

1.3.1 Hilbert's Theorem 90

Here is the desired lemma.

Lemma 1.23. Fix a field K not of characteristic not 2. Find $a, b \in K$ such that $[K(\sqrt{a},\sqrt{b}) : K] = 4$. Then $c \in K^\times$ is in the image of the norm map $\mathrm{N}\colon K(\sqrt{a},\sqrt{b}) \to K(\sqrt{ab})$ if and only if there exist $x \in K(\sqrt{a})$ and $y \in K(\sqrt{b})$ such that
$$c = \mathrm{N}_K^{K(\sqrt{a})}(x) \cdot \mathrm{N}_K^{K(\sqrt{b})}(y).$$

Proof of backward direction. Observe that we are still dealing with the tower of fields in (1.1). Now, note

$$\mathrm{Gal}(K(\sqrt{a},\sqrt{b})/K) = \{1,\sigma,\tau,\sigma\tau\},$$

where $\sigma\colon \sqrt{a}\mapsto\sqrt{a}$ and $\sigma\colon \sqrt{b}\mapsto -\sqrt{b}$ and $\tau\colon \sqrt{a}\mapsto -\sqrt{a}$ and $\tau\colon \sqrt{b}\mapsto\sqrt{b}$. (Notably, $\mathrm{Gal}(K(\sqrt{a})/K)=\langle\tau\rangle$ and $\mathrm{Gal}(K(\sqrt{b})/K)=\langle\sigma\rangle$.) We now want the following to be equivalent.

(a) There are $x,y\in K(\sqrt{a},\sqrt{b})$ such that $(\sigma-1)x=(\tau-1)y=0$ and $xy\cdot\sigma\tau(xy)=c$.

Indeed, $(\sigma-1)x=0$ means $x\in K(\sqrt{a})$, and similarly for $y\in K(\sqrt{b})$, so this statement is equivalent to $c=\mathrm{N}_K^{K(\sqrt{a})}(x)\cdot\mathrm{N}_K^{K(\sqrt{b})}(y)$ for $x\in K(\sqrt{a})$ and $y\in K(\sqrt{b})$.

(b) There is $z\in K(\sqrt{a},\sqrt{b})$ such that $z\cdot\sigma\tau(z)=c$.

Indeed, note $\sigma\tau(\sqrt{ab})=\sqrt{ab}$, so $\mathrm{Gal}(K(\sqrt{ab})/K)=\{1,\sigma\tau\}$. Thus, this is equivalent to c being in the image of the norm map $\mathrm{N}\colon K(\sqrt{a},\sqrt{b})\to K(\sqrt{ab})$.

By setting $z:=xy$, we thus see that (a) implies (b), so the hard part is showing the reverse direction.

Showing (b) implies (a) is somewhat harder. Assume (b), and observe that $z\cdot\sigma(z)=\mathrm{N}_{K(\sqrt{a})}^{K(\sqrt{a},\sqrt{b})}(z)$ is fixed by σ and hence in $K(\sqrt{a})$. Further, we may compute

$$\mathrm{N}_K^{K(\sqrt{a})}(z\cdot\sigma(z))=\mathrm{N}_K^{K(\sqrt{a},\sqrt{b})}(z)=z\cdot\sigma(z)\cdot\tau(z)\cdot\sigma\tau(z)$$

is an element of K. Now, we see $z\cdot\sigma\tau(z)=c$ is an element of K, so $\sigma(z)\cdot\tau(z)\in K$ as well. Thus, hitting this with σ, we see

$$\sigma(z)\cdot\tau(z)=\sigma(\sigma(z)\cdot\tau(z))=z\cdot\sigma\tau(z)=c$$

also, so we conclude $\sigma(z)\cdot\tau(z)=c$, so in fact $z\cdot\sigma(z)/c\in K(\sqrt{a})$ is an element of norm 1. We now appeal to Hilbert's theorem 90.

Theorem 1.24 (Hilbert 90)**.** Fix a cyclic extension of fields L/K with Galois group $\mathrm{Gal}(L/K)=\langle\sigma\rangle$. If $t\in L$ has $\mathrm{N}_K^L(t)=1$, then there exists $\alpha\in L$ such that $t=\sigma(\alpha)/\alpha$.

Remark 1.25. Of course, any element of the form $\sigma(\alpha)/\alpha$ will have norm 1 by some telescoping.

We will show Theorem 1.24 via group cohomology later, but we will use it freely for now. Pick up the promised $x\in K(\sqrt{a})$ such that

$$\frac{z\cdot\sigma(z)}{c}=\frac{\tau(x)}{x}.$$

Further, set $y:=\sigma\tau(z)/x$, and we compute

$$\tau(y)=\frac{\sigma(z)}{\tau(x)}\overset{*}{=}\frac{c}{z\cdot x}=\frac{\sigma\tau(z)}{x}=y.$$

Note we have used the definition of x at $\overset{*}{=}$. Thus, $y\in K(\sqrt{b})$, so to finish the proof, we check

$$xy\cdot\sigma\tau(xy)=\sigma\tau(z)\cdot(\sigma\tau)^2(z)=z\cdot\sigma\tau(z)=c,$$

so we are done. ∎

Roughly speaking, the hard direction of the above proof uses Theorem 1.24 to construct our α and β, and then everything else is more or less a computation.

1.3.2 Hasse–Minkowski

We are now ready to prove Theorem 1.13, modulo some more appeals to group cohomology. Here is the statement.

Theorem 1.13 (Hasse–Minkowski)**.** Let K be a number field, and let Q be a quadratic form on the K-vector space V. Then Q has a nontrivial zero in V if and only if Q has a nontrivial zero in $V \otimes_K K_v$ for all places v of K.

Proof. By adjusting the basis of V as in Remark 1.17, we may assume that $Q = a_1x_1^2 + \cdots + a_nx_n^2$. Additionally, if any of the variables are 0, say $a_1 = 0$, then $(1, 0, 0, \ldots, 0)$ is a nontrivial zero for both V and each $V \otimes_K K_v$, so there is nothing to say. As such, we normalize Q so that $a_1 = 1$.

We now induct on n. Here are our small cases. If $n = 1$, then there are never any zeroes at all by Lemma 1.21. For $n = 2$, we are studying $Q = x_1^2 + a_2x_2^2$, so we are done by Lemma 1.21 by appealing to the following result, which we will prove later.

Theorem 1.26. Fix a number field K. Then $\alpha \in K^\times$ is a square if and only if α is a square in each K_v for all places v.

For $n = 3$ and $n = 4$, we are again done by Lemma 1.21 upon appealing to the following result.

Theorem 1.27 (Hasse norm)**.** Fix a cyclic extension L/K of number fields. Given $a \in K^\times$, then a is in the image of the norm $L \to K$ if and only if a is in a norm in K_v for all places v.

Roughly speaking, Lemma 1.21 turns statements about quadratic forms into statements about norms, so we get a local-to-global principle via Theorem 1.27's local-to-global principle.

We are now almost ready for the inductive step. We make a few starting comments.

- A quadratic form of the form $Q_1(x_1, \ldots, x_m) - Q_2(y_1, \ldots, y_n)$ will represent 0 if and only if there exists some c represented by both Q_1 and Q_2. There isn't really anything to say here.
- If Q represents some $c \in K^\times$, then Q represents the entire equivalence class of c in $K^\times/K^{\times 2}$. Indeed, this is because Q is a quadratic form and thus homogeneous of degree 2.
- For each place v, we have $K_v^{\times 2}$ is an open subgroup of $K_v^\times$. Indeed, for archimedean v, this reduces to saying $\mathbb{R}_{>0} \subseteq \mathbb{R}^\times$ is open, and $\mathbb{C}^\times = \mathbb{C}^\times$ is open.

  We can argue for nonarchimedean places v explicitly, but we can give a more abstract argument via Hensel's lemma. Indeed, it suffices to provide a neighborhood of 1 in $K_v^\times$ (because $K_v^\times$ is a topological group), so we choose
  $$U \coloneqq \left\{a : \left|1^2 - a\right|_v < |2 \cdot 1|_v^2\right\}.$$
  Notably, for each $a \in U$, we see 1 witnesses the ability to solving $x^2 - a = 0$ in K_v by Hensel's lemma.

We now proceed with our induction. Assume $n \geq 5$. We may write
$$Q(x_1, \ldots, x_n) = ax_1^2 + bx_2^2 - R(x_3, \ldots, x_n),$$
for some quadratic form R in $n-2$ variables. To continue, we give another statement which comes from the Hasse norm theorem.

Theorem 1.28 (Hasse norm)**.** Fix a cyclic extension L/K of number fields, and let Q be a quadratic form in $n \geq 3$ variables. For each $a \in K^\times$, then there is a finite set of places S such that Q represents 0 in K_v for each $v \notin S$.

Proof. We give a proof from algebraic geometry. Take $K = \mathbb{Q}$ for simplicity. For simplicity, take $Q = ax^2 + by^2 + cz^2$, and note $V(Q) \subseteq \mathbb{P}^2_{\mathbb{Q}}$ is a genus-0 curve. For all but finitely many primes p, we see $\nu_p(a) = \nu_p(b) = \nu_p(c) = 0$, so we can base-change $V(Q)$ to $\mathbb{Z}_p$ and then $\mathbb{F}_p$, where $V(Q)$ remains a genus-0 curve. However, a genus-0 curve always has a point over a finite field, and then smoothness of $V(Q)$ allows us to lift the $\mathbb{F}_p$-point back to a $\mathbb{Z}_p$-point by Hensel's lemma. ■

So by Theorem 1.28, there are finitely many places S for which R does not represent 0.

Now, suppose that Q has a nontrivial 0 in each $V \otimes_K K_v$, and we must show that Q has a nontrivial 0 in V. We can deal with each $v \notin S$ because R represents everything by Lemma 1.19. Thus, focusing on some $v \notin S$, we see Q having a nontrivial zero in $V \otimes_K K_v$ implies that there is some $c_v \in K_v$ represented by both $ax_1^2 + bx_2^2$, so write

$$a\alpha_{1,v}^2 + b\alpha_{2,v}^2 = c_v = R(\alpha_{3,v}, \dots, \alpha_{n,v}).$$

By approximating, we choose $\alpha_i \in K$ arbitrarily close to each $\alpha_{i,v}$ in K_v so that $c = a\alpha_1^2 + b\alpha_2^2$ differs from c_v only be a square in $v \in S$. This is possible because $K_v^{\times 2}$ is open in $K_v^\times$. Note that R still represents c in each K_v for $v \in S$ because c is only a square away from c_v.

Thus, we see that the form

$$cY^2 - R(x_3, \dots, x_n)$$

will represent 0 in each K_v for all v. But this form has $n-1$ variables, so our induction kicks in and tells usu that $cY^2 - R$ represents 0 in K, so R represents c in K, so Q represents 0 in K. This completes the proof. ■

Remark 1.29. Professor Olsson thinks that the last part of this argument is a little too clever.

1.4 January 25

Last class, we were in the middle of proving Theorem 1.13. I have edited directly into that proof for continuity reasons.

1.4.1 Introducing G-modules

We would like to fill in the boxes in the proof of Theorem 1.13, so we introduce a little group cohomology. Fix a group G.

Definition 1.30 (G-module)**.** A *G-module* is an abelian group M equipped with a G-action. In other words, a G-module is a (left) $\mathbb{Z}[G]$-module. We will write the category of G-modules by Mod_G.

Warning 1.31. If G is not abelian, then $\mathbb{Z}[G]$ is not abelian, so we are not doing commutative algebra.

Recall that $\mathbb{Z}[G]$ is the free abelian group on G as letters, where multiplication is given by

$$\left(\sum_{g\in G} a_g g\right)\left(\sum_{h\in G} b_h h\right) = \sum_{g\in G}\sum_{h\in G} a_g b_h (gh).$$

In other words, we extend the multiplication $g \cdot h = gh$ linearly.

Example 1.32. Let $G = \langle\sigma\rangle$ be a finite group of order n. Then we see $\mathbb{Z}[x]/(x^n - 1) \cong \mathbb{Z}[G]$ by sending $x \mapsto \sigma$. Indeed, this certainly defines a homomorphism between these rings because $\sigma^n - 1 = 0$, and it is certainly surjective. Lastly, it is injective: $p(x) \in \mathbb{Z}[x]$ vanishes under this map if and only if $p(\sigma) = 0$. By taking $p \pmod{x^n - 1}$, we may assume that $p = 0$ or $\deg p < n$, but then $p(\sigma)$ will only vanish if $p = 0$.

Note that the following are equivalent to M being a G-module.

- M is a $\mathbb{Z}[G]$-module.
- There is a homomorphism $\mathbb{Z}[G] \to \mathrm{End}(M)$.
- By hitting this with the free-forgetful adjunction, this is equivalent to having a morphism $G \to \mathrm{Aut}(M)$. We are going to automorphisms because elements of G are invertible, so their image in $\mathrm{End}(M)$ needs to also be invertible.
- There is an action $\cdot\colon G \times M \to M$ satisfying the following conditions for $g, g' \in G$ and $m, m' \in M$.
  - $e \cdot m = m$.
  - $(g+g')(m+m') = gm + gm' + g'm + g'm'$.
  - $(gh) \cdot m = g(h \cdot m)$.

Here are some examples.

Example 1.33. Let $G = \langle \sigma \rangle$ be a finite group of order n. By Example 1.32, a G-module is a module over $\mathbb{Z}[x]/(x^n - 1)$.

Example 1.34. For any group G, the abelian group $\mathbb{Z}$ can be given a "trivial" G-action by $g \cdot k \coloneqq k$ for all $g \in G$ and $k \in \mathbb{Z}$.

In the future, when we write down $\mathbb{Z}$, we mean $\mathbb{Z}$ with the trivial G-action.

1.4.2 Some Functors

Cohomology is interested in deriving the invariant functor $(-)^G\colon \mathrm{Mod}_G \to \mathrm{Ab}$ which sends a G-module M to

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

Alternatively, $M^G \simeq \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, M)$. Indeed, a map $\varphi\colon \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, M)$ means that we are choosing an element $\varphi(1) \in M$, and making this a G-module morphism requires

$$g \cdot m = g \cdot \varphi(1) = \varphi(g \cdot 1) = \varphi(1) = m$$

for all $g \in G$. Thus, we see that $(-)^G$ is functorial automatically because $\mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, -)$ is.

There is also a notion of co-invariants, denoted $(-)_G\colon \mathrm{Mod}_G \to \mathrm{Ab}$ by

$$M_G \coloneqq M/I_G M,$$

where $I_G \subseteq \mathbb{Z}[G]$ is the submodule of elements of degree 0. Equivalently, $M_G = \mathbb{Z} \otimes_{\mathbb{Z}[G]} M$, so we see that this construction is functorial.

Here are some preliminary observations.

- The functor $(-)^G$ is left-exact. This holds because $(-)^G \simeq \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, -)$, and the Hom functor is left-exact.
- The functor $(-)_G$ is right-exact. This holds because $(-)_G \simeq \mathbb{Z} \otimes_{\mathbb{Z}[G]} -$, and the $\otimes$ functor is right-exact.
- For any element $x \in \mathbb{Z}[G]$, multiplication by x defines a morphism of abelian groups $x\colon M \to M$ for any G-module M. For example, if G is a finite group, define $N_G \coloneqq \sum_{g \in G} g$. We note $N_G\colon M \to M$ actually defines a map $M \to M^G$: indeed, for any $m \in M$ and $g \in G$, we see

  $$g \cdot N_G(m) = g \cdot \sum_{h \in G} hm = \sum_{h \in G} ghm = \sum_{h \in G} hm$$

  by re-indexing our sum. In fact, we note that $I_G M$ is in the kernel of this map because $N_G((g-1)m) = 0$ for all $g \in G$, and the elements $(g-1)m$ generate $I_G M$.

In light of the last observation, we note that we have a natural transformation

$$N_G \colon (-)_G \to (-)^G.$$

One can check naturality by hand, but we won't bother. Using the first two observations, we see we want to derive our left-exact functor to the right (which will give group cohomology), and we want to derive our right-exact functor to the left (which will give group homology). In particular, we will take

$$H^i(G,-) \coloneqq \operatorname{Ext}^i_{\mathbb{Z}[G]}(\mathbb{Z},-) \qquad \text{and} \qquad H_i(G,-) \coloneqq \operatorname{Tor}_i^{\mathbb{Z}[G]}(\mathbb{Z},-),$$

which defines group cohomology and group homology. It turns out that the norm map will connect these together to create Tate cohomology.

Remark 1.35. In practice, one can compute $H^\bullet(G,M)$ and $H_\bullet(G,M)$ by taking some $\mathbb{Z}[G]$-projective resolution

$$\cdots \to P_2 \to P_1 \to P_0 \to \mathbb{Z} \to 0$$

of $\mathbb{Z}$. Then $H^i(G,M) = H^i(\operatorname{Hom}^\bullet(P_\bullet, M))$ and $H_i(G,M) = H^i(P_\bullet \otimes_{\mathbb{Z}[G]} M)$.

1.5 January 27

Today, we continue talking around group cohomology.

1.5.1 Tate Cohomology

It will be convenient to connect group cohomology and group cohomology. Take G to be a finite group. Fix some projective resolution $P_\bullet$ of $\mathbb{Z}$. Then we have exact sequences

$$\cdots P_2 \otimes M \to P_1 \otimes M \to P_0 \otimes M \to M_G \to 0$$

and

$$0 \to M^G \to \operatorname{Hom}(P_0, M) \to \operatorname{Hom}(P_1, M) \to \operatorname{Hom}(P_2, M) \to \cdots.$$

But with G finite, we have a norm map $N_G \colon M_G \to M^G$, so we can splice these together to give one long sequence

$$\cdots P_2 \otimes M \to P_1 \otimes M \to P_0 \otimes M \to \operatorname{Hom}_{\mathbb{Z}}(P_0, M) \to \operatorname{Hom}_{\mathbb{Z}}(P_1, M) \to \operatorname{Hom}_{\mathbb{Z}}(P_2, M) \to \cdots,$$

where the map $P_0 \otimes M \to \operatorname{Hom}_{\mathbb{Z}}(P_0, M)$ is given by $P_0 \otimes M \to M_G \to M^G \to \operatorname{Hom}_{\mathbb{Z}}(P_0, M)$. We now define Tate cohomology is the cohomology of this complex, where degree-0 is at $\operatorname{Hom}_{\mathbb{Z}}(P_0, M)$. Explicitly, we have the following.

Definition 1.36 (Tate cohomology)**.** Fix a finite group G. Given a G-module M, we define the *Tate cohomology* as follows, for some $i \in \mathbb{Z}$.

$$\widehat{H}^i(G,M) \coloneqq \begin{cases} H^i(G,M) & \text{if } i \geq 1, \\ H_{-i-1}(G,M) & \text{if } i \leq -2, \\ \ker N_G & \text{if } i = -1, \\ M^G / N_G(M_G) & \text{if } i = 0, \end{cases}$$

where N_G is the norm map $N_G \colon M_G \to M^G$.

Let's see the computations at $i = -1$ and $i = 0$ more explicitly.

- At $i = -1$, we are computing
$$\frac{\ker(P_0 \otimes M \to M_G \to M^G)}{\operatorname{im}(P_1 \otimes M \to P_0 \otimes M)}.$$
However, the image $P_1 \otimes M \to P_0 \otimes M$ is exactly the kernel of the surjection $P_0 \otimes M \twoheadrightarrow M_G$, so we are just computing the kernel along $M_G \to M^G$. Indeed, letting I denote the image of $P_1 \otimes M \to P_0 \otimes M$, we get a morphism of exact sequences as follows.
$$\begin{array}{ccccccccc} 0 & \longrightarrow & I & \longrightarrow & P_0 \otimes M & \longrightarrow & M_G & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow{\scriptstyle N_G} & & \\ 0 & \longrightarrow & 0 & \longrightarrow & M^G & = & M^G & \longrightarrow & 0 \end{array}$$
Taking kernels, the snake lemma grants us an exact sequence
$$0 \to I \to \ker(P_0 \otimes M \to M^G) \to \ker(M_G \to M^G) \to 0,$$
so the claim follows.
- At $i = 0$, the computation is similar.

Remark 1.37. We can now see how norms might be important in the future.

1.5.2 Cohomology of Cyclic Groups

In this subsection, let $G = \langle \sigma \rangle$ be a cyclic group of order n. We saw in Example 1.32 that
$$\mathbb{Z}[G] = \frac{\mathbb{Z}[x]}{(x^n - 1)},$$
so for example $\mathbb{Z}[G]$ is commutative. In our case, we can right down a particularly nice (augmented) free resolution of $\mathbb{Z}$ as
$$\cdots \to \mathbb{Z}[G] \xrightarrow{T} \mathbb{Z}[G] \xrightarrow{N} \mathbb{Z}[G] \xrightarrow{T} \mathbb{Z}[G] \to \mathbb{Z} \to 0,$$
where $\mathbb{Z}[G] \to \mathbb{Z}$ is the usual augmentation map and $T \coloneqq (\sigma - 1)$ and $N \coloneqq N_G$. Indeed, let's see that this is exact.

- Note $\mathbb{Z}[G] \to \mathbb{Z}$ is of course surjective, so we are exact at $\mathbb{Z}$.
- Next, we see that the kernel of the map $\mathbb{Z}[G] \to \mathbb{Z}$ consists of the terms of degree 0, which are $\mathbb{Z}$-generated by elements of the form $\left(\sigma^i - \sigma^j\right)$ for indices i and j, but this means that we are $\mathbb{Z}[G]$-generated by $(\sigma - 1)$.
- Continuing, the kernel of the map $T \colon \mathbb{Z}[G] \to \mathbb{Z}[G]$ is given by the elements of the form $\sum_{i=0}^{n-1} a_i \sigma^i$ which when multiplied by T vanish. Explicitly, we see
$$T\left(\sum_{i=0}^{n-1} a_i \sigma^i\right) = \sum_{i=0}^{n-1} \left(a_{i-1} - a_i\right) \sigma^i,$$
where indices are taken $\pmod n$. Thus, this vanishes if and only if a_i is constant, so we see that we are in the kernel if and only if we take the form
$$\sum_{i=0}^{n-1} a\sigma^i = aN_G$$
for some $a \in \mathbb{Z}[G]$. So the kernel here is indeed the image of the map $N \colon \mathbb{Z}[G] \to \mathbb{Z}[G]$.

- Lastly, we can compute the kernel of the map $N\colon \mathbb{Z}[G] \to \mathbb{Z}[G]$ as the image of the map $T\colon \mathbb{Z}[G] \to \mathbb{Z}[G]$. We omit this computation.

The point is that we can compute group homology via the sequence

$$\cdots \to M \xrightarrow{T} M \xrightarrow{N} M \xrightarrow{T} M,$$

and we can compute the group cohomology via the sequence

$$M \xrightarrow{T} M \xrightarrow{N} M \to \cdots.$$

Splicing these together gives us Tate cohomology, which works properly because the map $M_G \to M^G$ is precisely the norm. In particular, we get the following nice result.

Proposition 1.38. Let $G = \langle \sigma \rangle$ be a cyclic group of order n. For any G-module M, the groups $\widehat{H}^i(G, M)$ are 2-periodic in $i \in \mathbb{Z}$.

Remark 1.39. Let's take a moment to figure out where we want to go. Fix a cyclic extension L/K of number fields, where G is the Galois group. For example, we wanted a statement like "if $a \in K^\times$ is a norm in K_v for each v, then a is a norm in K." This conclusion on a means we want a to vanish in

$$\frac{K^\times}{\mathrm{N}_K^L\left(L^\times\right)} = \frac{\left(L^\times\right)^G}{N_G\left(L^\times\right)} = \widehat{H}^0\left(G, L^\times\right).$$

Combining with our place data, we wanted some sort of statement like

$$\widehat{H}^0\left(G, L^\times\right) \to \prod_v \widehat{H}^0\left(G_v, L_v^\times\right)$$

to be true. Roughly speaking, this will reduce to some kind of cohomology on the idéles.

1.6 January 30

We continue discussing group cohomology.

1.6.1 Cocycles

We discuss cocycles, which will be an explicit way to discuss group cohomology.

Remark 1.40. These notions come from algebraic topology, where a group G gives rise to a space EG, which is constructed as functions $\mathrm{Mor}([n+1], G)$ at degree n satisfying certain conditions. One can use this to build a space which is contractible and has a free G-action; then $BG \coloneqq EG/G$ is the classifying space, the point of which is that $\pi_1(BG) = G$ and no other nontrivial homotopy groups. If you write everything out, you can get cocycles from this construction.

So let's write things out. For $n \geq 0$, define the G-module $P_n \coloneqq \mathbb{Z}\left[G^{n+1}\right]$, and define the differential $d\colon P_n \to P_{n-1}$ by

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

One can check by hand that $d^2 = 0$, so we get a complex

$$\cdots \to P_3 \to P_2 \to P_1 \to P_0 \to 0.$$

Here are some checks.

- Note that each P_n is a free $\mathbb{Z}[G]$-module, generated by the elements of the form $(1, g_1, \dots, g_n)$. Indeed, we can write
$$\mathbb{Z}[G] \cdot (1, g_1, \dots, g_n) = \bigoplus_{g \in G} \mathbb{Z}[(g, gg_1, \dots, gg_n)],$$
so looping over all basis elements completes this. As such, $P_n \cong \mathbb{Z}[G]^n$ for each $n \geq 0$.

- We would like to turn this into a resolution of $\mathbb{Z}$. Well, there is the usual augmentation map $\varepsilon \colon P_0 \to \mathbb{Z}$ given by $g \mapsto 1$. Additionally, the composite $P_1 \to P_0 \to \mathbb{Z}$ is the zero map: for each basis element (g_0, g_1), we see
$$\varepsilon d(g_0, g_1) = \varepsilon(g_1 - g_0) = 0.$$

- We now claim that $\varepsilon \colon P_\bullet \to \mathbb{Z}$ is an (augmented) free resolution. We know that it's free, so it remains to check our exactness. Note we already have surjectivity $P_0 \to \mathbb{Z}$, so we need to show that $H^n(P_\bullet) = 0$ for $n \geq 1$.

  Now, we want an isomorphism of some cohomology groups, so we would like to find a chain homotopy between id and zero. Explicitly, we would like to find group homomorphisms $h_n \colon P_n \to P_{n+1}$ fitting into the diagram
$$\begin{array}{ccccccccccc}
\cdots & \xrightarrow{d} & P_2 & \xrightarrow{d} & P_1 & \xrightarrow{d} & P_0 & \xrightarrow{\varepsilon} & \mathbb{Z} \\
 & & & \swarrow^{h_2} & & \swarrow^{h_1} & & \swarrow^{h_{-1}} & \\
\cdots & \xrightarrow[d]{} & P_2 & \xrightarrow[d]{} & P_1 & \xrightarrow[d]{} & P_0 & \xrightarrow[\varepsilon]{} & \mathbb{Z}
\end{array}$$
  so that $dh_n + h_{n-1}d = \mathrm{id}$. The point here is that, for $n \geq 1$, we see $z \in \ker(P_n \to P_{n-1})$ implies that $dh_n(z) + h_{n-1}(dz) = z$, but then $dh_n(z) = z$, so z is in the image of the map $P_{n+1} \to P_n$. The exactness will then follow.

  For $n \geq -1$, we define $h_n \colon P_n \to P_{n+1}$ by
$$h_n(g_0, \dots, g_n) \coloneqq (1, g_0, \dots, g_n).$$
  To check this works, we compute
$$\begin{aligned}
dh_n(g_0, \dots, g_n) + h_{n-1}d(g_0, \dots, g_n) &= d(1, g_0, \dots, g_n) + h_{n-1}\left(\sum_{i=0}^{n} (-1)^i (g_0, \dots, g_{i-1}, g_{i+1}, \dots, g_n)\right) \\
&= \left((g_0, \dots, g_n) - \sum_{i=0}^{n} (-1)^i (1, g_0, \dots, g_{i-1}, g_{i+1}, \dots, g_n)\right) \\
&\quad + \left(\sum_{i=0}^{n} (-1)^i (1, g_0, \dots, g_{i-1}, g_{i+1}, \dots, g_n)\right) \\
&= (g_0, \dots, g_n),
\end{aligned}$$
  which completes the computation.

Thus, we see we have a free resolution of $\mathbb{Z}$, so we can compute group cohomology as previously discussed in Remark 1.35. Explicitly, for a G-module M, we define
$$\widetilde{C}^n(G, M) \coloneqq \mathrm{Hom}_{\mathbb{Z}[G]}(P_n, M) \subseteq \mathrm{Mor}_G\left(G^{n+1}, M\right),$$
and the differential sends $f \in \widetilde{C}^n(G, M)$ to $f \circ d$, which is
$$(df)(g_0, \dots, g_n, g_{n+1}) = \sum_{i=0}^{n} (-1)^i f(g_0, \dots, g_{i-1}, g_{i+1}, \dots, g_n).$$
Indeed, we can see visually that this has constructed a G-module morphism.

The G-module $\widetilde{C}(G,M)$ has defined what are called "homogeneous cocycles." However, recall that P_n is a free $\mathbb{Z}[G]$-module generated by the elements of the form $(1,g_1,\dots,g_n)$, so we can think of $\operatorname{Hom}_{\mathbb{Z}[G]}(P_n,M)$ as functions $G^n \to M$, with no G-equivariance. However, our isomorphism $P_n \cong \mathbb{Z}[G]^n$ was moderately non-canonical, so our differential has changed somewhat. It is standard convention to define P_n as instead generated by

$$(1,g_1,g_1g_2,g_1g_2g_3,\dots,g_1\cdots g_n),$$

which makes our differential

$$(df)(g_1,\dots,g_{n+1}) = g_1f(g_2,\dots,g_{n+1}) + \sum_{i=1}^{n}(-1)^i f(g_1,\dots,g_ig_{i+1},\dots,g_n) + (-1)^{n+1}f(g_1,\dots,g_n).$$

This defines "inhomogeneous cocycles," which we define as $C^n(G,M)$.

Example 1.41. We discuss H^1. The differential $d\colon C^0(G,M)\to C^1(G,M)$ sends an element m to the function $g\mapsto (g-1)m$. Further, the differential $d\colon C^1(G,M)\to C^2(G,M)$ is given by

$$(df)(g_1,g_2) = g_1f(g_2) - f(g_1g_2) + f(g_1).$$

In total, $H^1(G,M)$ is isomorphic to

$$\frac{\{f : f(g_1g_2) = f(g_1) + g_1f(g_2)\}}{\{f : f(g) = (g-1)m \text{ for some } m\in M\}}.$$

For example, if the G-action is trivial, the kernel of this differential is just the homomorphisms $G\to M$, so $H^1(G,M)=\operatorname{Hom}(G,M)$.

1.7 February 1

Today we're going to talk about H^1.

Remark 1.42. There are many interpretations of H^1. For example, in algebraic geometry, we have $H^1(X,\mathcal{O}_X^\times) = \operatorname{Pic} X$. We won't discuss this, but we will see other things.

Remark 1.43. In this lecture, we will be more or less discussing faithfully flat descent.

1.7.1 Yoneda Extensions

We're going to walk through quite a few interpretations of H^1. To begin, recall $H^1(G,M)=\operatorname{Ext}^1_{\mathbb{Z}[G]}(\mathbb{Z},M)$, essentially by definition. This in some sense classifies certain exact sequences. Namely, $\operatorname{Ext}^1_{\mathbb{Z}[G]}(\mathbb{Z},M)$ classifies short exact sequences of G-modules

$$0\to M\to \mathcal{E}\to \mathbb{Z}\to 0$$

up to isomorphism of short exact sequences. (As an aside, note that all short exact sequences are $\mathbb{Z}$-split because $\mathbb{Z}$ is projective, so $\mathcal{E}\cong M\oplus\mathbb{Z}$ as abelian groups. Thus, the interesting part is the G-action.) Namely, an isomorphism of short exact sequences given by $\mathcal{E}$ and $\mathcal{E}'$ is a morphism $\varphi\colon E\to E'$ making the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M & \longrightarrow & \mathcal{E} & \longrightarrow & \mathbb{Z} & \longrightarrow & 0 \\ & & \| & & \downarrow{\scriptstyle\varphi} & & \| & & \\ 0 & \longrightarrow & M & \longrightarrow & \mathcal{E}' & \longrightarrow & \mathbb{Z} & \longrightarrow & 0 \end{array}$$

commute. Note φ is an isomorphism by the Snake lemma.

Let's see how this relates to cocycles. Namely, given a 1-cocycle $f\colon G \to M$, we can define $\mathcal{E}_f$ as the abelian group $\mathcal{E}_f \coloneqq M \oplus \mathbb{Z}$ with action defined by

$$g \cdot (m,n) \coloneqq (gm + nf(g), n).$$

Notably, $f(g) = g \cdot (0,1)$, so the map sending cocycles to extensions here is injective. We can now check by hand that this defines an action as

$$\begin{aligned} g_1(g_2 \cdot (m,n)) &= g_1 \cdot (g_2 m + nf(g_2), n) \\ &= (g_1 g_2 m + n g_1 f(g_2) + nf(g_1), n) \\ &\overset{*}{=} (g_1 g_2 m + nf(g_1 g_2), n) \\ &= (g_1 g_2) \cdot (m,n) \end{aligned}$$

where we have used the cocycle condition at $\overset{*}{=}$. Notably, we can read this argument backward to tell us that $Z^1(G,M)$ contains the data of a short exact of G-modules

$$0 \to M \to \mathcal{E} \to \mathbb{Z} \to 0$$

equipped with a section $s\colon \mathbb{Z} \to E$; explicitly, the choice of a section s grants a decomposition $\mathcal{E} \cong M \oplus \mathbb{Z}$, from which we can read the cocycle in and out of the G-action as described above.

To see how we mod out by coboundaries, we choose two sections $s, s'\colon \mathbb{Z} \to \mathcal{E}$, which can only differ by an element of $m \in M$. Tracking this through shows that the corresponding cocycle adjusts by exactly the coboundary given by $m \in M$.

Remark 1.44. On the homework, we will check that an exact sequence

$$0 \to M \to \mathcal{E} \to \mathbb{Z} \to 0$$

grants an exact sequence

$$0 \to M^G \to \mathcal{E}^G \to \mathbb{Z} \to H^1(G,M),$$

and one can check that the image of 1 under $\mathbb{Z} \to H^1(G,M)$ exactly corresponds to the short exact sequence we started with.

1.7.2 Hilbert's Theorem 90

Let's talk around Hilbert's theorem 90. Roughly speaking, a 1-cocycle $u_\bullet\colon G \to M$ is a function satisfying the relation

$$u_{g_1 g_2} = u_{g_1} \cdot g_1 u_{g_2}.$$

Note that the group law on $L^\times$ has been written multiplicatively.

For the proof, consider the category $\mathrm{Mod}(L/K)$ of G-linear L-modules. Explicitly, we want L-vector spaces V equipped with an L-semilinear action $\rho\colon G \to \mathrm{Aut}_K(V)$ such that

$$\rho_g(\ell v) = g\ell \cdot \rho_g(v).$$

For example, given a K-vector space V_0, we set $V \coloneqq V_0 \otimes_K L$ so that we have a natural G-action on L. We can see visually that

$$\rho_g(\ell' \cdot (v \otimes \ell)) = \rho_g(v \otimes \ell'\ell) = v \otimes g(\ell'\ell) = g\ell' \cdot (v \otimes \ell) = v\ell' \cdot \rho_g(v \otimes \ell).$$

The main result is as follows.

Theorem 1.45 (Faithfully flat descent)**.** The functor $\mathrm{Mod}_K \to \mathrm{Mod}(L/K)$ given by $V_0 \mapsto V_0 \otimes_K L$ is an equivalence of categories.

Remark 1.46. Using the theorem, we can recover the inverse functor as $V \mapsto V^G$ because

$$(V_0 \otimes_K L)^G \simeq V_0 \otimes_K L^G = V_0 \otimes_K K \simeq V_0.$$

To see our 1-cocycles, let's discuss Theorem 1.45 for one-dimensional L-vector spaces (V, ρ). Here, we write $V = Le$ for some basis $\{e\}$, and we define

$$u_g e \coloneqq \varphi_g(e)$$

so that the $u_g \in L^\times$ define our group action. Namely, we see $\varphi_g(\ell e) = g\ell \cdot u_g e$. Unsurprisingly, the group action condition given by ρ will give rise to the cocycle condition (and conversely): in one direction, we note $u_\bullet \colon G \to M$ is a cocycle because

$$u_{g_1 g_2} e = \rho_{g_1 g_2}(e) = \rho_{g_1}(\rho_{g_2} e) = \rho_{g_1}(u_{g_2} e) = (g_1 u_{g_2} \cdot u_{g_1}) \cdot e.$$

Lastly we note that adjusting V by isomorphism is equivalent to adjusting the basis, and we can check that the effect of adjusting the basis to $e' = ae$ merely adjusts the cocycle by $g \mapsto (g-1)a$. In total, $H^1(G, L^\times)$ consists of the 1-dimensional objects of $\operatorname{Mod}(L/K)$. (Notably, the tensor product provides the group structure on these objects.)

We now use Theorem 1.45. Each $(V, \rho) \in \operatorname{Mod}(L/K)$ should actually arise as the form $V_0 \otimes_K L$, and this corresponds to the identity element in $\operatorname{Mod}(L/K)$. Indeed, fixing some basis element $e \otimes 1 \in V_0 \otimes_K L$, we can compute our cocycle $u_\bullet$ as

$$u_g(e \otimes 1) = \rho_g(e \otimes 1) = e \otimes g1 = e \otimes 1,$$

so $u_g = 1$ everywhere. Thus, Theorem 1.45 will imply the following.

Theorem 1.47 (Hilbert 90)**.** Fix a finite Galois field extension L/K with Galois group $G = \operatorname{Gal}(L/K)$. Then $H^1(G, L^\times) = 0$.

Thus, it remains to show Theorem 1.45.

Proof of Theorem 1.45. We mentioned that the inverse functor is given by $(V, \rho) \mapsto V^G$. Thus, we divide the proof into checks.

1. We need an isomorphism $(V_0 \otimes_K L)^G = V_0$. This is clear.
2. We need an isomorphism $V^G \otimes_K L \simeq V$ in $\operatorname{Mod}(L/K)$. Well, the morphism is given by $v \otimes \ell \mapsto \ell v$.

   Now, the trick is to that it suffices to find a field extension Ω over K such that

   $$(V_\Omega)^G \otimes_\Omega (\Omega \otimes_K L) \to V \otimes_K \Omega$$

   is an isomorphism in the category $\operatorname{Mod}(L \otimes_K \Omega/\Omega)$. Namely, being an isomorphism will be reflected back down because we are working with vector spaces (namely, determinant does not change when we base-change to a larger field). Explicitly, we note V^G is the kernel of the map

   $$V \to \prod_{g \in G} V$$

   sending $v \mapsto (gv)_{g \in G}$, so $(V_\Omega)^G = V^G \otimes_K \Omega$. The point is that we are indeed allowed to base-change to the larger field, and we get to keep looking at G-invariants.

   Anyway, we now set $\Omega \coloneqq L$. We thus can compute

   $$V \otimes_K \Omega = V \otimes_L (L \otimes_K \Omega) = V \otimes_L \prod_{g \in G} L = \prod_{g \in G} V,$$

   where the G-action on $\prod_{g \in G} V$ is by permutation. Thus, the G-invariants do indeed become V. ∎

Remark 1.48. Our equivalence of categories is also compatible with a structure of tensor product over Mod_K and $\operatorname{Mod}(L/K)$.

1.8 February 3

Today we continue talking about H^1.

Remark 1.49. Roughly speaking, cohomology is "obstructions to something." The most bare-bones version of this is that cohomology measures the failure of some left exact-functors being fully exact.

1.8.1 Classification of Algebras

When G is cyclic, we have a canonical isomorphism

$$\widehat{H}^0(G, L^\times) \cong \widehat{H}^2(G, L^\times).$$

We understand $\widehat{H}^0(G, L^\times)$ as $K^\times / \mathrm{N}_K^L(L^\times)$, and it turns out that $\widehat{H}^2(G, L^\times)$ is understood as the "Brauer group" $\mathrm{Br}(L/K)$. Later in life, we might want to use stranger algebraic groups than $(-)^\times$, such as GL_n or PGL_n.

There is a notion of "non-abelian" cohomology, where a group G has an action on a group M (where M is not necessarily abelian!). In particular, we can simply define H^1 by cocycles as

$$H^1(G, M) = \frac{\{f : g_1 f(g_2) \cdot f(g_2) = f(g_1 g_2) \text{ for } g_1, g_2 \in M\}}{\{f : f(g) = (gm)m^{-1} \text{ for some fixed } m \in M\}}.$$

Notably, $H^1(G, M)$ is just a set, pointed by the trivial equivalence class.

As an application of this H^1, we pick up the following definition. Fix a Galois extension L/K with $G = \mathrm{Gal}(L/K)$. Given a K-algebra A, where the center of A contains K. Given that $A \otimes_K L \cong M_n(L)$, we are interested if $A \cong M_n(K)$.

Example 1.50. Take the field extension $\mathbb{C}/\mathbb{R}$, and let $\mathbb{H}$ be the quaternion algebra. We can see somewhat directly that $\mathbb{H} \otimes_{\mathbb{R}} \mathbb{C} \cong M_2(\mathbb{C})$, but we cannot have an isomorphism $\mathbb{H} \cong M_2(\mathbb{R})$. Indeed, just tracking where i and j and k go from $\mathbb{H}$ to $M_2(\mathbb{R})$, one can more or less write down lots of equations and see if they have a solution over $\mathbb{R}$, for which the answer turns out to be no.

To study this question, we (morally) expect that the G-invariants of $A \otimes_K L$ to go to G-invariants of $M_n(L)$. Well, suppose we have an isomorphism $\sigma \colon A \otimes_K L \to M_n(L)$, so given $g \in G$, we ask if the following diagram commutes.

$$\begin{array}{ccc} A \otimes_K L & \xrightarrow{\sigma} & M_n(L) \\ {\scriptstyle 1\otimes g}\downarrow & & \downarrow{\scriptstyle M_n(g)} \\ A \otimes_K L & \xrightarrow{\sigma} & M_n(L) \end{array} \tag{1.2}$$

Indeed, if this diagram commutes for all $g \in G$, then σ will restrict to an isomorphism

$$(A \otimes_K L)^{1\otimes G} \overset{\sigma}{\cong} M_n(L)^G = M_n(K).$$

Conversely, an isomorphism $A \cong M_n(K)$ makes our diagram commute essentially for free because we simply do not care about the G-action.

Remark 1.51. Comparing with Example 1.50, one notes that the isomorphism $\mathbb{H} \otimes_{\mathbb{R}} \mathbb{C} \cong M_2(\mathbb{C})$ cannot be compatible with the Galois action; indeed, any such isomorphism sends (say) i to a matrix whose entries are not purely real.

To check the commutativity of the diagram, we start from $M_n(L)$ and go clockwise. Namely, we are sending $g \in G$ to

$$f(g) \coloneqq g\sigma(1 \otimes g)^{-1}\sigma^{-1} \in \mathrm{Aut}_K(M_n(L)).$$

Explicitly, we want $f(g) = 1$ for all $g \in G$. Now, by the Skolem–Noether theorem, we have $\mathrm{Aut}_L(M_n(L)) \cong \mathrm{PGL}_n(L)$. We now claim that the $f(g) = 1$ condition reduces to a cocycle condition. Indeed,

$$\begin{aligned} f(g_1g_2) &= g_1g_2\sigma\left(1 \otimes g_2^{-1}g_1^{-1}\right)\sigma^{-1} \\ &= g_1g_2\sigma\left(1 \otimes g_2^{-1}\right)\sigma^{-1}\left(1 \otimes g_1^{-1}\right)\sigma\sigma^{-1} \\ &= g_1 f(g_2) f(g_1). \end{aligned}$$

As an aside, we note that our choice of isomorphism σ is only defined up to an automorphism in $\mathrm{PGL}_n(L)$, which one can check will only adjust f by a coboundary. In total, we see that the isomorphism class of A produces a cocycle class in $H^1(G, \mathrm{PGL}_n(L))$.

We can also go from the cocycle straight to the algebra. Indeed, the data of a K-algebra can be written down as some commutative diagrams dealing with A and $\otimes_K$. For example, associativity of our multiplication is the following diagram.

$$\begin{array}{ccc} A \otimes_K A \otimes_K A & \xrightarrow{1\otimes\mu} & A \otimes_K A \\ \downarrow{\scriptstyle \mu\otimes 1} & & \downarrow{\scriptstyle \mu} \\ A \otimes_K A & \xrightarrow{\mu} & A \end{array}$$

In this way, we can upgrade our equivalence $\mathrm{Mod}_K \simeq \mathrm{Mod}(L/K)$ to an equivalence $\mathrm{Alg}(K) \cong \mathrm{Alg}(L/K)$. As such, given our cocycle $f \in H^1(G, \mathrm{PGL}_n(L))$, we build our algebra as $M_n(L)$ equipped with a special G-action by

$$ga = g^{-1}f(g)a,$$

where this action is constructed by basically reading the diagram (1.2) backwards. One can check that this action is G-semilinear and so on, so we are safe.

Remark 1.52. In fact, we have a bijection from $Z^1(G, \mathrm{PGL}_n(L))$ with (classes of) K-algebras A equipped with an isomorphism $\sigma\colon A \otimes_K L \to M_n(L)$.

Let's take a step to H^2 for a moment. There is an exact sequence of G-modules

$$1 \to L^\times \to \mathrm{GL}_n(L) \to \mathrm{PGL}_n(L) \to 1.$$

Thus, even though we are studying $H^1(G, \mathrm{PGL}_n(L))$, we see that we might hope we can understand what's going on in $H^2(G, L^\times)$.

Well, we can just try to compute this like the Snake lemma. Given a cocycle $f\colon G \to \mathrm{PGL}_n(L)$, we can choose some lifted map $\widetilde{f}\colon G \to \mathrm{GL}_n(L)$. Roughly speaking, our element in H^2 will be the obstruction to $\widetilde{f}$ producing a cocycle. As such, we want to compute

$$(g_1, g_2) \mapsto g_1\widetilde{f}(g_2)\widetilde{f}(g_1)\widetilde{f}(g_1g_2)^{-1}.$$

Notably, we can see that this element is trivial in $\mathrm{PGL}_n(L)$ because f is a cocycle, so this must be an element of $L^\times$, meaning that we have described a 2-cocycle in $H^2(G, L^\times)$. One can check that adjusting f by a coboundary or changing the choice of lift does not adjust the class in H^2.

Remark 1.53. It turns out that this describes an isomorphism $\mathrm{Br}(L/K) \cong H^2(G, L^\times)$. Here, $\mathrm{Br}(L/K)$ is a further quotient of algebras where for example A is equivalent to $M_n(A)$.

1.9 February 6

Last class we discussed $H^1(G, \mathrm{PGL}_n(L))$. We continue talking about H^1.

1.9.1 Automorphisms of Projective Space

Roughly speaking, the key point in our discussion of $H^1(G, \mathrm{PGL}_n(L))$ was our application of the Skolem–Noether theorem to show $\mathrm{Aut}_L(M_n(L)) \cong \mathrm{PGL}_n(L)$. In general, one can play a similar game whenever you have some object with the correct automorphisms.

Thus, we also note $\mathrm{Aut}\,\mathbb{P}^{n-1}_L = \mathrm{PGL}_n(L)$. Indeed, for any automorphism α, we can draw the following square.

$$\begin{array}{ccc} \mathbb{P}^{n-1}_L & \xrightarrow{\alpha} & \mathbb{P}^{n-1}_L \\ \downarrow & & \downarrow \\ \mathrm{Spec}\, L & \xrightarrow{\alpha} & \mathrm{Spec}\, L \end{array}$$

Notably, we can see from this square that $\alpha^* \mathcal{O}_{\mathbb{P}^{n-1}_L}(1)$ is ample[1] and needs to generate $\mathrm{Pic}\,\mathbb{P}^{n-1}_L$ because α^* is an isomorphism, so we conclude that there is an isomorphism $\alpha^\flat \colon \alpha^* \mathcal{O}_{\mathbb{P}^{n-1}_L}(1) \to \mathcal{O}_{\mathbb{P}^{n-1}_L}$. (This isomorphism is not canonical!) Thus, taking global sections, we are getting a map

$$\Gamma(\mathbb{P}^{n-1}_L, \mathcal{O}_{\mathbb{P}^{n-1}_L}(1)) \cong \Gamma(\mathbb{P}^{n-1}_L, \mathcal{O}_{\mathbb{P}^{n-1}_L}(1)).$$

However, both of these are isomorphic to $Lx_0 \oplus \cdots L_{x_{n-1}}$, so the data of $(\alpha, \alpha^\flat)$ precisely describes an automorphism $L^n \to L^n$. If you mod out by the information of $\alpha^\flat$, it turns out that you exactly describe an element of $\mathrm{PGL}_n(L)$ instead of $\mathrm{GL}_n(L)$.

It turns out that one can do approximately the same story we gave last class to show that there is a bijection between K-schemes P such that $P \times_{\mathrm{Spec}\, K} \mathrm{Spec}\, L \cong \mathbb{P}^{n-1}_L$ and $H^1(G, \mathrm{PGL}_n(L))$. Proving this is a little harder than last time because it is less obvious that a cocycle will come from K-scheme.

Nonetheless, we note that we now have two identifications of $H^1(G, \mathrm{PGL}_n(L))$, so we should be able to take a central K-algebra A such that $A \otimes_K L \cong M_n(L)$ and produce a K-scheme P. These are called the Brauer–Severi schemes.

Example 1.54. Fix the field extension $\mathbb{C}/\mathbb{R}$ and let $\mathbb{H}$ denote the quaternions, which is the nontrivial element of our H^1. Then it turns out that the corresponding K-scheme P is $V\left(x^2 + y^2 + z^2\right) \subseteq \mathbb{P}^2_k$. Notably, the line bundle $\mathcal{O}_{\mathbb{P}^2_k}(1)$ will pull back to $\mathcal{O}_{\mathbb{P}^1_k}(2)$ because it needs to pull back something with global sections, and then we can also check the dimension of these global sections to complete.

Remark 1.55. One can show that the Brauer–Severi schemes are always projective and embed into $\mathbb{P}^n_K$. In fact, they have a K-point if and only if they are projective!

1.9.2 Moving to H^2

As usual, let L/K be a Galois extension with Galois group G. Recall from last class that we had a short exact sequence

$$1 \to L^\times \to \mathrm{GL}_n(L) \to \mathrm{PGL}_n(L) \to 1,$$

which gave rise (via cocycles!) to a map $\delta_n \colon H^1(G, \mathrm{PGL}_n(L)) \to H^2(G, L^\times)$. It turns out that this fits into an exact sequence (of pointed sets)

$$H^1(G, \mathrm{GL}_n(L)) \to H^1(G, \mathrm{PGL}_n(L)) \xrightarrow{\delta_n} H^2\left(G, L^\times\right),$$

which is a check that we omit.

[1] The ample line bundles in $\mathrm{Pic}\,\mathbb{P}^{n-1}_L$ are precisely the ones with global sections, and $\alpha^* \colon \mathrm{Pic}\,\mathbb{P}^{n-1}_L \to \mathrm{Pic}\,\mathbb{P}^{n-1}_L$ must send a line bundle with global sections to a line bundle with global sections.

Lemma 1.56. Fix everything as above.

(a) $H^1(G, \mathrm{GL}_n(L)) = 1$.

(b) If $n = [L : K]$, then δ_n is surjective.

Does $H^2(GL_n)$ vanish?

Proof. Here we go.

(a) We know from our discussion of Hilbert's theorem 90 that $H^1(G, \mathrm{GL}_n(L))$ is in natural bijection to isomorphism classes n-dimensional L-vector spaces with a given semilinear G-action. However, this category $\mathrm{Mod}(L/K)$ we showed (in Theorem 1.45) is just the K-vector spaces of dimension n, so there is only one up to isomorphism, completing the proof.

(b) This requires a trick. Fix a 2-cocycle $f\colon G^2 \to L^\times$. Working explicitly, we want $\rho\colon G \to \mathrm{GL}_n(L)$ such that

$$f(g, g') = \rho_g \cdot g\rho_{g'} \cdot \rho_{gg'}^{-1},$$

where we have identified $L^\times$ with its image in $\mathrm{GL}_n(L)$. Note that such a ρ grants us a 1-cocycle $\overline{\rho}\colon G \to \mathrm{PGL}_n(L)$ by modding out by $L^\times$ everywhere.

Well, we use an induced module: set $V \coloneqq \mathrm{Mor}(G, L)$, which we note has basis given by $e_s(g) \coloneqq 1_{s=g}(g)$ because G is finite. We may thus define $\rho_g\colon V \to V$ given by $\rho_g\colon e_s \mapsto f(g, s)e_s$. To finish, one can show that this $\rho_\bullet$ satisfies the needed equality. ∎

Corollary 1.57. If $n = [L : K]$, then there is a natural identification with central K-algebras A such that $A \otimes_K \cong M_n(L)$ and elements of $H^2(G, L^\times)$.

Proof. It suffices to show that our δ_n is an isomorphism. This follows directly from Lemma 1.56. ∎

Remark 1.58. In fact, we note that we can fully go backward from a 2-cocycle to its constructed 1-cocycle in $H^1(G, \mathrm{PGL}_n(L))$, and then we know how to turn that data into a central K-algebra A with $A \otimes_K L \cong M_n(L)$.

We are now ready to define the Brauer group.

Definition 1.59 (Brauer group)**.** Fix a Galois extension L/K, we define the *Brauer group* $\mathrm{Br}(L/K)$ as the set of isomorphism classes of central K-algebras A such that $A \otimes_K L \cong M_n(L)$.

We can extend this construction as follows: Corollary 1.57 grants us a natural isomorphism

$$H^2(G, L^\times) \to \mathrm{Br}(L/K).$$

Now, define

$$H^2\left(\mathrm{Gal}(K^{\mathrm{sep}}/K), (K^{\mathrm{sep}})^\times\right) \coloneqq \varinjlim_{K \subseteq L \subseteq K^{\mathrm{set}}} H^2(\mathrm{Gal}(L/K), L^\times).$$

On the other side, define $\mathrm{Br}\, K$ as the central K-algebras A such that $A \otimes_K K^{\mathrm{sep}} \cong M_n(K^{\mathrm{sep}})$ for some n, but we mod out by the equivalence $A \sim B$ if and only if $M_n(A) \cong M_m(B)$ for some n and m. Then one can show that the δ_ns induce an isomorphism

$$\mathrm{Br}\, K \cong H^2\left(\mathrm{Gal}(K^{\mathrm{sep}}/K), (K^{\mathrm{sep}})^\times\right),$$

which allows us to stop paying attention to the field L.

Remark 1.60. One can show that division rings are also in natural bijection with our algebras, giving us yet another identification.

1.10 February 8

We quickly remark on some sources. Our discussion of cohomology roughly follows [GS13] and [Mil20]. For a discussion of the Brauer group, we are roughly following Poonen.

1.10.1 Cohomology of Unramified Extensions

Today we will be discussing the following result; throughout, L/K is a Galois extension of local fields with Galois group G.

Theorem 1.61. Fix a local field K.

(a) For any finite Galois extension L/K with $G \coloneqq \mathrm{Gal}(L/K)$, we have $H^2(G, L^\times) \cong \frac{1}{\#G}\mathbb{Z}/\mathbb{Z}$.

(b) Taking the direct limit, we have $H^2(G_K, (K^{\mathrm{sep}})^\times) \cong \mathbb{Q}/\mathbb{Z}$.

Let's do the archimedean case first.

Lemma 1.62. We compute $H^2(\mathrm{Gal}(\mathbb{C}/\mathbb{R}), \mathbb{C}^\times) \cong \mathbb{Z}/2\mathbb{Z}$.

Proof. Write $G \coloneqq \mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \{1, \sigma\}$, where σ is complex conjugation. Now, recall from Proposition 1.38 that we may compute

$$H^2(G, \mathbb{C}^\times) \cong \widehat{H}^0(G, \mathbb{C}^\times) = \frac{(\mathbb{C}^\times)^G}{\mathrm{N}_G \mathbb{C}^\times} = \frac{\mathbb{R}^\times}{\{|z|^2 : z \in \mathbb{C}^\times\}} = \frac{\mathbb{R}^\times}{\mathbb{R}^+},$$

and this last group is indeed $\mathbb{Z}/2\mathbb{Z}$. ∎

Remark 1.63. Using Proposition 1.38 and Theorem 1.47, we see that

$$\widehat{H}^i(\mathrm{Gal}(\mathbb{C}/\mathbb{R}), \mathbb{C}^\times) \cong \begin{cases} 0 & \text{if } i \text{ is odd,} \\ \mathbb{Z}/2\mathbb{Z} & \text{if } i \text{ is even.} \end{cases}$$

We now move towards Theorem 1.61. Here is our first case.

Remark 1.64. For any extension L/K of local fields with residue field extension λ/κ, the subextension fixed by Frobenius is L^{unr}/K whose residue field extension remains λ/κ. But now L^{unr}/K is an unramified extension, and L/L^{unr} is totally ramified.

With the above remark in mind, our approach will be the following.

1. We will begin with L/K unramified and show $H^2(G, L^\times) = \frac{1}{\#G}\mathbb{Z}/\mathbb{Z}$. The intuition here is that our cohomological contribution will come from these unramified extensions.
2. Next, we will show that L/K being totally ramified yields $H^2(G, L^\times) = 0$.
3. Lastly, we will combine the above two cases accordingly.

Let's go at it. Let's set some notation. Quickly, recall the structure of $K^\times$: let $\pi_K \in \mathfrak{p}_K$ be a uniformizer for K so that $K^\times \cong \pi_K^{\mathbb{Z}} \times \mathcal{O}_K^\times$. However, we can express $\mathcal{O}_K^\times$ by

$$\mathcal{O}_K^\times = \varprojlim (\mathcal{O}_K/\mathfrak{p}_K^n)^\times .$$

Now, we can think about $\mathcal{O}_K^\times$ as decomposed as

$$1 \to \frac{1+\mathfrak{p}_K^{n-1}}{1+\mathfrak{p}_K^n} \to (A/\mathfrak{p}_K^n)^\times \to \left(A/\mathfrak{p}_K^{n-1}\right)^\times \to 1.$$

But now we see that the group on the left here is isomorphic to $(\mathcal{O}_K/\mathfrak{p}_K, +)$ by $a \mapsto 1 + a\mathfrak{p}_K^{n-1}$; one should check this works. There is a similar description for L.

Lemma 1.65. Let L/K be a finite unramified Galois extension of local fields with Galois group G. Then $\widehat{H}^i(G, \mathcal{O}_L^\times) = 0$.

Proof. We compute with Tate cohomology. Because G is generated by the Frobenius, it is cyclic, so there are two computations.

1. We show $H^1(G, \mathcal{O}_L^\times) = 0$. This is easier: indeed, Theorem 1.47 tells us that $H^1(G, L^\times) = 0$, and $\mathcal{O}_L^\times$ is a direct summand of $L^\times$, so we are done.
2. We show $\widehat{H}^0(G, \mathcal{O}_L^\times) = 0$. By definition of Tate cohomology, it's enough to show that the norm map

   $$\mathrm{N}_K^L \colon \mathcal{O}_L^\times \to \mathcal{O}_K^\times$$

   is surjective. Because N_K^L is continuous, so it suffices to show that it has dense image, so we show

   $$\mathrm{N}_K^L \colon \left(\frac{\mathcal{O}_L}{\mathfrak{p}_L^n}\right)^\times \to \left(\frac{\mathcal{O}_K}{\mathfrak{p}_K^n}\right)^\times$$

   is surjective for all n. (This is well-defined because $\mathfrak{p}_L = \mathfrak{p}_K\mathcal{O}_L$ because L/K is unramified!) We show this by induction. Well, for $n = 1$, we are showing that the norm map in an extension of finite fields is surjective. We can do this by hand: for an extension of finite fields $\mathbb{F}_{q^r}/\mathbb{F}_q$, let $g \in \mathbb{F}_{q^r}^\times$ generate so that

   $$N(g) = \prod_{i=0}^{r-1} g^{p^i} = g^{(q^r-1)/(q-1)}$$

   has order $q-1$ and is in $\mathbb{F}_q^\times$ and is thus a generator.

   Then for the inductive step, we draw the following morphism of short exact sequences.

   $$\begin{array}{ccccccccc}
   1 & \longrightarrow & \dfrac{1+\mathfrak{p}_L^n}{1+\mathfrak{p}_L^{n+1}} & \longrightarrow & \left(\dfrac{\mathcal{O}_L}{\mathfrak{p}_L^{n+1}}\right)^\times & \longrightarrow & \left(\dfrac{\mathcal{O}_L}{\mathfrak{p}_L^n}\right)^\times & \longrightarrow & 1 \\
   & & \downarrow & & \downarrow & & \downarrow & & \\
   1 & \longrightarrow & \dfrac{1+\mathfrak{p}_K^n}{1+\mathfrak{p}_K^{n+1}} & \longrightarrow & \left(\dfrac{\mathcal{O}_K}{\mathfrak{p}_K^{n+1}}\right)^\times & \longrightarrow & \left(\dfrac{\mathcal{O}_K}{\mathfrak{p}_K^n}\right)^\times & \longrightarrow & 1
   \end{array}$$

   Here, the vertical maps are all N_K^L. By induction, the right map is surjective, so by the Snake lemma, it suffices to show that the left map is surjective. Well, computing this map, we use the fact that π_K is a uniformizer for L to write

   $$\mathrm{N}_K^L\left(1 + a\pi_K^n\right) = \prod_{\sigma \in G} \left(1 + \sigma(a)\pi_K^n\right) \equiv 1 + \mathrm{T}_K^L(a)\pi_K^n \pmod{1+\mathfrak{p}_L^n}.$$

   Thus, it suffices to show that the trace map is surjective in an extension of finite fields $\mathbb{F}_{q^r}/\mathbb{F}_q$. Equivalently, we want to show that $\widehat{H}^0\left(\mathrm{Gal}(\mathbb{F}_{q^r}/\mathbb{F}_q), \mathbb{F}_{q^r}\right)$ vanishes, which is true because $\mathbb{F}_{q^r}$ is an induced module. ∎

Lemma 1.66. Let L/K be a finite unramified Galois extension of local fields with Galois group G. Then $H^2(G, L^\times) \cong \frac{1}{\#G}\mathbb{Z}/\mathbb{Z}$.

Proof. Because $L^\times \cong \pi_K^{\mathbb{Z}} \times \mathcal{O}_L^\times$, we use Lemma 1.65 to yield

$$H^2(G, L^\times) \cong H^2(G, \pi_K^{\mathbb{Z}}) \times H^2(G, \mathcal{O}_L^\times) \cong H^2(G, \mathbb{Z}),$$

where we are using the fact that π_K is fixed by G. Thus, we want to compute

$$H^2(G, \mathbb{Z}) \cong \widehat{H}^0(G, \mathbb{Z}) = \frac{\mathbb{Z}}{N_G\mathbb{Z}} = \frac{\mathbb{Z}}{\#G\mathbb{Z}},$$

which is what we wanted. ∎

Corollary 1.67. Fix a local field K. Then $H^2(\mathrm{Gal}(K^{\mathrm{unr}}/K), (K^{\mathrm{unr}})^\times) = \mathbb{Q}/\mathbb{Z}$.

Proof. Take direct limits of the above lemma. It is not too hard to check that everything works out here in our transition maps. ∎

1.11 February 10

Today we finish proving that $H^2(\mathrm{Gal}(K^{\mathrm{sep}}/K), K^{\mathrm{sep}\times}) \cong \mathbb{Q}/\mathbb{Z}$.

1.11.1 Cohomology of Ramified Extensions

Quickly, we pick up the following cohomological tool.

Proposition 1.68 (Restriction–inflation)**.** Fix a normal subgroup H of a group G. Given a G-module M such that $H^1(H, M) = H^2(H, M) = 0$, we have

$$H^2\left(G/H, M^H\right) \cong H^2(G, M).$$

Proof. We make a few remarks.

- The functor $(-)^H \colon \mathrm{Mod}_G \to \mathrm{Mod}_{G/H}$ preserves injectives. Indeed, this functor has an exact left adjoint: namely, we want an exact functor $L \colon \mathrm{Mod}_{G/H} \to \mathrm{Mod}_G$ such that any $M \in \mathrm{Mod}_G$ and $S \in \mathrm{Mod}_{G/H}$ has
$$\mathrm{Hom}_G(LS, M) \simeq \mathrm{Hom}_{G/H}\left(S, M^H\right).$$
Well, we simply define LS to be S viewed as a G-module via $G \to G/H$. Namely, a G-module morphism from $S \to M$ must be fixed by H because S is a trivial H-module, so we have really defined a morphism $S \to M^H$ as G/H-modules. Also, observe that L is exact because exactness can be checked in Ab, and we have done nothing to the underlying abelian groups.

  We now show that L tells us we preserve injectives. Well, let I be an injective G-module, and fix some embedding of $S \subseteq S'$ of H-modules. Given some morphism $S \to I^H$, we want to fill in the following arrow.

$$\begin{array}{ccccc} 0 & \longrightarrow & S & \longrightarrow & S' \\ & & & \searrow & \downarrow \\ & & & & I_H \end{array}$$

Hitting this with our exact adjunction, it is equivalent to fill in the following arrow.

$$\begin{array}{ccccc} 0 & \longrightarrow & LS & \longrightarrow & LS' \\ & & & \searrow & \downarrow \\ & & & & I \end{array}$$

However, I is injective, so such an arrow exists.

- We now compute cohomology. We are granted a left-exact sequence as follows.

$$0 \to M \to I^0 \to I^1 \to I^2 \to \cdots.$$

These injective G-modules are also injective H-modules (just write down the diagram), so we can compute group cohomology in G or H by taking cohomology of the above resolution. Namely,

$$\begin{aligned} H^\bullet(H, M) &= H^\bullet\left(I^{0H} \to I^{1H} \to \cdots\right), \\ H^\bullet(G, M) &= H^\bullet\left(I^{0G} \to I^{1G} \to \cdots\right). \end{aligned}$$

Now, because $H^1(H, M) = H^2(H, M)$, we know that

$$0 \to M^H \to I^{0H} \to I^{1H} \to I^{2H} \to I^{3H}$$

is exact, and the previous point tells us that this is the beginning of an injective resolution in $\mathrm{Mod}_{G/H}$. Now computing G/H-invariants, we see that

$$H^2\left(G/H, M^H\right) = \frac{\ker\left((I^{2H})^{G/H} \to (I^{3H})^{G/H}\right)}{\mathrm{im}\left((I^{1H})^{G/H} \to (I^{2H})^{G/H}\right)} = H^2(G, M),$$

which is what we wanted. ∎

Remark 1.69. In the background, this result really comes from a spectral sequence.

We now turn to totally ramified extensions L/K. Speaking philosophically, $H^2(\mathrm{Gal}(L/K), L^\times)$ is a class field theory question, a question about Brauer groups (one can simply translate everything into central simple algebras), or a geometry question via our Brauer–Severi varieties. Let's do geometry.

Lemma 1.70. Fix a totally ramified extension of local fields L/K. Given an $\mathcal{O}_K$-scheme $P_{\mathcal{O}_K}$ such that $P_{\mathcal{O}_L} \cong \mathbb{P}^n_{\mathcal{O}_L}$, we also have $P_{\mathcal{O}_K} \cong \mathbb{P}^n_{\mathcal{O}_K}$.

Proof. We provide a sketch.

1. To begin, one can show there is a closed embedding $P \hookrightarrow \mathbb{P}^M_K$ for some $M > 0$. Roughly speaking, one can pick up a line bundle $\mathcal{L}_{P_L}$ inducing the isomorphism $P_L \cong \mathbb{P}^n_L$, but the cocycle condition allows us to know it takes values in the roots of unity, so taking a large enough power means we induce an embedding to projective K-space. (To work with infinite extensions, we note that specifying such a morphism only needs a finite amount of polynomial data, so it's okay to pass to the colimit.) By abuse of notation, we say $\mathcal{L}_{P_K}$ is the line bundle yielding our embedding.

2. We claim that it is enough to show $P_K(K)$ is nonempty. Indeed, we want to show that there is a line bundle $\mathcal{M}$ on P_K such that $\mathcal{M}^{\otimes \deg \mathcal{L}_{P_K}} \cong \mathcal{L}_{P_K}$, which is enough because $\mathcal{M}$ will induce an isomorphism $P_K \to \mathbb{P}^M_k$, which is good enough.

   Well, we would like to chose $\mathcal{M}_L$ coming from $\mathbb{P}^n_L$ such that $\varepsilon\colon \mathcal{M}^{\otimes \deg \mathcal{L}_{P_K}} \cong \mathcal{L}_{P_L}$ and want it to be compatible with the Galois action, but this need not be the case. Namely, we would like for this morphism to be unique in some sense and therefore compatible with the Galois action. To get rid

of the extraneous automorphisms, we fix $x \in P_K(K)$ and consider pairs of line bundles $(\mathcal{U}, \rho)$ where $\rho\colon k_{\mathcal{U}}(x) \cong K$.

Notably, isomorphisms between such pairs are unique when they exist, but this category of pairs up to isomorphism is still just $\operatorname{Pic} P_K$, even with the tensor product. Reformulating our problem, we are trying to find a line bundle $\mathcal{M}^{\otimes \deg \mathcal{L}_{P_K}} \cong \mathcal{L}_{P_L}$ with the ρ, and this data will now be automatically compatible with the Galois action.

3. Note that having some $P_{\mathcal{O}_K} \subseteq \mathbb{P}^N_{\mathcal{O}_K}$ with $P_{\mathcal{O}_L} \cong \mathbb{P}^n_{\mathcal{O}_L}$ also grants us a B-point $\operatorname{Spec} \mathcal{O}_L \to P_{\mathcal{O}_L}$ by the valuative criterion. This story of our B-point with residue field k will give us a k-point coming from A as well because A and B have the same residue field.

   As such, unwrapping the algebraic geometry, we have a morphism $A \to k$ and a morphism $\widehat{\mathcal{O}}_{P_A,x} \to k$, and we would like to lift this to $\widehat{\mathcal{O}}_{P_A,x} \to A$, which will give us the desired A-point to finish. Well, map $\widehat{\mathcal{O}}_{P_A,x}$ to $\widehat{\mathcal{O}}_{P_k,x}$ and then left elements of $\mathfrak{m}/\mathfrak{m}^2$ to lift back to $\widehat{\mathcal{O}}_{P_A,x}$. This will define a map $A[\![x_\bullet]\!]$ to $\widehat{\mathcal{O}}_{P_A,x}$, which will finish the proof. ∎

1.12 February 13

We hopefully finish discussing $H^2(\operatorname{Gal}(L/K), L^\times)$ for local fields L today.

1.12.1 Finishing H^2

To finish up the computation of H^2, we make a final remark.

Proposition 1.71. Fix a local field K, and let $I \subseteq \operatorname{Gal}(K^{\mathrm{sep}}/K)$ be the kernel of the restriction map $\operatorname{Gal}(K^{\mathrm{sep}}/K) \to \operatorname{Gal}(K^{\mathrm{unr}}/K)$. Then $H^2(I, K^{\mathrm{sep}\times}) = 0$.

Proof. We claim that the image of $H^2(I, \mathcal{O}^\times_{K^{\mathrm{sep}}}) \to H^2(I, K^{\mathrm{sep}\times})$ vanishes. Indeed, fix some class $[f]$ in there, and because we have defined our cohomology as a colimit, it can be exhibited as from some finite extension as

$$[f_L] \in H^2(\operatorname{Gal}(L/K^{\mathrm{unr}}), \mathcal{O}_L^\times).$$

We can now show that $[f_L]$ is in the image of the map $H^1(\operatorname{Gal}(L/K^{\mathrm{unr}}), \mathrm{PGL}_n(\mathcal{O}_L)) \to H^2(\operatorname{Gal}(L/K^{\mathrm{unr}}), L^\times)$ for some n, which will be enough by the usual exact sequence. Indeed, we have a formula: set $n \coloneqq [L : K^{\mathrm{unr}}]$ and $G \coloneqq \operatorname{Gal}(L/K^{\mathrm{unr}})$, and let f_L be the desired cocycle. Then our proof of the vanishing of $H^2(\operatorname{Gal}(L/K^{\mathrm{unr}}), \mathcal{O}_L^\times)$ tells us that we are in fact in the image of $H^1(\operatorname{Gal}(L/K^{\mathrm{unr}}), \mathrm{PGL}_n(\mathcal{O}_L))$; explicitly, we have

$$M \coloneqq \bigoplus_{s \in G} \mathcal{O}_L e_s,$$

where the G-action is given by $\rho_g\colon e_s \mapsto f_L(g,s)$. This M is providing an element of $H^1(\operatorname{Gal}(L/K^{\mathrm{unr}}), \mathrm{PGL}_n(\mathcal{O}_L))$, which produces[2] an $\mathcal{O}_{K^{\mathrm{unr}}}$-scheme P which is isomorphic to $\mathbb{P}^{n-1}_{\mathcal{O}_L}$ over $\mathcal{O}_L$. But then last class we showed that this scheme must have vanishing class, so we are done.

Continuing, we actually claim that the map $H^2(I, \mathcal{O}^\times_{K^{\mathrm{sep}}}) \to H^2(I, K^{\mathrm{sep}\times})$ is surjective. Indeed, we have some exact sequence

$$0 \to \mathcal{O}_{K^{\mathrm{sep}}} \to K^{\mathrm{sep}\times} \xrightarrow{v} \mathbb{Q} \to 0,$$

where v is our valuation. Now, $H^2(I, \mathbb{Q})$ vanishes because $\mathbb{Q}$ is a divisible group (indeed, take any cocycle, using the colimit forces it into a finite extension, and then divisibility causes the cocycle to have vanishing class there). As such, our exact sequence will do the trick here. This finishes the proof. ∎

[2] It turns out that we can just take this as $\mathbb{P}_{\mathcal{O}_L} M$.

Remark 1.72. Let us explain further where $H^i(G,\mathbb{Q})=0$ for any finite group G and $i>0$. Indeed, the point is that the forgetful functor

$$(-)^G\colon \mathrm{Mod}_{\mathbb{Q}[G]}\to \mathrm{Vec}_{\mathbb{Q}}$$

is exact, which is enough because it causes our cohomology to vanish. Well, we note that we have two additive functors

$$M^G \hookrightarrow M \xrightarrow{\frac{1}{\#G}\sum_{g\in G} g} M^G$$

whose composite is the identity. In particular, using our lift, we get a canonical decomposition $M\cong M'\otimes M^G$, which tells us that $(-)^G$ should be an exact functor.

1.12.2 Back to Global Things

Fix an extension of global fields L/K with Galois group G. Given a place v of K, we note that we have a decomposition

$$L\otimes_K K_v\cong \prod_{w\mid v} L_w,$$

where L_w is the completion of L at some place w over v.

Proposition 1.73. Fix everything as above. For fixed L-place $w_0\mid v$, we have a G-module isomorphism

$$L\otimes_K K_v\cong \mathrm{Ind}_{G_{w_0}}^G L_{w_0}.$$

Proof. Recall $\mathrm{Ind}_{G_{w_0}}^G L_{w_0}=\mathrm{Mor}_{G_{w_0}}(G,L_{w_0})$. As such, we choose representatives $g_1,\dots,g_r$ for G/G_{w_0} to see that

$$\mathrm{Ind}_{G_{w_0}}^G L_{w_0}\cong \prod_{i=1}^r L_{w_0}g_i,$$

where the ith component dictates where g_i goes. But now the point is that the right-hand side remains r different copies of the completion L_{w_0}, which is in fact the same as $L\otimes_K K_v$ above. One should check that this commutes with the G-action, but indeed it does. ∎

Remark 1.74. One can replace everything with units as $L_w^\times$.

Corollary 1.75. Fix everything as above. For fixed L-place $w_0\mid v$, we have a canonical isomorphism

$$H^\bullet\left(G,\prod_{w\mid v} L_w^\times\right)\cong H^\bullet(G_{w_0},L_{w_0}^\times).$$

Proof. More generally, given a subgroup $H\subseteq G$, we have the sequence of functors

$$\mathrm{Mod}_H\xrightarrow{\mathrm{Ind}}\mathrm{Mod}_G\xrightarrow{(-)^G}\mathrm{Ab}.$$

Now, the functor Ind is exact and takes injectives to injectives (it has an exact left adjoint given by the restriction functor), so we can compute cohomology for given H-module either directly or by inducing first. The result follows. ∎

1.13 February 15

We continue moving towards the Hasse norm theorem.

1.13.1 Reducing to Cohomology

Recall for a moment that we are interested in proving the Hasse norm theorem, which is roughly the statement that

$$\frac{K^\times}{\mathrm{N}_K^L(L^\times)} \to \prod_v \frac{K_v^\times}{\mathrm{N}_{K_v}^{L_w}(L_w^\times)}$$

is injective for cyclic extensions of global fields L/K, where w is some fixed place over v. Well, using our Tate cohomology, we see that it is enough to show that the map

$$H^2(\mathrm{Gal}(L/K), L^\times) \to \prod_{v \in V_K} H^2(\mathrm{Gal}(L_w/K_v), L_w^\times)$$

is injective. The point here is to write down the short exact sequence

$$1 \to L^\times \to \mathbb{A}_L^\times \to \mathbb{A}_L^\times / L^\times \to 1,$$

where $\mathbb{A}_L^\times$ are the idéles. This grants us the exact sequence in cohomology given by

$$H^1(G, \mathbb{A}_L^\times / L^\times) \to H^2(G, L^\times) \to H^2(G, \mathbb{A}_L^\times).$$

But now we note

$$\mathbb{A}_L^\times = \operatorname*{colim}_{S \subseteq V_K} \mathbb{A}_{L,S_L}^\times,$$

where S_L refers to the pre-image of S under the restriction map $V_L \to V_K$. Notably, this is also an isomorphism of G-modules because we are looking at S_L-idéles. In particular, we have the following.

Proposition 1.76. Fix a finite Galois extension of global fields L/K. Then any $i \geq 0$ has

$$H^i(G, \mathbb{A}_L^\times) \cong \bigoplus_{v \in V_K} H^i(G_w, L_w^\times),$$

where w is some fixed place over v.

Proof. The point here is that we can write

$$H^i(G, \mathbb{A}_L^\times) = H^i\left(G, \operatorname*{colim}_{S \subseteq V_K} \mathbb{A}_{L,S_L}^\times\right) = \operatorname*{colim}_{S \subseteq V_K} H^2(G, \mathbb{A}_{L,S_L}^\times),$$

where this last equality holds by just checking by hand: indeed, there is of course a map from the left to the right by taking the given cocycle and pretending it is a colimit of cocycles; the inverse map simply says that any colimit of cocycles on the right can only have some bounded denominators because we're merely looking at a map $G^2 \to \mathbb{A}_{L,S_L}^\times$ to write down our cocycles.

Expanding this out, we get to write

$$H^i(G, \mathbb{A}_L^\times) = \operatorname*{colim}_{S \subseteq V_K} \left(\prod_{v \in S} H^i\left(G, \prod_{w|v} L_w^\times\right) \times \prod_{v \notin S} H^i\left(G, \prod_{w|v} \mathcal{O}_w^\times\right)\right).$$

Now, the arguments of Corollary 1.75, we see $\prod_{w|v} \mathcal{O}_w^\times = \mathrm{Ind}_{G_w}^G \mathcal{O}_w^\times$ and similar for $L_w^\times$, so this becomes

$$H^i(G, \mathbb{A}_L^\times) = \operatorname*{colim}_{S \subseteq V_K} \left(\prod_{v \in S} H^i(G, L_w^\times) \times \prod_{v \notin S} H^i(G_w, \mathcal{O}_w^\times)\right).$$

Now, for unramified places v, we see that $H^i(G_w, \mathcal{O}_w^\times)$ vanishes by Lemma 1.65, so by throwing those places in S, we may ignore them. Thus, we get

$$H^i(G, \mathbb{A}_L^\times) = H^i(G, \mathbb{A}_L^\times) = \operatorname*{colim}_{S \subseteq V_K} \prod_{v \in S} \prod_{v \in S} H^2(G_w, L_w^\times) = \bigoplus_{w \in V_L} H^2(G_v, L_v^\times),$$

which is what we wanted. ■

Remark 1.77. Passing to the separable closure, we see

$$\operatorname*{colim}_{K \subseteq L \subseteq K^{\text{sep}}} H^2(\text{Gal}(L/K), \mathbb{A}_L^\times)$$

is $\bigoplus_{v<\infty} \mathbb{Q}/\mathbb{Z}$ plus some finite number of $\frac{1}{2}\mathbb{Z}/\mathbb{Z}$ factors coming from infinite places.

Remark 1.78. Tracking through the above proof shows that the map $H^2(G, L^\times) \to H^2(G, \mathbb{A}_L^\times)$ factors into the map

$$H^2(G, L^\times) \to \bigoplus_v H^2(G_w, L_w^\times) \to \prod_{v \in V_K} H^2(G_w, L_w^\times).$$

In particular, we are getting that an element of $H^2(G, L^\times)$ vanishes in all but finitely many $H^2(G_w, L_w^\times)$ for free! Relating this back to our geometry, we are essentially saying that a K-quadratic form has a K_v-point for all but finitely many places v. But this is exactly Theorem 1.28, which we were able to show more directly.

Thus, we see that we want the map $H^2(G, L^\times) \to H^2(G, \mathbb{A}_L^\times)$ to be injective, so we see that what we really want to show is that $H^1(G, \mathbb{A}_L^\times / L^\times)$ vanishes from our exact sequence, which we will do eventually.

Remark 1.79. Note that the term before $H^1(G, \mathbb{A}_L^\times / L^\times)$ in our long exact sequence is

$$H^1(G, \mathbb{A}_L^\times) = \bigoplus_{v \in V_K} H^1(G_w, L_w^\times) = 0$$

from Proposition 1.76, so the kernel of $H^2(G, L^\times) \to H^2(G, \mathbb{A}_L^\times)$ is indeed exactly $H^1(G, \mathbb{A}_L^\times / L^\times)$.

Unfortunately, showing $H^1(G, \mathbb{A}_L^\times / L^\times)$ vanishes is genuinely difficult. Let's do it.

1.13.2 Cohomology of Cyclic Groups

We are going to want the following definition.

Definition 1.80 (Herbrand quotient)**.** Fix a finite cyclic group G and a G-module M. Because $\widehat{H}^\bullet(G, M)$ is 2-periodic, it is helpful to define the *Herbrand quotient*

$$h(G, M) := \frac{\#H^2(G, M)}{\#H^1(G, M)}$$

when these cohomology groups are finite.

Remark 1.81. In some sense, this is a "multiplicative" variant of the topological Euler characteristic.

Lemma 1.82. Fix a finite cyclic group G and a finite G-module M. Then $h(G, M) = 1$.

Proof. Set $G = \langle \sigma \rangle \cong \mathbb{Z}/n\mathbb{Z}$. We are interested in computing the cohomology of the complex

$$M \xrightarrow{T} M \xrightarrow{N} M \xrightarrow{T} M \to \cdots,$$

where $T = (\sigma - 1)$ and $N = N_G$.

- If $M^G = 0$, then the map T has $\ker T = M^G = 0$, so T is an isomorphism because M is finite. Further, $\operatorname{im} N_G \subseteq M^G = 0$, so $N = 0$. As such, we may compute our cohomology as $\widehat{H}^{-1}(G, M) = \widehat{H}^0(G, M) = 0$ via Tate cohomology.
- If $M^G = M$, then here T is the zero map, and N is the multiplication-by-n map, so we may compute

  $$\widehat{H}^{-1}(G, M) = \ker(n \colon M \to M) \qquad \text{and} \qquad \widehat{H}^0(G, M) = \frac{M}{nM}.$$

  Using the classification of finite abelian groups, these both have the same size.
- To finish the proof, we use induction on M. In particular, we have an exact sequence

  $$0 \to M^G \to M \to M' \to 0.$$

  If $M^G = 0$ or $M^G = M$, then the above cases finish. Otherwise, both M^G and M' have strictly smaller cardinality, so the multiplicativity of the Herbrand quotient tells us that $h(G, M) = h(G, M^G)h(G, M') = 1$, which is what we wanted. ∎

Remark 1.83. In particular, if you have an exact sequence like

$$0 \to M' \to M \to M'' \to 0,$$

then you get $h(G, M')h(G, M'') = h(G, M)$. This basically comes straight from the long exact sequence.

1.14 February 17

The homework is killing me.

1.14.1 Applications of Herbrand Quotients

Fix a finite cyclic group G. We continue discussing Herbrand quotients.

Corollary 1.84. Fix a finite extension of finite fields ℓ/κ with Galois group G. Then $H^2(G, \ell^\times) = 0$.

Proof. Note G is cyclic because these are finite fields, and $\ell^\times$ is finite, so $h(G, \ell^\times) = 1$. However, $H^1(G, \ell^\times) = 0$ by Hilbert's theorem 90, so it follows that $H^2(G, \ell^\times) = 0$ for free. ∎

Remark 1.85. This implies that the Brauer group over k vanishes, by taking the colimit over all ℓ/k.

Corollary 1.86. Fix a cyclic group G. Then let V be finite-dimensional G-representation over a field $\mathbb{Q}$. Given G-stable lattices $M_1, M_2 \subseteq V$, we have $h(G, M_1) = h(G, M_2)$.

Here, a lattice is a free $\mathbb{Z}$-submodule with $\mathbb{Z}$-rank equal to the dimension of V.

Proof. Let M_i have basis $\{v_{ij}\}_{j=1}^n$, where $n = \dim V$. Notably, we can write

$$v_{2i} = \sum_{j=1}^{n} c_{ij} v_{1j}$$

for some c_{ij}. Letting N be the product of the denominators of the c_{ij}, we see that multiplication by N grants an inclusion $N\colon M_1 \to M_2$. Thus, we get an exact sequence

$$0 \to M_1 \xrightarrow{N} M_2 \to M_2/NM_1 \to 0.$$

Notably, tensoring this with $\mathbb{Q}$ makes the left an isomorphism, so M_2/NM_1 must be a torsion abelian group which is finitely generated, implying that it must be finite. Thus, $h(G, M_2/NM_1) = 1$, so $h(G, M_1) = h(G, M_2)$ follows. ∎

Remark 1.87. One can actually describe G-representations for cyclic groups G somewhat concretely; let $G = \langle \sigma \rangle$ have order n. Namely, given a ring R, we would like to discuss $R[G]$-modules, where we see

$$R[G] = \frac{R[\sigma]}{(\sigma^n - 1)}.$$

For example, if R contains a primitive nth root of unity ζ (and R has characteristic not dividing p), then

$$R[G] \cong \prod_{i=1}^{n} \frac{R[\sigma]}{(\sigma - \zeta)} \cong R^n.$$

Thus, an $R[G]$-module is essentially just a direct sum of n different R-modules $M_1, \dots, M_n$, and then the G-action on M_i is given by $\sigma \mapsto \zeta^i$.

Remark 1.88. One can use the previous remark to show that $M_1 \otimes_K \Omega \cong M_2 \otimes_K \Omega$ implies that $M_1 \cong M_2$, when $K \subseteq \Omega$ is an inclusion of fields. Roughly speaking, the point is that we can decompose M_1 into a direct sum as described above, if we have enough roots of unity, then we are basically prescribing dimension at each graded component.

1.14.2 Herbrand Quotient Computation

We are going to show that $h(G, \mathbb{A}_L^\times / L^\times) = n$, when L/K is a cyclic extension of global fields of degree n.

Lemma 1.89. Fix an extension of global fields L/K. Then there exists a finite set of places T such that $\mathbb{A}_L^\times = L^\times \cdot \mathbb{A}_{L,T}^\times$ so that $\mathbb{A}_L^\times / L^\times = \mathbb{A}_{L,T}^\times / L^\times$.

Proof. The point is to hit all the ideal classes. Fix a set of places $S \subseteq V_K$ satisfying the following conditions.

- S contains the archimedean places.
- The finite part of S_L, made of primes $\{\mathfrak{P}_1, \dots, \mathfrak{P}_n\}$, generates the ideal class group of L.

In particular, the class group of L is finite, so we can find a finite set $S \subseteq V_K$ satisfying the above conditions.

We now set $T \coloneqq S_L$. Let's show this works. Fix an idéle $(\alpha_w)_{w \in V_L} \in \mathbb{A}_L^\times$. Then

$$\prod_{w<\infty} \mathfrak{P}_w^{\mathrm{val}_w(\alpha_w)}$$

is an ideal equivalent to some product

$$I \coloneqq \prod_{i=1}^{r} \mathfrak{P}_r^{v_r}.$$

In other words, there is $\beta \in L^\times$ such that $\mathrm{val}_w(\beta) = \mathrm{val}_w(\alpha_w) - \mathrm{val}_w(I)$. Choosing uniformizers $\pi_w \in \mathfrak{p}_w$, we note

$$\beta \cdot \left(\pi_w^{\mathrm{val}_w(I)}\right)_w$$

has the same valuation as α at every place w. In particular, the quotient lives in $\mathbb{A}_{L,\varnothing}^\times$, so we are now safe. ■

Remark 1.90. Note that making T larger does not hurt us, so we may assume that T is G-stable.

At the end of the day, we have a diagram which looks like the following.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathcal{O}_{L,T}^\times & \longrightarrow & \mathbb{A}_{L,T}^\times & \longrightarrow & \mathbb{A}_{L,T}^\times/\mathcal{O}_{L,T}^\times & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & L^\times & \longrightarrow & \mathbb{A}_L^\times & \longrightarrow & \mathbb{A}_L^\times/L^\times & \longrightarrow & 0 \end{array}$$

The induced morphism on the right is injective by the Snake lemma, and we note that the map $\mathbb{A}_{L,T}^\times \to \mathbb{A}_L^\times/L^\times$ is surjective by the lemma, so in fact the induced morphism on the right is also surjective. Thus, $\mathbb{A}_L^\times/L^\times = \mathbb{A}_{L,T}^\times/\mathcal{O}_{L,T}^\times$. (Here, $\mathcal{O}_{L,T}^\times$ are the T-units, which are the elements of $L^\times$ with vanishing valuation outside T.)

Remark 1.91. The arguments of Proposition 1.76 also tell us that

$$H^\bullet(G, \mathbb{A}_{L,S_L}^\times) = \prod_{v \in S} H^\bullet(G_w, L_w^\times) \times \prod_{w \notin S} H^\bullet(G_w, \mathcal{O}_w^\times),$$

and the right product vanishes if, for example, S contains the places of K which ramify over L.

1.15 February 22

Let's try to show global class field theory in a week.

1.15.1 The First Inequality

Fix a finite cyclic extension of global fields L/K with Galois group G. Last time we showed $\mathbb{A}_L^\times/L^\times = \mathbb{A}_{L,T}^\times/\mathcal{O}_{L,T}^\times$, where T is some sufficiently large G-equivariant subset of V_L. In particular, we want T to contain the archimedean places and to generate the class group. Thus, we have an exact sequence

$$1 \to \mathcal{O}_{L,T}^\times \to \mathbb{A}_{L,T}^\times \to \mathbb{A}_L^\times/L^\times \to 1,$$

so

$$h(G, \mathbb{A}_L^\times/L^\times) = \frac{h(G, \mathbb{A}_{L,T}^\times)}{h(G, \mathcal{O}_{L,T}^\times)}, \tag{1.3}$$

provided that these Herbrand quotients are finite. In fact, we can see that these are finite from the following proof: indeed, we have a long exact sequence as follows.

$$\begin{array}{ccccc} H^1(G,\mathcal{O}_{L,T}^\times) & \longrightarrow & H^1(G,\mathbb{A}_{L,T}^\times) & \longrightarrow & H^1(G,\mathbb{A}_L^\times/L^\times) \\ \uparrow & & & & \downarrow \\ H^2(G,\mathbb{A}_L^\times/L^\times) & \longrightarrow & H^2(G,\mathbb{A}_{L,T}^\times) & \longrightarrow & H^2(G,\mathcal{O}_{L,T}^\times) \end{array}$$

In particular, we are going to compute $h(G,\mathbb{A}_{L,T}^\times)$ and $h(G,\mathcal{O}_{L,T}^\times)$ on the nose, from which finiteness of $h(G,\mathbb{A}_L^\times/L^\times)$ also will follow. Let's see this.

Theorem 1.92. Fix a finite cyclic extension of global fields L/K with Galois group G, and choose a subset $S \subseteq V_K$ containing the archimedean and ramified places with $T \coloneqq S_L$.

(a) We have
$$h\left(G,\mathbb{A}_{L,T}^\times\right) = \prod_{v\in S} n_v,$$
where $n_v = [L_w : K_v]$ for a chosen place $w \in V_L$ over $v \in V_K$.

(b) We have
$$h\left(G,\mathcal{O}_{L,T}^\times\right) = \prod_{v\in S} n_v.$$

Proof. Quickly, note that the extension being Galois implies that $n_v = e(w/v)f(w/v)$ does not depend on the choice of w, so our products are well-defined. We show these one at a time.

(a) Observe that
$$\mathbb{A}_{L,T}^\times = \prod_{v\in S}\left(\prod_{w|v} L_w^\times\right) \times \prod_{v\notin S}\left(\prod_{w|v}\mathcal{O}_w^\times\right).$$
In particular, this is
$$\mathbb{A}_{L,T}^\times = \prod_{v\in S} \operatorname{Ind}_{G_w}^G L_w^\times \times \prod_{v\notin S} \operatorname{Ind}_{G_w}^G \mathcal{O}_w^\times,$$
where w is a chosen place over v. Taking cohomology and using Corollary 1.75, this is
$$H^\bullet(G,\mathbb{A}_{L,T}^\times) = \prod_{v\in S} H^\bullet(G_w,L_w^\times) \times \prod_{v\notin S} H^\bullet(G_w,\mathcal{O}_w^\times).$$
Because S contains all ramified places, we see that $H^\bullet(G_w,\mathcal{O}_w^\times) = 0$ always by Lemma 1.65, so we have left to compute the left product. Taking Herbrand quotients now, we see
$$H^\bullet(G,\mathbb{A}_{L,T}^\times) = \prod_{v\in S} h(G_w,L_w^\times),$$
so we appropriately claim that $h(G_w,L_w^\times) = n_v$, so we need a little more local class field theory.

By the usual exact sequence
$$1 \to \mathcal{O}_w^\times \to L_w^\times \to \mathbb{Z} \to 0,$$
we see $h(G_w,L_w^\times) = h(G_w,\mathbb{Z})h(G_w,\mathcal{O}_w^\times) = n_v h(G_w,\mathcal{O}_w^\times)$, so we want $h(G_w,\mathcal{O}_w^\times) = 1$. Our argument that $H^1(G_w,\mathcal{O}_w^\times) = 0$ for free, so we want to show $H^2(G_w,\mathcal{O}_w^\times) = 0$, which one can again check by going to residue fields. Roughly speaking, the Brauer–Severi variety argument from Lemma 1.70 still works, where we are now inputting the fact that the Brauer group of our extension of finite fields is trivial, which is certainly true from our computation of its Herbrand quotient in Lemma 1.82.

(b) Roughly speaking, the point is that $\mathcal{O}_{L,T}^\times$ will embed as a lattice into $V_\mathbb{R}$, where $V = \operatorname{Mor}(T, \mathbb{Z})$. (The G-action on V is given by $(gf)(t) = f\left(g^{-1}t\right)$.) Namely, our embedding $\iota\colon \mathcal{O}_{L,T}^\times \to V_\mathbb{R}$ is given by

$$\iota\colon x \mapsto (\log |x|_w)_{w\in T}.$$

This is of course a homomorphism, and Dirichlet's unit theorem tells us that the $\ker \iota$ is finite and that the image Λ is a lattice of the hyperplane

$$\sum_{w\in T} x_w = 0,$$

which comes from the product formula and recognizing that $\iota(x)$ is trivial on places outside T. Notably, we have a decomposition

$$V_\mathbb{R} = \Lambda_\mathbb{R} \oplus \mathbb{R}(1,\dots,1)$$

in fact of G-modules. (Indeed, both modules on the right are G-submodules of $V_\mathbb{R}$.) Setting $\Lambda' \coloneqq \Lambda \oplus \mathbb{Z}(1,\dots,1)$, we see $\Lambda'_\mathbb{R} = V_\mathbb{R}$.

We now compute. Note $h(G, \mathcal{O}_{L,T}^\times) = h(G,\Lambda)$ because their quotient is finite and contributes nothing by Lemma 1.82. On the other hand, we see $h(G,\Lambda') = h(G,\Lambda)h(G,\mathbb{Z}) = nh(G,\Lambda)$, so

$$nh(G,\mathcal{O}_{L,T}^\times) = h(G,\Lambda')$$

by rearranging. On the other hand, we note

$$V = \prod_{v\in S}\left(\prod_{w|v}\mathbb{Z}\right),$$

so

$$H^\bullet(G,V) = \prod_{v\in S} H^\bullet(G_w,\mathbb{Z})$$

by Corollary 1.75 as usual. Thus,

$$h(G,V) = \prod_{v\in S} h(G_w,\mathbb{Z}) = \prod_{v\in S} n_v.$$

Combining, we see we want to show $h(G,\Lambda') = h(G,V)$. However, these are both lattices of this real vector space, so with this in mind, it will be enough to give a G-module isomorphism $\Lambda' \otimes_\mathbb{Z} \mathbb{Q} \cong V \otimes_\mathbb{Z} \mathbb{Q}$ by Corollary 1.86. Well, using the fact our vector spaces are finite-dimensional, we compute

$$\operatorname{Hom}_{\mathbb{Q}[G]}(\Lambda'_\mathbb{Q}, V_\mathbb{Q}) \cong ((\Lambda'_\mathbb{Q})^\vee \otimes_\mathbb{Q} V_\mathbb{Q})^G = \ker\left((1-\sigma)\colon (\Lambda'_\mathbb{Q})^\vee \otimes_\mathbb{Q} V_\mathbb{Q} \to (\Lambda'_\mathbb{Q})^\vee \otimes_\mathbb{Q} V_\mathbb{Q}\right),$$

where $\sigma \in G$ is the generator. However, taking the kernel commutes with taking the tensor product with a field because these kernel computations can just look at bases, so we might as well be computing the kernel of

$$(1-\sigma)\colon (\Lambda'_\mathbb{R})^\vee \otimes_\mathbb{R} V_\mathbb{R} \to (\Lambda'_\mathbb{R})^\vee \otimes_\mathbb{R} V_\mathbb{R},$$

which we do know is isomorphic to $\operatorname{Hom}_{\mathbb{R}[G]}(\Lambda'_\mathbb{R}, V_\mathbb{R})$. However, we do now know that there is an isomorphism α in this last group, so we produce an element

$$\sum_{i=1}^n \beta_i \otimes v_i \in (\Lambda'_\mathbb{Q})^\vee \otimes_\mathbb{Q} V_\mathbb{R}$$

which corresponds to an $\mathbb{R}$-isomorphism. Selecting the v_i to be rational vectors sufficiently close to v_i, we may assume that the determinant of the corresponding linear map remains nonzero (as it is in the above case), so we get to pull back to the desired $\mathbb{Q}$-isomorphism $\Lambda'_\mathbb{Q} \cong V_\mathbb{Q}$. ∎

Corollary 1.93. Fix a finite cyclic extension of global fields L/K with Galois group G, and choose a subset $S \subseteq V_K$ containing the archimedean places with $T \coloneqq S_L$ and generating the ideal class group of L. Then $h\left(G, \mathbb{A}_L^\times / L^\times\right) = n$. In particular, it is finite.

Proof. This follows from the above theorem, combined with (1.3). ∎

1.16 February 24

We finish showing global class field theory. Fix a cyclic extension of global fields L/K with Galois group G. We want to show that $\widehat{H}^1(G, \mathbb{A}_L^\times/L^\times)$ vanishes, so because $h(G, \mathbb{A}_L^\times/L^\times) = n$, it suffices to show that $\widehat{H}^0(G, \mathbb{A}_L^\times/L^\times) \le n$. This is the second inequality.

Remark 1.94. The remainder of the proof will be quite technical. Roughly speaking Herbrand quotients play well in short exact sequences (like Euler characteristics), but getting an individual cohomology group is harder.

1.16.1 Remark on Restriction

We are going to want a little more group cohomology to continue. Fix a finite group G and a subgroup $H \subseteq G$. We have the following result.

Proposition 1.95. Fix a finite group G and a subgroup $H \subseteq G$. Then Ind_H^G is both a left and right adjoint for Res_H^G.

Proof. This proof is somewhat technical, but it's fairly direct. We have to provide the following natural transformations.

- There is a map $N \to \operatorname{Res}_H^G \operatorname{Ind}_H^G N$ for any H-module N. Well, this map is just given by $f \mapsto f(1)$.
- There is a map $\operatorname{Res}_H^G \operatorname{Ind}_H^G N \to N$ for any G-module N. Well, this map is just given by $f \mapsto f(1)$.
- There is a map $M \to \operatorname{Ind}_H^G \operatorname{Res}_H^G M$ for any G-module M. Well, this map is just given by $m \mapsto (g \mapsto gm)$.
- There is a map $\operatorname{Ind}_H^G \operatorname{Res}_H^G M \to M$ for any G-module M. Well, this map is just given by
$$\sum_{gH \in G/H} gfg^{-1}.$$
In particular, the H-invariance of f implies that the choice of coset representative gH does not matter.

We omit the adjunction checks. ∎

Remark 1.96. Note that the composition
$$M \to \operatorname{Ind}_H^G \operatorname{Res}_H^G M \to M$$
is simply multiplication by $[G : H]$. In particular, if H is the trivial subgroup, then the middle term vanishes, so we see that $H^\bullet(G, M)$ should be n-torsion.

Corollary 1.97. Fix a finite group G and a Sylow p-subgroup H. Then the map
$$H^\bullet(G, M)[p^\infty] \xrightarrow{\operatorname{Res}} H^\bullet(H, M)[p^\infty]$$
is injective.

Proof. Note the composite
$$H^\bullet(G, M)[p^\infty] \xrightarrow{\operatorname{Res}} H^\bullet(H, M)[p^\infty] \to H^\bullet(G, M)[p^\infty]$$
is multiplication by $[G : H]$, which is coprime to p, so this composite is an isomorphism. Thus, the left map is injective. ∎

Remark 1.98. Roughly speaking, it will be beneficial to go down to Sylow p-subgroups because these are solvable, so one can imagine we can then reduce to cyclic subgroups with some effort.

1.16.2 The Second Inequality

We are now ready for our main theorem.

Theorem 1.99. Fix a Galois extension of number fields L/K with Galois group G.

(a) $\left[\mathbb{A}_K^\times : K^\times \operatorname{N}_K^L(\mathbb{A}_L^\times)\right]$ is finite and divides $[L:K]$.

(b) $H^1(G, \mathbb{A}_L^\times / L^\times) = 0$.

(c) $H^2(G, \mathbb{A}_L^\times / L^\times)$ is finite with order dividing $[L:K]$.

Remark 1.100. Note that $\mathbb{A}_K^\times / K^\times N_K^L(\mathbb{A}_L^\times) = \widehat{H}^0(G, \mathbb{A}_L^\times/L^\times)$. To see this, we stare at the usual short exact sequence

$$1 \to L^\times \to \mathbb{A}_L^\times \to \mathbb{A}_L^\times / L^\times \to 1.$$

Because $H^1(G, L^\times) = 0$, this gives rise to the exact sequence

$$\frac{K^\times}{\operatorname{N}_K^L L^\times} \to \frac{\mathbb{A}_K^\times}{\operatorname{N}_K^L \mathbb{A}_L^\times} \to \widehat{H}^0(G, \mathbb{A}_L^\times/L^\times) \to 0,$$

so the claim follows.

Reductions. Let's provide some reductions.

- If G is cyclic then the above are all equivalent. Indeed, (a) and (c) are equivalent by periodicity of cohomology. Further, we see (c) is equivalent to $\#\widehat{H}^0(G, \mathbb{A}_L^\times/L^\times) \le n$. But this is equivalent to $\#\widehat{H}^1(G, \mathbb{A}_L^\times/L^\times) \le 1$ because $h(G, \mathbb{A}_L^\times/L^\times) = n$ here. However, this last inequality is equivalent to $\widehat{H}^1(G, \mathbb{A}_L^\times/L^\times) = 0$, which is (b).
- We reduce to the case where G is a p-group. Indeed, let $H \subseteq G$ be a Sylow p-subgroup. If we are given the theorem in the case L/L^H (where here the Galois group is a p-group), then we conclude by restricting via Corollary 1.97 that

  $$\#\widehat{H}^i(G, \mathbb{A}_L^\times/L^\times)[p^\infty] \le \#\widehat{H}^i(H, \mathbb{A}_L^\times/L^\times) \le \left[L : L^H\right] = \#H,$$

  so the order of p dividing $\widehat{H}^i(G, \mathbb{A}_L^\times/L^\times)$ is less than or equal to the order of p dividing $[L:K]$. Because the cohomology is $[L:K]$-torsion, we conclude that these are the only primes we have to worry about, so the theorem for p-groups (each of (a), (b), and (c)) implies the theorem in general by taking $i \in \{0,1,2\}$ by these injections.
- We reduce to the case where $G \cong \mathbb{Z}/p\mathbb{Z}$. Indeed, if not, by the proof of the Sylow theorems, we may assume G is a p-group, and there is a nontrivial proper normal subgroup $H \subseteq G$ such that we have the theorem for the extensions L/L^H and L^H/K.

  Let's start with (b). By Restriction–Inflation, we know that $H^1(G, \mathbb{A}_L^\times/L^\times) = 0$ will imply that

  $$H^1(G, \mathbb{A}_L^\times/L^\times) \cong H^1\left(G/H, (\mathbb{A}_L^\times/L^\times)^H\right) = H^1\left(G/H, \mathbb{A}_{L^H}^\times/(L^H)^\times\right),$$

  which vanishes because we know the theorem on the extension L^H/K. To see the last equality above, we can take H-invariants of the exact sequence

  $$1 \to L^\times \to \mathbb{A}_L^\times \to \mathbb{A}_L^\times/L^\times \to 1$$

to see $\mathbb{A}_{L^H}^\times/(L^H)^\times \cong (\mathbb{A}_L^\times/L^\times)^H$ because $H^1(H, L^\times) = 0$.

For (a), we see

$$\mathbb{A}_L^\times \supseteq K^\times \operatorname{N}_K^{L^H}(\mathbb{A}_{L^H}^\times) \supseteq K^\times \operatorname{N}_K^L(\mathbb{A}_L^\times),$$

and the left index is appropriately bounded by $[L^H : K]$, so it suffices to show that the right index is bounded by $[L : L^H]$. Well, for our bound, we know that the index

$$\mathbb{A}_{L^H}^\times \supseteq L^{H\times} \operatorname{N}_{L^H}^L(\mathbb{A}_L^\times)$$

divides $[L : L^H]$. Well, taking $\operatorname{N}_K^{L^H}$ of this inclusion, we see that the index of

$$\operatorname{N}_K^{L^H}(\mathbb{A}_{L^H}^\times) \supseteq \operatorname{N}_K^{L^H}(L^{H\times}) \operatorname{N}_K^{L^H}(\mathbb{A}_L^\times)$$

will still divide $[L : L^H]$ because there is a surjection from the previous quotient to this quotient. Thus, the index of

$$K^\times \operatorname{N}_K^{L^H}(\mathbb{A}_{L^H}^\times) \supseteq K^\times \operatorname{N}_K^{L^H}(\mathbb{A}_L^\times)$$

still divides $[L^H : K]$ because again there is a surjection from this above quotient to this one. This finishes.

Lastly, for (c), one looks at the long exact sequence and does some tricky thing.

- We can even reduce to the case where $\mu_p \in K$. We omit the details of this reduction. Roughly speaking, adjoining μ_p replaces K with an extension coprime to p, so because we are interested in showing that $\left[\mathbb{A}_K^\times : K^\times \operatorname{N}_K^L(\mathbb{A}_L^\times)\right]$ divides some smallish power of p, so adding in these factors coprime to p do not affect the argument. ∎

1.17 February 27

Today we hope to finish global class field theory but very fast.

1.17.1 Tate's Theorem

We are going to want the following result.

Theorem 1.101 (Tate). Fix a finite group G and a G-module M. Suppose that each subgroup $H \subseteq G$ satisfies the following conditions.

- $H^1(H, M) = 0$.
- $H^2(H, M)$ is cyclic of order $\#H$.

Then, for each r, there is an isomorphism $\widehat{H}^r(G, \mathbb{Z}) \cong \widehat{H}^{r+2}(G, M)$.

Proof. We provide a sketch. Roughly speaking, we are going to want to combine two different boundary maps. In particular, the short exact sequence

$$0 \to I_G \to \mathbb{Z}[G] \to \mathbb{Z} \to 0$$

tells us that $\widehat{H}^r(G, \mathbb{Z}) \cong \widehat{H}^{r+1}(G, I_G)$. We are now a single index away. Thus, we want to construct a short exact sequence

$$0 \to M \to \mathcal{E} \to I_G \to 0,$$

where $\mathcal{E}$ the boundary maps $\widehat{H}^{r+1}(G, I_G) \cong \widehat{H}^{r+2}(G, M)$ are isomorphisms.

Yoneda ext?

Fix a 2-cocycle $\varphi\colon G^2 \to M$ representing a generator of $H^2(G,M)$. Now, as an abelian group, we set

$$\mathcal{E} \coloneqq M \oplus I_G = M \oplus \bigoplus_{g \in G \setminus \{e\}} \mathbb{Z} x_g.$$

We need to give $\mathcal{E}$ a G action. For this, we define

$$h \cdot x_g \coloneqq x_{hg} - x_h + \varphi(h,g),$$

where $x_1 \coloneqq \varphi(1,1)$. One can check that this does in fact define a G-action. In particular, one can compute that the map $G \to I_G$ given by $g \mapsto x_g$ goes to the generator of $H^2(G,M)$ under the correct boundary map. One can finish by checking that our boundary maps are isomorphisms, which is good enough. ■

Example 1.102. Given a Galois extension of local fields L/K, then we see that the G-module $L^\times$ satisfies the above conditions by our discussion of local class field theory. In particular, $H^1(H,M)$ vanishes by Hilbert's theorem 90, and being cyclic followed from our rather lengthy and difficult computation. Then Theorem 1.101 promises us an isomorphism

$$G^{\mathrm{ab}} \cong \frac{I_G}{I_G^2} = H_1(G, I_G) = \widehat{H}^{-2}(G,\mathbb{Z}) \cong \widehat{H}^0(G, L^\times) = \frac{K^\times}{\mathrm{N}_K^L(L^\times)}.$$

In particular, if $G \cong \mathbb{Z}/p\mathbb{Z}$, then we see that taking pth powers kills our equivalence classes, so they must be norms.

Gaussian rationals?

1.17.2 Finishing the Second Inequality

We are now in the case where L/K has Galois group $\langle \gamma \rangle \cong \mathbb{Z}/p\mathbb{Z}$, and K contains μ_p. We thus claim that $L = K(\alpha^{1/p})$ for some $\alpha \in K^\times$. This is Kummer theory. Well, for some homomorphism $\chi\colon \langle\gamma\rangle \to \mu_p$, and set

$$W_\chi \coloneqq \{\alpha \in L : g\alpha = \chi(g)\alpha\}.$$

We claim that each of these W_χ is one-dimensional and have direct sum equal to L. For this, it's enough to check over an $\Omega \coloneqq \overline{K}$. Namely, we are looking for an isomorphism

$$\prod_{\sigma\colon L \hookrightarrow \Omega} \Omega \cong \bigoplus_\chi W_\chi \otimes_K \Omega,$$

and we can check this directly. In particular, we see $\mathrm{Hom}(\langle\gamma\rangle, \mu_p) \cong \mathbb{Z}/p\mathbb{Z}$, so we can decompose everything appropriately. Namely, pulling back elements of $\mathbb{Z}/p\mathbb{Z}$ allows us to recover elements of W_χ to make these one-dimensional and so on.

We are now interested in showing

$$\left[\mathbb{A}_K^\times : K^\times \, \mathrm{N}_K^L(\mathbb{A}_L^\times)\right] \mid \#G = p.$$

Thus, we want to show that we have "lots" of norms in $\mathbb{A}_K^\times$. As usual, choose a (large) finite subset $S \subseteq V_K$ satisfying the following constraints.

- S contains the infinite places.
- S contains the places lying over $(p) \in V_{\mathbb{Q}}$.
- S contains the places where α is not a unit.

Now, we consider the (large) field $M \coloneqq K(\sqrt[p]{\mathcal{O}_{K,S}^\times})$, which is finite over K because $\mathcal{O}_{K,S}^\times$ is finitely generated by Dirichlet's unit theorem. In fact, carefully tracking the unit theorem allows us to see $[M : K] = p^{\#S}$. Additionally, M/K is unramified outside S by checking at each place.

We are going to want the following result, quickly.

Lemma 1.103. Fix an abelian extension of number fields L/K. Suppose we have a subgroup $D \subseteq \mathbb{A}_K^\times$ contained in $\mathrm{N}_K^L(\mathbb{A}_L^\times)$ such that $K^\times D$ is dense in $\mathbb{A}_K^\times$. Then $L = K$.

Proof. We sketch. Roughly speaking, $D \subseteq \mathrm{N}_K^L(\mathbb{A}_K^\times)$ and our density result forces the groups

$$\frac{K_v}{\mathrm{N}_{K_v}^{L_w}(L_w^\times)}$$

to be small, for any place v lying under a place w. However, we do have a lower bound on this size from the first inequality (or alternatively, from local class field theory), so we will force $L = K$. ∎

As an application, one can use Example 1.102 and the above lemma to show that $\mathrm{Gal}(M/L)$ is generated by Frobenius elements Frob_v for various $v \notin S$. Notably, these Frobenius elements exist because M/K is unramified.

As such, we may find $T \subseteq V_K$ disjoint from S such that the Frobenius elements Frob_v for $v \in T$ generate $\mathrm{Gal}(M/L)$. We are now equipped to write down

$$E \coloneqq \prod_{v\in S} K_v^{\times p} \times \prod_{v\in T} K_v^\times \times \prod_{v\notin S\cup T} \mathcal{O}_v^\times.$$

The main claim, now, is that $E \subseteq \mathrm{N}_K^L(\mathbb{A}_L^\times)$. We go factor-by-factor.

- Given $v \in S$, we know that pth powers are norms by Example 1.102.
- For $v \in T$, our choice of T enforces $L_w = K_v$. In particular, the local Frobenius element of M/L is going to be the same as the local Frobenius element of M/K, so the extensions at L and K must coincide.
- For $v \notin S \cup T$, our extension is unramified, so we see that all units are norms.

In particular, we see that $\left[\mathbb{A}_K^\times : K^\times \mathrm{N}_K^L(\mathbb{A}_L^\times)\right]$ is divisible by $\left[\mathbb{A}_K^\times : K^\times E\right]$, so we might as well work with E. We can now compute

$$\left[\mathbb{A}_K^\times : K^\times E\right] = \frac{\left[\mathbb{A}_{K,S\cup T}^\times : E\right]}{\left[\mathcal{O}_{K,S\cup T}^\times : K^\times \cap E\right]},$$

roughly speaking by examining how E interacts with the idéles. One can now compute that $\left[\mathbb{A}_{K,S\cup T}^\times : E\right] = p^{2\#S}$ and $\left[\mathcal{O}_{K,S\cup T}^\times : K^\times \cap E\right] = p^{\#S+(\#S-1)}$, so the quotient is in fact size p. This completes the proof.

Remark 1.104. Combining with the first inequality, we must actually have $K^\times E = K^\times \mathrm{N}_K^L(\mathbb{A}_L^\times)$, which roughly tells us what our norms are.

THEME 2

ELLIPTIC CURVES

2.1 March 1

Let's talk about curves. Our language will follow [Har77, Chapter II, IV]. One can in theory just follow the classical language of [Sil09].

2.1.1 Introducing Curves

The definition of a curve in [Har77] is as follows.

Definition 2.1 (curve)**.** Fix an algebraically closed field k. Then a *k-curve* X is a 1-dimensional, integral, smooth, projective k-scheme.

Example 2.2. Fix an algebraically closed field k and a homogeneous polynomial $f \in k[x,y,z]$. Given that $\partial F/\partial x$ and $\partial F/\partial y$ and $\partial F/\partial z$ and F do not all simultaneously vanish, then $V(F) \subseteq \mathbb{P}^2_k$ is a field.

We would like to relax the requirement that k is algebraically closed.

Definition 2.3 (geometrically integral)**.** An S-scheme X is *geometrically integral* if and only if $X \times_S T$ is integral for any S-scheme T.

Definition 2.4 (curve)**.** Fix a field k. Then a *k-curve* is a 1-dimensional, geometrically integral, smooth, projective k-scheme.

Remark 2.5. Equivalently, we can require our curves to just be curves over an algebraically closed field over base-change to an algebraic closure. Roughly speaking, these properties are preserved by base-change and also local on the target with respect to flat base-change, so one can go back and forth.

Remark 2.6. As an aside, note that smoothness implies "locally integral," meaning that there is an open cover of integral domains. (One can check this locally.) Thus, connectedness here is equivalent to irreducible because we are already integral.

Many of the proofs we do will work by first taking a base-change to an algebraic closure and appealing to [Har77].

2.1.2 Divisors

Throughout, we fix a regular k-scheme X.

Definition 2.7 (divisor)**.** The *divisor group* on a regular k-scheme X, denoted $\mathrm{Div}(X)$, is the free abelian group on the closed points of X.

Note that being one-dimensional and integral implies that X has only closed points and a single generic point. We would like to define degree, but one must be a little careful because we are trying to relax algebraically closed hypotheses.

Example 2.8. Note (x^2+1) is a closed point of $\mathbb{A}^1_{\mathbb{R}} = \operatorname{Spec}\mathbb{R}[x]$. However, after base-changing by $\mathbb{C}$, we get the following diagram.

$$\begin{array}{ccccc} \operatorname{Spec}\dfrac{\mathbb{C}[x]}{(x^2+1)} & \longrightarrow & \operatorname{Spec}\mathbb{C}[x] & \longrightarrow & \operatorname{Spec}\mathbb{C} \\ \downarrow & & \downarrow & & \downarrow \\ \operatorname{Spec}\dfrac{\mathbb{R}[x]}{(x^2+1)} & \longrightarrow & \operatorname{Spec}\mathbb{R}[x] & \longrightarrow & \operatorname{Spec}\mathbb{R} \end{array}$$

The point here is that $\operatorname{Spec}\mathbb{C}[x]/(x^2+1)$ is two copies of $\mathbb{C}$! As such, we morally should count the divisor (x^2+1) as "containing" two closed points. Of course, the issue here is that the residue field of (x^2+1) is a degree-2 extension of $\mathbb{R}$.

Definition 2.9 (degree)**.** Fix a finite type, regular k-scheme X. The *degree* of a divisor

$$\sum_{p\in X}[k(p):k]n_p p$$

is $\sum_{p\in X} n_p$. Note this defines a homomorphism $\mathrm{Div}(X)\to\mathbb{Z}$.

Remark 2.10. We are assuming that, for a closed point p, the extension $k(p)/k$ is finite. Roughly speaking, one can see this affine-locally: $k(p)$ is the quotient of some finitely generated k-algebra $k[x_1,\dots,x_n]$ by a maximal ideal, which by some kind of Hilbert's Nullstellensatz will be a finite extension of k.

Remark 2.11. The point is that, for a field k, we have a homomorphism $\mathrm{Div}(X)\to\mathrm{Div}(X_{\overline{k}})$ by sending a point $p\in X$ to the points in the pre-image of the base-change map $X_{\overline{k}}\to X$ as a subscheme, and our definition shows that the following diagram commutes.

$$\begin{array}{ccc} \mathrm{Div}(X) & & \\ \downarrow & \searrow^{\deg} & \\ \mathrm{Div}(X_{\overline{k}}) & \xrightarrow[\deg]{} & \mathbb{Z} \end{array}$$

Indeed, the claim is that, for a closed point $p\in X$, the number of points $q\in X_{\overline{k}}$ (counted with multiplicity) which map down to $p\in X$ is the degree of the extension $k(p)/k$. I think one can just check this affine-locally.

Example 2.12. Let's try a purely inseparable extension. Take $X = \mathbb{A}^1_k = \operatorname{Spec} k[x]$ where $k = \mathbb{F}_p(t)$ for some prime p. Then we have the closed point given by $(x^p - t)$, and it has degree p. Here, our base-change diagram is as follows.

$$\begin{array}{ccccc}
\operatorname{Spec} \dfrac{\overline{\mathbb{F}_p(t)}[x]}{\left(x - t^{1/p}\right)^p} & \longrightarrow & \operatorname{Spec} \overline{\mathbb{F}_p(t)}[x] & \longrightarrow & \operatorname{Spec} \overline{\mathbb{F}_p(t)} \\
\downarrow & & \downarrow{\scriptstyle \pi} & & \downarrow \\
\operatorname{Spec} \dfrac{\mathbb{F}_p(t)[x]}{(x^p - t)} & \longrightarrow & \operatorname{Spec} \mathbb{F}_p(t)[x] & \longrightarrow & \operatorname{Spec} \mathbb{F}_p(t)
\end{array}$$

In particular, π^{-1} of our divisor $(x^p - t)$ goes to p copies of $\left(x - t^{1/p}\right)$. (Namely, one can look at the corresponding quasicoherent ideal sheaf of our closed embedding.)

2.1.3 Divisor Classes

We note that elements of $K(X)$ produce divisors as well.

Definition 2.13 (principal)**.** Fix a k-curve X. Given $f \in K(X)^\times$, we define the *principal divisor* by

$$\operatorname{div} f \coloneqq \sum_{p \in X} \operatorname{ord}_p(f),$$

where $\operatorname{ord}_p(f)$ is the valuation of f in the discrete valuation ring $\mathcal{O}_{X,p}$.

Note that the locations where f vanishes is some closed subscheme of X not equal to X and therefore dimension 0 and therefore finite. Arguing similarly to the locations f of negative valuation, we see that $\operatorname{div} f$ does in fact have finite support and will provide us with a divisor.

Lemma 2.14. Fix a k-curve C. Given any $f \in K(C)$, we have $\deg \operatorname{div} f = 0$.

Proof. We simply base-change to $\overline{k}$ and then appeal to [Har77]. Indeed, observe that the following diagram commutes.

$$\begin{array}{ccccc}
K(X)^\times & \xrightarrow{\operatorname{div}} & \operatorname{Div} X & \xrightarrow{\deg} & \mathbb{Z} \\
\downarrow & & \downarrow & & \| \\
K(X_{\overline{k}})^\times & \xrightarrow{\operatorname{div}} & \operatorname{Div} X_{\overline{k}} & \xrightarrow{\deg} & \mathbb{Z}
\end{array}$$

However, the bottom composite is the zero map by [Har77], so the top composite is also the zero map. ∎

As such, we have a class group.

Definition 2.15 (divisor class)**.** Fix a k-curve X. The quotient

$$\operatorname{Cl} X \coloneqq \frac{\operatorname{Div} X}{\{\operatorname{div} f : f \in K(X)^\times\}}$$

is called the *divisor class group* of X. Note that Lemma 2.14 implies that we have a well-defined degree map.

Remark 2.16. We quickly recall that $\operatorname{Cl} X \cong \operatorname{Pic} X$ by sending a divisor D to the line bundle

$$\mathcal{O}_X(D)(U) \coloneqq \left\{ f \in K(X)^\times : f|_U + D \geq 0 \right\}.$$

As such, one can roughly tell this entire story in terms of line bundles, which is perhaps more intuitive in some aspects.

2.2 March 3

Let's get started.

2.2.1 The Riemann–Roch Theorem

We are now ready to state the Riemann–Roch theorem.

Theorem 2.17 (Riemann–Roch)**.** Fix a k-curve X. There exists an integer $g \in \mathbb{Z}$ such that, for each line bundle $\mathcal{L}/X$, we have

$$h^0(X, \mathcal{L}) - h^0(X, \mathcal{L}^\vee \otimes \Omega^1_X) = \deg \mathcal{L} + 1 - g.$$

Here, $h^i(X, \mathcal{L}) = \dim_k H^i(X, \mathcal{L})$.

Remark 2.18. One definition of our "genus" g is $g \coloneqq h^0\left(X, \Omega^1_X\right)$.

Example 2.19. Taking $\mathcal{L} = \Omega^1_X$ gives $h^0(X, \Omega^1_X) - h^0(X, \mathcal{O}_X) = \deg \Omega^1_X + 1 - g$, so we see $\deg \Omega^1_X = 2g-2$.

Example 2.20. In all applications, we are going to ensure that $h^1(X, \mathcal{L})$ vanishes. By Serre duality, we see that $h^1(X, \mathcal{L}) = h^0\left(X, L^\vee \otimes \Omega^1_X\right) = \dim_k(\mathcal{L}^\vee \otimes \Omega^1_X)(X)$, which will vanish if

$$\deg\left(\mathcal{L}^\vee \otimes \Omega^1_X\right) = \deg \Omega^1_X - \deg \mathcal{L} \overset{?}{<} 0.$$

In other words, if $\deg \mathcal{L} > \deg \Omega^1_X = 2g - 2$, then $h^0(X, \mathcal{L}) = \deg \mathcal{L} + 1 - g$.

To continue our discussion, we will want to talk about complete linear systems.

Proposition 2.21. Fix a line bundle $\mathcal{L}$ on a k-curve X. Then $(\Gamma(X, \mathcal{L}) \setminus \{0\})/k^\times$ is in natural bijection with effective divisors D such that $\mathcal{O}_X(D) \cong \mathcal{L}$.

Proof. Given some $s \in \Gamma(X, \mathcal{L}) \setminus \{0\}$, we note that s produces a map $s \colon \mathcal{O}_X \to \mathcal{L}$, and because s is nonzero, this map is injective by checking at stalks: for each $x \in X$, then we have the commutative diagram as follows.

$$\begin{array}{ccc} \mathcal{O}_{X,x} & \xrightarrow{s_x} & \mathcal{L}_x \\ \downarrow & & \downarrow \\ K(X) & \xrightarrow{s_\eta} & \mathcal{L}_\eta \end{array}$$

Here, η is the generic point of X. Now, s being nonzero implies that s_η is nonzero in $K(X)$, so the bottom map is injective, so the top map should also be injective.

Now, for any closed point $x \in X$, our map at stalks $s_x \colon \mathcal{O}_{X,x} \to \mathcal{L}_x$ has $\mathcal{L}_x$ equal to some free module of rank 1, so by pulling back a uniformizer makes this map multiplication by some uniformizer $\pi_x^{n_x}$. We now set

$$\operatorname{div}_{\mathcal{L}}(s) \coloneqq \sum_{x \in X} n_x x,$$

and we note that $s|_x$ is trivial at only finitely many points, so this divisor's coefficients vanish for all but finitely many points. We now see that $s \colon \mathcal{O}_X \to \mathcal{L}$ tells us that this map is identified with the inclusion

$$\mathcal{L} \otimes \bigoplus_{x \in X} \mathcal{I}_x^{n_x} \to \mathcal{L}$$

by just checking at stalks everywhere (indeed, on the left, we are trivial at every point), so we conclude that $\mathcal{L} \cong \mathcal{O}_X(\operatorname{div}_{\mathcal{L}}(s))$.

To finish the bijection, we note that adjusting our s by an element of $k^\times$ will not change $\operatorname{div}_{\mathcal{L}}(s)$, and we can check that our map is both injective and surjective as such. We omit the rest of these checks. ∎

Example 2.22. If $\deg \mathcal{L} < 0$, then there are no effective divisors D with $\mathcal{L} \cong \mathcal{O}_X(D)$ because $\deg D \geq 0$ for all effective divisors D. Thus, we must have $\Gamma(X, \mathcal{L}) = 0$.

Example 2.23. If $\deg \mathcal{L} = 0$, then we see that the only effective divisor of degree 0 is $D = 0$, so we either have $\mathcal{L} \cong \mathcal{O}_X$ and so $\Gamma(X, \mathcal{L}) = 1$, or we have $\Gamma(X, \mathcal{L}) = 0$.

Example 2.24. In the case of $g = 1$, one sees that $\deg \Omega^1_X = 0$ and so $\deg \mathcal{L} = 1$ implies $\dim_k \mathcal{L}(X) = 1$. Roughly speaking, it follows that $\mathcal{L} \cong \mathcal{O}_X(p)$ for some closed point $p \in X$ with residue field k. Thus, there is a unique effective divisor D (of degree 1) such that $\mathcal{L} \cong \mathcal{O}_X(D)$, so we see that $D = p$ for some point p of residue field k. As such, $\mathcal{L} \cong \mathcal{O}_X(p)$.

The following special case will be important for us.

Theorem 2.25. Fix a k-curve X of genus 1. Then the map $X(k) \to \operatorname{Pic}^1(X)$ sending a point $x \in X$ to $\mathcal{O}_X(x)$ is a bijection. Here, Pic^1 refers to the degree-1 line bundles.

Proof. We show this in pieces.

- We show surjectivity. Fix a line bundle $\mathcal{L} \in \operatorname{Pic}^1(X)$ of degree 1. Then Example 2.24 tells us that $\mathcal{L} \cong \mathcal{O}_X(x)$ for some $x \in X$ with residue field k. We note that having residue field k is equivalent to being a k-point: on one hand, a k-point is a morphism $x \colon \operatorname{Spec} k \to X$ must induce the identity on $\operatorname{Spec} k$ with the structure morphism $\operatorname{Spec} k \to X \to \operatorname{Spec} k$, so we see that the residue field at x must be k. And conversely, if x has residue field k, then we immediately induce our morphism $x \colon \operatorname{Spec} k(x) \to X$.
- We show injectivity: suppose that $x, y \in X(k)$ grant $\mathcal{O}_X(x) = \mathcal{O}_X(y)$. Well, suppose $x \neq y$. This implies that we have an isomorphism $\mathcal{O}_X \cong \mathcal{O}_X(x - y)$. In particular, $1 \in \Gamma(X, \mathcal{O}_X)$ is mapped to some $f \in K(X)$ such that f has a pole at x and a zero at y. In particular, this gives a nonconstant map of degree 1 given by $f \colon X \to \mathbb{P}^1_k$ by taking the corresponding map $X \setminus \{y\} \to \mathbb{A}^1_k$ and extending it to $\mathbb{P}^1_k$. However, this requires that f is an isomorphism of curves, which is a contradiction because $g(X) \neq g(\mathbb{P}^1_k)$. ∎

Remark 2.26. In fact, we see that the injectivity argument holds for any k-curve X of nonzero genus.

2.2.2 Elliptic Curves

We are now ready to define elliptic curves.

Definition 2.27 (elliptic curve)**.** Fix a field k. An *elliptic curve* is a pair (E, e) where E is a k-curve of genus 1 and $e \in E(k)$.

Remark 2.28. Fix an elliptic curve (E, e) over a field k. The idea here is that we have a bijection $\mathrm{Pic}^1(E) \to \mathrm{Pic}^0(E)$ given by $\mathcal{L} \mapsto \mathcal{L} \otimes \mathcal{O}_E(-e)$, so combining with Theorem 2.25 tells us that $E(k)$ is in bijection with the abelian group $\mathrm{Pic}^0(E)$. In particular, $E(k)$ has the structure of an abelian group with identity element given by e!

Remark 2.29. Even when $g(X) > 1$, we note that the previous remark grants an inclusion $X(k) \hookrightarrow \mathrm{Pic}^0(X)$. Now, $X(k)$ does not inherit a group law, so we are perhaps motivated to simply work with the group $\mathrm{Pic}^0(X)$. Indeed, it turns out that there is a notion of the "Jacobian" which is an abelian variety with k-points given by $\mathrm{Pic}^0(X)$.

Remark 2.30. When $g(X) = 1$, even with no k-point in $X(k)$, then there is some scheme-theoretic isomorphism $X \cong \mathrm{Pic}^1(X)$, where now we see $\mathrm{Pic}^1(X)$ has some action by $\mathrm{Pic}^0(X)$. We will return to this later in the course.

The group law on Remark 2.28 can be made explicit via the "chord and tangent" method. For concreteness, write our elliptic curve as

$$E \colon y^2 = x^3 + Ax + B,$$

where E really refers to the projective variety in $\mathbb{P}^2_k$ of the corresponding homogenized polynomial. One ought to check smoothness and genus and so on, but we won't bother for the time being. Notably, our marked point $e \in E(k)$ is given by $[0 : 1 : 0] \in E$.

Now, fixing some $p, q \in E(k)$, we let L denote the line connecting them. One can explicitly do the algebra to see that $X \cap L$ will have three intersection points—writing L as $y = mx + b$, we see $m, b \in k$, so plugging in for

$$x^3 + Ax + B - (mx + b)^2 = 0$$

with roots given by p_x and q_x will have a third root $r_x \in k$. One can check that the corresponding point $(r_x, r_y) \in X(k)$ has $p + q = (r_x, -r_y)$, which describes our group law rather explicitly. The point is that adding together the three points coming from $X \cap L$ ought to vanish in the group law because all divisors of the form $X \cap L$ are linearly equivalent.

2.3 March 6

Good morning everyone.

2.3.1 Elliptic Curves as Cubics

Fix an elliptic k-curve (E, e). We want to view (E, e) as a planar curve of degree 3. Here is our claim.

Proposition 2.31. Fix an elliptic k-curve (E, e). Then the line bundle $\mathcal{O}_E(3e)$ determines a closed embedding $E \hookrightarrow \mathbb{P}^2_k$ of degree 3. In particular, we factor through $V(F)$ for some homogeneous cubic polynomial F.

Proof. We show our checks in sequence.

- Note that $h^0(E, \mathcal{O}_E(3e)) = 3$ by Example 2.20, so we will induce a projective morphism $E \to \mathbb{P}^2_k$ by choosing our three basis vectors. Equivalently, we can choose these three basis vectors as a surjective map $\mathcal{O}_E^3 \twoheadrightarrow \mathcal{O}_E$. In some sense, it is more natural to think about our projective morphism as $E \to \mathbb{P}\Gamma(E, \mathcal{O}_E(3e))$ sending $p \in E$ to the quotient map $\Gamma(E, \mathcal{O}_E(3e)) \to \mathcal{O}_E(3e)_p/\mathfrak{m}_p$. In particular, this quotient map uniquely determines an element of $\mathbb{P}\Gamma(E, \mathcal{O}_E(3e))$ due to the choice of basis of the one-dimensional k-vector space $\mathcal{O}_E(3e)_p/\mathfrak{m}_p$.

  The quick way to show that we are very ample is to note that any two points $p, q \in E$ grant

  $$h^0(E, \mathcal{O}_E(3e - p - q)) = 1 = h^0(E, \mathcal{O}_E(3e)) - 2,$$

  so the corresponding projective morphism separates points and tangent vectors and therefore induces a closed embedding.

  Technically we ought to show that $\mathcal{O}_E(3e)$ is very ample. To show that we are generated by global sections, we need surjectivity of the corresponding map on points given by

  $$\Gamma(E, \mathcal{O}_E(3e)) \otimes_k k(p) \to \mathcal{O}_E(3e)_p/\mathfrak{m}_p.$$

  Really, we need the map to be nonzero because the target is one-dimensional. Note that by base-changing E to $E_{k(p)}$, we can assume that p is a k-point. As such, we note that we have the exact sequence

  $$0 \to \mathcal{O}_E(3e - p) \to \mathcal{O}_E(3e) \to \mathcal{O}_E(3e)_p/\mathfrak{m}_p \to 0$$

  by tensoring up the exact sequence $0 \to \mathcal{I}_p \to \mathcal{O}_E \to k(p) \to 0$ with the locally free and hence flat sheaf $\mathcal{O}_E$. Taking global sections produces the exact sequence

  $$0 \to \Gamma(E, \mathcal{O}_E(3e - p)) \to \Gamma(E, \mathcal{O}_E(3e)) \to \mathcal{O}_E(3e)_p/\mathfrak{m}_p,$$

  but Example 2.20 tells us that $\dim_k \Gamma(E, \mathcal{O}_E(3e - p)) = 2 < 3 = \dim_k \Gamma(E, \mathcal{O}_E(3e))$, so the kernel is not full, so our map is nonzero, which is what we wanted.

- We now check that our projective morphism is a closed embedding. For this, we must check that we separate points and tangent vectors. Because E is a proper scheme (it's projective), to separate points, it is enough to check that two points go to different places in our projective space. Well, checking where two points $p, q \in E$ land, we are claiming that we are producing the same quotient map

  $$\Gamma(E, \mathcal{O}_E(3e)) \twoheadrightarrow \mathcal{O}_E(3e)_p/\mathfrak{m}_p \qquad \text{and} \qquad \Gamma(E, \mathcal{O}_E(3e)) \twoheadrightarrow \mathcal{O}_E(3e)_q/\mathfrak{m}_q.$$

  By a base-change of E, we may again assume that our points are k-rational. Now, above we computed the kernel of this map, so we would be requiring

  $$\Gamma(E, \mathcal{O}_E(3e - p)) \cap \Gamma(E, \mathcal{O}_E(3e - q)) = \Gamma(E, \mathcal{O}_E(3e - p - q))$$

  to be 2-dimensional, but in fact this is 1-dimensional by Example 2.20, so there is nothing to say here.

  Now, to separate tangent vectors, we want to see that the map

  $$\Gamma(E, \mathcal{O}_E(3e)) \to \Gamma(E, \mathcal{O}_E(3e)/(\mathcal{I}_p\mathcal{I}_q))$$

  is surjective, but again our dimensions jump appropriately by Example 2.20, so we must be surjective.

- Choose a basis for $V \coloneqq \Gamma(E, \mathcal{O}_E(3e))$ named $\{u, v, w\}$, so $\mathbb{P}\Gamma(E, \mathcal{O}_E(3e)) \cong \mathbb{P}^2_k$ with basis given by $\{u, v, w\}$. We now note that we have the inclusions

  $$\Gamma(E, \mathcal{O}_E) = \Gamma(E, \mathcal{O}_E(e)) \subsetneq \Gamma(E, \mathcal{O}_E(2e)) \subsetneq \Gamma(E, \mathcal{O}_E(3e))$$

  by Example 2.20. As such, we let $\{z\}$ denote a basis of $\Gamma(E, \mathcal{O}_E)$, and then we extend it to a basis $\{z, x\}$ of $\Gamma(E, \mathcal{O}_E(2e))$, and again we extend it to a basis $\{z, x, y\}$ of $\Gamma(E, \mathcal{O}_E(3e))$. Going up further require some more care.

- We see $\Gamma(E, \mathcal{O}_E(4e))$ has basis $\{z, x, y, x^2\}$, which are linearly independent because they have different valuations at e.
- Similarly, we see $\Gamma(E, \mathcal{O}_E(5e))$ has basis $\{z, x, y, x^2, xy\}$.
- However, $\Gamma(E, \mathcal{O}_E(6e))$ has basis $\{z, x, y, x^2, xy, y^2, x^3\}$, but we have dimension 6, so there must be a relation now.

Thus, we get to write down a relation between $\{z, x, y, x^2, xy, y^2, x^3\}$, which after multiplying through by the "scalar" z enough times grants us a homogeneous polynomial $F \in k[x, y, z]$ of degree 3 dictating this relation.

As such, for each $p \in X$, we see that $F \in \Gamma(E, \mathcal{O}_E(6e))$ will vanish in $\mathcal{O}_E(6e)_p/\mathfrak{m}_p$, so it follows from the construction of the map $E \to \mathbb{P}V$ that the image lands in $V(F)$. ■

2.4 March 8

Today we talk about algebraic geometry.

2.4.1 Group Schemes

Fix an elliptic k-curve (E, e). We are going to want to upgrade our group structure on $E(k)$ to a group scheme.

Definition 2.32 (group scheme)**.** Fix an S-scheme X. Then X, equipped with multiplication $\mu\colon X \times_S X \to X$ and identity $e\colon S \to X$ and inverse $\iota\colon X \to X$ morphisms, is a *group scheme* if and only if the following squares commute.

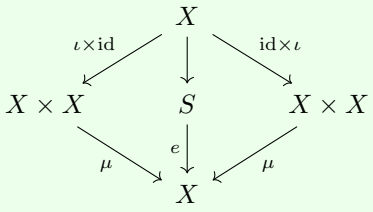
- Associativity.

$$\begin{array}{ccc} X \times_S X \times_S X & \xrightarrow{\mu \times \mathrm{id}_X} & X \times_S X \\ {\scriptstyle \mathrm{id}_X \times X}\downarrow & & \downarrow{\scriptstyle \mu} \\ X \times_S X & \xrightarrow{\mu} & X \end{array}$$

- Identity.

$$\begin{array}{ccccc} S \times_S X & = & X & = & X \times_S S \\ {\scriptstyle e \times \mathrm{id}_X}\downarrow & & \| & & \downarrow{\scriptstyle \mathrm{id}_X \times e} \\ X \times_S X & \xrightarrow{\mu} & X & \xleftarrow{\mu} & X \times_S X \end{array}$$

- Inverse.



We are not going to check these directly. Instead, we will adopt a functor-of-points point of view.

Roughly speaking, for an S-scheme X to take on a group scheme structure, it is enough for $h_X := \mathrm{Mor}_S(-, X)$ to lift to a contravariant functor $h_X^{\mathrm{ab}}\colon \mathrm{Sch}_S^{\mathrm{op}} \to \mathrm{Ab}$. This comes from the Yoneda lemma.

Theorem 2.33 (Yoneda)**.** Fix a category $\mathcal{A}$ and an object $A \in \mathcal{A}$. Then the functor taking $A \mapsto \mathrm{Mor}_{\mathcal{A}}(-, A)$ defined on $\mathcal{A} \to \mathrm{Fun}(\mathrm{Sch}_S^{\mathrm{op}}, \mathrm{Set}$ is fully faithful.

Proof. Omitted. ■

We will also want the fact that $\mathrm{Hom}(-, X \times_S Y) = \mathrm{Hom}(-, X) \times_{\mathrm{Hom}(-,S)} \mathrm{Hom}(-, Y)$, which is more or less the definition of the fiber product.

For example, let's construct our multiplication map. In particular, there is an addition map $\mu^{\mathrm{ab}} \colon h_X^{\mathrm{ab}} \times h_X^{\mathrm{ab}} \Rightarrow h_X^{\mathrm{ab}}$ because we are in the category of abelian groups. In particular, this map is given by the addition map

$$\mu_T^{\mathrm{ab}} \colon h_X^{\mathrm{ab}}(T) \times h_X^{\mathrm{ab}}(T) \to h_X^{\mathrm{ab}}(T).$$

Now, μ will produce a unique scheme morphism $\mu \colon X \times_S X \to X$ by the Yoneda lemma. A similar recipe gives us the inversion morphism $\iota \colon X \to X$ and the identity element, and the faithfulness of the Yoneda lemma allows us to lift diagrams satisfied by the natural transformations to diagrams satisfied by our scheme morphisms.

Remark 2.34. In fact, because we are outputting h_X^{ab} to Ab, we are in fact producing an abelian group structure on E.

So with our elliptic k-curve (E, e), we would like to upgrade our isomorphism

$$E(k) \cong \mathrm{Pic}^0(E)$$

to some isomorphism of schemes. The issue here is that we need to upgrade Pic to a functor.

Notation 2.35. Given S-schemes X and T, we define $X_T \coloneqq X \times_S T$.

Lemma 2.36. Fix an elliptic k-curve (E, e). Given a k-scheme S and a line bundle $\mathcal{L}$ on E_S, the function $s \mapsto \deg(\mathcal{L}|_{E_s})$ is locally constant on S.

Proof. We refer to [Har77, Theorem III.9.9]. ■

As such, to upgrade Pic to a scheme, we may try to define the functor $S \mapsto \mathrm{Pic}^0(E_S)$. This doesn't work: letting $\pi_S \colon E_S \to S$ denote the projection, it turns out to be problematic that line bundles $\mathcal{L}$ on S produce locally trivial line bundles $\pi_S^* \mathcal{L} \in \mathrm{Pic}^0(E_S)$. Roughly speaking, there now too many objects which look like the identity.

To fix this, we have the following definition.

Definition 2.37 (rigidified line bundle)**.** Fix an elliptic k-curve (E, e). Given a k-scheme S, a *rigidified line bundle* is a pair $(\mathcal{L}, \sigma)$ where $\mathcal{L}$ is a line bundle on E_S, and $\sigma \colon e_S^* \mathcal{L} \cong \mathcal{O}_S$ is an isomorphism. Here, $e_S \colon S \to E \times_k S$ is the section of π_S given by the structure map $S \to \mathrm{Spec}\, k \to E$ and the identity map $\mathrm{id}_S \colon S \to S$.

Quickly, we say that two such objects $(\mathcal{L}, \sigma)$ and $(\mathcal{L}', \sigma')$ are isomorphic if and only if there is an isomorphism $\varphi \colon \mathcal{L} \to \mathcal{L}'$ making the following diagram commute.

$$\begin{array}{ccc} e_S^* \mathcal{L} & \xrightarrow{e_S^* \varphi} & e_S^* \mathcal{L}' \\ & {\scriptstyle \sigma} \searrow \quad \swarrow {\scriptstyle \sigma'} & \\ & \mathcal{O}_S & \end{array}$$

Additionally, note that rigidified line bundles form a group under the tensor product.

Remark 2.38. We compute rigidified line bundles $(\mathcal{L}, \sigma)$ over $S = \mathrm{Spec}\, k$. Certainly we have all line bundles, but note that two rigidified line bundles $(\mathcal{L}, \sigma)$ and $(\mathcal{L}', \sigma')$ will have a unique isomorphism because an isomorphism $\mathcal{L} \cong \mathcal{L}'$ is only defined up to a scalar in $k^\times$.

Now here is the punchline.

Proposition 2.39. We have a functor $\mathrm{Pic}^0_E\colon \mathrm{Sch}_k^{\mathrm{op}} \to \mathrm{Ab}$ given by sending a k-scheme S to the group of rigidified line bundles $(\mathcal{L}, \sigma)$ over E_S such that $\deg \mathcal{L} = 0$.

Proof. That we produce an abelian group was discussed above. Functoriality comes because a k-morphism $f\colon S \to S'$ will make the sections commute as follows.

$$\begin{array}{ccc} E_S & \xrightarrow{f} & E_{S'} \\ {\scriptstyle e_S}\uparrow & & \uparrow{\scriptstyle e_{S'}} \\ S & \xrightarrow{f} & S' \end{array}$$

Now one can check that a rigidified line bundle on S' appropriately pull back to rigidified line bundles on S. ∎

We now claim that we have a natural isomorphism $h_E \Rightarrow \mathrm{Pic}^0_E(S)$. Quickly, we note that $h_E(S) = E(S)$ is in natural bijection with sections $x\colon S \to E_S$ such that $\pi_S \circ x = \mathrm{id}_S$ because we can simply set x to be determined by a map $S \to E$ and then apply the identity for $S \to S$. As such, we take a section $x\colon S \to E_S$ to the rigidified line bundle given by our section.

Lemma 2.40. Fix everything as above. Given a section $x\colon S \to E_S$, then x is a closed immersion and has image given by an effective Cartier divisor in E_S.

Proof. We refer to [SP, 062Y]. ∎

As such, given a section $x\colon S \to E_S$ to the line bundle given by

$$\mathcal{O}_{E_S}((e_S) - (x)) \otimes_{\mathcal{O}_{E_S}} \pi^* e_S^* \left((\mathcal{O}_{E_S}((e_S) - (x)))^{-1} \right).$$

This makes a rigidified line bundle, where our isomorphism σ arises from noting that hitting the above line bundle e_S^* makes this line bundle look like $\mathcal{L} \otimes \mathcal{L}^{-1} \cong \mathcal{O}_S$ for some line bundle $\mathcal{L} = e_S^* \mathcal{O}_{E_S}((e_S) - (x))$. Additionally, one can check that this construction is functorial in x, so we have indeed defined a natural transformation.

It remains to check that we have an isomorphism of functors. Roughly speaking, this is a special case of cohomology and base-change. Fix a rigidified line bundle $(\mathcal{L}, \sigma)$; then we need a section $x\colon S \to E_S$ producing this rigidified line bundle. Well, we set $\mathcal{M} \coloneqq \mathcal{L}(-e)^{-1}$. In the case where $S = \mathrm{Spec}\, k$, we observe that $H^0(E, M)$ is one-dimensional, and $H^i(E, \mathcal{M}) = 0$ for $i > 0$ because E is one-dimensional. As such, for general S, we see that $\pi_* \mathcal{M}$ is a line bundle with

$$(\pi_* \mathcal{M})(s) = \Gamma(E_s, \mathcal{M}|_{E_s})$$

for each $s \in S$. (This is by our cohomology and base change.) We now want to recover x. Well, one can check that the map $\pi^* \pi_* \mathcal{M} \to \mathcal{M}$ is injective with flat cokernel (see [SP, 00MF]). Taking the support of Q completes the proof.

Remark 2.41. Roughly speaking, in the $S = \mathrm{Spec}\, k$ case, we can recover $\mathcal{O}_E((e) - (x))$ as $\mathcal{L}$ by setting $\mathcal{M} \coloneqq \mathcal{L}(-e)^{-1}$ (which should hopefully by $\mathcal{O}_E((x))$), and then we can recover (x) from the line bundle $\mathcal{M}$. In particular, $H^0(E, \mathcal{O}_E((x)))$ has one-dimensional global sections, from which we can recover (x) by taking a cokernel as

$$\mathcal{O}_E \to \mathcal{O}_E(x) \to k(x) \to 0$$

because $k(x)$ is our skyscraper sheaf which produces (x). This is the motivation for the given proof.

2.5 March 10

Today we talk about morphisms of elliptic curves.

2.5.1 Morphisms Are Homomorphisms

Fix an elliptic k-curve (E, e). Last class we showed that we can extend the group law on $E(k)$ to produce an abelian group scheme $E(k)$. As such, we might be interested in homomorphisms between elliptic curves.

Definition 2.42 (isogeny)**.** Fix elliptic k-curves (E, e) and (E', e'). An *isogeny* is a nonconstant morphism $f\colon E \to E'$ such that $f(e) = e'$.

Theorem 2.43. Fix elliptic k-curves (E, e) and (E', e'). Given a morphism of curves $f\colon E \to E'$, actually f is a homomorphism. In particular, $f(S)\colon E(S) \to E(S')$ is a homomorphism for any k-scheme S.

Remark 2.44. Equivalently, if we give E the multiplication map m and E' the multiplication map m', then f being a homomorphism is requiring the following diagram to commute.

$$\begin{array}{ccc} E \times E & \xrightarrow{m} & E \\ {\scriptstyle f\times f}\downarrow & & \downarrow{\scriptstyle f} \\ E' \times E' & \xrightarrow{m'} & E' \end{array}$$

Proof. If f is constant (sending everything to e'), there is nothing to say. Otherwise, f is some finite morphism of curves.

Roughly speaking, this will fall out of some rigidity. We build the following diagram. Build the fiber product Z in the following diagram.

$$\begin{array}{ccc} Z & \longrightarrow & E' \\ \downarrow & \lrcorner & \downarrow \\ E \times E & \longrightarrow & E' \times E' \end{array}$$

Here, the bottom map sends $(x, y) \in E \times E \to (f(x + y), f(x) + f(y))$. Notably, f being a homomorphism is equivalent to having $Z \to E \times E$ to be an isomorphism.

However, everything is a variety, so it suffices to show that $Z(\overline{k}) \to E(\overline{k}) \times E(\overline{k})$ is surjective: this will tell us that the closed embedding $Z \to E \times E$ is surjective on closed points.[1] However, E is a variety, so closed points are dense, so this implies that Z is topologically the same as $E \times E$. But $E \times E$ is also reduced, so it has only one closed subvariety with the same topological space, so we get to conclude that $Z = E \times E$.

Now, a closed point of Z is a pair $(x, y, z) \in E \times E \times E'$ such that $f(x+y) = z = f(x)+f(y)$, so we see that it suffices to just show that $f\colon E(\overline{k}) \to E'(\overline{k})$ is a homomorphism. Base-changing to an algebraic closure, we just want to show that $f\colon E(k) \to E'(k)$ is a homomorphism when k is algebraically closed. Namely, we have reduced to checking the result on closed points.

We now have to examine our group law. Set $\lambda_E\colon E(k) \to \operatorname{Pic}^0(E)$ to be our bijection giving the group law on E. As such, we want the induced bottom arrow of the following diagram to be a homomorphism.

$$\begin{array}{ccc} E(k) & \xrightarrow{f} & E'(k) \\ \downarrow{\scriptstyle \lambda_E} & & \downarrow{\scriptstyle \lambda_{E'}} \\ \operatorname{Pic}^0 E & \dashrightarrow & \operatorname{Pic}^0 E' \end{array}$$

[1] In particular, we note that closed points p of a k-scheme X of finite type have residue field $k(p)$ which is finite over k, meaning that p is a $\overline{k}$-point. Indeed, $k(p)$ has residue field of the form $k[x_1, \dots, x_m]/\mathfrak{m}$ for some maximal ideal $\mathfrak{m}$, which must be finite over k by Hilbert's Nullstellensatz.

Roughly speaking, this is the norm map on ideals. We define $f_*\colon \operatorname{Div}^0 E \to \operatorname{Div}^0 E'$ by sending

$$f_*\colon x \to f(x).$$

Now, one can show that the following diagram commutes.

$$\begin{array}{ccc} k(E)^\times & \xrightarrow{\text{div}} & \operatorname{Div}^0 E \\ \downarrow & & \downarrow{\scriptstyle f_*} \\ k(E')^\times & \xrightarrow{\text{div}} & \operatorname{Div}^0 E' \end{array}$$

This is a standard result in algebraic geometry about divisors, but we can also see it from number theory: it suffices to check this for a set of finite points on its multiplicity around the diagram, for which we may reduce to affine subschemes. Namely, fix an affine open subscheme $\operatorname{Spec} A \subseteq E$. Because f is proper and quasifinite (it has finite fibers because the fibers must have dimension 0 for nonconstant maps f), so f is finite and in particular affine. Thus, the pre-image of $\operatorname{Spec} A$ is $\operatorname{Spec} B \subseteq E'$, so we are looking at a ring map $B \to A$. In fact, this is an embedding of rings (because f is dominant), and these are Dedekind domains because A and B are regular (and hence normal) integral domains of dimension 1. Then the above map can be purely checked on prime ideals, for which we refer to [GS13, Proposition 14, p. 17].

Anyway, the point is that we can check the commutativity of the diagram as follows.

$$\begin{array}{ccc} E(k) & \xrightarrow{f} & E'(k) \\ {\scriptstyle \lambda_E}\downarrow & & \downarrow{\scriptstyle \lambda_{E'}} \\ \operatorname{Pic}^0 E & \xrightarrow{f_*} & \operatorname{Pic}^0 E' \end{array} \qquad \begin{array}{ccc} x & \longmapsto & f(x) \\ \downarrow & & \downarrow \\ \mathcal{O}_E((x)-(e)) & \longmapsto & \mathcal{O}_E((f(x))-(e)) \end{array}$$

Now, f_* is a homomorphism, so we are done. ∎

Remark 2.45. The complex analytic situation roughly convinced us that this result ought to be true at the outset.

In particular, the above theorem tells us that isogenies are homomorphisms.

2.5.2 The Dual Isogeny

Given a morphism of elliptic k-curves $f\colon (E,e) \to (E',e')$, we note that we actually have a pullback map $f^*\colon \operatorname{Pic}^0 E \to \operatorname{Pic}^0 E'$, so we expect to have a scheme map $f^t\colon E' \to E$ in the other direction. Notably, if we look on the level of rigidified line bundles, there is actually a natural transformation $f^*\colon \operatorname{Pic}^0_{E'} \Rightarrow \operatorname{Pic}^0_E$: explicitly, for a test k-scheme S, we send the rigidified line bundle $(\mathcal{L}',\sigma)$ to $f^*\mathcal{L}'$ with the canonical isomorphism

$$e^* f^* \mathcal{L}' \cong (e')^* \mathcal{L}' \overset{\sigma}{\cong} \mathcal{O}_S.$$

One can check naturality and so on, but we won't bother. The point is that E represents the functor Pic^0_E, so we have induced a morphism $f^t\colon E' \to E$ following the above natural transformation.

2.5.3 Translations

Fix a morphism $f\colon (E,e) \to (E',e')$ of elliptic k-curves. As an aside, we note that not all morphisms are homomorphisms because of the condition $f(e) = e'$. For example, given a section $x\colon S \to E_S$, we can induce a translation map $t_x\colon S \to E_S$ by moving around the following diagram.

$$\begin{array}{ccc} E_S & \xrightarrow{t_x} & E_S \\ \| & & \uparrow{\scriptstyle m} \\ \{x\} \times_S E_S & \longrightarrow & E_S \times_S E_S \end{array}$$

In particular, if we imagine everything on closed points, we are basically mapping $y \mapsto x + y$.

2.6 March 13

Today we continue talking about the dual isogeny.

2.6.1 The Theorem of the Square

We begin with a remark.

Remark 2.46. Fix an elliptic curve (E, e). Then for closed points $x, y \in E(k)$, the definition of the group law has

$$(x) - (e) + (y) - (e) \sim (x + y) - (e)$$

by definition of the addition as coming from $\operatorname{Pic} E$. Thus, $(x) + (y) \sim (x + y) + (e)$ after cancelling out the redundant (e).

Now, to compute some dual isogenies, we want the following lemma.

Lemma 2.47. Fix an elliptic k-curve (E, e) and a reduced k-scheme S with projection $\pi_S \colon E_S \to S$. For any line bundle $\mathcal{L}$ of degree 0 on E_S. Then for any section $x \colon S \to E_S$ of π_S, we have

$$t_x^* \mathcal{L} \otimes_{\mathcal{O}_{E_S}} \pi_S^* x^* \mathcal{L}^{-1} \cong \mathcal{L} \otimes_{\mathcal{O}_{E_S}} \pi_S^* e_S^* \mathcal{L}$$

as line bundles on E_S.

Intuitively, we are saying that degree-0 line bundles are translation-invariant.

Proof. As perhaps to be expected, we will build up to the result from $S = \operatorname{Spec} k$ and then reduce to there.

1. Suppose $S = \operatorname{Spec} k$ where k is algebraically closed. Now, we can write $\mathcal{L}$ as a line bundle, so we can write it as a degree-0 divisor, which by Theorem 2.25 we know must look like $(e) - (y)$ for some $y \in E(k)$.

   Now, we calculate $t_{-x}^*(\mathcal{O}_E((e) - (y)))$ where $x \in E(S) = E(k)$. We may do this computation on the level of divisors, where we see t_{-x} will pull back the divisor $(e) - (y)$ along t_x to the divisor $(x) - (x + y)$; as such, $t_{-x}^*(\mathcal{O}_E((e) - (y))) = \mathcal{O}_E((x) - (x + y))$. But then

   $$(x) - (x + y) = (e) - (y)$$

   by definition of the group law, so we conclude that $t_{-x}^* \mathcal{L} = \mathcal{L}$. This is what we wanted, upon noting the terms $\pi_S^* x^* \mathcal{L}^{-1}$ are pullbacks of line bundles on $\operatorname{Spec} k$ and therefore simply one-dimensional vector spaces, so these terms do not matter in the tensor produce.

2. We now reduce to $S = \operatorname{Spec} k$. The point is that both sides of the desired equality are actually rigidified line bundles. Namely, we compute

   $$e_S^* \left(t_x^* \mathcal{L} \otimes \pi_S^* x^* \mathcal{L}^{-1} \right) = x^* \mathcal{L} \otimes x^* \mathcal{L}^{-1} = \mathcal{O}_S$$

   canonically; in particular, we have noted that $e_S^* t_x^* = (t_x \circ e_S)^* = x^*$. Similar holds for the other side, so we do indeed have rigidified line bundles. The moral of the story is that a rigidified line bundle is equivalent by the Yoneda lemma to providing a morphism of natural transformations from S to the category of its rigidified line bundles, so these two rigidified line bundles provide two scheme morphisms

   $$S \rightrightarrows \operatorname{Pic}_E^0 .$$

   Call the two maps R and L. However, our two maps agree on fibers by the field case: for any point $s \in S$, we have the pullback square

   $$\begin{array}{ccc} E_{k(s)} & \longrightarrow & E_S \\ \downarrow & \lrcorner & \downarrow \\ \operatorname{Spec} k(s) & \longrightarrow & S \end{array}$$

which by the previous step must have $R = L$ as maps on the left-hand arrow. Thus, R and L agree on all points. We now finish the proof in the usual way, using the hypothesis that S is a k-scheme with finite type. Namely, consider the following fiber product.

$$\begin{array}{ccc} Z & \longrightarrow & \mathrm{Pic}^0_E \\ \downarrow & \lrcorner & \downarrow \\ S & \underset{L}{\overset{R}{\rightrightarrows}} & \mathrm{Pic}^0_E \times \mathrm{Pic}^0_E \end{array}$$

Because R and L agree on all points, we see that Z becomes a closed subscheme of S containing all points (it's closed because the right map is the closed embedding $\Delta\colon E \to E \times E$), but then we must have $Z = S$ because this is a closed embedding and S is reduced. ■

Corollary 2.48 (Square)**.** As schemes on $S := E \times E$, we let $p_1, p_2\colon S \to E$ be the projections. Then, where m is the multiplication, we have

$$m^*\mathcal{L} \otimes p_1\mathcal{L}^{-1} \otimes p_2\mathcal{L}^{-1} \cong \mathcal{O}_S$$

for any degree-0 line bundle $\mathcal{L}$ on E.

Proof. Set $S = E$. Let $p_1, p_2\colon E \times E \to E$ be our projections, and let $p_1\colon E_E \to E$ be the projection of our base-change. The point is that $\Delta\colon E \times E \to E$ provides a section for p_1, which gives $t_x\colon E \times E \to E \times E$ can be tracked around to give the closed point $(x, y) \mapsto (x, x + y)$. Now, for any line bundle $\mathcal{M}$ of degree 0 on E, we see that

$$m^*\mathcal{M} \otimes p_1^*\mathcal{M}^{-1} \cong p_2^*\mathcal{M}$$

What? by tracking everything around and plugging into the previous theorem. This is called the theorem of the square. ■

Remark 2.49. Let's describe how to show Lemma 2.47 without the reduced hypothesis. The point is that Corollary 2.48 is almost the most general version of having a section $s\colon S \to E_S$. In particular, the map $E \times \mathrm{Pic}^0_E \to \mathrm{Pic}^0_E$ has a canonical section given by $\mathrm{id}_{\mathrm{Pic}^0_E}$ by the Yoneda lemma produces a rigidified line bundle $\mathcal{P}$ called the "Poincaré line bundle." This provides a "universal rigidified line bundle." We now make two remarks.

- The above proof merely wants to show that $R = L$ for some maps $R, L\colon S \to \mathrm{Pic}^0_E$. But this is a question local on S, so we may choose a trivializing open cover to assume that all line bundles are trivial (but rigidified).
- Then one can check that $\mathcal{P}$ is in fact the universal line bundle, obtaining the result by base-change in the following diagram.

$$\begin{array}{ccc} & E \times E \times \mathrm{Pic}^0_E & \qquad p_{23}^*\mathcal{P} \\ & \downarrow{\scriptstyle p_{13}} & \qquad \uparrow \\ S & \xrightarrow{(x,\mathcal{L})} E \times \mathrm{Pic}^0_E & \qquad \mathcal{P} \end{array}$$

Chasing our universal line bundle around using Corollary 2.48 is able to finish.

Remark 2.50. Translation-invariance characterizes degree-0 line bundles, so Lemma 2.47 does not hold in higher degrees. For example,

$$t_{-x}^*\mathcal{O}_E((e)) = \mathcal{O}_E((x)) \neq \mathcal{O}_E((e)),$$

so $\mathcal{O}_E((e))$ is not translation-invariant!

The point of talking about the theorem of the square is that we get the following result.

Notation 2.51. Fix an integer n. For an abelian group scheme G, we let $[n]_G \colon G \to G$ denote the multiplication-by-n map. We omit the G on the notation whenever possible.

Proposition 2.52. Fix an isogeny of elliptic k-curves $f \colon (E, e) \to (E', e')$. Then $f^t \circ f = [\deg f]_E$.

Proof. We track through our definitions. Because we are asking for two morphisms on varieties to be equal, it is enough to base-change to the algebraic closure and check that our morphisms agree on closed points. Namely, tracking through the definition of f^t, we know it makes the following diagram commute.

$$\begin{array}{ccc} E' & \xrightarrow{f^t} & E \\ \downarrow & & \downarrow \\ \mathrm{Pic}^0_{E'} & \xrightarrow{f^*} & \mathrm{Pic}^0_E \end{array}$$

Thus, $f^*\mathcal{O}_E((e) - f^t(x')) = f^*\mathcal{O}_{E'}((e) - (x'))$ for any $x' \in E'(k)$. Now here is our computation. We compute $f^t \circ f$. Set $x' \coloneqq f(x)$ for some $x \in E(k)$. Then

$$f^*\mathcal{O}_{E'}((e') - (f(x))) = \mathcal{O}_{E'}\left((\ker f) - (f^{-1}f(x))\right)$$

by computing f^* as pre-images on the level of divisors. However, because we are dealing with an abelian group scheme, we see that the pre-image $f^{-1}f(x) = x + \ker f$; here, $x + \ker f$ refers to $\ker f$ base-changed under t_{-x}. However, our degree-0 line bundles are translation-invariant, so

$$(\ker f) - (x + \ker f) = \sum_{y \in \ker f} ((y) - (x + y)) \sim (\deg f)((e) - (x)).$$

Thus,

$$\mathcal{O}_E\left((e) - f^t(f(x))\right) = \mathcal{O}_E((\deg f)((e) - (x))),$$

but by the uniqueness of effective divisors representing degree-1 line bundles, we conclude that $f^t(f(x)) = \deg f$. ∎

Remark 2.53. It will turn out that $g \coloneqq f \circ f^t$ is also multiplication by f. This roughly follows by computing $g \circ f = f \circ (\deg f) = (\deg f) \circ f$ and then cancelling the fs by Lemma 2.54, which is legal because f is an isogeny.

2.7 March 15

Ok, let me continue then.

2.7.1 More on Dual Isogenies

We have the following results on dual isogenies.

Lemma 2.54. Fix smooth, proper, projective, geometrically connected k-curves C and C' and D and D'. Given non-constant morphisms $f, g\colon C \to D$ and more non-constant morphisms $p\colon C' \to C$ such that

$$f \circ p = g \circ p.$$

Then $f = g$.

Proof. To begin, note that p is dominant because it is non-constant onto a one-dimensional scheme, but it is also proper, so it is both a continuous and closed map; in other words, the topology on C is merely given by the quotient topology from C', so we conclude that $f = g$ on topological spaces. For clarity, call this map h.

It remains to check equality on the level of sheaves. Here, we are looking at the composite

$$h^{-1}\mathcal{O}_D \rightrightarrows \mathcal{O}_C \hookrightarrow p_*\mathcal{O}_{C'},$$

where the map on the right is injective because p is dominant, and our scheme is reduced. ∎

Remark 2.55. We can also cancel on the other side, in a special case. Fix isogenies of elliptic curves $f, g\colon (E, e) \to (E', e')$ such that there is an isogeny $q\colon (E', e') \to (E'', e'')$ with $q \circ f = q \circ g$. Then we see that $q \circ (f - g)$ maps everything to e'', so $(f - g)$ maps to $\ker q \subseteq E'$. However, $\ker q$ is a closed subscheme of E' not equal to E', so it is zero-dimensional. But if $f - g$ is non-constant, then it is dominant and cannot land in such a closed subscheme, so we conclude that $f - g$ must be constantly e', finishing.

Proposition 2.56. Fix isogenies $f, g\colon (E, e) \to (E', e')$. Then $f^t + g^t = (f + g)^t$.

Proof. Here, the addition of the morphisms $f + g$ is defined as the composite of

$$E \xrightarrow{(f,g)} E' \times E' \xrightarrow{m} E'.$$

By taking the base-change to the algebraic closure, we may check our equality of morphisms on closed points. So one hand, for some $x' \in E'(k)$, we see that

$$\mathcal{O}_E\left((e) - (f+g)^t(x')\right) = (f+g)^*\mathcal{O}_{E'}((e') - (x')) = (f,g)^*m^*\mathcal{O}_{E'}((e') - (x')),$$

by definition of $(f + g)^t$. On the other hand, $f^t(x') + g^t(x')$ corresponds to the line bundle

$$f^*\mathcal{O}_{E'}((e') - (x')) \otimes g^*\mathcal{O}_{E'}((e') - (x')).$$

We would like to use Corollary 2.48, so we rewrite the above line bundle as

$$(f,g)^*p_1^*\mathcal{O}_{E'}((e') - (x')) \otimes (f,g)^*p_2^*\mathcal{O}_{E'}((e') - (x')),$$

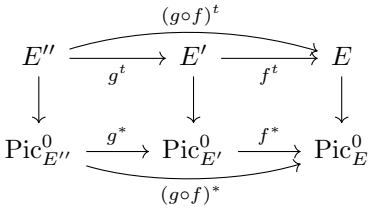
so by comparing our two line bundles, it is enough to show that

$$m_*\mathcal{O}_{E'}((e') - (x')) \cong p_1^*\mathcal{O}_{E'}((e') - (x')) \otimes p_2^*\mathcal{O}_{E'}((e') - (x')),$$

which holds by Corollary 2.48. ∎

Proposition 2.57. Fix isogenies $f\colon (E,e)\to(E',e')$ and $g\colon (E',e')\to(E'',e'')$. Then $(g\circ f)^t = f^t\circ g^t$.

Proof. Tracking through the definition of the dual isogeny, we see we are looking at the following large diagram.



Here, the bottom triangle commutes by properties of the pullback (we might only know this for the non-scheme-theoretic Pic^0, but then we can just check the equality on closed points), so by definition of $(g\circ f)^t$, the above triangle also commutes, which is what we wanted. ∎

Let's now build towards $(f^t)^t = f$.

Lemma 2.58. Fix an elliptic k-curve (E,e). Then $[m]^t = [m]$ for any $m\in\mathbb{Z}$.

Proof. We induct. For $m=1$, we can track around the usual diagram to see that ${\mathrm{id}_E}^t = \mathrm{id}_E$, which finishes. For the inductive step, we use Proposition 2.56 to see

$$[m\pm 1]^t = ([m]\pm[1])^t = [m]^t \pm [1]^t = [m]\pm[1] = [m\pm 1].$$

As such, we see that we may induct up and down from the base case of $m=1$ to get any $m\in\mathbb{Z}$. ∎

Lemma 2.59. Fix an elliptic k-curve (E,e). For any $m>0$, the map $[m]\colon E\to E$ is non-constant.

Proof. We begin by showing that it's enough to show that $\deg[2]>1$. Indeed, for any m, if $[m]$ is constant, then

$$[n] = [m] + [n-m] = [n-m],$$

so the maps are periodic $(\mathrm{mod}\ m)$, so the degree of the maps is bounded. However, if $\deg[2]>1$, then $\deg\left[2^k\right]\to\infty$ as $k\to\infty$.

We now work in characteristic not equal to 2 or 3, for concreteness. Then one can write $E\colon y^2 = x(x-1)(x-\lambda)$ over the algebraic closure, so we have a map $\pi\colon E\to\mathbb{P}^1_k$ given by $(x,y)\mapsto x$. Notably, there is an involution $\iota\colon E\to E$ given by $(x,y)\mapsto(x,-y)$ such that $\pi\circ\iota=\pi$, so we note

$$E[2] = \{p\in E(k) : 2P = e\} = \{p\in E(k) : \iota(P) = P\}.$$

However, the orbit of P under ι is exactly the pre-image of $\pi(P)\in\mathbb{P}^1_k$, so above we are asking for $p\in E[2]$ if and only if $\pi^{-1}(\{\pi p\})$ is a single point.

To continue, we note that the orbit of π has degree 2 because it corresponds to the field extension $k(x)\hookrightarrow k(x)[y]/\left(y^2 - x(x-1)(x-\lambda)\right)$. As such, we can use the Riemann–Hurwitz formula to compute

$$2g(E) - 2 = (\deg\pi)(2g(\mathbb{P}^1_k) - 2) + \sum_{p\in\mathbb{P}^1_k}(e_p - 1),$$

where e_p is the ramification index. (Notably, the above formula doesn't quite work in characteristic 2.) This will complete the proof upon rearranging: we see that only four points will live in $E[2]$. ∎

Corollary 2.60. Fix an elliptic k-curve (E, e). Then $\deg[m] = m^2$ for any $m \in \mathbb{Z}$.

Proof. By Proposition 2.52 and Lemma 2.58, we see that

$$[\deg[m]] = [m] \circ [m]^t = [m] \circ [m] = \left[m^2\right],$$

so we finish. It follows from Lemma 2.59 that we may say $m^2 = \deg[m]$ because multiplication by $\left|\deg[m] - m^2\right| \geq 0$ is constant and thus must just have $\left|\deg[m] - m^2\right| = 0$. ∎

Lemma 2.61. Fix an isogeny $f\colon (E, e) \to (E', e')$ of elliptic k-curves. Then $\deg f^t = \deg f$.

Proof. We use Proposition 2.52. On one hand, we see

$$\deg\left(f \circ f^t\right) = \deg f \cdot \deg f^t$$

(one can see that degree is multiplicative like this by comparing the field extensions $K(E') \subseteq K(E) \subseteq K(E')$), but on the other hand, we see

$$\deg\left([\deg f]\right) = [\deg f]^2$$

by Corollary 2.60. Comparing our degrees finishes. ∎

Proposition 2.62. Fix an isogeny $f\colon (E, e) \to (E', e')$ of elliptic k-curves. Then $\left(f^t\right)^t = f$.

Proof. By combining Lemma 2.61 and Proposition 2.52, we see that

$$f \circ f^t = [\deg f] = \left[\deg f^t\right] = \left(f^t\right)^t \circ f^t.$$

Cancelling on the right with Lemma 2.54 completes the proof. ∎

2.8 March 17

We now move more directly towards the Mordell–Weil theorem.

2.8.1 The Mordell–Weil Theorem

Here is our statement.

Theorem 2.63 (Mordell–Weil)**.** Fix a number field K. Given an elliptic K-curve (E, e), then the group $E(K)$ is finitely generated.

Our proof will take two steps. We will first show the following result.

Theorem 2.64 (Weak Mordell–Weil)**.** Fix a number field K. Given an elliptic K-curve (E, e), then the group $E(K)/rE(K)$ is finite for any $r \geq 1$.

Then our second step will use some theory of heights to recover Theorem 2.63.

So let's go at Theorem 2.64. It will be no surprise that our approach is cohomological. Let's describe the idea. Note $[m]\colon E \to E$ is a non-constant map by Lemma 2.59, so it is surjective (as a scheme map, so on geometric points for example), so one has an exact sequence

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

Formally, $E[m]$ is the kernel of $[m]$, which we can view as the pre-image of e under $[m]$, which is the following fiber product.

$$\begin{array}{ccc} E[m] & \longrightarrow & e \\ \downarrow & \lrcorner & \downarrow \\ E & \xrightarrow{[m]} & E \end{array}$$

Thus, viewing everything as a module over $G \coloneqq \mathrm{Gal}(\overline{K}/K)$, we get an inclusion

$$\frac{E(K)}{mE(K)} \to H^1\left(G, E[m](\overline{K})\right).$$

As such, the game is to control the image in this map.

Let's spend a moment discussing our H^1. Roughly speaking, some algebra is able to show that, as long as m is not divisible by $\operatorname{char} K$ (which is true because K is a number field), then $E[m](K) \cong (\mathbb{Z}/m\mathbb{Z})^2$ after some base-change of K to pick up all the m-torsion point. Then

$$H^1\left(G, (\mathbb{Z}/m\mathbb{Z})^2\right) = \mathrm{Hom}\left(G, (\mathbb{Z}/m\mathbb{Z})^2\right) = \mathrm{Hom}\left(G^{\mathrm{ab}}, \mathbb{Z}/m\mathbb{Z}\right)^2,$$

so elements here are in bijection with pairs (L, L') of cyclic extensions of degree m over K. In particular, we expect this H^1 to be quite infinite.

Being more explicit now, suppose we have some $P \in E(K)$. Then we lift it to some $Q \in E(\overline{K})$ such that $P = mQ$, and the corresponding element in $H^1(G, E[m](\overline{K}))$ is $\sigma \mapsto (\sigma - 1)Q$ for any σ. However, we can do a little better by thinking about the pre-image of P along $[m]\colon E \to E$ as fitting in the fiber product as follows.

$$\begin{array}{ccc} [m]^{-1}P & \longrightarrow & P \\ \downarrow & \lrcorner & \downarrow \\ E & \xrightarrow{[m]} & E \end{array}$$

And notably, the class of P in $H^1(G, E[m](\overline{K}))$ vanishes if and only if $T_P \coloneqq [m]^{-1}(P)$ has K-points.

Now, taking the equation for our elliptic curve E, one can clear denominators to make E actually into a scheme over $\mathcal{O}_K[1/(mN)]$ for N large enough. In fact, one can extend the addition, identity, smoothness, properness to E now as a curve over $\operatorname{Spec} \mathcal{O}_K[1/(mN)]$. In fact, by the valuative criterion for properness will still extend to a point over $\operatorname{Spec} \mathcal{O}_K[1/(mN)]$.

$$\begin{array}{ccc} \operatorname{Spec} K & \longrightarrow & E \\ \downarrow & \nearrow & \uparrow \\ \operatorname{Spec} \mathcal{O}_K[1/(mN)] & \longrightarrow & \operatorname{Spec} \mathcal{O}_K[1/(mN)] \end{array}$$

Notably, one hopes that we can now control $E[m]$ via this sort of spreading out.

To finish up for today, suppose we have a scheme S and a line bundle $\mathcal{L}$ over S equipped with an isomorphism $\sigma\colon \mathcal{L}^m \to \mathcal{O}_S$. By base-changing a little, we assume that S is a scheme over $\mathbb{Z}[1/m, \zeta_m]$. Then we can consider

$$\operatorname{Spec}_S\left(\mathcal{O}_S \oplus \mathcal{L} \oplus \mathcal{L}^2 \oplus \cdots \oplus \mathcal{L}^{m-1}\right),$$

which is intended to look like $\mathcal{O}_S[x]/\left(x^p - \mathcal{L}\right)$. The point is that the above scheme comes equipped with a $\mathbb{Z}/m\mathbb{Z}$-action by having a fixed generator $\gamma \in \mathbb{Z}/m\mathbb{Z}$ act by

$$\gamma \cdot (\ell_0, \ldots, \ell_{m-1}) = \left(\ell_0, \zeta_m \ell_1, \ldots, \zeta_m^{m-1} \ell_{m-1}\right).$$

It turns out that we can go backward: given a pair $(\mathcal{L}, \sigma)$ as above, we can take this to $\mathcal{L}$ to produce an element in $\mathrm{Pic}(S)[m]$, and one can ask for the kernel of this map, but it's just given by the set of ways to assign isomorphisms $\mathcal{O}_S^m \cong \mathcal{O}_S$, but it is just the set $\mathcal{O}_S^\times / \mathcal{O}_S^{\times m}$.

2.9 March 20

Today we discuss the weak Mordell–Weil theorem.

2.9.1 The Weak Mordell–Weil Theorem

In order to avoid algebraic geometry for a little, we give intuition via the following argument.

Proposition 2.65. Fix a number field K containing the rth roots of unity. Then $\mathcal{O}_K[1/N]^\times / \mathcal{O}_K[1/n]^{\times r}$ has finite image in $H^1(\mathrm{Gal}(\overline{K}/K), \mu_r)$ for any N divisible by r.

Proof. Note that this is roughly automatic by Dirichlet's unit theorem, which tells us that $\mathcal{O}_K[1/N]$ is a finitely generated abelian group already. However, let's give a more geometric argument.

The group scheme $\mathbb{G}_m \coloneqq \operatorname{Spec} \mathbb{Z}[x, 1/x]$ represents the functor $\mathrm{Sch}^{\mathrm{op}} \to \mathrm{Ab}$ given by $S \mapsto \Gamma(S, \mathcal{O}_S)^\times$. One can see this by gluing together the story on affine pieces; alternatively, we directly note that a morphism $\operatorname{Spec} \mathbb{Z}[x, 1/x]$ amounts to choosing a global section $x \in \Gamma(S, \mathcal{O}_S)$ which is a unit, which gives what we wanted.

We now claim that $\mathcal{O}_K[1/N]^\times / \mathcal{O}_K[1/N]^{r\times}$ has finite image in $H^1(\mathrm{Gal}(\overline{K}/K), \mu_r)$. To understand this, consider the short exact sequence

$$0 \to \mu_r \to \overline{K}^\times \xrightarrow{(-)^r} \overline{K}^\times \to 0$$

of modules over $G \coloneqq \mathrm{Gal}(\overline{K}/K)$. Then the long exact sequence yields

$$K^\times \xrightarrow{(-)^r} K^\times \xrightarrow{\partial} H^1(G, \mu_r) \to 0,$$

where the rightmost zero is by Hilbert's theorem 90. As such, we see that there is a map

$$\frac{\mathcal{O}_K[1/N]^\times}{\mathcal{O}_K[1/N]^{\times r}} \to \frac{K^\times}{K^{\times r}} \overset{\partial}{\cong} H^1(G, \mu_r).$$

Now, for the statement, we note there is a morphism $[r] \colon \mathbb{G}_m \to \mathbb{G}_m$ given by the ring map $\mathbb{Z}[x, 1/x] \to \mathbb{Z}[x, 1/x]$ by $x \mapsto x^r$. We now bound ramification. The point is that some $a \in \mathcal{O}_K[1/N]^\times$ induces a morphism $\operatorname{Spec} \mathcal{O}_K[1/N] \to \mathbb{G}_{m, \mathcal{O}_K[1/N]}$, where we have implicitly base-changed $\mathbb{G}_m$ here. As such, providing an rth root of a is equivalent to looking at the following fiber product.

$$\begin{array}{ccc} \operatorname{Spec} \dfrac{\mathcal{O}_K[1/N][x]}{(x^r - a)} & \longrightarrow & \operatorname{Spec} \mathcal{O}_K[1/N] \\ \downarrow & & \downarrow a \\ \mathbb{G}_{m, \mathcal{O}_K[1/N]} & \xrightarrow{[r]} & \mathbb{G}_{m, \mathcal{O}_K[1/N]} \end{array}$$

Namely, an rth root asserts asking for an $\mathcal{O}O_K[1/N]$-point of this fiber product; for brevity, set $A_a \coloneqq \mathcal{O}_K[1/N][x]/(x^r - a)$. Now, we can factor $x^r - a$ into a product of irreducibles F_i and set $L_i \coloneqq K[x]/(F_i(x))$, and we see that

$$A_a \otimes K = \prod_i L_i.$$

Note that there is a μ_r-action on $\operatorname{Spec} A_a$ by permuting the rth roots of A (here we use $\mu_r \subseteq K$), and this action permutes the factors L_i in the above product decomposition because $x^r - a$ is simply going to decompose itself into linear factors over the algebraic closure, and the μ_r-action permutes the factors of this decomposition.

Now, to see our finite image, we claim that $\partial(a) \in H^1(G, \mu_r)$ actually comes from $H^1(\mathrm{Gal}(L_i/K), \mu_r)$ for any fixed i. Indeed, to track our boundary map, we begin by choosing some $b \in \overline{K}^\times$ with $b^r = a$. However, by adjusting our b (by our transitive μ_r-action!), we may assume that the chosen b comes from L_i. Now, the corresponding cocycle in $H^1(G, \mu_r)$ when passed through boundary is

$$\partial a \colon \sigma \mapsto \frac{\sigma b}{b},$$

which we see will actually be defined in L_i. Passing this "restricted" cocycle through inflation provides what we want.

We now claim that

$$A = \prod_i \mathcal{O}_{L_i}[1/N],$$

and each L_i is unramified (over K) outside (N). We leave this claim as an exercise.

This will provide the desired finiteness: $H^1(\mathrm{Gal}(L_i/K), \mu_r)$ is finite (it's a finite group and a finite module), and there are only finitely many extensions over K of bounded degree and unramified outside some constant set. (To see this second claim, we note that being unramified outside some fix set of primes enforces some boundedness of the discriminant, and we can use the Minkowski bound to finish.) Now to finish the argument, we note that even as we vary $a \in \mathcal{O}_K[1/N]^\times$, there are only finitely many possibilities of the L_i, so we only have to check the image of finitely many maps

$$\mathrm{Inf} \colon H^1(\mathrm{Gal}(L/K), \mu_r) \to H^1(\mathrm{Gal}(\overline{K}/K), \mu_r),$$

so the image remains finite. ∎

Let's now do the same thing but for elliptic curves.

Theorem 2.64 (Weak Mordell–Weil)**.** Fix a number field K. Given an elliptic K-curve (E, e), then the group $E(K)/rE(K)$ is finite for any $r \geq 1$.

Proof. To be concrete, we write E as $y^2 = x^3 + ax + b$. (Namely, our number field K has characteristic zero, so this factoring is safe.) Smoothness, then, amounts to requiring $4a^3 - 27b^2 \neq 0$. We now choose N both divisible by 6 and by r, where $a, b \in \mathcal{O}_K[1/N]$ (after clearing denominators!), and $4a^3 - 27b^2$ is actually a unit in $\mathcal{O}_K[1/N]$.

We now define $\mathcal{E}$ to be defined by $y^2 = x^3 + ax + b$ (lying in projective space) to be a scheme over $S \coloneqq \mathrm{Spec}\, \mathcal{O}_K[1/N]$. In fact, $\mathcal{E}$ remains a group scheme, isomorphic to $\mathrm{Pic}^0_{\mathcal{E}/S}$ by running the exact same argument through. (In particular, the key ingredient to defining our rigidified line bundles is having a field-valued point for any field, but this is clear because we have the point $[0 : 1 : 0] \in E(\mathrm{Spec}\, A)$ for any ring A.) Notably, $\mathcal{E}$ is proper over S (because it's projective), and $\mathcal{E}$ is also smooth by computing the Jacobian (namely, $4a^3 - 27b^2$ is still a unit!).

We now apply the valuative criterion for properness. This tells us that a map $\mathrm{Spec}\, K \to E \to \mathcal{E}$ will extend to a map $\mathrm{Spec}\, \mathcal{O}_K[1/N] \to \mathcal{E}$ factoring in the following diagram.

$$\begin{array}{ccc} \mathrm{Spec}\, K & \longrightarrow & \mathcal{E} \\ \downarrow & \overset{!}{\nearrow} & \downarrow \\ \mathrm{Spec}\, \mathcal{O}_K[1/N] & = & \mathrm{Spec}\, \mathcal{O}_K[1/N] \end{array}$$

Now, for our result, we fix some $a \in E(K)$ and study the same fiber product $\mathcal{P}_a \coloneqq S \times_{\mathcal{E}} \mathcal{E}$ arising in the following pullback square.

$$\begin{array}{ccc} \mathcal{P}_a & \longrightarrow & S \\ \downarrow & & \downarrow{\scriptstyle a} \\ \mathcal{E} & \xrightarrow{[r]} & \mathcal{E} \end{array}$$

Let's now start the proof. We have a short exact sequence as follows.

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

As before, the long exact sequence here induces an inclusion

$$\partial\colon \frac{E(K)}{rE(K)} \hookrightarrow H^1(G, E[r](K)),$$

where $G \coloneqq \mathrm{Gal}(\overline{K}/K)$. We will show that the image of this inclusion is finite, which will finish the proof. For psychological reasons, we would like to assume that $E[r](\overline{K}) = E[r](K)$. Well, find some field L such that $E[r](\overline{K}) = E[r](L)$, and suppose we have the claim for L. Then we can draw the following diagram.

$$\begin{array}{ccc} & & H^1(\mathrm{Gal}(L/K), E[r](\overline{K})) \\ & & \downarrow \\ E(K)/rE(K) & \xrightarrow{\partial_K} & H^1(\mathrm{Gal}(\overline{L}/L), E[r](\overline{K})) \\ \downarrow & & \downarrow \\ E(L)/rE(L) & \xrightarrow{\partial_L} & H^1(\mathrm{Gal}(\overline{L}/L), E[r](\overline{K})) \end{array}$$

One can check by hand that the vertical right sequence is exact (this is on the homework), so if the bottom image is finite, then exactness says that the image of the middle map has size bounded by the product of the size of $H^1(\mathrm{Gal}(L/K), E[r](\overline{K}))$ and the image of ∂_L.

Now, similar to before, this will come down to bounding ramification and degree. Namely, for all $a \in E(K)$, we claim that there is an extension L_a/K unramified outside (N) and of degree bounded by r^2 such that $\partial(a)$ lies in the image of the map

$$\mathrm{Inf}\colon H^1(\mathrm{Gal}(L/K), E[r](K)) \to H^1(G, E[r](K)).$$

This will complete the proof of our finiteness because there are only finitely many extensions L of bounded degree and unramified outside (N), so we are really only checking the image of finitely many inflation maps from the finite groups $H^1(\mathrm{Gal}(L/K), E[r](K))$, so the total image of ∂ will be contained in this finite union of finite sets and hence be finite.

Roughly speaking,

$$\partial(a) \in \mathrm{im}\left(H^1(\mathrm{Gal}(L_a/K), E[r](K)) \to H^1(\mathrm{Gal}(\overline{K}/K), E[r](K))\right),$$

where L_a/K is an extension where $\mathcal{P}_a(L_a) \neq \varnothing$. Indeed, this is essentially how ∂ is defined: if we have $P_a(L_a) \neq \varnothing$, then we find an mth root in $\mathcal{E}$ for our point a (over L_a!), and then we can find our $\partial(a)$ as arising from over $\mathrm{Gal}(L_a/K)$ by tracking through the boundary morphism, where the point is that our choice of lift along $[r]\colon E \to E$ of a may live over this specified L_a.

We now attempt to find such an L_a. In words, assuming $m \nmid N$, the point is that $[m]\colon \mathcal{E} \to \mathcal{E}$ is finite étale of degree r^2, so

$$\mathcal{P}_a = \mathrm{Spec} \prod_i \mathcal{O}_{L_i}[1/N],$$

where the L_i/K is finite and unramified outside N. In fact, because the degree of our map is at most r^2, each of the L_i has degree at most r^2, so we may choose the L_a appropriately.

Maybe?

Let's see this directly. We proceed in steps.

1. Note that $\mathcal{P}_a \to S$ is a finite map of schemes because it is the base-change of the finite map $[r]\colon \mathcal{E} \to \mathcal{E}$; namely, we can check that $[r]\colon \mathcal{E} \to \mathcal{E}$ is proper because $\mathcal{E}$ is proper and separated over S, and it is quasi-finite because the number of points in a fiber of a point in $\mathcal{E}$ can be checked after the base-change to a field, and then we are looking at an elliptic curve and may appeal to Corollary 2.60. In particular, finite maps are affine, so we conclude that $\mathcal{P}_a$ can be written as $\mathrm{Spec}\, A_a$ where A_a is a finite $\mathcal{O}_K[1/N]$-algebra.

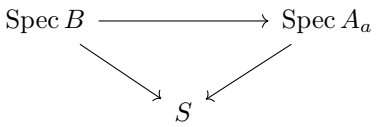
2. Now, we note that the multiplication map $[r]\colon E \to E$ has degree r^2, so we can see that $[r]_*\mathcal{O}_E$ is locally free of rank r^2 (checking on stalks, it's enough to see that $[r]_*\mathcal{O}_E$ is torsion-free on stalks—over the local ring—but there is no torsion because E is an integral scheme). Continuing, as a closed subscheme, we see
$$E[r] = \operatorname{Spec}([r]_*\mathcal{O}_E)(e)$$
by tracking through what this means: on divisors, we are asking for the points which go to e when multiplied by r. Here, we see that $([m]_*\mathcal{O}_E)(e)$ is a finite-dimensional K-algebra A, so it is Artinian and therefore a product of Artinian local rings
$$A = \prod_i A_i,$$
These A_i have a residue field $\kappa_i \coloneqq A_i/\mathfrak{m}_i$, and each κ_i is separable over K because $[r]$ is separable. Now, when r is coprime with the characteristic (as it is in our case), we have m^2 points in this fiber (because our map is separable), so $\sum_i \dim_k \kappa_i = r^2$ by this point-counting. But A needs to also have dimension r^2 over K, so we conclude that $A_i = \kappa_i$ is forced, so we can write
$$E[m] = \operatorname{Spec} \prod_i L_i',$$
where the L_i' are finite and separable over K with degrees summing to r^2.

3. We now claim that the map $\mathcal{P}_a \to S$ is flat. Indeed, we may check this stalk-locally: fix some prime $\mathfrak{p} \in S$, and let $\mathfrak{P}$ be the pre-image in A_a. As such, we are asking for the extension $\mathcal{O}_{S,\mathfrak{p}} \to A_{a,\mathfrak{P}}$ is flat.

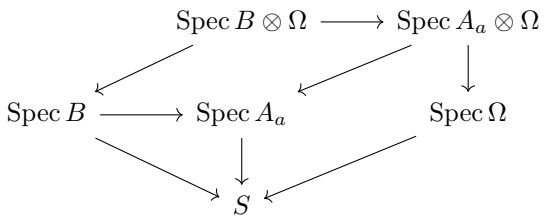
   Well, looking at residue fields, we see that the residue fields $A_a(\mathfrak{P})$ has dimension m^2 as a vector space over $\mathcal{O}_S(\mathfrak{p})$, so we can choose elements $x_1, \dots, x_{m^2} \in A_{a,\mathfrak{P}}$ which grant a basis over $A_a(\mathfrak{P})$. But then Nakayama's lemma tells us that we have a surjection
$$\mathcal{O}_{S,\mathfrak{p}}^{\oplus r^2} \twoheadrightarrow A_{a,\mathfrak{P}}$$
given by this basis. In fact, this is injective: we can check injectivity after localizing at the generic point, but then we are looking at an algebra of dimension r^2 over K (because we have lifted from a map of degree r^2), so the surjectivity of our map of vector spaces over dimension r^2.

4. Next up, we claim that A_a is the integral closure of $\mathcal{O}_K[1/N]$ sitting inside $A_a \otimes K = \prod_i L_i$ where the L_i are finite separable extensions over K, and each L_i is unramified over K outside (N).

   Well, let B be the integral closure of $\mathcal{O}_K[1/N]$ inside $A_a \otimes K$. Certainly each element of A_a is integral over $\mathcal{O}_K[1/N]$ because A_a is actually finite over $\mathcal{O}_K[1/N]$. Thus, we have an embedding $A_a \hookrightarrow B$, giving us the following diagram.



   Here, the map $\operatorname{Spec} B \to \operatorname{Spec} A_a$ is dominant. Now, letting Ω be an algebraic closure of K, we base-change, yielding the following diagram.



Now, $\operatorname{Spec} A_a \otimes \Omega$ has r^2 distinct points, so B must have at least r^2 distinct primes as well. It then follows that the map $A_a \to B$ is surjective by making an argument similar to above, arguing that B should be some product of fields and counting points/dimensions.

What?

In total, we may write

$$A_a = \prod_i \mathcal{O}_{L_i}[1/N]$$

by taking our integral closures appropriately. Notably, looking over each point, we see that the group $E[r]$ acts on the product of the fields $\prod_i L_i$ (which is the fiber over our point a). Thus, each extension L_i/K is Galois, so choosing a particular prime $\mathfrak{p} \in \operatorname{Spec} \mathcal{O}_K[1/N]$, we may factor it up in $\mathcal{O}_{L_i}[1/N]$ and find that all the ramification and inertial data must be the same due to our Galois action. As such, we compute these degrees locally to see

$$r^2 = \sum_i f_i e_i g_i,$$

where f_i is the inertial data, e_i is the ramification data, and g_i is the number of primes, where this ith index is the data at L_i/K.

On the other hand, we may count points to see that the number of points lying over $\mathfrak{p}$ in A_a amounts to the number of separable extensions $\kappa(\mathfrak{p})$ lying in the various residue fields, so

$$r^2 = \#\operatorname{Spec} A_a(\overline{\kappa(\mathfrak{p})}) = \sum_i f_i g_i.$$

In total, we see that each e_i must be 1, being unramified follows. ■

2.10 March 22

We finished the proof of the weak Mordell–Weil theorem. I just edited into those notes for continuity reasons.

2.11 March 24

Last class we finished proving the weak Mordell–Weil theorem (Theorem 2.64). Today we begin developing the theory of heights to prove the Mordell–Weil theorem (Theorem 2.63).

Remark 2.66. We do not expect $E(K)$ to be finitely generated when K is merely a local field. Roughly speaking, if $K = \mathbb{C}$, then we can describe our elliptic curve as $\mathbb{C}/(\mathbb{Z} + \mathbb{Z}\tau) \cong \mathbb{C}^\times/\exp(2\pi i\tau)^{\mathbb{Z}}$, which has infinitely many points. If $K = \mathbb{Q}_p$, some similar story is possible; namely, sometimes one can parameterize the points as $K^\times/q^{\mathbb{Z}}$ where $q \in \mathfrak{m}_K\mathcal{O}_K$.

2.11.1 Heights

Roughly speaking, we want to be generated by the "smallest" points on our elliptic curve, but this requires building a notion of "smallest." This is the purpose of heights.

Definition 2.67 (height)**.** Fix an abelian group A. Then a function $h\colon A \to \mathbb{R}$ is a *height function* if and only if it satisfies the following properties.

(a) Additivity: for fixed $Q \in A$, there exists a constant c_Q such that

$$h(P+Q) \le 2h(P) + c_Q$$

for any $P \in A$.

(b) Quadratic: there is $m \ge 2$ and a constant c_A such that

$$h(mP) \ge m^2 h(P) - c_A$$

for any $P \in A$.

(c) Bounded: the set $\{P \in A : h(P) \le c\}$ is finite for each c.

Here is our result.

Proposition 2.68. Fix an abelian group A equipped with a height function $h\colon A \to \mathbb{R}$. If A/mA is finite for all $m \ge 2$, then A is finitely generated.

Proof. Because our height function is quadratic, we can find representatives for A/mA for the m satisfying our quadratic condition; let the representatives be $Q_1, \dots, Q_r$, and to help us later, we let c_Q to be the maximum of c_{Q_i} over all Q_i. Now, for any $P_0 \in A$, we may write

$$P_0 = mP_1 + Q_{i_1}$$

for some P_1; repeating this process inductively, we see that we get

$$P_k = mP_{k+1} + Q_{i_{k+1}}$$

for each k. This is an issue because it looks like the height of P is getting smaller and smaller unless this vanishes. In particular, for each $k \ge 1$, we see

$$\begin{aligned} h(P_k) &\le \frac{1}{m^2}\left(h(mP_k) + c_A\right) \\ &\le \frac{1}{m^2}\left(h(P_{k-1} - Q_{k-1}) + c_A\right) \\ &\le \frac{1}{m^2}\left(2h(P_{k-1}) + c_Q + c_A\right). \end{aligned}$$

Working inductively, we see that

$$h(P_n) \le \left(\frac{2}{m^2}\right)^n h(P_0) + \left(\frac{1}{m^2} + \frac{2}{m^4} + \cdots + \frac{2^{n-1}}{m^{2n}}\right)(c_Q + c_A)$$

for any n. We now bound the geometric sum as

$$h(P_n) < \left(\frac{2}{m^2}\right)^n h(P_0) + \frac{c_A + c_Q}{m^2 - 2} \le 2^{-n} h(P) + \frac{c_A + c_Q}{2}.$$

Thus, for n, large enough, we see that each P_n has height bounded by $1 + \frac{c_A + c_Q}{2}$, so we may go ahead and claim that

$$\left\{P \in A : h(P) \le 1 + \frac{c_A + c_Q}{2}\right\} \cup \{Q_1, \dots, Q_r\}$$

will generate A. Indeed, for any $P_0 \in A$, we run the above process, we see that P_n has height bounded by $1 + \frac{c_A + c_Q}{2}$ for n large enough, so then we have

$$P_0 = Q_{i_1} + mQ_{i_2} + m^2 Q_{i_3} + \cdots + m^n Q_{i_n} + m^n P_n,$$

which completes the proof. ∎

Remark 2.69. The rationals $\mathbb{Q}^\times$ has a height function given by $\frac{a}{b} \mapsto \log(|b|) + \log(|a|)$ (where b is chosen to be minimal), but $\mathbb{Q}^\times$ is not finitely generated because $\mathbb{Q}^\times / \mathbb{Q}^{\times m}$ isn't finite for any $m \geq 2$!

2.11.2 Heights for Elliptic Curves

So to prove Theorem 2.63, it suffices to build a height function.

Definition 2.70. Fix a number field K. Define the function $H_K : \mathbb{P}^n_K \to \mathbb{R}_{>0}$ by

$$H_K([x_0 : \ldots : x_n]) = \prod_{v \in M_K} \max\{|x_0|_v, \ldots, |x_n|_v\}^{n_v}$$

where M_K is the set of places of K defined to extend the standard absolute values, and $n_v \coloneqq [K_v : \mathbb{Q}_p]$ where v lies over p. Then we define $H \coloneqq H_K^{1/[K:\mathbb{Q}]}$ and $h \coloneqq \log H_K$ to be a function $\mathbb{P}^n_K \to \mathbb{R}$.

Remark 2.71. Let's take a moment to explain this definition. Suppose we have a K-point in $\mathbb{P}^n_K$. This amounts to a morphism $K \to \mathbb{P}^n_{\mathbb{Z}}$, which is equivalent data to a line bundle $\mathcal{L}$ on K with generating sections $(x_0, \ldots, x_n)$. By clearing denominators in the $x_\bullet$, this provides a surjection $\mathcal{O}_K^{\oplus(n+1)} \to \mathcal{L}$. In total, we are being given two different projective modules L and $\mathcal{O}_K$ sitting in $L \otimes_{\mathcal{O}_K} K$, and then our height h is essentially measuring the difference between these.

Lemma 2.72. Fix a number field K. The function H_K is well-defined.

Proof. To begin, we remark that the product defining H is a finite product because any $x_\bullet \in K$ is going to be a unit in all but finitely many v, so only finitely many factors of the product are not equal to 1. So we can at least evaluate H on a vector $(x_0, \ldots, x_n)$.

Now, given $\lambda \in K^\times$, we must check that $H(x_0, \ldots, x_n) = H(\lambda x_0, \ldots, \lambda x_n)$. Well,

$$\begin{aligned} H(\lambda x_0, \ldots, \lambda x_n) &= \prod_{v \in M_K} \max\{|\lambda x_0|_v, \ldots, |\lambda x_n|_v\}^{n_v} \\ &= \prod_{v \in M_K} |\lambda|_v^{n_v/[K:\mathbb{Q}]} \cdot \prod_{v \in M_K} \max\{|\lambda x_0|_v, \ldots, |\lambda x_n|_v\}^{n_v}. \end{aligned}$$

The product formula tells us that the λ term vanishes, so we are done. ∎

Lemma 2.73. Fix an extension of number fields L/K. Then the diagram commutes, where the map $\mathbb{P}^n_k \subseteq \mathbb{P}^n_L$ is induced by $K \subseteq L$.

Proof. Track around the definitions and the definitions of our absolute values. ∎

Lemma 2.74. Fix a number field K. Then $\operatorname{im} H_K \subseteq [1, \infty)$.

Proof. Any vector $[x_0 : \ldots : x_n] \in \mathbb{P}^n_K$ can be scaled so that one of the x_i is equal to 1 (by placing it in a distinguished affine open subscheme), but then

$$\max\{|x_0|_v, \ldots, |x_n|_v\} \geq 1$$

for each $v \in M_K$, so the entire produce must be bounded below by 1, so $H_K([x_0 : \ldots : x_n]) \geq 1$ follows. ■

2.12 April 3

There will be no class or office hours on April 5 or April 12. Professor Olsson will post details about the term paper later today.

2.12.1 Finiteness of Heights

Last class we constructed a candidate height function H_K on $\mathbb{P}^n_K$ where K is a number field. To define our height function h on (E, e) over the field K, we use the composite

$$E(K) \to \mathbb{P}^1_K(K) \xrightarrow{\log H} \mathbb{R},$$

where $E \to \mathbb{P}^1_K$ is the hyperelliptic projection. Our next goal is to show that this function satisfies the conditions of being a height function given in Definition 2.67. Today we will focus on showing (c).

Lemma 2.75. Define $H \colon \mathbb{P}^n(\overline{\mathbb{Q}}) \to \mathbb{R}$ by $H(P) := H_K(P)^{1/[K:\mathbb{Q}]}$ where P is defined over K. Then $H(\sigma P) = H(P)$ for any $\sigma \in \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

Proof. Note that H does not depend on K by Lemma 2.73, so we might as well show that $H_K(P) = H_{\sigma K}(\sigma P)$. By expanding K to be Galois, we might as well assume that $K = \sigma K$. Then for any place $p \in M_{\mathbb{Q}}$, we claim

$$\prod_{v|p} \max\{|x_0|_v, \ldots, |x_n|_v\} \stackrel{?}{=} \prod_{v|p} \max\{|\sigma x_0|_v, \ldots, |\sigma x_n|_v\},$$

where $P = [x_0 : \ldots : x_n]$. But σ will only permute these places v dividing p by uniqueness of extending a place from $\mathbb{Q}$ to K, so we finish. ■

Lemma 2.76. Fix a constant C. Then the set $\{P \in \mathbb{P}^n_{\mathbb{Q}}(\mathbb{Q}) : H(P) \leq C\}$ is finite.

Proof. By scaling P appropriately, we may assume that $P = [x_0 : \ldots : x_n]$ where the x_i are integers with $\gcd(x_0, \ldots, x_n) = 1$. Essentially, one just needs to clear denominators.[2] We can now just compute directly. Indeed, for each prime p, we note that $|x_i|_p \leq 1$ for each i, and $\gcd(x_0, \ldots, x_n) = 1$ enforces that p does not divide at least one x_i, so

$$\max\{|x_0|_p, \ldots, |x_n|_p\} = 1.$$

Thus, all finite places disappear from our computation, and we are left with

$$H(P) = \max\{|x_0|_\infty, \ldots, |x_n|_\infty\},$$

and there are indeed only finitely many points $(x_0, \ldots, x_n)$ with $|x_i|_\infty \leq C$ for each i; in fact, there are at most $(2C+1)^{n+1}$ of them. ■

To continue, we use the following notation.

[2] Alternatively, one can use the valuative criterion: the map $P \colon \operatorname{Spec} \mathbb{Q} \to \mathbb{P}^n$ extends (uniquely) to a map $\operatorname{Spec} \mathbb{Z} \to\!\!\to \mathbb{P}^n$. To see that $\gcd(x_0, \ldots, x_n) = 1$ with this map, it is enough to note that the relevant map $\mathbb{Z}^n \to \mathbb{Z}$ is surjective, which comes from the injectivity of the map $\operatorname{Spec} \mathbb{Z} \to \mathbb{P}^n$.

Lemma 2.77. Fix a polynomial $f(t) \in \overline{\mathbb{Q}}[t]$ of degree d, and write

$$f(t) = a_0 t^0 + a_1 t^1 + \cdots + a_d t^d = a_d(t - \alpha_1) \cdots (t - \alpha_d).$$

Then

$$H([a_0 : \ldots : a_d]) \leq 2^{d-1} \prod_{i=1}^{d} H(\alpha_i),$$

where $H(\alpha_i) \coloneqq H([\alpha_i : 1])$.

Proof. Scaling the coefficients a_i will not affect either side of the inequality, so we may assume that $a_d = 1$. Now, by Vieta's formulae, we make work everywhere in $K \coloneqq \mathbb{Q}(\alpha_1, \ldots, \alpha_d)$. For notional reasons, we set $\varepsilon(v) \coloneqq 1 + 1_{v|\infty}$ so that

$$|x + y|_v \leq \varepsilon(v) \max\{|x|_v, |y|_v\}$$

for each place v. For any fixed place v, our goal is to show

$$\max\{|\alpha_0|_v, \ldots, |\alpha_d|_v\} \leq \varepsilon(v)^{d-1} \prod_{i=1}^{n} H(\alpha_i),$$

which will finish after taking an infinite product over all factors. (Notably, there are $[K : \mathbb{Q}]$ infinite places counted with multiplicity, so $H = H_K^{1/[K:\mathbb{Q}]}$ will perfectly cancel these places.) Well, for $d = 1$, we have $a_1 = -\alpha_1$, so there is nothing to say here. Then for our induction, we reorder our roots so that $|\alpha_1|_v$ is the largest absolute value. We now set

$$g(t) \coloneqq \frac{f(t)}{t - \alpha_1} = (t - \alpha_2) \cdots (t - \alpha_d) = b_{d-1} t^{d-1} + b_{d-2} t^{d-2} + \cdots + b_1 t + b_0,$$

where (for example) $b_{d-1} = 1$. By expanding, we see that $f(t) = (t - \alpha_1) g(t)$ implies $a_i = b_{i-1} - \alpha_1 b_i$ for each i. In total, we see

$$\begin{aligned}
\max_{0 \leq i \leq d} \{|a_i|_v\} &= \max_{0 \leq i \leq d} \{|b_{i-1} - \alpha_1 b_i|_v\} \\
&\leq \max_{0 \leq i \leq d} \varepsilon(v) \max\{|b_{i-1}|_v, |\alpha_1 b_i|_v\} \\
&\leq \varepsilon(v) \max_i \{|b_i|_v\} \max\{|\alpha_1|_v, 1\} \\
&\leq \varepsilon(v) \left(\varepsilon(v)^{d-2} \prod_{j=2}^{n} \max\{|\alpha_j|_v, 1\} \right) \max\{|\alpha_1|_v, 1\} \\
&\leq \varepsilon(v)^{d-1} \prod_{j=1}^{n} \max\{|\alpha_j|_v, 1\},
\end{aligned}$$

which is what we wanted. ∎

Remark 2.78. There is also a lower bound to the above result, but we don't need it.

And now here is our main bounding result.

Theorem 2.79. Fix a constants C and $d > 0$. Then

$$\#\{P \in \mathbb{P}^n(\overline{\mathbb{Q}}) : H(P) \leq C, [\mathbb{Q}(P) : \mathbb{Q}] \leq d\} < \infty.$$

Proof. For any $P = [x_0 : \dots : x_n]$, we see

$$H_{\mathbb{Q}(P)}(P) = \prod_v \max_i \{|x_i|_v\} \geq \max_i \prod_v \max\{|x_i|_v, 1\} = \max_i H_{\mathbb{Q}(P)}(x_i),$$

where the second inequality holds because the left factor takes the largest factor for each place v, and the second factor includes fewer large factors. Notably, $H(P) \leq C$ and $[\mathbb{Q}(P) : \mathbb{Q}] \leq d$ implies that $H(x_i) \leq C$ and $[\mathbb{Q}(x_i) : \mathbb{Q}] \leq d$ for each i, so by taking the union over all possible coordinates appropriately, it is enough to show that

$$\#\{x \in \overline{\mathbb{Q}} : H(x) \leq C, [\mathbb{Q}(x) : \mathbb{Q}] \leq d\} < \infty$$

for any C and d. Well, for any x in the above set, we let its set of Galois conjugates be $\{x_1, \dots, x_e\}$ so that the previous lemma yields

$$f_x(t) \coloneqq (t - x_1) \cdots (t - x_e) = a_e t^e + a_{e-1} t^{e-1} + \cdots + a_1 t + a_0$$

has

$$H([a_0 : \dots : a_e]) \leq 2^{e-1} \prod_i H(x_i) = 2^{e-1} H(x)^e \leq (2C)^d.$$

However, each element $x \in \overline{\mathbb{Q}}$ yields a unique point $[a_0 : \dots : a_e]$ on the other side, but there are only finitely many of these such points by Lemma 2.76. ∎

It follows that our height function h has the desired finiteness because the hyperelliptic projection $E \to \mathbb{P}^1_k$ is a 2-to-1 map, and we have the finiteness of $\mathbb{P}^1_k$.

2.13 April 7

Please send Professor Olsson a short email of about 1 paragraph to propose a term-paper topic.

2.13.1 Heights as Quadratic Forms

We are going to want the following result.

Theorem 2.80 ([Sil09, p. VIII.5.6]). Fix a map $f \colon \mathbb{P}^N_k \to \mathbb{P}^M_k$ of degree d. Then there are constants c_1 and c_2 such that

$$c_1 H(P)^d \leq H(f(P)) \leq c_2 H(P)^d.$$

In other words, $\log H(f(P)) = d \log H(P) + O(1)$.

Proof. Omitted for now. ∎

Now, recall that we defined our height function h_E on $E(\overline{K})$ by

$$E(\overline{K}) \xrightarrow{\pi} \mathbb{P}^1_k(\overline{K}) \xrightarrow{\log H} \mathbb{R},$$

where $\pi \colon E \to \mathbb{P}^1_k$ is the usual double-cover, and $\log H_{\mathbb{P}^1}$ is defined as we've been working. Last class, we showed that this height function h_E satisfies condition (c) for being a height function. It remains to show (a) and (b).

To warm us up, consider the map $\varphi \colon \mathbb{P}^1_k \times \mathbb{P}^1 \to \mathbb{P}^2_k$ by

$$\rho([\alpha_1 : \beta_1], [\alpha_2 : \beta_2]) \coloneqq [\beta_1\beta_2 : \alpha_1\beta_2 + \alpha_2\beta_1 : \alpha_1\alpha_2].$$

One can check by hand that this is base-point-free. The corresponding line bundle here is $\mathcal{O}(1) \boxtimes \mathcal{O}(1) = p_1^*\mathcal{O}(1) \otimes p_2^*\mathcal{O}(1)$. Global sections of this line bundle after looking affine-locally and appropriately gluing turn out to be

$$\Gamma\left(\mathbb{P}^1_k, \mathcal{O}(1)\right) \otimes_k \Gamma\left(\mathbb{P}^1_k, \mathcal{O}(1)\right).$$

Now, the three global sections are $v_1 \otimes v_2$ and $u_1 \otimes v_2 + v_2 \otimes u_1$ and $u_1 \otimes u_2$, where $\mathbb{P}^1 = \operatorname{Proj} k[u_1, v_1]$ and $\mathbb{P}^1 = \operatorname{Proj} k[u_2, v_2]$, respectively. We now have the following computation.

Proposition 2.81. Given $R_1, R_2 \in \mathbb{P}^1(\overline{K})$, we have

$$h_{\mathbb{P}^2}(\rho(R_1, R_2)) = h_{\mathbb{P}^1}(R_1) + h_{\mathbb{P}^1}(R_2) + O(1).$$

Proof. If $R_1 = [1:0]$, then the formulae directly give $h_{\mathbb{P}^1}(\rho(R_1)) = 0$ and

$$\rho(R_1, R_2) = [0 : \beta_2 : \alpha_2] \qquad \text{where} \qquad R_2 = [\alpha_2 : \beta_2].$$

So we see that $h_{\mathbb{P}^2}(\rho(R_1, R_2)) = h_{\mathbb{P}^1}(\rho(R_2))$ in this case. A symmetric argument works for $R_2 = [1:0]$ as well.

Otherwise, we may write $R_1 = [\alpha_1 : 1]$ and $R_2 = [\alpha_2 : 1]$, and we find that $\varphi(R_1, R_2) = [1 : \alpha_1 + \alpha_2 : \alpha_1\alpha_2]$. However, this means that $h_{\mathbb{P}^2}(\rho(R_1, R_2))$ is computing the height of the coefficients of $(T+\alpha_1)(T+\alpha_2)$. On the other hand, $h_{\mathbb{P}^1}(R_1) + h_{\mathbb{P}^1}(R_2)$ computes the height of those roots; thus, we are done by Lemma 2.77 combined with the lower bound which we didn't quite prove in full. ∎

We now return to discuss elliptic curves. Define $G\colon E \times E \to E \times E$ by $(P, Q) \mapsto (P + Q, P - Q)$. Explicitly, on schemes, this map is given by $(\mu, \mu \circ (1, -1))$. We now have the following result.

Proposition 2.82. There is a map $g\colon \mathbb{P}^2_k \to \mathbb{P}^2_k$ of degree 2 such that the following diagram commutes.

$$\begin{array}{ccccc} E \times E & \xrightarrow{(\pi,\pi)} & \mathbb{P}^1 \times \mathbb{P}^1 & \xrightarrow{\rho} & \mathbb{P}^2 \\ \downarrow & & & & \downarrow g \\ E \times E & \xrightarrow{(\pi,\pi)} & \mathbb{P}^1 \times \mathbb{P}^1 & \xrightarrow{\rho} & \mathbb{P}^2 \end{array}$$

Let's explain why this will finish our height computation. Define $\sigma\colon E \times E \to \mathbb{P}^2$ by $\varphi \circ (\pi, \pi)$. Note that

$$h_{\mathbb{P}^2}(\sigma(P+Q, P-Q)) = h_{\mathbb{P}^2}(\sigma \circ G(P, Q)) = h_{\mathbb{P}^2}(g \circ \sigma(P, Q)) = 2h_{\mathbb{P}^2}(\sigma(P, Q)) + O(1),$$

where we have used Theorem 2.80 in the last equality. Continuing, Proposition 2.81 tells us that

$$2h_{\mathbb{P}^2}(\sigma(P, Q)) + O(1) = 2(h_{\mathbb{P}^1}(\pi P) + h_{\mathbb{P}^1}(\pi Q)) + O(1).$$

On the other hand, $h_{\mathbb{P}^2}(\sigma(P+Q, P-Q)) = h_{\mathbb{P}^1}(\pi(P+Q)) + h_{\mathbb{P}^1}(\pi(P-Q))$ by Proposition 2.81 again, so combining yields

$$h_E(P+Q) + h_E(P-Q) = 2h_E(P) + 2h_E(Q) + O(1). \tag{2.1}$$

This is more or less a fuzzy parallelogram law.

Corollary 2.83. Fix an elliptic curve E over a number field K.

(a) Given $Q \in E(K)$, we have $h_E(P+Q) \le 2h_E(P) + O_Q(1)$ for any $P \in E(K)$.

(b) For any $m \ge 0$, we have $h_E(mP) = m^2 h_E(P) + O(m)$.

Proof. For (a), we see that (2.1) tells us that

$$h_E(P+Q) \le h_E(P+Q) + h_E(P-Q) = 2h_E(P) + 2h_E(Q) + O(1) = 2h_E(P) + O_Q(1).$$

Lastly, for (b), we induct on m. For $m = 0$ and $m = 1$, there is nothing to say. To induct, we suppose m and $m+1$, so we compute

$$h_E((m+2)P) = -h_E(mP) + 2h_E((m+1)P) + 2h_E(P) + O(m)$$

from (2.1). By the inductive hypothesis, we achieve

$$h_E((m+2)P) = \left(-m^2 + 2(m+1)^2 + 2\right) h_E(P) + O_m(1) = (m+2)^2 h_E(P) + O(m),$$

which completes the proof. ∎

Remark 2.84. The Néron–Tate "canonical" height takes (2.1) and fixes this into a bona fide quadratic form. Explicitly, one expects that

$$h_E(P) = \frac{1}{4^r} h_E\left(2^r P\right) + O\left(2^{-r}\right)$$

should not really have a big-O term, so we define

$$\hat{h}_E(P) \coloneqq \lim_{r\to\infty} \frac{1}{4^r} h_E\left(2^r P\right),$$

which does indeed converge.

Thus, Corollary 2.83 will complete showing that h_E is a height function. So it remains to show Proposition 2.82.

Proof of Proposition 2.82. For brevity, set $\mathcal{M} \coloneqq \mathcal{O}_E(e)$. By our computation of ρ previously, the map $E \times E \to \mathbb{P}^2$ is given by the line bundle $\mathcal{M}^{\otimes 2} \boxtimes \mathcal{M}^{\otimes 2}$. Notably, $\pi\colon E \to \mathbb{P}^1$ is given by $\mathcal{M}^{\otimes 2}$. As such, we have two steps.

1. We claim $G^*\left(\mathcal{M} \boxtimes \mathcal{M}\right) = \mathcal{M}^{\otimes 2} \boxtimes \mathcal{M}^{\otimes 2}$.
2. We need to check that the sections used to define $\sigma\colon E \times E \to \mathbb{P}^2$ do indeed yield a map g. Explicitly, we want global sections of $\Gamma\left(\mathbb{P}^2, \mathcal{O}_{\mathbb{P}^2}(2)\right)$ making the following diagram commute.

$$\begin{array}{ccc} \Gamma\left(E\times E, \mathcal{M}^{\otimes 4} \boxtimes \mathcal{M}^{\otimes 4}\right) & \longleftarrow & \Gamma\left(E\times E, \mathcal{M}^{\otimes 2} \boxtimes \mathcal{M}^{\otimes 2}\right) \\ \uparrow & & \uparrow \\ \Gamma\left(\mathbb{P}^2, \mathcal{O}(2)\right) & \dashleftarrow & \Gamma\left(\mathbb{P}^2, \mathcal{O}(1)\right) \end{array}$$

We will prove these on Monday. ∎

BIBLIOGRAPHY

[Har77] Robin Hartshorne. *Algebraic Geometry*. Graduate Texts in Mathematics, No. 52. New York: Springer-Verlag, 1977.

[Lam05] Tsit Yuen Lam. *Introduction to Quadratic Forms over Fields*. Graduate Studies in Mathematics. American Mathematics Society, 2005.

[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.

[Ser12] Jean-Pierre Serre. *A Course in Arithmetic*. Graduate Texts in Mathematics. Springer New York, 2012. URL: https://books.google.com/books?id=8fPTBwAAQBAJ.

[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.

[SP] The Stacks project authors. *The Stacks project*. https://stacks.math.columbia.edu. 2022.

List of Definitions