

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]

Contents	2
1 Quadratic Forms	4
1.1 January 18	4
1.1.1 House-Keeping	4
1.1.2 Course Overview	4
1.1.3 Quadratic Forms	6
1.2 January 20	7
1.2.1 Orthogonal Basis	7
1.2.2 Small Dimensions	8
1.3 January 20	10
1.3.1 Hilbert's Theorem 90	10
1.3.2 Hasse–Minkowski	12
1.4 January 25	13
1.4.1 Introducing G -modules	13
1.4.2 Some Functors	14
1.5 January 27	15
1.5.1 Tate Cohomology	15
1.5.2 Cohomology of Cyclic Groups	16
1.6 January 30	17
1.6.1 Cocycles	17
1.7 February 1	19
1.7.1 Yoneda Extensions	19
1.7.2 Hilbert's Theorem 90	20
1.8 February 3	22
1.8.1 Classification of Algebras	22
1.9 February 6	23
1.9.1 Automorphisms of Projective Space	24
1.9.2 Moving to H^2	24
1.10 February 8	26

1.10.1 Cohomology of Unramified Extensions	26
1.11 February 10	28
1.11.1 Finishing Local Class Field Theory	28
Bibliography	31
List of Definitions	32

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 $V(Q) \subseteq \mathbb{P}_K^n$ 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}_K^1 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 $\text{char } K \neq 2$.

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

- Quadratic: $Q(av) = a^2Q(v)$ for all $a \in K$ and $v \in V$.
- Bilinear: the function $B: V^2 \rightarrow K$ defined by $B(v, w) := \frac{1}{2}(Q(v+w) - Q(v) - Q(w))$ 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 $B: V \times V \rightarrow K$. A bilinear form $B: V^2 \rightarrow K$ gives a map $B: V \otimes_K V \rightarrow K$, which gives a map $B^*: V \rightarrow V^\vee$ by the tensor–hom adjunction. (Explicitly, $B^*: v \mapsto B(v, \cdot)$.) 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 $A = (a_{ij})_{1 \leq i, j \leq n}$. Explicitly, we see

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

so $B(e_i, e_j) = a_{ij} = e_i^\top B^* e_j$. 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

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

and so

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

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 $B: V \otimes_K V \rightarrow K$ induces an isomorphism $B^*: V \rightarrow V^\vee$.

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

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

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 $S = (s_{ij})_{1 \leq i, j \leq n}$ is the change-of-basis matrix. Then

$$B(e'_i, e'_j) = \sum_{k=1}^n \sum_{\ell=1}^n s_{ik} s_{j\ell} B(e_k, e_\ell) = \sum_{k=1}^n \sum_{\ell=1}^n s_{ik} a_{k\ell} s_{j\ell} = (S^T A S)_{ij},$$

so $S^T A S$ is our new matrix, meaning we have adjusted our 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 $\det B^* \in K / (K^{\times 2})$, where $B^*: V \rightarrow V^\vee$ is the associated linear transformation. Note that Q is non-degenerate if and only if $\text{disc } Q \neq \{0\}$.

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 $B(e_1, \cdot): V \rightarrow K$, 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 $n := \dim H$. 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

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

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

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

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 $R := Q - cy^2$ 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 $N: K(\sqrt{a}) \rightarrow K$.
- (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 $K(\sqrt{a}, \sqrt{b}) \rightarrow K(\sqrt{ab})$.

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 $Q_1 := x^2$ 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 $K \rightarrow K$.

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

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

for some $x, y \in K$, which is equivalent to $b \in \text{im } N_K^{K(\sqrt{a})}$.

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

$$\begin{array}{ccccc}
 & & K(\sqrt{a}, \sqrt{b}) & & \\
 & \swarrow & | & \searrow & \\
 K(\sqrt{a}) & & K(\sqrt{ab}) & & K(\sqrt{b}) \\
 & \swarrow & | & \searrow & \\
 & & K & &
 \end{array} \tag{1.1}$$

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 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 $K(\sqrt{a}, \sqrt{b}) \rightarrow K(\sqrt{ab})$ if and only if c is in the image of the norm map $K(\sqrt{b}) \rightarrow K$.
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

$$c = \frac{x^2 - by^2}{z^2 - aw^2} = \frac{N_K^{K(\sqrt{b})}(x + b\sqrt{y})}{N_K^{K(\sqrt{a})}(z + w\sqrt{a})},$$

so c is in the image of the map $N_K^{K(\sqrt{a})} = N_K^{K(\sqrt{b})}$ 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

$$c = \frac{x^2 - by^2}{z^2 - aw^2} = \frac{N_K^{K(\sqrt{b})}(x + y\sqrt{b})}{N_K^{K(\sqrt{a})}(z + w\sqrt{a})},$$

which is equivalent to $c = N_K^{K(\sqrt{a})}(\alpha) \cdot N_K^{K(\sqrt{b})}(\beta)$ for some $\alpha \in K(\sqrt{a})$ and $\beta \in K(\sqrt{b})$. We would like this last condition to be equivalent to $c \in N_K^{K(\sqrt{a}, \sqrt{b})}$. 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 $N : K(\sqrt{a}, \sqrt{b}) \rightarrow K(\sqrt{ab})$ if and only if there exist $x \in K(\sqrt{a})$ and $y \in K(\sqrt{b})$ such that

$$c = N_K^{K(\sqrt{a})}(x) \cdot N_K^{K(\sqrt{b})}(y).$$

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

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

where $\sigma: \sqrt{a} \mapsto \sqrt{a}$ and $\sigma: \sqrt{b} \mapsto -\sqrt{b}$ and $\tau: \sqrt{a} \mapsto -\sqrt{a}$ and $\tau: \sqrt{b} \mapsto \sqrt{b}$. (Notably, $\text{Gal}(K(\sqrt{a})/K) = \langle \tau \rangle$ and $\text{Gal}(K(\sqrt{b})/K) = \langle \sigma \rangle$.) 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 $c = N_K^{K(\sqrt{a})}(x) \cdot N_K^{K(\sqrt{b})}(y)$ 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 $\text{Gal}(K(\sqrt{ab})/K) = \{1, \sigma\tau\}$. Thus, this is equivalent to c being in the image of the norm map $N: K(\sqrt{a}, \sqrt{b}) \rightarrow K(\sqrt{ab})$.

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 $z \cdot \sigma(z) = N_{K(\sqrt{a})}^{K(\sqrt{a}, \sqrt{b})}(z)$ is fixed by σ and hence in $K(\sqrt{a})$. Further, we may compute

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

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 $\text{Gal}(L/K) = \langle \sigma \rangle$. If $t \in L$ has $N_K^L(t) = 1$, 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

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

Note we have used the definition of x at $*$. 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 $(1, 0, 0, \dots, 0)$ 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 $L \rightarrow K$ 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 $Q_1(x_1, \dots, x_m) - Q_2(y_1, \dots, y_n)$ 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

$$U := \{a : |1^2 - a|_v < |2 \cdot 1|_v^2\}.$$

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

$$Q(x_1, \dots, x_n) = ax_1^2 + bx_2^2 - R(x_3, \dots, x_n),$$

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 $V(Q) \subseteq \mathbb{P}_{\mathbb{Q}}^2$ 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

$$a\alpha_{1,v}^2 + b\alpha_{2,v}^2 = c_v = R(\alpha_3, \dots, \alpha_n).$$

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 by 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 us 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 $\mathbb{Z}[G] \rightarrow \text{End}(M)$.
- By hitting this with the free-forgetful adjunction, this is equivalent to having a morphism $G \rightarrow \text{Aut}(M)$. We are going to automorphisms because elements of G are invertible, so their image in $\text{End}(M)$ needs to also be invertible.
- There is an action $\cdot : G \times M \rightarrow M$ 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 $g \cdot k := k$ 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 $(-)^G : \text{Mod}_G \rightarrow \text{Ab}$ which sends a G -module M to

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

Alternatively, $M^G \simeq \text{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, M)$. Indeed, a map $\varphi : \text{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, M)$ 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 $\text{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, -)$ is.

There is also a notion of co-invariants, denoted $(-)_G : \text{Mod}_G \rightarrow \text{Ab}$ by

$$M_G := M/I_G M,$$

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 $(-)^G \simeq \text{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, -)$, 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 $x : M \rightarrow M$ for any G -module M . For example, if G is a finite group, define $N_G := \sum_{g \in G} g$. We note $N_G : M \rightarrow M$ actually defines a map $M \rightarrow M^G$: indeed, for any $m \in M$ and $g \in G$, we see

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

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

$$N_G: (-)_G \rightarrow (-)^G.$$

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

$$H^i(G, -) := \text{Ext}_{\mathbb{Z}[G]}^i(\mathbb{Z}, -) \quad \text{and} \quad H_i(G, -) := \text{Tor}_i^{\mathbb{Z}[G]}(\mathbb{Z}, -),$$

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

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

of \mathbb{Z} . Then $H^i(G, M) = H^i(\text{Hom}^\bullet(P_\bullet, M))$ 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 homology. Take G to be a finite group. Fix some projective resolution P_\bullet of \mathbb{Z} . Then we have exact sequences

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

and

$$0 \rightarrow M^G \rightarrow \text{Hom}(P_0, M) \rightarrow \text{Hom}(P_1, M) \rightarrow \text{Hom}(P_2, M) \rightarrow \cdots$$

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

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

where the map $P_0 \otimes M \rightarrow \text{Hom}_{\mathbb{Z}}(P_0, M)$ is given by $P_0 \otimes M \rightarrow M_G \rightarrow M^G \rightarrow \text{Hom}_{\mathbb{Z}}(P_0, M)$. We now define Tate cohomology is the cohomology of this complex, where degree-0 is at $\text{Hom}_{\mathbb{Z}}(P_0, M)$. 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 $i \in \mathbb{Z}$.

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

where N_G is the norm map $N_G: M_G \rightarrow M^G$.

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

- At $i = -1$, we are computing

$$\frac{\ker(P_0 \otimes M \rightarrow M_G \rightarrow M^G)}{\operatorname{im}(P_1 \otimes M \rightarrow P_0 \otimes M)}.$$

However, the image $P_1 \otimes M \rightarrow P_0 \otimes M$ is exactly the kernel of the surjection $P_0 \otimes M \twoheadrightarrow M_G$, so we are just computing the kernel along $M_G \rightarrow M^G$. Indeed, letting I denote the image of $P_1 \otimes M \rightarrow P_0 \otimes M$, we get a morphism of exact sequences as follows.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & I & \longrightarrow & P_0 \otimes M & \longrightarrow & M_G & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow N_G & & \\ 0 & \longrightarrow & 0 & \longrightarrow & M^G & \xlongequal{\quad} & M^G & \longrightarrow & 0 \end{array}$$

Taking kernels, the snake lemma grants us an exact sequence

$$0 \rightarrow I \rightarrow \ker(P_0 \otimes M \rightarrow M^G) \rightarrow \ker(M_G \rightarrow M^G) \rightarrow 0,$$

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

$$\cdots \rightarrow \mathbb{Z}[G] \xrightarrow{T} \mathbb{Z}[G] \xrightarrow{N} \mathbb{Z}[G] \xrightarrow{T} \mathbb{Z}[G] \rightarrow \mathbb{Z} \rightarrow 0,$$

where $\mathbb{Z}[G] \rightarrow \mathbb{Z}$ is the usual augmentation map and $T := (\sigma - 1)$ and $N := N_G$. Indeed, let's see that this is exact.

- Note $\mathbb{Z}[G] \rightarrow \mathbb{Z}$ is of course surjective, so we are exact at \mathbb{Z} .
- Next, we see that the kernel of the map $\mathbb{Z}[G] \rightarrow \mathbb{Z}$ consists of the terms of degree 0, which are \mathbb{Z} -generated by elements of the form $(\sigma^i - \sigma^j)$ for indices i and j , but this means that we are $\mathbb{Z}[G]$ -generated by $(\sigma - 1)$.
- Continuing, the kernel of the map $T: \mathbb{Z}[G] \rightarrow \mathbb{Z}[G]$ 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

$$T \left(\sum_{i=0}^{n-1} a_i \sigma^i \right) = \sum_{i=0}^{n-1} (a_{i-1} - a_i) \sigma^i,$$

where indices are taken $(\text{mod } n)$. 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

$$\sum_{i=0}^{n-1} a \sigma^i = a N_G$$

for some $a \in \mathbb{Z}[G]$. So the kernel here is indeed the image of the map $N: \mathbb{Z}[G] \rightarrow \mathbb{Z}[G]$.

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

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

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

and we can compute the group cohomology via the sequence

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

Splicing these together gives us Tate cohomology, which works properly because the map $M_G \rightarrow M^G$ 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 $\hat{H}^i(G, M)$ 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

$$\frac{K^\times}{N_K^L(L^\times)} = \frac{(L^\times)^G}{N_G(L^\times)} = \hat{H}^0(G, L^\times).$$

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

$$\hat{H}^0(G, L^\times) \rightarrow \prod_v \hat{H}^0(G_v, L_v^\times)$$

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

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 $\text{Mor}([n+1], G)$ at degree n satisfying certain conditions. One can use this to build a space which is contractible and has a free G -action; then $BG := EG/G$ 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 $P_n := \mathbb{Z}[G^{n+1}]$, and define the differential $d: P_n \rightarrow P_{n-1}$ by

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

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

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

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 $\varepsilon: P_0 \rightarrow \mathbb{Z}$ given by $g \mapsto 1$. Additionally, the composite $P_1 \rightarrow P_0 \rightarrow \mathbb{Z}$ 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 $\varepsilon: P_\bullet \rightarrow \mathbb{Z}$ is an (augmented) free resolution. We know that it's free, so it remains to check our exactness. Note we already have surjectivity $P_0 \rightarrow \mathbb{Z}$, 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 $h_n: P_n \rightarrow P_{n+1}$ fitting into the diagram

$$\begin{array}{ccccccc} \cdots & \xrightarrow{d} & P_2 & \xrightarrow{d} & P_1 & \xrightarrow{d} & P_0 \xrightarrow{\varepsilon} \mathbb{Z} \\ & & & \swarrow h_2 & \swarrow h_1 & \swarrow h_{-1} & \\ \cdots & \xrightarrow{d} & P_2 & \xrightarrow{d} & P_1 & \xrightarrow{d} & P_0 \xrightarrow{\varepsilon} \mathbb{Z} \end{array}$$

so that $dh_n + h_{n-1}d = \text{id}$. The point here is that, for $n \geq 1$, we see $z \in \ker(P_n \rightarrow P_{n-1})$ 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 $P_{n+1} \rightarrow P_n$. The exactness will then follow.

For $n \geq -1$, we define $h_n: P_n \rightarrow P_{n+1}$ by

$$h_n(g_0, \dots, g_n) := (1, g_0, \dots, g_n).$$

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

$$\tilde{C}^n(G, M) := \text{Hom}_{\mathbb{Z}[G]}(P_n, M) \subseteq \text{Mor}_G(G^{n+1}, M),$$

and the differential sends $f \in \tilde{C}^n(G, M)$ 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 $\tilde{C}(G, M)$ 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 $\text{Hom}_{\mathbb{Z}[G]}(P_n, M)$ as functions $G^n \rightarrow M$, 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

$$(1, g_1, g_1 g_2, g_1 g_2 g_3, \dots, g_1 \cdots g_n),$$

which makes our differential

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

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

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

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

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

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

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

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 $H^1(X, \mathcal{O}_X^\times) = \text{Pic } X$. 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 $H^1(G, M) = \text{Ext}_{\mathbb{Z}[G]}^1(\mathbb{Z}, M)$, essentially by definition. This in some sense classifies certain exact sequences. Namely, $\text{Ext}_{\mathbb{Z}[G]}^1(\mathbb{Z}, M)$ classifies short exact sequences of G -modules

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

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 $\varphi: \mathcal{E} \rightarrow \mathcal{E}'$ making the diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & M & \longrightarrow & \mathcal{E} & \longrightarrow & \mathbb{Z} \longrightarrow 0 \\ & & \parallel & & \downarrow \varphi & & \parallel \\ 0 & \longrightarrow & M & \longrightarrow & \mathcal{E}' & \longrightarrow & \mathbb{Z} \longrightarrow 0 \end{array}$$

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

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

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

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

$$\begin{aligned} g_1(g_2 \cdot (m, n)) &= g_1 \cdot (g_2m + nf(g_2), n) \\ &= (g_1g_2m + ng_1f(g_2) + nf(g_1), n) \\ &\stackrel{*}{=} (g_1g_2m + nf(g_1g_2), n) \\ &= (g_1g_2) \cdot (m, n) \end{aligned}$$

where we have used the cocycle condition at $*$. 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

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

equipped with a section $s: \mathbb{Z} \rightarrow \mathcal{E}$; 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 $s, s': \mathbb{Z} \rightarrow \mathcal{E}$, 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

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

grants an exact sequence

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

and one can check that the image of 1 under $\mathbb{Z} \rightarrow H^1(G, M)$ 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 $u_\bullet: G \rightarrow M$ is a function satisfying the relation

$$u_{g_1g_2} = u_{g_1} \cdot g_1u_{g_2}.$$

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

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

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

For example, given a K -vector space V_0 , we set $V := V_0 \otimes_K L$ 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 $\text{Mod}_K \rightarrow \text{Mod}(L/K)$ 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

$$u_g e := \varphi_g(e)$$

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 $u_\bullet: G \rightarrow M$ 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 $\text{Mod}(L/K)$. (Notably, the tensor product provides the group structure on these objects.)

We now use Theorem 1.45. Each $(V, \rho) \in \text{Mod}(L/K)$ should actually arise as the form $V_0 \otimes_K L$, and this corresponds to the identity element in $\text{Mod}(L/K)$. 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 $G = \text{Gal}(L/K)$. 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 $\text{Mod}(L/K)$. 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

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

is an isomorphism in the category $\text{Mod}(L \otimes_K \Omega/\Omega)$. 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

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

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 $\Omega := L$. 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 $\text{Mod}(L/K)$.

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

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

We understand $\hat{H}^0(G, L^\times)$ as $K^\times / N_K^L(L^\times)$, and it turns out that $\hat{H}^2(G, L^\times)$ is understood as the “Brauer group” $\text{Br}(L/K)$. 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 $G = \text{Gal}(L/K)$. 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 $\sigma : A \otimes_K L \rightarrow M_n(L)$, so given $g \in G$, we ask if the following diagram commutes.

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

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

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

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

$$f(g) := g\sigma(1 \otimes g)^{-1}\sigma^{-1} \in \text{Aut}_K(M_n(L)).$$

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

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

As an aside, we note that our choice of isomorphism σ is only defined up to an automorphism in $\text{PGL}_n(L)$, 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 $H^1(G, \text{PGL}_n(L))$.

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.

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

In this way, we can upgrade our equivalence $\text{Mod}_K \simeq \text{Mod}(L/K)$ to an equivalence $\text{Alg}(K) \cong \text{Alg}(L/K)$. As such, given our cocycle $f \in H^1(G, \text{PGL}_n(L))$, 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 $Z^1(G, \text{PGL}_n(L))$ with (classes of) K -algebras A equipped with an isomorphism $\sigma: A \otimes_K L \rightarrow M_n(L)$.

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

$$1 \rightarrow L^\times \rightarrow \text{GL}_n(L) \rightarrow \text{PGL}_n(L) \rightarrow 1.$$

Thus, even though we are studying $H^1(G, \text{PGL}_n(L))$, 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 $f: G \rightarrow \text{PGL}_n(L)$, we can choose some lifted map $\tilde{f}: G \rightarrow \text{GL}_n(L)$. Roughly speaking, our element in H^2 will be the obstruction to \tilde{f} producing a cocycle. As such, we want to compute

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

Notably, we can see that this element is trivial in $\text{PGL}_n(L)$ 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 $\text{Br}(L/K) \cong H^2(G, L^\times)$. Here, $\text{Br}(L/K)$ is a further quotient of algebras where for example A is equivalent to $M_n(A)$.

1.9 February 6

Last class we discussed $H^1(G, \text{PGL}_n(L))$. 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 $\mathrm{Aut} \mathbb{P}_L^{n-1} = \mathrm{PGL}_n(L)$. Indeed, for any automorphism α , we can draw the following square.

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

Notably, we can see from this square that $\alpha^* \mathcal{O}_{\mathbb{P}_L^{n-1}}(1)$ is ample¹ and needs to generate $\mathrm{Pic} \mathbb{P}_L^{n-1}$ because α^* is an isomorphism, so we conclude that there is an isomorphism $\alpha^b: \alpha^* \mathcal{O}_{\mathbb{P}_L^{n-1}}(1) \rightarrow \mathcal{O}_{\mathbb{P}_L^{n-1}}$. (This isomorphism is not canonical!) Thus, taking global sections, we are getting a map

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

However, both of these are isomorphic to $Lx_0 \oplus \cdots \oplus Lx_{n-1}$, so the data of (α, α^b) precisely describes an automorphism $L^n \rightarrow L^n$. If you mod out by the information of α^b , 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 $P \times_{\mathrm{Spec} K} \mathrm{Spec} L \cong \mathbb{P}_L^{n-1}$ 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 $V(x^2 + y^2 + z^2) \subseteq \mathbb{P}_k^2$. Notably, the line bundle $\mathcal{O}_{\mathbb{P}_k^2}(1)$ will pull back to $\mathcal{O}_{\mathbb{P}_k^1}(2)$ 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}_K^n . 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

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

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

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

which is a check that we omit.

¹ The ample line bundles in $\mathrm{Pic} \mathbb{P}_L^{n-1}$ are precisely the ones with global sections, and $\alpha^*: \mathrm{Pic} \mathbb{P}_L^{n-1} \rightarrow \mathrm{Pic} \mathbb{P}_L^{n-1}$ 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
 $H^2(\mathrm{GL}_n)$
 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 $f: G^2 \rightarrow L^\times$. Working explicitly, we want $\rho: G \rightarrow \mathrm{GL}_n(L)$ 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 $\bar{\rho}: G \rightarrow \mathrm{PGL}_n(L)$ by modding out by L^\times everywhere.

Well, we use an induced module: set $V := \mathrm{Mor}(G, L)$, which we note has basis given by $e_s(g) := 1_{s=g}(g)$ because G is finite. We may thus define $\rho_g: V \rightarrow V$ given by $\rho_g: e_s \mapsto f(g, s)e_s$. To finish, one can show that this ρ_\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 $A \otimes_K L \cong M_n(L)$ 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

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

Now, define

$$H^2(\mathrm{Gal}(K^{\mathrm{sep}}/K), (K^{\mathrm{sep}})^\times) := \varinjlim_{K \subseteq L \subseteq K^{\mathrm{sep}}} H^2(\mathrm{Gal}(L/K), L^\times).$$

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_n s induce an isomorphism

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

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 $G := \text{Gal}(L/K)$, we have $H^2(G, L^\times) \cong \frac{1}{\#G} \mathbb{Z}/\mathbb{Z}$.
- (b) Taking the direct limit, we have $H^2(G_K, (K^{\text{sep}})^\times) \cong \mathbb{Q}/\mathbb{Z}$.

Let's do the archimedean case first.

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

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

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

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

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

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

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

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 $\hat{H}^i(G, \mathcal{O}_L^\times) = 0$.

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 $\hat{H}^0(G, \mathcal{O}_L^\times) = 0$. By definition of Tate cohomology, it's enough to show that the norm map

$$N_K^L: \mathcal{O}_L^\times \rightarrow \mathcal{O}_K^\times$$

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

$$N_K^L: \left(\frac{\mathcal{O}_L}{\mathfrak{p}_L^n} \right)^\times \rightarrow \left(\frac{\mathcal{O}_K}{\mathfrak{p}_K^n} \right)^\times$$

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.

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

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

$$N_K^L(1 + a\pi_K^n) = \prod_{\sigma \in G} (1 + \sigma(a)\pi_K^n) \equiv 1 + \text{Tr}_K^L(a)\pi_K^n \pmod{1 + \mathfrak{p}_L^n}.$$

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 $\hat{H}^0(\text{Gal}(\mathbb{F}_{q^r}/\mathbb{F}_q), \mathbb{F}_{q^r})$ 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 $L^\times \cong \pi_K^\times \times \mathcal{O}_L^\times$, we use Lemma 1.65 to yield

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

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

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

which is what we wanted. ■

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

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 $H^2(\text{Gal}(K^{\text{sep}}/K), K^{\text{sep}\times}) \cong \mathbb{Q}/\mathbb{Z}$.

1.11.1 Finishing Local Class Field Theory

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

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

Proof. We make a few remarks.

- The functor $(-)^H: \text{Mod}_G \rightarrow \text{Mod}_{G/H}$ preserves injectives. Indeed, this functor has an exact left adjoint: namely, we want an exact functor $L: \text{Mod}_{G/H} \rightarrow \text{Mod}_G$ such that any $M \in \text{Mod}_G$ and $S \in \text{Mod}_{G/H}$ has

$$\text{Hom}_G(LS, M) \simeq \text{Hom}_{G/H}(S, M^H).$$

Well, we simply define LS to be S viewed as a G -module via $G \rightarrow G/H$. Namely, a G -module morphism from $S \rightarrow M$ must be fixed by H because S is a trivial H -module, so we have really defined a morphism $S \rightarrow M^H$ 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 $S \rightarrow I^H$, we want to fill in the following arrow.

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

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.

$$0 \rightarrow M \rightarrow I^0 \rightarrow I^1 \rightarrow I^2 \rightarrow \dots$$

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,

$$\begin{aligned} H^\bullet(H, M) &= H^\bullet(I^{0H} \rightarrow I^{1H} \rightarrow \dots), \\ H^\bullet(G, M) &= H^\bullet(I^{0G} \rightarrow I^{1G} \rightarrow \dots). \end{aligned}$$

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

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

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

$$H^2(G/H, M^H) = \frac{\ker((I^{2H})^{G/H} \rightarrow (I^{3H})^{G/H})}{\text{im}((I^{1H})^{G/H} \rightarrow (I^{2H})^{G/H})} = H^2(G, M),$$

which is what we wanted. ■

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

Corollary 1.70. Fix a local field K . If $H^2(\text{Gal}(K^{\text{sep}}/K^{\text{unr}}), K^{\text{sep}\times}) = 0$, then $H^2(\text{Gal}(K^{\text{sep}}/K), K^{\text{sep}\times}) \cong \mathbb{Q}/\mathbb{Z}$.

Proof. Combine Proposition 1.68 with Corollary 1.67. ■

We now turn to totally ramified extensions L/K . Speaking philosophically, $H^2(\text{Gal}(L/K), L^\times)$ 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 1.71. Fix a totally ramified extension of local fields L/K . Given a K -scheme P_K such that $P_L \cong \mathbb{P}_L^n$, we also have $P_K \cong \mathbb{P}_K^n$.

Proof. We provide a sketch.

1. To begin, one can show there is a closed embedding $P \hookrightarrow \mathbb{P}_K^M$ for some $M > 0$. Roughly speaking, one can pick up a line bundle \mathcal{L}_{P_L} inducing the isomorphism $P_L \cong \mathbb{P}_L^n$, 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 $P_K \rightarrow \mathbb{P}_k^M$, which is good enough.

Well, we would like to chose \mathcal{M}_L coming from \mathbb{P}_L^n such that $\varepsilon: \mathcal{M}^{\otimes \deg \mathcal{L}_{P_K}} \cong \mathcal{L}_{P_L}$ 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}, ρ) where $\rho: k_{\mathcal{U}}(x) \cong K$.

Notably, isomorphisms between such pairs are unique when they exist, but this category of pairs up to isomorphism is still just $\text{Pic } P_K$, 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 $P_{\mathcal{O}_K} \subseteq \mathbb{P}_{\mathcal{O}_K}^N$ with $P_{\mathcal{O}_L} \cong \mathbb{P}_{\mathcal{O}_L}^n$ also grants us a B -point $\text{Spec } \mathcal{O}_L \rightarrow P_{\mathcal{O}_L}$ 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 $A \rightarrow k$ and a morphism $\widehat{\mathcal{O}}_{P_A, x} \rightarrow k$, and we would like to lift this to $\widehat{\mathcal{O}}_{P_A, x} \rightarrow A$, 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. ■

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.

LIST OF DEFINITIONS

Brauer group, [25](#)

discriminant, [7](#)

G -module, [13](#)

non-degenerate, [6](#)

orthogonal, [7](#)

quadratic form, [6](#)

quadratic space, [7](#)

represents, [8](#)

Tate cohomology, [15](#)