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 $R := Q - cy^2$ 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 $Q_1 := x^2$ represents a. (Note Q_1 is non-degenerate: it has discriminant 1.)

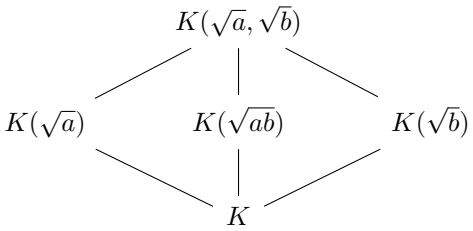
(c) If a is a square, then Q represents 0 (take $(x, y, z) = (\sqrt{a}, 1, 0)$), and b is indeed in the image of the norm map $K \to K$.

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 $z\coloneqq xy$, 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 $y\coloneqq\sigma\tau(z)/x$, 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. ∎

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.

[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