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 0 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.)

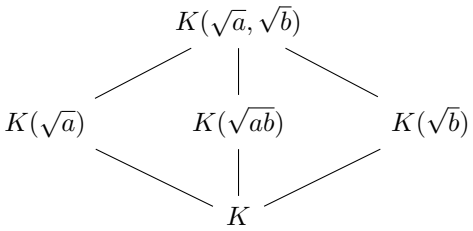
(c) If a is a square, then Q represents 0 (take $(x, y, z) = (\sqrt{a}, 1, 0)$), and b is indeed in the image of the norm map $K \to K$.

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 the following lemma. ■

Lemma 1.22. 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 $\alpha \in K(\sqrt{a})$ and $b \in K(\sqrt{b})$ such that

$$c = \mathrm{N}_K^{K(\sqrt{a})}(\alpha) \cdot \mathrm{N}_K^{K(\sqrt{b})}(\beta).$$

Proof. 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 $\tau\colon \sqrt{b} \mapsto \sqrt{b}$. 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, so this statement 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 $\beta \in K(\sqrt{b})$.

(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. We will finish the proof of this lemma next class. ■

Remark 1.23. 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.

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