Arithmetic Theory of Quadratic Forms

Lecture Notes for Harvard Summer Tutorial 2023

Kush Singhal

3 July - 11 August 2023

Contents

Notation

- $\mathbb{Q}$ denotes the field of rational numbers, and $\mathbb{Z}$ its ring of integers.
- $\mathbb{N}$ denotes the set of positive integers (in particular, we use the convention that $0 \notin \mathbb{N}$).
- Unless otherwise specified, the letter p is always going to denote a prime.
- For $a, b, n \in \mathbb{Z}$, we write $a \equiv b \pmod{n}$ to mean $n|(b-a)$.
- $\mathbb{F}_p$ denotes the finite field with p elements, i.e. $\mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z}$.
- $\mathbb{R}$ denotes the field of real numbers.
- $\mathbb{Q}_p$ will denote the field of p-adic numbers, and $\mathbb{Z}_p$ the ring of p-adic integers.
- Throughout, a ring will be assumed to be unital and commutative. An algebra over a ring will always be assumed to be unital and associative.
- Given a ring R, we write R^* to be the group of units of R. For instance, for k a field, we have $k^* = k\backslash\{0\}$.
- If V and W are vector spaces over k, then $\mathrm{Hom}_k(V, W)$ denotes the k-vector space of all k-linear maps $T : V \to W$. We let $GL(V)$ denote the group of all invertible k-linear maps $T : V \to V$. We write $M_n(k)$ and $GL_n(k)$ for $M(k^n)$ and $GL(k^n)$ respectively.
- For a matrix A, we denote its transpose by A^t.
- The phrase 'almost all' will always mean 'all but finitely many'.

0 Overview

This tutorial is about *quadratic forms*, i.e. quadratic homogeneous polynomials in n variables over various fields and rings. Given a quadratic form, say

$$f(x, y, z) = x^2 + y^2 + 3z^2 + 4xy$$

we can ask a few basic questions:

Q1) Can we understand the set of real numbers/rational numbers/p-adic numbers/integers that can be *represented* by f? More generally, for R some ring or field, which $a \in R$ can be written as

$$f(x, y, z) = a$$

for $x, y, z \in R$?

This question of course has many sub-questions, two examples being:

(a) Is the above set non-empty, i.e. can we find even one such $a \in R$?

(b) Is there an easy way to tell whether $a \in R$ can be represented by f without finding explicit solutions in x, y, z?

Q2) Can we classify quadratic forms? For instance, is there some (relatively) small set S of quadratic forms such that if we can answer the above question for all $f \in S$, then we can actually answer the above question for all quadratic forms?

Q3) Fixing $n \in \mathbb{Z}$, say, can we find the number of solutions to $f(x, y, z) = n$ for $x, y, z \in \mathbb{Z}$? Is the number of solutions finite or infinite? If the number of solutions is finite, can we write down a formula in the variable n?

In this tutorial, we try to answer the above three questions for quadratic forms over $\mathbb{Q}$ and $\mathbb{Z}$. We will see however that in trying to answer the question for the 'global field' $\mathbb{Q}$, we need to in fact answer the above questions for the *completions* of $\mathbb{Q}$, i.e. for $\mathbb{R}$ and for the p-adic numbers. This is the *local-global principle*. This principle is present everywhere in number theory, and guides how much modern research is done. The idea itself is simple: in order to study some object over $\mathbb{Q}$, we try to instead understand this object over each prime individually, and then try to stitch this 'local' information together to gain information about the original 'global' object over $\mathbb{Q}$. The prototypical example of a local-global principle is the *Hasse-Minkowski Theorem* for quadratic forms.

Another key idea is to use linear algebra and geometry to answer the above questions. The basic idea is that quadratic forms correspond to bilinear forms, which behave like inner products in some ways. By exploiting this analogy with inner products on vector space, we will develop a linear algebraic theory of *quadratic spaces* and *lattices*. This theory will lead to deeper insights into quadratic forms. Of course, it should be kept in mind that this will always be an analogy: one can develop the entire theory without having to mention vector spaces at all (indeed, this is what is done in [Cas78]). However, the linear-algebraic theory allows us to state things cleanly, and is a useful source of motivation and intuition.

Finally, towards the end of the tutorial, in our attempt to answer the third question above, we will see how the interplay between analytic and algebraic number theory gives us very explicit results about the number of representations by quadratic forms. This will culminate in the *Siegel-Weil mass formula*.

Of course, the entire story above can be generalised to number fields K and their ring of integers $\mathcal{O}_K$. In fact, we can even generalise the theory to function fields. The Hasse-Minkowski theorem extends to this setting as well, as will pretty much all of the algebraic theory.

For the sake of concreteness, I have decided to stick to $\mathbb{Q}$ and $\mathbb{Z}$ rather than general number fields. However, I will still make brief remarks about the theory over general number fields. Thus, if you are interested in the theory over an arbitrary number field, I would encourage you to read through the remarks I make. Those who are not familiar with the language of number fields may safely skip such remarks. I've tried to state results in as much generality as I can without having to add unnecessary complications.

Let us look at a concrete classical example to get a sense for the kind of results we're after. The binary quadratic form $f = x^2 + y^2$ was first studied by Fermat, and then by Gauss, Jacobi, and a whole litany of other famous number theorists. Fermat gave a complete answer for the first question.

Theorem 0.1 (Fermat)**.** *An odd prime is a sum of two integer squares if and only if it is 1 modulo 4.*
In our terminology, a prime p is represented by the binary quadratic form $f = x^2 + y^2$ over $\mathbb{Z}$ if and only if $p = 2$ or $p \equiv 1 \pmod 4$.

Corollary 0.1.1. *A number $n \in \mathbb{N}$ is represented by $x^2 + y^2$ over $\mathbb{Z}$ if and only if in the prime factorisation $n = p_1^{k_1} \cdots p_r^{k_r}$ for n, the exponent k_i must be even whenever $p_i \equiv 3 \pmod 4$.*

The second question was answered by Gauss in his *Disquisitiones Arithmeticae*. His general body of work on binary quadratic forms is a little too big for this section, but we will satisfy ourselves with the following result just to illustrate a positive answer to the second question above.

Theorem 0.2 (Gauss)**.** *Let $a, b, c \in \mathbb{Z}$, and set $f(x, y) = ax^2 + bxy + c^2$. Then there exist $\alpha, \beta, \gamma, \delta \in \mathbb{Z}$ with $\alpha\delta - \beta\gamma = 1$ and*

$$f(\alpha x + \beta y, \gamma x + \delta y) = x^2 + y^2$$

if and only if $b^2 - 4ac = -4$.

Finally, let us give an answer to the third question for $f = x^2 + y^2$ over $\mathbb{Z}$. Jacobi proved the following result using a very clever argument involving formal power series. However, from the modern perspective, this statement is a direct result of the Siegel-Weil Mass Formula.

Theorem 0.3 (Jacobi)**.** *Let $r(n)$ denote the number of integer solutions (x, y) to $x^2 + y^2 = n$. Then,*

$$r(n) = 4\left(\sum_{d|n, d\equiv 1 \pmod 4} 1 - \sum_{d|n, d\equiv 3 \pmod 4} 1\right),$$

i.e. $\frac{1}{4}r(n)$ is the difference between the number of divisors of n congruent to 1 modulo 4, minus the number of divisors of n congruent to 3 modulo 4.

We will revisit all of the above theorems above later on in the tutorial.

The main reference for the algebraic theory of quadratic forms is the excellent book by Timothy O'Meara [OMe73]. However, this book is quite old and so a lot of the notation and terminology is outdated. O'Meara also works over general number fields rather than just $\mathbb{Q}$. Another good reference is Cassels [Cas78]; the advantage with him is that he only works over $\mathbb{Q}$. For a computational point of view, as well as for applications in error correcting codes and so on, [CS13] is an excellent book. For the latter part on the Siegel-Weil Mass Formula, I don't know of any good complete expository references. I will thus mostly be following [Gar14] and [Li23] for the proof of the Siegel-Weil mass formula, and a variety of modern papers for applications of the formula.

Finally, a word on exercises. I have sprinkled a lot of exercises throughout the notes. These exercises are usually results from one of the references whose proof was straightforward enough. Quite a few of the exercises are extremely easy and can be proved within a couple of lines; most exercises should be easy enough!

1 Quadratic Spaces

Let us first introduce the basic language and terminology of quadratic forms. As mentioned in the overview, our approach is going to be a linear algebraic one, so that we can exploit some of the algebra and geometry inherent in quadratic forms.

Throughout, k is going to denote a field of characteristic not 2.

1.1 Definitions

Recall that a symmetric bilinear form B on a finite dimensional k-vector space V is a mapping

$$B : V \times V \to k$$

such that $B(ax + by, z) = aB(x, z) + bB(y, z)$ for $a, b \in k$ and $x, y, z \in V$, and such that $B(x, y) = B(y, x)$ for $x, y \in V$.

Remark 1.1. Alternatively, a symmetric bilinear form is an element of $\mathrm{Sym}^2(V^*)$.

Given a symmetric bilinear form B on a vector space V, we can set

$$Q : V \to k, \quad Q(x) := B(x, x).$$

Definition. A *quadratic space (over k)* is a finite dimensional vector space V over k equipped with a symmetric bilinear form B.

The *quadratic form* on V associated to B is the above map Q.
The quadratic space is said to be *n-ary* if the underlying space has dimension n. We say a quadratic space is *unary*, *binary*, *ternary*, *quaternary* for $n = 1, 2, 3, 4$ respectively.

We can of course recover the symmetric bilinear form from its corresponding quadratic form via the identity

$$B(x, y) = \frac{1}{2}\left(Q(x + y) - Q(x) - Q(y)\right).$$

Thus we can define a quadratic space by simply defining the associated quadratic form on the vector space.

Example 1.2. If V is a quadratic space, then for any $W \subset V$ a k-linear subspace of V we can restrict the quadratic form Q_V of V to W to get a new quadratic space $(W, Q_V|_W)$. The inclusion map $i : W \hookrightarrow V$ is an isometry.

Example 1.3. Classically, a quadratic form is supposed to be a homogeneous degree 2 polynomial in n variables. We can recover this notion here. Indeed, if $f \in k[x_1, ..., x_n]$ is a degree 2 homogeneous polynomial, then we can simply take $V = k^n$ and define the quadratic form

$$Q(v) = f(v_1, ..., v_n)$$

for $v = (v_1, ..., v_n) \in k^n$.

Example 1.4. Suppose $A \in M_n(k)$ is a symmetric matrix. Then, we can equip $V = k^n$ by the symmetric bilinear form

$$B(x, y) = x^t A y$$

where we view $x, y \in k^n$ as column vectors. This n-ary quadratic space is denoted by $\langle A \rangle$ in [OMe73].

Example 1.5. For $a \in k$, we can define a quadratic space by equipping the 1-dimensional space k by the quadratic form

$$Q_a(b) = ab^2$$

for $b \in k$. This quadratic space will be denoted by $< a >$. Notice that this coincides with the previous example; of course, we have $M_1(k) = k$ and $< a >$ defined here is precisely the quadratic space defined in the above example.

We can also define maps between quadratic spaces, in the obvious way.

Definition. A morphism of quadratic spaces $\sigma : (V, B_V) \to (W, B_W)$ over k is a k-linear map $\sigma : V \to W$ such that $B_W(\sigma v_1, \sigma v_2) = B_V(v_1, v_2)$ for $v_1, v_2 \in V$.

Equivalently, a morphism of quadratic spaces is a k-linear map that preserves the quadratic forms.

Definition. An *isometry* is a morphism of quadratic spaces that is injective.
Two quadratic spaces are *isomorphic* if there exists a surjective isometry between them.
For a quadratic space (V, Q), the *orthogonal group attached to V*, denoted by $O(V, Q)$, is the subgroup of $GL(V)$ consisting of isometries. If the Q is known, we can simply write $O(V)$.

Remark 1.6 (for those who know about reductive group schemes). $O(V)$ is the set of k-points of a certain reductive group scheme over k. In fact, the functor $R \mapsto O(V \otimes_k R)$ is an algebraic group, say denoted by $\mathbf{O}(V)$.

Example 1.7. By fixing a basis $x_1, ..., x_n$ for V, we can write

$$A = \left(B(x_i, x_j)\right)_{1 \le i,j \le n},$$

and then we see easily that $V \cong \langle A \rangle$. This is is the *Gram matrix of V (with respect to the basis $x_1, ..., x_n$).*

Example 1.8. Suppose $A, A' \in M_n(k)$ are symmetric matrices. Then $\langle A \rangle \cong \langle A' \rangle$ if and only if there exists $X \in GL_n(k)$ such that $A' = XAX^t$.

In particular, in the second example above, we see that $\det A' = (\det A)(\det X)^2$. This leads to the following definition.

Definition. The *discriminant* $\mathrm{disc}V$ of a quadratic space V is the element of $\{0\} \cup k^*/(k^*)^2$ given by $(\det A)(k^*)^2$ for any symmetric matrix A such that $V \cong \langle A \rangle$.

It is clear that the discriminant is an invariant of a quadratic space, i.e. $\mathrm{disc}V = \mathrm{disc}V'$ if $V \cong V'$. Note that multiplication of discriminants makes sense.

Finally, recall that we are interested in the set $Q(V)$, motivating the following definitions.

Definition. Let (V, Q) be a quadratic space. An element $a \in k$ is said to be *represented by* Q (or sometimes *represented by* V if the quadratic form on V is clear) if there exists $v \in V$ such that $Q(v) = a$.
A quadratic space is *universal* if $Q(V) = k$, i.e. every element of k is represented by the quadratic form on V.

It is easy to see that a is represented by a quadratic space (V, Q_V) if and only if there is an isometry $(< a >, Q_a) \hookrightarrow (V, Q_V)$.

Even though a quadratic space is a vector space with extra structure, as usual we often abuse notation and say that 'V is a quadratic space over k', when we really mean that V is a vector space over k equipped with a symmetric bilinear form B_V and corresponding quadratic form Q_V. If the vector space is clear from context, we sometimes omit the V from the subscript.

Now that we have a symmetric bilinear form on a vector space, we can try to generalise various notions from an introductory linear algebra course.

Definition. Let V be a quadratic space. Suppose $v, w \in V$. We say that v, w are *orthogonal* (with respect to the quadratic space structure on V) if $B(v, w) = 0$.

Given two subspaces $W_1, W_2 \subset V$ such that $V = W_1 \oplus W_2$ as k-vector spaces, we say that V is the *orthogonal sum of* W_1 *and* W_2, written $V = W_1 \perp W_2$, if every vector in W_1 is orthogonal to every vector in W_2.

Given a subspace $W \subset V$, we write $W^\perp$ to be the subspace of all $v \in V$ such that v is orthogonal to w for all $w \in W$.

A basis $v_1, ..., v_n$ is said to be *orthogonal* if v_i is orthogonal to v_j for all $i \neq j$.

These definitions satisfy various familiar/obvious properties, all of which are left as an exercise.

Exercise 1.9. Suppose V is a quadratic space. Then V always admits an orthogonal basis.

Exercise 1.10. If $V \cong \langle A_1 \rangle \perp \langle A_2 \rangle \perp \cdots \perp \langle A_r \rangle$ for symmetric matrices A_i, then

$$V \cong \left\langle \begin{pmatrix} A_1 & & & \\ & A_2 & & \\ & & \ddots & \\ & & & A_r \end{pmatrix} \right\rangle.$$

Exercise 1.11. If $V \cong W_1 \perp W_2$ then $\mathrm{disc}(V) = \mathrm{disc}(W_1)\mathrm{disc}(W_2)$.

References

[Cas78] John William Scott Cassels. *Rational quadratic forms*. Courier Dover Publications, 1978.

[CS13] John Horton Conway and Neil James Alexander Sloane. *Sphere packings, lattices and groups*. Vol. 290. Springer Science & Business Media, 2013.

[Gar14] Paul Garrett. *Proof of a Simple Case of the Siegel-Weil Formula*. 2014. URL: `https://www-users.cse.umn.edu/~garrett/m/v/easy_siegel_weil.pdf`.

[Li23] Chao Li. "From sum of two squares to arithmetic Siegel–Weil formulas". In: *Bulletin of the American Mathematical Society* (2023).

[OMe73] O. Timothy O'Meara. *Introduction to Quadratic Forms*. Springer-Verlag, New York, 1973.