Number Theory II
Spring 2010 Notes

Kimball Martin

Revised: May 12, 2019

Contents

Exercise 0.1. *Read the introduction. It's a roadmap for the course. In fact, you may want to reread it several times throughout the course to remember where we've been and where we're going.*

Introduction

Last semester, we saw some of the power of Algebraic Number Theory. The basic idea was the following. If for example, we wanted to determine

$$\text{Which numbers are of the form } x^2 + ny^2? \tag{0.1}$$

(For simplicity, assume n is squarefree.) Brahmagupta's composition law tells us that the product of two numbers of this form is again of this form, and therefore it make sense to first ask

$$\text{Which primes } p \text{ are of the form } x^2 + ny^2 = p? \tag{0.2}$$

The idea of Algebraic Number Theory is to work with the ring $\mathbb{Z}[\sqrt{-n}]$ so any p such that $p = x^2 + ny^2 = (x + y\sqrt{-n})(x - y\sqrt{-n})$ factors over $\mathbb{Z}[\sqrt{-n}]$. At this point one would like to use the Prime Divisor Property (or equivalently, Unique Factorization) to say that this means p is not prime in $\mathbb{Z}[\sqrt{-n}]$. Unfortunately this does not always hold in $\mathbb{Z}[\sqrt{-n}]$, and there were two things we did to overcome this obstacle. The first was to work with $\mathcal{O}_{\mathbb{Q}(\sqrt{-n})}$ which is sometimes larger than $\mathbb{Z}[\sqrt{-n}]$, and may have unique factorization when $\mathbb{Z}[\sqrt{-n}]$ does not (we saw this for the case $n = 3$—it happens for other values of n also, but still only finitely many times when $n > 0$).

Otherwise, we should use Dedekind's ideal theory. The main idea here is we have the Prime Divisor Property and Unique Factorization at the level of ideas. Hence if $p = x^2 + ny^2$, the ideal $(p) = p\mathcal{O}_{\mathbb{Q}(\sqrt{-n})}$ in $\mathcal{O}_{\mathbb{Q}(\sqrt{-n})}$ is not a prime ideal and factors into two principal prime ideals (not necessarily distinct) $(p) = \mathfrak{p}_1\mathfrak{p}_2$, each of norm p. Further, $\mathfrak{p}_1 = (x + y\sqrt{-n})$ and $\mathfrak{p}_2 = (x - y\sqrt{-n})$. In fact, with some slight modifications, the converse is also true. To understand this, we first need to understand the more basic question

$$\text{When is } p\mathcal{O}_{\mathbb{Q}(\sqrt{-n})} \text{ a prime ideal, and when does it factor?} \tag{0.3}$$

Once we know for which primes $p \in \mathbb{N}$, (p) is not prime in $\mathcal{O}_{\mathbb{Q}(\sqrt{-n})}$ (in which case we say p *splits* in $\mathbb{Q}(\sqrt{-n})$), we need to know

$$\text{What is the class group of } \mathbb{Q}(\sqrt{-n})? \tag{0.4}$$

to determine when (p) is a product of two principal ideals in $\mathcal{O}_{\mathbb{Q}(\sqrt{-n})}$. The first part of the semester will be motivated by these questions, though we shall spend a lot of our time pursuing related questions and topics along the way. In other words, our goal is not so much to seek a definitive answer to the question (0.2) (see [Cox]), but rather to use it as a guide to understand and pursue some important topics in number theory. Consequently, we will see how these ideas are related to (i) Dirichlet's class number formula, (ii) Dirichlet's theorem that any arithmetic progression with gcd 1 contains infinitely many primes and (iii) Kummer's approach to Fermat's Last Theorem. Some references for this part of the course are [Cohn], [Stewart–Tall], [Borevich–Shafarevich], and [Cox], or more generally, any book on Algebraic Number Theory.

Even knowing an answer to (0.2), we still won't have a complete answer to (0.1), since the converse to Brahmagupta's composition law is not true. For example $6 = x^2 + 5y^2$ for $x = y = 1$,

but neither 2 nor 3 are of the form x^2+5y^2. However, we can explain this via Gauss's theory of quadratic forms, which in this case says the product of any two numbers of the form $2x^2+2xy+3y^2$ is of the form x^2+5y^2. Hence the question of which numbers are of the form x^2+5y^2 doesn't quite reduce to just determining which primes are of this form. In the second part of the course we will use Gauss's theory to determine which numbers are of the form x^2+5y^2 by studying the two forms x^2+5y^2 and $2x^2+2xy+3y^2$ in tandem (as well as understanding where the second form came from). In fact, we will see there is another approach to this question via *Dirichlet's mass formula*, which in this case tells us the number of solutions to $x^2+5y^2=n$ and $2x^2+2xy+3y^2=n$. I will conclude this section on binary quadratic forms by presenting illustrating how these forms can be used to quantitatively study the failure of unique factorization in $\mathcal{O}_{\mathbb{Q}(\sqrt{-5})}$, a very interesting but largely neglectic topic. Some references for this section are [Cohn], [Cox], [Borevich–Shafarevich], [Landau], [Hurwitz], [Dirichlet] and [Narkiewicz]. In addition, many books on quadratic forms cover a large part of the material here, and some of the material in the next part.

The third and final part of the course is motivated by the theory of quadratic forms in n variables. Some of the theory of binary quadratic forms carries over to the case of more variables, but some crucial elements do not. We will not be attempting to develop a theory of quadratic forms in n variables, but rather introduce one of the key elements in this theory, the Hasse-Minkowski principle. Roughly, this principle says the following: an equation *should* have a solution in $\mathbb{Z}$ if and only if it has a solution in $\mathbb{Z}/p^k\mathbb{Z}$ for every prime power p^k. This statement is not true in general, but is in special cases. To understand this principle, we'll talk about valuations and p-adic numbers. The Hasse-Minkowski principle can then be used to prove Gauss's famous theorem about which numbers are the sum of three squares. We will follow [Serre] for this. Another important use of p-adic numbers is the modern formulation of higher reciprocity (higher than quadratic) laws. These higher reciprocity laws are given by *class field theory*, which is typically considered the crowning achievement in Algebraic Number Theory, most cleanly stated in the modern language of adèles. Time permitting, we will conclude with a brief discussion of adèles, class field theory and higher reciprocity laws. Some references this are [Ramakrishnan–Valenza], [Ono], [Kato–Kurokawa–Saito], [Cohn2], [Cohn3]. See also any book on Class Field Theory.

This may sound like a rather ambitious plan, and it is. Number Theory is a very rich subject, and one cannot learn even all the central topics of Algebraic Number Theory in a year long course. Any of these three parts could easily form a one semester long course by themselves (though perhaps the first or third more so than the second), and class field theory itself should be a year-long course. Consequently, we will not pursue many topics as deeply as they may deserve (such as Dirichlet's Units Theorem), but I will mention important results and ideas throughout the text, which will hopefully provide at least a good survey of the subject.

This course is not a standard course in number theory, which is the reason we are not following a text. Part of this is due to the fact that the first semester was a mix of elementary and algebraic number theory, whereas they are usually treated separately. But the main reason is my desire to treat the theory of binary quadratic forms (Questions (0.1) and (0.2) as well as the second part of the course), which is a very beautiful subject (and one of my interests, though not my primary research focus), but largely neglected in most modern treatments of Algebraic Number Theory (e.g., [Neukirch], [Marcus], [Janusz], [Lang], [Stewart–Tall], [Murty–Esmonde]). Notable exceptions are [Borevich–Shafarevich], [Cohn], and of course [Cox]. However [Borevich–Shafarevich] does not seem appropriate as a text for this class, [Cohn] virtually only treats quadratic fields, and [Cox] already assumes a fair amount of knowledge of algebraic number theory (he reviews it, but omits many

proofs). Additionally, [Cohn] and [Cox] say nothing about p-adic numbers. Conversely most books on quadratic forms do not seem to contain much algebraic number theory, and have a different focus than I intend for the course.

Furthermore, while the bulk of the first and third part of the course *are* part of a standard course in Algebraic Number Theory (usually without adèles), most Algebraic Number Theory courses in my experience focus on building up general theory for a long time, often requiring sizable tangents to develop the tools to prove theorems, before being able to get to many applications. While we will treat general number fields throughout the course (and see places where we need them for applications), we will in several places restrict our development of the theory to the case of quadratic fields (though not to the extent of [Cohn]), such as with Minkowski's theory or the class number formula. One critique of this approach might be that one loses much depth this way, however I believe we will gain at least as much as we lose, by being able to go that much deeper into the study of quadratic fields and quadratic forms, thus gaining a more complete and global understanding of the "quadratic" theory, and hopefully a better appreciation of the subject. And in the future, if you need to understand some aspects of the general theory, it would be good to first understand what happens in the simplest setting, that of quadratic fields.

In fact, it is with future aims in mind, that I want to spend a considerable amount of time at the end of the semester on p-adic numbers and adèles. Specifically, they are (i) crucial to understanding modern number theory, (ii) something you need to know about if you end up working with Ameya Pitale, Alan Roche, Ralf Schmidt or myself, and (iii) something that comes up often in the representation theory seminar. During the last week of the course, I will plan on giving survey lectures about class field theory, higher reciprocity laws, and how this leads into the *Langlands Program*, which is the general framework for most of the number theory research going on at OU and OSU.

Finally, since we will be using primarily my notes and not a text, please let me know of any possible errors or unclear portions you may find in the notes so I can address them.

I would like to thank my students for pointing out numerous errors and giving feedback. I hope you know who you are, because I no longer remember who exactly helped me provided feedback. Kudos also go to Keith Conrad, Filippo Alberto Eduardo and Victor Flynn for reporting other errors.

Part I
The first part

1 Number Fields

I will assume that every one is familiar with the material in the first year algebra sequence, notably groups, rings, fields, ideals and Galois theory, as well as the material from Number Theory I, though I will review some of the key definitions and results which the undergraduates may not be familiar with, and perhaps the graduate students have forgotten. In this first section, we will go over the basics of number fields, which will largely be a review of the second half of last semester, with some generalizations of notions introduced in the context of quadratic fields. However some fundamental notions will be new to us, such as discriminants. We will for the most part omit proofs of results covered last semester (even if we only sketched the proof) or in a standard Algebra course. For complete proofs, refer to any standard texts on Algebra and Algebraic Number Theory. Since the material in this chapter should be largely familiar to you, and the point is to fill in some things we missed last semester, we will go through this section rather quickly.

The presentation of the material in this chapter is based on [Stewart–Tall].

1.1 Algebraic Numbers

Let $R[x]$ denote the ring of polynomials in x with coefficients in a ring R. We say $p(x) \in R[x]$ is **monic** if the leading coefficient of $p(x)$ is 1. (All rings for us are commutative with 1.) By the Fundamental Theorem of Algebra, any polynomial in $\mathbb{Q}[x]$ factors into linear factors in $\mathbb{C}$. We say $\alpha \in \mathbb{C}$ is an **algebraic number** if it is the root of some $p(x) \in \mathbb{Q}[x]$ (or equivalently a polynomial in $\mathbb{Z}[x]$, but then we can't assume it's monic). Without loss of generality we may assume $p(x)$ is monic. If $p(x)$ is of smallest degree such that this is true, and we say $p(x)$ is the **minimum polynomial** of α (over $\mathbb{Q}$), and the **degree** $\deg(\alpha)$ of α defined to be the $\deg(p(x))$. If in fact $p(x) \in \mathbb{Z}[x]$, we say α is an **algebraic integer**.

Some basic facts from algebra are that

(i) the minimum polynomial $p(x)$ of α is uniquely determined (which is why we make the monic condition),

(ii) $p(x)$ is irreducible over $\mathbb{Q}$ (and therefore $\mathbb{Z}$ if $p(x) \in \mathbb{Z}[x]$), and

(iii) if $q(x) \in \mathbb{Z}[x]$ and $q(\alpha) = 0$, then $p(x)|q(x)$ ($\mathbb{Q}[x]$ or $\mathbb{Z}[x]$ if $p(x) \in \mathbb{Z}[x]$).

Lemma 1.1.1. *Let $\alpha \in \mathbb{C}$. Then $[\mathbb{Z}[\alpha] : \mathbb{Z}] < \infty$ if and only if α is an algebraic integer. In this case $\{1, \alpha, \cdots, \alpha^{m-1}\}$ is a $\mathbb{Z}$-basis of $\mathbb{Z}[\alpha]$ where $m = \deg(\alpha)$.*

This was Proposition 10.9 from last semester.

Lemma 1.1.2. *Suppose α is an algebraic number. Then $c\alpha$ is an algebraic integer for some $c \in \mathbb{Z}$.*

Proof. Suppose the minimum polynomial for α is $p(x) = x^n + \frac{a_{n-1}}{b_{n-1}}x^{n-1} + \cdots + \frac{a_1}{b_1}x + \frac{a_0}{b_0}$ where each $a_i, b_i \in \mathbb{Z}$. Let $c = b_0 b_1 \cdots b_{n-1}$. Then $p(\frac{y}{c}) = \frac{y^n}{c^n} + \frac{a_{n-1}}{b_{n-1}c^{n-1}}y^{n-1} + \cdots + \frac{a_1}{b_1 c}y + \frac{a_0}{b_0}$. Multiplying by c^n, we see

$$q(y) = c^n p(\frac{y}{c}) = y^n + \frac{a_{n-1}c}{b_{n-1}}y^{n-1} + \cdots \frac{a_1 c^{n-1}}{b_1}y + \frac{a_0 c^n}{b_0} \in \mathbb{Z}[y].$$

But $q(c\alpha) = c^n p(\alpha) = 0$, so y is an algebraic integer. □

Recall from algebra that if R is an integral domain (not the zero ring and has no zero divisors), we can form the smallest field F containing R by considering the set of fractions $F = \left\{\frac{a}{b} : a, b \in R, b \neq 0\right\}$. This is called the **field of fractions** or **fraction field** of R.

Theorem 1.1.3. *The set $\mathbb{B}$ of all algebraic integers form a subring of $\mathbb{C}$, and the set $\mathbb{A}$ of all algebraic numbers form its field of fractions.*

We omitted the proof last semester, so here it is, in all its glory.

Proof. Note that by the Lemma 1.1.1, $\mathbb{B}$ consists precisely of all elements $\alpha \in \mathbb{C}$ such that $[\mathbb{Z}[\alpha] : \mathbb{Z}] < \infty$. To show it is a subring of $\mathbb{C}$, we want to show if $\alpha, \beta \in \mathbb{B}$, then so are $\alpha + \beta, \alpha - \beta$ and $\alpha\beta$. But these elements are all clearly in $\mathbb{Z}[\alpha, \beta]$, and

$$[\mathbb{Z}[\alpha, \beta] : \mathbb{Z}] = [\mathbb{Z}[\alpha, \beta] : \mathbb{Z}[\alpha]] \cdot [\mathbb{Z}[\alpha] : \mathbb{Z}] \leq [\mathbb{Z}[\beta] : \mathbb{Z}] \cdot [\mathbb{Z}[\alpha] : \mathbb{Z}] < \infty.$$

Since $\mathbb{Z}[\alpha + \beta]$, $\mathbb{Z}[\alpha - \beta]$ and $\mathbb{Z}[\alpha\beta]$ are all contained in $\mathbb{Z}[\alpha, \beta]$, they must all have finite degree.

To see that $\mathbb{A}$ is its field of fractions, one runs through the same argument for fields. Namely, one shows that $[\mathbb{Q}(\alpha) : \mathbb{Q}] < \infty$ if and only if α is algebraic. The above argument shows $\mathbb{A}$ is a field. Lemma 1.1.2 shows that any element of $\mathbb{A}$ is a quotient of two elements in $\mathbb{B}$. □

Exercise 1.1. *Show by example that $[\mathbb{Z}[\alpha, \beta] : \mathbb{Z}[\alpha]]$ need not equal $[\mathbb{Z}[\beta] : \mathbb{Z}]$.*

Definition 1.1.4. *Let K be a subfield of $\mathbb{C}$ We say K is a* **number field** *if $[K : \mathbb{Q}] < \infty$. Its* **ring of integers** *is $\mathcal{O}_K = \mathbb{B} \cap K$.*

From now on we let K denote a number field.

Proposition 1.1.5. *K is the field of fractions of $\mathcal{O}_K$.*

This follows from Lemma 1.1.2 as in the proof of Theorem 1.1.3.

Proposition 1.1.6. *We have $K = \mathbb{Q}(\alpha)$ for some algebraic integer α.*

This is the Primitive Element Theorem from Galois theory. Here α is called a **primitive element** for K (over $\mathbb{Q}$).

Proposition 1.1.7. *We have $[K : \mathbb{Q}] = [\mathcal{O}_K : \mathbb{Z}]$.*

Proof. Let $\alpha_1, \ldots, \alpha_n$ be a $\mathbb{Z}$-basis for $\mathcal{O}_K$. By Lemma 1.1.2, any $x \in K$ is a $\mathbb{Q}$-linear combination of $\alpha_1, \ldots, \alpha_n$. Hence to see $\alpha_1, \ldots, \alpha_n$ is a $\mathbb{Q}$-basis for K it suffices to show they are linearly independent of $\mathbb{Q}$. Suppose $\frac{a_1}{b_1}\alpha_1 + \cdots + \frac{a_n}{b_n}\alpha_n = 0$ for some $a_i, b_i \in \mathbb{Z}$. Multiplying through by $b_1 b_2 \cdots b_n$, the fact that the α_i's are linearly independent over $\mathbb{Z}$ (and no $b_i = 0$) implies each $a_i = 0$. □

If $L \subseteq \mathbb{C}$ is a field containing K and $[L : K]$ is finite, we say L is a finite **extension** of K of **degree** $[L : K]$. Clearly this means L is also a number field since $[L : \mathbb{Q}] = [L : K] \cdot [K : \mathbb{Q}]$.

Corollary 1.1.8. *If L is a finite extension of K, then $[L : K] = [\mathcal{O}_L : \mathcal{O}_K]$.*

Proof. $[L : K] = [L : \mathbb{Q}]/[K : \mathbb{Q}] = [\mathcal{O}_L : \mathbb{Z}]/[\mathcal{O}_K : \mathbb{Z}] = [\mathcal{O}_L : \mathcal{O}_K]$. □

Suppose K is a *quadratic field*, i.e., $[K:\mathbb{Q}]=2$. Recall that we may write $K=\mathbb{Q}(\sqrt{d})$ where $d\in\mathbb{Z}$ is squarefree (and $d\neq 1$). Recall d squarefree means $n^2|d \implies n^2=1$.

Example 1.1.9. *Suppose $d\in\mathbb{Z}$ is squarefree, $d\neq 1$, and let $K=\mathbb{Q}(\sqrt{d})$. Then*

$$\mathcal{O}_K=\begin{cases}\mathbb{Z}[\frac{1+\sqrt{d}}{2}] & d\equiv 1 \bmod 4\\ \mathbb{Z}[\sqrt{d}] & d\equiv 2,3 \bmod 4.\end{cases}$$

If $d>0$, we say K is a **real quadratic field** *since $K\subseteq\mathbb{R}$. There are infinitely many units of $\mathcal{O}_K$, and they are generated by a fundamental unit $\epsilon=x+y\sqrt{n}$ (the smallest $\epsilon>1$ such that $N(\epsilon)=x^2-ny^2=\pm 1$) and -1.*

If $d<0$, we say K is an **imaginary quadratic field** *since $K\not\subseteq\mathbb{R}$. Here there are only finitely many units of $\mathcal{O}_K$, and precisely they are $\pm 1,\pm i$ (the 4-th roots of unity) if $d=-1$; they are $\pm 1,\pm\zeta_3,\pm\zeta_3^2$ (the 6-th roots of unity) if $d=-3$; and they are ± 1 (the 2-nd roots of unity) otherwise.*

(Recall the units of a ring R are the set of invertible elements and they are a group under multiplication.)

1.2 Some Galois theory

Let L/K be an extension of number fields of degree n, i.e., $[L:K]=n$. An embedding of $L\hookrightarrow\mathbb{C}$ is a field homomorphism from L into $\mathbb{C}$, i.e., a map $\sigma:L\to\mathbb{C}$ such that $\sigma(x+y)=\sigma(x)+\sigma(y)$, $\sigma(xy)=\sigma(x)\sigma(y)$, $\sigma(-x)=-\sigma(x)$ and $\sigma(x^{-1})=\sigma(x)^{-1}$. Necessarily $\sigma(0)=0$, $\sigma(1)=1$, and consequently σ fixes $\mathbb{Q}$, i.e., $\sigma(x)=x$ for each $x\in\mathbb{Q}$.

Example 1.2.1. *Let $L=\mathbb{Q}(i)$. A $\mathbb{Q}$-basis for L is $\{1,i\}$. If $\sigma:L\hookrightarrow\mathbb{C}$ is an embedding, it fixes 1, so it is determined by what it does to i. We must have $\sigma(i)^2=\sigma(i^2)=\sigma(-1)=-1$ so i must map to a square root of -1, i.e., either i or $-i$. One may check that both of these give embeddings, $\sigma_j:\mathbb{Q}(i)\to\mathbb{C}$ given by $\sigma_1(a+bi)=a+bi$ (the trivial embedding), and $\sigma_2(a+bi)=a-bi$ (complex conjugation).*

The **Galois group** of L/K, denoted $\mathrm{Gal}(L/K)$ is the group of all embeddings of $L\hookrightarrow\mathbb{C}$ which fix (each element of) K. The **Galois closure** of L/K is the smallest extension L' of L such that each $\sigma\in\mathrm{Gal}(L/K)$ maps into L'. We say the extension L/K is **Galois** if $L'=L$.

Example 1.2.2. *$K=\mathbb{Q}$ and $L=\mathbb{Q}(i)$. Every embedding of L into $\mathbb{C}$ fixes K, so $\mathrm{Gal}(L/K)=\{\sigma_1,\sigma_2\}$ from the example above. Every embedding lies in L, so L/K is Galois.*

By the Primitive Element Theorem, we may write $L=K(\alpha)$ where α is an algebraic integer. Let $f(x)\in K[x]$ be the minimum polynomial for α over K. This means $f(x)$ is the irreducible monic polynomial of smallest possible degree with coefficients in K (in fact $\mathcal{O}_K$ since α is an integer) such that $f(\alpha)=0$. It is not difficult to show that $\deg(f(x))=n$ (in fact, we already did in the case $K=\mathbb{Q}$).

Example 1.2.3. *$K=\mathbb{Q}(\sqrt{2})$ and $L=\mathbb{Q}(\sqrt[4]{2})=K(\alpha)$ where $\alpha^2=\sqrt{2}\in K$. The minimum polynomial for α over K is $f(x)=x^2-\sqrt{2}$. (Contrast this with the minimum polynomial for α over $\mathbb{Q}$: $p(x)=x^4-2$, of degree 4).*

Exercise 1.2. *In the above example, show L/K is Galois, but $L/\mathbb{Q}$ is not.*

Theorem 1.2.4. *Suppose $L = K(\alpha)$ and $f(x)$ is the minimum polynomial of α over K. The n roots of $f(x)$ are all distinct, call them $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_n$. Every embedding of $L \hookrightarrow \mathbb{C}$ permutes the roots $f(x)$, and $\mathrm{Gal}(L/K)$ acts transitively on the roots. Conversely, every embedding $L \hookrightarrow \mathbb{C}$ is uniquely determined by the way it permutes the roots of $f(x)$. Therefore, $\mathrm{Gal}(L/K)$ is isomorphic to a transitive subgroup of S_n. Further the Galois closure of L/K is $L' = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$, i.e., L/K is Galois if and only if L contains all the root of $f(x)$.*

See any reference on Galois theory. Here S_n denotes the symmetric group on n-letters, i.e., the permutations of $\{1, 2, \ldots, n\}$. Note that $L' = K(\alpha_1, \ldots, \alpha_n)$ is often called the **splitting field** of $f(x)$ (over K), since it is the smallest field such that $f(x)$ splits into linear factors.

Corollary 1.2.5. *Any quadratic extension L/K (i.e., $[L : K] = 2$) is Galois.*

Proof. Write $L = K(\alpha)$ and $f(x)$ as the minimum polynomial for α over K. It is immediate from the quadratic formula that once L contains one root of $f(x)$, it contains the other. Hence L/K is Galois by the above theorem. □

Example 1.2.6. *Let $n > 0$. The splitting field for $f(x) = x^2 + n$ over $K = \mathbb{Q}$ is $L = \mathbb{Q}(\sqrt{-n})$. This also splits the quadratic form $x^2 + ny^2$. The extension L/K is Galois by the above corollary, and the Galois group is given by the maps $\sigma_1(a + b\sqrt{-n}) = a + b\sqrt{-n}$ and $\sigma_2(a + b\sqrt{-n}) = a - b\sqrt{-n}$. The map σ_1 corresponds to the trivial permutation of the roots $\pm\sqrt{-n}$ of $f(x)$, and σ_2 interchanges these two roots.*

Exercise 1.3. *Let $K = \mathbb{Q}$ and $L = \mathbb{Q}(\sqrt[3]{2})$. Determine the splitting polynomial $f(x)$ for $\alpha = \sqrt[3]{2}$ over K. Using the above theorem, answer the following. (i) Is L/K Galois? If not, find the Galois closure. (ii) Determine $\mathrm{Gal}(L/K)$ explicitly (either as embeddings or permutations of roots of $f(x)$.*

All of the above is covered in any standard lectures on Galois theory (though we haven't stated the main theorems of Galois theory), but now we will be introducing notions that are more properly a part of a course on Algebraic Number Theory.

Definition 1.2.7. *Let $\alpha \in L$. The* **conjugates** *of α in L/K are the elements $\alpha^\sigma = \sigma(\alpha)$ where $\sigma \in \mathrm{Gal}(L/K)$. The* **norm** *of α from L to K is $N_{L/K}(\alpha) = \prod_{\sigma \in \mathrm{Gal}(L/K)} \alpha^\sigma$ and the* **trace** *of α from L to K is $\mathrm{Tr}_{L/K}(\alpha) = \sum_{\sigma \in \mathrm{Gal}(L/K)} \alpha^\sigma$.*

In the case $K = \mathbb{Q}$ and L is understood, we simply write $N(\alpha)$ and $\mathrm{Tr}(\alpha)$ for $N_{L/K}(\alpha)$ and $\mathrm{Tr}_{L/K}(\alpha)$. It is a standard fact from Galois theory that $\alpha \in L$ in fact lies in K if and only if $\alpha^\sigma = \alpha$ for each $\sigma \in \mathrm{Gal}(L/K)$.

Warning: If L/K is not Galois, then the conjugates of α in L/K may not lie in L. Precisely, if L/K is not Galois, then there exist $\sigma \in \mathrm{Gal}(L/K)$ such that the image of σ is not contained in L. Hence there is some $\alpha \in L$ such that the conjugate $\sigma(L) \notin L$. What is true is that they always lie in the Galois closure L' of L, by definition of the Galois closure.

Example 1.2.8. *Let $L = \mathbb{Q}(\sqrt{d})$ and $K = \mathbb{Q}$. For $\alpha = a + b\sqrt{d} \in L$, $N_{L/K}(\alpha) = N(\alpha) = a^2 - db^2$ and $\mathrm{Tr}_{L/K}(\alpha) = \mathrm{Tr}(\alpha) = 2a$.*

Lemma 1.2.9. *The norm map is multiplicative and the trace map is additive. For $\alpha \in L$, $N_{L/K}(\alpha)$, $\mathrm{Tr}_{L/K}(\alpha) \in K$. Further, if $\alpha \in \mathcal{O}_L$, then $N_{L/K}(\alpha) \in \mathcal{O}_K$ and $\mathrm{Tr}_{L/K}(\alpha) \in \mathcal{O}_K$.*

Proof. The first statement is immediate from the definitions. The second statement is true since the product and sum of all the conjugates of α are invariant under $\mathrm{Gal}(L/K)$, and therefore lie in K. For the last statement, observe α is an algebraic integer if and only if each of its conjugates are (since they all have the same minimum polynomial). □

Corollary 1.2.10. *Let α be an algebraic number of degree 2 and $L = \mathbb{Q}(\alpha)$. Then α is an algebraic integer if and only if $N_{L/\mathbb{Q}}(\alpha), \mathrm{Tr}_{L/\mathbb{Q}}(\alpha) \in \mathbb{Z}$.*

Proof. The $\Rightarrow$ direction follows from the lemma. The other direction follows from the fact that the minimum polynomial of α is $x^2 - \mathrm{Tr}_{L/\mathbb{Q}}(\alpha)x + N_{L/\mathbb{Q}}(\alpha)$, which was an exercise last semester. □

Note that this is not true for algebraic numbers of higher degree. In general if α is of degree n, one needs to consider the symmetric functions $\tau_j : L \to \mathbb{Q}$ where $L = \mathbb{Q}(\alpha)$ and $\tau_j(x)$ is the sum of all products of j conjugates. For instance if $x_1 = x, x_2, \ldots, x_n$ denote the n conjugates (not necessarily distinct numbers) of x, then

$$\begin{aligned}
\tau_1(x) =& x_1 + x_2 + \ldots + x_n = \mathrm{Tr}_{L/\mathbb{Q}}(x) \\
\tau_2(x) =& x_1x_2 + x_1x_3 + \cdots + x_1x_n + x_2x_3 + \cdots x_2x_n + \cdots + x_{n-1}x_n \\
& \vdots \\
\tau_n(x) =& x_1x_2 \cdots x_n = N_{L/\mathbb{Q}}(x).
\end{aligned}$$

Then one can show the minimum polynomial for α is

$$x^n + (-1)^{n-1}\tau_1(\alpha)x^{n-1} + \cdots - \tau_{n-1}(\alpha)x + \tau_n(\alpha).$$

Exercise 1.4. *Suppose $\alpha, \beta \in L$ are conjugates in L/K. Show $N_{L/K}(\alpha) = N_{L/K}(\beta)$ and $\mathrm{Tr}_{L/K}(\alpha) = \mathrm{Tr}_{L/K}(\beta)$.*

Exercise 1.5. *Let $\alpha \in \mathcal{O}_K$. Prove α is a unit of $\mathcal{O}_K$ if and only if $N_{K/\mathbb{Q}}(\alpha) = \pm 1$.*

Exercise 1.6. *Write down a $\mathbb{Q}$-basis for $K = \mathbb{Q}(\sqrt[3]{2})$. For each α in this basis, compute $N_{K/\mathbb{Q}}(\alpha)$ and $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha)$.*

Exercise 1.7. *Let $K = \mathbb{Q}(\sqrt{2})$ and $L = K(\sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Write down a $\mathbb{Q}$-basis for L. Compute $\mathrm{Gal}(L/K)$ and $\mathrm{Gal}(L/\mathbb{Q})$. (Hint for those who haven't seen Galois theory before: it's not so easy to find a primitive element for $L/\mathbb{Q}$ and determine its minimum polynomial, so it's better to just use the definition of the Galois group. Of course, if you know Galois theory, there are other ways to determine $\mathrm{Gal}(L/\mathbb{Q})$ and you may do it any you like.) For each α in this basis compute $N_{L/K}(\alpha)$ and $N_{L/Q}(\alpha)$. Check that $N_{L/\mathbb{Q}}(\alpha) = N_{K/\mathbb{Q}}(N_{L/K}(\alpha))$.*

One thing you may have noticed in the examples and exercises above is that $\mathrm{Gal}(L/K)$ tends to equal $[L : K]$. In fact this is always true and is one of the standard results in Galois theory, though you may have only proved it for Galois extensions.

Proposition 1.2.11. $|\mathrm{Gal}(L/K)| = [L : K]$.

Proof. Write $L = K(\alpha)$. Then $1, \alpha, \ldots, \alpha^{n-1}$ is a $\mathbb{Q}$-basis for K. Thus an embedding $\sigma : L \to \mathbb{C}$ which fixes every element of K is determined by what it does to α.

Let $f(x)$ be the minimum polynomial of α, which has degree $n = [L : K]$. Since σ is a field homomorphism, $\sigma(\alpha)$ must also have minimum polynomial $f(x)$. Since $f(x)$ has n distinct roots, $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_n$, there are n possibilities for $\sigma \in \mathrm{Gal}(L/K)$ given by $\sigma(\alpha) = \alpha_i$. One formally checks that each of these give an embedding into $\mathbb{C}$. □

1.3 Discriminants

Let K be a number field, $n = [K : \mathbb{Q}]$. Then $|\mathrm{Gal}(K/\mathbb{Q})| = n$. Write $\mathrm{Gal}(K/\mathbb{Q}) = \{\alpha_1, \ldots, \alpha_n\}$.

Definition 1.3.1. *Let $\{\alpha_1, \ldots, \alpha_n\}$ be a $\mathbb{Q}$-basis for K. The* **discriminant** *of $\{\alpha_1, \ldots, \alpha_n\}$ is*

$$\Delta[\alpha_1, \ldots, \alpha_n] = \det\left(\sigma_i(\alpha_j)\right)^2.$$

If $\alpha_1, \ldots, \alpha_n$ is a $\mathbb{Z}$-basis for $\mathcal{O}_K$, we define the **discriminant** *of K to be $\Delta_K = \Delta[\alpha_1, \ldots, \alpha_n]$.*

If R is a ring, we define the $M_n(R)$ to be the set of $n \times n$ matrices with coefficients in R. This is also a ring, with the obvious identity element, and the invertible elements of $M_n(R)$ form a group under multiplication, denoted by $\mathrm{GL}_n(R)$, and called the **general linear group** of rank n over R. If R is an integral domain, then $A \in M_n(R)$ lies in $\mathrm{GL}_n(R)$ if and only if $\det(A)$ is a unit in R.

Lemma 1.3.2. *Let $\{\alpha_1, \ldots, \alpha_n\}$ and $\{\beta_1, \ldots, \beta_n\}$ be two $\mathbb{Q}$-bases for K. Then we can write*

$$\begin{pmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_n \end{pmatrix} = C \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix}$$

for some $C \in \mathrm{GL}_n(\mathbb{Q})$. Then $\Delta[\beta_1, \ldots, \beta_n] = \det(C)^2 \Delta[\alpha_1, \ldots, \alpha_n]$.

Further, if $\{\alpha_1, \ldots, \alpha_n\}$ and $\{\beta_1, \ldots, \beta_n\}$ are $\mathbb{Z}$-bases (also called **integral bases***) for $\mathcal{O}_K$, then we may take $C \in \mathrm{GL}_n(\mathbb{Z})$. in the above. Consequently, $\Delta[\beta_1, \ldots, \beta_n] = \Delta[\alpha_1, \ldots, \alpha_n]$, i.e., Δ_K does not depend on the choice of the integral basis for $\mathcal{O}_K$.*

Proof. The fact that there is some such C is elementary linear algebra. The equation about determinants follows from $(\sigma_i(\beta_j)) = C\,(\sigma_i(\alpha_j))$, which holds because each σ_i fixes $\mathbb{Q}$. (If this isn't clear to you, just write out the equations $\beta_k = \sum c_{jk}\alpha_j$ for, say $n = 2$ or 3, and apply each σ_i.)

The second paragraph follows in the same way. Here we note that if $C \in \mathrm{GL}_n(\mathbb{Z})$, then $\det(C) = \pm 1$, so $\det(C)^2 = 1$. This provides at least one explanation for why we look at the *square* of the determinant in the definition of the discriminant—so that we can define Δ_K as an invariant of a number field, independent of choice of basis for $\mathcal{O}_K$. □

Exercise 1.8. *A priori, the discriminant $\Delta[\alpha_1, \ldots, \alpha_n]$ is defined for an* ordered $\mathbb{Q}$*-basis $\alpha_1, \ldots, \alpha_n$ of K. Show that the above lemma implies this discriminant does not depend upon the order, i.e., for any $\tau \in S_n$, show $\Delta[\alpha_{\tau(1)}, \ldots, \alpha_{\tau(n)}] = \Delta[\alpha_1, \ldots, \alpha_n]$.*

Note: the quantity $\det(\sigma_i(\alpha_j))$, which is one of the square roots of the discriminant, is called the **different** of $\{\alpha_1, \alpha_2, \cdots, \alpha_n\}$. We will not use the different in this course (I don't think), but you may see come up if it you look at other texts.

A note on terminology: one can form the different and discriminant for an arbitrary collection of n integers $\alpha_1, \ldots, \alpha_n$. Then the discriminant and different are nonzero if and only if $\alpha_1, \ldots, \alpha_n$ are linearly independent, i.e., form a $\mathbb{Q}$-basis for K. Furthermore, if $\alpha_1, \ldots, \alpha_n$ and $\beta_1, \ldots, \beta_n$ have different discriminants then the *submodules* $M = \{\sum n_i\alpha_i : n_i \in \mathbb{Z}\}$ and $N = \{\sum n_i\beta_i : n_i \in \mathbb{Z}\}$ are distinct.

Example 1.3.3. *Let $d \neq 1$ be a squarefree integer and $K = \mathbb{Q}(\sqrt{d})$. Suppose $d \equiv 2, 3 \bmod 4$ so $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$. We can take $\{\alpha_1, \alpha_2\} = \left\{1, \sqrt{d}\right\}$ as a choice for an integral basis for $\mathcal{O}_K$. We can write $\mathrm{Gal}(K/\mathbb{Q}) = \{\sigma_1, \sigma_2\}$ where σ_1 is trivial and σ_2 permutes $\sqrt{d}$ and $-\sqrt{d}$. Hence the matrix*

$$(\sigma_i(\alpha_j)) = \begin{pmatrix} 1 & \sqrt{d} \\ 1 & -\sqrt{d} \end{pmatrix},$$

which has determinant $-2\sqrt{d}$. Hence the discriminant of K is $\Delta_K = \Delta[1, \sqrt{d}] = 4d$.

Exercise 1.9. *Let $d \neq 1$ be a squarefree integer and $K = \mathbb{Q}(\sqrt{d})$. Suppose $d \equiv 1 \bmod 4$. Compute the discriminant Δ_K of K.*

Exercise 1.10. *Let K be a quadratic field of discriminant Δ. Show*

(i) $\Delta \equiv 0, 1 \bmod 4$,

(ii) K is uniquely determined by Δ, and

(iii) we can write

$$\mathcal{O}_K = \left\{ \frac{x + y\sqrt{\Delta}}{2} : x, y \in \mathbb{Z}, x \equiv 0 \bmod 2 \right\}$$

if $\Delta \equiv 0 \bmod 4$, and

$$\mathcal{O}_K = \left\{ \frac{x + y\sqrt{\Delta}}{2} : x, y \in \mathbb{Z}, x \equiv y \bmod 2 \right\}$$

if $\Delta \equiv 1 \bmod 4$.

Part (ii) of the above exercise means that the discriminant is a complete invariant for quadratic fields. The point of part (iii) is that, while there is a fundamental difference between $\mathcal{O}_K$ when $\Delta_K \equiv 0 \bmod 4$ and $\Delta_K \equiv 1 \bmod 4$ (which correspond to $d \neq 1 \bmod 4$ and $d \equiv 1 \bmod 4$ for $K = \mathbb{Q}(\sqrt{d})$ with d squarefree), we can always write an element of $\mathcal{O}_K$ of the form $\frac{x+y\sqrt{\Delta}}{2}$ with some simple congruence conditions on x, y. This will be useful when we want to treat both the $\Delta \equiv 0 \bmod 4$ and the $\Delta \equiv 1 \bmod 4$ cases together.

Now let's return to discriminants of general number fields.

Lemma 1.3.4. *Let $\alpha_1, \ldots, \alpha_n$ be a $\mathbb{Q}$-basis for K. Then $\Delta[\alpha_1, \ldots, \alpha_n] \in \mathbb{Q} \setminus \{0\}$. If $\alpha_1, \ldots, \alpha_n \in \mathcal{O}_K$, then $\Delta[\alpha_1, \ldots, \alpha_n] \in \mathbb{Z} \setminus \{0\}$.*

Proof. By the previous lemma, the discriminants of any two bases for K differ by rational squares. Hence it suffices to check that it is true for a single $\mathbb{Q}$-basis of K. Then the second statement follows from the first, since the discriminant is then a polynomial expression of algebraic integers, and thus an algebraic integer itself.

We can write $K = \mathbb{Q}(\alpha)$ where α is some algebraic number (integer if we like) of degree n. Then $\left\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\right\}$ is a $\mathbb{Q}$-basis for K. Let $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_n$ denote the (distinct) conjugates of

α. Then the conjugates of α^i are $\alpha_1^i = \alpha^i, \alpha_2^i, \ldots, \alpha_n^i$. Hence the determinant of this basis is the square of the discriminant of

$$A = \begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 & \cdots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \cdots & \alpha_2^{n-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \alpha_n & \alpha_n^2 & \cdots & \alpha_n^{n-1} \end{pmatrix}.$$

This matrix is a Vandermonde matrix, and it is a standard algebra exercise that this has determinant $\prod_{1 \le i < j \le n}(\alpha_j - \alpha_i)$. (The determinant is a polynomial in the α_i's, and clearly it is zero if some $\alpha_i = \alpha_j$, so each polynomial $\alpha_j - \alpha_i$ divides the determinant. Then one counts the degree of the polynomial, to show that this is correct up to a constant. Comparing coefficients of one of the terms gives the Vandermonde determinant formula. You could also prove this by induction, but the above argument seems simpler.)

Hence $\Delta[\alpha_1, \ldots, \alpha_n] = \prod_{i \neq j}(\alpha_j - \alpha_i)$. Note any $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ simply permutes the terms in this product, i.e., $\Delta[\alpha_1, \ldots, \alpha_n]$ is $\mathrm{Gal}(K/\mathbb{Q})$-invariant, and thus in $\mathbb{Q}$. It is clear from the product expression that it is nonzero. □

Exercise 1.11. *Verify the Vandermonde determinant formula given above for $n = 2$ and $n = 3$.*

While, the determination of $\mathcal{O}_K$ was simple for quadratic fields K, in general it is not so easy. There are algorithms to determine $\mathcal{O}_K$, but we will not focus on this problem in general, as we will only need explicit determinations of $\mathcal{O}_K$ in special cases. However, we will briefly indicate how one can use discriminants to help find a ring of integers. It suffices to find an integral basis for $\mathcal{O}_K$.

1. Guess a possible integral basis $\{\beta_1, \cdots, \beta_n\}$ for $\mathcal{O}_K$. Suppose $\{\alpha_1, \ldots, \alpha_n\}$ is an actual integral basis for $\mathcal{O}_K$. Then $\Delta[\beta_1, \cdots, \beta_n] = \det(C)^2 \Delta[\alpha_1, \ldots, \alpha_n] = \det(C)^2 \Delta_K$. In other words, $\Delta[\beta_1, \cdots, \beta_n]$ is a square (in $\mathbb{Z}$) times Δ_K. Hence if $\Delta[\beta_1, \ldots, \beta_n]$ is squarefree, then $\{\beta_1, \ldots, \beta_n\}$ is an integral basis for $\mathcal{O}_K$.

2. If $\Delta[\beta_1, \cdots, \beta_n]$ is not squarefree, $\{\beta_1, \cdots, \beta_n\}$ may still be a basis (see Example 1.3.3 above), but if it is not, then $\mathcal{O}_K$ contains an integer of the form $\frac{1}{p}(c_1\beta_1 + c_2\beta_2 + \cdots + c_n\beta_n)$ for some $c_n \in \mathbb{Z}$ and p is some prime such that $p^2 | \Delta[\beta_1, \cdots, \beta_n]$. Check to see if any numbers of this form give any new algebraic integers not generated by $\beta_1, \ldots, \beta_n$. If so, suitably modify the choice of $\beta_1, \ldots, \beta_n$ and repeat. If not, then $\beta_1, \ldots, \beta_n$ is an integral basis of $\mathcal{O}_K$.

Exercise 1.12. *In the last section, we considered general extensions of number fields L/K. One reason you might want to do this is the following. We want to use $K = \mathbb{Q}(\sqrt{-5})$ to study the form $x^2 + 5y^2$. However $\mathcal{O}_K$ does not have unique factorization. But we can embed K in the field $L = \mathbb{Q}(\sqrt{-5}, i)$ which does have unique factorization. Now one wants do determine $\mathcal{O}_L$. A first guess might be $\{1, \sqrt{-5}, i, \sqrt{5}\}$ is an integral basis for $\mathcal{O}_L$. It is certainly a $\mathbb{Q}$-basis for L. Compute the discriminant of this $\mathbb{Q}$-basis. Can you determine $\mathcal{O}_L$?*

However we will primarily be concerned with other applications of discriminants this semester, most immediately to ideals in the next section.

Discriminants are a fundamental invariant of number fields. Another thing they provide is natural way to at least partially order number fields. (There are only finitely many fields of a fixed discriminant.) The quadratic fields $\mathbb{Q}(\sqrt{d})$ can easily be ordered by d (which actually is a function of the discriminant, but how can one order fields of a more complicated form, such as $\mathbb{Q}(\sqrt{3}, \sqrt{-19})$

and $\mathbb{Q}(\sqrt{-7}, \sqrt{11})$?) Once one has some sort of ordering, it is meaningful to ask questions like what percentage of fields (of a certain type) have class number 1 or 2, or more generally, how many fields up to a certain point satisfy Property X?

We also remark that there is a geometric interpretation of determinants (and differents), which comes from the geometric interpretation of discriminants. For now, we will just mention it in the simplest case $K = \mathbb{Q}(\sqrt{-d})$ where $d > 0$ squarefree. Then if α, β is a $\mathbb{Q}$-basis for K, α and β generate a lattice $\Lambda = \langle \alpha, \beta \rangle = \{m\alpha + n\beta : m, n \in \mathbb{Z}\}$. Then $\text{vol}(\mathbb{C}/\Lambda) = \frac{1}{2}\sqrt{-\Delta[\alpha, \beta]}$. In particular, $\Delta_K = -4\text{vol}(\mathbb{C}/\mathcal{O}_K)^2$. We can state an analogue of this for arbitrary number fields when we study the *geometry of numbers*.

1.4 Ideals

Let K be a number field. Recall $\mathcal{I}$ is an **ideal** of $\mathcal{O}_K$ if $\mathcal{I}$ is a nonempty subset of $\mathcal{O}_K$ which is closed under addition and multiplication by $\mathcal{O}_K$. The **norm** of an ideal $\mathcal{I}$ of $\mathcal{O}_K$ is $N(\mathcal{I}) = |\mathcal{O}_K/\mathcal{I}|$.

Lemma 1.4.1. *For any nonzero ideal $\mathcal{I}$ of $\mathcal{O}_K$, the norm $N(\mathcal{I}) = |\mathcal{O}_K/\mathcal{I}|$ is always finite. Furthermore, if $\beta_1, \ldots, \beta_n$ is a $\mathbb{Z}$-basis for $\mathcal{O}_K$, then $N(\mathcal{I}) = \sqrt{\frac{\Delta[\beta_1, \ldots, \beta_n]}{\Delta_K}}$.*

Recall a **free abelian group of rank** n is a group isomorphic to $\mathbb{Z}^n$. For the proof, we use the fact that if A is a free abelian group of rank n, and B is a subgroup of A, then B is also free abelian of rank $\leq n$.

Proof. Let $n = [K : \mathbb{Q}]$. Then $\mathcal{O}_K$ is a free abelian group of rank n (w.r.t. addition). We can regard $\mathcal{I}$ as a subgroup of $\mathcal{O}_K$, which must also be free of rank $\leq n$. Let $i \in \mathcal{I}$ be nonzero. Then $(\mathcal{O}_K i, +)$ is a (free abelian) subgroup of $(\mathcal{I}, +)$ of rank n, hence $\mathcal{I}$ has rank n.

Now we let $\beta_1, \cdots, \beta_n$ be a $\mathbb{Z}$-basis for $\mathcal{I}$. Then there is a $\mathbb{Z}$-basis $\alpha_1, \cdots, \alpha_n$ of $\mathcal{O}_K$ such that for each i we can write $\beta_i = c_i\alpha_i$ for some $c_i \in \mathbb{Z}$. Then it is clear $\mathcal{O}_K/\mathcal{I} = \prod C_{c_i}$, where C_r denotes the cyclic group of order r. In particular $N(\mathcal{I})$ is finite.

Moreover, we have

$$\begin{pmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_n \end{pmatrix} = \begin{pmatrix} c_1 & & & \\ & c_2 & & \\ & & \ddots & \\ & & & c_n \end{pmatrix} \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix}.$$

By Lemma 1.3.2, we have $\Delta[\beta_1, \ldots, \beta_n] = N(\mathcal{I})^2\Delta[\alpha_1, \ldots, \alpha_n] = N(\mathcal{I})^2\Delta_K$. This gives the result since $N(\mathcal{I}) \geq 0$. □

Note that the norm of the zero ideal is infinite as we have defined it, though it may make more sense to define it to be 0 in light of the the next result, which relates norms of ideals to norms of elements. In any case, since we have no particular reason to work with the zero ideal, in order to simplify statements we will **from here on, assume all our ideals our nonzero**, unless explicitly stated otherwise.

Proposition 1.4.2. *Suppose $\mathcal{I} = (\alpha)$ is a principal ideal of $\mathcal{O}_K$. Then $N(\mathcal{I}) = |N_{K/\mathbb{Q}}(\alpha)|$.*

Here the norm on the left is the ideal norm, and the norm on the right is the norm of an element.

Proof. Let $\alpha_1, \ldots, \alpha_n$ be a $\mathbb{Z}$-basis for $\mathcal{O}_K$. Then $\beta_1 = \alpha\alpha_1, \ldots, \beta_n = \alpha\alpha_n$ is a $\mathbb{Z}$-basis for $\mathcal{I}$. Write $\mathrm{Gal}(K/\mathbb{Q}) = \{\sigma_1, \ldots, \sigma_n\}$. Note

$$\begin{aligned}
\Delta[\beta_1, \ldots, \beta_n] &= \det \begin{pmatrix} \sigma_1(\alpha)\sigma_1(\alpha_1) & \cdots & \sigma_1(\alpha)\sigma_1(\alpha_n) \\ \vdots & \ddots & \vdots \\ \sigma_n(\alpha)\sigma_n(\alpha_1) & \cdots & \sigma_n(\alpha)\sigma_n(\alpha_n) \end{pmatrix}^2 \\
&= \det \begin{pmatrix} \sigma_1(\alpha) & & & \\ & \sigma_2(\alpha) & & \\ & & \ddots & \\ & & & \sigma_n(\alpha) \end{pmatrix}^2 \det \begin{pmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_1(\alpha_n) \\ \vdots & \ddots & \vdots \\ \sigma_n(\alpha_1) & \cdots & \sigma_n(\alpha_n) \end{pmatrix}^2 \\
&= N_{K/\mathbb{Q}}(\alpha)^2 \Delta[\alpha_1, \ldots, \alpha_n] = N_{K/\mathbb{Q}}(\alpha)^2 \Delta_K.
\end{aligned}$$

Now apply the previous lemma. □

This implies that the ideal norm is multiplicative, at least for principal ideals. Of course, we want to know it's multiplicative for all ideals, and this basically follows from some simple isomorphism theorems, but at one point, to keep our argument as simple as possible, we will use fractional ideals. This is justified by Theorem 1.4.4 below (which we have already given last semester), whose proof does not rely on this result. Recall that the product of two ideals $\mathcal{I}$ and $\mathcal{J}$, is the ideal generated by all elements of the form ij for $i \in \mathcal{I}$ and $j \in \mathcal{J}$, i.e., $\mathcal{I}\mathcal{J} = \{\sum i_m j_m : i_m \in \mathcal{I}, j_m \in \mathcal{J}\}$.

Proposition 1.4.3. *Let $\mathcal{I}$, $\mathcal{J}$ be ideals of $\mathcal{O}_K$. Then $N(\mathcal{I}\mathcal{J}) = N(\mathcal{I})N(\mathcal{J})$.*

Proof. By the ring isomorphism theorem, $\mathcal{O}_K/\mathcal{I} \simeq (\mathcal{O}_K/\mathcal{I}\mathcal{J})/(\mathcal{I}/\mathcal{I}\mathcal{J})$. (Just think about the case where $\mathcal{O}_K = \mathbb{Z}, \mathcal{I} = (m), \mathcal{J} = (n)$. Then this says $\mathbb{Z}/m\mathbb{Z} \simeq (\mathbb{Z}/mn\mathbb{Z})/(m\mathbb{Z}/mn\mathbb{Z})$.) The details are in the exercise below. Hence $N(\mathcal{I}\mathcal{J}) = |\mathcal{I}/\mathcal{I}\mathcal{J}| \cdot N(\mathcal{I})$.

Now it suffices to show $\mathcal{O}_K/\mathcal{J} \simeq \mathcal{I}/\mathcal{I}\mathcal{J}$, say as abelian groups. Consider the map $\phi : \mathcal{O}_K \to \mathcal{I}/\mathcal{I}\mathcal{J}$ given by $\phi(\alpha) = \alpha\mathcal{I} + \mathcal{I}\mathcal{J}$ for $\alpha \in \mathcal{O}_K$. It is clear it is a group homomorphism. Note $\phi(\alpha) = \mathcal{I}\mathcal{J} \iff \alpha\mathcal{I} + \mathcal{I}\mathcal{J} = \mathcal{I}\mathcal{J} \iff \alpha\mathcal{I} \subseteq \mathcal{I}\mathcal{J}$, which, multiplying by $\mathcal{I}^{-1}$ is equivalent to $\alpha\mathcal{O}_K \subseteq \mathcal{J}$, which is equivalent to $\alpha \in \mathcal{J}$. Hence $\ker(\phi) = \mathcal{J}$. On the other hand, it is clear ϕ is surjective. Thus it induces the desired isomorphism $\phi : \mathcal{O}_K/\mathcal{J} \to \mathcal{I}/\mathcal{I}\mathcal{J}$. □

Exercise 1.13. *Show the map $\phi : \mathcal{O}_K/\mathcal{I}\mathcal{J} \to \mathcal{O}_K/\mathcal{I}$ given by $\alpha + \mathcal{I}\mathcal{J} \mapsto \alpha + \mathcal{I}$ for $\alpha \in \mathcal{O}_K$ is well-defined (i.e., ϕ does not depend on the choice of coset representative $\alpha \in \alpha + \mathcal{I}\mathcal{J}$), has kernel $\mathcal{I}/\mathcal{I}\mathcal{J}$, and is surjective. This gives the isomorphism $\mathcal{O}_K/\mathcal{I} \simeq (\mathcal{O}_K/\mathcal{I}\mathcal{J})/(\mathcal{I}/\mathcal{I}\mathcal{J})$ claimed above.*

If $\mathcal{I} \subseteq K$ such that $a\mathcal{I}$ is an ideal of $\mathcal{O}_K$ for some $a \in \mathcal{O}_K$, we say $\mathcal{I}$ is a **fractional ideal** of $\mathcal{O}_K$. Moreover a fractional or ordinary ideal $\mathcal{I}$ is called **principal**, if it is generated by a single element, i.e., if it is of the form $a\mathcal{O}_K$ for some $a \in K$. Denote by $\mathrm{Frac}(\mathcal{O}_K)$ the set of (nonzero) fractional ideals of $\mathcal{O}_K$, and $\mathrm{Prin}(\mathcal{O}_K)$ the set of (nonzero) principal fractional ideals of $\mathcal{O}_K$. Multiplication for fractional ideals is defined the same as for ordinary ideals.

Theorem 1.4.4. $\mathrm{Frac}(\mathcal{O}_K)$ *is an abelian group under multiplication, and* $\mathrm{Prin}(\mathcal{O}_K)$ *is a subgroup.*

If $\mathcal{I}, \mathcal{J}$ are ideals of $\mathcal{O}_K$, we say $\mathcal{J}$ divides $\mathcal{I}$ ($\mathcal{J}|\mathcal{I}$) if $\mathcal{J} \supseteq \mathcal{I}$, from which one can conclude from the above theorem that $\mathcal{I} = \mathcal{J}\mathcal{J}'$ for some ideal $\mathcal{J}'$. An ideal $\mathcal{I}$ of $\mathcal{O}_K$ is **proper** if $\mathcal{I} \neq \mathcal{O}_K$. We

say a proper ideal $\mathfrak{p}$ is **prime** if $\mathfrak{p}|\mathcal{I}\mathcal{J}$ implies $\mathfrak{p}|\mathcal{I}$ or $\mathfrak{p}|\mathcal{J}$ (technically, the zero ideal is prime, but we are ignoring the zero ideal), and it is **maximal** if $\mathcal{I}|\mathfrak{p}$ implies $\mathcal{I} = \mathfrak{p}$ or $\mathcal{I} = \mathcal{O}_K$.

Recall that $\mathfrak{p}$ is prime if and only if $\mathcal{O}_K/\mathfrak{p}$ is an integral domain, and $\mathfrak{p}$ is maximal if and only if $\mathcal{O}_K/\mathfrak{p}$ is a field. (Remark: this kind of result is one reason we don't allow for a field to have just one element.) Since every finite integral domain is a field, one is able to conclude every (nonzero) prime ideal is maximal and vice versa.

Theorem 1.4.5. (Prime ideal factorization) *Let $\mathcal{I}$ be a proper ideal of $\mathcal{O}_K$. Then $\mathcal{I} = \mathfrak{p}_1 \cdots \mathfrak{p}_r$ where the $\mathfrak{p}_i$'s are prime ideals of $\mathcal{O}_K$. Moreover the $\mathfrak{p}_i$'s are determined uniquely up to ordering.*

We proved these theorems last semester, modulo a couple of details about the first theorem. If you want to fill in these details for yourself, you can try to work it out yourself from the Chapter 12 notes from last semester, or see any text on Algebraic Number Theory, such as [Stewart–Tall].

Definition 1.4.6. *The quotient group* $\mathrm{Frac}(\mathcal{O}_K)/\mathrm{Prin}(\mathcal{O}_K)$ *is called the* **class group** *of K, and denoted $\mathcal{C}l(\mathcal{O}_K)$ or $\mathcal{C}l_K$. The size of the class group is called the* **class number** *of K, and denoted by h_K.*

Corollary 1.4.7. *$\mathcal{O}_K$ has unique factorization if and only if $h_K = 1$.*

Proof. Note $h_K = 1$ means $\mathcal{O}_K$ is a PID. Since every PID is a UFD (from algebra or last semester), the $\Leftarrow$ direction holds.

To prove the $\Rightarrow$ direction, suppose $\mathcal{O}_K$ has unique factorization. Suppose $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_K$. Let $n \in \mathfrak{p}$ and $n = \alpha_1 \cdots \alpha_k$ be unique factorization of n into (non-unit) irreducibles. Note each α_i satisfies the prime divisor property by unique factorization, each α_i is a prime element of $\mathcal{O}_K$, and therefore each (α_i) is a prime ideal. Hence $(n) = (\alpha_1)(\alpha_2)\cdots(\alpha_k)$ is the prime ideal factorization of (n).

On the other hand, since $\mathfrak{p}|(n)$, $\mathfrak{p}$ must equal one of the (α_i)'s by uniqueness of prime ideal factorization. Hence every prime ideal of $\mathcal{O}_K$ is principal. Then by prime ideal factorization again, every ideal must be principal. □

We mentioned last semester that there are only finitely many imaginary quadratic fields with unique factorization, and conjecturally infinitely many such real quadratic fields. We will a bit more talk more about this later, but first we need a way to compute the class group or class number of a field. In fact, perhaps even before that, we want to know the class number is finite. The standard proof for this is via Minkowski's theory of the *geometry of numbers*, and it will in fact give us a bound on the class number, which will in turn allow us to compute the class group in explicit examples. In fact, to get an idea of how one can do such a thing, you may want to look at the Chapter 12 notes from last semester, where, following Stillwell, I prove directly that $h_{\mathbb{Q}(\sqrt{-5})} = 2$, though we didn't have a chance to cover it in lecture last semester. The proof via Minkowski's theorem is somewhat less direct, and to keep things as simple as possible, we will only give a complete proof in the case of quadratic fields. A more sophisticated proof of the finiteness of the class group is via the theory of p-adic numbers and adèles which we will develop in Part III. Time permitting, we will give this proof in the 3rd part of the course for general number fields.

Another way to compute the class number is to use a formula of Dirichlet, which we will turn to after Minkowski's bound. An alternative way to compute the class number and group for quadratic fields will be given by Gauss's theory of binary quadratic forms in Part II (which historically came first).

1.5 Lattices

Before explaining Minkowski's geometry of numbers, we need to know some basic facts about lattices.

Definition 1.5.1. *A* **(complete) lattice** Λ *in* $\mathbb{R}^n$ *is a subset of* $\mathbb{R}^n$ *of the form* $\langle v_1, v_2, \ldots, v_n \rangle = \{\sum a_i v_i : a_i \in \mathbb{Z}\}$ *such that* $v_1, \ldots, v_n \in \mathbb{R}^n$ *are linearly independent over* $\mathbb{R}$*. The set* $v_1, \ldots, v_n$ *is called a* **basis** *for* Λ *(it is a* $\mathbb{Z}$*-basis). As both* $\mathbb{R}^n$ *and* Λ *are abelian groups under addition, we let* $\mathbb{R}^n/\Lambda$ *denote the quotient group. A* **fundamental domain** *for* Λ *(or* $\mathbb{R}^n/\Lambda$*) is a connected, locally convex*[*] Ω *of* $\mathbb{R}^n$ *such that* Ω *contains exactly one element from each coset of* $\mathbb{R}^n/\Lambda$*.*

In other words, the (complete) lattices in $\mathbb{R}^n$ are the $\mathbb{Z}$-spans of bases of $\mathbb{R}^n$. The adjective complete refers to the fact that the number of basis elements of the lattice is maximal. An incomplete lattice of $\mathbb{R}^n$ would be the $\mathbb{Z}$-span of a basis of a proper subspace of $\mathbb{R}^n$. However, for us, all lattices will be complete unless stated otherwise.

Note a lattice is a free abelian subgroup of $\mathbb{R}^n$ of rank n, but not all free abelian subgroups of rank n are lattices. For example, $\mathbb{Z}[\sqrt{2}] \subseteq \mathbb{R}$ is a free abelian subgroup of $\mathbb{R}^2$ of rank 2 (embedding $\mathbb{R}$ in $\mathbb{R}^2$), generated by 1 and $\sqrt{2}$, but not a lattice since 1 and $\sqrt{2}$ are not linearly independent over $\mathbb{R}$.

The main idea with fundamental domain is that it is a subset of $\mathbb{R}^n$ which looks like the quotient group $\mathbb{R}^n/\Lambda$. More precisely, it is a connected subset of $\mathbb{R}^n$ comprising exactly one representative from each coset of $\mathbb{R}^n/\Lambda$. The condition of local convexity is just to avoid pathological examples of fundamental domains (see examples below). In any case, it won't be important for us to understand the subtleties of what kinds of sets make up fundamental domains, but rather just the basic idea of what one is, and understanding what the "standard" fundamental domain is. Hopefully this should be clear when we look at the cases in $\mathbb{R}^1$ and $\mathbb{R}^2$.

It is a basic fact that any fundamental domain for Λ has the same volume (length in dimension 1, area in dimension 2). This volume is called the **volume** (or **covolume**) of the lattice Λ (or more properly the quotient $\mathbb{R}/\Lambda_n$), denoted $\mathrm{vol}(\Lambda)$ (or more properly $\mathrm{vol}(\mathbb{R}^n/\Lambda)$). (To be formally complete, we can get away without proving this fact about all fundamental domains having the same volume by defining the volume of the lattice to be the volume of the standard fundamental domain, defined below.) If Λ is an incomplete lattice, then $\mathbb{R}^n/\Lambda$ will have will have infinite volume.

Example 1.5.2. *Since any free abelian group of rank* n *is isomorphic, as an abelian group, to* $\mathbb{Z}^n$*, the most obvious example of a lattice in* $\mathbb{R}^n$ *is* $\mathbb{Z}^n$*. The standard fundamental domain for* $\mathbb{Z}^n$ *is* $\Omega = [0,1)^n \subseteq \mathbb{R}^n$*. It should be clear any element of* $\mathbb{R}^n$ *is a* $\mathbb{Z}^n$ *translate of exactly one element in* Ω*. It is obviously connected and convex, therefore locally convex. It is clear* $\mathrm{vol}(\Lambda) = 1$*.*

While all lattices of $\mathbb{R}^n$ are isomorphic as abelian groups, they also have an inherent geometry coming from $\mathbb{R}^n$, providing more structure. We will not need this, but just to clear up terminology, we will only say two lattices of $\mathbb{R}^n$ are isomorphic *as lattices* if they (or equivalently, their fundamental domains) have the same shape and size—precisely, they will be isomorphic if one is the image of the other by an isometry (distance preserving map) of $\mathbb{R}^n$. In linear algebra, you may have learned that the (linear) isometries of $\mathbb{R}^n$ are precisely the elements of $\mathrm{O}(n) = \left\{A \in \mathrm{GL}_n(\mathbb{R}) : A^t A = I\right\}$, the *real orthogonal group of rank* n. This means that two lattices of $\mathbb{R}^n$ are isomorphic if and only if (a basis of) one can be transformed into (a basis of) the other by an element of $\mathrm{O}(n)$.

[*] Locally convex means if two "nearby" points are in the set, then the line between them is in the set.

Example 1.5.3. *As a special case of the above example with $n = 1$, $\mathbb{Z}$ is a lattice in $\mathbb{R}$, as is $\Lambda_k = k\mathbb{Z}$. Notice that $\Lambda_k = \Lambda_{k'}$ if and only if $k = -k'$. These are all the lattices in $\mathbb{R}$, in $1-1$ correspondence with $\mathbb{R}_{>0}$, parameterized by this number k. A fundamental domain for $\mathbb{R}/\Lambda_k$ (sometimes also referred to as $\mathbb{R} \bmod k$) is $[0, k)$. In fact any half-open interval of length k is a fundamental domain for Λ_k, and there are no other fundamental domains because of the connectedness requirement. We think of $\mathbb{R}/\Lambda_k$ as the interval $[0, k]$ with the endpoints glued, hence topologically it is a circle. Geometrically, its length is $\mathrm{vol}(\Lambda_k) = k$.*

Example 1.5.4. *A lattice in $\mathbb{R}^2$ is determined by two generators, $u = (x_1, y_1)$ and $v = (x_2, y_2)$, provided they are linearly independent. Precisely, the lattice $\Lambda = \langle u, v\rangle$ generated by u and v is $\Lambda = \{mu + nv : m, n \in \mathbb{Z}\} \subseteq \mathbb{R}^2$. The standard fundamental domain for Λ is $\Omega = \{au + bv : a, b \in [0, 1)\}$. In other words, the standard fundamental domain for Λ is the interior of the parallelogram determined by 0, u, v and $u + v$, together with half of the boundary (since opposite boundary points are equivalent modulo Λ, we can only include half of them, and one of the corners). Any $\mathbb{R}^2$-translate of Ω is also a fundamental domain for Λ.*

We may think of the quotient group $\mathbb{R}^2/\Lambda$ as the fundamental domain (parallelogram) Ω, with the addition of two vectors being the sum in the fundamental domain, and if the vector lies outside of Ω, we let it wrap it around the edges of the parallelogram Pacman-style so the sum lies again in Ω. In other words, we think of $\mathbb{R}^2/\Lambda$ as the parallelogram Ω, with opposite sides glued. Topologically this is a torus.

Example 1.5.5. *Let $a, b > 0$. The volume of the lattice $\Lambda_{a,b} = \langle (a, 0), (0, b)\rangle$ is ab, since a fundamental domain is a rectangle with corners $0, (a, 0), (0, b), (a, b)$ (excluding appropriate boundary points). Two of these rectangular lattices $\Lambda_{a,b}$ and $\Lambda_{c,d}$ will be isomorphic if and only if $\{a, b\} = \{c, d\}$. Hence there are infinitely many non-isomorphic rectangular lattices of volume 1 given by $\Lambda_{a,\frac{1}{a}}$.*

To generalize the above examples, the **standard fundamental domain** for $\Lambda = \langle v_1, v_2 \ldots, v_n\rangle$ (or more properly for the basis $v_1, \ldots, v_n$) is $\Omega = \{\sum a_i v_i : a_i \in [0, 1)\}$. It is straightforward to show this is in fact a fundamental domain. Then $\mathbb{R}^n/\Lambda$ looks like an n-dimensional parallelogram (parallelopiped?) and topologically is an n-dimensional torus (the product of n circles). (To be complete, if we define volume of a lattice as the volume of a standard fundamental domain, one should show that any two bases of Λ are related by an element of $\mathrm{GL}_n(\mathbb{Z})$. Then, expressing the volumes of standard fundamental domains as determinants, one can conclude that the volume is independent of the choice of basis.)

Exercise 1.14. *Consider the lattice $\Lambda = \langle u = (1, 0), v = (\frac{1}{2}, \frac{\sqrt{3}}{2})\rangle$ in $\mathbb{R}^2$. Sketch the standard fundamental domain for $\{u, v\}$ compute its volume. Write down 2 other bases $\{u_1, v_1\}$, $\{u_2, v_2\}$ for Λ that do not just differ by sign (i.e., $\{u, v\} \neq \{\pm u_i, \pm v_i\}$ and $\{u_1, v_1\} \neq \{u_2, v_2\}$). Sketch the standard fundamental domains for $\{u_1, v_1\}$ and $\{u_2, v_2\}$ and check they have the same volume.*

Exercise 1.15. *Let $\Lambda = \langle u, v\rangle$ be a lattice in $\mathbb{R}^2$ such that $\Lambda \subseteq \mathbb{Z}^2$. Let Ω be the standard fundamental domain for the basis $\{u, v\}$ of Λ. Show the volume of $\mathbb{R}^2/\Lambda$ is the number of integral points in Ω, i.e., $\mathrm{vol}(\mathbb{R}^2/\Lambda) = |\Omega \cap \mathbb{Z}^2|$.*

Example 1.5.6. *Consider the lattice $\mathbb{Z}^2$ in $\mathbb{R}^2$. A non-rectangular fundamental domain may be constructed as follows. Start with a standard fundamental domain and remove a semicirclular shape*

from one of the sides, then glue this shape onto the opposite side. (Draw a picture). This is no longer convex, but it is still locally convex.

Now here is a non-example of a fundamental domain, which satisfies all properties except local convexity. Let Ω be the union of line segments L_y for $0 \leq y < 1$ where L_y is the line from $(0, y)$ (inclusive) to $(1, y)$ (exclusive) if y is rational and to $(-1, y)$ (exclusive) if y is irrational. Then it is clear Ω contains exactly one representative from each coset of $\mathbb{R}^2/\mathbb{Z}^2$, and it is connected since it is a union of horizontal line segments which are joined by the y axis, but it is not locally convex. (Think why, draw a picture.)

Now to apply this to ideal theory, we need to know Minkowski's Theorem. Recall $X \subseteq \mathbb{R}^n$ is called **symmetric** if $X = -X$.

Theorem 1.5.7. (Minkowski) *Let Λ be a lattice in $\mathbb{R}^n$ and X a bounded symmetric convex subset of $\mathbb{R}^n$. If $\mathrm{vol}(X) > 2^n \mathrm{vol}(\mathbb{R}^n/\Lambda)$, then X contains a nonzero point of Λ.*

Proof. (It may be helpful to draw a picture for $n = 2$.) Let L be the lattice $L = 2\Lambda$. It is clear $\mathrm{vol}(\mathbb{R}^n/L) = 2^n \mathrm{vol}(\mathbb{R}^n/\Lambda)$, so $\mathrm{vol}(X) > \mathrm{vol}(\mathbb{R}^n/L)$. Thus, if Ω is a fundamental domain for $\mathbb{R}^n/L$, the natural map from $\mathbb{R}^n$ to Ω cannot be injective when restricted to X. Thus there must be two points $x_1, x_2 \in X$ such that $x_1 \equiv x_2 \bmod L$ (i.e., they map to the same point in Ω), i.e., $x_1 - x_2 \in L$. Since X is symmetric $-x_2 \in X$. Then convexity implies $0 \neq \frac{1}{2}x_1 - \frac{1}{2}x_2 \in X \cap \Lambda$. □

Two classical applications of Minkowski's theorem are that it can be used to prove Fermat's two square theorem or Lagrange's four square theorem. See [Stewart–Tall] for both proofs, or the Chapter 8 notes from last semester for the proof of the four square theorem. However, we are more interested in the applications to ideals in the following sections.

1.6 The geometry of numbers: the quadratic case

What Minkowski termed the geometry of numbers is most plain to see in the imaginary quadratic case. Let $K = \mathbb{Q}(\sqrt{-d})$ with $d > 0$ squarefree. Then $\mathcal{O}_K$ is a lattice in $\mathbb{C} \simeq \mathbb{R}^2$. Hence, any ideal of $\mathcal{O}_K$ is a lattice in $\mathbb{C} \simeq \mathbb{R}^2$.

In fact, even if $K = \mathbb{Q}(\sqrt{d})$ is a real quadratic field, we may think of $\mathcal{O}_K$ as a lattice in $\mathbb{R}^2$. (As we remarked earlier with $\mathbb{Z}[\sqrt{2}]$, even though $K \subseteq \mathbb{R}$, $\mathcal{O}_K$ is not a lattice in $\mathbb{R}$, so Minkowski's idea was to embed K into $\mathbb{R}^2$.) The most naive way to do this is to regard an element $a + b\sqrt{d} \in K$ as the element $(a, b\sqrt{d})$ in $\mathbb{R}^2$. In other words, we are separating out the rational and irrational components on the x- and y- axes of $\mathbb{R}^2$, just like we separate the real and imaginary components of $\mathbb{Q}(\sqrt{-d})$ or $\mathbb{C}$ onto the x- and y- axes in the complex plane picture.

We can unify these two cases as follows. Suppose $K = \mathbb{Q}(\sqrt{d})$ is a real or imaginary quadratic field, i.e., $d > 1$ or $d < 0$ and assume d squarefree. Then we can embed K in $\mathbb{R}^2$ by the map $\phi : K \to \mathbb{R}^2$ such that $\phi(a + b\sqrt{d}) = (a, b\sqrt{|d|})$ for $a, b \in \mathbb{Q}$. In this picture $\mathcal{O}_K$, and thus any ideal of $\mathcal{O}_K$, is a lattice of $\mathbb{R}^2$.

We will work out the part of Minkowski's theory relevant for us in the case of quadratic fields. In the interest of time, we will just state the theorems in the general case, though the basic argument is the same.

Proposition 1.6.1. *Let $\mathcal{I}$ be an ideal of $\mathcal{O}_K$ with $\mathbb{Z}$-basis $\{\alpha, \beta\}$, regarded as a lattice in $\mathbb{R}^2$ via the embedding $\phi : K \to \mathbb{R}^2$ above. Then $\mathrm{vol}(\mathbb{R}^2/\mathcal{I}) = \frac{1}{2}|\Delta[\alpha, \beta]|^{1/2}$.*

In the case where K is imaginary quadratic and $\mathcal{I} = \mathcal{O}_K$, we briefly discussed this at the end of the section on discriminants.

Proof. Let $(x_1, y_1) = \phi(\alpha)$ and $(x_2, y_2) = \phi(\beta)$, so we can write $\alpha = x_1 + \frac{y_1}{\sqrt{|d|}}\sqrt{d}$ and $\beta = x_2 + \frac{y_2}{\sqrt{|d|}}\sqrt{d}$. Note $\Delta[\alpha, \beta] = \alpha\overline{\beta} - \overline{\alpha}\beta$. Since $\alpha\overline{\beta} = x_1x_2 + \frac{d}{|d|}y_1y_2 + (x_1y_2 + x_2y_1)\frac{\sqrt{d}}{\sqrt{|d|}}$, we have $|\Delta[\alpha, \beta]|^{1/2} = 2|x_1y_2 - x_2y_1|$. By the exercise below, this is twice the volume of the parallelogram with corners $(0, 0)$, (x_1, y_1), (x_2, y_2) and (x_1+x_2, y_1+y_2), which is the standard fundamental domain of the lattice $\mathcal{I} \subseteq \mathbb{R}^2$ (with respect to the basis $(x_1, y_1), (x_2, y_2)$). □

Exercise 1.16. *Let $u = (x_1, y_1)$ and $v = (x_2, y_2)$ be linearly independent vectors in $\mathbb{R}^2$. Show the parallelogram with corners 0, u, v and $u + v$ has area $|x_1y_2 - x_2y_1|$.*

Corollary 1.6.2. *With the notation of the previous proposition,* $\mathrm{vol}(\mathbb{R}^2/\mathcal{I}) = \frac{1}{2}N(\mathcal{I})\sqrt{|\Delta_K|}$.

This gives a geometric interpretation of the norm of an ideal in terms of the volume of the corresponding lattice.

Proof. This is immediate since $N(\mathcal{I}) = \sqrt{\frac{\Delta[\alpha,\beta]}{\Delta_K}}$ (Lemma 1.4.1.) □

Lemma 1.6.3. *For any ideal $\mathcal{I}$ of $\mathcal{O}_K$, there is a nonzero $\alpha \in \mathcal{I}$ such that*

$$|N(\alpha)| \leq \frac{2}{\pi}N(\mathcal{I})\sqrt{|\Delta_K|}.$$

Proof. From the previous corollary, Minkowski's theorem implies that if X is the (open) disc of radius r centered at the origin in $\mathbb{R}^2$, it contains a nonzero lattice point, i.e., a nonzero $\alpha \in \mathcal{I}$, whenever $\pi r^2 > 2N(\mathcal{I})\sqrt{|\Delta_K|}$. Suppose $r^2 > \frac{2}{\pi}N(\mathcal{I})\sqrt{|\Delta_K|} + \epsilon$ for some $\epsilon > 0$ so there is such an α.

Now if we write $\alpha = x + \frac{y}{\sqrt{|d|}}\sqrt{d}$, we see $N(\alpha) = x^2 \pm y^2$ according to whether K is imaginary quadratic or real quadratic. Now $\alpha \in X$ means $x^2 + y^2 < r^2$, which of course implies $|x^2 - y^2| < r^2$, so in either the imaginary or real case we have $|N(\alpha)| < r^2 = \frac{2}{\pi}N(\mathcal{I})\sqrt{|\Delta_K|} + \epsilon$. Taking $\epsilon \to 0$ gives the desired result. □

Recall if $\mathcal{I}, \mathcal{J}$ are fractional or ordinary ideals of a ring R, we say $\mathcal{I}$ and $\mathcal{J}$ are **equivalent** if $a\mathcal{I} = b\mathcal{J}$ for some $a, b \in R$ and write $\mathcal{I} \sim \mathcal{J}$. Via this equivalence, the class group of R (which we technically have only defined when R is the ring of integers of a number field) is just the group of equivalence classes of fractional ideals.

Lemma 1.6.4. *Let $\mathcal{I}$ be an ideal of $\mathcal{O}_K$. Then $\mathcal{I} \sim \mathcal{J}$ for some ideal $\mathcal{J}$ with norm $\leq \frac{2}{\pi}\sqrt{|\Delta_K|}$.*

Proof. For some $a \in \mathcal{O}_K$, $a\mathcal{I}^{-1} \subseteq \mathcal{O}_K$. Then $\mathcal{I}' = a\mathcal{I}^{-1}$ is a ideal of $\mathcal{O}_K$ such that $\mathcal{I}\mathcal{I}' = (a)$. Let $\alpha \in \mathcal{I}'$ such that $|N(\alpha)| \leq \frac{2}{\pi}N(\mathcal{I}')\sqrt{|\Delta_K|}$, whose existence is guaranteed by the previous lemma. Clearly $\mathcal{I}'|(\alpha)$ so we can write $(\alpha) = \mathcal{I}'\mathcal{J}$ where $\mathcal{J}$ is an ideal of $\mathcal{O}_K$. Now we are done, since $\mathcal{J} \sim \mathcal{I}'^{-1} \sim \mathcal{I}$ and $N(\mathcal{J}) = N(\mathcal{I}')/N((\alpha)) \leq \frac{2}{\pi}\sqrt{|\Delta_K|}$. □

The point is that this lemma allows us to bound, and subsequently determine, the class number in any explicit case, as well as use this to show it is finite in general. Let's first start of with our canonical example. Recall from Section 1.3, for $K = \mathbb{Q}(\sqrt{d})$ with $d \neq 1$ squarefree, the discriminant $\Delta_K = d$ if $d \equiv 1 \bmod 4$ and $\Delta_K = 4d$ if $d \equiv 2, 3 \bmod 4$.

Example 1.6.5. *The class number of* $K = \mathbb{Q}(\sqrt{-5})$ *is* 2*, and a set of representatives for the class group is* $\{\mathcal{O}_K, (2, 1+\sqrt{-5})\}$.

Proof. By the lemma, every ideal of $\mathcal{O}_K$ is equivalent to one of norm $\leq \frac{2}{\pi}\sqrt{20} \approx 2.85$. There is only one ideal of norm 1 (think back to the definition of the norm of an ideal), $\mathcal{O}_K$. Suppose $\mathfrak{p}$ is an ideal of norm 2. By Lemma 1.6.3 there is an nonzero $\alpha \in \mathfrak{p}$ with norm at most 5. However $\mathfrak{p}|\alpha$ implies $N(\mathfrak{p})|N(\alpha)$ means $N(\alpha)$ is even, i.e., $N(\alpha) = 2$ or 4. But there are no elements of norm 2 (it is not of the form $x^2 + 5y^2 = N(x + y\sqrt{-5})$), so we must have α is of norm 4, i.e., $\alpha = \pm 2$.

This means $\mathfrak{p}|(2)$, but the prime ideal factorization of (2) in $\mathcal{O}_K$ is $(2) = (2, 1+\sqrt{-5})^2$ either from last semester or the exercise below. Hence $(2, 1+\sqrt{-5})$ is the only ideal of norm 2, and it is not principal. □

A more elementary proof of the above fact is in the Chapter 12 notes from last semester, based off of what was in Stillwell. It still uses the lattice picture of ideals, but does not require Minkowski's theorem. In fact, a general proof of finiteness of the class group which avoids Minkowski's theorem is in [Lang].

Exercise 1.17. *Consider the ideal* $\mathfrak{p} = (2, 1+\sqrt{-5})$ *in* $\mathbb{Z}[\sqrt{-5}]$*. We proved several things about this ideal last semester, but using norms we can give more elegant arguments. In any case, this exercise, and the following ones, should be a good review for you.*

(i) Show $\mathfrak{p}|(2)$ *but* $\mathfrak{p} \neq (2)$*. Using norms, conclude* $N(\mathfrak{p}) = 2$*.*

(ii) From (i) conclude $\mathfrak{p}$ *is non-principal and prime.*

(iii) Show the prime factorization of (2) *is* $(2) = \mathfrak{p}^2$*.*

Exercise 1.18. *Consider the ideals* $\mathfrak{q} = (3, 1+\sqrt{-5})$ *and* $\overline{\mathfrak{q}} = (3, 1-\sqrt{-5})$ *in* $\mathbb{Z}[\sqrt{-5}]$*.*

(i) Show $N(\mathfrak{q}) = N(\overline{\mathfrak{q}}) = 3$*.*

(ii) Show $\mathfrak{q}$*,* $\overline{\mathfrak{q}}$ *are non-principal and prime.*

(iii) Show the prime factorization of (3) *is* $(3) = \mathfrak{q}\overline{\mathfrak{q}}$*.*

Exercise 1.19. *From the previous two exercises, determine the prime ideal factorization of* (6) *in* $\mathbb{Z}[\sqrt{-5}]$*. Explain how the non-unique factorization of elements* $6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$ *in* $\mathbb{Z}[\sqrt{-5}]$ *is resolved in terms of the prime ideal factorization of the ideal* (6)*.*

Exercise 1.20. *Let* $K = \mathbb{Q}(\sqrt{-5})$*. By the above exercises, together with the fact that* $h_K = 2$*,* $\mathfrak{p} \sim \mathfrak{q}$ *in the notation above. Show this explicitly by finding nonzero* $\alpha, \beta \in \mathcal{O}_K$ *such that* $\alpha\mathfrak{p} = \beta\mathfrak{q}$*.*

Exercise 1.21. *Using Lemma 1.6.4, show* $\mathbb{Q}(\sqrt{d})$ *has class number* 1 *for* $d = -1, -2, -3, -7, 2, 3, 5$*.*

These are all the cases where Lemma 1.6.4 immediately gives class number 1, but there are other cases.

Exercise 1.22. *Show* $\mathbb{Q}(\sqrt{-11})$ *has class number* 1*.*

The only other imaginary quadratic fields with class number 1, i.e., with unique factorization in their ring of integers, are $\mathbb{Q}(\sqrt{-d})$ with $d = 19, 43, 67, 163$ (making for a total of 9 such fields). It is not difficult to see that these fields all have class number 1—it is much harder to show that they are the only ones. This is Gauss's class number conjecture, and we will say a little more about this later. For now we will just say it was proven in 1934 by Heilbronn and Linfoot that there are only finitely many such imaginary quadratic fields, and eventually proved that there were no others by Heegner and Stark in the 50's and 60's.

Contrast this with the real quadratic case where it is conjectured that there are infinitely many instances of class number 1 (in fact, it is thought that about 75% should be). Tables of class numbers for small real and imaginary quadratic fields are given below.

Exercise 1.23. *Show $\mathbb{Q}(\sqrt{-6})$ has class number 2.*

Now we want to show the finiteness of the class number for a general quadratic field. We need to know one more small fact about ideals first.

Lemma 1.6.6. *Let K be a quadratic field and $n \in \mathbb{N}$. There are only finitely many ideals $\mathcal{I}$ of $\mathcal{O}_K$ such that $N(\mathcal{I}) = n$.*

Proof. Regarding $\mathcal{O}_K$ as a lattice in $\mathbb{R}^2$ as above, the ideals of norm n correspond to the lattices of $\mathbb{R}^2$ contained in $\mathcal{O}_K$ (i.e., sublattices of $\mathcal{O}_K$) of (co)volume $\frac{n}{2}\sqrt{|\Delta_K|}$ by Corollary 1.6.2. It is geometrically clear that there are only finitely many such (sub)lattices.

We will see another proof later when we study the behavior of primes in extensions. In particular we will show that if $N(\mathcal{I}) = n$, then $\mathcal{I}|(n)$. But there are only finitely many ideals dividing (n) by the uniqueness of prime ideal factorization. □

Theorem 1.6.7. *Let K be a quadratic field. Then $h_K < \infty$, i.e., $\mathcal{C}l_K$ is a finite abelian group.*

Proof. By Lemma 1.6.4, there is some n such that any equivalence class of ideals has a representative with norm $\leq n$. Now by the previous lemma, there are only finitely many ideals with norm $\leq n$. □

1.7 The geometry of numbers: the general case

Now suppose K is a number field of degree n. In order to look at $\mathcal{O}_K$ "geometrically", i.e., as a lattice, we need a way to embed K into $\mathbb{R}^n$. Of course if $\alpha_1, \ldots, \alpha_n$ is a basis for K (as a $\mathbb{Q}$-vector space), we could send $\sum c_i\alpha_i$ to $(c_1, \ldots, c_n) \in \mathbb{R}^n$, but there are two issues: (i) this is not at all canonical since it is highly dependent on the choice of basis, and (ii) there is no way with such an arbitrary embedding to relate $\mathrm{vol}(\mathbb{R}^n/\mathcal{I})$ with the discriminant/norm of an ideal $\mathcal{I}$ of $\mathcal{O}_K$ in order to get an analogue of Proposition 1.6.1 and its corollary.

In fact, if we look over the proof of Lemma 1.6.3, we see the key is that $|N(\alpha)|$ is $\leq$ the square of the distance from α to the origin in $\mathbb{R}^2$, with equality in the imaginary quadratic case. However, in some sense, the embedding we used in the real quadratic case, while perhaps the most obvious choice, was not natural in that it came from the "standard" basis $1, \sqrt{d}$ of $K = \mathbb{Q}(\sqrt{d})$. One might then ask if there is a more "natural" embedding of a real quadratic field $K = \mathbb{Q}(\sqrt{d}) \hookrightarrow \mathbb{R}^2$. There is, and the idea is to use the Galois group. Let σ_1, σ_2 be the embeddings of $K \hookrightarrow \mathbb{R}$ (all embeddings are real) given by $\sigma_1(a + b\sqrt{d}) = a + b\sqrt{d}$ and $\sigma_2(a + b\sqrt{d}) = a - b\sqrt{d}$.

Consider the embedding $K \hookrightarrow \mathbb{R}^2$ given by $\alpha \mapsto (\sigma_1(\alpha), \sigma_2(\alpha))$. This is "natural" since it does not depend upon a choice of basis for K over $\mathbb{Q}$, and the norm satisfies the desired geometric bound: if $\alpha = a+b\sqrt{d} \mapsto (x, y)$, then $x = a+b\sqrt{d}$, $y = a-b\sqrt{d}$, so $x^2+y^2 = 2(a^2+db^2) \geq 2|a^2-db^2| = 2N(\alpha)$. (Our naive embedding of a real quadratic field into $\mathbb{R}^2$ was of course perfectly fine for our goal in the previous section, but the problem was it is not so helpful in suggesting an appropriate generalization to arbitrary number fields. In fact, our naive embedding gives a better bound than the "natural" one given by the Galois group stated below.)

The standard presentation of the geometry of numbers is as follows. Let K be a number field of degree n. Then there are n embeddings of $K \hookrightarrow \mathbb{C}$, say $\sigma_1, \ldots, \sigma_n$. Assume the first s are

Table 1: Class numbers of small imaginary quadratic fields $K = \mathbb{Q}(\sqrt{d})$

d	h_K
-1	1
-2	1
-3	1
-5	2
-6	2
-7	1
-10	2
-11	1
-13	2
-14	4
-15	2
-17	4
-19	1
-21	4
-22	2
-23	3
-26	6
-29	6
-30	4
-31	3
-33	4
-34	4
-35	2
-37	2
-38	6
-39	4
-41	8
-42	4
-43	1
-46	4
-47	5
-51	2

Table 2: Class numbers of small real quadratic fields $K = \mathbb{Q}(\sqrt{d})$

d	h_K
2	1
3	1
5	1
6	1
7	1
10	2
11	1
13	1
14	1
15	1
17	1
19	1
21	1
22	1
23	1
26	2
29	1
30	2
31	1
33	1
34	2
35	2
37	1
38	1
39	2
41	1
42	2
43	1
46	1
47	1
51	2

real embeddings, i.e., $\sigma_1, \ldots, \sigma_s$ actually embed K in $\mathbb{R}$, and that the remaining σ_i's are *complex embeddings*, i.e., they do not map into $\mathbb{R}$. If σ_i is a complex embedding, then $\overline{\sigma}_i$ also is, where $\overline{\sigma}_i(\alpha) = \overline{\sigma_i(\alpha)}$ and the bar denotes usual complex conjugation. In particular, there are an even number $2t$ of complex embeddings, which occur in complex conjugate pairs. Let us denote them $\tau_1, \overline{\tau}_1, \ldots, \tau_t, \overline{\tau}_t$.

Now we define the embedding $\phi : K \to \mathbb{R}^s \times \mathbb{C}^t \simeq \mathbb{R}^{s+2t} = \mathbb{R}^n$ by

$$\phi(\alpha) = (\sigma_1(\alpha), \ldots, \sigma_s(\alpha), \tau_1(\alpha), \ldots, \tau_t(\alpha)).$$

This is natural, in that it does not depend upon a basis for K. It does technically depend on the ordering of the embeddings σ_i and τ_i, as well as a choice among each conjugate pair of complex embeddings τ_i and $\overline{\tau}_i$, but not in any significant way.

Example 1.7.1. *If $K = \mathbb{Q}(\sqrt{d})$ is a real quadratic field, then $s = 2$ and $t = 0$, and $\phi(\alpha) = (\sigma_1(\alpha), \sigma_2(\alpha))$ is the embedding described above.*

If $K = \mathbb{Q}(\sqrt{-d})$ is an imaginary quadratic field, then $s = 0$ and $t = 1$, and $\mathrm{Gal}(K/\mathbb{Q}) = \{\tau_1, \overline{\tau}_1\}$ where $\tau_1 : K \hookrightarrow \mathbb{C}$ is the trivial embedding. Then also $\phi(\alpha) = \tau_1(\alpha) = \alpha$ is the standard embedding into $\mathbb{C} \simeq \mathbb{R}^2$. If we had chosen τ_1 to be complex conjugation, then $\overline{\tau}_1$ would be the identity map on K and we would have that $\phi(\alpha) = \overline{\alpha}$ is the conjugate embedding into $\mathbb{C} \simeq \mathbb{R}^2$.

Thus this embedding generalizes both what we did in the imaginary quadratic case (which was basically nothing, just the standard identification of $\mathbb{C}$ with $\mathbb{R}^2$) as well as our second approach to the real quadratic case.

Example 1.7.2. *Let $K = \mathbb{Q}(\sqrt[3]{2})$. Then $\mathrm{Gal}(K/\mathbb{Q}) = \{\sigma_1, \tau_1, \overline{\tau}_1\}$ where σ_1 is the trivial automorphism of K, τ_1 maps $\sqrt[3]{2}$ to $\zeta_3\sqrt[3]{2}$ and τ_2 maps $\sqrt[3]{2}$ to $\zeta_3^2\sqrt[3]{2}$. Thus $\phi : K \hookrightarrow \mathbb{R} \times \mathbb{C} \simeq \mathbb{R}^3$ by*

$$\phi(a + b\sqrt[3]{2} + c\sqrt[3]{4}) = (a + b\sqrt[3]{2} + c\sqrt[3]{4}, a + b\zeta_3\sqrt[3]{2} + c\zeta_3^2\sqrt[3]{4}).$$

Exercise 1.24. *Let $K = \mathbb{Q}(\sqrt[4]{2})$. Write down explicitly the map ϕ in this case. Compute $\phi(3)$, $\phi(3 + \sqrt[4]{2})$ and $\phi(1 + 3\sqrt{2} + \sqrt[4]{2})$.*

Exercise 1.25. *Let $K = \mathbb{Q}(\sqrt{-5}, \sqrt{5})$. Write down explicitly the map ϕ in this case. Compute $\phi(1 + \sqrt{5})$, $\phi(1 + \sqrt{-5})$ and $\phi(2i)$.*

With the embedding ϕ given above, $\mathcal{O}_K$ is a lattice in $\mathbb{R}^n$, and as in the quadratic case we did earlier, one can prove the following.

Proposition 1.7.3. *Let $\mathcal{I}$ be an ideal of $\mathcal{O}_K$ with basis $\alpha_1, \ldots, \alpha_n$, regarded as a lattice in $\mathbb{R}^n$ via the embedding ϕ. Then $\mathrm{vol}(\mathbb{R}^n/\mathcal{I}) = 2^{-t}\Delta[\alpha_1, \ldots, \alpha_n] = 2^{-t}N(\mathcal{I})\sqrt{|\Delta_K|}$.*

Here t is the number of complex embeddings of $K \hookrightarrow \mathbb{C}$ as above. This proposition gives a geometric interpretation of discriminants for general number fields.

Lemma 1.7.4. *Let $\mathcal{I}$ be an ideal of $\mathcal{O}_K$. Then $\mathcal{I}$ is equivalent to an ideal of $\mathcal{O}_K$ with norm $\leq \left(\frac{2}{\pi}\right)^t \sqrt{|\Delta_K|}$.*

Note that in the case of real quadratic fields, this gives a weaker bound that what we got in the last section because there will be no factor of $\frac{2}{\pi}$ here. It's possible to improve the bound in the lemma by being more careful. Precisely one can show

Lemma 1.7.5. (Minkowski's bound) *Let $\mathcal{I}$ be an ideal of $\mathcal{O}_K$. Then $\mathcal{I}$ is equivalent to an ideal of $\mathcal{O}_K$ with norm $\leq \left(\frac{4}{\pi}\right)^t \frac{n!}{n^n}\sqrt{|\Delta_K|}$.*

This is better than the simple bound we gave in the previous section in real quadratic case, and the same as our previous bound in the imaginary quadratic case. The better bound in the real case is in line with the notion that the class numbers for real quadratic fields tend to be smaller than those for imaginary quadratic fields, though it provides no real explanation. In any case, we will not be concerned overly much with optimal bounds. For us, the main point is

Theorem 1.7.6. *Let K be a number field. Then $h_K < \infty$.*

The proof for the general case is the same as the quadratic case (Theorem 1.6.7), admitting one of the bounds in the previous lemmas. Complete proofs of these results should be available in any Algebraic Number Theory text.

1.8 Interlude: Dirichlet's Units Theorem

There are several applications of Minkowski's geometry of numbers to classical problems. Apart from the applications to class groups and quadratic forms discussed above, other applications are to bounding the number of lattice points enclosed by a polygon and bounding the number of balls that can fit in a given region (i.e., sphere packing bounds—a remarkable result around 15 years ago was the resolution of Kepler's conjecture on the optimal way to pack spheres in space).

In algebraic number theory, there is another major application of the geometry of numbers, and that is to prove Dirichlet's Units Theorem. Since we will not have need of this theorem, we will not prove it in the interest of time, but it is such a fundamental result about number fields we would be remiss not to mention it.

Theorem 1.8.1. (Dirichlet's Units Theorem) *Let s be the number of real embeddings and $2t$ be the number of complex embeddings of a number field K. Then the group of units U of $\mathcal{O}_K$ is isomorphic (as an abelian group) to $\mathbb{Z}^{s+t-1} \times C_{2m}$ for some $m \in \mathbb{N}$.*

The basic idea of the proof is to embed K in $\mathbb{R}^{s+2t}$. Since the units are multiplicative, applying logarithms coordinate-wise makes an additive subgroup of $\mathbb{R}^{s+2t}$, i.e., an incomplete lattice, which one shows is of rank $s + t - 1$.

We note that the determination of the finite cyclic group C_{2m} appearing in the theorem is simple to determine for any given K. It is simply given by the roots of unity which are contained in K, as any unit of finite order must be a root of unity, and all roots of unity are algebraic integers.

1.9 Debriefing

Dedekind introduced ideal theory to resolve the failure of unique factorization in $\mathcal{O}_K$ for arbitrary number fields K. The first suggestion that this is a good theory to look at is that it provides a clear characterization of when $\mathcal{O}_K$ does have unique factorization—namely, if and only if $\mathcal{O}_K$ is a PID, which is if and only if $h_K = 1$. (We stated this before the prime ideal factorization theorem last semester, even though we didn't prove the only if direction until this chapter.) The prime ideal factorization theorem tells us it in fact is an excellent theory to look at, and we saw how it resolved the non-unique factorization of $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ in $\mathbb{Z}[\sqrt{-5}]$. Historically, it was the 3rd approach to resolve these non-unique factorizations, coming after Gauss's theory of quadratic

forms (for quadratic fields) and Kummer's theory of "ideal numbers." These ideas are still very interesting, and we will discuss them in Part II.

We began this chapter by generalizing some ideas such as conjugates and norms from quadratic fields to arbitrary number fields using Galois groups. As you may be aware from algebra, in many cases the Galois group of an extension can be somewhat difficult to compute, but simple non-quadratic examples are still fairly easy to compute, as we have seen with examples.

The point is the Galois group of a degree n extension is a transitive subgroup of S_n acting on the n roots of the minimal polynomial of a primitive element. When $n = 2$, there is only one transitive subgroup of $S_2 \simeq C_2$, and the extension is necessarily Galois. Here it is immediate what the Galois group is. However for $n > 2$, there is more than one transitive subgroup of S_n (e.g., S_n, A_n, C_n), and one need to do some work to determine what is is. Further, sometimes the primitive element is obvious, but sometimes it is not, e.g., what is a primitive element for $\mathbb{Q}(\sqrt{2}, \sqrt{3})$? (You can show $\sqrt{2} + \sqrt{3}$ works by a degree argument and the characterization of quadratic fields, but that this can get complicated rather quickly. Even knowing this, how do you determine the minimum polynomial—what is the minimum polynomial of $\sqrt{2} + \sqrt{3}$?) In general, one probably wants to use the main theorem of Galois theory (which I won't review) to use the subfield lattice to help determine the Galois group. However, the examples we will cover will be simple enough that we don't need to use the full force of Galois theory to determine the Galois group.

Knowing the Galois group of K over $\mathbb{Q}$ it is easy to determine the conjugates and norm of an element in K. What is not so simple is determining the ring $\mathcal{O}_K$. There is an algorithm for doing this using discriminants, though it turns out to be fairly computational even for simple examples like $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. However, our main reason for looking at discriminants is that they provide a fundamental invariant of a number field K and its ideals (i.e., the ideals of $\mathcal{O}_K$). For K an imaginary quadratic field, the discriminant of $\mathcal{O}_K$ or an ideal $\mathcal{I}$ of $\mathcal{O}_K$ is essentially the volume of the corresponding lattice, as well as essentially the norm of the ideal squared. (We only defined the discriminant of a basis of an ideal, but by the formula in terms of the norm, this is clearly independent of the choice of basis.) Then with Minkowski's theorem, we were able to bound the norm of "minimal" representatives of the class group in terms of the discriminant, providing a proof of the finiteness of the class group $\mathcal{C}l_K$, as well as allowing us to explicitly determine the class group in particular cases.

On the other hand, for real quadratic fields $K \subseteq \mathbb{R}$, $\mathcal{O}_K$ is not a lattice, but we have seen at least two ways to embed K in $\mathbb{R}^2$ which makes $\mathcal{O}_K$ a lattice—the naive way, and the approach via Galois conjugates. The second approach generalizes for an arbitrary number field K of degree n, allowing us to view $\mathcal{O}_K$ as a lattice in $\mathbb{R}^n$. As before the norm and discriminant of the ideal are essentially the (co)volume of the lattice $\mathcal{O}_K$, and Minkowski's theorem allows us to show the class group is finite, and bound norms of a set of minimal representatives of the class group.

Stillwell talked about the shape of ideals in imaginary quadratic fields. Two lattices (ideals) in $\mathbb{C} \simeq \mathbb{R}^2$ will have the same shape if and only if they differ by a complex scalar (principal ideal). Hence two ideals will have the same shape if and only if they are equivalent. Thus the class number is the number of different possible shapes of ideals. Similarly, via the geometry of numbers developed by Minkowski, if two ideals are equivalent, they will have they same shape, regarded as lattices in $\mathbb{R}^n$.

The goal of this chapter was to show finiteness of the class group (at least a complete proof in the quadratic case, and the general case is similar in spirit), and show in some specific cases how we can determine the class number and class group. There are two reasons for this: (i) to understand

factorization in $\mathcal{O}_K$, which is a basic problem in algebraic number theory, and (ii) applications to Diophantine equations.

First off, the class group of K measures the failure of unique factorization in $\mathcal{O}_K$. The larger it is the more different the set of irreducible factorizations of some algebraic integer $\alpha \in \mathcal{O}_K$ can be. For example, K has class number 2 if and only if every element of $\mathcal{O}_K$ does not have unique factorization but any factorization into irreducibles has the same number of factors. We will come back to this idea in Part II.

Now what is the bearing of the class group on solving Diophantine equations? Well, first of all, the simplest case is when $\mathcal{O}_K$ has unique factorization, i..e, class number 1. We have shown the rings of integers of the fields $\mathbb{Q}(\sqrt{d})$ for $d = -1, -2, -3, -7, -11, 2, 3, 5$ all have unique factorization. Following the approach last semester, this makes it easy to determine which primes are of the form $x^2 + dy^2$ for $d = 1, 2, 3, 7$. In particular, we used unique factorization in $\mathbb{Z}[\sqrt{-2}]$ to show $y^3 = x^2 + 2$ has only one solution $(5, 3)$ in $\mathbb{N}$, and unique factorization in $\mathbb{Z}[\zeta_3]$ to show $x^3 + y^3 = z^3$ has no solutions in $\mathbb{N}$. Lamé gave an argument that $x^p + y^p = z^p$ has no solutions in n for p and odd prime whenever $\mathbb{Z}[\zeta_p]$ has unique factorization.

Even when $\mathbb{Z}[\sqrt{-d}]$ does not have unique factorization, we can still use knowledge of the class group to determine the primes of the form $x^2 + dy^2$. Specifically, we used the fact that $\mathbb{Z}[\sqrt{-5}]$ has class number 2 to determine the primes of the form $x^2 + 5y^2$ at the end of last semester. (Refer to last semester's Chapter 12 notes, or wait till we review this next chapter.) In order to approach this problem for general $d > 0$ squarefree, observe $p = x^2 + dy^2 = (x + y\sqrt{-d})(x - y\sqrt{-d})$, which means the prime p splits into prime ideals $(p) = (x + y\sqrt{-d})(x - y\sqrt{-d})$ in the ring $\mathbb{Z}[\sqrt{-d}]$. This is a particular case of the general question, given an extension of number fields L/K and a prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$, how do we determine how it behaves in L, i.e., what is the prime ideal factorization of $\mathfrak{p}\mathcal{O}_L$ in $\mathcal{O}_L$? This is another basic question of Algebraic Number Theory, and in particular when $K = \mathbb{Q}$, it will tell us what is the prime ideal factorization of (n) in $\mathcal{O}_L$. Hence, this is important for studying general Diophantine equations also, and this question will be the focus of the next chapter.

In the following chapter, we will briefly talk about cyclotomic fields $K = \mathbb{Q}(\zeta_p)$ where ζ_p is a primitive p-th root of unity and p is an odd prime. This is the next most important and basic type of number field after the quadratic fields. This will (i) give us a better understanding of the concepts discussed in this chapter for non-quadratic fields, and (ii) provide an opportunity for more applications. The most famous application of these fields is to Kummer's approach to Fermat's last theorem. While a complete proof of Kummer's result would take longer than we would like to spend on this, we will at least give a sketch of the argument using Dedekind's ideal theory (as opposed to Kummer's original approach via ideal numbers).

Finally, a look at the class number tables in this chapter shows that even in the simple case of quadratic fields, the class numbers behave with apparently little regularity, just like prime numbers seem to behave with little regularity. Thus it might seem unlikely that one could come up with an exact formula for the class number h_K. Remarkably, Dirichlet did just that, using the theory of L-functions, which itself is closely related to hidden regularities in prime numbers. This is what we will study at the end of Part I.

2 Primes in extensions

This chapter is about the following basic question: given an extension of number fields L/K and a prime ideal $\mathfrak{p}$ in $\mathcal{O}_K$, how does $\mathfrak{p}\mathcal{O}_L$ factor into prime ideals of $\mathcal{O}_L$? This question is intimately tied up with many questions of arithmetic. Going back to our motivating question of which primes p are of the form $p = x^2 + ny^2$ ($n \neq 1$ squarefree), we will see that these are essentialy the p for which (p) is a product of two principal ideals in $\mathbb{Q}(\sqrt{-n})$. After addressing this general question about splitting of prime ideals, we will apply this to primes of the form $x^2 + ny^2$.

Afterwards, we may do some more stuff, but then again maybe we won't.

Note: we will sometimes talk about "ideals" of K or L, or "primes" of K or L. This is merely a simplification of terminology and simply means (ordinary) ideals of $\mathcal{O}_K$ or $\mathcal{O}_L$, or prime ideals of $\mathcal{O}_K$ or $\mathcal{O}_L$.

Another piece of notation to be careful of: if $\alpha \in \mathcal{O}_K$, then (α) may represent $\alpha\mathcal{O}_K$ or $\alpha\mathcal{O}_L$ depending upon whether we are talking about ideals of K or ideals of L. This should hopefully be clear from context in most cases. If not, we will explicitly write $\alpha\mathcal{O}_K$ or $\alpha\mathcal{O}_L$.

The presentation of this material in this chapter is, for the most part, based on [Marcus] and, to a lesser extent, [Cohn] (for the quadratic case) and [Neukirch].

2.1 Splitting of primes

Throughout L/K denotes an extension of number fields. Before we give the basic definitions, let's recall what happens in the simplest example, which we studied last semester.

Example 2.1.1. *Let $K = \mathbb{Q}$ and $L = \mathbb{Q}(i)$. Since $\mathcal{O}_K = \mathbb{Z}$ is a PID, any prime ideal of $\mathcal{O}_K$ is of the form (p) where p is a prime of $\mathbb{Z}$. If $p = x^2 + y^2 = N_{L/K}(x + yi)$, then $p = \alpha\beta$ for some $\alpha, \beta \in \mathcal{O}_L$ and $(p) = (\alpha)(\beta)$ in $\mathcal{O}_L$, i.e., (p) is a product of two principal ideals in $\mathcal{O}_L$. Furthermore $\mathfrak{p}_1 = (\alpha)$ and $\mathfrak{p}_2 = (\beta)$ are both prime since they have norm p. The ideals $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are distinct except in the case $p = 2 = (1+i)(1-i)$ since $1 + i = -i(1 - i)$, i.e., $1 + i$ and $1 - i$ differ by units.*

If p is not a sum of two squares, then this means there is no element of norm p in $\mathcal{O}_L$, so p is irreducible in $\mathcal{O}_L$. Hence if some prime ideal $\mathfrak{p}$ of $\mathcal{O}_L$ divides (p) but $\mathfrak{p} \neq (p)$, then it can't be principal (otherwise, the generator of $\mathfrak{p}$ would divide p). However $h_L = 1$ so $\mathcal{O}_L$ is a PID. Thus $(p) = p\mathcal{O}_L = \{p\alpha : \alpha \in \mathcal{O}_L\}$ is itself a prime ideal.

Hence in this example, there are 3 possibilities for what happens to a prime ideal $p\mathcal{O}_K$ of K in the extension L:

(1) it splits *as a product of two distinct prime ideals $(p) = \mathfrak{p}_1\mathfrak{p}_2$ in $\mathcal{O}_L$ iff $\pm p = x^2 + y^2$ and $p \neq 2$, i.e., iff $p \equiv 1 \bmod 4$;*

(2) it ramifies *as the square of a prime ideal $(p) = 2\mathcal{O}_L = (1 + i)^2 = \mathfrak{p}^2$ in $\mathcal{O}_L$ iff $\pm p = 2$; and*

(3) it remains prime *or is* inert*, i.e., $p\mathcal{O}_L$ is a prime ideal of $\mathcal{O}_L$, if and only if $\pm p \neq x^2 + y^2$, i.e., iff $p \equiv 3 \bmod 4$.*

If $\mathfrak{a}$ is an ideal of $\mathcal{O}_K$, we define

$$\mathfrak{a}\mathcal{O}_L = \{a_1x_1 + a_2x_2 + \cdots + a_kx_k : a_i \in \mathfrak{a}, x_i \in \mathcal{O}_L\}.$$

Notice this is just like the definition of the product of two ideals of the same ring. It is easy to see that this is the smallest ideal of $\mathcal{O}_L$ which contains the set $\mathfrak{a}$ (see exercise below). Note if $\mathfrak{a} = (a)$ is a principal ideal of $\mathcal{O}_K$, then $\mathfrak{a}\mathcal{O}_L = (a) = \{ax : x \in \mathcal{O}_L\}$.

Exercise 2.1. *Let $\mathfrak{a}$ be an ideal of $\mathcal{O}_K$ and $\mathfrak{A}$ be an ideal of $\mathcal{O}_L$. Show $\mathfrak{a}\mathcal{O}_L$ is an ideal of $\mathcal{O}_L$ and $\mathfrak{A} \cap K = \mathfrak{A} \cap \mathcal{O}_K$ (justify this equality) is an ideal of $\mathcal{O}_K$. We call $\mathfrak{a}\mathcal{O}_L$ the* **extension** *of $\mathfrak{a}$ to L and $\mathfrak{A} \cap \mathcal{O}_K$ the* **restriction** *of $\mathfrak{A}$ to K.*

It is tradition to use gothic lower case letters for ideals of $\mathcal{O}_K$ and upper case gothic letters for ideals of $\mathcal{O}_L$. (Though I suppose it's also tradition to write $\mathcal{O}_K$ as $\mathfrak{O}_K$, I'm not as fond of that one.) However if $K = \mathbb{Q}$, we just use integers for the ideals of $\mathcal{O}_K = \mathbb{Z}$ since they are all principal, and lower case gothic letters for ideals of the extension L, as in the example above. If you have trouble writing gothic letters by hand, you can just write the corresponding roman letter with an underscore, or use another script.

While the extension and restriction of ideals are defined uniquely, this is not a 1-to-1 correspondence, as there are more ideals of $\mathcal{O}_L$ than ideals of $\mathcal{O}_K$. Precisely, we will see that different ideals of $\mathcal{O}_K$ extend to different ideals of $\mathcal{O}_L$, but different ideals of $\mathcal{O}_L$ can restrict to the same ideal of $\mathcal{O}_K$.

Definition 2.1.2. *Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$ and $\mathfrak{P}$ be a prime ideal of $\mathcal{O}_L$. We say $\mathfrak{P}$* **lies over** *(or* **lies above***) $\mathfrak{p}$ in L/K if $\mathfrak{P}|\mathfrak{p}\mathcal{O}_L$. We sometimes write this as $\mathfrak{P}|\mathfrak{p}$.*

Going back to the previous example, in case (1) $\mathfrak{p}_1$ and $\mathfrak{p}_2$ lie above (p); in case (2) $\mathfrak{p}$ lies above (p) and in case (3) $(p) = p\mathcal{O}_L$ lies above $(p) = p\mathcal{O}_K$.

Let $\mathfrak{p}$ be a prime (ideal) of $\mathcal{O}_K$ and $\mathfrak{P}$ be a prime (ideal) of $\mathcal{O}_L$.

Lemma 2.1.3. *The following are equivalent:*
(a) $\mathfrak{P}|\mathfrak{p}$, i.e., $\mathfrak{P}|\mathfrak{p}\mathcal{O}_L$
(b) $\mathfrak{P} \supseteq \mathfrak{p}$
(c) $\mathfrak{P} \cap \mathcal{O}_K = \mathfrak{P} \cap K = \mathfrak{p}$.

Proof. (a) $\Rightarrow$ (b) since $\mathfrak{P} \supseteq \mathfrak{p}\mathcal{O}_L \supseteq \mathfrak{p}$.

To see (b) $\Rightarrow$ (c), observe that $\mathfrak{P} \supseteq \mathfrak{p}$ implies $\mathfrak{P} \cap \mathcal{O}_K \supseteq \mathfrak{p}$. Since $\mathfrak{p}$ is maximal, and $\mathfrak{P} \cap \mathcal{O}_K$ is an ideal by the exercise above, we have $\mathfrak{P} \cap \mathcal{O}_K$ is either $\mathfrak{p}$ or $\mathcal{O}_K$. The latter is impossible since it would imply $1 \in \mathfrak{P}$.

To see (c) $\Rightarrow$ (b) $\Rightarrow$ (a), note that (c) implies $\mathfrak{P} \supseteq \mathfrak{p}$ is obvious, and then $\mathfrak{P} \supseteq \mathfrak{p}\mathcal{O}_L$ since $\mathfrak{P}$ is an ideal of $\mathcal{O}_L$. □

In light of the equivalence (a) $\iff$ (b), the notation $\mathfrak{P}|\mathfrak{p}$ for one ideal lying over another agrees with the usage of the notation $\mathcal{I}|\mathcal{J}$ to mean divides (contains) for ideals of $\mathcal{O}_K$.

Another thing this lemma shows is that two different ideals of L can restrict to the same ideal of K. For example if p is a prime of $K = \mathbb{Q}$, and $p\mathcal{O}_L = \mathfrak{p}_1\mathfrak{p}_2$ with $\mathfrak{p}_1 \neq \mathfrak{p}_2$, then $\mathfrak{p}_1$ and $\mathfrak{p}_2$ both restrict to the ideal $p\mathbb{Z}$ of $\mathbb{Z}$. More generally, all primes $\mathfrak{P}$ of $\mathcal{O}_L$ lying above a prime $\mathfrak{p}$ of $\mathcal{O}_K$ restrict to $\mathfrak{p}$.

Proposition 2.1.4. *Every prime $\mathfrak{P}$ of $\mathcal{O}_L$ lies above a unique prime $\mathfrak{p}$ of K. Conversely, every prime $\mathfrak{p}$ of K is contained in some prime $\mathfrak{P}$ of $\mathcal{O}_L$, i.e., there is some prime $\mathfrak{P}$ of $\mathcal{O}_L$ such that $\mathfrak{P}|\mathfrak{p}$.*

Proof. Suppose $\mathfrak{P} \cap \mathcal{O}_K|\mathfrak{a}\mathfrak{b}$ for some ideals $\mathfrak{a}$, $\mathfrak{b}$ of $\mathcal{O}_K$. Then $\mathfrak{P} \supseteq (\mathfrak{a}\mathcal{O}_L)(\mathfrak{b}\mathcal{O}_L)$ so $\mathfrak{P} \supset \mathfrak{a}\mathcal{O}_L$ or $\mathfrak{P} \supset \mathfrak{b}\mathcal{O}_L$ since $\mathfrak{P}$ is prime. Restricting to K, we see $\mathfrak{P} \cap \mathcal{O}_K|\mathfrak{a}$ or $\mathfrak{P} \cap \mathcal{O}_K|\mathfrak{b}$. Hence $\mathfrak{P} \cap \mathcal{O}_K$ is a prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ by definition, i.e., $\mathfrak{P}|\mathfrak{p}$. By the previous lemma, $\mathfrak{P}|\mathfrak{p}$ implies $\mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}$, hence

$\mathfrak{p}$ is unique. This proves the first statement, though technically one should also show $\mathfrak{P} \cap \mathcal{O}_K \neq \{0\}$. This is easy—see the exercise below.

The second statement is seemingly obvious: given $\mathfrak{p}$, the extension $\mathfrak{p}\mathcal{O}_L$ has a prime ideal factorization in $\mathcal{O}_L$, so any prime ideal $\mathfrak{P}$ occurring in the factorization lies above $\mathfrak{p}$. However as before, one needs to show a seemingly obvious technicality: $\mathfrak{p}\mathcal{O}_L \neq \mathcal{O}_L$ (otherwise $\mathfrak{p}\mathcal{O}_L$ would not have a prime ideal factorization). This is also an exercise. □

Exercise 2.2. *Let L/K be an extension of number fields and $\mathcal{I}$ be a (nonzero) ideal of $\mathcal{O}_L$. Show $\mathcal{I} \cap \mathcal{O}_K \neq \{0\}$. (You may want to consider using norms.)*

Exercise 2.3. *(a) Let $\mathfrak{a}$ be a proper ideal of $\mathcal{O}_K$. Show there exists a $\gamma \in K - \mathcal{O}_K$ such that $\gamma\mathfrak{a} \subseteq \mathcal{O}_K$.*

(b) Let L/K be an extension of number fields and $\mathfrak{p}$ a prime ideal of $\mathcal{O}_K$. Show $\mathfrak{p}\mathcal{O}_L \neq \mathcal{O}_L$. (Use (a) to get a contradiction if $\mathfrak{p}\mathcal{O}_L = \mathcal{O}_L$.)

Exercise 2.4. *(a) Let $\mathfrak{a}, \mathfrak{b}$ be ideals of K. Show $\mathfrak{a}\mathcal{O}_L | \mathfrak{b}\mathcal{O}_L \implies \mathfrak{a}|\mathfrak{b}$. (Think about prime factorizations in K and L.)*

(b) Show $\mathfrak{a}\mathcal{O}_L \cap \mathcal{O}_K = \mathfrak{a}$ for any ideal $\mathfrak{a}$ of $\mathcal{O}_K$, i.e., the restriction of an extension gives the ideal you started with. (Use (a) with $\mathfrak{b} = \mathfrak{a}\mathcal{O}_L \cap \mathcal{O}_K$.)

(c) Determine which ideals $\mathfrak{A}$ of L satisfy $(\mathfrak{A} \cap \mathcal{O}_K)\mathcal{O}_L = \mathfrak{A}$, i.e., determine when the extension of the restriction of an ideal is the ideal you started with.

Looking back at the case of $K = \mathbb{Q}$ and $L = \mathbb{Q}(i)$ from Example 2.1.1, we see sometimes the number of primes lying above $\mathfrak{p}$ is 1 and sometimes it is 2. In general, the number of primes above $\mathfrak{p}$ is never greater than $n = [L : K]$, and if we count with primes with "multiplicty" and "weight" it will always be n. Multiplicity is easy to imagine: if $[L : K] = 2$ and $\mathfrak{p} = \mathfrak{P}^2$ then it makes sense to count $\mathfrak{P}$ two times—technically this multiplicity is called the *ramification index* (or *ramification degree*). There is only one prime that is ramified in the extension $\mathbb{Q}(i)/\mathbb{Q}$, namely $2\mathbb{Z}[i] = (1+i)^2$.

The notion of some primes being "weighted" is a little more subtle, but it can obviously happen that $\mathfrak{p} = \mathfrak{P}$, i.e., a prime $\mathfrak{p}$ of K *remains prime* (or is *inert*) in L, i.e., $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}$ is prime in L. If we go back to Example 2.1.1, half of the primes in $\mathbb{Q}$ are inert in $\mathbb{Q}(i)$, the ones $\equiv 3 \bmod 4$, i.e., the primes not sums of 2 squares. One way to differentiate the case of inert and "split" primes in this example is the following. For split primes ($p \equiv 1 \bmod 4$), we have $\mathfrak{p}\mathcal{O}_L = p\mathcal{O}_L = \mathfrak{P}_1\mathfrak{P}_2$, then $[\mathcal{O}_L : \mathfrak{P}_i] = N(\mathfrak{P}_i) = p$ (this also holds for the ramified case of $p = 2$), but for inert primes ($p \equiv 1 \bmod 3$), then $\mathfrak{P} = \mathfrak{p}\mathcal{O}_L = p\mathcal{O}_L$ is prime in L and we have $[\mathcal{O}_L : \mathfrak{P}] = N(\mathfrak{P}) = N_{L/K}(p) = p^2$.

Hence, if we think of the exponent of p in $N(\mathfrak{P}) = [\mathcal{O}_L : \mathfrak{P}]$ as the "weight" of $\mathfrak{P}$, then we can say the weighted sum of the primes above $\mathfrak{p}$ (with multiplicity) is always 2, at least in Example 2.1.1. In general, when the base field $K \neq \mathbb{Q}$, this definition of weight needs to be appropriately modified, and we give the formal definitions of the appropriate multiplicity (ramification index) and weight (inertial degree) below.

Exercise 2.5. *Suppose $\mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}$. Show the ring embedding $\mathcal{O}_K \hookrightarrow \mathcal{O}_L$ yields a field embedding $\mathcal{O}_K/\mathfrak{p} \hookrightarrow \mathcal{O}_L/\mathfrak{P}$. In other words, the finite field $\mathcal{O}_L/\mathfrak{P}$ is an extension of $\mathcal{O}_K/\mathfrak{p}$.*

Definition 2.1.5. *Let $\mathfrak{p}$ be a prime of K. Suppose the prime ideal factorization of $\mathfrak{p}\mathcal{O}_L$ is $\mathfrak{p} = \prod \mathfrak{P}_i^{e_i}$ where each $\mathfrak{P}_i$ is distinct. The* **ramification index** *of $\mathfrak{P}_i$ over $\mathfrak{p}$ is $e(\mathfrak{P}_i|\mathfrak{p}) = e_i$ and the* **inertial degree** *of $\mathfrak{P}_i$ over $\mathfrak{p}$ is $f(\mathfrak{P}_i|\mathfrak{p}) = f_i = [\mathcal{O}_L/\mathfrak{P}_i : \mathcal{O}_K/\mathfrak{p}]$.*

This definition of inertial degree is really the natural generalization of the "weight" of $\mathfrak{P}$ we suggested in the case of $\mathbb{Q}(i)/\mathbb{Q}$ (see also lemma below). The previous exercise guarantees it makes sense. For instance, if $K = \mathbb{Q}$, then and $\mathfrak{P} = p\mathcal{O}_L$ is prime in L, then $f(\mathfrak{P}|(p)) = [\mathcal{O}_L/p\mathcal{O}_L : \mathbb{Z}/p\mathbb{Z}]$. Now $\mathcal{O}_L/p\mathcal{O}_L$ must be the finite field of order $N(p\mathcal{O}_L) = N_{L/\mathbb{Q}}(p) = p^n$ where $n = [L : K]$, which has degree n over $\mathbb{Z}/p\mathbb{Z}$, so the inertial degree is $f(\mathfrak{P}|(p)) = n$.

The above definition of inertial degree, is the standard one, but it is clearly equivalent to the following form, which will be useful to us.

Lemma 2.1.6. *The inertial degree $f_i = f(\mathfrak{P}_i|\mathfrak{p})$ satisfies $N(\mathfrak{P}_i) = N(\mathfrak{p})^{f_i}$.*

Proof. We know $\mathcal{O}_K/\mathfrak{p}$ is a finite field of some order, say $q = N(\mathfrak{p})$. By the exercise above $\mathcal{O}_L/\mathfrak{P}$ is an extension of $\mathcal{O}_K/\mathfrak{p}$, and the order of this extension field is $q^{f_i} = N(\mathfrak{P}_i)$ by the definition of the inertial degree. Hence $N(\mathfrak{p})^{f_i} = N(\mathfrak{P})$. □

Theorem 2.1.7. (The fundamental identity) *With the notation in the definition,*

$$\sum e_i f_i = n = [L : K].$$

For simplicity, we will omit some details of the proof when $K \neq \mathbb{Q}$.

Proof. Note

$$N(\mathfrak{p}\mathcal{O}_L) = \prod N(\mathfrak{P}_i)^{e_i} = \prod N(\mathfrak{p})^{e_i f_i},$$

by the previous lemma. Then the theorem follows from the statement that $N(\mathfrak{p}\mathcal{O}_L) = N(\mathfrak{p})^n$.

This is true but not entirely obvious—one must check some details. However in our main case of interest, which is $K = \mathbb{Q}$, it is particularly simple, and in the interest of time and simplicity we will restrict to when $K = \mathbb{Q}$. Then $\mathfrak{p} = (p)$ for some $p \in \mathbb{N}$ and $N(\mathfrak{p}\mathcal{O}_L) = N(p\mathcal{O}_L) = N_{L/K}(p) = p^n$. □

Hence if $\mathfrak{p}\mathcal{O}_L = \prod \mathfrak{P}_i^{e_i}$ (with each $\mathfrak{P}_i$ distinct), the number of $\mathfrak{P}_i$ lying above $\mathfrak{p}$ is at most $n = [L : K]$, and is exactly n if we count multiplicities e_i's and "weights" f_i's. Now let's give a couple names for different ways in which $\mathfrak{p}$ (i.e., $\mathfrak{p}\mathcal{O}_L$) can factor in $\mathcal{O}_L$.

Definition 2.1.8. *Write $\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^{g} \mathfrak{P}_i^{e_i}$ (with each $\mathfrak{P}_i$ distinct). If $e_i > 1$ for some i, we say $\mathfrak{p}$* **ramifies** *in L. Otherwise, we say $\mathfrak{p}$ is* **unramified** *in L.*

If $g > 1$, i.e. there is more than one prime of L above $\mathfrak{p}$, then we say $\mathfrak{p}$ is **split** *in L. If $g = 1$, i.e. there is only one prime of L above $\mathfrak{p}$, we say $\mathfrak{p}$ is* **nonsplit** *in L.*

If $g = n$, i.e. $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1\mathfrak{P}_2 \cdots \mathfrak{P}_n$, then we say $\mathfrak{p}$ is **totally split** *(or* **splits completely***) in L. If $g = 1$ and $e_1 = 1$, i.e. if $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1$, then we say $\mathfrak{p}$ is* **inert** *(or* **remains prime***) in L.*

Note by the fundamental identity, if $\mathfrak{p}$ is totally split in L, then $e_i = f_i = 1$ for each i. Similarly if $\mathfrak{p}$ is inert in L then $f(\mathfrak{P}|\mathfrak{p}) = n$ where $\mathfrak{P} = \mathfrak{p}\mathcal{O}_L$. In particular if $\mathfrak{p}$ is totally split or inert in L, then it is unramified. We will see shortly that ramification is a special phenomenon which only happens for finitely many primes.

We now give a couple of simple consequences of the lemma and fundamental identity.

Corollary 2.1.9. *Let $\mathfrak{p}$ be a prime ideal of K which lies above a prime $p \in \mathbb{N}$. Then $N(\mathfrak{p}) = p^k$ for some $1 \leq k \leq [K : \mathbb{Q}]$.*

Proof. It follows from the lemma above (or the argument before with the base field being $\mathbb{Q}$), that $N(\mathfrak{p}) = p^{f(\mathfrak{p}|(p))}$. We know $k = f(\mathfrak{p}|(p)) \leq n$ by the fundamental identity. □

Knowing this is useful in determining whether an ideal is prime or not, and in determining how a prime of $\mathbb{Q}$ splits in K. A consequence of this (without requiring the bound on k) is the fact that an ideal of K divides (the ideal generated by) its norm. Recall we mentioned this result can be used to prove that the class number of K is finite (see Lemma 1.6.6.

Corollary 2.1.10. *Let $\mathcal{I}$ be an ideal of K and $m = N(\mathcal{I})$. Then $\mathcal{I}|m\mathcal{O}_K$.*

Proof. Write $\mathcal{I} = \prod \mathfrak{p}_i$ where the $\mathfrak{p}_i$'s are (not necessarily distinct) prime ideals of K. Then $m = N(\mathcal{I}) = \prod N(\mathfrak{p}_i)$. By the previous corollary, we can write $N(\mathfrak{p}_i) = p_i^{f_i}$ for some f_i where $\mathfrak{p}_i|p_i$. In particular $\mathfrak{p}_i \supseteq p_i\mathcal{O}_K \supseteq p_i^{f_i}\mathcal{O}_K$. Hence

$$\mathcal{I} = \prod \mathfrak{p}_i \supseteq \prod \mathfrak{p}_i^{f_i}\mathcal{O}_K = m\mathcal{O}_K.$$

□

Now one might ask if all primes of L above $\mathfrak{p}$ have the same ramification index and inertial degree. This is not true in general, but it is true if we pass to the Galois closure of L. Precisely, we have the following.

Theorem 2.1.11. *Suppose L/K is Galois and write $\mathfrak{p} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$ where the $\mathfrak{P}_i$'s are distinct prime ideals of L. Then $\mathrm{Gal}(L/K)$ acts transitively on $\mathfrak{P}_1, \ldots, \mathfrak{P}_g$. In particular $e_1 = e_2 = \cdots = e_g$ and $f_1 = f_2 = \cdots = f_g$. In this case, if we set $e = e_1$ and $f = f_1$, we have*

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^e\mathfrak{P}_2^e \cdots \mathfrak{P}_g^e$$

and the fundamental identity becomes

$$n = efg.$$

Proof. Let $\sigma \in \mathrm{Gal}(L/K)$ and $\mathfrak{P}|\mathfrak{p}$. Since L/K is Galois, $\sigma(\mathfrak{P}) \subseteq \mathcal{O}_L$. It follows immediately from the definitions that $\sigma(\mathfrak{P})$ is an ideal of $\mathcal{O}_L$ and $\sigma(\mathfrak{P})$ is prime. Note if $x \in \mathfrak{p}$, then $\sigma(x) = x$ since $x \in \mathcal{O}_L$. Thus $\mathfrak{P} \supseteq \mathfrak{p}$ implies $\sigma(\mathfrak{P}) \supseteq \mathfrak{p}$, i.e., $\sigma(\mathfrak{P})|\mathfrak{p}$. This implies $\mathrm{Gal}(L/K)$ acts on $\mathfrak{P}_1, \ldots, \mathfrak{P}_g$.

Now we want to show this action is transitive. Suppose it is not, i.e., suppose $\mathfrak{P}, \mathfrak{P}'|\mathfrak{p}$ but $\mathfrak{P}' \neq \sigma(\mathfrak{P})$ for any $\sigma \in \mathrm{Gal}(L/K)$. By the Chinese Remainder Theorem (for general rings) there is an $x \in \mathcal{O}_L$ such that

$$x \equiv 0 \bmod \mathfrak{P}',\ x \equiv 1 \bmod \sigma(\mathfrak{P}) \text{ for all } \sigma \in \mathrm{Gal}(L/K).$$

Now $y = N_{L/K}(x) = \prod \sigma(x) \in \mathfrak{P}' \cap \mathcal{O}_K = \mathfrak{p}$. On the other hand $\mathfrak{P} \nmid (y) = \prod(\sigma(x))$ since no $\sigma(x) \in \mathfrak{P}$. But this means $y \notin \mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$, a contradiction.

This shows $\mathrm{Gal}(L/K)$ acts transitively on $\mathfrak{P}_1, \ldots, \mathfrak{P}_g$. On the other hand, $\mathrm{Gal}(L/K)$ fixes $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1}\mathfrak{P}_2^{e_2} \cdots \mathfrak{P}_g^{e_g}$, so all the ramification indices e_i are the same by uniqueness of prime ideal factorization. Also, because $\mathfrak{P}_1, \ldots, \mathfrak{P}_g$ are Galois conjugates of each other, they all have the same norm. Hence the all the inertial degrees f_i are the same. The restatement of the fundamental identity is immediate. □

When L/K is Galois, we say the ideals $\sigma(\mathfrak{P})$ are **conjugates** of $\mathfrak{P}$.

We remark that just like one can define the norm of elements from L to K, one can define the norm of ideals from L to K. Precisely, if $\mathfrak{A}$ is an ideal of L, then the norm from L to K of $\mathfrak{A}$ is

$$N_{L/K}(\mathfrak{A}) = \prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma(\mathfrak{A}) \cap \mathcal{O}_K.$$

Of course, this norm is an ideal, not a number, but remember that ideals are a sort of generalization of numbers. One can show this satisfies various nice properties, and thus it can be useful like the usual norm is useful.

Exercise 2.6. *Suppose L/K is Galois.*

(a) Suppose $\mathfrak{P}$ is a prime of L lying above $\mathfrak{p}$, a prime of K. Let $f = f(\mathfrak{P}|\mathfrak{p})$. Show $N_{L/K}(\mathfrak{P}) = \mathfrak{p}^f$.

(b) Show $N_{L/K}(\mathfrak{AB}) = N_{L/K}(\mathfrak{A})N_{L/K}(\mathfrak{B})$ for any ideals $\mathfrak{A}, \mathfrak{B}$ of $\mathcal{O}_L$.

(c) Let $\mathfrak{A}$ be an ideal of L with norm $n = N(\mathfrak{A}) = |\mathcal{O}_L/\mathfrak{A}|$. Show $N_{L/\mathbb{Q}}(\mathfrak{A}) = (n)$. In other words, the notion of an "ideal-valued norm" from L to K agrees with the original definition of the integer-valued norm when $K = \mathbb{Q}$ (identifying the principal ideal (n) with the integer n).

2.2 Splitting in quadratic fields

In this section, we will let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic field. As usual we will assume $d \neq 1$ is squarefree. Further p will denote a prime (element) of $\mathbb{Z}$ and $\mathfrak{p}$ will denote a prime (ideal) of $\mathcal{O}_K$.

In this case, the splitting of p (i.e., of $p\mathbb{Z}$) in K is particularly simple. By the fundamental identity there are at most 2 prime ideals of K lying above p (i.e., $p\mathbb{Z}$), counting multiplicity. Hence either p is inert in K, i.e., $p\mathcal{O}_K$ is a prime ideal of $\mathcal{O}_K$, or $p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2$ where $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are prime ideals of $\mathcal{O}_K$. When $\mathfrak{p}_1 = \mathfrak{p}_2$, p is ramified in $\mathcal{O}_K$, and when $\mathfrak{p}_1 \neq \mathfrak{p}_2$, p splits in $\mathcal{O}_K$. Note that since K is quadratic, p splitting and p splitting completely are one and the same.

Let $\Delta = \Delta_K$ be the discriminant of K. Recall $\Delta = d$ if $d \equiv 1 \bmod 4$ and $\Delta = 4d$ if $d \equiv 2, 3 \bmod 4$.

Let $\left(\frac{a}{p}\right)$ denote the **Kronecker symbol** mod p. If p is odd, $\left(\frac{a}{p}\right)$ is the ordinary Legendre symbol define for any $a \in \mathbb{Z}$, i.e., $\left(\frac{a}{p}\right) = 1$ when $\gcd(a, p) = 1$ and a is a square mod p, $\left(\frac{a}{p}\right) = -1$ when $\gcd(a, p) = 1$ and a is a nonsquare mod p, and $\left(\frac{a}{p}\right) = 0$ when $p|a$. If $p = 2$, we set

$$\left(\frac{a}{2}\right) = \begin{cases} 0 & 4|a \\ 1 & a \equiv 1 \bmod 8 \\ -1 & a \equiv 5 \bmod 8 \\ \text{undefined} & a \not\equiv 0, 1 \bmod 4. \end{cases}$$

This is an extension of the Legendre symbol where we have allowed $p = 2$ on the bottom, and $p|a$ for p odd. Note the definition for $p = 2$ satisfies

$$\left(\frac{a}{2}\right) = \left(\frac{2}{a}\right)$$

whenever $a \equiv 0, 1 \bmod 4$. Since the squares mod 8 are $0, 1, 4$, the Kronecker symbol mod 2 detects whether an $a \equiv 0, 1, \bmod 4$ is a square mod 8. The problem with $a \not\equiv 0, 1 \bmod 4$, is one cannot extend the Kronecker symbol to integer values for such a so that it is multiplicative in a. However, this is fine for us, since we only want that $\left(\frac{\Delta}{p}\right)$ is defined for any prime $p \in \mathbb{N}$, which it is since $\Delta \equiv 0, 1 \bmod 4$. The utility of this definition is apparent from the following result on the splitting of p in K.

Theorem 2.2.1. *Let $p \in \mathbb{N}$ be prime.*

(i) If $\left(\frac{\Delta}{p}\right) = 0$ then p is ramified in K.

(ii) If $\left(\frac{\Delta}{p}\right) = 1$ *then* p *is split in* K*.*
(iii) If $\left(\frac{\Delta}{p}\right) = -1$ *then* p *is inert in* K*.*

Note this say the primes with ramify in K are precisely the ones dividing Δ. In particular, there are finitely many.

Proof. Let $\mathfrak{p}$ be a prime of K lying above p. Then $\mathfrak{p}$ is a subgroup of $\mathcal{O}_K$ which is free of rank 2 over $\mathbb{Z}$. In particular, $\mathfrak{p}$ is generated (as an ideal) by at most 2 elements of $\mathcal{O}_K$. We may take one of them to be p, and write $\mathfrak{p} = (p, \pi)$ for some $\pi \in \mathcal{O}_K$. Write $\pi = \frac{a+b\sqrt{d}}{2}$. Further, since $N(\mathfrak{p})|N_{K/\mathbb{Q}}(\pi)$ we have $p|N_{K/\mathbb{Q}}(\pi) = \frac{a^2-db^2}{4}$, so $a^2 \equiv db^2 \bmod p$ (in fact, mod $4p$).

We first prove the contrapositive of (iii). Suppose $p\mathcal{O}_K$ is not inert and p is odd. Then $\mathfrak{p} \neq p\mathcal{O}_K$, so $p \nmid \pi$, i.e., a and b are not both divisible by p. This implies $b \not\equiv 0 \bmod p$. Let b^{-1} such that $b^{-1}b \equiv 1 \bmod p$. Then $a^2 \equiv db^2 \bmod p$ implies $(ab^{-1})^2 \equiv d \bmod p$, i.e., d is a square mod p so either $\left(\frac{d}{p}\right) = 1$ or 0, according to whether $p \nmid d$ or $p|d$. Since $\Delta = d$ or $\Delta = 4d$, $\left(\frac{d}{p}\right) \neq -1$ implies $\left(\frac{\Delta}{p}\right) \neq -1$. This proves (iii).

A similar argument works for $p = 2$.

Now suppose $\left(\frac{\Delta}{p}\right) = 0$ and p odd. Then $\left(\frac{\Delta}{p}\right) = \left(\frac{d}{p}\right)$, so $p|d$. In this case, we can take $\mathfrak{p} = (p, \sqrt{d})$. To see this, observe that any element of $\mathfrak{p}$ looks like

$$\frac{1}{2}((x + y\sqrt{d})p + (z + w\sqrt{d})\sqrt{d}) = \frac{1}{2}(px + dw + (z + py)\sqrt{d})$$

for some $x, y, z, w \in \mathbb{Z}$. Since $p|d$, this means

$$\mathcal{O}_K \supsetneq (p, \sqrt{d}) = \left\{\frac{1}{2}(px + y\sqrt{d}) : x, y \in \mathbb{Z}\right\} \cap \mathcal{O}_K \supsetneq p\mathcal{O}_K.$$

Hence $\mathfrak{p} = (p, \sqrt{d})$ lies above p. Thus $p\mathcal{O}_K = \mathfrak{p}\overline{\mathfrak{p}}$ where $\overline{\mathfrak{p}}$ is the conjugate ideal of $\mathfrak{p}$ in K, but $\overline{\mathfrak{p}} = (p, -\sqrt{d}) = \mathfrak{p}$, so p is ramified in K.

The case of $\left(\frac{\Delta}{p}\right) = 0$ and $p = 2$ is an exercise below.

Now assume $\left(\frac{\Delta}{p}\right) = 1$ and p odd, so that $\left(\frac{\Delta}{p}\right) = \left(\frac{d}{p}\right) = 1$. Let $a \in \mathbb{Z}$ be such that $a^2 \equiv d \bmod p$. Note $p \nmid a$ since $p \nmid d$. We claim we can take $\overline{p} = (p, a + \sqrt{d})$. Then the conjugate ideal is $\overline{\mathfrak{p}} = (p, a - \sqrt{d})$. It is clear that$\mathfrak{p}, \overline{\mathfrak{p}} \supsetneq p\mathcal{O}_K$, so it suffices to show $\mathfrak{p} \neq \mathcal{O}_K$. To see this, observe that

$$\mathfrak{p}\overline{\mathfrak{p}} = (p^2, pa + p\sqrt{d}, pa - p\sqrt{d}, a^2 - d) \subseteq p\mathcal{O}_K.$$

Hence $p\mathcal{O}_K = \mathfrak{p}\overline{\mathfrak{p}}$ (and $\mathfrak{p}, \overline{\mathfrak{p}}$ are primes of K). It remains to show $\mathfrak{p} \neq \overline{\mathfrak{p}}$. If $\mathfrak{p} = \overline{\mathfrak{p}}$, then we would have $2a = a + \sqrt{d} - a - \sqrt{d} \in \mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$, which is impossible since $p \nmid 2a$. This shows p splits in K.

Suppose $\left(\frac{\Delta}{p}\right) = 1$ and $p = 2$. Then $\Delta \equiv 1 \bmod 8$. Then as in the p odd case one shows one can take $\mathfrak{p} = (2, \frac{1+\sqrt{d}}{2})$, $\overline{\mathfrak{p}} \neq \mathfrak{p}$ and $\mathfrak{p}\overline{\mathfrak{p}} = 2\mathcal{O}_K$. □

Exercise 2.7. *Suppose* $\left(\frac{\Delta}{2}\right) = 0$*. Show* $\mathfrak{p} = (2, \pi)$ *is a proper ideal of* K *containing* $2\mathcal{O}_K$*, where* $\pi = \sqrt{d}$ *or* $1 + \sqrt{d}$ *according to whether* d *is even or odd. Use this to verify (i) in the above theorem for* $p = 2$*.*

Exercise 2.8. *Let* $K = \mathbb{Q}(\sqrt{-5})$*. Determine which primes of* $\mathbb{Q}$ *ramify in* K *and which are unramified. Then determine which primes of* $\mathbb{Q}$ *split completely in* K *and which are inert.*

Note that in the course of the proof of the above theorem, we were able to explicitly describe the prime ideals of K lying above p. For convenient reference, we summarize this below.

Corollary 2.2.2. *If $p \neq 2$ is ramified in K, then $\mathfrak{p} = (p, \sqrt{d})$ is a prime of K lying above p. (For $p = 2$ ramified in K, see Exercise 2.7 above.) If $p \neq 2$ splits in K, then $\mathfrak{p} = (p, a + \sqrt{d})$ is a prime of K lying above p for any a such that $a^2 \equiv d \bmod p$. If 2 splits in K, then $d \equiv 1 \bmod 4$ and $\mathfrak{p} = (2, \frac{1+\sqrt{d}}{2})$ is a prime of K lying above 2.*

The above theorem is very useful for many things. One application is to determining class numbers and class groups of quadratic fields.

Example 2.2.3. *Let $K = \mathbb{Q}(\sqrt{-19})$. This has determinant $\Delta = -19$. By Lemma 1.6.4 (or Minkowski's bound, which is the same in this case), every ideal of $\mathcal{O}_K$ is equivalent to one of norm at most $\frac{2}{\pi}\sqrt{19} \approx 2.85$. There is only ideal of norm one, namely $\mathcal{O}_K$, which is principal. Any ideal of norm 2 must lie above 2 (Corollary 2.1.9), but $\left(\frac{\Delta}{2}\right) = -1$ since $\Delta = -19 \equiv 5 \bmod 8$, i.e., 2 is inert in K. Hence there is no ideal of norm 2, which means the class number $h_K = 1$.*

Exercise 2.9. *Show $K = \mathbb{Q}(\sqrt{-15})$ has class number 2.*

Exercise 2.10. *Show $K = \mathbb{Q}(\sqrt{-43})$ has class number 1.*

Another application of the above theorem is to determining primes of the form $x^2 + ny^2$, which we consider next.

2.3 Primes of the form $x^2 + ny^2$

Recall that one of our motivating questions, both this semester and last semester, was to study numbers of the form $x^2 + ny^2$. Any two number of the form $x^2 + ny^2$ have a product which is also of the form $x^2 + ny^2$ by Brahmagupta's composition law, so this question largely reduces to the question of which primes p are of the form $x^2 + ny^2$.

It is clear that $p = x^2 + ny^2$ means p is reducible in the ring of integers of $K = \mathbb{Q}(\sqrt{-n})$. For simplicity, we assume n is a square free integer, and put $d = -n$, so $K = \mathbb{Q}(\sqrt{d})$ which coincides with the notation in the previous section. For the result below we will allow n to be negative, because it is no extra work (it just involves including a $\pm$ sign), though our main interest is in $n > 0$.

We will also assume $n \neq -1$, because then $K = \mathbb{Q}$. So the case of $n = -1$ is particularly simple, as our question is: which primes are of the form $p = x^2 - y^2 = (x-y)(x+y)$. But this factorization means (say for $p > 0$) that $x - y = 1$ so $p = 2y + 1$, i.e., all odd $p > 0$ are of the form $x^2 - y^2$. Interchanging x and y also shows that any odd $p < 0$ is of the form $x^2 - y^2$.

Proposition 2.3.1. *Let p be a prime of $\mathbb{Z}$. If $p = x^2 + ny^2$ for some $x, y \in \mathbb{Z}$, then $p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2$ where $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are (not necessarily distinct) principal prime ideals of $\mathcal{O}_K$. Conversely, if $p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2$ where $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are principal prime ideals of $\mathcal{O}_K$, then*

(i) $\pm p$ is of the form $x^2 + ny^2$ if $n \equiv 1, 2 \bmod 4$;

(ii) $\pm 4p$ is of the form $x^2 + ny^2$ if $n \equiv 3 \bmod 4$.

Proof. ($\Rightarrow$) As above, set $d = -n$ to match with notation from the previous section. Suppose $p = x^2 + ny^2 = x^2 - dy^2 = (x + y\sqrt{d})(x - y\sqrt{d})$. Since p is squarefree, both x and y must be nonzero so $\alpha = x + y\sqrt{d}$ and $\beta = x - y\sqrt{-d}$ are nonzero nonunits of $\mathcal{O}_K$. Thus $p\mathcal{O}_K = (\alpha)(\beta)$

is the prime ideal factorization of $p\mathcal{O}_K$. (The ideals (α) and (β) are prime either by the argument that $N_{K/\mathbb{Q}}(\alpha) = N_{K/\mathbb{Q}}(\beta) = \pm p$ or using the fundamental identity to count the prime ideals in the factorization of $p\mathcal{O}_K$).

($\Leftarrow$) Suppose $p\mathcal{O}_K$ is a product of two principal prime ideals $\mathfrak{p}_1 = (\alpha)$ and $\mathfrak{p}_2 = (\beta)$. Since the ideals (α) and (β) are conjugate, we may assume α and β are conjugate, i.e., $\alpha = x + y\sqrt{d}$, $\beta = x - y\sqrt{d}$ for some $x, y \in \mathbb{Q}$. Then $N_{K/\mathbb{Q}}(\alpha) = N_{K/\mathbb{Q}}(\beta) = p$, and the factorization $p\mathcal{O}_K = (\alpha)(\beta)$ implies $p = u\alpha\beta = u(x^2 - dy^2)$ for some unit u of $\mathcal{O}_K$. Since $x^2 - dy^2 \in \mathbb{Z}$, we must have $u = \pm 1$.

If $d \equiv 2, 3 \bmod 4$, then we may assume $x, y \in \mathbb{Z}$ so we have shown (i). If $d \equiv 1 \bmod 4$, then $x, y \in \frac{1}{2}\mathbb{Z}$ and (ii) follows. □

Note that we can rephrase the $n \equiv 1, 2 \bmod 4$ case as follows: $\pm p = x^2 + ny^2$ if and only if $p\mathcal{O}_K$ is a product of 2 (not necessarily distinct) principal ideals in $\mathcal{O}_K$.

When $n > 0$, the $\pm$ sign here is moot: negative p are never of the form $x^2 + ny^2$, but for $n < 0$ the distinction of whether p or $-p$ is of the form $x^2 + ny^2$ is somewhat more subtle. Our main focus is when $n > 0$, so we will not worry about this now, but it can be treated via the general theory of binary quadratic forms. We will discuss binary quadratic forms in Part II, but again our focus there will be mostly on the "positive" cases.

One can make a similar if and only if statement when $n \equiv 3 \bmod 4$.

Exercise 2.11. *Suppose $n \equiv 3 \bmod 4$. Show $p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2$ for two (not necessarily distinct) prime ideals $\mathfrak{p}_1, \mathfrak{p}_2$ of $\mathcal{O}_K$ if and only if $\pm 4p = x^2 + ny^2$ for some $x, y \in \mathbb{Z}$.*

To see that these two cases are necessary, look at $K = \mathbb{Q}(\sqrt{-11})$. Then $p = 3 = \frac{1+\sqrt{-11}}{2}\frac{1-\sqrt{-11}}{2}$ so p splits in $\mathcal{O}_K$, but $3 \neq x^2 + 11y^2$ for $x, y \in \mathbb{Z}$. Of course $12 = 4 \cdot 3 = 1^2 + 11 \cdot 1^2$.

We remark that one could treat the $n \equiv 3 \bmod 4$ and the $n \equiv 1, 2 \bmod 4$ uniformly as follows: $\pm p = x^2 + ny^2$ if and only if $p\mathbb{Z}[\sqrt{-n}]$ is a product of two proper principal ideals of $\mathbb{Z}[\sqrt{-n}]$. However the issue with this is that the ideals of $\mathbb{Z}[\sqrt{-n}]$ (when $n \equiv 3 \bmod 4$) are more difficult to study than $\mathcal{O}_K$, e.g., the prime ideal factorization theorem does not hold for $\mathbb{Z}[\sqrt{-n}]$.

Now let's see how we can use this to give alternative (simpler) proofs of some of our main results from last semester. New cases are contained in the exercises. Below p denotes a prime number in $\mathbb{N}$ and $x, y \in \mathbb{Z}$.

Corollary 2.3.2. (Fermat's two square theorem) *We can write $p = x^2 + y^2$ if and only if $p = 2$ or $p \equiv 1 \bmod 4$.*

Proof. By the proposition, $p = x^2 + y^2$ if and only if p is a product of two (not necessarily distinct) principal ideals in $\mathbb{Q}(i)$. ($-p$ cannot be a sum of 2 squares so the $\pm$ in the proposition is not an issue here.) Since we know the class number of $\mathbb{Q}(i)$ is 1, we in fact have $p = x^2 + y^2$ if and only if p splits or ramifies in $\mathbb{Q}(i)$.

Here $\Delta = \Delta_{\mathbb{Q}(i)} = -4$, so by Theorem 2.2.1, $p = x^2 + y^2$ if and only if $p = 2$ (the ramified case) or $\left(\frac{\Delta}{p}\right) = \left(\frac{-4}{p}\right) = \left(\frac{-1}{p}\right) = 1$. But the first supplementary law to quadratic reciprocity tells us $\left(\frac{-1}{p}\right) = 1$ if and only if $p \equiv 1 \bmod 4$. □

Exercise 2.12. *We have $p = x^2 + 2y^2$ if and only if $p = 2$ or $p \equiv 1, 3 \bmod 8$.*

We proved this in Chapter 9 last semester, but you should give a simpler argument using the above results. Then we left the case of $x^2 + 3y^2$ as an exercise in Chapter 9, which you may recall was considerably more challenging than the $x^2 + 2y^2$ case. In fact, we still haven't made things any

easier on ourselves for this case since this corresponds to $d \equiv 1 \bmod 4$ above. It may be worthwhile to see what the issue is, so let's go through this.

Suppose $p = x^2 + 3y^2$. Then by the above proposition $p\mathcal{O}_K$ is a product of two principal ideals of $\mathcal{O}_K$, where $K = \mathbb{Q}(\sqrt{-3})$. In this case $h_K = 1$, so every ideal is principal. Hence p either splits or ramifies in $\mathcal{O}_K$ which means $\left(\frac{\Delta}{p}\right) = \left(\frac{-3}{p}\right) = \left(\frac{p}{3}\right) = 0$ or 1, i.e., $p = 3$ or $p \equiv 1 \bmod 3$. Clearly $p = 3$ is of the form $x^2 + 3y^2$. It remains to show if $p \equiv 1 \bmod 3$, then $p = x^2 + 3y^2$. By this same computation of $\left(\frac{\Delta}{p}\right)$, if $p \equiv 1 \bmod 3$, the p splits into two (prinicipal) ideals of K. However since $d = -n \equiv 1 \bmod 4$, the above proposition only tells us that $4p = x^2 + 3y^2$. For instance $4 \cdot 7 = 5^2 + 3 \cdot 1^2$. It is not clear how to conclude that we must have $p = (x')^2 + 3(y')^2$ for some x', y', though it is true. Roughly, one might like to use Brahmagupta's composition law (the product of two numbers of the form $x^2 + ny^2$ is again of this form—this is simple, but not pretty, computation) in reverse: $4 = 1^2 + 3 \cdot 1^2$ and $4p$ are both of the form $x^2 + 3y^2$, so their *quotient* $p = 4p/4$ should be. We will see that one can more or less do just this using Gauss's theory of binary quadratic forms in Part II. Hence for now, we will forget about the case $n \equiv 3 \bmod 4$ (i.e., $d \equiv 1 \bmod 4$).

Corollary 2.3.3. *We have $p = x^2 + 5y^2$ if and only if $p = 5$ or $p \equiv 1, 9 \bmod 20$.*

Proof. Let $K = \mathbb{Q}(\sqrt{-5})$ so $\Delta = \Delta_K = -20$. Only two primes p ramify in K, $p = 2$ and $p = 5$. Clearly $2 \neq x^2 + 5y^2$ and $5 = x^2 + 5y^2$, so from now on, assume p is unramified. (By the proposition above, this corresponds to the fact that $2\mathcal{O}_K$ is the square of the nonprincipal ideal $(2, 1 + \sqrt{-5})$ and $5\mathcal{O}_K$ is the square of the principal ideal $(\sqrt{-5})$.)

Note that p is split in K if and only if $\left(\frac{\Delta}{p}\right) = \left(\frac{-5}{p}\right) = 1$, i.e., if and only if $p \equiv 1, 3, 7, 9 \bmod 20$.

($\Rightarrow$) If $p = x^2 + 5y^2$, then p splits in K by the proposition, so $p \equiv 1, 3, 7, 9 \bmod 20$. On the other hand, $x^2 + 5y^2 \equiv x^2 + y^2 \equiv 0, 1, 2 \bmod 4$ so $p \not\equiv 3, 7 \bmod 20$. (Alternatively, one can look at the squares mod 20.)

($\Leftarrow$) Suppose $p \equiv 1, 9 \bmod 20$ but $p \neq x^2 + 5y^2$. The congruence conditions imply $p\mathcal{O}_K = \mathfrak{p}\overline{\mathfrak{p}}$ where $\mathfrak{p}$ is a prime ideal of K, and $p \neq x^2 + 5y^2$ means $\mathfrak{p}$ is nonprincipal. Since $h_K = 2$, this means $\mathfrak{p} \sim (2, 1 + \sqrt{-5})$, i.e., $\mathfrak{p} = \alpha(2, 1 + \sqrt{-5})$ for some $\alpha \in K$.

Write $\alpha = \frac{a}{c} + \frac{b}{d}\sqrt{-5}$ for some $a, b, c, d \in \mathbb{Z}$. Note that 2α and $(1 + \sqrt{-5})\alpha$ must lie in $\mathcal{O}_K$. Since $2\alpha \in \mathcal{O}_K$, $c|2$ and $d|2$ so we can write $\alpha = \frac{a + b\sqrt{-5}}{2}$ (replacing a and b with $2a$ and $2b$ if necessary). Then one has

$$(2)\mathfrak{p} = (a + b\sqrt{-5})(2, 1 + \sqrt{-5}).$$

Taking norms yields

$$2p = a^2 + 5b^2.$$

Reducing this equation mod 5 yields $a^2 \equiv 2, 3 \bmod 5$ (since $p \equiv 1, 4 \bmod 5$), which is a contradiction. □

For a slightly different argument, see last semester's Chapter 12 Notes. One could simplify this proof if we knew we could use Brahmagupta's composition law in reverse (see above remarks on x^2+3y^2). In particular, for the argument in the ($\Leftarrow$) direction, $\mathfrak{p} \sim (2, 1+\sqrt{-5})$ means $(a+b\sqrt{-5})\mathfrak{p} = (c + d\sqrt{-5})(2, 1 + \sqrt{-5})$ for some $a, b, c, d \in \mathbb{Z}[\sqrt{-5}]$. Taking norms gives $p(a^2 + 5b^2) = 2(c^2 + 5d^2)$. Since 2 is not of the form $x^2 + 5y^2$, one would like to conclude p is not either, but it is not obvious how to make this argument work. We will essentially be able to via genus theory in Part II.

Before moving on, let us observe there is another interesting characterization of which primes are of the form $x^2 + 5y^2$. Suppose $n > 0$ and $n \equiv 1, 2, \bmod 3$. As before, set $K = \mathbb{Q}(\sqrt{-n})$. When

$h_K = 1$, the above proposition and the theorem if that a prime p is of the form $x^2 + ny^2$ if and only if $\left(\frac{\Delta}{p}\right) = 0$ or 1. By quadratic reciprocity, one can then essentially say an prime p is of the form $x^2 + ny^2$ if and only if p is a square mod Δ. (One can formalize this with a different extension of the Legendre symbol called the Jacobi symbol—we won't go through the details, but you can observe it in the simplest case: $p \neq 2$ is of the form $x^2 + y^2$ if and only if p is a square mod $\Delta_{\mathbb{Q}(i)} = -4$.)

When $h_K = 2$ (or larger), the problem is the quadratic residue symbol can essentially only detect 2 things—whether p is split or inert (or ramified). But we need to distinguish when a p splits into principal ideals and when p splits into nonprincipal ideals. Check the following criterion for $x^2 + 5y^2$.

Exercise 2.13. *Let $K = \mathbb{Q}(\sqrt{-5})$, and $p \in \mathbb{N}$ be a rational prime. Show $p = x^2 + 5y^2$ if and only if $\left(\frac{\Delta}{p}\right) = 1$ and p is a square mod Δ.*

One can treat other forms $x^2 + ny^2$ similar to $x^2 + 5y^2$ when the class number of $\mathbb{Q}(\sqrt{-n})$ is 2.

Exercise 2.14. *Determine all primes of the form $x^2 + 6y^2$.*

When the class number of $K = \mathbb{Q}(\sqrt{-n})$ is larger than 2, determining the primes of the form $x^2 + ny^2$ can get considerably more complicated, and the solution will depend upon the structure of the class group $\mathcal{C}l_K$. In general, primes of the form $x^2 + ny^2$ are not characterized just by simple congruence conditions (though it always will be if $\mathcal{C}l_K \simeq (\mathbb{Z}/2\mathbb{Z})^r$). We will explore some of the issues involved in Part II.

2.4 General splitting results

In this section, let L/K be an extension of number fields, let $\mathfrak{p}$ denote a prime of K and $\mathfrak{P}$ denote a prime of L. If $\mathfrak{p}\mathcal{O}_L = \prod \mathfrak{P}_i^{e_i}$ with the $\mathfrak{P}_i$'s distinct prime ideals of L, then f_i denotes the inertial degree $f_i = f(\mathfrak{P}_i|\mathfrak{p})$.

In Section 2.2, we saw that it is simple to understand completely the way a prime $\mathfrak{p}$ splits in L when $K = \mathbb{Q}$ and L is quadratic. (It is also not much harder when K is arbitrary and L/K is quadratic.) In general things are not so simple, but there are some general fundamental results which describe the splitting of primes in L/K. We will not give complete proofs in both the interest of time and simplicity.

Note that $\mathcal{O}_K[\alpha]$ is a free $\mathcal{O}_K$-module of rank $n = [L : K]$, so it has finite index (either as an abelian group or $\mathcal{O}_K$-module) in $\mathcal{O}_L$. Thus $\mathcal{O}_L/\mathcal{O}_K[\alpha]$ is a finite abelian group.

Theorem 2.4.1. *Write $L = K(\alpha)$ and let $q(x) \in \mathcal{O}_K[x]$ be the minimum polynomial for α over K. Suppose p is a prime of $\mathbb{Z}$ such that $p \nmid |\mathcal{O}_L/\mathcal{O}_K[\alpha]|$ and $\mathfrak{p}$ is a prime ideal of K lying above p. Write*

$$q(x) \equiv q_1(x)^{e_1} q_2(x)^{e_2} \cdots q_g(x)^{e_g} \bmod \mathfrak{p}$$

where the q_i's are distinct irreducible polynomials (of positive degree) in the finite field $\mathcal{O}_K/\mathfrak{p}$. Then

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1}\mathfrak{P}_2^{e_2} \cdots \mathfrak{P}_g^{e_g}$$

for distinct prime ideals $\mathfrak{P}_1, \ldots, \mathfrak{P}_g$ of $\mathcal{O}_L$ such that $f_i = f(\mathfrak{P}_i|\mathfrak{p}) = \deg q_i(x)$.

This theorem provides a way to determine how prime ideals $\mathfrak{p}$ of K split in L. For technical reasons, a finite number of primes $\mathfrak{p}$ are excluded from this result.

Proof. (Sketch.) One first shows

$$\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L \simeq (\mathcal{O}_K[\alpha])/(\mathfrak{p}\mathcal{O}_K[\alpha]) \simeq (\mathcal{O}_K/\mathfrak{p})[x]/(\overline{q}(x)),$$

where $\overline{q}(x)$ is the image of $q(x)$ in $(\mathcal{O}_K/\mathfrak{p})[x]$. The first isomorphism requires that $\mathfrak{p}\mathcal{O}_L + \mathfrak{F} = \mathcal{O}_L$ where the *conductor* $\mathfrak{F}$ is the largest ideal of $\mathcal{O}_L$ contained in $\mathcal{O}_K[\alpha]$. This is where the technicality that $p \nmid |\mathcal{O}_L/\mathcal{O}_K[\alpha]|$ comes in. The second isomorphism is straightforward.

Then one can use the Chinese Remainder Theorem (for general rings, whose proof is essentially the same as for $\mathbb{Z}$),

$$(\mathcal{O}_K/\mathfrak{p})[x]/(\overline{q}(x)) \simeq \bigoplus_{i=1}^{g} (\mathcal{O}_K/\mathfrak{p})[x]/(\overline{q}_i(x)^{e_i}),$$

where $\overline{q}_i(x)$ is the image of $q_i(x)$ in $(\mathcal{O}_K/\mathfrak{p})[x]$. □

Exercise 2.15. *Suppose $K = \mathbb{Q}$ and $L = \mathbb{Q}(\sqrt{-5})$. Determine $|\mathcal{O}_L/\mathcal{O}_K[\alpha]|$ where $\alpha = \sqrt{-5}$. Verify the above theorem in this case.*

Theorem 2.4.2. *Consider the extension $K/\mathbb{Q}$. Then a prime (p) of $\mathbb{Q}$ ramifies in K if and only if $p|\Delta_K$.*

In particular, only finitely many primes of $\mathbb{Q}$ ramify in K.

Corollary 2.4.3. *Let L/K be an extension of number fields. If a prime $\mathfrak{p}$ of K ramifies in L, then $\mathfrak{p}$ lies above a prime of $\mathbb{N}$ dividing Δ_L. In particular, only finitely many primes $\mathfrak{p}$ of K ramify in L.*

Exercise 2.16. *Deduce this corollary from the previous theorem.*

3 Zeta and L-functions

In this section we will use analytic methods to (i) develop a formula for class numbers, and (ii) use this to prove Dirichlet's theorem in arithmetic progressions: that any arithmetic progression: $a+m, a+2m, a+3m, \ldots$ contains infinitely many primes $\gcd(a,m)=1$.

This chapter follows [Cohn], though our presentation is reversed from his, together with some supplementary material taken from various other sources. More general treatments are found in [Marcus] and [Neukirch], though they do not do everything we will do here.

3.1 Zeta functions

Recall one defines the **Riemann zeta function** by

$$\zeta(s) = \sum \frac{1}{n^s}. \tag{3.1}$$

One knows from calculus that this converges for $s > 1$ (compare with

$$\int_1^\infty \frac{1}{x^s} dx = \frac{x^{1-s}}{1-s}\Big]_{x=1}^{\infty} = \frac{1}{1-s} < \infty.)$$

Euler observed that (for $s > 1$) one also has the product expansion

$$\zeta(s) = \sum \frac{1}{n^s} = \prod_p \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \cdots\right) = \prod \frac{1}{1-p^{-s}}.$$

Here p runs over all primes of $\mathbb{N}$. The last equality just follows from the formula for a geometric series: $\sum_{n=0}^{\infty} a^n = \frac{1}{1-a}$ if $|a| < 1$. To see the why product expansion (middle equality) is valid, it's perhaps easiest to first notice that it is *formally* true for $s = 1$,* where it says

$$\sum \frac{1}{n} = \left(1 + \frac{1}{2} + \frac{1}{2^2} + \frac{1}{2^3} + \cdots\right)\left(1 + \frac{1}{3} + \frac{1}{3^2} + \frac{1}{3^3} + \cdots\right)\left(1 + \frac{1}{5} + \frac{1}{5^2} + \frac{1}{5^3} + \cdots\right)\cdots \tag{3.2}$$

What does this (formal) infinite product on the right mean? It just means a (formal) limit of the sequence of finite subproducts:

$$1 + \frac{1}{2} + \frac{1}{2^2} + \frac{1}{2^3} + \cdots = \sum_{n \in \mathbb{N}_2} \frac{1}{n}$$

$$\left(1 + \frac{1}{2} + \frac{1}{2^2} + \frac{1}{2^3} + \cdots\right)\left(1 + \frac{1}{3} + \frac{1}{3^2} + \frac{1}{3^3} + \cdots\right) = 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{2\cdot 3} + \frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{2^2\cdot 3} + \frac{1}{2\cdot 3^2} + \cdots$$
$$= \sum_{n \in \mathbb{N}_{2,3}} \frac{1}{n}$$

*When $s = 1$, neither side of the equality actually converges, but the explanation for why both sides should be equal is perhaps more transparent. Here "formally" is not to be confused with rigorously—we mean we can formally manipulate one side to get to the other.

$$\left(1+\frac{1}{2}+\frac{1}{2^2}+\frac{1}{2^3}+\cdots\right)\left(1+\frac{1}{3}+\frac{1}{3^2}+\frac{1}{3^3}+\cdots\right)\left(1+\frac{1}{5}+\frac{1}{5^2}+\frac{1}{5^3}+\cdots\right)=\sum_{n\in\mathbb{N}_{2,3,5}}\frac{1}{n}$$

$$\vdots$$

where $\mathbb{N}_{p_1,p_2,\ldots,p_k}=\left\{p_1^{e_1}p_2^{e_2}\cdots p_k^{e_k}:e_i\in\mathbb{N}\cup\{0\}\right\}$, i.e., $\mathbb{N}_{p_1,p_2,\ldots,p_k}$ is the set of natural numbers which only contain the primes $p_1,\ldots p_k$ in their prime decomposition.

We now prove rigorously that the formal product expansion for $\zeta(s)$ given above is valid for $s>1$.

Definition 3.1.1. *Let $\{p\}$ denote the set of primes of $\mathbb{N}$. Let $a_p\in\mathbb{C}$ for each p. We define*

$$\prod_p a_p=\lim_{n\to\infty}\prod_{n<x}a_p.$$

Hence we will say $\prod a_p$ **converges (diverges)** *if the limit on the right does. We say $\prod a_p$* **converges absolutely** *if*

$$\lim_{n\to\infty}\prod_{i<n}a_{p_i}$$

converges for any ordering $\{p_1,p_2,p_3,\ldots\}$ of the set of primes $\{p\}$.

In other words, a product converges absolutely if it converges regardless of the way we order the terms in the product. One can of course similarly define infinite product over any denumerable index set

Example 3.1.2. *If some $a_p=0$, then after some point (no matter how the p's are ordered), we will have a finite subproduct of $\prod a_p=0$. Thus $\prod a_p$ will converge to 0 absolutely.*

Note that if every $a_p>0$, then $\log(\prod a_p)=\sum\log a_p$. An immediate consequence is that $\prod a_p$ converges (absolutely) if and only if the series $\sum\log a_p$ converges (absolutely).

Proposition 3.1.3. *Let $(a_n)_{n=1}^{\infty}$ be a totally multiplicative sequence of complex numbers, i.e., $a_{mn}=a_ma_n$ for any $m,n\in\mathbb{N}$, and assume $a_1=1$. If $\sum a_n$ converges absolutely, then so does $\prod_p\frac{1}{1-a_p}$ and*

$$\sum_{n=1}^{\infty}a_n=\prod_p\frac{1}{1-a_p},$$

where the product is taken over all primes p of $\mathbb{N}$.

Proof. Suppose $\sum a_n$ converges absolutely. Let $\epsilon>0$. Then for some $N\in\mathbb{N}$ we can say

$$\sum_{n>N}|a_n|<\epsilon.$$

Let $\{p_1,p_2,\ldots\}$ be any ordering of the set of primes of $\mathbb{N}$. Then there is some $K\in\mathbb{N}$ such that $\{p_1,\ldots,p_K\}$ contains all $\leq N$. Observe

$$\prod_{i=1}^{K}\frac{1}{1-a_{p_i}}=\prod_{i=1}^{K}\left(1+a_p+a_p^2+\cdots\right)=\sum_{n\in\mathbb{N}_{p_1,\ldots,p_K}}a_n.$$

Since $\mathbb{N}_{p_1,\ldots,p_K}$ contains $1,\ldots,N$, we have

$$\left|\sum_{n=1}^{\infty} a_n - \prod_{i=1}^{K} \frac{1}{1-a_{p_i}}\right| \leq \left|\sum_{n>N} a_n\right| \leq \sum_{n>N} |a_n| < \epsilon.$$

□

Corollary 3.1.4. *For any $s > 1$ the* **Euler product expansion**

$$\zeta(s) = \prod \frac{1}{1-p^{-s}} \tag{3.3}$$

is valid.

Proof. Apply the proposition with $a_n = n^{-s}$. □

The Euler product expansion demonstrates that the zeta function captures information about primes. In fact, it contains a surprising amount of information about primes. The simplest application of the zeta function to the study of primes is Euler's proof of the infinitude of primes.

Theorem 3.1.5. *There are infinitely many primes.*

Proof. Assume there are finitely many primes, $p_1,\ldots,p_k$. Then

$$\zeta(s) = \frac{1}{1-p_1^{-s}} \cdot \frac{1}{1-p_2^{-s}} \cdots \frac{1}{1-p_k^{-s}} \to \frac{1}{1-1/p_1} \cdot \frac{1}{1-1/p_2} \cdots \frac{1}{1-1/p_k} < \infty$$

as $s \to 1$. On the other hand

$$\zeta(s) = \sum \frac{1}{n^s} \to \sum \frac{1}{n} = \infty$$

as $s \to 1$. Contradiction. □

Exercise 3.1. *For any integer $k > 1$, one can show $1/\zeta(k)$ represents the probability that k "randomly chosen" integers are coprime (have gcd 1). Let $f(x) = x$ on $[-\pi, \pi)$, compute the Fourier coefficients and apply Parseval's identity. Use this to compute $\zeta(2)$, and hence determine the probability that 2 randomly chosen integers are coprime. (Alternatively, you can try to derive the product expansion*

$$\frac{\sin x}{x} = \prod_{n=1}^{\infty} \left(1 - \left(\frac{x}{n\pi}\right)^2\right),$$

and look at the x^2 coefficient to find $\zeta(2)$.)

We will briefly discuss some deeper connections of $\zeta(s)$ to the study of primes, but first let us give a generalization of the Riemann zeta function.

Definition 3.1.6. *Let K be a number field. The* **Dedekind zeta function** *for K is*

$$\zeta_K(s) = \sum_{\mathfrak{a}} \frac{1}{N(\mathfrak{a})^s},$$

for $s > 1$ where $\mathfrak{a}$ runs over all (nonzero) ideals of $\mathcal{O}_K$.

As before, one can show this series indeed converges for all $s > 1$, and we have an Euler product expansion

$$\zeta_K(s) = \prod_{\mathfrak{p}} \frac{1}{1 - N(\mathfrak{p})^{-s}}$$

valid for $s > 1$ as above. Hence the Dedekind zeta function can be used to study the prime ideals of of K.

We remark that another way to write the above definition is

$$\zeta_K(s) = \sum \frac{a_n}{n^s}$$

where a_n denotes the number of ideals of K with norm n (convince yourself of this). Consequently, the Dedekind zeta function can be used to study the number of ideals of norm n. However, we will be interested in it for its applications to the class number h_K of K.

3.2 Interlude: Riemann's crazy ideas

Riemann published a single paper in number theory, *On the Number of Primes Less Than a Given Magnitude* in 1859, which was 8 pages long, contained no formal proofs, and essentially gave birth to all of analytic number theory. We will summarize the main ideas here.

We only defined the Riemann zeta function for real $s > 1$, but in fact Riemann considered it for complex values of s. In general if $a > 0$ and $z \in \mathbb{C}$, then one defines

$$a^z = e^{z \ln a}$$

where

$$e^z = \sum \frac{z^n}{n!}.$$

This allows one formally to make sense of the definition

$$\zeta(s) = \sum \frac{1}{n^s}$$

for $s \in \mathbb{C}$, and one can show the sum actually converges provided $\mathrm{Re}(s) > 1$. Riemann showed that $\zeta(s)$ can be extended (uniquely) to a differentiable function on all of $\mathbb{C}$ except at $s = 1$, where $\zeta(s)$ has a *pole* (must be ∞). However the above series expression is only valid for $\mathrm{Re}(s) > 1$.

Riemann showed that $\zeta(s)$ has a certain symmetry around the line $\mathrm{Re}(s) = \frac{1}{2}$, namely one has the *functional equation*

$$\zeta(1 - s) = \Gamma^*(s)\zeta(s)$$

where $\Gamma^*(s)$ is a function closely related to the Γ function. The functional equation says one can compute $\zeta(1 - s)$ in terms of $\zeta(s)$, so we can indirectly use the series for $\zeta(s)$ to compute $\zeta(s)$ when $\mathrm{Re}(s) < 0$. The region $0 < \mathrm{Re}(s) < 1$ is called the *critical strip*, and the central line of symmetry $\mathrm{Re}(s) = \frac{1}{2}$ is called the *critical line*.

Let $\{\rho\}$ denote the set of zeroes of $\zeta(s)$ inside of the critical strip. There are countably (infinitely) many, and let us order them by their absolute value. Let

$$f(x) = \pi(x) + \frac{1}{2}\pi(x^{1/2}) + \frac{1}{3}\pi(x^{1/3}) + \cdots$$

where $\pi(x)$ is the number of primes less than x. Riemann discovered the following formula for $f(x)$

$$f(x) = \mathrm{Li}(x) - \sum_{\rho} \mathrm{Li}(x^{\rho}) - \log(2) + \int_x^{\infty} \frac{dt}{t(t^2-1)\ln t}$$

where $\mathrm{Li}(x) = \int_0^x \frac{dt}{\ln t}$. Hence this formula relates $\pi(x)$ with the (values of Li at the) zeroes of $\zeta(s)$. In fact, using Möbius inversion, one can rewrite $\pi(x)$ in terms of $f(x)$ (and therefore the zeroes of $\zeta(s)$) as

$$\pi(x) = f(x) - \frac{1}{2}f(x^{1/2}) - \frac{1}{3}(x^{1/3}) - \cdots$$

Essentially this says the following: if we know exactly where all the zeroes ρ of $\zeta(s)$ are we know exactly where the primes are (these are the places on the real line where $\pi(x)$ jumps).

Here is where Riemann made his famous conjecture, the *Riemann hypothesis*, that all the zeroes of $\zeta(s)$ lying in the critical strip actually lie on the critical line. (It is easy to see from series expansion that $\zeta(s) \neq 0$ for $\mathrm{Re}(s) \geq 1$. Then by the functional equation, $\zeta(1-s) = 0$ for $\mathrm{Re}(s) > 1$ if and only if $\Gamma^*(s) = 0$, which happens precisely for s a positive odd integer. Thus the only zeroes of $\zeta(s)$ outside of the critical strip, are the so-called *trivial zeroes* occurring when $s = -2k$, $k \in \mathbb{N}$.)

In 1896, Hadamard and de la Vallée Poussin used Riemann's ideas to prove the *prime number theorem*, that

$$\pi(x) \sim \mathrm{Li}(x) \sim \frac{x}{\ln x}$$

as $x \to \infty$. (This notation means $\pi(x)$ is approximately $\frac{x}{\ln x}$ for x large.) This is important, for example, in cryptography where one wants to know that the primes don't get too thinly spread out, so that large primes provide suitably secure keys for RSA. The Riemann hypothesis is equivalent to the "best possible bound" for the error term in the prime number theorem, precisely that

$$|\pi(x) - \mathrm{Li}(x)| < \frac{1}{8\pi}\sqrt{x}\ln(x)$$

for $x \geq 2657$. The Riemann hypothesis has natural generalizations to Dedekind zeta functions and L-functions (see below). Due to a host of applications, the generalized Riemann hypothesis is considered one of the most important open problems in mathematics.

3.3 Dirichlet L-functions

Let $m \in \mathbb{N}$. In 1837 (before Riemann!)*, Dirichlet introduced L-functions as a generalization of the Riemann zeta function in order to study the primes mod m. In particular, Dirichlet used these L-functions to show that there are infinitely many primes $\equiv a \bmod m$, which will be one of the main results of this chapter. This result had been conjectured by Euler for $a = 1$ and by Legendre in general.

Let's start with the example of $p \equiv 1 \bmod 4$. (Last semester we were able to use a trick together with the first supplemental law of quadratic reciprocity to show there are infinitely many primes $p \equiv 1 \bmod 4$, and the case of $p \equiv 3 \bmod 4$ was an exercise using a different trick. Legendre tried to use quadratic reciprocity to treat the general case, but was unsuccessful, and as far as I know, there is no proof of the general case which does not use Dirichlet L-functions.)

*Riemann's zeta function was studied before Riemann as a function of natural numbers by Euler.

Knowing Euler's proof of the infinitude of primes, one might be tempted to try to define a series by

$$\prod_{p\equiv 1 \bmod 4} \frac{1}{1-p^{-s}}.$$

This expands out as a sum

$$\sum_{n\in\mathbb{N}_1} \frac{1}{n^s}$$

where $\mathbb{N}_1$ is the set of all natural numbers which only contain primes $\equiv 1 \bmod 4$ in their prime factorization. If the number of such primes is finite then the product expansion converges as $s \to 1$, and one would like to show the series expansion diverges to obtain a contradiction. However summing over $\mathbb{N}_1$ is not a natural thing to do and there is no simple way to directly analyze it. Hence we will have to be a little more subtle than this.

Dirichlet, being smarter than this, had the following idea using characters. Let's first recall a couple things about characters of finite abelian groups.

Definition 3.3.1. *Let G be a finite abelian group. A* **character** *(or* **1-dimensional representation***) of G is a group homomorphism into $\mathbb{C}^\times$. The set of characters of G is denoted by $\hat{G}$, and is called the* **dual** *of G.*

Exercise 3.2. *Let G be a finite abelian group. Let $\chi, \lambda \in \hat{G}$.*

(i) Show $\chi\lambda$, defined by $(\chi\lambda)(g) = \chi(g)\lambda(g)$, is also in $\hat{G}$.

(ii) Show $\overline{\chi}$, defined by $\overline{\chi}(g) = \overline{\chi(g)}$, is also in $\hat{G}$. (Here the bar denotes complex conjugation.)

(iii) For any $g \in G$, show $\chi(g)$ is a (not necessarily primitive) n-th root of unity[†] where n is the order of g in G.

(iv) Deduce that $\overline{\chi}\chi = \chi_0$, where χ_0 denotes the **trivial character***, i.e., $\chi_0(g) = 1$ for all $g \in G$.*

(v) Conclude that $\hat{G}$ is an abelian group.

Proposition 3.3.2. *Let G be finite abelian group. Then $\hat{G} \simeq G$.*

Proof. Let us first prove the proposition in the case $G = C_n$ (the cyclic group of order n). Let α be a generator of G. By (iii) of the exercise above, if $\chi \in \hat{G}$, then $\chi(\alpha)$ must be an n-th root of unity ζ. Furthermore any n-th root of unity ζ defines (uniquely) a character on G by setting $\chi(\alpha^k) = \zeta^k$. (Observe this is character, and that nothing else can be.) In other words, a character is determined by what it does to a generator of G.

Let ζ_n denote a primitive n-th root of unity (take $\zeta_n = e^{2\pi i/n}$ if you wish). There are n n-th roots of unity, given by $\zeta_n^0 = 1, \zeta_n, \zeta_n^2, \ldots, \zeta_n^{n-1}$. Hence there are precisely n distinct character of G, $\chi_0, \chi_1, \chi_2, \ldots, \chi_{n-1}$ given by $\chi_i(\alpha) = \zeta_n^i$. It is obvious then that $(\chi_i\chi_j)\alpha = \zeta_n^{i+j}$, i.e., $\chi_i\chi_j = \chi_{i+j \bmod n}$. Hence $\hat{G} \simeq \mathbb{Z}/n\mathbb{Z} \simeq C_n$.

Now that we have prove the proposition in the case where G is cyclic, let us assume G is an arbitrary finite abelian group. Then we know by the classification of such groups, $G \simeq \prod C_{n_i}^{r_i}$. Set $\zeta_{n_i} = e^{2\pi i/n_i}$ and let $\alpha_i \in G$ be a generator for C_{n_i}. As above, we can define characters χ_{ij} on C_{n_i} by $\chi_{ij}(\alpha_i) = \zeta_{n_i}^j$. We can extend each χ_{ij} to a character on G by setting $\chi_{ij}(\alpha_k) = 1$ whenever $i \neq k$ and using multiplicativity. In other words, view and $g \in G$ as

$$g = (\alpha_1^{e_1}, \alpha_2^{e_2}, \ldots, \alpha_t^{e_t})$$

[†] $\zeta \in \mathbb{C}$ is a *primitive* n-th root of unity if $\zeta^n = 1$ but $\zeta^d \neq 1$ for any $d|n$. For example there are four 4-th roots of unity: $\pm 1, \pm i$, but only $\pm i$ are primitive.

and set

$$\chi_{ij}(g) = \zeta_{n_i}^{je_i}.$$

Hence for each i, we get disjoint subgroups of $\hat{G}$ each isomorphic to $\hat{C}_{n_i} \simeq C_{n_i}$. It is straightforward to check that any character of G is a product of some χ_{ij}'s, i.e., we have

$$\hat{G} \simeq \prod \hat{C}_{n_i} \simeq \prod C_{n_i} \simeq G.$$

□

We will be interested in the case where $G = (\mathbb{Z}/m\mathbb{Z})^\times$.

Example 3.3.3. *Suppose $G = (\mathbb{Z}/2\mathbb{Z})^\times$. Then $G = \{1\} = C_1$ so $\hat{G} = \{\chi_0\}$. In other words, the only character of G is the trivial one χ_0 which sends 1 to 1.*

Example 3.3.4. *Suppose $G = (\mathbb{Z}/3\mathbb{Z})^\times$. Then $G = \{1, 2\} \simeq C_2$ (here 1 and 2 represent the corresponding congruence classes in $\mathbb{Z}/3\mathbb{Z}$). Since 2 generates G and has order 2, there are two possibilities for characters:*

$$\chi_0 : 1 \mapsto 1, \ \ 2 \mapsto 1$$

and

$$\chi_1 : 1 \mapsto 1, \ \ 2 \mapsto -1$$

So $\hat{G} = \{\chi_0, \chi_1\} \simeq C_2$.

Note that $G = (\mathbb{Z}/4\mathbb{Z})^\times \simeq C_2$ also, so this case is essentially the same as $(\mathbb{Z}/3\mathbb{Z})^\times$.

Example 3.3.5. *Suppose $G = (\mathbb{Z}/5\mathbb{Z})^\times$. Then $G = \{1, 2, 3, 4\} \simeq C_4$. Here 2 generates G, so a character of G is determined by what 4-th root of unity 2 maps to. Explicitly, we have 4 characters, whose values are read off of the following* **character table***:*

	1	2	3	4
χ_0	1	1	1	1
χ_1	1	-1	-1	1
χ_2	1	i	$-i$	-1
χ_3	1	$-i$	i	-1

Looking at this table, it is easy to see $\hat{G}$ is cyclic of order four, generated either by χ_2 or χ_3.

Exercise 3.3. *Determine all characters of $(\mathbb{Z}/15\mathbb{Z})^\times$ and $(\mathbb{Z}/16\mathbb{Z})^\times$. (Write them down in character tables like our $(\mathbb{Z}/5\mathbb{Z})^\times$ case. Feel free to order the columns and rows however you find easiest.)*

Theorem 3.3.6. *Let $\mathbb{C}G = \{f : G \to \mathbb{C}\}$ denote the space of complex valued functions from a finite abelian group G into $\mathbb{C}$ (the* **group algebra** *of G). This is a $|G|$-dimensional vector space over $\mathbb{C}$. The characters $\chi \in \hat{G}$ form a $\mathbb{C}$-basis for $\mathbb{C}G$.*

We omit the proof, and in fact we do not need this precise result, but it is helpful for motivation. What this means for us is the following. We want to study the primes p in a congruence class mod m. As long as $p \nmid m$, we have $p \equiv a \bmod m$ for some $a \in (\mathbb{Z}/m\mathbb{Z})^\times$. Let $\{\chi\}$ denote the the set of characters of $G = (\mathbb{Z}/m\mathbb{Z})^\times$ and fix $a \in (\mathbb{Z}/m\mathbb{Z})^\times$. Consider the function $f \in \mathbb{C}G$ given by

$$f : (\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{C}$$

$$f(x) = \begin{cases} 1 & x = a \\ 0 & \text{else.} \end{cases}$$

In other words, f tells me if $p \bmod m$ is a or not. What the above says is that

$$f(x) = \sum c_\chi \chi(x)$$

for some $c_\chi \in \mathbb{C}$. Hence knowing $\chi(p \bmod m)$ for all χ tells us whether $p \equiv a \bmod m$ or not. Slightly more generally, the above theorem says knowing $\chi(p \bmod m)$ for all χ and $p \nmid m$ is the same as knowing $p \bmod m$ for all $p \nmid m$. Put another way, the characters of $(\mathbb{Z}/m\mathbb{Z})^\times$ distinguish all the (invertible) congruence classes mod m. This suggest it is possible to study the primes $\equiv a \bmod m$ using the characters of $(\mathbb{Z}/m\mathbb{Z})^\times$. To somehow connect this with something like the zeta function, one actually wants to think of the characters of $(\mathbb{Z}/m\mathbb{Z})^\times$ as "characters" of $\mathbb{Z}$.

Definition 3.3.7. *Let χ be a character of $(\mathbb{Z}/m\mathbb{Z})^\times$. We extend χ to a function*

$$\chi : \mathbb{Z} \to \mathbb{C}$$

by

$$\chi(a) = \begin{cases} \chi(a \bmod m) & \text{if } a \text{ is invertible } \bmod m \\ 0 & \text{else.} \end{cases}$$

The resulting function $\chi : \mathbb{Z} \to \mathbb{C}$ is called a **Dirichlet character** $\bmod m$.

Note that the values of χ only depend upon congruence classes mod m. Then our remarks before the definition can be rephrased as follows: knowing the value of $\chi(p)$ for every Dirichlet character $\chi \bmod m$ and every $p \nmid m$ is equivalent to knowing the value of $p \bmod m$ for every $p \nmid m$.

Example 3.3.8. *Consider χ_2 from our earlier $(\mathbb{Z}/5\mathbb{Z})^\times$ example. Then the corresponding Dirichlet character is*

$$\chi_2(a) = \begin{cases} 0 & a \equiv 0 \bmod 5 \\ 1 & a \equiv 1 \bmod 5 \\ i & a \equiv 2 \bmod 5 \\ -i & a \equiv 3 \bmod 5 \\ -1 & a \equiv 4 \bmod 5. \end{cases}$$

Exercise 3.4. *Let χ be a Dirichlet character mod m. Then $\chi(ab) = \chi(a)\chi(b)$ for any $a, b \in \mathbb{Z}$.*

Definition 3.3.9. *Let χ be a Dirichlet character mod m. Then* **Dirichlet L-function** *(or* **L-series***) for χ is given by*

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}. \tag{3.4}$$

for $s > 1$.

Note that since $|\chi(n)| \leq 1$ for all n (see Exercise 3.2(iii)), we can say

$$|L(s, \chi)| \leq \sum \frac{1}{n^s} = \zeta(s) \ \ (s > 1),$$

hence the series defining $L(s,\chi)$ converges absolutely for $s>1$. Because χ is multiplicative by the exercise above, the same expansion trick we used for $\zeta(s)$ above works to give a product expansion

$$L(s,\chi)=\prod_p \frac{1}{1-\chi(p)p^{-s}}, \tag{3.5}$$

which again is valid for $s>1$. (Just apply Proposition 3.1.3 with $a_n=\frac{\chi(n)}{n^s}$.)

Just like $\zeta(1)=\infty$ told us there were infinitely many primes, the most important value of $L(s,\chi)$ for primes in arithmetic progressions is $L(1,\chi)$ (which is not typically ∞—it will be if and only if $\chi=\chi_0$ is the trivial character mod m).

Example 3.3.10. *To return to the case of studying primes $\equiv 1 \bmod 4$, look at the Dirichlet characters mod 4. Since $(\mathbb{Z}/4\mathbb{Z})^\times \simeq C_2$, there are only two Dirichlet characters mod 4. We can write them as*

$$\chi_0(a)=\begin{cases}0 & a\equiv 0,2 \bmod 4\\ 1 & a\equiv 1,3 \bmod 4\end{cases}$$

(the trivial character) and

$$\chi_1(a)=\begin{cases}0 & a\equiv 0,2 \bmod 4\\ 1 & a\equiv 1 \bmod 4\\ -1 & a\equiv 3 \bmod 4\end{cases}$$

(the nontrivial character). Then, for $s>1$, we have

$$L(s,\chi_0)=\sum_{n\ odd}\frac{1}{n^s}=\prod_{p\neq 2}\frac{1}{1-p^{-s}}$$

and

$$L(s,\chi_1)=\sum_{n\equiv 1 \bmod 4}\frac{1}{n^s}-\sum_{n\equiv 3 \bmod 4}\frac{1}{n_s}=\prod_{p\equiv 1 \bmod 4}\frac{1}{1-p^{-s}}\cdot\prod_{p\equiv 3 \bmod 4}\frac{1}{1+p^{-s}}.$$

Hence these L-functions are not too far from our original naive suggestion, and they are not too difficulty (though not trivial) to analyze. We also note that $L(s,\chi_0)$ is essentially $\zeta(s)$—it is off by a single factor

$$\zeta(s)=\frac{1}{1-2^{-s}}L(s,\chi_0),$$

so $L(1,\chi_0)=(1-2^{-1})\zeta(1)=\infty$.

From the series expansion of $L(s,\chi_1)$ it's not to hard to see that

$$L(1,\chi_1)=1-\frac{1}{3}+\frac{1}{5}-\frac{1}{7}+\frac{1}{9}-\cdots=\frac{\pi}{4}$$

(The latter equality, known as Leibnitz's formula, follows from let $x\to 1$ in the Taylor series for $\arctan(x)$.) Now we can use this to show there are infinitely many primes $\equiv 1 \bmod 4$ and $\equiv 3 \bmod 4$.

Suppose there were finitely many primes $p\equiv 3 \bmod 4$. Then the above formula for $L(s,\chi_1)$ shows

$$\zeta(s)/L(s,\chi_1)=\frac{1}{1-2^{-s}}\prod_{p\equiv 3 \bmod 4}\frac{1+p^{-s}}{1-p^{-s}}$$

for $s > 1$. But then letting $s \to 1$ yields

$$\frac{1}{1-\frac{1}{2}} \cdot \prod_{p \equiv 3 \bmod 4} \frac{1+\frac{1}{p}}{1-\frac{1}{p}} = \zeta(1) \cdot \frac{4}{\pi} = \infty,$$

which is a contradiction since the left hand side must be finite if there are only finitely many $p \equiv 3 \bmod 4$.

Similarly suppose there were finitely many primes $p \equiv 1 \bmod 4$. Then

$$\begin{aligned}
\zeta(s)L(s,\chi_1) &= \frac{1}{1-2^{-s}} \left(\prod_{p \equiv 1 \bmod 4} \frac{1}{1-p^{-s}} \right)^2 \prod_{p \equiv 3 \bmod 4} \frac{1}{1-p^{-2s}} \\
&= \frac{1}{1-2^{-s}} \left(\prod_{p \equiv 1 \bmod 4} \frac{1}{1-p^{-s}} \right)^2 \left(\zeta(2s)(1-2^{-2s}) \prod_{p \equiv 1 \bmod 4} (1-p^{-2s}) \right) \\
&= (1+2^{-s}) \prod_{p \equiv 1 \bmod 4} \frac{1-p^{-2s}}{(1-p^{-s})^2} \cdot \zeta(2s).
\end{aligned}$$

for $s > 1$. Letting $s \to 1$, we see the right hand side is finite, since $\zeta(2) = \frac{\pi^2}{6} < \infty$ and the product has only finitely many terms, but the left hand side approaches $\zeta(1)/L(s,\chi_1) = \frac{4}{\pi}\infty = \infty$, a contradiction.

Hence just knowing that $0 < |L(1,\chi_1)| < \infty$ allows us to conclude there are infinitely many primes $p \equiv 1 \bmod 4$ and infinitely many $p \equiv 3 \bmod 4$.

Theorem 3.3.11. (Dirichlet's theorem on arithmetic progressions) *Suppose* $\gcd(a,m) = 1$. *Then there are infinitely many primes $p \equiv a \bmod m$.*

Proof. Let $\{\chi\}$ be the set of Dirichlet characters mod m. We consider the complex logarithm defined by

$$\log(1+z) = z - \frac{z^2}{2} + \frac{z^3}{3} - \cdots.$$

for $|z| < 1$. Then for any χ, we have

$$\left| \log\left(\frac{1}{1-\chi(p)p^{-s}} \right) \right| = |\log(1-\chi(p)p^{-s})| = \left| \frac{\chi(p)}{p^s} + \frac{\chi(p^2)}{2p^{2s}} + \frac{\chi(p^3)}{3p^{3s}} + \cdots \right|.$$

It follows from the Taylor expansion of $\log(1+x)$ that

$$\log\left(\frac{1}{1-\chi(p)p^{-s}} \right) = -\log(1-\chi(p)p^{-s}) = \frac{\chi(p)}{p^s} + \epsilon_p(s)$$

where $\epsilon_p(s)$ is an error term satisfying $|\epsilon_p(s)| < \frac{1}{p^{2s}}$. Hence

$$\log L(s,\chi) = \sum_p \frac{\chi(p)}{p^s} + \epsilon_\chi(s)$$

where $\epsilon_\chi(s) = \sum_p \epsilon_p(s)$ so $|\epsilon_\chi(s)| < \sum \frac{1}{p^{2s}}$.

Now consider the sum

$$\sum_{\chi} \chi^{-1}(a) \log L(s,\chi) = \sum_{\chi,p} \frac{\chi^{-1}(a)\chi(p)}{p^s} + \epsilon(s) \tag{3.6}$$

where $\epsilon(s) = \sum_{\chi} \chi^{-1}(a)\epsilon_{\chi}(s)$ is an error term. Now we appeal to a fundamental result from representation theory (see exercise below), the orthogonality relation for characters. This is essentially a refinement of Theorem 3.3.6, saying that the characters $\hat{G}$ of a group G form an *orthogonal* basis for $\mathbb{C}G$. In our case, the orthogonality relation says

$$\sum_{\chi} \chi^{-1}(a)\chi(p) = \begin{cases} \phi(m) & a \equiv p \bmod m \\ 0 & \text{else.} \end{cases}$$

(Here $\phi(m) = |(\mathbb{Z}/m\mathbb{Z})^{\times}|$.) Hence by first summing over χ, we see the only p that contribute are those $\equiv a \bmod m$. In other words

$$\sum_{\chi} \chi^{-1}(a) \log L(s,\chi) = \phi(m) \sum_{p \equiv a \bmod m} \frac{\chi(p)}{p^s} + \epsilon(s). \tag{3.7}$$

It is straightforward to check that the error term $\epsilon(s)$ remains bounded as $s \to 1$ (exercise below). Thus if there are only finitely many primes $p \equiv a \bmod m$, then the right hand side converges as $s \to 1$. In other words, it suffices to show the left hand diverges when $s \to 1$.

Consider the trivial character χ_0. Then

$$L(s,\chi_0) = \prod_{p \nmid m} \frac{1}{1-p^{-s}} = \prod_{p|m} (1-p^{-s}) \cdot \zeta(s),$$

hence $L(s,\chi_0) \to \prod_{p|m}(1-p^{-1}) \cdot \zeta(1) = \infty$ as $s \to 1$. Thus $\log L(s,\chi_0) \to \infty$ as $s \to 1$. This means the sum (3.6) must tend to ∞ as $s \to 1$ *provided* no single term $\chi^{-1}(a) \log L(s,\chi) \to -\infty$ as $s \to 1$. This follows from the fact that $L(s,\chi) \neq 0$, which is the content of Proposition 3.4.7 in the next section. □

The fact that $L(s,\chi) \neq 0$ follows from *Dirichlet's class number formula*, which is itself of great interest. Historically, Dirichlet proved his class number formula, and used this to prove his theorem on arithmetic progressions, though now there are other proofs that $L(1,\chi) \neq 0$. We will follow Dirichlet's approach (at least the presentation in [Cohn]) and prove the class number formula, and use this to conclude the proof of Theorem 3.3.11 in the next section.

Exercise 3.5. *Let $G = \mathbb{Z}/n\mathbb{Z}$. Let $a, b \in G$. Show*

$$\sum_{\chi \in \hat{G}} \chi^{-1}(a)\chi(b) = \begin{cases} |G| & a = b \\ 0 & \textit{else.} \end{cases}$$

(Hint: use the fact that we know explicitly what the characters are as in the proof of Proposition 3.3.2.) This proves the orthogonality relation we used above in the case of cyclic groups.

Exercise 3.6. *Check that the error term $\epsilon(s)$ appearing in the proof is bounded as $s \to 1$.*

3.4 The class number formula

The class number formula will fall out of analysis of the Dedekind zeta function. Let $K = \mathbb{Q}(\sqrt{d})$ where $d \neq 1$ is squarefree. Let $\Delta = \Delta_K$. Recall that for $s > 1$,

$$\zeta_K(s) = \prod_{\mathfrak{p}} \frac{1}{1 - N(\mathfrak{p})^{-s}}.$$

If $\mathfrak{p}|p$ where p is a prime of $\mathbb{N}$, then $N(\mathfrak{p}) = p$ if p is split or ramified and $N(\mathfrak{p}) = p^2$ if p is inert. If p splits in K there are 2 prime ideals $\mathfrak{p}$ lying above p, and otherwise there is just 1. So we can rewrite

$$\begin{aligned}
\zeta_K(s) &= \prod_{p \text{ ramified}} \frac{1}{1-p^{-s}} \prod_{p \text{ split}} \left(\frac{1}{1-p^{-s}}\right)^2 \prod_{p \text{ inert}} \frac{1}{1-p^{-2s}} \\
&= \prod_{p \text{ ramified}} \frac{1}{1-p^{-s}} \prod_{p \text{ split}} \left(\frac{1}{1-p^{-s}}\right)^2 \prod_{p \text{ inert}} \left(\frac{1}{1-p^{-s}}\right)\left(\frac{1}{1+p^{-s}}\right) \\
&= \prod_{p} \frac{1}{1-p^{-}s} \prod_{p \text{ split}} \frac{1}{1-p^{-s}} \prod_{p \text{ inert}} \frac{1}{1+p^{-s}} \\
&= \zeta(s) \prod_{p \text{ split}} \frac{1}{1-p^{-s}} \prod_{p \text{ inert}} \frac{1}{1+p^{-s}}.
\end{aligned}$$

Note that the two products on the right, look like one of Dirichlet's L-functions. In fact, we know p splits in K if and only if $\left(\frac{\Delta}{p}\right) = 1$, and p is inert in K if and only if $\left(\frac{\Delta}{p}\right) = -1$. Hence if we extend the Kronecker symbol $\left(\frac{\Delta}{p}\right)$ to a function from $\mathbb{Z} \to \mathbb{C}$ by

$$\chi_\Delta(n) = \begin{cases} 0 & \gcd(n, \Delta) > 1 \\ \left(\frac{\Delta}{p_1}\right)^{e_1}\left(\frac{\Delta}{p_2}\right)^{e_2} \cdots \left(\frac{\Delta}{p_k}\right)^{e_k} & n > 0, n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k} \text{ and } \gcd(n, \Delta) = 1 \\ \chi_\Delta(-n)\chi_\Delta(|\Delta| - 1) & n < 0. \end{cases}$$

One easily checks that χ_Δ is a totally multiplicative function on $\mathbb{Z}$ which depends only upon congruences classes mod Δ. Restricting to $(\mathbb{Z}/\Delta\mathbb{Z})^\times$ gives only nonzero values, so we get a (group) character of $(\mathbb{Z}/\Delta\mathbb{Z})^\times$. In other words, χ_Δ is a Dirichlet character mod Δ, and one has (for $s > 1$)

$$L(s, \chi_\Delta) = \prod_{\chi_\Delta(p) = \left(\frac{\Delta}{p}\right) = 0} 1 \cdot \prod_{\chi_\Delta(p) = \left(\frac{\Delta}{p}\right) = 1} \frac{1}{1-p^{-s}} \cdot \prod_{\chi_\Delta(p) = \left(\frac{\Delta}{p}\right) = -1} \frac{1}{1+p^{-s}}.$$

In other words, we have shown

Lemma 3.4.1. *For $s > 1$,*

$$\zeta_K(s) = \zeta(s) L(s, \chi_\Delta).$$

Theorem 3.4.2. (Dirichlet's class number formula for imaginary quadratic fields) *Let $K = \mathbb{Q}(\sqrt{d})$ where $d < 0$ is squarefree. Then*

$$L(1, \chi_\Delta) = \lim_{s \to 1} \frac{\zeta_K(s)}{\zeta(s)} = \frac{2\pi h_K}{w\sqrt{-\Delta}},$$

where w is the number of roots of unity in $\mathcal{O}_K$, i.e., $w = 6$ if $d = -3$, $w = 4$ if $d = -1$ and $w = 2$ otherwise.

Theorem 3.4.3. (Dirichlet's class number formula for real quadratic fields) *Let $K = \mathbb{Q}(\sqrt{d})$ where $d > 1$ is squarefree. Then*

$$L(1, \chi_\Delta) = \lim_{s \to 1} \frac{\zeta_K(s)}{\zeta(s)} = \frac{2 \log \eta \, h_K}{\sqrt{\Delta}},$$

where η is the fundamental unit in $\mathcal{O}_K$.

(For us, the fundamental unit η of $\mathcal{O}_K$ where K is real quadratic is the unique unit $\eta > 1$ such that any unit of $\mathcal{O}_K$ is of the form $\pm\eta^m$ for some $m \in \mathbb{Z}$.)

The quantity $\lim_{s \to 1} \frac{\zeta_K(s)}{\zeta(s)}$ is called the *residue of* $\zeta_K(s)$ at $s = 1$. The idea is that while $\zeta_K(s)$ and $\zeta(s)$ both have a simple pole at $s = 1$*, these poles should cancel in the quotient to give us a finite number that tells us about the arithmetic of K. Indeed, the quotient $\zeta_K(s)/\zeta(s) = L(1, \chi_\Delta)$ is (or can be continued to) a well-defined continuous function at $s = 1$.

Example 3.4.4. *Let $\Delta = -4$. The quadratic field of discriminant $\Delta = -4$ is $K = \mathbb{Q}(i)$, and Dirichlet's class number formula says*

$$L(1, \chi_{-4}) = \frac{2\pi h_K}{4\sqrt{4}} = \frac{\pi h_K}{4}.$$

But we saw last section, that

$$L(1, \chi_{-4}) = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \cdots = \frac{\pi}{4},$$

hence the class number formula provides another proof that $h_K = 1$. Or if one wishes to approach things from the opposite direction, we see that the fact that $h_K = 1$ (which we proved in two other ways before: by showing $\mathbb{Z}[i]$ is a Euclidean domain and by using Minkowski's bound) implies Leibnitz's formula for $\pi = 4(1 - 1/3 + 1/5 - \cdots)$.

Exercise 3.7. *Using the fact that $\mathbb{Q}(\sqrt{-3})$ has class number 1, determine value of the series*

$$1 - \frac{1}{2} + \frac{1}{4} - \frac{1}{5} + \frac{1}{7} - \frac{1}{8} + \cdots$$

from the class number formula.

Exercise 3.8. *Analogous to the previous exercise, explicate the class number formula in the cases $\mathbb{Q}(\sqrt{-5})$ and $\mathbb{Q}(\sqrt{2})$. (I.e., write down explicitly what the series $L(1, \chi_\Delta)$ is and determine its value from the class number formula.)*

Now you may think above exercises, while interesting, are sort of the opposite of what we want. Instead of using h_K to determine $L(1, \chi_\Delta)$, we would prefer to use $L(1, \chi_\Delta)$ to determine the class number, as we gave an alternate proof for $h_{\mathbb{Q}(i)} = 1$ in the example above. Thus we will need some way of evaluating the series $L(1, \chi_\Delta) = \sum_{n \geq 1} \frac{\chi_\Delta(n)}{n}$ (which converges conditionally).

In fact, one can write down a finite expression for $L(1, \chi_\Delta)$ to actually compute class numbers and we will discuss this later. First we want to prove the class number formula. This immediately implies $L(1, \chi_\Delta) \neq 0$ for any Δ. From this one can deduce that $L(1, \chi) \neq 0$ for any Dirichlet character χ, which will complete the proof of Dirichlet's theorem on primes in arithmetic progressions.

The proof of the class number formula relies on simple geometric lattice point counting problems.

*This means that they go to infinity at the "same rate" as $\frac{1}{1-s}$.

Lemma 3.4.5. (Gauss) *Suppose A, B, C are integers with $B^2 - 4AC < 0$. The number $\lambda(T)$ of lattice points (points in $\mathbb{Z}^2$) contained in the solid ellipse*

$$Ax^2 + Bxy + Cy^2 \leq T$$

satisfies

$$\lambda(T) = \frac{2\pi T}{\sqrt{4AC - B^2}} + O(\sqrt{T})$$

Recall the big-O notation means the following: for $f, g : \mathbb{R} \to \mathbb{R}$, we say

$$f(x) = O(g(x))$$

if $|f(x)| \leq cg(x)$ for all $x > X$ where X and c are some constants. Another way to say this is that $f(x) = O(g(x))$ means $\limsup_{x\to\infty} \frac{|f(x)|}{g(x)} < \infty$ (assuming g is positive).

Proof. First we observe the area of the ellipse is $\frac{2\pi T}{\sqrt{4AC-B^2}}$. To see this, note that there is a change of variables

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$$

for some θ such that $Ax^2+Bxy+Cy^2 = A'x'^2+C'y'^2$ for some A', C'. (In other words, we just rotate the ellipse so its major and minor axes are on the x' and y' axes.) However since the determinant of this transformation (a rotation matrix) is 1, the determinant B^2-4AC of the form $Ax^2+Bxy+Cy^2$ equals the determinant $-4A'C'$ of the form $A'x'^2 + C'y'^2$. (Just check this explicitly.) Since the major and minor axes of the ellipse must have length $2\sqrt{T/A'}$ and $2\sqrt{T/B'}$, we know the area of the ellipse is $A(T) = \frac{\pi T}{\sqrt{A'C'}} = \frac{2\pi T}{\sqrt{4AC-B^2}}$.

Now we can tile $\mathbb{R}^2$ with squares, with each square having area one and centered about some lattice point $(x, y) \in \mathbb{Z}^2$. Let $m(T)$ be the number of squares completely contained in our ellipse $Ax^2 + Bxy + Cy^2 \leq T$ and $M(T)$ be the smallest number of squares which completely contain the ellipse. Since $\lambda(T)$ is the number of squares whose center is contained in the ellipse, we clearly have

$$m(T) \leq \lambda(T) \leq M(T).$$

The point is that $m(T)$ and $M(T)$ are both roughly the area $A(T)$ of the ellipse. Precisely, let $n(T)$ denote the number of squares which intersect the boundary $Ax^2 + Bxy + Cy^2 = T$ of the ellipse. Note that $m(T) \geq A(T) - n(T)$ and $M(T) \leq A(T) + n(T)$. (Draw a picture.) Thus

$$A(T) - n(T) \leq \lambda(T) \leq A(T) + n(T)$$

for all n. So it suffices to show that

$$n(T) = O(\sqrt{T}).$$

Interchanging x and y if necessary, we may assume that $A \leq C$, so the ellipse is wider in the x-direction than it is tall in the y-direction. Then $n(T) \leq 8 + 8\sqrt{T/A} = O(\sqrt{T})$ by the exercise below. □

Exercise 3.9. *Show there are 4 points of slope ± 1 on the ellipse $Ax^2+Bxy+Cy^2 = T$ with $A \leq C$. This breaks the ellipse up into 4 arcs. Show each arc intersects at most $2 + 2\sqrt{T/A}$ squares in the tiling above by considering projections onto the x- and y- axes.*

To put the proof in simpler terms, the number of lattice points in an ellipse is essentially the area of the ellipse, with some error term which is essentially determined by the arclength. If the area increases like T, then the arclength will increase like $\sqrt{T}$, hence the $O(\sqrt{T})$ bound on the error.

Let $F(T)$ denote the number of (nonzero) ideals $\mathcal{I}$ of $\mathcal{O}_K$ with norm $N(\mathcal{I}) \leq T$. We know $F(T)$ is finite for any T.

Lemma 3.4.6. *We have*

$$F(T) = \kappa h_K T + O(\sqrt{T})$$

where

$$\kappa = \begin{cases} \frac{2\pi}{w\sqrt{-\Delta}} & \Delta < 0 \\ \frac{2\log \eta}{\sqrt{\Delta}} & \Delta > 0, \end{cases}$$

using the notation above.

The number κ is called Dirichlet's structure constant. So in this notation Dirichlet's class number formula reads (in both cases) $L(1, \chi_\Delta) = \kappa h_K$.

Proof. For a nonzero ideal $\mathcal{I}$ of $\mathcal{O}_K$, set $G(\mathcal{I}, T) = \{(\alpha) \subseteq \mathcal{I} : 0 < |N(\alpha)| \leq T\}$, i.e., $G(\mathcal{I}, T)$ is the number of principal ideals contained in $\mathcal{I}$ of (absolute) norm at most T. Suppose $\mathcal{J}$ is an ideal of $\mathcal{O}_K$ equivalent to $\mathcal{I}^{-1}$. Then $\mathcal{I}\mathcal{J} = (\alpha)$ is a principal ideal contained in $\mathcal{I}$. Conversely, any principal ideal $(\alpha) \subseteq \mathcal{I}$ is of this form $\alpha = \mathcal{I}\mathcal{J}$ for $\mathcal{J} \sim \mathcal{I}^{-1}$ and we have

$$N(\mathcal{J}) \leq T \iff |N(\alpha)| = N(\mathcal{J}\mathcal{I}) \leq TN(\mathcal{I}).$$

Hence $G(\mathcal{I}, TN(\mathcal{I}))$ is the number of ideals of norm $\leq T$ which are equivalent to $\mathcal{I}^{-1}$. Thus we may write

$$F(T) = G(\mathcal{I}_1, TN(\mathcal{I}_1)) + G(\mathcal{I}_2, TN(\mathcal{I}_2)) + \cdots + G(\mathcal{I}_h, TN(\mathcal{I}_h))$$

where $\mathcal{I}_1, \ldots, \mathcal{I}_h$ are a set of ideal representatives for the class group $\mathcal{C}l_K$. Consequently, the lemma follows if we can show

$$G(I, TN(\mathcal{I})) = \kappa T + O(\sqrt{T})$$

for any ideal $\mathcal{I}$ of $\mathcal{O}_K$.

Suppose $\Delta < 0$. Let β_1, β_2 be a $\mathbb{Z}$-basis for $\mathcal{I}$. Write $\alpha = \beta_1 x + \beta_2 y$. Then

$$N(\alpha) = \alpha\overline{\alpha} = Ax^2 + Bxy + Cy^2,$$

where $A = N(\beta_1)$, $B = Tr(\beta_1\overline{\beta}_2)$ and $C = N(\beta_2)$. Hence the number of α with norm $\leq TN(\mathcal{I})$ is the number of lattice points (points of $\mathbb{Z}^2$) contained inside the solid ellipse $Ax^2 + Bxy + Cy^2 \leq TN(\mathcal{I})$. Note α and α' generate the same principal ideal if and only if they differ by units. Hence $G(\mathcal{I}, TN(\mathcal{I}))$ is $\frac{1}{w}$ times the number of nonzero lattice points inside the ellipse $Ax^2 + Bxy + Cy^2 \leq TN(\mathcal{I})$. This ellipse has discriminant $B^2 - 4AC = \Delta[\beta_1, \beta_2] = \Delta_K N(\mathcal{I})^2$, so the desired estimate of $G(I, TN(\mathcal{I}))$ follows from Gauss's lemma above.

Suppose $\Delta > 0$. The idea is basically the same. If β_1, β_2 is a $\mathbb{Z}$-basis for $\mathcal{I}$ and $\alpha = \beta_1 x + \beta_2 y$ then

$$|N(\alpha)| = |Ax^2 + Bxy + Cy^2|$$

where $A = N(\beta_1)$, $B = Tr(\beta_1\overline{\beta}_2)$ and $C = N(\beta_2)$. However there will be infinitely many solutions to $|N(\alpha)| \leq TN(\mathcal{I})$ owing to the infinitude of units. But there is a one-to-one correspondence of

elements $\alpha \in \mathcal{I}$ satisfying $1 \leq |\alpha/\overline{\alpha}| < \eta^2$, $\alpha > 0$ and principal subideals (α) of $\mathcal{I}$. Hence we may write $G(\mathcal{I}, TN(\mathcal{I}))$ as the number of nonzero solutions to the following system of equations:

$$-T \leq Ax^2 + Bxy + Cy^2 \leq T,$$
$$1 \leq |\frac{\beta_1 x + \beta_2 y}{\overline{\beta}_1 x + \overline{\beta}_2 y}| < \eta^2,$$
$$\beta_1 x + \beta_2 y > 0.$$

Since the discriminant $B^2 - 4AC$ of the quadratic form $Ax^2 + Bxy + Cy^2$ is positive, one gets not an ellipse but a hyperbolic region from the first equation. The latter two equations leave us with two finite hyperbolic sectors to count lattice points in. By setting up an appropriate integral one can show the area is $\frac{2 \log \eta T}{\sqrt{\Delta}}$. For more details, see [Cohn]. □

Now we can prove the class number formula.

Proof. We want to show $L(s, \chi_\Delta) = \kappa h_K$. Recall we can write $\zeta_K(s) = \sum \frac{a_n}{n^s}$ where a_n is the number of ideals of norm n. Hence

$$\begin{aligned}
\zeta_K(s) &= \frac{F(1)}{1^s} + \frac{F(2) - F(1)}{2^s} + \frac{F(3) - F(2)}{3^s} + \cdots \\
&= F(1)\left(\frac{1}{1^s} - \frac{1}{2^s}\right) + F(2)\left(\frac{1}{2^s} - \frac{1}{3^s}\right) + \cdots \\
&= \sum_{T=1}^{\infty} F(T)\left\{\frac{1}{T^s} - \frac{1}{(T+1)^s}\right\}.
\end{aligned}$$

For a fixed T, we have

$$\begin{aligned}
\frac{1}{T^s} - \frac{1}{(T+1)^s} &= \frac{1}{T^s}\left\{1 - \left(\frac{T}{T+1}\right)^s\right\} \\
&= \frac{1}{T^s}\left\{1 - \left(1 + \frac{1}{T}\right)^{-s}\right\} \\
&= \frac{1}{T^s}\left\{1 - \left(1 - \frac{s}{T} + \frac{s(s+1)}{2!T^2} - \frac{s(s+1)(s+2)}{3!T^3} + \cdots\right)\right\} \\
&= \frac{s}{T^{s+1}} + \epsilon(T, s).
\end{aligned}$$

The third line follows from the Taylor expansion of $(1+x)^{-s}$ about $x = 0$, and the $\epsilon(T, s)$ is an error term satisfying $|\epsilon(T, s)| < C\frac{s^2}{T^{s+2}}$ for some constant C from Taylor's theorem with remainder. Hence

$$\zeta_K(s) = \left(s \sum_{T=1}^{\infty} \cdot \frac{F(T)}{T^{s+1}} + \sum_{T=1}^{\infty} F(T)\epsilon(T, s)\right).$$

Bear in mind that we will want to take the limit as $s \to 1^+$. By the above lemma, we know $F(T) \leq C_1 T$ for some C_1. So for s in the range $1 < s < 2$, we have

$$\sum_{T=1}^{\infty} F(T)|\epsilon(T, s)| \leq CC_1 s^2 T \sum_{T=1}^{\infty} \frac{1}{T^{s+2}} \leq 4C \sum_{n=1}^{\infty} \frac{1}{n^2} = 4C\zeta(2) < \infty.$$

Thus we may write

$$\zeta_K(s) = s\sum_{T=1}^{\infty} \frac{F(T)}{T^{s+1}} + \text{f.e.}$$

where f.e. (finite error) represents an error term which remains finite as $s \to 1^+$. Again using the lemma above, we have

$$\zeta_K(s) = s\kappa h_k \underbrace{\sum_{T=1}^{\infty} \frac{1}{T^s}}\, \zeta(s) + \epsilon_2(T) s \sum_{T=1}^{\infty} \frac{1}{T^{s+1}} + \text{f.e.},$$

where $\epsilon_2(T)$ is an error term satisfying $|\epsilon_2(T)| \leq C_2\sqrt{T}$ for some constant C_2. Then the middle term satisfies

$$|\epsilon_2(T)| s \sum_{T=1}^{\infty} \frac{1}{T^{s+1}} \leq 2C_2 \sum_{T=1}^{\infty} \frac{1}{T^{s+\frac{1}{2}}} \leq 2C_2\zeta(s+\frac{1}{2}) \leq 2C_2\zeta(\frac{3}{2}) < \infty$$

for $1 < s < 2$. So we may write

$$\zeta_K(s) = s\kappa h_k \zeta(s) + \text{f.e.}$$

Dividing both sides by $\zeta(s)$ and sending $s \to 1^+$ gives the class number formula. □

Proposition 3.4.7. *Let χ be a nontrivial Dirichlet character mod m. Then $0 < |L(1,\chi)| < \infty$.*

This result completes the proof of Dirichlet's theorem on primes in arithmetic progressions.

Proof. If χ is nontrivial, one can show the series $\sum \frac{\chi(n)}{n}$ for $L(1,\chi)$ converges conditionally as one shows the alternating harmonic series converges in calculus. One shows that the series $L(s,\chi) = \sum \frac{\chi(n)}{n^s}$ converges uniformly for $s \geq 1$ so that $\sum \frac{\chi(n)}{n}$ actually equals $\lim_{s\to 1} L(s,\chi)$. The details are standard analysis and we will omit them. It remains to show $L(1,\chi) \neq 0$.

First suppose χ is a *real character*, i.e., the image of χ is contained in $\mathbb{R}$. In particular, χ can only take on the values ± 1 and 0. We claim that $\chi(n) = \chi_\Delta(n)$ for some discriminant Δ of a quadratic field K.

Recall that $(\mathbb{Z}/m\mathbb{Z})^\times = \prod(\mathbb{Z}/p_i^{e_i}\mathbb{Z})^\times$ where $m = \prod p_i^{e_i}$ by the Chinese Remainder Theorem. This means any Dirichlet character mod m is just a product of Dirichlet characters mod $p_i^{e_i}$. Hence it suffices to prove the claim when $m = p^e$ for some prime p. Assume p is odd. (The case $p = 2$ is an exercise below.) In this case $(\mathbb{Z}/m\mathbb{Z})^\times$ is cyclic.

Let ξ be the restriction of χ to $G = (\mathbb{Z}/m\mathbb{Z})^\times$, i.e., ξ is the group character of $G = (\mathbb{Z}/m\mathbb{Z})^\times$ which gives rise to the Dirichlet character $\chi : \mathbb{Z} \to \mathbb{R}$. Note that ξ only takes on values ± 1 so $\xi^2 = 1$. If ξ is trivial, then so is χ, contrary to our assumption. Hence ξ must be an element of order 2 in $\hat{G}$. (ξ is called a quadratic character.) But $\hat{G} \simeq G$ is cyclic, so there is only 1 element of order 2 in $\hat{G}$. Let $K = \mathbb{Q}(\sqrt{p})$ if $p \equiv 1 \bmod 4$ and $K = \mathbb{Q}(\sqrt{-p})$ if $p \equiv 3 \bmod 4$, so $|\Delta| = p$ where $\Delta = \Delta_K$. Thus $\left(\frac{\Delta}{\cdot}\right)$ defines a quadratic character of $(\mathbb{Z}/p\mathbb{Z})^\times$. Composing this with the natural map from $(\mathbb{Z}/p^e\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times$ (just taking elements mod p) gives a nontrivial quadratic character of $(\mathbb{Z}/p^e\mathbb{Z})^\times$, which must equal ξ since it has order 2 in $\hat{G}$. Hence $\chi_\Delta = \chi$. (χ_Δ is naturally a Dirichlet character mod p, but it may also be regarded as a Dirichlet character mod $m = p^e$.)

This proves the claim that any real Dirichlet character mod m is of the form χ_Δ for some quadratic field discriminant Δ (which will sometimes be positive and sometimes be negative). But the class number formula immediately implies that $L(1,\chi_\Delta) \neq 0$.

Now suppose χ is a *complex character*, i.e., the image of χ is not contained in $\mathbb{R}$. Note the derivative

$$L'(s,\chi) = -\sum_{n=1}^{\infty} \frac{\chi(n)\log n}{n^s}$$

exists and is continuous for $s \geq 1$ (this series converges uniformly). If χ' is a complex Dirichlet character mod m such that $L(s,1) = 0$, then by the mean value theorem for any $s > 1$ there is a $1 < s_0 < s$ such that,

$$L(s,\chi') = L(s,\chi') - L(1,\chi') = L'(s_0,\chi')(s-1).$$

Similarly we have $L(s,\overline{\chi}') = L'(s_0,\overline{\chi}')(s-1)$ where $\overline{\chi}'$ is the complex conjugate of χ' (which is easily seen to also be a Dirichlet character mod m). This means that $L(s,\chi')$ and $L(s,\overline{\chi}')$ go to 0 at least as fast as $s-1$ as $s \to 1$ (faster if $L'(s_0,\chi')$ also goes to 0).

From (3.7) with $a = 1$, we have

$$\sum_{\chi} \log L(s,\chi) = \phi(m) \sum_{p \equiv 1 \bmod m} \frac{1}{p^s} + \text{f.e.}$$

where χ runs over all Dirichlet characters mod m and f.e. represents an error term which remains finite as $s \to 1$. As $s \to 1$, both $\log L(s,\chi')$ and $\log L(s,\overline{\chi}')$ approach $-\infty$ at least as fast as $\log(s-1)$. But there is only one term on the left, $\log L(s,\chi_0)$ where χ_0 is the trivial Dirichlet character mod m, which goes to ∞. It goes to ∞ at the same rate as $\log \zeta(s)$, which is $-\log(s-1)$. Hence the left hand side of the above equation goes to $-\infty$, but the right hand side stays positive (in fact goes to $+\infty$), a contradiction. □

Exercise 3.10. *Suppose χ is a real Dirichlet character mod $m = 2^e$. Using the fact that $(\mathbb{Z}/m\mathbb{Z})^\times \simeq C_2 \times C_{2^{e-2}}$ for $e > 1$, show $\chi = \chi_\Delta$ for Δ the discriminant of some quadratic field.*

Exercise 3.11. *Determine all* real *nontrivial Dirichlet characters mod m for $m = 3, 5, 6, 9, 15$. For each of these characters χ determine a quadratic field discriminant Δ such that $\chi = \chi_\Delta$. For which χ we can choose a $\Delta > 0$ so that $\chi = \chi_\Delta$ and when we can choose a $\Delta < 0$?*

In the proof for real characters, we used a Dirichlet character mod p to get a Dirichlet character mod p^e.

Exercise 3.12. *If χ is a Dirichlet character mod m, is it a Dirichlet character mod mn for any n?*

We have now seen how to prove the class number formula (omitting some details in the real quadratic case), and how one can use this to prove Dirichlet's theorem on arithmetic progressions. Of course, the natural thing to try to use this formula for is computing class numbers. Dirichlet could do this by obtaining a finite expression for $L(1,\chi)$ using *Gauss sums*.

Let χ be a Dirichlet character mod m. We say χ is **even** if $\chi(-1) = 1$ and χ is **odd** if $\chi(-1) = -1$. By multiplicativity, these conditions are equivalent to the conditions $\chi(-n) = \chi(n)$ and $\chi(-n) = -\chi(n)$, respectively, justifying the terminology of even and odd. For $k \in \mathbb{N} \cup \{0\}$, define the k-th **Gauss sum** associated to χ to be

$$\tau_k(\chi) = \sum_{a \in (\mathbb{Z}/m\mathbb{Z})^\times} \chi(a) e^{2\pi i a k/m}.$$

From the definition, notice that the Gauss sums are something like "Fourier coefficients" for χ.

We will assume that χ is **primitive**, which means that χ is nontrivial and (regarded as a character of $(\mathbb{Z}/m\mathbb{Z})^\times$) it does not come from a character of $(\mathbb{Z}/d\mathbb{Z})^\times$ for any proper divisor d of m. (If $d|m$, then any character of $(\mathbb{Z}/d\mathbb{Z})^\times$ gives a character of $(\mathbb{Z}/m\mathbb{Z})^\times$ just by composition with the mod d map $(\mathbb{Z}/m\mathbb{Z})^\times \to (\mathbb{Z}/d\mathbb{Z})^\times$.)

Exercise 3.13. *Determine which Dirichlet characters mod m are primitive for $m = 4, 8, 15$. Find a formula for the number of primitive Dirichlet characters mod m for any $m \in \mathbb{N}$.*

Proposition 3.4.8. *Let χ be a primitive character mod m. Then*

$$L(1,\chi) = \begin{cases} \frac{\pi i \tau_1(\chi)}{m^2} \sum_{k \in (\mathbb{Z}/m\mathbb{Z})^\times} \chi^{-1}(k) k & \chi \text{ odd} \\ -\frac{\tau_1(\chi)}{m} \sum_{k \in (\mathbb{Z}/m\mathbb{Z})^\times} \chi^{-1}(k) \log \sin \frac{k\pi}{m} & \chi \text{ even.} \end{cases}$$

Proof. For $s > 1$, the absolute convergence of the L-series for $L(s,\chi)$ implies we can write

$$L(s,\chi) = \sum_{a \in (\mathbb{Z}/m\mathbb{Z})^\times} \left\{ \chi(a) \sum_{n \in m\mathbb{N}+a} \frac{1}{n^s} \right\}.$$

Note the characters for the additive group $(\mathbb{Z}/m\mathbb{Z})$ are just given by $\omega_k(a) = e^{2\pi i a k/m}$ for $0 \le k \le m-1$. Hence the character orthogonality relations, namely that

$$\sum_{k=0}^{m-1} \omega_k(a) \omega_k^{-1}(n) = \begin{cases} m & a \equiv n \bmod m \\ 0 & \text{else,} \end{cases}$$

tell us we can rewrite the inner sum above as

$$\frac{1}{m} \sum_{n=1}^{\infty} \frac{\sum_{k=0}^{m-1} \omega_k(a) \omega_k^{-1}(n)}{n^s} = \frac{1}{m} \sum_{n=1}^{\infty} \frac{\sum_{k=0}^{m-1} e^{2\pi i (a-n)k/m}}{n^s}.$$

Plugging this in to our first equation gives

$$L(s,\chi) = \frac{1}{m} \sum_{k=0}^{m-1} \left\{ \tau_k(\chi) \sum_{n=1}^{\infty} \frac{\omega^{-nk}}{n^s} \right\},$$

for $s > 1$, where $\omega = e^{2\pi i/m}$. It is easy to see the Dirichlet series $\sum_{n=1}^{\infty} \frac{\omega^{-nk}}{n^s}$ converges for $s > 1$, and as $s \to 1^+$, one can check it approaches $-\log(1-\omega^{-k})$. (Plugging in $s = 1$ gives the Taylor expansion for $-\log(1-z)$ evaluated at $z = \omega^{-k}$.) This gives

$$L(1,\chi) = -\frac{1}{m} \sum_{k=1}^{m-1} \tau_k(\chi) \log(1-\omega^{-k}).$$

(Up to here, we do not need that χ is primitive, just nontrivial.)

We again use some simple character theory to obtain that

$$\tau_k(\chi) = \begin{cases} \chi^{-1}(k) \tau_1(\chi) & \gcd(k,m) = 1 \\ 0 & \gcd(k,m) > 1. \end{cases}$$

Then

$$L(1,\chi) = -\frac{\tau_1(\chi)}{m} \sum_{k \in (\mathbb{Z}/m\mathbb{Z})^\times} \chi^{-1}(k) \log(1-\omega^{-k}).$$

We can replace k with $-k$ in the sum and pull out a $\chi(-1)$ to get

$$L(1,\chi) = -\frac{\chi(-1)\tau_1(\chi)}{m} \sum_{k \in (\mathbb{Z}/m\mathbb{Z})^\times} \chi^{-1}(k) \log(1-\omega^{k}).$$

Using the fact that

$$\log(1-\omega^k) = \log 2 + \log \sin \frac{k\pi}{m} + \left(\frac{k}{m} - \frac{1}{2}\right)\pi i$$

one can write

$$L(1,\chi) = -\frac{\chi(-1)\tau_1(\chi)}{m} \sum_{k \in (\mathbb{Z}/m\mathbb{Z})^\times} \chi^{-1}(k) \left(\log \sin \frac{k\pi}{m} + \frac{k\pi i}{m}\right).$$

Note that the $\log 2$ terms drop out since $\sum_k \chi^{-1}(k) = 0$ by orthogonality relations. One finishes the proof by checking that $\sum_k \chi^{-1}(k) \log \sin \frac{k\pi}{m} = 0$ if χ is odd and $\sum_k \chi^{-1}(k)k = 0$ if χ is even. □

This immediately gives a more useable version of Dirichlet's class number formula. Though the version we give below comes from one additional simplification—namely, since $h_K > 0$, we only need a formula for the absolute value $|L(1,\chi)|$ to compute h_K. By taking absolute values in the above proposition, one can get rid of the Gauss sum (which has absolute value $\sqrt{m}$). We omit the details of the complete simplification, but in the end, one has the following.

Theorem 3.4.9. (Dirichlet's class number formula, second form) *Let $K = \mathbb{Q}(\sqrt{d})$ be the quadratic field of discriminant Δ. Then*

$$h_K = \begin{cases} \frac{1}{2-\chi_\Delta(2)} \left| \sum_{1 \le k < |\Delta|/2} \chi_\Delta(k) \right| & \Delta < 0, \Delta \neq -3, -4 \\ \frac{1}{\log \eta} \left| \sum_{1 \le k < \Delta/2} \chi_\Delta(k) \log \sin \frac{k\pi}{\Delta} \right| & \Delta > 0. \end{cases}$$

Here η denotes the fundamental unit of $\mathcal{O}_K$ when $\Delta > 0$.

Note with this form of the class number formula, we can effectively compute the class number of any quadratic field, and this is much easier than the approach via Minkowski's bound (though in the real quadratic case one needs to determine the fundamental unit). Additionally, since $\chi_\Delta(n) = 0$ unless $\gcd(n,\Delta) = 1$, we may restrict the above sums to k relatively prime to Δ.

Example 3.4.10. *For $d = -2$, i.e., $K = \mathbb{Q}(\sqrt{-2})$, we see $\Delta = -8$,*

$$\chi_\Delta(n) = \begin{cases} 1 & n \text{ odd} \\ 0 & n \text{ even}, \end{cases}$$

so

$$h_K = \frac{1}{2}|\chi_\Delta(1) + \chi_\Delta(3)| = 1.$$

Exercise 3.14. *Using the second form of the class number formula compute h_K where $K = \mathbb{Q}(\sqrt{d})$ for $d = -5, -6, -7, -10, 2$.*

3.5 Postlude: Beyond Dirichlet

In this chapter we have shown (modulo a few details) two landmark results in number theory:

(i) Dirichlet's theorem on primes in arithmetic progressions
(ii) Dirichlet's class number formula for quadratic fields

both of which used Dirichlet L-functions. Subsequent key developments in number theory, generalizing the above, are

(I) prime density theorems
(II) class number formulas for general number fields.

Let us first discuss the density theorems. Let $\mathcal{P}$ denote the set of primes in $\mathbb{N}$, and $S \subseteq \mathcal{P}$. We say S has **(natural) density**[‡] ρ if

$$\lim_{x\to\infty} \frac{|\{p \in S : p < x\}|}{|\{p \in \mathcal{P} : p < x\}|} = \rho.$$

Of course any finite set of primes will have density 0, but infinite sets of primes can have density 0 also. Using this notion, one can strengthen Dirichlet's theorem on arithmetic progressions to the following:

Theorem 3.5.1. *Let $m > 1$ and $a \in \mathbb{N}$ such that $\gcd(a, m) = 1$. Then the set of primes $\equiv a \bmod m$ has density $\frac{1}{\phi(m)}$.*

In other words, the number of primes $\equiv a \bmod m$ is the same for any $a \in (\mathbb{Z}/m\mathbb{Z})^\times$. Or put another way, the primes are distributed equally among the invertible congruence classes mod m. For example, there are the same number or primes $\equiv 1 \bmod 4$ as there are $\equiv 3 \bmod 4$ (in the sense of density). This is one example of a statistical regularity that prime numbers satisfy, despite their apparent randomness. Proving this requires significantly more sophisticated analysis of Dirichlet L-functions.

Another way to think about distribution of primes is in terms of how they split in extensions K of $\mathbb{Q}$. For example the above statement about the number of primes $\equiv 1 \bmod 4$ being the same as the number of primes $\equiv 3 \bmod 4$ can be recast as saying the number of primes with split in $\mathbb{Q}(i)$ is the same as the number of primes which are inert in $\mathbb{Q}(i)$. In fact the above theorem is essentially equivalent to the following

Theorem 3.5.2. *Let K be a quadratic field. The set of primes in $\mathcal{P}$ which split in K has density $\frac{1}{2}$, as does the set of primes which remain inert in K.*

In other words, half the primes split in K and half remain prime in K, for any quadratic field K. This is a special case of a very strong theorem, called the *Chebotarev density theorem*. This provides much stronger regularity results about distributions of primes than just considering congruence classes. We haven't defined everything we need at this point to state the complete theorem, but here is a (corollary of a) special case.

Theorem 3.5.3. *Let K be a number field of degree n and S be the set of primes in $\mathcal{P}$ which split completely in K. Then S has density $\rho \geq \frac{1}{n}$. Further $\rho = \frac{1}{n}$ if and only if $K/\mathbb{Q}$ is Galois.*

[‡]There is another weaker notion of density, now called Dirichlet density, that coincides with natural density if the natural density exists, which is essentially what Dirichlet originally considered.

A proof of Chebotarev density involves a more general kind of L-function called an Artin L-function. The basic idea is the following. Even though we have several Dirichlet characters mod m for a given m, the most important Dirichlet characters are those of the form χ_Δ where Δ is the discriminant of some quadratic field K.

On the other hand, if we start with some number field K, there is a natural group associated to it, $\mathrm{Gal}(K/\mathbb{Q})$, and so one can look at the irreducible representations ρ of $\mathrm{Gal}(K/\mathbb{Q})$. Artin defined an L-function $L(s,\rho)$ associated to each such Galois representation ρ in order to study how the primes split in $K/\mathbb{Q}$ (or more generally, an arbitrary extension L/K). This L-function has some L-series expansion as well as an Euler product. If ρ is the trivial character of $\mathrm{Gal}(K/\mathbb{Q})$, then $L(s,\rho)$ is essentially $\zeta_K(s)$ (they have the same Euler product expansions except at a finite number of primes).

In the case where K is quadratic, then $\mathrm{Gal}(K/\mathbb{Q})$ has only 2 irreducible representations, both of dimension 1, i.e., both characters. If ρ is the nontrivial character of $\mathrm{Gal}(K/\mathbb{Q})$, then $L(s,\rho) = L(s,\chi_\Delta)$ where $\Delta = \Delta_K$. If ρ_0 is the trivial character, then $L(s,\rho_0) = L(s,\chi_0)$ where χ_0 is the trivial Dirichlet character mod Δ. Hence the Artin L-functions are a generalization of (at least the most important cases of) Dirichlet L-functions. In this quadratic case we have

$$L(s,\rho_0)L(s,\rho) = L(s,\chi_0)L(s,\chi) \simeq \zeta_K(s)L(s,\chi) = \zeta(s),$$

where $\simeq$ means equal up to a finite number of factors in the Euler product.

Similarly in the case of K a general number field, we have

$$\prod_\rho L(s,\rho) \simeq \zeta_K(s) \prod_{\rho \text{ nontrivial}} L(s,\rho) = \zeta(s),$$

where ρ runs over all irreducible representations of $\mathrm{Gal}(K/\mathbb{Q})$. One has the following generalization of Dirichlet's class number formula.

Theorem 3.5.4. (General class number formula) *Let K be a number field and $\{\rho\}$ be the set of irreducible representations of* $\mathrm{Gal}(K/\mathbb{Q})$*. Then*

$$\prod_{\rho \text{ nontrivial}} L(1,\rho) = \lim_{s\to 1^+} \frac{\zeta_K(s)}{\zeta(s)} = \frac{2^{r_1}(2\pi)^{r_2}R}{w\sqrt{|\Delta_K|}}h_K,$$

where r_1 (resp. r_2) is the number of real (resp. complex) embeddings of K, w is the number of roots of unity in K, and R is the regulator *of K.*

The regulator is basically the volume of a certain lattice which comes up in Dirichlet's units theorem. This provides a way to compute and study class numbers for number fields of degree greater than 2. In the case $K = \mathbb{Q}(\zeta_p)$ where ζ_p is a primitive p-th root of unity, the class number formula provides a way to determine which primes are *regular*, i.e., for which p is $\gcd(p, h_K) = 1$. The significance of this is that Kummer was able to prove Fermat's Last Theorem in the case of regular prime exponents.

In fact, Wiles proved Fermat's Last Theorem by (more or less) proving the Taniyama–Shimura Conjecture, which is itself a statement about L-functions. To certain curves (irreducible smooth cubic curves) called *elliptic curves* E one associates an L-function $L(s,E)$. (It can be given by an Euler product where the factor corresponding to the prime p is given by the number of points on E mod p.) On the other hand, one also has L-functions $L(s,f)$ attached to *modular forms* f, which

are certain periodic functions on the upper half plane. (The Euler product factors are given by the p-th Fourier coefficients in a certain Fourier expansion.) The Taniyama–Shimura Conjecture is that every elliptic curve E corresponds to a modular form f in the sense that $L(s, E) = L(s, f)$. (Going from modular forms to elliptic curves is easier, and is known by work of Eichler and Shimura.)

While the whole story is rather involved, let me just say that it is difficult to directly compare elliptic curves and modular forms, but one can associate to both of these objects certain 2-dimensional Galois representations. Thus to prove Taniyama–Shimura, one wants to show the Galois representations coming from elliptic curves are contained in the set of Galois representations coming from modular forms. In a herculian endeavor, Wiles reduced (a sufficient part of) the Taniyama–Shimura conjecture to a theorem of Langlands and Tunnell (also a very difficult result) which tells us every (odd) 2-dimensional complex Galois representation $\rho : \mathrm{Gal}(K/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{C})$ with solvable image corresponds to a modular form.

Let me emphasize 2 points:

1) L-functions provide a practical (though not typically easy) way to compare objects of different types: geometric objects (curves and varieties), algebraic/arithmetic objects (number fields/Galois representations) and analytic objects (modular/automorphic forms).

2) Galois representations and/or automorphic forms/automorphic representations provide a general framework for studying many number theoretic problems. For example, if K is an abelian extension of $\mathbb{Q}$, i.e., $K/\mathbb{Q}$ is Galois with abelian Galois group, then all representations of $\mathrm{Gal}(K/\mathbb{Q})$ are 1-dimensional. Hence the theory of 1-dimensional Galois representations provides a way to study abelian extensions of $\mathbb{Q}$, and contains the case of Dirichlet characters and everything we did in this chapter. The fact that 1-dimensional Galois representations correspond to "1-dimensional" automorphic forms is essentially *class field theory*, which provides a way to understand the abelian extensions of a number field, and is the crowning achievement of classical algebraic number theory.

In this context, we can view the Taniyama-Shimura conjecture as a sort of "2-dimensional" analogue of class field theory. A large amount of present work in modern number theory is studying higher-dimensional analogues of class field theory (often called non-abelian class field theory). In fact, this is essentially the area of research Ralf Schmidt, Ameya Pitale and I specialize in (and it is related to Alan Roche and Tomasz Prezbinda's research as well). For example, in my thesis I proved that certain 4-dimensional Galois representations with solvable image correspond to automorphic forms.

We will give a brief introduction to class field theory and higher-dimensional analogues in Part III.

Part II
The second part

4 Binary Quadratic Forms

A **binary quadratic form** (over $\mathbb{Z}$) is a binary (two variable) polynomial of the form $Q(x,y) = ax^2 + bxy + cy^2$, where $a, b, c \in \mathbb{Z}$. This generalizes the forms $x^2 + ny^2$ that we looked at earlier, and we will see that looking at general binary quadratic forms will help us with the study of the forms $x^2 + ny^2$.

Recall the two main questions about a quadratic form $Q(x,y)$ are:

(1) What numbers n are represented by Q, i.e., when is $n = Q(x,y)$ solvable?

(2) If n is represented by Q, what are the solutions to $n = Q(x,y)$?

Using Gauss's theory of composition of quadratic forms, we will be able to obtain very nice results on these problems, though it is surprisingly difficult to give a complete explicit answer even to the first question for an arbitrary binary quadratic form. It turns out the main obstruction to answering these questions completely is closely related to the class groups of quadratic fields. In light of this, there appears to be no elementary answer to (1) in general, though as we have seen with $x^2 + dy^2$ for $d = 1, 2, 3, 5, 6$, there is in special cases. Nevertheless, the theory one obtains in the end is quite beautiful and powerful.

In regards to the second question, for a given n and Q, it is not hard to answer the question computationally. Further, using Gauss's theory of composition, one can study the structure of the solutions in general. However to explicitly say what the solutions are requires some explicit computations. We will not focus so much on explicit computation, but rather general theory. In particular, we will study the following related question.

(2') What is the number $r_Q(n)$ of solutions to $n = Q(x,y)$?

Note this is somehow weaker, but much more reasonable to ask in general, than (2), and it also contains (1) as a special case. Specifically, (1) just asks for which n is $r_Q(n) > 0$. Modulo some obstruction coming from class groups, Dirichlet proved a beautiful formula for $r_Q(n)$, which (apart from this obstruction) answers (1) and (2') at the same time.

Now you might have wondered if $r_Q(n)$ is always finite. The way we defined it in (2'), it is not: for example $x^2 - 2y^2 = n$ has infinitely many solutions for $n = 1$ because there are infinitely many units in the ring of integer of $\mathbb{Q}(\sqrt{2})$. However, one can still make sense of $r_Q(n)$ by counting solutions "up to units." If one does this, there will always be finitely many (possibly zero) solutions to $x^2 - 2y^2 = n$ for any n.

However, for simplicity of exposition, we will restrict to forms $ax^2 + bxy + cy^2$ whose **discriminant** $b^2 - 4ac < 0$. These will correspond to imaginary quadratic fields and the number of solutions to $ax^2 + bxy + cy^2 = n$ will be finite for any n, so we can get by with our naive definition of $r_Q(n)$.

For the basic theory we will more or less follow a combination of [Cox], [Cohn] and [Buell]. For a nice historical treatment of quadratic forms, see [Scharlau–Opolka]. Much of the material is rather elementary, and in the interest of time, we will often not give complete proofs. Most treatments of binary quadratic forms do not cover Dirichlet's formula for $r_Q(n)$, but [Dirichlet], [Landau] and [Hurwitz] are some sources.

4.1 Reduction theory

Let $Q(x,y) = ax^2 + bxy + cy^2$ be a binary quadratic form ($a, b, c \in \mathbb{Z}$). The **discriminant** of Q is $\Delta = \Delta_Q = b^2 - 4ac$. This is a fundamental invariant of the form Q.

Exercise 4.1. *Show there is a binary quadratic form of discriminant $\Delta \in \mathbb{Z}$ if and only if $\Delta \equiv 0, 1 \bmod 4$. Consequently, any integer $\equiv 0, 1 \bmod 4$ is called a* **discriminant**.

We say two forms $ax^2 + bxy + cy^2$ and $Ax^2 + Bxy + Cy^2$ are **equivalent** if there is an invertible change of variables

$$x' = rx + sy,\ y' = tx + uy,\ r, s, t, u \in \mathbb{Z}$$

such that

$$a(x')^2 + bx'y' + c(y')^2 = Ax^2 + Bxy + Cy^2.$$

Note that the change of variables being invertible means the matrix

$$\begin{pmatrix} r & s \\ t & u \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}).$$

In fact, in terms of matrices, we can write the above change of variables as

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} r & s \\ t & u \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}.$$

Going further, observe that

$$\begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = ax^2 + bxy + cy^2,$$

so we can think of the quadratic form $ax^2 + bxy + cy^2$ as being the symmetric matrix $\begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}$. It is easy to see that two quadratic forms $ax^2 + bxy + cy^2$ and $Ax^2 + Bxy + Cy^2$ are equivalent if and only if

$$\begin{pmatrix} A & B/2 \\ B/2 & C \end{pmatrix} = \tau^T \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} \tau \tag{4.1}$$

for some $\tau \in \mathrm{GL}_2(\mathbb{Z})$.

Note that the discriminant of $ax^2 + bxy + cy^2$ is $-4\mathrm{disc}\begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}$.

Lemma 4.1.1. *Two equivalent forms have the same discriminant.*

Proof. Just take the matrix discriminant of Equation (4.1) and use the fact that any element of $\mathrm{GL}_2(\mathbb{Z})$ has discriminant ± 1. □

What this means then is that $\mathrm{GL}_2(\mathbb{Z})$ acts on the space $\mathcal{F}_\Delta$ of binary quadratic forms of discriminant Δ for any Δ. The importance of equivalent forms is in the following.

We say $Q(x,y) \in \mathcal{F}_\Delta$ **represents** an integer n if $Q(x,y) = n$ for some $x, y \in \mathbb{Z}$.

Lemma 4.1.2. *Two equivalent forms represent the same integers.*

Proof. This is obvious from the definition of equivalence—just make the change of variables! □

To prove some basic results, it will be helpful to have more refined notions of equivalence and representations of integers.

Definition 4.1.3. *We say two forms $ax^2+bxy+cy^2$ and $Ax^2+Bxy+Cy^2$ are* **properly equivalent** *if they satisfy Equation (4.1) for some $\tau \in \mathrm{SL}_2(\mathbb{Z})$. In this case we will write $ax^2+bxy+cy^2 \sim Ax^2+Bxy+Cy^2$.*

Recall $\mathrm{SL}_2(\mathbb{Z})$ means 2×2 integer matrices of determinant 1, so $\mathrm{GL}_2(\mathbb{Z}) = \mathrm{SL}_2(\mathbb{Z}) \cup \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \mathrm{SL}_2(\mathbb{Z})$ since $\mathrm{GL}_2(\mathbb{Z})$ consists of matrices of determinant ± 1 In other words the quotient $\mathrm{GL}_2(\mathbb{Z})/\mathrm{SL}_2(\mathbb{Z})$ consists of two cosets. We can take $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ as a set of representatives for these cosets.

Clearly proper equivalence implies equivalence but the converse is not true. In fact, the notion of proper equivalence turns out to give a nicer theory as we will see below.*

Example 4.1.4. *Using the matrix $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ we see $ax^2+bxy+cy^2$ is always equivalent to $ax^2-bxy+cy^2$. Sometimes they are properly equivalent (e.g., $2x^2 \pm 2xy + 3y^2$—see exercise below) and sometimes they are not (e.g., $3x^2 \pm 2xy + 5y^2$—see exercise below).*

Exercise 4.2. *Determine the discriminants of $Q_1(x,y) = 2x^2+2xy+3y^2$, $Q_2(x,y) = 2x^2-2xy+3y^2$, $Q_3(x,y) = 3x^2+2xy+5y^2$ and $Q_4(x,y) = 3x^2-2xy+5y^2$. Show Q_1 and Q_2 are properly equivalent but Q_3 and Q_4 are not. (If you have trouble, see the theorem below.)*

Exercise 4.3. *Fix $a,b,c \in \mathbb{Z}$ and let $Q_1(x,y) = ax^2+bxy+cy^2$ and $Q_2(x,y) = cx^2+bxy+ay^2$.*
(i) Show Q_1 and Q_2 are equivalent.
(ii) If $b=0$ show Q_1 and Q_2 are properly equivalent.
(iii) Can you find a,b,c so that Q_1 and Q_2 are equivalent by not properly equivalent? (One often calls this improper equivalence*.)*

There are three types of binary quadratic forms $Q(x,y) = ax^2+bxy+cy^2$ based on the sign of the discriminant $\Delta = b^2-4ac$:

1) If $\Delta = 0$, then Q factors into two linear forms and we say Q is **degenerate**. Otherwise Q is **nondegenerate**. If $\Delta = b^2-4ac = 0$, then $Q(x,y) = (\sqrt{a}x + \sqrt{c}y)^2$ and it is easy to see what numbers Q represents. Hence, one may just consider nondegenerate forms.

2) If $\Delta < 0$, then $Q(x,y)$ has no real roots. In other words, considering x,y real, the graph of $z = Q(x,y)$ in $\mathbb{R}^3$ never crosses the $z=0$ plane. Hence $Q(x,y)$ takes on either only positive values or negative values (and zero if $x=y=0$). Accordingly we say, Q is either a **positive definite** form (e.g., x^2+y^2) or a **negative definite** form (e.g., $-x^2-y^2$). Note positive definite implies $a,c>0$ and negative definite implies $a,c<0$. (This is not if and only if: $x^2-100000xy+y^2$ is not positive definite.) Since $-Q$ will be positive definite whenever Q is negative definite, it suffices to study the positive definite case.

*For this reason, many authors use the term "equivalence of forms" to mean proper equivalence. If you consult other references, take note of this.

3) If $\Delta > 0$, then $Q(x, y)$ has a real root and $Q(x, y)$ takes on positive and negative values for $x, y \in \mathbb{Z}$. In this case, we say Q is an **indefinite** form. Note whenever a and c have different sign (or one is 0), Q must be indefinite. The theory of indefinite forms is similar to the theory of (positive) definite forms, but there are some technical differences which make it more complicated. For simplicity, as well as the fact that positive definite forms tend to be of more interest, we will restrict our study to positive definite forms, though we will make some comments about what happens for indefinite forms along the way.

Hence, **from now on, we assume all our forms are positive definite** (in particular have discriminant $\Delta < 0$) unless otherwise stated.

Definition 4.1.5. *Let $Q(x, y) = ax^2+bxy+cy^2$ be a (positive definite) form. We say Q is* **reduced** *if*

$$|b| \leq a \leq c$$

and $b \geq 0$ if $a = c$ or $a = |b|$.

Lagrange introduced the notion of reduced forms, and the point is the following.

Theorem 4.1.6. *Any (positive definite) form Q is properly equivalent to a unique reduced form.*

Proof. First we will show Q is properly equivalent to a reduced form $ax^2 + bxy + cy^2$. Suppose $|b|$ is minimal such that there is a form $R(x, y) = ax^2 + bxy + cy^2$ with $Q \sim R$. If $|b| > a$, then there exists $m \in \mathbb{Z}$ such that $|2am + b| < |b|$. But this implies

$$R'(x, y) = R(x + my, y) = ax^2 + (2am + b)xy + (am^2 + bm + c)y^2 \sim R(x, y) = ax^2 + bxy + cy^2,$$

so $R' \sim Q$ has smaller xy coefficient than $ax^2 + bxy + cy^2$, contradicting the choice of R. Hence $|b| \leq a$ and similarly $|b| \leq c$. If necessary, we may replace $R(x, y)$ with $R(y, -x) = cx^2 - bxy + ay^2$ to assume $|b| \leq a \leq c$.

We also need to show we can take $b \geq 0$ if $a = c$ or $a = |b|$. If $a = c$, then the xy-coefficient of either $R(x, y)$ or $R(y, -x)$ is nonnegative, so we may assume $b \geq 0$. Similarly if $b = -a$, then $R(x + y, y) = ax^2 + ax + cy^2$, so again we may assume $b \geq 0$ (in fact $b > 0$ since $a > 0$). This shows Q is properly equivalent to some reduced form $R(x, y) = ax^2 + bxy + cy^2$.

Now we show that this R is unique. Suppose not, so $Q \sim S$ where $S = dx^2 + exy + fy^2$ is also reduced. Interchanging R and S if necessary, we may assume $a \geq d$. Recall $R \sim S$ means we can write

$$S(x, y) = R(rx + sy, tx + uy) = a(rx + sy)^2 + b(rx + sy)(tx + uy) + c(tx + uy)^2$$

with $r, s, t, u \in Z$ such that $ru - st = 1$.

Since S clearly represents d and, we know $R \sim S$, we know R represents d. Thus

$$d = ax_0^2 + bx_0y_0 + cy_0^2 \geq a(x_0^2 + y_0^2) + bx_0y_0 \geq a(x_0^2 + y_0^2) - a|x_0y_0| \geq a|x_0y_0|$$

for some $x_0, y_0 \in \mathbb{Z}$. Since $d \leq a$ we must either have $x_0y_0 = 0$ or $|x_0y_0| = 1$. We will finish the proof in three cases.

First suppose $y_0 = 0$. Then $d = ax_0^2$ together with $d \leq a$ means $x_0^2 = 1$ and $d = a$. Then the x^2-coefficient of $S(x, y)$ is

$$ar^2 + brt + ct^2 = R(r, t) = d = a.$$

Observe the minimum nonzero value of a reduced form $R(x,y)$ is obtained precisely when $(x,y) = (\pm 1, 0)$, so we must have $r = \pm 1, t = 0$.[†] (Hence the minimum positive value of a reduced form is the x^2-coefficient, in this case a.) Further $ru - st = ru = 1$ implies $u = r^{-1}$. Then the xy-coefficient of $S(x,y)$ is

$$2ars + bru = 2ars + b = b \pm 2as = e.$$

Since S is reduced, we have $|e| \leq d = a$, but the only was this can happen is if $s = 0$ (which means $R = S$) or if $b = a$ and $s = \pm 1$, which means $e = -d$, which we have excluded from our definition of reduced. This shows uniqueness when $y_0 = 0$.

Next suppose $x_0 = 0$. Similar to the above, we see $d = c$ and looking at the x^2-coefficient of $S(x,y)$ one can conclude $r = 0, s = t = \pm 1$ as the second smallest minimum nonzero value of a reduced form $R(x,y)$ is c and is obtained precisely when $(x,y) = (0, \pm 1)$[§]—see Remark below. This means the xy-coefficient of $S(x,y)$ must be $b + 2cu$. Then $|e| = |b + 2cu| \leq a \leq c$ means either $u = 0$ (so $R = S$) or $b = a = c$ and $u = -1$ in which case $S(x,y) = ax^2 - axy + ay^2$, which is not reduced.

Finally suppose $|x_0 y_0| = 1$. The above inequalities for d say $a \geq d \geq a|x_0 y_0|$ so $a = d$. The rest follows like the $y_0 = 0$ case. □

Remark. It should be fairly obvious that for a reduced form $R(x,y) = ax^2 + bxy + cy^2$ the minimum nonzero value is obtained is a, which happen precisely when $(x,y) = (\pm 1, 0)$ (assuming $a < c$). It may be less clear that the second smallest nonzero value obtained is c, but both of these assertions follow from the simple exercise that $R(x,y) \geq (a - |b| + c)\min(x^2, y^2)$. If you want, you can work this out on your own, but I'm not assigning it as homework.

The above theorem tells us that if we want to study positive definite forms, it suffices to consider reduced forms.

4.2 The mass formula

One of the most important early discoveries about quadratic forms is that they are better studied collectively than individually. Precisely, we make the following

Definition 4.2.1. *Let Δ be a discriminant. The* **form class group** *$\mathcal{C}l(\Delta)$ of discriminant Δ is the set of proper equivalence classes of forms of discriminant Δ, i.e., $\mathcal{C}l(\Delta) = \mathcal{F}_\Delta / \sim$.*

We will later see how to define a group structure on this, justifying the name. From the last section, we know we can take a set of representatives for $\mathcal{C}l(\Delta)$ to be the set of reduced forms of discriminant Δ.

Proposition 4.2.2. *For any discriminant Δ, the number $h(\Delta) := |\mathcal{C}l(\Delta)| < \infty$.*

Proof. Note $h(\Delta)$ is the number of reduced forms of discriminant Δ. If $ax^2 + bxy + cy^2$ is reduced of discriminant Δ, then $|b| \leq a \leq c$ so $4b^2 \leq 4ac = b^2 + \Delta$, i.e., $3b^2 \leq |\Delta|$. In other words, there are only finitely many choices for b. Each choice for b determines ac, and the product ac determines a finite number of choices for a and c. □

[†] If $a = c$, the minimum nonzero value of the form is also obtained at $(0, \pm 1)$, which corresponds to $r = 0, t = \pm 1$. Though we technically omit this case here, we can actually absorb this situation into our argument for the subsequent $x_0 = 0$ case.

[§] Again, technically if $a = c$, this actually gives the minimum nonzero value of the form, but this does not affect our argument.

Using the notion of the class group, we can get a formula for the number of representations of n by a quadratic form of discriminant Δ. It will be convenient to consider proper representations.

Definition 4.2.3. *We say $Q(x,y) \in \mathcal{F}_\Delta$* **properly represents** *n if $n = Q(x,y)$ for some $x, y \in \mathbb{Z}$ with $\gcd(x,y) = 1$. In this case, the solution (x,y) is called a* **proper representation** *of n by Q.*

Example 4.2.4. *Let $Q(x,y) = x^2 + y^2$. Then Q represents $4 = 2^2 + 0^2 = Q(2,0)$, but it does not properly represent 4 since $\gcd(2,0) = 2$ and $(\pm 2, 0)$ and $(0, \pm 2)$ are the only solutions to $Q(x,y) = 4$.*

On the other hand even though 25 has an improper representation *by Q, namely $25 = 5^2 + 0^2 = Q(5,0)$ and $\gcd(5,0) = 5$, 25 also has a* proper representation *by Q: $25 = 3^2 + 4^2 = Q(3,4)$ and $\gcd(3,4) = 1$. Hence we say $Q(x,y)$ properly represents 25.*

Lemma 4.2.5. *$Q(x,y)$ represents n if and only if $Q(x,y)$ properly represents m for some $m|n$ such that $\frac{n}{m}$ is a square.*

Proof. ($\Rightarrow$) Suppose $Q(x,y)$ represents n. If Q properly represents n, we can just take $m = n$ and we are done. If not, then $Q(x,y) = n$ for some x, y with $\gcd(x,y) = d > 1$. Then $Q(x/d, y/d) = Q(x,y)/d^2$ is a proper representation of $m = n/d^2$.

($\Leftarrow$). Suppose $Q(x,y)$ properly represents m where $n = d^2 m$. Then $Q(dx, dy) = d^2 Q(x,y) = d^2 m = n$. □

In other words, understanding what numbers are properly represented by Q tells us which numbers are represented by Q, since the latter numbers are just squares times the former numbers. Let $r_Q(n)$ (resp. $R_Q(n)$) denote the number of proper representations (resp. number of representations) of Q by n.

Theorem 4.2.6. (Dirichlet's mass formula, first version) *Let $d > 1$ be squarefree and set $\Delta = -4d$. Let $Q_1, Q_2, \ldots, Q_h$ be a set of representatives for the form class group $\mathcal{C}l(\Delta)$. Then*

$$r_{Q_1}(n) + r_{Q_2}(n) + \cdots + r_{Q_h}(n) = 2 \prod_{p|n} \left(1 + \left(\frac{\Delta}{p}\right)\right)$$

where p runs over prime divisors of $n > 0$ and $\gcd(n, \Delta) = 1$.

(This statement is from [Cox], but seems to be only be correct when $d \equiv 1 \bmod 4$.)

There are many different versions of the statement of this result, but the above one is the most applicable to the forms $x^2 + dy^2$ (with d squarefree). The proof of the mass formula is quite elementary, and we will omit it now, but John Paul will present a proof of the following version later this semester.

Theorem 4.2.7. (Dirichlet's mass formula, second version) *Let Δ be the discriminant of an imaginary quadratic field, $Q_1, Q_2, \ldots, Q_h$ a set of representatives for $\mathcal{C}l(\Delta)$ and $n > 0$ such that $\gcd(n, \Delta) = 1$. Then*

$$R_{Q_1}(n) + R_{Q_2}(n) + \cdots + R_{Q_h}(n) = w \sum_{k|n} \left(\frac{\Delta}{k}\right),$$

where w is the number of units in the ring of integers of $\mathbb{Q}(\sqrt{\Delta})$.

(Recall $\left(\frac{\Delta}{1}\right) = 1$ for any Δ.)

The first version of the mass formula immediately gives

Corollary 4.2.8. *Suppose $\Delta = -4d$ with $d > 1$ squarefree. Then $n > 0$ relatively prime to Δ is properly represented by some form of discriminant Δ if and only if $\left(\frac{\Delta}{p}\right) = 1$ for all primes $p|n$.*

The point is that while it is difficult to study the numbers represented by an *individual* quadratic form in general, it is relatively easy to understand which numbers are represented by *some* quadratic form of discriminant Δ, for fixed Δ. However, if the class number $h(\Delta) = 1$, then the above formulas are in fact formulas for a specific $r_Q(n)$ (resp. $R_Q(n)$).

Example 4.2.9. *Consider $Q(x, y) = x^2+y^2$. This has discriminant $\Delta = -4$, which is the discriminant of the quadratic field $\mathbb{Q}(i)$. If $ax^2+bxy+cy^2$ is a reduced form of discriminant -4, then $3b^2 \leq 4$ (see proof of Proposition 4.2.2), so $b = 0$ or $b = \pm 1$. Clearly $b = \pm 1$ makes $b^2 - 4ac = 1 - 4ac = -4$ unsolvable, so $b = 0$. Then we must have $ac = 1$ so $a = c = 1$ (since we are just working with positive definite forms). In particular the class number $h(-4) = 1$, and $\{Q\}$ is a set of representatives for $\mathcal{C}l(\Delta)$.*

Then the second version of Dirichlet's mass formula reads

$$R_Q(n) = 4 \sum_{k|n} \left(\frac{\Delta}{k}\right),$$

for n odd. If $n = p$ is prime, then for $p \equiv 1 \bmod 4$ we have

$$R_Q(p) = 4 \left\{ \left(\frac{\Delta}{1}\right) + \left(\frac{\Delta}{p}\right) \right\} = 4(1 + 1) = 8$$

and if $p \equiv 3 \bmod 4$ we have

$$R_Q(p) = 4 \left\{ \left(\frac{\Delta}{1}\right) + \left(\frac{\Delta}{p}\right) \right\} = 4(1 - 1) = 0.$$

In other words, $x^2 + y^2$ represents an odd prime p if and only if $p \equiv 1 \bmod 4$. So Dirichlet's mass formula gives Fermat's two square theorem as a special case.

Moreover, it tells us two more things about $x^2 + y^2$. If $p = x_0^2 + y_0^2$ is odd, then $x_0 \neq y_0$ so $(\pm x_0, \pm y_0)$ and $(\pm y_0, \pm x_0)$ are also solutions to $Q(x, y) = p$. This accounts for 8 solutions. Since $R_Q(p) = 8$, this means up to sign and interchanging x and y, $p = x_0^2 + y_0^2$ is the only way to write p as a sum of 2 squares.

Recall Brahmagupta's composition tells us the product of two numbers of the form $x^2 + y^2$ is again of the form $x^2 + y^2$. Since $2 = 1^2 + 1^2$ and $p^2 = p^2 + 0^2$ for any p, we know that n is of the form $x^2 + y^2$ if any $p|n$ with $p \equiv 3 \bmod 4$ occurs to an even power in the prime factorization of n.

In fact, these are the only n represented by $x^2 + y^2$, and we can actually prove this for n odd using the mass formula. Indeed, suppose n is odd and not of the above form, i.e., there is a prime $p \equiv 3 \bmod 4$ dividing n which occurs to an odd power in the prime factorization of n. Let D_1 be the set of divisors k of n such that p occurs to an even power in the prime factorization of k, and let $D_2 = \{pk : k \in D_1\}$. Then $D_1 \cup D_2$ are the divisors of n and D_1 and D_2 are disjoint. So

$$R_Q(n) = 4 \left\{ \sum_{k \in D_1} \left(\frac{\Delta}{k}\right) + \sum_{pk \in D_2} \left(\frac{\Delta}{pk}\right) \right\} = 4 \sum_{k \in D_1} \left\{ \left(\frac{\Delta}{k}\right) + \left(\frac{\Delta}{p}\right)\left(\frac{\Delta}{k}\right) \right\} = 0$$

since $\left(\frac{\Delta}{p}\right) = -1$.

Exercise 4.4. *Determine the reduced forms of discriminant Δ for $\Delta = -3, -8, -12, -20, -24$. In particular, determine $h(\Delta)$ for these Δ.*

Exercise 4.5. *Use Dirichlet's mass formula and Brahmagupta's composition law to determine to which odd numbers are of the form $x^2 + 2y^2$.*

Exercise 4.6. *Use Dirichlet's mass formula, Brahmagupta's composition law and (i) to determine to which numbers prime to 6 are of the form $x^2 + 3y^2$.*

4.3 The form class group

The idea behind Gauss's composition of binary quadratic forms comes from Brahmagupta composition, which says the product of two numbers of the form $x^2 + dy^2$ is again of the form $x^2 + dy^2$. Precisely, Brahmagupta's composition law is

$$(x_1^2 + dy_1^2)(x_2^2 + dy_2^2) = (x_1x_2 - dy_1y_2)^2 + d(x_1y_2 + x_2y_1)^2 = X^2 + dY^2$$

where $X = x_1x_2 - dy_1y_2$, $Y = x_1y_2 + x_2y_1$. Gauss's composition says that if Q_1 and Q_2 are quadratic forms of discriminant Δ, then there is a form Q_3 of the same discriminant such that

$$Q_1(x_1, y_1)Q_2(x_2, y_2) = Q_3(X, Y)$$

where X, Y are some (homogeneous) quadratic expressions in x_1, y_1, x_2 and y_2. In other words, the product of a number of represented by Q_1 with a number represented by Q_2 is represented by Q_3. We will write this composition as

$$Q_1 \circ Q_2 = Q_3$$

and this will make $\mathcal{C}l(\Delta)$ into a finite abelian group.

However, the explicit determination of X, Y and the coefficients of Q_3 in Gauss's composition is rather complicated and we will not describe it explicitly. Instead, we will approach Gauss composition via ideals. But to get a feeling of how this composition can be done without ideal, we will briefly explain Dirichlet's approach to Gauss composition.

Two forms $Q_1(x, y) = a_1x^2 + b_1xy + c_2y^2$ and $Q_2(x, y) = a_2x^2 + b_2xy + c_2y^2$ of discriminant Δ are called **united** if $\gcd(a_1, a_2, \frac{b_1+b_2}{2}) = 1$. If they are united, there exist $B, C \in \mathbb{Z}$ such that $a_1x^2 + b_1xy + c_2y^2 \sim a_1x^2 + Bxy + a_2Cy^2$ and $a_2x^2 + b_2xy + c_2y^2 \sim a_2x^2 + Bxy + a_1Cy^2$. Then the **Dirichlet composition** is defined to be

$$Q_1 \circ Q_2 = a_1a_2x^2 + Bxy + Cy^2.$$

To see that this follows our notion of what composition should be, observe

$$(a_1x^2 + Bxy + a_2Cy^2)(a_2x^2 + Bxy + a_1Cy^2) = a_1a_2X^2 + BXY + CY^2$$

where $X = x_1x_2 - Cy_1y_2$ and $Y = a_1x_1y_2 + a_2x_2y_1 + By_1y_2$. One can check that the latter form has discriminant Δ. Note that Dirichlet composition does not define composition of any two forms of discriminant Δ (only united forms), but it is enough to define a composition (or multiplication) law on the proper equivalences classes $\mathcal{C}l(\Delta)$.

Now we will present the approach to Gauss's composition via ideals. For simplicity we will work with forms whose discriminant Δ is the discriminant of a quadratic field. We say Δ is a **fundamental discriminant** if $\Delta = \Delta_K$ for some quadratic field K.

Exercise 4.7. *Let Δ be the discriminant of $Q(x,y) = ax^2 + bxy + cy^2$. Show if Δ is a fundamental discriminant, then Q is* **primitive**, *i.e.,* $\gcd(a,b,c) = 1$.

We remark that in working with quadratic forms, one often restricts to primitive forms, since any form is just a multiple of a primitive form.

From now on, for the rest of this section **we assume $\Delta < 0$ is a fundamental discriminant**. Let $K = \mathbb{Q}(\sqrt{\Delta})$ be the imaginary quadratic field of discriminant Δ.

Definition 4.3.1. *Let $\mathcal{I}$ be an ideal of $\mathcal{O}_K$ with ordered $\mathbb{Z}$-basis $\{\alpha, \beta\}$. Then the* **quadratic form associated to $\mathcal{I}$** *is*

$$Q_{\mathcal{I}}(x,y) = N(\alpha x - \beta y)/N(\mathcal{I}) = ax^2 + bxy + cy^2.$$

Here the first norm is the norm of the element $\alpha x + \beta y \in \mathcal{O}_K$, and the second is of course the ideal norm. Explicitly we have

$$N(\alpha x + \beta y) = N(\alpha)x^2 - Tr(\alpha\overline{\beta})xy + N(\beta)y^2$$

so $a = N(\alpha)/N(\mathcal{I})$, $b = -Tr(\alpha\overline{\beta})/N(\mathcal{I})$ and $c = N(\beta)/N(\mathcal{I})$ in the definition above. Technically, the form $Q_{\mathcal{I}}$ depends upon the choice of an ordered $\mathbb{Z}$-basis for $\mathcal{I}$, but it is not too difficult to see that a different basis will lead to a properly equivalent form. Further $Q_{\mathcal{I}}$ has discriminant Δ.

Example 4.3.2. *Let $\Delta = -4$ so $K = \mathbb{Q}(i)$. Consider the ideals $\mathcal{I} = \langle 1, i\rangle = \mathbb{Z}[i]$ and $\mathcal{J} = \langle 1+i, 1-i\rangle = (1+i)$ of $\mathcal{O}_K$. Then*

$$Q_{\mathcal{I}}(x,y) = N(x - iy)/N(\mathcal{I}) = N(x + iy) = x^2 + y^2$$

and

$$Q_{\mathcal{J}}(x,y) = N((1+i)x - (1-i)y)/N(\mathcal{J}) = (2x^2 - Tr(2i) + 2y^2)/2 = x^2 + y^2.$$

So we see different (but equivalent) ideals may lead to the same form.

Exercise 4.8. *Let $\Delta = -20$ so $K = \mathbb{Q}(\sqrt{-5})$ and consider the ideals $\mathcal{I} = \langle 2, 1 + \sqrt{-5}\rangle$ and $\mathcal{J} = \langle 3, 1 + \sqrt{-5}\rangle$. Compute $\mathbb{Q}_{\mathcal{I}}$ and $\mathbb{Q}_{\mathcal{J}}$. Check they have discriminant Δ. Are they properly equivalent?*

Definition 4.3.3. *Let $Q(x,y) = ax^2 + bxy + cy^2$ be a form of discriminant Δ. The* **ideal of $\mathcal{O}_K$ associated to Q** *is*

$$\mathcal{I}_Q = (a, \frac{b - \sqrt{\Delta}}{2}).$$

Lemma 4.3.4. *For any form Q, $Q_{\mathcal{I}_Q} = Q$. In other words, if we take the ideal $\mathcal{I}_Q = (a, \frac{b-\sqrt{\Delta}}{2})$ associated to $Q(x,y) = ax^2 + bxy + cy^2$, then the form $N(ax + \frac{b-\sqrt{\Delta}}{2}y)/N(\mathcal{I}_Q)$ associated to $\mathcal{I}_Q$ equals Q.*

This lemma says the association $\mathcal{I} \mapsto Q_{\mathcal{I}}$ is a right inverse to $Q \mapsto \mathcal{I}_Q$. The proof is elementary. However the converse is not true in general. What we can say is the following

Lemma 4.3.5. *Let $\mathcal{I}$ be an ideal of $\mathcal{O}_K$ and let $Q_{\mathcal{I}}$ be the associated form. If $\mathcal{J} = \mathcal{I}_{Q_{\mathcal{I}}}$ is the ideal associated to $Q_{\mathcal{I}}$, then $\mathcal{J} \sim \mathcal{I}$.*

Then we can *define* multiplication of forms $Q_{\mathcal{I}}$ and $Q_{\mathcal{J}}$ associated to ideals by $Q_{\mathcal{I}} \circ Q_{\mathcal{J}} = Q_{\mathcal{I}\mathcal{J}}$. Upon showing the map $\mathcal{C}l_K \to \mathcal{C}l(\Delta)$ induced by $\mathcal{I} \mapsto Q_{\mathcal{I}}$ is surjective, this defines a multiplication on the form class group $\mathcal{C}l(\Delta)$. Precisely, one gets

Theorem 4.3.6. *We have an isomorphism*

$$\begin{aligned} \mathcal{C}l_K &\simeq \mathcal{C}l(\Delta) \\ \mathcal{I} &\rightarrowtail Q_{\mathcal{I}} \\ \mathcal{I}_Q &\leftarrowtail Q. \end{aligned}$$

Proofs may be found in [Cohn] and [Cox]. The proof are not difficult, but we omit them in the interest of time.

Exercise 4.9. *Show $x^2 + \frac{-\Delta}{4}y^2$ is the identity of $\mathcal{C}l(\Delta)$ if $\Delta \equiv 0 \bmod 4$ and $x^2 - xy + \frac{1-\Delta}{4}y^2$ is the identity of $\mathcal{C}l(\Delta)$ if $\Delta \equiv 1 \bmod 4$.*

Exercise 4.10. *Show $Q_2(x,y) = ax^2 - bxy + cy^2$ is the inverse of $Q_1(x,y) = ax^2 + bxy + cy^2$. We know Q_1 and Q_2 are always equivalent by a transformation of determinant -1, namely $(x,y) \mapsto (x,-y)$. Deduce that $Q_1 \sim Q_2$ if and only if Q_1 has order 2 in $\mathcal{C}l(\Delta_{Q_1})$.*

Exercise 4.11. *We say $Q(x,y) = ax^2 + bxy + cy^2$ is* **ambiguous** *if $a|b$. Show if Q is ambiguous, then Q has order 1 or 2 in $\mathcal{C}l(\Delta_Q)$.*

In fact it can be shown that Q has order ≤ 2 in the form class group if and only if $Q \sim Q'$ for some ambiguous form Q'. In this case, the reduced form in the proper equivalence class of Q is either ambiguous (so $b = a$ or $b = 0$) or of the form $ax^2 + bxy + ay^2$.

Exercise 4.12. *Determine all reduced forms of discriminant $\Delta = -84$. Use this to deduce $\mathbb{Q}(\sqrt{-21})$ has class group isomorphic to $V_4 = C_2 \times C_2$.*

4.4 Genus theory

As in the previous section, let K be an imaginary quadratic field of discriminant Δ. Dirichlet's mass formula tells us which numbers are represented by *some* form in $\mathcal{F}_\Delta$, but it doesn't tell us which numbers are represented by a specific form of discriminant Δ. The problem of distinguishing between forms (or rather equivalence classes of forms) of discriminant Δ is not at all a simple problem in general, however there is a simple approach which gives a complete solution when the class group is isomorphic to C_2^r.

To motivate genus theory, let's consider our favorite example.

Example 4.4.1. *Let $\Delta = -20$ so $K = \mathbb{Q}(\sqrt{-5})$. The reduced forms of discriminant Δ are $Q_1(x,y) = x^2 + 5y^2$ and $Q_2(x,y) = 2x^2 + 2xy + 3y^2$. Hence $\mathcal{C}l_K \simeq \mathcal{C}l(\Delta)$ has order 2, so must be isomorphic to C_2. From the exercises in the previous section, Q_1 is the identity and Q_2 has order 2 in $\mathcal{C}l(\Delta)$.*

First let us determine the primes represented by Q_1 and Q_2. By the mass formula (first version) we know

$$R_{Q_1}(p) + R_{Q_2}(p) = r_{Q_1}(p) + r_{Q_2}(p) = 2(1 + \left(\frac{\Delta}{p}\right)) = \begin{cases} 4 & p \equiv 1,3,7,9 \bmod 20 \\ 0 & p \equiv 11,13,17,19 \bmod 20 \end{cases}$$

for $p \nmid \Delta$. (Note for p prime, $R_Q(p) = r_Q(p)$ for any form Q.) Note that if $R_{Q_1}(p) > 0$ for $p \nmid 20$, then $R_{Q_1}(p) \geq 4$ because if (x, y) is a solution to $x^2 + 5y^2 = p$, then so are $(\pm x, \pm y)$, which gives 4 different solutions as long as $p \neq 5$. In other words, any $p \equiv 1, 3, 7, 9 \bmod 20$ is represented either by Q_1 or Q_2, but not both.

However, looking at what numbers relatively prime to 20 are of the form $x^2 + 5y^2$ mod 20 we see 3 and 7 are not possible. Similarly, simple computations show that 1 and 9 are not of the form $2x^2 + 2xy + 3y^2$ mod 20. (In fact, it suffices to observe $x^2 + 5y^2$ does not represent $3 \bmod 4$ and $2x^2 + 2xy + 3y^2$ does not represent $1 \bmod 4$.) Hence we have

$$p \text{ is represented by } \begin{cases} Q_1 & \iff p = 5 \text{ or } p \equiv 1, 9 \bmod 20 \\ Q_2 & \iff p = 2 \text{ or } p \equiv 3, 7 \bmod 20 \end{cases}$$

Now we can ask what integers $n > 0$ are represented by Q_1. By the mass formula (first form), we know if Q_1 represents n, then n cannot be divisible by any prime p such that $\left(\frac{\Delta}{p}\right) = -1$, i.e., any $p \equiv 11, 13, 17, 19 \bmod 20$. Write $n = \prod p_i^{e_i} \cdot \prod q_j^{f_j}$ where each p_i is represented by Q_1 and each q_j is represented by Q_2. Gauss's composition says n is represented by $\prod_i Q_1^{e_i} \cdot \prod_j Q_2^{f_j}$ (where the multiplication here denotes Gauss composition). In other words, n is represented by Q_1 if $\sum f_j$ is even and n is represented by Q_2 if $\sum f_j$ is odd.

We would like to say the above statement about which n's are represented by Q_1 and which are represented by Q_2 is if and only if. Note that Q_1 represents $0, 1, 2 \bmod 4$ and $0, 1, 4 \bmod 5$, where as Q_2 represents $0, 2, 3 \bmod 4$ and $0, 2, 3 \bmod 5$. The only overlap here are the numbers $\equiv 0, 2 \bmod 4$ and $\equiv 0 \bmod 5$. Hence Q_1 and Q_2 cannot *represent the same numbers, except possibly for numbers divisible by 10. The case where n is not prime to the discriminant is more subtle, and we will not prove this, but it turns out Q_1 and Q_2 never represent the same numbers, so the above characterization of numbers represented by Q_1 (or Q_2) is if and only if.*

Genus theory allow us to generalize the above example to separate (at least partially) representations by different forms of discriminant Δ.

Definition 4.4.2. *Let $Q_1, Q_2 \in \mathcal{F}_\Delta$. We say Q_1 and Q_2 are in the same* **genus** *if they represent the same values mod Δ. The* **principal genus** *is the genus containing the identity of the form class group.*

It is a theorem that Q_1 and Q_2 are in the same genus if and only if Q_1 and Q_2 represent the same values mod m for every m. What is more important for us however, is that forms in different genera (the plural of genus) represent disjoint sets of numbers in $(\mathbb{Z}/\Delta\mathbb{Z})^\times$. This is the content of the following proposition.

Proposition 4.4.3. *Regard $\chi_\Delta = \left(\frac{\Delta}{\cdot}\right)$ as a real character of $(\mathbb{Z}/\Delta\mathbb{Z})^\times$. Let $H = \ker \chi_\Delta$. Let Q_0 (resp. Q) be in the prinicipal genus (resp. any genus) of $\mathcal{F}_\Delta$ and H_0 (resp. H_Q) denote the set of values in $(\mathbb{Z}/\Delta\mathbb{Z})^\times$ represented by Q_0 (resp Q). Then H_0 is a subgroup of H and H_Q is a coset of H_0 in H.*

(Note that H being the kernel of a group homomorphism, is a subgroup of $(\mathbb{Z}/\Delta\mathbb{Z})^\times$.)

For instance, in the above example, with $Q_0 = x^2 + 5y^2$ and $Q = 2x^2 + 2xy + 3y^2$, we have $H = \{1, 3, 7, 9\} \subseteq (\mathbb{Z}/20\mathbb{Z})^\times$, $H_0 = \{1, 9\}$ and $H_Q = \{3, 7\} = 3\{1, 9\}$.

Proof. Let $n \in (\mathbb{Z}/\Delta\mathbb{Z})^\times$. If n is represented by a form of discriminant Δ, we have $n \in H = \ker \chi_\Delta$ by Dirichlet's mass formula. To see that H_0 is a subgroup of H, observe it must be closed under multiplication by Gauss composition. To show it is closed under inversion, note by Exercise 4.9, we can assume $Q_0 = x^2 - \frac{\Delta}{4}y^2$ or $x^2 + xy + \frac{1-\Delta}{4}y^2$. Using either Brahmagupta or Dirichlet composition, it is straightforward to explicitly check H_0 is closed under inverses (and is nonempty—it contains 1).

It follows from Gauss composition that H_Q must be a translate of H_0 in H. □

Since the cosets of H_0 in H are disjoint, the integers n relatively prime to Δ can only be represented by forms in a single genus of $\mathcal{F}_\Delta$. In particular, if we want to determine which numbers are of the form $x^2 + dy^2$ (say relatively prime to $\Delta = -4d$), we can at least say n are represented by some form in the principal genus. In particular, if, up to equivalence, $x^2 + dy^2$ is the only form in the principal genus, we can say exactly which primes are represented by $x^2 + dy^2$ by (i) the mass formula and (ii) considerations mod Δ. In this case, we say Δ has **one class per genus** (see exercise below).

Exercise 4.13. *Let $Q_1, \ldots, Q_h$ denote representatives for $\mathcal{C}l(\Delta)$. Using Gauss composition, show the number of Q_i in a given genus is the same for each genus.*

Exercise 4.14. *Pick representatives Q_1, Q_2 for $\mathcal{C}l(-24)$. Determine what values Q_1 and Q_2 represent mod 24. Using this with Dirichlet's mass formula, determine all primes represented by Q_1 and all primes represented by Q_2. In particular, you should get a determination of all primes of the form $x^2 + 6y^2$.*

Now of course it's natural to ask, for which discriminants Δ do we have one class per genus? It's clearly true if the class number $h(\Delta) = 1$. We know there are only 9 fundamental discriminants $\Delta < 0$ with class number 1 (Gauss's class number problem), and this was easy to determine. Conversely, it is still an unsettled problem (also posed by Gauss) for which Δ have one class per genus. It is conjectured that there are precisely 65 fundamental discriminants (and 101 arbitrary negative discriminants) $\Delta < 0$ with one class per genus. It is not too difficult to show the following.

Theorem 4.4.4. *The principal genus of $\mathcal{C}l(\Delta)$ consists of the subgroup of squares of $\mathcal{C}l(\Delta)$.*

Corollary 4.4.5. *Δ has one class per genus if and only if $\mathcal{C}l(\Delta) \simeq C_2^r$ for some $r \geq 0$.*

We remark that for a specific r, we can compute all imaginary quadratic fields with class group C_2^r. There shouldn't be any for large enough r, and this is the most difficult part.

In the case of one class per genus, one can always determine the primes of the form $x^2 + dy^2$ by simple congruence conditions. However, at least conjecturally, this only happens finitely many times (for negative Δ). In the rest of the cases, the determination of primes of the form $x^2 + dy^2$ is more complicated.

Example 4.4.6. *Consider $Q_0 = x^2 + 14y^2$. This has discriminant $\Delta = -56$ and corresponds to the field $K = \mathbb{Q}(\sqrt{-14})$. There are 3 other reduced forms of discriminant -56, given by $Q_1 = 2x^2 + 7y^2$, $Q_2 = 3x^2 + 2xy + 5y^2$ and $Q_3 = 3x^2 - 2xy + 5y^2$. It is easy to check the (form) class group $\mathcal{C}l(\Delta) \simeq C_4$ (see exercise below). One can show $p = x^2 + 14y^2$ if and only if (i) $\left(\frac{-14}{p}\right) = 1$, and (ii) $(x^2+1)^2 \equiv 8 \bmod p$ has a solution. See [Cox]. We will discuss this briefly in the next chapter.*

Exercise 4.15. *Check that $Q_2 \circ Q_2 \sim Q_3 \circ Q_3 \sim Q_1$. Conclude $\mathcal{C}l(-56) \simeq C_4$.*

5 Non-unique factorizations

In this chapter we briefly discuss some aspects of non-unique factorization, ending with an application of quadratic forms (and more generally ideals) to factorization problems in rings of integers.

5.1 Principalization

Let K be a number field. Kummer approach to resolving the non-unique factorization of $\mathcal{O}_K$ was essentially to work in a larger ring of integers R where every (nonzero nonunit) element of $\mathcal{O}_K$ factors uniquely (up to order and units) into irreducibles in R. We can recast this approach in Dedekind's language of ideals with the following notion.

Definition 5.1.1. *We say an finite extension L of K is a* **principalization field** *for K, or* **principalizes** *K, if $\mathcal{I}\mathcal{O}_L$ is a a principal ideal of L for any ideal $\mathcal{I}$ of $\mathcal{O}_K$.*

Some authors instead say K *capitulates* in L.

Proposition 5.1.2. *Suppose L principalizes K. Leta be a nonzero nonunit in $\mathcal{O}_K$ and write $a\mathcal{O}_K = \prod \mathfrak{p}_i$ be the prime ideal factorization of $a\mathcal{O}_K$ in $\mathcal{O}_K$. Write $\mathfrak{p}_i\mathcal{O}_L = (\alpha_i)$ for some $\alpha_i \in \mathcal{O}_L$. If $a = \prod \beta_j$ is any irreducible factorization of a in $\mathcal{O}_K$, then each β_j is, up to a unit of $\mathcal{O}_L$, a subproduct of the α_i's.*

In other words all irreducible factorizations of a in $\mathcal{O}_K$, comes from different groupings of a single (not necessarily irreducible) factorization $a = \prod \alpha_j$ in $\mathcal{O}_L$. E.g., we may have something like

$$a = \underbrace{(\alpha_1 \cdots \alpha_{i_1})}_{\beta_1}\underbrace{(\alpha_{i_1+1} \cdots \alpha_{i_2})}_{\beta_2} \cdots \underbrace{(\alpha_{i_k+1} \cdots \alpha_m)}_{\beta_{k+1}}$$

and any irreducible (or even non-irreducible) factorization of a in $\mathcal{O}_K$, just comes from a regrouping of the α_i's.

Proof. Since L principalizes K, then for each i, we can write $\mathfrak{p}_i\mathcal{O}_L = (\alpha_i)$ for some $\alpha_i \in \mathcal{O}_L$. (It is not necessarily true that each α_i is irreducible.) Hence

$$a\mathcal{O}_L = \prod(\mathfrak{p}_i\mathcal{O}_L) = \prod(\alpha_i).$$

On the other hand,

$$a\mathcal{O}_K = \prod(\beta_j)$$

so each (β_j) is a subproduct of the $\mathfrak{p}_i$'s, say $\beta_j = \mathfrak{p}_{j_1}\mathfrak{p}_{j_2}\cdots\mathfrak{p}_{j_k}$ so $\beta_j = u\alpha_{j_1}\ldots\alpha_{j_k}$ for some unit $u \in \mathcal{O}_L$. □

Example 5.1.3. *Let $K = \mathbb{Q}(\sqrt{-5})$ and $L = \mathbb{Q}(\sqrt{-5}, \sqrt{2})$. To show L principalizes K, it suffices to show $(2, \sqrt{-5})\mathcal{O}_L$ is principal since $(2, \sqrt{-5}) \subseteq \mathcal{O}_K$ generates the class group of K. (Justify to yourself that this is sufficient.) Note that $(2, \sqrt{-5})^2 = (2)$. On the other hand $(2) = (\sqrt{2})^2$ in $\mathcal{O}_L$. Since $(\sqrt{2})$ is prime in $\mathcal{O}_L$, we must have $(\sqrt{2}) = (2, \sqrt{-5})\mathcal{O}_L$ by the unique prime ideal factorization in $\mathcal{O}_L$. Thus L is a principalization field for K.*

Let's see how we can resolve the non-unique factorization

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

in $\mathcal{O}_K$ using principalization. Recall the prime ideal factorization of (6) *in $\mathcal{O}_K$ is*

$$(6) = (2, 1+\sqrt{-5})^2(3, 1+\sqrt{-5})(3, 1-\sqrt{-5}).$$

One can check that

$$(2, 1+\sqrt{-5})\mathcal{O}_L = (\sqrt{2})$$

(we did this above) and

$$(3, 1+\sqrt{-5})\mathcal{O}_L = (\frac{\sqrt{2}+\sqrt{-10}}{2})$$

$$(3, 1-\sqrt{-5})\mathcal{O}_L = (\frac{\sqrt{2}-\sqrt{-10}}{2})$$

(we'll discuss this below). The above proposition says the irreducible factorizations of 6 *in $\mathcal{O}_K$ come from different groupings of the factorization*

$$6 = \underbrace{(\sqrt{2}\cdot\sqrt{2})}_{2}\underbrace{(\frac{\sqrt{2}+\sqrt{-10}}{2}\cdot\frac{\sqrt{2}-\sqrt{-10}}{2})}_{3} = \underbrace{(\sqrt{2}\cdot\frac{\sqrt{2}+\sqrt{-10}}{2})}_{1+\sqrt{-5}}\underbrace{(\sqrt{2}\cdot\frac{\sqrt{2}-\sqrt{-10}}{2})}_{1-\sqrt{-5}}.$$

Thus we see principalization provides an alternative viewpoint to the resolution of non-unique factorization in a ring of integers $\mathcal{O}_K$. Furthermore, we will see there are some advantages to using principalization (essentially Kummer's approach) instead of ideal theory (Dedekind's approach) by giving an application of principalization in the next section, even though these two approaches are more or less equivalent by Proposition 5.1.2.

Now of course it is natural to ask when K has a principalization field and how can we find one. It turns out to be quite easy to answer.

Proposition 5.1.4. *Let $\mathcal{I}_1, \ldots, \mathcal{I}_h$ be ideals of $\mathcal{O}_K$ which generate the class group. If e_j is the order of $\mathcal{I}_j$ in $\mathcal{C}l_K$, then we can write $\mathcal{I}_j^{e_j} = (\alpha_j)$ for some $\alpha_j \in \mathcal{O}_K$. Then $L = K(\sqrt[e_1]{\alpha_1}, \ldots, \sqrt[e_h]{\alpha_h})$ is a principalization field for K.*

The proof is immediate.

It is worthwhile to remark that even though passing to $\mathcal{O}_L$ resolves non-unique factorization in $\mathcal{O}_K$ (in the sense of Proposition 5.1.2), it is not necessarily the case that any element of $\mathcal{O}_L$ has a unique irreducible factorization in $\mathcal{O}_L$. In particular, there are examples of number fields K such that no finite extension L of K has class number 1. This was shown by Golod and Shafarevich in 1964 with the example of $K = \mathbb{Q}(\sqrt{-3\cdot 5\cdot 7\cdot 11\cdot 13\cdot 17\cdot 19})$.

One particular principalization field is particularly noteworthy, and is important for studying primes of the form $x^2 + dy^2$.

We say L/K is an **abelian** extension if it is Galois and $\mathrm{Gal}(L/K)$ is abelian. Further, L/K is **unramified** if every prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ is unramified in L.

Definition 5.1.5. *The* **Hilbert class field** *$HCF(K)$ is the maximal unramified abelian extension of K.*

An important component of *class field theory*, which we hope to discuss in Part III, is the following result.

Theorem 5.1.6. *$H = HCF(K)$ is a well-defined finite extension of K satisfying $\mathrm{Gal}(H/K) = \mathcal{C}l_K$. Further H principalizes K.*

Example 5.1.7. *Let $K = \mathbb{Q}$. Then any nontrivial extension L of K must be ramified (since the $|\Delta_L| > 1$ and any $p|\Delta_L$ ramifies in L), hence there is only one unramifed extension of $\mathbb{Q}$—namely $\mathbb{Q}$ itself. Thus $HCF(\mathbb{Q}) = \mathbb{Q}$.*

More generally if $h_K = 1$, the above theorem tells us $HCF(K) = K$.

Example 5.1.8. *Let $K = \mathbb{Q}(\sqrt{-5})$. If L/K is unramified, then $p|\Delta_L$ implies $p|\Delta_K = -20$. One might be tempted to guess the Hilbert class field of K is $L = \mathbb{Q}(\sqrt{-5}, \sqrt{2})$ from Example 5.1.3. Indeed L/K is abelian with Galois group $\simeq C_2 \simeq \mathcal{C}l_K$, but it is not unramified. The Hilbert class field of K is $\mathbb{Q}(\sqrt{-5}, i)$.*

Exercise 5.1. *Check $HCF(\mathbb{Q}(\sqrt{-5})) = \mathbb{Q}(\sqrt{-5}, i)$ using the definition and the theorem above.*

One use of the Hilbert class field can be seen in the following result ([Cox]).

Theorem 5.1.9. *Let $d > 0$ be squarefree and $d \not\equiv 3 \bmod 4$. Let $K = \mathbb{Q}(\sqrt{-d})$, $H = HCF(K)$, and p be an odd prime not dividing $\Delta = -4d$. Write $H = K(\alpha)$ and let $f(x)$ be the minimum polynomial for α. Then the following are equivalent:*

(i) p is represented by $x^2 + dy^2$

(ii) p splits completely in H

(iii) $\left(\frac{\Delta}{p}\right) = 1$ and $f(x)$ has a root mod p.

Exercise 5.2. *Check the above theorem in the case of $d = 5$.*

5.2 Counting non-unique factorizations

In this section, we will show how one can use quadratic forms to determine and count the irreducible factorizations of an integer in $\mathcal{O}_K$, where K is a quadratic field with class number 2. (In fact, one can treat the case of $\mathcal{C}l_K \simeq C_2^r$ by the same approach.) For simplicity, we will just go through the specific case of $K = \mathbb{Q}(\sqrt{-5})$.

Afterwards, we will discuss what happens in an arbitrary number field, where one must use ideal theory to obtain the analogous result. In particular, this gives a qualitative and quantitative way to see that the class group $\mathcal{C}l_K$ really does measure the failure of unique factorization in $\mathcal{O}_K$ in a precise way. Both these results and this approach using principalization seems to be new (in fact I proved it just to show you how the class group measures the failure of unique factorization in $\mathcal{O}_K$!), see [Martin] for more details. For an introduction to other work on irreducible factorizations (in different directions), see [Narkiewicz].

Let $K = \mathbb{Q}(\sqrt{-5})$ so $\Delta = \Delta_K = -20$. Denote by $\mathfrak{C}_1$ the set of principal ideals in $\mathcal{O}_K$ and $\mathfrak{C}_2$ the set of nonprinicpal ideals of $\mathcal{O}_K$. The reduced forms of discriminant Δ are $Q_1(x, y) = x^2 + 5y^2$ and $Q_2(x, y) = 2x^2 + 2xy + 3y^2$.

Let $\mathcal{P}_0$ denote the primes $p \in \mathbb{N}$ which are not represented by Q_1 or Q_2 and $\mathcal{P}_i$ denote the primes $p \in \mathbb{N}$ which are represented by Q_i for $i = 1, 2$. Then $\mathcal{P}_0$ is the set of inert primes in $K/\mathbb{Q}$, $\mathcal{P}_1$ is the set of primes p such that the ideal $p\mathcal{O}_K$ factors into two principal ideals in $\mathcal{O}_K$, and $\mathcal{P}_2$ is the set of primes p such that $p\mathcal{O}_K$ factors into two nonprincipal ideals of $\mathcal{O}_K$.

Set

$$\mathcal{P}_i^{ram} = \{p \in \mathcal{P}_i : p \text{ is ramified in } K\}, \text{ and}$$
$$\mathcal{P}_i^{unr} = \{p \in \mathcal{P}_i : p \text{ is unramified in } K\}.$$

Explicitly, we have $\mathcal{P}_0 = \{p : p \equiv 11, 13, 17, 19 \bmod 20\}$, $\mathcal{P}_1^{ram} = \{5\}$, $\mathcal{P}_1^{unr} = \{p : p \equiv 1, 9 \bmod 20\}$, $\mathcal{P}_2^{ram} = \{2\}$ and $\mathcal{P}_2^{unr} = \{p : p \equiv 3, 7 \bmod 20\}$.

If $p \in \mathcal{P}_0 \cup \mathcal{P}_1$ then any prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ lying above p is in $\mathfrak{C}_1$, and if $q \in \mathcal{P}_2$, then any prime ideal of $\mathcal{O}_K$ lying above q is in $\mathfrak{C}_2$. Specifically, if $q = 2 \in \mathcal{P}_2^{ram}$, then $q\mathcal{O}_K = \mathfrak{r}^2$ where $\mathfrak{r}$ is the prime ideal $(2, 1 + \sqrt{-5})$ of $\mathcal{O}_K$, and if $q \in \mathcal{P}_2^{unr}$ then $q = \mathfrak{q}\overline{\mathfrak{q}}$ where $\mathfrak{q}$ and $\overline{\mathfrak{q}}$ are distinct prime ideals of $\mathcal{O}_K$. Here $\overline{\mathfrak{q}}$ denotes the conjugate ideal of $\mathfrak{q}$ in $K/\mathbb{Q}$.

Now let $n > 1$ and write the prime ideal factorization of $n\mathcal{O}_K$ as

$$(n) = \mathfrak{p}_1^{d_1} \cdots \mathfrak{p}_r^{d_r} \mathfrak{q}_1^{e_1} \overline{\mathfrak{q}}_1^{e_1} \cdots \mathfrak{q}_s^{e_s} \overline{\mathfrak{q}}_s^{e_s} \mathfrak{r}^f,$$

where each $\mathfrak{p}_i \in \mathfrak{C}_1$, $\mathfrak{q}_j \in \mathfrak{C}_2$ with conjugate $\overline{\mathfrak{q}}_j$, and the $\mathfrak{p}_i$'s, $\mathfrak{q}_j$'s, $\overline{\mathfrak{q}}_j$'s and $\mathfrak{r}$ are all distinct. Since each $\mathfrak{p}_i = (\pi_i)$ for some irreducible π_i of $\mathcal{O}_K$, any irreducible factorization of n must contain (up to units) $\pi_1^{d_1} \cdots \pi_r^{d_r}$. Thus it suffices to consider irreducible factorizations of $n' = n/(\pi_1^{d_1} \cdots \pi_r^{d_r})$.

Let q_j be the prime in $\mathbb{N}$ such that $\mathfrak{q}_j$ lies above q_j. Since $\mathfrak{q}_j$ is nonprincipal, we must have that $q_j \in \mathcal{P}_2$, i.e., q_j is represented by Q_2. Note that we can factor the quadratic form into linear factors

$$Q_2(x, y) = (\sqrt{2}x + \frac{\sqrt{2} + \sqrt{-10}}{2}y)(\sqrt{2}x + \frac{\sqrt{2} - \sqrt{-10}}{2}y) \tag{5.1}$$

over the field $L = K(\sqrt{2})$. Hence, while q_j is irreducible over $\mathcal{O}_K$ (otherwise the prime ideal factors of $q_j\mathcal{O}_K$ would be principal), the fact that $q_j = Q_2(x, y)$ for some x, y gives us a factorization $q_j = \alpha_j\overline{\alpha}_j$ in L where $\alpha_j = \sqrt{2}x + \frac{\sqrt{2}+\sqrt{-10}}{2}y$ and $\overline{\alpha}_j = \sqrt{2}x + \frac{\sqrt{2}-\sqrt{-10}}{2}y$. Since $\sqrt{2}, \frac{\sqrt{2}\pm\sqrt{-10}}{2} \in \mathcal{O}_L$, we have $\alpha_j \in \mathcal{O}_L$ (in fact irreducible).

Since α_j and $\overline{\alpha}_j$ are conjugate with respect to the nontrivial element of $\mathrm{Gal}(K/\mathbb{Q})$, the ideals $(\alpha_j) \cap \mathcal{O}_K$ and $(\overline{\alpha}_j) \cap \mathcal{O}_K$ must be conjugate ideals of $\mathcal{O}_K$ which divide q_j, and hence in some order equal $\mathfrak{q}_j$ and $\overline{\mathfrak{q}}_j$. Thus, up to a possible switching α_j and $\overline{\alpha}_j$, we can write $\mathfrak{q}_j\mathcal{O}_L = (\alpha_j)$ and $\overline{\mathfrak{q}}_j\mathcal{O}_L = (\overline{\alpha}_j)$. Similarly $\mathfrak{r}\mathcal{O}_L = (\sqrt{2})$.

This means the following. If $n' = \prod \beta_i$ is any irreducible factorization of n' in $\mathcal{O}_K$, we have

$$\prod(\beta_i) = (n') = \mathfrak{r}^f \mathfrak{q}_1^{e_1} \overline{\mathfrak{q}}_1^{e_1} \cdots \mathfrak{q}_s^{e_s} \overline{\mathfrak{q}}_s^{e_s} = (\sqrt{2})^f \prod_{j=1}^{s} (\alpha_j)^{e_j} (\overline{\alpha}_j)^{e_j}$$

as ideals of $\mathcal{O}_L$. From Proposition 5.1.2, we know that each (β_i) is a subproduct of the product of ideals on the right. In other words, to the irreducible factorizations of $\mathcal{O}_K$ come from different groupings of the factorization

$$n' = \sqrt{2}^f \prod_{j=1}^{s} \alpha_j^{e_j} \overline{\alpha}_j^{e_j}. \tag{5.2}$$

Thus to determine the factorizations of of n' in $\mathcal{O}_K$, it suffices to determine when a product of the α_{ij} is an irreducible element of $\mathcal{O}_K$. But this is simple! Note from the factorization of $Q_2(x, y)$ in (5.1), we see that each $\alpha_{ij} \in \sqrt{2}K$. Hence the product of any two α_i's (or $\sqrt{2} \cdot \alpha_j$ or $\sqrt{2} \cdot \sqrt{2}$) lies in K, and therefore $\mathcal{O}_K$, and must be irreducible since no individual $\alpha_j \in \mathcal{O}_K$. In other words,

the irreducible factorizations of n' in $\mathcal{O}_K$ are precisely what we get from grouping the terms on the right of (5.2) in pairs. What we have proved is the following.

If $\{a_i\}$ is a collection of distinct objects, denote the multiset containing each a_i with cardinality m_i by $\left\{a_i^{(m_i)}\right\}$. Let $\eta_K(n)$ denote the number of distinct (up to order and units) irreducible factorizations of n in $\mathcal{O}_K$.

Proposition 5.2.1. *With notation as above ($K = \mathbb{Q}(\sqrt{-5})$), the irreducible factorizations of n in $\mathcal{O}_K$ are, up to units, $n = \prod \pi_i \prod \beta_k$ where each β_k is a product of two numbers of the following types: $\sqrt{2}, \alpha_j$, or $\overline{\alpha}_j$. In particular, $\eta_K(n)$ is the number of ways we can arrange the multiset $\left\{\sqrt{2}^{(f)}, \alpha_j^{(e_j)}, \overline{\alpha}_j^{(e_j)}\right\}$ in pairs.*

The **length** of an irreducible factorization is the number of irreducibles occurring in the factoriziation, with multiplicity.

Corollary 5.2.2. *Any two irreducible factorizations of n in $\mathcal{O}_K$ have the same length.*

Hence the above result tells us about the structure of the irreducible factorizations in $\mathcal{O}_K$, not just their number. In fact, the above approach tells us how to explicitly obtain all irreducible factorizations of some n in $\mathcal{O}_K$.

Example 5.2.3. *Let $n = 2 \cdot 7^2 \cdot 29$. Here $29 \in \mathcal{P}_1$ and $2, 7 \in \mathcal{P}_2$. We have*

$$2 = Q_2(1,0) = \sqrt{2} \cdot \sqrt{2}$$

$$7 = Q_2(1,1) = \underbrace{(\sqrt{2} + \frac{\sqrt{2} + \sqrt{-10}}{2})}_{\alpha}\underbrace{(\sqrt{2} + \frac{\sqrt{2} - \sqrt{-10}}{2})}_{\overline{\alpha}}$$

$$29 = Q_1(3,2) = 3^2 + 5 \cdot 2^2 = \underbrace{(3 + 2\sqrt{-5})}_{\pi}\underbrace{(3 - 2\sqrt{-5})}_{\overline{\pi}}$$

using the factorization of Q_1 and Q_2 into linear forms over $\mathcal{O}_L$. Then the above tells us the irreducible factorizations of n in $\mathcal{O}_K$ are precisely those obtained from grouping the terms in square brackets on the right in pairs in the following factorization in $\mathcal{O}_L$:

$$n = \pi\overline{\pi}\left[\sqrt{2} \cdot \sqrt{2} \cdot \alpha \cdot \alpha \cdot \overline{\alpha} \cdot \overline{\alpha}\right].$$

Precisely, we have $\eta_K(n) = 5$ factorizations and they are explicitly given by

$$n = \pi\overline{\pi}(\sqrt{2}\sqrt{2})(\alpha\alpha)(\overline{\alpha}\overline{\alpha})$$

$$n = \pi\overline{\pi}(\sqrt{2}\sqrt{2})(\alpha\overline{\alpha})(\alpha\overline{\alpha})$$

$$n = \pi\overline{\pi}(\sqrt{2}\alpha)(\sqrt{2}\alpha)(\overline{\alpha}\overline{\alpha})$$

$$n = \pi\overline{\pi}(\sqrt{2}\alpha)(\sqrt{2}\overline{\alpha})(\alpha\overline{\alpha})$$

$$n = \pi\overline{\pi}(\sqrt{2}\overline{\alpha})(\sqrt{2}\overline{\alpha})(\alpha\alpha).$$

(Each product of two terms in $\mathcal{O}_L$ in parentheses above is an irreducible element of $\mathcal{O}_K$. If you feel a need, you can compute these products explicitly, and check that they are all distinct factorizations in $\mathcal{O}_K$.)

Exercise 5.3. *Determine all irreducible factorizations of $n = 60$ in $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$.*

Exercise 5.4. *Let $p \in \mathbb{N}$ be prime and $e \geq 1$. Determine a formula for $\eta_K(p^e)$ where $K = \mathbb{Q}(\sqrt{-5})$. (It will depend on the value of $p \bmod 20$ as well as e.)*

Exercise 5.5. *Let $q_1, \ldots, q_k$ be distinct primes in $\mathcal{P}_2^{unr}$. Show $\eta_K(q_1 \cdots q_k) = (2k-1)!! = (2k-1)(2k-3)(2k-5)\cdots 3 \cdot 1$. (Again $K = \mathbb{Q}(\sqrt{-5})$.)*

We remark that there seems to be no simple algebraic formula for $\eta_K(n)$ for general n, despite the fairly simple combinatorial description. However, there is a simple way to compute $\eta_K(n)$ in terms of generating functions, a technique often used in combinatorics. We give it precisely in the following alternate version of the above proposition.

Proposition 5.2.4. *Let $K = \mathbb{Q}(\sqrt{-5})$, $L = K(\sqrt{2})$ and $n > 1$. Write the prime ideal factorization of (n) in $\mathcal{O}_K$ as $(n) = \prod \mathfrak{p}_i^{d_i} \prod \mathfrak{q}_j^{e_j}$, where each $\mathfrak{p}_i \in \mathfrak{C}_1$, $\mathfrak{q}_j \in \mathfrak{C}_2$ and the $\mathfrak{p}_i$'s and $\mathfrak{q}_j$'s are all distinct. Let $\pi_i \in \mathcal{O}_K$ and $\alpha_j \in \mathcal{O}_L$ such that $\mathfrak{p}_i = (\pi_i)$ and $\mathfrak{q}_j \mathcal{O}_L = (\alpha_j)$. Then the irreducible nonassociate factorizations of n are precisely $n = u \prod \pi_i^{d_i} \prod \beta_k$ where u is a unit, each β_k is a product of two (not necessarily distinct) α_j's and $\prod \beta_k = \prod \alpha_j^{e_j}$.*

In particular $\eta_K(n)$ is the number of ways we can arrange the multiset $\left\{\alpha_j^{(e_j)}\right\}$ in pairs, i.e., the number of partitions of this multiset into sub-multisets of size 2. In other words, if the number of distinct $\mathfrak{q}_j$'s is m, then $\eta_K(n)$ is the coefficient of $\prod x_j^{e_j}$ in the formal power series expansion of $\prod_{i \leq j} \frac{1}{1-x_i x_j}$ in $\mathbb{Z}[[x_1, x_2, \ldots, x_m]]$.

In fact we stated this proposition for $n \in \mathcal{O}_K$, not just $n \in \mathbb{Z}$, but it is no more difficult to prove. Moreover, the description of $\eta_K(n)$ in terms of coefficients of a power series is essentially a tautology (use the geometric series expansion for $\frac{1}{1-x_i x_j}$ and count).

In general, one can prove an analogue of the above using (just) ideals, and the proof is just as simple as the case of $K = \mathbb{Q}(\sqrt{-5})$ we did with quadratic forms. The advantage of the quadratic forms approach above however is one can explicitly write down the irreducible factorizations of a rational integer n in $\mathcal{O}_K$ in terms of the explicit representations of $p|n$ by quadratic forms of discriminant Δ_K, provided $\mathcal{C}l_K \simeq C_2^r$. See [Martin] for the details when $r > 1$.

(The problem when $\mathcal{C}l_K \not\simeq C_2^r$, which is tied to the one class per genus problem, is that if Q is a quadratic form which does not have order 2 in $\mathcal{C}l(\Delta)$, then there is no number field L such that Q factors into linear forms over $\mathcal{O}_L$. One can always factor Q into linear forms over some quadratic field, since Q is just a quadratic polynomial, but the problem is that the coefficients of these linear forms will only be algebraic *integers* when Q is ambiguous, hence of order 2 in $\mathcal{C}l(\Delta)$.)

In [Martin], we prove the following.

Theorem 5.2.5. *Let K be a number field and $\mathcal{C}l_K = \{\mathfrak{C}_i\}$. Let $n \in \mathcal{O}_K$ be a nonzero nonunit. Suppose the prime ideal factorization of $n\mathcal{O}_K$ is $(n) = \prod_{(i,j) \in T} \mathfrak{p}_{ij}$ where the $\mathfrak{p}_{ij}$'s are (not necessarily distinct) prime ideals such that $\mathfrak{p}_{ij} \in \mathfrak{C}_i$, and T is some finite index set. Let K_i be a principalization field for $\mathfrak{C}_i$, so $\mathfrak{p}_{ij}\mathcal{O}_{K_i} = (\alpha_{ij})$ for some $\alpha_{ij} \in \mathcal{O}_{K_i}$. Let $L = \prod K_i$.*

Then the irreducible factorizations of n in $\mathcal{O}_K$ are precisely the factorizations of the form $n = \prod \beta_l$ where $\prod \beta_l \sim \prod \alpha_{ij}$ in $\mathcal{O}_L$ and each β_l is of the form $\beta_l \sim \prod_{(i,j) \in S} \alpha_{ij}$ in $\mathcal{O}_L$ for S a minimal (nonempty) subset of T such that $\prod_{(i,j) \in S} \mathfrak{C}_i = \mathfrak{I}$. (Here each β_l is irreducible in $\mathcal{O}_K$.)

In other words, all irreducible factorizations n in $\mathcal{O}_K$ come from different groupings of the factorization $n \sim \prod \alpha_{ij}$ in $\mathcal{O}_L$. Now a grouping of terms of this factorization in $\mathcal{O}_L$ gives an

irreducible factorization in $\mathcal{O}_K$ if and only if every group of terms gives an irreducible element of $\mathcal{O}_K$ (possibly up to a unit in $\mathcal{O}_L$). A product of α_{ij}'s gives an element of $\mathcal{O}_K$ if and only if the corresponding product of ideal classes $\mathfrak{C}_i$ is trivial in $\mathcal{C}l_K$, and this element of $\mathcal{O}_K$ will be irreducible if and only if no proper subproduct of the corresponding ideal classes is trivial.

It should be clear that this theorem gives a precise way that the class group measures the failure of unique factorization in $\mathcal{O}_K$. In particular, the larger the class group, the more complicated the structure of the irreducible factorizations of an element can become.

Corollary 5.2.6. *Let K be a number field and $\mathcal{C}l_K = \{\mathfrak{C}_i\}$. Let $n \in \mathcal{O}_K$ be a nonzero nonunit. Suppose $(n) = \prod_{(i,j)\in T} \mathfrak{p}_{ij}^{e_{ij}}$, where the $\mathfrak{p}_{ij}$'s are distinct prime ideals, each $\mathfrak{p}_{ij} \in \mathfrak{C}_j$ and T is some index set. Let U be the multiset $U = \left\{(i,j)^{(e_{ij})} : (i,j) \in T\right\}$. Then $\eta_K(n)$ is the number of ways one can partition the multiset $\left\{x_{ij}^{e_{ij}}\right\}$ into minimal subsets V such that $\prod_{x_{ij}\in V} \mathfrak{C}_i = \mathfrak{I}$.*

Exercise 5.6. *Deduce the following result of Carlitz: Let K be a number field. We say $\mathcal{O}_K$ is half-factorial if every irreducible factorization of a given $n \in \mathcal{O}_K$ has the same length. Then $\mathcal{O}_K$ if half-factorial if and only if $h_K \leq 2$.*

In general, one defines the **elasticity** ρ_K of $\mathcal{O}_K$ to be $\max_{n\in\mathcal{O}_K} \rho_K(n)$ where $\rho_K(n)$ is the maximum ratio of lengths of two irreducible factorizations of n in $\mathcal{O}_K$. Similarly, one can use our theorem above to determine ρ_K in terms of the structure of the class group (it depends upon more than just h_K). See [Narkiewicz] for complete statements (needless to say, proved there without recourse to our theorem).

Part III

Part III

In this, the final part of the course, we will introduce the notions of local and global viewpoints of number theory, which began with the notion of p-adic numbers. (p as usual denote a rational prime.) The basic idea is that many problems in number theory can be treated by looking at solutions mod m. We saw, say with the example of $x^2 + y^2$, that we can rule out any number $\equiv 3 \bmod 4$ being of the form $x^2 + y^2$.

On the other hand, suppose, for a given n, we knew a mod m solution to

$$x^2 + y^2 \equiv n \bmod m$$

for each m. Hasse's idea was that if these *local* solutions (solutions mod m for each m) are "sufficiently compatible," then we can paste them together to actually construct a *global* solution in $\mathbb{Z}$. In fact it suffices to consider the cases where $m = p^e$ is a prime power. What it means for the solutions to be sufficiently compatible means is the following. Consider $x^2 + y^2 = 244$. A solution to this in $\mathbb{Z}$ would mean in particular we have solutions mod 2 and mod 4. Here are two:

$$x^2 + y^2 \equiv 1^2 + 1^2 \equiv 0 \bmod 2, \;\; x^2 + y^2 \equiv 0^2 + 2^2 \equiv 0 \bmod 4$$

In the mod 2 solution x, y must both be odd, but in the mod 4 solution both x and y are even, so there is no way to paste together these local solutions to get a solution in integers, hence we say they are not compatible.

Essentially what the p-adic integers $\mathbb{Z}_p$ are, are the elements of

$$(\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p^2\mathbb{Z}) \times (\mathbb{Z}/p^3\mathbb{Z}) \times \cdots$$

which are compatible in the above sense. In other words, a p-adic integer $x = (x_n)$ gives a congruence class $x_n \bmod p^n$ for each n such that $x_{n+1} \equiv x_n \bmod p^n$. We can form the field of fractions of the p-adic integers to obtain the field of p-adic number $\mathbb{Q}_p$. The advantage of this is we can use field theory, which is much stronger than ring theory, whereas we couldn't do this with a single $\mathbb{Z}/p^n\mathbb{Z}$, since $\mathbb{Z}/p^n\mathbb{Z}$ doesn't embed in a field as there are nontrivial zero divisors (unless $n = 1$). (Even though $\mathbb{Z}_p$ "contains" all of these $\mathbb{Z}/p^n\mathbb{Z}$'s, it turns out to be an integral domain.)

After discussing the p-adic numbers, we will discuss applications to quadratic forms in several variables. This naturally leads into the topic of modular forms, which is slated to be taught next year, and we will not discuss them in any detail here.

We will follow this with an introduction to adéles, which is considered a *global* way of studying things. Just like the p-adic numbers put together information mod p^n for all n, the adèles $\mathbb{A}_{\mathbb{Q}}$ put together $\mathbb{Q}_p$ for all p. Moreover, one can do all this over an arbitrary number field. Namely, for any number field K and prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$, one can define the field $K_{\mathfrak{p}}$ of $\mathfrak{p}$-adic numbers. Then one define the adéles $\mathbb{A}_K$ of K, which is essentially a product of all the $K_{\mathfrak{p}}$'s. It turns out that $\mathbb{A}_K$ provides an alternative way to study the class group $\mathcal{C}l_K$ as well as *class field theory*, which studies the abelian extensions of K.

The adelic picture is important for several reasons, not least of which is it allows for a vast generalization of class field theory, known as *Langlands' program*, or *non-abelian class field theory*. As a special case, Langlands' program (together with Wiles' famous work) includes the famous

Taniyama–Shimura(–Weil) correspondence between elliptic curves and modular forms, which is famous for proving Fermat's Last Theorem. While (abelian) class field theory is more or less considered a closed book now (which is of course not to say that everything is known about abelian extensions), the Langlands' program is only in a toddler stage, and lies at the heart of the research of several faculty members here. The Langlands' program and the generalized (or grand) Riemann hypothesis are the two most important outstanding problems in both number theory and the theory of automorphic forms/representations.

Time permitting, we will give a brief introduction to abelian class field theory and Langlands' program. The second semester of next year's Modular Forms course should contain a more detailed introduction to Langlands' program.

6 p-adic numbers

Throughout this chapter p will denote a fixed prime number of $\mathbb{N}$.

In the introduction to Part III, we briefly described the p-adic integers are elements in

$$(a_n) \in (\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p^2\mathbb{Z}) \times (\mathbb{Z}/p^3\mathbb{Z}) \times \cdots$$

which are compatible in the sense that the natural map $\mathbb{Z}/p^{n+1}\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ maps a_{n+1} to a_n. There are several different ways to describe the p-adic numbers, which were first introduced by Hensel at the end of the 1800's. Before we proceed into the formalities of the p-adic numbers, it may be interesting to describe Hensel's original viewpoint of the p-adic numbers.

The basic idea came from an analogy with algebraic geometry. The basic premise of modern mathematics is that to study some object X, it is helpful to study functions on X. In particular, to study the complex numbers $\mathbb{C}$, one may choose to study the polynomial ring $\mathbb{C}[x]$. (The space $\mathbb{C}$ is the set of **points**, and the ring $\mathbb{C}[x]$ is called the **coordinate ring** of $\mathbb{C}$.) One of the early observations in complex algebraic geometry was that the set of maximal ideals of $\mathbb{C}[x]$ is just the set of (principal) ideals generated by a linear polynomial of the form $x - p_0$ for some point $p_0 \in \mathbb{C}$. In other words, there is a bijection between $\mathbb{C}$ and the maximal ideals of $\mathbb{C}[x]$, given by a point $p_0 \in \mathbb{C}$ corresponds to the ideal of all polynomials which vanish at p_0. Further if $f(x) \in \mathbb{C}[x]$, then we have the map

$$\begin{aligned} \mathbb{C}[x] &\to \mathbb{C}[x]/(x - p_0) \simeq \mathbb{C} \\ f(x) &\mapsto f(p_0), \end{aligned}$$

i.e., to mod out by a maximal idea $(x - p_0)$ in $\mathbb{C}[x]$, just means substituting in $x = p_0$ for a polynomial $f(x) \in \mathbb{C}[x]$, i.e., this "mod $(x - p_0)$" map $\mathbb{C}[x] \to \mathbb{C}$ just sends a polynomial $f(x)$ to its value at a point p_0.

Now instead, let's try to imagine $\mathbb{Z}$ in place of $\mathbb{C}[x]$ as a coordinate ring. What should the space of points be? Well, in analogy with the above, a good candidate is the set of maximal ideals of $\mathbb{Z}$, i.e., the set of all nonzero prime ideals (p) of $\mathbb{Z}$. In other words, if we consider the space $\mathcal{P} = \{p\mathbb{Z} : p \in \mathbb{N}\}$ of points as the natural number primes, then the coordinate ring "$\mathcal{P}[x]$," i.e., the "polynomials on the space $\mathcal{P}$," are just the integers $n \in \mathbb{Z}$. How do we evaluate a "polynomial" $n \in \mathbb{Z}$ on a point $p \in \mathcal{P}$? Just consider the map

$$\begin{aligned} \mathbb{Z} &\to \mathbb{Z}/p\mathbb{Z} \\ n &\mapsto n \bmod p. \end{aligned}$$

In other words, the analogue of polynomials in one variable over $\mathbb{C}$, when we replace $\mathbb{C}$ with the set of primes $\mathcal{P}$, are the functions on $\mathcal{P}$ given by integers $n \in \mathbb{Z}$ such that $n(p) = n \bmod p$. One obvious difference is that for any $p_0 \in \mathbb{C}$, the space $\mathbb{C}[x]/(x - p_0) \simeq \mathbb{C}$, so all functions in the coordinate ring $\mathbb{C}[x]$ really map into $\mathbb{C}$. But in the case of $p \in \mathcal{P}$, the spaces $\mathbb{Z}/p\mathbb{Z}$ are all non-isomorphic, so it's harder to think of $n(p) = n \bmod p \in \mathbb{Z}/p\mathbb{Z}$ as a function, since its image lands in a different space ($\mathbb{Z}/p\mathbb{Z}$) for each p.

To go further with this analogy, one can ask about a notion of derivatives of the functions $n(p) = n \bmod p$. Observe for a polynomial $f(x) \in \mathbb{C}[x]$, we can always write $f(x)$ in the form

$$f(x) = a_0 + a_1(x - p_0) + a_2(x - p_0)^2 + \cdots + a_k(x - p_0)^k$$

where each $a_i \in \mathbb{C}$, and the m-th derivative at p_0 is just given by $m!a_m$. Similarly, for any $n \in \mathbb{Z}$, we can write n in the form

$$n = a_0 + a_1 p + a_2 p^2 + \cdots + a_k p^k$$

where $0 \leq a_i < p$, so the m-th derivative at p should be $m!a_m$.

Since power series are such a powerful tool in function theory, Hensel wanted to apply the techniques of power series to number theory. If we work with more general functions than polynomials in $\mathbb{C}[x]$, namely analytic functions at p_0, we can write them as power series about $x = p_0$

$$f(x) = a_0 + a_1(x - p_0) + a_2(x - p_0)^2 + \cdots \in \mathbb{C}[[x]] \ \ (a_i \in \mathbb{C}).$$

Analogously, we can consider formal power series in a prime $p \in \mathcal{P}$ given by

$$n = a_0 + a_1 p + a_2 p^2 + \cdots \in \mathbb{Z}_p \ \ (0 \leq a_i < p).$$

These formal power series are the p-adic integers $\mathbb{Z}_p$. (Note $\mathbb{Z}_p$ contains $\mathbb{Z}$ by just restrict to finite sums, i.e., "polynomials" in p.)

Even more generally than analytic functions at p_0, one often considers meromorphic functions on $\mathbb{C}$ which may have a pole (go to infinity) at p_0, e.g., the Riemann zeta function $\zeta(s)$ has a pole at $s = 1$. These functions still have a series expansion at p_0, but it needs to start with some negative power of $x - p_0$. These are called Laurent series, and explicitly are of the form

$$f(x) = a_{-k}(x-p_0)^{-k} + a_{1-k}(x-p_0)^{1-k} + \cdots + a_0 + a_1(x-p_0) + a_2(x-p_0)^2 + \cdots \in \mathbb{C}((x)) \ \ (a_i \in \mathbb{C}).$$

Analogous to this, one can take formal power series in p with coefficients between 0 and p with a finite number of negative terms

$$n = a_{-k}p^{-k} + a_{1-k}p^{1-k} + \cdots + a_0 + a_1 p + a_2 p^2 + \cdots \in \mathbb{Q}_p \ \ (0 \leq a_i < p),$$

and this will give us the p-adic numbers $\mathbb{Q}_p$. (Note $\mathbb{Q}_p$ contains all rational numbers with denominator a power of p.)

This analogy may seem a little far fetched, and you might wonder if Hensel had one too many beers at this point, but the usefulness of the p-adic numbers allows us to recognize his ideas as brilliant, as opposed to crazy talk. We summarize the analogy in the table below, though to fully appreciate it, one should be familiar with complex function theory. Nevertheless, even if you are not, it may be helpful to refer back to this table after learning more about $\mathbb{Z}_p$ and $\mathbb{Q}_p$.

We can now explain why $\mathbb{Z}_p$ and $\mathbb{Q}_p$ are called *local* objects, specifically, local rings and local fields. A power or Laurent series expansion of some function $f(x)$ around a point p_0 may only

Table 3: Complex functions vs. p-adic numbers

$\mathbb{C}$—space of points	$\mathcal{P} = \{p\}$—set of primes
$\mathbb{C}[x]$—polynomials over $\mathbb{C}$ $f(x) = a_0 + a_1(x-p_0) + \cdots a_k(x-p_0)^k$	$\mathbb{Z}$—"polynomials" over $\mathcal{P}$ $n = a_0 + a_1 p + \cdots + a_k p^k$
functions analytic at p_0 $f(x) = \sum_{i=0}^{\infty} a_i(x-p_0)^i$	$\mathbb{Z}_p$—p-adic integers $n = \sum_{i=0}^{\infty} a_i p^i$
functions meromorphic at p_0 $f(x) = \sum_{i=-k}^{\infty} a_i(x-p_0)^i$	$\mathbb{Q}_p$—p-adic numbers $n = \sum_{i=-k}^{\infty} a_i p^i$

converge nearby p_0, even though the function may be defined (as a meromorphic function) on all of $\mathbb{C}$. Since a power series is essentially meaningless outside its radius of convergence, power series in general only give *local* information about functions $f(x)$ (namely, near p_0). Similarly, the elements of $\mathbb{Z}_p$ and $\mathbb{Q}_p$ will give "local" information about the prime $p \in \mathcal{P}$.

The main references I will be using for this chapter are [Neukirch] and [Serre], as these were the books I originally learned the theory from, though most if not all of this material may be found in many books on algebraic number theory, and of course any book specifically on p-adic numbers, of which there are a few. There is also a nice analytic/topological presentation in [Ramakrishnan–Valenza], which leads into adèles.

6.1 Definitions

Fix a prime $p \in \mathbb{N}$.

Definition 6.1.1. *The set of* p**-adic integers**, *denoted* $\mathbb{Z}_p$, *are the formal power series of the form*

$$\sum_{i=0}^{\infty} a_i p^i = a_0 + a_1 p + a_2 p^2 + \cdots, \quad 0 \le a_i < p.$$

Observe the series $\sum_{i=0}^{\infty} a_i p^i$ converges if and only if it is finite, i.e., if $a_i = 0$ for all $i > k$ for some k. In this case, this finite sum is an integer, and we can get any non-negative integer this way. Accordingly we will view $\mathbb{N} \cup \{0\} \subseteq \mathbb{Z}_p$.

We can abbreviate this representation as an "infinite" base p representation of a "number:"

$$\sum_{i=0}^{\infty} a_i p^i = \cdots a_2 a_1 a_0$$

Note if the series is in fact finite, then this really is the base p representation of the corresponding integer:

$$\underbrace{a_k a_{k-1} \cdots a_2 a_1 a_0}_{\text{base } p} = a_0 + a_1 p + a_2 p^2 + \cdots + a_k p^k.$$

Naively, we can think of a p-adic integer x as just a sequence $(a_i)_0^\infty$ of numbers between 0 and p, but the p-adic numbers will have more structure than just this. We define addition and multiplication on $\mathbb{Z}_p$ by just extending the usual addition and multiplication on base p representations of positive integers.

Example 6.1.2. *Let* $x = 1 + 4 \cdot 5 + 3 \cdot 5^2, y = \sum_{i=0}^{\infty} 1 \cdot 5^i \in \mathbb{Z}_5$*, and* $z = 4 + 2 \cdot 5^2 + \sum_{i=3}^{\infty} 4 \cdot 5^i$*. We can compute the sums*

$$\begin{array}{rll} & \cdots 0000341 & x \\ + & \cdots 1111111 & y \\ \hline & \cdots 1112002 & x+y \end{array} \qquad \begin{array}{rll} & \cdots 0000341 & x \\ + & \cdots 4444104 & z \\ \hline & \cdots 0000000 & x+z \end{array} \qquad \begin{array}{rll} & \cdots 1111111 & y \\ + & \cdots 4444104 & z \\ \hline & \cdots 1110220 & y+z \end{array}$$

and we can compute a product

$$\begin{array}{rll} & \cdots 1111111 & 1 \times \cdots 1111111 \\ + & \cdots 4444440 & 40 \times \cdots 1111111 \\ + & \cdots 3333300 & 300 \times \cdots 1111111 \\ \hline & \cdots 4444401 & x \cdot y \end{array}$$

Since $x + z = \cdots 00000$*, we may identify* x *with* 396 *and* z *with* -396 *in* $\mathbb{Z}_5$*.*

It is easy to see in general, that for any $x \in \mathbb{Z}_p$, the additive inverse of x (the additive zero is of course $\cdots 00000 \in \mathbb{Z}_p$) also lies in $\mathbb{Z}_p$. Hence we may regard $\mathbb{Z} \subseteq \mathbb{Z}_p$.

Exercise 6.1. *Find the* 7*-adic representations for* -7 *and* -121*.*

Exercise 6.2. *Let* $x = 64 \in \mathbb{Z}_7$ *and* $y = 4 + 6 \cdot 7 + \sum_{i=2}^{\infty} 2 \cdot 7^i \in \mathbb{Z}_7$*. Compute* $x + y$ *and* $x \cdot y$*.*

Exercise 6.3. *What are the* p*-adic representations for* -1 *and* $\frac{1}{1-p}$ *for arbitrary* p*?*

Proposition 6.1.3. *We have that* $\mathbb{Z}_p$ *is a ring with* $\mathbb{Z}$ *as a subring.*

The proof of this is elementary—it is just base p arithmetic with infinite sequences—but we will see another justification for this from a more algebraic description below. The statement about $\mathbb{Z}$ being a subring just means that with the identification of $\mathbb{Z} \subseteq \mathbb{Z}_p$ described above, the addition and multiplication defined on $\mathbb{Z}_p$ are compatible with those on $\mathbb{Z}$, which is evident from the way we defined them. Specifically, let ϕ_n denote the natural maps

$$\cdots \longrightarrow \mathbb{Z}/p^{n+1}\mathbb{Z} \xrightarrow{\phi_n} \mathbb{Z}/p^n\mathbb{Z} \longrightarrow \cdots \xrightarrow{\phi_2} \mathbb{Z}/p^2\mathbb{Z} \xrightarrow{\phi_1} \mathbb{Z}/p\mathbb{Z}$$

Definition 6.1.4. *The* **projective limit** *(or* **inverse limit***) of* $\mathbb{Z}/p^n\mathbb{Z}$ *(with respect to* ϕ_n*) as* $n \to \infty$ *is*

$$\varprojlim \mathbb{Z}/p^n\mathbb{Z} = \left\{ (x_n) \in \prod_n \mathbb{Z}/p^n\mathbb{Z} : \phi_n(x_{n+1}) = x_n \text{ for all } n \geq 1 \right\}$$

In other words an element (x_n) of $\varprojlim \mathbb{Z}/p^n\mathbb{Z}$ is a sequence of elements $x_n \in \mathbb{Z}/p^n\mathbb{Z}$ which is compatible in the sense that $x_{n+1} \equiv x_n \bmod \mathbb{Z}/p^n\mathbb{Z}$. (Recall a direct or injective limit, written $\varinjlim$, is for when we have a sequence of objects which are successively included in each other. A projective limit is for when we have a sequences of objects which are successive quotients (or *projections*) of

each other. This is the natural way to construct an object X, in this case $\varprojlim \mathbb{Z}/p^n\mathbb{Z}$, such that each $\mathbb{Z}/p^n\mathbb{Z}$ is a quotient of $\varprojlim \mathbb{Z}/p^n\mathbb{Z}$. It's of course not the smallest space X such that every $\mathbb{Z}/p^n\mathbb{Z}$ is a quotient of X—that would be $\mathbb{Z}$—but it is certainly just as natural, if not more so. If you doubt this, try to figure out how you could *construct* $\mathbb{Z}$ from the set of $\mathbb{Z}/p^n\mathbb{Z}$'s.)

The reason for the compatibility requirements was already described in the introduction to Part III. To state this reason a little differently, the idea was that we want to use $\mathbb{Z}_p$ to study solutions to equations in $\mathbb{Z}$. If we just look at $\prod_n \mathbb{Z}/p^n\mathbb{Z}$, it's not very meaningful. Note that any element $(x_n) \in \mathbb{Z}_p$ is the limit of integers $x_n \in \mathbb{Z}$, whereas a non-compatible sequence is not a limit of integers. For instance, the sequence $(1, 2, 3, 0, 0, 0, \ldots)$ in $\prod \mathbb{Z}/p^n\mathbb{Z}$

Proposition 6.1.5. *We have a bijection*

$$\begin{aligned} \mathbb{Z}_p &\to \varprojlim \mathbb{Z}/p^n\mathbb{Z} \\ \sum_{n=0}^{\infty} a_n p^n &\mapsto (s_n)_{n=1}^{\infty} \end{aligned}$$

where s_n is the (image in $\mathbb{Z}/p^n\mathbb{Z}$) of the n-th partial sum

$$s_n = a_0 + a_1 p + a_2 p^2 + \cdots + a_{n-1} p^{n-1}.$$

From now on we use this bijection to identify $\mathbb{Z}_p$ with $\varprojlim \mathbb{Z}/p^n\mathbb{Z}$, and sometimes write our p-adic integers as formal power series expansions in p, and sometimes write them as sequences in the projective limit of the $\mathbb{Z}/p^n\mathbb{Z}$'s. There are some nice features of the projective limit approach.

First, there is a natural map from $\mathbb{Z} \to \mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z}$ given by

$$a \mapsto (a \bmod p, a \bmod p^2, a \bmod p^3, \ldots) \in \prod_n \mathbb{Z}/p^n\mathbb{Z}$$

for any $a \in \mathbb{Z}$. Further we can just define addition of and multiplication of elements of $\prod \mathbb{Z}/p^n\mathbb{Z}$. Then it is immediate that $\mathbb{Z}_p$ is a ring with $\mathbb{Z}$ as a subring, i.e., the proof of Proposition 6.1.3 is immediate. (We did not actually check that the two definitions of addition and multiplication match, but this is certainly true when we restrict to the subring $\mathbb{Z}$, since $+$ and $\cdot$ are the standard operations then. Since we can approximate any $x \in \mathbb{Z}_p$ as a limit of $x_n \in \mathbb{Z}$, a density argument shows $+$ and $\cdot$ extend in a unique way to $\mathbb{Z}_p$, so the two definitions of $+$ and $\cdot$ agree.)

Example 6.1.6. *Suppose $p = 2$. Consider $n = 75 \in \mathbb{Z}$. As a power series, we can write $n = 1 \cdot 1 + 1 \cdot 2 + 1 \cdot 2^3 + 1 \cdot 2^6$. Alternatively, we can write*

$$n = (1 \bmod 2, 3 \bmod 4, 3 \bmod 8, 11 \bmod 16, 11 \bmod 64, 75 \bmod 128, 75 \bmod 256, 75 \bmod 512, \ldots)$$

as a sequence in the projective limit of $\mathbb{Z}/2^n\mathbb{Z}$. Note in the projective limit version, it's easier to write down $-n$, namely

$$-n = (-1, -3, -3, -11, -11, -75, -75, -75, -75, \ldots).$$

The usefulness of p-adic integers is that the precisely capture the answer of when an equation is solvable mod p^n for all n.

Proposition 6.1.7. *Consider a polynomial $F(x_1, \ldots, x_k) \in \mathbb{Z}[x_1, \ldots, x_k]$. Then*

$$F(x_1, \ldots, x_k) \equiv 0 \bmod p^n$$

is solvable for all n if and only if

$$F(x_1, \ldots, x_k) = 0$$

is solvable in $\mathbb{Z}_p$.

Proof. ($\Leftarrow$) Suppose we have a $\mathbb{Z}_p$-solution $F(x,_1, \ldots, x_k) = 0$. Write $x_i = (x_{i1}, x_{i2}, x_{i3}, \ldots) \in \prod \mathbb{Z}/p^n\mathbb{Z}$. Then $F(x_{1n}, \ldots x_{kn}) \equiv 0 \bmod p^n$ for each n.

($\Rightarrow$) Let $x_{1n}, \ldots x_{kn} \in \mathbb{Z}/p^n\mathbb{Z}$ be a solution to $F(x_{1n}, \ldots, x_{kn}) \in \mathbb{Z}/p^n\mathbb{Z}$ for each n. One would like to say that $x_i = (x_{in}) \in \mathbb{Z}_p$, but the (x_{in})'s will not in general be compatible. Nevertheless, we can construct a compatible sequence of solutions.

By the (infinite) pigeonhole principle, there is a $(y_{11}, \ldots, y_{k1}) \in (\mathbb{Z}/p\mathbb{Z})^k$ such that

$$(x_{1n}, \ldots, x_{kn}) \equiv (y_{11}, \ldots, y_{k1}) \bmod p$$

for infinitely many n. Then $F(y_{11}, y_{21}, \ldots, y_{k1}) \equiv 0 \bmod p$ since any of the $(x_{1n}, \ldots, x_{kn})$ above give a solution mod p.

Similarly, there is a $(y_{12}, \ldots, y_{k2}) \in (\mathbb{Z}/p^2\mathbb{Z})^k$ such that

$$(y_{12}, \ldots, y_{k2}) \equiv (y_{11}, \ldots, y_{k1}) \bmod p$$

and

$$(x_{1n}, \ldots, x_{kn}) \equiv (y_{12}, \ldots, y_{k2}) \bmod p^2$$

for infinitely many n. Again we have $F(y_{12}, y_{22}, \ldots, y_{k2}) \equiv 0 \bmod p^2$.

We continue this ad infinitum, and set $y_i = (y_{in}) \in \prod_n \mathbb{Z}/p^n\mathbb{Z}$, so in fact each $y_i \in \mathbb{Z}_p$. Then we have $F(y_1, \ldots, y_k) = 0 \in \mathbb{Z}_p$ since this expression must be 0 in each component of $\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z}$. □

In many cases, one can reduce checking the solvabilty of an equation mod p^n to simply solvability mod p. Here is a special case.

Lemma 6.1.8. (Hensel) *Let $f(x) \in \mathbb{Z}[x]$, p a prime and $n \in \mathbb{N}$. If $p = 2$, we assume $n \geq 2$. Suppose $f(a) \equiv 0 \bmod p^n$ for some $a \in \mathbb{Z}$, but $p \nmid f'(a)$. Then for each $n \geq 1$ there is an $b \in \mathbb{Z}/p^{n+1}\mathbb{Z}$ such that $f(b) \equiv 0 \bmod p^{n+1}$ and $b \equiv a \bmod p^n$.*

Starting with $n = 1$ (or 2 if $p = 2$) applying this inductively, we see that if we have a root a of a one-variable polynomial $f(x)$ mod p (or mod 4), it lifts to a root a_n mod p^n for all n, provided $f'(a) \neq 0$. In fact, these roots a_n can be chosen to be compatible so that $(a_n) \in \prod \mathbb{Z}/p^n\mathbb{Z}$ lies in $\mathbb{Z}_p$.

Here $f'(x)$ is the formal derivative of $f(x)$, in other words the derivative as a real polynomial.

Proof. The Taylor series for $f(x)$ (regarded as a function of a real variable x) about $x = a$ is

$$f(x) = f(a) + f'(a)(x-a) + \frac{f''(a)(x-a)^2}{2!} + \cdots + \frac{f^{(d)}(a)(x-a)^d}{d!}$$

where d is the degree of $f(x)$. Suppose we take x of the form $x = a + p^n y$. Then we have

$$f(x) = f(a) + f'(a)p^n y + \frac{f''(a)p^{2n}y^2}{2!} + \cdots + \frac{f^{(d)}p^{dn}y^d}{d!}$$

By induction on j, it is easy to see for $j \geq 2$ (or $j \geq 3$ if $p = 2$) that p^{n+1} divides $\frac{p^{jn}}{j!}$. In other words, we can have

$$f(x) \equiv f(a) + f'(a)p^n y \bmod p^{n+1}.$$

Since $f(a) \equiv 0 \bmod p^n$, we can write $f(a) = a_0 p^n$ so

$$f(x) \equiv a_0 p^n + f'(a)yp^n \equiv (a_0 + f'(a)y)p^n \bmod p^{n+1}.$$

Since $f'(a)$ is nonzero mod p, we can choose $0 \leq y < p$ such that $a_0 + f'(a)y \equiv 0 \bmod p$, so $f(x) \equiv 0 \bmod p^{n+1}$ and we can take $b = x$. □

There are several ways in which one can generalize Hensel's lemma, but we will not worry about these here.

Exercise 6.4. *Let $a = a_0 + a_1 p + a_2 p^2 + \cdots \in \mathbb{Z}_p$. Show a is a unit in $\mathbb{Z}_p$ if and only if $a_0 \neq 0$.*

Exercise 6.5. *Show $\mathbb{Z}_p$ is an integral domain, i.e., there are no zero divisors.*

Exercise 6.6. *Show $x^2 = 2$ has a solution in $\mathbb{Z}_7$.*

Exercise 6.7. *Write $\frac{2}{3}$ as a 5-adic integer.*

Since $\mathbb{Z}_p$ has no zero divisors, it has a field of fractions. By Exercise 6.4, we know the only nonzero elements of $\mathbb{Z}_p$ which are not invertible (w.r.t. multiplication) are the elements divisible by p, hence the field of fractions is obtained by adjoining $\frac{1}{p}$ to $\mathbb{Z}_p$, i.e., the field of fractions of $\mathbb{Z}_p$ is $\mathbb{Z}_p[\frac{1}{p}]$. Note that we can write the elements of $\mathbb{Z}_p[\frac{1}{p}]$ uniquely in the form $p^{-d}a$ where $a \in \mathbb{Z}_p$ and $d \geq 0$. If $a = a_0 + a_1 p + a_2 p^2 + \cdots$, we can write

$$p^{-d}a = a_0 p^{-d} + a_1 p^{1-d} + a_2 p^{2-d} + \cdots = \sum_{n \geq -d} a'_n p^n \tag{6.1}$$

where $a'_n = a_{n+d}$. Thus we may define the p-adic numbers as formal series starting with some finite negative power of p (called a formal Laurent series in p).

Definition 6.1.9. *The* **p-adic numbers** *$\mathbb{Q}_p$ is the set of formal Laurent series*

$$\mathbb{Q}_p = \left\{ \sum_{n \geq -d} a_n p^n : 0 \leq a_n < p, d \geq 0 \right\}.$$

We identify $\mathbb{Q}_p$ with the field of fractions $\mathbb{Z}_p[\frac{1}{p}]$ of $\mathbb{Z}_p$ as in (6.1).

Exercise 6.8. *Write $\frac{5}{12}$ as a 2-adic number.*

6.2 Valuations

If R is an integral domain, a map $|\cdot| : R \to \mathbb{R}$ which satisfies

(i) $|x| \geq 0$ with equality if and only if $x = 0$,
(ii) $|xy| = |x||y|$, and
(iii) $|x + y| \leq |x| + |y|$

is called an **absolute value** on R. Two absolute values $|\cdot|_1$ and $|\cdot|_2$ are equivalent on R if $|\cdot|_2 = |\cdot|_1^c$ for some $c > 0$. If we have an absolute value $|\cdot|$ on R, by (ii), we know $|1 \cdot 1| = |1| = 1$. Similarly, we know $|-1|^2 = |1| = 1$, and therefore $|-x| = |x|$ for all $x \in R$.

Now a absolute value $|\cdot|$ on R makes R into a metric space with distance $d(x, y) = |x - y|$. (The fact $|-x| = |x|$ guarantees $|y-x| = |x-y|$ so the metric is symmetric, and (iii) gives the triangle inequality.) Recall that any metric space is naturally embued with a topology. Namely, a basis of open (resp. closed) neighborhoods around any point $x \in R$ is given by the set of open (resp. closed) balls $B_r(x) = \{y \in R : d(x, y) = |x - y| < r\}$ (resp. $\overline{B}_r(x) = \{y \in R : d(x, y) = |x - y| \leq r\}$) centered at x with radius $r \in \mathbb{R}$.

Ostrowski's Theorem says, that up to equivalence, every absolute value on $\mathbb{Q}$ is of one of the following types:

$|\cdot|_0$, the trivial absolute value, which is 1 on any non-zero element
$|\cdot|_\infty$, the usual absolute value on $\mathbb{R}$
$|\cdot|_p$, the **p-adic absolute value**, defined below, for any prime p.

Here the p-adic absolute value defined on $\mathbb{Q}$ is given by

$$|x| = p^{-n}$$

where $x = p^n \frac{a}{b}$ with $p \nmid a, b$. (Note any $x \in \mathbb{Q}$ can be uniquely written as $x = p^n \frac{a}{b}$ where $p \nmid a, b$ and $\frac{a}{b}$ is reduced.)

In particular, if $x \in \mathbb{Z}$ is relatively prime to p, we have $|x| = 1$. More generally, if $x \in \mathbb{Z}$, $|x| = p^{-n}$ where n is the number of times p divides x.

Note any integer $x \in \mathbb{Z}$ satisfies $|x|_p \leq 1$, and $|x|_p$ will be close to 0 if x is divisible by a high power of p. So two integers $x, y \in \mathbb{Z}$ will be close with respect to the p-adic metric if $p^n | x - y$ for a large n, i.e., if $x \equiv y \bmod p^n$ for large n.

Example 6.2.1. *Suppose $p = 2$. Then*

$$|1|_2 = 1,\ \ |2|_2 = \frac{1}{2},\ \ |3|_2 = 1,\ \ |4|_2 = \frac{1}{4},\ \ |5|_2 = 1,\ \ |6|_2 = \frac{1}{2}, \ldots$$

$$|\frac{3}{4}|_2 = 4,\ \ |\frac{12}{17}|_2 = \frac{1}{4},\ \ |\frac{57}{36}|_2 = 4.$$

With respect to $|\cdot|_2$, the closed ball $\overline{B}_{1/2}(0)$ of radius $\frac{1}{2}$ about 0 is simply all rationals (in reduced form) with even numerator. Similarly $\overline{B}_{1/4}(0)$ of radius $\frac{1}{4}$ about 0 is simply all all rationals (in reduced form) whose numerator is congruent to 0 mod 4.

Exercise 6.9. *Prove $|\cdot|_p$ is an absolute value on $\mathbb{Q}$.*

Recall, for a space R with an absolute value $|\cdot|$, one can define Cauchy sequences (x_n) in R—namely, for any $\epsilon > 0$, $|x_m - x_n| < \epsilon$ for all m, n large. One forms the completion of R with respect to $|\cdot|$ by taking equivalence classes of Cauchy sequences. Everyone knows that the completion of $\mathbb{Q}$ with respect to $|\cdot|_\infty$ is $\mathbb{R}$. On the other hand, the completion of $\mathbb{Q}$ with respect to $|\cdot|_p$ is $\mathbb{Q}_p$. To see this, observe that

$$\begin{aligned} x_0 &= a_{-d}p^{-d} + a_{1-d}p^{1-d} + \cdots + a_0 \\ x_1 &= a_{-d}p^{-d} + a_{1-d}p^{1-d} + \cdots + a_0 + a_1 p \\ x_2 &= a_{-d}p^{-d} + a_{1-d}p^{1-d} + \cdots + a_0 + a_1 p + a_2 p^2 \\ &\vdots \end{aligned}$$

gives a Cauchy sequence in $\mathbb{Q}$ with respect to $|\cdot|_p$. Precisely $|x_{n+1} - x_n|_p = |a_{n+1}p^{n+1}|_p = \frac{1}{p^{n+1}}$ (unless $x_{n+1} = x_n$, in which case it is of course 0). Hence these are Cauchy sequences, and their limits are just formal Laurent series in $\mathbb{Q}_p$. Hence $\mathbb{Q}_p$ is contained in the completion of $\mathbb{Q}$ with respect to $|\cdot|_p$. It is also not hard to see that any Cauchy sequence in $\mathbb{Q}_p$ converges (convince yourself).

Hence, the $\mathbb{Q}_p$'s are an arithmetic analogue of $\mathbb{R}$, just being completions of the absolute values on $\mathbb{Q}$ ($\mathbb{Q}$ is already complete with respect to the trivial absolute value—$\mathbb{Q}$ is totally disconnected with respect to $|\cdot|_0$). This approach to constructing $\mathbb{Q}_p$ gives both an absolute value and a topology on $\mathbb{Q}_p$, which are the most important things to understand about $\mathbb{Q}_p$.

Precisely, write any $x \in \mathbb{Q}_p$ as

$$x = a_m p^m + a_{m+1}p^{m+1} + \cdots, \ \ a_m \neq 0$$

for some $m \in \mathbb{Z}$. Then we define the **p-adic (exponential) valuation**[*] (or **ordinal**) of x to be

$$\mathrm{ord}_p(x) = m.$$

Then

$$|x|_p = p^{-m} = p^{-\mathrm{ord}_p(x)}.$$

Proposition 6.2.2. $\mathbb{Z}_p = \{x \in \mathbb{Q}_p : \mathrm{ord}_p(x) \geq 0\} = \{x \in \mathbb{Q}_p : |x|_p \leq 1\}$. *In particular $\mathbb{Z}_p$ is a closed (topologically) subring of $\mathbb{Q}_p$.*

Proof. This is clear since

$$\mathbb{Z}_p = \left\{ \sum_{n \geq 0} a_n p^n \right\},$$

so $\mathbb{Z}_p$ is precisely the set of $x \in \mathbb{Q}_p$ with $\mathrm{ord}_p(x) \geq 0$. □

Corollary 6.2.3. *The group of units $\mathbb{Z}_p^\times$ of $\mathbb{Z}_p$ is*

$$\mathbb{Z}_p^\times = \{x \in \mathbb{Q}_p : \mathrm{ord}_p(x) = 0\} = \{x \in \mathbb{Q}_p : |x|_p = 1\}.$$

[*]One often calls absolute values $|\cdot|$ valuations on a field. Thus sometimes there is a question of whether one means the exponential valuation or the absolute value by the term "valuation." For clarity, we will reserve the term valuation for exponential valuation, and always refer to our absolute values as absolute values.

Even the term exponential valuation is somewhat confusing, as the exponential valuation is really the negative logarithm $-\log_p |\cdot|$ of the absolute value. "The exponent valuation" might be clearer terminology.

Proof. This is immediate from Exercise 6.4. □

Exercise 6.10. *Let $p = 5$. Determine $\mathrm{ord}_p(x)$ and $|x|_p$ for $x = 4, 5, 10, \frac{217}{150}, \frac{60}{79}$. Describe the (open) ball of radius $\frac{1}{10}$ centered around 0 in $\mathbb{Q}_p$.*

Exercise 6.11. *Let $x \in \mathbb{Q}$ be nonzero. Show*

$$|x|_\infty \cdot \prod_p |x|_p = 1.$$

This result will be important for us later.

Despite the fact that $\mathbb{R}$ and $\mathbb{Q}_p$ are analogous in the sense that they are both completions of nontrivial absolute values on $\mathbb{Q}$, there are a couple of fundamental ways in which the p-adic absolute value and induced topology are different from the usual absolute value and topology on $\mathbb{R}$.

Definition 6.2.4. *Let $|\cdot|$ be an absolute value on a field F. If $|x + y| \leq \max\{|x|, |y|\}$, we say $|\cdot|$ is* **nonarchimedean**. *Otherwise $|\cdot|$ is* **archimedean**.

The nonarchimedean triangle inequality, $|x + y| \leq \max\{|x|, |y|\}$, is called the **strong triangle inequality**.

Proposition 6.2.5. *$|\cdot|_\infty$ is archimedean but $|\cdot|_p$ is nonarchimedean for each p.*

Proof. Everyone knows $|\cdot|_\infty$ or $\mathbb{Q}$ or $\mathbb{R}$ is archimedean—this is what we are use to and the proof is just $|1 + 1|_\infty = 2 > 1 = \max\{|1|_\infty, |1|_\infty\}$.

Now let's show $|\cdot|_p$ is nonarchimedean on $\mathbb{Q}$. Since $\mathbb{Q}$ is dense in $\mathbb{Q}_p$ ($\mathbb{Q}_p$ is the completion of $\mathbb{Q}$), this will imply $|\cdot|_p$ is nonarchimedean on $\mathbb{Q}_p$ also. Let $x, y \in \mathbb{Q}$. Write $x = p^m \frac{a}{b}$, $y = p^n \frac{c}{d}$, where a, b, c, d are relatively prime to p, and $m, n \in \mathbb{Z}$. Without loss of generality, assume $m \leq n$. Then we can write

$$x + y = p^m \left(\frac{a}{b} + p^{n-m}\frac{c}{d}\right) = p^m \frac{ad + p^{n-m}bc}{bd}.$$

Since $n \geq m$, the numerator on the right is an integer. The denominator are relatively prime to p since b, d are, though the numerator is possibly divisible by p (though only if $n = m$ and $p|(ad+bc)$). This means that we can write $x + y = p^{m+k}\frac{e}{f}$ where $e, f \in \mathbb{Z}$ are prime to p and $k \geq 0$. Thus

$$|x + y|_p = p^{-m-k} \leq p^{-m} = \max\left\{p^{-m}, p^{-n}\right\} = \max\{|x_p|, |y_p|\}$$

□

Notice that our proof shows that we actually have equality $|x + y|_p = \max\{|x|_p, |y|_p\}$ (since $k = 0$ above) except possibly in the case $|x|_p = |y|_p$.

Exercise 6.12. *Find two integers $x, y \in \mathbb{Z}$ such that*
(i) $|x|_3 = |y|_3 = \frac{1}{3}$ but $|x + y|_3 = \frac{1}{9}$.
(ii) $|x|_3 = |y|_3 = |x + y|_3 = \frac{1}{3}$.

Proposition 6.2.6. *Every ball $B_r(x)$ in $\mathbb{Q}_p$ is both open and closed. Thus the singleton sets in $\mathbb{Q}_p$ are closed.*

Using the fact that the balls are closed, one can show that $\mathbb{Q}_p$ is *totally disconnected*, i.e., its connected components are the singleton sets. However the singleton sets are not open, as that would imply $\mathbb{Q}_p$ has the discrete topology, i.e., every set would be both open and closed.

Proof. Each ball is open by definition. The following two exercises show $B_r(x)$ is also closed.

Then for any $x \in \mathbb{Q}_p$, the intersection of the closed sets $\bigcap_{r>0} B_r(x) = \{x\}$, which must be closed. □

Exercise 6.13. *Show* $B_r(x) = x + B_r(0) = \{x + y : y \in B_r(0)\}$.

Exercise 6.14. *Show that* $B_r(0)$ *is closed for any* $r \in \mathbb{R}$.

Your proof of the second exercise should make use of the fact that $|\cdot|_p$ is a *discrete* absolute value, i.e., the valuation $\mathrm{ord}_p : \mathbb{Q}_p \to \mathbb{R}$ actually has image $\mathbb{Z}$, which is a discrete subset of $\mathbb{R}$. In other words, the image of $|\cdot|_p = p^{-\mathrm{ord}_p(\cdot)}$, namely $p^{\mathbb{Z}}$, is discrete in $\mathbb{R}$ except for the limit point at 0. On the other hand, the image of the ordinary absolute value $|\cdot|_\infty$ on $\mathbb{R}$ is a *continuous* subset of $\mathbb{R}$, namely $\mathbb{R}_{\geq 0}$.

Another strange, but nice thing, about analysis on $\mathbb{Q}_p$ is that a series $\sum x_n$ converges if and only if $x_n \to 0$ in $\mathbb{Q}_p$.

While these are some very fundamental differences between $\mathbb{R}$ and $\mathbb{Q}_p$, you shouldn't feel that $\mathbb{Q}_p$ is too unnatural—just different from what you're familiar with. To see that $\mathbb{Q}_p$ isn't too strange, observe the following:

Proposition 6.2.7. $\mathbb{Q}_p$ *and* $\mathbb{R}$ *are both Hausdorff and locally compact, but not compact.*

Proof. The results for $\mathbb{R}$ should be familiar, so we will just show them for $\mathbb{Q}_p$.

Recall a space is Hausdorff if any two points can be separated by open sets. $\mathbb{Q}_p$ is Hausdorff since it is a metric space: namely if $x \neq y \in \mathbb{Q}_p$, let $d = d(x, y) = |x + y|_p$. Then for $r \leq \frac{d}{2}$, $B_r(x)$ and $B_r(y)$ are open neighborhoods of x and y which are disjoint.

Recall a Hausdorff space is locally compact if every point has a compact neighborhood. Around any $x \in \mathbb{Q}_p$, we can take the closed ball $\overline{B}_r(x)$ of radius r. This is a closed and (totally) bounded set in a complete metric space, and therefore compact. (In fact one could also take the open ball $\overline{B}_r(x)$, since we know it is closed from the previous exercise.)

Perhaps more instructively, one can show $\overline{B}_r(x)$ is sequentially compact in $\mathbb{Q}_p$, which is equivalent to compactness being a metric space. We may take a specific r if we want, say $r = 1$. Further since $\overline{B}_1(x) = x + \overline{B}_1(0)$ by the exercise above, it suffices to show $\overline{B}_1(0) = \{x \in \mathbb{Q}_p : |x|_p \leq 1\} = \mathbb{Z}_p$ is sequentially compact. If

$$\begin{aligned} x_1 &= a_{10} + a_{11}p + a_{12}p^2 + \cdots \\ x_2 &= a_{20} + a_{21}p + a_{22}p^2 + \cdots \\ x_3 &= a_{30} + a_{31}p + a_{32}p^2 + \cdots \\ &\vdots \end{aligned}$$

is a Cauchy sequence, then for any $\epsilon > 0$, there is an $N \in \mathbb{N}$ such that $|x_m - x_n|_p < \epsilon$ for all $m, n > N$. Take $\epsilon = p^{-r}$ for $r > 0$. Then $|x_m - x_n|_p < \epsilon = p^{-r}$ means $x_m \equiv x_n \bmod p^{r+1}$, i.e., the coefficients of $1, p, p^2, \ldots, p^r$ must be the same for all x_m, x_n with $m, n > N$. Let $a_0, a_1, \ldots, a_r$

denote these coefficients. We can do this for larger and larger r (note that $a_0, \ldots, a_{r-1}$ will never change) to get a sequence (a_n), and then it is clear that the above sequence converges to

$$x = a_0 + a_1 p + a_2 p^2 + \cdots \in \mathbb{Z}_p.$$

This provides a second proof of local compactness.

To see $\mathbb{Q}_p$ is not compact, observe the sequence $x_1 = p^{-1}$, $x_2 = p^{-2}$, $x_3 = p^{-3}, \ldots$ has no convergent subsequence. Geometrically, $|x_n| = p^n$, so this is a sequence of points getting further and further from 0, and the distance to 0 goes to infinity. □

We remark that $\mathbb{Q}$, with either usual subspace topology coming from $\mathbb{R}$ or the one coming from $\mathbb{Q}_p$, is a space which is not locally compact. The reason is any open neighborhood about a point is not complete—the limit points are contained in the completion of $\mathbb{Q}$ (w.r.t. to whichever absolute value we are considering), but not in $\mathbb{Q}$. (The trivial absolute value $|\cdot|_0$ induces the discrete topology on $\mathbb{Q}$, meaning single points are open sets, so it is trivially locally compact.)

The general definition of a **local field** is a locally compact field, hence we see that $\mathbb{Q}_p$ and $\mathbb{R}$ are local fields, whereas $\mathbb{Q}$ (with the usual topology) is not.

7 Quadratic forms in n variables

In order to understand quadratic forms in n variables over $\mathbb{Z}$, one is let to study quadratic forms over various rings and fields such as $\mathbb{Q}$, $\mathbb{Q}_p$, $\mathbb{R}$ and $\mathbb{Z}_p$. This is consistent with the basic premise of algebraic number theory, which was the idea that to study solutions of a Diophantine equation in $\mathbb{Z}$, it is useful study the equation over other rings.

Definition 7.0.1. *Let R be a ring. A* **quadratic form** *in n variables (or n-ary quadratic form) over R is a homogenous polynomial of degree 2 in $R[x_1, x_2, \ldots, x_n]$.*

For example $x^2 - yz$ is a ternary (3 variable) quadratic form over any ring, since the coefficients ± 1 live inside any ring R. On the other hand $x^2 - \frac{1}{2}yz$ is not a quadratic form over $\mathbb{Z}$, since $-\frac{1}{2} \notin \mathbb{Z}$, but it can be viewed as a quadratic form over $\mathbb{Q}$, $\mathbb{Z}_p$ for $p \neq 2$, $\mathbb{Q}_2$, $\mathbb{R}$ or $\mathbb{C}$ since $-\frac{1}{2}$ lies in each of those rings. In fact it can be viewed as a quadratic form over $\mathbb{Z}/n\mathbb{Z}$ for any odd n, as -2 is invertible mod n whenever n is odd.

The subject of quadratic forms is vast and central to many parts of mathematics, such as linear algebra and Lie theory, algebraic topology, and Riemannian geometry, as well as number theory. One cannot hope to cover everything about quadratic forms, even just in number theory, in a single course, let alone one or two chapters. I will describe the classification of quadratic forms over $\mathbb{Q}_p$ and $\mathbb{R}$ without proof, explain how one can use this to study forms over $\mathbb{Z}_p$ and $\mathbb{Z}$, subsequently prove Gauss' and Lagrange's theorems on sums of 3 and 4 squares, and then briefly explain some of the general theory of representation of numbers by quadratic forms. In particular, we will describe how studying forms over $\mathbb{Z}_p$ generalizes Gauss's genus theory and lead to Siegel's mass formula, which is a generalization of Dirichlet's mass formula to n-ary quadratic forms.

The main "algebraic" question about quadratic forms is how they can be classified, up to equivalence.

Definition 7.0.2. *Let $Q_1(x) = Q_1(x_1, \ldots, x_n)$ and $Q_2(x) = Q_2(x_1, \ldots, x_n)$ be n-ary quadratic forms over a ring R. We say Q_1 and Q_2 are* **equivalent over** *R denoted $Q_1 \sim Q_2$, or $Q_1 \sim_R Q_2$ when we want to specify R, if there exists*

$$\sigma \in \mathrm{GL}_n(R)$$

such that

$$Q_2(x) = Q_1(\sigma x).$$

In other words, two forms will be equivalent over R if one is obtained from the other by an invertible (linear) change of variables over R. This is the same as our definition of equivalence (not proper equivalence) for binary quadratic forms over $\mathbb{Z}$. Note that equivalent forms over R will represent the same numbers.

References for this chapter are [Serre], [Cassels], [Gerstein] and [Iwaniec].

7.1 Quadratic forms over fields

The main question about quadratic forms over fields is how they can be classified, and we start with fields because the classification over fields is much simpler than the classification over rings.

Let F be a field of characteristic not 2, and Q be an n-ary quadratic form over F. We can write

$$Q(x_1, \ldots, x_n) = \sum_{i \leq j} c_{ij} x_i x_j = \begin{pmatrix} x_1 & x_2 & \cdots & x_n \end{pmatrix} A \begin{pmatrix} x_1 & & \\ x_2 & & \\ \vdots & & x_n \end{pmatrix}$$

where A is a symmetric matrix in $M_n(F)$. Precisely let $A = (a_{ij})$ where

$$a_{ij} = \begin{cases} c_{ii} & i = j \\ \frac{1}{2} c_{ij} & i < j \\ \frac{1}{2} c_{ji} & i > j \end{cases}.$$

For example if $Q(x_1, x_2, x_3) = x_1^2 + 2x_2^2 + 3x_3^2 + 4x_1x_2 + 5x_1x_3 + 6x_2x_3$, then we may write

$$Q(x_1, x_2, x_3) = \begin{pmatrix} x_1 & x_2 & x_3 \end{pmatrix} \begin{pmatrix} 1 & 1 & \frac{5}{2} \\ 1 & 2 & 3 \\ \frac{5}{2} & 3 & 3 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}.$$

In this way, quadratic forms in n variables correspond to symmetric $n \times n$ matrices. Symmetric $n \times n$ matrices A correspond to symmetric bilinear forms $B(x, y) = x^T A y$ on F^n, hence quadratic forms $Q(x)$ are essentially the same as symmetric bilinear forms $B(x, y)$ (just set $Q(x) = B(x, x)$), which is how they arise in linear algebra and Lie groups.

We say Q is **nondegenerate** if the determinant of the associated matrix is nonzero. This essentially means that Q is not equivalent to a quadratic form in less than n variables. We will always assume this.

The first classification results for quadratic forms were in the cases $F = \mathbb{R}$ and $F = \mathbb{C}$. Let's first go through these.

Theorem 7.1.1. (Sylvester) *Let Q be be a nondegenerate quadratic form in n-variables over $\mathbb{R}$. Then Q is equivalent to $x_1^2 + \cdots + x_k^2 - x_{k+1}^2 - \cdots - x_n^2$ for some $1 \leq k \leq n$. Further no two of these are equivalent.*

Proof. Since any symmetric matrix is diagonalizable over R, up to equivalence we may assume the matrix for Q is $\mathrm{diag}(a_1, \ldots, a_n)$, i.e., Q is the *diagonal* form $a_1x_1^2 + a_2x_2^2 + \cdots a_nx_n^2$. What Q being nondegenerate means is that no $a_i = 0$ (or else the determinant of the diagonal matrix would be 0). Thus we can make the (invertible) change of variables which replaces each x_i with $\frac{1}{\sqrt{|a_i|}} x_i$. Under this transformation, Q becomes

$$Q(x_1, \ldots, x_n) = sgn(a_1)x_1^2 + sgn(a_2)x_2^2 + \cdots + sgn(a_n)x_n^2,$$

where $sgn(a_i) = \frac{a_i}{|a_i|}$ is the sign of a_i. Since we can permute the x_i's, we can in fact assume the first k a_i's are positive and the remaining a_i's are negative.

This shows any Q is equivalent to some $x_1^2 + \cdots + x_k^2 - x_{k+1}^2 - \cdots - x_n^2$. Note that the a_i's are the eigenvalues of the matrix A for Q. Sylvester showed that the number of positive and negative eigenvalues of $S^T AS$ is the same for any invertible matrix S. (This known as Sylvester's law of inertia.) This proves the classification theorem. □

If we think back to the notion of definite and indefinite forms, only two forms (up to equivalence) are definite (represent only positive or negative values), namely the positive definite form $x_1^2+\cdots+x_n^2$ and the negative definite form $-x_1^2-\cdots-x_n^2$.

Contrast what happens over $\mathbb{R}$ with what happens over $\mathbb{Q}$.

Theorem 7.1.2. *Let Q be a nondegenerate quadratic form in n-variables over $\mathbb{C}$. Then Q is equivalent to $x_1^2+x_2^2+\cdots x_n^2$.*

Proof. As in the real case, we may assume Q is of the form $a_1x_1^2+\cdots+a_nx_n^2$. But now $\sqrt{a_i}\in\mathbb{C}$ for all i, so making the change of variables $\frac{1}{\sqrt{a_i}}x_i$, proves the theorem. □

Over $\mathbb{C}$, there is no real notion of definite or indefinite since squares may be positive or negative. In any case, there is only one form over $\mathbb{C}$, up to equivalence.

Note that both over $\mathbb{R}$ and $\mathbb{C}$, the classification of quadratic forms is much simpler than the classification of binary quadratic forms over $\mathbb{Z}$. For one, there are infinitely many equivalence classes of binary quadratic forms (with no restriction on the discriminant), and even for a fixed discriminant the structure is rather complicated (though surprisingly beautiful, in that we have Gauss's composition law) In particular, while the discriminant is an invariant of the form over $\mathbb{Z}$, this is not true over $\mathbb{R}$ or $\mathbb{C}$. Over $\mathbb{R}$, there is a single invariant of a quadratic form, called the *signature* of the form, which is the number of $+1$ coefficients minus the number of -1 coefficients, assuming the form is written as $x_1^2+\cdots+x_k^2-x_{k+1}^2-\cdots-x_n^2$.

In general, for a quadratic form Q over any field F (characteristic not 2), we may make a change of variables to write Q as a diagonal form

$$Q(x_1,\ldots,x_n)=a_1x_1^2+a_2x_2^2+\cdots+a_nx_n^2.$$

Then the question of classification becomes simply a question of whether each $\sqrt{a_i}\in F$. If so, then we can make a change of variables $x_i\mapsto\frac{1}{\sqrt{a_i}}x_i$ to see Q is equivalent to $x_1^2+\cdots+x_n^2$. In particular, if F is algebraically closed, $\sqrt{a_i}$ is always in F, so there is only one (nondegenerate) quadratic form in n-variables up to equivalence.

In light of the above, the following result should be fairly evident.

Proposition 7.1.3. *Any n-ary form Q over F is equivalent to*

$$a_1x_1^2+a_2x_2^2+\cdots+a_nx_n^2,$$

where each a_i lies in a set of representatives for $F^\times/F^{\times(2)}$. Here $F^{\times(2)}$ denotes the subgroup of squares of $F^\times$.

One can show there are three invariants for a quadratic form $Q=a_1x_1^2+\cdots a_nx_n^2$, the **rank** (or number of variables) n, the **discriminant** $\operatorname{disc}(Q)=a_1a_2\cdots a_n$, and the **Hasse invariant** $\epsilon(Q)=\prod_{i<j}\left(\frac{a_i,a_j}{F}\right)=\pm1$. Here $\left(\frac{a,b}{F}\right)$ is the **Hilbert symbol** which is defined to be $+1$ if $ax^2+by^2=z^2$ has a nonzero solution over F and -1 otherwise.

Proposition 7.1.4. *For p odd, a set of representatives for $\mathbb{Q}_p^\times/\mathbb{Q}_p^{\times(2)}$ is $\{1,p,u,up\}$ where $u\in\mathbb{Z}$ satisfies $\left(\frac{u}{p}\right)=-1$. This quotient group is isomorphic to $C_2\times C_2$.*

Proposition 7.1.5. *A set of representatives for $\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times(2)}$ is $\{\pm1,\pm2,\pm5,\pm10\}$. This quotient group is isomorphic to C_2^3.*

Theorem 7.1.6. *Let Q_1 and Q_2 be quadratic forms over $\mathbb{Q}_p$. They are equivalent if and only if they have the same rank, discriminant and Hasse invariant.*

See [Serre] for proofs.

Things are much more complicated over $\mathbb{Q}$ since the quotient group $\mathbb{Q}^\times/\mathbb{Q}^{\times(2)}$ is infinite. For instance, the primes $2, 3, 5, 7, 11, 13, \ldots$ are all distinct in $\mathbb{Q}^\times/\mathbb{Q}^{\times(2)}$, as can be easily checked by the exercise below.

Exercise 7.1. *Suppose p and q are two distinct primes p and q. Show p and q do not differ by a rational square. Consequently $\mathbb{Q}^\times/\mathbb{Q}^{\times(2)}$ is infinite.*

The way to study forms over the *global field* $\mathbb{Q}$ is by reducing the question to studying forms over the *local fields* $\mathbb{Q}_p$. To be a little more precise, the philosophy is that we can study problems over $\mathbb{Q}$ by studying the associated problems in *all* of its completions (w.r.t. nontrivial absolute values), in other words in each $\mathbb{Q}_p$ and $\mathbb{R}$. This notion is called **Hasse's local-to-global principle**.

The simplest precise form of the local-to-global principle is the following theorem of Hasse and Minkowski. For a quadratic form Q over a field F, we always have $Q(0) = 0$, and the simplest representation question is whether $Q(x) = 0$ for any nonzero $x \in F^n$. If $Q(x) = 0$ for some $0 \neq x \in F^n$, we say Q **represents** 0 (nontrivially), or Q is **isotropic**.

Theorem 7.1.7. (Hasse–Minkowski) *Let Q be a quadratic form over $\mathbb{Q}$. Then Q represents 0 (nontrivially) over $\mathbb{Q}$ if and only if it does over $\mathbb{Q}_p$ for each p and over $\mathbb{R}$.*

We remark that this statement makes sense because any form over $\mathbb{Q}$ can be regarded as a form over $\mathbb{Q}_p$ or $\mathbb{R}$ since $\mathbb{Q} \subseteq \mathbb{Q}_p$ and $\mathbb{Q} \subseteq \mathbb{R}$.

Proof. (Sketch) Let Q be a quadratic form of rank n over $\mathbb{Q}$. By the above we can write $Q(x_1, \ldots, x_n) = a_1x_1^2 + a_2x_2^2 + \cdots + a_nx_n^2$ with each $a_i \in \mathbb{Q}$. Since Q represents 0 (over $\mathbb{Q}$, $\mathbb{Q}_p$ or $\mathbb{R}$) if and only if the form $\frac{1}{a_1}Q$ does, we may replace Q with $\frac{1}{a_1}Q$ to assume that $a_1 = 1$. Also, by replacing x_i with an appropriate multiple c_ix_i, we may assume each $a_i \in \mathbb{Z}$ and squarefree. Further it is clear that if Q represents 0 over $\mathbb{Q}$, it also will over the completions $\mathbb{Q}_p$ and $\mathbb{R}$. Hence it suffice to show that Q represents 0 over $\mathbb{Q}$ if it does over each $\mathbb{Q}_p$ and $\mathbb{R}$. We consider various cases.

$n = 1$. If $n = 1$, then we have $Q(x_1) = x_1^2$, so Q does not represent 0 (nontrivially) over any field, and there is nothing to prove.

$n = 2$. If $n = 2$, write $Q(x, y) = x^2 - ay^2$ (here $a = -a_2$). Then Q represents 0 over a field F if and only if $x^2 = ay^2$ has a solution in F, i.e., if and only if $a = (\frac{x}{y})^2$ has a solution in F, i.e., if and only if a is a square in F. So we want to prove that if a is a square in $\mathbb{Q}_p$ and a is a square in $\mathbb{R}$, then a is a square in $\mathbb{Q}$. The condition that $a \in \mathbb{R}^{\times(2)}$ just means $a > 0$. Note that $a \in \mathbb{Q}_p^{\times(2)}$ means that $\mathrm{ord}_p(a)$ is even for each p (since $a = b^2$ implies $\mathrm{ord}_p(a) = 2\mathrm{ord}_p(b)$).

Write $a = \frac{r}{s}$ where $r, s \in \mathbb{Z}$ in reduced form. If p is a prime dividing r or s, then $\mathrm{ord}_p(a)$ even means that p occurs to an even power in the prime factorization of r and s (it will be positive for one of r and s, and 0 for the other). Hence $\frac{r}{s} = a$ is a square in $\mathbb{Q}$.

$n \geq 3$. One can treat the cases $n = 3$ (due to Legendre) and $n = 4$ separately, and then prove the theorem for $n \geq 5$ by induction on n by breaking the form up into the sum of a binary form with a form of rank $n - 2$. This is done with fairly elementary p-adic analysis. □

Now one might wonder if the Hasse–Minkowski theory unnecessarily complicates the problem by requiring us to check things over infinitely many fields $\mathbb{Q}_p$. In practice however, one only needs things for finitely many primes. This can even be seen in our proof of the $n = 2$ case: to check if $a = \frac{r}{s}$ is a square in $\mathbb{Q}$, it suffices to check it over $\mathbb{R}$ and $\mathbb{Q}_p$ for just the primes p dividing r and s.

One reason representing 0 is a basic question is the following.

Proposition 7.1.8. *Suppose Q represents 0 over F. Then Q is* **universal**, *i.e., Q represents every element of F.*

The proof is fairly simple: A nontrivial representation $Q(x_1, \dots, x_n) = 0$ implies Q "contains" a product of linear forms. For example, $x_1^2 + x_2^2 - x_3^2 = x_1^2 + (x_2 + x_3)(x_2 - x_3) = x_1^2 + yz$ where $y = x_2 + x_3$, $z = x_2 - x_3$. Setting $x_1 = 0$, $y = 1$ and letting z vary, we see this form is universal. The general argument is similar, but we will not go through the details—in any event, this example is essentially the case we will be considering in the next section.

In fact, the Hasse–Minkowski theorem really contains information about a form representing any $a \in \mathbb{Q}$.

Exercise 7.2. *Consider a form $Q(x_1, \dots, x_n)$ over $\mathbb{Q}$ and set $Q_a(x_1, \dots, x_{n+1}) = Q(x_1, \dots, x_n) - ax_{n+1}^2$ for $a \in \mathbb{Q}$. Show Q represents a if and only if Q_a represents 0. (Hint: use Proposition 7.1.8.)*

Exercise 7.3. *Let Q be a quadratic form over $\mathbb{Q}$. Deduce from Hasse–Minkowski that Q represents some $a \in \mathbb{Q}$ over $\mathbb{Q}$ if and only if it does over $\mathbb{R}$ and each $\mathbb{Q}_p$. (Hint: use the previous exercise.)*

One can show that *any* quadratic form of rank ≥ 4 over $\mathbb{Q}_p$ represents all p-adic numbers. Then from previous exercise, one can deduce that for any Q of rank ≥ 4, Q represents $a \in \mathbb{Q}$ over $\mathbb{Q}$ if and only if it does over $\mathbb{R}$. With this you should easily be able to convince yourself that form of rank ≥ 4 over $\mathbb{Q}$ either represents (i) all nonnegative rationals, (ii) all nonpositive rationals, or (iii) all rationals, just based on the signs of the coefficients of the form.

This suggests the following phenonemon—it is easy to determine what numbers are represented by a form Q with rank ≥ 4 (at least over $\mathbb{Q}$), and it is also fairly easy to determine what numbers are represented by a form of rank 2 (or 1), but the case of rank 3 is considerably more subtle. This phenomenon persists when restricting to forms over $\mathbb{Z}$ as well. This notion of some problems being easy in low dimensions and high dimensions, but very subtle in middle (often 3 or 4) dimensions, occurs in other areas of mathematics also, a famous example being the classification of n-manifolds, which is "simple" in dimensions ≤ 2 or ≥ 5.

7.2 Sums of Squares

Ideally, one would like to use the Hasse–Minkowski theorem to reduce representation problems over $\mathbb{Z}$ to problems over $\mathbb{Z}_p$. The general situation is rather complicated, so for simplicity and completeness, we will show how to apply these ideas to the cases of sums of three and four squares, following [Serre] and [Gerstein].

Let's start with the sum of 3 squares over a field F. Recall the Hilbert symbol $\left(\frac{a,b}{F}\right)$ is 1 if $ax^2 + by^2 - z^2$ represents 0 and is -1 else. Hence $x^2 + y^2 + z^2$ represents 0 over F if and only if $\left(\frac{-1,-1}{F}\right) = 1$. We claim that this is the case if $F = \mathbb{Q}_p$, p odd. One can treat specific cases via simple applications of quadratic reciprocity and Hensel's lemma.

Exercise 7.4. *Suppose $p \equiv 1 \bmod 4$. Show -1 is a square in $\mathbb{Z}_p$. Deduce $x^2 + y^2 + z^2$ represents 0 over $\mathbb{Q}_p$ (in fact $\mathbb{Z}_p$), i.e., $\left(\frac{-1,-1}{\mathbb{Q}_p}\right) = 1$.*

Exercise 7.5. *Suppose $p \equiv 3 \bmod 8$. Show -2 is a square in $\mathbb{Z}_p$. Deduce $x^2+y^2+z^2$ represents 0 over $\mathbb{Q}_p$ (in fact $\mathbb{Z}_p$), i.e., $\left(\frac{-1,-1}{\mathbb{Q}_p}\right) = 1$.*

For the general case (well, really we only need it for $p \equiv 7 \bmod 8$ after the above exercises) we will appeal to the following formula.

Proposition 7.2.1. *Suppose p is odd, $a, b \in \mathbb{Q}_p$, and write $a = p^\alpha u$, $b = p^\beta v$, where u, v are units of $\mathbb{Z}_p$. Then*

$$\left(\frac{a,b}{\mathbb{Q}_p}\right) = (-1)^{\alpha\beta\frac{p-1}{2}} \left(\frac{u}{p}\right)^\beta \left(\frac{v}{p}\right)^\alpha.$$

(One extends the Legendre symbol $\left(\frac{\cdot}{p}\right)$ to $\mathbb{Z}_p^\times$ by putting $\left(\frac{a}{p}\right) = \left(\frac{a_0}{p}\right)$ for $a = a_0 + a_1 p + a_2 p^2 + \cdots$. However, we will only apply the above formula in the case where $a, b \in \mathbb{Z}$.)

Exercise 7.6. *Let p be odd. Compute $\left(\frac{-1,-1}{\mathbb{Q}_p}\right)$. Deduce that $x^2+y^2+z^2$ is universal over $\mathbb{Q}_p$.*

Lemma 7.2.2. *Let $\alpha \in \mathbb{Q}^\times$. Then α is a sum of 3 rational squares if and only if $\alpha > 0$ and $-\alpha \in \mathbb{Q}_2^{\times(2)}$.*

Proof. By Hasse–Minkowski, α is represented by $Q = x^2+y^2+z^2$ over $\mathbb{Q}$ if and only if α is represented by Q over each $\mathbb{Q}_p$ and $\mathbb{R}$. The representation condition over $\mathbb{R}$ is equivalent to $\alpha > 0$. By the above exercise, we know $x^2+y^2+z^2$ represents all α in $\mathbb{Q}_p$ for p odd, so it suffices to show $x^2+y^2+z^2$ represents α in $\mathbb{Q}_2$ if and only if $-\alpha \notin \mathbb{Q}_2^{\times(2)}$.

By an earlier exercise $x^2+y^2+z^2$ represents α in $\mathbb{Q}_2$ if and only if $x^2+y^2+z^2-\alpha w^2$ represents 0. One can show a rank 4 quadratic form $a_1x^2+a_2y^2+a_3z^2+a_4w^2$ over $\mathbb{Q}_p$ does *not* represent 0 if and only if the discriminant is a square and the Hasse symbol $\epsilon = \prod_{i<j}\left(\frac{a_i,a_j}{\mathbb{Q}_p}\right) = -\left(\frac{-1,-1}{\mathbb{Q}_p}\right)$. When $p=2$, we have $\left(\frac{-1,-1}{\mathbb{Q}_p}\right) = -1$ so this Hasse symbol condition holds if the discriminant $a_1a_2a_3a_4$ is a square, which in our case is just $-\alpha$. This proves the lemma. □

To pass to representations over $\mathbb{Z}$, we need the following.

Lemma 7.2.3. (Davenport–Cassels) *Let Q be a positive definite quadratic form of rank n over $\mathbb{Q}$ given by a symmetric matrix $A = (a_{ij}) \in M_n(\mathbb{Z})$. Suppose*

(DCH) for all $x \in \mathbb{Q}^n$, there is a $y \in \mathbb{Z}^n$ such that $Q(x-y) < 1$.

Then if Q represents an integer m over $\mathbb{Q}$, it does over $\mathbb{Z}$.

As in the binary case, positive definite means $Q(x) \geq 0$ with equality only if $x = 0 \in \mathbb{Q}^n$.

Proof. Write $\langle u, v\rangle = u^T A v$ for $u, v \in \mathbb{Q}^n$, so that $\langle v, v\rangle = Q(v)$.

Suppose $Q(v) = \langle v, v\rangle = m$ where $v \in \mathbb{Q}^n$. Multiplying through by denominators in $v = (v_1, \ldots, v_n)$, there is a multiple $x = tv \in \mathbb{Z}^n$ of v (for some $t \in \mathbb{Z}$) such that $Q(x) = Q(tv) = t^2 m$. Choose v and t such that t is minimal. We want to show $t = 1$.

(DCH) tells us there is a $y \in \mathbb{Z}^n$ such that $z = \frac{x}{t} - y \in \mathbb{Q}^n$ satisfies $Q(z) = \langle z, z\rangle < 1$. If $\langle z, z\rangle = 0$, then $z = 0$ (since Q is positive definite), so $\frac{x}{t} = y \in \mathbb{Z}^n$ and $t = 1$.

Now suppose $\langle z, z\rangle \neq 0$. Set

$$a = \langle y, y\rangle - m,\ b = 2(mt - \langle x, y\rangle),\ t' = at + b,\ x' = ax + by.$$

Then $a, b, t' \in \mathbb{Z}$, and it is easy to compute that $\langle x', x'\rangle = mt'^2$ and $tt' = t^2\langle z, z\rangle$. Consequently $t' = t\langle z, z\rangle < t$, contradicting the minimality of t. □

Theorem 7.2.4. (Gauss) *A positive integer n is a sum of 3 squares if and only if $n \neq 4^j(8k+7)$.*

Proof. Let $x = (x_1, x_2, x_3) \in \mathbb{Q}^3$. Choose $y = (y_1, y_2, y_3) \in \mathbb{Z}^3$ such that $|x_i - y_i| \leq \frac{1}{2}$. Then

$$Q(x-y) = (x_1-y_1)^2 + (x_2-y_2)^2 + (x_3-y^3)^2 \leq \frac{1}{4} + \frac{1}{4} + \frac{1}{4} < 1,$$

i.e., the form $x^2 + y^2 + z^2$ satisfies (DCH). By the Davenport–Cassels Lemma and the previous lemma, n is a sum of 3 squares if and only if $-n \in \mathbb{Q}_2^{\times(2)}$. Since $-n \in \mathbb{Z} \subseteq \mathbb{Z}_2$, this is equivalent to $-n$ is a square in $\mathbb{Z}_2$ (since $x^2 = -n$ in $\mathbb{Q}_2$ implies $|x^2|_2 = |-n|_2 \leq 1$ which implies $|x|_2 \leq 1$).

Write

$$-n = 2^e(1 + a_1 \cdot 2 + a_2 \cdot 2^2 + \cdots) \in \mathbb{Z}_2.$$

If n is a square e must be even, and then n is a square in $\mathbb{Z}_2$ if and only if

$$\frac{-n}{2^e} = 1 + a_1 \cdot 2 + a_2 \cdot 2^2 + \cdots$$

is. Using a slight generalization of Hensel's lemma, we see $a \in \mathbb{Z}_2^\times$ is a square if and only if it is mod 8, i.e., if and only if $a \equiv 1 \bmod 8$. Hence $-n$ is a square in $\mathbb{Q}_p$ if and only if $-n = 4^j(8m+1)$, i.e., if and only if $n = 4^j(8k+7)$. □

Corollary 7.2.5. (Lagrange) *Every positive integer n is a sum of 4 squares.*

Proof. If $n \neq 4^j(8k+7)$, then it is a sum of 4 squares since it is a sum of 3 squares. If $n = 4^j(8k+7)$ then $m = 8k+6$ is the sum of 3 squares so $8k+7 = m + 1^2$ is the sum of 4 squares, whence n is also. □

We remark that we can't use the Davenport–Cassels Lemma for sums of 4 squares because (DCH) fails.

Corollary 7.2.6. (Gauss) *Ever positive integer n is a sum of 3 triangular numbers.*

(Recall a triangular number is one of the form $\frac{m(m+1)}{2}$.)

Proof. Applying the 3 squares theorem to $8n+3$, we see $8n+3 = x^2+y^2+z^2$ for some $x, y, z \in \mathbb{Z}$. But since the only squares mod 8 are $0, 1, 4$, we must have $x^2 \equiv y^2 \equiv z^2 \equiv 1 \bmod 8$, so x, y and z are odd. Write $x = 2a+1$, $y = 2b+1$, $z = 2c+1$. Then

$$\frac{a(a+1)}{2} + \frac{b(b+1)}{2} + \frac{c(c+1)}{2} = \frac{1}{8}\left((2a+1)^2 + (2b+1)^2 + (2c+1)^2 - 3\right) = \frac{1}{8}(8n+3-3) = n.$$

□

7.3 Siegel's mass formula

Here we give a brief summary of Siegel's mass formula, following [Iwaniec].

Let Q be a positive definite quadratic form over $\mathbb{Z}$ of rank r. The **genus** of Q is the set forms over $\mathbb{Z}$ which are equivalent to Q over each $\mathbb{Q}_p$ and $\mathbb{R}$. The group of **automorphs** $\mathrm{Aut}(Q)$ of Q is the set of $\sigma \in \mathrm{GL}_r(\mathbb{Z})$ such that $\sigma^T A \sigma = A$, where A is the symmetric matrix associated to Q. We say solutions $Q(x) = n$ and $Q(y) = n$ are equivalent if $y = \sigma x$ for some automorph σ of Q.

The number of automorphs $\mathrm{Aut}(Q)$ in general can be different for different forms in the same genus. Let $gen(Q)$ denote the set of equivalence classes of forms in the genus of Q. The **genus mass** of Q is

$$w(Q) = \frac{1}{|\mathrm{Aut}(Q)| m(gen(Q))}$$

where

$$m(gen(Q)) = \sum_{Q_j \in gen(Q)} \frac{1}{|\mathrm{Aut}(Q_j)|}.$$

The total mass is

$$\sum_{Q_j \in gen(Q)} w(Q_j) = 1.$$

Then the number of ways n can be represented by some form in the genus of Q is

$$r_{gen(Q)}(n) = \sum_{Q_j \in gen(Q)} w(Q_j) r_{Q_j}(n).$$

Siegel's mass formula then states

$$r_{gen(Q)}(n) = \prod_p \delta_p(n, Q) \cdot \delta_\infty(n, Q)$$

where $\delta_p(n, Q)$ is the "density" of solutions $Q(x) = n$ in $\mathbb{Z}_p^r$. When $r = 2$ this is essentially Dirichlet's mass formula.

So as in the binary case, when we have one class per genus (e.g., for sums of 3 or 4 squares), one knows the individual $r_Q(n)$'s. But this only happens finitely often, and in general it is hard to separate out the information about individual forms Q.

To attempt to do this, one approach is to associate to Q a **modular form**

$$\Theta_Q(z) = \sum_{n \geq 0} r_Q(n) e^{2\pi i n z},$$

which is a meromorphic function. Notice the $r_Q(n)$'s are Fourier coefficients for Θ_Q. Consequently, one can apply analytic methods to study the $r_Q(n)$'s and obtain beautiful formulas in many cases. Iwaniec uses analytic number theory to show an *asymptotic* formula for $r_Q(n)$ (as $n \to \infty$) for *individual* Q's.

We will not introduce modular forms or discuss other results in this direction here, but the study of quadratic forms and modular forms is a rich area, and there are many interesting open questions still out there.

8 Adèles

Adèles and idèles were introduced in the early 20th century as an approach to class field theory, which may be viewed as a vast generalization of quadratic reciprocity. First we introduce the notion of adèles $\mathbb{A}_{\mathbb{Q}}$ and idèles $\mathbb{A}_{\mathbb{Q}}^{\times}$ over $\mathbb{Q}$. Then we will discuss $\mathfrak{p}$-adic numbers for arbitrary number fields K, and use these to define the adèles $\mathbb{A}_K$ and idèles $\mathbb{A}_K^{\times}$ of a number field K. One defines the quotient group $\mathbb{A}_K^{\times}/K^{\times}$ to be the *idèle class group* of K. Our goal will be to show that this is essentially the ideal class group of K, and then use this to describe some of the main results of class field theory.

8.1 $\mathbb{A}_{\mathbb{Q}}$

The **adèles** of $\mathbb{Q}$ are the ring

$$\mathbb{A}_{\mathbb{Q}} = \left\{ (\alpha_2, \alpha_3, \alpha_5, \ldots; \alpha_\infty) \in \prod_p \mathbb{Q}_p \times \mathbb{R} : \alpha_p \in \mathbb{Z}_p \text{ for a.a. } p \right\}.$$

Here "for a.a. (almost all)" p means for all but finitely many primes p.

Exercise 8.1. *With addition and multiplication defined component-wise, show $\mathbb{A}_{\mathbb{Q}}$ is a ring.*

Note that $\mathbb{A}_{\mathbb{Q}}$ puts together the information one gets from all the completions of $\mathbb{Q}$, but the whole direct product $\prod \mathbb{Q}_p \times \mathbb{R}$ is too large to work with by itself, so we only consider sequences where almost all terms are p-adic integers. This is analogous to an infinite direct sum of vector spaces V_i. Specifically, $\bigoplus_{i=1}^{\infty} V_i = \{(v_i) \in \prod V_i : v_i = 0 \text{ for a.a. } i\}$. For instance if each $V_i = \mathbb{R}$, then a basis for $\bigoplus V_i$ is $\{e_i\}$ where $e_i = (0, \ldots, 0, 1, 0, \ldots)$ is the vector with a 1 in the i-th coordinate and 0's elsewhere. If one removes the "for almost all i" condition, then $(1, 1, 1, \ldots) = e_1 + e_2 + e_3 + \cdots$ would be in the direct sum, but this is not a finite linear combination of basis elements.

Let us simplify now our notation slightly.

We call a nontrivial absolute value on $\mathbb{Q}$ a **place** of $\mathbb{Q}$. Hence the places of $\mathbb{Q}$ are $|\cdot|_v$ where v is either a prime p or $v = \infty$. The places $v = p$ are called **finite places**, and the place $v = \infty$ is called the **real place** or **infinite place**.[†] Let $\mathbb{Q}_v$ denote the completion of $\mathbb{Q}$ w.r.t. $|\cdot|_v$, so $\mathbb{Q}_p$ still denotes $\mathbb{Q}_p$ and now $\mathbb{Q}_\infty$ denotes $\mathbb{R}$. Let $\mathbb{Z}_v$ denote the set $\{x_v \in \mathbb{Q}_v : |x_v|_v \leq 1\}$, so that $\mathbb{Z}_v = \mathbb{Z}_p$ if $v = p$ and $\mathbb{Z}_\infty = [-1, 1]$. While $\mathbb{Z}_p$ is the completion of $\mathbb{Z}$ in each $\mathbb{Q}_p$, $\mathbb{Z}_\infty$ admittedly has little to do with $\mathbb{Z}$. Nevertheless this notation is convenient. We also remark that $\mathbb{Z}_v$ is compact inside each $\mathbb{Q}_v$. In fact when $v < \infty$, i.e., $v = p$, $\mathbb{Z}_v$ is open in $\mathbb{Q}_v$.

Now we can denote the adèles as

$$\mathbb{A}_{\mathbb{Q}} = \left\{ (\alpha_v) \in \prod \mathbb{Q}_v : \alpha_v \in \mathbb{Z}_v \text{ for a.a. } v \right\}.$$

While the condition $\alpha_v \in \mathbb{Z}_v$ for a.a. v may at first glance look stronger than the condition $\alpha_p \in \mathbb{Z}_p$ for a.a. p because $v = \infty$ is allowed, thinking about it for a second shows they are equivalent. (Think about it for a second: $\alpha \in \mathbb{A}_{\mathbb{Q}}$ means the local components α_v can lie outside of $\mathbb{Z}_v$ only for v in some finite set S of places (S of course depends on α— it is like the "support" of an element

[†]It is standard to call places primes and still use the letter p, since they correspond to the usual primes and infinity. Then the ordinary primes are called finite primes, and denoted by $p < \infty$, and the infinite place is called the infinite prime $p = \infty$.

y in the infinite direct sum $R^\infty = \bigoplus_{i=1}^\infty \mathbb{R}$, which is the set of i for which the i-th component of y is nonzero. We can always add the place ∞ to S if it is not included, and S will still be finite, meaning we have the condition α_v can lie outside of $\mathbb{Z}_v$ for $v \in S \cup \{\infty\}$.)

The following examples will tell us a little bit about $\mathbb{A}_\mathbb{Q}$.

Example 8.1.1. *Let $x = \frac{a}{b} \in \mathbb{Q}$ with $a, b \in \mathbb{Z}$. Let $\alpha = (x, x, x, \ldots)$. Note that $\frac{1}{b} \in \mathbb{Z}_p$ for any p s.t. $p \nmid b$. Hence $x = \frac{a}{b} \in \mathbb{Z}_p$ for any p s.t. $p \nmid b$, i.e., $x = \alpha_v \in \mathbb{Z}_v$ for almost all v. Thus $\alpha \in \mathbb{A}_\mathbb{Q}$.*

Hence we have an (injective) ring homomorphism from $\mathbb{Q} \to \mathbb{A}_\mathbb{Q}$ given by

$$x \mapsto (x, x, x, \ldots).$$

So the additive identity of $\mathbb{A}_\mathbb{Q}$ is $(0, 0, 0, \ldots)$ and the multiplicative identity of $\mathbb{A}_\mathbb{Q}$ is $1 = (1, 1, 1, \ldots)$. We will typically identify elements of $\mathbb{Q}$ with their image in $\mathbb{A}_\mathbb{Q}$ under this map.

Example 8.1.2. *Let $\alpha = (1, 0, 0, 0, \ldots), \beta = (0, 1, 1, 1, \ldots)$. Since each component $\alpha_v, \beta_v \in \mathbb{Z}_v$ for all v, we have $\alpha, \beta \in \mathbb{A}_\mathbb{Q}$. Then $\alpha\beta = (0, 0, 0, \ldots) = 0 \in \mathbb{A}_\mathbb{Q}$. In other words, α and β are zero divisors in $\mathbb{A}_\mathbb{Q}$, so $\mathbb{A}_\mathbb{Q}$ is not an integral domain.*

Proposition 8.1.3. *For $\alpha = (\alpha_v) \in \mathbb{A}_\mathbb{Q}$, let $|\alpha| = \prod_v |\alpha_v|_v$. Then $|\cdot| : \mathbb{A}_\mathbb{Q} \to \mathbb{R}$ satisfies*
(i) $|\alpha| \geq 0$
(ii) $|\alpha\beta| = |\alpha||\beta|$

Proof. First note that $|\alpha|$ is well defined: since $\alpha = (\alpha_v) \in \mathbb{A}_\mathbb{Q}$ satisfies $\alpha_v \in \mathbb{Z}_v$ for almost all v, we have $|\alpha_v|_v \leq 1$ for almost all v, and therefore the infinite product $|\alpha| = \prod_v |\alpha|_v$ converges. It is clear that $|\alpha| \geq 0$.

Further (ii) follows immediately because it does for each $|\alpha|_v$. □

Example 8.1.4. *Taking $\alpha = (1, 0, 0, 0, \ldots)$ from the previous example, we see $|\alpha| = |1|_2 \prod_{v \neq 2} |0|_v = 0$, so $|\cdot|$ can be zero on nonzero elements. Therefore, $|\cdot|$ cannot technically be an absolute value. Of course, our earlier definition of absolute values was only for integral domains because any multiplicative homomorphism $|\cdot| : R \to \mathbb{R}$ for a non-integral domain must be 0 on some zero divisors. ($\alpha\beta = 0$ implies $|\alpha||\beta| = |\alpha\beta| = 0$ so either $|\alpha|$ or $|\beta|$ is 0.)*

However we can even find $\alpha \in \mathbb{A}_\mathbb{Q}$ which is not a zero divisor such that $|\alpha| = 0$. Namely consider $\alpha = (\alpha_v)$ where $\alpha_p = p$ and $\alpha_\infty = 1$. Each component $\alpha_v \in \mathbb{Z}_v$ so $\alpha \in \mathbb{A}_\mathbb{Q}$, but

$$\alpha = \prod_p |p|_p \cdot |1|_\infty = \prod_p \frac{1}{p} = 0.$$

In fact, another crucial property of absolute values fails also, namely the triangle inequality.

Exercise 8.2. *Find $\alpha, \beta \in \mathbb{A}_\mathbb{Q}$ such that $|\alpha + \beta| > |\alpha| + |\beta|$.*

Example 8.1.5. *Let $x \in \mathbb{Q}$ and $\alpha = (x, x, x, \ldots)$. If $x = 0$, then $|\alpha| = 0$. Otherwise $|\alpha| = 1$ by Exercise 6.11.*

The fact that $\mathbb{A}_\mathbb{Q}$ is not an integral domain makes it a little hard to work with, but the **idèles** $\mathbb{A}_\mathbb{Q}^\times = \{\alpha \in \mathbb{A}_\mathbb{Q} : \alpha \text{ invertible}\}$, namely the multiplicative subgroup of $\mathbb{A}_\mathbb{Q}$, become a nice space to work with.

Proposition 8.1.6. *The idèle group $\mathbb{A}_\mathbb{Q}^\times = \{(\alpha_v) \in \prod_v \mathbb{Q}_v^\times : \alpha_v \in \mathbb{Z}_v^\times \text{ for a.a. } v\}$.*

Note that technically we did not define $\mathbb{Z}_v^\times$ for $v = \infty$, but as above including or removing a single place $v = \infty$ from a "for all but finitely many" condition does not change anything. However, if one wishes, one can set $\mathbb{Z}_v^\times = \{\alpha_v \in \mathbb{Q}_v^\times : |\alpha_v|_v = 1\}$ so $\mathbb{Z}_v = \mathbb{Z}_p$ for $v = p$ and $\mathbb{Z}_v = \{-1, 1\}$ for $v = \infty$.

Proof. Let $\alpha = (\alpha_v) \in \mathbb{A}_\mathbb{Q}^\times$. It is clear that $\alpha_v \in \mathbb{Q}_v^\times$ for all v, otherwise some component will be zero.

Let $\beta = (\beta_v) = \alpha^{-1} \in \mathbb{A}_\mathbb{Q}$. Since $\beta_v \in \mathbb{Z}_v$ and $\alpha_v \in \mathbb{Z}_v$ for almost all v, there is a finite set S of places v such that $\alpha_v, \beta_v \in \mathbb{Z}_v$ for all $v \notin S$. Then $\alpha\beta = (1, 1, 1, \ldots)$ means $\alpha_v\beta_v = 1$ for all v, so $\alpha_v, \beta_v \in \mathbb{Z}_v^\times$ for all $v \notin S$, i.e., $\alpha_v \in \mathbb{Z}_v^\times$ for a.a. v.

This proves $\subseteq$. $\supseteq$ is straightforward—see the next exercise. □

Exercise 8.3. *Let $\alpha = (\alpha_v) \in \mathbb{A}_\mathbb{Q}$ such that $\alpha_v \neq 0$ for all v and $\alpha_v \in \mathbb{Z}_v$ for almost all v. Show there is a $\beta \in \mathbb{A}_\mathbb{Q}$ such that $\alpha\beta = 1 = (1, 1, 1, \ldots)$.*

One can use the topologies on $\mathbb{Q}_v$ and $\mathbb{Q}_v^\times$ to define topologies on the additive group of adèles and multiplicative group of idèles, to make them both into topological groups. (We already defined the topology on $\mathbb{Q}_v$ in terms of a basis of neighborhoods. One can do the same thing for $\mathbb{Q}_v^\times$, or just give $\mathbb{Q}_v^\times$ the subspace topology from $\mathbb{Q}_v^\times \subseteq \mathbb{Q}_v$. Both methods give the same topology.) To define a topology on a group, it suffices to specify a basis of open neighborhoods of the identity.

A basis of open neighborhoods of 0 in $\mathbb{A}_\mathbb{Q}$ is given by a collection of sets of the form

$$\prod_{v \in S} U_v \prod_{v \notin S} \mathbb{Z}_v \subseteq \mathbb{A}_\mathbb{Q}$$

where S is a finite set of places containing ∞ and for each $v \in S$, U_v is an open neighborhood of 0 in $\mathbb{Q}_v$. Note the requirement that $\infty \in S$ is because $\mathbb{Z}_\infty = [-1, 1]$ is a closed set in $\mathbb{Q}_\infty = \mathbb{R}$, so we do not want $v = \infty$ occurring in the product on the right.

Similarly, a basis of open neighborhoods of 1 in $\mathbb{A}_\mathbb{Q}^\times$ is given by a collections of sets of the form

$$\prod_{v \in S} U_v \prod_{v \notin S} \mathbb{Z}_v^\times \subseteq \mathbb{A}_\mathbb{Q}$$

where S is a finite set of places containing ∞ and for each $v \in S$, U_v is an open neighborhood of 1 in $\mathbb{Q}_v^\times$.

We remark that one can also form a topology of $\mathbb{A}_\mathbb{Q}$ by taking the product topology on $\prod \mathbb{Q}_v$, and put the subspace topology on $\mathbb{A}_\mathbb{Q}$. This is different than the topology we described above, and this topology induced by the product topology is too strong for our purposes. Similar remarks are true for the topology on $\mathbb{A}_\mathbb{Q}^\times$. Further, the topology on $\mathbb{A}_\mathbb{Q}^\times$ is *not* the subspace topology induced from the inclusion $\mathbb{A}_\mathbb{Q}^\times \subseteq \mathbb{A}_\mathbb{Q}$, as the open sets in the subspace topology will be too large. For example,

Exercise 8.4. *Consider the open set $U = \mathbb{R} \times \prod_p \mathbb{Z}_p \subseteq \mathbb{A}_\mathbb{Q}$. This is an open neighborhood of 1 in $\mathbb{A}_\mathbb{Q}$. Show the restriction $U \cap \mathbb{A}_\mathbb{Q}^\times$ contains but does not equal the open neighborhood $V = \mathbb{R}^\times \times \prod_p \mathbb{Z}_p^\times$ of 1 in $\mathbb{A}_\mathbb{Q}^\times$.*

A similar, but slightly more technical, argument shows that if $V = \prod_{v \in S} U_v \prod_{v \notin S} \mathbb{Z}_v^\times$ is an open neighborhood of 1 in $\mathbb{A}_\mathbb{Q}$ (where as usual S is a finite set of places), then there is no open neighborhood U of 1 in $\mathbb{A}_\mathbb{Q}$ whose restriction to $\mathbb{A}_\mathbb{Q}^\times$ will be contained in V.

Proposition 8.1.7. *$\mathbb{A}_{\mathbb{Q}}$ and $\mathbb{A}_{\mathbb{Q}}^{\times}$ are locally compact. Furthermore,*

(i) a subset U of $\mathbb{A}_{\mathbb{Q}}$ is relatively compact if and only if $U \subseteq \prod_v K_v$ where each K_v is compact in $\mathbb{Q}_v$ and $K_v = \mathbb{Z}_v$ for almost all v; and

(ii) a subset U of $\mathbb{A}_{\mathbb{Q}}^{\times}$ is relatively compact if and only if $U \subseteq \prod_v K_v$ where each K_v is compact in $\mathbb{Q}_v^{\times}$ and $K_v = \mathbb{Z}_v^{\times}$ for almost all v.

(Recall a set is called *relatively compact* if its closure is compact.)

Proposition 8.1.8. *$\mathbb{Q}$ and $\mathbb{Q}^{\times}$ are discrete subgroups of $\mathbb{A}_{\mathbb{Q}}$ and $\mathbb{A}_{\mathbb{Q}}^{\times}$.*

Proposition 8.1.9. *$\mathbb{A}_{\mathbb{Q}}/\mathbb{Q}$ is compact with the quotient topology, and*

$$\mathbb{A}_{\mathbb{Q}}/\mathbb{Q} \simeq \varprojlim_n \mathbb{R}/n\mathbb{Z} = \{(a_1, a_2, a_3, a_4, \ldots) : a_n \in \mathbb{R}/n\mathbb{Z},\ a_n \in a_m + m\mathbb{Z} \text{ if } m|n\}\,.$$

Thus just like $\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z}$, we can view $\mathbb{A}_{\mathbb{Q}}/\mathbb{Q}$ as a projective limit, i.e., as a way of putting together all the $\mathbb{R}/n\mathbb{Z}$'s in a compatible way.

See [Ramakrishnan–Valenza] for proofs.

8.2 $\mathfrak{p}$-adic fields

There are several ways to treat the theory of $\mathfrak{p}$-adic fields, just like there are several ways to treat the theory of p-adic numbers. One common way of defining them is as finite extensions of $\mathbb{Q}_p$. However, I will opt for a concrete approach via completions w.r.t. absolute values, as it is in my mind more natural.

Let K be a number field and $\mathfrak{p}$ a prime ideal of K.

In the case $K = \mathbb{Q}$ and $\mathfrak{p} = (p)$, one defines the p-adic absolute value by $|x|_p = p^{-m}$ where $x = p^m \frac{a}{b}$ and a, b are relatively prime to p. If $x = p^m a \in \mathbb{Z}$, another way to say this is that $|x|_p = p^{-m}$ where m is the highest power of p that divides x, i.e., m is the unique integer such that

$$\mathfrak{p}^m = (p)^m \supseteq (x) \not\subseteq \mathfrak{p}^{m+1} = (p)^{m+1}.$$

In fact, using fractional ideals, we can say the same thing even if $x \notin \mathbb{Z}$. Specifically, we have a filtration of $\mathbb{Q}$:

$$\cdots \supseteq \mathfrak{p}^{-2} \supseteq \mathfrak{p}^{-1} \supseteq \mathfrak{p}^0 = \mathbb{Z} \supseteq \mathfrak{p}^1 \supseteq \mathfrak{p}^2 \supseteq \cdots$$

We define $\mathrm{ord}_p(x)$ to be the largest m such that x (or (x) if you prefer) is contained in $\mathfrak{p}^m = (p)^m$, and then set $|x|_p = p^{-\mathrm{ord}_p(x)}$.

Now we return to the general case.

Definition 8.2.1. *Let K be a number field and $\mathfrak{p}$ be a prime ideal of K. For $x \in K$, define the* **$\mathfrak{p}$-adic valuation** $\mathrm{ord}_{\mathfrak{p}}(x)$ *to be the largest integer m such that $x \in \mathfrak{p}^m$. Then the* **$\mathfrak{p}$-adic absolute value** *on K is given by $|x|_{\mathfrak{p}} = N(\mathfrak{p})^{-\mathrm{ord}_{\mathfrak{p}}(x)}$.*

Exercise 8.5. *Let $\mathfrak{p}$ be a prime ideal of K lying above a prime p of $\mathbb{Q}$. Then for $x \in \mathbb{Q} \subseteq K$, show $|x|_{\mathfrak{p}} = |x|_p^f$ where $f = f(\mathfrak{p}|p)$ is the inertial degree of $\mathfrak{p}$ above p.*

As in the case $K = \mathbb{Q}$, these give, up to equivalence, all non-archimedean absolute values on K. The archimedean values are slightly more complicated then the case of $\mathbb{Q}$, and they are essentially parametrized by $\mathrm{Gal}(K/\mathbb{Q})$. This is because if we want to restrict the usual absolute value on $\mathbb{R}$ or

$\mathbb{C}$ to K, it depends upon the embedding of K into $\mathbb{R}$ or $\mathbb{C}$, and the embeddings of K into $\mathbb{C}$ was precisely our definition for the Galois group $\mathrm{Gal}(K/\mathbb{Q})$.

Let $\{\sigma_1, \dots \sigma_r\}$ denote the set of real embeddings of K and $\{\tau_1, \overline{\tau}_1, \dots, \tau_s, \overline{\tau}_s\}$ denote the set of complex embeddings of K. Then we define the archimedean absolute values

$$|x|_{\sigma_i} = |\sigma_i(x)|_{\mathbb{R}}$$

and

$$|x|_{\tau_j} = |\tau_j(x)|_{\mathbb{C}}$$

where $|\cdot|_{\mathbb{R}}$ is the usual absolute value on $\mathbb{R}$ and $|z|_{\mathbb{C}} = z\overline{z}$ is the *square* of the usual absolute value on $\mathbb{C}$. It is immediate from the definition of equivalence that $\big| \; cdot|_{\mathbb{C}}$ is equivalent to the usual absolute value on $\mathbb{C}$, but it is preferable for us to take this normalization, as $|z|_{\mathbb{C}}$ is more like a norm than $\sqrt{|\cdot|_{\mathbb{C}}}$. In particular it maps $\mathbb{Z}[i]$ into $\mathbb{Z}$. For instance $|1+i|_{\mathbb{C}} = (1+i)(1-i) = 2$, but if we use the usual absolute value, then $|1+i| = \sqrt{2}$.

Example 8.2.2. *Let $K = \mathbb{Q}(\sqrt{3})$. Then $\mathrm{Gal}(K/\mathbb{Q}) = \{\sigma_1, \sigma_2\}$ where $\sigma_1(\sqrt{3}) = \sqrt{3}$ and $\sigma_2(\sqrt{3}) = -\sqrt{3}$. Then*

$$|1+\sqrt{3}|_{\sigma_1} = |1+\sqrt{3}|_{\mathbb{R}} \neq |1-\sqrt{3}|_{\mathbb{R}} = |1+\sqrt{3}|_{\sigma_2}.$$

Example 8.2.3. *Let $K = \mathbb{Q}(\sqrt{-3})$. Then $\mathrm{Gal}(K/\mathbb{Q}) = \{\tau, \overline{\tau}\}$ where $\tau(\sqrt{-3}) = i\sqrt{3}$. Then*

$$|1+\sqrt{-3}|_{\tau} = |1+i\sqrt{3}|_{\mathbb{C}} = |1-i\sqrt{3}|_{\mathbb{C}} = |1+\sqrt{-3}|_{\overline{\tau}}.$$

In general, no absolute values corresponding to two different σ_i's or τ_j's will be equivalent, but we will always have $|\cdot|_{\tau_j} = |\cdot|_{\overline{\tau}_j}$ since $|z|_{\mathbb{C}} = |\overline{z}|_{\mathbb{C}}$.

Theorem 8.2.4. *The places (equivalence classes of non-trivial absolute values) on K are precisely given by*

(i) $v = \mathfrak{p}$ where $\mathfrak{p}$ is a prime ideal of K (non-archimedean places)

(ii) $v = \sigma_i$ where σ_i is a real embedding of K (real places)

(iii) $v = \tau_j$ where τ_j runs over the set of complex embedding of K, up to complex conjugation (complex places).

Definition 8.2.5. *For a place v of K, let K_v denote the completion of K with respect to $|\cdot|_v$. Let $\mathcal{O}_{K_v} = \{x \in K_v : |x|_v \leq 1\}$ and $\mathcal{O}_{K_v}^{\times} = \{x \in K_v : |x|_v = 1\}$.*

If $v = \mathfrak{p}$ is a non-archimedean place, we call K_v the **$\mathfrak{p}$-adic numbers** *and $\mathcal{O}_{K_v}$ the* **$\mathfrak{p}$-adic integers** *over K.*

If $K = \mathbb{Q}$ and $\mathfrak{p} = (p)$ this coincides with our previous definitions. Most of the results on p-adic numbers over $\mathbb{Q}$ extend to $\mathfrak{p}$-adic numbers over K, but due to time constraints we will not explain these in detail except where we need to. A similar remark is true for the theory of adèles and idèles, which we can now define.

Definition 8.2.6. *The* **adèles** *of K are*

$$\mathbb{A}_K = \{\alpha = (\alpha_v) : \alpha_v \in K_v \text{ for all } v,\ \alpha_v \in \mathbb{Z}_v \text{ for a.a. } v\} \subset \prod_v K_v.$$

Similarly, the **idèles** *of K are*

$$\mathbb{A}_K^{\times} = \big\{\alpha = (\alpha_v) : \alpha_v \in K_v^{\times} \text{ for all } v,\ \alpha_v \in \mathbb{Z}_v^{\times} \text{ for a.a. } v\big\} \subset \prod_v K_v^{\times}.$$

In both statements, v runs over the set of places of K.

As with $\mathbb{Q}$, K and $K^\times$ embed diagonally into $\mathbb{A}_K$ and $\mathbb{A}_K^\times$, and in this way we will regard K and $K^\times$ as additive and multiplicative subgroups of $\mathbb{A}_K$ and $\mathbb{A}_K^\times$. One defines the absolute value on $\mathbb{A}_K$ or $\mathbb{A}_K^\times$ by

$$|\alpha| = |\alpha|_{\mathbb{A}_K} = \prod_v |\alpha_v|_v$$

where $\alpha = (\alpha_v) \in \mathbb{A}_K$. We will usually simply denote the absolute value on $\mathbb{A}_K$ by $|\cdot|$, but sometimes we will use $|\cdot|_{\mathbb{A}_K}$ for clarity.

Definition 8.2.7. *The* **idèle class group** *of K is $C_K = \mathbb{A}_K^\times / K^\times$.*

While $\mathbb{A}_K/K$ is compact, it is not the case that $\mathbb{A}_K^\times/K^\times$ is, owing to the fact that the open sets of $\mathbb{A}_K^\times$ are much smaller than the open sets of $\mathbb{A}_K$ (see above remarks about the difference between the topologies on $\mathbb{A}_\mathbb{Q}$ and $\mathbb{A}_\mathbb{Q}^\times$). However one can prove the following.

Theorem 8.2.8. *Let $\mathbb{A}_K^1 \subset \mathbb{A}_K^\times$ be the subgroup of idèles of K having absolute value 1. Then $K^\times \subseteq \mathbb{A}_K^1$ and the* **norm 1 idèle class group**

$$C_K^1 = \mathbb{A}_K^1 / K^\times$$

is compact.

Recall in the case $K = \mathbb{Q}$, you proved in Exercise 6.11 that the adèlic absolute value $|(x, x, x, \ldots)|_{\mathbb{A}_\mathbb{Q}} = 1$ for $x \in \mathbb{Q}^\times$. A similar argument shows that $|x|_{\mathbb{A}_K} = |(x, x, x, \ldots)|_{\mathbb{A}_K} = 1$ for any $x \in K^\times$, which means $K^\times \subseteq \mathbb{A}_K^1$.

Definition 8.2.9. *The* **∞-idèles** *are defined to be*

$$\mathbb{A}_{K,\infty}^\times = \left\{(\alpha_v) \in \mathbb{A}_K^\times : \alpha_v \in \mathcal{O}_{K_v}^\times \text{ for all } v < \infty\right\} \subseteq \mathbb{A}_K^\times$$

Exercise 8.6. *Check $\mathbb{A}_{K,\infty}^\times$ is a subgroup of $\mathbb{A}_K^\times$. Show its intersection with the subgroup $K^\times$, i.e. $\mathbb{A}_{K,\infty}^\times \cap K^\times$, is the group of units $\mathcal{O}_K^\times$ (regarded as a subgroup of $\mathbb{A}_K^\times$).*

Theorem 8.2.10. *The map*

$$\begin{aligned} \mathbb{A}_K^\times &\to \mathcal{C}l_K \\ \alpha = (\alpha_v) &\mapsto \prod \mathfrak{p}^{\mathrm{ord}_\mathfrak{p}(\alpha_\mathfrak{p})} \end{aligned}$$

is a surjective homomorphism with kernel $K^\times \cdot \mathbb{A}_{K,\infty}^\times$. In particular, this defines an isomorphism

$$C_K / \mathbb{A}_{K,\infty}^\times \simeq \mathcal{C}l_K$$

of the idèle class group mod the ∞-idèles with Dedekind's ideal class group.

Proof. Note that if $\alpha_\mathfrak{p} \in \mathcal{O}_{K_\mathfrak{p}}^\times$, then $\mathrm{ord}_\mathfrak{p}(\alpha_\mathfrak{p}) = 0$ so $\mathfrak{p}^{\mathrm{ord}_\mathfrak{p}(\alpha_\mathfrak{p})} = (1) = \mathcal{O}_K$. Since $\alpha \in \mathbb{A}_K^\times$ means $\alpha_\mathfrak{p} \in \mathcal{O}_{K_\mathfrak{p}}^\times$ for all but finitely many $\mathfrak{p}$, the product in the definition of the homomorphism is in fact a finite product so the definition makes sense. It is then obvious it is a homomorphism.

Exercise 8.7. *(i) Show for $\mathbb{A}_{K,\infty}^\times$ is in the kernel of the above map into $\mathcal{C}l_K$*

(ii) Show $K^\times$ is kernel of the above map into $\mathcal{C}l_K$. (Hint: show if $x \in \mathcal{O}_K^\times$, then the ideal $(x) = x\mathcal{O}_K = \prod \mathfrak{p}^{\mathrm{ord}_\mathfrak{p}(x)}$.)

It is not much more difficult to show that these subgroups give the whole kernel.

To complete the proof, one needs to show the above map is surjective. Let $\mathcal{I}$ be an arbitrary ideal in $\mathcal{C}l_K$, and write the prime ideal factorization as $\mathcal{I} = \prod_{\mathfrak{p}\in S} \mathfrak{p}^{e_\mathfrak{p}}$ where S is some finite set of primes. Then we can construct an idèle $\alpha = (\alpha_v)$ where $\alpha_v = 1$ if $v \notin S$ and $\alpha_\mathfrak{p} = \varpi_\mathfrak{p}^{e_\mathfrak{p}}$. Here $\varpi_\mathfrak{p}$ is a **uniformizer** of $\mathcal{O}_{K_\mathfrak{p}}$, i.e., $\mathrm{ord}_\mathfrak{p}(\varpi_\mathfrak{p}) = 1$. To see that such a $\varpi_\mathfrak{p}$ always exists, just take $\varpi_\mathfrak{p} \in \mathcal{O}_K$ such that $\varpi_\mathfrak{p} \in \mathfrak{p}$ but $\varpi_\mathfrak{p} \notin \mathfrak{p}^2$. □

This leads us to a topological proof of

Corollary 8.2.11. *The ideal class group $\mathcal{C}l_K$ is finite.*

Proof. We consider the above map restricted to $\mathbb{A}_K^1$. It is easy to see that this is still surjective—in our construction of α above, we were free to do what we want at the infinite places so we can ensure $|\alpha| = 1$. Hence we have an isomorphism

$$C_K^1/\mathbb{A}_{K,\infty}^1 \simeq \mathcal{C}l_K$$

where $\mathbb{A}_{K,\infty}^1 = \mathbb{A}_{K,\infty}^\times \cap \mathbb{A}_K^\times$. However C_K^1 is compact, and $\mathbb{A}_{K,\infty}^1$ is an open subset. Hence the quotient $\mathcal{C}l_K$ is both compact and discrete, whence finite. □

8.3 Elements of class field theory

Class field theory is regarded as the crowning acheivement of algebraic number theory, just as quadratic reciprocity was the crowning achievement of elementary number theory. Class field theory is often described as a characterization of the abelian extensions of a number field, but its explicit forms generalize quadratic and higher reciprocity laws.

What do we mean by higher reciprocity laws? Well the most basic way of thinking about quadratic reciprocity is a way to tell if something is a square mod p. Cubic reciprocity is a way to tell if something is a cube mod $\mathfrak{p}$, and similarly there are notions of biquadratic (4th power) and higher reciprocity laws. Looked at from the point of view of rings of integers, quadratic reciprocity tells us about the way primes split in quadratic extensions. So you might guess cubic reciprocity should tell us about the way primes split in (normal) cubic extensions, and so on. In general, *Artin reciprocity* (a more explicit form class field theory) tells us how primes split in abelian extensions.

Even to state the main theorems of class field theory is not so simple, and we still need to make some more definitions.

Let L/K be an extension of number fields. Let $\mathfrak{P}$ be a prime ideal of L lying above $\mathfrak{p}$, a prime ideal of K. The **decomposition group** of L/K at $\mathfrak{P}$ is

$$G(\mathfrak{P}|\mathfrak{p}) = \{\sigma \in \mathrm{Gal}(L/K) : \sigma(\mathfrak{P}) = \mathfrak{P}\}.$$

Recall that $\mathrm{Gal}(L/K)$ acts on the primes of L above $\mathfrak{p}$, so the $G(\mathfrak{P}|\mathfrak{p})$ is just the stabilizer of $\mathfrak{P}$. Each element of $G(\mathfrak{P}|\mathfrak{p})$ extends to an automorphism of the completion $L_\mathfrak{P}$ which is trivial on $K_\mathfrak{p}$. One can define Galois groups for extensions of local fields ($L_\mathfrak{P}/K_\mathfrak{p}$ is a finite extension of degree $f(\mathfrak{P}|\mathfrak{p})$) and show $\mathrm{Gal}(L_\mathfrak{P}/K_\mathfrak{p}) \simeq G(\mathfrak{P}|\mathfrak{p})$.

As in the case of number fields one can define a **norm** from $L_\mathfrak{P}$ to $K_\mathfrak{p}$ given by

$$N_{\mathfrak{P}|\mathfrak{p}}(x) = N_{L_\mathfrak{P}/K_\mathfrak{p}}(x) = \prod_{\sigma\in\mathrm{Gal}(L_\mathfrak{P}/K_\mathfrak{p})} \sigma(x).$$

One can also do something similar for the archimedean, or infinite, places. In particular, if v is an infinite place of L (i.e., an element of $\mathrm{Gal}(/\mathbb{Q})$, up to complex conjugation) and w is an infinite place of K (i.e., an element of $\mathrm{Gal}(K/\mathbb{Q})$ up to complex conjugation), we write $v|w$ if the embedding $v : L \hookrightarrow \mathbb{C}$ restricted to K gives the embedding $w : K \hookrightarrow \mathbb{C}$ (up to complex conjugation). If $v|w$, then $N_{v|w}(z) = z$ if $L_v = K_w = \mathbb{R}$ or $\mathbb{C}$, and $N_{v|w}(z) = z\overline{z}$ if $L_v = \mathbb{C}$ and $K_w = \mathbb{R}$.

Using this, one can define a **norm** from $\mathbb{A}_L^\times$ to $\mathbb{A}_K^\times$ given by

$$N_{L/K}((\alpha_v)_v) = (\prod_{v|w} N_{v|w}(\alpha_v))_w$$

Exercise 8.8. *Let $x \in L^\times$ and regard $x = (x, x, x, \ldots) \in \mathbb{A}_L^\times$. Show the idèlic norm $N_{L/K}(x)$ lies in $K^\times \subseteq \mathbb{A}_K^\times$.*

For a number field K, let $\overline{K}$ denote its algebraic closure, and for a group G let G^{ab} denote is abelianization (quotient via the commutator subgroup). Note that $\mathrm{Gal}(\overline{K}/K)^{ab}$ "contains" the Galois group of any abelian extension L/K as a quotient. In fact, there is a maximal abelian extension K^{ab} of K inside $\overline{K}$ (infinite degree of course), and we will have $\mathrm{Gal}(K^{ab}/K) = \mathrm{Gal}(\overline{K}/K)^{ab}$. The extension K^{ab} contains all finite abelian extensions of K.

Now we can at least state some of the "non-explicit" assertions of class field theory:

Theorem 8.3.1. *Let K be a number field. There is a homomorphism, called the* **Artin map**,

$$\theta_K : C_K \to \mathrm{Gal}(K^{ab}/K)$$

such that

(i) For every finite abelian extension L/K, let $\theta_{L/K}$ denote the composition of

$$\theta_{L/K} : C_K \overset{\theta_K}{\to} \mathrm{Gal}(K^{ab}/K) \to \mathrm{Gal}(L/K)$$

Then $\ker \theta_{L/K} = N_{L/K}(C_L)$, which yields an isomorphism

$$C_K/(N_{L/K}C_L) = \mathbb{A}_K^\times/(K^\times \cdot N_{L/K}(\mathbb{A}_L^\times)) \simeq \mathrm{Gal}(L/K)$$

(ii) Given any open subgroup of N of C_K of finite index, there is a finite abelian extension L of K with $N = \ker \theta_{L/K}$. Hence

$$C_K/N \simeq \mathrm{Gal}(L/K).$$

There are also some functoriality results which say how the Artin maps θ_K and θ_L are related for an extension L/K, but we will pass over these now.

Let $\zeta_n = e^{2\pi i/n}$.

Corollary 8.3.2. (Kronecker–Weber) *Every abelian extension of $\mathbb{Q}$ is contained in $\mathbb{Q}(\zeta_n)$ for some n.*

An equivalent way to state this is that the maximal abelian extension $\mathbb{Q}^{ab}$ of $\mathbb{Q}$ in $\overline{\mathbb{Q}}$ is the compositum of the extensions $\mathbb{Q}(\zeta_n)$ for all n.

The basic idea of the proof is the following. Class field theory says the abelian extensions of $\mathbb{Q}$ correspond to the open subgroups of the idèle class group $C_\mathbb{Q}$. To understand what these are, we want to determine the structure of $\mathbb{A}_\mathbb{Q}^\times$. Specifically, one can show

$$\mathbb{A}_\mathbb{Q}^\times \simeq \mathbb{Q}^\times \times \mathbb{R}_{>0} \times \hat{\mathbb{Z}}^\times$$

where $\hat{\mathbb{Z}}^\times = \varprojlim(\mathbb{Z}/n\mathbb{Z})^\times = \prod_p \mathbb{Z}_p^\times$. Consequently

$$C_{\mathbb{Q}} \simeq \mathbb{R}_{>0} \times \hat{\mathbb{Z}}^\times.$$

Hence if U is an open subgroup of $C_{\mathbb{Q}}$ with finite index, then U must be of the form $U \simeq \mathbb{R}_{>0} \times U'$ where U' is an open subgroup of finite index in $\mathbb{Z}^\times$. (Since there are no nontrivial open subgroups of finite index in $\mathbb{R}_{>0}$.) Then one uses a basis of neighborhoods for 1 in $\hat{\mathbb{Z}}^\times$ to show that U must contain $N_{K/\mathbb{Q}}(C_K)$ where K is some $\mathbb{Q}(\zeta_n)$. Consequently the extension corresponding to U must contain K. (The functor from open subgroups of C_K to abelian extensions of K is contravariant (i.e., inclusion-reversing), just like the functor from subgroups of the absolute Galois group of K to extensions of K.)

The above theorem of class field theory was established by Takagi, but the existence of a homomorphism θ_K was given abstractly. It was Artin who was able to give it in an explicit fashion, which we now briefly describe.

Let L/K be a Galois extension of number fields, $\mathfrak{p}$ a prime of K and $\mathfrak{P}$ a prime of L lying above $\mathfrak{p}$. Let $f = f(\mathfrak{p}|p)$ where p is the prime of $\mathbb{Q}$ lying under $\mathfrak{p}$, so the residue field $\mathcal{O}_K/\mathfrak{p}$ has order $q = p^f$. The **Frobenius map** $Fr_q : x \mapsto x^q$ generates the Galois group $\mathrm{Gal}((\mathcal{O}_L/\mathfrak{P})/(\mathcal{O}_K/\mathfrak{p}))$. The decomposition group maps to $\mathrm{Gal}((\mathcal{O}_L/\mathfrak{P})/(\mathcal{O}_K/\mathfrak{p}))$ via

$$\phi : G(\mathfrak{P}|\mathfrak{p}) \to \mathrm{Gal}((\mathcal{O}_L/\mathfrak{P})/(\mathcal{O}_K/\mathfrak{p}))$$

by

$$\sigma \mapsto (a\mathfrak{P} \mapsto \sigma(a)\mathfrak{P}).$$

This is an isomorphism if $\mathfrak{P}|\mathfrak{p}$ is unramified, and in this case and we let the **Frobenius element** $\phi_{\mathfrak{P}|\mathfrak{p}}$ of $\mathrm{Gal}(\mathfrak{P}|\mathfrak{p}) \subseteq \mathrm{Gal}(L/K)$ be the inverse image $\phi_{\mathfrak{P}|\mathfrak{p}} = \phi^{-1}(Fr_q)$ of Fr_q in $\mathrm{Gal}(\mathfrak{P}|\mathfrak{p})$.

Exercise 8.9. *Let L/K be a Galois extension of number fields. Let $\mathfrak{P}$ and $\mathfrak{P}'$ be primes of L lying above $\mathfrak{p}$. Show the decomposition groups $G(\mathfrak{P}|\mathfrak{p})$ and $G(\mathfrak{P}'|\mathfrak{p})$ are conjugate in* $\mathrm{Gal}(L/K)$.

We regard each Frobenius element $\phi_{\mathfrak{P}|\mathfrak{p}} \in \mathrm{Gal}(\mathfrak{P}|\mathfrak{p})$ as an element of $\mathrm{Gal}(L/K)$. The above exercise implies for two primes $\mathfrak{P}$ and $\mathfrak{P}'$ of L above $\mathfrak{p}$, the Frobenius elements $\phi_{\mathfrak{P}|\mathfrak{p}}$ and $\phi_{\mathfrak{P}'|p}$ are conjugate in $\mathrm{Gal}(L/K)$.

If L/K is abelian, then the conjugacy classes of $\mathrm{Gal}(L/K)$ are just single elements and the Frobenius $\phi_{\mathfrak{P}|\mathfrak{p}} \in \mathrm{Gal}(L/K)$ does not depend upon the choice of prime $\mathfrak{P}$ above $\mathfrak{p}$. Hence in this case we define the **Frobenius at $\mathfrak{p}$** to be

$$\phi_{\mathfrak{p}} = \left(\frac{L/K}{\mathfrak{p}}\right) := \phi_{\mathfrak{P}|\mathfrak{p}} \in \mathrm{Gal}(L/K)$$

where $\mathfrak{P}$ is a prime of L above $\mathfrak{p}$. The symbol $\left(\frac{L/K}{\mathfrak{p}}\right)$ is called the **Artin symbol**.

One can similarly define the Artin symbol $\left(\frac{L/K}{v}\right)$ for any place v of K, which will be some element of $\mathrm{Gal}(L/K)$. See [Neukirch] for the complete details.

Theorem 8.3.3. (Artin) *Let L/K be a finite abelian extension of number fields. Let $\varpi_{\mathfrak{p}}$ be a uniformizer for $\mathcal{O}_{K_{\mathfrak{p}}}$, i.e., an element of $\mathcal{O}_{K_{\mathfrak{p}}}$ such that $\mathrm{ord}_{\mathfrak{p}}(\varpi_{\mathfrak{p}}) = 1$. Let $x_{\mathfrak{p}} = (\alpha_v) \in \mathbb{A}_K^\times$ be the idèle such that $\alpha_v = \varpi_{\mathfrak{p}}$ for $v = \mathfrak{p}$ and $\alpha_v = 1$ otherwise.*

We may take Artin map θ_K above such that

$$\theta_{L/K}(x_{\mathfrak{p}}) = \phi_{\mathfrak{p}} = \left(\frac{L/K}{\mathfrak{p}}\right)$$

for all primes $\mathfrak{p}$ of K which are unramified in L/K.

The Artin symbol can be used to describe n-th power reciprocity laws. In order to make sense of this, we should define n-th power residue symbols $\left(\frac{a}{p}\right)_n$. This should be 1 if a is an n-th power mod p. But if this is going to be multiplicative, it can't simply be -1 if a is not an n-th power mod p (think about the case $n = 3$). What we need is $\left(\frac{a}{p}\right)_n$ should give a group homomorphism into the n-th roots of unity, such that the kernel is precisely the set of n-th powers mod p. In fact because of this, it won't make sense to define n-th power residue symbols over $\mathbb{Q}$ (or $\mathbb{Z}$), but only over number fields which contain the n-th roots of unity.

Let μ_n denote the n-th roots of unity.

Definition 8.3.4. *Let K be a number field containing μ_n and v be a place of K. The* **n-th Hilbert symbol**

$$\left(\frac{-,-}{v}\right)_n : K_v^\times \times K_v^\times \to \mu_n$$

is given by

$$\left(\frac{K_v(\sqrt[n]{b})/K_v}{v}\right)\sqrt[n]{b} = \phi_v(\sqrt[n]{b}) = \left(\frac{a,b}{v}\right)_n \sqrt[n]{b}.$$

In other words, the Frobenius $\phi_v = \left(\frac{K_v(\sqrt[n]{b})/K_v}{v}\right)$ is an element of $\mathrm{Gal}(K_v(\sqrt[n]{b})/K_v)$. But the conjugates of $\sqrt[n]{b}$ in $K_v(\sqrt[n]{b})/K_v$ are just $\sqrt[n]{b}$ times the n-th roots of unity. Hence $\phi_v(\sqrt[n]{b})$ is some n-th root of unity times $\sqrt[n]{b}$, and we let the n-th Hilbert symbol $\left(\frac{a,b}{v}\right)_n$ be that root of unity.

Theorem 8.3.5. *Let K be a number field containing μ_n and v be a place of K. For $a, b \in K^\times$, we have*

$$\prod_v \left(\frac{a,b}{v}\right)_n = 1.$$

Proof. We have

$$\prod_v \left(\frac{a,b}{v}\right)_n \sqrt[n]{b} = \prod_v \left(\frac{K_v(\sqrt[n]{b})/K_v}{v}\right)\sqrt[n]{b} = \prod_v \theta_{K(\sqrt[n]{b})/K}(a)\sqrt[n]{b}.$$

However, any element of $K^\times$ is in the kernel of the Artin map $\theta_{K(\sqrt[n]{b})/K}$, so the above must equal $\sqrt[n]{b}$ and the asserted product formula follows. □

Definition 8.3.6. *Let $a \in K^\times$ where $\mu_n \subseteq K$. For $\mathfrak{p}$ a prime of K, we define the* **n-th power residue symbol** *to be*

$$\left(\frac{a}{\mathfrak{p}}\right)_n = \left(\frac{a, \varpi_{\mathfrak{p}}}{\mathfrak{p}}\right)_n$$

where $\varpi_{\mathfrak{p}}$ is a uniformizer for $K_{\mathfrak{p}}$. If $b \in K^\times$, we set

$$\left(\frac{a}{b}\right)_n = \prod_{\mathfrak{p}_i \nmid n} \left(\frac{a}{\mathfrak{p}_i}\right)_n^{e_i},$$

where $(b) = \prod \mathfrak{p}_i^{e_i}$ ideal of K.

It is not too hard to check that

$$\left(\frac{a}{\mathfrak{p}}\right)_n = 1 \iff a \equiv x^n \bmod \mathfrak{p}$$

and more generally

$$\left(\frac{a}{\mathfrak{p}}\right)_n \equiv a^{\frac{N(\mathfrak{p})-1}{n}} \bmod \mathfrak{p}.$$

Theorem 8.3.7. (n-th power reciprocity) *Suppose $\mu_n \subseteq K^\times$. If $a, b \in K^\times$, then*

$$\left(\frac{a}{b}\right)_n = \left(\frac{b}{a}\right)_n \prod_{v|n\infty} \left(\frac{a,b}{v}\right)_n.$$

This follows simply from the above product formula (the previous theorem). See [Neukirch].

In particular, if a and b are prime elements of $\mathcal{O}_K$ (i.e., they generate prime ideals of $\mathcal{O}_K$), and $\prod_{v|n\infty} \left(\frac{a,b}{v}\right)_n = 1$, then a is an n-th power mod b if and only if b is an n-th power mod a.

Corollary 8.3.8. (Quadratic Reciprocity) *Let $K = \mathbb{Q}$ and $n = 2$. Let a, b be odd coprime integers. Then*

$$\left(\frac{a}{b}\right)_2 \left(\frac{b}{a}\right)_2 = (-1)^{\frac{a-1}{2}\frac{b-1}{2}} (-1)^{\frac{sgn(a)-1}{2}\frac{sgn(b)-1}{2}},$$

and

$$\left(\frac{-1}{b}\right)_2 = (-1)^{\frac{b-1}{2}}, \left(\frac{2}{b}\right)_2 = (-1)^{\frac{b^2-1}{8}}.$$

Corollary 8.3.9. (Cubic Reciprocity) *Let $K = \mathbb{Q}(\zeta_3)$ and $n = 3$. Suppose p, q are primes (i.e., they generate prime ideals) in $\mathcal{O}_K$ such that $p, q \equiv \pm 1 \bmod 3$. (If (α) is prime in $\mathcal{O}_K$ which does not lie above 3, then it has 6 associates, 2 of which are $\equiv \pm 1 \bmod 3$.) Then if p and q lie above different primes of $\mathbb{Q}$, we have*

$$\left(\frac{p}{q}\right)_3 = \left(\frac{q}{p}\right)_3.$$

Hence class field theory generalizes quadratic and higher reciprocity laws.

8.4 Non-abelian class field theory

The n-th power reciprocity law says that if p and q are prime elements of $K \supset \mu_n$, then we can determine whether p is an n-th power mod q based on whether or not q is an n-th power mod p. In particular, we have

$$\left(\frac{p}{q}\right)_n = \left(\frac{q}{p}\right)_n$$

if the product $\prod_{v|n\infty} \left(\frac{p,q}{v}\right)_n = 1$. The proof of this reciprocity law is essentially to look at the Artin map

$$\theta_{L/K} : C_K \to \mathrm{Gal}(L/K)$$

for the extension L/K where $L = K(\sqrt[n]{a})$. Since this applies only to abelian extensions, we see the need for the requirement that $\mu_n \subseteq K$ from the point of view of class field theory. Specifically,

assuming none of the n-roots of $x^n - a$ lie in K, the extension $K(\sqrt[n]{a})/K$ is abelian (in fact cyclic of degree n) if and only if $\mu_n \subset K$.

Hence if one wanted to extend the n-th power reciprocity law to $\mathbb{Q}$, one would want some sort of non-abelian version of class field theory. In fact, one might guess a reciprocity law roughly of the following form: *Let $f(x)$ be an irreducible polynomial over $\mathbb{Z}$. If p and q are odd primes not dividing n, then one can determine when*

$$f(x) \equiv p \text{ is solvable mod } q$$

in terms of when

$$f(x) \equiv q \text{ is solvable mod } p.$$

Indeed this is essentially what n-th power reciprocity says in the case $f(x) = x^n$. Though it seems likely that a "non-abelian reciprocity law" will be more complicated than this.

To put the notion of reciprocity in a little more imprecise way, recall that $x^2 \equiv q \bmod p$ has a solution, i.e., $x^2 - q$ has a root mod p, if and only if p is split in $\mathbb{Q}(\sqrt{q})$. Similarly if p and q are primes in K, then $x^n \equiv q \bmod p$ has a solution if and only if $x^n - q$ has a root mod p, which means p is split in $K(\sqrt[n]{q})$. If $K(\sqrt[n]{q})/K$ is Galois, i.e., if $\mu_n \subset K$, we can in fact say $x^n \equiv q \bmod p$ if and only if p splits completely in $K(\sqrt[n]{q})/K$. Hence we may think of n-th power reciprocity as a description of which primes split in $K(\sqrt[n]{q})/K$. Class field theory can then be thought of as a description of which primes split in an abelian extension L/K. Thus non-abelian class field theory, or a non-abelian reciprocity law, should be a description of which primes split in a non-abelian extension L/K.

Before we think about what the statement of non-abelian class field theory should look like in general, we sketch out an example.

Example 8.4.1. *(Koike, 1985) Let $f(x)$ be an irreducible polynomial of degree 3 over $\mathbb{Q}$, and let K be the splitting field of $f(x)$. Assume $\mathrm{Gal}(K/\mathbb{Q}) \simeq S_3$ and K contains an imaginary quadratic extension. One can to associate to $f(x)$ the* elliptic curve

$$E : y^2 = f(x)$$

as well as a corresponding modular form

$$F : \mathfrak{H} = \{z \in \mathbb{C} : Im(z) > 0\} \to \mathbb{C}$$

$$F(\tau) = \sum_{n=1}^{\infty} a_n e^{2\pi i n \tau},$$

where the a_n's are certain Fourier coefficients which determine the function $F(\tau)$.

Let n_p be the number of solutions $\#E(\mathbb{F}_p)$ to $y^2 \equiv f(x) \bmod p$. Then the precise correspondence between E and F is that $a_p = p + 1 - n_p$. One version of a non-abelian reciprocity law in this case say that, apart from p lying in a finite set of primes,

$$p \text{ splits completely in } K \iff a_p = 2.$$

Hence we can describe the set of primes which split completely in K in terms of either (i) arithmetic data associated to an elliptic curve, or (ii) arithmetic data associated to a modular form.

Langlands' conjecture

In order to think about how one might set up a general non-abelian class field theory, let's go back to understanding what (abelian) class field theory says. Class field theory says there is an homomorphism from the idèle class group $C_K = \mathbb{A}_K/K^\times$ to $\mathrm{Gal}(K^{ab}/K)$, which satisfies certain properties. In particular, we have an isomorphism $C_K/N_{L/K}C_L \simeq \mathrm{Gal}(L/K)$ for any finite abelian extension L/K.

If one wants to extend this to non-abelian extensions L/K, one might look for "non-abelian class groups" $G(K)$ such that $G(K)$ is related to $\mathrm{Gal}(\overline{K}/K)$ and, for any finite Galois extension L/K, we have $G(K)/N_{L/K}(G(L)) \simeq \mathrm{Gal}(L/K)$, where $N_{L/K}(G(L))$ is a certain (normal?) subgroup of $G(K)$ associated to the "non-abelian class group" $G(L)$ of L. It is not clear how such a "non-abelian class group" could be constructed. However there are very specific conjectures for a non-abelian generalization if look at the dual picture, i.e., put things in terms of group representations and L-functions.

If G is a locally compact abelian group, we can consider the set of (unitary) characters, $\hat{G}$, consisting of continuous homomorphisms $G \to S^1$. The set $\hat{G}$ is naturally made into a locally compact abelian group, called the **dual group** of G. Pontryagin duality says that the dual group of $\hat{G}$ is isomorphic to G in a canonical way. Thus, to study C_K or $\mathrm{Gal}(K^{ab}/K)$, it is equivalent to study their dual groups. Characters $\omega : C_K \to S^1$ are called **idèle class characters** or **Hecke characters**. Characters $\chi : \mathrm{Gal}(K^{ab}/K) \to S^1$ are called 1-dimensional **Galois representations**. More generally, an n-dimensional (complex) Galois representation is a continuous homomorphism $\rho : \mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}_n(\mathbb{C})$. But a 1-dimensional representation (i.e., a character) of $\chi : \mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}_1(\mathbb{C}) = \mathbb{C}^\times$ will have image in S^1 factor through $\mathrm{Gal}(K^{ab}/K)$, so this agrees with our definition above.

Consider a 1-dimensional Galois representation $\chi : \mathrm{Gal}(K^{ab}/K) \to \mathbb{C}^\times$. By composition with the Artin map, we get a Hecke character

$$\chi \rightsquigarrow \omega = \chi \circ \theta_K.$$

Since the Artin map is not an isomorphism, so one does not necessarily (in fact does not) get all Hecke characters this way, but one gets all *finite order* Hecke characters this way. (A character ω is finite order if $\omega^m = 1$ for some natural number m.) Namely, continuity of χ implies χ has finite image, so it factors through (the Galois group of) a finite abelian extension $\chi : \mathrm{Gal}(L/K) \to \mathbb{C}^\times$, consequently ω will factor through C_K/N, where $N = N_{L/K}(C_L)$. For a finite abelian group G, the group of characters $\hat{G}$ is actually (non-canonically) isomorphic to G, so the above correspondence of 1-dimensional Galois representations with finite order Hecke characters gives a bijection (in fact isomorphism)

$$\left\{\omega : C_K/N \to \mathbb{C}^\times\right\} \overset{1-1}{\longleftrightarrow} \left\{\chi : \mathrm{Gal}(L/K) \to \mathbb{C}^\times\right\}.$$

This correspondence of Galois representations and finite order Hecke characters is equivalent to abelian class field theory.

Now the natural guess for a "higher dimensional," or non-abelian analogue of this would be to get a correspondence with n-dimensional representations of $\mathrm{Gal}(\overline{K}/K)$ for any n. (Again, by continuity, any given representation will factor through a finite extension $\mathrm{Gal}(L/K)$. Moreover, if $n > 1$ and the representation is irreducible, then L/K will not be abelian.) The question is, what group should we pick on the left? This was an insight of Langlands (building on the work of many

before him). Note that we can view the idèle class group as

$$C_K = \mathbb{A}_K^\times / K^\times = \mathrm{GL}_1(K)\backslash \mathrm{GL}_1(\mathbb{A}_K).$$

(Read the latter as $\mathrm{GL}_1(\mathbb{A}_K)$ mod $\mathrm{GL}_1(K)$. We typically write the mod on the left as above however—we also sometimes write $K^\times \backslash \mathbb{A}_K^\times$. Of course in this case our groups our abelian, so it doesn't matter which side we mod out on, but it will for the non-abelian groups below. The reason for putting mod on the left is because we sometimes want to mod out by another subgroup on the right—of course which goes on the left and which on the right is just a matter of convention.)

Conjecture 8.4.2. (Langlands) *There is a (partial)* $1-1$ *correspondence*

$$\{\textit{automorphic representations } \pi \textit{ of } \mathrm{GL}_n(K)\backslash \mathrm{GL}_n(\mathbb{A}_K)\} \overset{1-1}{\dashleftarrow} \left\{n\textit{-dimensional representations } \rho \textit{ of } \mathrm{Gal}(\overline{K}/K)\right\}.$$

Roughly, an **automorphic representation** of a locally compact group G is a irreducible representation of G on $L^2(G)$. The diagonal subgroup $\mathrm{GL}_n(K) \subset \mathrm{GL}_n(\mathbb{A}_K)$ is not normal (for $n > 1$), so the quotient $\mathrm{GL}_n(K)\backslash \mathrm{GL}_n(\mathbb{A}_K)$ is not actually a group. Hence this requires some explanation.

First note if G is a finite group, $L^2(G)$ is just the $\mathbb{C}$-vector space of $\mathbb{C}$-valued functions on G. We can take for a basis $\{e_g\}_{g\in G}$ where e_g is the characteristic function of g in G. Hence $L^2(G) \simeq \mathbb{C}[G]$, the group algebra, and we know $\mathbb{C}[G]$ decomposes as a direct sum of the irreducible representations of G.

When G is not finite, things are more complicated, but in any event G acts on the space $L^2(G)$ by right multiplication, i.e., $g : f(x) \to f(xg)$ for any $f \in L^2(G)$. In fact if $G = \mathrm{GL}_n(\mathbb{A}_K)$, G acts on $L^2(\mathrm{GL}_n(K)\backslash \mathrm{GL}_n(\mathbb{A}_K))$ in the same way. This representation, the *right regular representation* on $L^2(\mathrm{GL}_n(K)\backslash \mathrm{GL}_n(\mathbb{A}_K))$, decomposes into irreducible constituents. What we mean by an automorphic representation of $\mathrm{GL}_n(\mathbb{A}_K)$ (or $\mathrm{GL}_n(K)\backslash \mathrm{GL}_n(\mathbb{A}_K)$) is one of these irreducible constituents. The term *automorphic* means that the representation is realized on a space of *automorphic forms*, which are functions on $\mathrm{GL}_n(\mathbb{A}_K)$ invariant under $\mathrm{GL}_n(K)$. When $n > 1$, automorphic representations are infinite-dimensional representations, and are studied using more harmonic analysis than algebra, per say.

Langlands' conjecture states that to each n-dimensional Galois representation $\rho : \mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}_n(\mathbb{C})$, there is associated (in a way we shall describe below) an automorphic representation $\pi = \pi(\rho)$ of $\mathrm{GL}_n(\mathbb{A}_K)$. However in general there will be more automorphic representations than n-dimensional Galois representations, i.e., not every automorphic representation will correspond to a Galois representation. This is indicated by the dashed arrow going from left to right in the conjecture above. This is true even when $n = 1$, the left hand side is just the set of Hecke characters of C_K, and and so one needs to restrict to finite order Hecke characters to get an honest $1-1$ correspondence between these two sets of representations in this case.

This conjecture of Langlands suggests that the conjectural group $G(K)$ should contain in some way each $\mathrm{GL}_n(K)\backslash \mathrm{GL}_n(\mathbb{A}_K)$, so that the representations of $G(K)$ correspond to all Galois representations. However this situation is even more ambiguous than the state of Langlands' conjecutre above, and in any case understanding the conjecture above would be extraordinary progress to developing a non-abelian class field theory. For these reasons, we will spend the rest of our time trying to explain what the above conjecture means.

L-functions

To describe the conjecture of Langlands above*, one needs to specify exactly how the representations should correspond. The answer comes via the construction of L-functions associated to each representations. Let's first see what happens in the case $n = 1$.

Suppose χ is a 1-dimensional representation of $\mathrm{Gal}(\overline{K}/K)$. Then χ factors through a finite abelian extension

$$\chi : \mathrm{Gal}(L/K) \to \mathbb{C}^\times = \mathrm{GL}_1(\mathbb{C}).$$

If $\mathfrak{p}$ is a prime of K, recall we have a Frobenius element $\phi_\mathfrak{p} \in G(\mathfrak{P}|\mathfrak{p}) \subseteq \mathrm{Gal}(L/K)$ where $\mathfrak{P}$ is a prime of L above $\mathfrak{p}$. Then we define the L-function associated to χ to be

$$L(s, \chi) = \prod_{\mathfrak{p} \text{ unram}} \frac{1}{1 - \chi(\phi_\mathfrak{p}) N(\mathfrak{p})^{-s}}.$$

One can regard this as a generalization of the Dirichlet L-series, as specializing to the case $K = \mathbb{Q}$ and $L = \mathbb{Q}(\zeta_m)$ gives the Dirichlet L-functions mod m.

On the other hand, if ω is a Hecke character

$$\omega : C_K = K^\times \backslash \mathbb{A}_K^\times \to \mathbb{C}^\times,$$

we can view ω as a character of $\mathbb{A}_K^\times$ which is trivial on $K^\times$. This gives a character

$$\omega_v : K_v^\times \to \mathbb{C}^\times$$

for any place v of K simply by restricting to the v-component of $\mathbb{A}_K^\times$. Specifically $\omega_v(x_v) = \omega(1, \ldots, 1, x_v, 1 \ldots)$ where the x_v occurs in the v-th place. Then one can think of $\omega = \prod_v \omega_v$. When $v = \mathfrak{p}$, we say $\omega_\mathfrak{p}$ is **unramified** if $\omega_\mathfrak{p}$ is trivial on $\mathcal{O}_{K_\mathfrak{p}}^\times$. Then one can define the **Hecke L-function**

$$L(s, \omega) = \prod_{\omega_\mathfrak{p} \text{ unram}} \frac{1}{1 - \omega_\mathfrak{p}(\varpi_\mathfrak{p}) N(\mathfrak{p})^{-s}},$$

where $\varpi_\mathfrak{p}$ is a uniformizer for $\mathcal{O}_{K_\mathfrak{p}}$.

We say the Galois character χ and the Hecke character ω correspond if

$$L(s, \chi) = L(s, \omega),$$

i.e. if $\chi(\phi_\mathfrak{p}) = \omega_\mathfrak{p}(\varpi_\mathfrak{p})$ for each unramified $\mathfrak{p}$. This is the L-function interpretation of class field theory. This explicit correspondence of L-functions is amounts the explicit description of the Artin map.

Now we can define L-functions for higher-dimensional representations. Let

$$\rho : \mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}_n(\mathbb{C})$$

be an n-dimensional Galois representation. Continuity of ρ means there is a finite extension L/K such that ρ restricted to the subgroup $\mathrm{Gal}(\overline{K}/L)$ is trivial, i.e., ρ factors through

$$\rho : \mathrm{Gal}(L/K) \to \mathrm{GL}_n(\mathbb{C}).$$

*This conjecture is also called the **strong Artin conjecture** or the **modularity conjecture**. Indeed Langlands made a series of far-reaching related conjectures, so if one just says "Langlands conjecture," it is not always clear which one is being referred to.

For any prime $\mathfrak{p}$ of K and $\mathfrak{P}$ of L with $\mathfrak{P}|\mathfrak{p}$, we have a surjective homomorphism

$$G(\mathfrak{P}|\mathfrak{p}) \to \mathrm{Gal}((\mathcal{O}_L/\mathfrak{P})/(\mathcal{O}_K/\mathfrak{p})).$$

Recall the group on the left, the decomposition group of $\mathfrak{P}|\mathfrak{p}$, is just the subgroup of $\mathrm{Gal}(L/K)$ which stablizes $\mathfrak{P}$. If the inertial degree $f(\mathfrak{P}|\mathfrak{p}) = 1$, in particular if $\mathfrak{p}$ is unramified in L/K, then this map is an isomorphism and the group on the right is generated by $Fr_q : x \to x^q$ where $q = N(\mathfrak{p})$. In this case, the Frobenius element $\phi_{\mathfrak{P}|\mathfrak{p}} \in G(\mathfrak{P}|\mathfrak{p}) \subseteq \mathrm{Gal}(L/K)$. Since all the primes of L lying above $\mathfrak{p}$ are conjugate in $\mathrm{Gal}(L/K)$, all the elements $\phi_{\mathfrak{P}|\mathfrak{p}}$ are conjugate as $\mathfrak{P}$ ranges over the primes above $\mathfrak{p}$. We let the **Frobenius** $\phi_{\mathfrak{p}} = \phi_{\mathfrak{P}|\mathfrak{p}}$ for some $\mathfrak{P}$, so this is well-defined up to conjugacy. Of course if L/K is abelian, each element is its own conjugacy class, and $\phi_{\mathfrak{p}}$ is well-defined as an element of $\mathrm{Gal}(L/K)$.

Since almost all primes $\mathfrak{p}$ of K are unramified, we can define the (partial) **Artin L-function** by

$$L(s, \rho) = \prod_{\mathfrak{p} \text{ unram}} \frac{1}{\det(I_n - \rho(\phi_{\mathfrak{p}})N(\mathfrak{p})^{-s})}.$$

Note even though $\phi_{\mathfrak{p}}$ is only well defined up to conjugacy in $\mathrm{Gal}(L/K)$, the quantity $\det(I_n - \rho(\phi_{\mathfrak{p}})N(\mathfrak{p})^{-s})$ is well defined because the determinant is invariant under conjugation. We say this is a partial L-function because the full or completed Artin L-function is actually defined as a product of terms over all places v (including the archimedean ones), but the partial and the full L-function only differ by a product of finitely many terms (which are well understood). For simplicity we will not define the full L-function, but just mention that at unramified primes $\mathfrak{p}$, one needs to take into account the kernel of the map $G(\mathfrak{P}|\mathfrak{p}) \to \mathrm{Gal}((\mathcal{O}_L/\mathfrak{P})/(\mathcal{O}_K/\mathfrak{p}))$, called the inertial subgroup of $G(\mathfrak{P}|\mathfrak{p})$.

Let π be an automorphic representation of $\mathrm{GL}_n(\mathbb{A}_K) \subset \prod_v \mathrm{GL}_n(K_v)$. Then $\pi = \otimes \pi_v$ where each π_v is a representation of $\mathrm{GL}_n(K_v)$. For $v = \mathfrak{p}$, we say $\pi_{\mathfrak{p}}$ is **unramified** if $\pi_{\mathfrak{p}}$ restricted to the subgroup $\mathrm{GL}_n(\mathcal{O}_{K_{\mathfrak{p}}})$ is trivial. At such a place, π_v is induced from n 1-dimensional representations $\omega_1, \ldots, \omega_n$ placed on the diagonal subgroup of $\mathrm{GL}_n(K_v)$. Set

$$A(\pi_v) = \mathrm{diag}(\omega_1(\varpi_{\mathfrak{p}}), \ldots, \omega_n(\varpi_{\mathfrak{p}})).$$

Then we define the (partial) **automorphic L-function**

$$L(s, \pi) = \prod_{\pi_{\mathfrak{p}} \text{ unram}} \frac{1}{\det(I_n - A(\pi_{\mathfrak{p}})N(\mathfrak{p})^{-s})}.$$

Now we can restate Langlands' conjecture above in more precise terms

Conjecture 8.4.3. (Langlands) *There is a (partial)* $1-1$ *correspondence*

$$\{\textit{automorphic representations } \pi \textit{ of } \mathrm{GL}_n(\mathbb{A}_K)\} \overset{1-1}{\dashleftarrow\!\dashrightarrow} \{n\textit{-dimensional representations } \rho \textit{ of } \mathrm{Gal}(\overline{K}/K)\}$$

such that

$$L(s, \pi) = L(s, \rho),$$

i.e., for almost all primes $\mathfrak{p}$ *of* K*, we have*

$$\det(I_n - A(\pi_{\mathfrak{p}})N(\mathfrak{p})^{-s}) = \det(I_n - \rho(\phi_{\mathfrak{p}})N(\mathfrak{p})^{-s}).$$

(If the local factors—called local L-factors or local L-functions—agree for $L(s,\pi)$ and $L(s,\rho)$ for almost all places, one can show that the local factors (in the completed L-functions) will all be the same.)

The first application of **Langlands program** (this program of attaching automorphic representations to Galois representations, which has grown into a much more general setting than what we have presented) is to the following.

Conjecture 8.4.4. (Artin) *Let $\rho : \mathrm{Gal}(\overline{K}/K)$ be an irreducible nontrivial Galois representation. Then $L(s,\rho)$ is entire.*

If ρ is trivial, then $L(s,\rho) = \zeta_K(s)$, the Dedekind zeta function of K, has a pole at $s = 1$. If ρ is not trivial, Artin conjectures $L(s,\rho)$ is entire, i.e., it has no poles. (The L-function as defined, converges for $Re(s)$ large, but is known to have meromorphic continuation to the whole complex plane.) If ρ is 1-dimensional, then this is known because $\rho = \chi$ corresponds to a Hecke character ω, and the Hecke L-functions $L(s,\omega)$ for nontrivial ω are known to be entire. It is also easy to see that if ρ is induced from a 1-dimensional representation χ, then $L(s,\rho) = L(s,\chi)$ so $L(s,\rho)$ is entire.

Not much was known about Artin's conjecture for higher dimensional representations. However, it is known that if π is a *cuspidal* automorphic representation, then $L(s,\pi)$ is entire, so if $\rho \leftrightarrow \pi$, then $L(s,\rho)$ is also entire. (Any automorphic representation corresponding to a nontrivial irreducible Galois representation will be cuspidal.) Hence Langlands conjecture implies Artin's conjecture, wherefore the above conjecture of Langlands is sometimes called the strong Artin conjecture. (In fact, the strong Artin conjecture and the Artin conjecture are known to be equivalent in the case of 2 or 3 dimensional representations. It is not clear if they should be equivalent in higher dimensions.)

The first success of the Langlands program is the following result.

Theorem 8.4.5. (Langlands, Tunnell) *Suppose $\rho : \mathrm{Gal}(L/K) \to \mathrm{GL}_2(\mathbb{C})$ is an irreducible 2-dimensional representation. If the image of ρ is solvable (a solvable subgroup of $\mathrm{GL}_2(\mathbb{C})$), then $\rho \leftrightarrow \pi$ for some cuspidal automorphic representation π of $\mathrm{GL}_2(\mathbb{A}_K)$.*

This gave new instances of Artin's conjecture. We remark that Artin's conjecture, together with the Grand Riemann Hypothesis (the analogue of the Riemann Hypothesis for more general L-functions), yields estimates for the error term in the prime number theorem.

However, there is a much more famous consequence of this theorem of Langlands and Tunnell—Fermat's Last Theorem. Very roughly, Frey, Ribet and Serre showed that Fermat's Last Theorem follows from the Taniyama–Shimura conjecture, which says that to each elliptic curve over $\mathbb{Q}$, there is an associated modular form, in the sense that their associated L-functions are equal. To prove Taniyama–Shimura, one associates to an elliptic curve E a family of *p-adic* Galois representations $\rho_p : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Q}_p)$. This much is not difficult. Wiles essentially showed that (for "semistable" E, which is sufficient for Fermat's Last Theorem) one can (reduce to a case where one can) further associate to E a 2-dimensional *complex* Galois representation $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{C})$, where ρ has solvable image. Then Langlands–Tunnell applies, and ρ (and hence the elliptic curve E) corresponds to an automorphic representation π of $\mathrm{GL}_2(\mathbb{A}_\mathbb{Q})$. This representation π is naturally associated to some modular form f, and this gave Taniyama–Shimura (for semistable curves, which was enough for Fermat's last theorem—the general case was finished later), and hence Fermat's last theorem.

References

[Borevich–Shafarevich] Borevich, A. I.; Shafarevich, I. R. Number theory. Translated from the Russian by Newcomb Greenleaf. Pure and Applied Mathematics, Vol. 20 Academic Press, New York-London 1966.

[Buell] Buell, Duncan A. Binary quadratic forms. Classical theory and modern computations. Springer-Verlag, New York, 1989.

[Cassels] Cassels, J.W.S. Rational quadratic forms, Academic Press, 1978.

[Cohn] Cohn, Harvey. Advanced number theory. Reprint of A second course in number theory, 1962. Dover Books on Advanced Mathematics. Dover Publications, Inc., New York, 1980.

[Cohn2] Cohn, Harvey. A classical invitation to algebraic numbers and class fields. Universitext. Springer-Verlag, New York-Heidelberg, 1978.

[Cohn3] Cohn, Harvey. Introduction to the construction of class fields. Corrected reprint of the 1985 original. Dover Publications, Inc., New York, 1994.

[Cox] Cox, David A. Primes of the form $x^2 + ny^2$. Fermat, class field theory and complex multiplication. A Wiley-Interscience Publication. John Wiley & Sons, Inc., New York, 1989.

[Dirichlet] Dirichlet, P. G. L. Lectures on number theory. Supplements by R. Dedekind. Translated from the 1863 German original and with an introduction by John Stillwell. History of Mathematics, 16. American Mathematical Society, Providence, RI; London Mathematical Society, London, 1999.

[Frolich–Taylor] Fröhlich, A.; Taylor, M. J. Algebraic number theory. Cambridge Studies in Advanced Mathematics, 27. Cambridge University Press, Cambridge, 1993.

[Gerstein] Gerstein, Larry J. Basic quadratic forms, Graduate Studies in Mathematics, 90. American Mathematical Society, Providence, RI, 2008.

[Hurwitz] Hurwitz, Adolf. Lectures on number theory. Translated from the German and with a preface by William C. Schulz. Translation edited and with a preface by Nikolaos Kritikos. Universitext. Springer-Verlag, New York, 1986.

[Iwaniec] Iwaniec, Henryk. Topics in classical automorphic forms. Graduate Studies in Mathematics, 17. American Mathematical Society, Providence, RI, 1997.

[Janusz] Janusz, Gerald J. Algebraic number fields. Second edition. Graduate Studies in Mathematics, 7. American Mathematical Society, Providence, RI, 1996.

[Kato–Kurokawa–Saito] Kato, Kazuya; Kurokawa, Nobushige; Saito, Takeshi Number theory. 1. Fermat's dream. Translated from the 1996 Japanese original by Masato Kuwata. Translations of Mathematical Monographs, 186. Iwanami Series in Modern Mathematics. American Mathematical Society, Providence, RI, 2000.

[Landau] Landau, Edmund. Elementary number theory. Translated by J. E. Goodman. Chelsea Publishing Co., New York, N.Y., 1958.

[Lang] Lang, Serge. Algebraic number theory. Second edition. Graduate Texts in Mathematics, 110. Springer-Verlag, New York, 1994.

[Marcus] Marcus, Daniel A. Number fields. Universitext. Springer-Verlag, New York-Heidelberg, 1977.

[Martin] Martin, Kimball. Non-unique factorizations and principalization in number fields, *Preprint.*

[Murty–Esmonde] Murty, M. Ram; Esmonde, Jody Problems in algebraic number theory. Second edition. Graduate Texts in Mathematics, 190. Springer-Verlag, New York, 2005.

[Narkiewicz] Narkiewicz, Wladyslaw. Elementary and analytic theory of algebraic numbers. Third edition. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2004.

[Neukirch] Neukirch, Jürgen. Algebraic number theory. Translated from the 1992 German original and with a note by Norbert Schappacher. With a foreword by G. Harder. Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], 322. Springer-Verlag, Berlin, 1999.

[Ono] Ono, Takashi. An introduction to algebraic number theory. Translated from the second Japanese edition by the author. The University Series in Mathematics. Plenum Press, New York, 1990.

[Ramakrishnan–Valenza] Ramakrishnan, Dinakar; Valenza, Robert J. Fourier analysis on number fields. Graduate Texts in Mathematics, 186. Springer-Verlag, New York, 1999.

[Scharlau–Opolka] Scharlau, Winfried; Opolka, Hans From Fermat to Minkowski. Lectures on the theory of numbers and its historical development. Translated from the German by Walter K. B?hler and Gary Cornell. Undergraduate Texts in Mathematics. Springer-Verlag, New York, 1985.

[Serre] Serre, J.-P. A course in arithmetic. Translated from the French. Graduate Texts in Mathematics, No. 7. Springer-Verlag, New York-Heidelberg, 1973.

[Stewart–Tall] Stewart, Ian; Tall, David. Algebraic number theory and Fermat's last theorem. Third edition. A K Peters, Ltd., Natick, MA, 2002.