Lectures on the Dirichlet Class Number Formula for Imaginary Quadratic Fields

Tom Weston

Contents

Introduction

These notes were written to serve as a companion to a series of five lectures I presented at the Ross mathematics program from July 26 to July 30, 2004. The first chapter is an expanded version of a lecture I have given many times stating the Dirichlet class number formula for imaginary quadratic fields in terms of complex lattices. The remainder of the notes are a proof of this formula.

The primary motivation behind these notes was the sudden realization that the proof of the class number formula for imaginary quadratic fields is in fact not terribly difficult. As is well known, this is primarily due to the finiteness of the group of units in this case. In fact, several topics (most notably Euler products) in the notes are not even strictly needed for the proof of the class number formula but are included because they help to illuminate the key ideas (and also because I had already written up some of the material before realizing that it was unnecessary.)

Although most of these notes were written without consulting outside sources, there are a few exceptions which I should call attention to. The proof that complex lattices are classified by the fundamental domain is based on that in [**4**, Theorem VII.1]. The approach to the proof of unique factorization of ideals is inspired by that of [**1**, Section XI.8]. The material on Dirichlet series is a synthesis of that in [**2**, Lemma VII.1] and [**3**, Theorem 7.11] (rewritten to avoid any explicit discussion of absolute convergence). Finally, the proof of the key estimate on lattice points of bounded absolute value is taken from [**2**, pp. 160–161].

The reader interested in further pursuing these topics is strongly encouraged to begin with [**2**] and [**4**].

It is a pleasure to thank Rob Benedetto and Keith Conrad for helping me to overcome my inherent inability to do analysis during the preparation of these notes.

CHAPTER 1

Complex lattices and infinite sums of Legendre symbols

1. Complex lattices

Definition 1.1. A *complex lattice* Λ is a subset $\Lambda \subseteq \mathbf{C}$ of the complex numbers for which there exists $\alpha, \beta \in \Lambda$ such that:

(1) α, β are not real multiples of one another;
(2) Λ is precisely the set of integer linear combinations of α and β:

$$\Lambda = \big\{ m\alpha + n\beta \,;\, m, n \in \mathbf{Z} \big\}.$$

Any such pair α, β is called a *basis* of Λ. The basis is said to be *normalized* if the imaginary part of β/α is positive.

Let α, β be a basis of a complex lattice Λ. Note that the condition (1) is equivalent to the condition that both α and β are non-zero and that the ratio β/α is not real. In particular, since

$$\operatorname{im}\left(\frac{\alpha}{\beta}\right) = -\frac{|\alpha|^2}{|\beta|^2} \cdot \operatorname{im}\left(\frac{\beta}{\alpha}\right)$$

it follows that for a basis α, β of Λ exactly one of the orderings α, β and β, α yields a normalized basis of Λ. (The normalization is really just a convenient choice of ordering and should not be taken too seriously.)

Example 1.2. The simplest way to give examples of complex lattices is by specifying a basis. Let α, β be non-zero complex numbers such that the imaginary part of β/α is positive. Then α, β are a normalized basis of the lattice

$$\langle \alpha, \beta \rangle := \big\{ m\alpha + n\beta \,;\, m, n \in \mathbf{Z} \big\}.$$

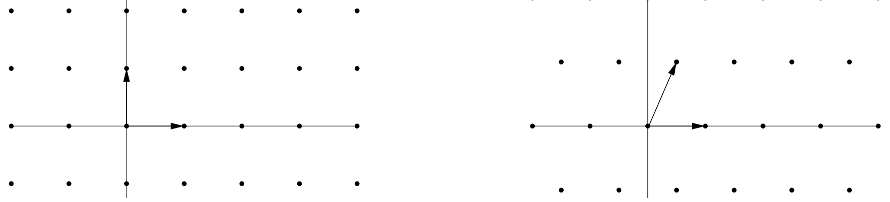

FIGURE 1. The lattices $\langle 1, i \rangle$ and $\langle 2, 1 + \sqrt{-5} \rangle$

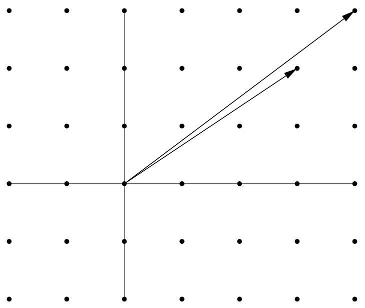

FIGURE 2. The lattice $\langle 3+2i, 4+3i\rangle$

As the example of $\langle 1, i\rangle$ and $\langle 3+2i, 4+3i\rangle$ shows, a given complex lattice has many different normalized bases. It is not difficult to give a complete description of all possible bases of a complex lattice. Indeed, let Λ be a complex lattice with normalized basis α, β. Let α', β' be another basis of Λ. Then in particular $\alpha', \beta' \in \Lambda$, so that they can be expressed as integer linear combinations of α and β: that is, there exist integers a, b, c, d such that

$$\alpha' = a\alpha + b\beta \tag{1}$$

$$\beta' = c\alpha + d\beta. \tag{2}$$

On the other hand, since α', β' are a basis of Λ, we can also write α, β as integer linear combinations of α', β': there exist integers a', b', c', d' such that

$$\alpha = a'\alpha' + b'\beta' \tag{3}$$

$$\beta = c'\alpha' + d'\beta'. \tag{4}$$

Substituting (1) and (2) into (3) we find that

$$\alpha = (a'a + b'c)\alpha + (a'b + b'd)\beta.$$

However, since α, β are assumed to not be real multiples of one another, this can only hold if

$$a'a + b'c = 1 \qquad \text{and} \qquad a'b + b'd = 0.$$

Solving these equations for a', b' yields

$$a' = \frac{d}{ad - bc}$$
$$b' = \frac{-b}{ad - bc}.$$

(Note that we must have $ad - bc \neq 0$, for otherwise we would have $b = d = 0$ in which case α' and β' would both be multiplies of α and thus could not possibly be a basis.) Similarly, substituting (1) and (2) into (4) we find that

$$c' = \frac{-c}{ad - bc}$$
$$d' = \frac{a}{ad - bc}.$$

In particular, $ad - bc$ divides the greatest common divisor e of a, b, c, d. On the other hand, clearly e^2 divides $ad - bc$. It follows that $e = \pm 1$, so that $ad - bc = \pm 1$. These steps are reversible, so that we have proven the first half of the next lemma.

LEMMA 1.3. *Let Λ be a complex lattice and let α, β be a normalized basis of Λ. Let $a, b, c, d \in \mathbf{Z}$ satisfy $ad - bc = \pm 1$. Then*

$$a\alpha + b\beta, c\alpha + d\beta$$

is also a basis of Λ and every basis of Λ has this form for some a, b, c, d as above. It is a normalized basis if and only if $ad - bc = 1$.

PROOF. It remains to prove the last statement. Set $j = \beta/\alpha$ and let x, y denote the real and imaginary part of j. We compute

$$\begin{aligned}\frac{c\alpha + d\beta}{a\alpha + b\beta} &= \frac{c + dj}{a + bj} \\ &= \frac{(c + dj)(a + b\bar{j})}{(a + bj)(a + b\bar{j})} \\ &= \frac{ac + adj + bc\bar{j} + bdj\bar{j}}{|a + bj|^2} \\ &= \frac{(ac + adx + bcx + bd|j|^2) + (ad - bc)yi}{|a + bj|^2}.\end{aligned}$$

Here $\bar{j} = x - yi$ is the complex conjugate of j. We thus obtain the crucial formula

$$\operatorname{im}\left(\frac{c + dj}{a + bj}\right) = \frac{ad - bc}{|a + bj|^2} \cdot \operatorname{im}(j). \tag{5}$$

Since $\operatorname{im}(j) > 0$ by assumption, this shows that $a\alpha + b\beta, c\alpha + d\beta$ is still normalized if and only if $ad - bc$ is positive, and thus if and only if $ad - bc = 1$. □

2. Homothety

We now consider the question of determining all possible shapes of lattices. Here we consider two complex lattices Λ and Λ' to have the "same shape" if one can be rotated and scaled to yield the other. (There is no need to consider translations since the origin gives a fixed common point in each lattice.)

We can take advantage of the arithmetic of the complex numbers to give a remarkably simple description of this relationship. To do this we need to consider rotations in the the complex plane. Let $x + yi$ be a complex number and let θ be an angle. By simple trigonometry, one finds that the point obtained from $x + yi$ by rotating counterclockwise about the origin by the angle θ is

$$(x \cos\theta - y \sin\theta) + (x \sin\theta + y \cos\theta)i.$$

This complex number can also be written as

$$(\cos\theta + i \sin\theta) \cdot (x + yi).$$

By Euler's formula $e^{i\theta} = \cos\theta + i \sin\theta$ we can further simplify this to

$$e^{i\theta} \cdot (x + yi).$$

That is, one can rotate a complex number by an angle θ simply by multiplying by $e^{i\theta}$.

Suppose now that Λ and Λ' have the same shape. This should mean that there is a positive real number r and an angle θ such that every element of Λ' is obtained by rotating by θ and scaling by r some element of Λ. That is,

$$\begin{aligned}\Lambda' &= \{re^{i\theta}\cdot\lambda\,;\ \lambda\in\Lambda\}\\ &= re^{i\theta}\cdot\Lambda.\end{aligned}$$

Since every complex number can be written in the form $re^{i\theta}$ (its *polar form*), this suggests the following simple definition, which we will use as our precise definition of two lattices having the "same shape".

Definition 1.4. Two complex lattices Λ, Λ' are *homothetic*, written $\Lambda \sim \Lambda'$, if there is a non-zero complex number γ such that

$$\Lambda' = \gamma\cdot\Lambda.$$

One checks immediately that this is an equivalence relation on the set of complex lattices; that is, the relation of homothety is reflexive, symmetric and transitive.

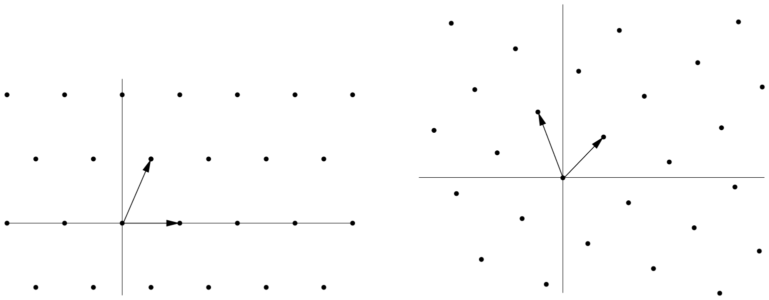

FIGURE 3. The lattices $\langle 2, 1+\sqrt{-5}\rangle$ and $(1+i)\cdot\langle 2, 1+\sqrt{-5}\rangle$

Our goal in the remainder of this section is to classify all complex lattices up to homothety. That is, we would like to be able to give a reasonably simple set of complex lattices such that any given complex lattice Λ is homothetic to exactly one of the given ones, and we would like to have an algorithm to determine which one it is.

A naive solution to this problem is as follows. Consider a complex lattice $\Lambda = \langle\alpha,\beta\rangle$. Then the lattices homothetic to Λ are precisely the lattices

$$\langle\gamma\alpha,\gamma\beta\rangle$$

as γ runs through the non-zero complex numbers. Said differently, $\langle\alpha,\beta\rangle$ is homothetic to $\langle\alpha',\beta'\rangle$ if $\beta/\alpha = \beta'/\alpha'$.

While this analysis is correct, it is only half of the story. The other half is the fact that a given lattice has many different bases. In particular, $\langle\alpha,\beta\rangle$ and $\langle\alpha',\beta'\rangle$ may well be homothetic even if $\beta/\alpha \neq \beta'/\alpha'$, since some other pair of bases could have the same ratio. We will get around this difficulty in the clumsiest possible way: rather than considering the ratio of a single basis of Λ, we will consider the ratios of every basis of Λ.

Definition 1.5. Let Λ be a complex lattice. The $\mathcal{J}$*-set* of Λ is the set

$$\mathcal{J}(\Lambda) := \left\{\frac{\beta}{\alpha}\,;\ \alpha,\beta \text{ normalized basis of } \Lambda\right\}.$$

Note that $\mathcal{J}(\Lambda)$ is a subset of the set of all complex numbers with positive imaginary part.

Let Λ be a lattice and choose a normalized basis α, β. Set $j = \beta/\alpha$. We determined all possible bases of Λ in Lemma 1.3, so that the $\mathcal{J}$-set of Λ is simply

$$\begin{aligned} \mathcal{J}(\Lambda) &= \left\{ \frac{c\alpha + d\beta}{a\alpha + b\beta} \,;\, a, b, c, d \in \mathbf{Z}, ad - bc = 1 \right\} \\ &= \left\{ \frac{c + dj}{a + bj} \,;\, a, b, c, d \in \mathbf{Z}, ad - bc = 1 \right\}. \end{aligned} \tag{6}$$

Taking (a, b, c, d) equal to $(1, 0, 1, 1)$ and $(0, 1, -1, 0)$ shows in particular that

$$j + 1, \frac{-1}{j} \in \mathcal{J}(\Lambda). \tag{7}$$

(Said differently, this corresponds to the simple fact that if α, β is a normalized basis of Λ, then so are $\alpha, \alpha + \beta$ and $-\beta, \alpha$.) Of course, we could have started with a basis α', β' of Λ giving rise to any ratio $j' \in \mathcal{J}(\Lambda)$, so that the relation (7) holds for any element $j \in \mathcal{J}(\Lambda)$: that is, the set $\mathcal{J}(\Lambda)$ is closed under translation by 1 in the real direction (which is not difficult to visualize) and under negative reciprocals (which is much harder to visualize). We give two examples of $\mathcal{J}$-sets below.

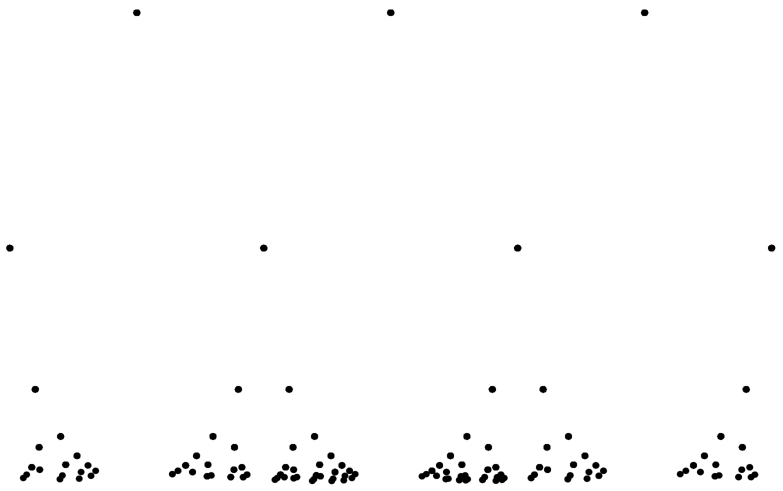

FIGURE 4. $\mathcal{J}(1, i)$

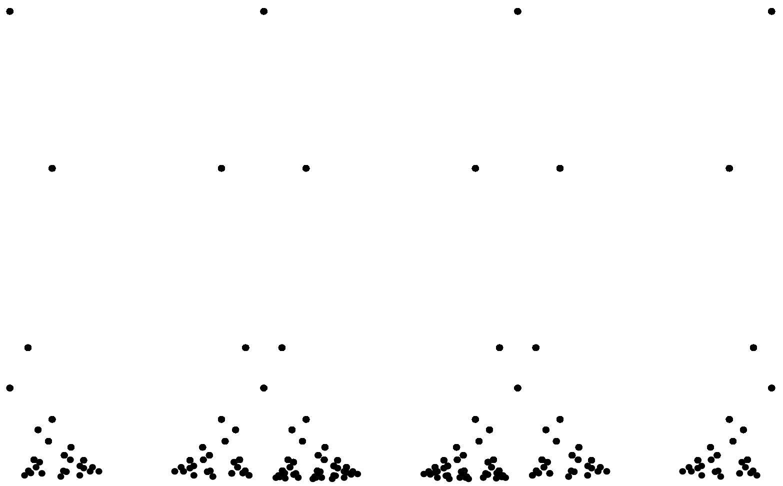

FIGURE 5. $\mathcal{J}(2, 1+\sqrt{-5})$

The next lemma gives the sense in which $\mathcal{J}$-sets are a (rather unsatisfactory) solution to the homothety classification problem. It shows that two lattices are homothetic if and only if they have identical $\mathcal{J}$-sets. Of course, it is not immediately clear how to verify that two $\mathcal{J}$-sets are identical, so that this lemma is not immediately useful.

LEMMA 1.6. *Let Λ be a complex lattice.*

(1) *Let j be a complex number with positive imaginary part. Then $\Lambda \sim \langle 1, j\rangle$ if and only if $j \in \mathcal{J}(\Lambda)$.*
(2) *Let Λ' a second complex lattice. Then*

$$\Lambda \sim \Lambda' \quad \Leftrightarrow \quad \mathcal{J}(\Lambda) = \mathcal{J}(\Lambda') \quad \Leftrightarrow \quad \mathcal{J}(\Lambda) \cap \mathcal{J}(\Lambda') \neq \emptyset.$$

PROOF.

(1) Suppose first that $j \in \mathcal{J}(\Lambda)$. Then there is a normalized basis α, β of Λ with $j = \beta/\alpha$. Thus

$$\Lambda = \langle \alpha, \beta\rangle = \alpha \cdot \langle 1, j\rangle \sim \langle 1, j\rangle .$$

Conversely, if $\Lambda \sim \langle 1, j\rangle$, then there is a complex number γ such that $\gamma, \gamma j$ is a normalized basis of Λ. Thus $j = \gamma j/\gamma$ lies in $\mathcal{J}(\Lambda)$, as desired.

(2) Suppose first that $\Lambda \sim \Lambda'$. Then there is a non-zero complex number γ such that $\Lambda' = \gamma \cdot \Lambda$, so that every normalized basis of Λ' is obtained by scaling a normalized basis of Λ by γ. It follows that $\mathcal{J}(\Lambda) = \mathcal{J}(\Lambda')$. That the second condition implies the third is obvious. Finally, suppose that $\mathcal{J}(\Lambda) \cap \mathcal{J}(\Lambda') \neq \emptyset$ and fix j in this intersection. Then by (1) we have

$$\Lambda \sim \langle 1, j\rangle \sim \Lambda',$$

as desired.

□

Lemma 1.6 proves much more than that homothetic lattices have identical $\mathcal{J}$-sets: it shows that to show that two lattices are homothetic it suffices to find a single common element in their $\mathcal{J}$-sets. In particular, if we could somehow pick out a particular element of the $\mathcal{J}$-set, in a way which does not depend on the original lattice, then this single element would entirely describe the homothety class of lattices with this $\mathcal{J}$-set. That is, we would like to define a complex number $j(\Lambda) \in \mathcal{J}(\Lambda)$ in some way that makes no reference to the lattice Λ but only to the set $\mathcal{J}(\Lambda)$. It will then follow from Lemma 1.6 that two lattices Λ, Λ' are homothetic if and only if $j(\Lambda) = j(\Lambda')$.

There are many possible ways to do this. The one we choose is based on (7) and a visual inspection of the $\mathcal{J}$-sets for $\langle 1, i\rangle$ and $\langle 2, 1+\sqrt{-5}\rangle$. It appears in the examples that the elements of a $\mathcal{J}$-set are clustered near the real axis, becoming more and more sparse as the imaginary part increases, until at some point a maximum imaginary part is reached. We begin by proving this.

Lemma 1.7. *Let Λ be a complex lattice. Then for any $j \in \Lambda$, the set*

$$\{\mathrm{im}(j')\,;\, j' \in \mathcal{J}(\Lambda), \mathrm{im}(j') > \mathrm{im}(j)$$

is finite.

Proof. Recall that by (6) we have

$$\mathcal{J}(\Lambda) = \left\{ \frac{c+dj}{a+bj}\,;\, a,b,c,d \in \mathbf{Z}, ad-bc=1 \right\}.$$

By (5) we also have

$$\mathrm{im}\left(\frac{c+dj}{a+bj}\right) = \frac{1}{|a+bj|^2}\cdot \mathrm{im}(j).$$

In particular,

$$\mathrm{im}\left(\frac{c+dj}{a+bj}\right) > \mathrm{im}(j)$$

if and only if $|a+bj| < 1$. However, there are only finitely many integers a, b with this property. Indeed, $|a+bj| \geq 1$ as soon as $|b| \geq 1/\mathrm{im}(j)$, while for each of the finitely many b with $|b| < 1/\mathrm{im}(j)$ there are at most two values of a such that $|a+bj| < 1$. Any imaginary part in $\mathcal{J}(\Lambda)$ larger than $\mathrm{im}(j)$ must come from one of these finitely many pairs (a,b), so that there are at most finitely many such imaginary parts. □

It follows from Lemma 1.7 that the (infinite) set

$$\{\mathrm{im}(j)\,;\, j \in \mathcal{J}(\Lambda)\}$$

has a maximum element; indeed, we simply have to choose any $j_0 \in \mathcal{J}(\Lambda)$ and then select among the finitely many imaginary parts larger than that $\mathrm{im}(j_0)$. (Note that we are not asserting that there are only finitely many $j \in \mathcal{J}(\Lambda)$ with $\mathrm{im}(j) > \mathrm{im}(j_0)$, but rather that among the possibly infinitely many such j there are only finitely many different values of $\mathrm{im}(j)$.)

Note that if $j \in \mathcal{J}(\Lambda)$ has maximum imaginary part, then certainly $|j| \geq 1$ since otherwise $-1/j \in \mathcal{J}(\Lambda)$ would have larger imaginary part. Also, $j+m \in \mathcal{J}(\Lambda)$ also has maximum imaginary part for any $m \in \mathbf{Z}$. In particular, in our effort to pick out a distinguished element of $\mathcal{J}(\Lambda)$, we might as well require that the real part is as small as possible: we can certainly obtain a real part between $-\frac{1}{2}$ and $\frac{1}{2}$. Being a bit careful about the boundaries, we are thus led to consider the region $\mathcal{F} \subseteq \mathbf{C}$ defined by

$$\mathcal{F} = \left\{ z \in \mathbf{C}\,;\ \mathrm{im}(z) > 0, |z| \geq 1, -\frac{1}{2} < \mathrm{re}(z) \leq \frac{1}{2} \text{ and } \mathrm{re}(z) \geq 0 \text{ if } |z| = 1 \right\}.$$

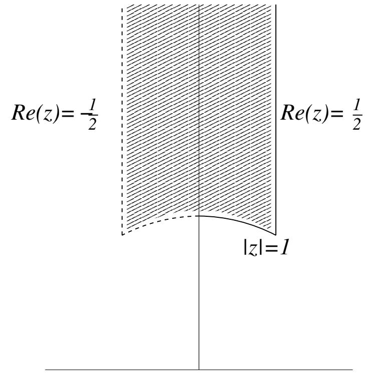

FIGURE 6. The domain $\mathcal{F}$

PROPOSITION 1.8. *Let Λ be a complex lattice. The intersection $\mathcal{J}(\Lambda) \cap \mathcal{F}$ consists of exactly one element, which we call $j(\Lambda)$.*

PROOF. We have seen above that $\mathcal{J}(\Lambda) \cap \mathcal{F}$ contains at least one element. Suppose that it contains two elements j_1, j_2; we must show that $j_1 = j_2$. We may assume without loss of generality that $\mathrm{im}(j_1) \geq \mathrm{im}(j_2)$. There exist $a, b, c, d \in \mathbf{Z}$, $ad - bc = 1$, such that

$$j_1 = \frac{c + dj_2}{a + bj_2}$$

and thus as before

$$\mathrm{im}(j_1) = \frac{1}{|a + bj_2|^2} \cdot \mathrm{im}(j_2).$$

Thus $|a+bj_2| \leq 1$. However, certainly $\mathrm{im}(j_2) \geq \sqrt{3}/2$ since $j_2 \in \mathcal{F}$. Thus $|a+bj_2| \geq \sqrt{3}b/2$, so that we can only have $|a + bj_2| \leq 1$ if $b = -1, 0, 1$.

If $b = 0$, then $a = \pm 1$; as $ad - bc = 1$, we thus must have $d = a$. Therefore

$$j_1 = j_2 \pm c.$$

Since $\mathcal{F}$ does not contain any elements differing by a non-zero integer, it follows that $j_1 = j_2$, as desired. The cases of $b = \pm 1$ are similar and left to the exercises. □

Proposition 1.8 gives the first part of the classification of complex lattices up to homothety: every complex lattice is homothetic to a unique lattice of the form $\langle 1, j \rangle$ with $j \in \mathcal{F}$ (namely $\langle 1, j(\Lambda) \rangle$), and no two lattices $\langle 1, j \rangle$ and $\langle 1, j' \rangle$ with $j, j' \in \mathcal{F}$, $j \neq j'$ are homothetic. Our last task is to give a computational method for determining $j(\Lambda)$ for a lattice Λ. We will give an algorithm that allows one to compute $j(\Lambda)$ given any single element $j \in \mathcal{J}(\Lambda)$ (which in turn can be obtained as the ratio of a normalized basis of Λ).

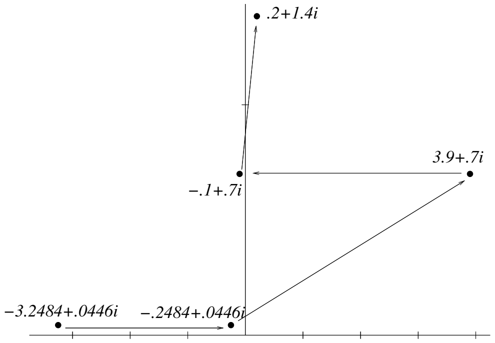

FIGURE 7. Computing $j(1, -3.2484 + .0446i)$

PROPOSITION 1.9. *Let Λ be a lattice and fix $j \in \mathcal{J}(\Lambda)$. Then $j(\Lambda)$ can be obtained via the following algorithm.*

(1) *Set $j_0 = j$ and $k = 0$.*
(2) *Let $j_{k+1} = j_k + m$ for the unique $m \in \mathbf{Z}$ such that*

$$-\frac{1}{2} < \operatorname{re}(j_k + m) \leq \frac{1}{2}.$$

(3) *If $j_{k+1} \in \mathcal{F}$, then $j(\Lambda) = j_{k+1}$. If not, then let $j_{k+2} = -1/j_{k+1}$.*
(4) *If $j_{k+2} \in \mathcal{F}$, then $j(\Lambda) = j_{k+2}$. If not, then return to step 2, replacing k by $k + 2$.*

PROOF. Note first that $j_k \in \mathcal{J}(\Lambda)$ for all $k \geq 0$, as $j_0 \in \mathcal{J}(\Lambda)$ and $\mathcal{J}(\Lambda)$ is closed under integer translation and negative reciprocals. It thus suffices to show that for some k we have $j_k \in \mathcal{F}$.

We have $\operatorname{im}(j_{k+1}) \geq \operatorname{im}(j_k)$ for all k. Indeed, this is clear for k even (since then $\operatorname{im}(j_{k+1}) = \operatorname{im}(j_k)$), while for k odd it follows from the fact that if $j_k \notin \mathcal{F}$ for k odd, then $|j_k| \leq 1$, so that

$$\operatorname{im}(j_{k+1}) = \frac{1}{|j_k|^2} \cdot \operatorname{im}(j_k) \geq \operatorname{im}(j_k).$$

Suppose now that there is some odd k such that $j_k \notin \mathcal{F}$ and $\operatorname{im}(j_{k+1}) = \operatorname{im}(j_k)$. We must then have $|j_k| = |j_{k+1}| = 1$. However, $|\operatorname{re}(j_k)| \leq \frac{1}{2}$ since k is odd. As $j_k \notin \mathcal{F}$, it follows from the definition of the boundary of $\mathcal{F}$ that this can only occur if $\operatorname{re}(j_k) < 0$. But then $j_{k+1} = -\operatorname{re}(j_k) + \operatorname{im}(j_k)i \in \mathcal{F}$, so that the algorithm terminates at this step.

Otherwise we have $\operatorname{im}(j_{k+1}) > \operatorname{im}(j_k)$ for all odd k. But by Lemma 1.7 this can not continue forever, so that we must eventually have $j_k \in \mathcal{F}$. □

3. Complex multiplication

Let Λ be a complex lattice and let γ be a complex number. If γ is an integer, then $\gamma \cdot \Lambda$ is always a sublattice of Λ (that is, a subset of Λ which is itself a complex lattice) which is homothetic to Λ. If γ is not an integer, then $\gamma \cdot \Lambda$ is still homothetic to Λ, but it is probably not a sublattice of Λ. Occasionally, however, $\gamma \cdot \Lambda$ is still a sublattice of Λ.

DEFINITION 1.10. Let γ be a complex number which is not an integer. A complex lattice Λ is said to have *complex multiplication by* γ if $\gamma \cdot \Lambda$ is a sublattice of Λ. We also refer to Λ as a *CM lattice* and say that it has *CM by* γ.

That is, a CM lattice is a lattice Λ which has a sublattice, different from the obvious sublattices $n \cdot \Lambda$ for $n \in \mathbf{Z}$, which is homothetic to Λ itself. The examples below show that $\langle 1, i \rangle$ has CM by i (note that in this case $i \cdot \langle 1, i \rangle$ actually equals $\langle 1, i \rangle$. This is quite rare; see Exercise 1.3), $\left\langle 2, 1 + \sqrt{-5} \right\rangle$ has CM by $\sqrt{-5}$, and that $\left\langle 1, \frac{3}{4} + \frac{5}{4} i \right\rangle$ does not have CM by i.

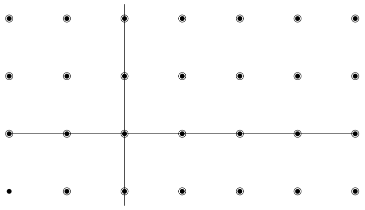

FIGURE 8. The lattices $\langle 1, i \rangle$ and $i \cdot \langle 1, i \rangle$

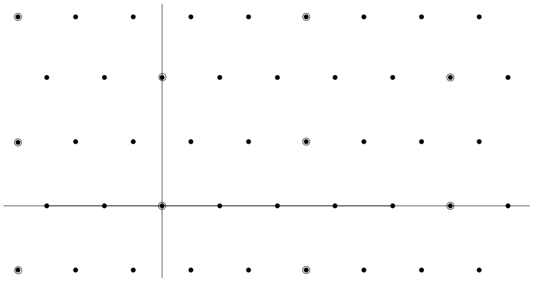

FIGURE 9. The lattices $\left\langle 2, 1 + \sqrt{-5} \right\rangle$ and $\sqrt{-5} \cdot \left\langle 2, 1 + \sqrt{-5} \right\rangle$

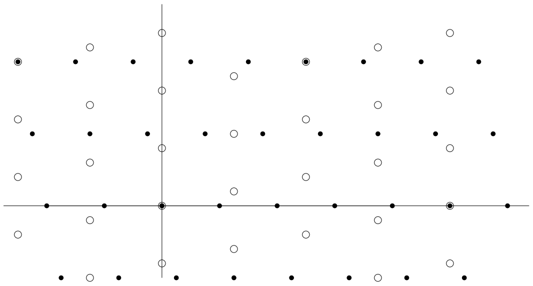

FIGURE 10. The lattices $\left\langle 1, \frac{3}{4} + \frac{5}{4} i \right\rangle$ and $i \cdot \left\langle 1, \frac{3}{4} + \frac{5}{4} i \right\rangle$

One might guess that any lattice has CM by some γ, and that for any $\gamma \in \mathbf{C}-\mathbf{Z}$ there are many lattices with CM by γ. Surprisingly, this guess is very far from the truth.

Lemma 1.11. *Let Λ be a complex lattice with CM by γ. Then*

$$\gamma = \tfrac{1}{2}(B \pm \sqrt{B^2-4C}) \tag{8}$$

for some integers B, C with $B^2-4C<0$.

Proof. Let α, β be a basis for Λ. Since $\gamma \cdot \Lambda$ is a sublattice of Λ, both $\gamma \cdot \alpha$ and $\gamma \cdot \beta$ must lie in Λ. That is, there are integers a, b, c, d such that

$$\gamma \cdot \alpha = a \cdot \alpha + b \cdot \beta$$
$$\gamma \cdot \beta = c \cdot \alpha + d \cdot \beta.$$

(Note that this immediately implies that γ is not real: if it were, then we must have $b=0$ since β is not a real multiple of α. But then $\gamma = a$ is an integer, which is not allowed.) Thus

$$\gamma = a + b \cdot \frac{\beta}{\alpha}$$
$$\gamma = c \cdot \frac{\alpha}{\beta} + d.$$

Therefore

$$\frac{\gamma - a}{b} = \frac{c}{\gamma - d}$$

so that

$$\gamma^2 - (a+d)\gamma + (ad-bc) = 0.$$

Taking $B = a+d$ and $C = ad-bc$ and applying the quadratic formula now gives the above formula. □

We can improve somewhat on Lemma 1.11. By Exercise 1.2 a lattice Λ has CM by γ if and only if it has CM by $\gamma + n$ for any integer n. If B in (8) is even, we thus may replace γ by

$$\sqrt{\left(\frac{B}{2}\right)^2 - C},$$

while if B is odd we may replace γ by

$$\frac{1}{2} + \frac{1}{2}\sqrt{B^2-4C}$$

where $B^2 - 4C \equiv 1 \pmod 4$. That is, it suffices to consider lattices with CM by numbers of the form

$$\sqrt{-n} \text{ or } \frac{1+\sqrt{-n}}{2} \text{ for } n \equiv 3 \pmod 4$$

with n a positive integer.

For the remainder of this chapter we will focus on the case of CM by $\sqrt{-n}$ with $n \equiv 1, 2 \pmod 4$ squarefree. The other case of special interest is that of CM by $\frac{1+\sqrt{-n}}{2}$ for $n \equiv 3 \pmod 4$ squarefree; we leave this case to the exercises.

For $n \equiv 1, 2 \pmod 4$ let Λ be a lattice with CM by $\sqrt{-n}$: that is,

$$\sqrt{-n} \cdot \Lambda \subseteq \Lambda.$$

If $\gamma \cdot \Lambda$ is homothetic to Λ, then

$$\sqrt{-n} \cdot (\gamma \cdot \Lambda) = \gamma \cdot (\sqrt{-n} \cdot \Lambda) \subseteq \gamma \cdot \Lambda$$

so that $\gamma \cdot \Lambda$ also has CM by $\sqrt{-n}$. That is, complex multiplication is preserved by homothety. It thus makes sense to look for all homothety classes of lattices with CM by $\sqrt{-n}$. Equivalently, since any lattice is homothetic to a unique lattice $\langle 1, j\rangle$ with $j \in \mathcal{F}$, it is the same to find all $j \in \mathcal{F}$ such that $\langle 1, j\rangle$ has CM by $\sqrt{-n}$.

This is an easy application of the results of the previous section. We have

$$\sqrt{-n} \cdot \langle 1, j\rangle \subseteq \langle 1, j\rangle$$

if and only if there exist integers a, b, c, d such that

$$\sqrt{-n} = -a + bj$$
$$\sqrt{-n} \cdot j = c + dj.$$

(The reason for the extraneous sign will become clear momentarily.) Thus

$$j = \frac{a + \sqrt{-n}}{b}.$$

Solving the second equation for c we also find that

$$\frac{ad + n}{b} + \frac{d - a}{b}\sqrt{-n} = c.$$

Since c is an integer and $\sqrt{-n}$ is imaginary, this means that we must have $a = d$ and $a^2 + n$ must be divisible by b. The steps above are reversible, so that we have obtained the following theorem.

Theorem 1.12. *Let $n \equiv 1, 2 \pmod 4$ be a squarefree positive integer. Then every lattice with CM by $\sqrt{-n}$ is homothetic to a unique lattice of the form*

$$\left\langle 1, \frac{a + \sqrt{-n}}{b} \right\rangle$$

with:

(1) $a, b \in \mathbf{Z}$;
(2) $0 < b \leq 2\sqrt{\frac{n}{3}}$;
(3) $-b < 2a \leq b$;
(4) $a^2 + n \geq b^2$ *(and $a \geq 0$ if $a^2 + n = b^2$);*
(5) b *divides* $a^2 + n$.

Proof. We saw above that every lattice with CM by $\sqrt{-n}$ is homothetic to a unique lattice $\left\langle 1, \frac{a+\sqrt{-n}}{b} \right\rangle$ with $a, b \in \mathbf{Z}$, $a^2 + n$ divisible by b and $\frac{a+\sqrt{-n}}{b} \in \mathcal{F}$. The conditions (3) and (4) simply express the latter fact. Condition (2) is in fact redundant (it is implied by (3) and (4)) but is convenient to have written down anyway. □

Definition 1.13. Let n be a squarefree positive integer which is congruent to 1 or 2 modulo 4. We define the *class group $\mathcal{C}l(-n)$* to be the set of complex numbers $\frac{a+\sqrt{-n}}{b}$ satisfying the above conditions (1)–(5).

We will see later that $\mathcal{C}l(-n)$ indeed has a natural (although not at all obvious) structure of abelian group. For the time being we content ourselves with the following fact.

Corollary 1.14. *The class group $\mathcal{C}l(-n)$ is finite.*

Proof. It is clear from (2) and (3) that there are at most finitely many pairs of integers a, b satisfying the conditions (1)–(5) of Theorem 1.12. $\square$

We define the *class number* $h(-n)$ to be the size of $\mathcal{C}l(-n)$: that is, it is the number of homothety classes of lattices with CM by $\sqrt{-n}$. (This is not really the optimal definition if n is not of the form we have been considering, which is why we have restricted to this case.)

Example 1.15. We compute $\mathcal{C}l(-5)$ using Theorem 1.12. By (2) we must have $1 \leq b \leq 2\sqrt{\frac{5}{3}} < 3$. For $b = 1$ we must have $a = 0$ by (2). The pair $(0, 1)$ satisfies (4) and (5), so that it yields one element of $\mathcal{C}l(-5)$. For $b = 2$ we must have $a = 0, 1$ by (2), but only the pair $(1, 2)$ satisfies (5). Thus

$$\mathcal{C}l(-5) = \left\{ \sqrt{-5}, \frac{1 + \sqrt{-5}}{2} \right\}$$

so that $h(-5) = 2$. The first j-invariant corresponds to the rectangular lattice $\langle 1, \sqrt{-5} \rangle$, while the second corresponds to the lattice $\langle 2, 1 + \sqrt{-5} \rangle$ of Figure 1.

Example 1.16. We compute $\mathcal{C}l(-14)$ using Theorem 1.12. By (2) we have $1 \leq b \leq 2\sqrt{\frac{14}{3}} < 5$. For $b = 1$, by (3) we must have $a = 0$. The pair $(0, 1)$ satisfies (4) and (5), so that this gives one element of $\mathcal{C}l(-14)$. For $b = 2$ we must have $a = 0, 1$, but only $(0, 2)$ satisfies (5). For $b = 3$ we must have $a = -1, 0, 1$, but only $(-1, 3)$ and $(1, 3)$ satisfy (5). Finally, for $b = 4$ we have $a = -1, 0, 1, 2$, but none of these pairs satisfy both (4) and (5). We conclude that

$$\mathcal{C}l(-14) = \left\{ \sqrt{-14}, \frac{\sqrt{-14}}{2}, \frac{-1 + \sqrt{-14}}{3}, \frac{1 + \sqrt{-14}}{3} \right\}$$

and thus $h(-14) = 4$.

For later reference we give a brief table of class numbers $h(-n)$ for selected squarefree $n \equiv 1, 2 \pmod 4$. These are all easily computed using Theorem 1.12 (and a computer program for the last two).

n	2	5	6	10	13	14	17	21	22	26	29	30	15701	2905509
$h(-n)$	1	2	2	2	2	4	4	4	2	6	6	4	132	2188

4. L-series

We now turn to something completely different. For a squarefree integer n let

$$L(-n) = \sum_{m=1}^{\infty} \left(\frac{-n}{m} \right) \cdot \frac{1}{m}.$$

Here $\left(\frac{\cdot}{p} \right)$ is the *extended Legendre symbol*: for a prime $p \neq 2$,

$$\left(\frac{a}{p} \right) = \begin{cases} 1 & a \text{ a non-zero square modulo } p \\ -1 & a \text{ not a square modulo } p \\ 0 & p \mid a \end{cases}$$

while

$$\left(\frac{a}{2}\right) = \begin{cases} 1 & a \equiv 1 \pmod 8 \\ -1 & a \equiv 5 \pmod 8 \\ 0 & \text{otherwise.} \end{cases}$$

(We give a unified definition of $\left(\frac{a}{p}\right)$ in Chapter 4.) For a general positive integer $m = p_1^{e_1} \cdots p_r^{e_r}$ we set

$$\left(\frac{a}{m}\right) = \left(\frac{a}{p_1}\right)^{e_1} \cdots \left(\frac{a}{p_r}\right)^{e_r}.$$

The convergence of $L(-n)$ is far from obvious and quite slow; nevertheless, it does converge, as we will prove in Chapter 4.

For example, we have

$$L(-5) = 1 + \frac{1}{3} + \frac{1}{7} + \frac{1}{9} - \frac{1}{11} - \frac{1}{13} - \frac{1}{17} - \frac{1}{19} + \frac{1}{21} + \cdots .$$

Summing this for $m \leq 10000000$ one finds that

$$L(-5) \approx 1.404963.$$

We include also a table of $L(-n)$ for several other values of n; the value given is the sum over $m \leq 10000000$.

n	$L(-n)$
2	1.110721
6	1.282550
10	0.993459
13	0.871321
14	1.679252
17	1.523896
21	1.371104
22	0.669790
26	1.848351
29	1.750137
30	1.147148
15701	1.654738
2905509	2.016229

In fact, there is a second interesting formula for $L(-n)$,

$$L(-n) = \prod_{p \text{ prime}} \frac{p}{p - \left(\frac{-n}{p}\right)},$$

as an infinite product over primes. However, the only proofs of this formula of which the author is aware involve complex analysis and are beyond the scope of these notes. (We will almost, but not quite, prove this formula in Chapter 4.)

Let us return to the value

$$L(-5) \approx 1.404963.$$

This number is close to, but slightly less than, the square root of 2. This is reminiscent of another famous coincidence of numbers: π is close to, but slightly less than, the square root of 10. At this point we become curious and compute

$$\frac{\pi}{\sqrt{10}} \cdot \sqrt{2} \approx 1.404963.$$

This is no accident.

THEOREM 1.17 (Dirichlet).

$$L(-5) = \frac{\pi}{\sqrt{5}}.$$

At this point it is hard to resist comparing the values $L(-n)$ with $\frac{\pi}{\sqrt{n}}$. In fact, to get the most striking result we'll throw in an extra factor of 2.

n	$L(-n)$	$L(-n)/\frac{\pi}{2\sqrt{n}}$
2	1.110721	1.00000
6	1.282550	2.00000
10	0.993459	2.00000
13	0.871321	2.00000
14	1.679252	4.00000
17	1.523896	4.00000
21	1.371104	4.00000
22	0.669790	2.00000
26	1.848351	6.00000
29	1.750137	6.00000
30	1.147148	4.00000
15701	1.654738	132.000
2905509	2.016229	2187.92

The numbers in the right-hand column are remarkably close to integers. In fact, they are remarkably close to integers we have seen before.

THEOREM 1.18 (Dirichlet). *Let* $n \equiv 1, 2 \pmod 4$ *be a squarefree integer greater than* 1. *Then*

$$L(-n) = \frac{\pi}{2\sqrt{n}} \cdot h(-n).$$

The same formula holds for $n \equiv 3 \pmod 4$, $n > 3$, with $h(-n)$ as in Exercise 1.5, except that the factor of 2 in the denominator disappears. There are also similar formulas for $n = 1, 3$ with slightly different denominators. In fact, Dirichlet's formula for $n = 1$ reduces to the familiar formula

$$\frac{\pi}{4} = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \frac{1}{9} - \frac{1}{11} + \cdots$$

obtained from the power series for $\tan^{-1}(x)$.

This is one of the most remarkable and beautiful formulas in mathematics. In this chapter we have given the fastest approach to defining the relevant quantities in terms of complex lattices and infinite sums. In order to actually prove the theorem, however, it is necessary to relate both sides to the arithmetic of the ring $\mathbf{Z}[\sqrt{-n}]$. This is the goal of the remaining chapters.

5. Appendix: Lattice points of bounded absolute value

In this section we prove a result about lattice points which will be crucial in Chapter 5. We include the proof here since the result can be stated and proved entirely in the framework of complex lattices.

Let $\Lambda = \langle \alpha, \beta \rangle$ be a complex lattice. Let P denote the parallelogram with vertices at the origin, α, β, and $\alpha + \beta$. Let A denote the area of P; we leave it to the reader to check that A is independent of the choice of basis (although this fact will also follow from Lemma 1.19 below).

Fix $t > 0$. Our goal is to estimate how many points of Λ have absolute value at most t. Alternately, if

$$C_t = \{z \in \mathbf{C}\,;\, |z| \le t\},$$

then we wish to determine the size of $\Lambda \cap C_t$. It is not difficult to formulate a guess. For any $\lambda \in \Lambda$ let P_λ denote the translate of P by λ; it is a parallelogram congruent to P with one vertex at λ. Since C_t has area πt^2 and since the parallelograms P_λ tile the plane, we would expect C_t to contain approximately $\pi t^2/A$ of the translates P_λ and thus approximately $\pi t^2/A$ of the points λ. Our goal in this section is to determine the error in this approximation.

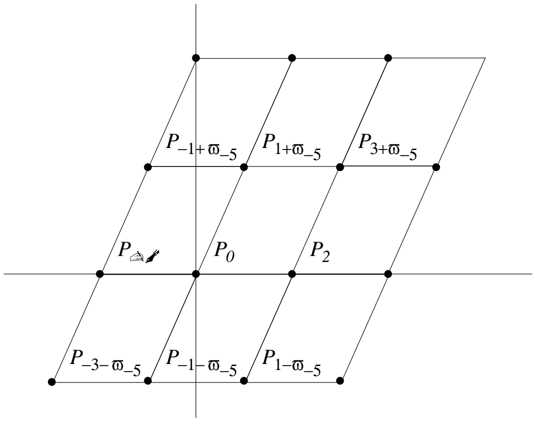

FIGURE 11. Some lattice parallelograms for $\langle 2, 1 + \sqrt{-5} \rangle$.

LEMMA 1.19. *There is a constant C depending only on Λ such that*

$$\left| \#\Lambda \cap C_t - \frac{\pi t^2}{A} \right| \le C \cdot t$$

for all $t \ge 1$.

The precise value of the constant C will not be relevant in the applications. This is quite common when using estimates: the crucial thing is that the quantity we are counting grows like a constant times t^2 and the error grows like a constant times t, so that for large t the approximation becomes relatively accurate. We note that this estimate does not hold for t near zero since the origin always lies in $\Lambda \cap C_t$. Nevertheless, this failure is uniquely uninteresting and will not be a problem in the applications.

Proof. Let

$$\begin{aligned} n(t) &= \text{number of } \lambda \in \Lambda \cap C_t \\ n_1(t) &= \text{number of } \lambda \in \Lambda \text{ such that } P_\lambda \subseteq C_t \\ n_2(t) &= \text{number of } \lambda \in \Lambda \text{ such that } P_\lambda \text{ intersects } C_t. \end{aligned}$$

(For $\Lambda = \langle 2, 1+\sqrt{-5}\rangle$, the picture below shows that $n(t) = 29$, while $n_1(t) = 18$ and $n_2(t) = 42$.)

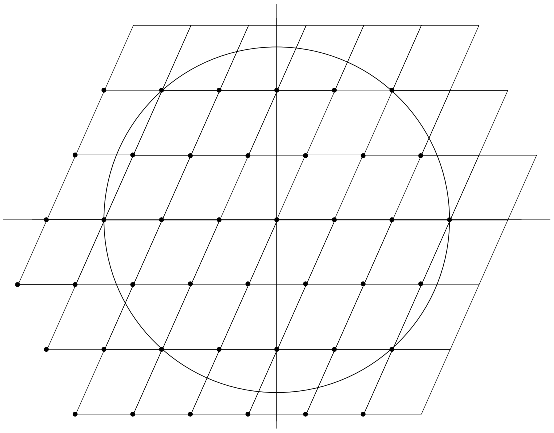

FIGURE 12. $\langle 2, 1+\sqrt{-5}\rangle \cap C_6$

If P_λ lies in C_t, then certainly λ lies in C_t; similarly, if λ lies in C_t, then certainly P_λ intersects C_t. Thus

$$n_1(t) \leq n(t) \leq n_2(t).$$

Since C_t has area πt^2 it can not possibly contain more than $\pi t^2/A$ disjoint translates of P, so that

$$n_1(t) \leq \frac{\pi t^2}{A}.$$

Similarly, since the translates of P which intersect C_t cover all of C_t, we must have

$$\frac{\pi t^2}{A} \leq n_2(t).$$

Unfortunately, these inequalities go the wrong way and do not allow us to say anything about $n(t)$ itself.

To remedy this, we perturb our circle slightly. Let δ denote the length of the longer diagonal of P. (In contrast to the area A, the length δ does depend on the choice of basis α, β, but this does not affect the proof below.) Then δ is the longest distance in P, so that for any $\lambda \in \Lambda \cap C_t$ we must have $P_\lambda \subseteq C_{t+\delta}$; that is,

$$n(t) \leq n_1(t+\delta) \leq \frac{\pi(t+\delta)^2}{A}.$$

Similarly, if P_λ intersects $C_{t-\delta}$, then it (and in particular λ) must be contained in C_t, so that

$$\frac{\pi(t-\delta)^2}{A} \leq n_2(t-\delta) \leq n(t).$$

Combining these inequalities we find that

$$\left|n(t) - \frac{\pi t^2}{A}\right| \leq \frac{\pi}{A}\left(2t\delta + \delta^2\right) \leq C \cdot t$$

with $C = \frac{\pi}{A}(2\delta + \delta^2)$. □

6. Exercises

Exercise 1.1. Complete the proof of Lemma 1.8.

Exercise 1.2. Show that a lattice Λ has CM by $\gamma \in \mathbf{C} - \mathbf{Z}$ if and only if it has CM by $\gamma + n$ for all $n \in \mathbf{Z}$.

Exercise 1.3. Find all homothety classes of lattices Λ for which there exist $\gamma \in \mathbf{C} - \mathbf{Z}$ with $\gamma \cdot \Lambda = \Lambda$.

Exercise 1.4. Compute the class group $\mathcal{C}l(-26)$.

Exercise 1.5. Fix a squarefree positive integer $n \equiv 3 \pmod 4$. Show that the lattice $\langle 1, j \rangle$ with $j \in \mathcal{F}$ has CM by ϖ_{-n} if and only if

$$j = \frac{a + \sqrt{-n}}{b}$$

where

1. $a, b \in \mathbf{Z}$ with a odd and b even;
2. $0 < b \leq 2\sqrt{\frac{n}{3}}$;
3. $-b < 2a \leq b$;
4. $a^2 + n \geq b^2$ (and $a \geq 0$ if $a^2 + n = b^2$);
5. $2b$ divides $a^2 + n$.

We define the *class group* $\mathcal{C}l(-n)$ in this case to be the set of complex numbers of the form $\frac{a+\sqrt{-n}}{b}$ with a, b as above.

Exercise 1.6. Compute the class group $\mathcal{C}l(-23)$.

Exercise 1.7. Compute the class group $\mathcal{C}l(-163)$.

Exercise 1.8. Determine for which primes p the lattice $\langle 1, i \rangle$ has a point of absolute value p.

Exercise 1.9.

1. Determine for which primes $p \leq 100$ the lattice $\left\langle 1, \sqrt{-5} \right\rangle$ has a point of absolute value p.
2. Determine for which primes $p \leq 100$ the lattice $\left\langle 2, 1 + \sqrt{-5} \right\rangle$ has a point of absolute value $2p$. Any conjectures?

CHAPTER 2

Ideal factorizations

1. Algebraic integers

Fix a squarefree positive integer n. Our goal in this section is to study factorization in the field

$$\mathbf{Q}(\sqrt{-n}) = \{a + b\sqrt{-n}\,;\ a, b \in \mathbf{Q}\}.$$

Of course, every non-zero element of a field is a unit, so that this analysis is rather silly for $\mathbf{Q}(\sqrt{-n})$ itself. Motivated by the classic example of the integers $\mathbf{Z}$ inside the field $\mathbf{Q}$, we should instead attempt to define a certain natural subring of $\mathbf{Q}(\sqrt{-n})$ and develop a theory of factorization in this subring.

The most obvious choice for subring is of course

$$\mathbf{Z}[\sqrt{-n}] = \{a + b\sqrt{-n}\,;\ a, b \in \mathbf{Z}\}.$$

However, this definition is rather arbitrary, and, as we will see, this ring is not always quite as large as we will need. To define the rings we wish to study, we focus on quadratic equations. Specifically, any $\alpha = a + b\sqrt{-n} \in \mathbf{Q}(\sqrt{-n})$ is a root of the quadratic polynomial

$$x^2 - 2ax + (a^2 + nb^2)$$

with rational coefficients. We will call this polynomial the *characteristic polynomial* of α. If α is irrational (that is, if $b \neq 0$), then by Exercise 2.2 this is the unique quadratic monic polynomial with rational coefficients having α as a root; if α is rational, then it is simply $(x - \alpha)^2$.

If α actually lies in $\mathbf{Z}[\sqrt{-n}]$, then the characteristic polynomial of α has integer coefficients rather than merely rational coefficients. However, if $n \equiv 3 \pmod 4$, then are are other elements of $\mathbf{Q}(\sqrt{-n})$ whose characteristic polynomials have integer coefficients: namely those with $2a, 2b \in \mathbf{Z}$ and $2a \equiv 2b \pmod 2$. (See Exercise 2.3.) These are the extra element we will need.

Definition 2.1. The *ring of algebraic integers* $\mathcal{O}_{-n}$ of $\mathbf{Q}(\sqrt{-n})$ is the set of all $\alpha \in \mathbf{Q}(\sqrt{-n})$ such that the characteristic polynomial of α has integer coefficients.

We have seen above that

$$\mathcal{O}_{-n} = \begin{cases} \{a + b\sqrt{-n}\,;\ a, b \in \mathbf{Z}\} & n \equiv 1, 2 \pmod 4; \\ \{a + b\sqrt{-n}\,;\ 2a, 2b \in \mathbf{Z}, 2a \equiv 2b \pmod 2\} & n \equiv 3 \pmod 4. \end{cases}$$

In each case $\mathcal{O}_{-n}$ is actually closed under addition and multiplication, so that it is a ring. It will sometimes be convenient to use a slightly different description of $\mathcal{O}_{-n}$. Set

$$\varpi_{-n} = \begin{cases} \sqrt{-n} & n \equiv 1, 2 \pmod 4 \\ \frac{1+\sqrt{-n}}{2} & n \equiv 3 \pmod 4. \end{cases}$$

Then one checks immediately that for any n we have

$$\mathcal{O}_{-n} = \{a + b\varpi_{-n}\,;\, a, b \in \mathbf{Z}\}.$$

The coefficients of the characteristic polynomial of $\alpha \in \mathcal{O}_{-n}$ are extremely useful invariants.

Definition 2.2. For $\alpha \in \mathcal{O}_{-n}$, the *norm* $\mathrm{N}(\alpha)$ and *trace* $\mathrm{tr}(\alpha)$ of α are the coefficients of the characteristic polynomial

$$x^2 - \mathrm{tr}(\alpha)x + \mathrm{N}(\alpha)$$

of α.

Thus, if $\alpha = a + b\sqrt{-n}$, then $\mathrm{tr}(\alpha) = 2a$ and $\mathrm{N}(\alpha) = a^2 + nb^2$. Alternately, if $\alpha = a + b\varpi_{-n}$ with $a, b \in \mathbf{Z}$, then

$$\mathrm{tr}(\alpha) = \begin{cases} 2a & n \equiv 1, 2 \pmod 4; \\ 2a + b & n \equiv 3 \pmod 4; \end{cases}$$

$$\mathrm{N}(\alpha) = \begin{cases} a^2 + nb^2 & n \equiv 1, 2 \pmod 4; \\ a^2 + ab + \frac{1+n}{4}b^2 & n \equiv 3 \pmod 4. \end{cases}$$

In order to prove the basic properties of the norm and trace it is convenient to introduce conjugation.

Definition 2.3. For $\alpha = a + b\sqrt{-n} \in \mathcal{O}_{-n}$, the *conjugate* $\bar{\alpha}$ of α is defined by

$$\bar{\alpha} = a - b\sqrt{-n} \in \mathcal{O}_{-n}.$$

Note that the characteristic polynomial of α factors as

$$x^2 - 2ax + (a^2 + nb^2) = (x - \alpha)(x - \bar{\alpha}).$$

In particular, we have

$$\mathrm{tr}(\alpha) = \alpha + \bar{\alpha} \text{ and } \mathrm{N}(\alpha) = \alpha \cdot \bar{\alpha}.$$

Lemma 2.4. *For $\alpha, \beta \in \mathcal{O}_{-n}$ we have*

$$\mathrm{tr}(\alpha + \beta) = \mathrm{tr}(\alpha) + \mathrm{tr}(\beta)$$

$$\mathrm{N}(\alpha \cdot \beta) = \mathrm{N}(\alpha) \cdot \mathrm{N}(\beta).$$

Proof. The map

$$\mathcal{O}_{-n} \to \mathcal{O}_{-n}$$
$$\alpha \mapsto \bar{\alpha}$$

sending $\alpha \in \mathcal{O}_{-n}$ to its conjugate $\bar{\alpha}$ is easily checked to be a homomorphism: that is,

$$\overline{\alpha + \beta} = \bar{\alpha} + \bar{\beta}$$

$$\overline{\alpha \cdot \beta} = \bar{\alpha} \cdot \bar{\beta}.$$

Thus

$$\mathrm{N}(\alpha \cdot \beta) = (\alpha\beta) \cdot (\overline{\alpha\beta}) = (\alpha\beta) \cdot (\bar{\alpha}\bar{\beta}) = (\alpha\bar{\alpha}) \cdot (\beta\bar{\beta}) = \mathrm{N}(\alpha) \cdot \mathrm{N}(\beta).$$

The proof for the trace is similar. □

The norm is very useful for transferring multiplication problems from $\mathcal{O}_{-n}$ to the integers $\mathbf{Z}$. Its key properties are summarized in the next lemma. Recall that for $\alpha, \beta \in \mathcal{O}_{-n}$ we say that α *divides* β, written $\alpha \mid \beta$, if there exists $\gamma \in \mathcal{O}_{-n}$ such that $\beta = \gamma \cdot \alpha$. An element $\alpha \in \mathcal{O}_{-n}$ is a *unit* if it divides 1, while it is *irreducible* if it is not a unit and if for any factorization $\alpha = \beta \cdot \gamma$ with $\beta, \gamma \in \mathcal{O}_{-n}$, one of β, γ is a unit.

Lemma 2.5.

(1) *If* $\alpha \mid \beta$ *in* $\mathcal{O}_{-n}$*, then* $\mathrm{N}(\alpha) \mid \mathrm{N}(\beta)$ *in* $\mathbf{Z}$*.*
(2) $\alpha \in \mathcal{O}_{-n}$ *is a unit if and only if* $\mathrm{N}(\alpha) = 1$*.*
(3) *If* $\mathrm{N}(\alpha)$ *is prime in* $\mathbf{Z}$*, then* α *is irreducible in* $\mathcal{O}_{-n}$*.*

Note that the converse of (1) need not be true: if $\mathrm{N}(\alpha) \mid \mathrm{N}(\beta)$, it is not necessarily true that $\alpha \mid \beta$. We will also see that the converse of (3) need not be true either: there are many irreducible elements with composite norm.

Proof.

(1) If $\beta = \alpha \cdot \gamma$, then $\mathrm{N}(\beta) = \mathrm{N}(\alpha) \cdot \mathrm{N}(\gamma)$, so that $\mathrm{N}(\alpha) \mid \mathrm{N}(\beta)$.
(2) If $\alpha \in \mathcal{O}_{-n}$ is a unit, then by (1) we have that $\mathrm{N}(\alpha)$ divides 1 in $\mathbf{Z}$, so that $\mathrm{N}(\alpha) = \pm 1$. However, $\mathrm{N}(\alpha)$ is visibly positive, so that we must thus have $\mathrm{N}(\alpha) = 1$. Conversely, if $\mathrm{N}(\alpha) = 1$, then $\alpha \cdot \bar{\alpha} = 1$, so that α is a unit.
(3) By (1) and (2) any factorization of α into non-units gives a factorization of $\mathrm{N}(\alpha)$ into non-units. In particular, if $\mathrm{N}(\alpha)$ is prime, then α itself can not factor in $\mathcal{O}_{-n}$.

□

It is now a simple matter to determine all units in $\mathcal{O}_{-n}$.

Corollary 2.6. *For $n = 1$ the units in $\mathcal{O}_{-n}$ are $\{\pm 1, \pm i\}$. For $n = 3$ the units in $\mathcal{O}_{-n}$ are $\{\pm 1, \pm\omega, \pm\omega^2\}$ with $\omega = \frac{-1+\sqrt{-3}}{2}$. For all other n, the only units in $\mathcal{O}_{-n}$ are $\{\pm 1\}$.*

Proof. Let $\alpha = a + b\sqrt{-n}$ be a unit in $\mathcal{O}_{-n}$. We have

$$\mathrm{N}(\alpha) = a^2 + nb^2 = 1.$$

If $n \equiv 1, 2 \pmod 4$ then we have $a, b \in \mathbf{Z}$, so that this can only occur if $a = \pm 1$, $b = 0$ (corresponding to the units ± 1) or if $n = 1$, $a = 0$, $b = \pm 1$ (corresponding to the units $\pm i$ of $\mathbf{Z}[i]$). If $n \equiv 3 \pmod 4$, then we have

$$(2a)^2 + n(2b)^2 = 4$$

with $2a, 2b \in \mathbf{Z}$. If $n > 3$ then the only solutions of this equation are again $a = \pm 1$, $b = 0$. When $n = 3$ we also have the solutions $a = \pm\frac{1}{2}$, $b = \pm\frac{1}{2}$. We leave it to the reader to check that these yield the four additional units of $\mathcal{O}_{-3}$ given above. □

2. Irreducibles in $\mathbf{Z}[\sqrt{-5}]$

When $n \leq 3$ it is well-known that the ring $\mathcal{O}_{-n}$ has unique factorization. The situation becomes more complicated beginning with $n = 5$. In this section we consider some examples in the ring of algebraic integers $\mathbf{Z}[\sqrt{-5}]$ of $\mathbf{Q}(\sqrt{-5})$.

We first list the irreducibles with small norm in $\mathbf{Z}[\sqrt{-5}]$. Recall that two elements α, β are said to be *associates* if their ratio is a unit. Since the only units of $\mathbf{Z}[\sqrt{-5}]$ are ± 1, this merely corresponds to negation in this case. We list below only one representative of each pair of associate irreducibles.

N	irreducibles of norm N
4	2
5	$\sqrt{-5}$
6	$1+\sqrt{-5}$, $1-\sqrt{-5}$
9	$2+\sqrt{-5}$, $2-\sqrt{-5}$, 3
14	$3+\sqrt{-5}$, $3-\sqrt{-5}$
21	$1+2\sqrt{-5}$, $1-2\sqrt{-5}$, $4+\sqrt{-5}$, $4-\sqrt{-5}$
29	$3+2\sqrt{-5}$, $3-2\sqrt{-5}$
41	$6+\sqrt{-5}$, $6-\sqrt{-5}$
46	$1+3\sqrt{-5}$, $1-3\sqrt{-5}$
49	$2+3\sqrt{-5}$, $2-3\sqrt{-5}$, 7

Note that it is not difficult to construct such a table inductively; for example, if $1+2\sqrt{-5}$ were to factor, it would have to factor into elements of norm 3 and 7; since such elements do not exist in $\mathbf{Z}[\sqrt{-5}]$, it follows that $1+2\sqrt{-5}$ must be irreducible.

The table above raises many questions. Why do the primes 29 and 41 factor in $\mathbf{Z}[\sqrt{-5}]$, while $3, 7, 11, 13, 17, 19, 23, 31, 37, 43$ do not? (The prime 5 is obviously a special case; in fact, so is 2, although not as obviously.) For some primes this is easy to answer. Specifically, suppose that a prime $p \neq 2, 5$ factors in $\mathbf{Z}[\sqrt{-5}]$:

$$p = (a+b\sqrt{-5}) \cdot (a-b\sqrt{-5})$$

with $a, b \in \mathbf{Z}$. In particular, $p = a^2 + 5b^2$, so that

$$a^2 \equiv -5b^2 \pmod{p}.$$

Clearly $0 < a, b < p$; thus we may divide by b^2 to obtain

$$(ab^{-1})^2 \equiv -5 \pmod{p}.$$

Thus if p factors in $\mathbf{Z}[\sqrt{-5}]$, then -5 is a square modulo p, as we have exhibited its square root. Using quadratic reciprocity one can show that this is the case if and only if

$$p \equiv 1, 3, 7, 9 \pmod{20}.$$

Thus any prime $p \equiv 11, 13, 17, 19 \pmod{20}$ can not possibly factor in $\mathbf{Z}[\sqrt{-5}]$. In particular, this explains why $11, 13, 17, 19, 31, 37$ are irreducible in $\mathbf{Z}[\sqrt{-5}]$.

This still leaves the primes $3, 7, 23, 43$. Here the reasons behind the failure to factor are much more subtle. The argument above is not reversible, so that there is no guarantee that these primes must factor; this is fortunate, as we know that they do not. It is exactly the failure of these primes to factor which causes unique factorization to fail, as we will see.

We turn now to the classic counterexample to unique factorization in $\mathbf{Z}[\sqrt{-5}]$. The element 6 has norm $36 = 2^2 \cdot 3^2$ and thus could factor as either a product of an element of norm 4 and of norm 9 or as two elements of norm 6. In fact, both possibilities do occur:

$$6 = 2 \cdot 3 = (1+\sqrt{-5}) \cdot (1-\sqrt{-5}).$$

Since all irreducibles above are not associate to one another, this gives two different factorizations of 6 into irreducibles in $\mathbf{Z}[\sqrt{-5}]$, so that $\mathbf{Z}[\sqrt{-5}]$ does not have unique factorization.

In particular, this appears to give a counterexample to the fundamental theorem of arithmetic: 2 divides the product $(1+\sqrt{-5})\cdot(1-\sqrt{-5})$ and has no non-unit common divisors with $1-\sqrt{-5}$, yet 2 does not divide $1+\sqrt{-5}$. The key observation, however, is that, while 2 and $1+\sqrt{-5}$ have no common divisors, they are not really relatively prime.

Recall that if a, b are relatively prime integers, then there exist integers x, y such that $ax+by=1$. This is not true with the apparently relatively prime elements $2, 1+\sqrt{-5}$ in $\mathbf{Z}[\sqrt{-5}]$: there are no $x, y \in \mathbf{Z}[\sqrt{-5}]$ such that

$$2x+(1+\sqrt{-5})y=1.$$

(See Example 2.8 below.) If we attempt to instead define the greatest common divisor of $2, 1+\sqrt{-5}$ as the smallest (in norm) element of $\mathbf{Z}[\sqrt{-5}]$ which can be expressed as a linear combination of 2 and $1+\sqrt{-5}$ we run into other problems: 2 is the smallest such element, but there are other linear combinations (like $1+\sqrt{-5}$) which are not divisible by 2.

We have now seen that a fundamental failing of $\mathbf{Z}[\sqrt{-5}]$ is that we can find no element which has all the properties of the greatest common divisor of 2 and $1+\sqrt{-5}$: there is no element which simultaneously divides all common divisors of 2 and $1+\sqrt{-5}$ and can be written as a linear combination of 2 and $1+\sqrt{-5}$. The solution to this problem is absurdly simple: instead of attempting to pick out a smallest linear combination of 2 and $1+\sqrt{-5}$, we will consider the set of all linear combinations:

$$(2, 1+\sqrt{-5}) := \left\{2x+(1+\sqrt{-5})y\,;\, x, y \in \mathbf{Z}[\sqrt{-5}]\right\}.$$

This is an example of an *ideal* of $\mathbf{Z}[\sqrt{-5}]$. It is not an element of $\mathbf{Z}[\sqrt{-5}]$, but rather is a set of elements which is closed under certain operations. We will see below that it behaves exactly like the greatest common divisor of 2 and $1+\sqrt{-5}$.

3. Ideals

Fix once again a squarefree positive integer n.

Definition 2.7. An *ideal* I of $\mathcal{O}_{-n}$ is a subset of $\mathcal{O}_{-n}$ such that:

(1) if $\alpha, \beta \in I$, then $\alpha+\beta \in I$;
(2) if $\alpha \in \mathcal{O}_{-n}$ and $\beta \in I$, then $\alpha \cdot \beta \in I$;
(3) there is at least one non-zero element α in I.

(Usually the last axiom is not included in the definition of an ideal; for our purposes, however, we prefer to exclude the zero ideal.)

Note that we require than an ideal I is not merely closed under multiplication of its own elements, but under multiplying its elements by any element of $\mathcal{O}_{-n}$. The fundamental example is the following: if $\alpha_1, \ldots, \alpha_r$ are elements of $\mathcal{O}_{-n}$, then the *ideal* $(\alpha_1, \ldots, \alpha_r)$ *generated by* $\alpha_1, \ldots, \alpha_r$ is the set of all $\mathcal{O}_{-n}$-linear combinations of the α_i:

$$(\alpha_1, \ldots, \alpha_r) := \{\alpha_1 x_1 + \cdots + \alpha_r x_r\,;\, x_i \in \mathcal{O}_{-n}\}.$$

(We leave it to the reader to check that this really is an ideal of $\mathcal{O}_{-n}$ so long as at least one of the α_i is non-zero.) This ideal should be thought of as the greatest common divisor of $\alpha_1, \ldots, \alpha_r$.

As we shall see, ideals are very well-suited for questions involving factorizations. To give one example, if α and β are associates, then the ideals (α) and (β) are identical. Later, when we consider factorizations into ideals, this will mean that the annoying unit issue (that is, that factorizations are only determined up to ± 1 in $\mathbf{Z}$ and up to powers of i in $\mathbf{Z}[i]$) will not come up.

Example 2.8. Consider the ideal $(2, 1+\sqrt{-5})$ of $\mathbf{Z}[\sqrt{-5}]$. A $\mathbf{Z}[\sqrt{-5}]$-linear combination of 2 and $1+\sqrt{-5}$ has the form

$$2(a+b\sqrt{-5}) + (1+\sqrt{-5})(c+d\sqrt{-5}) = (2a+c-5d) + (2b+c+d)\sqrt{-5}$$

for $a, b, c, d \in \mathbf{Z}$. It is not difficult to see that we can choose a, b, c, d to obtain any element $\alpha = e + f\sqrt{-5}$ of $\mathbf{Z}[\sqrt{-5}]$ such that $e \equiv f \pmod 2$. Thus

$$(2, 1+\sqrt{-5}) = \{e + f\sqrt{-5}; e, f \in \mathbf{Z}, e \equiv f \pmod 2\}.$$

Example 2.9. Consider the ideal $(2, \sqrt{-5})$ of $\mathbf{Z}[\sqrt{-5}]$. Note that

$$1 = 2 \cdot 3 + \sqrt{-5} \cdot \sqrt{-5}$$

is a linear combination of 2 and $\sqrt{-5}$ and thus lies in $(2, \sqrt{-5})$. Since an ideal is also closed under multiplication by any element of $\mathbf{Z}[\sqrt{-5}]$, and every element of $\mathbf{Z}[\sqrt{-5}]$ is a multiple of 1, it follows that

$$(2, \sqrt{-5}) = (1) = \mathbf{Z}[\sqrt{-5}].$$

In other words, the elements 2 and $\sqrt{-5}$ really are relatively prime in the strong sense in $\mathbf{Z}[\sqrt{-5}]$.

An ideal I is said to be *principal* if there exists a single element $\alpha \in I$ such that $I = (\alpha)$. (Thus a principal ideal is simply the set of all multiples of a fixed element α.)

Example 2.10. We claim that the ideal $(29, 13-\sqrt{-5})$ of $\mathbf{Z}[\sqrt{-5}]$ is principal with generator $3+2\sqrt{-5}$. To see this, we must show that

$$(29, 13-\sqrt{-5}) \subseteq (3+2\sqrt{-5}) \tag{9}$$

and

$$(3+2\sqrt{-5}) \subseteq (29, 13-\sqrt{-5}). \tag{10}$$

Since $(3+2\sqrt{-5})$ is the set of multiples of $3+2\sqrt{-5}$, for (9) this amounts to checking that $3+2\sqrt{-5}$ divides both of 29 and $13-\sqrt{-5}$ (for then every linear combination will also be divisible by $3+2\sqrt{-5}$), which it does:

$$29 = (3+2\sqrt{-5}) \cdot (3-2\sqrt{-5})$$
$$13-\sqrt{-5} = (3+2\sqrt{-5}) \cdot (1-\sqrt{-5}).$$

For (10) it suffices to exhibit $3+2\sqrt{-5}$ as a linear combination of 29 and $13-\sqrt{-5}$, for then every multiple of $3+2\sqrt{-5}$ can also be expressed as a linear combination of 29 and $13-\sqrt{-5}$. The required expression is simply:

$$3+2\sqrt{-5} = 29 \cdot 1 + (13-\sqrt{-5}) \cdot (-2).$$

This example shows that, unlike the elements 2 and $1+\sqrt{-5}$, the elements 29 and $13-\sqrt{-5}$ do have a well-behaved greatest common divisor in $\mathbf{Z}[\sqrt{-5}]$, namely, $3+2\sqrt{-5}$.

We now consider some basic operations with ideals. It is important to note that any useful definition must depend only on the underlying set of the ideal, and not on a particular choice of generators. Of course, after this is done we will obtain a formula for the operation in terms of generators; the key requirement is that this formula gives the same underlying ideal for any choice of generators. By applying this formula in the special case of principal ideals we should be able to determine what operation on elements the ideal operation is a generalization of.

Let I, J be ideals of $\mathcal{O}_{-n}$. The simplest operation on ideals is the sum:

$$I + J = \{\alpha + \beta\,;\ \alpha \in I, \beta \in J\}.$$

One checks immediately from the definitions that $I + J$ is an ideal of $\mathcal{O}_{-n}$; in fact, if $I = (\alpha_1, \ldots, \alpha_r)$ and $J = (\beta_1, \ldots, \beta_s)$, then

$$I + J = (\alpha_1, \ldots, \alpha_r, \beta_1, \ldots, \beta_s).$$

In particular, if $I = (\alpha)$ and $J = (\beta)$ are principal, then $I + J = (\alpha, \beta)$ is the greatest common divisor of α and β. That is, addition of ideals corresponds not to addition of elements (there is no operation on ideals which corresponds to addition of elements), but instead to the greatest common divisor.

The product of ideals is slightly more subtle. Indeed, the natural guess

$$\{\alpha \cdot \beta\,;\ \alpha \in I, \beta \in J\}$$

need not be closed under addition and thus may not actually be an ideal. We rectify this problem in the simplest possible way: we close it up under addition. That is, define

$$I \cdot J = \{\alpha_1\beta_1 + \cdots + \alpha_m\beta_m\,;\ m \geq 1, \alpha_i \in I, \beta_i \in J\}$$

as the set of all sums of products of elements of I and J. This time closure under addition is automatic (you simply need to increase m to combine two elements), as is strong closure under multiplication. If $I = (\alpha_1, \ldots, \alpha_r)$ and $J = (\beta_1, \ldots, \beta_s)$, then $I \cdot J$ is generated by the products $\alpha_i \cdot \beta_j$ for $1 \leq i \leq r$ and $1 \leq j \leq s$. In particular, if $I = (\alpha)$ and $J = (\beta)$ are principal, then $I \cdot J = (\alpha \cdot \beta)$. Thus the product of ideals does correspond to the usual product of elements. Note that multiplication of ideals is visibly commutative and associative. The *unit ideal* $\mathcal{O}_{-n} = (1)$ acts as an identity element: $I \cdot \mathcal{O}_{-n} = I$ for any ideal I.

The next lemma is immediate from the definitions.

Lemma 2.11. *Let I, J be ideals of $\mathcal{O}_{-n}$. Then $I \cdot J \subseteq I$.*

Note that this lemma is opposite our usual intuition: multiples of an ideal are in fact smaller (as sets) than the original ideal. Also, Lemma 2.11 shows that the set of ideals of $\mathcal{O}_{-n}$ do not form a group under multiplication: if $I \neq \mathcal{O}_{-n}$ is a non-unit ideal, then $I \cdot J \subseteq I \subsetneq \mathcal{O}_{-n}$ for any ideal J, so that we can not possibly find an inverse for I.

Example 2.12. Consider the ideals

$$\begin{aligned} I_2 &= (2, 1 + \sqrt{-5}) \\ I_2' &= (2, 1 - \sqrt{-5}) \\ I_3 &= (3, 1 + \sqrt{-5}) \\ I_3' &= (3, 1 - \sqrt{-5}) \end{aligned}$$

of $\mathbf{Z}[\sqrt{-5}]$. We compute

$$I_2 \cdot I_2' = (4, 2 + 2\sqrt{-5}, 2 - 2\sqrt{-5}, 6) = (2)$$

since $2 = 6 - 4$ lies in $I_2 \cdot I_2'$ and divides each of the generators. Similarly,

$$I_3 \cdot I_3' = (9, 3 + 3\sqrt{-5}, 3 - 3\sqrt{-5}, 6) = (3).$$

On the other hand,

$$I_2 \cdot I_3 = (6, 2 + 2\sqrt{-5}, 3 + 3\sqrt{-5}, -4 + 2\sqrt{-5}) = (1 + \sqrt{-5})$$

and

$$I_2' \cdot I_3' = (6, 2 - 2\sqrt{-5}, 3 - 3\sqrt{-5}, -4 - 2\sqrt{-5}) = (1 - \sqrt{-5}).$$

We claim that these calculations explain the equation

$$2 \cdot 3 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5}).$$

Indeed, reinterpreting this equation as an equality of products of ideals, the four ideals above give a refinement of these factorizations:

$$(I_2 \cdot I_2') \cdot (I_3 \cdot I_3') = (I_2 \cdot I_3) \cdot (I_2' \cdot I_3')$$

in which the same factors appear on both sides. The counterexample to unique factorization arises from regrouping the four non-principal ideals to give different principal ideals. Thus unique factorization is repaired once we allow factorizations into ideals and not merely into elements. (In the interest of full disclosure, we should mention that in fact $I_2 = I_2'$; this has no effect on our above analysis, however.) Our next goal is to prove this in general.

4. Unique factorization of ideals

We now work towards a proof of unique factorization of ideals of $\mathcal{O}_{-n}$. Let I and J be ideals of $\mathcal{O}_{-n}$. We say that I *divides* J, written $I \mid J$, if there exists an ideal K such that $I \cdot K = J$. Lemma 2.11 shows that if $I \mid J$, then $J \subseteq I$. Our first task is to prove that the converse of this is true as well. For this we need the following key lemma.

Lemma 2.13. *Let I be an ideal of $\mathcal{O}_{-n}$. Define an ideal $\bar{I}$ by*

$$\bar{I} = \{\bar{\alpha}\,;\, \alpha \in I\}.$$

Then $I \cdot \bar{I}$ is principal. In fact, there is an integer d such that $I \cdot \bar{I} = (d)$.

Proof. Note that for any non-zero $\alpha \in I$, the product $\alpha\bar{\alpha}$ is a positive integer in $I \cdot \bar{I}$. In particular, $I \cdot \bar{I}$ contains positive integers; we define d to be the least positive integer in $I \cdot \bar{I}$. We claim first that d divides every other rational integer in $I \cdot \bar{I}$. Indeed, if an integer e lies in $I \cdot \bar{I}$, then by closure under addition and strong closure under multiplication so does the remainder $e - dq$, $0 \leq e - dq < d$, when e is divided by d. As d is assumed to be the smallest positive integer in $I \cdot \bar{I}$, this remainder must vanish, so that d divides e.

We claim that $I \cdot \bar{I} = (d)$. The fact that (d) is a subset of $I \cdot \bar{I}$ is immediate from the definitions and the fact that $d \in I \cdot \bar{I}$. To prove the other direction, since an arbitrary element of $I \cdot \bar{I}$ is a sum of products $\alpha\bar{\beta}$ with $\alpha, \beta \in I$, it suffices to show that any such $\alpha\bar{\beta}$ is divisible by d in $\mathcal{O}_{-n}$. Consider the element $\alpha\bar{\beta}/d$ of $\mathbf{Q}(\sqrt{-n})$. We have

$$\operatorname{tr}\left(\frac{\alpha\bar{\beta}}{d}\right) = \frac{1}{d}(\alpha\bar{\beta} + \bar{\alpha}\beta) \in \mathbf{Z}$$

since $\alpha\bar{\beta} + \bar{\alpha}\beta$ is an integer lying in $I \cdot \bar{I}$ and thus is divisible by d. Similarly,

$$\mathrm{N}\left(\frac{\alpha\bar{\beta}}{d}\right) = \frac{\alpha\bar{\alpha}}{d} \cdot \frac{\beta\bar{\beta}}{d} \in \mathbf{Z}.$$

In particular, the characteristic polynomial of $\alpha\bar{\beta}/d$ has integer coefficients, so that $\alpha\bar{\beta}/d$ lies in $\mathcal{O}_{-n}$ by definition. Thus d divides $\alpha\bar{\beta}$ in $\mathcal{O}_{-n}$, as desired. □

In the above proof it is crucial that we use the full ring of algebraic integers $\mathcal{O}_{-n}$ and not its subring $\mathbf{Z}[\sqrt{-n}]$ when $n \equiv 3 \pmod 4$. Indeed, we will see in Exercise 2.5 that the ideals of $\mathbf{Z}[\sqrt{-n}]$ do not possess unique factorization in this case.

Proposition 2.14. *let I, J be ideals of $\mathcal{O}_{-n}$. Then $I \mid J$ if and only if $J \subseteq I$.*

Proof. We have already seen that if $I \mid J$ then $J \subseteq I$. For the converse, assume that $J \subseteq I$. Let d be the positive integer such that $I \cdot \bar{I} = (d)$. Note that d divides any element of $J \cdot \bar{I} \subseteq I \cdot \bar{I}$, so that

$$K := \tfrac{1}{d}\bar{I} \cdot J = \left\{ \tfrac{1}{d} \sum \bar{\alpha}_i \beta_i \,;\, \alpha_i \in I, \beta_i \in J \right\} \subseteq \mathbf{Q}(\sqrt{-n})$$

is in fact a subset of $\mathcal{O}_{-n}$. One checks easily that K is an ideal of $\mathcal{O}_{-n}$. We compute

$$I \cdot K = \tfrac{1}{d} I \cdot \bar{I} \cdot J = \tfrac{1}{d}(d) \cdot J = (1) \cdot J.$$

(We leave it to the reader to justify this last line of calculations.) Thus I divides J, as claimed. □

We can also use Lemma 2.13 to develop a theory of norms of ideals. Specifically, for an ideal I we define the norm $\mathrm{N}(I)$ to be the positive integer d such that $I \cdot \bar{I} = (d)$. The next lemma is then immediate from the definitions.

Lemma 2.15.

(1) $\mathrm{N}(I \cdot J) = \mathrm{N}(I) \cdot \mathrm{N}(J)$ *for any ideals I, J of $\mathcal{O}_{-n}$.*
(2) *If $I = (\alpha)$ is a principal ideal, then* $\mathrm{N}(I) = \mathrm{N}(\alpha)$.

Now that we have a good divisibility theory for ideals we should define an appropriate notion of prime ideals. We do this in the usual way.

Definition 2.16. An ideal I of $\mathcal{O}_{-n}$ is *prime* if it is not the unit ideal and if its only ideal divisors are the unit ideal and itself.

We can use Proposition 2.14 to prove the ideal analogue of the fundamental theorem of arithmetic.

Lemma 2.17. *A non-unit ideal I of $\mathcal{O}_{-n}$ is prime if and only if it has the property that whenever I divides a product $J \cdot K$, then I divides at least one of J and K.*

Proof. Suppose first that I has the property above and let J be an ideal dividing I; thus there is an ideal K such that $I = J \cdot K$. Our hypothesis on I thus implies that I must divide either J or K. If I divides J, then we must have $I = J$ since $I \subseteq J$ and $J \subseteq I$. If I divides K, then similarly $I = K$, so that $J = \mathcal{O}_{-n}$ by cancellation (Exercise 2.6). Thus the only possible divisors of I are $\mathcal{O}_{-n}$ and I, so that I is prime.

Conversely, suppose that a prime ideal I divides a product $J \cdot K$. By Proposition 2.14 the ideal $I + J$ certainly divides both I. In particular, since I is prime, $I + J$ must equal either $\mathcal{O}_{-n}$ or I. If $I + J = I$, then J is contained in I, so that I divides J.

To complete the proof we must show that if $I + J = \mathcal{O}_{-n}$, then I divides K. Fix $k \in K$. Since $I + J = \mathcal{O}_{-n}$ and $1 \in \mathcal{O}_{-n}$, we may choose $i \in I$ and $j \in J$ such that $i + j = 1$. Since I contains $J \cdot K$, the product jk lies in I. As

$$jk = (1 - i)k = k - ik$$

and ik lies in I, it follows that $k \in I$. Thus I contains K, so that I divides K by Proposition 2.14. □

We have seen that every ideal of $\mathcal{O}_{-n}$ divides the principal ideal generated by some integer (namely, its norm). The expected strengthening of this for prime ideals is not difficult.

Lemma 2.18. *Let I be a prime ideal of $\mathcal{O}_{-n}$. Then there is a prime number p such that I divides (p).*

Proof. Let d denote the norm of I, so that I divides (d). Decomposing d as a product of integer primes, we find that I divides

$$(p_1)\cdots(p_r)$$

for some (not necessarily distinct) integer primes $p_1, \ldots, p_r$. Since I is prime, it follows that I must divide (p_i) for some i. □

The next proposition thus gives (almost) all prime ideals of $\mathcal{O}_{-n}$. (See Exercise 2.10 for the case of $p = 2$.)

Proposition 2.19. *Let p be an odd prime. Then in $\mathcal{O}_{-n}$ we have*

$$(p) = \begin{cases} (p) & \left(\frac{-n}{p}\right) = -1; \\ (p, a+\sqrt{-n})(p, a-\sqrt{-n}) & \left(\frac{-n}{p}\right) = 1, a \in \mathbf{Z} \text{ such that } a^2 \equiv -n \pmod{p}; \\ (p, \sqrt{-n})^2 & \left(\frac{-n}{p}\right) = 0 \end{cases}$$

where each ideal on the right-hand side is prime. In the latter two cases the two factors on the right each have norm p (while the ideal (p) itself has norm p^2, of course).

Proof. Assume first that $\left(\frac{-n}{p}\right) = -1$. To show that (p) itself is prime, let I be a non-unit ideal dividing (p); we must show that $I = (p)$. If not, then there exists an element $\alpha = a + b\varpi_{-n} \in I$ which is not divisible by p. Note first that I has norm p: indeed, $\mathrm{N}(I)$ divides $\mathrm{N}(p) = p^2$ and can not equal p^2 since $I \neq (p)$. In particular $\mathrm{N}(\alpha)$, which lies in $I \cdot \bar{I}$, must be divisible by p; that is,

$$p \mid a^2 + nb^2 \quad \text{if} \quad n \equiv 1, 2 \pmod{4}$$

or

$$p \mid a^2 + ab + \tfrac{1+n}{4}b^2 \quad \text{if} \quad n \equiv 3 \pmod{4}.$$

In either case we must have $p \nmid b$, since if $p \mid b$ we also have $p \mid a$ so that $p \mid \alpha$. In the first case we then find that

$$\left(ab^{-1}\right)^2 \equiv -n \pmod{p}$$

while in the second

$$\left(2ab^{-1}+1\right)^2 \equiv -n \pmod{p}.$$

This contradicts the assumption that $\left(\frac{-n}{p}\right) = -1$, so that we must in fact have $I = (p)$. Thus (p) is prime in this case.

Assume next that $\left(\frac{-n}{p}\right) = 1$. Choose $a \in \mathbf{Z}$ such that $a^2 \equiv -n \pmod{p}$. Then

$$(p, a+\sqrt{-n})(p, a-\sqrt{-n}) = (p^2, pa + p\sqrt{-n}, pa - p\sqrt{-n}, a^2+n) = (p)$$

since p^2 and $2pa$ lie in this product and a is not divisible by p. This gives the desired factorization. Since (p) has norm p^2 and both of these ideals are proper divisors of (p), they must both have norm p and thus must be prime.

Finally, suppose that $\left(\frac{-n}{p}\right) = 0$, so that p divides n. Then

$$(p, \sqrt{-n})^2 = (p^2, p\sqrt{-n}, -n) = (p)$$

since p divides n and n is squarefree. The same argument as above shows that $(p, \sqrt{-n})$ must be prime of norm p. □

At this point the proof of unique factorization of ideals follows the usual pattern.

THEOREM 2.20. *Let I be a non-unit ideal of $\mathcal{O}_{-n}$. Then there exist prime ideals $I_1, \ldots, I_r$ such that*

$$I = I_1 \cdots I_r.$$

The ideals $I_1, \ldots, I_r$ are unique up to reordering.

PROOF. We proceed by induction on $\mathrm{N}(I)$. If I is prime, then we simply take $r = 1$ and $I_1 = I$. If I is not prime, then by definition I has a divisor J different from $\mathcal{O}_{-n}$ and I. Let K be the ideal such that $I = JK$. We must have $\mathrm{N}(J), \mathrm{N}(K) < \mathrm{N}(I)$, so that by the induction hypothesis both J and K factor as a product of prime ideals. Taking the product of these factorizations gives the desired factorization of I.

To see uniqueness, we again proceed by induction on $\mathrm{N}(I)$. Let I be an ideal of smallest norm which has two different factorizations into prime ideals:

$$I = I_1 \cdots I_r = J_1 \cdots J_s.$$

In particular, the prime ideal I_1 divides $J_1 \cdots J_s$, so that I_1 divides J_j for some index j. But J_j is also prime, so that this forces $I_1 = J_j$. Canceling these ideals from each side we obtain

$$I_2 \cdots I_r = J_1 \cdots J_{j-1} \cdot J_{j+1} \cdots J_s.$$

But these products have norm less than $\mathrm{N}(I)$, so that they must coincide by the induction hypothesis. It follows that the two original factorizations of I were identical as well. □

EXAMPLE 2.21. Let us factor the principal ideal $(-55 + 187\sqrt{-5})$ in $\mathbf{Z}[\sqrt{-5}]$. This ideal has norm

$$\mathrm{N}(-55 + 187\sqrt{-5}) = 177870 = 2 \cdot 3 \cdot 5 \cdot 7^2 \cdot 11^2.$$

As the ideals (2), (3), (5), (7) all factor, while (11) is already prime, it follows that we must have

$$(-55 + 187\sqrt{-5}) = I_2 \cdot I_3 \cdot I_5 \cdot I_7^2 \cdot (11)$$

where I_2, I_3, I_5 and I_7 have norm 2, 3, 5 and 7 respectively. (We can not have the two different prime ideals of norm 7 occurring, as their product equals (7); thus (7) would divide $(-55 + 187\sqrt{-5})$, so that 7 would divide $-55 + 187\sqrt{-5}$, which it does not.) There are unique prime ideals of norm 2 and 5, so that to complete the factorization we must determine which ideal of each pair

$$(3, 1 - \sqrt{-5}), \quad (3, 1 + \sqrt{-5})$$
$$(7, 3 - \sqrt{-5}), \quad (7, 3 + \sqrt{-5})$$

divides $(-55 + 187\sqrt{-5})$.

For this we must work a bit harder. Recall that

$$(2, 1+\sqrt{-5}) \cdot (3, 1-\sqrt{-5}) = (1-\sqrt{-5})$$

$$(2, 1+\sqrt{-5}) \cdot (3, 1+\sqrt{-5}) = (1+\sqrt{-5}).$$

Since we know $(2, 1+\sqrt{-5})$ divides $(-55+187\sqrt{-5})$, we can determine which of the primes of norm 3 divide $(-55+187\sqrt{-5})$ by determining which of $1-\sqrt{-5}$ and $1+\sqrt{-5}$ divide $-55+187\sqrt{-5}$. In fact, it is $1-\sqrt{-5}$, so that $(3, 1-\sqrt{-5})$ divides $(-55+187\sqrt{-5})$. Similarly,

$$(2, 1+\sqrt{-5}) \cdot (7, 3-\sqrt{-5}) = (3-\sqrt{-5})$$

$$(2, 1+\sqrt{-5}) \cdot (7, 3+\sqrt{-5}) = (3+\sqrt{-5})$$

and $3+\sqrt{-5}$ divides $-55+187\sqrt{-5}$, so that $(7, 3+\sqrt{-5})$ divides $(-55+187\sqrt{-5})$. Thus

$$(-55+187\sqrt{-5}) = (2, 1+\sqrt{-5}) \cdot (3, 1-\sqrt{-5}) \cdot (\sqrt{-5}) \cdot (7, 3+\sqrt{-5})^2 \cdot (11)$$

is the factorization into prime ideals.

5. Exercises

Exercise 2.1. Verify that $\mathbf{Q}(\sqrt{-n})$ is a field.

Exercise 2.2. If $a, b \in \mathbf{Q}$ and $b \neq 0$, verify that the polynomial $x^2 + 2ax + (a^2+nb^2)$ is the unique monic quadratic polynomial with rational coefficients having $a + b\sqrt{-n}$ as a root.

Exercise 2.3. Verify that $a+b\sqrt{-n}$ with $a, b \in \mathbf{Q}$ has characteristic polynomial with integer coefficients if and only if $a, b \in \mathbf{Z}$ or $n \equiv 3 \pmod 4$, $2a, 2b \in \mathbf{Z}$ and $2a \equiv 2b \pmod 2$.

Exercise 2.4. Let n be a squarefree positive integer. An *order* in $\mathcal{O}_{-n}$ is a subring of $\mathcal{O}_{-n}$ which contains at least one irrational number. Let R be an order in $\mathcal{O}_{-n}$. Show that there is a positive integer f (called the *conductor* of R) such that

$$R = \{a + fb\varpi_{-n}\,;\, a, b \in \mathbf{Z}\}.$$

Exercise 2.5. Let $n \equiv 3 \pmod 4$ be a squarefree positive integer and consider the order $\mathbf{Z}[\sqrt{-n}]$ of conductor 2 in $\mathcal{O}_{-n}$. Let I denote the ideal $(2, 1+\sqrt{-n})$ of $\mathbf{Z}[\sqrt{-n}]$. Show that $I^2 = (2) \cdot I$ and conclude that unique factorization of ideals in $\mathbf{Z}[\sqrt{-n}]$ fails. (In fact, the ideals of the order of conductor f relatively prime to f do have unique factorization, although we do not prove this here.)

Exercise 2.6. Prove cancellation for ideals: if I, J, K are ideals of $\mathcal{O}_{-n}$ such that $I \cdot K = J \cdot K$, then $I = J$.

Exercise 2.7. Use factorization into ideals to explain the counterexample

$$55 = (7+\sqrt{-6}) \cdot (7-\sqrt{-6})$$

to unique factorization in $\mathbf{Z}[\sqrt{-6}]$.

Exercise 2.8. Show that the two prime factors of (101) in $\mathbf{Z}[\sqrt{-5}]$ are principal.

Exercise 2.9. Let I be the ideal $(3, 1+\sqrt{-14})$ in $\mathbf{Z}[\sqrt{-14}]$. Show that I^4 is principal but I, I^2, I^3 are not.

Exercise 2.10. Let n be a squarefree positive integer. Show that the ideal (2) factors into prime ideals as follows:

$$(2) = \begin{cases} (2, 1+\sqrt{-n})^2 & n \equiv 1 \pmod 4; \\ (2, \sqrt{-n})^2 & n \equiv 2 \pmod 4; \\ (2) & n \equiv 3 \pmod 8; \\ (2, \varpi_{-n}) \cdot (2, 1+\varpi_{-n}) & n \equiv 7 \pmod 8. \end{cases}$$

Exercise 2.11. Use the ideal factorization of Example 2.21 to find all factorizations of $-55 + 187\sqrt{-5}$ into irreducibles in $\mathbf{Z}[\sqrt{-5}]$.

Exercise 2.12. Factor the principal ideal $(3 + 68\sqrt{-5})$ into prime ideals in $\mathbf{Z}[\sqrt{-5}]$.

CHAPTER 3

Ideals and lattices

In the examples of the previous lecture, we repeatedly saw that a product of non-principal ideals of $\mathbf{Z}[\sqrt{-5}]$ is actually principal. In fact, this is always true in $\mathbf{Z}[\sqrt{-5}]$. This fact can be interpreted as implying that the failure of unique factorization in $\mathbf{Z}[\sqrt{-5}]$ is fairly mild: an irreducible element in $\mathbf{Z}[\sqrt{-5}]$ can at worst factor into a product of two prime ideals. For larger values of n, however, more complex behavior is possible. The possibilities are captured by the ideal class group. In this chapter we define the ideal class group of an imaginary quadratic field and then relate it to the class groups of the first lecture.

1. The ideal class group

Let n be a squarefree positive integer and let $\mathcal{O}_{-n}$ denote the ring of algebraic integers in $\mathbf{Q}(\sqrt{-n})$. We have already seen that the set of ideals of $\mathcal{O}_{-n}$ does not form a group, as there are no inverses. On the other hand, we have seen that any ideal divides a principal ideal. This suggests that if we consider all *principal ideals* to be the identity element, then we should be able to obtain inverses of ideals. This is what we now do.

Definition 3.1. Two ideals I, J are said to be *similar*, written $I \sim J$, if there are $\alpha, \beta \in \mathcal{O}_{-n}$ such that $(\alpha) \cdot I = (\beta) \cdot J$. One checks immediately that similarity is an equivalence relation on the set of ideals. An equivalence class for similarity is called an *ideal class*; we write the ideal class of an ideal I as $\mathcal{C}_I$. Thus if $\mathcal{C}$ is an ideal class, then we have $\mathcal{C} = \mathcal{C}_I$ for any $I \in \mathcal{C}$. The *ideal class group* $\mathcal{C}l(-n)$ of $\mathcal{O}_{-n}$ is the set of all ideal classes in $\mathcal{O}_{-n}$.

Note that the ideal class $\mathcal{C}_{\mathcal{O}_{-n}}$ consists of all principal ideals. Indeed, any principal ideal (α) is similar to $\mathcal{O}_{-n}$ since

$$(1) \cdot (\alpha) = (\alpha) \cdot \mathcal{O}_{-n};$$

conversely, if I is similar to $\mathcal{O}_{-n}$, then

$$(\alpha) \cdot I = (\beta) \cdot \mathcal{O}_{-n} = (\beta)$$

from which it follows that α divides β and $I = (\beta/\alpha)$. We will simply write $\mathcal{C}_1$ for the ideal class of principal ideals.

Example 3.2. We will see later that there are only two ideal classes in $\mathbf{Z}[\sqrt{-5}]$: the principal class, and a class of all non-principal ideals. For example,

$$(2, 1+\sqrt{-5}) \sim (3, 1+\sqrt{-5})$$

since

$$(3) \cdot (2, 1+\sqrt{-5}) = (1-\sqrt{-5}) \cdot (3, 1+\sqrt{-5}).$$

We have not yet developed the tools needed to prove that such relations exist for arbitrary pairs of non-principal ideals in $\mathbf{Z}[\sqrt{-5}]$.

The next lemma shows that the product of ideals is compatible with similarity.

Lemma 3.3. *Let I, I', J, J' be ideals of $\mathcal{O}_{-n}$ such that $I \sim J$ and $I' \sim J'$. Then $I \cdot I' \sim J \cdot J'$.*

Proof. By the definition of similarity, there exist $\alpha, \beta, \alpha', \beta' \in \mathcal{O}_{-n}$ such that

$$(\alpha) \cdot I = (\beta) \cdot J$$

$$(\alpha') \cdot I' = (\beta') \cdot J'.$$

Thus

$$(\alpha\alpha') \cdot (I \cdot I') = (\beta\beta') \cdot (J \cdot J')$$

so that $I \cdot I' \sim J \cdot J'$. □

We may use Lemma 3.3 to define the product of two ideal classes $\mathcal{C}$ and $\mathcal{C}'$ as follows: pick $I \in \mathcal{C}$ and $J \in \mathcal{C}'$, so that $\mathcal{C} = \mathcal{C}_I$ and $\mathcal{C}' = \mathcal{C}_J$. Define

$$\mathcal{C} \cdot \mathcal{C}' = \mathcal{C}_{I \cdot J};$$

that is,

$$\mathcal{C}_I \cdot \mathcal{C}_J = \mathcal{C}_{I \cdot J}.$$

The resulting ideal class $\mathcal{C}_{I \cdot J}$ is independent of the choice of I, J by Lemma 3.3. The next proposition shows that this definition makes $\mathcal{C}l(-n)$ into a group.

Proposition 3.4. *The above product makes $\mathcal{C}l(-n)$ into an abelian group with identity element the class $\mathcal{C}_1$ of principal ideals.*

Proof. Associativity and commutativity are straightforward from the corresponding properties of the ideal product; for example if $\mathcal{C}, \mathcal{C}'$ are ideal classes, then

$$\mathcal{C} \cdot \mathcal{C}' = \mathcal{C}_I \cdot \mathcal{C}_J = \mathcal{C}_{I \cdot J} = \mathcal{C}_{J \cdot I} = \mathcal{C}_J \cdot \mathcal{C}_I = \mathcal{C}' \cdot \mathcal{C}$$

where $I \in \mathcal{C}$ and $J \in \mathcal{C}'$. The class $\mathcal{C}_1$ of principal ideals functions as the identity since

$$\mathcal{C} \cdot \mathcal{C}_1 = \mathcal{C}_I \cdot \mathcal{C}_{\mathcal{O}_{-n}} = \mathcal{C}_{I \cdot \mathcal{O}_{-n}} = \mathcal{C}_I = \mathcal{C}$$

for $I \in \mathcal{C}$.

The most interesting part is inverses. In fact, for an ideal class $\mathcal{C}$, we define the inverse class by

$$\mathcal{C}^{-1} = \{\bar{I}\,;\, I \in \mathcal{C}\}$$

with $\bar{I}$ the conjugate ideal of I as in Lemma 2.13. (We leave it to the reader to check that this is an ideal class.) Fix $I \in \mathcal{C}$; then

$$\mathcal{C} \cdot \mathcal{C}^{-1} = \mathcal{C}_I \cdot \mathcal{C}_{\bar{I}} = \mathcal{C}_{I \cdot \bar{I}} = \mathcal{C}_{(\mathrm{N}(I))} = \mathcal{C}_1$$

since $(\mathrm{N}(I))$ is principal. (Note that we are taking advantage of the fact that we may choose any ideals in $\mathcal{C}$ and $\mathcal{C}^{-1}$ when computing the product.) □

Unfortunately, our ability to say anything interesting about ideal class groups is severely limited at the moment, as we have no techniques for showing that any ideals are not principal. Without further ado we thus turn to the question of computing ideal class groups.

2. Ideals as complex lattices

The key insight is that an ideal of $\mathcal{O}_{-n}$, when regarded as a subset of the complex numbers $\mathbf{C}$, is a complex lattice with CM by ϖ_{-n}, where as usual

$$\varpi_{-n} = \begin{cases} \sqrt{-n} & n \equiv 1, 2 \pmod 4; \\ \frac{1+\sqrt{-n}}{2} & n \equiv 3 \pmod 4. \end{cases}$$

Lemma 3.5. *Let I be an ideal of $\mathcal{O}_{-n}$. Regarding I as a subset of the complex numbers, it is a complex lattice with CM by ϖ_{-n}. If m is the least positive integer in I and $a + b\sqrt{-n}$ is an element of I with minimal positive coefficient of $\sqrt{-n}$, then $m, a + b\sqrt{-n}$ is a lattice basis of I.*

Note that if $n \equiv 3 \pmod 4$, then the number b above may be a half-integer instead of an integer.

Proof. To show that I is a lattice it suffices to prove that

$$I = \left\{ mx + (a + b\sqrt{-n})y \,;\, x, y \in \mathbf{Z} \right\}$$

with $m, a + b\sqrt{-n}$ as in the statement of the lemma. It is clear from the definition of ideal that any linear combination of m and $a + b\sqrt{-n}$ lies in I, so that it suffices to show that an arbitrary $c + d\sqrt{-n} \in I$ can be expressed as an integer linear combination of m and $a + b\sqrt{-n}$.

We can choose an integer y such that $0 \leq d - by < b$. Since

$$(c + d\sqrt{-n}) - y(a + b\sqrt{-n}) = (c - ay) + (d - by)\sqrt{-n}$$

lies in I and b is the minimal positive coefficient of $\sqrt{-n}$ occurring in I, it follows that in fact $d = by$. In particular,

$$c - ay = (c + d\sqrt{-n}) - y(a + b\sqrt{-n}) \in I$$

is an integer and thus must be divisible by m by a similar argument. (Note that $c - ay$ really is an integer since the only rational numbers in $\mathcal{O}_{-n}$ are integers.) That is, there exists an integer x such that $c - ay = mx$. Thus

$$c + d\sqrt{-n} = mx + (a + b\sqrt{-n})y$$

as desired.

The fact that I has CM by ϖ_{-n} is immediate from the fact that it is an ideal of $\mathcal{O}_{-n}$ and thus is closed under multiplication by $\varpi_{-n} \in \mathcal{O}_{-n}$. □

The connection between ideal class groups and the lattice class groups of Chapter 1 arises from the observation that similarity of ideals corresponds to homothety of lattices.

Lemma 3.6. *Two ideals I, J of $\mathcal{O}_{-n}$ are similar if and only if they are homothetic as lattices. In particular, I, J are similar if and only if $j(I) = j(J)$ with $j(\cdot)$ the j-invariant of the ideal regarded as a lattice.*

For the ideals $(2, 1 + \sqrt{-5})$ and $(3, 1 + \sqrt{-5})$ of $\mathcal{O}_{-5}$, this similarity can be seen in the pictures below.

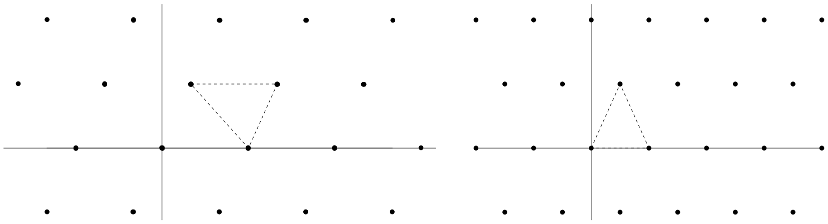

FIGURE 13. The ideals $(2, 1+\sqrt{-5})$ and $(3, 1+\sqrt{-5})$

PROOF. Suppose first that I and J are similar. Then there exist non-zero $\alpha, \beta \in \mathcal{O}_{-n}$ such that $(\alpha) \cdot I = (\beta) \cdot J$; that is, $I = \frac{\beta}{\alpha} \cdot J$, so that I and J are homothetic.

Conversely, if I and J are homothetic as lattices, then there exists $\alpha \in \mathbf{C}^\times$ such that $I = \alpha \cdot J$. In particular, fixing some non-zero $j \in J$, we have $\alpha \cdot j \in I$; since both I and J lie in $\mathcal{O}_{-n}$, it follows that

$$\alpha = \frac{\alpha \cdot j}{j} \in \mathbf{Q}(\sqrt{-n}).$$

Thus there is a non-zero integer m such that $m \cdot \alpha \in \mathcal{O}_{-n}$. (One may simply take m to be the least common multiple of the denominators of the coefficients of α.) Now

$$(m) \cdot I = (m \cdot \alpha) \cdot J$$

and $m, m \cdot \alpha \in \mathcal{O}_{-n}$, so that I and J are similar ideals. □

The last result we need to relate the two notions of class group is the fact that any lattice with CM by ϖ_{-n} is homothetic to some ideal of $\mathcal{O}_{-n}$.

LEMMA 3.7. *Let $\frac{a+\sqrt{-n}}{b}$ be the j-invariant of a lattice with CM by ϖ_{-n} as in Theorem 1.12 and Exercise 1.5. Then $(b, a+\sqrt{-n})$ is an ideal of $\mathcal{O}_{-n}$ which has j-invariant $\frac{a+\sqrt{-n}}{b}$ when regarded as a complex lattice.*

PROOF. We claim that $b, a+\sqrt{-n}$ is a lattice basis of the ideal $I := (b, a+\sqrt{-n})$. By Lemma 3.5 to check this it suffices to check that b is the least positive integer in I and that there is no element of I of the form $c+\frac{1}{2}\sqrt{-n}$. For the former statement, by Exercise 3.1 the only integers in I are linear combinations of b and a^2+n. The latter quantity is divisible by b, so that b will indeed be the least positive integer in I. The fact that $c+\frac{1}{2}\sqrt{-n} \notin I$ for any c is clear when $n \equiv 1, 2 \pmod 4$ and follows from the fact that b is even when $n \equiv 3 \pmod 4$.

Since $\frac{a+\sqrt{-n}}{b}$ lies in $\mathcal{F}$ by assumption, it follows that the ideal I has j-invariant $\frac{a+\sqrt{-n}}{b}$, as desired. □

We can combine the above results to show that our two notions of class groups coincide. For clarity we write $\mathcal{C}l(-n)$ for the ideal class group of $\mathcal{O}_{-n}$ and $\mathcal{C}l'(-n)$ for the set of homothety classes of lattices with CM by ϖ_{-n}.

COROLLARY 3.8. *Let n be a squarefree positive integer. The map $\mathcal{C}l(-n) \to \mathcal{C}l'(-n)$ sending an ideal class $\mathcal{C}$ to $j(I)$ for any $I \in \mathcal{C}$ is a bijection.*

Proof. Lemma 3.6 shows that similar ideals are homothetic, so that any ideals in an ideal class gives rise to homothetic lattices and thus to the same j-invariant; thus the map $\mathcal{C}l(-n) \to \mathcal{C}l'(-n)$ is well-defined. Lemma 3.6 also shows that it is injective, as if $\mathcal{C}_I$ and $\mathcal{C}_J$ are ideal classes containing homothetic ideals, then I and J must be similar so that $\mathcal{C}_I = \mathcal{C}_J$. Lemma 3.7 shows that the map is surjective. □

3. Example: $n = 14$

In this section we illustrate the methods we have developed in the case of $\mathbf{Z}[\sqrt{-14}]$. We have already seen that in terms of lattices we have

$$\mathcal{C}l(-14) = \left\{\sqrt{-14}, \frac{\sqrt{-14}}{2}, \frac{-1+\sqrt{-14}}{3}, \frac{1+\sqrt{-14}}{3}\right\}.$$

Proposition 3.5 allows us to easily write down ideals of each j-invariant:

$$\begin{aligned} j(\mathcal{O}_{-14}) &= \sqrt{-14} \\ j(2, \sqrt{-14}) &= \frac{\sqrt{-14}}{2} \\ j(3, 1-\sqrt{-14}) &= \frac{1-\sqrt{-14}}{3} \\ j(3, 1+\sqrt{-14}) &= \frac{1+\sqrt{-14}}{3} \end{aligned}$$

For ease of notation, set

$$\begin{aligned} \mathcal{C}_1 &= \mathcal{C}_{\mathcal{O}_{-14}} \\ \mathcal{C}_2 &= \mathcal{C}_{(2,\sqrt{-14})} \\ \mathcal{C}_3 &= \mathcal{C}_{(3,1-\sqrt{-14})} \\ \mathcal{C}_3' &= \mathcal{C}_{(3,1+\sqrt{-14})} \end{aligned}$$

We can compute the group structure of $\mathcal{C}l(-14)$ as follows. We already know that $\mathcal{C}_1$ is the identity. The fact that

$$(2, \sqrt{-14})^2 = (2)$$

is principal implies that $\mathcal{C}_2^2 = \mathcal{C}_1$. Similarly, the fact that

$$(3, 1-\sqrt{-14}) \cdot (3, 1+\sqrt{-14}) = (3)$$

implies that $\mathcal{C}_3 \cdot \mathcal{C}_3' = \mathcal{C}_1$. So far we have the following multiplication table:

$\cdot$	$\mathcal{C}_1$	$\mathcal{C}_2$	$\mathcal{C}_3$	$\mathcal{C}_3'$
$\mathcal{C}_1$	$\mathcal{C}_1$	$\mathcal{C}_2$	$\mathcal{C}_3$	$\mathcal{C}_3'$
$\mathcal{C}_2$	$\mathcal{C}_2$	$\mathcal{C}_1$	?	?
$\mathcal{C}_3$	$\mathcal{C}_3$	?	?	$\mathcal{C}_1$
$\mathcal{C}_3'$	$\mathcal{C}_3'$	?	$\mathcal{C}_1$	?

The ideal class $\mathcal{C}_2 \cdot \mathcal{C}_3$ is represented by

$$\begin{aligned} (2, \sqrt{-14}) \cdot (3, 1-\sqrt{-14}) &= (6, 3\sqrt{-14}, 2-2\sqrt{-14}, 14+\sqrt{-14}) \\ &= (6, 14+\sqrt{-14}) = (6, 2+\sqrt{-14}). \end{aligned}$$

We can compute the ideal class of this ideal by computing its j-invariant as in Proposition 1.9. The elements $6, 2+\sqrt{-14}$ are a lattice basis by Lemma 3.5, so that one finds that

$$j(6, 2+\sqrt{-14}) = \frac{1+\sqrt{-14}}{3}.$$

Thus $(6, 2+\sqrt{-14}) \in \mathcal{C}_3'$ so that $\mathcal{C}_2 \cdot \mathcal{C}_3 = \mathcal{C}_3'$. Taking inverses, this also implies that $\mathcal{C}_2 \cdot \mathcal{C}_3' = \mathcal{C}_3$.

We could continue in this fashion to compute the entire multiplication table. Alternately, we can resort to some trickery:

$$\mathcal{C}_3' \cdot \mathcal{C}_3' = (\mathcal{C}_2 \cdot \mathcal{C}_3) \cdot \mathcal{C}_3' = \mathcal{C}_2 \cdot (\mathcal{C}_3 \cdot \mathcal{C}_3') = \mathcal{C}_2 \cdot \mathcal{C}_1 = \mathcal{C}_2.$$

Taking inverses shows that $\mathcal{C}_3 \cdot \mathcal{C}_3 = \mathcal{C}_2$, completing the multiplication table:

$\cdot$	$\mathcal{C}_1$	$\mathcal{C}_2$	$\mathcal{C}_3$	$\mathcal{C}_3'$
$\mathcal{C}_1$	$\mathcal{C}_1$	$\mathcal{C}_2$	$\mathcal{C}_3$	$\mathcal{C}_3'$
$\mathcal{C}_2$	$\mathcal{C}_2$	$\mathcal{C}_1$	$\mathcal{C}_3'$	$\mathcal{C}_3$
$\mathcal{C}_3$	$\mathcal{C}_3$	$\mathcal{C}_3'$	$\mathcal{C}_2$	$\mathcal{C}_1$
$\mathcal{C}_3'$	$\mathcal{C}_3'$	$\mathcal{C}_3$	$\mathcal{C}_1$	$\mathcal{C}_2$

Let us consider some larger primes. The prime $p = 5$ factors as

$$(5) = (5, 1+\sqrt{-14})(5, 1-\sqrt{-14}).$$

One computes

$$j(5, 1+\sqrt{-14}) = \frac{-1+\sqrt{-14}}{3};$$

that is,

$$(5, 1+\sqrt{-14}) \in \mathcal{C}_3.$$

Similarly,

$$(5, 1-\sqrt{-14}) \in \mathcal{C}_3'.$$

The prime $p = 7$ factors as

$$(7) = (7, \sqrt{-14})^2.$$

(Right away this tells us that the ideal class of $(7, \sqrt{-14})$ has order 1 or 2, so that it is either $\mathcal{C}_1$ or $\mathcal{C}_2$.) We compute

$$j(7, \sqrt{-14}) = \frac{\sqrt{-14}}{2}$$

so that $(7, \sqrt{-14}) \in \mathcal{C}_2$.

The prime $p = 11$ does not factor, so that next interesting prime is $p = 13$:

$$(13) = (13, 5+\sqrt{-14}) \cdot (13, 5-+\sqrt{-14}).$$

One computes

$$j(13, 5+\sqrt{-14}) = \frac{1+\sqrt{-14}}{3}$$
$$j(13, 5-+\sqrt{-14}) = \frac{-1+\sqrt{-14}}{3}$$

so that

$$(13, 5+\sqrt{-14}) \in \mathcal{C}_3'$$
$$(13, 5-\sqrt{-14}) \in \mathcal{C}_3.$$

In particular, since $\mathcal{C}_3 \cdot \mathcal{C}_3' = \mathcal{C}_1$, we know that the ideal

$$(5, 1+\sqrt{-14}) \cdot (13, 5+\sqrt{-14})$$

is principal! In fact,

$$(5, 1+\sqrt{-14}) \cdot (13, 5+\sqrt{-14}) = (65, 31+\sqrt{-14}) = (3-2\sqrt{-14})$$

as one checks fairly easily.

The smallest prime which factors as a product of principal ideals is $p = 23$; it factors as

$$(23) = (23, 3+\sqrt{-14}) \cdot (23, 3-\sqrt{-14})$$

where

$$(23, 3+\sqrt{-14}) = (3+\sqrt{-14})$$
$$(23, 3-\sqrt{-14}) = (3-\sqrt{-14}).$$

Note that we have now answered our earlier question as to for which primes p there exist irreducibles of $\mathcal{O}_{-n}$ of norm p: such an irreducible exists if and only if there is a principal ideal of norm p, which in turn exists if and only if p factors (so that $\left(\frac{-n}{p}\right) = 1$) into principal ideals (so that the ideal factors of p have j-invariant equal to ϖ_{-n}).

4. Exercises

Exercise 3.1. Let $I = (b, a+\sqrt{-n})$ be an ideal of $\mathcal{O}_{-n}$ with a, b as in Theorem 1.12 or Exercise 1.5. Show that the only integers in I are linear combinations of b and $a^2 + n$.

In the next three exercises we give criteria for ideal class groups to contain non-trivial elements.

Exercise 3.2. Let n be a squarefree positive integer. Show that the ideals of $\mathcal{O}_{-n}$ of norm 2 are not principal if either $n \equiv 1, 2 \pmod 4$ and $n \geq 5$ or $n \equiv 7 \pmod 8$ and $n \geq 15$. (Hint: It is easy to compute the j-invariant of a lattice if the ratio of an obvious basis lies in $\mathcal{F}$.)

Exercise 3.3. Let n be a squarefree positive integer. Show that the ideals of $\mathcal{O}_{-n}$ of norm 3 are not principal in any of the following cases:

- $n \equiv 2, 5, 6, 9 \pmod{12}$ and $n \geq 9$;
- $n \equiv 3 \pmod{12}$ and $n \geq 27$;
- $n \equiv 11 \pmod{12}$ and $n \geq 35$.

(Hint: the obvious ideal generators are not lattice bases in the last two cases.)

Exercise 3.4. Let $n \equiv 3 \pmod 4$ be a squarefree positive integer. Show that the ideals of $\mathcal{O}_{-n}$ of norm 5 are not principal in any of the following cases:

- $n \equiv 11 \pmod{20}$ and $n \geq 91$;
- $n \equiv 15 \pmod{20}$ and $n \geq 75$;
- $n \equiv 19 \pmod{20}$ and $n \geq 99$.

Exercise 3.5. Find all squarefree positive $n \leq 300$ such that $h(-n) = 1$. (Hint: Use Exercises 3.2–3.4 to eliminate most values of n.) In fact, every n with $h(-n) = 1$ will be in your list, although this is very difficult to prove.

Exercise 3.6. Let $J = (b, a + \sqrt{-n})$ be an ideal with a, b as in Theorem 1.12 or Exercise 1.5. Prove that

$$\mathrm{N}(J) = \begin{cases} b & n \equiv 1, 2 \pmod 4; \\ 2b & n \equiv 3 \pmod 4). \end{cases}$$

Exercise 3.7. Let $n \equiv 1, 2 \pmod 4$ be a squarefree integer and fix an ideal class $\mathcal{C} \in \mathcal{C}l(-n)$ with j-invariant $\frac{a+\sqrt{-n}}{b}$ as in Theorem 1.12. Let p be a prime such that $\left(\frac{-n}{p}\right) = 1$. Prove that $\mathcal{C}$ contains an ideal of norm p if and only if there are $x, y \in \mathbf{Z}$ such that

$$bx^2 + 2axy + \frac{a^2 + n}{b} y^2 = p.$$

(Hint: Let $J = (b, a + \sqrt{-n}) \in \mathcal{C}$. Suppose I is an ideal in $\mathcal{C}$ of norm p and let $\bar{I}$ denote the conjugate ideal. Let α be a generator of the principal ideal $\bar{I} \cdot J$. Then $\alpha \in J$, so that it can be expressed as $bx + (a + \sqrt{-n})y$ for some $x, y \in \mathbf{Z}$.) Can you find an algorithm to determine x and y?

Exercise 3.8. Use Exercise 3.7 to show that a prime $p \neq 2, 5$ satisfies $\left(\frac{-5}{p}\right) = 1$ if and only if there are integers x, y such that one of the two equations

$$p = x^2 + 5y^2$$
$$p = 2x^2 + 2xy + 3y^2$$

is satisfied.

Exercise 3.9. Use Exercise 3.7 to show that a prime $p \neq 2, 7$ satisfies $\left(\frac{-14}{p}\right) = 1$ if and only if there are integers x, y such that one of the three equations

$$p = x^2 + 14y^2$$
$$p = 2x^2 + 7y^2$$
$$p = 3x^2 + 2xy + 5y^2$$

is satisfied.

CHAPTER 4

The Riemann Zeta Function

1. Dirichlet series

Consider an infinite sequence

$$a_1, a_2, a_3, \ldots$$

of real numbers. Often in combinatorics one studies such a sequence by introducing the *generating function*

$$f(x) := \sum_{m=1}^{\infty} a_m x^m$$

and attempting to study the properties of the resulting function $f(x)$. A function of this form, however, is best suited to the study of additive questions. In order to study multiplicative questions, as is usually of interest in number theory, it is necessary to introduce Dirichlet series.

Definition 4.1. A (real) *Dirichlet series* is a function of the form

$$f(s) := \sum_{m=1}^{\infty} a_m m^{-s}$$

for real numbers $a_1, a_2, \ldots$.

The use of the variable s is traditional and impossible to fight at this point. The fundamental example of a Dirichlet series is the *Riemann zeta function*

$$\zeta(s) := \sum_{m=1}^{\infty} m^{-s}$$

obtained with $a_m = 1$ for all m. This function will play a crucial role in all that follows.

Before we can even begin to study Dirichlet series we had best deal with issues of convergence. For example, it is immediate from the integral test that the series defining $\zeta(s)$ converges for all $s > 1$ and diverges for $s \leq 1$. A general convergence result is given in the next proposition. Although it might seem more natural to give a criterion in terms of bounds on the coefficients a_m, in our applications it will be crucial to have a result which takes into account partial cancellation occurring among the coefficients.

Proposition 4.2. *Let $a_1, a_2, \ldots$ be a sequence of real numbers. Suppose that there are real numbers $c, r > 0$ such that*

$$\left| \sum_{m=1}^{M} a_m \right| \leq cM^r$$

for all $M \geq 1$. Then the Dirichlet series

$$\sum_{m=1}^{\infty} a_m m^{-s}$$

converges for all $s > r$. The resulting function of s is continuous.

For example, for the Riemann zeta function we have

$$\sum_{m=1}^{M} a_m = M$$

so that we may apply Proposition 4.2 with $c = 1$ and $r = 1$ to obtain the expected region of convergence for $\zeta(s)$. Note that Proposition 4.2 also provides the additional information that $\zeta(s)$ is a continuous function of s for $s > 1$.

Proof. To understand the convergence of $\sum a_m m^{-s}$ we first must estimate the tail $\sum_{m \geq M} a_m m^{-s}$ for M large. Set

$$A_M = \sum_{m=1}^{M} a_m;$$

by hypothesis we know that $|A_M| \leq cM^r$. Fix $s > r$. For positive integers M, N with $M < N$ a simple rearrangement of terms shows that

$$\sum_{m=M}^{N} a_m m^{-s} = A_N N^{-s} - A_{M-1} M^{-s} + \sum_{m=M}^{N-1} A_m \left(m^{-s} - (m+1)^{-s}\right).$$

Thus

$$\left|\sum_{m=M}^{N} a_m m^{-s}\right| \leq c\left(N^{r-s} + (M-1)^{r-s} + \sum_{m=M}^{N-1} m^r (m^{-s} - (m+1)^{-s})\right).$$

Exercise 4.1 shows that

$$m^{-s} - (m+1)^{-s} \leq s m^{-s-1}$$

so that we obtain

$$\begin{aligned}\left|\sum_{m=M}^{N} a_m m^{-s}\right| &\leq c\left(N^{r-s} + (M-1)^{r-s} + s \cdot \sum_{m=M}^{N-1} m^{r-s-1}\right)\\ &\leq c\left(N^{r-s} + (M-1)^{r-s} + s \cdot \sum_{m=M}^{\infty} m^{r-s-1}\right)\end{aligned}$$

(since adding positive terms can only increase the sum)

$$\leq c\left(N^{r-s} + (M-1)^{r-s} + s \cdot \int_{M-1}^{\infty} m^{r-s-1}\right)$$

(since this integral is easily seen to be larger than the sum)

$$\begin{aligned}&\leq c\left(N^{r-s} + (M-1)^{r-s} + \frac{s}{s-r}(M-1)^{r-s}\right)\\ &\leq c\left(N^{r-s} + \frac{2s-r}{s-r}(M-1)^{r-s}\right).\end{aligned}$$

Letting N go to infinity, we find that

$$\left|\sum_{m=M}^{\infty} a_m m^{-s}\right| \leq \frac{c(2s-r)}{s-r}(M-1)^{r-s}. \tag{11}$$

Since $s > r$ this goes to zero as M goes to infinity, which is precisely what it means for the sum $\sum_{m=1}^{\infty} a_m m^{-s}$ to converge.

We turn now to the continuity of the resulting function

$$f(s) := \sum_{m=1}^{\infty} a_m m^{-s}$$

for $s > r$. Fix $\varepsilon > 0$. We must show that there is a $\delta > 0$ such that

$$|t-s| < \delta \quad \Rightarrow \quad |f(t) - f(s)| < \varepsilon.$$

To do this we must estimate the difference $|f(t) - f(s)|$. Applying the triangle inequality and (11) we find that

$$\begin{aligned} |f(t)-f(s)| &\leq \left|f(t) - \sum_{m=1}^{M} a_m m^{-t}\right| + \left|\sum_{m=1}^{M} a_m m^{-t} - \sum_{m=1}^{M} a_m m^{-s}\right| \\ &\quad + \left|\sum_{m=1}^{M} a_m m^{-s} - f(s)\right| \\ &= \left|\sum_{m=M+1}^{\infty} a_m m^{-t}\right| + \left|\sum_{m=1}^{M} a_m m^{-t} - \sum_{m=1}^{M} a_m m^{-s}\right| + \left|\sum_{m=M+1}^{\infty} a_m m^{-s}\right| \\ &\leq \frac{c(2t-r)}{t-r} M^{r-t} + \frac{c(2s-r)}{s-r} M^{r-s} + \left|\sum_{m=1}^{M} a_m m^{-t} - \sum_{m=1}^{M} a_m m^{-s}\right| \end{aligned}$$

for any $M \geq 1$.

Fix now some s_0, $r < s_0 < s$. We may choose M large enough so that for all $t > s_0$ we have

$$\frac{c(2t-r)}{t-r} M^{r-t} < \frac{\varepsilon}{3}.$$

(Note that s_0 plays an important role, in that if we let t get too close to r then $\frac{1}{t-r}$ would blow up on us. We need s_0 to prevent this from occurring.) Thus

$$|f(t)-f(s)| \leq \frac{2}{3}\varepsilon + \left|\sum_{m=1}^{M} a_m m^{-t} - \sum_{m=1}^{M} a_m m^{-s}\right|$$

for all $t > s_0$. Finally, the finite sum

$$\sum_{m=1}^{M} a_m m^{-t}$$

is a continuous function of t, so that we may find a δ, $0 < \delta < s - s_0$, such that

$$\left|\sum_{m=1}^{M} a_m m^{-t} - \sum_{m=1}^{M} a_m m^{-s}\right| < \frac{\varepsilon}{3}$$

for all t with $|t-s| < \delta$. For such t we have

$$|f(t) - f(s)| < \varepsilon$$

as desired. □

2. The residue at $s = 1$ of the Riemann zeta function

We return now to the special case of the Riemann zeta function. We will especially be interested in its behavior near $s = 1$. Formally evaluating $\zeta(s)$ at $s = 1$ yields the harmonic series

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots .$$

This series is divergent, so that we certainly expect $\zeta(s)$ to go to infinity as s approaches 1. However, we can not immediately jump to this conclusion: it doesn't make any sense to discuss the continuity of $\zeta(s)$ at $s = 1$, so that it is not at all clear that

$$\lim_{s \to 1^+} \zeta(s) = \zeta(1),$$

whatever this equation would mean.

Instead we use the easy estimate

$$\zeta(s) = \sum_{m=1}^{\infty} m^{-s} \geq \int_1^{\infty} \frac{dx}{x^s} = \frac{1}{s-1} \tag{12}$$

for $s > 1$. (See Figure 14.) Taking the limit as s goes to 1, it follows that indeed

$$\lim_{s \to 1^+} \zeta(s) = \infty.$$

This fact may be used in conjunction with the Euler product for $\zeta(s)$ (discussed in the next section) to show that the sum of the reciprocals of the primes diverges; see Exercise 4.3.

For our own applications we will need more precise information about the behavior of $\zeta(s)$ as s approaches 1. The inequality (12) suggests that $\zeta(s)$ behaves like the function $\frac{1}{s-1}$ as s approaches 1. This leads to the following definition.

Definition 4.3. Let $f(s)$ be a function defined for $s > r$ such that

$$\lim_{s \to r^+} f(s) = \infty.$$

We say that $f(s)$ has a *simple pole* at $s = r$ if

$$\lim_{s \to r^+} (s - r) f(s)$$

exists and is non-zero; in this case we call the value of this limit the *residue* of $f(s)$ at $s = r$.

Essentially, if $f(s)$ has a simple pole at $s = r$ with residue c, then $f(s)$ behaves very much like $\frac{c}{s-r}$ as s approaches r. Thus we expect that $\zeta(s)$ has a simple pole with residue 1 at $s = 1$.

It is not at all difficult to verify this. Indeed, we simply need an upper bound on $\zeta(s)$ to go with (12).

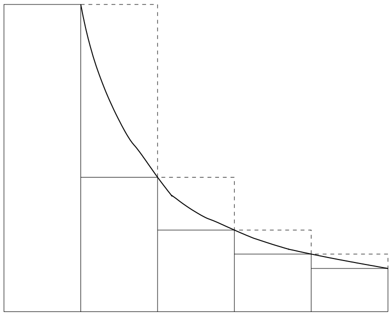

FIGURE 14. Bounding $\zeta(s)$

In fact, we have

$$\int_1^\infty \frac{dt}{t^s} \le \zeta(s) \le 1 + \int_1^\infty \frac{dt}{t^s}$$
$$\frac{1}{s-1} \le \zeta(s) \le \frac{s}{s-1}$$

for all $s > 1$. Thus

$$1 \le (s-1)\zeta(s) \le s;$$

taking the limit as s approaches 1 thus yields the following proposition.

PROPOSITION 4.4. *The Riemann zeta function $\zeta(s)$ has a simple pole with residue* 1 *at $s = 1$.*

We give a different, and somewhat better, proof of this proposition in Exercises 4.5 and 4.6.

3. Euler products

The Dirichlet series of interest in number theory have an additional special property: they have decompositions as infinite products over prime numbers. Although we will not need these results in our proof of the class number formula, these Euler products are extremely useful in the applications of Dirichlet series, as we will see in the exercises.

We first consider the case of the Riemann zeta function. Note that for a prime p and $s > 0$ we have $p^{-s} < 1$, so that

$$\big(1 - p^{-s}\big)^{-1} = 1 + p^{-s} + p^{-2s} + p^{-3s} + \cdots$$

Multiplying these qualities for $p = 2$ and $p = 3$ we find that

$$\begin{aligned}&\big(1 - 2^{-s}\big)^{-1} \cdot \big(1 - 3^{-s}\big)^{-1}\\ &\qquad = \big(1 + 2^{-s} + 4^{-s} + 8^{-s} + \cdots\big) \cdot \big(1 + 3^{-s} + 9^{-s} + 27^{-s} + \cdots\big)\\ &\qquad\qquad = 1 + 2^{-s} + 3^{-s} + 4^{-s} + 6^{-s} + 8^{-s} + 9^{-s} + 12^{-s} + 16^{-s} + \cdots\end{aligned}$$

where the final sum is the sum of m^{-s} as m runs over all positive integers divisible only by 2 and 3. Multiplying by a factor of $(1 - 5^{-s})^{-1}$ will add in all terms with 5 as a prime factor as well. Ignoring all issues of convergence, we will thus obtain exactly the Riemann zeta function after multiplying by the factors for every prime p.

Proposition 4.5. *For $s > 1$ we have*

$$\zeta(s) = \prod_p \left(1 - p^{-s}\right)^{-1}$$

where the product is over all prime numbers p.

Recall that an infinite product $\prod_{m=1}^{\infty} a_m$ is said to *converge* if the partial products $P_m := a_1 \cdots a_m$ converge to a number L as m goes to infinity.

Rather than prove Proposition 4.5 directly, we instead prove a general form which will be useful later. A sequence $a_1, a_2, a_3, \dots$ is said to be *multiplicative* if $a_{mn} = a_m \cdot a_n$ for all relatively prime m, n; it is said to be *completely multiplicative* if $a_{mn} = a_m \cdot a_n$ for all m, n.

Proposition 4.6. *Let $a_1, a_2, \dots$ be a multiplicative sequence such that there is a constant $c > 0$ with $\sum_{m=1}^{M} |a_m| \leq cM$ for all M. Then*

$$\sum_{m=1}^{\infty} a_m m^{-s} = \prod_p \left(\sum_{j=0}^{\infty} a_{p^j} p^{-js} \right)$$

for $s > 1$. If also $a_1, a_2, \dots$ is completely multiplicative and $|a_p| \leq p$ for all primes p, then in fact

$$\sum_{m=1}^{\infty} a_m m^{-s} = \prod_p \left(1 - a_p p^{-s}\right)^{-1}$$

for all $s > 1$.

In particular the proposition asserts that the products above converge for $s > 1$.

Proof. Fix $s > 1$. We assume first that $a_m \geq 0$ for all m. By Proposition 4.2 and the assumption that $\sum_{m=1}^{M} a_m \leq cM$ we know that $\sum_{m=1}^{\infty} a_m m^{-s}$ converges. Let p_i denote the i^{th} prime number and for $n \geq 1$ let S_n denote the set of all positive integers divisible only by $p_1, \dots, p_n$. The sum

$$\sum_{m \in S_n} a_m m^{-s}$$

is convergent since it is bounded by $\sum_m a_m m^{-s}$. Since every $m \in S_n$ can be written uniquely in the form $p_1^{j_1} \cdots p_n^{j_n}$ for $j_1, \dots, j_n \geq 0$, by the multiplicativity of the a_m we have

$$\begin{aligned}
\sum_{m \in S_n} a_m m^{-s} &= \sum_{j_1, \dots, j_n \geq 0} a_{p_1^{j_1}} \cdots a_{p_n^{j_n}} \left(p_1^{j_1} \cdots p_n^{j_n}\right)^{-s} \\
&= \sum_{j_1, \dots, j_n \geq 0} a_{p_1^{j_1}} p_1^{-j_1 s} \cdots a_{p_n^{j_n}} p_n^{-j_n s} \\
&= \prod_{i=1}^{n} \left(\sum_{j=0}^{\infty} a_{p_i^j} p_i^{-js} \right).
\end{aligned}$$

Since the sequence of sums

$$\sum_{m \in S_1} a_m m^{-s}, \sum_{m \in S_2} a_m m^{-s}, \sum_{m \in S_3} a_m m^{-s}, \dots$$

converge to $\sum_m a_m m^{-s}$, the same is thus true of the sequence of partial products

$$\prod_{i=1}^{1}\left(\sum_{j=0}^{\infty} a_{p_i^j} p_i^{-js}\right), \prod_{i=1}^{2}\left(\sum_{j=0}^{\infty} a_{p_i^j} p_i^{-js}\right), \prod_{i=1}^{3}\left(\sum_{j=0}^{\infty} a_{p_i^j} p_i^{-js}\right), \ldots .$$

Thus

$$\prod_{i=1}^{\infty}\left(\sum_{j=0}^{\infty} a_{p_i^j} p_i^{-js}\right)$$

converges and equals $\sum_{m=1}^{\infty} m^{-s}$, as desired.

If some a_m are negative, we apply the above argument to the $|a_m|$ to see that the sum

$$\sum_{j_1,\ldots,j_n \geq 0} a_{p_1^{j_1}} p_1^{-j_1 s} \cdots a_{p_n^{j_n}} p_n^{-j_n s}$$

is absolutely convergent and thus can be rearranged to $\sum_{m \in S_n} a_m m^{-s}$. With this in hand, the argument above applies directly to the a_m to prove the proposition in this case.

Finally, assume that the a_m are completely multiplicative. Since $a_{p_i} \leq p_i$ we have $a_{p_i} p_i^{-s} < 1$, so that

$$\begin{aligned}\left(1 - a_{p_i} p_i^{-s}\right)^{-1} &= 1 + a_{p_i} p_i^{-s} + a_{p_i}^2 p_i^{-2s} + a_{p_i}^3 p_i^{-3s} + \cdots \\ &= 1 + a_{p_i} p_i^{-s} + a_{p_i^2} p_i^{-2s} + a_{p_i^3} p_i^{-3s} + \cdots .\end{aligned}$$

Substituting this into the infinite product above yields the desired formula. □

4. L-functions

Fix a squarefree positive integer n and let $f(x)$ denote the characteristic polynomial of ϖ_{-n}; thus

$$f(x) = \begin{cases} x^2 + n & n \equiv 1, 2 \pmod 4 \\ x^2 - x + \frac{1+n}{4} & n \equiv 3 \pmod 4. \end{cases}$$

For a prime p we define the *extended Legendre symbol* $\left(\frac{-n}{p}\right)$ to be one less than the number of roots of $f(x)$ in $\mathbf{F}_p$. Then $\left(\frac{-n}{p}\right)$ agrees with the usual Legendre symbol for p odd (see Exercise 4.7), while

$$\left(\frac{-n}{2}\right) = \begin{cases} 1 & n \equiv 7 \pmod 8; \\ -1 & n \equiv 3 \pmod 8; \\ 0 & n \equiv 1, 2 \pmod 4. \end{cases}$$

For an arbitrary positive integer $m = p_1^{e_1} \cdots p_r^{e_r}$, we define

$$\left(\frac{-n}{m}\right) = \left(\frac{-n}{p_1}\right)^{e_1} \cdots \left(\frac{-n}{p_r}\right)^{e_r}.$$

Note that we have $\left(\frac{-n}{m}\right) \cdot \left(\frac{-n}{m'}\right) = \left(\frac{-n}{mm'}\right)$ for any $m, m' \geq 1$.

In order to define a Dirichlet series based on the Legendre symbol, we need the following fact.

Lemma 4.7. *We have*

$$\sum_{m=b}^{b+4n-1} \left(\frac{-n}{m}\right) = 0$$

for any $b \geq 1$*.*

Proof. Let S denote the sum above. By Exercise 4.8 $\left(\frac{-n}{m}\right)$ depends only on the residue of m in $\mathbf{Z}/4n$, so that it makes sense to write

$$S = \sum_{m \in \mathbf{Z}/4n} \left(\frac{-n}{m}\right).$$

By Exercise 4.9 we may choose $m_0 \in (\mathbf{Z}/4n)^{\times}$ such that $\left(\frac{-n}{m_0}\right) = -1$. Now

$$\begin{aligned} -S &= \left(\frac{-n}{m_0}\right) \cdot S \\ &= \left(\frac{-n}{m_0}\right) \cdot \sum_{m \in \mathbf{Z}/4n} \left(\frac{-n}{m}\right) \\ &= \sum_{m \in \mathbf{Z}/4n} \left(\frac{-n}{m_0 m}\right) \\ &= \sum_{m' \in \mathbf{Z}/4n} \left(\frac{-n}{m'}\right) \end{aligned}$$

(since $m' := m_0 m$ runs through $\mathbf{Z}/4n$ as m does)

$$= S.$$

Thus $S = 0$, as claimed. □

Define the *L-function* $L_{-n}(s)$ by

$$L_{-n}(s) := \sum_{m=1}^{\infty} \left(\frac{-n}{m}\right) m^{-s}.$$

The basic properties of $L_{-n}(s)$ are given in the next proposition.

Proposition 4.8. $L_{-n}(s)$ *converges to a continuous function for* $s > 0$*. For* $s > 1$ *there is a product expansion*

$$L_{-n}(s) = \prod_p \left(1 - \left(\frac{-n}{p}\right) p^{-s}\right)^{-1}.$$

Proof. Let $A_M = \sum_{m=1}^{M} \left(\frac{-n}{m}\right)$. By Lemma 4.7 we have $A_M = 0$ whenever M is divisible by $4n$. In particular, for any M

$$|A_M| = \left| \sum_{m=1}^{4n\lfloor M/4n \rfloor} \left(\frac{-n}{m}\right) + \sum_{m=4n\lfloor M/4n \rfloor + 1}^{M} \left(\frac{-n}{m}\right) \right| = \left| \sum_{m=4n\lfloor M/4n \rfloor + 1}^{M} \left(\frac{-n}{m}\right) \right| \leq 4n$$

since $\left| \left(\frac{-n}{m}\right) \right| \leq 1$ for all m. We may thus apply Proposition 4.2 with $c = 4n$ and $r = 0$ to obtain the first part of the proposition. The second part follows immediately from Proposition 4.6 and the definition of $\left(\frac{-n}{\cdot}\right)$ as a completely multiplicative function. □

In fact, the Euler product formula above still holds at $s = 1$. Unfortunately, the only proof of this we know involves complex analysis and is well beyond the scope of these notes.

5. Exercises

Exercise 4.1. Show that

$$m^{-s} - (m+1)^{-s} \leq sm^{-s-1}$$

for any $m > 0$ and $s > 0$. (Hint: apply the mean value theorem to the function $f(x) = x^{-s}$ on the interval $[m, m+1]$.)

Exercise 4.2. Show that the sum

$$\sum_{p \text{ prime}} \sum_{j=2}^{\infty} \frac{1}{jp^{js}}$$

is convergent for any $s > \frac{1}{2}$. (Hint: you can get away with some very crude approximations here.)

Exercise 4.3.

(1) Use the product formula to show that

$$\log \zeta(s) = -\sum_{p} \log(1 - p^{-s})$$

for any $s > 1$. (Note: you should never take the logarithm of zero, so you should check that all terms involved are positive.)

(2) Use the power series

$$\log(1-x) = -\sum_{j=1}^{\infty} \frac{x^j}{j}$$

to deduce that

$$\log \zeta(s) = \sum_{p} \sum_{j=1}^{\infty} jp^{-js}$$

for all $s > 1$. (This series is absolutely convergent, so that the order of summation does not affect the sum.)

(3) Rewrite the above expression as

$$\sum_{p} \frac{1}{p^s} = \log \zeta(s) - \sum_{p} \sum_{j=2}^{\infty} \frac{1}{jp^{js}}.$$

Use Exercise 4.2 to conclude that

$$\lim_{s \to 1^+} \sum_{p} \frac{1}{p^s} = \infty. \tag{13}$$

Unfortunately, it is not clear that

$$\lim_{s \to 1^+} \sum_{p} \frac{1}{p^s} = \sum_{p} \frac{1}{p} \tag{14}$$

(whatever precisely this means), so that this does not by itself show that the sum of the reciprocal of the primes diverges. (This does at least imply that there are infinitely many primes, for if there were only finitely many, then (14) would be obvious and (13) would then yield a contradiction.)

Exercise 4.4.

(1) With notation as in the proof of Proposition 4.6, show that

$$\log\left(\sum_{m\in S_n} m^{-s}\right) = \sum_{i=1}^{n}\frac{1}{p_i^s} + \sum_{i=1}^{n}\sum_{j=2}^{\infty}\frac{1}{jp_i^{js}},$$

with all sums involved absolutely convergent, for any $s > 0$.

(2) Take $s = 1$ above and take the limit as n goes to infinity to conclude that the sum of the reciprocals of the primes diverges.

Exercise 4.5. In the next two exercises we sketch an alternate proof that $\zeta(s)$ has a simple pole at $s = 1$ with residue 1. This proof has the advantage of giving information about $\zeta(s)$ for all $s > 0$ (whatever that means).

(1) Show that the Dirichlet series

$$\tilde{\zeta}(s) = \sum_{m=1}^{\infty}(-1)^{m+1}m^{-s}$$

converges to a continuous function for all $s > 0$.

(2) Use the power series

$$\log(1+x) = \sum_{j=1}^{\infty}(-1)^{j+1}\frac{x^j}{j}$$

(valid for $-1 < x \leq 1$) to show that

$$\tilde{\zeta}(1) = \log 2.$$

(The order of summation in the definition of $\tilde{\zeta}(s)$ is crucial here.)

(3) Show that

$$\zeta(s)\cdot(1-2^{1-s}) = \tilde{\zeta}(s)$$

for all $s > 1$. (This formula allows us to define $\zeta(s)$ to be $\tilde{\zeta}(s)/(1-2^{1-s})$ for all $s > 0$, $s \neq 1$.)

(4) Assuming that $\tilde{\zeta}(s)$ is differentiable at $s = 1$, evaluate

$$\lim_{s\to 1^+}(s-1)\zeta(s) = \lim_{s\to 1}\frac{(s-1)\tilde{\zeta}(s)}{1-2^{1-s}}.$$

Exercise 4.6. In this exercise we sketch a proof that $\tilde{\zeta}(s)$ is a differentiable function for all $s > 0$, with derivative the Dirichlet series

$$\sum_{m=1}^{\infty}(-1)^{m+1}\log m\cdot m^{-s}. \tag{15}$$

(In fact, Dirichlet series are always differentiable in their region of convergence.)

(1) Show that (15) converges for $s > 0$.

(2) Fix $s > 0$ and s_0, $0 < s_0 < s$. Use the mean value theorem to show that

$$\left|\sum_{m=M}^{N}(-1)^{m+1}m^{s} - \sum_{m=M}^{N}(-1)^{m+1}m^{-t}\right| \leq |s-t|\cdot\left|\sum_{m=M}^{N}(-1)^{m+1}\log m\cdot m^{s_0}\right|$$

for all $t > s_0$.

(3) Conclude that there are constants C_M such that

$$\left|\sum_{m=M}^{\infty}(-1)^{m+1}m^{s}-\sum_{m=M}^{\infty}(-1)^{m+1}m^{-t}\right|<C_M|s-t|$$

for all $t>s_0$ and such that

$$\lim_{M\to\infty}C_M=0.$$

(4) Use the triangle inequality to show that

$$\left|\frac{\tilde\zeta(s)-\tilde\zeta(t)}{s-t}-\sum_{m=1}^{\infty}(-1)^{m+1}\log m\cdot m^{-s}\right|\leq \tag{16}$$

$$\left|\frac{\sum_{m=M+1}^{\infty}(-1)^{m+1}m^{-s}-\sum_{m=M+1}^{\infty}(-1)^{m+1}m^{-t}}{s-t}\right|-$$

$$\left|\frac{\sum_{m=1}^{M}(-1)^{m+1}m^{-s}-\sum_{m=1}^{M}(-1)^{m+1}m^{-t}}{s-t}-\sum_{m=1}^{M}(-1)^{m+1}\log m\cdot m^{-s}\right|+$$

$$\left|\sum_{m=M+1}^{\infty}(-1)^{m+1}\log m\cdot m^{-s}\right|.$$

(5) Fix $\varepsilon>0$. To prove that $\tilde\zeta(s)$ is differentiable we must show that there is a δ, $0<\delta<s-s_0$, such that (16) is less than ε for all t with $|s-t|<\delta$. Show first that there is $M>0$ such that the first and third terms on the right-hand side of (16) are bounded by $\frac{\varepsilon}{3}$ for all $t>s_0$.

(6) With M as above, show that there is a δ, $0<\delta<s-s_0$, such that the second term on the right-hand side of (16) bounded by $\frac{\varepsilon}{3}$ for all t with $|s-t|<\delta$.

Exercise 4.7. Show that the extended Legendre symbol $\left(\frac{\cdot}{p}\right)$ agrees with the usual Legendre symbol for p an odd prime.

Exercise 4.8. Let n be a squarefree positive integer.

(1) Let m be a positive integer; if $n\equiv 1,2\pmod 4$, assume also that m is odd. Prove that:

$$\left(\frac{-n}{m}\right)=\begin{cases}(-1)^{(m-1)/2}\left(\frac{m}{n}\right) & n\equiv 1\pmod 4;\\ \left(\frac{m}{n}\right) & n\equiv 3\pmod 4;\\ (-1)^{(m^2+4m-5)/8}\left(\frac{m}{n/2}\right) & n\equiv 2\pmod 8;\\ (-1)^{(m^2-1)/8}\left(\frac{m}{n/2}\right) & n\equiv 6\pmod 8;\end{cases}$$

with $\left(\frac{m}{n}\right)$ and $\left(\frac{m}{n/2}\right)$ the usual Jacobi symbol.

(2) Conclude that in any case $\left(\frac{n}{\cdot}\right)$ is periodic modulo $4n$:

$$m\equiv m'\pmod{4n}\quad\Rightarrow\quad\left(\frac{-n}{m}\right)=\left(\frac{-n}{m'}\right).$$

Exercise 4.9. Let n be a squarefree positive integer. Show that there exists a positive integer m, relatively prime to $4n$, such that $\left(\frac{-n}{m}\right)=-1$.

CHAPTER 5

The Dedekind zeta function

1. Ideals of fixed norm

Fix a squarefree positive integer n. For $m \geq 1$ let a_m denote the number of ideals of $\mathcal{O}_{-n}$ of norm m. For example, by Proposition 2.19 for a prime p we have

$$a_p = \begin{cases} 2 & \left(\frac{-n}{p}\right) = 1 \\ 1 & \left(\frac{-n}{p}\right) = 0 \\ 0 & \left(\frac{-n}{p}\right) = -1. \end{cases}$$

The basic facts about these numbers are given in the next lemma.

Lemma 5.1.

(1) *The sequence $a_1, a_2, \ldots$ is multiplicative.*
(2) *For a prime p*

$$\sum_{j=0}^{\infty} a_{p^j} p^{-js} = \begin{cases} (1-p^{-s})^{-2} & \left(\frac{-n}{p}\right) = 1 \\ (1-p^{-s})^{-1} & \left(\frac{-n}{p}\right) = 0 \\ (1-p^{-2s})^{-1} & \left(\frac{-n}{p}\right) = -1 \end{cases}$$

for $s > 1$.

Proof.

(1) Let m, m' be relatively prime. Consider the map

$$\{\text{ideals of norm } m\} \times \{\text{ideals of norm } m'\} \to \{\text{ideals of norm } mm'\}$$

sending a pair (I, I') to the product $I \cdot I'$. It follows from the unique factorization of ideals in $\mathcal{O}_{-n}$ that this map is bijective: indeed, any ideal of norm mm' can be uniquely factored as a product of an ideal of norm m and an ideal of norm m' by simply grouping together its prime ideal factors of norm dividing m and m', respectively. Thus $a_m a_{m'} = a_{mm'}$, as claimed.

(2) Suppose first that $\left(\frac{-n}{p}\right) = 1$ and let I, J be the two prime ideals of norm p. Then the ideals of norm p^j are exactly $I^i J^{j-i}$ for $i = 0, \ldots, j$; thus $a_{p^j} = j + 1$. The lemma in this case now follows from Exercise 5.1.

The proofs in the other two cases are entirely similar, using that $a_{p^j} = 1$ for all $j \geq 0$ if $\left(\frac{-n}{p}\right) = 0$, while

$$a_{p^j} = \begin{cases} 1 & j \text{ even} \\ 0 & j \text{ odd} \end{cases}$$

if $\left(\frac{-n}{p}\right) = -1$.

$\square$

2. Ideals of bounded norm

We wish to use the sequence $a_1, a_2, \ldots$ defined above to define a Dirichlet series. In order to understand the convergence of this series, we must find a bound on the sums

$$A_m := \sum_{m=1}^{M} a_m$$

for $M \geq 1$. In this section we use lattices and the finiteness of the ideal class group to obtain such a bound.

Let us first set some notation. Let w denote the number of units in $\mathcal{O}_{-n}$, so that $w = 2$ unless $n = 1, 3$. Let h denote the class number of $\mathcal{O}_{-n}$. For an ideal class $\mathcal{C}$ define $a_m(\mathcal{C})$ to the the number of ideals I in the class $\mathcal{C}$ which have norm m; thus

$$a_m = \sum_{\mathcal{C} \in \mathcal{C}l(-n)} a_m(\mathcal{C}).$$

Define $A_m(\mathcal{C}) = \sum_{m=1}^{M} a_m(\mathcal{C})$. We will bound A_m by bounding $A_m(\mathcal{C})$ for each $\mathcal{C} \in \mathcal{C}l(-n)$.

Let us begin with the class $\mathcal{C}_1$ of principal ideals. A principal ideal I of norm m is generated by an element α of $\mathcal{O}_{-n}$ of norm m. How many generators does I have? Well, if

$$I = (\alpha) = (\alpha'),$$

then $\alpha \mid \alpha'$ and $\alpha' \mid \alpha$, so that α and α' are associates. Any element of $\mathcal{O}_{-n}$ has exactly w associates, so that

$$a_m(\mathcal{C}_1) = \frac{1}{w} \cdot b_m$$

where b_m denotes the number of elements of $\mathcal{O}_{-n}$ of norm m.

We now estimate $B_M := \sum_{m=1}^{M} b_m$ by viewing $\mathcal{O}_{-n}$ as a complex lattice with lattice basis $1, \varpi_{-n}$. Since $\mathrm{N}(\alpha) = |\alpha|^2$ for $\alpha \in \mathcal{O}_{-n}$, we have

$$\begin{aligned} B_M &= \{\alpha \in \mathcal{O}_{-n}\,;\, \mathrm{N}(\alpha) \leq M\} \\ &= \{\alpha \in \mathcal{O}_{-n}\,;\, |\alpha| \leq \sqrt{M}\}. \end{aligned}$$

As the parallelogram with vertices $0, 1, \varpi_{-n}, 1 + \varpi_{-n}$ has area

$$A = \begin{cases} \sqrt{n} & n \equiv 1, 2 \pmod 4 \\ \frac{\sqrt{n}}{2} & n \equiv 3 \pmod 4, \end{cases}$$

Lemma 1.19 shows that there is a constant C_1' such that

$$\left| B_M - \frac{\pi}{A} M \right| \leq C_1' \cdot \sqrt{M}$$

for all $M \geq 1$. In particular,

$$\left| A_m(\mathcal{C}_1) - \frac{\pi}{Aw} M \right| \leq C_1 \cdot \sqrt{M}$$

with $C_1 = C_1'/w$. That is, $A_m(\mathcal{C}_1)$ is approximately $\frac{\pi}{Aw}M$ with an error bounded by a constant times $\sqrt{M}$. Remarkably, the same estimate holds for arbitrary ideal classes.

PROPOSITION 5.2. *There is a constant C' such that*

$$\left|A_M(\mathcal{C}) - \frac{\pi}{Aw}M\right| \leq C' \cdot \sqrt{M}$$

for all $M \geq 1$ and for any ideal class $\mathcal{C}$.

PROOF. Let $\frac{a+\sqrt{-n}}{b}$ be the j-invariant of the inverse ideal class $\mathcal{C}^{-1}$ as in Theorem 1.12 or Exercise 1.5. Let J denote the ideal $(b, a+\sqrt{-n})$ in the ideal class $\mathcal{C}^{-1}$. If I is an ideal in $\mathcal{C}$, then $I \cdot J$ is a principal ideal contained in J. In fact, since by Proposition 2.14 any ideal contained in J is divisible by J, the map

$$\begin{aligned} (17) \qquad \{I \in \mathcal{C}\,;\, \mathrm{N}(I) = m\} &\to \{I' \subseteq J\,;\, I' \text{ principal and } \mathrm{N}(I') = m\,\mathrm{N}(J)\} \\ I &\mapsto I \cdot J \end{aligned}$$

is a bijection.

Let $b_m(J)$ denote the number of elements of J of norm $m \cdot \mathrm{N}(J)$; thus by (17) we have

$$a_m(\mathcal{C}) = \frac{1}{w} \cdot b_m(J).$$

Let $B_M(J) = \sum_{m=1}^{M} b_m(J)$. Every element of J has norm divisible by $\mathrm{N}(J)$, so that in fact

$$\begin{aligned} B_M(J) &= \#\{\alpha \in K\,;\, \mathrm{N}(\alpha) \leq M \cdot \mathrm{N}(J)\} \\ &= \#\{\alpha \in K\,;\, |\alpha| \leq \sqrt{M \cdot \mathrm{N}(J)}\}. \end{aligned}$$

Since the parallelogram with vertices $0, b, a+\sqrt{-n}, a+b+\sqrt{-n}$ has area $b\sqrt{n}$, by Lemma 1.19 there is a constant C_J' such that

$$\left|B_M(J) - \frac{\pi}{b\sqrt{n}}M \cdot \mathrm{N}(J)\right| \leq C_J'\sqrt{\mathrm{N}(J)} \cdot \sqrt{M}$$

for all $M \geq 1$. By Exercise 3.6 we have

$$A = \frac{b\sqrt{n}}{\mathrm{N}(J)}$$

(with A the area of the fundamental parallelogram of $\mathcal{O}_{-n}$, as before) so that

$$\left|A_M(\mathcal{C}) - \frac{\pi}{Aw}M\right| \leq C_{\mathcal{C}} \cdot \sqrt{M}$$

with

$$C_{\mathcal{C}} = \frac{1}{w}C_J'\sqrt{\mathrm{N}(J)}.$$

Taking C' to be the largest of the constants $\mathbf{C}_{\mathcal{C}}$ as $\mathcal{C}$ runs through the finitely many ideal classes of $\mathcal{O}_{-n}$ proves the proposition. □

Summing over all ideal classes of $\mathcal{O}_{-n}$ we obtain the following result.

COROLLARY 5.3. *There is a constant C such that*

$$\left|A_M - \frac{h\pi}{Aw}M\right| \leq C \cdot \sqrt{M}$$

for all $M \geq 1$.

3. The Dedekind zeta function

We continue with the notation of the previous section. We define the *Dedekind zeta function* of $\mathcal{O}_{-n}$ as the Dirichlet series

$$\zeta_{-n}(s) = \sum_{m=1}^{\infty} a_m m^{-s}.$$

The basic facts about $\zeta_{-n}(s)$ are in the next result.

Proposition 5.4. *The Dedekind zeta function converges for $s > 1$ and has the Euler product*

$$\zeta_{-n}(s) = \prod_{p,\left(\frac{-n}{p}\right)=1} \left(1-p^{-s}\right)^{-2} \cdot \prod_{p,\left(\frac{-n}{p}\right)=0} \left(1-p^{-s}\right)^{-1} \cdot \prod_{p,\left(\frac{-n}{p}\right)=-1} \left(1-p^{-2s}\right)^{-1}$$

for $s > 1$. It has a simple pole at $s = 1$ with residue

$$\frac{h\pi}{Aw}.$$

Proof. By Corollary 5.3 there is a constant C such that

$$\left| A_M - \frac{h\pi}{Aw} M \right| \leq C \cdot \sqrt{M}$$

for all $M \geq 1$. Thus

$$|A_M| \leq \left(\frac{h\pi}{Aw} + C \right) \cdot M$$

so that the Dirichlet series defining $\zeta_{-n}(s)$ converges for $s > 1$ by Proposition 4.2. The existence of the desired Euler product is immediate from Proposition 4.6 and Lemma 5.1.

To compute the residue at $s = 1$, define a Dirichlet series

$$f(s) = \sum_{m=1}^{\infty} \left(a_m - \frac{h\pi}{Aw} \right) m^{-s}.$$

Then

$$\left| \sum_{m=1}^{M} \left(a_m - \frac{h\pi}{Aw} \right) \right| = \left| A_M - \frac{h\pi}{Aw} M \right| \leq C\sqrt{M},$$

so that $f(s)$ converges for $s > \frac{1}{2}$. Furthermore, for $s > 1$ we have

$$\zeta_{-n}(s) = f(s) + \frac{h\pi}{Aw}\zeta(s)$$

with $\zeta(s)$ the Riemann zeta function. Since $f(s)$ is defined at $s = 1$, it follows that

$$\lim_{s \to 1^+} \zeta_{-n}(s) = f(1) + \frac{h\pi}{Aw} \cdot \lim_{s \to 1^+} \zeta(s) = \infty.$$

Furthermore,

$$\begin{aligned} \lim_{s \to 1^+} (s-1)\zeta_{-n}(s) &= \lim_{s \to 1^+} (s-1) f(s) + \frac{h\pi}{Aw} \cdot \lim_{s \to 1^+} (s-1)\zeta(s) \\ &= (1-1)f(1) + \frac{h\pi}{Aw} \cdot \lim_{s \to 1^+} (s-1)\zeta(s) \\ &= \frac{h\pi}{Aw} \end{aligned}$$

by Proposition 4.4. □

4. The class number formula

The last result needed for the class number formula is a factorization of the Dedekind zeta function.

Proposition 5.5. *For $s > 1$*

$$\zeta_{-n}(s) = \zeta(s) \cdot L_{-n}(s).$$

Proof. This is most easily done on the level of Euler factors. We have

$$\begin{aligned}
\zeta_{-n}(s) = &\prod_{p,\left(\frac{-n}{p}\right)=1} \left(1-p^{-s}\right)^{-2} \cdot \prod_{p,\left(\frac{-n}{p}\right)=0} \left(1-p^{-s}\right)^{-1} \cdot \prod_{p,\left(\frac{-n}{p}\right)=-1} \left(1-p^{-2s}\right)^{-1} \\
&= \prod_{p,\left(\frac{-n}{p}\right)=1} \left(1-p^{-s}\right)^{-2} \cdot \prod_{p,\left(\frac{-n}{p}\right)=0} \left(1-p^{-s}\right)^{-1} \\
&\quad \cdot \prod_{p,\left(\frac{-n}{p}\right)=-1} \left(1-p^{-s}\right)^{-1}\left(1+p^{-s}\right)^{-1} \\
&= \prod_{p} \left(1-p^{-s}\right)^{-1} \cdot \prod_{p} \left(1-\left(\frac{-n}{p}\right)p^{-s}\right)^{-1} \\
&= \zeta(s) \cdot L_{-n}(s).
\end{aligned}$$

□

Corollary 5.6. *Let n be a squarefree positive integer and let*

$$w_{-n} = \begin{cases} 2 & n \neq 1,3 \\ 4 & n = 1 \\ 6 & n = 3. \end{cases}$$

Let $h(-n)$ denote the class number of $\mathcal{O}_{-n}$. If $n \equiv 1, 2 \pmod 4$, then

$$L_{-n}(1) = \frac{h(-n)\pi}{\sqrt{n}w_{-n}}.$$

If $n \equiv 3 \pmod 4$, then

$$L_{-n}(1) = \frac{2h(-n)\pi}{\sqrt{n}w_{-n}}.$$

Proof. Since $L_{-n}(s)$ is continuous for $s > 0$, we have

$$\begin{aligned}
L_{-n}(1) &= \lim_{s\to 1^+} L_{-n}(s) \\
&= \lim_{s\to 1^+} \frac{\zeta_{-n}(s)}{\zeta(s)} \\
&= \lim_{s\to 1^+} \frac{(s-1)\zeta_{-n}(s)}{(s-1)\zeta(s)} \\
&= \frac{\lim_{s\to 1^+}(s-1)\zeta_{-n}(s)}{\lim_{s\to 1^+}(s-1)\zeta(s)} \\
&= \frac{h(-n)\pi/Aw_{-n}}{1}
\end{aligned}$$

with A either $\sqrt{n}$ or $\sqrt{n}/2$ depending on n modulo 4. □

Since

$$L_{-n}(1) = \sum_{m=1}^{\infty} \left(\frac{-n}{m}\right) \cdot \frac{1}{m}$$

this proves the class number formula in the form of the first lecture.

As an obvious but nonetheless important corollary, we have the following result, which will be used in Exercise 5.5 to prove that there exist infinitely many primes p for which $-n$ is a quadratic residue.

Corollary 5.7. *For any squarefree positive integer n we have $L_{-n}(1) > 0$.*

5. Exercises

Exercise 5.1. Fix an integer m. Show that the series

$$\sum_{j=0}^{\infty} (j+1) m^{-js}$$

converges to

$$(1 - m^{-s})^{-2}$$

for $s > 0$. (Hint: Treat the sum as a power series in m^{-s}.)

Exercise 5.2. Let n be a squarefree positive integer and let a_m denote the number of ideals of $\mathcal{O}_{-n}$ of norm m. Show that

$$a_m = \sum_{d|m} \left(\frac{-n}{d}\right)$$

where the sum is over the positive divisors of m.

Exercise 5.3. Use Exercise 5.2 to give a proof of Proposition 5.5 without using Euler products.

Exercise 5.4. Mimic Exercise 4.3 to show that

$$\log L_{-n}(s) = \sum_{p} \left(\frac{-n}{p}\right) p^{-s} + \sum_{p} \sum_{j=2}^{\infty} \frac{1}{j} \left(\frac{-n}{p}\right) p^{-js}$$

for $s > 1$ with $L_{-n}(s) > 0$. Use Corollary 5.7 and Exercise 4.2 to conclude that

$$\lim_{s \to 1^+} \sum_{p} \left(\frac{-n}{p}\right) p^{-s}$$

exists.

Exercise 5.5.

(1) Show that

$$\sum_{p, \left(\frac{-n}{p}\right)=1} p^{-s} + \frac{1}{2} \cdot \sum_{p, \left(\frac{-n}{p}\right)=0} p^{-s} = \frac{1}{2} \cdot \left(\sum_{p} p^{-s} + \sum_{p} \left(\frac{-n}{p}\right) p^{-s} \right)$$

for $s > 1$.

(2) Use Exercises 4.3 and 5.4 to conclude that

$$\lim_{s \to 1^+} \sum_{p, \left(\frac{-n}{p}\right)=1} p^{-s} = \infty.$$

(3) Explain why this implies that there are infinitely many primes p with $\left(\frac{-n}{p}\right) = 1$.

(4) Modify this argument to show that there are infinitely many primes p with $\left(\frac{-n}{p}\right) = -1$.

Bibliography

[1] Michael Artin, *Algebra*, Prentice Hall, New Jersey, 1991.
[2] Daniel Marcus, *Number fields*, Springer-Verlag, New York, 1977.
[3] Walter Rudin, *Principles of mathematical analysis*, McGraw Hill, New York, 1976.
[4] Jean-Pierre Serre, *A course in arithmetic*, Springer-Verlag, New York, 1973.