CHAPTER 13

Quadratic Number Fields

Rien n'est beau que le vrai.

—Hermann Minkowski

In this chapter, we see how ideals substitute for elements in some interesting rings. We will use various facts about plane lattices, and in order not to break up the discussion, we have collected them together in Section 13.10 at the end of the chapter.

13.1 ALGEBRAIC INTEGERS

A complex number α that is the root of a polynomial with rational coefficients is called an *algebraic number*. The kernel of the substitution homomorphism $\varphi: \mathbb{Q}[x] \to \mathbb{C}$ that sends x to an algebraic number α is a principal ideal, as are all ideals of $\mathbb{Q}[x]$. It is generated by the monic polynomial of lowest degree in $\mathbb{Q}[x]$ that has α as a root. If α is a root of a product gh of polynomials, then it is a root of one of the factors. So the monic polynomial of lowest degree with root α is irreducible. We call this polynomial the *irreducible polynomial* for α over $\mathbb{Q}$.

• An algebraic number is an *algebraic integer* if its (monic) irreducible polynomial over $\mathbb{Q}$ has integer coefficients.

The cube root of unity $\omega = e^{2\pi i/3} = \frac{1}{2}(-1 + \sqrt{-3})$ is an algebraic integer because its irreducible polynomial over $\mathbb{Q}$ is $x^2 + x + 1$, while $\alpha = \frac{1}{2}(-1 + \sqrt{3})$ is a root of the irreducible polynomial $x^2 - x - \frac{1}{2}$ and is not an algebraic integer.

Lemma 13.1.1 A rational number is an algebraic integer if and only if it is an ordinary integer.

This is true because the irreducible polynomial over $\mathbb{Q}$ for a rational number a is $x - a$. □

A *quadratic number field* is a field of the form $\mathbb{Q}[\sqrt{d}]$, where d is a fixed integer, positive or negative, which is not a square in $\mathbb{Q}$. Its elements are the complex numbers

$$a + b\sqrt{d}, \quad \text{with } a \text{ and } b \text{ in } \mathbb{Q}, \tag{13.1.2}$$

The notation $\sqrt{d}$ stands for the positive real square root if $d > 0$ and for the positive imaginary square root if $d < 0$. The field $\mathbb{Q}[\sqrt{d}]$ is a *real quadratic number field* if $d > 0$, and an *imaginary quadratic number field* if $d < 0$.

If d has a square integer factor, we can pull it out of the radical without changing the field. So we assume *d square-free*. Then d can be any one of the integers

$$d = -1, \pm 2, \pm 3, \pm 5, \pm 6, \pm 7, \pm 10, \ldots$$

We determine the algebraic integers in a quadratic number field $\mathbb{Q}[\sqrt{d}]$ now. Let δ denote $\sqrt{d}$, let $\alpha = a + b\delta$ be an element of $\mathbb{Q}[\delta]$ that is not in $\mathbb{Q}$, that is, with $b \neq 0$, and let $\alpha' = a - b\delta$. Then α and α' are roots of the polynomial

$$(x - \alpha')(x - \alpha) = x^2 - 2ax + (a^2 - b^2 d), \tag{13.1.3}$$

which has rational coefficients. Since α is not a rational number, it is not the root of a linear polynomial. So this quadratic polynomial is irreducible over $\mathbb{Q}$. It is therefore the irreducible polynomial for α over $\mathbb{Q}$.

Corollary 13.1.4 A complex number $\alpha = a + b\delta$ with a and b in $\mathbb{Q}$ is an algebraic integer if and only if $2a$ and $a^2 - b^2 d$ are ordinary integers. □

This corollary is also true when $b = 0$ and $\alpha = a$.

The possibilities for a and b depend on congruence modulo 4. Since d is assumed to be square free, we can't have $d \equiv 0$, so $d \equiv 1, 2$, or 3 modulo 4.

Lemma 13.1.5 Let d be a square-free integer, and let r be a rational number. If $r^2 d$ is an integer, then r is an integer.

Proof. The square-free integer d cannot cancel a square in the denominator of r^2. □

A *half integer* is a rational number of the form $m + \frac{1}{2}$, where m is an integer.

Proposition 13.1.6 The algebraic integers in the quadratic field $\mathbb{Q}[\delta]$, with $\delta^2 = d$ and d square free, have the form $\alpha = a + b\delta$, where:

- If $d \equiv 2$ or 3 modulo 4, then a and b are integers.
- If $d \equiv 1$ modulo 4, then a and b are either both integers, or both half integers.

The algebraic integers form a ring R, the *ring of integers* in F.

Proof. We assume that $2a$ and $a^2 - b^2 d$ are integers, and we analyze the possiblities for a and b. There are two cases: Either a is an integer, or a is a half integer.

Case 1: a is an integer. Then $b^2 d$ must be an integer. The lemma shows that b is an integer.

Case 2: $a = m + \frac{1}{2}$ is a half integer. Then $a^2 = m^2 + m + \frac{1}{4}$ will be in the set $\mathbb{Z} + \frac{1}{4}$. Since $a^2 - b^2 d$ is an integer, $b^2 d$ is also in $\mathbb{Z} + \frac{1}{4}$. Then $4b^2 d$ is an integer and the lemma shows that $2b$ is an integer. So b is a half integer, and then $b^2 d$ is in the set $\mathbb{Z} + \frac{1}{4}$ if and only if $d \equiv 1$ modulo 4.

The fact that the algebraic integers form a ring is proved by computation. □

The imaginary quadratic case $d < 0$ is easier to handle than the real case, so we concentrate on it in the next sections. When $d < 0$, the algebraic integers form a lattice in the complex plane. The lattice is rectangular if $d \equiv 2$ or 3 modulo 4, and "isosceles triangular" if $d \equiv 1$ modulo 4.

When $d = -1$, R is the ring of Gauss integers, and the lattice is square. When $d = -3$, the lattice is equilateral triangular. Two other examples are shown below.

$d = -5$ $d = -7$

(13.1.7) Integers in Some Imaginary Quadratic Fields.

Being a lattice is a very special property of the rings that we consider here, and the geometry of the lattices helps to analyze them.

When $d \equiv 2$ or 3 modulo 4, the integers in $\mathbb{Q}[\delta]$ are the complex numbers $a + b\delta$, with a and b integers. They form a ring that we denote by $\mathbb{Z}[\delta]$. A convenient way to write all the integers when $d \equiv 1$ modulo 4 is to introduce the algebraic integer

$$\eta = \tfrac{1}{2}(1 + \delta). \tag{13.1.8}$$

It is a root of the monic integer polynomial

$$x^2 - x + h, \tag{13.1.9}$$

where $h = (1 - d)/4$. The algebraic integers in $\mathbb{Q}[\delta]$ are the complex numbers $a + b\eta$, with a and b integers. The ring of integers is $\mathbb{Z}[\eta]$.

13.2 FACTORING ALGEBRAIC INTEGERS

The symbol R will denote the ring of integers in an imaginary quadratic number field $\mathbb{Q}[\delta]$. To focus your attention, it may be best to think at first of the case that d is congruent 2 or 3 modulo 4, so that the algebraic integers have the form $a + b\delta$, with a and b integers.

When possible, we denote ordinary integers by Latin letters $a, b, \ldots$, elements of R by Greek letters $\alpha, \beta, \ldots$, and ideals by capital letters $A, B, \ldots$ We work exclusively with nonzero ideals.

If $\alpha = a + b\delta$ is in R, its complex conjugate $\overline{\alpha} = a - b\delta$ is in R too. These are the roots of the polynomial $x^2 - 2ax + (a^2 - b^2d)$ that was introduced in Section 13.1.

- The *norm* of $\alpha = a + b\delta$ is $N(\alpha) = \overline{\alpha}\alpha$.

The norm is equal to $|\alpha|^2$ and also to $a^2 - b^2d$. It is a positive integer for all $\alpha \neq 0$, and it has the multiplicative property:

$$N(\beta\gamma) = N(\beta)N(\gamma). \tag{13.2.1}$$

This property gives us some control of the factors of an element. If $\alpha = \beta\gamma$, then both terms on the right side of (13.2.1) are positive integers. To check for factors of α, it is enough to look at elements β whose norms divide the norm of α. This is manageable when $N(\alpha)$ is small. For one thing, it allows us to determine the units of R.

Proposition 13.2.2 Let R be the ring of integers in an imaginary quadratic number field.

- An element α of R is a unit if and only if $N(\alpha) = 1$. If so, then $\alpha^{-1} = \overline{\alpha}$.
- The units of R are $\{\pm 1\}$ unless $d = -1$ or -3.
- When $d = -1$, R is the ring of Gauss integers, and the units are the four powers of i.
- When $d = -3$, the units are the six powers of $e^{2\pi i/6} = \frac{1}{2}(1 + \sqrt{-3})$.

Proof. If α is a unit, then $N(\alpha)N(\alpha^{-1}) = N(1) = 1$. Since $N(\alpha)$ and $N(\alpha^{-1})$ are positive integers, they are both equal to 1. Conversely, if $N(\alpha) = \overline{\alpha}\alpha = 1$, then $\overline{\alpha}$ is the inverse of α, so α is a unit. The remaining assertions follow by inspection of the lattice R. □

Corollary 13.2.3 Factoring terminates in the ring of integers in an imaginary quadratic number field.

This follows from the fact that factoring terminates in the integers. If $\alpha = \beta\gamma$ is a proper factorization in R, then $N(\alpha) = N(\beta)N(\gamma)$ is a proper factorization in $\mathbb{Z}$. □

Proposition 13.2.4 Let R be the ring of integers in an imaginary quadratic number field. Assume that $d \equiv 3$ modulo 4. Then R is not a unique factorization domain except in the case $d = -1$, when R is the ring of Gauss integers.

Proof. This is analogous to what happens when $d = -5$. Suppose that $d \equiv 3$ modulo 4 and that $d < -1$. The integers in R have the form $a + b\delta$ which $a, b \in \mathbb{Z}$, and the units are ± 1. Let $e = (1 - d)/2$. Then

$$2e = 1 - d = (1 + \delta)(1 - \delta).$$

The element $1 - d$ factors in two ways in R. Since $d < -1$, there is no element $a + b\delta$ whose norm is equal to 2. Therefore 2, which has norm 4, is an irreducible element of R. If R were a unique factorization domain, 2 would divide either $1 + \delta$ or $1 - \delta$ in R, which it does not: $\frac{1}{2}(1 \pm \delta)$ is not an element of R when $d \equiv 3$ modulo 4. □

There is a similar statement for the case $d \equiv 2$ modulo 4. (This is Exercise 2.2.) But note that the reasoning breaks down when $d \equiv 1$ modulo 4. In that case, $\frac{1}{2}(1+\delta)$ is in R, and in fact there are more cases of unique factorization when $d \equiv 1$ modulo 4. A famous theorem enumerates these cases:

Theorem 13.2.5 The ring of integers R in the imaginary quadratic field $\mathbb{Q}[\sqrt{d}]$ is a unique factorization domain if and only if d is one of the integers $-1, -2, -3, -7, -11, -19, -43, -67, -163$.

Gauss proved that for these values of d, R has unique factorization. We will learn how to do this. He also conjectured that there were no others. This much more difficult part of the theorem was finally proved by Baker, Heegner, and Stark in the middle of the 20th century, after people had worked on it for more than 150 years. We won't be able to prove their theorem.

13.3 IDEALS IN $\mathbb{Z}[\sqrt{-5}]$

Before going to the general theory, we describe the ideals in the ring $R = \mathbb{Z}[\sqrt{-5}]$ as lattices in the complex plane, using an ad hoc method.

Proposition 13.3.1 Let R be the ring of integers in an imaginary quadratic number field. Every nonzero ideal of R is a sublattice of the lattice R. Moreover,

- If $d \equiv 2$ or 3 modulo 4, a sublattice A is an ideal if and only if $\delta A \subset A$.
- If $d \equiv 1$ modulo 4, a sublattice A is an ideal if and only if $\eta A \subset A$ (see (13.1.8)).

Proof. A nonzero ideal A contains a nonzero element α, and $(\alpha, \alpha\delta)$ is an independent set over $\mathbb{R}$. Also, A is discrete because it is a subgroup of the lattice R. Therefore A is a lattice (Theorem 6.5.5).

To be an ideal, a subset of R must be closed under addition and under multiplication by elements of R. Every sublattice A is closed under addition and multiplication by integers. If A is also closed under multiplication by δ, then it is closed under multiplication by an element of the form $a + b\delta$, with a and b integers. This includes all elements of R if $d \equiv 2$ or 3 modulo 4. So A is an ideal. The proof in the case $d \equiv 1$ modulo 4 is similar. □

We describe ideals in the ring $R = \mathbb{Z}[\delta]$, when $\delta^2 = -5$.

Lemma 13.3.2 Let $R = \mathbb{Q}[\delta]$ with $\delta^2 = -5$. The lattice A of integer combinations of 2 and $1 + \delta$ is an ideal.

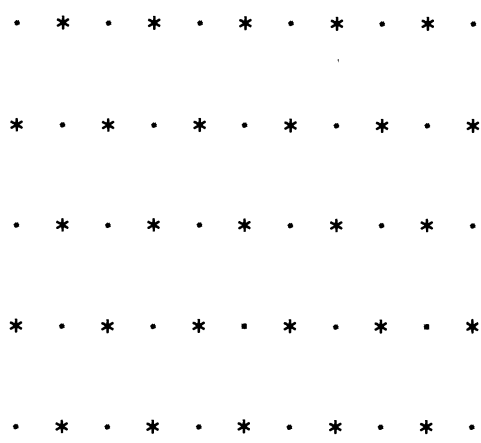
Proof. The lattice A is closed under multiplication by δ, because $\delta \cdot 2$ and $\delta \cdot (1+\delta)$ are integer combinations of 2 and $1 + \delta$. □

Figure 13.3.4 shows this ideal.

Theorem 13.3.3 Let $R = \mathbb{Z}[\delta]$, where $\delta = \sqrt{-5}$, and let A be a nonzero ideal of R. Let α be a nonzero element of A of minimal norm (or minimal absolute value). Then either

- The set $(\alpha, \alpha\delta)$ is a lattice basis for A, and A is the principal ideal (α), or
- The set $(\alpha, \frac{1}{2}(\alpha + \alpha\delta))$ is a lattice basis for A, and A is not a principal ideal.

This theorem has the following geometric interpretation: The lattice basis $(\alpha, \alpha\delta)$ of the principal ideal (α) is obtained from the lattice basis $(1, \delta)$ of the unit ideal R by multiplying by α. If we write α in polar coordinates $\alpha = re^{i\theta}$, then multiplication by α rotates the complex plane through the angle θ and stretches by the factor r. So all principal ideals are similar geometric figures. Also, the lattice with basis $(\alpha, \frac{1}{2}(\alpha + \alpha\delta))$ is obtained from the lattice $(2, 1 + \delta)$ by multiplying by $\frac{1}{2}\alpha$. All ideals of the second type are geometric figures similar to the one shown below (see also Figure 13.7.4).



(13.3.4) The Ideal $(2, 1 + \delta)$ in the Ring $\mathbb{Z}[\sqrt{-5}]$.

Similarity classes of ideals are called *ideal classes*, and the number of ideal classes is the *class number* of R. The theorem asserts that the class number of $\mathbb{Z}[\sqrt{-5}]$ is two. Ideal classes for other quadratic imaginary fields are discussed in Section 13.7.

Theorem 13.3.3 is based on the following simple lemma about lattices:

Lemma 13.3.5 Let A be a lattice in the complex plane, let r be the minimum absolute value among nonzero elements of A, and let γ be an element of A. Let n be a positive integer. The interior of the disk of radius $\frac{1}{n}r$ about the point $\frac{1}{n}\gamma$ contains no element of A other than the center $\frac{1}{n}\gamma$. The center may lie in A or not.

Proof. If β is an element of A in the interior of the disk, then $|\beta - \frac{1}{n}\gamma| < \frac{1}{n}r$, which is to say, $|n\beta - \gamma| < r$. Moreover, $n\beta - \gamma$ is in A. Since this is an element of absolute value less than the minimum, $n\beta - \gamma = 0$. Then $\beta = \frac{1}{n}\gamma$ is the center of the disk. □

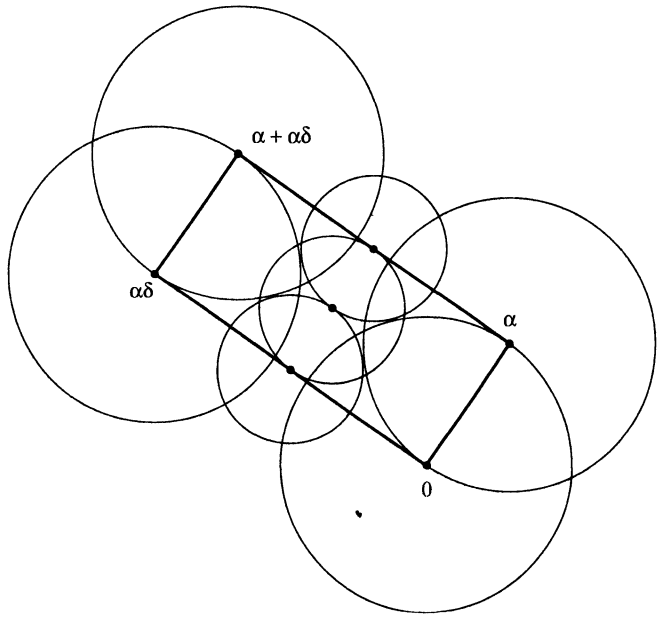
Proof of Theorem 13.3.3. Let α be a nonzero element of an ideal A of minimal absolute value r. Since A contains α, it contains the principal ideal (α), and if $A = (\alpha)$ we are in the first case.

Suppose that A contains an element β not in the principal ideal (α). The ideal (α) has the lattice basis $\mathbf{B} = (\alpha, \alpha\delta)$, so we may choose β to lie in the parallelogram $\Pi(\mathbf{B})$ of linear combinations $r\alpha + s\alpha\delta$ with $0 \leq r, s \leq 1$. (In fact, we can choose β so that $0 \leq r, s < 1$. See Lemma 13.10.2.) Because δ is purely imaginary, the parallelogram is a rectangle. How large

the rectangle is, and how it is situated in the plane, depend on α, but the ratio of the side lengths is always 1: $\sqrt{5}$. We'll be done if we show that β is the midpoint $\frac{1}{2}(\alpha + \alpha\delta)$ of the rectangle.

Figure 13.3.6 shows disks of radius r about the four vertices of such a rectangle, and also disks of radius $\frac{1}{2}r$ about three half lattice points, $\frac{1}{2}\alpha\delta$, $\frac{1}{2}(\alpha + \alpha\delta)$, and $\alpha + \frac{1}{2}\alpha\delta$. Notice that the interiors of these seven disks cover the rectangle. (It would be fussy to check this by algebra. Let's not bother. A glance at the figure makes it clear enough.)

According to Lemma 13.3.5, the only points of the interiors of the disks that can be elements of A are their centers. Since β is not in the principal ideal (α), it is not a vertex of the rectangle. So β must be one of the three half lattice points. If $\beta = \alpha + \frac{1}{2}\alpha\delta$, then since α is in A, $\frac{1}{2}\alpha\delta$ will be in A too. So we have only two cases to consider: $\beta = \frac{1}{2}\alpha\delta$ and $\beta = \frac{1}{2}(\alpha + \alpha\delta)$.



This exhausts the information we can get from the fact that A is a lattice. We now use the fact that A is an ideal. Suppose that $\frac{1}{2}\alpha\delta$ is in A. Multiplying by δ shows that $\frac{1}{2}\alpha\delta^2 = -\frac{5}{2}\alpha$ is in A. Then since α is in A, $\frac{1}{2}\alpha$ is in A too. This contradicts our choice of α as a nonzero element of minimal absolute value. So β cannot be equal to $\frac{1}{2}\alpha\delta$. The remaining possibility is that β is the center $\frac{1}{2}(\alpha + \alpha\delta)$ of the rectangle. If so, we are in the second case of the theorem. □

13.4 IDEAL MULTIPLICATION

Let R be the ring of integers in an imaginary quadratic number field. As usual, the notation $A = (\alpha, \beta, \ldots, \gamma)$ means that A is the the ideal of R generated by the elements $\alpha, \beta, \ldots, \gamma$. It consists of all linear combinations of those elements, with coefficients in the ring.

Since a nonzero ideal A is a lattice, it has a lattice basis (α, β) consisting of two elements. Every element of A is an *integer* combination of α and β. We must be careful to distinguish between the concepts of a lattice basis and a generating set for an ideal. Any lattice basis generates the ideal, but the converse is false. For instance, a principal ideal is generated as an ideal by a single element, whereas a lattice basis has two elements.

Dedekind extended the notion of divisibility to ideals using the following definition of ideal multiplication:

- Let A and B be ideals in a ring R. The *product ideal* AB consists of all *finite sums of products*

$$\sum_i \alpha_i \beta_i, \text{ with } \alpha_i \text{ in } A \text{ and } \beta_i \text{ in } B. \tag{13.4.1}$$

This is the smallest ideal of R that contains all of the products $\alpha\beta$.

The definition of ideal multiplication may not be quite as simple as one might hope, but it works well. Notice that it is a commutative and associative law, and that it has a unit element, namely R. (This is one of the reasons that R is called the unit ideal.)

$$AB = BA, \quad A(BC) = (AB)C, \quad AR = RA = A. \tag{13.4.2}$$

We omit the proof of the next proposition, which is true for arbitrary rings.

Proposition 13.4.3 Let A and B be ideals of a ring $\mathcal{R}$.

(a) Let $\{\alpha_1, \ldots, \alpha_m\}$ and $\{\beta_1, \ldots, \beta_n\}$ be generators for the ideals A and B, respectively. The product ideal AB is generated as ideal by the mn products $\alpha_i\beta_j$: Every element of AB is a linear combination of these products with coefficients in the ring.

(b) The product of principal ideals is principal: If $A = (\alpha)$ and $B = (\beta)$, then AB is the principal ideal $(\alpha\beta)$ generated by the product $\alpha\beta$.

(c) Assume that $A = (\alpha)$ is a principal ideal and let B be arbitrary. Then AB is the set of products $\alpha\beta$ with β in B: $AB = \alpha B$. □

We go back to the example of the ring $R = \mathbb{Z}[\delta]$ with $\delta^2 = -5$, in which

$$2 \cdot 3 = 6 = (1 + \delta)(1 - \delta). \tag{13.4.4}$$

If factoring in R were unique, there would be an element γ in R dividing both 2 and $1 + \delta$, and then 2 and $1 + \delta$ would be in the principal ideal (γ). There is no such element. However, there is an *ideal* that contains 2 and $1 + \delta$, namely the ideal $(2, 1 + \delta)$ generated by these two elements, the one depicted in Figure 13.3.4.

We can make four ideals using the factors of 6:

$$A = (2, 1 + \delta), \quad \overline{A} = (2, 1 - \delta), \quad B = (3, 1 + \delta), \quad \overline{B} = (3, 1 - \delta). \tag{13.4.5}$$

In each of these ideals, the generators that are given happen to form lattice bases. We denote the last of them by $\overline{B}$ because it is the complex conjugate of B:

$$\overline{B} = \{\overline{\beta} \mid \beta \in B\}. \tag{13.4.6}$$

It is obtained by reflecting B about the real axis. The fact that $\overline{R} = R$ implies that the complex conjugate of an ideal is an ideal. The ideal $\overline{A}$, the complex conjugate of A, is equal to A. This accidental symmetry of the lattice A doesn't occur very often.

We now compute some product ideals. Proposition 13.4.3**(a)** tells us that the ideal $\overline{A}A$ is generated by the four products of the generators $(2, 1-\delta)$ and $(2, 1+\delta)$ of $\overline{A}$ and A:

$$\overline{A}A = (4, 2+2\delta, 2-2\delta, 6).$$

Each of the four generators is divisible by 2, so $\overline{A}A$ is contained in the principal ideal (2). (The notation (2) stands for the ideal $2R$ here.) On the other hand, 2 is an element of $\overline{A}A$ because $2 = 6 - 4$. Therefore $(2) \subset \overline{A}A$. This shows that $\overline{A}A = (2)$.

Next, the product AB is generated by four products:

$$AB = (6, 2+2\delta, 3+3\delta, (1+\delta)^2).$$

Each of these four elements is divisible by $1+\delta$, and $1+\delta$ is the difference of two of them, so it is an element of AB. Therefore AB is equal to the principal ideal $(1+\delta)$. One sees similarly that $\overline{A}\,\overline{B} = (1-\delta)$ and that $\overline{B}B = (3)$.

The principal ideal (6) is the product of four ideals:

$$(13.4.7) \qquad (6) = (2)(3) = (\overline{A}A)(\overline{B}B) = (\overline{A}\,\overline{B})(AB) = (1-\delta)(1+\delta)$$

Isn't this beautiful? The ideal factorization $(6) = \overline{A}A\overline{B}B$ has provided a common refinement of the two factorizations (13.4.4).

In the next section, we prove unique factorization of ideals in the ring of integers of any imaginary quadratic number field. The next lemma is the tool that we will need.

Lemma 13.4.8 Main Lemma. Let R be the ring of integers in an imaginary quadratic number field. The product of a nonzero ideal A of R and its conjugate $\overline{A}$ is a principal ideal, generated by a positive ordinary integer n: $\overline{A}A = (n) = nR$.

This lemma would be false for any ring smaller than R, for example, if one didn't include the elements with half integer coefficients, when $d \equiv 1$ modulo 4.

Proof. Let (α, β) be a lattice basis for the ideal A. Then $(\overline{\alpha}, \overline{\beta})$ is a lattice basis for $\overline{A}$. Moreover, $\overline{A}$ and A are generated as ideals by these bases, so the four products $\overline{\alpha}\alpha$, $\overline{\alpha}\beta$, $\overline{\beta}\alpha$, and $\overline{\beta}\beta$ generate the product ideal $\overline{A}A$. The three elements $\overline{\alpha}\alpha$, $\overline{\beta}\beta$, and $\overline{\beta}\alpha + \overline{\alpha}\beta$ are in $\overline{A}A$. They are algebraic integers equal to their complex conjugates, so they are rational numbers, and therefore ordinary integers (13.1.1). Let n be their greatest common divisor in the ring of integers. It is an integer combination of those elements, so it is also an element of $\overline{A}A$. Therefore $(n) \subset \overline{A}A$. If we show that n divides each of the four generators of $\overline{A}A$ in R, it will follow that $(n) = \overline{A}A$, and this will prove the lemma.

By construction, n divides $\overline{\alpha}\alpha$ and $\overline{\beta}\beta$ in $\mathbb{Z}$, hence in R. We have to show that n divides $\overline{\alpha}\beta$ and $\overline{\beta}\alpha$. How can we do this? There is a beautiful insight here. We use the definition of an algebraic integer. If we show that the quotients $\gamma = \overline{\alpha}\beta/n$ and $\overline{\gamma} = \overline{\beta}\alpha/n$ are algebraic integers, it will follow that they are elements of the ring of integers, which is R. This will mean that n divides $\overline{\alpha}\beta$ and $\overline{\beta}\alpha$ in R.

The elements γ and $\overline{\gamma}$ are roots of the polynomial $p(x) = x^2 - (\overline{\gamma} + \gamma)x + (\overline{\gamma}\gamma)$:

$$\overline{\gamma} + \gamma = \frac{\overline{\beta}\alpha + \overline{\alpha}\beta}{n}, \quad \text{and} \quad \overline{\gamma}\gamma = \frac{\overline{\beta}\alpha}{n}\frac{\overline{\alpha}\beta}{n} = \frac{\overline{\alpha}\alpha}{n}\frac{\overline{\beta}\beta}{n}.$$

By its definition, n divides each of the three integers $\overline{\beta}\alpha + \overline{\alpha}\beta$, $\overline{\alpha}\alpha$, and $\overline{\beta}\beta$. The coefficients of $p(x)$ are integers, so γ and $\overline{\gamma}$ are algebraic integers, as we hoped. (See Lemma 12.4.2 for the case that γ happens to be a rational number.) □

Our first applications of the Main Lemma are to divisibility of ideals. In analogy with divisibility of elements of a ring, we say that an ideal A *divides* another ideal B if there is an ideal C such that B is the product ideal AC.

Corollary 13.4.9 Let R be the ring of integers in an imaginary quadratic number field.

(a) *Cancellation Law*: Let A, B, C be nonzero ideals of R. Then $AB = AC$ if and only if $B = C$. Similarly, $AB \subset AC$, if and only if $B \subset C$, and $AB < AC$ if and only if $B < C$.

(b) Let A and B be nonzero ideals of R. Then $A \supset B$ if and only if A divides B, i.e., if and only if there is an ideal C such that $B = AC$.

Proof. **(a)** It is clear that if $B = C$, then $AB = AC$. If $AB = AC$, then $\overline{A}AB = \overline{A}AC$. By the Main Lemma, $\overline{A}A = (n)$, so $nB = nC$. Dividing by n shows that $B = C$. The other assertions are proved in the same way.

(b) We first consider the case that a principal ideal (n) generated by an ordinary integer n contains an ideal B. Then n divides every element of B in R. Let $C = n^{-1}B$ be the set of quotients, the set of elements $n^{-1}\beta$ with β in B. You can check that C is an ideal and that $nC = B$. Then B is the product ideal $(n)C$, so (n) divides B.

Now suppose that an ideal A contains B. We apply the Main Lemma again: $\overline{A}A = (n)$. Then $(n) = \overline{A}A$ contains $\overline{A}B$. By what has been shown, there is an ideal C such that $\overline{A}B = (n)C = \overline{A}AC$. By the Cancellation Law, $B = AC$.

Conversely, if A divides B, say $B = AC$, then $B = AC \subset AR = A$. □

13.5 FACTORING IDEALS

We show in this section that nonzero ideals in rings of integers in imaginary quadratic fields factor uniquely. This follows rather easily from the Main Lemma 13.4.8 and its Corollary 13.4.9, but before deriving it, we define the concept of a prime ideal. We do this to be consistent with standard terminology: the prime ideals that appear are simply the maximal ideals.

Proposition 13.5.1 Let $\mathcal{R}$ be a ring. The following conditions on an ideal $\mathcal{P}$ of $\mathcal{R}$ are equivalent. An ideal that satisfies these conditions is called a *prime ideal.*

(a) The quotient ring $\mathcal{R}/\mathcal{P}$ is an integral domain.

(b) $\mathcal{P} \neq \mathcal{R}$, and if a and b are elements of $\mathcal{R}$ such that $ab \in \mathcal{P}$, then $a \in \mathcal{P}$ or $b \in \mathcal{P}$.

(c) $\mathcal{P} \neq \mathcal{R}$, and if A and B are ideals of $\mathcal{R}$ such that $AB \subset \mathcal{P}$, then $A \subset \mathcal{P}$ or $B \subset \mathcal{P}$.

Condition **(b)** explains the term "prime." It mimics the important property of a prime integer, that if a prime p divides a product ab of integers, then p divides a or p divides b.

Proof. **(a)** $\Longleftrightarrow$ **(b)**: The conditions for $\mathcal{R}/\mathcal{P}$ to be an integral domain are that $\mathcal{R}/\mathcal{P} \neq \{0\}$ and $\overline{a}\,\overline{b} = 0$ implies $\overline{a} = 0$ or $\overline{b} = 0$. These conditions translate to $\mathcal{P} \neq \mathcal{R}$ and $ab \in \mathcal{P}$ implies $a \in \mathcal{P}$ or $b \in \mathcal{P}$.

(b) $\Rightarrow$ **(c)**: Suppose that $ab \in \mathcal{P}$ implies $a \in \mathcal{P}$ or $b \in \mathcal{P}$, and let A and B be ideals such that $AB \subset \mathcal{P}$. If $A \not\subset \mathcal{P}$, there is an element a in A that isn't in $\mathcal{P}$. Let b be any element of B. Then ab is in AB and therefore in $\mathcal{P}$. But a is not in $\mathcal{P}$, so b is in $\mathcal{P}$. Since b was an arbitrary element of B, $B \subset \mathcal{P}$.

(c) $\Rightarrow$ **(b)**: Suppose that $\mathcal{P}$ has the property **(c)**, and let a and b be elements of $\mathcal{R}$ such that ab is in $\mathcal{P}$. The principal ideal (ab) is the product ideal $(a)(b)$. If $ab \in \mathcal{P}$, then $(ab) \subset \mathcal{P}$, and so $(a) \subset \mathcal{P}$ or $(b) \subset \mathcal{P}$. This tells us that $a \in \mathcal{P}$ or $b \in \mathcal{P}$. □

Corollary 13.5.2 Let $\mathcal{R}$ be a ring.

(a) The zero ideal of $\mathcal{R}$ is a prime ideal if and only if $\mathcal{R}$ is an integral domain.

(b) A maximal ideal of $\mathcal{R}$ is a prime ideal.

(c) A principal ideal (α) is a prime ideal of $\mathcal{R}$ if and only if α is a prime element of $\mathcal{R}$.

Proof. **(a)** This follows from (13.5.1)**(a)**, because the quotient ring $\mathcal{R}/(0)$ is isomorphic to $\mathcal{R}$.

(b) This also follows from (13.5.1)**(a)**, because when $\mathcal{M}$ is a maximal ideal, $\mathcal{R}/\mathcal{M}$ is a field. A field is an integral domain, so $\mathcal{M}$ is a prime ideal. Finally, **(c)** restates (13.5.1)**(b)** for a principal ideal. □

This completes our discussion of prime ideals in arbitrary rings, and we go back to the ring of integers in an imaginary quadratic number field.

Corollary 13.5.3 Let R be the ring of integers in an imaginary quadratic number field, let A and B be ideals of R, and let P be a prime ideal of R that is not the zero ideal. If P divides the product ideal AB, then P divides one of the factors A or B.

This follows from (13.5.1)**(c)** when we use (13.4.9)**(b)** to translate inclusion into divisibility.□

Lemma 13.5.4 Let R be the ring of integers in an imaginary quadratic number field, and let B be a nonzero ideal of R. Then

(a) B has finite index in R,

(b) there are finitely many ideals of R that contain B,

(c) B is contained in a maximal ideal, and

(d) B is a prime ideal if and only if it is a maximal ideal.

Proof. **(a)** is Lemma 13.10.3**(d)**, and **(b)** follows from Corollary 13.10.5

(c) Among the finitely many ideals that contain B, there must be at least one that is maximal.

(d) Let P be a nonzero prime ideal. Then by **(a)**, P has finite index in R. So R/P is a finite integral domain. A finite integral domain is a field. (This is Chapter 11, Exercise 7.1.) Therefore P is a maximal ideal. The converse is (13.5.2)**(b)**. □

Theorem 13.5.5 Let R be the ring of integers in an imaginary quadratic field F. Every proper ideal of R is a product of prime ideals. The factorization of an ideal into prime ideals is unique except for the ordering of the factors.

Proof. If an ideal B is a maximal ideal, it is itself a prime ideal. Otherwise, there is an ideal A that properly contains B. Then A divides B, say $B = AC$. The cancellation law shows that C properly contains B too. We continue by factoring A and C. Since only finitely many ideals contain B, the process terminates, and when it does, all factors will be maximal and therefore prime.

If $P_1 \cdots P_r = Q_1 \cdots Q_s$, with P_i and Q_j prime, then P_1 divides $Q_1 \cdots Q_s$, and therefore P_1 divides one of the factors, say Q_1. Then P_1 contains Q_1, and since Q_1 is maximal, $P_1 = Q_1$. The uniqueness of factorization follows by induction when one cancels P_1 from both sides of the equation. □

Note: This theorem extends to rings of algebraic integers in other number fields, but it is a very special property. Most rings do not admit unique factorization of ideals. The reason is that in most rings, $P \supset B$ does not imply that P divides B, and then the analogy between prime ideals and prime elements is weaker. □

Theorem 13.5.6 The ring of integers R in an imaginary quadratic number field is a unique factorization domain if and only if it is a principal ideal domain, and this is true if and only if the class group C of R is the trivial group.

Proof. A principal ideal domain is a unique factorization domain (12.2.14). Conversely, suppose that R is a unique factorization domain. We must show that every ideal is principal. Since the product of principal ideals is principal and since every nonzero ideal is a product of prime ideals, it suffices to show that every nonzero prime ideal is principal.

Let P be a nonzero prime ideal of R, and let α be a nonzero element of P. Then α is a product of irreducible elements, and because R has unique factorization, they are prime elements (12.2.14). Since P is a prime ideal, P contains one of the prime factors of α, say π. Then P contains the principal ideal (π). But since π is a prime element, the principal ideal (π) is a nonzero prime ideal, and therefore a maximal ideal. Since P contains (π), $P = (\pi)$. So P is a principal ideal. □

13.6 PRIME IDEALS AND PRIME INTEGERS

In Section 12.5, we saw how Gauss primes are related to integer primes. A similar analysis can be made for the ring R of integers in a quadratic number field, but we should speak of prime ideals rather than of prime elements. This complicates the analogues of some parts of Theorem 12.5.2. We consider only those parts that extend directly.

Theorem 13.6.1 Let R be the ring of integers in an imaginary quadratic number field.

(a) Let P be a nonzero prime ideal of R. Say that $\overline{P}P = (n)$ where n is a positive integer. Then n is either an integer prime or the square of an integer prime.

(b) Let p be an integer prime. The principal ideal $(p) = pR$ is either a prime ideal, or the product $\overline{P}P$ of a prime ideal and its conjugate.

(c) Assume that $d \equiv 2$ or 3 modulo 4. An integer prime p generates a prime ideal (p) of R if and only if d is not a square modulo p, and this is true if and only if the polynomial $x^2 - d$ is irreducible in $\mathbb{F}_p[x]$.

(d) Assume that $d \equiv 1$ modulo 4, and let $h = \frac{1}{4}(1 - d)$. An integer prime p generates a prime ideal (p) of R if and only if the polynomial $x^2 - x + h$ is irreducible in $\mathbb{F}_p[x]$.

Corollary 13.6.2 With the notation as in the theorem, any proper ideal strictly larger than (p) is a prime, and therefore a maximal, ideal. □

• An integer prime p is said to *remain prime* if the principal ideal $(p) = pR$ is a prime ideal. Otherwise, the principal ideal (p) is a product $\overline{P}P$ of a prime ideal and its conjugate, and in this case the prime p is said to *split*. If in addition $\overline{P} = P$, the prime p is said to *ramify*.

Going back to the case $d = -5$, the prime 2 ramifies in $\mathbb{Z}[\sqrt{-5}]$ because $(2) = \overline{A}A$ and $\overline{A} = A$. The prime 3 splits. It does not ramify, because $(3) = \overline{B}B$ and $\overline{B} \neq B$ (see (13.4.5)).

Proof of Theorem 13.6.1. The proof follows that of Theorem 12.5.2 closely, so we omit the proofs of **(a)** and **(b)**. We discuss **(c)** in order to review the reasoning. Suppose $d \equiv 2$ or 3 modulo 4. Then $R = \mathbb{Z}[\delta]$ is isomorphic to the quotient ring $\mathbb{Z}[x]/(x^2 - d)$. A prime integer p remains prime in R if and only if $\tilde{R} = R/(p)$ is a field. (We are using a tilde here to avoid confusion with complex conjugation.) This leads to the diagram

(13.6.3)
$$\begin{array}{ccc} \mathbb{Z}[x] & \xrightarrow[(p)]{\text{kernel}} & \mathbb{F}_p[x] \\ \Big\downarrow{\scriptstyle \text{kernel } (x^2-d)} & & \Big\downarrow{\scriptstyle \text{kernel } (x^2-d)} \\ \mathbb{Z}[\delta] & \xrightarrow[(p)]{\text{kernel}} & \tilde{R} \end{array}$$

This diagram shows that $\tilde{R}$ is a field if and only if $x^2 - d$ is irreducible in $\mathbb{F}_p[x]$.

The proof of **(d)** is similar. □

Proposition 13.6.4 Let A, B, C be nonzero ideals with $B \supset C$. The index $[B:C]$ of C in B is equal to the index $[AB:AC]$.

Proof. Since A is a product of prime ideals, it suffices to show that $[B:C] = [PB:PC]$ when P is a nonzero prime ideal. The lemma for an arbitrary ideal A follows when we multiply by one prime ideal at a time.

There is a prime integer p such that either $P = (p)$ or $\overline{P}P = (p)$ (13.6.1). If P is the principal ideal (p), the formula to be shown is $[B:C] = [pB:pC]$, and this is rather obvious (see (13.10.3)**(c)**).

Suppose that $(p) = \overline{P}P$. We inspect the chain of ideals $B \supset PB \supset \overline{P}PB = pB$. The cancellation law shows that the inclusions are strict, and $[B:pB] = p^2$. Therefore

$[B:PB] = p$. Similarly, $[C:PC] = p$ (13.10.3)**(b)**. The diagram below, together with the multiplicative property of the index (2.8.14), shows that $[B:C] = [PB:PC]$.

$$\begin{array}{ccc} B & \supset & C \\ \cup & & \cup \\ PB & \supset & PC \end{array}$$

□

13.7 IDEAL CLASSES

As before, R denotes the ring of integers in an imaginary quadratic number field. We have seen that R is a principal ideal domain if and only if it is a unique factorization domain (13.5.6). We define an equivalence relation on nonzero ideals that is compatible with multiplication of ideals, and such that the principal ideals form one equivalence class.

- Two nonzero ideals A and A' of R are *similar* if, for some complex number λ,

$$A' = \lambda A. \tag{13.7.1}$$

Similarity of ideals is an equivalence relation whose geometric interpretation was mentioned before: A and A' are similar if and only if, when regarded as lattices in the complex plane, they are similar geometric figures, by a similarity that is orientation-preserving. To see this, we note that a lattice looks the same at all of its points. So a geometric similarity can be assumed to relate the element 0 of A to the element 0 of A'. Then it will be described as a rotation followed by a stretching or shrinking, that is, as multiplication by a complex number λ.

- Similarity classes of ideals are called *ideal classes*. The class of an ideal A will be denoted by $\langle A \rangle$.

Lemma 13.7.2 The class $\langle R \rangle$ of the unit ideal consists of the principal ideals.

Proof. If $\langle A \rangle = \langle R \rangle$, then $A = \lambda R$ for some complex number λ. Since 1 is in R, λ is an element of A, and therefore an element of R. Then A is the principal ideal (λ). □

We saw in (13.3.3) that there are two ideal classes in the ring $R = \mathbb{Z}[\delta]$, when $\delta^2 = -5$. Both of the ideals $A = (2, 1 + \delta)$ and $B = (3, 1 + \delta)$ represent the class of nonprincipal ideals. They are shown below, in Figure 13.7.4. Rectangles have been put into the figure to help you visualize the fact that the two lattices are similar geometric figures.

We see below (Theorem 13.7.10) that there are always finitely many ideal classes. The number of ideal classes in R is called the *class number* of R.

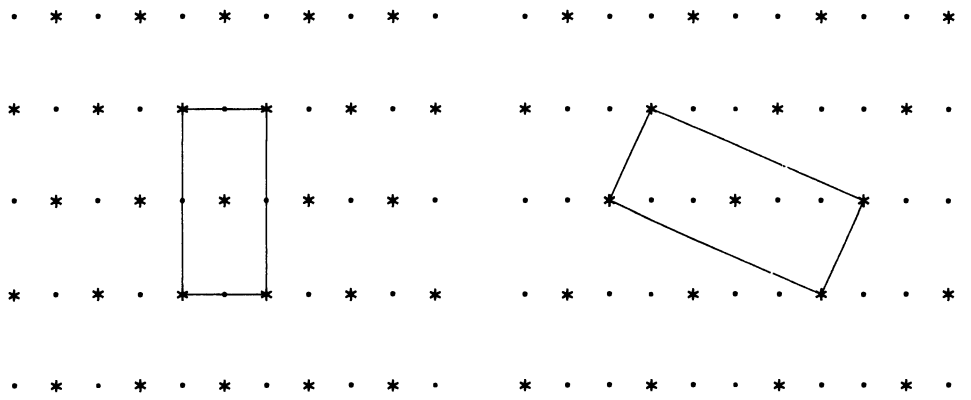
Proposition 13.7.3 The ideal classes form an abelian group $\mathcal{C}$, the *class group* of R, the law of composition being defined by multiplication of ideals: $\langle A \rangle \langle B \rangle = \langle AB \rangle$:

$$(\text{class of } A)(\text{class of } B) = (\text{class of } AB).$$

Proof. Suppose that $\langle A \rangle = \langle A' \rangle$ and $\langle B \rangle = \langle B' \rangle$, i.e., $A' = \lambda A$ and $B' = \gamma B$ for some complex numbers λ and γ. Then $A'B' = \lambda\gamma AB$, and therefore $\langle AB \rangle = \langle A'B' \rangle$. This shows that the law of composition is well defined. The law is commutative and associative because

multiplication of ideals is commutative and associative, and the class $\langle R \rangle$ of the unit ideal is an identity element that we denote by 1, as usual. The only group axiom that isn't obvious is that every class $\langle A \rangle$ has an inverse. But this follows from the Main Lemma, which asserts that $\overline{A}A$ is a principal ideal (n). Since the class of a principal ideal is 1, $\langle \overline{A} \rangle \langle A \rangle = 1$ and $\langle \overline{A} \rangle = \langle A \rangle^{-1}$. □

The class number is thought of as a way to quantify how badly unique factorization of elements fails. More precise information is given by the structure of C as a group. As we have seen, the class number of the ring $R = \mathbb{Z}[\sqrt{-5}]$ is two. The class group of R has order two. One consequence of this is that the product of any two nonprincipal ideals of R is a principal ideal. We saw several examples of this in (13.4.7).



(13.7.4) The Ideals $A = (2, 1 + \delta)$ and $B = (3, 1 + \delta)$, $\delta^2 = -5$.

Measuring an Ideal

The Main Lemma tells us that if A is a nonzero ideal, then $\overline{A}A = (n)$ is the principal ideal generated by a positive integer. That integer is defined to be the *norm* of A. It will be denoted by $N(A)$:

(13.7.5) $N(A) = n$, if n is the positive integer such that $\overline{A}A = (n)$.

The norm of an ideal is analogous to the norm of an element. As is true for norms of elements, this norm is multiplicative.

Lemma 13.7.6 If A and B are nonzero ideals, then $N(AB) = N(A)N(B)$. Moreover, the norm of the principal ideal (α) is equal to $N(\alpha)$, the norm of the element α.

Proof. Say that $N(A) = m$ and $N(B) = n$. This means that $\overline{A}A = (m)$ and $\overline{B}B = (n)$. Then $(\overline{AB})(AB) = (\overline{A}A)(\overline{B}B) = (m)(n) = (mn)$. So $N(AB) = mn$.

Next, suppose that A is the principal ideal (α), and let $n = N(\alpha)$ $(= \overline{\alpha}\alpha)$. Then $\overline{A}A = (\overline{\alpha})(\alpha) = (\overline{\alpha}\alpha) = (n)$, so $N(A) = n$ too. □

We now have four ways to measure the size of an ideal A:

- the norm $N(A)$,
- the index $[R:A]$ of A in R,
- the area $\Delta(A)$ of the parallelogram spanned by a lattice basis for A,
- the minimum value taken on by the norm $N(\alpha)$, of the nonzero elements of A.

The relations among these measures are given by Theorem 13.7.8 below. To state that theorem, we need a peculiar number:

$$\mu = \begin{cases} 2\sqrt{\frac{|d|}{3}} & \text{if } d \equiv 2 \text{ or } 3 \pmod 4 \\ \sqrt{\frac{|d|}{3}} & \text{if } d \equiv 1 \pmod 4. \end{cases} \tag{13.7.7}$$

Theorem 13.7.8 Let R be the ring of integers in an imaginary quadratic number field, and let A be a nonzero ideal of R. Then

(a) $N(A) = [R:A] = \dfrac{\Delta(A)}{\Delta(R)}$.

(b) If α is a nonzero element of A of minimal norm, $N(\alpha) \leq N(A)\mu$.

The most important point about **(b)** is that the coefficient μ doesn't depend on the ideal.

Proof. **(a)** We refer to Proposition 13.10.6 for the proof that $[R:A] = \frac{\Delta(A)}{\Delta(R)}$. In outline, the proof that $N(A) = [R:A]$ is as follows. Reference letters have been put over the equality symbols. Let $n = N(A)$. Then

$$n^2 \overset{1}{=} [R:nR] \overset{2}{=} \left[R:\overline{A}A\right] \overset{3}{=} [R:A]\left[A:\overline{A}A\right] \overset{4}{=} [R:A]\left[R:\overline{A}\right] \overset{5}{=} [R:A]^2.$$

The equality labeled 1 is Lemma 13.10.3**(b)**, the one labeled 2 is the Main Lemma, which says that $nR = \overline{A}A$, and 3 is the multiplicative property of the index. The equality 4 follows from Proposition 13.6.4: $[A : \overline{A}A] = [RA : \overline{A}A] = [R : \overline{A}]$. Finally, the ring R is equal to its complex conjugate $\overline{R}$, and 5 comes down to the fact that $[\overline{R}:\overline{A}] = [R:A]$.

(b) When $d \equiv 2, 3$ modulo 4, R has the lattice basis $(1, \delta)$, and when $d \equiv 1$ modulo 4, R has the lattice basis $(1, \eta)$. The area $\Delta(R)$ of the parallelogram spanned by this basis is

$$\Delta(R) = \begin{cases} \sqrt{|d|} & \text{if } d \equiv 2 \text{ or } 3 \text{ modulo } 4 \\ \frac{1}{2}\sqrt{|d|} & \text{if } d \equiv 1 \text{ modulo } 4. \end{cases} \tag{13.7.9}$$

So $\mu = \frac{2}{\sqrt{3}}\Delta(R)$. The length of the shortest vector in a lattice is estimated in Lemma 13.10.8: $N(\alpha) \leq \frac{2}{\sqrt{3}}\Delta(A)$. We substitute $\Delta(A) = N(A)\Delta(R)$ from part **(a)** into this inequality, obtaining $N(\alpha) \leq N(A)\mu$. □

Theorem 13.7.10

(a) Every ideal class contains an ideal A with norm $N(A) \leq \mu$.

(b) The class group $\mathcal{C}$ is generated by the classes of prime ideals P whose norms are prime integers $p \leq \mu$.

(c) The class group $\mathcal{C}$ is finite.

Proof of Theorem 13.7.10. **(a)** Let A be an ideal. We must find an ideal C in the class $\langle A \rangle$ whose norm is at most μ. We choose a nonzero element α in A, with $N(\alpha) \leq N(A)\mu$. Then A contains the principal ideal (α), so A divides (α), i.e., $(\alpha) = AC$ for some ideal C, and $N(A)N(C) = N(\alpha) \leq N(A)\mu$. Therefore $N(C) \leq \mu$. Now since AC is a principal ideal, $\langle C \rangle = \langle A \rangle^{-1} = \langle \overline{A} \rangle$. This shows that the class $\langle \overline{A} \rangle$ contains an ideal, namely C, whose norm is at most μ. Then the class $\langle A \rangle$ contains $\overline{C}$, and $N(\overline{C}) = N(C) \leq \mu$.

(b) Every class contains an ideal A of norm $N(A) \leq \mu$. We factor A into prime ideals: $A = P_1 \cdots P_k$. Then $N(A) = N(P_1) \cdots N(P_k)$, so $N(P_i) \leq \mu$ for each i. The classes of prime ideals with norm $\leq \mu$ generate $\mathcal{C}$. The norm of a prime ideal P is either a prime integer p or the square p^2 of a prime integer. If $N(P) = p^2$, then $P = (p)$ (13.6.1). This is a principal ideal, and its class is trivial. We may ignore those primes.

(c) We show that there are finitely many ideals A with norm $N(A) \leq \mu$. If we write such an ideal as a product of prime ideals, $A = P_1 \cdots P_k$, and if $m_i = N(P_i)$, then $m_1 \cdots m_k \leq \mu$. There are finitely many sets of integers m_i, each a prime or the square of a prime, that satisfy this inequality, and there are at most two prime ideals with norms equal to a given integer m_i. So there are finitely many sets of prime ideals such that $N(P_1 \cdots P_k) \leq \mu$. □

13.8 COMPUTING THE CLASS GROUP

The table below lists a few class groups. In the table, $\lfloor \mu \rfloor$ denotes the *floor* of μ, the largest integer $\leq \mu$. If n is an integer and if $n \leq \mu$, then $n \leq \lfloor \mu \rfloor$.

d	$\lfloor \mu \rfloor$	*class group*
-2	1	C_1
-5	2	C_2
-7	1	C_1
-14	4	C_4
-21	5	$C_2 \times C_2$
-23	2	C_3
-47	3	C_5
-71	4	C_7

(13.8.1) Some Class Groups

To apply Theorem 13.7.10, we examine the prime integers $p \leq \lfloor \mu \rfloor$. If p splits (or ramifies) in R, we include the class of one of its two prime ideal factors in our set of

generators for the class group. The class of the other prime factor is its inverse. If p remains prime, its class is trivial and we discard it.

Example 13.8.2 $d = -163$. Since $-163 \equiv 1$ modulo 4, the ring R of integers is $\mathbb{Z}[\eta]$, where $\eta = \frac{1}{2}(1 + \delta)$, and $\lfloor \mu \rfloor = 8$. We must inspect the primes $p = 2, 3, 5$, and 7. If p splits, we include one of its prime divisors as a generator of the class group. According to Theorem 13.6.1, an integer prime p remains prime in R if and only if the polynomial $x^2 - x + 41$ is irreducible modulo p. This polynomial happens to be irreducible modulo each of the primes 2, 3, 5, and 7. So the class group is trivial, and R is a unique factorization domain. □

For the rest of this section, we consider cases in which $d \equiv 2$ or 3 modulo 4. In these cases, a prime p splits if and only if $x^2 - d$ has a root in $\mathbb{F}_p$. The table below tells us which primes need to be examined.

	$p \leq \mu$
$-d \leq 2$	
$-d \leq 6$	2
$-d \leq 17$	2, 3
$-d \leq 35$	2, 3, 5
$-d \leq 89$	2, 3, 5, 7
$-d \leq 123$	2, 3, 5, 7, 11

(13.8.3) Primes Less Than μ, When $d \equiv 2$ or 3 Modulo 4

If $d = -1$ or -2, there are no primes less than μ, so the class group is trivial, and R is a unique factorization domain.

Let's suppose that we have determined which of the primes that need to be examined split. Then we will have a set of generators for the class group. But to determine its structure we still need to determine the relations among these generators. It is best to analyze the prime 2 directly.

Lemma 13.8.4 Suppose that $d \equiv 2$ or 3 modulo 4. The prime 2 ramifies in R. The prime divisor P of the principal ideal (2) is

- $P = (2, 1 + \delta)$, if $d \equiv 3$ modulo 4,
- $P = (2, \delta)$, if $d \equiv 2$ modulo 4.

The class $\langle P \rangle$ has order two in the class group unless $d = -1$ or -2. In those cases, P is a principal ideal. In all cases, the given generators form a lattice basis of the ideal P.

Proof. Let P be as in the statement of the lemma. We compute the product ideal $\overline{P}P$. If $d \equiv 3$ modulo 4, $\overline{P}P = (2, 1 - \delta)(2, 1 + \delta) = (4, 2 + 2\delta, 2 - 2\delta, 1 - d)$, and if $d \equiv 2$ modulo 4, $\overline{P}P = (2, -\delta)(2, \delta) = (4, 2\delta, -d)$. In both cases, $\overline{P}P = (2)$. Theorem 15.10.1 tells us that the ideal (2) is either a prime ideal or the product of a prime ideal and its conjugate, so P must be a prime ideal.

We note also that $\overline{P} = P$, so 2 ramifies, $\langle P\rangle = \langle P\rangle^{-1}$, and $\langle P\rangle$ has order 1 or 2 in the class group. It will have order 1 if and only if it is a principal ideal. This happens when $d = -1$ or -2. If $d = -1$, $P = (1 + \delta)$, and if $d = -2$, $P = (\delta)$. When $d < -2$, the integer 2 has no proper factor in R, and then P is not a principal ideal. □

Corollary 13.8.5 If $d \equiv 2$ or 3 modulo 4 and $d < -2$, the class number is even. □

Example 13.8.6 $d = -26$. Table 13.8 tells us to inspect the primes $p = 2, 3$, and 5. The polynomial $x^2 + 26$ is reducible modulo 2, 3, and 5, so all of those primes split. Let's say that

$$(2) = \overline{P}P, \quad (3) = \overline{Q}Q, \quad \text{and } (5) = \overline{S}S.$$

We have three generators $\langle P\rangle$, $\langle Q\rangle$, $\langle S\rangle$ for the class group, and $\langle P\rangle$ has order 2. How can we determine the other relations among these generators? The secret method is to compute norms of a few elements, hoping to get some information. We don't have to look far: $N(1 + \delta) = 27 = 3^3$ and $N(2 + \delta) = 30 = 2 \cdot 3 \cdot 5$.

Let $\alpha = 1 + \delta$. Then $\overline{\alpha}\alpha = 3^3$. Since $(3) = \overline{Q}Q$, we have the ideal relation

$$(\overline{\alpha})(\alpha) = (\overline{Q}Q)^3.$$

Because ideals factor uniquely, the principal ideal (α) is the product of one half of the terms on the right, and $(\overline{\alpha})$ is the product of the conjugates of those terms. We note that 3 doesn't divide α in R. Therefore $\overline{Q}Q = (3)$ doesn't divide (α). It follows that (α) is either Q^3 or $\overline{Q}^3$. Which it is depends on which prime factor of (3) we label as Q.

In either case, $\langle Q\rangle^3 = 1$, and $\langle Q\rangle$ has order 1 or 3 in the class group. We check that 3 has no proper divisor in R. Then since Q divides (3), it cannot be a principal ideal. So $\langle Q\rangle$ has order 3.

Next, let $\beta = 2 + \delta$. Then $\overline{\beta}\beta = 2 \cdot 3 \cdot 5$, and this gives us the ideal relation

$$(\overline{\beta})(\beta) = \overline{P}P\overline{Q}Q\overline{S}S.$$

Therefore the principal ideal (β) is the product of one half of the ideals on the right and $(\overline{\beta})$ is the product of the conjugates of those ideals. We know that $\overline{P} = P$. If we don't care which prime factors of (3) and (5) we label as Q and S, we may assume that $(\beta) = PQS$. This gives us the relation $\langle P\rangle\langle Q\rangle\langle S\rangle = 1$.

We have found three relations:

$$\langle P\rangle^2 = 1, \quad \langle Q\rangle^3 = 1, \quad \text{and } \langle P\rangle\langle Q\rangle\langle S\rangle = 1.$$

These relations show that $\langle Q\rangle = \langle S\rangle^2$, $\langle P\rangle = \langle S\rangle^3$, and that $\langle S\rangle$ has order 6. The class group is a cyclic group of order 6, generated by a prime ideal divisor of 5.

The next lemma explains why the method of computing norms works.

Lemma 13.8.7 Let P, Q, S be prime ideals of the ring R of imaginary quadratic integers, whose norms are the prime integers p, q, s, respectively. Suppose that the relation

$\langle P\rangle^i\langle Q\rangle^j\langle S\rangle^k = 1$ holds in the class group $\mathcal{C}$. Then there is an element α in R with norm equal to $p^iq^js^k$.

Proof. By definition, $\langle P\rangle^i\langle Q\rangle^j\langle S\rangle^k = \langle P^iQ^jS^k\rangle$. If $\langle P^iQ^jS^k\rangle = 1$, the ideal $P^iQ^jS^k$ is principal, say $P^iQ^jS^k = (\alpha)$. Then

$$(\overline{\alpha})(\alpha) = (\overline{P}P)^i(\overline{Q}Q)^j(\overline{S}S)^k = (p)^i(q)^j(s)^k = (p^iq^js^k).$$

Therefore $N(\alpha) = \overline{\alpha}\alpha = p^iq^js^k$. □

We compute one more class group.

Example 13.8.8 $d = -74$. The primes to inspect are 2, 3, 5, and 7. Here 2 ramifies, 3 and 5 split, and 7 remains prime. Say that $(2) = \overline{P}P$, $(3) = \overline{Q}Q$, and $(5) = \overline{S}S$. Then $\langle P\rangle$, $\langle Q\rangle$, and $\langle S\rangle$ generate the class group, and $\langle P\rangle$ has order 2 (13.8.4). We note that

$$\begin{aligned} N(1+\delta) &= 75 = 3\cdot 5^2 \\ N(4+\delta) &= 90 = 2\cdot 3^2\cdot 5 \\ N(13+\delta) &= 243 = 3^5 \\ N(14+\delta) &= 270 = 2\cdot 3^3\cdot 5 \end{aligned}$$

The norm $N(13+\delta)$ shows that $\langle Q\rangle^5 = 1$, so $\langle Q\rangle$ has order 1 or 5. Since 3 has no proper divisor in R, Q isn't a principal ideal. So $\langle Q\rangle$ has order 5. Next, $N(1+\delta)$ shows that $\langle S\rangle^2 = \langle Q\rangle$ or $\langle\overline{Q}\rangle$, and therefore $\langle S\rangle$ has order 10. We eliminate $\langle Q\rangle$ from our set of generators. Finally, $N(4+\delta)$ gives us one of the relations $\langle P\rangle\langle Q\rangle^2\langle S\rangle = 1$ or $\langle P\rangle\langle Q\rangle^2\langle\overline{S}\rangle = 1$. Either one allows us to eliminate $\langle P\rangle$ from our list of generators. The class group is cyclic of order 10, generated by a prime ideal divisor of (5).

13.9 REAL QUADRATIC FIELDS

We take a brief look at real quadratic number fields, fields of the form $\mathbb{Q}[\sqrt{d}]$, where d is a square-free positive integer, and we use the field $\mathbb{Q}[\sqrt{2}]$ as an example. The ring of integers in this field is a unique factorization domain:

$$R = \mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}. \tag{13.9.1}$$

It can be shown that unique factorization of ideals into prime ideals is true for the ring of integers in any real quadratic number field, and that the class number is finite [Cohn], [Hasse]. It is conjectured that there are infinitely many values of d for which the ring of integers has unique factorization.

When d is positive, $\mathbb{Q}[\sqrt{d}]$ is a subfield of the real numbers. Its ring of integers is not embedded as a lattice in the complex plane. However, we can represent R as a lattice in $\mathbb{R}^2$ by associating to the algebraic integer $a + b\sqrt{d}$ the point (u, v) of $\mathbb{R}^2$, where

$$u = a + b\sqrt{d}, \quad v = a - b\sqrt{d}. \tag{13.9.2}$$

The resulting lattice is depicted below for the case $d = 2$. The reason that the hyperbolas have been put into the figure will be explained presently.

Recall that the field $Q[\sqrt{d}]$ is isomorphic to the abstractly constructed field

$$F = \mathbb{Q}[x]/(x^2 - d). \tag{13.9.3}$$

If we replace $\mathbb{Q}[\sqrt{d}]$ by F and denote the residue of x in F by δ, then δ is an abstract square root of d rather than the positive real square root, and F is the set of elements $a + b\delta$, with a and b in $\mathbb{Q}$. The coordinates u, v represent the two ways that the abstractly defined field F can be embedded into the real numbers, namely, u sends $\delta \rightsquigarrow \sqrt{d}$ and v sends $\delta \rightsquigarrow -\sqrt{d}$.

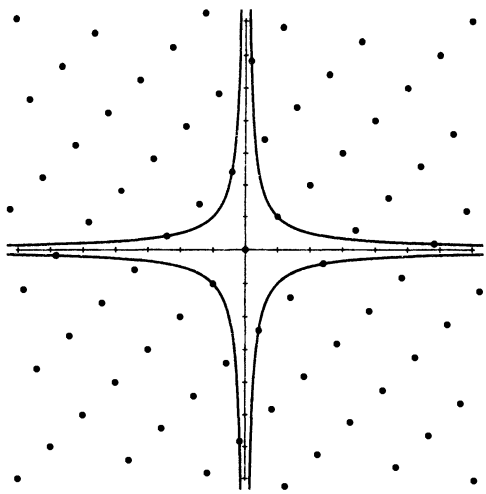
For $\alpha = a + b\delta \in \mathbb{Q}[\delta]$, we denote by α' the "conjugate" element $a - b\delta$. The *norm* of α is

$$N(\alpha) = \alpha'\alpha = a^2 - b^2 d. \tag{13.9.4}$$

If α is an algebraic integer, then $N(\alpha)$ is an ordinary integer. The norm is multiplicative:

$$N(\alpha\beta) = N(\alpha)N(\beta). \tag{13.9.5}$$

However, $N(\alpha)$ is not necessarily positive. It isn't equal to $|\alpha|^2$.



(13.9.6) The Lattice $\mathbb{Z}[\sqrt{2}]$.

One significant difference between real and imaginary quadratic fields is that the ring of integers in a real quadratic field always contains infinitely many units. Since the norm of an algebraic integer is an ordinary integer, a unit must have norm ± 1, and if $N(\alpha) = \pm 1$, then the inverse of α is $\pm\alpha'$, so α is a unit. For example,

$$\alpha = 1 + \sqrt{2}, \quad \alpha^2 = 3 + 2\sqrt{2}, \quad \alpha^3 = 7 + 5\sqrt{2}, \ldots \tag{13.9.7}$$

are units in the ring $R = \mathbb{Z}[\sqrt{2}]$. The element α has infinite order in the group of units.

The condition $N(\alpha) = a^2 - 2b^2 = \pm 1$ for units translates in (u, v)-coordinates to

$$uv = \pm 1. \tag{13.9.8}$$

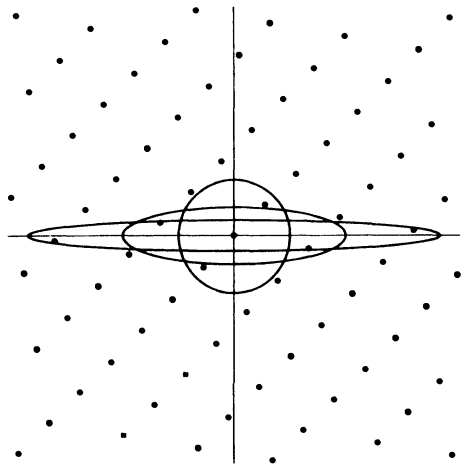
So the units are the points of the lattice that lie on one of the two hyperbolas $uv = 1$ and $uv = -1$, the ones depicted in Figure 13.9.6. It is remarkable that the ring of integers in a real quadratic field always has infinitely many units or, what amounts to the same thing, that the lattice always contains infinitely many points on these hyperbolas. This is far from obvious, either algebraically or geometrically, but a few such points are visible in the figure.

Theorem 13.9.9 Let R be the ring of integers in a real quadratic number field. The group of units in R is an infinite group.

We have arranged the proof as a sequence of lemmas. The first one follows from Lemma 13.10.8 in the next section.

Lemma 13.9.10 For every $\Delta_0 > 0$, there exists an $r > 0$ with the following property: Let L be a lattice in the (u, v)-plane P, let $\Delta(L)$ denote the area of the parallelogram spanned by a lattice basis, and suppose that $\Delta(L) \leq \Delta_0$. Then L contains a nonzero element γ with $|\gamma| < r$. □

Let Δ_0 and r be as above. For $s > 0$, we denote by D_s the elliptical disk in the (u, v) plane defined by the inequality $s^{-2}u^2 + s^2v^2 \leq r^2$. So D_1 is the circular disk of radius r. The figure below shows three of the disks D_s.



(13.9.11) Elliptical Disks that Contain Points of the Lattice.

Lemma 13.9.12 With notation as above, let L be a lattice that contains no point on the coordinate axes except the origin, and such that $\Delta(L) \leq \Delta_0$.

(a) For any $s > 0$, the elliptical disk D_s contains a nonzero element of L.

(b) For any point $\alpha = (u, v)$ in the disk D_s, $|uv| \leq \frac{r^2}{2}$.

Proof. **(a)** The map $\varphi: \mathbb{R}^2 \to \mathbb{R}^2$ defined by $\varphi(x, y) = (sx, s^{-1}y)$ maps D_1 to D_s. The inverse image $L' = \varphi^{-1}L$ of L contains no point on the axes except the origin. We note that φ is an area-preserving map, because it multiplies one coordinate by s and the other by s^{-1}.

Therefore $\Delta(L') \leq \Delta_0$. Lemma 13.9.10 shows that the circular disk D_1 contains a nonzero element of L', say γ. Then $\alpha = \varphi(\gamma)$ is an element of L in the elliptical disk D_s.

(b) The inequality is true for the circular disk D_1. Let φ be the map defined above. If $\alpha = (u, v)$ is in D_s, then $\varphi^{-1}(\alpha) = (s^{-1}u, sv)$ is in D_1, so $|uv| = |(s^{-1}u)(sv)| \leq \frac{r^2}{2}$. □

Lemma 13.9.13 With the hypotheses of the previous lemma, the lattice L contains infinitely many points (u, v) with $|uv| \leq \frac{r^2}{2}$.

Proof. We apply the previous lemma. For large s, the disk D_s is very narrow, and it contains a nonzero element of L, say α_s. The elements α_s cannot lie on the e_1-axis but they must become arbitrarily close to that axis as s tends to infinity. It follows that there are infinitely many points among them, and if $\alpha_s = (u_s, v_s)$, then $|u_s v_s| \leq \frac{r^2}{2}$. □

Let R be the ring of integers in a real quadratic field, and let n be an integer. We call two elements β_i of R *congruent modulo* n if n divides $\beta_1 - \beta_2$ in R. When $d \equiv 2$ or 3 modulo 4 and $\beta_i = m_i + n_i\delta$, this simply means that $m_1 \equiv m_2$ and $n_1 \equiv n_2$ modulo n. The same is true when $d \equiv 1$ modulo 4, except that one has to write $\beta_i = m_i + n_i\eta$. In all cases, there are n^2 congruence classes modulo n.

Theorem 13.9.9 follows from the next lemma.

Lemma 13.9.14 Let R be the ring of integers in a real quadratic number field.

(a) There is a positive integer n such that the set S of elements of R with norm n is infinite. Moreover, there are infinitely many pairs of elements of S that are congruent modulo n.

(b) If two elements β_1 and β_2 of R with norm n are congruent modulo n, then β_2/β_1 is a unit of R.

Proof. **(a)** The lattice R contains no point on the axes other than the origin, because u and v aren't zero unless both a and b are zero. If α is an element of R whose image in the plane is the point (u, v), then $|N(\alpha)| = uv$. Lemma 13.9.13 shows that R contains infinitely many points with norm in a bounded interval. Since there are finitely many integers n in that interval, the set of elements of R with norm n is infinite for at least one of them. The fact that there are finitely many congruence classes modulo n proves the second assertion.

(b) We show that β_2/β_1 is in R. The same argument will show that β_1/β_2 is in R, hence that β_2/β_1 is a unit. Since β_1 and β_2 are congruent, we can write $\beta_2 = \beta_1 + n\gamma$, with γ in R. Let β_1' be the conjugate of β_1. So $\beta_1\beta_1' = n$. Then $\beta_2/\beta_1 = (\beta_1 + n\gamma)/\beta_1 = 1 + \beta_1'\gamma$. This is an element of R, as claimed. □

13.10 ABOUT LATTICES

A lattice L in the plane $\mathbb{R}^2$ is *generated*, or *spanned* by a set S if every element of L can be written as an integer combination of elements of S. Every lattice L has a *lattice basis* $\mathbf{B} = (v_1, v_2)$ consisting of two elements. An element of L is an integer combination of the lattice basis vectors in exactly one way (see (6.5.5)).

Some notation:

(13.10.1)

$\Pi(\mathbf{B})$: the parallelogram of linear combinations $r_1v_1 + r_2v_2$ with $0 \le r_i \le 1$.
Its vertices are 0, v_1, v_2, and $v_1 + v_2$.

$\Pi'(\mathbf{B})$: the set of linear combinations $r_1v_1 + r_2v_2$ with $0 \le r_i < 1$. It is obtained by deleting the edges $[v_1, v_1 + v_2]$ and $[v_2, v_1 + v_2]$ from $\Pi(\mathbf{B})$.

$\Delta(L)$: the area of $\Pi(\mathbf{B})$.

$[M:L]$: the index of a sublattice L of a lattice M - the number of additive cosets of L in M.

We will see that $\Delta(L)$ is independent of the lattice basis, so that notation isn't ambiguous. The other notation has been introduced before. For reference, we recall Lemma 6.5.8:

Lemma 13.10.2 Let $\mathbf{B} = (v_1, v_2)$ be a basis of $\mathbb{R}^2$, and let L be the lattice of integer combinations of $\mathbf{B}$. Every vector v in $\mathbb{R}^2$ can be written uniquely in the form $v = w + v_0$, with w in L and v_0 in $\Pi'(\mathbf{B})$. □

Lemma 13.10.3 Let $K \subset L \subset M$ be lattices in the plane, and let $\mathbf{B}$ be a lattice basis for L. Then

(a) $[M:K] = [M:L][L:K]$.

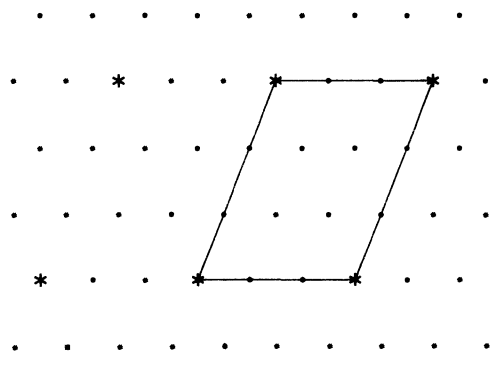
(b) For any positive integer n, $[L:nL] = n^2$.

(c) For any positive real number r, $[M:L] = [rM:rL]$.

(d) $[M:L]$ is finite, and is equal to the number of points of M in the region $\Pi'(\mathbf{B})$.

(e) The lattice M is generated by L together with the finite set $M \cap \Pi'(\mathbf{B})$.

Proof. **(d),(e)** We can write an element x of M uniquely in the form $v + y$, where v is in L and y is in $\Pi'(\mathbf{B})$. Then v is in M, and so y is in M too. Therefore x is in the coset $y + L$. This shows that the elements of $M \cap \Pi'(\mathbf{B})$ are representative elements for the cosets of L in M. Since there is only one way to write $x = v + y$, these cosets are distinct. Since M is discrete and $\Pi'(\mathbf{B})$ is a bounded set, $M \cap \Pi'(\mathbf{B})$ is finite.



(13.10.4) $L = \{\cdot\}$ $3L = \{*\}$.

Formula **(a)** is the multiplicative property of the index (2.8.14). **(b)** follows from **(a)**, because the lattice nL is obtained by stretching L by the factor n, as is illustrated above for the case that $n = 3$. **(c)** is true because multiplication by r stretches both lattices by the same amount. □

Corollary 13.10.5 Let $L \subset M$ be lattices in $\mathbb{R}^2$. There are finitely many lattices between L and M.

Proof. Let $\mathbf{B}$ be a lattice basis for L, and let N be a lattice with $L \subset N \subset M$. Lemma 13.10.3**(e)** shows that N is generated by L and by the set $N \cap \Pi'(\mathbf{B})$, which is a subset of the finite set $M \cap \Pi'(\mathbf{B})$. A finite set has finitely many subsets. □

Proposition 13.10.6 If $L \subset M$ are lattices in the plane, $[M:L] = \dfrac{\Delta(L)}{\Delta(M)}$.

Proof. Say that $\mathbf{C}$ is the lattice basis (u_1, u_2) of M. Let n be a large positive integer, and let M_n denote the lattice with basis $\mathbf{C}_n = (\frac{1}{n}u_1, \frac{1}{n}u_2)$. Let Γ' denote the small region $\Pi'(\mathbf{C}_n)$. Its area is $\frac{1}{n^2}\Delta(M)$. The translates $x + \Gamma'$ of Γ' with x in M_n cover the plane without overlap, and there is exactly one element of M_n in each translate $x + \Gamma'$, namely x. (This is Lemma 13.10.2.)

Let B be a lattice basis for L. We approximate the area of $\Pi(\mathbf{B})$ in the way that one approximates a double integral, using translates of Γ'. Let $r = [M : L]$. Then $[M_n : L] = [M_n : M][M : L] = n^2 r$. Lemma 13.10.3**(d)** tells us that the region $\Pi'(\mathbf{B})$ contains $n^2 r$ points of the lattice M_n. Since the translates of Γ' cover the plane, the translates by these $n^2 r$ points cover $\Pi(\mathbf{B})$ approximately.

$$\Delta(L) \approx n^2 r \Delta(M_n) = r\Delta(M) = [M:L]\Delta(M).$$

The error in this approximation comes from the fact that $\Pi'(\mathbf{B})$ is not covered precisely along its boundary. One can bound this error in terms of the length of the boundary of $\Pi(\mathbf{B})$ and the diameter of Γ' (its largest linear dimension). The diameter tends to zero as $n \to \infty$, and so does the error. □

Corollary 13.10.7 The area $\Delta(L)$ of the parallelogram $\Pi(\mathbf{B})$ is independent of the lattice basis $\mathbf{B}$.

This follows when one sets $M = L$ in the previous proposition. □

Lemma 13.10.8 Let v be a nonzero element of minimal length of a lattice L. Then $|v|^2 \leq \frac{2}{\sqrt{3}}\Delta(L)$.

The inequality becomes an equality for an equilateral triangular lattice.

Proof. We choose an element v_1 of L of minimal length. Then v_1 generates the subgroup $L \cap \ell$, where ℓ is the line spanned by v_1, and there is an element v_2 such that (v_1, v_2) is a

lattice basis of L (see the proof of (6.5.5)). A change of scale changes $|v_1|^2$ and $\Delta(L)$ by the same factor, so we may assume that $|v_1| = 1$. We position coordinates so that $v_1 = (1, 0)^t$.

Say that $v_2 = (b_1, b_2)^t$. We may assume that b_2 is positive. Then $\Delta(L) = b_2$. We may also adjust v_2 by adding a multiple of v_1, to make $-\frac{1}{2} \leq b_1 < \frac{1}{2}$, so that $b_1^2 \leq \frac{1}{4}$. Since v_1 has minimal length among nonzero elements of L, $|v_2|^2 = b_1^2 + b_2^2 \geq |v_1|^2 = 1$. Therefore $b_2^2 \geq \frac{3}{4}$. Thus $\Delta(L) = b_2 \geq \frac{\sqrt{3}}{2}$, and $|v_1|^2 = 1 \leq \frac{2}{\sqrt{3}}\Delta(L)$. □

Nullum vero dubium nobis esse videtur,
quin multa eaque egregia in hoc genere adhuc lateant
in quibus alii vires suas exercere possint.

—Carl Friedrich Gauss

EXERCISES

Section 1 Algebraic Integers

1.1. Is $\frac{1}{2}(1 + \sqrt{5})$ an algebraic integer?

1.2. Prove that the integers in $\mathbb{Q}[\sqrt{d}]$ form a ring.

1.3. **(a)** Let α be a complex number that is the root of a monic integer polynomial, not necessarily an irreducible polynomial. Prove that α is an algebraic integer.

(b) Let α be an algebraic number that is the root of an integer polynomial $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$. Prove that $a_n\alpha$ is an algebraic integer.

(c) Let α be an algebraic integer that is the root of a monic integer polynomial $x^n + a_{n-1}n^{n-1} + \cdots + a_1 x + a_0$. Prove that α^{-1} is an algebraic integer if and only if $a_0 = \pm 1$.

1.4. Let d and d' be integers. When are the fields $\mathbb{Q}(\sqrt{d})$ and $\mathbb{Q}(\sqrt{d'})$ distinct?

Section 2 Factoring Algebraic Integers

2.1. Prove that 2, 3, and $1 \pm \sqrt{-5}$ are irreducible elements of the ring $R = \mathbb{Z}[\sqrt{-5}]$ and that the units of this ring are ± 1.

2.2. For which negative integers $d \equiv 2$ modulo 4 is the ring of integers in $\mathbb{Q}[\sqrt{d}]$ a unique factorization domain?

Section 3 Ideals in $\mathbb{Z}[\sqrt{-5}]$

3.1. Let α be an element of $R = \mathbb{Z}[\delta]$, $\delta = \sqrt{-5}$, and let $\gamma = \frac{1}{2}(\alpha + \alpha\delta)$. Under what circumstances is the lattice with basis (α, γ) an ideal?

3.2. Let $\delta = \sqrt{-5}$. Decide whether or not the lattice of integer combinations of the given vectors is an ideal: **(a)** $(5, 1 + \delta)$, **(b)** $(7, 1 + \delta)$, **(c)** $(4 - 2\delta, 2 + 2\delta, 6 + 4\delta)$.

3.3. Let A be an ideal of the ring of integers R in an imaginary quadratic field. Prove that there is a lattice basis for A, one of whose elements is an ordinary positive integer.

3.4. For each ring R listed below, use the method of Proposition 13.3.3 to describe the ideals in R. Make a drawing showing the possible shapes of the lattices in each case.

(a) $R = \mathbb{Z}[\sqrt{-3}]$, **(b)** $R = \mathbb{Z}[\frac{1}{2}(1+\sqrt{-3})]$, **(c)** $R = \mathbb{Z}[\sqrt{-6}]$,

(d) $R = \mathbb{Z}[\frac{1}{2}(1+\sqrt{-7})]$, **(e)** $R = \mathbb{Z}[\sqrt{-10}]$

Section 4 Ideal Multiplication

4.1. Let $R = \mathbb{Z}[\sqrt{-6}]$. Find a lattice basis for the product ideal AB, where $A = (2, \delta)$ and $B = (3, \delta)$.

4.2. Let R be the ring $\mathbb{Z}[\delta]$, where $\delta = \sqrt{-5}$, and let A denote the ideal generated by the elements **(a)** $3+5\delta, 2+2\delta$, **(b)** $4+\delta, 1+2\delta$. Decide whether or not the given generators form a lattice basis for A, and identify the ideal $\overline{A}A$.

4.3. Let R be the ring $\mathbb{Z}[\delta]$, where $\delta = \sqrt{-5}$, and let A and B be ideals of the form $A = (\alpha, \frac{1}{2}(\alpha+\alpha\delta))$, $B = (\beta, \frac{1}{2}(\beta+\beta\delta))$. Prove that AB is a principal ideal by finding a generator.

Section 5 Factoring Ideals

5.1. Let $R = \mathbb{Z}[\sqrt{-5}]$.

(a) Decide whether or not 11 is an irreducible element of R and whether or not (11) is a prime ideal of R.

(b) Factor the principal ideal (14) into prime ideals in $\mathbb{Z}[\delta]$.

5.2. Let $\delta = \sqrt{-3}$ and $R = \mathbb{Z}[\delta]$. This is not the ring of integers in the imaginary quadratic number field $\mathbb{Q}[\delta]$. Let A be the ideal $(2, 1+\delta)$.

(a) Prove that A is a maximal ideal, and identify the quotient ring R/A.

(b) Prove that $\overline{A}A$ is not a principal ideal, and that the Main Lemma is not true for this ring.

(c) Prove that A contains the principal ideal (2) but that A does not divide (2).

5.3. Let $f = y^2 - x^3 - x$. Is the ring $\mathbb{C}[x, y]/(f)$ an integral domain?

Section 6 Prime Ideals and Prime Integers

6.1. Let $d = -14$. For each of the primes $p = 2, 3, 5, 7, 11$, and 13, decide whether or not p splits or ramifies in R, and if so, find a lattice basis for a prime ideal factor of (p).

6.2. Suppose that d is a negative integer, and that $d \equiv 1$ modulo 4. Analyze whether or not 2 remains prime in R in terms of congruence modulo 8.

6.3. Let R be the ring of integers in an imaginary quadratic field.

(a) Suppose that an integer prime p remains prime in R. Prove that $R/(p)$ is a field with p^2 elements.

(b) Prove that if p splits but does not ramify, then $R/(p)$ is isomorphic to the product ring $\mathbb{F}_p \times \mathbb{F}_p$.

6.4. When d is congruent 2 or 3 modulo 4, an integer prime p remains prime in the ring of integers of $\mathbb{Q}[\sqrt{d}]$ if the polynomial $x^2 - d$ is irreducible modulo p.

(a) Prove that this is also true when $d \equiv 1$ modulo 4 and $p \neq 2$.

(b) What happens to $p = 2$ when $d \equiv 1$ modulo 4?

6.5. Assume that d is congruent 2 or 3 modulo 4.

(a) Prove that a prime integer p ramifies in R if and only if $p = 2$ or p divides d.

(b) Let p be an integer prime that ramifies, and say that $(p) = P^2$. Find an explicit lattice basis for P. In which cases is P a principal ideal?

6.6. Let d be congruent to 2 or 3 modulo 4. An integer prime might be of the form $a^2 - b^2 d$, with a and b in $\mathbb{Z}$. How is this related to the prime ideal factorization of (p) in the ring of integers R?

6.7. Suppose that $d \equiv 2$ or 3 modulo 4, and that a prime $p \neq 2$ does not remain prime in R. Let a be an integer such that $a^2 \equiv d$ modulo p. Prove that $(p, a + \delta)$ is a lattice basis for a prime ideal that divides (p).

Section 7 Ideal Classes

7.1. Let $R = \mathbb{Z}[\sqrt{-5}]$, and let $B = (3, 1 + \delta)$. Find a generator for the principal ideal B^2.

7.2. Prove that two nonzero ideals A and A' in the ring of integers in an imaginary quadratic field are similar if and only if there is a nonzero ideal C such that both AC and $A'C$ are principal ideals.

7.3. Let $d = -26$. With each of the following integers n, decide whether n is the norm of an element α of R. If it is, find α: $n = 75,\ 250,\ 375,\ 5^6$.

7.4. Let $R = \mathbb{Z}[\delta]$, where $\delta^2 = -6$.

(a) Prove that the lattices $P = (2, \delta)$ and $Q = (3, \delta)$ are prime ideals of R.

(b) Factor the principal ideal (6) into prime ideals explicitly in R.

(c) Determine the class group of R.

Section 8 Computing the Class Group

8.1. With reference to Example 13.8.6, since $\langle P \rangle = \langle S \rangle^3$ and $\langle Q \rangle = \langle S \rangle^2$, Lemma 13.8.7 predicts that there are elements whose norms are $2 \cdot 5^3$ and $3^2 \cdot 5^2$. Find such elements.

8.2. With reference to Example 13.8.8, explain why $N(4 + \delta)$ and $N(14 + \delta)$ don't lead to contradictory conclusions.

8.3. Let $R = \mathbb{Z}[\delta]$, with $\delta = \sqrt{-29}$. In each case, compute the norm, explain what conclusions one can draw about ideals in R from the norm computation, and determine the class group of R: $N(1 + \delta)$, $N(4 + \delta)$, $N(5 + \delta)$, $N(9 + 2\delta)$, $N(11 + 2\delta)$.

8.4. Prove that the values of d listed in Theorem 13.2.5 have unique factorization.

8.5. Determine the class group and draw the possible shapes of the lattices in each case:
(a) $d = -10$, **(b)** $d = -13$, **(c)** $d = -14$, **(d)** $d = -21$.

8.6. Determine the class group in each case:
(a) $d = -41$, **(b)** $d = -57$, **(c)** $d = -61$, **(d)** $d = -77$, **(e)** $d = -89$.

Section 9 Real Quadratic Fields

9.1. Prove that $1 + \sqrt{2}$ is an element of infinite order in the group of units of $\mathbb{Z}[\sqrt{2}]$.

9.2. Determine the solutions of the equation $x^2 - y^2 d = 1$ when d is a positive integer.

9.3. **(a)** Prove that the size function $\sigma(\alpha) = |N(\alpha)|$ makes the ring $\mathbb{Z}[\sqrt{2}]$ into a Euclidean domain, and that this ring has unique factorization.

(b) Make a sketch showing the principal ideal $(\sqrt{2})$ of $R = \mathbb{Z}[\sqrt{2}]$, in the embedding depicted in Figure 13.9.6.

9.4. Let R be the ring of integers in a real quadratic number field. What structures are possible for the group of units in R?

9.5. Let R be the ring of integers in a real quadratic number field, and let U_0 denote the set of units of R that are in the first quadrant in the embedding (13.9.2).

(a) Prove that U_0 is an infinite cyclic subgroup of the group of units.

(b) Find a generator for U_0 when $d = 3$ and when $d = 5$.

(c) Draw a figure showing the hyperbolas and the units in a reasonable size range for $d = 3$.

Section 10 About Lattices

10.1. Let M be the integer lattice in $\mathbb{R}^2$, and let L be the lattice with basis $((2, 3)^t, (3, 6)^t)$. Determine the index $[M:L]$.

10.2. Let $L \subset M$ be lattices with bases $\mathbf{B}$ and $\mathbf{C}$, respectively, and let A be the integer matrix such that $\mathbf{B}A = \mathbf{C}$. Prove that $[M:L] = |\det A|$.

Miscellaneous Problems

M.1. Describe the subrings S of $\mathbb{C}$ that are lattices in the complex plane.

***M.2.** Let $R = \mathbb{Z}[\delta]$, where $\delta = \sqrt{-5}$, and let p be a prime integer.

(a) Prove that if p splits in R, say $(p) = \overline{P}P$, then exactly one of the ellipses $x^2 + 5y^2 = p$ or $x^2 + 5y^2 = 2p$ contains an integer point.

(b) Find a property that determines which ellipse has an integer point.

M.3. Describe the prime ideals in **(a)** the polynomial ring $\mathbb{C}[x, y]$ in two variables,

(b) the ring $\mathbb{Z}[x]$ of integer polynomials.

M.4. Let L denote the integer lattice $\mathbb{Z}^2$ in the plane $\mathbb{R}^2$, and let P be a polygon in the plane whose vertices are points of L. *Pick's Theorem* asserts that the area $\Delta(P)$ is equal to $a + b/2 - 1$, where a is the number of points of L in the interior of P, and b is the number of points of L on the boundary of P.

(a) Prove Pick's Theorem.

(b) Derive Proposition 13.10.6 from Pick's Theorem.