FACTORING IN QUADRATIC FIELDS

KEITH CONRAD

1. Introduction

For a squarefree integer d, let

$$K = \mathbf{Q}[\sqrt{d}] = \{x + y\sqrt{d} : x, y \in \mathbf{Q}\}.$$

This is called a *quadratic field* and has degree 2 over $\mathbf{Q}$. Similarly, set

$$\mathbf{Z}[\sqrt{d}] = \{a + b\sqrt{d} : a, b \in \mathbf{Z}\}.$$

This is a subring of $\mathbf{Q}[\sqrt{d}]$.

We will define a concept of "integers" for K, which will play the same role in K as the ordinary integers $\mathbf{Z}$ do in $\mathbf{Q}$. The integers of K will contain $\mathbf{Z}[\sqrt{d}]$ but may be larger. Unique factorization in the integers of K does not always hold, but we can recover unique factorization if we broaden our view of what we should be trying to factor.

2. Conjugation

In addition to the basic field operations, a quadratic field has an additional operation of *conjugation*, which generalizes complex conjugation. For $\alpha = x+y\sqrt{d} \in K$, set its conjugate to be

$$\overline{\alpha} = x - y\sqrt{d}.$$

It is left to the reader to check by a direct calculation that conjugation has the following properties:

$$\overline{\alpha + \beta} = \overline{\alpha} + \overline{\beta}, \quad \overline{\alpha\beta} = \overline{\alpha} \cdot \overline{\beta}, \quad \overline{\overline{\alpha}} = \alpha, \tag{2.1}$$

and also

$$\overline{\alpha} = \alpha \iff \alpha \in \mathbf{Q}. \tag{2.2}$$

In terms of Galois theory, conjugation is the nontrivial element of $\mathrm{Gal}(K/\mathbf{Q})$.

For any $\alpha \in K$, $\alpha + \overline{\alpha}$ and $\alpha\overline{\alpha}$ are rational, either because $\alpha + \overline{\alpha}$ and $\alpha\overline{\alpha}$ are fixed by conjugation (use the algebraic properties in (2.1) to check that) or because one can explicitly compute

$$\alpha + \overline{\alpha} = 2x, \quad \alpha\overline{\alpha} = x^2 - dy^2 \tag{2.3}$$

where $\alpha = x + y\sqrt{d}$.

Definition 2.1. For $\alpha \in K$, set $\mathrm{Tr}(\alpha) = \alpha + \overline{\alpha}$ and $\mathrm{N}(\alpha) = \alpha\overline{\alpha}$. These are called the *trace* and *norm* of α.

Explicit formulas for the trace and norm are in (2.3). Note $\mathrm{Tr}\colon K \to \mathbf{Q}$ and $\mathrm{N}\colon K \to \mathbf{Q}$. For $q \in \mathbf{Q}$, $\mathrm{Tr}(q) = 2q$ and $\mathrm{N}(q) = q^2$.

Theorem 2.2. *The trace is additive and the norm is multiplicative. That is,* $\mathrm{Tr}(\alpha + \beta) = \mathrm{Tr}(\alpha) + \mathrm{Tr}(\beta)$ *and* $\mathrm{N}(\alpha\beta) = \mathrm{N}(\alpha)\,\mathrm{N}(\beta)$.

Proof. Just compute. □

Every $\alpha \in K$ is the root of a monic polynomial of degree 2 with rational coefficients:

$$(X-\alpha)(X-\overline{\alpha}) = X^2 - (\alpha+\overline{\alpha})X + \alpha\overline{\alpha} = X^2 - \mathrm{Tr}(\alpha)X + \mathrm{N}(\alpha). \tag{2.4}$$

This has α and $\overline{\alpha}$ as its two roots, and the coefficients are the trace (up to sign) and the norm. The coefficients of (2.4) might not be in $\mathbf{Z}$: if $\alpha = 1/2$ then (2.4) is $X^2 - X + 1/4$.

3. Integers in a quadratic field

Restricting attention to those elements of K whose polynomial in (2.4) has coefficients in $\mathbf{Z}$ will define for us what the integers of K are.

Definition 3.1. An element $\alpha \in K$ is called an *integer* of K if the polynomial (2.4) has coefficients in $\mathbf{Z}$. Equivalently, α is an integer of K precisely when its trace and norm are in $\mathbf{Z}$.

Example 3.2. If α lies in $\mathbf{Z}[\sqrt{d}]$ then (2.4) has integer coefficients, so α is an integer of K.

Example 3.3. If $d \equiv 1 \bmod 4$ then $\frac{1+\sqrt{d}}{2}$ is not in $\mathbf{Z}[\sqrt{d}]$ but it is an integer of $\mathbf{Q}[\sqrt{d}]$ since it is a root of $X^2 - X + \frac{1-d}{4}$, whose coefficients are in $\mathbf{Z}$.

Theorem 3.4. *The integers of K are*

$$\{a + b\sqrt{d} : a, b \in \mathbf{Z}\} \text{ if } d \not\equiv 1 \bmod 4$$

and

$$\left\{a + b\left(\frac{1+\sqrt{d}}{2}\right) : a, b \in \mathbf{Z}\right\} \text{ if } d \equiv 1 \bmod 4.$$

Proof. A direct calculation shows that both of the sets consist of integers in K. (To treat the second case, write the elements as $(a + \frac{b}{2}) + \frac{b}{2}\sqrt{d}$ to calculate the trace and norm using (2.3).) We have to show, conversely, that every integer of K has the indicated form.

Let $\alpha = x + y\sqrt{d}$ be an integer of K. This is equivalent to saying $2x \in \mathbf{Z}$ and $x^2 - dy^2 \in \mathbf{Z}$. The first condition means x is half of an ordinary integer ($x = \frac{1}{2}(2x)$), so either $x \in \mathbf{Z}$ or x is half an odd number.

If $x \in \mathbf{Z}$ then $x^2 \in \mathbf{Z}$, so $dy^2 \in \mathbf{Z}$. Then $y \in \mathbf{Z}$ because d *is squarefree.* (If y has a prime factor in its denominator, the square of that prime wouldn't be cancelled by d so that $dy^2 \in \mathbf{Z}$.) Therefore α has the necessary form, with $a = x$ and $b = y$ if $d \not\equiv 1 \bmod 4$, or $a = x - y$ and $b = 2y$ if $d \equiv 1 \bmod 4$.

If x is half an odd number, write $x = a/2$ with a odd. Then the norm of α is $x^2 - dy^2 = a^2/4 - dy^2$, so multiplying through by 4 implies

$$a^2 - d(2y)^2 \in 4\mathbf{Z} \tag{3.1}$$

In particular, $d(2y)^2 \in \mathbf{Z}$. Because d is squarefree, $2y$ is in $\mathbf{Z}$ so either y is in $\mathbf{Z}$ or is half an odd number. If $y \in \mathbf{Z}$ then $a^2 - d(2y)^2 = a^2 - 4dy^2$ is odd (recall a is odd), but this contradicts (3.1). Therefore $y = b/2$ with b an odd number, so

$$\alpha = x + y\sqrt{d} = \frac{a}{2} + \frac{b}{2}\sqrt{d} = \frac{a-b}{2} + b\left(\frac{1+\sqrt{d}}{2}\right),$$

which has the necessary form because $a - b$ is divisible by 2. □

To unify the notation, set

$$\omega = \begin{cases} \sqrt{d}, & \text{if } d \not\equiv 1 \bmod 4, \\ \frac{1+\sqrt{d}}{2}, & \text{if } d \equiv 1 \bmod 4. \end{cases}$$

Then ω is in $\mathcal{O}_K$ and the elements of $\mathcal{O}_K$ take the form

$$\mathbf{Z}[\omega] = \{a + b\omega : a, b \in \mathbf{Z}\}$$

in all cases. They form a subring of K.

We will denote the integers of K as $\mathcal{O}_K$, so $\mathcal{O}_K = \mathbf{Z}[\omega]$. Table 1 gives some examples.

K	$\mathbf{Q}[i]$	$\mathbf{Q}[\sqrt{2}]$	$\mathbf{Q}[\sqrt{5}]$	$\mathbf{Q}[\sqrt{-5}]$	$\mathbf{Q}[\sqrt{-14}]$
$\mathcal{O}_K$	$\mathbf{Z}[i]$	$\mathbf{Z}[\sqrt{2}]$	$\mathbf{Z}[(1+\sqrt{5})/2]$	$\mathbf{Z}[\sqrt{-5}]$	$\mathbf{Z}[\sqrt{-14}]$

TABLE 1. Integers in Quadratic Fields

Remember that $\mathbf{Z}[\sqrt{d}] \subset \mathcal{O}_K$, but when $d \equiv 1 \bmod 4$ the set $\mathcal{O}_K$ is strictly larger than $\mathbf{Z}[\sqrt{d}]$.

We defined the integers of K to be those α such that the particular polynomial (2.4) has coefficients in $\mathbf{Z}$. Here is a more abstract characterization of $\mathcal{O}_K$. It will be important in one proof later (for Theorem 5.4) and is closer to the definition that is needed when K is replaced by a finite extension of $\mathbf{Q}$ of degree greater than 2.

Theorem 3.5. *An element $\alpha \in K$ is in $\mathcal{O}_K$ if and only if it is the root of some monic polynomial $X^2 + mX + n \in \mathbf{Z}[X]$.*

Proof. If $\alpha \in \mathcal{O}_K$ then (2.4) is a polynomial of the desired type. Conversely, suppose $\alpha^2 + m\alpha + n = 0$ for some m and n in $\mathbf{Z}$.

Case 1: $\alpha \in \mathbf{Q}$. Write α in reduced form as $\alpha = a/b$ where $a, b \in \mathbf{Z}$ and $(a, b) = 1$. Then $(a/b)^2 + m(a/b) + n = 0$, so $a^2 + mab + nb^2 = 0$. Thus $a^2 = -mab - nb^2 = b(-ma - nb)$, so $b|a^2$. Since $(a, b) = 1$ it follows that $b = \pm 1$, so $\alpha = a/b = \pm a \in \mathbf{Z} \subset \mathcal{O}_K$.

Case 2: $\alpha \notin \mathbf{Q}$. In addition to the relation $\alpha^2 + m\alpha + n = 0$ we have the relation $\alpha^2 - \mathrm{Tr}(\alpha)\alpha + \mathrm{N}(\alpha) = 0$ from (2.4), where $\mathrm{Tr}(\alpha)$ and $\mathrm{N}(\alpha)$ are in $\mathbf{Q}$. Subtracting the second relation from the first, the α^2 terms cancel and we obtain

$$(m + \mathrm{Tr}(\alpha))\alpha + (n - \mathrm{N}(\alpha)) = 0. \tag{3.2}$$

If $m + \mathrm{Tr}(\alpha) \neq 0$ then we can solve for α in (3.2) to get $\alpha \in \mathbf{Q}$, but we are not in that case. Therefore $m + \mathrm{Tr}(\alpha) = 0$, so $n - \mathrm{N}(\alpha) = 0$. This implies $\mathrm{Tr}(\alpha) = -m \in \mathbf{Z}$ and $\mathrm{N}(\alpha) = n \in \mathbf{Z}$, so α is an integer of K by definition. □

Theorem 3.6. *For $m \in \mathbf{Z}$ and $\alpha = a + b\omega \in \mathbf{Z}[\omega]$, $m|\alpha$ in $\mathbf{Z}[\omega]$ if and only if $m|a$ and $m|b$ in $\mathbf{Z}$.*

Proof. If $m|a$ and $m|b$ in $\mathbf{Z}$ then easily $m|\alpha$. Conversely, if $m|\alpha$ then $a + b\omega = m(a' + b'\omega)$ for some a' and b' in $\mathbf{Z}$. Therefore $a = ma'$ and $b = mb'$, so $m|a$ and $m|b$ in $\mathbf{Z}$. □

We will use Theorem 3.6 often without comment in numerical examples, *e.g.*, $5 + \sqrt{-6}$ is not divisible by 3 in $\mathbf{Z}[\sqrt{-6}]$.

Theorem 3.7. *For any quadratic field K, $\mathcal{O}_K \cap \mathbf{Q} = \mathbf{Z}$ and every element of K is a ratio of elements from $\mathcal{O}_K$.*

Proof. Any element of $\mathcal{O}_K$ is $a + b\omega$ with a and b in $\mathbf{Z}$. Since $\omega \notin \mathbf{Q}$, if $a + b\omega \in \mathbf{Q}$ then $b = 0$, so $a + b\omega = a \in \mathbf{Z}$.

To show every element of K can be written as the ratio of two elements of $\mathcal{O}_K$, if $\alpha = x + y\sqrt{d}$ with rational x and y and we write the fractions x and y with a common denominator, say $x = a/c$ and $y = b/c$ for some $c \in \mathbf{Z}$, then

$$x + y\sqrt{d} = \frac{a + b\sqrt{d}}{c}. \tag{3.3}$$

Since $\mathbf{Z}[\sqrt{d}] \subset \mathcal{O}_K$, we're done. □

Theorem 3.7 says (in part) that the notion of integer in a quadratic field does not introduce any unexpected new integers inside of $\mathbf{Q}$: the rational numbers which are integers in K are the plain integers $\mathbf{Z}$.

Theorem 3.8. *If $\alpha \in \mathcal{O}_K$ then $\overline{\alpha} \in \mathcal{O}_K$.*

Proof. Since α and $\overline{\alpha}$ have the same trace and the same norm, the integrality of $\overline{\alpha}$ is immediate from Definition 3.1. For an alternate proof, show the sets described by Theorem 3.4 are preserved by conjugation. □

Although both the trace and norm will be important, the norm will play a more dominant role. The reason is that we are going to be interested in multiplicative questions (like factoring), and the norm turns multiplicative relations in $\mathcal{O}_K$ into multiplicative relations in $\mathbf{Z}$, where we are more comfortable. The next two theorems illustrate this idea.

Let $\mathcal{O}_K^\times$ denote the unit group of $\mathcal{O}_K$. Examples of units include i in $\mathbf{Z}[i]$ and $1 + \sqrt{2}$ (with inverse $\sqrt{2} - 1$) in $\mathbf{Z}[\sqrt{2}]$.

Theorem 3.9. *For any quadratic field K, $\mathcal{O}_K^\times = \{\alpha \in \mathcal{O}_K : \mathrm{N}(\alpha) = \pm 1\}$ and $\mathcal{O}_K^\times \cap \mathbf{Q} = \{\pm 1\}$.*

Proof. Let $\alpha \in \mathcal{O}_K$. If α is a unit, then $\alpha\beta = 1$ for some $\beta \in \mathcal{O}_K$. Taking norms of both sides, $\mathrm{N}(\alpha)\,\mathrm{N}(\beta) = \mathrm{N}(1) = 1$ in $\mathbf{Z}$, so $\mathrm{N}(\alpha) = \pm 1$. Conversely, assume $\mathrm{N}(\alpha) = \pm 1$. Since $\mathrm{N}(\alpha) = \alpha\overline{\alpha}$, we get $\alpha\overline{\alpha} = \pm 1$. Therefore $\pm\overline{\alpha}$ is an inverse for α, and this lies in $\mathcal{O}_K$ by Theorem 3.8.

To show $\mathcal{O}_K^\times \cap \mathbf{Q} = \{\pm 1\}$, the inclusion $\supset$ is obvious. For the inclusion $\subset$, let $q \in \mathcal{O}_K^\times \cap \mathbf{Q}$. Then $\mathrm{N}(q) = \pm 1$ since $q \in \mathcal{O}_K^\times$, so $q^2 = \pm 1$ since q is rational. Thus $q = \pm 1$. □

Example 3.10. The units in $\mathbf{Z}[\sqrt{-14}]$ are ± 1: any $a + b\sqrt{-14}$ has norm $a^2 + 14b^2$, which is never -1 and is 1 only for $a = \pm 1$ and $b = 0$.

We say a nonzero $\alpha \in \mathcal{O}_K$ is *irreducible* if α is not a unit and any factorization $\alpha = \beta\gamma$ in $\mathcal{O}_K$ requires β or γ is a unit in $\mathcal{O}_K$.

Theorem 3.11. *If $\alpha \in \mathcal{O}_K$ has a norm which is prime in $\mathbf{Z}$ then α is irreducible in $\mathcal{O}_K$.*

Proof. Suppose $\alpha = \beta\gamma$ with β and γ in $\mathcal{O}_K$. Then taking norms of both sides gives us $\mathrm{N}(\alpha) = \mathrm{N}(\beta)\,\mathrm{N}(\gamma)$ in $\mathbf{Z}$. Since $\mathrm{N}(\alpha)$ is prime, either $\mathrm{N}(\beta)$ or $\mathrm{N}(\gamma)$ is ± 1, so (by Theorem 3.9) either β or γ is a unit in $\mathcal{O}_K$. Thus α doesn't have a nontrivial factorization in $\mathcal{O}_K$, so it is irreducible. □

Example 3.12. In $\mathbf{Z}[\sqrt{-14}]$, $3 + \sqrt{-14}$ has norm 23, so $3 + \sqrt{-14}$ is irreducible in $\mathbf{Z}[\sqrt{-14}]$.

Remark 3.13. Negative primes are allowed in Theorem 3.11. For instance, in $\mathbf{Z}[\sqrt{3}]$ the norm of $1 + 2\sqrt{3}$ is -11, so $1 + 2\sqrt{3}$ is irreducible.

The criterion in Theorem 3.11 is sufficient to show an element of $\mathcal{O}_K$ is irreducible, but it is *not* necessary.

Example 3.14. In $\mathbf{Z}[\sqrt{-14}]$, $\mathrm{N}(3) = 9$ is not prime in $\mathbf{Z}$, but 3 is irreducible in $\mathbf{Z}[\sqrt{-14}]$. Indeed, suppose $3 = \alpha\beta$ in $\mathbf{Z}[\sqrt{-14}]$ with non-units α and β. Taking norms of both sides, $9 = \mathrm{N}(\alpha)\,\mathrm{N}(\beta)$ in $\mathbf{Z}$. The norms of α and β must be 3 (they are positive since norms look like a^2+14b^2, and they are not 1 since α and β are not units), but the equation $3 = a^2+14b^2$ has no solutions in $\mathbf{Z}$, so there are no elements with norm 3.

Similarly, since $\mathrm{N}(5) = 25$ and 5 is not a norm from $\mathbf{Z}[\sqrt{-14}]$, 5 is irreducible in $\mathbf{Z}[\sqrt{-15}]$.

Example 3.15. The norm of $1+\sqrt{-14}$ is 15, which factors in $\mathbf{Z}$, but $1+\sqrt{-14}$ is irreducible in $\mathbf{Z}[\sqrt{-14}]$. To see why, write $1+\sqrt{-14} = \alpha\beta$ and take norms to get $15 = \mathrm{N}(\alpha)\,\mathrm{N}(\beta)$ in $\mathbf{Z}$. Since 3 and 5 are not norms from $\mathbf{Z}[\sqrt{-14}]$, one of α or β has norm 1, so α or β is a unit.

Theorem 3.16. *Every nonzero non-unit in $\mathcal{O}_K$ is a product of irreducibles in $\mathcal{O}_K$.*

Proof. We argue by induction on $|\mathrm{N}(\alpha)|$. If $|\mathrm{N}(\alpha)| = 2$ then α has prime norm so α is irreducible and thus is its own irreducible factorization. Suppose $|\mathrm{N}(\alpha)| = n \geq 3$ and all elements with norm of absolute value from 2 to $n-1$ admit a factorization into irreducibles. If α is irreducible then it has an irreducible factorization. If α is not irreducible then we can write $\alpha = \beta\gamma$ where β and γ are not units. Therefore $|\mathrm{N}(\beta)|$ and $|\mathrm{N}(\gamma)|$ are both less than $|\mathrm{N}(\alpha)|$, so by the inductive hypothesis we have

$$\beta = \pi_1 \cdots \pi_r, \quad \gamma = \pi_1' \cdots \pi_{r'}',$$

where π_i and π_j' are irreducible in $\mathcal{O}_K$. Thus

$$\alpha = \beta\gamma = \pi_1 \cdots \pi_r \pi_1' \cdots \pi_{r'}'$$

is a product of irreducibles. □

For some quadratic fields (such as $\mathbf{Q}[i]$ and $\mathbf{Q}[\sqrt{2}]$), their integers have unique factorization into irreducibles. But very often $\mathcal{O}_K$ does not have unique factorization.

Example 3.17. In $\mathbf{Z}[\sqrt{-14}]$, 15 has the two factorizations

$$3 \cdot 5 = (1 + \sqrt{-14})(1 - \sqrt{-14}). \tag{3.4}$$

These are irreducible factorizations by Examples 3.14 and 3.15. No factor in one product is a unit multiple of a factor in the other product since the units in $\mathbf{Z}[\sqrt{-14}]$ are ± 1.

The irreducible element 3 divides $(1 + \sqrt{-14})(1 - \sqrt{-14})$, but it does not divide either factor. This is not like the behavior of primes p in $\mathbf{Z}$, where $p|ab$ always implies $p|a$ or $p|b$.

Example 3.18. Here is a much more striking instance of non-unique factorization in $\mathbf{Z}[\sqrt{-14}]$:

$$3 \cdot 3 \cdot 3 \cdot 3 = (5 + 2\sqrt{-14})(5 - 2\sqrt{-14}). \tag{3.5}$$

What makes (3.5) more interesting than (3.4) is that the number of irreducible factors on both sides is not the same. To see that $5 + 2\sqrt{-14}$ is irreducible in $\mathbf{Z}[\sqrt{-14}]$, if it has a non-unit proper factor then that factor has norm properly dividing $\mathrm{N}(5 + \sqrt{-14}) = 81$, so the norm is 3, 9, or 27. No element has norm 3 or 27, and the elements of norm 9 are ± 3, neither of which are factors of $5 + 2\sqrt{-14}$. The same proof shows $5 - 2\sqrt{-14}$ is irreducible.

Example 3.19. In $\mathbf{Z}$, when relatively prime numbers have a product that is a perfect square, the two numbers are a square up to multiplication by ± 1. This is proved using unique factorization in $\mathbf{Z}$. In $\mathbf{Z}[\sqrt{-14}]$, where there is no unique factorization, the corresponding result is false. Let's take a look at a simple example.

Consider the equation

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

The factors on the left have no common factor in $\mathbf{Z}[\sqrt{-14}]$ besides ± 1 (if $\delta|2$ and $\delta|(-7)$ then δ divides $-7(-1)-3\cdot 2 = 1$, so δ is a unit), and their product is a perfect square, but neither factor is a square up to a unit multiple: if $2 = \pm(a+b\sqrt{-14})^2 = \pm(a^2-14b^2+2ab\sqrt{-14})$ then $ab = 0$ so a or b is 0, but then $2 \neq \pm(a^2-14b^2)$. Similarly, 7 is not a square up to unit multiple.

4. Ideals

Instead of working with elements in $\mathcal{O}_K$, where unique factorization can fail, we will develop a multiplicative theory for the ideals of $\mathcal{O}_K$. We will generally denote ideals with small gothic letters like $\mathfrak{a}$ and $\mathfrak{b}$.

Theorem 4.1. *Every ideal in $\mathcal{O}_K$ is finitely generated, with at most two generators.*

Proof. An ideal in $\mathcal{O}_K$ is a subgroup of $\mathcal{O}_K$. As an additive group, $\mathcal{O}_K \cong \mathbf{Z}^2$. Therefore by the classification of finitely generated abelian groups, any subgroup of $\mathcal{O}_K$ is zero or is isomorphic to $\mathbf{Z}$ or to $\mathbf{Z}^2$. This implies that an ideal (a special kind of subgroup of $\mathcal{O}_K$) has at most 2 generators as a $\mathbf{Z}$-module, so it has at most 2 generators as an ideal (*i.e.*, as an $\mathcal{O}_K$-module). □

For a finite set of elements $\alpha_1, \ldots, \alpha_m$ in $\mathcal{O}_K$, the ideal they generate is denoted

$$\begin{aligned}(\alpha_1, \ldots, \alpha_m) &:= \{\alpha_1\gamma_1 + \cdots + \alpha_m\gamma_m : \gamma_i \in \mathcal{O}_K\} \\ &= \alpha_1\mathcal{O}_K + \cdots + \alpha_m\mathcal{O}_K.\end{aligned}$$

The order in which we write down the generators of an ideal doesn't matter, *e.g.*, $(\alpha_1, \alpha_2, \alpha_3) = (\alpha_3, \alpha_1, \alpha_2)$. What is much more important to remember, though, is that different finite sets can produce the same ideal.

Example 4.2. In $\mathbf{Z}[\sqrt{-14}]$, we will show

$$(17 + 2\sqrt{-14}, 20 + \sqrt{-14}) = (3 - \sqrt{-14}).$$

In $\mathbf{Z}[\sqrt{-14}]/(3-\sqrt{-14})$, $\sqrt{-14} = 3$. Squaring, $-14 = 9$, so $23 = 0$. Therefore $17 + 2\sqrt{-14} = 17 + 6 = 0$ and $20 + \sqrt{-14} = 23 = 0$, so $3 - \sqrt{-14}$ divides $17 + 2\sqrt{-14}$ and $20 + \sqrt{-14}$. This implies the ideal on the right is inside the ideal on the left. In $\mathbf{Z}[\sqrt{-14}]/(17+2\sqrt{-14}, 20+\sqrt{-14})$ we have $\sqrt{-14} = -20$ and $17 = -2\sqrt{-14}$. Substituting the first equation into the second, $17 = 40$, so $23 = 0$. Therefore $3 - \sqrt{-14} = 23 = 0$, so the ideal on the right is in the ideal on the left.

Example 4.3. We show the ideal $(2, \sqrt{-14})$ in $\mathbf{Z}[\sqrt{-14}]$ is not principal, by contradiction. Say $(2, \sqrt{-14}) = (\alpha)$. Then, since $2 \in (2, \sqrt{-14})$ we have $2 \in (\alpha)$, so $\alpha|2$ in $\mathbf{Z}[\sqrt{-14}]$. Writing $2 = \alpha\beta$ in $\mathbf{Z}[\sqrt{-14}]$ and taking norms, $4 = \mathrm{N}(\alpha)\,\mathrm{N}(\beta)$ in $\mathbf{Z}$, so $\mathrm{N}(\alpha)|4$ in $\mathbf{Z}$. Similarly, since $\sqrt{-14} \in (\alpha)$ we get $\mathrm{N}(\alpha)|14$ in $\mathbf{Z}$. Thus $\mathrm{N}(\alpha)$ is a common divisor of 4 and 14, so $\mathrm{N}(\alpha)$ is 1 or 2. The norm's values are $x^2 + 14y^2$ with $x, y \in \mathbf{Z}$, which is never 2. Therefore $\mathrm{N}(\alpha) = 1$, so α is a unit and $(\alpha) = (1)$. But that means $1 \in (2, \sqrt{-14})$,

contradicting the fact that every element of $(2, \sqrt{-14})$ has even norm. Hence $(2, \sqrt{-14})$ is not principal.

Since ideals can be described with different sets of generators, we will avoid defining any concept about ideals in terms of a choice of generators. However, since it is the generator description that we always make computations with, we will always try to check how a new definition looks in terms of generators for the ideals involved.

Theorem 4.4. *Let $\mathfrak{a} = (\alpha_1, \ldots, \alpha_m)$ and $\mathfrak{b} = (\beta_1, \ldots, \beta_n)$ be two ideals in $\mathcal{O}_K$. Then the following are equivalent:*

(a) $\mathfrak{a} \subset \mathfrak{b}$,
(b) *each α_i is in $\mathfrak{b}$,*
(c) *each α_i is an $\mathcal{O}_K$-linear combination of the β_j's.*

Proof. If $\mathfrak{a} \subset \mathfrak{b}$ then each α_i belongs to $\mathfrak{b}$, which means each α_i is an $\mathcal{O}_K$-linear combination of the β_j's. This shows $(a) \Rightarrow (b) \Rightarrow (c)$. Finally, if each α_i is an $\mathcal{O}_K$-linear combination of the β_j's then each α_i is in $\mathfrak{b}$, so (since $\mathfrak{b}$ is closed under $\mathcal{O}_K$-scaling and addition) any sum of $\mathcal{O}_K$-multiples of the different α_i's is in $\mathfrak{b}$. That is what a typical element of $\mathfrak{a}$ looks like, so $\mathfrak{a} \subset \mathfrak{b}$. □

Corollary 4.5. *In the notation of Theorem 4.4, we have $\mathfrak{a} = \mathfrak{b}$ if and only if every α_i is an $\mathcal{O}_K$-linear combination of the β_j's and every β_j is an $\mathcal{O}_K$-linear combination of the α_i's.*

Proof. To say $\mathfrak{a} = \mathfrak{b}$ means $\mathfrak{a} \subset \mathfrak{b}$ and $\mathfrak{b} \subset \mathfrak{a}$. Use Theorem 4.4 to interpret these inclusions in terms of linear combinations. □

Example 4.6. For α_1 and α_2 in $\mathcal{O}_K$, $(\alpha_1, \alpha_2) = (\alpha_1, \alpha_2 + \gamma\alpha_1)$ for any $\gamma \in \mathcal{O}_K$.

Example 4.7. In $\mathbf{Z}[\sqrt{-14}]$, $(2, 1 + \sqrt{-14}) = (1)$ because in $\mathbf{Z}[\sqrt{-14}]/(2, 1 + \sqrt{-14})$ we have $2 = 1 + \sqrt{-14}$, so $\sqrt{-14} = 1$. Squaring, $-14 = 1$, so $15 = 0$. Since also $2 = 0$, so $14 = 0$, we have $1 = 15 - 14 = 0$ so the quotient ring is the zero ring, which means $(2, 1 + \sqrt{-14}) = \mathbf{Z}[\sqrt{-14}] = (1)$.

Example 4.8. In $\mathbf{Z}[\sqrt{-14}]$ we will show

$$(2 + \sqrt{-14}, 7 + 2\sqrt{-14}) = (3, 1 - \sqrt{-14}).$$

In $\mathbf{Z}[\sqrt{-14}]/(2 + \sqrt{-14}, 7 + 2\sqrt{-14})$ we have $\sqrt{-14} = -2$, so $0 = 7 + 2\sqrt{-14} = 3$ and $1 - \sqrt{-14} = 1 - (-2) = 3 = 0$. Thus $(3, 1 - \sqrt{-14})$ vanishes in the quotient ring, so $(3, 1-\sqrt{-14}) \subset (2+\sqrt{-14}, 7+2\sqrt{-14})$. For the reverse inclusion, in $\mathbf{Z}[\sqrt{-14}]/(3, 1-\sqrt{-14})$ we have $\sqrt{-14} = 1$ and $3 = 0$, so $2 + \sqrt{-14} = 3 = 0$ and $7 + 2\sqrt{-14} = 9 = 0$.

Is $(3, 1 - \sqrt{-14})$ the unit ideal? No, because as in Example 4.3 a calculation shows every element of $(3, 1 - \sqrt{-14})$ has norm divisible by 3, so $1 \notin (3, 1 + \sqrt{-14})$.

Example 4.9. In $\mathbf{Z}[\sqrt{-14}]$,

$$(4 + \sqrt{-14}, 2 - \sqrt{-14}, 7 - 2\sqrt{-14}, 7 + \sqrt{-14}) = (3, 1 + \sqrt{-14}).$$

To see this, we work in $\mathbf{Z}[\sqrt{-14}]/(3, 1 + \sqrt{-14})$. In this ring, $\sqrt{-14} = -1$ and $3 = 0$. Each generator in the ideal on the left vanishes in this ring, so the ideal on the left is contained in the ideal on the right. For the reverse inclusion, $-2(2 - \sqrt{-14}) + (7 - 2\sqrt{-14}) = 3$ and $2(4 + \sqrt{-14}) - (7 + \sqrt{-14}) = 1 + \sqrt{-14}$.

Theorem 4.10. *If an ideal in $\mathcal{O}_K$ contains two elements of $\mathbf{Z}$ which are relatively prime then the ideal is the unit ideal. In particular, an ideal is the unit ideal if it contains two elements whose norms are relatively prime in $\mathbf{Z}$.*

Proof. Let $\mathfrak{a}$ be an ideal and a and b be elements of $\mathfrak{a}$ which are in $\mathbf{Z}$ and relatively prime. We can write $1 = ax + by$ for some x and y in $\mathbf{Z}$. The right side is in $\mathfrak{a}$, so $1 \in \mathfrak{a}$, so $\mathfrak{a} = (1)$.

Since the norm of any $\alpha \in \mathfrak{a}$ is also in $\mathfrak{a}$ (because $\mathrm{N}(\alpha)$ is a multiple of α and ideals contain any multiple of their elements), two relatively prime norms of elements in $\mathfrak{a}$ are themselves elements of $\mathfrak{a}$. So $\mathfrak{a} = (1)$ by the previous paragraph. □

Theorem 4.11. *Any ideal in $\mathcal{O}_K$ which has a set of generators from $\mathbf{Z}$ is a principal ideal.*

Proof. Let $\mathfrak{a} = (a_1, \ldots, a_m)$ where $a_i \in \mathbf{Z}$. Let d be the greatest common divisor of the a_i's in $\mathbf{Z}$. Then every a_i is a $\mathbf{Z}$-multiple of d, so any element of $\mathfrak{a}$ is divisible by d in $\mathcal{O}_K$. This shows $\mathfrak{a} \subset (d) = d\mathcal{O}_K$. Conversely, since $\mathbf{Z}$ is a PID it is possible to write $d = c_1a_1 + \cdots + c_ma_m$ for some $c_i \in \mathbf{Z}$, so any $\mathcal{O}_K$-multiple of d is an $\mathcal{O}_K$-linear combination of the a_i's. This shows $(d) \subset \mathfrak{a}$, so $\mathfrak{a} = (d)$. □

The point of Theorem 4.11 is that it tells us that if we happen to find an ideal with generators all taken from $\mathbf{Z}$, we can write the ideal in a much simpler form with a single generator from $\mathbf{Z}$. This will play a role in the key theorem about ideals (Theorem 5.4).

Theorem 4.12. *For α and β in $\mathcal{O}_K$, $(\alpha) = (\beta)$ if and only if α and β are equal up to multiplication by a unit in $\mathcal{O}_K$.*

Proof. Equality of (α) and (β) is equivalent to $\alpha|\beta$ and $\beta|\alpha$, which is equivalent to α and β being unit multiples, by cancellation. This includes the case when they are both 0. □

Now we define multiplication of ideals.

Definition 4.13. For ideals $\mathfrak{a}$ and $\mathfrak{b}$ in $\mathcal{O}_K$, the *product* $\mathfrak{ab}$ is the set of all finite sums $\sum_{k=1}^{r} x_k y_k$, with $r \geq 1$, $x_k \in \mathfrak{a}$ and $y_k \in \mathfrak{b}$.

Where does this definition come from? Well, whatever the product of $\mathfrak{a}$ and $\mathfrak{b}$ ought to mean, it should at least be an ideal containing the pairwise products xy where $x \in \mathfrak{a}$ and $y \in \mathfrak{b}$. Then, since an ideal has to be closed under addition, the product of $\mathfrak{a}$ and $\mathfrak{b}$ should include all finite sums $\sum_{k=1}^{r} x_k y_k$ with $x_k \in \mathfrak{a}$ and $y_k \in \mathfrak{b}$. This is exactly what Definition 4.13 is about, and $\mathfrak{ab}$ is an ideal in $\mathcal{O}_K$. The following theorem describes multiplication of ideals in terms of generators.

Theorem 4.14. *If $\mathfrak{a} = (\alpha_1, \ldots, \alpha_m)$ and $\mathfrak{b} = (\beta_1, \ldots, \beta_n)$ then*

$$\mathfrak{ab} = (\alpha_1\beta_1, \ldots, \alpha_i\beta_j, \ldots, \alpha_m\beta_n).$$

In particular, $(\alpha)(\beta) = (\alpha\beta)$.

Proof. Any element of $\mathfrak{ab}$ has the form $x_1y_1 + \cdots + x_ry_r$ where $x_k \in \mathfrak{a}$ and $y_k \in \mathfrak{b}$. We can write each x_k as an $\mathcal{O}_K$-linear combination of the α_i's and each y_k as an $\mathcal{O}_K$-linear combination of the β_j's. Multiplying out the product x_ky_k shows it is an $\mathcal{O}_K$-linear combination of the $\alpha_i\beta_j$'s. Then a sum of such products is another $\mathcal{O}_K$-linear combination of the $\alpha_i\beta_j$'s, so the elements of $\mathfrak{ab}$ do lie in the ideal $(\alpha_1\beta_1, \ldots, \alpha_i\beta_j, \ldots, \alpha_m\beta_n)$. Conversely, every element of this ideal is an $\mathcal{O}_K$-linear combination of the $\alpha_i\beta_j$'s, so it is a sum

$$\sum_{i=1}^{m}\sum_{j=1}^{n} \gamma_{ij}\alpha_i\beta_j \tag{4.1}$$

where $\gamma_{ij} \in \mathcal{O}_K$. Since $\gamma_{ij}\alpha_i \in \mathfrak{a}$ and $\beta_j \in \mathfrak{b}$, the sum (4.1) is of the form $\sum_{k=1}^{r} x_k y_k$ with $x_k \in \mathfrak{a}$ and $y_k \in \mathfrak{b}$, so the sum belongs to $\mathfrak{ab}$. □

Notice that even though we know all ideals require at most two generators (Theorem 4.1), the simplest description of generators for a product of ideals will use more than two generators. This is why our treatment of ideals has to allow generating sets of size greater than 2.

Example 4.15. We compute a product of ideals in $\mathbf{Z}[\sqrt{-14}]$. Let $\mathfrak{a} = (5+\sqrt{-14}, 2+\sqrt{-14})$ and $\mathfrak{b} = (4+\sqrt{-14}, 2-\sqrt{-14})$. Then

$$\begin{aligned}\mathfrak{ab} &= (5+\sqrt{-14}, 2+\sqrt{-14})(4+\sqrt{-14}, 2-\sqrt{-14}) \\ &= (6+9\sqrt{-14}, -6+6\sqrt{-14}, 24-3\sqrt{-14}, 18).\end{aligned}$$

It is left as an exercise to show this ideal equals $(6, 3\sqrt{-14})$.

Corollary 4.16. *For ideals $\mathfrak{a}$ and $\mathfrak{b}$, $\mathfrak{ab} = (0)$ if and only if $\mathfrak{a} = (0)$ or $\mathfrak{b} = (0)$.*

Proof. If $\mathfrak{a} = (0)$ or $\mathfrak{b} = (0)$ then the product $\mathfrak{ab}$ is (0) from the formula in Theorem 4.14. If $\mathfrak{a} \neq (0)$ and $\mathfrak{b} \neq (0)$, then $\mathfrak{a}$ has a nonzero element x and $\mathfrak{b}$ has a nonzero element y. Then $\mathfrak{ab}$ contains xy, which is not zero, so $\mathfrak{ab} \neq (0)$. □

Theorem 4.17. *Multiplication of ideals is commutative and associative. That is, for ideals $\mathfrak{a}$, $\mathfrak{b}$, and $\mathfrak{c}$ in $\mathcal{O}_K$,*

$$\mathfrak{ab} = \mathfrak{ba}, \quad (\mathfrak{ab})\mathfrak{c} = \mathfrak{a}(\mathfrak{bc}).$$

The unit ideal (1) is a multiplicative identity.

Proof. The product $\mathfrak{ab}$ is the ideal with generators xy where $x \in \mathfrak{a}$ and $y \in \mathfrak{b}$. The product $\mathfrak{ba}$ has generators yx for $y \in \mathfrak{b}$ and $x \in \mathfrak{a}$. These are the same sets of generators, so $\mathfrak{ab} = \mathfrak{ba}$. The rest of the proof is left to the reader. □

Corollary 4.18. *For an ideal $\mathfrak{a} = (\alpha_1, \ldots, \alpha_m)$ and a principal ideal (γ),*

$$(\gamma)\mathfrak{a} = (\gamma\alpha_1, \ldots, \gamma\alpha_m).$$

Proof. Left to the reader. □

Example 4.19. In Example 4.3 we showed the ideal $(2, \sqrt{-14})$ in $\mathbf{Z}[\sqrt{-14}]$ is not principal. We will show this in a different way now. Squaring the ideal,

$$(2, \sqrt{-14})^2 = (2, \sqrt{-14})(2, \sqrt{-14}) = (4, 2\sqrt{-14}, -14) = (2)(2, \sqrt{-14}, -7).$$

Since 2 and 7 are relatively prime in $\mathbf{Z}$, $(2, \sqrt{-14}, -7) = (1)$ by Theorem 4.10. Therefore

$$(2, \sqrt{-14})^2 = (2)(1) = (2). \tag{4.2}$$

If $(2, \sqrt{-14}) = (\alpha)$ then $(2) = (\alpha)^2 = (\alpha^2)$, so $\alpha^2 = \pm 2$. Taking norms, $\mathrm{N}(\alpha)^2 = 4$, so $\mathrm{N}(\alpha) = 2$. But no element of $\mathbf{Z}[\sqrt{-14}]$ has norm 2, so we have a contradiction.

Definition 4.20. For an ideal $\mathfrak{a}$, its conjugate ideal is $\overline{\mathfrak{a}} := \{\overline{\alpha} : \alpha \in \mathfrak{a}\}$.

What does this mean in terms of specific generators?

Theorem 4.21. *If $\mathfrak{a} = (\alpha_1, \ldots, \alpha_m)$ then $\overline{\mathfrak{a}} = (\overline{\alpha}_1, \ldots, \overline{\alpha}_m)$. In particular, if $\mathfrak{a} = (\alpha)$ is principal then $\overline{\mathfrak{a}} = (\overline{\alpha})$ is also principal. For any ideals $\mathfrak{a}$ and $\mathfrak{b}$, $\overline{\mathfrak{ab}} = \overline{\mathfrak{a}}\,\overline{\mathfrak{b}}$ and $\overline{\overline{\mathfrak{a}}} = \mathfrak{a}$.*

Proof. An element of $\mathfrak{a}$ has the form $\sum_{i=1}^m \gamma_i\alpha_i$ with $\gamma_i \in \mathcal{O}_K$. Its conjugate is $\sum_{i=1}^m \overline{\gamma}_i\overline{\alpha}_i$, so $\overline{\mathfrak{a}} \subset (\overline{\alpha}_1, \ldots, \overline{\alpha}_m)$. Any element of $(\overline{\alpha}_1, \ldots, \overline{\alpha}_m)$ is a sum $\sum_{i=1}^m \delta_i\overline{\alpha}_i$, which is the conjugate of $\sum_{i=1}^m \overline{\delta}_i\alpha_i \in \mathfrak{a}$, so $(\overline{\alpha}_1, \ldots, \overline{\alpha}_m) \subset \overline{\mathfrak{a}}$. Thus $\overline{\mathfrak{a}} \subset (\overline{\alpha}_1, \ldots, \overline{\alpha}_m)$.

The rest of the theorem is left to the reader to prove. □

Example 4.22. When an *element* of $\mathcal{O}_K$ is equal to its conjugate then it is in $\mathbf{Z}$. But when an *ideal* in $\mathcal{O}_K$ is equal to its conjugate, it need not be an ideal with generators from $\mathbf{Z}$. For instance, in $\mathbf{Z}[\sqrt{-14}]$ we have $\overline{(2, \sqrt{-14})} = (2, -\sqrt{-14}) = (2, \sqrt{-14})$, so the ideal $(2, \sqrt{-14})$ is equal to its conjugate. This ideal does not have a set of generators from $\mathbf{Z}$, since if it did then it would be a principal ideal (Theorem 4.11) and we know this ideal is not principal (Example 4.3).

Example 4.23. We will prove that the ideal $(3, 1+\sqrt{-14})$ in $\mathbf{Z}[\sqrt{-14}]$ is not principal and not equal to its conjugate ideal. To begin, we check that

$$(3, 1 + \sqrt{-14})(3, 1 - \sqrt{-14}) = (3). \tag{4.3}$$

Multiplying together the generators,

$$\begin{aligned}(3, 1 + \sqrt{-14})(3, 1 - \sqrt{-14}) &= (9, 3 - 3\sqrt{-14}, 3 + 3\sqrt{-14}, 15)\\ &= (3)(3, 1 - \sqrt{-14}, 1 + \sqrt{-14}, 5),\end{aligned}$$

and the second ideal on the right contains 3 and 5, which are relatively prime in $\mathbf{Z}$, so the second ideal is (1). Thus $(3, 1+\sqrt{-14})(3, 1-\sqrt{-14}) = (3)(1) = (3)$ and (4.3) is established.

Suppose, to argue by contradiction, that $(3, 1 + \sqrt{-14}) = (\alpha)$ is a principal ideal. Then (4.3) becomes $(\alpha)(\overline{\alpha}) = (3)$. The product $(\alpha)(\overline{\alpha})$ is $(\alpha\overline{\alpha}) = (\mathrm{N}(\alpha))$, so for this to be (3) requires $\mathrm{N}(\alpha) = \pm 3$. But norms on $\mathbf{Z}[\sqrt{-14}]$ are positive and never equal 3. (The equation $x^2 + 14y^2 = 3$ has no solutions in $\mathbf{Z}$.) Hence we have a contradiction and $(3, 1 + \sqrt{-14})$ is not principal.

To show $(3, 1 + \sqrt{-14})$ does not equal its conjugate ideal, assume otherwise. Then (4.3) becomes $(3, 1+\sqrt{-14})^2 = (3)$. But we can compute the square of that ideal independently:

$$\begin{aligned}(3, 1 + \sqrt{-14})^2 &= (3, 1 + \sqrt{-14})(3, 1 + \sqrt{-14})\\ &= (9, 3 + 3\sqrt{-14}, -13 + 2\sqrt{-14}).\end{aligned}$$

This is not (3) since $-13 + 2\sqrt{-14} \notin (3)$: multiples of 3 in $\mathbf{Z}[\sqrt{-14}]$ have the coefficients of 1 and $\sqrt{-14}$ both divisible by 3.

Having spent some time with multiplication of ideals, we turn to divisibility of ideals.

Definition 4.24. Set $\mathfrak{a}|\mathfrak{b}$ if $\mathfrak{b} = \mathfrak{a}\mathfrak{c}$ for some ideal $\mathfrak{c}$. We say $\mathfrak{a}$ *divides* $\mathfrak{b}$ and that $\mathfrak{b}$ is a multiple of $\mathfrak{a}$, or that $\mathfrak{a}$ is a factor or divisor of $\mathfrak{b}$.

The first important property of ideal divisibility is that, on principal ideals, it exactly reflects divisibility of the generators as elements of $\mathcal{O}_K$.

Theorem 4.25. *For α and β in $\mathcal{O}_K$, $(\alpha)|(\beta)$ if and only if $\alpha|\beta$.*

Proof. Suppose $\alpha|\beta$ in $\mathcal{O}_K$. Then $\beta = \alpha\gamma$ for some $\gamma \in \mathcal{O}_K$, so $(\beta) = (\alpha\gamma) = (\alpha)(\gamma)$. Thus $(\alpha)|(\beta)$. Conversely, if $(\alpha)|(\beta)$ then $(\beta) = (\alpha)\mathfrak{c}$ for some ideal $\mathfrak{c}$. Write $\mathfrak{c} = (\gamma_1, \ldots, \gamma_r)$, so

$$(\beta) = (\alpha\gamma_1, \ldots, \alpha\gamma_r).$$

Then β is an $\mathcal{O}_K$-linear combination of the products $\alpha\gamma_k$:

$$\beta = \sum_{k=1}^{r} \delta_k \alpha\gamma_k = \alpha \sum_{k=1}^{r} \delta_k \gamma_k,$$

so $\alpha|\beta$ in $\mathcal{O}_K$. □

Theorem 4.26. *For $\alpha \in \mathcal{O}_K$ and ideal $\mathfrak{b} = (\beta_1, \ldots, \beta_m)$ in $\mathcal{O}_K$, the following are equivalent:*

- $(\alpha)|\mathfrak{b}$,
- $\alpha|\beta_j$ *for all* j,
- $(\alpha) \supset \mathfrak{b}$.

Proof. If $(\alpha)|\mathfrak{b}$ then $\mathfrak{b} = (\alpha)\mathfrak{c}$ for some ideal $\mathfrak{c}$. Write $\mathfrak{c} = (\gamma_1, \ldots, \gamma_n)$, so $\mathfrak{b} = (\alpha\gamma_1, \ldots, \alpha\gamma_n)$. It follows that every element of $\mathfrak{b}$ is divisible by α, so in particular $\alpha|\beta_j$ for each j. Therefore $\beta_j \in (\alpha)$ for all j, so $\mathfrak{b} \subset (\alpha)$. Finally, from this inclusion we can write each β_j as a multiple of α, so $\mathfrak{b}$ has the ideal (α) as a factor. □

Theorem 4.27. *For ideals $\mathfrak{a}$ and $\mathfrak{b}$, if $\mathfrak{a}|\mathfrak{b}$ then $\mathfrak{a} \supset \mathfrak{b}$. In particular, if $\mathfrak{a}|\mathfrak{b}$ and $\mathfrak{b}|\mathfrak{a}$ then $\mathfrak{a} = \mathfrak{b}$.*

Proof. Suppose $\mathfrak{a}|\mathfrak{b}$, say $\mathfrak{b} = \mathfrak{a}\mathfrak{c}$. Ideals are $\mathcal{O}_K$-modules, so $\mathfrak{a}\mathfrak{c} \subset \mathfrak{a}$. □

Let's summarize the situation right now. We have replaced multiplication and divisibility among elements of $\mathcal{O}_K$ with multiplication and divisibility among ideals in $\mathcal{O}_K$. Insofar as elements of $\mathcal{O}_K$ are concerned, their multiplicative and divisibility relations are accurately reflected in the behavior of the principal ideals they generate. This is what the end of Theorem 4.14 and Theorem 4.25 tell us. (Moreover, by Theorem 4.12, replacing elements with principal ideals lets us suppress unit multiple ambiguities.) What do we gain by using ideals in place of elements? We can save unique factorization!

Example 4.28. Let $\mathfrak{p} = (3, 1 + \sqrt{-14})$ and $\mathfrak{q} = (5, 1 + \sqrt{-14})$. We saw in (4.3) that $(3) = \mathfrak{p}\overline{\mathfrak{p}}$. In a similar way, $(5) = \mathfrak{q}\overline{\mathfrak{q}}$, $\mathfrak{p}\mathfrak{q} = (1 + \sqrt{-14})$, and $\overline{\mathfrak{p}}\overline{\mathfrak{q}} = (1 - \sqrt{-14})$. Then the principal ideal (15) can be factored as

$$(15) = (3)(5) = \mathfrak{p}\overline{\mathfrak{p}}\mathfrak{q}\overline{\mathfrak{q}}$$

and as

$$(15) = (1 + \sqrt{-14})(1 - \sqrt{-14}) = \mathfrak{p}\mathfrak{q}\overline{\mathfrak{p}}\overline{\mathfrak{q}}.$$

From the viewpoint of factoring the element 15, (3.4) shows it has non-unique irreducible factorizations. But if we replace those irreducible factors by the principal ideals they generate, they no longer look irreducible (each of the principal ideals $(3), (5), (1 + \sqrt{-14})$, and $(1 - \sqrt{-14})$ factors into a product of ideals as described just above with $\mathfrak{p}$, $\mathfrak{q}$, and their conjugate ideals) and in fact the non-unique factorization disappears: all that is happening on the level of ideals is that certain (non-principal) ideals are being multiplied in different ways. Similarly, (3.5) is not strange on the level of ideal factorizations, since $(3)^4 = \mathfrak{p}^4\overline{\mathfrak{p}}^4$, $(5 + 2\sqrt{-14}) = \mathfrak{p}^4$, and $(5 - 2\sqrt{-14}) = \overline{\mathfrak{p}}^4$ for $\mathfrak{p}$ as above. (It is left to the reader to check these formulas for $\mathfrak{p}^4$ and $\overline{\mathfrak{p}}^4$. As a first step, check $\mathfrak{p}^2 = (9, 2 - \sqrt{-14})$.)

Example 4.29. In $\mathbf{Z}[\sqrt{-14}]$, $2 \cdot (-7) = \sqrt{-14}^2$ is a perfect square and 2 and -7 have no common factors, but 2 and -7 are not perfect squares up to unit multiple (Example 3.19).

This mysterious state of affairs is explained when we pass to ideals. Let $\mathfrak{a} = (2, \sqrt{-14})$ and $\mathfrak{b} = (7, \sqrt{-14})$. Then $(2) = \mathfrak{a}^2$ (see (4.2)), $(-7) = (7) = \mathfrak{b}^2$, and

$$\mathfrak{ab} = (14, 2\sqrt{-14}, 7\sqrt{-14}, -14) = (\sqrt{-14})(\sqrt{-14}, 2, 7, \sqrt{-14}) = (\sqrt{-14}),$$

so passing from elements to the principal ideals they generate turns the equation $2 \cdot (-7) = \sqrt{-14}^2$ into $\mathfrak{a}^2\mathfrak{b}^2 = (\mathfrak{ab})^2$, and now what we expect should be squares are squares, as ideals.

Our main goal is to show that nonzero ideals in $\mathcal{O}_K$ admit unique factorization into prime ideals. The first step, in the next section, is to establish an analogue for ideals of the cancellation law for non-zero integers.

5. Cancelling ideals

Definition 5.1. An ideal $\mathfrak{c}$ in $\mathcal{O}_K$ is called *cancelable* if whenever $\mathfrak{ac} = \mathfrak{bc}$ for ideals $\mathfrak{a}$ and $\mathfrak{b}$ in $\mathcal{O}_K$ we have $\mathfrak{a} = \mathfrak{b}$.

Obviously the zero ideal (0) is not cancelable, for the same reason the element 0 can't be cancelled.

Theorem 5.2. *Nonzero principal ideals are cancelable. That is, for nonzero γ in $\mathcal{O}_K$ and ideals $\mathfrak{a}$ and $\mathfrak{b}$, if $\mathfrak{a}(\gamma) = \mathfrak{b}(\gamma)$ then $\mathfrak{a} = \mathfrak{b}$.*

Proof. We will show $\mathfrak{a} \subset \mathfrak{b}$. The reverse inclusion is handled similarly.

It is not hard to see that $\mathfrak{a}(\gamma) = \gamma\mathfrak{a}$ is the set of multiples of $\mathfrak{a}$ by γ. Since we can cancel γ as a common factor in products, the relations $\gamma\mathfrak{a} = \gamma\mathfrak{b}$ and $\mathfrak{a} = \mathfrak{b}$ are clearly equivalentl □

Corollary 5.3. *Any nonzero ideal in $\mathcal{O}_K$ with a nonzero principal multiple is cancelable.*

Proof. Let $\mathfrak{c}$ be an ideal with a nonzero principal multiple, say $\mathfrak{cc}' = (\gamma)$ with $\gamma \neq 0$. Then if $\mathfrak{ac} = \mathfrak{bc}$, multiply both sides by $\mathfrak{c}'$ to get $\mathfrak{a}(\gamma) = \mathfrak{b}(\gamma)$, so $\mathfrak{a} = \mathfrak{b}$ by Theorem 5.2. □

It turns out that *every* nonzero ideal in $\mathcal{O}_K$ has a nonzero principal multiple, so by Corollary 5.3 every nonzero ideal in $\mathcal{O}_K$ is cancelable. We're going to show ideals have principal multiples using conjugate ideals. Here is the key result.

Theorem 5.4. *For any ideal $\mathfrak{a}$ in $\mathcal{O}_K$, the product $\mathfrak{a}\overline{\mathfrak{a}}$ is a principal ideal.*

Up to this point, we have not used Theorem 3.4, which explicitly describes all of the integers of K. For instance, we could have done everything so far in $\mathbf{Z}[\sqrt{d}]$ (defining ideals in $\mathbf{Z}[\sqrt{d}]$ using $\mathbf{Z}[\sqrt{d}]$-linear combinations, principal ideals, conjugate ideals, and ideal multiplication), even when $\mathcal{O}_K \neq \mathbf{Z}[\sqrt{d}]$, without running into a problem. But to prove Theorem 5.4 we are going to construct some elements about which all we know is that they are in $\mathcal{O}_K$. If $\mathcal{O}_K \neq \mathbf{Z}[\sqrt{d}]$ then Theorem 5.4 is *false* for $\mathbf{Z}[\sqrt{d}]$.

Example 5.5. When $d \equiv 1 \bmod 4$, so $\mathcal{O}_K \neq \mathbf{Z}[\sqrt{d}]$, we have the following equality of ideals in $\mathbf{Z}[\sqrt{d}]$:

$$\begin{aligned}(2, 1+\sqrt{d})(2, 1+\sqrt{d}) &= (4, 2(1+\sqrt{d})) \\ &= (4, 2+2\sqrt{d}) \\ &= (2)(2, 1+\sqrt{d}).\end{aligned}$$

If Theorem 5.4 were true for the ideal $(2, 1+\sqrt{d})$ then Corollary 5.3 would imply that this ideal in $\mathbf{Z}[\sqrt{d}]$ is cancelable. But then when we cancel this ideal in the equation $(2, 1+\sqrt{d})^2 = (2)(2, 1+\sqrt{d})$ we'd get $(2, 1+\sqrt{d}) = (2)$, which is false since $1+\sqrt{d} \notin 2\mathbf{Z}[\sqrt{d}]$.

If we work in $\mathcal{O}_K = \mathbf{Z}[(1+\sqrt{d})/2]$ then the non-cancelable aspect disappears because $(2, 1+\sqrt{d}) = (2)(1,(1+\sqrt{d})/2) = (2)$.

Our approach to Theorem 5.4 relies on the following theorem, which is the heart of the approach and is the first time we need the trace in the context of ideals.

Theorem 5.6. *Let $\mathfrak{a} = (\alpha, \beta)$ be an ideal in $\mathcal{O}_K$ with two generators. Then*

$$\mathfrak{a}\overline{\mathfrak{a}} = (\mathrm{N}(\alpha), \mathrm{Tr}(\alpha\overline{\beta}), \mathrm{N}(\beta)).$$

Proof. If α or β is 0 then the theorem is easy. We may assume α and β are nonzero.

By a direct computation,

$$\mathfrak{a}\overline{\mathfrak{a}} = (\alpha,\beta)(\overline{\alpha},\overline{\beta}) = (\alpha\overline{\alpha}, \alpha\overline{\beta}, \beta\overline{\alpha}, \beta\overline{\beta}) = (\mathrm{N}(\alpha), \alpha\overline{\beta}, \overline{\alpha}\beta, \mathrm{N}(\beta)).$$

We want to show

$$(\mathrm{N}(\alpha), \alpha\overline{\beta}, \overline{\alpha}\beta, \mathrm{N}(\beta)) = (\mathrm{N}(\alpha), \mathrm{Tr}(\alpha\overline{\beta}), \mathrm{N}(\beta)).$$

Since $\mathrm{Tr}(\alpha\overline{\beta}) = \alpha\overline{\beta} + \overline{\alpha}\beta$, the ideal on the right is inside the ideal on the left. For the reverse inclusion, we need to show $\alpha\overline{\beta}$ and $\overline{\alpha}\beta$ are in the ideal on the right. We will give the argument for $\alpha\overline{\beta}$, in two different ways.

Our first method is based on [1, p. 276]. Let d be the greatest common divisor of $\mathrm{N}(\alpha), \mathrm{Tr}(\alpha\overline{\beta})$, and $\mathrm{N}(\beta)$ in $\mathbf{Z}$. So d is a factor of all three numbers and, moreover, it is a $\mathbf{Z}$-linear combination of them. Therefore $(\mathrm{N}(\alpha), \mathrm{Tr}(\alpha\overline{\beta}), \mathrm{N}(\beta)) = (d)$, so we need to show $\alpha\overline{\beta} \in (d) = d\mathcal{O}_K$. Using the definition of integers of K, we check that $\alpha\overline{\beta}/d$ has trace and norm in $\mathbf{Z}$. It trace is

$$\mathrm{Tr}\left(\frac{\alpha\overline{\beta}}{d}\right) = \frac{\alpha\overline{\beta} + \overline{\alpha}\beta}{d} = \frac{\mathrm{Tr}(\alpha\overline{\beta})}{d},$$

which is in $\mathbf{Z}$ since d is a factor of $\mathrm{Tr}(\alpha\overline{\beta})$. Its norm is

$$\mathrm{N}\left(\frac{\alpha\overline{\beta}}{d}\right) = \frac{\alpha\overline{\beta}\overline{\alpha}\beta}{d^2} = \frac{\mathrm{N}(\alpha)}{d}\frac{\mathrm{N}(\beta)}{d},$$

which is in $\mathbf{Z}$ since d is a factor of the norms of α and β.

Our second proof that $\alpha\overline{\beta} \in (\mathrm{N}(\alpha), \mathrm{Tr}(\alpha\overline{\beta}), \mathrm{N}(\beta))$ will follow notes of Stark [3], which were meant to be Chapter 9 of [2] if a second edition of [2] ever appeared. Let $\gamma = \alpha/\beta \in K = \mathbf{Q}[\sqrt{d}]$. It is a root of

$$\begin{aligned}(X-\gamma)(X-\overline{\gamma}) &= X^2 - (\gamma+\overline{\gamma})X + \gamma\overline{\gamma} \\ &= X^2 - \left(\frac{\alpha\overline{\beta}+\overline{\alpha}\beta}{\beta\overline{\beta}}\right)X + \frac{\mathrm{N}(\alpha)}{\mathrm{N}(\beta)} \\ &= X^2 - \frac{\mathrm{Tr}(\alpha\overline{\beta})}{\mathrm{N}(\beta)}X + \frac{\mathrm{N}(\alpha)}{\mathrm{N}(\beta)}.\end{aligned}$$

Let c be the least common denominator of $\mathrm{Tr}(\alpha\overline{\beta})/\mathrm{N}(\beta)$ and $\mathrm{N}(\alpha)/\mathrm{N}(\beta)$ and write

$$\frac{\mathrm{N}(\alpha)}{\mathrm{N}(\beta)} = \frac{a}{c}, \quad \frac{\mathrm{Tr}(\alpha\overline{\beta})}{\mathrm{N}(\beta)} = \frac{b}{c},$$

where $a, b, c \in \mathbf{Z}$ have no common factor greater than 1. Then

$$\mathrm{N}(\alpha) = ka, \quad \mathrm{Tr}(\alpha\overline{\beta}) = kb, \quad \mathrm{N}(\beta) = kc$$

for some integer k, so

$$(\mathrm{N}(\alpha), \mathrm{Tr}(\alpha\overline{\beta}), \mathrm{N}(\beta)) = (ka, kb, kc) = (k)(a,b,c) = (k)(1) = (k). \tag{5.1}$$

Since

$$\gamma^2 - \frac{b}{c}\gamma + \frac{a}{c} = 0 \Longrightarrow (c\gamma)^2 - b(c\gamma) + ac = 0,$$

$c\gamma = c\alpha/\beta$ is the root of a quadratic with integer coefficients and leading coefficient 1. Therefore $c\alpha/\beta \in \mathcal{O}_K$ by Theorem 3.5. At the same time, $c\alpha/\beta = c\alpha\overline{\beta}/\mathrm{N}(\beta) = \alpha\overline{\beta}/k$, so $\alpha\overline{\beta} \in k\mathcal{O}_K = (k)$. By (5.1), $\alpha\overline{\beta} \in (\mathrm{N}(\alpha), \mathrm{Tr}(\alpha\overline{\beta}), \mathrm{N}(\beta))$. □

Here is a generalization of Theorem 5.6 to ideals described by more than two generators. (No ideal in $\mathcal{O}_K$ needs more than two generators, but ideals which arise from a calculation might have more than two generators.)

Theorem 5.7. *If $\mathfrak{a} = (\alpha_1, \ldots, \alpha_m)$ has m generators then $\mathfrak{a}\overline{\mathfrak{a}}$ is generated by the m integers $\mathrm{N}(\alpha_1), \ldots, \mathrm{N}(\alpha_m)$ and $\frac{m(m-1)}{2}$ integers $\mathrm{Tr}(\alpha_i\overline{\alpha}_j)$ where $i < j$.*

Proof. The case $m = 1$ is easy. The case $m = 2$ is Theorem 5.6. We will use the case $m = 2$ to handle more generators. By a direct calculation,

$$\begin{aligned} \mathfrak{a}\overline{\mathfrak{a}} &= (\alpha_1, \ldots, \alpha_m)(\overline{\alpha}_1, \ldots, \overline{\alpha}_m) \\ &= (\mathrm{N}(\alpha_1), \ldots, \mathrm{N}(\alpha_m), \alpha_1\overline{\alpha}_2, \alpha_2\overline{\alpha}_1, \ldots, \alpha_i\overline{\alpha}_j, \alpha_j\overline{\alpha}_i, \ldots), \end{aligned}$$

where $i < j$. By Theorem 5.6, the four numbers $\mathrm{N}(\alpha_i), \alpha_i\overline{\alpha}_j, \alpha_j\overline{\alpha}_i, \mathrm{N}(\alpha_j)$ and the three numbers $\mathrm{N}(\alpha_i), \mathrm{Tr}(\alpha_i\overline{\alpha}_j), \mathrm{N}(\alpha_j)$ are $\mathcal{O}_K$-linear combinations of each other. Therefore we can replace $\alpha_i\overline{\alpha}_j$ and $\alpha_j\overline{\alpha}_i$ with $\mathrm{Tr}(\alpha_i\overline{\alpha}_j)$ in the generating set for $\mathfrak{a}\overline{\mathfrak{a}}$, and that concludes the proof. □

Now we can prove Theorem 5.4 very quickly.

Proof. By Theorem 5.7, $\mathfrak{a}\overline{\mathfrak{a}}$ has a set of generators from $\mathbf{Z}$. Therefore $\mathfrak{a}\overline{\mathfrak{a}}$ is principal by Theorem 4.11. □

Here is a simple but useful application of Theorem 5.4.

Theorem 5.8. *For ideals $\mathfrak{a}$ and $\mathfrak{b}$ in $\mathcal{O}_K$, $\mathfrak{a}|\mathfrak{b}$ if and only if $\mathfrak{a} \supset \mathfrak{b}$.*

Proof. When $\mathfrak{a} = (0)$, we have $(0)|\mathfrak{b} \Leftrightarrow \mathfrak{b} = (0) \Leftrightarrow (0) \supset \mathfrak{b}$. So we may suppose $\mathfrak{a} \neq (0)$. By Theorem 4.27, $\mathfrak{a}|\mathfrak{b} \Rightarrow \mathfrak{a} \supset \mathfrak{b}$. Now assume $\mathfrak{a} \supset \mathfrak{b}$. Then $\mathfrak{a}\overline{\mathfrak{a}} \supset \mathfrak{b}\overline{\mathfrak{a}}$. Write $\mathfrak{a}\overline{\mathfrak{a}} = (a)$ (by Theorem 5.4), so $(a) \supset \mathfrak{b}\overline{\mathfrak{a}}$. By Theorem 4.26, $(a)|\mathfrak{b}\overline{\mathfrak{a}}$, so $(a)\mathfrak{c} = \mathfrak{b}\overline{\mathfrak{a}}$. Now multiply by $\mathfrak{a}$: $(a)\mathfrak{c}\mathfrak{a} = \mathfrak{b}(a)$. Cancelling (a), which is not (0), gives $\mathfrak{a}\mathfrak{c} = \mathfrak{b}$, so $\mathfrak{a}|\mathfrak{b}$. □

The slogan to remember Theorem 5.8 by is "to contain is to divide." This is especially useful to keep in mind because the divisibility and inclusion relations are reversed: the factor is the larger ideal.

Corollary 5.9. *The divisors of an ideal $\mathfrak{a}$ are precisely the ideals $\mathfrak{d}$ satisfying $\mathfrak{d} \supset \mathfrak{a}$. In particular, $\alpha \in \mathfrak{a}$ if and only if $\mathfrak{a}|(\alpha)$.*

Proof. This is immediate from Theorem 5.8. □

Since the ideals dividing $\mathfrak{a}$ are the ideals containing $\mathfrak{a}$, it is very easy to create divisors of $\mathfrak{a}$: if $\mathfrak{a} = (\alpha_1, \ldots, \alpha_m)$ and $\alpha \notin \mathfrak{a}$, then $(\alpha_1, \ldots, \alpha_m, \alpha)$ is an ideal properly containing $\mathfrak{a}$, so this ideal is a proper factor of $\mathfrak{a}$. Of course, if we're not careful this factor is likely to be (1).

Definition 5.10. The sum of two ideals $\mathfrak{a}$ and $\mathfrak{b}$ is

$$\mathfrak{a} + \mathfrak{b} = \{x + y : x \in \mathfrak{a}, y \in \mathfrak{b}\}.$$

This is easily checked to be an ideal. The next theorem describes $\mathfrak{a}+\mathfrak{b}$ in terms of generators.

Theorem 5.11. *If* $\mathfrak{a}=(\alpha_1,\ldots,\alpha_m)$ *and* $\mathfrak{b}=(\beta_1,\ldots,\beta_n)$ *then*

$$\mathfrak{a}+\mathfrak{b}=(\alpha_1,\ldots,\alpha_m,\beta_1,\ldots,\beta_n).$$

Proof. This is left to the reader. Look at the proof of Theorem 4.14 for inspiration if any is needed. □

Theorem 5.12. *For ideals* $\mathfrak{a}$ *and* $\mathfrak{b}$*, the ideal* $\mathfrak{a}+\mathfrak{b}$ *is a common divisor of* $\mathfrak{a}$ *and* $\mathfrak{b}$ *which all other common divisors divide.*

Proof. Since $\mathfrak{a}\subset\mathfrak{a}+\mathfrak{b}$ and $\mathfrak{b}\subset\mathfrak{a}+\mathfrak{b}$, $\mathfrak{a}+\mathfrak{b}$ is a divisor of both $\mathfrak{a}$ and $\mathfrak{b}$ because "to contain is to divide." For any ideal $\mathfrak{d}$ dividing both $\mathfrak{a}$ and $\mathfrak{b}$ we have $\mathfrak{a}\subset\mathfrak{d}$ and $\mathfrak{b}\subset\mathfrak{d}$. As $\mathfrak{d}$ is closed under addition of its elements, we get by Definition 5.10 that $\mathfrak{a}+\mathfrak{b}\subset\mathfrak{d}$, so $\mathfrak{d}$ is a divisor of $\mathfrak{a}+\mathfrak{b}$. □

We call $\mathfrak{a}+\mathfrak{b}$ the *greatest common divisor* of $\mathfrak{a}$ and $\mathfrak{b}$ since Theorem 5.12 shows that it has exactly the same feature as the usual greatest common divisor of (positive) integers. Because divisibility of ideals is the same as reverse containment, the greatest common divisor of two ideals is actually the "smallest" ideal containing both $\mathfrak{a}$ and $\mathfrak{b}$, in the sense of inclusions of ideals.

Example 5.13. Among the ideals of $\mathbf{Z}[\sqrt{-14}]$, the principal ideals (3) and $(1+\sqrt{-14})$ have greatest common divisor $(3)+(1+\sqrt{-14})=(3,1+\sqrt{-14})$, which is a non-principal ideal. That is, $\mathfrak{d}|(3)$ and $\mathfrak{d}|(1+\sqrt{-14})$ if and only if $\mathfrak{d}|(3,1+\sqrt{-14})$.

Since every ideal in $\mathcal{O}_K$ has the form $(\alpha_1,\ldots,\alpha_m)$, every ideal in $\mathcal{O}_K$ is the greatest common divisor of principal ideals because

$$(\alpha_1,\ldots,\alpha_m)=\alpha_1\mathcal{O}_K+\cdots+\alpha_m\mathcal{O}_K=(\alpha_1)+\cdots+(\alpha_m).$$

This shows how the principal ideals "control" all the ideals in $\mathcal{O}_K$.

6. Ideal norms

For a nonzero ideal $\mathfrak{a}$, Theorem 5.7 says $\mathfrak{a}\overline{\mathfrak{a}}$ is generated by elements of $\mathbf{Z}$, so it is principal with a generator in $\mathbf{Z}$. The generator can be chosen in $\mathbf{Z}^+$ by changing its sign if necessary. (Easily $(a)=(-a)$.) This generator is unique, because if a and b are in $\mathbf{Z}^+$ and $(a)=(b)$ as ideals in $\mathcal{O}_K$ then $a=bu$ for some $u\in\mathcal{O}_K^\times\cap\mathbf{Q}=\{\pm1\}$ (Theorem 3.9), so $u=1$ since a and b are positive.

Definition 6.1. For a nonzero ideal $\mathfrak{a}$ in $\mathcal{O}_K$, set $\mathrm{N}\mathfrak{a}$ to be the positive integer which generates $\mathfrak{a}\overline{\mathfrak{a}}$:

$$\mathfrak{a}\overline{\mathfrak{a}}=(\mathrm{N}\mathfrak{a}),\quad \mathrm{N}\mathfrak{a}\in\mathbf{Z}^+.$$

We call $\mathrm{N}\mathfrak{a}$ the (ideal) *norm* of $\mathfrak{a}$.

Example 6.2. By (4.3), in $\mathbf{Z}[\sqrt{-14}]$ the ideal $(3,1+\sqrt{-14})$ has norm 3.

Theorem 6.3. *The ideal norm is compatible with the element norm on principal ideals: if* $\mathfrak{a}=(\alpha)$ *then* $\mathrm{N}\mathfrak{a}=|\,\mathrm{N}(\alpha)|$.

Proof. We have $\mathfrak{a}\overline{\mathfrak{a}}=(\alpha)(\overline{\alpha})=(\alpha\overline{\alpha})=(\mathrm{N}(\alpha))=(|\,\mathrm{N}(\alpha)|)$. This equals $(\mathrm{N}\mathfrak{a})$, so $\mathrm{N}\mathfrak{a}=|\,\mathrm{N}(\alpha)|$ since both are positive integers. □

Theorem 6.4. *For nonzero ideals* $\mathfrak{a}$ *and* $\mathfrak{b}$, $\mathrm{N}(\mathfrak{ab}) = \mathrm{N}\mathfrak{a}\,\mathrm{N}\mathfrak{b}$.

Proof. We have

$$(\mathrm{N}(\mathfrak{ab})) = \mathfrak{ab}\overline{\mathfrak{a}}\overline{\mathfrak{b}} = \mathfrak{ab}\overline{\mathfrak{a}}\,\overline{\mathfrak{b}} = \mathfrak{a}\overline{\mathfrak{a}}\mathfrak{b}\overline{\mathfrak{b}} = (\mathrm{N}\mathfrak{a})(\mathrm{N}\mathfrak{b}) = (\mathrm{N}\mathfrak{a}\,\mathrm{N}\mathfrak{b}).$$

Therefore the positive integers $\mathrm{N}(\mathfrak{ab})$ and $\mathrm{N}\mathfrak{a}\,\mathrm{N}\mathfrak{b}$ each generate the same principal ideal in $\mathcal{O}_K$, so they are equal. □

Corollary 6.5. *For nonzero ideals* $\mathfrak{a}$ *and* $\mathfrak{b}$*, if* $\mathfrak{a}|\mathfrak{b}$ *then* $\mathrm{N}\mathfrak{a}|\,\mathrm{N}\mathfrak{b}$ *in* $\mathbf{Z}$.

Proof. Write $\mathfrak{b} = \mathfrak{ac}$ and take norms of both sides. □

The converse of Corollary 6.5 is false: The ideals $\mathfrak{a} = (1 + \sqrt{-14})$ and $\mathfrak{b} = (1 - \sqrt{-14})$ in $\mathbf{Z}[\sqrt{-14}]$ have equal norm but $\mathfrak{a}$ does not divide $\mathfrak{b}$.

Note $\mathrm{N}\mathfrak{a} = 1$ if and only if $\mathfrak{a} = (1)$. In one direction, it is trivial that $\mathrm{N}((1)) = 1$. Conversely, if $\mathrm{N}\mathfrak{a} = 1$ then $\mathfrak{a}\overline{\mathfrak{a}} = (1)$, so $\mathfrak{a}|(1)$. Therefore $\mathfrak{a} \supset (1) = \mathcal{O}_K$, so $\mathfrak{a} = (1)$. Thus any ideal $\mathfrak{a} \neq (1)$ has $\mathrm{N}\mathfrak{a} > 1$. This will be important later when we prove theorems about ideal factorization by induction on the ideal norm.

We did not define the norm of the ideal (0), but it is perfectly natural to set $\mathrm{N}((0)) = 0$. All results about ideal norms so far now extend to the zero ideal, but the next property is specific to nonzero ideals.

Corollary 6.6. *For a nonzero ideal* $\mathfrak{a}$*, any ideal factor of* $\mathfrak{a}$ *other than* $\mathfrak{a}$ *has norm less than* $\mathrm{N}\mathfrak{a}$.

Proof. Let $\mathfrak{b}$ be a factor of $\mathfrak{a}$ other than $\mathfrak{a}$, so $\mathfrak{a} = \mathfrak{bc}$ and $\mathfrak{c} \neq (1)$. Since $\mathrm{N}\mathfrak{a} = \mathrm{N}\mathfrak{b}\,\mathrm{N}\mathfrak{c}$ with $\mathrm{N}\mathfrak{a} \neq (0)$ and $\mathrm{N}\mathfrak{c} > 1$, $\mathrm{N}\mathfrak{b} < \mathrm{N}\mathfrak{a}$. □

In practice, how do we compute the norm of an ideal $\mathfrak{a}$ in $\mathcal{O}_K$? Theorem 5.7 provides an algorithm: for a set of generators for $\mathfrak{a}$, compute the greatest common divisor (in $\mathbf{Z}$) of the norms and "cross-traces" of the generators as described in the statement of Theorem 5.7. That number is the norm. Let's look at some examples in $\mathbf{Z}[\sqrt{-14}]$.

Example 6.7. Let $\mathfrak{a} = (3, 1 + \sqrt{-14})$. The ideal $\mathfrak{a}\overline{\mathfrak{a}}$ is generated by $\mathrm{N}(3), \mathrm{Tr}(3(1 - \sqrt{-14}))$, and $\mathrm{N}(1 + \sqrt{-14})$, which are 9, 6, and 15. Their greatest common divisor is 3, so $\mathrm{N}(3, 1 + \sqrt{-14}) = 3$.

Example 6.8. Let $\mathfrak{a} = (1 + \sqrt{-14}, 1 - \sqrt{-14})$. The norm is the greatest common divisor of $\mathrm{N}(1 \pm \sqrt{-14}) = 15$ and $\mathrm{Tr}((1 + \sqrt{-14})^2) = -26$. Since 15 and -26 are relatively prime, $\mathrm{N}\mathfrak{a} = 1$. Therefore $\mathfrak{a} = (1)$. Notice in particular that $\mathrm{N}\mathfrak{a}$ is *not* the greatest common divisor of the norms of a set of generators; we needed the trace term as well.

Example 6.9. Let $\mathfrak{a} = (4+\sqrt{-14}, 2-\sqrt{-14})$. Since $\mathrm{N}(4+\sqrt{-14}) = 30$, $\mathrm{Tr}((4+\sqrt{-14})(2+\sqrt{-14})) = -12$, and $\mathrm{N}(2 - \sqrt{-14}) = 18$, $\mathrm{N}\mathfrak{a} = 6$.

7. Prime ideals and unique factorization

We will factor nonzero ideals into products of prime ideals after working out some properties of prime ideals.

Theorem 7.1. *If an ideal is prime then its conjugate ideal is prime.*

Proof. The rings $\mathcal{O}_K/\mathfrak{p}$ and $\mathcal{O}_K/\overline{\mathfrak{p}}$ are isomorphic by applying conjugation to congruence classes. Therefore one ring is an integral domain if and only if the other ring is. □

Lemma 7.2. *For any nonzero ideal $\mathfrak{a}$ in $\mathcal{O}_K$, $\mathcal{O}_K/\mathfrak{a}$ is finite.*

Proof. Pick $\alpha \in \mathfrak{a}$ with $\alpha \neq 0$. The number $\mathrm{N}(\alpha) = \alpha\overline{\alpha}$ is nonzero and lies in $\mathfrak{a}$, so there is a natural ring homomorphism $\mathcal{O}_K/(\mathrm{N}(\alpha)) \to \mathcal{O}_K/\mathfrak{a}$, which is surjective. We will show $\mathcal{O}_K/(\mathrm{N}(\alpha))$ is finite, so $\mathcal{O}_K/\mathfrak{a}$ is finite too.

For any nonzero $n \in \mathbf{Z}$, $\mathcal{O}_K/(n) = \mathbf{Z}[\omega]/(n)$ is finite since, as an additive group, it is isomorphic to $\mathbf{Z}^2/n\mathbf{Z}^2 \cong (\mathbf{Z}/n\mathbf{Z})^2$. □

Theorem 7.3. *For an ideal $\mathfrak{p}$ in $\mathcal{O}_K$, the following are equivalent:*

(1) *$\mathfrak{p}$ is a nonzero prime ideal,*
(2) *$\mathfrak{p}$ is a maximal ideal,*
(3) *$\mathfrak{p}$ is a proper ideal and when $\mathfrak{p} = \mathfrak{a}\mathfrak{b}$ either $\mathfrak{a} = (1)$ or $\mathfrak{b} = (1)$.*

Proof. If $\mathfrak{p}$ is a nonzero prime ideal then $\mathcal{O}_K/\mathfrak{p}$ is a finite integral domain, and thus is a field, so $\mathfrak{p}$ is a maximal ideal. Thus (1) implies (2), and obviously (2) implies (1).

If $\mathfrak{p}$ is maximal and $\mathfrak{p} = \mathfrak{a}\mathfrak{b}$ then $\mathfrak{p} \subset \mathfrak{a}$. Therefore $\mathfrak{a} = (1)$ or $\mathfrak{a} = \mathfrak{p}$. In the second case $\mathfrak{p} = \mathfrak{p}\mathfrak{b}$, so $\mathfrak{b} = (1)$ since $\mathfrak{p}$ is cancelable. Thus (2) implies (3).

To show (3) implies (2), let $\mathfrak{p} \subset \mathfrak{a}$. Then $\mathfrak{a}|\mathfrak{p}$, so $\mathfrak{p} = \mathfrak{a}\mathfrak{b}$ for some ideal $\mathfrak{b}$. By (3), $\mathfrak{a} = (1)$ or $\mathfrak{b} = (1)$, and in the second case $\mathfrak{a} = \mathfrak{p}$. Hence $\mathfrak{p}$ is maximal, since $\mathfrak{p} \neq (1)$ by hypothesis. □

Here is a numerical criterion to recognize a prime ideal.

Theorem 7.4. *An ideal whose norm is prime in $\mathbf{Z}$ is a prime ideal.*

Proof. Let $\mathrm{N}\mathfrak{a} = p$ be prime. If $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$, then taking norms shows $p = \mathrm{N}\mathfrak{b}\,\mathrm{N}\mathfrak{c}$. Since p is prime, either $\mathfrak{b}$ or $\mathfrak{c}$ has norm 1, so either $\mathfrak{b}$ or $\mathfrak{c}$ is (1). □

Example 7.5. In $\mathbf{Z}[\sqrt{-14}]$, the ideal $(3, 1+\sqrt{-14})$ has norm 3, so it is a prime ideal. Similarly, $(3, 1-\sqrt{-14})$, $(5, 1+\sqrt{-14})$, and $(5, 1-\sqrt{-14})$ are prime ideals.

The converse to Theorem 7.4 is false: an ideal can be prime without having prime norm.

Example 7.6. In $\mathbf{Z}[\sqrt{-14}]$, we will show the ideal (11), whose norm is 121, is prime. Assume $(11) = \mathfrak{a}\mathfrak{b}$ with $\mathfrak{a} \neq (1)$ and $\mathfrak{b} \neq (1)$. Then taking norms implies $121 = \mathrm{N}\mathfrak{a}\,\mathrm{N}\mathfrak{b}$, so $\mathrm{N}\mathfrak{a} = 11$. Write $\mathfrak{a} = (\alpha_1, \ldots, \alpha_m)$. Since $\alpha_i \in \mathfrak{a}$ we have $\mathfrak{a}|(\alpha_i)$ by Theorem 5.8, so taking norms gives $11|\,\mathrm{N}(\alpha_i)$. Which elements of $\mathbf{Z}[\sqrt{-14}]$ have norm divisible by 11?

If $x + y\sqrt{-14}$ satisfies $x^2 + 14y^2 \equiv 0 \bmod 11$ then $x^2 \equiv -3y^2 \bmod 11$. Since $-3 \not\equiv \square \bmod 11$ we must have $y \equiv 0 \bmod 11$ and then $x \equiv 0 \bmod 11$. That implies $x + y\sqrt{-14}$ is divisible by 11 in $\mathbf{Z}[\sqrt{-14}]$.

Returning to the setup where $(11) = \mathfrak{a}\mathfrak{b}$, the previous paragraph implies that each element of $\mathfrak{a}$ is a multiple of 11. Factoring 11 from each generator gives $\mathfrak{a} = (11)\mathfrak{c}$ for some ideal $\mathfrak{c}$. But then $\mathrm{N}\mathfrak{a}$ is divisible by 121, while $\mathrm{N}\mathfrak{a} = 11$. This is a contradiction, so (11) is a prime ideal in $\mathbf{Z}[\sqrt{-14}]$.

To prove unique factorization in the positive integers, there are three steps:

- show prime numbers satisfy the property $p|ab \Rightarrow p|a$ or $p|b$ in $\mathbf{Z}$,
- show by induction that every positive integer > 1 has a prime factorization,
- show by induction that the prime factorization is unique, using the first step and cancellation to reduce to a smaller case.

The following theorem is the analogue of the first step above. The corresponding formulation for irreducible elements is false (Example 3.17).

Theorem 7.7. *If $\mathfrak{p}$ is a prime ideal and $\mathfrak{p}|\mathfrak{a}\mathfrak{b}$ then $\mathfrak{p}|\mathfrak{a}$ or $\mathfrak{p}|\mathfrak{b}$.*

Proof. We will assume $\mathfrak{p}$ does not divide $\mathfrak{a}$ and prove $\mathfrak{p}|\mathfrak{b}$. The ideal $\mathfrak{p}+\mathfrak{a}$ is a common divisor of $\mathfrak{p}$ and $\mathfrak{a}$. The only divisors of $\mathfrak{p}$ are $\mathfrak{p}$ and (1) since $\mathfrak{p}$ is prime. Because $\mathfrak{p}$ does not divide $\mathfrak{a}$, $\mathfrak{p}+\mathfrak{a} \neq \mathfrak{p}$. Therefore $\mathfrak{p}+\mathfrak{a} = (1)$, so $1 = x + \alpha$ for some $x \in \mathfrak{p}$ and $\alpha \in \mathfrak{a}$. Then for any $\beta \in \mathfrak{b}$,

$$\beta = 1 \cdot \beta = x\beta + \alpha\beta \in \mathfrak{p} + \mathfrak{a}\mathfrak{b} \subset \mathfrak{p},$$

which shows $\mathfrak{b} \subset \mathfrak{p}$. Thus $\mathfrak{p}|\mathfrak{b}$. □

Corollary 7.8. *If $\mathfrak{p}$ is prime and $\mathfrak{p}|\mathfrak{a}_1 \cdots \mathfrak{a}_r$ then $\mathfrak{p}|\mathfrak{a}_i$ for some i.*

Proof. Induct on r. □

Now we work out the analogue of the second step towards unique factorization.

Theorem 7.9. *Every nonzero ideal $\neq (1)$ admits a prime ideal factorization.*

Proof. Mimic the proof of Theorem 3.16 by using induction on the ideal norm. □

Theorem 7.10. *The prime factorization of a nonzero ideal $\neq (1)$ is unique up to the order of the factors. That is, for any nonzero $\mathfrak{a} \neq (1)$, if*

$$\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_r = \mathfrak{q}_1 \cdots \mathfrak{q}_s$$

where the $\mathfrak{p}_i$'s and $\mathfrak{q}_j$'s are prime, then the number of prime ideals in both factorizations is the same and $\mathfrak{p}_i = \mathfrak{q}_i$ after a suitable relabelling of the indices.

Proof. We argue by induction on the norm of the ideal. A prime ideal has no factorization into a product of primes except itself, so unique factorization is settled for prime ideals. This includes ideals with norm 2. For $n \geq 3$, suppose all ideals with norm from 2 to $n-1$ have unique prime factorization. Let $\mathfrak{a}$ be an ideal with norm n and two prime ideal factorizations:

$$\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_r = \mathfrak{q}_1 \cdots \mathfrak{q}_s.$$

Here we may take $r > 1$ and $s > 1$ since we may suppose $\mathfrak{a}$ is not a prime ideal.

Because $\mathfrak{p}_1|\mathfrak{a}$ we can say $\mathfrak{p}_1|\mathfrak{q}_1 \cdots \mathfrak{q}_s$. By Corollary 7.8, $\mathfrak{p}_1$ divides some $\mathfrak{q}_j$. Since ideal multiplication is commutative, we can relabel the $\mathfrak{q}_j$'s so that $\mathfrak{p}_1|\mathfrak{q}_1$. Then since $\mathfrak{q}_1$ is prime we must have $\mathfrak{p}_1 = \mathfrak{q}_1$ (since $\mathfrak{p}_1 \neq (1)$). Because all nonzero ideals in $\mathcal{O}_K$ are cancelable, we can remove $\mathfrak{p}_1$ from the two prime factorizations:

$$\mathfrak{p}_2 \cdots \mathfrak{p}_r = \mathfrak{q}_2 \cdots \mathfrak{q}_s.$$

This is a prime ideal factorization of an ideal with norm $\mathrm{N}\mathfrak{a}/\mathrm{N}\mathfrak{p}_1 < \mathrm{N}\mathfrak{a} = n$, so the inductive hypothesis applies: the number of prime ideals on both sides is the same (so $r-1 = s-1$, hence $r = s$) and after a suitable relabelling $\mathfrak{p}_i = \mathfrak{q}_i$ for $i = 2, \ldots, r$. We have $\mathfrak{p}_1 = \mathfrak{q}_1$ already, so we are done. □

We will work out examples of prime ideal factorizations in Section 9.

Remark 7.11. That we prove theorems about ideals by induction on their norm does not actually mean there is always an ideal with any positive integer for its norm. For instance, there are no ideals in $\mathbf{Z}[\sqrt{-14}]$ with norm 11, as we saw in Example 7.6. That means some cases of these induction arguments are actually empty cases.

The next theorem shows that non-principal ideals in $\mathcal{O}_K$ are the obstruction to unique factorization of elements in $\mathcal{O}_K$.

Theorem 7.12. *There is unique factorization of elements of $\mathcal{O}_K$ if and only if every ideal in $\mathcal{O}_K$ is principal.*

Proof. First suppose $\mathcal{O}_K$ has unique factorization of elements.

Step 1: For any irreducible π in $\mathcal{O}_K$, the principal ideal (π) is prime.

Let $\mathfrak{a}$ be an ideal dividing (π), so $\mathfrak{a} \supset (\pi)$. We want to show $\mathfrak{a}$ is (1) or (π). Suppose $\mathfrak{a} \neq (\pi)$, so there is an $\alpha \in \mathfrak{a}$ with $\alpha \notin (\pi)$. Writing $(\pi) = \mathfrak{a}\mathfrak{b}$, $\mathfrak{b}|(\pi)$ and for every $\beta \in \mathfrak{b}$ we have $\alpha\beta \in \mathfrak{a}\mathfrak{b} = (\pi)$, so $\pi|\alpha\beta$. By unique factorization of elements, π is an irreducible factor of either α or β. Since π does not divide α, we must have $\pi|\beta$, so $\beta \in (\pi)$. This holds for all $\beta \in \mathfrak{b}$, so $\mathfrak{b} \subset (\pi)$. Since $\mathfrak{b}|(\pi)$ and $(\pi)|\mathfrak{b}$, $\mathfrak{b} = (\pi)$. Therefore $(\pi) = \mathfrak{a}(\pi)$, so $\mathfrak{a} = (1)$.

Step 2: Every prime ideal in $\mathcal{O}_K$ is principal.

Let $\mathfrak{p}$ be a prime ideal. Then $\mathfrak{p}|(a)$ for some nonzero $a \in \mathbf{Z}$, such as $\mathrm{N}\mathfrak{p}$. Factor a into irreducibles in $\mathcal{O}_K$ (Theorem 3.16), say $a = \pi_1 \cdots \pi_r$. Then $(a) = (\pi_1) \cdots (\pi_r)$, so $\mathfrak{p}$ divides some (π_i). Since (π_i) is prime by Step 1, $\mathfrak{p} = (\pi_i)$.

Step 3: Every ideal in $\mathcal{O}_K$ is principal.

The zero ideal is obviously principal. Any nonzero ideal is a product of prime ideals, which are principal by Step 2, so their product is principal.

This concludes the "only if" direction.

Now assume every ideal in $\mathcal{O}_K$ is principal. We want to show $\mathcal{O}_K$ has unique factorization of elements. The existence of factorization into irreducibles is Theorem 3.16. To get uniqueness, we just need to show for any irreducible π that when $\pi|\alpha\beta$ in $\mathcal{O}_K$ either $\pi|\alpha$ or $\pi|\beta$. (The analogue of this property for prime ideals in Theorem 7.7 was used to prove uniqueness of prime ideal factorizations.) Suppose $\pi|\alpha\beta$ and π does not divide α. We want to show $\pi|\beta$. The only factors of π are units and unit multiples of π, so the only common factors of π and α are units. The ideal (π, α) is principal by hypothesis, say $(\pi, \alpha) = (\delta)$, so δ is a common factor of π and α. Thus δ is a unit, so $(\pi, \alpha) = (1)$. That means $\pi x + \alpha y = 1$ for some x and y in $\mathcal{O}_K$. Multiplying through by β, $\pi\beta x + \alpha\beta y = \beta$. Since $\pi|\alpha\beta$, we conclude that $\pi|\beta$. □

8. Constructing prime ideals

We have seen some examples of prime ideals, such as $(3, 1+\sqrt{-14})$ and (11) in $\mathbf{Z}[\sqrt{-14}]$, but what does a general prime ideal in $\mathcal{O}_K$ look like? We will describe the prime ideals in $\mathcal{O}_K$ in terms of prime numbers.

Theorem 8.1. *Every prime ideal in $\mathcal{O}_K$ divides a unique prime number. That is, if $\mathfrak{p}$ is prime then $\mathfrak{p}|(p)$ for one prime p in $\mathbf{Z}^+$.*

Proof. The ideal $\mathfrak{p}\overline{\mathfrak{p}} = (\mathrm{N}\mathfrak{p})$ is divisible by $\mathfrak{p}$ and has a generator in $\mathbf{Z}^+$. Since $\mathfrak{p} \neq (1)$, $\mathrm{N}\mathfrak{p} > 1$. Factor $\mathrm{N}\mathfrak{p}$ into primes in $\mathbf{Z}^+$, say

$$\mathrm{N}\mathfrak{p} = p_1 p_2 \cdots p_r.$$

Then $\mathfrak{p}\overline{\mathfrak{p}} = (p_1 p_2 \dots p_r) = (p_1) \cdots (p_r)$, so $\mathfrak{p}$ divides some (p_i) by Corollary 7.8.

For the uniqueness, assume $\mathfrak{p}|(p)$ and $\mathfrak{p}|(q)$ for two different prime numbers p and q. Then $p \in \mathfrak{p}$ and $q \in \mathfrak{p}$. Since p and q are relatively prime, $\mathfrak{p}$ contains a pair of relatively prime integers, so $\mathfrak{p} = (1)$. This is a contradiction. □

Corollary 8.2. *Every prime ideal in $\mathcal{O}_K$ has norm p or p^2 for some prime number p.*

Proof. Let $\mathfrak{p}$ be a prime ideal in $\mathcal{O}_K$. Then there is a prime number p such that $\mathfrak{p}|(p)$. Taking ideal norms, $\mathrm{N}\mathfrak{p}|\,\mathrm{N}((p))$. Since $\mathrm{N}((p)) = |\,\mathrm{N}(p)| = p^2$, $\mathrm{N}\mathfrak{p}$ is p or p^2. □

There are two ways to characterize the unique prime number p such that $\mathfrak{p}|(p)$: p is the only prime number in $\mathfrak{p}$ and $\mathrm{N}\mathfrak{p}$ is a power of p.

The importance of Theorem 8.1 is that it says we can discover every prime ideal in $\mathcal{O}_K$ by factoring prime numbers in $\mathcal{O}_K$. For instance, in $\mathbf{Z}[\sqrt{-14}]$ we know $(2) = (2, \sqrt{-14})^2$ and $(3) = (3, 1 + \sqrt{-14})(3, 1 - \sqrt{-14})$. Therefore $(2, \sqrt{-14})$ is the only prime ideal with 2-power norm and $(3, 1 + \sqrt{-14})$ and $(3, 1 - \sqrt{-14})$ are the only prime ideals with 3-power norm. (By Example 4.23, $(3, 1 + \sqrt{-14}) \neq (3, 1 - \sqrt{-14})$.)

The following theorem describes how each prime number (really, the principal ideal generated by each prime number) factors in $\mathcal{O}_K$, and thus shows us what all the prime ideals of $\mathcal{O}_K$ look like.

Theorem 8.3. *Let $K = \mathbf{Q}[\sqrt{d}]$ be a quadratic field with squarefree d and $\mathcal{O}_K = \mathbf{Z}[\omega]$, with $f(X)$ the quadratic polynomial having ω and $\overline{\omega}$ as roots:*

$$f(X) = \begin{cases} X^2 - d, & \text{if } d \not\equiv 1 \bmod 4, \\ X^2 - X + \frac{1-d}{4}, & \text{if } d \equiv 1 \bmod 4. \end{cases}$$

For each prime number p, the way (p) factors in $\mathcal{O}_K$ matches the way $f(X)$ factors modulo p:

1. *If $f(X) \bmod p$ is irreducible then (p) is prime in $\mathcal{O}_K$ with norm p^2.*
2. *If $f(X) \equiv (X - c)(X - c') \bmod p$ with $c \not\equiv c' \bmod p$ then $(p) = \mathfrak{p}\overline{\mathfrak{p}}$ where $\mathfrak{p} \neq \overline{\mathfrak{p}}$ and the conjugate ideals $\mathfrak{p}$ and $\overline{\mathfrak{p}}$ have norm p.*
3. *If $f(X) \equiv (X - c)^2 \bmod p$ then $(p) = \mathfrak{p}^2$ and $\mathrm{N}\mathfrak{p} = p$.*

In particular, prime ideals in $\mathcal{O}_K$ have prime norm except for principal primes (p) where p is a prime number such that $f(X) \bmod p$ is irreducible.

Note the exponent of p in the norms of prime ideals dividing (p) matches the degrees of the irreducible factors of $f(X) \bmod p$.

Proof. Since $\mathcal{O}_K = \mathbf{Z}[\omega] \cong \mathbf{Z}[X]/(f(X))$, $\mathcal{O}_K/(p) \cong \mathbf{Z}[X]/(p, f(X)) \cong (\mathbf{Z}/p\mathbf{Z})[X]/(f(X))$. That is the key. We will compare the ring structures of $\mathcal{O}_K/(p)$ and $(\mathbf{Z}/p\mathbf{Z})[X]/(f(X))$ to see that the way (p) factors in $\mathcal{O}_K$ resembles the way $f(X)$ factors in $(\mathbf{Z}/p\mathbf{Z})[X]$.

If $f(X) \bmod p$ is irreducible then $(\mathbf{Z}/p\mathbf{Z})[X]/(f(X))$ is a field. If $f(X) \equiv (X - c)(X - c') \bmod p$ with $c \not\equiv c' \bmod p$ then

$$\begin{aligned} (\mathbf{Z}/p\mathbf{Z})[X]/(f(X)) &\cong (\mathbf{Z}/p\mathbf{Z})[X]/(X - c) \times (\mathbf{Z}/p\mathbf{Z})[X]/(X - c') \\ &\cong (\mathbf{Z}/p\mathbf{Z}) \times (\mathbf{Z}/p\mathbf{Z}) \end{aligned}$$

is a direct product of two fields, which is not a field and has no nonzero nilpotent elements. If $f(X) \equiv (X - c)^2 \bmod p$ then $(\mathbf{Z}/p\mathbf{Z})[X]/(X - c)^2$ has a nonzero nilpotent element: $X - c \bmod (X - c)^2$. Thus the way $f(X)$ factors in $(\mathbf{Z}/p\mathbf{Z})[X]$ is reflected in the ring structure of $(\mathbf{Z}/p\mathbf{Z})[X]/(f(X))$.

The ring $\mathcal{O}_K/(p)$ is a field if and only if (p) is a maximal ideal, which is equivalent to (p) being prime (since $(p) \neq (0)$). Therefore, by the previous paragraph, $f(X) \bmod p$ is irreducible if and only if (p) is prime in $\mathcal{O}_K$.

If (p) is not prime then $(p) = \mathfrak{a}\mathfrak{b}$ where $\mathfrak{a}$ and $\mathfrak{b}$ are not (1). Taking norms, $p^2 = \mathrm{N}\mathfrak{a}\,\mathrm{N}\mathfrak{b}$, so $\mathfrak{a}$ and $\mathfrak{b}$ both have norm p and therefore are prime ideals. In fact, since $\mathrm{N}\mathfrak{a} = p$ we have $(p) = (\mathrm{N}\mathfrak{a}) = \mathfrak{a}\overline{\mathfrak{a}}$, so by unique prime ideal factorization we must have $\mathfrak{b} = \overline{\mathfrak{a}}$. Write $\mathfrak{a}$ as $\mathfrak{p}$, since it is a prime ideal. The factorization of (p) is $\mathfrak{p}\overline{\mathfrak{p}}$, where $\overline{\mathfrak{p}}$ may or may not equal $\mathfrak{p}$. If $\overline{\mathfrak{p}} = \mathfrak{p}$ then $\mathcal{O}_K/(p) = \mathcal{O}_K/\mathfrak{p}^2$ has a nonzero nilpotent element (the class of

any element of $\mathfrak{p} - \mathfrak{p}^2$), so $f(X) \equiv (X-c)^2 \bmod p$ for some c by the previous paragraph. If $\overline{\mathfrak{p}} \neq \mathfrak{p}$ then $\mathcal{O}_K/(p) = \mathcal{O}_K/\mathfrak{p}\overline{\mathfrak{p}}$ is not a field and has no nonzero nilpotent elements: if $x^m \equiv 0 \bmod \mathfrak{p}\overline{\mathfrak{p}}$ then $\mathfrak{p}$ and $\overline{\mathfrak{p}}$ both divide $(x^m) = (x)^m$, so both divide (x) by their primality, so $\mathfrak{p}\overline{\mathfrak{p}}|(x)$ because $\mathfrak{p} \neq \overline{\mathfrak{p}}$. Therefore $x \equiv 0 \bmod \mathfrak{p}\overline{\mathfrak{p}}$. By the previous paragraph, we must have $f(X) \equiv (X-c)(X-c') \bmod p$ with $c \not\equiv c' \bmod p$ in this case. □

Corollary 8.4. *If (p) is not prime in $\mathcal{O}_K$ then $f(X) \bmod p$ has a root. For any root $c \bmod p$, $(p, \omega - c)$ is one of the prime ideals dividing (p).*

Proof. By Theorem 8.3, $(p) = \mathfrak{p}\overline{\mathfrak{p}}$ for a prime ideal $\mathfrak{p}$. Set $\mathfrak{a} = (p, \omega - c)$. Since $p \in \mathfrak{a}$, $\mathfrak{a}|(p)$. Because $\omega - c \notin (p)$, $\mathfrak{a} \neq (p)$, so either $\mathfrak{a}$ is one of the prime ideals dividing (p) or $\mathfrak{a} = (1)$. We want to show $\mathfrak{a} \neq (1)$, so we will look at $\mathrm{N}\mathfrak{a}$. The norm of $\mathfrak{a}$ is the greatest common divisor of $\mathrm{N}(p) = p^2$, $\mathrm{Tr}(p(\overline{\omega} - c)) = p\,\mathrm{Tr}(\overline{\omega} - c)$, and $\mathrm{N}(\omega - c) = f(c) \equiv 0 \bmod p$. These are all divisible by p, so $p|\,\mathrm{N}\mathfrak{a}$. Hence $\mathfrak{a} \neq (1)$, so $\mathfrak{a}$ is $\mathfrak{p}$ or $\overline{\mathfrak{p}}$. The roles of $\mathfrak{p}$ and $\overline{\mathfrak{p}}$ have so far been symmetric, so we can set $\mathfrak{p} = \mathfrak{a} = (p, \omega - c)$. □

Example 8.5. How does (2) factor in the integers of $\mathbf{Q}[\sqrt{-39}]$? Although $X^2 + 39 \equiv (X+1)^2 \bmod 2$, it is incorrect to conclude that $(2) = \mathfrak{p}^2$ because the integers of $\mathbf{Q}[\sqrt{-39}]$ are not $\mathbf{Z}[\sqrt{-39}]$. The relevant polynomial is not $X^2 + 39$, but rather $X^2 - X + 10$ (which has $(1+\sqrt{-39})/2$ as a root). Since $X^2 - X + 10 \equiv X(X-1) \bmod 2$, the correct factorization of (2) is $\mathfrak{p}\overline{\mathfrak{p}}$.

When $p \neq 2$, how the quadratic polynomial $f(X)$ factors modulo p is determined by its discriminant: there are two different roots if the discriminant is a nonzero square mod p, no roots if the discriminant is not a square mod p, and a repeated root if the discriminant is 0 mod p. The two formulas for $f(X)$ are $X^2 - d$ and $X^2 - X + \frac{1-d}{4}$, which have respective discriminants $4d$ and d, so the way $f(X) \bmod p$ factors is determined by the Legendre symbol $(\frac{d}{p})$. (This Legendre symbol is 0 when $p|d$.) What can we say when $p = 2$? The way $f(X) \bmod 2$ factors depends on $d \bmod 8$. We can translate the results of Corollary 8.4 into simple formulas based on $(\frac{d}{p})$ and $d \bmod 8$, which we record in Tables 2 and 3. The second column in each table describes how (p) factors into prime ideals in the integers of $\mathbf{Q}[\sqrt{d}]$. In both tables, we write $\overline{\mathfrak{p}}$ when $\mathfrak{p} \neq \overline{\mathfrak{p}}$. In Table 2, $c \bmod p$ is a root of $f(X) \bmod p$.

$(\frac{d}{p})$	(p)	$\mathfrak{p}$
1	$\mathfrak{p}\overline{\mathfrak{p}}$	$(p, \omega - c)$
-1	$\mathfrak{p}$	(p)
0	$\mathfrak{p}^2$	$(p, \omega - c)$

TABLE 2. $p \neq 2$

$d \bmod 8$	(2)	$\mathfrak{p}$
1	$\mathfrak{p}\overline{\mathfrak{p}}$	$(2, \frac{1+\sqrt{d}}{2})$
5	$\mathfrak{p}$	(2)
3, 7	$\mathfrak{p}^2$	$(2, \sqrt{d}-1)$
even	$\mathfrak{p}^2$	$(2, \sqrt{d})$

TABLE 3. $p = 2$

In Theorem 4.1, we noted that any ideal in $\mathcal{O}_K$ requires at most two generators (over $\mathcal{O}_K$), for the simple reason that $\mathcal{O}_K \cong \mathbf{Z}^2$ as abelian groups and any subgroup of $\mathbf{Z}^2$ requires at most 2 generators (over $\mathbf{Z}$, and thus also over $\mathcal{O}_K$). In other words, although ideals are rather special kinds of subgroups of $\mathcal{O}_K$, the proof of Theorem 4.1 paid no attention to this. However, there *is* something which is special about generators for ideals which doesn't hold for generators of subgroups of $\mathbf{Z}^2$. In a subgroup of $\mathbf{Z}^2$, not every nonzero element has to be part of a 2-element generating set (over $\mathbf{Z}$). For instance, the only elements of $\mathbf{Z}^2$ which can be part of a 2-element generating set of $\mathbf{Z}^2$ itself are those vectors with relatively prime coordinates. Compare that with the next result.

Theorem 8.6. *If $\mathfrak{a}$ is a nonzero ideal in $\mathcal{O}_K$ and α is any nonzero element of $\mathfrak{a}$ then $\mathfrak{a} = (\alpha, \beta)$ for a suitably chosen $\beta \in \mathfrak{a}$.*

The proof of Theorem 8.6 requires an analogue of the Chinese remainder theorem for $\mathcal{O}_K$, building on unique factorization of ideals, and is omitted.

9. Worked examples

We will compute some prime ideal factorizations in $\mathbf{Z}[\sqrt{-14}]$. First we specialize Tables 2 and 3 to small primes in $\mathbf{Z}[\sqrt{-14}]$. See Table 4.

p	(p)	$\mathfrak{p}$
2	$\mathfrak{p}_2^2$	$\mathfrak{p}_2 = (2, \sqrt{-14})$
3	$\mathfrak{p}_3\overline{\mathfrak{p}}_3$	$\mathfrak{p}_3 = (3, \sqrt{-14}+1)$
5	$\mathfrak{p}_5\overline{\mathfrak{p}}_5$	$\mathfrak{p}_5 = (5, \sqrt{-14}+1)$
7	$\mathfrak{p}_7^2$	$\mathfrak{p}_7 = (7, \sqrt{-14})$
11	(11)	(11)
13	$\mathfrak{p}_{13}\overline{\mathfrak{p}}_{13}$	$\mathfrak{p}_{13} = (13, \sqrt{-14}+5)$
17	(17)	(17)
19	$\mathfrak{p}_{19}\overline{\mathfrak{p}}_{19}$	$\mathfrak{p}_{19} = (19, \sqrt{-14}+9)$
23	$\mathfrak{p}_{23}\overline{\mathfrak{p}}_{23}$	$\mathfrak{p}_{23} = (\sqrt{-14}+3)$

Table 4. Factoring (p) in $\mathbf{Z}[\sqrt{-14}]$

The way (p) factors in $\mathbf{Z}[\sqrt{-14}]$ is determined by the way $X^2 + 14$ factors mod p, and that is determined by $(\frac{-14}{p})$ if $p \neq 2$. If $(\frac{-14}{p}) = 1$ then (p) is a product of two different (conjugate) ideals with norm p. When $-14 \equiv c^2 \bmod p$, one of the prime factors $\mathfrak{p}$ is $(p, \sqrt{-14} - c)$. If $(\frac{-14}{p}) = -1$ then (p) is a prime ideal with norm p^2. If $p = 2$ or 7 then (p) is the square of a prime ideal with norm p. The initial odd p such that $(\frac{-14}{p}) = 1$ are 3, 5, 13, and 19. Therefore we have the factorizations in Table 4, where we leave a principal ideal unfactored if it stays prime (*e.g.*, $p = 11$). The last ideal, $\mathfrak{p}_{23}$, should be $(23, \sqrt{-14}+3)$ according to the general methods for computing prime ideals. But in this particular case $23 = (3 + \sqrt{-14})(3 - \sqrt{-14})$, so we can drop 23 as a generator of the ideal. The prime ideal factors of 2, 3, 5, 7, 13, and 19 in the table are non-principal since the equation $x^2 + 14y^2 = p$ has no solution for these values of p.

With this information we can start factoring ideals with generators not in $\mathbf{Z}$. The central idea is to compute the norm of the ideal and use our knowledge of prime factorization of the norm in $\mathbf{Z}$ to help us. Remember that prime ideals only have prime-power norm.

Example 9.1. We will factor $(1+\sqrt{-14})$. The ideal has norm 15. Writing $(1+\sqrt{-14})$ as a product of prime ideals, the product of their norms is 15, so $(1+\sqrt{-14})$ must be the product of a prime ideal of norm 3 and a prime ideal of norm 5. Since $1+\sqrt{-14} \in \mathfrak{p}_3$ and $1+\sqrt{-14} \in \mathfrak{p}_5$, $(1+\sqrt{-14})$ is divisible by $\mathfrak{p}_3$ and $\mathfrak{p}_5$. Hence $(1+\sqrt{-14}) = \mathfrak{p}_3\mathfrak{p}_5$.

Example 9.2. We will factor $(5+2\sqrt{-14})$, which was left to the reader at the end of Example 4.28. Since $\mathrm{N}(5+2\sqrt{-14}) = 81$, the only possible prime ideal factors of $(5+2\sqrt{-14})$ are $\mathfrak{p}_3$ and $\overline{\mathfrak{p}}_3$. But it can't be divisible by both, since then it is divisible by $\mathfrak{p}_3\overline{\mathfrak{p}}_3 = (3)$ and we know (3) doesn't divide $(5+2\sqrt{-14})$ because 3 doesn't divide $5+2\sqrt{-14}$ in $\mathbf{Z}[\sqrt{-14}]$. Therefore $(5+2\sqrt{-14})$ is a power of $\mathfrak{p}_3$ or a power of $\overline{\mathfrak{p}}_3$. Considering its norm is 81, $(5+2\sqrt{-14})$ is either $\mathfrak{p}_3^4$ or $\overline{\mathfrak{p}}_3^4$. Which one is correct?

In $\mathbf{Z}[\sqrt{-14}]/\mathfrak{p}_3 \cong \mathbf{Z}/3\mathbf{Z}$ we have $1+\sqrt{-14} = 0$, so $5+2\sqrt{-14} = 3 = 0$. Thus $\mathfrak{p}_3 | (5+2\sqrt{-14})$, so $(5+2\sqrt{-14}) = \mathfrak{p}_3^4$.

Example 9.3. The ideal $\mathfrak{a} = (2+3\sqrt{-14})$ has norm $130 = 2\cdot 5\cdot 13$. Therefore $\mathfrak{p}_2|\mathfrak{a}$. Does $\mathfrak{p}_5$ or $\overline{\mathfrak{p}}_5$ divide $\mathfrak{a}$? The ideal $(1+\sqrt{-14})$ is divisible by $\mathfrak{p}_5$ and not by $\overline{\mathfrak{p}}_5$, so let's look at the greatest common divisor of $\mathfrak{a}$ and $(1+\sqrt{-14})$, which is $(2+3\sqrt{-14}, 1+\sqrt{-14})$. Its norm is 1, so we must have $\overline{\mathfrak{p}}_5|\mathfrak{a}$. To decide if $\mathfrak{p}_{13}$ or $\overline{\mathfrak{p}}_{13}$ divides $\mathfrak{a}$, we look at $(2+3\sqrt{-14}, 5+\sqrt{-14})$, which is the greatest common divisor of $\mathfrak{a}$ and $(5+\sqrt{-14})$; it is either $\mathfrak{p}_{13}$ or (1). A calculation shows $(2+3\sqrt{-14}, 5+\sqrt{-14})$ has norm 13, so $\mathfrak{p}_{13}|\mathfrak{a}$. We finally have the prime factorization of $\mathfrak{a}$: $\mathfrak{p}_2\overline{\mathfrak{p}}_5\mathfrak{p}_{13}$.

Example 9.4. The ideal $\mathfrak{a} = (7+3\sqrt{-14})$ has norm $175 = 5^2\cdot 7$. Therefore $\mathfrak{p}_7|\mathfrak{a}$. Either $\mathfrak{p}_5$ or $\overline{\mathfrak{p}}_5$ divides $\mathfrak{a}$ (but not both, since otherwise their product (5) divides $\mathfrak{a}$, which is not the case). The ideal $(7+3\sqrt{-14}, 1+\sqrt{-14})$ has norm 1, so $\mathfrak{p}_5$ does not divide $\mathfrak{a}$. Therefore $\mathfrak{a} = \overline{\mathfrak{p}}_5^2\mathfrak{p}_7$.

As exercises, verify the prime ideal factorizations in Table 5. The first step in each case is to compute the norm of the ideal to obtain a list of possible prime ideal factors from Table 4.

Ideal	Factorization
$(5+\sqrt{-14})$	$\overline{\mathfrak{p}}_3\mathfrak{p}_{13}$
$(2+\sqrt{-14})$	$\mathfrak{p}_2\overline{\mathfrak{p}}_3^2$
$(4+\sqrt{-14})$	$\mathfrak{p}_2\mathfrak{p}_3\overline{\mathfrak{p}}_5$
$(7+\sqrt{-14})$	$\mathfrak{p}_3^2\mathfrak{p}_7$
$(7+2\sqrt{-14})$	$\overline{\mathfrak{p}}_3\mathfrak{p}_5\mathfrak{p}_7$
$(17+2\sqrt{-14})$	$\mathfrak{p}_3\mathfrak{p}_5\overline{\mathfrak{p}}_{23}$
$(20+\sqrt{-14})$	$\mathfrak{p}_2\overline{\mathfrak{p}}_3^2\overline{\mathfrak{p}}_{23}$

TABLE 5. Factoring ideals in $\mathbf{Z}[\sqrt{-14}]$

These factorizations provide new ways of working out the ideal calculations in examples from Section 4. For instance, to redo Example 4.15 with Table 5, $(5+\sqrt{-14}, 2+\sqrt{-14}) = \overline{\mathfrak{p}}_3$ and $(4+\sqrt{-14}, 2-\sqrt{-14}) = \mathfrak{p}_2\mathfrak{p}_3$ (note $\overline{\mathfrak{p}}_2 = \mathfrak{p}_2$), so the product of these ideals is $\mathfrak{p}_2\mathfrak{p}_3\overline{\mathfrak{p}}_3 = \mathfrak{p}_2(3) = (2,\sqrt{-14})(3) = (6, 3\sqrt{-14})$.

REFERENCES

[1] J. R. Goldman, "The Queen of Mathematics: An Historically Motivated Guide to Number Theory," A. K. Peters, Wellesley, MA, 1998.

[2] H. M. Stark, "An Introduction to Number Theory," MIT Press, Cambridge, 1978.
[3] H. M. Stark, personal notes.