How Do Elements Really Factor in $\mathbb{Z}[\sqrt{-5}]$?

Scott T. Chapman, Felix Gotti, and Marly Gotti

Abstract Most undergraduate level abstract algebra texts use $\mathbb{Z}[\sqrt{-5}]$ as an example of an integral domain which is not a unique factorization domain (or UFD) by exhibiting two distinct irreducible factorizations of a nonzero element. But such a brief example, which requires merely an understanding of basic norms, only scratches the surface of how elements actually factor in this ring of algebraic integers. We offer here an interactive framework which shows that while $\mathbb{Z}[\sqrt{-5}]$ is not a UFD, it does satisfy a slightly weaker factorization condition, known as half-factoriality. The arguments involved revolve around the Fundamental Theorem of Ideal Theory in algebraic number fields.

Dedicated to David F. Anderson on the occasion of his retirement.

1 Introduction

Consider the integral domain

$$\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}.$$

Your undergraduate abstract algebra text probably used it as the base example of an integral domain that is not a unique factorization domain (or UFD). The Fundamental Theorem of Arithmetic fails in $\mathbb{Z}[\sqrt{-5}]$ as this domain contains elements with

Scott T. Chapman
Sam Houston State University, Huntsville, TX 77341, e-mail: scott.chapman@shsu.edu

Felix Gotti
UC Berkeley, Berkeley, CA 94720 e-mail: felixgotti@berkeley.edu

Marly Gotti
University of Florida, Gainesville, FL 32611 e-mail: marlycormar@ufl.edu

2010 AMS *Mathematics Subject Classification*: Primary 11R11, 13F15, 20M13.

multiple factorizations into irreducibles; for example,

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

even though $2, 3, 1 - \sqrt{-5}$, and $1 + \sqrt{-5}$ are pairwise non-associate irreducible elements in $\mathbb{Z}[\sqrt{-5}]$. To argue this, the norm on $\mathbb{Z}[\sqrt{-5}]$, i.e.,

$$N(a + b\sqrt{-5}) = a^2 + 5b^2, \tag{2}$$

plays an important role, as it is a multiplicative function satisfying the following properties:

- $N(\alpha) = 0$ if and only if $\alpha = 0$;
- $N(\alpha\beta) = N(\alpha)N(\beta)$ for all $\alpha, \beta \in \mathbb{Z}[\sqrt{-5}]$;
- α is a unit if and only if $N(\alpha) = 1$ (i.e., ± 1 are the only units of $\mathbb{Z}[\sqrt{-5}]$);
- if $N(\alpha)$ is prime, then α is irreducible.

However, introductory abstract algebra books seldom dig deeper than what Equation (1) does. The goal of this paper is to use ideal theory to describe exactly how elements in $\mathbb{Z}[\sqrt{-5}]$ factor into products of irreducibles. In doing so, we will show that $\mathbb{Z}[\sqrt{-5}]$ satisfies a nice factorization property, which is known as *half-factoriality*. Thus, we say that $\mathbb{Z}[\sqrt{-5}]$ is a *half-factorial domain* (or HFD). Our journey will require nothing more than elementary algebra, but will give the reader a glimpse of how The Fundamental Theorem of Ideal Theory resolves the non-unique factorizations of $\mathbb{Z}[\sqrt{-5}]$. The notion that unique factorization in rings of integers could be recovered via ideals was important in the late 1800's in attempts to prove Fermat's Last Theorem (see [9, Chapter 11]).

Our presentation is somewhat interactive, as many steps that follow from standard techniques of basic algebra are left to the reader as exercises. The only background we expect from the reader are introductory courses in linear algebra and abstract algebra. Assuming such prerequisites, we have tried to present here a self-contained and friendly approach to the phenomenon of non-uniqueness of factorizations occurring in $\mathbb{Z}[\sqrt{-5}]$. More advanced and general arguments (which apply to any ring of integers) can be found in [8] and [9].

2 Integral Bases and Discriminants

Although in this paper we are primarily concerned with the phenomenon of non-unique factorizations in the particular ring of integers $\mathbb{Z}[\sqrt{-5}]$, it is more enlightening from an algebraic perspective to introduce our needed concepts for arbitrary commutative rings with identity, rings of integers, or quadratic rings of integers, depending on the most appropriate context for each concept being introduced. In what follows, we shall proceed in this manner while trying, by all means, to keep the exposition as elementary as possible.

An element $\alpha \in \mathbb{C}$ is said to be *algebraic* provided that it is a root of a nonzero polynomial with rational coefficients, while α is said to be an *algebraic integer* provided that it is a root of a monic polynomial with integer coefficients. It is not hard to argue that every subfield of $\mathbb{C}$ contains $\mathbb{Q}$ and is a $\mathbb{Q}$-vector space.

Definition 2.1. A subfield K of $\mathbb{C}$ is called an *algebraic number field* provided that it has finite dimension as a vector space over $\mathbb{Q}$. The subset

$$\mathscr{O}_K := \{\alpha \in K \mid \alpha \text{ is an algebraic integer}\}$$

of K is called the *ring of integers* of K.

The ring of integers of any algebraic number field is, indeed, a ring. The reader is invited to verify this observation. If α is a complex number, then $\mathbb{Q}(\alpha)$ denotes the smallest subfield of $\mathbb{C}$ containing α. It is well known that a subfield K of $\mathbb{C}$ is an algebraic number field if and only if there exists an algebraic number $\alpha \in \mathbb{C}$ such that $K = \mathbb{Q}(\alpha)$ (see, for example, [6, Theorem 2.17]). Among all algebraic number fields, we are primarily interested in those that are two-dimensional vector spaces over $\mathbb{Q}$.

Definition 2.2. An algebraic number field that is a two-dimensional vector space over $\mathbb{Q}$ is called a *quadratic number field*. If K is a quadratic number field, then $\mathscr{O}_K$ is called a *quadratic ring of integers*.

For $\alpha \in \mathbb{C}$, let $\mathbb{Z}[\alpha]$ denote the set of all polynomial expressions in α having integer coefficients. Clearly, $\mathbb{Z}[\alpha]$ is a subring of $\mathbb{Q}(\alpha)$. It is also clear that, for $d \in \mathbb{Z}$, the field $\mathbb{Q}(\sqrt{d})$ has dimension at most two as a $\mathbb{Q}$-vector space and, therefore, it is an algebraic number field. Moreover, if $d \notin \{0,1\}$ and d is squarefree (i.e., d is not divisible by the square of any prime), then it immediately follows that $\mathbb{Q}(\sqrt{d})$ is a two-dimensional vector space over $\mathbb{Q}$ and, as a result, a quadratic number field. As we are mainly interested in the case when $d = -5$, we propose the following exercise.

Exercise 2.3. Let $d \in \mathbb{Z} \setminus \{0,1\}$ be a squarefree integer such that $d \equiv 2,3 \pmod 4$. Prove that $\mathbb{Z}[\sqrt{d}]$ is the ring of integers of the quadratic number field $\mathbb{Q}(\sqrt{d})$.

Remark. When $d \in \mathbb{Z} \setminus \{0,1\}$ is a squarefree integer satisfying $d \equiv 1 \pmod 4$, it is not hard to argue that the ring of integers of $\mathbb{Q}(\sqrt{d})$ is $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$. However, we will not be concerned with this case as our case of interest is $d = -5$.

For d as specified in Exercise 2.3, the elements of $\mathbb{Z}[\sqrt{d}]$ can be written in the form $a + b\sqrt{d}$ for $a, b \in \mathbb{Z}$. The *norm* N on $\mathbb{Z}[\sqrt{d}]$ is defined by

$$N(a + b\sqrt{d}) = a^2 - db^2$$

(cf. Equation (2)). The norm N on $\mathbb{Z}[\sqrt{d}]$ also satisfies the four properties listed in the introduction.

Let us now take a look at the structure of an algebraic number field K with linear algebra in mind. For $\alpha \in K$ consider the function $m_\alpha \colon K \to K$ defined via multiplication by α, i.e., $m_\alpha(x) = \alpha x$ for all $x \in K$. One can easily see that m_α is a linear transformation of $\mathbb{Q}$-vector spaces. Therefore, after fixing a basis for the $\mathbb{Q}$-vector space K, we can represent m_α by a matrix M. The *trace* of α, which is denoted by $\operatorname{Tr}(\alpha)$, is defined to be the trace of the matrix M. It is worth noting that $\operatorname{Tr}(\alpha)$ does not depend on the chosen basis for K. Also, notice that $\operatorname{Tr}(\alpha) \in \mathbb{Q}$. Furthermore, if $\alpha \in \mathscr{O}_K$, then $\operatorname{Tr}(\alpha) \in \mathbb{Z}$ (see [10, Lemma 4.1.1], or Exercise 2.5 for the case when $K = \mathbb{Q}(\sqrt{d})$).

Definition 2.4. Let K be an algebraic number field that has dimension n as a $\mathbb{Q}$-vector space. The *discriminant* of a subset $\{\omega_1, \dots, \omega_n\}$ of K, which is denoted by $\Delta[\omega_1, \dots, \omega_n]$, is $\det T$, where T is the $n \times n$ matrix $\big(\operatorname{Tr}(\omega_i \omega_j)\big)_{1 \le i,j \le n}$.

With K as introduced above, if $\{\omega_1, \dots, \omega_n\}$ is a subset of $\mathscr{O}_K$, then it follows that $\Delta[\omega_1, \dots, \omega_n] \in \mathbb{Z}$ (see Exercise 2.5 for the case when $K = \mathbb{Q}(\sqrt{d})$). In addition, the discriminant of any basis for the $\mathbb{Q}$-vector space K is nonzero; we will prove this for $K = \mathbb{Q}(\sqrt{d})$ in Proposition 2.10.

Exercise 2.5. Let $d \in \mathbb{Z} \setminus \{0,1\}$ be a squarefree integer such that $d \equiv 2,3 \pmod 4$.

1. If $\alpha = a_1 + a_2\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$, then $\operatorname{Tr}(\alpha) = 2a_1$.
2. If, in addition, $\beta = b_1 + b_2\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$, then

$$\Delta[\alpha, \beta] = \left(\det \begin{bmatrix} \alpha & \sigma(\alpha) \\ \beta & \sigma(\beta) \end{bmatrix} \right)^2 = 4d(a_1 b_2 - a_2 b_1)^2,$$

where $\sigma(x + y\sqrt{d}) = x - y\sqrt{d}$ for all $x, y \in \mathbb{Z}$.

Example 2.6. Let $d \notin \{0,1\}$ be a squarefree integer such that $d \equiv 2,3 \pmod 4$. It follows from Exercise 2.5 that the subset $\{1, \sqrt{d}\}$ of the ring of integers $\mathbb{Z}[\sqrt{d}]$ satisfies that $\Delta[1, \sqrt{d}] = 4d$.

We proceed to introduce the concept of integral basis.

Definition 2.7. Let K be an algebraic number field of dimension n as a vector space over $\mathbb{Q}$. The elements $\omega_1, \dots, \omega_n \in \mathscr{O}_K$ form an *integral basis* for $\mathscr{O}_K$ if for each $\beta \in \mathscr{O}_K$ there are unique $z_1, \dots, z_n \in \mathbb{Z}$ satisfying $\beta = z_1\omega_1 + \cdots + z_n\omega_n$.

Example 2.8. Let $d \in \mathbb{Z} \setminus \{0,1\}$ be a squarefree integer such that $d \equiv 2,3 \pmod 4$. Clearly, every element in $\mathbb{Z}[\sqrt{d}]$ is an integral linear combination of 1 and $\sqrt{d}$. Suppose, on the other hand, that $a_1 + a_2\sqrt{d} = b_1 + b_2\sqrt{d}$ for some $a_1, a_2, b_1, b_2 \in \mathbb{Z}$. Note that $a_2 = b_2$; otherwise $\sqrt{d} = \frac{a_1 - b_1}{b_2 - a_2}$ would be a rational number. As a result, $a_1 = b_1$. Thus, we have verified that every element of $\mathbb{Z}[\sqrt{d}]$ can be uniquely written as an integral linear combination of 1 and $\sqrt{d}$. Hence, the set $\{1, \sqrt{d}\}$ is an integral basis for $\mathbb{Z}[\sqrt{d}]$.

In general, the ring of integers of any algebraic number field has an integral basis (see [6, Theorem 3.27]). On the other hand, although integral bases are not unique, any two integral bases for the same ring of integers have the same discriminant. We shall prove this for $\mathbb{Z}[\sqrt{d}]$ in Theorem 2.13.

Notation: If S is a subset of the complex numbers, then we let $S^\bullet$ denote $S \setminus \{0\}$.

Lemma 2.9. *Let K be an algebraic number field of dimension n as a $\mathbb{Q}$-vector space. An integral basis for $\mathscr{O}_K$ is a basis for K as a vector space over $\mathbb{Q}$.*

Proof. Suppose that $\{\omega_1, \ldots, \omega_n\}$ is an integral basis for $\mathscr{O}_K$, and take rational coefficients $q_1, \ldots, q_n$ such that

$$q_1\omega_1 + \cdots + q_n\omega_n = 0.$$

Multiplying the above equality by the common denominator of the nonzero q_i's and using the fact that $\{\omega_1, \ldots, \omega_n\}$ is an integral basis for the ring of integers $\mathscr{O}_K$, we obtain that $q_1 = \cdots = q_n = 0$. Hence, $\{\omega_1, \ldots, \omega_n\}$ is a linearly independent set of the $\mathbb{Q}$-vector space K. As K has dimension n over $\mathbb{Q}$, the set $\{\omega_1, \ldots, \omega_n\}$ is a basis for the vector space K over $\mathbb{Q}$. □

Proposition 2.10. *Let $d \in \mathbb{Z} \setminus \{0,1\}$ be a squarefree integer with $d \equiv 2,3 \pmod 4$. If $\{\alpha_1, \alpha_2\}$ is a vector space basis for $\mathbb{Q}(\sqrt{d})$ contained in $\mathbb{Z}[\sqrt{d}]$, then $\Delta[\alpha_1, \alpha_2] \in \mathbb{Z}^\bullet$.*

Proof. From the fact that $\{\alpha_1, \alpha_2\} \subseteq \mathbb{Z}[\sqrt{d}]$, it follows that $\Delta[\alpha_1, \alpha_2] \in \mathbb{Z}$. So suppose, by way of contradiction, that $\Delta[\alpha_1, \alpha_2] = 0$. Taking $\{\omega_1, \omega_2\}$ to be an integral basis for $\mathbb{Z}[\sqrt{d}]$, one has that

$$\begin{aligned} \alpha_1 &= z_{1,1}\omega_1 + z_{1,2}\omega_2 \\ \alpha_2 &= z_{2,1}\omega_1 + z_{2,2}\omega_2, \end{aligned}$$

for some $z_{i,j} \in \mathbb{Z}$. Using Exercise 2.5, we obtain

$$\begin{aligned} \Delta[\alpha_1, \alpha_2] &= \left(\det \begin{bmatrix} \alpha_1 & \sigma(\alpha_1) \\ \alpha_2 & \sigma(\alpha_2) \end{bmatrix}\right)^2 = \left(\det \left(\begin{bmatrix} z_{1,1} & z_{1,2} \\ z_{2,1} & z_{2,2} \end{bmatrix} \begin{bmatrix} \omega_1 & \sigma(\omega_1) \\ \omega_2 & \sigma(\omega_2) \end{bmatrix}\right)\right)^2 \\ &= \left(\det \begin{bmatrix} z_{1,1} & z_{1,2} \\ z_{2,1} & z_{2,2} \end{bmatrix}\right)^2 \left(\det \begin{bmatrix} \omega_1 & \sigma(\omega_1) \\ \omega_2 & \sigma(\omega_2) \end{bmatrix}\right)^2 = \left(\det \begin{bmatrix} z_{1,1} & z_{1,2} \\ z_{2,1} & z_{2,2} \end{bmatrix}\right)^2 \Delta[\omega_1, \omega_2], \quad (3) \end{aligned}$$

where $\sigma(x + y\sqrt{d}) = x - y\sqrt{d}$ for all $x, y \in \mathbb{Z}$. If $\omega_1 = 1$ and $\omega_2 = \sqrt{d}$, then

$$\det \begin{bmatrix} z_{1,1} & z_{2,1} \\ z_{1,2} & z_{2,2} \end{bmatrix} = \det \begin{bmatrix} z_{1,1} & z_{1,2} \\ z_{2,1} & z_{2,2} \end{bmatrix} = 0,$$

and so there are elements $q_1, q_2 \in \mathbb{Q}$ not both zero with

$$\begin{bmatrix} z_{1,1} & z_{2,1} \\ z_{1,2} & z_{2,2} \end{bmatrix} \begin{bmatrix} q_1 \\ q_2 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}.$$

Hence,

$$\begin{aligned} 0 &= \omega_1(q_1 z_{1,1} + q_2 z_{2,1}) + \omega_2(q_1 z_{1,2} + q_2 z_{2,2}) \\ &= q_1(z_{1,1}\omega_1 + z_{1,2}\omega_2) + q_2(z_{2,1}\omega_1 + z_{2,2}\omega_2) \\ &= q_1\alpha_1 + q_2\alpha_2, \end{aligned}$$

which is a contradiction because the set $\{\alpha_1, \alpha_2\}$ is linearly independent in the vector space $\mathbb{Q}(\sqrt{d})$. Thus, $\Delta[\alpha_1, \alpha_2] \neq 0$, as desired. □

Exercise 2.11. Let $d \in \mathbb{Z} \setminus \{0, 1\}$ be a squarefree integer with $d \equiv 2, 3 \pmod 4$. Show that $\Delta[\alpha_1, \alpha_2] \neq 0$ whenever $\{\alpha_1, \alpha_2\}$ is a basis for the $\mathbb{Q}$-vector space $\mathbb{Q}(\sqrt{d})$.

Using Lemma 2.9 and Exercise 2.5, we obtain the following important result.

Corollary 2.12. Let $d \in \mathbb{Z} \setminus \{0, 1\}$ be a squarefree integer with $d \equiv 2, 3 \pmod 4$. The discriminant of each integral basis for $\mathbb{Z}[\sqrt{d}]$ is in $\mathbb{Z}^{\bullet}$.

Notation: Let $\mathbb{N}$ denote the set of positive integers, and set $\mathbb{N}_0 = \{0\} \cup \mathbb{N}$.

Theorem 2.13. *Let $d \in \mathbb{Z} \setminus \{0, 1\}$ be a squarefree integer with $d \equiv 2, 3 \pmod 4$. Any two integral bases for $\mathbb{Z}[\sqrt{d}]$ have the same discriminant.*

Proof. Let $\{\alpha_1, \alpha_2\}$ and $\{\omega_1, \omega_2\}$ be integral bases for $\mathbb{Z}[\sqrt{d}]$, and let $z_{i,j}$ be defined as in the proof of Proposition 2.10. Since $\Delta[\alpha_1, \alpha_2]$ and $\Delta[\omega_1, \omega_2]$ are both integers, Equation (3) in the proof of Proposition 2.10, along with the fact that $\left(\det \begin{bmatrix} z_{1,1} & z_{1,2} \\ z_{2,1} & z_{2,2} \end{bmatrix}\right)^2 \in \mathbb{N}$, implies that $\Delta[\omega_1, \omega_2]$ divides $\Delta[\alpha_1, \alpha_2]$. Using a similar argument, we can show that $\Delta[\alpha_1, \alpha_2]$ divides $\Delta[\omega_1, \omega_2]$. As both discriminants have the same sign, $\Delta[\alpha_1, \alpha_2] = \Delta[\omega_1, \omega_2]$. □

Using Example 2.6 and Example 2.8, we obtain the following corollary.

Corollary 2.14. Let $d \in \mathbb{Z} \setminus \{0, 1\}$ be a squarefree integer with $d \equiv 2, 3 \pmod 4$. Every integral basis for $\mathbb{Z}[\sqrt{d}]$ has discriminant $4d$.

3 General Properties of Ideals

Let R be a commutative ring with identity. In most beginning algebra classes, the units, irreducibles, and associate elements in R are standard concepts of interest. Recall that the units of R are precisely the invertible elements, while nonunit elements $x, y \in R$ are associates if $a = ub$ for a unit u of R. A nonunit $x \in R^\bullet := R \setminus \{0\}$ is irreducible if whenever $x = uv$ in R, then either u or v is a unit.

To truly understand factorizations in $\mathbb{Z}[\sqrt{-5}]$, we will need to know first how ideals of $\mathbb{Z}[\sqrt{-5}]$ are generated. Recall that a subset I of a commutative ring R with identity is called an ideal of R provided that I is a subring with the property that $rI \subseteq I$ for all $r \in R$. It follows immediately that if $x_1, \dots, x_k \in R$, then the set

$$I = \langle x_1, \dots, x_k \rangle = \{r_1x_1 + \cdots + r_kx_k \mid \text{ each } r_i \in R\}$$

is an ideal of R, that is, the ideal generated by $x_1, \dots, x_k$. Recall that I is said to be principal if $I = \langle x \rangle$ for some $x \in R$, and R is said to be a principal ideal domain (or a PID) if each ideal of R is principal. The zero ideal $\langle 0 \rangle$ and the entire ring $R = \langle 1 \rangle$ are principal ideals. May it be that all the ideals of $\mathbb{Z}[\sqrt{-5}]$ are principal? It turns out that the answer is "no" as we shall see in the next example.

Example 3.1. The ring of integers $\mathbb{Z}[\sqrt{-5}]$ is not a PID. We argue that the ideal

$$I = \langle 2, 1 + \sqrt{-5} \rangle$$

is not principal. If $I = \langle \alpha \rangle$, then α divides both 2 and $1 + \sqrt{-5}$. The reader will verify in Exercise 3.2 below that both of these elements are irreducible and nonassociates. Hence, $\alpha = \pm 1$ and $I = \langle \pm 1 \rangle = \mathbb{Z}[\sqrt{-5}]$. Now we show that $3 \notin I$. Suppose there exist $a, b, c, d \in \mathbb{Z}$ so that

$$(a + b\sqrt{-5})2 + (c + d\sqrt{-5})(1 + \sqrt{-5}) = 3.$$

Expanding the previous equality, we obtain

$$\begin{aligned} 2a + c - 5d &= 3 \\ 2b + c + d &= 0. \end{aligned} \tag{4}$$

After subtracting, we are left with $2(a - b) - 6d = 3$, which implies that 2 divides 3 in $\mathbb{Z}$, a contradiction.

Exercise 3.2. Show that the elements 2 and $1 + \sqrt{-5}$ are irreducible and nonassociates in $\mathbb{Z}[\sqrt{-5}]$. (Hint: use the norm function.)

Let us recall that a proper ideal I of a commutative ring R with identity is said to be prime if whenever $xy \in I$ for $x, y \in R$, then either $x \in I$ or $y \in I$. In addition, we know that an element $p \in R \setminus \{0\}$ is said to be prime provided that the principal ideal $\langle p \rangle$ is prime. It follows immediately that, in any integral domain, every prime element is irreducible.

Exercise 3.3. Let P be an ideal of a commutative ring R with identity. Show that P is prime if and only if the containment $IJ \subseteq P$ for ideals I and J of R implies that either $I \subseteq P$ or $J \subseteq P$.

Example 3.4. We argue that the ideal $I = \langle 2 \rangle$ is not prime in $\mathbb{Z}[\sqrt{-5}]$ and will in fact use Equation (1). Since $(1-\sqrt{-5})(1+\sqrt{-5}) = 2 \cdot 3$, it follows that

$$(1-\sqrt{-5})(1+\sqrt{-5}) \in \langle 2 \rangle.$$

Now if $1-\sqrt{-5} \in \langle 2 \rangle$, then there is an element $\alpha \in \mathbb{Z}[\sqrt{-5}]$ with $1-\sqrt{-5} = 2\alpha$. But then $\alpha = \frac{1}{2} - \frac{\sqrt{-5}}{2} \notin \mathbb{Z}[\sqrt{-5}]$, a contradiction. A similar argument works with $1+\sqrt{-5}$. Hence, $\langle 2 \rangle$ is not a prime ideal in $\mathbb{Z}[\sqrt{-5}]$.

We remind the reader that a proper ideal I of a commutative ring R with identity is called maximal if for each ideal J the containment $I \subseteq J \subseteq R$ implies that either $J = I$ or $J = R$. What we ask the reader to verify in the next exercise is a well-known result from basic abstract algebra.

Exercise 3.5. Let I be a proper ideal of a commutative ring R with identity, and let $R/I = \{r + I \mid r \in R\}$ be the quotient ring of R by I.

1. Show that I is prime if and only if R/I is an integral domain.
2. Show that I is maximal if and only if R/I is a field. Deduce that maximal ideals are prime.

Example 3.6. We expand our analysis of $I = \langle 2, 1+\sqrt{-5} \rangle$ in Example 3.1 by showing that I is a prime ideal in $\mathbb{Z}[\sqrt{-5}]$. To do this, we first argue that an element $\alpha = z_1 + z_2\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$ is contained in I if and only if z_1 and z_2 have the same parity. If $\alpha \in I$, then there are integers a, b, c, and d so that

$$z_1 + z_2\sqrt{-5} = (a + b\sqrt{-5})2 + (c + d\sqrt{-5})(1+\sqrt{-5}).$$

Adjusting the equations from (4) yields

$$\begin{aligned} 2a + c - 5d &= z_1 \\ 2b + c + d \ &= z_2. \end{aligned} \tag{5}$$

Notice that if $c \equiv d \pmod 2$, then both z_1 and z_2 are even, while $c \not\equiv d \pmod 2$ implies that both z_1 and z_2 are odd. Hence, z_1 and z_2 must have the same parity. Conversely, suppose that z_1 and z_2 have the same parity. As, clearly, every element of the form $2k_1 + 2k_2\sqrt{-5} = 2(k_1 + k_2\sqrt{-5})$ is in I, let us assume that z_1 and z_2 are both odd. The equations in (5) form a linear system that obviously has solutions over $\mathbb{Q}$ for any choice of z_1 and z_2 in $\mathbb{Z}$. By solving this system, we find that a and b are dependent variables and

$$a = \frac{z_1 - c + 5d}{2} \quad \text{and} \quad b = \frac{z_2 - c - d}{2}.$$

Letting c be any even integer and d any odd integer now yields a solution with both a and b integers. Thus, $z_1 + z_2\sqrt{-5} \in I$.

Now consider $\mathbb{Z}[\sqrt{-5}]/I$. As I is not principal (Example 3.1), $1 \notin I$. Therefore $1 + I \neq 0 + I$. If $c_1 + c_2\sqrt{-5} \notin I$, then c_1 and c_2 have opposite parity. If c_1 is odd and c_2 even, then $((c_1 - 1) + c_2\sqrt{-5}) + I = 0 + I$ implies that $(c_1 + c_2\sqrt{-5}) + I = 1 + I$. If c_1 is even and c_2 odd, then $((c_1 - 1) + c_2\sqrt{-5}) + I = 0 + I$ again implies that $(c_1 + c_2\sqrt{-5}) + I = 1 + I$. Hence, $\mathbb{Z}[\sqrt{-5}]/I \cong \{0 + I, 1 + I\} \cong \mathbb{Z}_2$. Since $\mathbb{Z}_2$ is a field, I is a maximal ideal and thus prime (by Exercise 3.5).

Exercise 3.7. Show that $\langle 3, 1 - 2\sqrt{-5}\rangle$ and $\langle 3, 1 + 2\sqrt{-5}\rangle$ are prime ideals in the ring of integers $\mathbb{Z}[\sqrt{-5}]$.

Let R be a commutative ring with identity. If every ideal of R is finitely generated, then R is called a *Noetherian ring*. In addition, R satisfies the *ascending chain condition on ideals* (ACC) if every increasing (under inclusion) sequence of ideals of R eventually stabilizes.

Exercise 3.8. Let R be a commutative ring with identity. Show that R is Noetherian if and only if it satisfies the ACC.

We shall see in Theorem 4.3 that the rings of integers $\mathbb{Z}[\sqrt{d}]$ are Noetherian and, therefore, satisfy the ACC.

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

In this section we explore the algebraic structure of all ideals of $\mathbb{Z}[\sqrt{-5}]$ under ideal multiplication, encapsulating the basic properties of multiplication of ideals. Let us begin by generalizing the notion of an integral basis, which also plays an important role in ideal theory.

Definition 4.1. Let K be an algebraic number field of dimension n as a vector space over $\mathbb{Q}$, and let I be a proper ideal of the ring of integers $\mathcal{O}_K$. The elements $\omega_1, \ldots, \omega_n \in I$ form an *integral basis* for I provided that for each $\beta \in I$ there exist unique $z_1, \ldots, z_n \in \mathbb{Z}$ satisfying that $\beta = z_1\omega_1 + \cdots + z_n\omega_n$.

With notation as in the above definition, notice that if $\{\omega_1, \ldots, \omega_n\}$ is an integral basis for I, then $I = \langle \omega_1, \ldots, \omega_n \rangle$. Care is needed here as the converse is not necessarily true. For instance, $\{3\}$ is not an integral basis for the ideal $I = \langle 3 \rangle$ of $\mathbb{Z}[\sqrt{-5}]$ (note that $3\sqrt{-5} \in I$).

Exercise 4.2. Argue that $\{3, 3\sqrt{-5}\}$ is an integral basis for the ideal $I = \langle 3 \rangle$ of the ring of integers $\mathbb{Z}[\sqrt{-5}]$.

We now show that every proper ideal of $\mathbb{Z}[\sqrt{-5}]$ has an integral basis.

Theorem 4.3. *Let $d \in \mathbb{Z} \setminus \{0,1\}$ be a squarefree integer with $d \equiv 2,3 \pmod 4$. Every nonzero proper ideal of $\mathbb{Z}[\sqrt{d}]$ has an integral basis. Hence, every ideal of $\mathbb{Z}[\sqrt{d}]$ is finitely generated.*

Proof. Let I be a nonzero proper ideal of $\mathbb{Z}[\sqrt{d}]$. To find an integral basis for I consider the collection $\mathscr{B}$ of all subsets of I which form a vector space basis for $\mathbb{Q}(\sqrt{d})$. Note that if $\{\omega_1, \omega_2\}$ is an integral basis for $\mathbb{Z}[\sqrt{d}]$ and $\alpha \in I^\bullet$, then the subset $\{\alpha\omega_1, \alpha\omega_2\}$ of I is also a linearly independent subset inside the vector space $\mathbb{Q}(\sqrt{d})$. As a result, the collection $\mathscr{B}$ is nonempty. As $I \subseteq \mathbb{Z}[\sqrt{d}]$, Proposition 2.10 ensures that $\Delta[\delta_1, \delta_2] \in \mathbb{Z}^\bullet$ for every member $\{\delta_1, \delta_2\}$ of $\mathscr{B}$. Then we can take a pair $\{\delta_1, \delta_2\}$ in $\mathscr{B}$ and assume that the absolute value of its discriminant, i.e., $|\Delta[\delta_1, \delta_2]|$, is as small as possible. We argue now that $\{\delta_1, \delta_2\}$ is an integral basis for I.

Assume, by way of contradiction, that $\{\delta_1, \delta_2\}$ is not an integral basis for I. Since $\{\delta_1, \delta_2\}$ is a basis for $\mathbb{Q}(\sqrt{d})$ as a vector space over $\mathbb{Q}$, there must exist $\beta \in I$ and $q_1, q_2 \in \mathbb{Q}$ such that $\beta = q_1\delta_1 + q_2\delta_2$, where not both q_1 and q_2 are in $\mathbb{Z}$. Without loss of generality, we can assume that $q_1 \in \mathbb{Q} \setminus \mathbb{Z}$. Write $q_1 = z + r$, where $z \in \mathbb{Z}$ and $0 < r < 1$. Let

$$\begin{aligned} \delta_1^* &= \beta - z\delta_1 = (q_1 - z)\delta_1 + q_2\delta_2 \\ \delta_2^* &= \delta_2. \end{aligned}$$

It is easy to verify that $\{\delta_1^*, \delta_2^*\}$ is linearly independent and thus is another vector space basis for $\mathbb{Q}(\sqrt{d})$ which consists of elements of I, that is, $\{\delta_1^*, \delta_2^*\}$ is a member of $\mathscr{B}$. Proceeding as we did in the proof of Proposition 2.10, we find that

$$\Delta[\delta_1^*, \delta_2^*] = r^2 \Delta[\delta_1, \delta_2];$$

this is because $\left(\det \begin{bmatrix} q_1 - z & q_2 \\ 0 & 1 \end{bmatrix}\right)^2 = r^2$. It immediately follows from $0 < r < 1$ that $|\Delta[\delta_1^*, \delta_2^*]| < |\Delta[\delta_1, \delta_2]|$, contradicting the minimality of $|\Delta[\delta_1, \delta_2]|$. Hence, $\{\delta_1, \delta_2\}$ is an integral basis for I, which completes the proof. □

Theorem 4.3 yields the next important corollary.

Corollary 4.4. Let $d \in \mathbb{Z} \setminus \{0,1\}$ be a squarefree integer with $d \equiv 2,3 \pmod 4$. If I is a proper ideal of the ring of integers $\mathbb{Z}[\sqrt{d}]$, then there exist elements $\alpha_1, \alpha_2 \in I$ such that $I = \langle \alpha_1, \alpha_2 \rangle$. Thus, $\mathbb{Z}[\sqrt{d}]$ is a Noetherian ring.

Remark. One can actually say much more. For d as in Corollary 4.4, the following stronger statement is true: if I is a nonzero proper ideal of $\mathbb{Z}[\sqrt{d}]$ and $\alpha_1 \in I^\bullet$, then there exists $\alpha_2 \in I$ satisfying that $I = \langle \alpha_1, \alpha_2 \rangle$. This condition is known as the $1\frac{1}{2}$-*generator property*. The interested reader can find a proof of this result in [9, Theorem 9.3].

Definition 4.5. A pair $(M, *)$, where M is a set and $*$ is a binary operation on M, is called a *monoid* if $*$ is associative and there exists $e \in M$ satisfying that $e * x = x * e = x$ for all $x \in M$. The element e is called the *identity element*. The monoid M is called *commutative* if the operation $*$ is commutative.

Let R be a commutative ring with identity. Recall that we have a natural multiplication on the collection consisting of all ideals of R, that is, for any two ideals I and J of R, the product

$$IJ = \Big\{ \sum_{i=1}^{k} a_i b_i \;\Big|\; k \in \mathbb{N},\ a_1, \dots, a_k \in I, \text{ and } b_1, \dots, b_k \in J \Big\} \tag{6}$$

is again an ideal. It is not hard to check that ideal multiplication is both associative and commutative, and satisfies that $RI = I$ for each ideal I of R. This amounts to arguing the following exercise.

Exercise 4.6. Let R be a commutative ring with identity. Show that the set of all ideals of R is a commutative monoid under ideal multiplication.

Example 4.7. To give the reader a notion of how ideal multiplication works, we show that

$$\langle 2, 1+\sqrt{-5}\rangle^2 = \langle 2 \rangle.$$

It follows by (6) that ideal multiplication can be achieved by merely multiplying generators. For instance,

$$\begin{aligned}\langle 2, 1+\sqrt{-5}\rangle^2 &= \langle 2, 1+\sqrt{-5}\rangle\langle 2, 1+\sqrt{-5}\rangle \\ &= \langle 4, 2(1+\sqrt{-5}), 2(1+\sqrt{-5}), -2(2-\sqrt{-5})\rangle.\end{aligned}$$

Since 2 divides each of the generators of $\langle 2, 1+\sqrt{-5}\rangle^2$ in $\mathbb{Z}[\sqrt{-5}]$, we clearly have that $\langle 2, 1+\sqrt{-5}\rangle^2 \subseteq \langle 2 \rangle$. To verify the reverse inclusion, let us first observe that $2\sqrt{-5} = 4 - 2(2-\sqrt{-5}) \in \langle 2, 1+\sqrt{-5}\rangle^2$. As $2\sqrt{-5} \in \langle 2, 1+\sqrt{-5}\rangle^2$, one immediately sees that $2 = 2(1+\sqrt{-5}) - 2\sqrt{-5} \in \langle 2, 1+\sqrt{-5}\rangle^2$. Hence, the inclusion $\langle 2 \rangle \subseteq \langle 2, 1+\sqrt{-5}\rangle^2$ holds, and equality follows.

Exercise 4.8. Verify that the next equalities hold:

$$\begin{aligned}\langle 3 \rangle &= \langle 3, 1-2\sqrt{-5}\rangle\langle 3, 1+2\sqrt{-5}\rangle, \\ \langle 1-\sqrt{-5}\rangle &= \langle 2, 1+\sqrt{-5}\rangle\langle 3, 1+2\sqrt{-5}\rangle, \\ \langle 1+\sqrt{-5}\rangle &= \langle 2, 1+\sqrt{-5}\rangle\langle 3, 1-2\sqrt{-5}\rangle.\end{aligned}$$

Example 4.8 is no accident. Indeed, every nonprincipal ideal of $\mathbb{Z}[\sqrt{-5}]$ has a multiple which is a principal ideal as it is established in the following theorem.

Theorem 4.9. *Let I be an ideal of $\mathbb{Z}[\sqrt{-5}]$. Then there exists a nonzero ideal J of $\mathbb{Z}[\sqrt{-5}]$ such that IJ is principal.*

Proof. If I is a principal ideal, then the result follows by letting $J = \langle 1 \rangle$. So suppose $I = \langle \alpha, \beta \rangle$ is not a principal ideal of $\mathbb{Z}[\sqrt{-5}]$, where $\alpha = a + b\sqrt{-5}$ and $\beta = c + d\sqrt{-5}$. Notice that it is enough to verify the existence of such an ideal J when $\gcd(a,b,c,d) = 1$, and we make this assumption. It is easy to check that $\alpha\overline{\beta} + \overline{\alpha}\beta = 2ac + 10bd \in \mathbb{Z}$. Hence, $\alpha\overline{\alpha}$, $\alpha\overline{\beta} + \overline{\alpha}\beta$, and $\beta\overline{\beta}$ are all integers. Let

$$\begin{aligned} f &= \gcd(\alpha\overline{\alpha}, \alpha\overline{\beta} + \overline{\alpha}\beta, \beta\bar{\beta}) \\ &= \gcd(a^2 + 5b^2, 2ac + 10bd, c^2 + 5d^2). \end{aligned}$$

Take $J = \langle \overline{\alpha}, \overline{\beta} \rangle$. We claim that $IJ = \langle f \rangle$. Since $f = \gcd(\alpha\overline{\alpha}, \alpha\overline{\beta} + \overline{\alpha}\beta, \beta\overline{\beta})$, there are integers z_1, z_2, and z_3 so that

$$f = z_1 \alpha\overline{\alpha} + z_2 \beta\overline{\beta} + z_3(\alpha\overline{\beta} + \overline{\alpha}\beta).$$

Because $IJ = \langle \alpha\overline{\alpha}, \alpha\overline{\beta}, \beta\overline{\alpha}, \beta\overline{\beta} \rangle$, we have that f is a linear combination of the generating elements. Thus, $f \in IJ$ and, therefore, $\langle f \rangle \subseteq IJ$.

To prove the reverse containment, we first show that f divides $bc - ad$. Suppose, by way of contradiction, that this is not the case. Notice that $25 \nmid f$; otherwise $25 \mid a^2 + 5b^2$ and $25 \mid c^2 + 5d^2$ would imply that $5 \mid \gcd(a,b,c,d)$. On the other hand, $4 \mid f$ would imply $4 \mid a^2 + 5b^2$ and $4 \mid c^2 + 5d^2$, forcing a, b, c, and d to be even, which is not possible as $\gcd(a,b,c,d) = 1$. Hence, $4 \nmid f$ and $25 \nmid f$. Because

$$\begin{aligned} 2c(a^2 + 5b^2) - a(2ac + 10bd) &= 10b(bc - ad) \\ 2a(c^2 + 5d^2) - c(2ac + 10bd) &= 10d(ad - bc), \end{aligned}$$

f must divide both $10b(bc - ad)$ and $10d(bc - ad)$. As, by assumption, $f \nmid bc - ad$, there must be a prime p and a natural n such that $p^n \mid f$ but $p^n \nmid bc - ad$. If $p = 2$, then $4 \nmid f$ forces $n = 1$. In this case, both $a^2 + 5b^2$ and $c^2 + 5d^2$ would be even, and so $2 \mid a - b$ and $2 \mid c - d$, which implies that $2 \mid bc - ad$, a contradiction. Thus, $p \neq 2$. On the other hand, if $p = 5$, then again $n = 1$. In this case, $5 \mid a^2 + 5b^2$ and $5 \mid c^2 + 5d^2$ and so 5 would divide both a and c, contradicting that $5 \nmid bc - ad$. Then, we can assume that $p \notin \{2,5\}$. As $p^n \mid 10b(bc - ad)$ but $p^n \nmid bc - ad$, we have that $p \mid 10b$. Similarly, $p \mid 10d$. Since $p \notin \{2,5\}$, it follows that $p \mid b$ and $p \mid d$. Now the fact that p divides both $a^2 + 5b^2$ and $c^2 + 5d^2$ yields that $p \mid a$ and $p \mid c$, contradicting that $\gcd(a,b,c,d) = 1$. Hence, $f \mid bc - ad$.

Let us verify now that $f \mid ac + 5bd$. If f is odd, then $f \mid ac + 5bd$. Assume, therefore, that $f = 2f_1$, where $f_1 \in \mathbb{Z}$. As $4 \nmid f$, the integer f_1 is odd. Now, $f \mid a^2 + 5b^2$ implies that a and b have the same parity. Similarly, one sees that c and d have the same parity. As a consequence, $ac + 5bd$ is even. Since f_1 is odd, it must divide $(ac + 5bd)/2$, which means that f divides $ac + 5bd$, as desired.

Because f divides both $\alpha\overline{\alpha}$ and $\beta\overline{\beta}$ in $\mathbb{Z}$, proving that $IJ \subseteq \langle f \rangle$ amounts to verifying that f divides both $\alpha\overline{\beta}$ and $\overline{\alpha}\beta$ in $\mathbb{Z}[\sqrt{-5}]$. Since f divides both $ac+5bd$ and $bc-ad$ in $\mathbb{Z}$, one has that

$$x = \frac{ac+5bd}{f} \in \mathbb{Z} \quad \text{and} \quad y = \frac{bc-ad}{f} \in \mathbb{Z}.$$

Therefore

$$\alpha\overline{\beta} = ac+5bd+(bc-ad)\sqrt{-5} = (x+y\sqrt{-5})f \in \langle f \rangle.$$

Also, $\overline{\alpha}\beta = \overline{\alpha\overline{\beta}} = (x-y\sqrt{-5})f \in \langle f \rangle$. Hence, the reverse inclusion $IJ \subseteq \langle f \rangle$ also holds, which completes the proof. □

A commutative monoid $(M,*)$ is said to be *cancellative* if for all $a,b,c \in M$, the equality $a*b = a*c$ implies that $b = c$. By Exercise 4.6, the set

$$\mathscr{I} := \{I \mid I \text{ is an ideal of } \mathbb{Z}[\sqrt{-5}]\}$$

is a commutative monoid. As the next corollary states, the set $\mathscr{I}^\bullet := \mathscr{I} \setminus \{\langle 0 \rangle\}$ is indeed a commutative cancellative monoid.

Corollary 4.10. The set $\mathscr{I}^\bullet$ under ideal multiplication is a commutative cancellative monoid.

Proof. Because $\mathscr{I}$ is a commutative monoid under ideal multiplication, it immediately follows that $\mathscr{I}^\bullet$ is also a commutative monoid. To prove that $\mathscr{I}^\bullet$ is cancellative, take $I,J,K \in \mathscr{I}^\bullet$ such that $IJ = IK$. By Theorem 4.9, there exists an ideal I' of $\mathbb{Z}[\sqrt{-5}]$ and $x \in \mathbb{Z}[\sqrt{-5}]^\bullet$ with $I'I = \langle x \rangle$. Then

$$\langle x \rangle J = I'IJ = I'IK = \langle x \rangle K.$$

As $x \neq 0$ and the product in $\mathbb{Z}[\sqrt{-5}]^\bullet$ is cancellative, $J = K$. □

5 The Fundamental Theorem of Ideal Theory

We devote this section to prove a version of the Fundamental Theorem of Ideal Theory for the ring of integers $\mathbb{Z}[\sqrt{-5}]$. To do this, we need to develop a few tools. In particular, we introduce the concept of a fractional ideal of $\mathbb{Z}[\sqrt{-5}]$ and show that the set of such fractional ideals is an abelian group.

Let us begin by exploring the relationship between the concepts of prime and maximal ideals. We recall that every proper ideal of a commutative ring R with identity is contained in a maximal ideal, which implies, in particular, that maximal ideals always exist.

Exercise 5.1. Show that every maximal ideal of a commutative ring with identity is prime.

Prime ideals, however, are not necessarily maximal. The following example sheds some light upon this observation.

Example 5.2. Let $\mathbb{Z}[X]$ denote the ring of polynomials with integer coefficients. Clearly, $\mathbb{Z}[X]$ is an integral domain. It is not hard to verify that the ideal $\langle X \rangle$ of $\mathbb{Z}[X]$ is prime. Because $2 \notin \langle X \rangle$, one obtains that $\langle X \rangle \subsetneq \langle 2, X \rangle$. It is left to the reader to argue that $\langle 2, X \rangle$ is a proper ideal of $\mathbb{Z}[X]$. Since $\langle X \rangle \subsetneq \langle 2, X \rangle \subsetneq \mathbb{Z}[X]$, it follows that $\langle X \rangle$ is not a maximal ideal of $\mathbb{Z}[X]$. (An alternate argument can easily be given using Exercise 3.5.)

In the ring of integers $\mathcal{O}_K$ of any algebraic number field K, every nonzero prime ideal is maximal (see, for instance, [6, Proposition 5.21]). Let us establish this result here for our case of interest.

Proposition 5.3. *Let $d \in \mathbb{Z} \setminus \{0,1\}$ be a squarefree integer with $d \equiv 2,3 \pmod 4$. Then every nonzero prime ideal of $\mathbb{Z}[\sqrt{d}]$ is maximal.*

Proof. Let P be a nonzero prime ideal in $\mathbb{Z}[\sqrt{d}]$, and let $\{\omega_1, \omega_2\}$ be an integral basis for $\mathbb{Z}[\sqrt{d}]$. Fix $\beta \in P^\bullet$. Note that $n := N(\beta) = \beta\bar{\beta} \in P \cap \mathbb{N}$. Consider the finite subset

$$S = \big\{ n_1\omega_1 + n_2\omega_2 + P \mid n_1, n_2 \in \{0, 1, \dots, n-1\} \big\}$$

of $\mathbb{Z}[\sqrt{d}]/P$. Take $x \in \mathbb{Z}[\sqrt{d}]$. As $\{\omega_1, \omega_2\}$ is an integral basis, there exist $z_1, z_2 \in \mathbb{Z}$ such that $x = z_1\omega_1 + z_2\omega_2$ and, therefore, $x + P = n_1\omega_1 + n_2\omega_2 + P \in S$, where $n_i \in \{0, \dots, n-1\}$ and $n_i \equiv z_i \pmod n$. Hence, $\mathbb{Z}[\sqrt{d}]/P = S$, which implies that $\mathbb{Z}[\sqrt{d}]/P$ is finite. It follows by Exercise 3.5(1) that $\mathbb{Z}[\sqrt{d}]/P$ is an integral domain. As a result, $\mathbb{Z}[\sqrt{d}]/P$ is a field (see Exercise 5.4 below). Thus, Exercise 3.5(2) guarantees that P is a maximal ideal. □

Exercise 5.4. Let R be a finite integral domain. Show that R is a field.

Although the concepts of (nonzero) prime and maximal ideals coincide in $\mathbb{Z}[\sqrt{d}]$, we will use both terms depending on the ideal property we are willing to apply.

Lemma 5.5. *If I is a nonzero ideal of a Noetherian ring R, then there exist nonzero prime ideals $P_1, \dots, P_n$ of R such that $P_1 \cdots P_n \subseteq I$.*

Proof. Assume, by way of contradiction, that the statement of the lemma does not hold. Because R is a Noetherian ring and, therefore, satisfies the ACC, there exists an ideal I of R that is maximal among all the ideals failing to satisfy the statement of the lemma. Clearly, I cannot be prime. By Exercise 3.3, there exist ideals J and K of R such that $JK \subseteq I$ but neither $J \subseteq I$ nor $K \subseteq I$. Now notice that the ideals $J' = I + J$ and $K' = I + K$ both strictly contain I. The maximality of I implies that both J' and K' contain products of nonzero prime ideals. Now the fact that $J'K' \subseteq I$ would also imply that I contains a product of nonzero prime ideals, a contradiction. □

Recall that if R is an integral domain contained in a field F, then the field of fractions of R is the smallest subfield of F containing R. If K is an algebraic number field, then it is not hard to argue that the field of fractions of $\mathscr{O}_K$ is precisely K.

Definition 5.6. Let R be an integral domain with field of fractions F. A *fractional ideal* of R is a subset of F of the form $\alpha^{-1}I$, where $\alpha \in R^\bullet$ and I is an ideal of R.

With notation as in the previous definition, it is clear that every ideal of R is a fractional ideal. However, fractional ideals are not necessarily ideals. The product of fractional ideals is defined similarly to the product of standard ideals. Therefore it is easily seen that the product of two fractional ideals is again a fractional ideal. Indeed, for elements α and β of $R^\bullet$ and for ideals I and J of R, we only need to observe that $(\alpha^{-1}I)(\beta^{-1}J) = (\alpha\beta)^{-1}IJ$.

Notation: Let $\mathscr{F}$ denote the set of all fractional ideals of $\mathbb{Z}[\sqrt{-5}]$, and set $\mathscr{F}^\bullet := \mathscr{F} \setminus \{\langle 0 \rangle\}$.

Definition 5.7. Let R be an integral domain with field of fractions F. For a fractional ideal I of R, the set

$$I^{-1} := \{\alpha \in F \mid \alpha I \subseteq R\}$$

is called the *inverse* of I.

Exercise 5.8. Show that the inverse of a fractional ideal is again a fractional ideal.

Lemma 5.9. *Let $d \in \mathbb{Z} \setminus \{0,1\}$ be a squarefree integer with $d \equiv 2,3 \pmod 4$. If I is a proper ideal of the ring of integers $\mathbb{Z}[\sqrt{d}]$, then $\mathbb{Z}[\sqrt{d}]$ is strictly contained in the fractional ideal I^{-1}.*

Proof. Since I is a proper ideal of $\mathbb{Z}[\sqrt{d}]$, then there exists a maximal ideal M of $\mathbb{Z}[\sqrt{d}]$ containing I. Fix $\alpha \in M^\bullet$. By the definition of the inverse of an ideal, $\mathbb{Z}[\sqrt{d}] \subseteq M^{-1}$. Since $\mathbb{Z}[\sqrt{d}]$ is a Noetherian ring, Lemma 5.5 ensures the existence of $m \in \mathbb{N}$ and prime ideals $P_1, \dots, P_m$ in $\mathbb{Z}[\sqrt{d}]$ such that $P_1 \cdots P_m \subseteq \langle \alpha \rangle \subseteq M$. Assume that m is the minimum natural number satisfying this property. Since M is a prime ideal (Exercise 5.1), by Exercise 3.3 there exists $P \in \{P_1, \dots, P_m\}$ such that $P \subseteq M$. There is no loss of generality in assuming that $P = P_1$. Now, by Proposition 5.3, the ideal P_1 is maximal, which implies that $P_1 = M$. By the minimality of m, there exists $\alpha' \in P_2 \cdots P_m \setminus \langle \alpha \rangle$. Therefore, we find that $\alpha^{-1}\alpha' \notin \mathbb{Z}[\sqrt{d}]$ and $\alpha' M = \alpha' P_1 \subseteq P_1 \cdots P_m \subseteq \langle \alpha \rangle$, that is $\alpha^{-1}\alpha' M \subseteq \langle 1 \rangle = \mathbb{Z}[\sqrt{d}]$. As a result, $\alpha^{-1}\alpha' \in M^{-1} \setminus \mathbb{Z}[\sqrt{d}]$. Hence, we find that $\mathbb{Z}[\sqrt{d}] \subsetneq M^{-1} \subseteq I^{-1}$, and the proof follows. □

We focus throughout the remainder of our work on the ring of integers $\mathbb{Z}[\sqrt{-5}]$. This, via Theorem 4.9, will substantially simplify our remaining arguments.

Lemma 5.10. *If $I \in \mathscr{I}^\bullet$ and $\alpha \in \mathbb{Q}(\sqrt{-5})$, then $\alpha I \subseteq I$ implies $\alpha \in \mathbb{Z}[\sqrt{-5}]$.*

Proof. Let I and α be as in the statement of the lemma. By Theorem 4.9, there exists a nonzero ideal J of $\mathbb{Z}[\sqrt{-5}]$ such that $IJ = \langle \beta \rangle$ for some $\beta \in \mathbb{Z}[\sqrt{-5}]$. Then $\alpha\langle \beta \rangle = \alpha IJ \subseteq IJ = \langle \beta \rangle$, which means that $\alpha\beta = \sigma\beta$ for some $\sigma \in \mathbb{Z}[\sqrt{-5}]$. As $\beta \neq 0$, it follows that $\alpha = \sigma \in \mathbb{Z}[\sqrt{-5}]$. □

Theorem 5.11. *The set $\mathscr{F}^\bullet$ is an abelian group under multiplication of fractional ideals.*

Proof. Clearly, multiplication of fractional ideals is associative. In addition, it immediately follows that the fractional ideal $\mathbb{Z}[\sqrt{-5}] = 1^{-1}\langle 1 \rangle$ is the identity. The most involved part of the proof consists in arguing that each fractional ideal is invertible.

Let $M \in \mathscr{I}^\bullet$ be a maximal ideal of $\mathbb{Z}[\sqrt{-5}]$. By definition of M^{-1}, we have that $MM^{-1} \subseteq \mathbb{Z}[\sqrt{-5}]$, which implies that $MM^{-1} \in \mathscr{I}^\bullet$. As $M = M\mathbb{Z}[\sqrt{-5}] \subseteq MM^{-1}$ and M is maximal, $MM^{-1} = M$ or $MM^{-1} = \mathbb{Z}[\sqrt{-5}]$. As M is proper, Lemma 5.9 ensures that M^{-1} strictly contains $\mathbb{Z}[\sqrt{-5}]$, which implies, by Lemma 5.10, that $MM^{-1} \neq M$. So $MM^{-1} = \mathbb{Z}[\sqrt{-5}]$. As a result, each maximal ideal of $\mathbb{Z}[\sqrt{-5}]$ is invertible.

Now suppose, by way of contradiction, that not every ideal in $\mathscr{I}^\bullet$ is invertible. Among all the nonzero non-invertible ideals take one, say J, maximal under inclusion (this is possible because $\mathbb{Z}[\sqrt{-5}]$ satisfies the ACC). Because $\mathbb{Z}[\sqrt{-5}]$ is an invertible fractional ideal, $J \subsetneq \mathbb{Z}[\sqrt{-5}]$. Let M be a maximal ideal containing J. By Lemma 5.9, one has that $\mathbb{Z}[\sqrt{-5}] \subsetneq M^{-1} \subseteq J^{-1}$. This, along with Lemma 5.10, yields $J \subsetneq JM^{-1} \subseteq JJ^{-1} \subseteq \mathbb{Z}[\sqrt{-5}]$. Thus, JM^{-1} is an ideal of $\mathbb{Z}[\sqrt{-5}]$ strictly containing J. The maximality of J now implies that $JM^{-1}(JM^{-1})^{-1} = \mathbb{Z}[\sqrt{-5}]$ and, therefore, $M^{-1}(JM^{-1})^{-1} \subseteq J^{-1}$. Then

$$\mathbb{Z}[\sqrt{-5}] = JM^{-1}(JM^{-1})^{-1} \subseteq JJ^{-1} \subseteq \mathbb{Z}[\sqrt{-5}],$$

which forces $JJ^{-1} = \mathbb{Z}[\sqrt{-5}]$, a contradiction.

Finally, take $F \in \mathscr{F}^\bullet$. Then there exist an ideal $I \in \mathscr{I}^\bullet$ and $\alpha \in \mathbb{Z}[\sqrt{-5}]^\bullet$ such that $F = \alpha^{-1}I$. So one obtains that

$$(\alpha I^{-1})F = (\alpha I^{-1})(\alpha^{-1}I) = I^{-1}I = \mathbb{Z}[\sqrt{-5}].$$

As a consequence, the fractional ideal αI^{-1} is the inverse of F in $\mathscr{F}^\bullet$. Because each nonzero fractional ideal of $\mathbb{Z}[\sqrt{-5}]$ is invertible, $\mathscr{F}^\bullet$ is a group. Since the multiplication of fractional ideals is commutative, $\mathscr{F}^\bullet$ is abelian. □

Corollary 5.12. If $I \in \mathscr{I}^\bullet$ and $\alpha \in I^\bullet$, then $IJ = \langle \alpha \rangle$ for some $J \in \mathscr{I}^\bullet$.

Proof. Let I and α be as in the statement of the corollary. As $\alpha^{-1}I$ is a nonzero fractional ideal, there exists a nonzero fractional ideal J such that $\alpha^{-1}IJ = \mathbb{Z}[\sqrt{-5}]$, that is $IJ = \langle \alpha \rangle$. Since $\beta I \subseteq JI = \langle \alpha \rangle \subseteq I$ for all $\beta \in J$, Lemma 5.10 guarantees that $J \subseteq \mathbb{Z}[\sqrt{-5}]$. Hence, J is a nonzero ideal of $\mathbb{Z}[\sqrt{-5}]$. □

Theorem 5.13. *[The Fundamental Theorem of Ideal Theory] Let I be a nonzero proper ideal of $\mathbb{Z}[\sqrt{-5}]$. There exists a unique (up to order) list of prime ideals $P_1,\dots,P_k$ of $\mathbb{Z}[\sqrt{-5}]$ such that $I = P_1 \cdots P_k$.*

Proof. Suppose, by way of contradiction, that not every ideal in $\mathscr{I}^\bullet$ can be written as the product of prime ideals. From the set of ideals of $\mathbb{Z}[\sqrt{-5}]$ which are not the product of primes ideals, take one, say I, maximal under inclusion. Clearly, I is not prime. Therefore I is contained in a maximal ideal P_1, and such containment must be strict by Exercise 5.1. By Lemma 5.9, one has that $\mathbb{Z}[\sqrt{-5}] \subsetneq P_1^{-1}$ and so $I \subseteq IP_1^{-1}$. Now Lemma 5.10 ensures that the latter inclusion is strict. The maximality of I now implies that $IP_1^{-1} = P_2 \cdots P_k$ for some prime ideals $P_2,\dots,P_k$. This, along with Theorem 5.11, ensures that $I = P_1 \cdots P_k$, a contradiction.

To argue uniqueness, let us assume, by contradiction, that there exists an ideal having two distinct prime factorizations. Let m be the minimum natural number such that there exists $I \in \mathscr{I}$ with two distinct factorizations into prime ideals, one of them containing m factors. Suppose that

$$I = P_1 \cdots P_m = Q_1 \cdots Q_n. \tag{7}$$

Because $Q_1 \cdots Q_n \subseteq P_m$, there exists $Q \in \{Q_1,\dots,Q_n\}$ such that $Q \subseteq P_m$ (Exercise 3.3). By Proposition 5.3, both Q and P_m are maximal ideals, which implies that $P_m = Q$. As $IQ^{-1} \subseteq II^{-1} \subseteq \mathbb{Z}[\sqrt{-5}]$, it follows that $IQ^{-1} \in \mathscr{I}$. Multiplying the equality (7) by the fractional ideal Q^{-1}, we obtain that IQ^{-1} is an ideal of $\mathbb{Z}[\sqrt{-5}]$ with two distinct factorizations into prime ideals such that one of them, namely $P_1 \cdots P_{m-1}$, contains less than m factors. As this contradicts the minimality of m, uniqueness follows. □

An element a of a commutative monoid M is said to be an *atom* if for all $x,y \in M$ such that $a = xy$, either x is a unit or y is a unit (i.e., has an inverse). A commutative cancellative monoid is called *atomic* if every nonzero nonunit element can be factored into atoms.

Corollary 5.14. The monoid $\mathscr{I}^\bullet$ is atomic.

6 The Class Group

To understand the phenomenon of non-unique factorization in $\mathbb{Z}[\sqrt{-5}]$, we first need to understand certain classes of ideals of $\mathbb{Z}[\sqrt{-5}]$. Let

$$\mathscr{P} := \{I \in \mathscr{I} \mid I \text{ is a principal ideal of } \mathbb{Z}[\sqrt{-5}]\}.$$

Two ideals $I,J \in \mathscr{I}$ are *equivalent* if $\langle\alpha\rangle I = \langle\beta\rangle J$ for some $\alpha,\beta \in \mathbb{Z}[\sqrt{-5}]^\bullet$. In this case, we write $I \sim J$. It is clear that $\sim$ defines an equivalence relation on $\mathbb{Z}[\sqrt{-5}]$.

The equivalence classes of $\sim$ are called *ideal classes*. Let $I\mathscr{P}$ denote the ideal class of I, and we also let $\mathscr{C}(\mathbb{Z}[\sqrt{-5}])$ denote the set of all nonzero ideal classes. Now define a binary operation $*$ on $\mathscr{C}(\mathbb{Z}[\sqrt{-5}])$ by

$$I\mathscr{P} * J\mathscr{P} = (IJ)\mathscr{P}.$$

It turns out that $\mathscr{C}(\mathbb{Z}[\sqrt{-5}])$ is, indeed, a group under the $*$ operation.

Theorem 6.1. *The set of ideal classes $\mathscr{C}(\mathbb{Z}[\sqrt{-5}])$ is an abelian group under $*$.*

Proof. Because the product of ideals is associative and commutative, so is $*$. Also, it follows immediately that $\langle 1\rangle\mathscr{P} * I\mathscr{P} = (\langle 1\rangle I)\mathscr{P} = I\mathscr{P}$ for each $I \in \mathscr{I}^\bullet$, which means that $\mathscr{P} = \langle 1\rangle\mathscr{P}$ is the identity element of $\mathscr{C}(\mathbb{Z}[\sqrt{-5}])$. In addition, as any two nonzero principal ideals are in the same ideal class, Theorem 4.9 ensures that, for any $I\mathscr{P} \in \mathscr{C}(\mathbb{Z}[\sqrt{-5}])$, there exists $J \in \mathscr{I}^\bullet$ such that $I\mathscr{P} * J\mathscr{P} = IJ \in \mathscr{P} = \langle 1\rangle\mathscr{P}$. So $J\mathscr{P}$ is the inverse of $I\mathscr{P}$ in $\mathscr{C}(\mathbb{Z}[\sqrt{-5}])$. Hence, $\mathscr{C}(\mathbb{Z}[\sqrt{-5}])$ is an abelian group. □

Definition 6.2. The group $\mathscr{C}(\mathbb{Z}[\sqrt{-5}])$ is called the *class group* of $\mathbb{Z}[\sqrt{-5}]$, and the order of $\mathscr{C}(\mathbb{Z}[\sqrt{-5}])$ is called the *class number* of $\mathbb{Z}[\sqrt{-5}]$.

Recall that if $\theta\colon R \to S$ is a ring homomorphism, then $\ker\theta = \{r \in R \mid \theta(r) = 0\}$ is an ideal of R. Moreover, the First Isomorphism Theorem for rings states that $R/\ker\theta \cong \theta(R)$.

Definition 6.3. Let K be an algebraic number field. For any nonzero ideal I of $\mathscr{O}_K$, the cardinality $|\mathscr{O}_K/I|$ is called the *norm* of I and is denoted by $N(I)$.

Proposition 6.4. *Let $d \in \mathbb{Z}\setminus\{0,1\}$ be a squarefree integer with $d \equiv 2,3 \pmod 4$. Then $N(I)$ is finite for all nonzero ideals I of $\mathbb{Z}[\sqrt{d}]$.*

Proof. Take $n = \alpha\bar{\alpha}$ for any nonzero $\alpha \in I$. Then $n \in I \cap \mathbb{N}$. As $\langle n\rangle \subseteq I$, it follows that $|\mathbb{Z}[\sqrt{d}]/I| \le |\mathbb{Z}[\sqrt{d}]/\langle n\rangle|$. In addition, each element of $\mathbb{Z}[\sqrt{d}]/\langle n\rangle$ has a representative $n_1 + n_2\sqrt{d}$ with $n_1, n_2 \in \{0, 1, \dots, n-1\}$. Hence, $\mathbb{Z}[\sqrt{d}]/\langle n\rangle$ is finite and, therefore, $N(I) = |\mathbb{Z}[\sqrt{d}]/I| < \infty$. □

As ideal norms generalize the notion of standard norms given in (2), we expect they satisfy some similar properties. Indeed, this is the case.

Exercise 6.5. Let I and P be a nonzero ideal and a nonzero prime ideal of $\mathbb{Z}[\sqrt{-5}]$, respectively. Show that $|\mathbb{Z}[\sqrt{-5}]/P| = |I/IP|$.

Proposition 6.6. *$N(IJ) = N(I)N(J)$ for all $I, J \in \mathscr{I}^\bullet$.*

Proof. By factoring J as the product of prime ideals (Theorem 5.13) and applying induction on the number of factors, we can assume that J is a prime ideal. Consider the ring homomorphism $\theta \colon \mathbb{Z}[\sqrt{-5}]/IJ \to \mathbb{Z}[\sqrt{-5}]/I$ defined by $\theta(\alpha + IJ) = \alpha + I$. It follows immediately that θ is surjective and $\ker \theta = \{\alpha + IJ \mid \alpha \in I\}$. Therefore

$$\frac{\mathbb{Z}[\sqrt{-5}]/IJ}{I/IJ} \cong \mathbb{Z}[\sqrt{-5}]/I$$

by the First Isomorphism Theorem. As IJ is nonzero, $|\mathbb{Z}[\sqrt{-5}]/IJ| = N(IJ)$ is finite and so $|\mathbb{Z}[\sqrt{-5}]/IJ| = |\mathbb{Z}[\sqrt{-5}]/I| \cdot |I/IJ|$. Since J is prime, we can use Exercise 6.5 to conclude that

$$\begin{aligned} N(IJ) &= |\mathbb{Z}[\sqrt{-5}]/IJ| = |\mathbb{Z}[\sqrt{-5}]/I| \cdot |I/IJ| \\ &= |\mathbb{Z}[\sqrt{-5}]/I| \cdot |\mathbb{Z}[\sqrt{-5}]/J| = N(I)N(J). \end{aligned}$$

□

Corollary 6.7. If $N(I)$ is prime for some $I \in \mathscr{I}^\bullet$, then I is a prime ideal.

Let us verify now that the ideal norm is consistent with the standard norm on principal ideals.

Proposition 6.8. $N(\langle \alpha \rangle) = N(\alpha)$ *for all* $\alpha \in \mathbb{Z}[\sqrt{-5}]^\bullet$.

Proof. Set $S = \big\{a + b\sqrt{-5} \mid a, b \in \{0, 1, \dots, n-1\}\big\}$. Clearly, $|S| = n^2$. In addition,

$$\mathbb{Z}[\sqrt{-5}]/\langle n \rangle = \{s + \langle n \rangle \mid s \in S\}.$$

Note that if $s + \langle n \rangle = s' + \langle n \rangle$ for $s, s' \in S$, then we have $s = s'$. As a consequence, $N(\langle n \rangle) = n^2 = N(n)$ for each $n \in \mathbb{N}$. It is also easily seen that the map $\theta \colon \mathbb{Z}[\sqrt{-5}] \to \mathbb{Z}[\sqrt{-5}]/\langle \bar{\alpha} \rangle$ defined by $\theta(x) = \bar{x} + \langle \bar{\alpha} \rangle$ is a surjective ring homomorphism with $\ker \theta = \langle \alpha \rangle$. Therefore the rings $\mathbb{Z}[\sqrt{-5}]/\langle \alpha \rangle$ and $\mathbb{Z}[\sqrt{-5}]/\langle \bar{\alpha} \rangle$ are isomorphic by the First Isomorphism Theorem. This implies that $N(\langle \alpha \rangle) = N(\langle \bar{\alpha} \rangle)$. Because $\alpha\bar{\alpha} \in \mathbb{N}$, using Proposition 6.6, one obtains

$$N(\langle \alpha \rangle) = \sqrt{N(\langle \alpha \rangle) N(\langle \bar{\alpha} \rangle)} = \sqrt{N(\langle \alpha\bar{\alpha} \rangle)} = \alpha\bar{\alpha} = N(\alpha).$$

□

Lemma 6.9. *If P is a nonzero prime ideal in $\mathbb{Z}[\sqrt{-5}]$, then P divides exactly one ideal $\langle p \rangle$, where p is a prime number.*

Proof. For $\alpha \in P^\bullet$, it follows that $z = \alpha\bar{\alpha} \in P \cap \mathbb{N}$. Then, writing $z = p_1 \cdots p_k$ for some prime numbers $p_1, \dots, p_k$, we get $\langle z \rangle = \langle p_1 \rangle \cdots \langle p_k \rangle$. As $\langle p_1 \rangle \cdots \langle p_k \rangle \subseteq P$, we have that $\langle p_i \rangle \subseteq P$ for some $i \in \{1, \dots, k\}$ (Exercise 3.3). As $p_i \in P^\bullet$, Corollary 5.12

ensures that P divides $\langle p_i \rangle$. For the uniqueness, note that if P divides $\langle p \rangle$ and $\langle p' \rangle$ for distinct primes p and p', then the fact that $mp + np' = 1$ for some $m, n \in \mathbb{Z}$ would imply that P divides the full ideal $\langle 1 \rangle = \mathbb{Z}[\sqrt{-5}]$, a contradiction.

□

Theorem 6.10. *The class group of* $\mathbb{Z}[\sqrt{-5}]$ *is* $\mathbb{Z}_2$.

Proof. First, we verify that every nonzero ideal I of $\mathbb{Z}[\sqrt{-5}]$ contains a nonzero element α with $N(\alpha) \le 6N(I)$. For $I \in \mathscr{I}^\bullet$, take $B = \lfloor \sqrt{N(I)} \rfloor$ and define

$$S_I := \big\{ a + b\sqrt{-5} \mid a, b \in \{0, 1, \dots, B\} \big\} \subsetneq \mathbb{Z}[\sqrt{-5}].$$

Observe that $|S_I| = (B+1)^2 > N(I)$. Thus, there exist $\alpha_1 = a_1 + b_1\sqrt{-5} \in S_I$ and $\alpha_2 = a_2 + b_2\sqrt{-5} \in S_I$ such that $\alpha = \alpha_1 - \alpha_2 \in I \setminus \{0\}$ and

$$N(\alpha) = (a_1 - a_2)^2 + 5(b_1 - b_2)^2 \le 6B^2 \le 6N(I).$$

Now, let $I\mathscr{P}$ be a nonzero ideal class of $\mathbb{Z}[\sqrt{-5}]$. Take $J \in \mathscr{I}^\bullet$ satisfying $IJ\mathscr{P} = \mathscr{P}$. By the argument given in the previous paragraph, there exists $\beta \in J^\bullet$ such that $N(\beta) \le 6N(J)$. By Corollary 5.12, there exists an ideal $K \in \mathscr{I}^\bullet$ such that $JK = \langle \beta \rangle$. Using Proposition 6.6 and Proposition 6.8, one obtains

$$N(J)N(K) = N(\langle \beta \rangle) = N(\beta) \le 6N(J),$$

which implies that $N(K) \le 6$. Because $KJ \sim IJ$ (they are both principal), it follows that $K \in I\mathscr{P}$. Hence, every nonzero ideal class of $\mathbb{Z}[\sqrt{-5}]$ contains an ideal whose norm is at most 6.

To show that the class group of $\mathbb{Z}[\sqrt{-5}]$ is $\mathbb{Z}_2$, let us first determine the congruence relations among ideals of norm at most 6. Every ideal P of norm $p \in \{2, 3, 5\}$ must be prime by Corollary 6.7. Moreover, by Lemma 6.9, Theorem 5.13, and Proposition 6.6, the ideal P must show in the prime factorization

$$\langle p \rangle = P_1^{n_1} \cdots P_k^{n_k} \tag{8}$$

of the ideal $\langle p \rangle$. The following ideal factorizations have been already verified in Example 4.7 and Exercise 4.8:

$$\begin{aligned} \langle 2 \rangle &= \langle 2, 1 + \sqrt{-5} \rangle^2, \\ \langle 3 \rangle &= \langle 3, 1 - 2\sqrt{-5} \rangle \langle 3, 1 + 2\sqrt{-5} \rangle, \\ \langle 5 \rangle &= \langle \sqrt{-5} \rangle^2. \end{aligned} \tag{9}$$

In addition, we have proved in Example 3.6 and Exercise 3.7 that the ideals on the right-hand side of the first two equalities in (9) are prime. Also, the fact that $N(\langle \sqrt{-5} \rangle) = N(\sqrt{-5}) = 5$ implies that the ideal $\langle \sqrt{-5} \rangle$ is prime. It follows now by the uniqueness of Theorem 5.13 that the ideals on the right-hand side of the equalities (9) are the only ideals of $\mathbb{Z}[\sqrt{-5}]$ having norm in the set $\{2,3,5\}$. Once again, combining Lemma 6.9, Theorem 5.13, and Proposition 6.6, we obtain that any ideal I whose norm is 4 must be a product of prime ideals dividing $\langle 2\rangle$, which forces $I=\langle 2\rangle$. Similarly, any ideal J with norm 6 must be the product of ideals dividing the ideals $\langle 2\rangle$ and $\langle 3\rangle$. The reader can readily verify that,

$$\langle 1-\sqrt{-5}\rangle = \langle 2,1+\sqrt{-5}\rangle\langle 3,1+2\sqrt{-5}\rangle \tag{10}$$

$$\langle 1+\sqrt{-5}\rangle = \langle 2,1+\sqrt{-5}\rangle\langle 3,1-2\sqrt{-5}\rangle. \tag{11}$$

Therefore $\langle 1-\sqrt{-5}\rangle$ and $\langle 1+\sqrt{-5}\rangle$ are the only two ideals having norm 6. Now since we know all ideals of $\mathbb{Z}[\sqrt{-5}]$ with norm at most 6, it is not difficult to check that $|\mathscr{C}(\mathbb{Z}[\sqrt{-5}])|=2$. Because each principal ideal of $\mathbb{Z}[\sqrt{-5}]$ represents the identity ideal class $\mathscr{P}$, we find that

$$\langle 1\rangle\mathscr{P} = \langle 2\rangle\mathscr{P} = \langle\sqrt{-5}\rangle\mathscr{P} = \langle 1-\sqrt{-5}\rangle\mathscr{P}.$$

On the other hand, we have seen that the product of $\langle 2,1+\sqrt{-5}\rangle$ and each of the three nonprincipal ideals with norm at most 6 is a principal ideal. Thus,

$$\langle 2,1+\sqrt{-5}\rangle\mathscr{P} = \langle 3,1+2\sqrt{-5}\rangle\mathscr{P} = \langle 3,1-2\sqrt{-5}\rangle\mathscr{P}.$$

Since there are only two ideal classes, $\mathscr{C}(\mathbb{Z}[\sqrt{-5}])=\mathbb{Z}_2$. □

Exercise 6.11. Verify the equalities (10), and (11).

From this observation, we deduce an important property of the ideals of $\mathbb{Z}[\sqrt{-5}]$.

Corollary 6.12. If $I,J\in\mathscr{I}^\bullet$ are not principal, then IJ is principal.

7 Half-factoriality

The class group, in tandem with The Fundamental Theorem of Ideal Theory, will allow us to determine exactly what elements of $\mathbb{Z}[\sqrt{-5}]$ are irreducible.

Proposition 7.1. *Let α be a nonzero nonunit element in $\mathbb{Z}[\sqrt{-5}]$. Then α is irreducible in $\mathbb{Z}[\sqrt{-5}]$ if and only if*

1. *$\langle\alpha\rangle$ is a prime ideal in $\mathbb{Z}[\sqrt{-5}]$ (and hence α is a prime element), or*
2. *$\langle\alpha\rangle = P_1P_2$ where P_1 and P_2 are nonprincipal prime ideals of $\mathbb{Z}[\sqrt{-5}]$.*

Proof. ($\Rightarrow$) Suppose α is irreducible in $\mathbb{Z}[\sqrt{-5}]$. If $\langle\alpha\rangle$ is a prime ideal, then we are done. Assume $\langle\alpha\rangle$ is not a prime ideal. Then by Theorem 5.13 there are prime ideals

$P_1,\dots,P_k$ of $\mathbb{Z}[\sqrt{-5}]$ with $\langle\alpha\rangle = P_1\cdots P_k$ for some $k\ge 2$. Suppose that one of the P_i's is a principal ideal. Without loss of generality, assume that $P_1 = \langle\beta\rangle$ for some prime β in $\mathbb{Z}[\sqrt{-5}]$. Using the class group, $P_2\cdots P_k = \langle\gamma\rangle$, where γ is a nonzero nonunit of $\mathbb{Z}[\sqrt{-5}]$. Thus, $\langle\alpha\rangle = \langle\beta\rangle\langle\gamma\rangle$ implies that $\alpha = (u\beta)\gamma$ for some unit u of $\mathbb{Z}[\sqrt{-5}]$. This contradicts the irreducibility of α in $\mathbb{Z}[\sqrt{-5}]$. Therefore all the P_i's are nonprincipal. Since the class group of $\mathbb{Z}[\sqrt{-5}]$ is $\mathbb{Z}_2$, it follows that k is even. Now suppose that $k>2$. Using Corollary 6.12 and proceeding in a manner similar to the previous argument, $P_1P_2 = \langle\beta\rangle$ and $P_3\cdots P_k = \langle\gamma\rangle$, and again $\alpha = u\beta\gamma$ for some unit u, which contradicts the irreducibility of α. Hence, either $k=1$ and α is a prime element, or $k=2$.

($\Leftarrow$) If $\langle\alpha\rangle$ is a prime ideal, then α is prime and so irreducible. Then suppose that $\langle\alpha\rangle = P_1P_2$, where P_1 and P_2 are nonprincipal prime ideals of $\mathbb{Z}[\sqrt{-5}]$. Let $\alpha = \beta\gamma$ for some $\beta,\gamma\in\mathbb{Z}[\sqrt{-5}]$, and assume, without loss of generality, that β is a nonzero nonunit of $\mathbb{Z}[\sqrt{-5}]$. Notice that $\langle\beta\gamma\rangle = \langle\beta\rangle\langle\gamma\rangle = P_1P_2$. Because P_1 and P_2 are nonprincipal ideals, $\langle\beta\rangle\notin\{P_1,P_2\}$. As a consequence of Theorem 5.13, we have that $\langle\beta\rangle = P_1P_2$. This forces $\langle\gamma\rangle = \langle 1\rangle$, which implies that $\gamma\in\{\pm 1\}$. Thus, α is irreducible. □

Let us use Proposition 7.1 to analyze the factorizations presented in (1) at the beginning of the exposition. As the product of any two nonprincipal ideals of $\mathbb{Z}[\sqrt{-5}]$ is a principal ideal, the decompositions

$$\begin{aligned}\langle 6\rangle = \langle 2\rangle\langle 3\rangle &= \langle 2,\, 1+\sqrt{-5}\rangle^2\langle 3,\, 1-\sqrt{-5}\rangle\langle 3,\, 1+\sqrt{-5}\rangle\\ &= \langle 2,\, 1+\sqrt{-5}\rangle\langle 3,\, 1+\sqrt{-5}\rangle\langle 2,\, 1+\sqrt{-5}\rangle\langle 3,\, 1-\sqrt{-5}\rangle\\ &= \langle 1+\sqrt{-5}\rangle\langle 1-\sqrt{-5}\rangle\end{aligned}$$

yield that $2\cdot 3$ and $(1+\sqrt{-5})(1-\sqrt{-5})$ are the only two irreducible factorizations of 6 in $\mathbb{Z}[\sqrt{-5}]$. Thus, any two irreducible factorizations of 6 in $\mathbb{Z}[\sqrt{-5}]$ have the same factorization length. We can take this observation a step further.

Theorem 7.2. *If α is a nonzero nonunit of $\mathbb{Z}[\sqrt{-5}]$ and $\beta_1,\dots,\beta_s,\gamma_1,\dots,\gamma_t$ are irreducible elements of $\mathbb{Z}[\sqrt{-5}]$ with $\alpha = \beta_1\cdots\beta_s = \gamma_1\cdots\gamma_t$, then $s=t$.*

Proof. Let $\alpha = \omega_1\cdots\omega_m$ be a factorization into irreducibles of α in $\mathbb{Z}[\sqrt{-5}]$. By Theorem 5.13, there are unique prime ideals $P_1,\dots,P_k$ in $\mathbb{Z}[\sqrt{-5}]$ satisfying that $\langle\alpha\rangle = P_1\cdots P_k$. Suppose that exactly d of these prime ideals are principal and assume, without loss, that $P_i = \langle\alpha_i\rangle$ for all $i\in\{1,\dots,d\}$, where each α_i is prime in $\mathbb{Z}[\sqrt{-5}]$. Since the class group of $\mathbb{Z}[\sqrt{-5}]$ is $\mathbb{Z}_2$, there exists $n\in\mathbb{N}$ such that $k-d=2n$. Hence,

$$\langle\alpha\rangle = (P_1\cdots P_d)\,(P_{d+1}\cdots P_k) = \langle\alpha_1\cdots\alpha_d\rangle\,(P_{d+1}\cdots P_k)\,,$$

and any factorization into irreducibles of α will be of the form $u\alpha_1\cdots\alpha_d\cdot\beta_1\cdots\beta_n$, where each ideal $\langle\beta_j\rangle$ is the product of two ideals chosen from $P_{d+1},\dots,P_k$. As a result, $m=d+n$ and, clearly, $s=t=m$, completing the proof. □

Thus, while some elements of $\mathbb{Z}[\sqrt{-5}]$ admit many factorizations into irreducibles, the number of irreducible factors in any two factorizations of a given element is the same. As we mentioned in the introduction, this phenomenon is called half-factoriality. Since the concept of half-factoriality does not involve the addition of $\mathbb{Z}[\sqrt{-5}]$, it can also be defined for commutative monoids.

Definition 7.3. An atomic monoid M is called *half-factorial* if any two factorizations of each nonzero nonunit element of M have the same number of irreducible factors.

Half-factorial domains and monoids have been systematically studied since the 1950's, when Carlitz gave a characterization theorem of half-factorial rings of integers, which generalizes the case of $\mathbb{Z}[\sqrt{-5}]$ considered in this exposition.

Theorem 7.4 (Carlitz [1]). *Let R be the ring of integers in a finite extension field of $\mathbb{Q}$. Then R is half-factorial if and only if R has class number less than or equal to two.*

A list of factorization inspired characterizations of class number two can be found in [3]. In addition, a few families of half-factorial domains in a more general setting are presented in [7]. We will conclude this paper by exhibiting two simple examples of half-factorial monoids, using the second one to illustrate how to compute the number of factorizations in $\mathbb{Z}[\sqrt{-5}]$ of a given element.

Example 7.5 (Hilbert monoid). It is easily seen that

$$H = \{1 + 4k \mid k \in \mathbb{N}_0\}$$

is a multiplicative submonoid of $\mathbb{N}$. The monoid H is called *Hilbert monoid*. It is not hard to verify (Exercise 7.6) that the irreducible elements of H are

1. the prime numbers p satisfying $p \equiv 1 \pmod 4$ and
2. $p_1 p_2$, where p_1 and p_2 are prime numbers satisfying $p_i \equiv 3 \pmod 4$.

Therefore every element of H is a product of irreducibles. Also, in the factorization of any element of H into primes, there must be an even number of prime factors congruent to 3 modulo 4. Hence, any factorization of an element $x \in H$ comes from pairing the prime factors of x that are congruent to 3 modulo 4. This implies that H is half-factorial. For instance, $x = 5^2 \cdot 3^2 \cdot 11 \cdot 13 \cdot 19$ has exactly two factorizations into irreducibles, each of them contains five factors:

$$x = 5^2 \cdot 13 \cdot (3^2) \cdot (11 \cdot 19) = 5^2 \cdot 13 \cdot (3 \cdot 11) \cdot (3 \cdot 19).$$

Exercise 7.6. Argue that the irreducible elements of the Hilbert monoid are precisely those described in Example 7.5.

Definition 7.7. Let p be a prime number.

1. We say that p is *inert* if $\langle p \rangle$ is a prime ideal in $\mathbb{Z}[\sqrt{-5}]$.
2. We say that p is *ramified* if $\langle p \rangle = P^2$ for some prime ideal P in $\mathbb{Z}[\sqrt{-5}]$.
3. We say that p *splits* if $\langle p \rangle = PP'$ for two distinct prime ideals in $\mathbb{Z}[\sqrt{-5}]$.

Prime numbers p can be classified according to the above definition. Indeed, we have seen that p is ramified when $p \in \{2,5\}$. It is also known that p splits if $p \equiv 1,3,7,9 \pmod{20}$ and is inert if $p \not\equiv 1,3,7,9 \pmod{20}$ (except 2 and 5). A proof of this result is given in [8].

Example 7.8. When $n \geq 2$, the submonoid $\mathbb{X}_n$ of the additive monoid $\mathbb{N}_0^{n+1}$ given by

$$\mathbb{X}_n = \{(x_1,\dots,x_{n+1}) \mid x_i \in \mathbb{N}_0 \text{ and } x_1 + \dots + x_n = x_{n+1}\}$$

is a half-factorial Krull monoid with divisor class group $\mathbb{Z}_2$ (see [5, Section 2] for more details). Following [4], we will use $\mathbb{X}_n$ to count the number of distinct factorizations into irreducibles of a given nonzero nonunit $\alpha \in \mathbb{Z}[\sqrt{-5}]$. Let

$$\langle \alpha \rangle = P_1^{n_1} \cdots P_k^{n_k} Q_1^{m_1} \cdots Q_t^{m_t},$$

where the P_i's are distinct prime ideals in the trivial class ideal of $\mathbb{Z}[\sqrt{-5}]$, the Q_j's are distinct prime ideals in the nontrivial class ideal of $\mathbb{Z}[\sqrt{-5}]$, and $m_1 \leq \dots \leq m_t$. Then the desired number of factorizations $\eta(\alpha)$ of α in $\mathbb{Z}[\sqrt{-5}]$ is given by

$$\eta(\alpha) = \eta_{\mathbb{X}_t}\left(m_1,\dots,m_t,\frac{m_1 + \dots + m_t}{2}\right),$$

which, when $t = 3$, can be computed by the formula

$$\eta_{\mathbb{X}_3}(x_1,x_2,x_3,x_4) = \sum_{j=0}^{\lfloor x_1/2 \rfloor} \sum_{k=0}^{x_1-2j} \left(\left\lfloor \frac{\min\{x_2 - k, x_3 - x_1 + 2j + k\}}{2} \right\rfloor + 1 \right).$$

For instance, let us find how many factorizations $1980 = 2^2 \cdot 3^2 \cdot 5 \cdot 11$ has in $\mathbb{Z}[\sqrt{-5}]$. We have seen that 5 ramifies as $\langle 5 \rangle = P_1^2$, where P_1 is principal. As 11 is inert, $P_2 = \langle 11 \rangle$ is prime. In addition, 3 splits as $\langle 3 \rangle = Q_1 Q_2$, where Q_1 and Q_2 are nonprincipal. Finally, 2 ramifies as $\langle 2 \rangle = Q_3^2$, where Q_3 is nonprincipal. Therefore one has that $\langle 1980 \rangle = P_1^2 P_2 Q_1^2 Q_2^2 Q_3^4$, and so

$$\eta(1980) = \eta_{\mathbb{X}_3}(2,2,4,4) = \sum_{j=0}^{1} \sum_{k=0}^{2-2j} \left(\left\lfloor \frac{\min\{2 - k, 2 + 2j + k\}}{2} \right\rfloor + 1 \right) = 6.$$

Acknowledgements

It is a pleasure for the authors to thank the referee, whose helpful suggestions vastly improved the final version of this paper.

References

1. L. Carlitz, *A characterization of algebraic number fields with class number two*, Proc. Amer. Math. Soc. **11** (1960) 391–392.
2. S. T. Chapman, *A tale of two monoids: A friendly introduction to nonunique factorizations*, Math. Mag. **87** (2014) 163–173.
3. S. T. Chapman, *So what is class number 2*, to appear in *Amer. Math. Monthly*.
4. S. T. Chapman, J. Herr, and N. Rooney, *A factorization formula for class number two*, J. Number Theory **79** (1999) 58–66.
5. S. T. Chapman, U. Krause, and E. Oeljeklaus, *Monoids determined by a homogeneous linear diophantine equation and the half-factorial property*, J. Pure Appl. Algebra **151** (2000) 107–133.
6. F. Jarvis, *Algebraic Number Theory*, Springer Undergraduate Mathematics Series, Springer, New York, 2014.
7. H. Kim, *Examples of half-factorial domains*, Canad. Math. Bull. **43** (2000) 362–367.
8. D. Marcus, *Number Fields*, Springer-Verlag, New York Inc., 1977.
9. H. Pollard and H. G. Diamond, *The Theory of Algebraic Numbers*, Courier Corporation, New York, 1998.
10. M. Ram Murty and J. Esmonde, *Problems in Algebraic Number Theory*, Graduate Text in Mathematics Vol. 190, Springer, New York, 2005.