

4-2004

## Factorability in the ring $Z[\sqrt{-5}]$

Laura Lynch

Florida Atlantic University, llynch@ccga.edu

Follow this and additional works at: <http://digitalcommons.unl.edu/mathstudent>



Part of the [Science and Mathematics Education Commons](#)

---

Lynch, Laura, "Factorability in the ring  $Z[\sqrt{-5}]$ " (2004). *Dissertations, Theses, and Student Research Papers in Mathematics*. 15.  
<http://digitalcommons.unl.edu/mathstudent/15>

This Article is brought to you for free and open access by the Mathematics, Department of at DigitalCommons@University of Nebraska - Lincoln. It has been accepted for inclusion in Dissertations, Theses, and Student Research Papers in Mathematics by an authorized administrator of DigitalCommons@University of Nebraska - Lincoln.

**Factorability in the ring  $\mathbb{Z}[\sqrt{-5}]$**

by

Laura Lynch

A Thesis presented to the Faculty of  
The Honors College of Florida Atlantic University  
In Partial Fulfillment of Requirements for the Degree of  
Bachelor of Arts in Liberal Arts and Sciences  
with a Concentration in Mathematics  
Under the Supervision of Professor Stephanie Fitchett

Harriet L. Wilkes Honors College  
of Florida Atlantic University

Jupiter, Florida

April 2004

# Factorability in the ring $\mathbb{Z}[\sqrt{-5}]$

by

Laura Lynch

This thesis was prepared under the direction of the candidate's thesis advisor, Dr. Stephanie Fitchett, and has been approved by the members of her supervisory committee. It was submitted to the faculty of The Harriet L. Wilkes Honors College and was accepted in partial fulfillment of the requirements for the degree of Bachelor of Arts in Liberal Arts and Sciences.

SUPERVISORY COMMITTEE:

---

Dr. Stephanie Fitchett

---

Dr. Eugene Belogay

---

Dr. Ryan Karr

---

Dean, Harriet L. Wilkes Honors College

---

Date

# Acknowledgments

First and foremost, I would like to thank Dr. Stephanie Fitchett, my advisor. She has been a great inspiration for the three years I have attended the Honors College and she has been a wonderful advisor. I also want to thank my two readers, Dr. Eugene Belogay and Dr. Ryan Karr. In particular, I would like to thank Dr. Belogay for his corrections of my many grammatical errors and Dr. Karr for his assistance with my computer algorithm.

# Abstract

Author: Laura Lynch  
Title: Factorability in the ring  $\mathbf{Z}[\sqrt{-5}]$   
Institution: Harriet L. Wilkes Honors College, Florida Atlantic University  
Thesis Advisor: Stephanie Fitchett  
Concentration: Mathematics  
Year: 2004

The fundamental theorem of arithmetic says that any integer greater than 2 can be written uniquely as a product of primes. For the ring  $\mathbb{Z}[\sqrt{-5}]$ , although unique factorization holds for ideals, unique factorization fails for elements. We investigate both elements and ideals of  $\mathbb{Z}[\sqrt{-5}]$ . For elements, we examine irreducibility (the analog of primality) in  $\mathbb{Z}[\sqrt{-5}]$  and look at how often and how badly unique factorization fails. For ideals, we examine irreducibility again and a proof for unique factorization.

# Contents

List of Tables	vi
List of Figures	vii
<b>1 Introduction</b>	<b>1</b>
<b>2 Background</b>	<b>4</b>
2.1 Basic Definitions . . . . .	4
2.2 Perfect Squares modulo $p$ . . . . .	7
<b>3 Reducibles</b>	<b>8</b>
3.1 Norms . . . . .	8
3.2 Rational Integers . . . . .	11
3.3 When is a general element reducible? . . . . .	16
<b>4 Irreducibles</b>	<b>21</b>
4.1 Irreducibility Algorithm . . . . .	21
4.2 Comparing $\mathbb{Z}[\sqrt{-5}]$ with $\mathbb{Z}$ . . . . .	23
4.3 Approximating $IR(n)$ . . . . .	26
4.4 How often and how badly does unique factorization fail? . . . . .	28
<b>5 Factorizations of Ideals</b>	<b>30</b>
5.1 Definitions and Results from Ideal Theory . . . . .	30
5.2 How ideals factor . . . . .	34
<b>6 Dedekind Domains</b>	<b>39</b>
6.1 Quadratic Number Rings . . . . .	39
6.2 Dedekind domains . . . . .	43
6.3 Unique Factorization for Ideals . . . . .	46
<b>7 Conclusions</b>	<b>51</b>
<b>8 Appendix A</b>	<b>53</b>
<b>9 Appendix B</b>	<b>57</b>
<b>10 Appendix C</b>	<b>58</b>
<b>References</b>	<b>61</b>

## List of Tables

1	Perfect Squares modulo 10 . . . . .	10
2	Possible Norms modulo 10 . . . . .	10
3	Comparison between number of irreducibles and number of primes. . . . .	24
4	Density of primes and irreducibles . . . . .	26

## List of Figures

1	Graph of Reducibles and Interesting Reducibles . . . . .	20
2	$IR(n)$ and $\pi(n)$ . . . . .	25
3	$IR(n)$ and $\frac{Count(n)}{\ln(Count(n))}$ . . . . .	27
4	$IR(n)$ and $4.16 \cdot \frac{Count(n)}{\ln(Count(n))}$ . . . . .	28



# 1 Introduction

In describing the natural understanding we have of factoring, the famous mathematician Paul Erdős would have said, “Every baby knows that any integer greater than one can be factored into a product of primes.” While Erdős often exaggerated what babies know, it is certainly true that most grade school children know it. Moreover, the Fundamental Theorem of Arithmetic states that such a factorization is unique, up to the ordering of the primes. Surprisingly, although factorizations are unique for the integers, factorizations are not unique in general. One setting in which unique factorization fails is the ring  $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$ . For instance, the number 6 has two different factorizations in this ring:

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

To verify that the two factorizations are truly different, we would need to know that the factors 2, 3,  $1 - \sqrt{-5}$ , and  $1 + \sqrt{-5}$  are “prime” in  $\mathbb{Z}[\sqrt{-5}]$ ; we will see that later in Chapter 3.

The ring  $\mathbb{Z}[\sqrt{-5}]$  is interesting for many reasons. It is, as we will see in Chapter 6, the first complex quadratic number ring where unique factorization fails for elements. So, in looking at this ring, we will be interested in when an element can be factored, what the factorizations are, how many factorizations exist, and how many elements have more than one factorization. As it turns out, although unique factorization fails for *elements* of  $\mathbb{Z}[\sqrt{-5}]$ , it holds for *ideals* in  $\mathbb{Z}[\sqrt{-5}]$ . This result comes from the fact that  $\mathbb{Z}[\sqrt{-5}]$  is what is called a Dedekind domain.

In Chapter 2, we define an “irreducible” element in  $\mathbb{Z}[\sqrt{-5}]$  as the analog to a “prime” number in  $\mathbb{Z}$ . We also review some definitions and results from ring theory and number theory.

In Chapter 3, we begin to analyze the reducible elements of  $\mathbb{Z}[\sqrt{-5}]$ . If an integer (number of the form  $a + 0\sqrt{-5}$ ) factors in  $\mathbb{Z}$ , it will factor in  $\mathbb{Z}[\sqrt{-5}]$ . For prime numbers, however, the situation is more complicated. For example,  $29 = (3 + 2\sqrt{-5})(3 - 2\sqrt{-5})$ , but 11 remains unfactorable. We then provide sufficient conditions for reducibility. For example,  $a + b\sqrt{-5}$  is reducible if  $a \equiv \pm b \pmod{6}$ .

Of course, we also want to know when an element is irreducible and Chapter 4 presents a naïve algorithm to decide when an element of  $\mathbb{Z}[\sqrt{-5}]$  is irreducible; we use it to study the density of “primes” in the two settings. The algorithm also provides data for investigating how often and how badly unique factorization fails in  $\mathbb{Z}[\sqrt{-5}]$ . A discussion of this data is included at the end of Chapter 4.

Historically, the ring  $\mathbb{Z}[\sqrt{-5}]$  motivated Richard Dedekind to develop the entire theory of ideals [D]. Dedekind discovered that factorization for ideals is unique. His remarkable insight into this ring opened up an entire area of study in algebra and algebraic number theory, namely, the theory of *Dedekind domains*. In Chapter 5, we look at factorizations of ideals in the ring. We also classify again what happens to primes from  $\mathbb{Z}$  in  $\mathbb{Z}[\sqrt{-5}]$ , but this time as ideals.

Classical results in the theory of quadratic forms explain why factorization is not unique in  $\mathbb{Z}[\sqrt{-5}]$ . It turns out that when there is only one equivalence class of quadratic forms corresponding to a quadratic number ring, elements of the ring have

unique factorization; when a ring has more than one corresponding equivalence class of quadratic forms, however, unique factorization fails. This is the case for  $\mathbb{Z}[\sqrt{-5}]$ , where the corresponding quadratic forms are  $x^2 + 5y^2$  and  $2x^2 + 2xy + 3y^2$ . For more insight into the theory of quadratic forms, see p.10 of [D]. In Chapter 6, we look at quadratic numbers rings to show that  $\mathbb{Z}[\sqrt{-5}]$  is the smallest of its kind for which unique factorization fails. Then we take another look at Dedekind domains and prove Dedekind's result of unique factorization for ideals.

## 2 Background

We will use  $\mathbb{Z}$  for the set of integers,  $\mathbb{Q}$  for the set of rational numbers, and  $\mathbb{C}$  for the set of complex numbers.

### 2.1 Basic Definitions

In order to study  $\mathbb{Z}[\sqrt{-5}]$ , we must first understand some of the underlying ideas in basic abstract algebra.

**Definition 2.1.** A ring is a nonempty set with two binary operations, addition and multiplication, such that, for all  $x, y, z$  in the ring:

- (1)  $x + y = y + x$
- (2)  $(x + y) + z = x + (y + z)$
- (3) There exists an additive identity,  $0$ , such that  $x + 0 = x$ .
- (4) There exists an additive inverse,  $-x$ , such that  $x + -x = 0$ .
- (5)  $x(yz) = (xy)z$
- (6)  $x(y + z) = xy + xz$  and  $(y + z)x = yx + zx$

Moreover, a ring is called commutative if, in addition to (1)-(6),  $xy = yx$  for all  $x, y$  in the ring. A ring for which there exists a multiplicative identity,  $1$ , such that  $1 \cdot x = x \cdot 1 = x$  for all  $x$  is called a ring with identity.

Most systems of numbers in which the usual notions of addition and multiplication hold, such as  $\mathbb{Z}$ ,  $\mathbb{Q}$  or  $\mathbb{Z}[\sqrt{-5}]$ , are commutative rings with identity. The set of even integers, for instance, is a commutative ring without identity.

**Definition 2.2.** A unit is a nonzero element  $x$  of a commutative ring such that there is a nonzero element  $y$  in the ring with  $xy = 1$ . A zero-divisor is a nonzero element  $x$  of a commutative ring such that there is a nonzero element  $y$  in the ring with  $xy = 0$ .

In  $\mathbb{Z}[\sqrt{-5}]$ , note that there are no zero divisors. Indeed, if there were zero divisors, there would exist non-zero elements  $a + b\sqrt{-5}$  and  $c + d\sqrt{-5}$  such that  $(a + b\sqrt{-5})(c + d\sqrt{-5}) = (ac - 5bd) + (ad + bc)\sqrt{-5} = 0$ . This would imply  $ac = 5bd$  and  $ad = -bc$ . Assuming that  $c$  and  $d$  are not zero,  $\frac{bc}{d} = \frac{-5bd}{c}$  which implies either  $b = 0$  or  $c^2 = -5d^2$ . If  $b = 0$ , then  $ac = 0$  which implies  $a = 0$  as  $c \neq 0$ , contradicting the fact that  $a + b\sqrt{-5}$  is non-zero. Since both  $c^2$  and  $d^2$  are nonnegative, the only way  $c^2$  could equal  $-5d^2$  is if  $c = d = 0$ , which contradicts our assumption. Thus, there do not exist zero-divisors in the ring. We will see in Chapter 3 that the only units in  $\mathbb{Z}[\sqrt{-5}]$  are  $\pm 1$ .

**Definition 2.3.** An integral domain is a commutative ring with identity and no zero-divisors.

By the above argument, the ring  $\mathbb{Z}[\sqrt{-5}]$  is an integral domain.

**Definition 2.4.** A field is a commutative ring with identity in which every nonzero element is a unit.

An example of a field is  $\mathbb{Q}$ , since the set of rationals is closed under addition, subtraction, and multiplication, and every nonzero element has a multiplicative inverse in  $\mathbb{Q}$ .

**Definition 2.5.** A nonzero, nonunit element  $\alpha$  of a commutative ring that is divisible only by units and itself is called irreducible. An element  $\alpha$  of a commutative ring  $R$  is reducible if there exist nonzero, non-unit elements  $\beta, \gamma \in R$  such that  $\alpha = \beta\gamma$ .

In other words, a nonzero, non-unit element that is not irreducible is reducible. Examples of irreducible elements are 2, 3, and  $1 \pm \sqrt{-5}$ , which we saw in the introduction, and whose irreducibility will be confirmed in Chapter 3. Examples of reducible elements are  $2 + 2\sqrt{-5} = 2(1 + \sqrt{-5})$  and  $29 = (3 + 2\sqrt{-5})(3 - 2\sqrt{-5})$ .

**Definition 2.6.** Let  $R$  be a commutative ring. The polynomial ring  $R[x]$  over  $R$  is just the set of polynomials in the indeterminate  $x$  with coefficients in  $R$ , namely  $R[x] = \{a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \mid a_i \in R, n \in \mathbb{N}\}$ .

Some examples of polynomial rings include  $\mathbb{Q}[x]$  and  $\mathbb{Z}[x]$ , the sets of polynomials with coefficients in  $\mathbb{Q}$  and  $\mathbb{Z}$ , respectively. It is well-known that there exists a well-defined division algorithm for the set of integers. That is, for  $a, b \in \mathbb{Z}$  where  $b \neq 0$ , there exists  $q, r \in \mathbb{Z}$  such that  $a = bq + r$  where  $0 \leq r < b$ . Analogous to the integers, the polynomial ring  $F[x]$  where  $F$  is a field has a well-defined division algorithm (see p. 286 of [G]). That is, for all  $a(x), b(x) \in F[x]$  where  $b(x) \neq 0$ , there exists  $q(x)$  and  $r(x)$  such that  $a(x) = b(x)q(x) + r(x)$  where  $0 \leq \deg r(x) < \deg b(x)$  and the  $\gcd(a, b)$  can be found by repeated use of the division algorithm. We will use the division algorithm for integers in Proposition 5.12 and for polynomial rings in Proposition 6.6 to say that if  $a$  and  $b$  are relatively prime, we can find a linear combination of  $a$  and  $b$  that equals 1.

## 2.2 Perfect Squares modulo $p$

In the following chapter, we will need to determine when an integer is a perfect square modulo  $p$ . This section summarizes the relevant notation and results from number theory that we will need.

**Definition 2.7.** *Let  $p$  be a prime. The Legendre symbol for an integer  $a$  is defined as follows:*

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a perfect square mod } p, \\ -1 & \text{if } a \text{ is not a perfect square mod } p, \\ 0 & \text{gcd}(a, p) > 1. \end{cases}$$

We will use the following well-known theorems about Legendre Symbols. Proofs can be found in any elementary number theory textbook. See p. 561 of [HJ], for instance.

**Theorem 2.8.** *Let  $a \equiv b \pmod{p}$  where  $p$  is a prime. Then  $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$ .*

**Theorem 2.9.** *Let  $a, b, p \in \mathbb{Z}$  where  $p$  is a prime. Then  $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \left(\frac{b}{p}\right)$ .*

**Theorem 2.10.** *Let  $p$  be an odd prime. Then  $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$ .*

**Theorem 2.11 (Quadratic Reciprocity Theorem).** *Let  $p, q$  be odd primes.*

*Then  $\left(\frac{q}{p}\right) \left(\frac{p}{q}\right) = (-1)^{\frac{q-1}{2} \cdot \frac{p-1}{2}}$ .*

### 3 Reducibles

The failure of unique factorization in  $\mathbb{Z}[\sqrt{-5}]$  is the motivation for our study. However, before we study the factorizations of an element, we must determine when an element has non-trivial factorization, that is, when it is reducible. This chapter describes various sufficient conditions for reducibility of an element. We begin our study with norms and show how they can help us determine if an element is reducible.

#### 3.1 Norms

**Definition 3.1.** *The element  $\bar{\alpha} = a - bi$  is called the conjugate of  $\alpha = a + bi$ .*

**Definition 3.2.** *The norm  $N$  of  $\alpha \in \mathbb{C}$  is defined to be  $N(\alpha) = \alpha\bar{\alpha} = |\alpha|^2$ .*

Notice that the norm  $N$  is the square of the usual norm in  $\mathbb{C}$ . Using the square of the usual norm allows us to avoid irrational numbers since, for  $a, b \in \mathbb{Z}$ , the norm  $N(a + b\sqrt{-5}) = a^2 + 5b^2$  is an integer. Interestingly enough,  $N(\alpha)$  satisfies the usual norm properties shown below.

**Lemma 3.3.** *Let  $\alpha \in \mathbb{Z}[\sqrt{-5}]$ . Then  $N(\alpha) = 1$  if and only if  $\alpha = \pm 1$ .*

*Proof.* Let  $\alpha = a + b\sqrt{-5}$  and  $1 = N(\alpha) = a^2 + 5b^2$ . Then  $b$  must be 0 and  $a$  must be  $\pm 1$ . □

**Lemma 3.4.** *Let  $\alpha, \beta \in \mathbb{C}$ . Then  $N(\alpha\beta) = N(\alpha)N(\beta)$ .*



*Proof.* The multiplicative property of our norm follows from the same property of the usual complex norm, but we prove it here anyway. Let  $\alpha = a + bi$  and  $\beta = c + di$ .

Then

$$\begin{aligned}
 N(\alpha\beta) &= N((a + bi)(c + di)) \\
 &= N((ac - bd) + (ad + bc)i) \\
 &= (ac - bd)^2 + (ad + bc)^2 \\
 &= a^2c^2 - 2abcd + b^2d^2 + a^2d^2 + 2abcd + b^2c^2 \\
 &= a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2 \\
 &= a^2(c^2 + d^2) + b^2(c^2 + d^2) \\
 &= (a^2 + b^2)(c^2 + d^2) \\
 &= N(\alpha)N(\beta).
 \end{aligned}$$

□

These lemmas also prove that the only units are  $\pm 1$  since  $\alpha\beta = 1$  implies  $N(\alpha)N(\beta) = 1$  which implies  $N(\alpha) = N(\beta) = 1$ . Lemma 3.4 simply says that the multiplicative property of norms holds for  $\alpha, \beta \in \mathbb{Z}[\sqrt{-5}]$ . Of course, since not every integer has the form  $a^2 + 5b^2$ , not every integer will be the norm of an element in  $\mathbb{Z}[\sqrt{-5}]$ . The following lemma and proposition help us see exactly what integers can be norms.

**Lemma 3.5.** *There are no perfect squares ending in 2, 3, 7, or 8.*

*Proof.* Since we are looking at the last digit of a given number, we need only look at the integers mod 10. Consider Table 1.

$x \pmod{10}$	0	1	2	3	4	5	6	7	8	9
$x^2 \pmod{10}$	0	1	4	9	6	5	6	9	4	1

Table 1: Perfect Squares modulo 10

Since 2, 3, 7, and 8, are not squares modulo 10, there do not exist perfect squares in  $\mathbb{Z}$  ending in 2, 3, 7, or 8. □

With this in mind, we can now limit the number of possible norms.

**Proposition 3.6.** *There are no norms ending in 2, 3, 7, or 8.*

*Proof.* We want to show that for any  $a, b \in \mathbb{Z}$ , the norm  $N(a + b\sqrt{-5}) = a^2 + 5b^2$  does not end in 2, 3, 7, or 8. Look at  $a^2 + 5b^2 \pmod{10}$ . From the lemma above, the possible values of  $a^2 \pmod{10}$  are 0, 1, 4, 5, 6, or 9, and a quick check shows the possible values of  $5b^2 \pmod{10}$  are just 0 and 5. Thus the possible values of  $a^2 + 5b^2$  are just 0, 1, 4, 5, 6, and 9, as shown in Table 2.

$a^2 \pmod{10}$	0	0	1	1	4	4	5	5	6	6	9	9
$5b^2 \pmod{10}$	0	5	0	5	0	5	0	5	0	5	0	5
$a^2 + 5b^2 \pmod{10}$	0	5	1	6	4	9	5	0	6	1	9	4

Table 2: Possible Norms modulo 10

Thus, there do not exist any norms in  $\mathbb{Z}[\sqrt{-5}]$  that end with 2, 3, 7, or 8. □

Now that we have established some properties of the norm, we can find a way to determine when an element is, in fact, reducible. If an element is reducible in  $\mathbb{Z}[\sqrt{-5}]$ , then its norm must have a nontrivial factorization in which the integer factors must be possible norms in  $\mathbb{Z}[\sqrt{-5}]$ . If no such factorization exists, the element must be irreducible. Consider, for example, the element  $1 + \sqrt{-5}$  of norm 6. If  $1 + \sqrt{-5} = \alpha\beta$ , then  $N(1 + \sqrt{-5}) = N(\alpha\beta) = N(\alpha)N(\beta)$ . The only nontrivial factorization of  $6 \in \mathbb{Z}$  is  $2 \cdot 3$ , and by Proposition 3.6, no elements in  $\mathbb{Z}[\sqrt{-5}]$  have norms 2 or 3, so no such  $\alpha, \beta$  exist, and  $1 + \sqrt{-5}$  is irreducible. Similarly, 2, 3, and  $1 - \sqrt{-5}$  are irreducible, which verifies the assertion in the introduction that  $(1 + \sqrt{-5})(1 - \sqrt{-5})$  and  $(2)(3)$  are distinct factorizations of 6.

On the other hand, consider the element  $7 + \sqrt{-5}$  of norm 54. By Proposition 3.6, the only possible norms that multiply to 54 are 6 and 9. So, if there exists a factorization of  $7 + \sqrt{-5}$ , the factors must have norms 6 and 9. Checking all the factors with norms 6 and 9, one can find that

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

so  $7 + \sqrt{-5}$  is reducible.

## 3.2 Rational Integers

We just saw how norms can help us determine the reducibility of an element, but this strategy can be quite time-consuming. We would like to find concrete conditions to determine reducibility, that is, we would like statements of the form “if an element is

of a particular form, it is reducible.” Let us begin with the set  $\mathbb{Z}$ . The set of integers is contained in  $\mathbb{Z}[\sqrt{-5}]$ . So, if a number is reducible in  $\mathbb{Z}$ , it will automatically be reducible in  $\mathbb{Z}[\sqrt{-5}]$ . However, if a number is prime in  $\mathbb{Z}$ , it is not necessarily irreducible in  $\mathbb{Z}[\sqrt{-5}]$ .

**Definition 3.7.** *If  $p$  is a prime number in  $\mathbb{Z}$ , we say  $p$  is a rational prime in  $\mathbb{Z}[\sqrt{-5}]$ .*

The factorization of rational primes in  $\mathbb{Z}[\sqrt{-5}]$  is well-known. For example, the rational prime 5 becomes reducible as  $5 = (\sqrt{-5})(-\sqrt{-5})$  and 41 becomes reducible as  $41 = (6 + \sqrt{-5})(6 - \sqrt{-5})$ , but 13 remains irreducible. The following lemma explains what happens when a rational prime is reducible.

**Lemma 3.8.** *If  $p$  is a rational prime and reducible, then  $-5$  is a square modulo  $p$ .*

*Proof.* Let  $p$  be reducible. If  $p = \alpha\beta$  where  $\alpha, \beta$  are not units, then  $p^2 = N(p) = N(\alpha\beta) = N(\alpha)N(\beta)$  and  $N(\alpha) = p$ . If  $\alpha = a + b\sqrt{-5}$ , then  $a^2 + 5b^2 = p$ . Then  $a^2 + 5b^2 \equiv 0 \pmod{p}$  which implies  $a^2 \equiv -5b^2 \pmod{p}$ . Thus  $(ab^{-1})^2 \equiv -5 \pmod{p}$  since  $b$  is a unit in  $\mathbb{Z}_p$ .  $\square$

After presenting the following lemma, we can describe exactly what happens to rational primes in  $\mathbb{Z}[\sqrt{-5}]$ .

**Lemma 3.9.** *Let  $p$  be a prime. If  $\gcd(a, p) = 1$ , then  $y \equiv ax \pmod{p}$  has a solution  $(x_0, y_0)$  with  $0 < |x_0| < \sqrt{p}$  and  $0 < |y_0| < \sqrt{p}$ .*

*Proof.* Let  $k = \lceil \sqrt{p} \rceil$ , and consider the set  $S = \{y - ax \mid 0 \leq x, y \leq k - 1\}$ , which has at most  $k^2$  distinct elements. There exist  $y_1 - ax_1, y_2 - ax_2 \in S$  with  $x_1 \neq x_2$  or  $y_1 \neq y_2$  such that  $y_1 - ax_1 \equiv y_2 - ax_2 \pmod{p}$  by the pigeonhole principle (since  $k^2 > p$ ). If  $x_1 = x_2$ , then  $y_1 \equiv y_2 \pmod{p}$  which implies  $y_1 = y_2$ , since  $|y_1 - y_2| \leq k - 1 < p$ , which is impossible. Similarly, if  $y_1 = y_2$ , we would have  $x_1 = x_2$ , which is impossible. So  $y_1 - y_2 \equiv a(x_1 - x_2) \pmod{p}$ . Let  $x_0 = x_1 - x_2$  and  $y_0 = y_1 - y_2$ . Then  $y_0 \equiv ax_0 \pmod{p}$ . By the way we defined  $S$ , we know  $0 < x_1, x_2, y_1, y_2 < \sqrt{p}$  so  $0 < |x_1 - x_2|, |y_1 - y_2| < \sqrt{p}$ . Thus  $0 < |x_0|, |y_0| < \sqrt{p}$  and  $(x_0, y_0)$  is the desired solution.  $\square$

**Theorem 3.10.** *Let  $R = \mathbb{Z}[\sqrt{-5}]$ , and let  $p$  be a rational prime in  $R$ . Then*

1.  $p = 5$  is the square of an irreducible element.
2. If  $p \equiv 1$  or  $9 \pmod{20}$ , then  $p$  is reducible.
3. If  $p = 2$  or  $p \equiv 3, 7, 11, 13, 17,$  or  $19 \pmod{20}$ , then  $p$  is irreducible.

*Proof.* We will break the proof down into the following three cases.

1. Let  $p = 5$ . It is easy to see that  $5 = (\sqrt{-5})(-\sqrt{-5})$ . We also know  $\sqrt{-5}$  is irreducible as  $N(\sqrt{-5}) = 5$  and the only integers that divide 5 are 1 (where all elements with norm 1 are units) and 5 (where only  $\pm\sqrt{-5}$  have norm 5).

Thus  $p$  acts like the square of an irreducible.

2. Let  $p \equiv 1 \pmod{20}$ . By the Quadratic Reciprocity Theorem,  $\left(\frac{5}{p}\right) \left(\frac{p}{5}\right) = (-1)^{\frac{5-1}{2} \cdot \frac{p-1}{2}} = (-1)^{p-1} = 1$ , so  $\left(\frac{-5}{p}\right) = \left(\frac{-1}{p}\right) \left(\frac{5}{p}\right) = (-1)^{\frac{p-1}{2}} \left(\frac{p}{5}\right) = (-1)^{\frac{p-1}{2}} \left(\frac{20k+1}{5}\right) =$

$(-1)^{\frac{p-1}{2}}\left(\frac{1}{5}\right) = 1$ . Thus, there exists a solution  $z_0$  to  $z^2 \equiv -5 \pmod{p}$ . By Lemma 3.9, there exist  $x_0, y_0$  such that  $y_0 \equiv z_0 x_0 \pmod{p}$ , with  $0 < |x_0|, |y_0| < \sqrt{p}$ . Then  $y_0^2 \equiv (z_0 x_0)^2 \pmod{p}$  which implies  $y_0^2 \equiv -5x_0^2 \pmod{p}$  and so  $y_0^2 + 5x_0^2 = kp$  for some  $k \in \mathbb{Z}$ . Since  $0 < |x_0|, |y_0| < \sqrt{p}$ , we see  $y_0^2 + 5x_0^2 < 6p$ . Therefore,  $0 < k < 6$ . Since  $y_0^2 + 5x_0^2 = kp$  and  $p \equiv 1 \pmod{20}$ ,  $y_0^2 \equiv k \pmod{5}$ . Since  $0, \pm 1$  are the only squares modulo 5,  $k \equiv 0, \pm 1 \pmod{5}$ . So,  $k = 1, 4$ , or  $5$ .

**Case 1:** If  $k = 1$ , then  $p = y_0^2 + 5x_0^2 = (y_0 + x_0\sqrt{-5})(y_0 - x_0\sqrt{-5})$ .

**Case 2:** If  $k = 4$ , then  $y_0^2 + 5x_0^2 = 4p$ , so  $y_0^2 + x_0^2 \equiv 0 \pmod{4}$ . Since 0 and 1 are the only squares modulo 4,  $x_0^2 \equiv y_0^2 \equiv 0 \pmod{4}$ , which means  $x_0 = 2a$  and  $y_0 = 2b$  for some  $a, b \in \mathbb{Z}$ . Then  $4b^2 + 20a^2 = 4p$  and  $p = (b + a\sqrt{-5})(b - a\sqrt{-5})$ .

**Case 3:** If  $k = 5$ , then  $y_0^2 + 5x_0^2 = 5p$  and so  $5|y_0$ . Say  $y_0 = 5a$ . Then  $25a^2 + 5x_0^2 = 5p$ , so  $5a^2 + x_0^2 = p$  and  $p = (x_0 + a\sqrt{-5})(x_0 - a\sqrt{-5})$ .

Therefore, we can find a factorization of  $p$  for all  $k$ , so if  $p \equiv 1 \pmod{20}$ , the  $p$  is reducible.

Let  $p \equiv 9 \pmod{20}$ . Then  $\left(\frac{-5}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{5}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{p}{5}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{20k+9}{5}\right) = (-1)^{\frac{p-1}{2}\frac{5-1}{2}}\left(\frac{4}{5}\right) = 1$ . Thus, there exists a solution  $z_0$  to  $z^2 \equiv -5 \pmod{p}$ . As before,  $y_0^2 + 5x_0^2 = kp$ , but now we have  $p \equiv 9 \pmod{20}$ . So  $y_0^2 \equiv -k \pmod{5}$ . Then we still have  $k \equiv 0, \pm 1 \pmod{5}$  as the possible values for  $k$ , which all yield factorizations of  $p$ . Thus,  $p$  is reducible for all  $p \equiv 1, 9 \pmod{20}$ .

3. Let  $p = 2$ . To show it is irreducible, we will consider the norm. If  $2 = \alpha\beta$ , then  $4 = N(2) = N(\alpha\beta) = N(\alpha)N(\beta)$ . The possible values for  $N(\alpha)N(\beta)$  are  $2 \cdot 2$  and  $4 \cdot 1$ . There do not exist elements with norm 2, so without loss of generality, let  $N(\alpha) = 4$  and  $N(\beta) = \pm 1$ . Then,  $\beta = 1$  and 2 is irreducible by definition. Let  $p \equiv 3$  or  $7 \pmod{20}$ . The norm  $N(p) = p^2 = p \cdot p$ . As we saw in Lemma 3.6, there does not exist an element in  $\mathbb{Z}[\sqrt{-5}]$  with norm  $p$ , thus a rational prime  $p$  that is congruent to 3 or 7 mod 20 is irreducible in  $\mathbb{Z}[\sqrt{-5}]$ . Let  $p \equiv 11 \pmod{20}$ . By Lemma 3.8, we need only to show that  $-5$  is not a square modulo  $p$ . This is the same as showing that the Legendre symbol  $\left(\frac{-5}{p}\right)$  is  $-1$ . Applying Theorems 2.10 and 2.11 shows  $\left(\frac{-5}{p}\right) = \left(\frac{-1}{p}\right) \left(\frac{5}{p}\right) = (-1)^{\frac{p-1}{2}} \left(\frac{5}{p}\right) = -\left(\frac{5}{p}\right)$  and from the proof of part 2  $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right)$  so  $\left(\frac{5}{p}\right) = \left(\frac{20k+11}{5}\right) = \left(\frac{1}{5}\right) = 1$ . Therefore,  $\left(\frac{-5}{p}\right) = -1$ , so  $-5$  is not a perfect square mod  $p$  and, by our lemma,  $p$  is irreducible. Similar arguments show that if  $p \equiv 13, 17, 19 \pmod{20}$ , then  $p$  is irreducible in  $\mathbb{Z}[\sqrt{-5}]$ . Here are the details.

Let  $p \equiv 13 \pmod{20}$ . Then  $\left(\frac{-5}{p}\right) = \left(\frac{-1}{p}\right) \left(\frac{5}{p}\right) = (-1)^{\frac{p-1}{2}} \left(\frac{5}{p}\right) = \left(\frac{5}{p}\right)$  and so  $\left(\frac{-5}{p}\right) = \left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = \left(\frac{20k+13}{5}\right) = \left(\frac{3}{5}\right) = -1$ .

Let  $p \equiv 17 \pmod{20}$ . Then  $\left(\frac{-5}{p}\right) = \left(\frac{-1}{p}\right) \left(\frac{5}{p}\right) = (-1)^{\frac{p-1}{2}} \left(\frac{5}{p}\right) = \left(\frac{5}{p}\right)$  and so  $\left(\frac{-5}{p}\right) = \left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = \left(\frac{20k+17}{5}\right) = \left(\frac{7}{5}\right) = \left(\frac{2}{5}\right) = -1$ .

Let  $p \equiv 19 \pmod{20}$ . Then  $\left(\frac{-5}{p}\right) = \left(\frac{-1}{p}\right) \left(\frac{5}{p}\right) = (-1)^{\frac{p-1}{2}} \left(\frac{5}{p}\right) = -\left(\frac{5}{p}\right)$  and so  $\left(\frac{-5}{p}\right) = -\left(\frac{5}{p}\right) = -\left(\frac{p}{5}\right) = -\left(\frac{20k+19}{5}\right) = -\left(\frac{9}{5}\right) = -\left(\frac{4}{5}\right) = -1$ . In each case, since  $-5$  is not a square mod  $p$ ,  $p$  is irreducible in  $\mathbb{Z}[\sqrt{-5}]$  by Lemma 3.8.

□

### 3.3 When is a general element reducible?

We saw what happens to rational integers in our ring, but we really want to know when a general element  $a + b\sqrt{-5}$  is reducible in  $\mathbb{Z}[\sqrt{-5}]$ . Let's start with the trivial cases. Since we need not consider the 0 element, we may assume that at least one of  $a, b$  is not 0. If  $a = 0$  and  $b \neq 0$ , then  $b\sqrt{-5}$  is irreducible if and only if  $b = \pm 1$ . If  $a \neq 0$  and  $b = 0$ , then the element is simply an integer. If  $a$  is factorable in  $\mathbb{Z}$ , it will be reducible in  $R$ . However, if  $a$  is prime in  $\mathbb{Z}$ , then we must refer to Theorem 3.10.

When we study reducibility of a general element  $a + b\sqrt{-5}$ , we must realize that the set of elements of  $\mathbb{Z}[\sqrt{-5}]$  contains the set of integers. In fact, a simple integer pair  $(a, b)$  generates four elements of  $\mathbb{Z}[\sqrt{-5}]$ :  $a + b\sqrt{-5}$ ,  $a - b\sqrt{-5}$ ,  $-a + b\sqrt{-5}$ , and  $-a - b\sqrt{-5}$ . The following result shows that to determine the reducibility of these four elements it is enough to consider only one of them.

**Proposition 3.11.** *For  $a, b \in \mathbb{Z}$ , the following statements are equivalent:*

- (1)  $a + b\sqrt{-5}$  is reducible.
- (2)  $a - b\sqrt{-5}$  is reducible.
- (3)  $-a + b\sqrt{-5}$  is reducible.
- (4)  $-a - b\sqrt{-5}$  is reducible.



*Proof.* Assume  $a + b\sqrt{-5}$  is reducible. Then there exists  $m, n, s, t \in \mathbb{Z}$  such that  $a + b\sqrt{-5} = (m + n\sqrt{-5})(s + t\sqrt{-5})$ . This means  $a = ms - 5nt$  and  $b = mt + ns$ .

Then

$$-a - b\sqrt{-5} = -(ms - 5nt) - (mt + ns)\sqrt{-5} = (m + n\sqrt{-5})(-s - t\sqrt{-5}),$$

$$a - b\sqrt{-5} = (ms - 5nt) - (mt + ns)\sqrt{-5} = (-m + n\sqrt{-5})(-s + t\sqrt{-5}),$$

and

$$-a + b\sqrt{-5} = -(ms - 5nt) + (mt + ns)\sqrt{-5} = (-m + n\sqrt{-5})(s - t\sqrt{-5}).$$

Thus (1) implies (2), (3), and (4). Analogous arguments show that each one of (2), (3), and (4) implies the other three statements.  $\square$

It is important to note that, although the signs of  $a$  and  $b$  do not affect the *(ir)reducibility* of  $a + b\sqrt{-5}$  and its counterparts, the signs do matter in determining the actual *factorizations* of  $a + b\sqrt{-5}$  and its counterparts, as shown in the above proof. We will use this fact in the following chapter.

We can sometimes determine reducibility of  $a + b\sqrt{-5}$  based on properties of  $a$  and  $b$ . The next five propositions do just this.

**Proposition 3.12.** *Let  $a, b \in \mathbb{Z}$ . If  $\gcd(a, b) > 1$ , then  $a + b\sqrt{-5}$  is reducible.*

*Proof.* Let  $\gcd(a, b) = r > 1$ , that is,  $a = rs$  and  $b = rt$  for some integers  $s$  and  $t$ .

Then

$$a + b\sqrt{-5} = r(s + t\sqrt{-5}),$$

so  $a + b\sqrt{-5}$  is reducible.  $\square$

**Proposition 3.13.** *Let  $a, b \in \mathbb{Z}$ . If  $a$  is a multiple of 5, then  $a + b\sqrt{-5}$  is reducible.*

*Proof.* Let  $a = 5m$  for some  $m \in \mathbb{Z}$ . Then

$$a + b\sqrt{-5} = 5m + b\sqrt{-5} = (\sqrt{-5})(-m\sqrt{-5} + b),$$

so  $a + b\sqrt{-5}$  is reducible. □

**Proposition 3.14.** *If  $a \equiv \pm b \pmod{6}$  and  $a^2 + 5b^2 > 6$ , then  $a + b\sqrt{-5}$  is reducible.*

*Proof.* If  $a = \pm b$ , then  $a + b\sqrt{-5}$  is reducible by Proposition 3.12. So assume  $a \neq \pm b$  and  $a^2 + 5b^2 > 6$ . First, let  $a \equiv b \pmod{6}$ . Then  $a = b + 6k$  for some  $k \in \mathbb{Z}$  and

$$\begin{aligned} a + b\sqrt{-5} &= (b + 6k) + b\sqrt{-5} \\ &= (k + b + 5k) + (-k + k + b)\sqrt{-5} \\ &= ((k + b) - k\sqrt{-5})(1 + \sqrt{-5}). \end{aligned}$$

Since  $(k + b) - k\sqrt{-5}$  is not a unit for  $k \neq 0$  and  $1 + \sqrt{-5}$  is not a unit, we see that  $a + b\sqrt{-5}$  is reducible.

Now let  $a \equiv -b \pmod{6}$ . Then  $a = 5b + 6k$  for some  $k \in \mathbb{Z}$  and

$$\begin{aligned} (5b + 6k) + b\sqrt{-5} &= (k + 5(b + k)) + (b + k - k)\sqrt{-5} \\ &= (k + (k + b)\sqrt{-5})(1 - \sqrt{-5}). \end{aligned}$$

Since  $k + (k + b)\sqrt{-5}$  is not a unit for  $k \neq 0$  and  $1 - \sqrt{-5}$  is not a unit, we see that  $a + b\sqrt{-5}$  is reducible. □

Proposition 3.14 implies that at least one third of all the elements in the ring are reducible (since one third of all elements have the form  $a \equiv \pm b \pmod{6}$ ).

**Proposition 3.15.** *If  $a \equiv \pm 2b \pmod{9}$  and  $a^2 + 5b^2 > 9$ , then  $a + b\sqrt{-5}$  is reducible.*

*Proof.* First, let  $a \equiv 2b \pmod{9}$  and write  $a = 2b + 9k$  for some  $k \in \mathbb{Z}$ . Then

$$\begin{aligned} a + b\sqrt{-5} &= (2b + 9k) + b\sqrt{-5} \\ &= (4k + 2b + 5k) + (-2k + 2k + b)\sqrt{-5} \\ &= (2 + \sqrt{-5})((2k + b) - k\sqrt{-5}). \end{aligned}$$

To see that  $(2k + b) - k\sqrt{-5}$  is not a unit, note that it would only be a unit if  $k = 0$  and  $b = \pm 1$ , which would imply  $a^2 + 5b^2 = 9 \not> 9$ . Since  $2 + \sqrt{-5}$  is also not a unit,  $a + b\sqrt{-5}$  is reducible.

Now, let  $a \equiv -2b \pmod{9}$  and write  $a = -2b + 9k$  for some  $k \in \mathbb{Z}$ . Then

$$\begin{aligned} a + b\sqrt{-5} &= (-2b + 9k) + b\sqrt{-5} \\ &= (4k - 2b + 5k) + (2k - 2k + b)\sqrt{-5} \\ &= (2 - \sqrt{-5})((2k - b) + k\sqrt{-5}) \end{aligned}$$

To see that  $(2k - b) + k\sqrt{-5}$  is not a unit, note that it would be a unit only if  $k = 0$  and  $b = \pm 1$ , which would again imply  $a^2 + 5b^2 = 9 \not> 9$ . Since  $2 - \sqrt{-5}$  is also not a unit,  $a + b\sqrt{-5}$  is reducible.  $\square$

The five propositions above are rather straight forward. So a natural question is how powerful are these results? Using the algorithm described in the next chapter, we can examine these questions. It turns out that these propositions account for all the reducible elements up to norm 400. The “first” reducible element that does not fall into one of these cases is  $19 + 3\sqrt{-5}$ , with norm 406. In fact, of the 250 reducible elements with norm less than 1000, only 10 do not fall under the assumption of our

propositions. If we go up to norm 10,000, only 214 out of 1620 reducible elements are not described by our propositions. Figure 1 gives a graphical representation of the reducible elements with norm under 1000. The term “interesting reducible” refers to those elements not covered by the above five propositions.

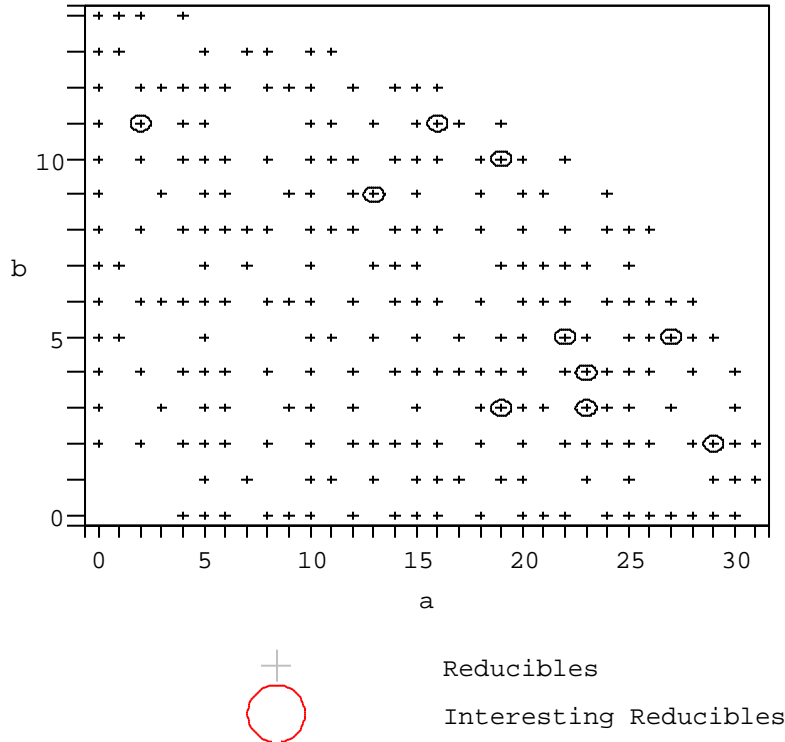


Figure 1: Graph of Reducibles and Interesting Reducibles

Of course, even though these theorems are powerful, they do not cover all the cases. When given a general element, we need to check if it falls under the conditions of one of our five propositions. If it does not, we need a different approach, which is the purpose of the algorithm described in Chapter 4.

## 4 Irreducibles

Although the sufficient conditions in Chapter 3 cover many reducible cases, they do not cover all reducible elements. We want something that can definitively tell us when a given element is irreducible, much like the various tests for primality that exist for the rational integers.

### 4.1 Irreducibility Algorithm

At the end of Section 3.1, we introduced a way to determine the factors of a given element. It turns out that these computations can also determine if an element is irreducible. If, by looking at the elements whose norms are factors of the norm of our element, we do not find two elements that multiply to the element in question, then our element is irreducible. Let's look at an example. Consider the element  $7 + 5\sqrt{-5}$  with norm 174. If it factors, Lemma 3.4 shows that the factors must have norms that divide 174. So let us consider the factorizations of 174 and throw out the impossible norms. We can check that

$$174 = 2 \cdot 3 \cdot 29 = 1 \cdot 174 = 2 \cdot 87 = 3 \cdot 58 = 6 \cdot 29.$$

Since the only factorization involving products of possible (nontrivial) norms is  $6 \cdot 29$ , we need only look at all elements of norms 6 and 29, namely  $\pm 1 \pm \sqrt{-5}$  and  $\pm 3 \pm 2\sqrt{-5}$ . Let's compute the possible products:

$$(1 + \sqrt{-5})(3 + 2\sqrt{-5}) = -9 + 5\sqrt{-5}$$

$$(1 + \sqrt{-5})(-3 - 2\sqrt{-5}) = 9 + 5\sqrt{-5}$$

$$(1 - \sqrt{-5})(3 - 2\sqrt{-5}) = -9 - 5\sqrt{-5}$$

$$(1 - \sqrt{-5})(-3 + 2\sqrt{-5}) = 9 - 5\sqrt{-5}$$

$$(1 + \sqrt{-5})(3 - 2\sqrt{-5}) = 15 + \sqrt{-5}$$

$$(1 + \sqrt{-5})(-3 + 2\sqrt{-5}) = -15 + \sqrt{-5}$$

$$(1 - \sqrt{-5})(3 + 2\sqrt{-5}) = 15 - \sqrt{-5}$$

$$(1 - \sqrt{-5})(-3 - 2\sqrt{-5}) = -15 - \sqrt{-5}$$

Since none of these multiply to  $7 + 5\sqrt{-5}$ , it must be irreducible. Thus, with some computations, we can definitively find when a given element is irreducible!

We would like to know which elements are reducible and which are irreducible. However, the above technique requires an exhausting amount of work by hand. So we want to design a computer algorithm to give us a list of elements and tell us whether each element is (ir)reducible. We will use the following simple algorithm (for the code in Maple, see Appendix A).

1. Create a list  $S$  of all positive integer pairs  $(a, b)$  and compute the norms of the corresponding elements  $\pm a \pm b\sqrt{-5}$ .
2. Check each element in  $S$  for reducibility using Propositions 3.12 – 3.15.
3. For each element  $a + b\sqrt{-5}$  of  $S$ , find all non-trivial two-factor factorizations of  $N(a + b\sqrt{-5})$ , where the factors are themselves norms.
4. For each nontrivial factorization  $N(a + b\sqrt{-5}) = st$  found in step 2, multiply

all elements of norm  $s$  with all elements of norm  $t$ . If there are two elements whose product is  $a + b\sqrt{-5}$ , then  $a + b\sqrt{-5}$  is reducible. If no such pair is found,  $a + b\sqrt{-5}$  is irreducible.

## 4.2 Comparing $\mathbb{Z}[\sqrt{-5}]$ with $\mathbb{Z}$

With the algorithm, we can determine an endless number of irreducible elements (supposing that there are infinitely many rational primes  $p \equiv 3, 7, 11, 13, 17, 19 \pmod{20}$ ). This allows us to study the irreducibles in our ring in a more efficient way and even compare them with irreducibles in other rings, such as the ring of integers. The set of irreducibles in  $\mathbb{Z}$  is just the set of rational primes (primes in  $\mathbb{Z}$ ). One of the most widely studied aspects of primes in  $\mathbb{Z}$  is their density amongst the other integers. In fact, there is a function,  $\pi(n)$ , which denotes the number of primes up to and including  $n$ . So the obvious question arises: What is the density of irreducibles in  $\mathbb{Z}[\sqrt{-5}]$  and is it similar to that of the primes in the integers?

We want to define a function  $IR(n)$  for  $\mathbb{Z}[\sqrt{-5}]$  that is somehow analogous to  $\pi(n)$  for the integers. Since  $\mathbb{Z}[\sqrt{-5}]$  is not an ordered set, we can not talk about the elements of  $\mathbb{Z}[\sqrt{-5}]$  “less than”  $n$ , but we can talk about the elements with norm less than or equal to  $n$ .

Recall that elements in our ring look like  $\pm a \pm b\sqrt{-5}$ . Do we want to count all of these? The function  $\pi(n)$  only counts the positive numbers (those found on the right of the real line). Analogously, we want to count only those elements on the

right half of the complex plane. So let  $IR(n)$  be the number of irreducibles of the form  $a \pm b\sqrt{-5}$  with norms up to a given  $n$  with  $a, b \geq 0$ . As an example, take  $n = 20$ . Then

$$\pi(20) = |\{2, 3, 5, 7, 11, 13, 17, 19\}| = 8$$

and

$$IR(20) = |\{2, 3, \pm\sqrt{-5}, 1 \pm \sqrt{-5}, 2 \pm \sqrt{-5}, 3 \pm \sqrt{-5}\}| = 10.$$

Is  $IR(n)$  the right analogy to  $\pi(n)$ ? Let's consider for a moment the number 7, an element in both rings. For the function  $\pi(n)$ , we need only go up to  $n = 7$  to count the number of primes up to 7, but for  $IR(n)$ , we must go up to  $n = 49$ , the norm of 7, to count the number of primes. So maybe the right analog for  $\pi(n)$  is  $IR(n^2)$  instead of  $IR(n)$ . Let's look at some values.

$n$	10	100	1000	10000
$\pi(n)$	4	25	168	1229
$IR(n)$	8	35	237	1832
$IR(n^2)$	35	1832	*	*

Table 3: Comparison between number of irreducibles and number of primes.

We immediately see that  $IR(n^2)$  is not the right comparison as the value for  $n = 100$  is already at 1832! However, there does seem to be a similarity in general shape between  $\pi(n)$  and  $IR(n)$ . Let's look at this graphically in Figure 2.



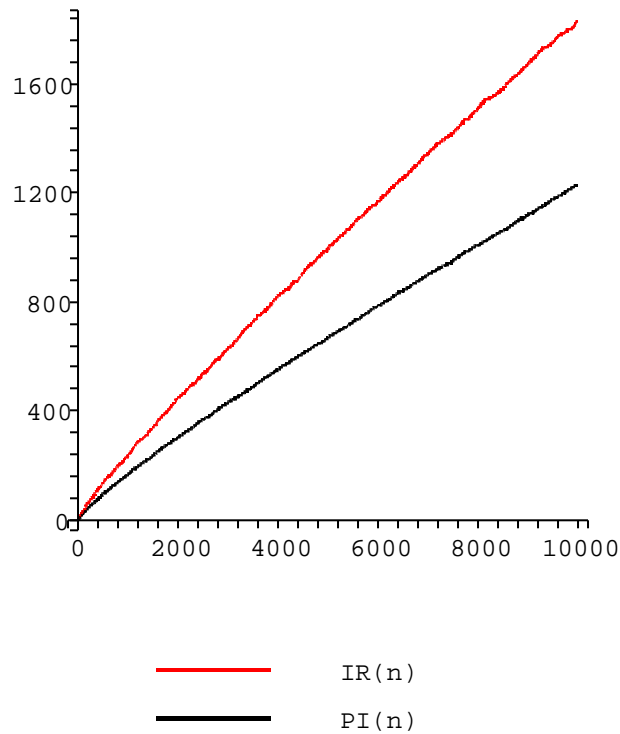


Figure 2:  $IR(n)$  and  $\pi(n)$

It appears that  $\pi(n)$  is much smaller than  $IR(n)$  as  $n$  increases. However, the number of elements in our ring up to a given norm  $n$  is different from the number of elements in  $\mathbb{Z}$  up to a given  $n$ . Going back to our previous example of  $n = 20$ , there are 20 positive integers up to  $n = 20$ , yet 15 elements in  $\mathbb{Z}[\sqrt{-5}]$  with norm less than 20 and  $a \geq 0$ . So we can modify our comparison to reflect this difference. Since we began discussing the density of primes and irreducibles, let us now compare  $\frac{\pi(n)}{n}$  with  $\frac{IR(n)}{Count(n)}$  where  $Count(n)$  is the number of elements up to a norm  $n$  much like for the set of integers  $n$  is the number of elements up to  $n$ .

$n$	10	100	1000	10000
$Count(n)$	10	75	718	4357
$\frac{\pi(n)}{n}$	.4	.25	.17	.12
$\frac{IR(n)}{Count(n)}$	.8	.47	.33	.26

Table 4: Density of primes and irreducibles

It is easy to see from the table that  $\frac{IR(n)}{Count(n)}$  is about 2 times larger than  $\frac{\pi(n)}{n}$ , at least up to norm 10,000. This suggests that, as  $n$  gets larger, the density of irreducibles follows a pattern similar to that of the density of rational primes.

### 4.3 Approximating $IR(n)$

The following well-known theorem gives us an approximation for the number of primes up to a given  $n$ .

**Theorem 4.1 (Prime Number Theorem).** *The number of prime numbers up to a given  $n$ , denoted  $\pi(n)$  is approximated by the function  $\frac{n}{\ln(n)}$  for large  $n$ .*

*Proof.* See pp. 278-291 in [A]. □

Inspired by the Prime Number Theorem, we might guess that  $IR(n)$  is approximated by  $\frac{Count(n)}{\ln(Count(n))}$ .

We can see on Figure 3 that  $\frac{Count(n)}{\ln(Count(n))}$  vastly underestimates  $IR(n)$ , so we try to multiply it by some constant, as in Figure 4. Our constant (in this case 4.16)

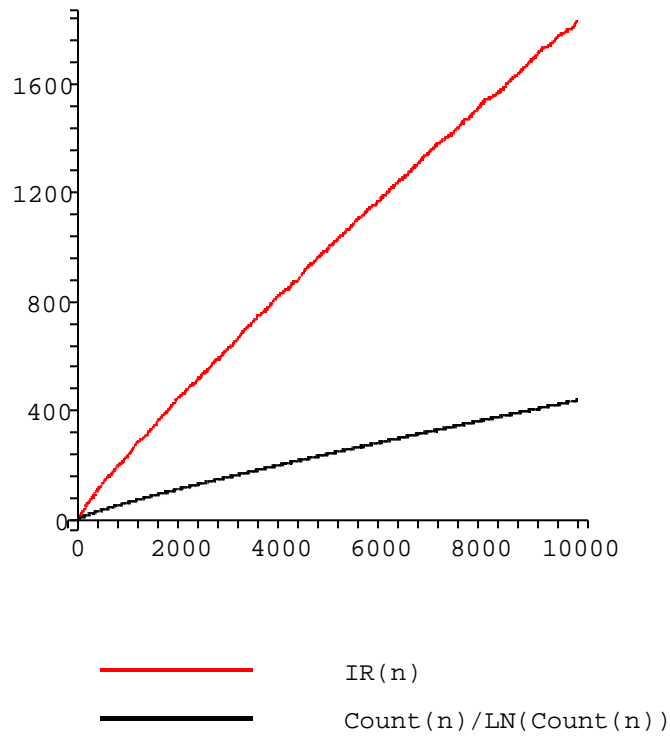


Figure 3:  $IR(n)$  and  $\frac{Count(n)}{\ln(Count(n))}$

comes from determining a linear fit for the two functions  $IR(n)$  and  $\frac{Count(n)}{\ln(Count(n))}$  of the form  $y = Ax$ .

Although this is a good approximation up to norm 10,000, its easy to see that the difference between the two functions will grow large as  $n$  gets larger as  $4.16 \frac{Count(n)}{\ln(Count(n))}$  is more concave down. Thus, we have not found a good fit for  $IR(n)$ . Finding a good approximation is actually a rather complicated task that relates to Riemann Zeta functions. For more information, see Chapter 12 in [A].

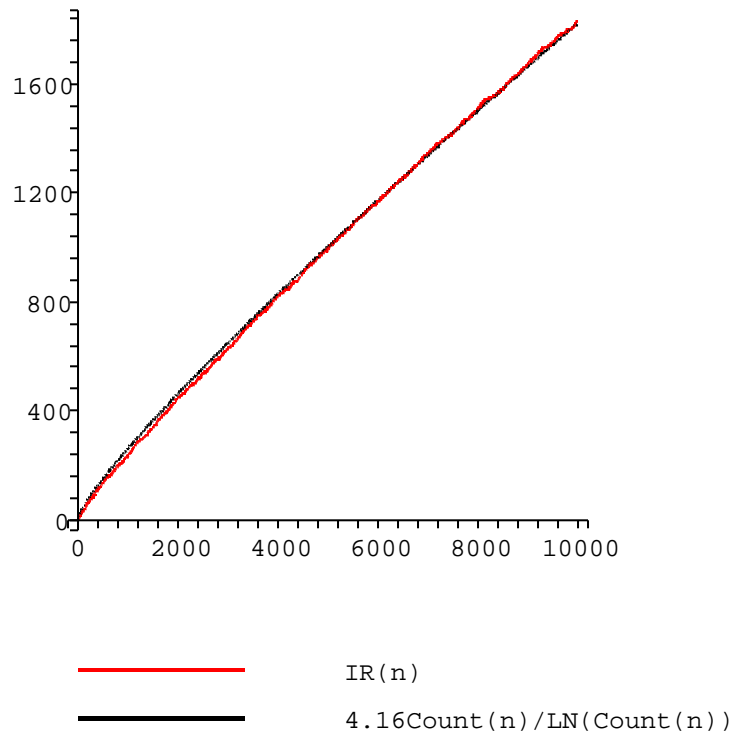


Figure 4:  $\text{IR}(n)$  and  $4.16 \cdot \frac{\text{Count}(n)}{\text{LN}(\text{Count}(n))}$

#### 4.4 How often and how badly does unique factorization fail?

Now that we have an algorithm to determine the reducibility of an element, we can use it to check just how badly unique factorization fails. We will return to looking at only elements of the form  $a + b\sqrt{-5}$  where  $a, b > 0$  (Proposition 3.11 implies that if unique factorization fails for  $a + b\sqrt{-5}$ , it will also imply for  $a - b\sqrt{-5}$ .) It turns out that, of the 375 elements (250 of which are reducible) up to norm 1,000, only 44 have non-unique factorizations. Of these 44 elements, 38 have only two factorizations, 5 have three factorizations, and only one has four factorizations. The first element with three factorizations is 21, whose factorizations are  $(3)(7)$ ,  $(4 + \sqrt{-5})(4 - \sqrt{-5})$ ,

and  $1+2\sqrt{-5})(1-2\sqrt{-5})$  and the only element with four factorizations is  $24+6\sqrt{-5}$ . This element has four factorizations as two of its factors, 6 and  $12 + 3\sqrt{-5}$ , each have two factorizations themselves. So, in a sense, unique factorization does not fail that badly (at least up to norm 1,000).

To take this point even further, of the 44 elements with more than one factorization, there are 14 that have non-unique factorizations because one of their factors has non-unique factorizations as well. For example, 12 has non-unique factorizations because 6 has non-unique factorizations. The factorizations of 6, as we saw in the introduction, are  $(2)(3)$  and  $(1 + \sqrt{-5})(1 - \sqrt{-5})$ ; the factorizations of 12 are simply  $(2)(2)(3)$  and  $(2)(1 + \sqrt{-5})(1 - \sqrt{-5})$ . Of these 14 elements, 11 have two factorizations, 2 have three factorizations, and 1 has four factorizations (the element  $24 + 6\sqrt{-5}$  mentioned above. It turns out that only the elements with more than 2 factorizations actually have two factors that fail to have unique factorization.

Of the 16 elements (less than norm 1,000) with 3 irreducible factors per factorization, 11 of them have a factor that has non-unique factorizations and of the 4 elements (less than norm 1,000) with 4 factors per factorization, 3 of them have a factor that has non-unique factorizations. Thus only 30 of the 375 elements with norm less than 1,000 are interesting cases where unique factorization fails.

## 5 Factorizations of Ideals

In the previous chapters, we studied when and how the elements of  $\mathbb{Z}[\sqrt{-5}]$  factor, and even how many factorizations they have. Now, we turn to the ideals of  $\mathbb{Z}[\sqrt{-5}]$ , where unique factorization holds.

### 5.1 Definitions and Results from Ideal Theory

Before we study the ideals, we must first establish what an ideal is and some results that are necessary for our study. From now on, we will assume that all rings are commutative and have an identity.

**Definition 5.1.** *A subset  $S$  of a ring  $R$  is a subring of  $R$  if  $S$  is itself a ring with the operations of  $R$  and  $1 \in S$ .*

**Definition 5.2.** *A subring  $I$  of a commutative ring  $R$  is called an ideal of  $R$  if  $ra$  is in  $I$  for every  $r \in R$  and every  $a \in I$ .*

In any ring  $R$ ,  $\{0\}$  is an ideal since  $a \cdot 0 = 0 \in R$  for all  $a \in R$ , and the entire ring is an ideal as it is closed under multiplication. We can also create ideals generated by any other element of the ring.

**Definition 5.3.** *An ideal  $I$  of a ring  $R$  is a principal ideal if there exists  $a \in R$  such that  $I = (a) = \{ar \mid r \in R\}$ . In other words,  $I$  is generated by  $a$ .*

An example of a principal ideal is  $(2)$  in  $\mathbb{Z}$ . This is simply the set of even integers. Another example is  $(2)$  in  $\mathbb{Z}[\sqrt{-5}]$ , which is the set of elements  $a + b\sqrt{-5}$  where 2

divides both  $a$  and  $b$ .

**Definition 5.4.** Let  $R$  be a commutative ring with unity and let  $a_1, a_2, \dots, a_n$  be elements of  $R$ . Then  $I = (a_1, a_2, \dots, a_n) = \{r_1 a_1 + r_2 a_2 + \dots + r_n a_n \mid r_i \in R\}$  is an ideal of  $R$  and is called the ideal generated by  $a_1, a_2, \dots, a_n$ .

Some examples of ideals generated by specific elements in  $\mathbb{Z}[\sqrt{-5}]$  are

$$(\sqrt{-5}) = \{r\sqrt{-5} \mid r \in \mathbb{Z}[\sqrt{-5}]\} = \{a\sqrt{-5} - 5b \mid a, b \in \mathbb{Z}\}$$

and

$$(2, 1 + \sqrt{-5}) = \{r2 + s(1 + \sqrt{-5}) \mid r, s \in \mathbb{Z}[\sqrt{-5}]\}.$$

We can also define operations on ideals.

**Definition 5.5.** The sum of two ideals  $I$  and  $J$  is defined as  $I + J = \{a + b \mid a \in I, b \in J\}$ . The product of two ideals  $I$  and  $J$  is defined as  $IJ = \{\sum a_i b_i \mid a_i \in I, b_i \in J\}$ .

As irreducible elements acted as the building blocks for elements in  $\mathbb{Z}[\sqrt{-5}]$ , prime ideals will do the same for ideals of  $\mathbb{Z}[\sqrt{-5}]$ .

**Definition 5.6.** A prime ideal  $I$  of a commutative ring  $R$  is a proper ideal of  $R$  in which for all  $a, b \in R$   $ab \in I$  implies  $a \in I$  or  $b \in I$ .

**Definition 5.7.** A proper ideal of a ring is an ideal that is strictly smaller than the entire ring. A maximal ideal  $I$  of  $R$  is a proper ideal of  $R$  for which, whenever  $J$  is an ideal of  $R$  and  $I \subseteq J \subseteq R$ , then  $J = I$  or  $J = R$ .

The rest of this section describes results necessary for our analysis in the remainder of this thesis.

**Definition 5.8.** *If  $R \subseteq S$ , where  $R$  and  $S$  are rings, then  $S$  is said to be integral over  $R$  provided that every element of  $S$  is integral over  $R$ , namely, for any  $s \in S$ , there exists a nonzero monic polynomial  $f(x) \in R[x]$  such that  $f(s) = 0$ . If every element in  $S$  that is integral over  $R$  actually belongs to  $R$ , then  $R$  is called integrally closed in  $S$ .*

**Notation.** *Let  $R$  be a ring and  $I$  be an ideal of  $R$ . Then  $R/I = \{r + I \mid r \in R\}$  is called the quotient ring of  $R$  by  $I$ .*

Some examples are  $\mathbb{Z}/(2)$ , which is just  $\mathbb{Z}_2 = \{0, 1\}$ , and  $\mathbb{Z}[\sqrt{-5}]/(6)$ , which is just  $\mathbb{Z}_6[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}_6\}$ .

The following two propositions are taken from [G, p.259].

**Proposition 5.9.** *Let  $R$  be a commutative ring with identity and let  $I$  be an ideal. Then  $R/I$  is an integral domain if and only if  $I$  is prime.*

*Proof.* First, suppose that  $R/I$  is an integral domain. Let  $a, b \in R$  such that  $ab \in I$ . Then  $(a + I)(b + I) = ab + I = I$  which implies either  $a + I = I$  or  $b + I = I$  since  $R/I$  is an integral domain. If  $a + I = I$ , then  $a \in I$ . If  $b + I = I$ , then  $b \in I$ . Therefore, since either  $a \in I$  or  $b \in I$ ,  $I$  is prime.

Now, assume  $I$  is prime. We know  $R/I$  is a commutative ring with identity so we need only show it has no zero divisors. Suppose  $a + I, b + I \in R/I$  such that



$(a + I)(b + I) = 0 + I = I$ . Then  $ab \in I$ , which implies  $a \in I$  or  $b \in I$ . Thus,  $a + I = 0 + I$  or  $b + I = 0 + I$ . So,  $R/I$  has no zero divisors and  $R/I$  is an integral domain.  $\square$

**Proposition 5.10.** *Let  $R$  be a commutative ring with identity and let  $I$  be an ideal of  $R$ . Then  $R/I$  is a field if and only if  $I$  is maximal.*

*Proof.* First, suppose  $R/I$  is a field and  $J$  is an ideal of  $R$  such that  $I \subset J$ . Let  $a \in J$ , but  $a \notin I$ . Then  $a + I$  is a nonzero element of  $R/I$  and, therefore, since  $R/I$  is a field, there exists  $b \in I$  such that  $(a + I)(b + I) = 1 + I$ . Since  $a \in J$ , we have  $ab \in J$ , and since  $1 + I = (a + I)(b + I) = ab + I$ , we have  $1 - ab \in I \subset J$ . So  $1 = (1 - ab) + ab \in J$  and  $J = R$  as  $J$  contains the identity. Thus  $I$  is maximal by definition.

Now, suppose  $I$  is maximal and let  $a \in R$  but  $a \notin I$ . To show  $R/I$  is a field, we need only to show that  $a + I$  has a multiplicative inverse. Consider the ideal  $J = \{ar + b \mid r \in R, b \in I\}$ . Then  $I \subsetneq J$ . Since  $I$  is maximal and  $I \neq J$ , we have  $J = R$  and so  $J$  must contain the identity. There exists  $b' \in I$  and  $c \in R$  such that  $1 = ac + b'$  and so  $1 + I = ac + b' + I = ac + I = (a + I)(c + I)$ . Thus  $a + I$  has a multiplicative inverse and  $R/I$  is a field.  $\square$

**Proposition 5.11.** *Every maximal ideal is a prime ideal.*

*Proof.* Let  $M$  be a maximal ideal. Then by Proposition 5.10,  $R/M$  is a field. Since every field is an integral domain, we see by Proposition 5.9 that  $M$  is prime.  $\square$

## 5.2 How ideals factor

In the previous chapter, we considered factorizations of elements in  $\mathbb{Z}[\sqrt{-5}]$ ; here we look at factorizations of ideals in  $\mathbb{Z}[\sqrt{-5}]$ . Much like an element of a ring  $R$ , an ideal is reducible if it can be expressed as the product of two proper, nontrivial ideals.

Let us first consider principal ideals. Say we have an element  $a \in \mathbb{Z}$  such that  $a = bc$ . Then the ideal generated by  $a$  can be factored as  $(a) = (b)(c)$ . Thus, for any composite integer, the corresponding ideal generated by that integer will also be reducible. What about rational primes in  $\mathbb{Z}[\sqrt{-5}]$ ? We know how they factor as elements (Theorem 3.10), but how do they factor as ideals? We know that if a prime is reducible as an element, it will be reducible as an ideal but if it is irreducible as an element, will it be irreducible as an ideal? It turns out that sometimes it is irreducible as an ideal but sometimes it is not. An ideal generated by an irreducible element is not necessarily irreducible as an ideal, as we will see in Theorem 5.16. First, we need to establish a way of factoring an ideal generated by certain rational primes.

**Proposition 5.12.** *Let  $p$  be an odd rational prime and suppose there exists  $z \in \mathbb{Z}$  such that  $z^2 \equiv -5 \pmod{p}$ . Then  $(p) = (z + \sqrt{-5}, p)(z - \sqrt{-5}, p)$ . Moreover,  $(z + \sqrt{-5}, p)$  and  $(z - \sqrt{-5}, p)$  are prime ideals.*

*Proof.* Consider the ideal  $(z + \sqrt{-5}, z - \sqrt{-5}, p, \frac{z^2+5}{p})$ . This ideal contains both  $p$  and  $(z + \sqrt{-5}) + (z - \sqrt{-5}) = 2z$ , which are relatively prime since  $z \not\equiv 0 \pmod{p}$  and

$p \neq 2$ . Then 1 is in the ideal as we can use the extended Euclidean algorithm to find a linear combination of  $p$  and  $2z$  that equals 1, and so  $R = (z + \sqrt{-5}, z + \sqrt{-5}, p, \frac{z^2+5}{p})$ . So we need only show  $(p, z - \sqrt{-5})(p, z + \sqrt{-5}) = (p)(z + \sqrt{-5}, z + \sqrt{-5}, p, \frac{z^2+5}{p})$ . For simplicity, let  $I = (p, z - \sqrt{-5})$ ,  $J = (p, z + \sqrt{-5})$ ,  $K = (p)$ , and  $L = (z + \sqrt{-5}, z + \sqrt{-5}, p, \frac{z^2+5}{p})$ . We will first show  $IJ \subseteq KL$ . To show this containment, it is enough to show the four elements  $p^2, p(z + \sqrt{-5}), p(z - \sqrt{-5}), (z - \sqrt{-5})(z + \sqrt{-5}) \in IJ$  are in  $KL$ . It is easy to see  $p^2 = pp \in KL, p(z + \sqrt{-5}) \in KL, p(z - \sqrt{-5}) \in KL$ , and  $(z - \sqrt{-5})(z + \sqrt{-5}) = z^2 + 5 = p\frac{z^2+5}{p} \in KL$ . So,  $IJ \subseteq KL$ . To show  $KL \subseteq IJ$ , consider the elements  $pp, p(z + \sqrt{-5}), p(z - \sqrt{-5}), p\frac{z^2+5}{p} \in KL$ . It is again easy to see  $pp = p^2 \in IJ, p(z + \sqrt{-5}) \in IJ, p(z - \sqrt{-5}) \in IJ, p\frac{z^2+5}{p} = z^2 + 5 = (z - \sqrt{-5})(z + \sqrt{-5}) \in IJ$ . So  $KL \subseteq IJ$  which implies  $KL = IJ$ . Thus  $(p) = (z + \sqrt{-5}, p)(z - \sqrt{-5}, p)$ .

Now we will show  $(z + \sqrt{-5}, p)$  and  $(z - \sqrt{-5}, p)$  are prime ideals. Consider  $\frac{\mathbb{Z}[\sqrt{-5}]}{(p, z \pm \sqrt{-5})} \cong \frac{\mathbb{Z}_p[\sqrt{-5}]}{(z \pm \sqrt{-5})} \cong \mathbb{Z}_p$ . Of course  $\mathbb{Z}_p$  is an integral domain and by Proposition 5.10  $(z \pm \sqrt{-5}, p)$  is maximal. Since every maximal ideal is prime,  $(z + \sqrt{-5}, p)$  is prime.  $\square$

Note that this proposition applies to rational primes that are reducible and some that are irreducible as elements.

**Example 5.13.** Consider  $p = 23$  (an irreducible element by Theorem 3.10). We know  $8^2 \equiv -5 \pmod{23}$  and so  $(23) = (8 + \sqrt{-5}, 23)(8 - \sqrt{-5}, 23)$ .

**Example 5.14.** Consider  $p = 89$  (a reducible element by Theorem 3.10). We

know  $23^2 \equiv -5 \pmod{89}$  and so  $(89) = (23 + \sqrt{-5}, 89)(23 - \sqrt{-5}, 89)$ . In this case,  $3 \pm 4\sqrt{-5}$  is a factor of both  $23 + \sqrt{-5}$  and  $89$ , so  $(89) = (23 + \sqrt{-5}, 89)(23 - \sqrt{-5}, 89) = (3 + 4\sqrt{-5})(3 - 4\sqrt{-5})$  which says  $(89)$  is actually the product of principal ideals.

It turns out that we can find  $z$  such that  $z^2 \equiv -5 \pmod{p}$  for all  $p$  such that  $p \equiv 1, 3, 7, 9 \pmod{20}$ . We will see this in Theorem 5.16

**Definition 5.15.** Let  $R$  be a number ring. A rational prime  $p$  in  $R$  is said to split if it can be factored into a product of two irreducibles in  $R$ . A rational prime  $p$  in  $R$  is said to ramify if it is the square of an irreducible element of  $R$ . Finally, a rational prime that neither splits nor ramifies must itself be irreducible, and is sometimes said to stay prime.

**Theorem 5.16.** Let  $\mathbb{Z}[\sqrt{-5}]$ , and let  $p$  be a rational prime in  $\mathbb{Z}[\sqrt{-5}]$ . Then

1.  $(p)$  ramifies if  $p = 2$  or  $p = 5$ .
2.  $(p)$  splits if  $-5$  is a square modulo  $p$ . This can occur in one of two ways:
  - (a) If  $p \equiv 1$  or  $9 \pmod{20}$ , then  $p$  factors in  $\mathbb{Z}[\sqrt{-5}]$  as a product of two irreducibles  $a$  and  $b$  of  $\mathbb{Z}[\sqrt{-5}]$ . Then  $(p) = (a)(b)$ .
  - (b) If  $p \equiv 3$  or  $7 \pmod{20}$ , then  $p$  is reducible as an element and  $(p)$  is reducible as an ideal.
3. The element  $p$  is irreducible in  $\mathbb{Z}[\sqrt{-5}]$  (and thus the ideal  $(p)$  is irreducible)

if  $-5$  is not a square modulo  $p$ , which is exactly when  $p \equiv 11, 13, 17$ , or  $19 \pmod{20}$ .

*Proof.* We will break the proof into four cases.

1. Let  $p = 2$ . Then  $(p) = (2) = (1 + \sqrt{-5}, 2)(1 - \sqrt{-5}, 2)$  by Proposition 5.12. Since  $2 - (1 - \sqrt{-5}) = 1 + \sqrt{-5}$ , we have  $(1 + \sqrt{-5}, 2) = (1 - \sqrt{-5}, 2)$ . Thus  $(2) = (1 + \sqrt{-5}, 2)^2$ . Let  $p = 5$ ; then  $(p) = (5) = (\sqrt{-5})(-\sqrt{-5}) = (\sqrt{-5})^2$ .

(a) Let  $p \equiv 1, 9 \pmod{20}$ . By Theorem 3.10,  $p = ab$  for some non-units  $a, b \in \mathbb{Z}[\sqrt{-5}]$ . Thus  $(p) = (a)(b)$ .

(b) Let  $p \equiv 3 \pmod{20}$ . We want to show that there exists  $z$  such that  $z^2 \equiv -5 \pmod{p}$ . Then,  $(p)$  would be reducible by Proposition 5.12.

Analogous to the proof of Theorem 3.10, we will use Legendre Symbols.

So  $\left(\frac{-5}{p}\right) = \left(\frac{-1}{p}\right) \left(\frac{5}{p}\right) = (-1)^{\frac{p-1}{2}} \left(\frac{5}{p}\right) = (-1)^{\frac{20k+3-1}{2}} \left(\frac{5}{p}\right) = -\left(\frac{5}{p}\right)$  and  $\left(\frac{-5}{p}\right) = -\left(\frac{5}{p}\right) = -\left(\frac{p}{5}\right) = -\left(\frac{20k+3}{5}\right) = -\left(\frac{3}{5}\right) = 1$ . Thus, there exists

$z$  such that  $z^2 \equiv -5 \pmod{p}$  and  $(p)$  is reducible. Let  $p \equiv 7 \pmod{20}$ .

Then  $\left(\frac{-5}{p}\right) = \left(\frac{-1}{p}\right) \left(\frac{5}{p}\right) = (-1)^{\frac{p-1}{2}} \left(\frac{5}{p}\right) = (-1)^{\frac{20k+7-1}{2}} \left(\frac{5}{p}\right) = -\left(\frac{5}{p}\right)$  and  $\left(\frac{-5}{p}\right) = -\left(\frac{5}{p}\right) = -\left(\frac{p}{5}\right) = -\left(\frac{20k+7}{5}\right) = -\left(\frac{2}{5}\right) = 1$ . Thus, by Proposi-

tion 5.12,  $(p) = (p, z + \sqrt{-5})(p, z - \sqrt{-5})$  for  $p \equiv 3$  or  $7 \pmod{20}$ .

2. For  $p \equiv 11, 13, 17, 19 \pmod{20}$ , we know there does not exist  $z$  such that  $z^2 \equiv -5 \pmod{p}$  by Theorem 3.10. Thus  $x^2 + 5$  is irreducible in  $\mathbb{Z}_p[x]$  and

$\frac{\mathbb{Z}_p[x]}{(x^2+5)}$  is an integral domain. Of course,  $\frac{\mathbb{Z}_p[x]}{(x^2+5)} \cong \frac{\mathbb{Z}[x]}{(p, x^2+5)} \cong \frac{\mathbb{Z}[\sqrt{-5}]}{(p)}$ . Therefore,

if  $p \equiv 11, 13, 17$ , or  $19 \pmod{20}$ , then  $(p)$  is irreducible.

□

So far, we have looked at all of the principal ideals in  $\mathbb{Z}[\sqrt{-5}]$  generated by rational integers, but what about those generated by a general element? We can nontrivially factor the ideal generated by a reducible elements: if  $\alpha = \beta\gamma$ , then  $(\alpha) = (\beta)(\gamma)$ . Let's look at some examples. The ideal  $(2 + 4\sqrt{-5})$  can be factored into  $(2)(1+2\sqrt{-5})$  and the ideal  $(7+\sqrt{-5})$  can be factored into  $(1+\sqrt{-5})(2-\sqrt{-5})$ . What about irreducible elements in our ring? We already saw that  $(23) = (8 + \sqrt{-5}, 23)(8 - \sqrt{-5}, 23)$  where 23 is irreducible in our ring. So we know that there exist irreducible elements that are reducible as ideals.

Let us consider an ideal in  $\mathbb{Z}[\sqrt{-5}]$  generated by more than one rational integer. If  $\gcd(a, b) = r$ , then the ideal  $(a, b)$  is equal to the ideal  $(r)$ . If  $\gcd(a, b) = 1$ , then the ideal  $(a, b)$  is  $R$ , where  $R$  is the whole ring. This works in general: for an ideal  $(a, b, c, d, \dots)$  where  $a, b, c, d, \dots \in \mathbb{Z}$ , if  $\gcd(a, b, c, d, \dots) = r$ , then  $(a, b, c, d, \dots) = (r)$  (Note that the ideal  $(1)$  is the whole ring.) We will see at the end of Chapter 6 that all ideals in  $\mathbb{Z}[\sqrt{-5}]$  can actually be factored uniquely as products of prime ideals, even though the generating elements can not be factored uniquely into irreducibles.

## 6 Dedekind Domains

When we studied the factorizations of elements and ideals in  $\mathbb{Z}[\sqrt{-5}]$ , we said without proof that unique factorization fails for elements but does not fail for ideals. This chapter will examine why unique factorization fails for elements but holds for ideals.

### 6.1 Quadratic Number Rings

Before we show that our ring is a quadratic number ring and explain why unique factorization fails, we need a bit of theory.

**Definition 6.1.** Let  $\alpha \in \mathbb{C}$ . Define  $\mathbb{Q}(\alpha)$  to be the smallest field contained in  $\mathbb{C}$  that contains both  $\mathbb{Q}$  and  $\alpha$ .

**Proposition 6.2.** The field  $\mathbb{Q}(\alpha)$  is exactly equal to the set

$$\left\{ \frac{p(\alpha)}{q(\alpha)} \mid p(\alpha), q(\alpha) \in \mathbb{Q}[\alpha], \text{ with } q(\alpha) \neq 0 \right\}.$$

*Proof.* By definition,  $\mathbb{Q}(\alpha)$  is the smallest field containing both  $\mathbb{Q}$  and  $\alpha$ . Since fields are closed under addition and multiplication, we have  $\alpha^n \in \mathbb{Q}(\alpha)$  for all  $n \in \mathbb{N}$  and  $c\alpha^n \in \mathbb{Q}(\alpha)$  for all  $c \in \mathbb{Q}$  and for all  $n \in \mathbb{N}$ . Thus,  $c_n\alpha^n + c_{n-1}\alpha^{n-1} + \cdots + c_1\alpha + c_0 \in \mathbb{Q}(\alpha)$  for all  $c_i \in \mathbb{Q}$  and  $n \in \mathbb{N}$ . Since  $\mathbb{Q}(\alpha)$  is a field,  $\frac{1}{b_m\alpha^m + b_{m-1}\alpha^{m-1} + \cdots + b_1\alpha + b_0} \in \mathbb{Q}(\alpha)$  whenever  $b_m\alpha^m + \cdots + b_0 \neq 0$ . Then

$$(c_n\alpha^n + \cdots + c_0) \left( \frac{1}{b_m\alpha^m + \cdots + b_0} \right) = \frac{c_n\alpha^n + \cdots + c_0}{b_m\alpha^m + \cdots + b_0} \in \mathbb{Q}(\alpha).$$

Therefore,  $\left\{ \frac{p(\alpha)}{q(\alpha)} \right\} \subseteq \mathbb{Q}(\alpha)$ . Of course,  $\left\{ \frac{p(\alpha)}{q(\alpha)} \right\}$  is a field containing  $\alpha$  and  $\mathbb{Q}$ , and since  $\mathbb{Q}(\alpha)$  is the smallest such field, we have  $\left\{ \frac{p(\alpha)}{q(\alpha)} \right\} = \mathbb{Q}(\alpha)$ .  $\square$

We want to show that  $\mathbb{Q}(\alpha) = \mathbb{Q}[\alpha]$  because elements of  $\mathbb{Q}[\alpha]$  are easier to manipulate. In order to do so, we need more terminology and results.

**Definition 6.3.** *If a complex number is a root of a nonzero monic polynomial in  $\mathbb{Q}[x]$ , it is called an algebraic number. If it is a root of a nonzero monic polynomial in  $\mathbb{Z}[x]$ , it is called an algebraic integer.*

Some examples that are both algebraic numbers and algebraic integers are  $\sqrt{-5}$ , as  $\sqrt{-5}$  is a root of the monic polynomial  $x^2 + 5$ , and  $-1$ , as  $-1$  is a root of  $x + 1$ . An example of an algebraic number that is not an algebraic integer is  $\frac{1}{2}$  as it is a root of  $x - \frac{1}{2}$ , which is not in  $\mathbb{Z}[x]$ , and  $2x - 1$ , which is not monic. Any other polynomial satisfied by  $\frac{1}{2}$  is either not in  $\mathbb{Z}[x]$  or is not monic. It is interesting to point out (but more difficult to show) that  $\pi$  and  $e$  are not algebraic numbers.

**Lemma 6.4.** *Let  $\alpha \in \mathbb{C}$  be algebraic over  $\mathbb{Q}$ . Then there exists a monic irreducible polynomial  $f(x) \in \mathbb{Q}[x]$  such that  $f(\alpha) = 0$  and the degree of  $f$  is minimal among all the nonzero polynomials where  $\alpha$  is a root.*

*Proof.* Let  $I = \{h(x) \in \mathbb{Q}[x] \mid h(\alpha) = 0\}$ . We know that  $I$  is non-empty as  $\alpha$  is a root of some polynomial over  $\mathbb{Q}$  and that  $I$  is an ideal as  $hg(\alpha) = h(\alpha)g(\alpha) = 0 \cdot g(\alpha) = 0$  for all  $g(x) \in \mathbb{Q}[x]$  and  $h(\alpha) - g(\alpha) = 0 - 0 = 0$ . Let  $f(x) \in I$  be a polynomial of minimal degree. Since every nonzero element of  $\mathbb{Q}$  is a unit, we can multiply  $f(x)$



by the reciprocal of the leading coefficient to make it a monic polynomial. We need only show that  $f(x)$  is irreducible. Assume that it is not, i.e.,  $f(x) = r(x)s(x)$  where  $r(x), s(x) \in \mathbb{Q}[x]$  and  $\deg r, \deg s < \deg f$ . Then  $0 = f(\alpha) = r(\alpha)s(\alpha)$  which implies either  $r(\alpha)$  or  $s(\alpha)$  is zero and either  $r(x)$  or  $s(x)$  is in  $I$ . This contradicts the minimality of  $f(x)$  in  $I$ , so  $f$  is irreducible.  $\square$

**Lemma 6.5.** *Let  $\alpha \in \mathbb{C}$  be algebraic over  $\mathbb{Q}$ , let  $f(x) \in \mathbb{Q}[x]$  be the minimal monic irreducible polynomial for  $\alpha$ , and let  $I = \{h(x) \in \mathbb{Q}[x] \mid h(\alpha) = 0\}$ . Then  $I = (f(x))$ .*

*Proof.* It is easy to see that  $(f(x)) \subseteq I$ , since for all  $g(x) \in \mathbb{Q}[x]$ , the product  $f(x)g(x) = 0 \cdot g(x) = 0$ , which implies  $f(x)g(x) \in I$ . To show  $I \subseteq (f(x))$ , let  $h(x) \in I$ . Then there exists  $q(x), r(x) \in \mathbb{Q}[x]$  such that  $h(x) = f(x)q(x) + r(x)$  where  $0 \leq \deg r(x) < \deg f(x)$  by the division algorithm. Substituting  $x = \alpha$ , we see that  $0 = h(\alpha) = f(\alpha)q(\alpha) + r(\alpha) = 0 \cdot q(\alpha) + r(\alpha) = r(\alpha)$ . Therefore,  $r(\alpha) \in I$ , which contradicts the minimality of  $\deg f$  in  $I$  unless  $r(x) = 0$ . Therefore,  $h(x) = f(x)q(x) \in (f(x))$ .  $\square$

**Proposition 6.6.** *If  $\alpha$  is an algebraic number, then  $\mathbb{Q}[\alpha] = \mathbb{Q}(\alpha)$ .*

*Proof.* By definition,  $\mathbb{Q}[\alpha]$  is a ring and  $\mathbb{Q}(\alpha)$  is a field, so it is easy to see that  $\mathbb{Q}[\alpha] \subseteq \mathbb{Q}(\alpha)$ , since  $\mathbb{Q}[\alpha]$  contains  $\mathbb{Q}$  and  $\alpha$ . To show equality, we need only show that  $\mathbb{Q}[\alpha]$  is a field. We will do so by defining a surjective map  $\phi : \mathbb{Q}[x] \rightarrow \mathbb{Q}[\alpha]$  and showing that  $\frac{\mathbb{Q}[x]}{\ker \phi}$  is a field. Let  $\phi : \mathbb{Q}[x] \rightarrow \mathbb{Q}[\alpha]$  be defined by  $\phi(f(x)) = f(\alpha)$ . This map is surjective as any element  $a_0 + a_1\alpha + a_2\alpha^2 + \dots + a_n\alpha^n \in \mathbb{Q}[\alpha]$  is mapped from  $a_0 + a_1x + a_2x^2 + \dots + a_nx^n \in \mathbb{Q}[x]$ . Let  $f$  be the minimal monic irreducible

polynomial for  $\alpha$ . We want to show that  $\ker \phi = (f(x))$ . Of course, by the way we defined  $I$  and by Lemma 6.5,  $\ker \phi = I = (f(x))$ . Now we want to show that  $(f(x))$  is maximal. Suppose there exists  $M$  such that  $(f(x)) \subseteq M \subseteq \mathbb{Q}[x]$  and let  $h(x) \in M \setminus (f(x))$ . Then  $\gcd(f(x), h(x)) = 1$  since  $f(x)$  is irreducible and  $\mathbb{Q}[x]$  is a unique factorization domain. Using the extended Euclidean algorithm in  $\mathbb{Q}[x]$ , there exists  $a(x), b(x)$  such that  $f(x)a(x) + h(x)b(x) = 1 \in M$ . If  $M$  contains 1, it must be the whole ring. Thus,  $M = R$  and  $(f(x))$  is maximal. If  $(f(x))$  is maximal, then  $\frac{\mathbb{Q}[x]}{(f(x))}$  is a field by Proposition 5.10. Since  $\frac{\mathbb{Q}[x]}{(f(x))}$  is isomorphic to  $\mathbb{Q}[\alpha]$ , we have that  $\mathbb{Q}[\alpha]$  is a field and  $\mathbb{Q}[\alpha] = \mathbb{Q}(\alpha)$ .  $\square$

**Definition 6.7.** A number field has the form  $\mathbb{Q}(\alpha)$ , where  $\alpha$  is an algebraic number.

If we want to look at algebraic integers in a number field  $\mathbb{Q}(\alpha)$  (where  $\alpha$  again is an algebraic number), we can look at  $\mathbb{Z}[\alpha]$ . However,  $\mathbb{Z}[\alpha]$  does not always contain all algebraic integers of  $\mathbb{Q}(\alpha)$ . For example, in the ring  $\mathbb{Q}(\sqrt{-3})$ ,  $\frac{-1+\sqrt{-3}}{2}$  is an algebraic integer as it is a root of  $x^2 + x + 1 \in \mathbb{Q}[x]$ ; in fact, the algebraic integers of  $\mathbb{Q}(\sqrt{-3})$  are the elements of  $\mathbb{Z}[\frac{-1+\sqrt{-3}}{2}]$ . In  $\mathbb{Q}(\sqrt{-5})$ , however, the algebraic integers are exactly the set of elements in  $\mathbb{Z}[\sqrt{-5}]$ . In studying the algebraic integers of quadratic number fields (number fields of the form  $\mathbb{Q}(\sqrt{d})$  where  $d \in \mathbb{Z}$  and  $d$  is not a perfect square), we are actually studying *quadratic number rings*.

**Definition 6.8.** For a quadratic number field  $\mathbb{Q}(\sqrt{d})$ , the corresponding quadratic number ring is the set  $\{\alpha \in \mathbb{Q}(\sqrt{d}) \mid \alpha \text{ is an algebraic integer}\}$ .

The corresponding quadratic number ring for  $\mathbb{Q}(\sqrt{d})$  depends on the integer  $d$ ,

as shown in the following proposition.

**Proposition 6.9.** *The number ring corresponding to  $\mathbb{Q}(\sqrt{d})$ , where  $d \in \mathbb{Z}$  is square free, is*

- $\mathbb{Z}[\sqrt{d}]$  if  $d \equiv 2$  or  $3 \pmod{4}$ , and
- $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$  if  $d \equiv 1 \pmod{4}$ .

*Proof.* See page 55 of [SD] for a discussion. □

As we look at various extensions of  $\mathbb{Z}$ , it turns out that unique factorization holds in  $\mathbb{Z}[i]$  and in  $\mathbb{Z}(\sqrt{-2})$ . It fails in  $\mathbb{Z}(\sqrt{-3})$  because  $4 = 2 \cdot 2 = (1 + \sqrt{-3})(1 - \sqrt{-3})$ . However,  $\mathbb{Z}(\sqrt{-3})$  is not a number ring. The corresponding number ring for  $\mathbb{Q}(\sqrt{-3})$  is actually  $\mathbb{Z}\left[\frac{-1+\sqrt{-3}}{2}\right]$ , where unique factorization *does* hold (looking at the factorization of 4 above, we see that  $1 - \sqrt{-3}$  is no longer irreducible). Continuing on, we see that  $\mathbb{Z}(\sqrt{-4})$  is a subset of  $\mathbb{Z}(i)$  and so the next complex extension of  $\mathbb{Z}$  is  $\mathbb{Z}[\sqrt{-5}]$ . We have already stated that unique factorization fails in this ring and the previous proposition shows that it is a number ring. Thus, if we consider  $\mathbb{Z}[\sqrt{-d}]$ , where  $d$  is a positive square free integer,  $d = 5$  gives the first complex quadratic number ring, in which unique factorization fails.

## 6.2 Dedekind domains

We are now ready to take a look at the ideals in  $\mathbb{Z}[\sqrt{-5}]$ . Richard Dedekind studied our ring and its ideals, in particular. In fact,  $\mathbb{Z}[\sqrt{-5}]$  is the quintessential example of what is now known as a Dedekind Domain.

The point of the following sections is to show that unique factorization does hold for ideals in Dedekind domains (and therefore in our ring), but before we get to that, we must define a Dedekind domain.

**Theorem 6.10.** *Let  $R$  be a commutative ring with identity. Then the following conditions are equivalent:*

1.  *$R$  satisfies the ascending chain condition on ideals. That is, every chain of ideals  $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots \subseteq I_k \subseteq \cdots$  must have  $I_n = I_{n+1} = I_{n+2} = \cdots$  for some  $n$ .*
2. *Every ideal of  $R$  is finitely generated.*
3. *Every nonempty set of ideals of  $R$  has a maximal element.*

*Proof.* See [M, Exercise 3.12]. □

**Definition 6.11.** *If any of the conditions of Theorem 6.10 hold for a commutative ring  $R$  with identity, we say that  $R$  is a Noetherian ring.*

Noetherian rings are named after Emmy Noëther, probably the most famous female mathematician.

**Theorem 6.12.** *Let  $R$  be an integral domain. Then the following conditions are equivalent:*

1.  *$R$  satisfies all three of the following properties:*
  - (a)  *$R$  is a Noetherian ring.*

(b) Every nonzero prime ideal of  $R$  is maximal.

(c)  $R$  is integrally closed in its quotient field.

2. Every nonzero ideal of  $R$  can be written uniquely as a product of prime ideals of  $R$ .

*Proof.* See [M, p.130]. □

**Definition 6.13.** *If either of the conditions of the Theorem 6.12 hold for an integral domain  $R$ , we say that  $R$  is a Dedekind domain.*

**Proposition 6.14.** *The ring  $\mathbb{Z}[\sqrt{-5}]$  is a Dedekind domain.*

The proof relies on a substantial amount of background information that we have not developed, so we provide a sketch of the proof below.

*Proof.* (Sketch) We will show  $\mathbb{Z}[\sqrt{-5}]$  satisfies the three properties in condition (1) of Theorem 6.12.

(a) Since a nonzero ideal of  $\mathbb{Z}$  is generated by its smallest positive element, every ideal of  $\mathbb{Z}$  is principal and so  $\mathbb{Z}$  is Noetherian. The Hilbert Basis Theorem guarantees that  $\mathbb{Z}[x]$  is also Noetherian (see pg. 391 of [H]). Consider  $\phi : \mathbb{Z}[x] \rightarrow \mathbb{Z}[\sqrt{-5}]$  defined by  $\phi(f(x)) = f(\sqrt{-5})$ . We see that  $\phi$  is surjective as any element  $a + b\sqrt{-5}$  is the image of  $a + bx$ . Since the homomorphic image of a Noetherian ring is Noetherian,  $\mathbb{Z}[\sqrt{-5}]$  is Noetherian.

(b) Let  $P$  be a nonzero prime ideal. To show that  $P$  is maximal, we will show that  $\mathbb{Z}[\sqrt{-5}]/P$  is a field. Let  $0 \neq \alpha \in P$ . Then  $\alpha\bar{\alpha} = N(\alpha) \in P$ . Thus,

$(N(\alpha)) \subseteq P$  and  $\mathbb{Z}[\sqrt{-5}]/(N(\alpha))$  is finite, so  $\mathbb{Z}[\sqrt{-5}]/P$  is finite as well. By Proposition 5.9,  $\mathbb{Z}[\sqrt{-5}]/P$  is a finite integral domain. Since all finite integral domains are fields, we have that  $P$  is maximal by Proposition 5.10.

(c)  $\mathbb{Z}[\sqrt{-5}]$  is integrally closed in  $\mathbb{Q}(\sqrt{-5})$ . Let  $\alpha \in \mathbb{Q}(\sqrt{-5})$  be integral over  $\mathbb{Z}[\sqrt{-5}]$ . Then  $\alpha$  is integral over  $\mathbb{Z}$  and  $\alpha \in \mathbb{Q}(\sqrt{-5}) \setminus \mathbb{Q}$  implies  $\alpha$  is a root of a monic irreducible polynomial of degree 2 in  $\mathbb{Z}[x]$ . The roots of this polynomial must be  $\alpha$  and  $\bar{\alpha}$ , thus if  $\alpha = a + b\sqrt{-5}$ , then  $a, b \in \mathbb{Z}$ .

□

### 6.3 Unique Factorization for Ideals

We now prove Dedekind's famous theorem that every ideal in a Dedekind domain can be factored uniquely, up to ordering, as a product of prime ideals (Theorem 6.20). The main theorem requires quite a bit of preliminary work, which we now present, borrowing from Chapter 3 (pp. 127-134) of [M].

**Lemma 6.15.** *If  $R$  is a Dedekind Domain and  $I \neq (0)$  is an ideal of  $R$ , then  $I$  contains a product of nonzero prime ideals of  $R$ .*

*Proof.* Let  $S = \{J \mid J \text{ is an ideal of } R \text{ and } J \text{ does not contain a product of nonzero prime ideals}\}$ . If  $S$  is non-empty, then  $S$  has a maximal element since  $R$  is Noetherian by the definition of a Dedekind domain. Say  $M$  is a maximal element in  $S$ . Then  $M$  is not a prime ideal since it would contain a product of primes. Therefore, there

exists  $r, s \in R$  such that  $rs \in M$ , where  $r \notin M$  and  $s \notin M$ . Now,  $M+(r)$  and  $M+(s)$  are ideals strictly larger than  $M$ , thus they are not in  $S$  and must contain products of nonzero prime ideals. Say  $P_1 \cdots P_u \subseteq M+(r)$  and  $Q_1 \cdots Q_v \subseteq M+(s)$ , where  $P_i, Q_j$  are prime ideals of  $R$ . Then  $P_1 \cdots P_u Q_1 \cdots Q_v \subseteq (M+(r))(M+(s)) \subseteq M$ , so  $M$  contains a product of prime ideals, which is a contradiction. Therefore,  $S$  is empty.  $\square$

**Lemma 6.16.** *Let  $R$  be a Dedekind Domain with quotient field  $F$ , and let  $I$  be an ideal of  $R$ , where  $I \neq R$ . Then there exists  $\gamma \in F \setminus R$  such that  $\gamma I \subseteq R$ .*

*Proof.* Let  $0 \neq \alpha \in I$ . Then  $(\alpha)$  contains a product of prime ideals by the above lemma. Let  $r = \min \{s \mid P_1 \cdots P_s \subseteq (\alpha)\}$ , where  $P_1, \dots, P_s$  are nonzero prime ideals. That is, suppose there exist prime ideals  $P_1, P_2, \dots, P_r$  such that  $P_1 \cdots P_r \subseteq (\alpha)$  but no product of  $r-1$  or fewer nonzero prime ideals is in  $(\alpha)$ . Since  $I \neq R$ , the ideal  $I$  is contained in some maximal ideal  $M$ . Then  $P_1 \cdots P_r \subseteq (\alpha) \subseteq I \subseteq M$ . We want to show that  $P_j \subseteq M$  for some  $j$ . Assume the opposite. Then for each  $i$  such that  $1 \leq i \leq r$  there exists  $a_i \in M \setminus P_i$  and  $a_1 \cdots a_r \in P_1 \cdots P_r \subseteq M$  but  $a_i \notin M$  for all  $i$ . This contradicts the fact that  $M$  is a prime ideal. Therefore,  $P_j \subseteq M$  for some  $j$ . Assume  $P_1 \subseteq M$ . Then every nonzero prime ideal of  $R$  is maximal since  $R$  is a Dedekind domain, so  $P_1 = M$ . Therefore,  $P_1 \cdots P_r \subseteq (\alpha) \subseteq I \subseteq P_1$ . Since  $P_2 \cdots P_r \not\subseteq (\alpha)$  by minimality of  $r$ , there exists  $\beta \in P_2 \cdots P_r \setminus (\alpha)$ . Then  $\frac{\beta}{\alpha} = \frac{1}{\alpha} \beta \in \frac{1}{\alpha} (P_2 \cdots P_r) \subseteq F$ , but  $\frac{\beta}{\alpha} \notin R$ ; since that would imply  $\beta = r\alpha \in (\alpha)$  for some  $r \in R$ . Let  $\gamma = \frac{\beta}{\alpha}$ . Now we need only to show  $\gamma I \subseteq R$ . Let  $\delta \in I \subseteq P_1$ . Since

$P_1\beta \subseteq P_1(P_2 \cdots P_r) \subseteq (\alpha)$ ,  $\delta\beta \in P_1\beta \subseteq (\alpha)$ , which means  $\delta\beta = r\alpha$  for some  $r \in R$ .

Then  $\gamma\delta = \frac{\beta}{\alpha}\delta = \frac{r\alpha}{\alpha} \in R$ . Thus  $\gamma I \subseteq R$ . □

**Lemma 6.17.** *Let  $R$  be a Dedekind domain and  $I$  be a nonzero ideal of  $R$ . Then there exists a nonzero ideal  $J$  of  $R$  such that  $IJ$  is a principal ideal.*

*Proof.* Let  $I$  be a nonzero ideal of  $R$  and suppose  $\alpha \in I$ . Define  $J := \{\beta \in R \mid \beta I \subseteq (\alpha)\}$ . Then  $J$  is a nonzero ideal of  $R$  containing  $\alpha$ , and  $IJ \subseteq (\alpha)$ . We want to show  $IJ = (\alpha)$ . Let  $L = \frac{1}{\alpha}IJ = \{\frac{1}{\alpha}(\sum a_i b_i) \mid a_i \in I, b_i \in J\}$ . Then  $L \subseteq R$  since  $IJ \subseteq (\alpha)$ , and  $L$  is an ideal of  $R$ . We want to show  $L = R$ . Assume  $L \subsetneq R$ . Then, by Lemma 6.16, there exists  $\gamma \in F \setminus R$  such that  $\gamma L \subseteq R$ . Note that  $J \subseteq L$  since every  $\beta$  in  $J$  can be written as  $\beta = \frac{1}{\alpha}\alpha\beta \in \frac{1}{\alpha}IJ = L$ . Thus,  $\gamma J \subseteq \gamma L \subseteq R$  and so  $\gamma JI = \gamma(JI) = \gamma((\alpha)L) = (\gamma L)(\alpha) \subseteq R(\alpha) = (\alpha)$ . By the definition of  $J$ ,  $\gamma J \subseteq J$ . Since  $R$  is a Noetherian ring,  $J$  is finitely generated, say  $J = (\beta_1, \dots, \beta_t)$ . Since  $\gamma J \subseteq J$ , there exists  $z_{i,j} \in R$  such that

$$\begin{bmatrix} \gamma\beta_1 \\ \gamma\beta_2 \\ \vdots \\ \gamma\beta_t \end{bmatrix} = \begin{bmatrix} z_{1,1}\beta_1 + z_{1,2}\beta_2 + \dots + z_{1,t}\beta_t \\ z_{2,1}\beta_1 + z_{2,2}\beta_2 + \dots + z_{2,t}\beta_t \\ \vdots \\ z_{t,1}\beta_1 + z_{t,2}\beta_2 + \dots + z_{t,t}\beta_t \end{bmatrix}.$$



So

$$\begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix} = \begin{bmatrix} (z_{1,1} - \gamma)\beta_1 + z_{1,2}\beta_2 + \dots + z_{1,t}\beta_t \\ z_{2,1}\beta_1 + (z_{2,2} - \gamma)\beta_2 + \dots + z_{2,t}\beta_t \\ \vdots \\ z_{t,1}\beta_1 + z_{t,2}\beta_2 + \dots + (z_{t,t} - \gamma)\beta_t \end{bmatrix}.$$

This says  $\begin{bmatrix} \beta_1 \\ \vdots \\ \beta_t \end{bmatrix}$  is a solution to  $A\vec{x} = \vec{0}$  where  $A = [(z_{i,j} - \gamma)I]$  and  $\det A = 0$ . Since, up to a sign,  $\det A$  is a monic polynomial in  $\gamma$  with coefficients in  $R$ ,  $\gamma$  is integral over  $R$ . Therefore, since  $R$  is a Dedekind domain and thus integrally closed,  $\gamma \in R$ . This contradicts the fact that we chose  $\gamma$  so that it was not in  $R$ . Thus  $L = R$  and  $\frac{1}{\alpha}IJ = R$ , which implies  $IJ = (\alpha)$ .  $\square$

**Lemma 6.18.** *Let  $I, J, L$  be ideals in a Dedekind Domain  $R$ . Assume  $I \neq 0$  and  $IJ = IL$ . Then  $J = L$ .*

*Proof.* Let  $I, J, L$  be ideals where  $I \neq 0$  and  $IJ = IL$ . Then by Lemma 6.17, there exists an ideal  $H$  of  $R$  such that  $IH$  is principal. Say  $IH = (\alpha)$ . Then  $JH = LH$  implies  $JIH = LIH$ , which implies  $J(\alpha) = L(\alpha)$ . We need only show that we can cancel the  $(\alpha)$ , i.e., for any element  $\beta \in J$  we can find an element  $\gamma \in L$  such that  $\beta = \gamma$ . Let  $\beta \in J$ . Then  $\beta\alpha \in J(\alpha) = L(\alpha)$ . So for some  $\gamma_i \in L$ , we have  $\beta\alpha = \sum \gamma_i(r_i\alpha) = (\sum r_i\gamma_i)\alpha = \gamma\alpha$  for  $\gamma = \sum r_i\gamma_i \in L$ . Since  $R$  is an integral domain,  $\beta = \gamma$  and thus  $J \subseteq L$ . An analogous argument shows  $L \subseteq J$ , so  $L = J$ .  $\square$

**Lemma 6.19.** *Let  $0 \neq J \subseteq K$  be ideals in a Dedekind domain. There exists an ideal  $I$  such that  $J = KI$ .*

*Proof.* Assume  $J \subseteq K$  and let  $L$  be an ideal such that  $LK$  is principal. Say  $LK = (\alpha)$ . Then  $LJ \subseteq LK = (\alpha)$  and  $\frac{1}{\alpha}LJ$  is an ideal of  $R$ . Let  $I = \frac{1}{\alpha}LJ$ . We see that  $IK = \frac{1}{\alpha}LJK = \frac{1}{\alpha}(LK)J = \frac{1}{\alpha}(\alpha)J = J$ .  $\square$

**Theorem 6.20.** *Every proper nonzero ideal in a Dedekind Domain  $R$  can be uniquely written as a product of prime ideals.*

*Proof.* We must show both the existence and the uniqueness. We will begin with the existence. Let  $S = \{I \mid I \neq 0, I \neq R, I \neq P_1^{a_1} \cdots P_k^{a_k}\}$ . That is, the set  $S$  is the set of all nonzero proper ideals that can not be written as a product of prime ideals. If  $S$  is not the empty set, then  $S$  has a maximal element  $J$ , since  $R$  is Noetherian by the definition of Dedekind domain. Since  $J \neq R$ , the ideal  $J$  is contained in some maximal ideal  $M$ . By Lemma 6.19, there exists an ideal  $I$  such that  $MI = J$  and so  $J = MI \subseteq I$ . If  $J = I$ , then  $MI = I$  and  $M = R$  by Lemma 6.18, which is a contradiction. So,  $J \subsetneq I$ . By the maximality of  $J$  in  $S$ , we have  $I = P_1^{a_1} \cdots P_k^{a_k}$ . So  $J = MI$  is a product of prime ideals, too. This contradicts the fact that  $J \in S$ , so  $S$  is empty.

Now, we must show uniqueness. Suppose  $P_1 \cdots P_r = Q_1 \cdots Q_s$  for prime ideals  $P_i, Q_i$ . Then  $Q_1 \cdots Q_s \subseteq P_1$  which implies  $Q_k \subseteq P_1$  for some  $j = 1, \dots, s$ . Let  $j = 1$ . Since every prime ideal is maximal by Theorem 6.12,  $P_1 = Q_1$ . By Lemma 6.18, we have  $P_2 \cdots P_r = Q_2 \cdots Q_s$  and by induction,  $r = s$  and  $P_i = Q_i$  for all  $i$ .  $\square$

## 7 Conclusions

In studying the ring  $\mathbb{Z}[\sqrt{-5}]$ , we established many results about its elements and its ideals. For elements, we established the following five very powerful conditions for reducibility, namely, an element  $a + b\sqrt{-5}$  is reducible when at least one of the following conditions is satisfied:

- One of  $a - b\sqrt{-5}$ ,  $-a + b\sqrt{-5}$ , or  $-a - b\sqrt{-5}$  is reducible.
- $\gcd(a, b) > 1$ .
- $a$  is a multiple of 5.
- $a$  is congruent to  $\pm b \pmod{6}$  where  $a \neq b$ .
- $a$  is congruent to  $\pm 2b \pmod{9}$  and  $a^2 + 5b^2 > 9$ .

We designed a computer algorithm to determine reducibility for elements that do not fall into any of the above five cases. Finally, we explained how often and how badly unique factorization fails for elements of  $\mathbb{Z}[\sqrt{-5}]$ . We have also studied reducibility for ideals, in particular for ideals generated by integers. We have proved exactly what happens to ideals generated by rational primes in our ring. We also glanced at the work of Richard Dedekind, who had the insight to take our ring and develop a whole theory that described it and other rings. Dedekind's work explains exactly why unique factorization holds for ideals.

Although we generated several powerful results for the ring  $\mathbb{Z}[\sqrt{-5}]$ , there is still much to be done. Even though it gives us a definite answer, our naïve algorithm is

not very efficient. In Chapter 4, we compared irreducibles in our ring to primes in the set of integers, however, we did not reach any conclusive results. So we wonder if there is a good approximation for the number of irreducible elements. What occurs after norm 10,000? Throughout our study, we did not go beyond that norm. We conjecture that similar patterns hold for the number of irreducibles and how badly unique factorization holds, but are these assumptions true?

In all of the above, we have studied and discovered many interesting properties of the ring  $\mathbb{Z}[\sqrt{-5}]$ . Perhaps the most interesting is the simple fact that unique factorization fails for elements but holds for ideals. This division creates an interesting dichotomy between elements and ideals, particularly being that ideals are, in some sense, a generalization of elements of the ring.

## 8 Appendix A

The following is the Maple code for the algorithm described in Chapter 4.

We begin by creating a list of possible elements with norm  $< 10001$ . Entries of the list will look like  $[\text{norm}, i, j]$  for an element  $i + j\sqrt{-5}$ .

```
> S:=[]:
> n:=10000:
> for i from 0 to floor(sqrt(n)) do
>   for j from 0 to floor(sqrt(n/5)) while i^2 + 5*j^2 < n+1 do
>     S := [op(S), [expand(i^2+5*j^2), i, j]];
>   od;
> od;
```

Next, we sort our list in ascending order of norms.

```
> prec := (x,y) -> evalb(op(1,x) < op(1,y));
> S:= sort(S,prec):
```

Now, we want to check irreducibility. To do this, we first make a list of every norm that divides any particular norm. The following function returns all possible factors for a given norm. Note that we start at  $k = 2$  because the  $S[1]$  element is the identity element 1.

```
> getpossiblefactors := proc(n)
> local k,
> T;
> T:=[];
> k:=2;
> while k < nops(S) do
>   if modp(n,S[k][1]) = 0 and n <> S[k][1] then
>     T := [op(T),S[k]]
>     fi;
>     k:=k+1;
```

```

> od:
> return(T);
> end:

```

Now that we have a function to give all factors for a norm, we need a list of all norms, so that we can make our database of all factors for all norms.

```

> listofnorms := {};
> for i from 1 to nops(S) do
>   listofnorms:=listofnorms union {S[i][1]}:
> od:
> listofnorms:

```

Finally, we define the function  $L[n]$ , our database of factors for a given norm.

When we input a norm  $n$ , Maple will output all factors of that norm.

```

> L := 'L':
> i := 2:
> n := listofnorms[i]:
> while n < listofnorms[nops(listofnorms)] do
>   L[n] := getpossiblefactors(n):
>   i := i+1:
>   n := listofnorms[i]:
> od:
> L[n] := getpossiblefactors(n):

```

To make a list a irreducible elements, we first make a list of all reducible elements.

To do so, we take care of the easy cases (those found in Propositions 3.12 and 3.13),

then we will perform step 3 of our algorithm (Chapter 4).

```

> R:={}:
> for k from 1 to nops(S) do
>   for i from 1 to nops(L[S[k][1]])
>   do for j from i to nops(L[S[k][1]]) do
>   R := R union {'if'(gcd(S[k][2],S[k][3])>1 and
>   S[k][2]<>0 and S[k][3]<>0,
>   S[k],
>   'if'(S[k][2] mod 5=0,

```

```

>         'if'(S[k][2]>0,
>         S[k],
>         'if'(S[k][3]>1,
>         S[k],
>         NULL)),
> 'if'(S[k][2] = (L[S[k][1]][i][2])*(L[S[k][1]][j][2]) -
> 5*(L[S[k][1]][i][3])*(L[S[k][1]][j][3]) and S[k][3] =
> (L[S[k][1]][i][2])*(L[S[k][1]][j][3]) +
> (L[S[k][1]][i][3])*(L[S[k][1]][j][2])),
>         S[k],
> 'if'(S[k][2] = (L[S[k][1]][i][2])*(L[S[k][1]][j][2]) -
> 5*(-L[S[k][1]][i][3])*(L[S[k][1]][j][3]) and S[k][3] =
> (L[S[k][1]][i][2])*(-L[S[k][1]][j][3]) +
> (L[S[k][1]][i][3])*(L[S[k][1]][j][2])),
>         S[k],
> 'if'(S[k][2] = (L[S[k][1]][i][2])*(-L[S[k][1]][j][2]) -
> 5*(L[S[k][1]][i][3])*(L[S[k][1]][j][3]) and S[k][3] =
> (L[S[k][1]][i][2])*(L[S[k][1]][j][3]) +
> (L[S[k][1]][i][3])*(-L[S[k][1]][j][2])),
>         S[k],
> 'if'(S[k][2] = (L[S[k][1]][i][2])*(L[S[k][1]][j][2]) -
> 5*(-L[S[k][1]][i][3])*(L[S[k][1]][j][3]) and S[k][3] =
> (L[S[k][1]][i][2])*(L[S[k][1]][j][3]) +
> (-L[S[k][1]][i][3])*(L[S[k][1]][j][2])),
>         S[k],
> 'if'(S[k][2] = (-L[S[k][1]][i][2])*(L[S[k][1]][j][2]) -
> 5*(L[S[k][1]][i][3])*(L[S[k][1]][j][3]) and S[k][3] =
> (-L[S[k][1]][i][2])*(L[S[k][1]][j][3]) +
> (L[S[k][1]][i][3])*(L[S[k][1]][j][2])),
>         S[k],
> 'if'(S[k][2] = (L[S[k][1]][i][2])*(-L[S[k][1]][j][2]) -
> 5*(-L[S[k][1]][i][3])*(-L[S[k][1]][j][3]) and S[k][3] =
> (L[S[k][1]][i][2])*(-L[S[k][1]][j][3]) +
> (L[S[k][1]][i][3])*(-L[S[k][1]][j][2])),
>         S[k],
> 'if'(S[k][2] = (L[S[k][1]][i][2])*(L[S[k][1]][j][2]) -
> 5*(-L[S[k][1]][i][3])*(-L[S[k][1]][j][3]) and S[k][3] =
> (L[S[k][1]][i][2])*(-L[S[k][1]][j][3]) +
> (-L[S[k][1]][i][3])*(L[S[k][1]][j][2])),
>         S[k],
> 'if'(S[k][2] = (-L[S[k][1]][i][2])*(L[S[k][1]][j][2]) -
> 5*(L[S[k][1]][i][3])*(-L[S[k][1]][j][3]) and S[k][3] =
> (-L[S[k][1]][i][2])*(-L[S[k][1]][j][3]) +
> (-L[S[k][1]][i][3])*(-L[S[k][1]][j][2])),
>         S[k],
> 'if'(S[k][2] = (-L[S[k][1]][i][2])*(L[S[k][1]][j][2]) -
> 5*(L[S[k][1]][i][3])*(-L[S[k][1]][j][3]) and S[k][3] =
> (-L[S[k][1]][i][2])*(-L[S[k][1]][j][3]) +

```

```

> (L[S[k][1]][i][3])*(L[S[k][1]][j][2]),
> S[k],
> NULL))))))))))}};od;od;od;
> R:= R minus {[0,0,0]}:
> R:= convert(R,list):
> R:= sort(R,prec);

```

Now that we have a list of all reducible elements, we can simply subtract it from our list  $S$  of all elements. Notice that we must also subtract the elements 0 and 1 from our list, as they are neither reducible nor irreducible. Of course, all of our calculations thus far have only looked at elements in the first quadrant of the complex plane. We want the first half the complex plane. So, we will consider each element  $a + b\sqrt{-5}$ . If  $b \neq 0$ , we will add  $a - b\sqrt{-5}$  to our list.

```

> SS:={}:
> S:= convert(S,set):
> for i from 1 to nops(S) do
> SS:= SS union {'if'(S[i][3]<>0,
> S[i][1],S[i][2],-S[i][3]], NULL)}: od:
> S:=S union SS:
> RR:={}:
> R:= convert(R,set):
> for i from 1 to nops(R)do
> RR:= RR union {'if'(R[i][3]<>0,
> R[i][1],R[i][2],-R[i][3]], NULL)}: od:
> R:= R union RR:
> IR:= S minus R:
> IR:= IR minus {[0,0,0]}:
> IR:= IR minus {[1,1,0]}:
> IR:= convert(IR,list):
> IR:= sort(IR,prec);
> S:= convert(S,list):
> S:= sort(S,prec):
> R:= convert(R,list):
> R:= sort(R,prec):

```



## 9 Appendix B

The following table describes all elements up to norm 100.

<i>Norm</i>	<i>Irreducibles</i>	<i>Reducibles</i>
4	2	
5	$\sqrt{-5}$	
6	$1 + \sqrt{-5}$	
9	$3, 2 + \sqrt{-5}$	
14	$3 + \sqrt{-5}$	
16		4
20		$2\sqrt{-5}$
21	$1 + 2\sqrt{-5}, 4 + \sqrt{-5}$	
24		$2 + 2\sqrt{-5}$
25		5
29	$3 + 2\sqrt{-5}$	
30		$5 + \sqrt{-5}$
36		$6, 4 + 2\sqrt{-5}$
41	$6 + \sqrt{-5}$	
45		$3\sqrt{-5}, 5 + 2\sqrt{-5}$
46	$1 + 3\sqrt{-5}$	
49	$7, 2 + 3\sqrt{-5}$	
51		$3 + 3\sqrt{-5}$
54		$7 + \sqrt{-5}$
56		$6 + 2\sqrt{-5}$
61	$4 + 3\sqrt{-5}$	
64		8
69	$8 + \sqrt{-5}, 7 + 2\sqrt{-5}$	
70		$5 + 3\sqrt{-5}$
80		$4\sqrt{-5}$
81		$9, 6 + 3\sqrt{-5}, 1 + 4\sqrt{-5}$
84		$8 + 2\sqrt{-5}, 2 + 4\sqrt{-5}$
86	$9 + \sqrt{-5}$	
89	$3 + 4\sqrt{-5}$	
94	$7 + 3\sqrt{-5}$	
96		$4 + 4\sqrt{-5}$
100		10

## 10 Appendix C

The following is a list of all elements with more than one factorization up to norm 1,000. The elements are grouped by the number of factors per factorization.

Elements with two factors per factorization:

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

$$9 = (3)(3) = (2 + \sqrt{-5})(2 - \sqrt{-5})$$

$$12 + 3\sqrt{-5} = (3)(4 + \sqrt{-5}) = (2 - \sqrt{-5})(1 + 2\sqrt{-5})$$

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

$$14 = (2)(7) = (3 + \sqrt{-5})(3 - \sqrt{-5})$$

$$4 + 6\sqrt{-5} = (2)(2 + 3\sqrt{-5}) = (3 + \sqrt{-5})(3 + \sqrt{-5})$$

$$16 + 2\sqrt{-5} = (2)(8 + \sqrt{-5}) = (1 - \sqrt{-5})(1 + 3\sqrt{-5})$$

$$7 + 7\sqrt{-5} = (7)(1 + \sqrt{-5}) = (3 + \sqrt{-5})(4 + \sqrt{-5})$$

$$17 + 5\sqrt{-5} = (1 + \sqrt{-5})(7 - 2\sqrt{-5}) = (2 - \sqrt{-5})(1 + 3\sqrt{-5})$$

$$3 + 9\sqrt{-5} = (1 + \sqrt{-5})(8 + \sqrt{-5}) = (3)(1 + 3\sqrt{-5})$$

$$21 = (3)(7) = (4 - \sqrt{-5})(4 + \sqrt{-5}) = (1 - 2\sqrt{-5})(1 + 2\sqrt{-5})$$

$$14 + 7\sqrt{-5} = (2 + \sqrt{-5})(7) = (4 - \sqrt{-5})(1 + 2\sqrt{-5})$$

$$4 + 10\sqrt{-5} = (2)(2 + 5\sqrt{-5}) = (1 + \sqrt{-5})(9 + \sqrt{-5})$$

$$22 + 4\sqrt{-5} = (2)(11 + 2\sqrt{-5}) = (1 + \sqrt{-5})(7 - 3\sqrt{-5})$$

$$18 + 8\sqrt{-5} = (2)(9 + 4\sqrt{-5}) = (3 - \sqrt{-5})(1 + 3\sqrt{-5})$$

$$21 + 7\sqrt{-5} = (3 + \sqrt{-5})(7) = (3 - \sqrt{-5})(2 + 3\sqrt{-5})$$

$$27 + 3\sqrt{-5} = (1 + \sqrt{-5})(7 - 4\sqrt{-5}) = (1 - \sqrt{-5})(2 + 5\sqrt{-5}) = (3)(9 + \sqrt{-5})$$

$$28 + 2\sqrt{-5} = (2)(14 + \sqrt{-5}) = (1 - \sqrt{-5})(3 + 5\sqrt{-5})$$

$$29 + \sqrt{-5} = (1 - \sqrt{-5})(4 + 5\sqrt{-5}) = (2 + \sqrt{-5})(7 - 3\sqrt{-5})$$

$$21 + 9\sqrt{-5} = (1 + \sqrt{-5})(11 - 2\sqrt{-5}) = (3)(7 + 3\sqrt{-5})$$

$$19 + 11\sqrt{-5} = (3 + \sqrt{-5})(8 + \sqrt{-5}) = (4 - \sqrt{-5})(1 + 3\sqrt{-5})$$

$$31 + \sqrt{-5} = (1 + \sqrt{-5})(6 - 5\sqrt{-5}) = (3 + \sqrt{-5})(7 - 2\sqrt{-5}) = (1 - 2\sqrt{-5})(1 + 3\sqrt{-5})$$

$$26 + 8\sqrt{-5} = (2)(13 + 4\sqrt{-5}) = (1 + \sqrt{-5})(11 - 3\sqrt{-5})$$

Elements with 3 factors per factorization:

$$12 = (2)(2)(3) = (2)(1 - \sqrt{-5})(1 + \sqrt{-5})$$

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

$$18 = (2)(3)(3) = (2)(2 - \sqrt{-5})(2 + \sqrt{-5}) = (1 - \sqrt{-5})(1 + \sqrt{-5})(3)$$

$$12 + 6\sqrt{-5} = (2)(3)(2 + \sqrt{-5}) = (1 - \sqrt{-5})(1 + \sqrt{-5})(2 + \sqrt{-5})$$

$$20 + 2\sqrt{-5} = (2)(\sqrt{-5})(1 - 2\sqrt{-5}) = (-\sqrt{-5})(1 + \sqrt{-5})(3 + \sqrt{-5})$$

$$18 + 6\sqrt{-5} = (2)(3)(3 + \sqrt{-5}) = (1 - \sqrt{-5})(1 + \sqrt{-5})(3 + \sqrt{-5})$$

$$15 + 9\sqrt{-5} = (-\sqrt{-5})(1 + \sqrt{-5})(1 + 2\sqrt{-5}) = (\sqrt{-5})(3)(3 - \sqrt{-5})$$

$$25 + \sqrt{-5} = (-\sqrt{-5})(1 + \sqrt{-5})(4 + \sqrt{-5}) = (\sqrt{-5})(2 - \sqrt{-5})(3 - \sqrt{-5})$$

$$18 + 9\sqrt{-5} = (3)(3)(3 + \sqrt{-5}) = (2 - \sqrt{-5})(2 + \sqrt{-5})(2 + \sqrt{-5})$$

$$27 = (3)(3)(3) = (3)(2 - \sqrt{-5})(2 + \sqrt{-5})$$

$$6 + 12\sqrt{-5} = (2)(3)(1 + 2\sqrt{-5}) = (2)(2 + \sqrt{-5})(4 + \sqrt{-5}) = (1 - \sqrt{-5})(1 + \sqrt{-5})(1 + 2\sqrt{-5})$$

$$24 + 6\sqrt{-5} = (2)(3)(4 + \sqrt{-5}) = (2)(2 - \sqrt{-5})(1 + \sqrt{-5}) = (1 - \sqrt{-5})(1 + \sqrt{-5})(4 + \sqrt{-5})$$

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

$$28 = (2)(2)(7) = (2)(3 - \sqrt{-5})(3 + \sqrt{-5})$$

$$8 + 12\sqrt{-5} = (2)(2)(2 + 3\sqrt{-5}) = (2)(3 + \sqrt{-5})(3 + \sqrt{-5})$$

$$15 + 12\sqrt{-5} = (\sqrt{-5})(3)(41\sqrt{-5}) = (\sqrt{-5})(2 + \sqrt{-5})(1 - 2\sqrt{-5})$$

$$30 + 3\sqrt{-5} = (\sqrt{-5})(3)(1 - 2\sqrt{-5}) = (\sqrt{-5})(2 - \sqrt{-5})(4 - \sqrt{-5})$$

$$30 + 4\sqrt{-5} = (2)(\sqrt{-5}) = (2 - 3\sqrt{-5}) = (\sqrt{-5})(3 - \sqrt{-5})(3 + \sqrt{-5})$$

Elements with 4 factors per factorization:

$$24 = (2)(2)(2)(3) = (2)(2)(1 + \sqrt{-5})(1 - \sqrt{-5})$$

$$12 + 12\sqrt{-5} = (2)(2)(3)(1 + \sqrt{-5}) = (2)(1 - \sqrt{-5})(1 + \sqrt{-5})(1 + \sqrt{-5})$$

$$30 = (2)(3)(-\sqrt{-5})(\sqrt{-5}) = (-\sqrt{-5})(\sqrt{-5})(1 + \sqrt{-5})(1 - \sqrt{-5})$$

$$20 + 10\sqrt{-5} = (2)(-\sqrt{-5})(\sqrt{-5})(2 + \sqrt{-5}) = (\sqrt{-5})(\sqrt{-5})(1 - \sqrt{-5})(1 - \sqrt{-5})$$

## References

- [A] Tom M. Apostol, *Introduction to Analytic Number Theory*, Springer-Verlag, 1976.
- [D] Richard Dedekind, *Theory of Algebraic Integers*, translated by John Stillwell, Cambridge University Press, 1996.
- [G] Joseph A. Gallian, *Contemporary Abstract Algebra*, Fifth Edition, Houghton Mifflin Company, 2002.
- [HJ] Jeff Holt and John Jones, *Discovering Number Theory*, W.H. Freeman and Company, 2001.
- [H] Thomas W. Hungerford, *Algebra*, Springer-Verlag, 1974.
- [M] Richard A. Mollin, *Algebraic Number Theory*, Chapman and Hall/CRC, 1999.
- [SD] H.P.F. Swinnerton-Dyer, *A Brief Guide to Algebraic Number Theory*, Cambridge University Press, 2001.