NUMBER RINGS AND DEDEKIND DOMAINS

by

Mary C. Harrison

A thesis submitted to the faculty of
The University of North Carolina at Charlotte
in partial fulfillment of the requirements
for the degree of Master of Science in
Mathematics

Charlotte

2019

Approved by:

_____

Dr. Evan Houston

_____

Dr. Gabor Hetyei

_____

Dr. Kevin McGoff

ABSTRACT

MARY C. HARRISON. Number rings and dedekind domains. (Under the direction of DR. EVAN HOUSTON)

In this paper, we study number rings and their factorization properties. We begin with an introduction to number fields and number rings. Then we consider the ring $\mathbb{Z}[i]$, which is a unique factorization domain, where each element factors uniquely into a product of prime elements. We classify all irreducible elements in this ring. Then we consider an example of non-unique factorization in the ring $\mathbb{Z}[\sqrt{-5}]$, which is not a unique factorization domain. Then we introduce the idea of a Dedekind domain. The main discussion of the paper is to prove that number rings are Dedekind domains, then to prove that in a Dedekind domain, every ideal factors uniquely into a product of prime ideals. Then we consider an example of a ring that is not a Dedekind domain, and we find an example of non-unique prime ideal factorization. Finally, we conclude by proving how the primes split in the quadratic fields.

TABLE OF CONTENTS

CHAPTER 1: INTRODUCTION

Definition 1. *A number field is a subfield of* $\mathbb{C}$ *having finite degree over* $\mathbb{Q}$.

We know that every number field has the form $\mathbb{Q}[\alpha]$ for some $\alpha \in \mathbb{C}$, where α is the root of some polynomial over $\mathbb{Q}$ [3, Theorem 2, Appendix 2]. If we suppose α is the root of some *irreducible* polynomial f of degree n, then $\mathbb{Q}[\alpha]$ is naturally a vector space over $\mathbb{Q}$ with basis $1, \alpha, \ldots, \alpha^{n-1}$, since $0 = f(\alpha) = a_n\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_1\alpha + a_0$, thus α^n (and any higher powers) can be written as a linear combination of the basis vectors. Hence every element in the number field $\mathbb{Q}[\alpha]$ can be expressed as

$$a_0 + a_1\alpha + ... + a_{n-1}\alpha^{n-1}$$

where each $a_i \in \mathbb{Q}$.

Quadratic fields are the number fields having the form $\mathbb{Q}[\sqrt{m}]$, where m is a square-free integer. When $m > 0$, we call $\mathbb{Q}[\sqrt{m}]$ a real quadratic field, and if $m < 0$, we call it an imaginary quadratic field. Another type of number field is a cyclotomic field. These are the fields of the form $\mathbb{Q}[\omega]$, where $\omega = e^{2\pi i/m}$. $\mathbb{Q}[\omega]$ is called the m^{th} cyclotomic field.

These number fields all contain a ring, called a number ring, having a unique factorization property. This ring consists of the algebraic integers in the field. Note that for the purposes of this paper, all rings considered will be commutative rings with unity.

In the following chapter, we introduce the notion of an algebraic integer and a number ring. We will study some properties of these and as an example, we will find all the algebraic integers in the quadratic fields. Then, we will define embedding, trace, norm, and discriminant, and prove some results about them. These results will be useful for proving theorems in Chapter 5.

In Chapter 3 we study an example of a specific quadratic number ring, $\mathbb{Z}[i]$, that is a unique factorization domain. This means every element factors uniquely into a product of irreducible elements. Eventually, we want to discuss the factorization properties of general number rings, which do not always have the same factorization properties as $\mathbb{Z}[i]$.

Chapter 4 gives an example of a ring, $\mathbb{Z}[\sqrt{-5}]$, that does not have the same factorization properties as $\mathbb{Z}[i]$, because we can find an example of elements that do not factor uniquely into irreducible elements.

In Chapter 5 we have the main discussion of the paper. Armed with many definitions and preliminary results, we will prove that number rings satisfy the three qualifications of a Dedekind domain: they are Noetherian, integerally closed, and every nonzero prime ideal is maximal. Then we will show that in a Dedekind domain, every ideal factors uniquely into a product of prime ideals. This done, we can refer back to Chapter 4 and see that the ring discussed there, although factorization into irreducible elements may not be unique, factorization of ideals into products of prime ideals is always possible and unique.

In Chapter 6 we look at an example of a ring that is not a Dedekind domain, $\mathbb{Z}[\sqrt{-3}]$ therefore we can find an example of an ideal that cannot be factored uniquely into prime ideals.

Finally, in Chapter 7 we consider the "splitting" of primes in quadratic fields. In particular, we will describe how each extension of an ideal of $\mathbb{Z}$ factors into prime ideals in a quadratic number ring.

CHAPTER 2: NUMBER RINGS

Definition 2. *A complex number is an algebraic integer if it is the root of some monic (with leading coefficient* 1*) polynomial having coefficients in* $\mathbb{Z}$*. It is true, as we will see in this section, that every algebraic integer is the root of some monic irreducible polynomial with coefficients in* $\mathbb{Z}$*. If* α *is an algebraic integer, we say* α *is integral over* $\mathbb{Z}$*.*

The following will allow us to prove that every algebraic integer is the root of a monic irreducible polynomial with coefficients in $\mathbb{Z}$.

Definition 3. *An element* $f(x) \in \mathbb{Z}[x]$ *is said the be primitive if the greatest common divisor of its coefficients is 1.*

Lemma 4. *(Gauss) If* $f(x), g(x) \in \mathbb{Z}[x]$ *are primitive, then so is* $f(x)g(x)$*.*

Proof. Let $f(x)$ and $g(x)$ be primitive, and let $h(x) = f(x)g(x)$ and suppose to the contrary that some prime p divides the coefficients of $h(x)$. Reducing coefficients modulo p, we have $0 = \overline{h(x)} = \overline{f(x)} \cdot \overline{g(x)}$. Now, since the ring $\mathbb{Z}_p[x]$ has no zero divisors, we must have either $\overline{f(x)}$ or $\overline{g(x)}$ is the zero polynomial. That is, p divides the coefficients of $f(x)$ or $g(x)$, contradicting the assumption that both are primitive. So $h(x)$ must also be primitive. □

Lemma 5. *Let* $f(x) \in \mathbb{Z}[x]$*. If* $f(x)$ *is irreducible in* $\mathbb{Z}[x]$*, then it is also irreducible in* $\mathbb{Q}[x]$*.*

Proof. Since $f(x)$ is irreducible in $\mathbb{Z}[x]$, then it is primitive. Suppose to the contrary that $f(x) = g(x)h(x)$, where $g(x), h(x) \in \mathbb{Q}[x]$. Choose positive integers a, b such that $ag(x), bh(x) \in \mathbb{Z}[x]$. Then choose positive integers c, d such that $\frac{a}{c}g(x), \frac{b}{d}h(x)$ are primitive in $\mathbb{Z}[x]$. Then $\frac{ab}{cd}f(x) = \frac{a}{c}g(x) \cdot \frac{b}{d}h(x)$, and by lemma 4, $\frac{ab}{cd}f(x)$ is

primitive in $\mathbb{Z}[x]$, so $\frac{ab}{cd}$ must equal 1. Thus we have $f(x) = \frac{a}{c}g(x) \cdot \frac{b}{d}h(x)$. Since $f(x)$ is irreducible in $\mathbb{Z}[x]$, we must have either $\frac{a}{c}g(x) = 1$ or $\frac{b}{d}h(x) = 1$. That is, either $f(x)$ or $g(x)$ is a constant polynomial in $\mathbb{Q}[x]$. Thus $f(x)$ is irreducible in $\mathbb{Q}[x]$. □

Theorem 6. *Let α be an algebraic integer. The monic irreducible polynomial over $\mathbb{Q}$ having α as a root lies in $\mathbb{Z}[x]$.*

Proof. Let $f(x) \in \mathbb{Z}[x]$ be a monic polynomial of minimum degree having α as a root. Since $f(x)$ is monic, it is also primitive. Now if $f(x)$ is reducible in $\mathbb{Z}[x]$, then since it is primitive, we would have a factorization $f(x) = g(x)h(x)$, where $g(x)$ and $h(x)$ have smaller degree than $f(x)$. Then α is a root of $g(x)$ or $h(x)$, contradicting that $f(x)$ is of minimum degree. Thus $f(x)$ is irreducible in $\mathbb{Z}[x]$. Now by Lemma 5, $f(x)$ is also irreducible in $\mathbb{Q}[x]$, and thus $f(x)$ is the minimum polynomial of α. □

Now we can use the preceding theorem to classify all the algebraic integers in a quadratic field.

Theorem 7. *Let $m \in \mathbb{Z}$ be square-free. The set of algebraic integers in $\mathbb{Q}[\sqrt{m}]$ is*

$$\{a + b\sqrt{m} : a, b \in \mathbb{Z}\} \text{ if } m \equiv 2 \text{ or } 3 (mod\ 4)$$

$$\{\frac{a + b\sqrt{m}}{2} : a, b \in \mathbb{Z}, a \equiv b (mod\ 2)\} \text{ if } m \equiv 1 (mod\ 4)$$

Proof. Let $\alpha = r + s\sqrt{m}$ be an algebraic integer with $r, s \in \mathbb{Q}$ First, note that

$$x^2 - 2rx + r^2 - ms^2 \tag{2.1}$$

is the monic irreducible polynomial of α. Indeed, any polynomial of smaller degree would not have rational coefficients, and any monic polynomial of degree 2 having α as a root must be the same as (2.1). So by Theorem 6, we must have $2r, r^2 - ms^2 \in \mathbb{Z}$. Since we know $r, s \in \mathbb{Q}$, we can write $s = \frac{a}{c}$, where $a, c \in \mathbb{Z}$ are coprime.

First, note that since $2r \in \mathbb{Z}$, we have $(2r)^2 = 4r^2 \in \mathbb{Z}$. Then since $r^2 - ms^2 \in \mathbb{Z}$, we also have $4r^2 - 4ms^2 \in \mathbb{Z}$, thus $4ms^2 \in \mathbb{Z}$. We will proceed by considering two cases.

Case 1: Suppose c is odd. If $c > 1$, then $c \nmid 4$ so $c^2 \nmid 4$. Also $c^2 \nmid m$ since m is

square-free, but we may have $c \mid m$. Then $4ms^2 \in \mathbb{Z} \implies \frac{4ma^2}{c^2} \in \mathbb{Z} \implies c^2 \mid 4ma^2$. Since neither c nor c^2 divide 4, we have $c^2 \mid ma^2$ and since $c^2 \nmid m$, we either have $c^2 \mid a^2$ or $c \mid a^2$. In either case, since a and c are coprime, and $c > 1$ we have a contradiction, so $c = \pm 1$. Then $s \in \mathbb{Z}$. Now, since $r^2 - ms^2 \in \mathbb{Z}$ and $ms^2 \in \mathbb{Z}$, then $r^2 \in \mathbb{Z} \implies r \in \mathbb{Z}$.

Case 2: Suppose c is even. Then $c = 2k$ for some integer k. Again, since $4ms^2 \in \mathbb{Z}$, we have $\frac{4ma^2}{4k^2} \in \mathbb{Z}$, which implies that $4k^2 \mid 4ma^2$. Then since m is squarefree, we must have $k \mid a$, say $a = jk$ for some integer j. Then $s = \frac{a}{c} = \frac{jk}{2k} = \frac{j}{2}$. Switching notation, we get $s = \frac{a}{2}$. Now, since $2r$ is an integer, then either $r \in \mathbb{Z}$ or $r = \frac{b}{2}$ for some integer b. Since $r^2 - m\frac{a^2}{4} \in \mathbb{Z}$ and m is squarefree, this implies that $r^2 \notin \mathbb{Z}$, so $r \notin \mathbb{Z}$. Then $r = \frac{b}{2}$ for some integer b.

So there are only two cases. If $s \in \mathbb{Z}$ then $r \in \mathbb{Z}$. This case, as we will see shortly, occurs only when $m \equiv 2$ or $3 (\text{mod } 4)$. Otherwise, $s = \frac{a}{2}$ and $r = \frac{b}{2}$. Then we have $4r^2 - 4ms^2 \equiv 0 (mod\ 4) \implies b^2 \equiv ma^2 (\text{mod } 4)$. And since every square is congruent to 0 or 1 modulo 4, and since $b \neq 0$, we have $m \equiv 1 (\text{mod } 4)$. On the other hand, if $m \equiv 1 (\text{mod } 4)$, then if $s = \frac{a}{2}$ and $r = \frac{b}{2}$ for odd integers a, b, then for $r + s\sqrt{m}$ to be integral over $\mathbb{Z}$, from equation (1), we need only show that $r^2 - ms^2 \in \mathbb{Z}$. To that end, observe that $r^2 - ms^2 = \frac{b^2 - ma^2}{4}$, and since $m \equiv 1 (\text{mod } 4)$, we have $b^2 - ma^2 \equiv b^2 - a^2 \equiv 1 - 1 = 0 (\text{mod } 4)$, since a, b are odd, so their squares are congruent to 1 modulo 4. So $4 \mid b^2 - ma^2$. Finally we have $r^2 - ms^2 = \frac{b^2 - ma^2}{4} \in \mathbb{Z}$, thus $r + s\sqrt{m}$ is integral over $\mathbb{Z}$. This completes the proof. □

Theorem 8. *The following are equivalent for $\alpha \in \mathbb{C}$:*

(1) *α is an algebraic integer.*

(2) *The additive group of the ring $\mathbb{Z}[\alpha]$ is finitely generated.*

(3) *α is a member of some subring of $\mathbb{C}$ having finitely generated additive group.*

(4) *$\alpha A \subseteq A$ for some finitely generated additive subgroup $A \subseteq \mathbb{C}$.*

This is Theorem 2 in *Number Fields* by Daniel A. Marcus [3].

Corollary 9. *If α and β are algebraic integers, then so are $\alpha + \beta$ and $\alpha\beta$.*

Proof. We know by (2) that the additive groups of $\mathbb{Z}[\alpha]$ and $\mathbb{Z}[\beta]$ are finitely generated. Then so is the additive group of $\mathbb{Z}[\alpha, \beta]$. Finally, since $\mathbb{Z}[\alpha, \beta]$ contains $\alpha + \beta$ and $\alpha\beta$, by (3), this implies that they are algebraic integers. □

Definition 10. *Let $\mathbb{A}$ denote the set of all algebraic integers, that is, the complex numbers that satisfy a monic polynomial over $\mathbb{Z}$. Then the intersection of $\mathbb{A}$ with any given number field K is called the number ring corresponding to the number field K.*

Corollary 9 shows that this intersection $\mathbb{A} \cap K$ is truly a ring. Later, as the main discussion of this paper, we will show that these number rings have special factorization properties.

Theorem 11. *Let K be a number field of degree n over $\mathbb{Q}$. Then there are exactly n embeddings (1-1 homomorphisms) of K into $\mathbb{C}$* [3].

Definition 12. *Let K be a number field with degree n over $\mathbb{Q}$. By the previous theorem, we know there are n embeddings of K into $\mathbb{C}$, say $\sigma_1, \ldots, \sigma_n$. For $\alpha \in K$, we define the trace of α relative to K by $Tr_K(\alpha) = \sigma_1(\alpha) + \ldots + \sigma_n(\alpha)$. We define the norm of α relative to K to be $N_K(\alpha) = \sigma_1(\alpha) \cdot \ldots \cdot \sigma_n(\alpha)$.*

Note that the norm function is multiplicative, which follows easily from the definition.

Example 13. In the quadratic field $\mathbb{Q}[i]$, we know there are exactly two embeddings of $\mathbb{Q}[i]$ into $\mathbb{C}$. We have

$$\sigma_1(a + bi) = a + bi$$

$$\sigma_2(a + bi) = a - bi$$

It is easy to see that these are both 1-1 homomorphisms, so these are the embeddings of $\mathbb{Q}[i]$ into $\mathbb{C}$. Then we can calculate trace and norm of any element in $\mathbb{Q}[i]$.

$Tr_K(a + bi) = \sigma_1(a + bi) + \sigma_2(a + bi) = (a + bi) + (a - bi) = 2a$, and

$N_K(a + bi) = \sigma_1(a + bi) \cdot \sigma_2(a + bi) = (a + bi)(a - bi) = a^2 + b^2$.

The following lemma gives us a property of norm that will be needed to prove a result in the next chapter.

Lemma 14. *$\alpha \in \mathbb{Z}[i]$ is a unit $\Leftrightarrow N(\alpha) = 1$.*

Proof. Suppose $\alpha = a + bi$ is a unit. Then there exists $\beta \in \mathbb{Z}[i]$ such that $\alpha\beta = 1$. Now, we have $N(\alpha)N(\beta) = N(1) = 1$, so $N(\alpha)$ must be a unit in $\mathbb{Z}$. This implies $N(\alpha) = 1$ since norm is positive and 1 and -1 are the only units in $\mathbb{Z}$. For the other direction, suppose $N(\alpha) = 1$. Then $1 = N(\alpha) = a^2 + b^2$, where $a, b \in \mathbb{Z}$. This implies $a = \pm 1$ and $b = 0$ or $a = 0$ and $b = \pm 1$. In the first case, $\alpha = \pm 1$, which is a unit in $\mathbb{Z}[i]$. In the second case, $\alpha = \pm i$, which is also a unit in $\mathbb{Z}[i]$. So α is a unit $\Leftrightarrow$ $N(\alpha) = 1$. □

Definition 15. *Let K be a number field and let $(\alpha_1, ..., \alpha_n)$ be an n-tuple of elements in K. Let A be the $n \times n$ matrix whose i, j^{th} entry is $Tr_K(\alpha_i\alpha_j)$. Then the discriminant of $(\alpha_1, ..., \alpha_n)$ (with respect to K) is defined by $disc(\alpha_1, ..., \alpha_n) = det(A)$.*

Theorem 16. *With the notation from the definition above, let B by the $n \times n$ matrix whose i, j^{th} entry is $\sigma_i(\alpha_j)$. Then $disc(\alpha_1, ...\alpha_n) = det(B)^2$.*

Proof. It can be verified that $B^tB = A$, where A is as in the definition above. Then $\det(B)^2 = \det(B)\det(B) = \det(B^t)\det(B) = \det(B^tB) = \det(A) = \text{disc}(\alpha_1, ...\alpha_n)$. □

CHAPTER 3: CLASSIFICATION OF ALL IRREDUCIBLE ELEMENTS IN $\mathbb{Z}[i]$

Definition 17. *A domain D is called a unique factorization domain (UFD), if each element of D factors uniquely into a product of irreducible elements.*

Definition 18. *An integral domain D is called a Euclidian domain if there is a function d from the nonzero elements of D to the nonnegative integers such that:*
(1) *$d(a) \leq d(ab)$ for all nonzero $a, b \in D$*
(2) *If $a, b \in D$, $b \neq 0$, then there exist elements $q, r \in D$ such that $a = bq + r$, where $r = 0$ or $d(r) < d(b)$.*

Lemma 19. [2, Corollary to Theorem 18.4] *Every Euclidian domain is a UFD.*

Theorem 20. *$\mathbb{Z}[i]$ is a UFD.*

Proof. In Gallian's *Contemporary Abstract Algebra*, Example 7 in Chapter 18 tells us that $\mathbb{Z}[i]$ is a Euclidian domain, therefore, by the preceding lemma, it is a UFD. □

Since $\mathbb{Z}[i]$ is a UFD, we can express every element of $\mathbb{Z}[i]$ as a unique product of irreducible elements. In this section, we will fully classify these irreducible elements in $\mathbb{Z}[i]$. At this point, we can discuss a corollary of Theorem 20 that will be useful for classifying the irreducible elements in $\mathbb{Z}[i]$.

Corollary 21. *Every prime $p \equiv 1 (mod\ 4)$ is a sum of two squares.*

Proof. Let $p \equiv 1 (\text{mod } 4)$. Then $p = 4k + 1$ for some $k \in \mathbb{Z}$. Since $\mathbb{Z}_p^*$ is a cyclic group under multiplication, we can find a generator, say $a \in \mathbb{Z}_p$. Then each element $1, 2, ..., p-1 \in \mathbb{Z}_p$ is congruent to one of $a^1, a^2, ..., a^{p-1}$ modulo p, in no particular order [1, Corollary to Theorem 8.6]. So we have

$$\begin{aligned}(p-1)! &= (p-1)(p-2)...(2)(1) \\ &\equiv a^1 a^2 ... a^{p-1}\end{aligned}$$

$$= a^{\frac{1}{2}(p-1)p}$$

$$= a^{\frac{1}{2}(4k)(4k+1)}$$

$$= (a^{4k^2+k})^2$$

Now, by Wilson's Theorem [1, Theorem 5.4], $(p-1)! \equiv -1 (\text{mod } p)$, so we have $-1 \equiv (a^{4k^2+k})^2 (\text{mod } p)$. To simplify notation, we will say $-1 \equiv n^2 (\text{mod } p)$ for some integer n.

Now, we will show that p cannot be irreducible in $\mathbb{Z}[i]$. To this end, first we will show that irreducible elements in a UFD are also prime. Let p be some irreducible element, and suppose $p \mid ab$ for some a, b. Then $ab = pk$ for some k. Then let $a = a_1 a_2 ... a_n$, $b = b_1 b_2 ... b_m$, $k = k_1 k_2 ... k_j$, where a_i, b_i, k_i are all irreducible for every i. Then

$$p(k_1 k_2 ... k_j) = (a_1 a_2 ... a_n)(b_1 b_2 ... b_m)$$

Since factorization into irreducible elements is unique, and every element in the equation is irreducible, we must have $p = a_i$ for some i or $p = b_i$ for some i. Then $p \mid a$ or $p \mid b$, which implies that p is prime. So irreducible elements in a UFD are prime.

Now suppose to the contrary that p is irreducible in $\mathbb{Z}[i]$. Then p is prime in $\mathbb{Z}[i]$. Since $p \mid n^2 + 1$ from above, we have $p \mid (n+i)(n-i)$, and since p is prime, we have $p \mid n+i$ or $p \mid n-i$. If $p \mid n+i$, then $n+i = p(a+bi)$ for some $a+bi \in \mathbb{Z}[i]$. Then $n + i = ap + bpi \implies bp = 1$, which implies that p is a unit, a contradiction. A similar contradiction results if $p \mid n-i$. Either way there is a contradiction, so we must have that p is reducible in $\mathbb{Z}[i]$.

Finally, since p is reducible in $\mathbb{Z}[i]$, we can write $p = (a+bi)(c+di)$ where $a+bi$ and $c+di$ are not units. Taking the norm of this equation, we have $p^2 = (a^2+b^2)(c^2+d^2)$ which implies that $p = a^2 + b^2 = c^2 + d^2$. So p is the sum of two squares. □

Lemma 22. *If $N(\alpha) = p$, where p is prime, then α is irreducible.*

Proof. Let $N(\alpha) = p$, where p is prime, and suppose to the contrary that α is reducible

in $\mathbb{Z}[i]$. Then $\alpha = \beta\gamma$, where β and γ are both non-units. Then $N(\alpha) = N(\beta\gamma) = N(\beta)N(\gamma)$. Now from lemma 14 we have $N(x) = 1 \Leftrightarrow x$ is a unit, so $N(\beta) \neq 1$ and $N(\gamma) \neq 1$. Then β and γ both have norm greater than 1 $\implies$ $N(\alpha)$ is not prime, a contradiction. So α must be irreducible. □

Lemma 23. *If $N(\alpha) = p^2$, where p is a prime in $\mathbb{Z}$ such that $p \equiv 3(mod\ 4)$, then α is irreducible in $\mathbb{Z}[i]$.*

Proof. Suppose $\alpha = \beta\gamma$. We want to show either β or γ is a unit. Since $p^2 = N(\alpha) = N(\beta)N(\gamma)$, then either $N(\beta) = p$ and $N(\gamma) = p$ or one of $N(\beta)$, $N(\gamma)$ is p^2 and the other is 1. In the second case, either β or γ is a unit, and we're done. Consider the first case. Set $\beta = c + di$, so we have $p = N(\beta) = c^2 + d^2$. But $p \equiv 3(\text{mod } 4)$, and this kind of prime cannot be expressed as the sum of two squares [1, Theorem 13.2 (Fermat)]. So we have a contradiction. Therefore either β or γ is a unit and α is irreducible. □

Equipped with the preceding theorem and lemmas, we can now prove the main result of this section.

Theorem 24. *The irreducibles in $\mathbb{Z}[i]$ are the elements of the form*
$\alpha = p$, where p is prime in $\mathbb{Z}$ and $p \equiv 3(mod\ 4)$
$\alpha = pi$, where p is prime in $\mathbb{Z}$ and $p \equiv 3(mod\ 4)$
$\alpha = a + bi$, where $a \neq 0$, $b \neq 0$, and $N(a + bi) = a^2 + b^2 = p$, where p is prime.

Proof. Consider $\alpha = a + bi$. First, suppose $b = 0$. Then $\alpha = a$. If a is not prime, then clearly it is reducible. Suppose a is prime. First, if $a = 2$ then $2 = (1 + i)(1 - i)$, so α is reducible. If $a \neq 2$, then either a either has the form $4k + 1$ or $4k + 3$. If a has the form $4k + 3$, then $N(\alpha) = a^2$ and where a is prime and $a \equiv 3(\text{mod } 4)$. So by Lemma 23, $a = \alpha$ is irreducible. If a has the form $4k + 1$ by Corollary 21 we know that it can be written as the sum of two nonzero squares, say $a = x^2 + y^2$. Then $(x + yi)(x - yi) = x^2 + y^2 = a = \alpha$. So α is reducible.

Now, suppose $a = 0$. Then $\alpha = bi$. If b is not prime, then clearly it is reducible,

and therefore α is reducible. Suppose b is prime. Then, as above, b either has the form $4k+1$ or $4k+3$. If b has the form $4k+3$, $N(\alpha) = b^2$, where b is prime and $b \equiv 3 (\text{mod } 4)$. So by Lemma 23, $bi = \alpha$ is irreducible. If b has the form $4k+1$, then as above, $b = x^2 + y^2$ for nonzero x and y, so $(x+yi)(y+xi) = x^2 i + y^2 i = bi = \alpha$, so α is reducible.

Finally, suppose $a \neq 0$ and $b \neq 0$, and $gcd(a,b) = 1$ (otherwise α is clearly reducible). If $N(\alpha) = a^2 + b^2 = p$, then α is irreducible by Lemma 22. Now, suppose $\alpha = a + bi$ is irreducible, and suppose for contradiction that $N(\alpha) = pq$, where p and q are primes. Note that

$$N(\alpha) = a^2 + b^2 = (a+bi)(a-bi) = pq$$

Now, since $\mathbb{Z}[i]$ is a PID and $a+bi$ is irreducible, it is also prime. Then $a+bi$ divides either p or q. Say $a+bi \mid p$. Then $(a+bi)(c+di) = p \implies p = (ac-bd) + (ad+bc)i$, which gives us equations

$$ac - bd = p \tag{3.1}$$

$$ad + bc = 0 \tag{3.2}$$

Solving (3.2) for d and plugging into (3.1), we have $ac + \frac{b^2 c}{a} = p$. Multiplying by $\frac{a}{c}$ yields $a^2 + b^2 = \frac{pa}{c}$. We also have $a^2 + b^2 = pq$, so $pq = \frac{pa}{c} \implies q = \frac{a}{c} \implies c = \frac{a}{q}$. Similarly, solving (3.2) for c and plugging into (3.1) gives $-\frac{a^2 d}{b} - bd = p$. Multiplying by $\frac{b}{d}$ gives $-a^2 - b^2 = \frac{pb}{d}$, and since $a^2 + b^2 = pq$, we have $pq = -\frac{pb}{d} \implies q = -\frac{b}{d} \implies d = -\frac{b}{q}$.

Then we have $p = (a+bi)(c+di) = (a+bi)(\frac{a}{q} - \frac{b}{q}i)$, but $gcd(a,b) = 1 \implies q = 1$. So $N(\alpha) = pq = p$.

Thus $\alpha = a + bi$ is irreducible $\Leftrightarrow N(\alpha) = p$. $\square$

CHAPTER 4: EXAMPLE OF NON-UNIQUE FACTORIZATION

Not all rings have the same unique factorization properties that $\mathbb{Z}[i]$ has. In this ring, factorization into irreducible elements is unique since it is a UFD. There are, however, rings in which we can find examples of factorization into irreducible elements that is not necessarily unique. We will discuss one such example here.

In the ring $\mathbb{Z}[\sqrt{-5}]$, we have

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

Now, to show that this is truly an example of non-unique factorization, we must show that $2, 3, 1 + \sqrt{-5}$, and $1 - \sqrt{-5}$ are not associates of each other, which is clear, and that they are irreducible in $\mathbb{Z}[\sqrt{-5}]$. Then we have found an example of non-unique factorization into irreducible elements. To that end, we will first consider two lemmas.

Lemma 25. *If $\beta \mid \alpha$ in $\mathbb{Z}[\sqrt{-5}]$ then $N(\beta) \mid N(\alpha)$.*

Proof. Since $\beta \mid \alpha$, there is some $\gamma \in \mathbb{Z}[\sqrt{-5}]$ such that $\alpha = \beta\gamma$. Now, since norm is multiplicative, we have $N(\alpha) = N(\beta\gamma) = N(\beta)N(\gamma)$. Thus $N(\beta) \mid N(\gamma)$. □

Lemma 26. *There are no elements with norm 2 or 3 in $\mathbb{Z}[\sqrt{-5}]$.*

Proof. If we suppose there is an element whose norm is 2, then $N(a + b\sqrt{-5}) = a^2 + 5b^2 = 2$. If $b \geq 1$ then $a^2 + 5b^2 \geq 5$, so b must be 0. Then we have $a^2 = 2$, but there is no such integer a. So there is no element of norm 2.

Similarly, if we have an element with norm 3, then $b = 0$, and $a^2 = 3$, and again, there is no such a. So there are no elements of norm 2 or 3 in $\mathbb{Z}[\sqrt{-5}]$. □

Now, we have $N(2) = 4$, $N(3) = 9$, $N(1 + \sqrt{-5}) = 6$, and $N(1 - \sqrt{-5}) = 6$. If any of these elements is reducible, then it has a factor whose norm is either 2 or 3,

since 2 and 3 are the only factors of 4, 9 and 6. But by Lemma 26, there are no such elements. So 2, 3, $1 + \sqrt{-5}$, and $1 - \sqrt{-5}$ are irreducible in $\mathbb{Z}[\sqrt{-5}]$, and we have found an example of non-unique factorization.

CHAPTER 5: DEDEKIND DOMAINS

We turn now to the main discussion of this paper: that number rings, although they are not necessarily UFDs, do have special factorization properties that we will discuss here. We begin with some definitions.

Definition 27. *The set of algebraic integers in a subfield K of $\mathbb{C}$ is called the integral closure of $\mathbb{Z}$ in K. A ring R is said to be integrally closed in its quotient field S if no element of $S \setminus R$ satisfies a monic polynomial with coefficients in $\mathbb{Z}$.*

Example 28. Take for example $R = \mathbb{Z}[\sqrt{-3}]$. This ring has quotient field $\mathbb{Q}[\sqrt{-3}]$. We know from Theorem 7 that this field contains algebraic integers that are not in $\mathbb{Z}[\sqrt{-3}]$. For example, $\alpha = \frac{1+\sqrt{-3}}{2}$ is integral over $\mathbb{Z}$. Indeed, if $f(x) = x^2 - x + 1$, then

$$\begin{aligned} f(\alpha) &= f\left(\frac{1+\sqrt{-3}}{2}\right) \\ &= \left(\frac{1+\sqrt{-3}}{2}\right)^2 - \left(\frac{1+\sqrt{-3}}{2}\right) + 1 \\ &= \frac{1}{4} + \frac{1}{2}\sqrt{-3} - \frac{3}{4} - \frac{1}{2} - \frac{1}{2}\sqrt{-3} + 1 = 0 \end{aligned}$$

Thus the ring $\mathbb{Z}[\sqrt{-3}]$ is not integrally closed.

Theorem 29. *If K is a number field, then the ring R of algebraic integers in K has quotient field K.*

Proof. Since K is a field, we know the quotient field of R is contained in K. To show K is contained in the quotient field of R, let $\alpha \in K$ be algebraic over $\mathbb{Q}$. We want to show that α is in the quotient field of R. We have the equation

$$\alpha^n + a_{n-1}\alpha^{n-1} + ... + a_1\alpha + a_0 = 0 \tag{5.1}$$

with each $a_i \in \mathbb{Q}$. Choose $b \in \mathbb{Z}$ such that $ba_i \in \mathbb{Z}$ for every i. Multiply (5.1) by b^n to

get $(b\alpha)^n + ba_{n-1}(b\alpha)^{n-1} + ... + b^{n-1}a_1(b\alpha) + b^n a_0 = 0$. This shows that $b\alpha$ is integral over $\mathbb{Z}$. Then we must have $b\alpha = r \in R$, so $\alpha = r/b$ is in the quotient field of R. $\square$

Definition 30. *A prime ideal of an integral domain is an ideal I having the property that if $a, b \in R$ and $ab \in I$, then either $a \in I$ or $b \in I$.*

Example 31. In $\mathbb{Z}$, the prime ideals are the ideals that are generated by the prime elements in $\mathbb{Z}$.

Let $I = (p)$ be the ideal in the integers generated by the prime p. We know that if $ab \in I$, then we must have $ab = pk$ for some $k \in \mathbb{Z}$. We know by Euclid's Lemma that if a prime divides a product elements, then it must divide one of the elements, so either $p \mid a$, which implies $a \in I$ or $p \mid b$ which implies $b \in I$.

Any other ideal in the integers cannot be prime, because if it is generated by an element that is not prime, say $I = (pq)$, where p and q are non-units, then the element pq is in I, but neither p nor q is in I.

Definition 32. *A ring is said to be Noetherian if it satisfies the ascending chain condition for ideals. That is, if we have $I_1 \subseteq I_2 \subseteq \ldots I_k \subseteq I_{k+1} \subseteq \ldots$, then there must be some n such that $I_n = I_{n+1} = \ldots$*

It is well known that a ring R is Noetherian if and only if every ideal of R is finitely generated. This equivalent definition will be useful for our purposes.

Definition 33. *A Dedekind domain is an integral domain that is Noetherian, integrally closed, and having the property that every nonzero prime ideal is maximal.*

Since our goal is to show that every number ring is a Dedekind domain, we need to show that every number ring satisfies the three conditions listed above. The following lemmas and theorems deal with these conditions. First we'll need some framework for the proofs.

Definition 34. *Let R be a domain. An R-module is a set M, equipped with the binary operation $+$ on M and scalar mulitiplication $R \times M \to M$ such that*

(1) *M is an abelian group under $+$*

(2) *$(r+s)m = rm + sm$ for each $r, s \in R$ and $m \in M$*

(3) *$r(m+n) = rm + rn$ for each $r \in R$ and $m, n \in M$*

(4) *$(rs)m = r(sm)$ for each $r, s \in R$ and $m \in M$*

(5) *$1m = m$ for each $m \in M$*

Definition 35. *An R-module is said to be Noetherian if it satisfies the ascending chain condition on submodules. That is, every strictly increasing sequence of submodules eventually terminates. Equivalently, an R-module is Noetherian if every submodule is finitely generated.*

Lemma 36. *Let R be a Noetherian domain, and let M be a cyclic R-module (that is, $M = R\alpha$ for some $\alpha \in M$). Then M is a Noetherian R-module.*

Proof. Let N be a submodule of M. We will show that N is finitely generated. Write $M = R\alpha$ and let $I = \{x \in R : x\alpha \in N\}$. Then I is and ideal of R, and since R is Noetherian, I is finitely generated, say $I = (a_1, ...a_n)$ with $a_i \in R$. Now let $\beta \in N$. Then since $\beta \in M$ also, we have $\beta = r\alpha$ for some $r \in R$. Then $r \in I$, so $r = r_1a_1 + ... + r_na_n$ with $r_i \in R$. Finally, $\beta = r\alpha = r_1a_1\alpha + ... + r_na_n\alpha$, so N is finitely generated (by $a_1\alpha, \dots a_n\alpha$) as desired. □

Lemma 37. *Let M be a Noetherian R-module and let N be a submodule. Then N is a Noetherian R-module as well.*

Proof. A submodule of N is automatically a submodule of M, so it is finitely generated, and N is therefore Noetherian. □

Definition 38. *Let M be an R-module, and let N be a submodule. Then, since M is an abelian group under addition, we can form the quotient group M/N. This is naturally an R-module ($r(\alpha + N) = r\alpha + N$ for $r \in R, \alpha \in M$), called the quotient module of M with respect to N.*

Lemma 39. *Let M be an R-module. If M has a submodule N such that N and M/N are Noetherian, then M is Noetherian.*

Proof. Let L be a sumbodule of M. To show M is Noetherian, we need to show that L is finitely generated. Note that $L \cap N$ is finitely generated since N is Noetherian. Now, claim $L/(L \cap N) \cong (L+N)/N$. Granting this, since $(L+N)/N$ is a sumbodule of M/N, $L/(L \cap N)$ is finitely generated. Write $L/(L \cap N) = R(\alpha_1 + L \cap N) + \ldots + R(\alpha_r + L \cap N)$ and $L \cap N = R\alpha_{r+1} + \ldots + R\alpha_n$. Let $\beta \in L$, then $\beta + L \cap N = a_1(\alpha_1 + L \cap N) + \ldots + a_r(\alpha_r + L \cap N)$ for $a_i \in R$, that is,

$$\beta = a_1\alpha_1 + \ldots + a_r\alpha_r + \gamma$$

for some $\gamma \in L \cap N$. But γ may be written as a linear combination of $\alpha_{r+1}, \ldots, \alpha_n$, so β is a linear combination of $\alpha_1, \ldots, \alpha_n$ and thus L is finitely generated.

To prove the claim, define $h : L \to (L + N)/N$ by $h(l) = l + N$. Then this mapping is well-defined since $f, g \in L$ such that $f = g$ implies that $f + N = g + N$. Now, clearly, if $l \in L \cap N$ then $l \in N$ so $l \in ker(h)$. Now let $l \in ker(h)$. Then $h(l) = 0 + N$ which implies that $l \in N$. So $ker(h) = L \cap N$ and the claim follows from the First Isomorphism Theorem [2, Theorem 10.3]. □

Lemma 40. *Let R be a Noetherian domain, and let M be a finitely generated R-module. Then M is a Noetherian R-module.*

Proof. If M is generated by a single element, then by Lemma 36, M is Noetherian. Now we will induct on n, the number of generators of M. Suppose the result holds for $n - 1$. Then let $M = \sum_{i=1}^{n} R\alpha_i$. Again, we know that $R\alpha_1$ is Noetherian by Lemma 36. Also the quotient module $M/R\alpha_1$ can be generated by $n-1$ elements, so by our induction assumption, this module is also Noetherian. Then, by Lemma 39, M is Noetherian. □

Theorem 41. *Every number ring is a Noetherian ring.*

Proof. Let R denote the ring of algebraic integers in a number field K. To show that R is Noetherian, we want to show that every ideal is finitely generated.

First we will show that R is a Noetherian $\mathbb{Z}$-module. Then, since ideals of R are simply R-submodules of R, they are also $\mathbb{Z}$-submodules of R, so they are finitely generated by the definition of Noetherian.

To show R is Noetherian, we will show that R is itself a finitely generated $\mathbb{Z}$-module. Then by Lemma 40, since $\mathbb{Z}$ is Noetherian, R is Noetherian as a finitely generated $\mathbb{Z}$-module.

To show that R is finitely generated, we will show that it is a submodule of some finitely generated $\mathbb{Z}$-module. Then clearly R must also be finitely generated. For this, take $\{\alpha_1, ..., \alpha_n\}$ to be a vector space basis for K over $\mathbb{Q}$. By Theorem 29, K is the quotient field of R, so there exists some $a \in R$ such that $a\alpha_i \in R$ for every i. Then $\{a\alpha_1, ..., a\alpha_n\}$ is also a basis for K over $\mathbb{Q}$, and we can change notation and assume that the α_i are in R.

Now take some $\alpha \in R$, and express it as $\alpha = c_1\alpha_1 + ... + c_n\alpha_n$, for $c_i \in \mathbb{Q}$. Let $d = disc(\alpha_1, ..., \alpha_n)$. We claim that $dc_i \in \mathbb{Z}$ for every i. Granting this claim, we have

$$\alpha = (dc_1)(\frac{\alpha_1}{d}) + ... + (dc_n)(\frac{\alpha_n}{d})$$

putting α in the finitely generated $\mathbb{Z}$-module $\mathbb{Z}(\frac{\alpha_1}{d}) + ... + \mathbb{Z}(\frac{\alpha_n}{d})$, completing the proof.

We turn now to the claim. Let $\sigma_1, ..., \sigma_n$ be the embeddings of K into $\mathbb{C}$. Apply each σ_i to $\alpha = c_1\alpha_1 + ... + c_n\alpha_n$. Then for $1 \leq j \leq n$ we have the equation $\sigma_j(\alpha) = c_1\sigma_j(\alpha_1) + ... + c_n\sigma_j(\alpha_n)$. Using Cramer's Rule to solve for c_j yields $c_j = \frac{d_j}{e}$, where e is the determinant of the matrix A whose i, j^{th} entry is $\sigma_i(\alpha_j)$ and d_j is the determinant of the matrix formed from A by replacing the j^{th} column of A by $\sigma_i(\alpha)$. By theorem 16, $e^2 = d$. Now e and d_j are in R. Moreover, $dc_j = d_j e \implies dc_j \in R$. On the other hand, $dc_j \in \mathbb{Q}$, and we therefore have $dc_j \in \mathbb{Z}$ (since $\mathbb{Z}$ is integrally closed in $\mathbb{Q}$). This proves the claim. □

Theorem 42. *Let R be the ring of integers in the number field K. Then R is integrally closed.*

Proof. We know from Theorem 29 that R has K as its field of fractions. Let some

element $\alpha \in K$ be integral over R. Then we have

$$\alpha^n + a_{n-1}\alpha^{n-1} + ... + a_1\alpha + a_0 = 0 \tag{5.2}$$

for $a_i \in R$. Let M be the ring $\mathbb{Z}[a_0, a_1, ..., a_{n-1}, \alpha]$, that is, the smallest subring of $\mathbb{C}$ containing all the elements $a_0, a_1, ..., a_{n-1}, \alpha$. Since M is a ring and $\alpha \in M$, we have $\alpha M \subseteq M$. If we show that M is a finitely generated $\mathbb{Z}$-module, then we have that α is integral over $\mathbb{Z}$ by Theorem 8, from which we have $\alpha \in R$, completing the proof.

Now we will show that M is a finitely generated $\mathbb{Z}$-module. Since $a_0 \in R$, it is an algebraic integer, so we have the equation

$$b_0 + b_1a_0 + b_2a_0^2 + ... + b_{k_0-1}a_0^{k_0-1} + a_0^{k_0} = 0 \tag{5.3}$$

Let A be the $\mathbb{Z}$-module $\mathbb{Z} + \mathbb{Z}a_0 + \mathbb{Z}a_0^2 + ... + \mathbb{Z}a_0^{k_0-1}$. Equation (5.3) shows that $a_0^{k_0} \in A$. Multiply everything by a_0 to get

$$a_0b_0 + b_1a_0^2 + b_2a_0^3 + ... + b_{k_0-1}a_0^{k_0} + a_0^{k_0+1} = 0$$

which shows that $a_0^{k_0+1} \in A$. Continuing this process, we see that A contains all positive powers of a_0, thus $A = \mathbb{Z}[a_0]$, so $\mathbb{Z}[a_0]$ is finitely generated by $1, a_0, ..., a_0^{k_0-1}$. We can apply this same arguments to any a_i, so $\mathbb{Z}[a_i]$ is finitely generated, and it follows that $\mathbb{Z}[a_0, a_1, ..., a_{n-1}]$ is finitely generated, generated by the products $a_0^{i_0}a_1^{i_1}...a_{n-1}^{i_n-1}$ for $0 \leq i_j < k_j$ for every j. Now we can use equation (5.2) to show M is finitely generated by products $a_0^{i_0}a_1^{i_1}...a_{n-1}^{i_n-1}\alpha^i$ for $0 \leq i_j < k_j$ and $0 \leq i < n$. □

Theorem 43. *Every number ring R is a Dedekind domain.*

Proof. By Theorem 41, we have that R is Noetherian. By Theorem 42 we also have that R is integrally closed. Finally, we need to show that every nonzero prime ideal in R is maximal. To do this, suppose P is a nonzero prime ideal of R.

Take some $\alpha \in P$, $\alpha \neq 0$. Then we have an equation of integrality

$$\alpha^n + a_{n-1}\alpha^{n-1} + ... + a_1\alpha + a_0 = 0$$

Thus $a_0 \in P$ and $a_0 \in \mathbb{Z}$. So $P \cap \mathbb{Z} \neq \{0\}$. Then $P \cap \mathbb{Z}$ must be prime, because if it isn't, then P isn't prime. Prime ideals in $\mathbb{Z}$ must be principal and maximal, say $P \cap \mathbb{Z} = (p)$. Suppose for contradiction that P is not maximal. Then $P \subsetneq I$ for some

ideal $I \subsetneq R$. Note that since $(p) \subset P$ and all prime ideals are maximal in $\mathbb{Z}$, we must have $I \cap \mathbb{Z} = (p)$. Now choose some element $r \in I \setminus P$. Write the integral equation

$$a_n r^n + a_{n-1} r^{n-1} + ... + a_1 r + a_0 = 0$$

From this we have $-a_0 = a_n r^n + a_{n-1} r^{n-1} + ... + a_1 r \in I$ and we know $a_0 \in \mathbb{Z}$ so $a_0 \in (p) \subset P$. Thus $a_0 \in P \implies a_n r^n + a_{n-1} r^{n-1} + ... + a_1 r \in P$. Now, factoring out r we have $a_n r^n + a_{n-1} r^{n-1} + ... + a_1 r = r(a_n r^{n-1} + a_{n-1} r^{n-2} + ... + a_1)$. Now, since we know $r \notin P$, we must have $a_n r^{n-1} + a_{n-1} r^{n-2} + ... + a_1 \in P$. This implies $a_1 \in P$. Continue. Eventually from this process we obtain $r \in P$, a contradiction. So P must be maximal. Thus we have that R is a Dedekind domain. □

Now that we have established that number rings are Dedekind domains, we will discuss the significance of that fact. As shown in Chapter 3, we know that not every number ring is a unique factorization domain. But now, since we know number rings are Dedekind domains, we can look at their special factorization properties.

Definition 44. *Let R be a domain with quotient field K, and I a nonzero ideal of R. Set $I^{-1} = \{x \in K : xI \subseteq R\}$. Then I^{-1} is called the inverse of I. I is said to be invertible if $II^{-1} = R$.*

Theorem 45. *In a Dedekind domain R, every ideal factors uniquely into a product of prime ideals.*

Proof. We will start by showing that for every ideal I there exist prime ideals $P_1, P_2, ..., P_k$ such that $I \subseteq P_i$ for every i and $P_1 \cdot ... \cdot P_k \subseteq I$. Suppose not. Then, using the fact that R is Noetherian, choose an ideal J that is maximal among the ideals for which there are no such prime ideals. In particular, J cannot be prime, so we can find some $a, b \in R \setminus J$ such that $ab \in J$. Then the ideals (J, a) and (J, b) are strictly bigger than J. So, since J was a maximal offender, there exist $P_1, P_2, ..., P_r$ and $Q_1, Q_2, ..., Q_s$ such that $(J, a) \subseteq P_i$ for every i, $(J, b) \subseteq Q_i$ for every i, $P_1 \cdot ... \cdot P_r \subseteq (J, a)$ and $Q_1 \cdot ... \cdot Q_s \subseteq (J, b)$. But then clearly we also have $J \subseteq P_i$ and $J \subseteq Q_i$ and $P_1 \cdot ... \cdot P_r \cdot Q_1 \cdot ... \cdot Q_s \subseteq (J, a)(J, b) \subseteq J$, contradicting that J was

an offender.

Now, we claim that each maximal ideal is invertible. Let P be a maximal ideal, $a \in P$, $a \neq 0$. Using what we proved above, there exist prime ideals $P_1, ..., P_k$ with $a \in P_i$ for every i and $P_1 \cdot ... \cdot P_k \subseteq (a) \subseteq P$. Suppose k is minimal. Then $P_i \subseteq P$ for some i, say $i = 1$. Then $P_2 \cdot ... \cdot P_k \not\subseteq (a)$ since k is minimal, and $a^{-1}P_2 \cdot ... \cdot P_k \not\subseteq R$. But $a^{-1}P_2 \cdot ... \cdot P_k \cdot P \subseteq R$, so that $a^{-1}P_2 \cdot ... \cdot P_k \subseteq P^{-1} \setminus R$. That is, $R \subsetneq P^{-1}$. Now, because $R \subseteq P^{-1}$, we have $P \subseteq PP^{-1}$. If $PP^{-1} \neq R$, then PP^{-1} must be in some maximal ideal, for which P is the only candidate. So $PP^{-1} \subseteq P$ which implies $P = PP^{-1}$. By theorem 8 this implies that P^{-1} is integral over R, contradicting that R is integrally closed. So $PP^{-1} = R$, and thus P is invertible.

Now we claim that every nonzero ideal is the product of prime ideals. Suppose not. Then let I be maximal among the ideals that cannot be expressed as a product of primes. Then I itself clearly isn't prime, so find some maximal prime ideal P such that $I \subset P$. Consider IP^{-1}. Clearly $I \subseteq IP^{-1}$, and $I \neq IP^{-1}$ (otherwise P^{-1} is integral). So $IP^{-1} \subseteq II^{-1} \subseteq R$, so IP^{-1} is an ideal of R. Hence IP^{-1} is a product of prime ideals. However, then $I = (IP^{-1})P$, since $PP^{-1} = R$, so I is a product of prime ideals, contradicting our assumption. So every nonzero ideal is a product of primes.

Finally, we will show that this representation of nonzero ideals into products of prime ideals is unique. Suppose

$$I = P_1 \cdot ... \cdot P_r = Q_1 \cdot ... \cdot Q_s \tag{5.4}$$

Then $P_1 \cdot ... \cdot P_r \subseteq Q_1$. Hence $P_i \subseteq Q_1$ for some i, say $i = 1$. Now, using the property that every nonzero prime ideal is maximal, we know P_1 is maximal, so we must have $P_1 = Q_1$. Multiply (5.4) by P_1^{-1}, and we have $P_2 \cdot ... \cdot P_r = Q_2 \cdot ... \cdot Q_s$. By induction, $r = s$ and after reordering, $P_i = Q_i$ for every i. This completes the proof. □

Now, we refer back to the example considered in Chapter 4. We know from Theorem 7 that $\mathbb{Z}[\sqrt{-5}]$ is a number ring. So although we were able to find an

example of non-uninque factorization into irreducible elements, we now know that in this ring, every ideal factors uniquely into a product of prime ideals. In Chapter 7, we will see how some of the ideals in this ring factor into products of prime ideals.

CHAPTER 6: EXAMPLE OF A RING THAT IS NOT A DEDEKIND DOMAIN

We saw in Example 28 that the ring $\mathbb{Z}[\sqrt{-3}]$ is not integrally closed, so it is not a number ring, and in this case it is not a Dedekind domain. In this ring, we do not have unique factorization into prime ideals.

Consider the ideal $I = (2, 1+\sqrt{-3})$. First, we show that $I^2 = 2I$. Noting that $-2+2\sqrt{-3} = 2+2\sqrt{-3}-4$, we have

$$\begin{aligned} I^2 &= (2^2, (1+\sqrt{-3})^2, 2(1+\sqrt{-3})) \\ &= (4, -2+2\sqrt{-3}, 2+2\sqrt{-3}) \\ &= (4, 2+2\sqrt{-3}) \\ &= (2(2), 2(1+\sqrt{-3})) \\ &= 2I \end{aligned}$$

so $I^2 = 2I$. Also, we can clearly see that $I \neq (2)$, since $(2) = \{2a+2b\sqrt{-3} : a, b \in \mathbb{Z}\}$, and this set clearly does not contain the element $1+\sqrt{-3} \in I$.

Now we will show that I is prime. Since elements in I have the form $2(a+b\sqrt{-3}) + (1+\sqrt{-3})(c+d\sqrt{-3}) = (2a+c-3d) + (c+d)\sqrt{-3}$, we can see from here that I is the set of $a+b\sqrt{-3}$ such that $a \equiv b (\text{mod } 2)$. Now take some product of elements $(a+b\sqrt{-3})(c+d\sqrt{-3}) = (ac-3bd) + (bc+ad)\sqrt{-3} \in I$. Then $ac-3bd \equiv bc+ad (\text{mod } 2)$. Now if $a \not\equiv b$ and $c \not\equiv d (\text{mod } 2)$, then there are four options for what a, b, c, and d are equivalent to modulo 2, but in any case we get a contradiction. So we must have either $a \equiv b$ or $c \equiv d (\text{mod } 2)$. Thus one of the two elements from the product is in I, and I is prime.

Now, we will start by showing that if we could factor each ideal into a product of primes in this ring, then that factorization would not be unique. Suppose to the

contrary that (2) can be written as a product of prime ideals. Then $(2) = P_1 \cdot P_2 \cdot \ldots \cdot P_k$. Then we have $I \cdot I = (2) \cdot I = P_1 \cdot P_2 \cdot \ldots \cdot P_k \cdot I$ and since I is a prime ideal, we have two distinct prime ideal factorizations of the same ideal since $I \neq (2) = P_1 \cdot P_2 \cdot \ldots \cdot P_k$.

We can show further that the ideal (2) cannot be written as a product of primes at all. Let P be some prime ideal containing (2). Then $(2) \subsetneq P$ since (2) is not itself prime. Take some element $a + b\sqrt{-3} \in P \setminus (2)$. Then at least one of a, b is odd. Suppose $a = 2k + 1$ and $b = 2j$. Then $1 = (2k + 1 + 2j\sqrt{-3}) - (2k + 2j\sqrt{-3}) \in P$, contradicting that P is prime. If $a = 2k$ and $b = 2j + 1$ then $\sqrt{-3} = (2k + (2j + 1)\sqrt{-3}) - (2k + 2j\sqrt{-3}) \in P$, which implies $-3 = \sqrt{-3}\sqrt{-3} \in P$ which would give $1 = 3 - 2 \in P$, resulting in a contradiction again. Then a and b must both be odd. Then since (2) is made of all $a + b\sqrt{-3}$ such that a and b are even, we have that $P = I$ since I is the set of all elements such that a and b have the same parity.

Thus I is the only ideal that contains (2), so if (2) is a product of prime ideals, it must be a power of I. But $(2) \subsetneq I$, and $I^2 = (4, -2 + 2\sqrt{-3}, 2 + 2\sqrt{-3}) \subsetneq (2)$, and then $I^k \subsetneq (2)$ for all $k \geq 2$. It follows that (2) cannot be written as a product of prime ideals.

CHAPTER 7: SPLITTING OF PRIMES IN QUADRATIC FIELDS

Now, since we know that in a number ring every ideal factors uniquely into a product of prime ideals, we can consider how this looks in the number rings corresponding to quadratic fields.

Lemma 46. *Let R be the ring of algebraic integers in $\mathbb{Q}[\sqrt{m}]$ (m squarefree), and let p be prime. Then R/pR is naturally a 2-dimensional vector space over $\mathbb{Z}/p\mathbb{Z}$.*

Proof. R/pR is naturally a $\mathbb{Z}/p\mathbb{Z}$-module with scalar multiplication $(z + p\mathbb{Z})(r + pR) = zr + P$ for $z \in \mathbb{Z}$ and $r \in R$. Since R is generated over $\mathbb{Z}$ by two elements (either $\{1, \sqrt{m}\}$ or $\{1, \frac{1+\sqrt{m}}{2}\}$, depending on m), R/pR is generated over $\mathbb{Z}/p\mathbb{Z}$ by two elements. So that $\dim_{\mathbb{Z}/p\mathbb{Z}} R/pR \leq 2$. On the other hand, we can show that $1 + pR$ and $\sqrt{m} + pR$ are linearly independent over $\mathbb{Z}/p\mathbb{Z}$. Indeed, if we have

$$(a + p\mathbb{Z})(1 + pR) + (b + p\mathbb{Z})(\sqrt{m} + pR) = pR$$

then, multiplying and simplifying, we have $a + pR + b\sqrt{m} + pR = 0$, thus $a + b\sqrt{m} + pR = 0$, which implies that $a + b\sqrt{m} \in pR$. Thus $p \mid a$ and $p \mid b$, so our original scalar terms were 0, and we have that the two elements are linearly independent. Thus $\dim_{\mathbb{Z}/p\mathbb{Z}} R/pR = 2$. □

The following is Theorem 25 in Marcus' *Number Fields* [3]. We will give a proof based on what we have developed in this paper.

Theorem 47. *Let p be prime and let $R = \mathbb{A} \cap \mathbb{Q}[\sqrt{m}]$.*

If $p \mid m$, then $pR = (p, \sqrt{m})^2$ (1)

If $p = 2$ and m is odd, then

$$2R = \begin{cases} (2, 1+\sqrt{m})^2 & \text{if } m \equiv 3 \pmod 4 \quad (2) \\ \left(2, \frac{1+\sqrt{m}}{2}\right)\left(2, \frac{1-\sqrt{m}}{2}\right) & \text{if } m \equiv 1 \pmod 8 \quad (3) \\ \text{prime} & \text{if } m \equiv 5 \pmod 8 \quad (4) \end{cases}$$

If p is odd, $p \nmid m$, then

$$pR = \begin{cases} (p, n+\sqrt{m})(p, n-\sqrt{m}) & \text{if } m \equiv n^2 \pmod p \quad (5) \\ \text{prime} & \text{if } m \text{ is not a square mod } p \quad (6) \end{cases}$$

Proof. For (1), since $(p, \sqrt{m})^2 = (p^2, p\sqrt{m}, m)$ and $p \mid m$, we have $(p, \sqrt{m})^2 \subseteq pR$. On the other hand, since the gcd of any two integers can be expressed as a linear combination of those elements, $(p, \sqrt{m})^2$ contains the gcd of p^2 and m, which is p, so it contains pR. It remains only to show that $(p, \sqrt{m})$ is maximal (and therefore prime).

To do that, first suppose to the contrary that $\sqrt{m} \in pR$. If $m \equiv 2$ or $3 (\text{mod } 4)$ then $\sqrt{m} = p(a + b\sqrt{m})$ where $a, b \in \mathbb{Z}$. This implies that $1 = pb$ where $p > 1$ and b is an integer, which is a contradiction. If $m \equiv 1 (\text{mod } 4)$, then $\sqrt{m} = p(\frac{a}{2} + \frac{b}{2}\sqrt{m})$ where a and b are integers. This implies that $1 = \frac{pb}{2}$, and $2 = pb$ for some integer b, so p must be 2, but we have $p \mid m$ and m is odd. So we have a contradiction in this case as well. Thus $\sqrt{m} \notin pR$. Thus $pR \subsetneq (p, \sqrt{m})$. We also have $(p, \sqrt{m}) \subsetneq R$, since any integer that isn't divisible by p will not be in $(p, \sqrt{m})$. So we have the ascending chain $pR \subsetneq (p, \sqrt{m}) \subsetneq R$, and then $(0) = pR/pR \subsetneq (p, \sqrt{m})/pR \subsetneq R/pR$. And since these are all proper subspaces, and the dimension of R/pR is 2, there is no room for anymore ideals in this chain, thus $(p, \sqrt{m})$ is maximal, and hence it is prime.

For (2), we have $(2, 1+\sqrt{m})^2 = (4, 2+2\sqrt{m}, 1+m+2\sqrt{m}) \subseteq 2R$. To show containment in the other direction, we observe that $(1+m+2\sqrt{m}) - (2+2\sqrt{m}) = m - 1 \equiv 2 (\text{mod } 4)$, so the ideal contains 4 and an element equivalent to 2 mod 4, so

it contains the gcd of those two elements, which is 2. Thus $2R \subseteq (2, 1+\sqrt{m})^2$ and we have $2R = (2, 1+\sqrt{m})^2$.

Now we need to show that $(2, 1+\sqrt{m})$ is maximal. First, we can easily see that $1+\sqrt{m} \notin 2R$ since if it was, we would have $1+\sqrt{m} = 2(a+b\sqrt{m})$ which would give $a = b = \frac{1}{2}$, which is not possible since $m \equiv 3 (\text{mod } 4)$. So we have $2R \subsetneq (2, 1+\sqrt{m})$. We also know elements in this ideal have the form $2(a+b\sqrt{m})+(1+\sqrt{m})(c+d\sqrt{m}) = (2a+c+md)+(2b+c+d)\sqrt{m}$. Now, if $(2, 1+\sqrt{m})$ is not a proper ideal of R, then it contains 1, in which case $2a+c+md = 1$ and $2b+c+d = 0$. Solve the second equation for c and substitue into the first equation to get $1 = 2a-2b-d+md = 2a-2b+d(m-1)$ and since $m-1$ is even, this is a contradiction. So we have $2R \subsetneq (2, 1+\sqrt{m}) \subsetneq R$. Now we can use the lemma like we did in (1) to show that $(2, 1+\sqrt{m})$ is maximal and therefore prime.

For (3), first note that $m \equiv 1 (\text{mod } 8)$ implies that $m \equiv 1 (\text{mod } 4)$. So $1-m$ is divisible by 4, and we have $\left(2, \frac{1+\sqrt{m}}{2}\right)\left(2, \frac{1-\sqrt{m}}{2}\right) = \left(4, 1+\sqrt{m}, 1-\sqrt{m}, \frac{1-m}{4}\right) \subseteq 2R$. Also since $-(1+\sqrt{m})-(1-\sqrt{m})+4 = 2$, we have $2R \subseteq \left(2, \frac{1+\sqrt{m}}{2}\right)\left(2, \frac{1-\sqrt{m}}{2}\right)$. Thus $2R = \left(2, \frac{1+\sqrt{m}}{2}\right)\left(2, \frac{1-\sqrt{m}}{2}\right)$.

Again, we must show that both $\left(2, \frac{1+\sqrt{m}}{2}\right)$ and $\left(2, \frac{1-\sqrt{m}}{2}\right)$ are maximal to show they are prime. The proof is similar to the proofs in parts (1) and (2), so we omit it.

For (4), we note again that $m \equiv 5 (\text{mod } 8)$ implies that $m \equiv 1 (\text{mod } 4)$. Now we need to show that 2 is prime in R. Let $2 \mid \left(\frac{a+b\sqrt{m}}{2}\right)\left(\frac{c+d\sqrt{m}}{2}\right)$. So we have

$$2\left(\frac{e+f\sqrt{m}}{2}\right) = \left(\frac{a+b\sqrt{m}}{2}\right)\left(\frac{c+d\sqrt{m}}{2}\right) \tag{7.1}$$

Note that the pairs a, b and c, d and e, f all have the same parity. If a, b are even, then we have $\left(\frac{a+b\sqrt{m}}{2}\right) = 2\left(\frac{(a/2)+(b/2)\sqrt{m}}{2}\right)$, so 2 divides on of the elements in the product and is therefore prime, as desired. A similar result follows if c, d are even.

Suppose a, b, c, d are all odd. Clearing fractions and taking norms of (7.1), we get $16(e^2 - mf^2) = (a^2 - mb^2)(c^2 - md^2)$. Now, since e, f have the same parity, $e^2 - mf^2$ is always even, so we have $2^5 = 32 \mid (a^2 - mb^2)(c^2 - md^2)$. So we must

have $2^3 = 8$ divides one of the elements $a^2 - mb^2$ or $c^2 - md^2$. If $8 \mid a^2 - mb^2$ then we have $a^2 \equiv mb^2 (\text{mod } 8)$ and since b is odd, it's coprime to 8, so we can divide to get $(\frac{a}{b})^2 \equiv m (\text{mod } 8)$. But this gives a contradiction since all squares mod 8 are congruent to $0, 1, 4$. A similar contradiction arises if $8 \mid c^2 - md^2$. Thus 2 is prime in R and we have that $2R$ is a prime ideal.

For (5), we have $(p, n+\sqrt{m})(p, n-\sqrt{m}) = (p^2, pn+p\sqrt{m}, pn-p\sqrt{m}, n^2-m)$. We have $n^2 \equiv m (\text{mod } p)$, so p divides n^2-m and all other generators, so $(p, n+\sqrt{m})(p, n-\sqrt{m}) \subseteq pR$. Now, this ideal also contains the element $(pn+p\sqrt{m})+(pn-\sqrt{m}) = 2pn$. So it also contains the gcd of p^2 and $2pn$, which must be p, since p is odd and p clearly cannot divide n. So we also have $pR \subseteq (p, n + \sqrt{m})(p, n - \sqrt{m})$ and thus $pR = (p, n + \sqrt{m})(p, n - \sqrt{m})$.

Now we only need to show that $(p, n + \sqrt{m})$ and $(p, n - \sqrt{m})$ are maximal and therefore prime. Again, the proof is similar to the ones above, so it is omitted.

Finally, for (6), we just need to show that pR is maximal, and thus prime. Take some $a + b\sqrt{m} \in R \setminus pR$. Then we claim that $(p, a + b\sqrt{m}) = R$. If this is the case, then we have shown that pR is maximal and we're done.

To prove the claim, first note that $a^2-mb^2 = (a+b\sqrt{m})(a-b\sqrt{m}) \in (p, a+b\sqrt{m})$. Now suppose to the contrary that $p \mid a^2 - mb^2$. Then if p divides b, it must also divide a, contradicting that $a+b\sqrt{m} \notin pR$. So p cannot divide b. Then we can find a multiplicative inverse of b mod p, and we have $(\frac{a}{b})^2 \equiv m (\text{mod } p)$, contradicting that m is not a square mod p. So $p \nmid a^2 - mb^2$. Then $(p, a + b\sqrt{m})$ must contain the gcd of p and $a^2 - mb^2$, which we have just shown is 1. This completes the proof of the claim. □

To apply this theorem, (1)-(4) are very straightforward applications, but for (5) and (6) we need to know if m is a square mod p, which is the same thing as determining if m is a quadratic residue of p. In more complicated cases, this can be done with the help of Gauss' Law of Quadratic Reciprocity [1, Theorem 9.9]. We will

consider two simple examples.

Example 48. Take the number ring $R = \mathbb{A} \cap \mathbb{Q}[\sqrt{15}] = \mathbb{Z}[\sqrt{15}]$. Applying the theorem, we have

$$2R = (2, 1 + \sqrt{15})^2 \qquad \text{by (2)}$$

$$3R = (3, \sqrt{15})^2 \qquad \text{by (1)}$$

$$5R = (5, \sqrt{15})^2 \qquad \text{by (1)}$$

$$7R = (7, 1 + \sqrt{15})(7, 1 - \sqrt{15}) \qquad \text{by (5)}$$

$$11R = (11, 2 + \sqrt{15})(11, 2 - \sqrt{15}) \qquad \text{by (5)}$$

The first three are direct applications of the theorem, for $7R$, we need to know that $m = 15$ is a square mod $p = 7$. This is easy, since $15 \equiv 1 \equiv 1^2 (\text{mod } 7)$. For $11R$, we can see that $15 \equiv 4 \equiv 2^2 (\text{mod } 11)$.

Example 49. We can also consider $R = \mathbb{A} \cap \mathbb{Q}[\sqrt{-3}]$.

$$2R = \left(2, \frac{1 + \sqrt{-3}}{2}\right)\left(2, \frac{1 - \sqrt{-3}}{2}\right) \qquad \text{by (3)}$$

$$3R = (3, \sqrt{-3})^2 \qquad \text{by (1)}$$

$$5R = \text{prime} \qquad \text{by (6)}$$

$$7R = (7, 2 + \sqrt{-3})(7, 2 - \sqrt{-3}) \qquad \text{by (5)}$$

Again, the first two are easily verified using the theorem, but for $5R$ and $7R$ we must know if -3 is a quadratic residue of these primes. For $5R$, we can quickly find all quadratic residues:

$$1^2 \equiv 1 (\text{mod } 5) \qquad 2^2 \equiv 4 (\text{mod } 5)$$

$$3^2 \equiv 4 (\text{mod } 5) \qquad 4^2 \equiv 1 (\text{mod } 5)$$

so clearly $-3 \equiv 2 (\text{mod } 5)$ is not a quadratic residue of 5. For $7R$, we have $-3 \equiv 4 = 2^2 (\text{mod } 7)$, so -3 is a quadratic residue of 7.

REFERENCES

[1] D. M. Burton, *Elementary Number Theory*, McGraw-Hill, New York, 2011.

[2] J. A. Gallian, *Contemporary Abstract Algebra*, Brooks/Cole, 2013.

[3] D. A. Marcus, *Number Fields*, Springer-Verlag, New York, 1977.