2015

Restoring Factorization in Integral Domains

Susan Kirk
Virginia Commonwealth University

Restoring Factorization in Integral Domains

A thesis submitted in partial fulfillment of the requirements for the degree of Master of Science at Virginia Commonwealth University.

by

Susan L. Kirk
Master of Science

Director: Dr. Taylor, Advisor, Associate Professor
Department of Mathematics and Applied Mathematics

Virginia Commonwealth University
Richmond, Virginia
April 2015

Acknowledgements

Thanks to my family.

Table of Contents

Abstract

RESTORING FACTORIZATION IN INTEGRAL DOMAINS

By Susan L. Kirk, Master of Science in Mathematical Sciences

A thesis submitted in partial fulfillment of the requirements for the degree of Master of Science at Virginia Commonwealth University.

Virginia Commonwealth University, 2015

Director: Dr. Taylor, Advisor, Associate Professor, Department of Mathematics and Applied Mathematics

This is an expository thesis on integral domains which are not unique factorization domains. We focus on restoring a type of unique factorization using prime ideals within quadratic integer rings. In particular, we examine which quadratic integer rings will admit such factorization.

In this paper we consider integral domains which lack unique factorization, such as the prime factorization that exists in the integers. We discuss a way to restore a type of unique factorization using the construct of *ideals*.

The first chapter of our paper provides background Ring Theory and assumes basic abstract algebra knowledge. Necessary theorems are presented, some without proof, and examples are given.

The second chapter focuses mainly on Quadratic Integer Rings. In particular, quadratic integer rings in which we can restore a type of factorization using prime ideals. Interesting history relative to the study is included where appropriate.

Chapter 1

Preliminaries

In this chapter we provide the necessary definitions and background information from ring theory to understand the paper. Basic abstract algebra knowledge is assumed and most theorems will be stated without proof. Where appropriate, references are given.

1.1 Ring Theory

Definition 1 *A **Ring** is a non-empty set* R *with two binary operations: (*$+$ *addition and* $\times$ *multiplication) that satisfy the following properties for all* $a, b, c \in R$*:*

1. *If* $a, b \in R$*, then* $a + b \in R$ *(closure under addition)*
2. $a + (b + c) = (a + b) + c$ *(associative property for addition)*
3. $a + b = b + a$ *(commutative property for addition)*
4. *There exists a unique element* $0 \in R$ *such that* $0 + a = a = a + 0$ *for all* $a \in R$ *(additive identity exists)*
5. *For every element* $a \in R$*, there exists a unique element* a^{-1} *such that* $a^{-1}+a = 0 = a+a^{-1}$ *(additive inverses exist)*

6. *If* $a, b \in R$*, then* $ab \in R$ *(closure under multiplication)*

7. $a(bc) = (ab)c$ *(associative property for multiplication)*

8. $a(b + c) = ab + ac$ *and* $(a + b)c = ac + bc$ *(distributive properties)*

We denote the set R with the two binary operations as $(R, +, \times)$. The first five properties above show that every ring is an Abelian Group under addition.

Example 1 *The integers* $\mathbb{Z}$ *is a ring where* 0 *is the additive identity and the additive identity of each element* z *is just* $-z$*.*

Example 2 *The set* $M_n(R)$ *of* $n \times n$ *matrices with entries from the ring* R *is a ring. The* $n \times n$ *zero matrix is the unique additive identiy element of* $M_n(R)$*.*

We say a ring R is *commutative* if $ab = ba$ for all a, b in R. The ring R is called *a ring with unity* (or *a ring with identity*) if R contains a multiplicative identity $1 \neq 0$ such that $1a = a = a1$ for all $a \in R$.

Example 3 *The set* E *of even integers is a commutative ring since for all* $a, b \in E, ab = ba$*. Note that there is no even integer* x *such that* $xa = a = ax$ *for all nonzero* $a \in E$*, so* E *is not a ring with unity.*

Example 4 *The set* $M_n(\mathbb{R})$ *of* $n \times n$ *matrices with real number entries is a ring. The unique identity element of* $M_n(\mathbb{R})$ *is the* $n \times n$ *identity matrix, thus* $M_n(\mathbb{R})$ *is a ring with unity. Notice* $M_n(\mathbb{R})$ *is not commutative since matrix multiplication is not commutative.*

Rings can have a several extra multiplication properties such as a multiplicative identity $1 \neq 0$ and multiplication can be commutative.

Example 5 *The set* $\mathbb{Z}/6\mathbb{Z}$ *with addition and multiplication defined as modulo* 6 *is a commutative ring with unity. In fact, for any* $n \in \mathbb{Z}$*, where* n *is not prime, the quotient group* $\mathbb{Z}/n\mathbb{Z}$ *is a commutative ring with unity.*

A subring S of a ring R is analogous to a subgroup of a group. That is, if S is a subset of a ring R, such that:

1. if $a, b \in S$, then $a + b \in S$ (closed under ring addition)
2. if $a, b \in S$, then $ab \in S$ (closed under ring multiplication)
3. $0 \in S$ (the additive identity of the ring R is also in S)
4. if $a \in S$, then there exists some $a^{-1} \in S$ such that $a + a^{-1} = 0$

then S is a subring of R.

Example 6 *The integers $\mathbb{Z}$ is a subring of the rationals $\mathbb{Q}$.*

An element a of a ring R is called a **zero divisor** if $a \neq 0$ and there exists some nonzero element $b \in R$ such that either $ab = 0$ or $ba = 0$.

Example 7 *In $\mathbb{Z}/6\mathbb{Z} = \{0, 1, 2, 3, 4, 5\}$, we see that $2 \times 3 = 6 = 0$ mod 6, but $2 \neq 0$ and $3 \neq 0$. So 2 and 3 are called zero divisors in $\mathbb{Z}/6\mathbb{Z}$. In fact, every nonzero element in $\mathbb{Z}/n\mathbb{Z}$ that is not relatively prime to n is a zero divisor.*

1.2 Integral Domains

The type of rings that will be of focus in this paper are commutative rings with identity that have no zero divisors.

Definition 2 *An **Integral Domain** is a commutative ring R with identity $1 \neq 0$ that satisfies the axiom: whenever $a, b \in R$ and $ab = 0$, then $a = 0$ or $b = 0$.*

The condition $1 \neq 0$ is needed to exclude the zero ring. Notice that the axiom says that R has no zero divisors.

Example 8 *The set $\mathbb{Z}$ is an integral domain.*

Example 9 *Consider the set* $\mathbb{Z}\left[\sqrt{-17}\,\right] = \left\{a + b\left[\sqrt{-17}\,\right] \mid a, b \in \mathbb{Z}\right\}$ *where addition and multliplication of elements is defined as:*

$$(a + b\sqrt{-17}) + (c + d\sqrt{-17}) = (a + c) + (b + d)\sqrt{-17}$$

$$(a + b\sqrt{-17})(c + d\sqrt{-17}) = ac + (ad + bc)\sqrt{-17} - 17bd.$$

$\mathbb{Z}\left[\sqrt{-17}\,\right]$ *is an integral domain.*

A nonzero element u in an integral domain R is called a **unit** if there exists some nonzero $v \in R$ such that $uv = 1 = vu$.

So the units of a ring are the elements in the ring which have multiplicative inverses.

Now, we need a way to measure the size of individual elements in a domain.

Definition 3 *Let* R *be an integral domain. A function* $N : R \to \mathbb{Z}^+ \cup 0$ *with* $N(0) = 0$ *is called the* ***norm*** *on the integral domain* R*. The norm is called a positive norm if* $N(a) > 0$ *for all* $a \neq 0$*. Also,* $N(ab) \leqslant N(a)N(b)$ *for all* $a, b \in R, a, b \neq 0$*.*

By this definition, any particular integral domain could have several norms. One familiar norm is the absolute value function on the integers. We say that an element has *minimum norm* if $N(u) = \pm 1$. We can now define the units of a ring using the norm.

Definition 4 *A* ***unit*** u *of a ring* R *is a nonzero element that has minimum norm,* N*,* $N(u) = \pm 1$*.*

In $\mathbb{Z}$, the only units are the integers 1 and -1, since $|1| = 1 = |-1|$, where the norm on the integers is the usual absolute value function.

Definition 5 *An element* b *in a commutative ring with unity is called an* ***associate*** *of an element* a *if* $a = bu$ *for some unit* u*.*

Example 10 *In* $\mathbb{Z}$*,* 3 *and* -3 *are associates since* $-3 = 3(-1)$ *and* -1 *is a unit in* $\mathbb{Z}$*. So associates differ from each other by a unit.*

Definition 6 *An **irreducible** element is a nonzero, nonunit element whose only divisors are its associates and the units of the domain.*

So, an element p of an integral domain is irreducible if and only if whenever $p = rs$, then r or s is a unit.

Example 11 *In $\mathbb{Z}$, the irreducible elements are all of the prime integers, since the only divisors of a prime integer are itself and 1 and -1, the units of $\mathbb{Z}$.*

Definition 7 *An integral domain R is a **Unique Factorization Domain (UFD)** if every nonzero, nonunit element $r \in R$ has the following two properties:*

1. $r = p_1 p_2 \cdots p_n$ *(finite product of not necessarily distinct irreducible elements)*

2. *this decomposition is unique up to associates.*

That is, if $r = p_1 p_2 \cdots p_n$ and $r = q_1 q_2 \cdots q_m$, then $m = n$ and p_i is an associate of q_j for some j.

So a UFD is an integral domain where every nonzero element has a **unique** factorization into a product of **irreducible** elements. We consider associate factors equivalent. In UFD's, prime and irreducible are the same. The integers, $\mathbb{Z}$, is a UFD in which we are familiar with the notion of *unique factorization* per the Fundamental Theorem of Arithmetic. In a UFD, *prime* and *irreducible* are the same, so we can think of prime elements in $\mathbb{Z}$ as a reference.

Example 12 *The polynomial ring $\mathbb{Z}[x]$ is a an example of an integral domain that is also a UFD. The polynomial ring in variables x and y with rational coefficients, $\mathbb{Q}[x, y] = \mathbb{Q}[x][y]$ is also a UFD.*

We take unique factorization such as the prime factorization of integers for granted, however, there are many sets of numbers that do not have unique factorization of individual elements.

Definition 8 *Let* R *be a ring, let* A *be a subset of* R *and let* $r \in R$.

1. $rA = \{ra \mid a \in A\}$ *and* $Ar = \{ar \mid a \in A\}$

2. *A subset* A *of* R *is a* ***left ideal*** *of* R *if*

   - A *is a subring of* R, *and*
   - A *is closed under left multiplication by elements from* R, *i.e.,* $rA \subseteq A$ *for all* $r \in R$.

   Similary, A *is a* ***right ideal*** *of* R *if*

   - A *is a subring of* R, *and*
   - A *is closed under right multiplication by elements from* R, *i.e.,* $Ar \subseteq A$ *for all* $r \in R$.

3. *A subset* A *that is both a left ideal and a right ideal is called an* ***ideal*** *of* R.

An ideal is a subring with an absorption property. Whenever any element r from the ring R is multiplied by an element a from the ideal, then the element ra (and ar) is in the ideal. We write the ideal A of the ring R as $A \triangleleft R$.

Example 13 *Consider* $\mathbb{Z}$.

$$2\mathbb{Z} = \{2a \mid a \in \mathbb{Z}\} = \{\ldots, -4, -2, 0, 2, 4, \ldots\} \text{ is an ideal in } \mathbb{Z}$$

$$3\mathbb{Z} = \{3a \mid a \in \mathbb{Z}\} = \{\ldots, -6, -3, 0, 3, 6, \ldots\} \text{ is an ideal in } \mathbb{Z}$$

We denote these ideals as (2) *and* (3) *and call them the ideal generated by* 2 *and the ideal generated by* 3 *since in both instances, the ideal consists of ring multiples of* 2 *and* 3 *respectively. In fact, since these ideals can be generated by a single element, they are called principal ideals*

Ideals can be multiplied together, but the product of ideals includes more than just the products of individual ideal elements.

Definition 9 *Let* A *and* B *be ideals of the ring* R. *The* ***product*** *of* A *and* B, *denoted* AB, *is the set of all finite sums of elements of the form* ab *where* $a \in A$ *and* $b \in B$.

Example 14 *In $\mathbb{Z}$, let $A = 2\mathbb{Z}$ and $B = 3\mathbb{Z}$. Then AB consists of all finite sums of elements of the form $(2a)(3b)$ where $a, b \in \mathbb{Z}$. So, $5 \in AB$ since $5 = (2 * 1) + (3 * 1)$. Also, $1 \in AB$ since $1 = (2 * 2) + (3 * -1)$. Thus $AB = \mathbb{Z}$.*

Just as rings can have extra properties, ideals can also have extra properties.

Definition 10 *In a commutative ring R with unity, an ideal P is called **prime** if $P \neq R$ and whenever $ab \in P$, then $a \in P$ or $b \in P$.*

Example 15 *In $\mathbb{Z}$, (2) and (3) are prime ideals since every element in (2) is a ring multiple of 2. Similarly, any element in (3), is of the form $3r$ for some $r \in \mathbb{Z}$.*

Example 16 *If R is an integral domain, then the zero ideal is prime.*

Definition 11 *An ideal M of a ring R with unity is called **maximal** if*

1. *$M \neq R$*
2. *whenever J is an ideal such that $M \subseteq J \subseteq R$,*
   then either $M = J$ or $J = R$. (M is not contained in any other proper ideal.

Showing that an ideal is prime or maximal can be very tedious depending on the ideal and ring given. The following theorem provides a nice way to determine whether an ideal is prime or maximal.

Theorem 1 *Let R be a commutative ring with identity and P an ideal in R. If the quotient ring R/P is an integral domain, then P is a prime ideal in R.*

Definition 12 *A **principal ideal domain (PID)** is an integral domain in which every ideal is principal.*

That is, every ideal can be generated by one *smallest* element of the ideal. Unique factorization holds in PIDs.

Definition 13 *An integral domain* R *is called* ***Noetherian*** *or is said to satisfy the* ***Ascending Chain Condition (ACC) on principal ideals*** *provided that whenever*

$$(a_1) \subseteq (a_2) \subseteq (a_3) \subseteq \dots$$

then there exists a positive integer n *such that* $(a_i) = (a_n)$ *for all* $i \geqslant n$.

This means that every chain of principal ideals terminates at some point.

Theorem 2 *[3, p565] The following are equivalent:*

1. R *is a Noetherian ring*
2. *Every nonempty set of ideals of* R *contains a maximal element under inclusion*
3. *Every ideal of* R *is finitely generated.*

Example 17 *The integral domains* $\mathbb{Z}\left[\sqrt{-19}\,\right]$ *and* $\mathbb{Z}\left[\sqrt{-43}\,\right]$ *are examples of PIDs.*

In a PID, every nonzero prime ideal is also a maximal ideal.

Definition 14 *Two ideals* A, B *of an algebraic integer ring* $\mathscr{O}$ *(or* $\mathbb{Z}[\sqrt{d}]$*) are said to be equivalent,* $A \sim B$*, if there exist nonzero elements* $a, b \in \mathscr{O}$ *such that* $(a)A = (b)B$.

The equivalance classes of this equivalance relation are called **ideal classes**. The number of ideal classes, $h_{\mathscr{O}}$, is called the class number of $\mathscr{O}$.

Theorem 3 *Let* A *be an ideal in the quadratic integer ring* $\mathscr{O}$*. Then the class number* $h_{\mathscr{O}} = 1$ *iff* $\mathscr{O}$ *is a PID.*

Proof 1 $(\Rightarrow)$*Let* A *an ideal in the quadratic integer ring* $\mathscr{O}$*. Suppose the class number* $h_{\mathscr{O}} = 1$*. Then* $A \sim \mathscr{O}$ *means that there exist nonzero elements* $\alpha, \beta, r \in \mathscr{O}$ *and* $\alpha \in A$ *and* $\beta \in B$ *such*

that $(\alpha)A = (\beta)\mathscr{O}$*. Then*

$$\alpha a = \beta r$$
$$\alpha^{-1}\alpha a = \alpha^{-1}\beta r$$
$$a = \alpha^{-1}\beta \in (\alpha^{-1}\beta)$$

Since $a \in A$*, then* $A \subseteq (\alpha^{-1}\beta)$*.* ($\Leftarrow$)*Let* $x \in (\alpha_{-1}\beta)$*. So* $x = \alpha_{-1}\beta$*. Since* $A \sim \mathscr{O}$*, then* $\mathscr{O} \sim A$ *and there exists nonzero elements* $\alpha, \beta, r \in \mathscr{O}$ *such that* $(\beta)\mathscr{O} = (\alpha)A$*. Then*

$$\beta r = \alpha a$$
$$\beta = \alpha a$$
$$\alpha_{-1}\beta = \alpha_{-1}\alpha a$$
$$\alpha_{-1}\beta = a \in A.$$

Thus $(\alpha_{-1}\beta) \subseteq A$*. Then* $A = (\alpha_{-1}\beta)$*. Therefore every ideal is principal and* $\mathscr{O}$ *is a PID.* ($\Leftarrow$)*Suppose* $\mathscr{O}$ *is a PID. Then every ideal is principal and can be generated by one smallest element. Supposes* A, B *are ideals in* $\mathscr{O}$*. (We show that* $A \sim B$*). Since* $\mathscr{O}$ *is a PID, then* $A = (a)$ *and* $B = (b)$ *for some nonzero elements* $a \in A$ *and* $b \in B$*. Let* $\alpha, \beta, r \in \mathscr{O}$*. Let* $x \in (\alpha)A$*. Then* $x = \alpha a$*. Then*

$$\alpha a = r$$
$$\alpha^{-1}\alpha a = \alpha^{-1}r$$
$$a = \alpha^{-1}r$$
$$\beta a = \beta\alpha^{-1}r = \beta r = \beta$$
$$\beta ab = \beta b \in (\beta)B$$

Thus $(\alpha)A \subseteq (\beta)B$. *Now suppose* $x \in (\beta)B$. *Then* $x = \beta b$. *Then*

$$\begin{aligned} \beta b &= r \\ \beta^{-1}\beta b &= \beta^{-1} r \\ b &= \beta^{-1} r = r \\ ba &= ra = a \\ \alpha b a &= \alpha a \in (\alpha)A. \end{aligned}$$

Thus $(\beta)B \subseteq (\alpha)A$. *Then* $(\alpha)A = (\beta)B$. *Therefore* $A \sim B$, *that is the two ideals are equivalent. Thus* $\mathcal{O}$ *has only one equivalence class (one ideal class). Therefore the ideal class number* $h_{\mathcal{O}} = 1$.

So the class number $h_{\mathcal{O}}$ of an integral domain D measures how far D is from being a PID, with class number one being PIDs. Essentially, each ideal in a PID is an ideal *once removed* from the other ideals. That is, you can get to each ideal by merely "'multiplying"' the given ideal by *one* other ideal.

Proposition 1 *[5, p179] If* A *and* B *are ideals, such that* $B \subset A$, *there there is an ideal* C *such that* $A = BC$.

We can think of this proposition as *to contain is to divide*.

Definition 15 *For any integral domain* D *with fraction field* K, *a* ***fractional ideal*** *of* D *is a submodule of the form* $d^{-1}I$ *for some nonzero* $d \in D$ *and ideal* $I \in D$.

Example 18 *Let* D *be an integral domain with* $d \in D$ *and* I *an ideal in* D. *Then the ideal* $d^{-1}I$ *where* $d = 1$ *is a fractional ideal. In fact, all of the ideals of* D *with* $d = 1$ *as a "'denominator"', are fractional ideals of* D.

Now we have an equivalent definition for the class number of an integral domain.

Definition 16 *If* D *is an integral domain, then the quotient of the group of invertible fractonal ideals of* D *by the subgroup of nonzero principal fractional ideals of* D *is called the* ***class group*** D. *The order of the class group of* D *is called the* ***class number*** *of* D.

The fractional ideals are merely products of ideals with appropriate invertible integral domain elements. These invertible elements appear similar to denominators in fractions, hence the terminology.

Definition 17 *An integral domain* R *is a* ***Euclidean Domain*** *if there is a norm* N *such that for any two elements* $a, b \in R, b \neq 0$*, there exists some* $q, r \in R$ *such that* $a = qb + r$ *where either* $r = 0$ *or* $N(r) < N(b)$.

Euclidean Domains are integral domains equipped with a division algorithm. The associates of an element are the divisors of that element. If R is a commutative ring and $a, b \in R$ and $b \neq 0$, then a is a *multiple* of b if there exists an element $c \in R$ such that $a = bc$. That is, $b|a$ (a divides b) in R *iff* $a \in (b)$ *iff* $(a) \subseteq (b)$. That is, the ideal generated by the element $a \in R$ is contained in the ideal generated by the element $b \in R$.

Definition 18 *A* ***greatest common divisor*** *of* a *and* b *is a nonzero element* d *such that* $d|a$, $d|b$*, and if* $d'|a$ *and* $d'|b$*, then* $d'|d$.

Example 19 $\mathbb{Z}\left[\sqrt{-1}\,\right] = \mathbb{Z}[i\,] = \{a + bi \mid a, b \in \mathbb{Z}\}$ *is the ring of Gaussian Integers. The Gaussian Integers is a Euclidean Domain that was first developed by Gauss to prove that every algebraic equation has a real or imaginary root.*

Unique factorization also holds in Euclidean Domains.

Example 20 *Units in* $\mathbb{Z}[i] = \mathbb{Z}\left[\sqrt{-1}\,\right]$ *are* ± 1 *and* $\pm i$

- *since* $N(1) = N(1 + 0\sqrt{-1}) = (1 + 0\sqrt{-1})(1 - 0\sqrt{-1}) = \mathbf{1}$.
- *and* $N(i) = N(0 + \sqrt{-1}) = (0 + \sqrt{-1})(0 - \sqrt{-1}) = \mathbf{1}$.

Definition 19 *A* ***field*** *is an integral domain in which every nonzero element has a multiplicative inverse.*

Example 21 *The most familiar fields are* $\mathbb{Q}, \mathbb{R}, \mathbb{C}$*. In these fields, arithmetic works in the usual way. The set* $\mathbb{Z}/p\mathbb{Z}$ *where* p *is a prime, is a field in which arithmetic is performed modulo* p.

Example 22 $\mathbb{Q}[d] = \left\{ a + b\left[\sqrt{d}\right] \mid a, b \in \mathbb{Z} \right\}$ *where* d *is a square-free integer is a* ***quadratic field****.*

The following theorem is the analog of Theorem 1 for prime ideals. This will provide us an alternative way to determine if an ideal is maximal.

Theorem 4 *Let* R *be a commutative ring with unity. Let* M *be an ideal of* R*. Then* M *is a* ***maximal ideal*** *iff* R/M *is a* ***field****.*

Theorem 5 *Let* I *be an ideal of the ring* R*, a ring with unity. Then*

1. $I = R$ *iff* I *contains a unit*

2. *Let* R *be commutative,*

   then R *is a* ***field*** *iff its only ideals are* $\mathbf{0}$ *(the zero ideal) and* R *(the whole ring).*

We are looking at sets of numbers or domains with increasing algebraic structure. From lowest algebraic structure to highest we have: Rings, Integral Domains, Unique Factorization Domains (UFD), Principal Ideal Domains (PID), Euclidean Domains, Fields.

Chapter 2

Factorization in Integral Domains

Every positive integer has a unique prime factorization, however, many sets of numbers do not admit unique factorization. The concept of *ideals* originated from the study of certain numbers which had ideal, or desirable, properties of behavior according to the work of German mathematician E. E. Kummer. The theory of *ideals* was further developed by Dedekind to restore a type of unique factorization in certain integral domains. One major question is whether unique factorization can be restored in every integral domain. This *factorization* involves the factorization of ideals into a unique product of prime ideals in specific integral domains of *algebraic integers*.

2.1 General Factorization

We first look at factorization, or lack of it, in select integral domains. Specifically, for which values of square-free integers d the integral domain $\mathbb{Z}[\sqrt{d}] = \left\{ a + b\sqrt{d} | a, b \in \mathbb{Z} \right\}$ has unique factorization. We want to understand what special properties of d determine the algebraic structure of these integral domains. Karl Fredrich Gauss (1777-1855) discussed the solutions of binomial equations of the form $x^n = 1$ in his *Disquisitiones Arithmeticae* in 1801. He developed the theory of biquadratic residues and introduced the complex numbers notation $a + bi$ and found that every algebraic equation has a

real or imaginary root [1, p447]. While he was just a student, Gauss proved the law of quadratic reciprocity which is as follows:

Theorem 6 *[5, p60] (Law of Quadratic reciprocity). Let* p *and* q *be odd primes. Then*

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

2. $(\frac{2}{p}) = (-1)^{\frac{(p^2-1)}{8}}$.

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

Building upon Gauss's work, Ernst E. Kummer (1810-1893) studied complex numbers of the form $a + \sum bj$ where j is a complex root of the equation $j^p - 1 = 0$, where p is prime. He found that unique factorization of elements into products of prime numbers does not hold for all complex numbers. He then began the study of regular primes or ideal primes which had ideal or desirable behavior. Through the work of Kummer and Dedekind, the concept of ideal primes was developed into the modern abstract algebra notion of *ideals*. The idea of attempting to restore a notion of unique factorization is rather subtle. Some integral domains do not have factorization at all as the next example illustrates.

Example 23 *The integral domain* $\mathbb{Q}_{\mathbb{Z}}[x]$ *is the set of polynomials with rational coefficients and integer constant terms. Elements such as* $x^2 + 1, x, \frac{x}{3},$, *and* 3 *are in* $\mathbb{Q}_{\mathbb{Z}}[x]$. *It can be shown that* 3 *is irreducible in* $\mathbb{Q}_{\mathbb{Z}}[x]$. *Note that* $x = 3 * (\frac{x}{3})$. *Simarly,* 3 *is an irreducible factor of* $\frac{x}{3}$ *since* $\frac{x}{3} = 3 * 3 * (\frac{x}{3})$. *We can continue in this fashion indefinitely. Since:*

$$x = 3 * (\frac{1}{3}x) = 3 * 3 * (\frac{1}{9}x) = \cdots 3 * 3 * \cdots 3 * (\frac{1}{3^n}x) = \cdots$$

So, the element x *cannot be factored as a (finite) product of irreducibles of* $\mathbb{Q}_{\mathbb{Z}}[x]$. *So,* $\mathbb{Q}_{\mathbb{Z}}[x]$ *is not a Unique Factorization Domain.*

Another problem that exists is that of determining whether a given factorization is unique. Many integral domains have factorization of elements, but that factorization fails to be unique.

2.2 Quadratic Integer Rings

As we saw in the previous section, not all integral domains have unique factorization. In fact, there are specific types of integral domains called *quadratic integer rings* that are also Unique Factorization Domains. We first define some needed terminology.

Definition 20 *An **Algebraic Number** is a complex number α which is the root of a monic polynomial $x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1x + a_0$, with $a_i \in \mathbb{Q}$.*

Example 24 *The element $\alpha = i$ is an algebraic number in the polynomial ring $\mathbb{Q}[x]$ since $\alpha = i$ is a complex root of the polynomial $p(x) = x^2 + 1$. that is, $p(\alpha) = 0$.*

Definition 21 *An **Algebraic Integer** is a complex number α which is the root of a monic polynomial $x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1x + a_0$, with $a_i \in \mathbb{Z}$.*

Note that $\alpha = i$, from the previous example is also an algebraic integer.

Definition 22 *A field K is **algebraically closed** if every polynomial with coefficients in K has a root in K.*

Theorem 7 *(The Fundamental Theorem of Algebra) The field $\mathbb{C}$ is algebraically closed.*

Equivalently, every nonconstant polynomial in $\mathbb{C}[x]$ has a root in $\mathbb{C}$. Studying quadratic equations in 1785, Legendre (1752-1833) proved the equation $x^2 + py^2 = qz^2$ with $p \equiv 1 (\text{mod } 4)$ and $q \equiv 3 (\text{ mod } 4)$ which shows that

$$\text{if } q \text{ is a square modulo } p, \text{ then } p \text{ is a square modulo } q.$$

Definition 23 *A **Quadratic Integer** is a complex number that is the root of some monic quadratic polynomial with integer coefficients.*

Example 25 *In $\mathbb{Z}\left[\sqrt{-5}\,\right]$, every element $r + s\sqrt{-5}$ is a quadratic integer because it is the root of the monic polynomial*

$$x^2 - 2rx + (r^2 + ds^2) = \left(x - (r + s\sqrt{-5})\right)(x - (r - s\sqrt{-5})\right).$$

Definition 24 *Let $d \neq 1$ be a square-free integer, with no integer divisors of the form c^2 except ± 1. The **ring of quadratic integers** defined as $\mathscr{O} = \mathscr{O}_{\mathbb{Q}(\sqrt{d})} = \mathbb{Z}[\omega] = \{a + b\,[\omega\,] \mid a, b \in \mathbb{Z}\}$ where*

$$\omega = \begin{cases} \sqrt{d} \;\; \textit{if} \;\; d \equiv 2, 3 \; \textit{mod} \; 4 \\ \frac{1+\sqrt{d}}{2} \;\; \textit{if} \;\; d \equiv 1 \; \textit{mod} \; 4 \end{cases}$$

is contained in the quadratic field $\mathbb{Q}(\sqrt{d})$.

We will refer to these rings as either of type $\mathbb{Z}\left[\sqrt{d}\right]$ when $d \equiv 2, 3 \bmod 4$ or $\mathbb{Z}\,[\omega]$ when $d \equiv 1 \bmod 4$. When $d \equiv 1 \bmod 4$, there are quadratic integers that are not included in $\mathbb{Z}\left[\sqrt{d}\right]$. However, when $d \equiv 2, 3 \bmod 4$, then $\mathbb{Z}\left[\sqrt{d}\right]$ is the domain of all quadratic integers in the quadratic field $\mathbb{Q}(\sqrt{d})$.

Example 26 *When $d = -3$, $\mathbb{Z}[\omega]$ is denoted as $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}] = \{a + b\,[\omega] \mid a, b \in \mathbb{Z}\}$. This quadratic integer ring includes all of the integers (let $b = 0$), plus a subset of the quadratic field $\mathbb{Q}(\sqrt{-3})$. So, $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$ is similar to a field extension in abstract algebra, except that $\mathbb{Z}$ is a Euclidean Domain not a field (since all elements do not have multiplicative inverses).*

The elements of the quadratic integer ring $\mathscr{O}$ contained in the quadratic field $\mathbb{Q}(\sqrt{d})$ have many analogous properties to the euclidean domain $\mathbb{Z}$ contained in the field $\mathbb{Q}$. This leads us to the main objective of this paper through the following theorem.

Theorem 8 *Let t be an algebraic number and R the domain of all algebraic integers in $\mathbb{Q}(t)$. Then **every proper ideal in R is the unique product of prime ideals.***

(We will give a proof of this theorem later in the paper). We will look at the domain $\mathbb{Z}\left[\sqrt{-5}\,\right]$ to illustrate this theorem. Specifically, we will take the element 6 which cannot be factored uniquely in $\mathbb{Z}\left[\sqrt{-5}\,\right]$ and show that we can instead decompose the principal ideal (6) into a unique product of prime ideals in $\mathbb{Z}\left[\sqrt{-5}\,\right]$.

Definition 25 *Let* d *be a square-free integer. For* $a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$*, the* ***field norm*** *is defined as:*

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

Definition 26 *Let* d *be a square-free integer. For* $a + b\omega \in \mathscr{O}$*, the* ***quadratic integer norm*** *is defined as:*

$$N(a + b\omega) = (a + b\omega)(a + b\bar{\omega}) = \begin{cases} a^2 - db^2, \text{ if } d \equiv 2, 3 \text{ mod } 4 \\ a^2 + ab + \frac{1-d}{4}b^2, \text{ if } d \equiv 1 \text{ mod } 4 \end{cases}$$

where

$$\bar{\omega} = \begin{cases} -\sqrt{d}, \text{ if } d \equiv 2, 3 \text{ mod } 4 \\ \frac{1-\sqrt{d}}{2}, \text{ if } d \equiv 1 \text{ mod } 4. \end{cases}$$

Note that the quadratic integer norm is the same as the field norm when $d \equiv 2, 3 \bmod 4$. We use the quadratic integer norm since elements in $\mathscr{O}$ are contained inside the field extension $\mathbb{Q}(\sqrt{d})$. We look at the quadratic integer ring $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$ where $d = -3$ to illustrate the quadratic integer norm.

Example 27 *Let* $d = -3$ *and let* $\rho = \frac{-1+\sqrt{-3}}{2} = -1 + \frac{1+\sqrt{-3}}{2} \in \mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$*. The norm*

$$\begin{aligned} N(\rho) &= (-1 + (\frac{1+\sqrt{-3}}{2}))(-1 + (\frac{1-\sqrt{-3}}{2})) \\ &= 1 - (\frac{1-\sqrt{-3}}{2}) - (\frac{1+\sqrt{-3}}{2}) + (\frac{1+\sqrt{-3}}{2})(\frac{1-\sqrt{-3}}{2}) \\ &= 1 - \frac{1}{2} + \frac{\sqrt{-3}}{2} - \frac{1}{2} - \frac{\sqrt{-3}}{2} + \frac{1}{4} - \frac{\sqrt{-3}}{4} + \frac{\sqrt{-3}}{4} - \frac{-3}{4} \\ &= 1 \end{aligned}$$

We will focus on norms of the quadradic integer rings $\mathbb{Z}\left[\sqrt{d}\right]$ where the norm is a function $N : \mathbb{Z}\left[\sqrt{d}\right] \to \mathbb{Z}$ defined as

$$N(s + t\sqrt{d}) = (s + t\sqrt{d})(s - t\sqrt{d}) = s^2 - t^2 d.$$

Many norms are multiplicative, that is $N(ab) \leqslant N(a)N(b)$. However, for the quadratic integer norm, we have a stronger condition which is useful for proving and disproving properties within certain integral domains.

Theorem 9 *Let* d *be a square-free integer. For all* $a, b \in \mathbb{Z}\left[\sqrt{d}\right]$,

1. $N(a) = 0$ *if and only if* $a = 0$.
2. $N(ab) = N(a)N(b)$.

We will use this multiplicative property of norms in our upcoming proofs.

Theorem 10 *Let* d *be a square-free integer. Then* $u \in \mathbb{Z}\left[\sqrt{d}\right]$ *is a unit if and only if* $N(u) = \pm 1$.

We say that a nonzero element has *minimum norm* if $N(u) = \pm 1$. Of course not every quadratic integer ring has the same number of units. Just because an element is a unit in one ring, does not guarantee it is a unit in other rings.

Example 28 *Units in* $\mathbb{Z}[i] = \mathbb{Z}\left[\sqrt{-1}\right]$, *the Gaussian Integers, are* ± 1 *and* $\pm i$ *since*

$$N(1) = N(1 + 0\sqrt{-1}) = (1 + 0\sqrt{-1})(1 - 0\sqrt{-1}) = \boldsymbol{1}$$

$$N(i) = N(0 + \sqrt{-1}) = (0 + \sqrt{-1})(0 - \sqrt{-1}) = \boldsymbol{1}$$

Example 29 *In the complex quadratic integer ring* $\mathbb{Z}\left[\sqrt{-5}\right] = \left\{a + b\left[\sqrt{-5}\right] \mid a, b \in \mathbb{Z}\right\}$, *the only units are* ± 1.

Example 30 *In the ring* $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$ *(when* $d = -3 \equiv 1$ *mod* 4*), the units* u *have norm* $N(u) = \pm 1$*. The units of* $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$ *are* $\pm 1, \pm\rho, \pm\rho^2$*, where* $\rho = \frac{-1+\sqrt{-3}}{2}$*.*

So the ring $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$ has a finite number of units which are very different in form than the units in the Guassian Integers.

Example 31 *When* $d < 0$*, (except for* $d = -1, -3$*), the only units of* $\mathbb{Z}\left[\sqrt{d}\,\right]$ *are* ± 1*.*

Example 32 *[3, p230] and [5, p191] When* $d > 0$*, the quadratic integer rings* $\mathscr{O} = \mathbb{Z}\left[\sqrt{d}\,\right]$ *have infinitely many units. There exists a unit* $u > 1$ *such that every unit is of the form* $\pm u^m$ *for* $m \in \mathbb{Z}$*.*

The mathematician H.G. Stark [2, p1] showed that when $d < 0$, there are exactly nine quadratic integer rings $\mathbb{Z}[\omega]$ which are Unique Factorization Domains (UFDs). These occur when $d = \{-1, -2, -3, -7, -11, -19, -43, -67, -163\}$. It is interesting to note that $-1 \equiv 3$ mod 4 and $-2 \equiv 2$ mod 4, but all other values of d are $d \equiv 1$ mod 4. Stark stated that when the class number $h_{\mathscr{O}} = 1$ of the quadratic integer ring $\mathscr{O}_{\mathbb{Q}(\sqrt{d})}$ for $d \leqslant -19$, then $d \equiv 19$ mod 24. The only values of d between 1 and 200 are $19, 43, 67, 139, 163$. However, he rules out the case when $d = -139$, since two nonequivalent quadratic equations can have the same discriminant.

So, when $d = -5$, we prove that the integral domain $\mathbb{Z}\left[\sqrt{-5}\,\right]$ is not a UFD since factorization of individual elements is *not unique*.

Example 33 *Consider the element* $6 = 6 + 0\sqrt{-5} \in \mathbb{Z}\left[\sqrt{-5}\,\right]$*. It is easy to see that*

$$6 = 2 \times 3 \qquad \textit{and that}$$
$$6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

where $2, 3, (1 + \sqrt{-5}), (1 - \sqrt{-5})$ *are irreducible in* $\mathbb{Z}\left[\sqrt{-5}\,\right]$*. Thus we cannot get a unique factorization using the elements in* $\mathbb{Z}\left[\sqrt{-5}\,\right]$*.*

So, the *quadratic integer ring* $\mathbb{Z}\left[\sqrt{-5}\,\right]$ is not a Unique Factorization Domain. We will use this particular quadratic integer ring as an example in what follows.

Domains can also fail to be UFDs if factorization is not even possible, as illustrated earlier in the integral domain $\mathbb{Q}_{\mathbb{Z}}[x]$.

In $\mathbb{Z}\left[\sqrt{-5}\,\right]$, $1+\sqrt{-5}$ is irreducible even though it does not look similar to other prime numbers such as 2 and 3. We use the norm defined on $\mathscr{O}$ to show that $1+\sqrt{-5}$ is irreducible. Suppose for the sake of contradiction that $(1+\sqrt{-5})$ *is* reducible in $\mathbb{Z}\left[\sqrt{-5}\,\right]$. Then $(1+\sqrt{-5}) = ab$ for some a, b in $\mathbb{Z}\left[\sqrt{-5}\,\right]$. (We show that either a or b is a unit). By the properties of norms of elements of $\mathbb{Z}\left[\sqrt{d}\right]$, where d is a square-free integer, the norm of a product is equal to the product of the norm. That is

$$N(ab) = N(a)N(b) = N(1+\sqrt{-5}) = (1+\sqrt{-5})(1-\sqrt{-5}) = 6.$$

This means (without loss of generality) possible norms for the element a are $1, 2, 3$, or 6 (positive integer factors of 6). Let $a = s + t\sqrt{-5}$. If $N(a) = 2$, then $2 = (s+t\sqrt{-5})(s - t\sqrt{-5}) = s^2 + 5t^2$ but there are no integers s, t that satisfy that, so $N(a) \neq 2$. If $N(a) = 3$, then $3 = s^2 + 5t^2$ but again, there are no integers s, t that will work, so $N(a) \neq 3$. This leaves $N(a) = 1$ which means a is a unit. Or $N(a) = 6$ and $N(b) = 1$ which means b is a unit. Thus $(1+\sqrt{-5})$ is **irreducible** in $\mathbb{Z}\left[\sqrt{-5}\,\right]$.

This leads us to the question: is there some other notion of **unique** factorization in $\mathbb{Z}\left[\sqrt{-5}\,\right]$ that does not involve the individual elements? Gauss proved that $\mathbb{Z}[i]$ is a UFD (where i is a complex fourth root of 1) and developed the Law of Biquadratic Reciprocity to find solutions to $x^4 \equiv c \bmod 4$ if they exist. Kummer thought since i is a complex fourth root of 1, perhaps other theorems for congruences of modulo p might exist in the integral domain

$$\mathbb{Z}[\theta] = \left\{a_0 + a_1\theta + a_2\theta^2 + \ldots a_{p-1}\theta^{p-1} | a_i \in \mathbb{Z}\right\}$$

where $\theta = \cos\left(\frac{2\pi}{p}\right) + i\sin\left(\frac{2\pi}{p}\right)$ is a complex pth root of 1. However, he found that since $\mathbb{Z}[\theta]$ was not necessarily a UFD, these theorem attempts failed. Kummer did eventually discover what he called *ideal numbers* d for which $\mathbb{Z}\left[\sqrt{d}\,\right]$ is a UFD. These ideal numbers became the basis for the modern abstract algebra term *ideals*.

We saw that (2) and (3) are prime ideals in $\mathbb{Z}$. In fact, the prime ideals in $\mathbb{Z}$ are the ideals generated by the prime numbers in $\mathbb{Z}$. These ideals are also principal ideals in $\mathbb{Z}$. We now look at the principal ideal (6) in the integral domain $\mathbb{Z}\left[\sqrt{-5}\,\right]$. If (6) is indeed a prime ideal in $\mathbb{Z}\left[\sqrt{-5}\,\right]$, then our work is done.

Example 34 *Consider* $(6) = \left\{6a \mid a \in \mathbb{Z}\left[\sqrt{-5}\,\right]\right\}$, *the principal ideal generated by* 6, *in* $\mathbb{Z}\left[\sqrt{-5}\,\right]$. *Note that* $6 \in (6)$ *and* $6 = 2 \times 3$, *but* $2 \notin (6)$ *and* $3 \notin (6)$. *So,* (6) *is NOT a prime ideal in* $\mathbb{Z}\left[\sqrt{-5}\,\right]$.

Since (6) is not a prime ideal in $\mathbb{Z}$ and since $\mathbb{Z} \subseteq \mathbb{Z}\left[\sqrt{-5}\,\right]$, it follows that (6) would also not be prime in $\mathbb{Z}\left[\sqrt{-5}\,\right]$. That is, the ideal property of *not prime* carries up. We now want to show that in $\mathbb{Z}\left[\sqrt{-5}\,\right]$, the ideal (6) can be written as a product of prime ideals. We first try the obvious approach of factoring (6) into the product of the ideals $(2) = \left\{2a \mid a \in \mathbb{Z}\left[\sqrt{-5}\,\right]\right\}$ and $(3) = \left\{3a \mid a \in \mathbb{Z}\left[\sqrt{-5}\,\right]\right\}$. We prove that $(6) = (2)(3)$ in $\mathbb{Z}\left[\sqrt{-5}\,\right]$.

Proof 2 $(\Rightarrow)$ *Suppose* $x \in (6) = \left\{6a \mid a \in \mathbb{Z}\left[\sqrt{-5}\,\right]\right\}$. *Then* $x = 6(r + s\sqrt{-5})$ *for some* $r, s \in \mathbb{Z}$. *And* $x = 2(3(r + s\sqrt{-5}) \in (2)(3)$. *Thus* $(6) \subseteq (2)(3)$.

$(\Leftarrow)$*Now suppose* $x \in (2)(3)$. *Then* $x = a_1b_1 + \ldots + a_nb_n$ *where* $a_i \in (2)$ *and* $b_i \in (3)$. *Then*

$$x = 2(r_1 + s_1\sqrt{-5})3(r_1' + s_1'\sqrt{-5}) + \ldots + 2(r_n + s_n\sqrt{-5})3(r_n' + s_n'\sqrt{-5})$$

which implies

$$x = 6[(r_1 + s_1\sqrt{-5}\,)(r_1' + s_1'\sqrt{-5}) + \ldots + (r_n + s_n\sqrt{-5})(r_n' + s_n'\sqrt{-5})]$$

And $x = 6(r + s\sqrt{-5}) \in (6)$. *Thus* $(2)(3) \subseteq (6)$. *Therefore,* $(6) = (2)(3)$.

Now we must determine if the ideal (2) and (3) are prime ideals in $\mathbb{Z}\left[\sqrt{-5}\,\right]$. If they are indeed prime, our work is done.

Example 35 *We saw that* $6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ *and* $6 \in (2)$, *but neither* $(1 + \sqrt{-5})$ *nor* $(1-\sqrt{-5})$ *are in* (2). *So,* (2) *is not a prime ideal in* $\mathbb{Z}\left[\sqrt{-5}\,\right]$. *Similarly,* $6 \in (3)$, *but* $(1+\sqrt{-5})$ *and* $(1 - \sqrt{-5}) \notin (3)$. *So,* (3) *is not a prime ideal in* $\mathbb{Z}\left[\sqrt{-5}\,\right]$ *either.*

Once again, we have not found the prime ideals we were hoping to find as the factors of (6). This illustrates that properties of an ideal depend upon the specific ring in which the ideal is being viewed.

We now look at generating ideals from two *irreducible* elements, 2 and $(1 + \sqrt{-5})$ in the domain $\mathbb{Z}\left[\sqrt{-5}\,\right]$. Let $P_1 = (2, 1 + \sqrt{-5})$, $P_1 = \left\{2a + (1 + \sqrt{-5})b \mid a, b \in \mathbb{Z}\left[\sqrt{-5}\,\right]\right\}$. We now prove that an element $r+s\sqrt{-5} \in P_1$ ***if and only if*** r, s are both even or both odd.

Proof 3 $(\Rightarrow)$ *Suppose* $r+s\sqrt{-5} \in P_1 = (2, 1+\sqrt{-5}) = \left\{2a + (1 + \sqrt{-5})b \mid a, b \in \mathbb{Z}\left[\sqrt{-5}\,\right]\right\}$. *Then*

$$\begin{aligned} r + s\sqrt{-5} &= 2(a_1 + a_2\sqrt{-5} + (1 + \sqrt{-5})(b_1 + b_2\sqrt{-5}) \\ &= 2a_1 + 2a_2\sqrt{-5} + b_1 + b_2\sqrt{-5} + b_1\sqrt{-5} - 5b_2 \\ &= (2a_1 + b_1 - 5b_2) + (2a_2 + b_1 + b_2)\sqrt{-5} \end{aligned}$$

let $m = (2a_1 + b_1 - 5b_2)$ *and let* $n = (2a_2 + b_1 + b_2)$. *Then*

$$\begin{aligned} m - n &= (2a_1 + b_1 - 5b_2) - (2a_2 + b_1 - b_2) \\ &= 2a_1 + b_1 - 5b_2 - 2a_2 - b_1 - b_2 \\ &= 2a_1 - 2a_2 - 6b_2 \\ &= 2(a_1 - a_2 - 3b_2) \\ &= 2k \qquad\qquad \textit{let} \quad k = (a_1 - a_2 - 3b_2) \end{aligned}$$

Then $m - n = 2k \Rightarrow 2|(m - n) \Rightarrow m \equiv n(\ mod\ 2)$ *which means* m, n *are either both odd or both even.*

Case(i)

Suppose m, n *are both even. Then* $m = (2a_1 + b_1 - 5b_2) = 2x$ *and* $n = (2a_2 + b_1 + b_2) = 2y$ *for some* $x, y \in \mathbb{Z}$. *Then*

$$\begin{aligned} r + s\sqrt{-5} &= 2x + 2y\sqrt{-5} \\ r + s\sqrt{-5} - 2y\sqrt{-5} &= 2x \\ r - (2y - s)\sqrt{-5} &= 2x \end{aligned}$$

Letting $s = 2y - s$, *then* $r - s = 2x \Rightarrow 2|(r - s) \Rightarrow r \equiv s(\ mod\ 2)$.

Case(ii)

Suppose m, n *are both odd. Then* $m = (2a_1 + b_1 - 5b_2) = 2x + 1$ *and* $n = (2a_2 + b_1 + b_2) = 2y + 1$

for some $x, y \in \mathbb{Z}$. *Then*

$$\begin{aligned} r + s\sqrt{-5} &= (2x+1) + (2y+1)\sqrt{-5} \\ &= 2x + 1 + 2y\sqrt{-5} + \sqrt{-5} \\ r + s\sqrt{-5} - 2y\sqrt{-5} - 1 - \sqrt{-5} &= 2x \\ r - 1 + (s - 2y - 1)\sqrt{-5} &= 2x \\ (r-1) - (2y - s + 1)\sqrt{-5} &= 2x \end{aligned}$$

Letting $r = r - 1$ *and* $s = (2y - s + 1)$, *then* $r - s = 2x \Rightarrow 2|(r - s) \Rightarrow r \equiv s(\ mod\ 2)$.
Thus $r + s\sqrt{-5} \in P_1 \Rightarrow r \equiv s(\ mod\ 2)$.

($\Leftarrow$) *Suppose* $r + s\sqrt{-5} \in \mathbb{Z}\left[\sqrt{-5}\,\right]$ *and* $r \equiv s(\ mod\ 2)$. *Then either* r, s *are both even or both odd. Case(i) Suppose* r, s *are both even. Then*

$$\begin{aligned} r + s\sqrt{-5} &= 2m + 2n\sqrt{-5} \quad \textit{for some} \quad m, n \in \mathbb{Z} \\ &= 2(m + n\sqrt{-5}) \in P_1 \qquad\qquad (\textit{let} \quad b = 0). \end{aligned}$$

Then $r + s\sqrt{-5} \in P_1$.

Case(ii) Suppose r, s *are both odd. Then*

$$\begin{aligned} r + s\sqrt{-5} &= (2m+1) + (2n+1)\sqrt{-5} \quad \textit{for some} \quad m, n \in \mathbb{Z} \\ &= 2m + 1 + 2n\sqrt{-5} + 1 + \sqrt{-5} \\ &= 2m + 2n\sqrt{-5} + 1 + \sqrt{-5} \\ &= 2(m + n\sqrt{-5} + (1 + \sqrt{-5}) \in P_1 \qquad\qquad (\textit{let} \quad b = 0). \end{aligned}$$

Then $r + s\sqrt{-5} \in P_1$. *In both cases,* $r + s\sqrt{-5} \in P_1$. *Thus* $r \equiv s(\ mod\ 2) \Rightarrow r + s\sqrt{-5} \in P_1$.
Therefore, $r + s\sqrt{-5} \in P_1$ ***iff*** r, s *are both even or both odd.*

Then the quotient ring $\mathbb{Z}\left[\sqrt{-5}\,\right]/P_1$ has only two cosets: $0 + P_1$ (all of P_1) and $1 + P_1$ (what is left, that is $(r + 1) \equiv s(\bmod 2)$ implies $2|(r - s + 1)$). Thus $\mathbb{Z}\left[\sqrt{-5}\,\right]/P_1$ is isomorphic to the field $\mathbb{Z}/2\mathbb{Z}$,

$$\mathbb{Z}\left[\sqrt{-5}\,\right]/P_1 \cong \mathbb{Z}/2\mathbb{Z}$$

When we start with a commutative ring with unity (here we have an integral domain $\mathbb{Z}\left[\sqrt{-5}\,\right]$ and mod out by an ideal P_1 resulting in a field $\mathbb{Z}/2\mathbb{Z}$, then our ideal P_1 is a **maximal** ideal in the integral domain that we started with $\mathbb{Z}\left[\sqrt{-5}\,\right]$. Since fields are integral domains (with extra properties), then the maximal ideal is also a **prime** ideal. We have finally found one prime ideal, P_1, and will use this ideal to start building a product of prime ideals with the goal of factoring (6) completely. We now show that $P_1P_1 = P_1^2 = (2)$

Proof 4 $(\Rightarrow)$

Suppose $r + s\sqrt{-5} \in P_1^2 = \left\{(2a + (1 + \sqrt{-5})b)(2a + (1 + \sqrt{-5})b) \mid a, b \in \mathbb{Z}\left[\sqrt{-5}\,\right]\right\}$ *is the ideal in* $\mathbb{Z}\left[\sqrt{-5}\,\right]$. *Then*

$$
\begin{aligned}
r + s\sqrt{-5} &= \left(2a + (1+\sqrt{-5})b\right)\left(2a + (1+\sqrt{-5})b\right) \in P_1^2 \textit{ for some } a, b \in \mathbb{Z}\left[\sqrt{-5}\,\right] \\
&= 4a^2 + 4ab\left(1+\sqrt{-5}\right) + b^2\left(2\sqrt{-5} - 4\right) \\
&= 4a^2 + 4ab\left(1+\sqrt{-5}\right) + 2b^2\left(\sqrt{-5} - 2\right) \\
&= 2\left[2a^2 + 2ab\left(1+\sqrt{-5}\right) + b^2\left(\sqrt{-5} - 2\right)\right] \\
&\qquad \left(\textit{let } a = a_1 + a_2\sqrt{-5} \textit{ and } b = b_1 + b_2\sqrt{-5} \textit{ where } a_1, a_2, b_1, b_2 \in \mathbb{Z}\right) \\
&= 2\left[2(a_1 + a_2\sqrt{-5})(a_1 + a_2\sqrt{-5}) + 2(a_1 + a_2\sqrt{-5})(b_1 + b_2\sqrt{-5})(1+\sqrt{-5})\right. \\
&\qquad \left. +(b_1 + b_2\sqrt{-5})(b_1 + b_2\sqrt{-5})(\sqrt{-5} - 2)\right] \\
&= 2\left[2(a_1^2 + 2a_2\sqrt{-5} - 5a_2^2) + 2(a_1b_1 + a_1b_2\sqrt{-5} + a_2b_1\sqrt{-5} - 5a_2b_2)(1+\sqrt{-5})\right. \\
&\qquad \left. +(b_1^2 + 2b_2\sqrt{-5} - 5b_2^2)(\sqrt{-5} - 2)\right] \\
&= 2\left[\underbrace{2a_1^2 - 10a_2^2 + 2a_1b_1 - 10a_2b_2 - 10a_1b_2 - 10a_2b_1 - 10b_2 - 2b_1^2 + 10b_2^2}_{c_1}\right. \\
&\qquad \left. + \underbrace{(4a_2 + 2a_1b_2 + 2a_2b_1 + 2a_1b_1 - 10a_2b_2 - 10b_2 + b_1^2 - 5b_2^2)}_{c_2}\sqrt{-5}\right] \\
r + s\sqrt{-5} &= 2(c_1 + c_2\sqrt{-5}) \in (2) = \left\{2c \mid c \in \mathbb{Z}\left[\sqrt{-5}\,\right]\right\}.
\end{aligned}
$$

Then $r + s\sqrt{-5} \in (2)$. *Thus* $P_1^2 \subseteq (2)$.

($\Leftarrow$)*Suppose* $r + s\sqrt{-5} \in (2) = \left\{2c \mid c \in \mathbb{Z}\left[\sqrt{-5}\,\right]\right\}$. *Then* $r + s\sqrt{-5} = 2(a + b\sqrt{-5})$ *for some* $a, b \in \mathbb{Z}\left[\sqrt{-5}\,\right]$ *and* $r + s\sqrt{-5} = 2a + 2b\sqrt{-5}$. *Equating integers, we have* $r = 2a$ *and* $s = 2b$ *which means* r, s *are both even. This means that* $r + s\sqrt{-5} \in P_1 = \left(2, 1+\sqrt{-5}\right)$. *Since* $P_1 \subseteq P_1^2$ *by construction, then* $r + s\sqrt{-5} \in P_1^2$. *Thus* $(2) \subseteq P_1^2$. *Therefore,* $(2) = P_1^2$.

We found one of the prime ideals P_1 that make up the decomposition of (6). Since $(2)(3) = (6)$, it makes sense to try to form another prime ideal from two more irreducible elements of $\mathbb{Z}\left[\sqrt{-5}\right]$ which are also factors of 6, 3 and $(1+\sqrt{-5})$. Let $P_2 = (3, 1+\sqrt{-5}) = \left\{3a + (1+\sqrt{-5})b \mid a, b \in \mathbb{Z}\left[\sqrt{-5}\right]\right\}$. To ensure that P_2 is a prime ideal in $\mathbb{Z}\left[\sqrt{-5}\right]$, we

prove that the quotient ring $\mathbb{Z}\left[\sqrt{-5}\right]/P_2$ is isomorphic to the field $\mathbb{Z}/3\mathbb{Z}$ by showing that it only has three distinct cosets. We use a similar tactic as above, by showing that an element $s + r\sqrt{-5} \in P_2$ ***iff*** $r \equiv s \mod 3$.

Proof 5 ($\Rightarrow$)*Suppose* $s + r\sqrt{-5} \in P_2 = \left\{3a + (1+\sqrt{-5})b \mid a, b \in \mathbb{Z}\left[\sqrt{-5}\right]\right\}$. *Then*

$$\begin{aligned} s + r\sqrt{-5} &= 3(a_1 + a_2\sqrt{-5}) + (1+\sqrt{-5})(b_1 + b_2\sqrt{-5}) \\ &= 3a_1 + 3a_2\sqrt{-5} + b_1 + b_2\sqrt{-5} + b_1\sqrt{-5} - 5b_2 \\ &= \underbrace{(3a_1 + b_1 - 5b_2)}_{r} + \underbrace{(3a_2 + b_2 + b_1)}_{s}\sqrt{-5} \end{aligned}$$

Equating integers we have $r = 3a_1 + b_1 - 5b_2$ *and* $s = 3a_2 + b_2 + b_1$. *Subtracting* s *from* r *we have*

$$\begin{aligned} r - s &= 3a_1 + b_1 - 5b_2 - (3a_2 + b_2 + b_1) \\ &= 3a_1 + b_1 - 5b_2 - 3a_2 - b_2 - b_1) \\ &= 3a_1 - 3a_2 - 6b_2 \\ &= 3(a_1 - a_2 - 2b_2) \\ &= 3k \qquad\qquad (\textit{let } k = a_1 - a_2 - 2b_2) \end{aligned}$$

Then $r - s = 3k$ *means* $3|(r-s)$. *Thus* $r \equiv s \mod 3$. ($\Leftarrow$)*Suppose that* $r \equiv s \pmod 3$. *Then* $(r-s) = 3k$ *for some* $k \in \mathbb{Z}$. *Then* $r = 3k + s$. *Substituting, we have*

$$\begin{aligned} s + r\sqrt{-5} &= (3k+3) + s\sqrt{-5} \\ &= 3k + (1+\sqrt{-5})s \in P_2. \end{aligned}$$

Thus $s + r\sqrt{-5} \in P_2$. *Therefore* $s + r\sqrt{-5} \in P_2$ ***iff*** $r \equiv s \mod 3$.

We claim that $\mathbb{Z}\left[\sqrt{-5}\right]/P_2$ has exactly three distinct cosets, $0 + P_2$, $1 + P_2$ and $2 + P_2$. We know that elements of P_2 must be divisible by three, since an element $r + s\sqrt{-5} \in P_2$

when $r \equiv s \mod 3$. So, if $r \not\equiv s \mod 3$, then $3 \nmid (r-s)$. Then either $3|(r-s+1)$ (meaning an element $r + s\sqrt{-5} \in 1 + P_2$) or $3|(r-s+2)$ (meaning an element $r + s\sqrt{-5} \in 2 + P_2$). Thus the quotient ring $\mathbb{Z}\left[\sqrt{-5}\right]/P_2$ can be partitioned into three distinct cosets: $0 + P_2$, $1 + P_2$ and $2 + P_2$. We use this information and the First Isomorphism Theorem for Rings to prove that $\mathbb{Z}\left[\sqrt{-5}\right]/P_2 \cong \mathbb{Z}/3\mathbb{Z}$ and therefore the ideal P_2 is a prime ideal in $\mathbb{Z}\left[\sqrt{-5}\right]$.

Proof 6 *Let* $P_2 = (3, 1+\sqrt{-5}) = \left\{3a + (1+\sqrt{-5})b \mid a, b \in \mathbb{Z}\left[\sqrt{-5}\right]\right\}$. *Then* $3 \mid (r-2)$ $\Rightarrow r - s = 3k$ *for some* $k \in \mathbb{Z}$. *Define the ring homomorphism* $\phi : \mathbb{Z}\left[\sqrt{-5}\right] \to \mathbb{Z}/3\mathbb{Z}$ *as* $\phi(r + s\sqrt{-5}) = (r + s\sqrt{-5})/P_2$. *Then*

$$\begin{aligned}
\textit{ker}\ \phi &= \left\{r + s\sqrt{-5} \in \mathbb{Z}\left[\sqrt{-5}\right] \mid \phi(r + s\sqrt{-5}) = 0\right\} \\
&= \left\{r + s\sqrt{-5} \in \mathbb{Z}\left[\sqrt{-5}\right] \mid (r + s\sqrt{-5})/P_2 = 0\right\} \\
&= \left\{r + s\sqrt{-5} \in \mathbb{Z}\left[\sqrt{-5}\right] \mid 3a + (1+\sqrt{-5})b \mid a, b \in \mathbb{Z}\left[\sqrt{-5}\right]\right\} \\
&= P_2
\end{aligned}$$

(That is, the elements of P_2 *when modded out by* P_2 *equals* 0*). By the First Isomorphism Theorem for Rings,*

$$\mathbb{Z}\left[\sqrt{-5}\right]/P_2 \cong \mathbb{Z}/3\mathbb{Z}.$$

Since every field is also an integral domain, the field $\mathbb{Z}/3\mathbb{Z}$ *is an integral domain. This implies that the ideal* P_2 *is a prime ideal in* $\mathbb{Z}\left[\sqrt{-5}\right]$.

Similary, let $P_3 = \left\{3a + (1-\sqrt{-5})b \mid a, b \in \mathbb{Z}\left[\sqrt{-5}\right]\right\}$. Then $\mathbb{Z}\left[\sqrt{-5}\right]/P_3$ also has three cosets: $0 + P_3, 1 + P_3, 2 + P_3$, thus

$$\mathbb{Z}\left[\sqrt{-5}\right]/P_3 \cong \mathbb{Z}/3\mathbb{Z}$$

So, P_3 is a *prime* ideal in $\mathbb{Z}\left[\sqrt{-5}\right]$. We have found two more prime ideals in the decomposition of (6) in $\mathbb{Z}\left[\sqrt{-5}\right]$. Now we confirm that $P_2P_3 = (3)$.

Proof 7 *Let* $P_2 = (3, 1+\sqrt{-5}) = \left\{3a + (1+\sqrt{-5})b \mid a, b \in \mathbb{Z}\left[\sqrt{-5}\right]\right\}$ *and* $P_3 = \left\{3a + (1-\sqrt{-5})b \mid a, b \in \mathbb{Z}\left[\sqrt{-5}\,\right]\right\}$. ($\Rightarrow$) *Let* $r + s\sqrt{-5} \in P_2P_3$. *Then*

$$\begin{aligned}
r + s\sqrt{-5} &= (3a + (1+\sqrt{-5})b)(3c + (1-\sqrt{-5})d) \text{ for some } a, b, c, d \in \mathbb{Z}\left[\sqrt{-5}\right] \\
&= 9ac + 3ad(1-\sqrt{-5}) + 3bc(1+\sqrt{-5} + bd(1+\sqrt{-5})(1-\sqrt{-5}) \\
&= 9ac + 3ad(1-\sqrt{-5}) + 3bc(1+\sqrt{-5} + bd(1-\sqrt{-5}+\sqrt{-5}+5) \\
&= 9ac + 3ad(1-\sqrt{-5}) + 3bc(1+\sqrt{-5} + 6bd \\
&= 3\left(3ac + ad(1-\sqrt{-5}) + bc(1+\sqrt{-5}) + 2bd\right) \\
&= 3\left(3ac + ad - ad\sqrt{-5} + bc + bc\sqrt{-5} + 2bd\right) \\
&= 3\left((\underbrace{3ac + ad + bc + 2bd}_{m}) + (\underbrace{bc - ad}_{n})\sqrt{-5}\right) \\
&= 3\left(m + n\sqrt{-5}\right) \\
&= 3\left((m_1 + m_2\sqrt{-5}) + (n_1 + n_2\sqrt{-5})\sqrt{-5}\right) \qquad \left(\text{since } m, n \in \mathbb{Z}\left[\sqrt{-5}\,\right]\right) \\
&= 3\left(m_1 + m_2\sqrt{-5} + n_1\sqrt{-5} - 5n_2\right) \\
&= 3\left((m_1 - 5n_2) + (m_2 + n_1)\sqrt{-5}\right) \in (3).
\end{aligned}$$

Thus $P_2P_3 \subseteq (3)$. ($\Leftarrow$) *Let* $r + s\sqrt{-5} \in (3) = \left\{3a \mid a \in \mathbb{Z}\left[\sqrt{-5}\,\right]\right\}$. *Then* $r + s\sqrt{-5} = 3(a + b\sqrt{-5}) = 3a + 3b\sqrt{-5}$ *for some* $a, b \in \mathbb{Z}$. *Equating integers, we have* $r = 3a$ *and* $s = 3b$. *Then* $r - s = 3z - 3b = 3(a-b) = 3k$ (*let* $k = a - b$). *This means that* $3 \mid (r - s)$ *and* $r \equiv s (mod\ 3)$ *and* $r + s\sqrt{-5} \in P_2$. *Since* $P_2 \subseteq P_2P_3$ *by construction, then* $r + s\sqrt{-5} \in P_2P_3$. *Thus* $(3) \subseteq P_2P_3$. *Therefore,* $P_2P_3 = (3)$.

We have shown that (3) can be decomposed into the product of the two prime ideals P_2 and P_3. $(3) = P_2P_3$ where $P_2 = (3, 1+\sqrt{-5})$ and $P_3 = (3, 1-\sqrt{-5})$. We also showed that $(2) = P_1P_1 = P^2$ where $P_1 = (2, 1+\sqrt{-5})$. Now we can express (6) as a product of four **prime** ideals in $\mathbb{Z}\left[\sqrt{-5}\,\right]$:

$$(6) = (2)(3) = P_1^2P_2P_3$$

We have shown that in the integral domain $\mathbb{Z}\left[\sqrt{-5}\right]$, which lacks unique factorization of individual elements, that it is possible to factor the ideal (6) into the unique product of prime ideals

$$(6) = P_1^2 P_2 P_3.$$

This *prime ideal factorization* resembles the prime factorization that we are familiar with in the integers and is the next best thing to prime factorization in integral domains that are not Unique Factorization Domains. This is possible in any quadratic integer ring. R. Dedekind developed theory that generalized this prime factorization of ideals based on Kummer's ideal numbers. The following two lemmas will be necessary to prove his result.

Lemma 1 *[5, p176] Let* R *be an algebraic integer ring. For any ideal* A *in* R*, the quotient ring* R/A *is finite.*

Lemma 2 *[5, p179] If* A *and* B *are ideals such that* $B \supset A$*, then there exists an ideal* C *such that* $A = BC$*.*

Theorem 11 *Let* t *be an algebraic number and* R *the domain of all algebraic integers in* $\mathbb{Q}(t)$*. Then* ***every proper ideal in*** R ***is the unique product of prime ideals.***

A complete proof of this theorem can be found in Ireland and Rosen's *A Classical Introduction to Modern Number Theory* [5, p174]. We will prove the first part of the theorem that every ideal can be written as a product of prime ideals.

Proof 8 *[5, p180] Let* A *be a proper ideal in the quadratic integer ring* $\mathbb{Z}\left[\sqrt{d}\right]$*. Since* $\mathbb{Z}\left[\sqrt{d}\right]/A$ *is finite,* A *is contained in a maximal ideal* P_1 *(by Zorn's lemma, in an arbitrary commutative ring with identity a proper ideal is contained in a maximal ideal). And, we can show that* $A = P_1 B_1$ *for some ideal* B_1*. If* $B_1 \neq \mathbb{Z}\left[\sqrt{d}\right]$*, then* B_1 *is contained in a maximal ideal* P_2 *and so* $A = P_1 P_2 B_2$*. If* $B_2 \neq \mathbb{Z}\left[\sqrt{d}\right]$*, we can continue building a product of ideals. Notice that we have an ascending chain of ideals:*

$$A \subset B_1 \subset B_2 \subset \cdots$$

Since $\mathbb{Z}\left[\sqrt{d}\right]$ *is a Noetherian ring, this ascending chain of ideals terminates when* $B_t = \mathbb{Z}\left[\sqrt{d}\right]$. *Thus*

$$A = P_1 P_2 \cdots P_2.$$

In conclusion, we found there were nine negative values of d for which $\mathbb{Z}[\sqrt{d}]$ is a Unique Factorization Domain (UFD), but it is not known how many $d > 0$ exist that yield UFDs. The negative d values that yield UFD's are:

$$\{-1, -2, -3, -7, -11, -19, -43, -67, -163\}.$$

At first, there appeared to be a relationship between the d values and equivalence classes modulo 4, since all but two of the d values were $d \equiv 1 \bmod 4$. However, this turned out not to be the case.

The mathematician H. M. Stark introduced the term *class number one* and found nine values of $d < 0$ for which the complex quadratic field $\mathbb{Q}(\sqrt{d})$ has class number one:

$$\{-3, -4, -7, -8, -11, -19, -43, -67, -163\}.$$

These two sets above are the same since $\sqrt{-4} = 2\sqrt{-1}$ and $\sqrt{-8} = 4\sqrt{-2}$. This means that the quadratic fields $\mathbb{Q}(\sqrt{-4})$ and $\mathbb{Q}(\sqrt{-1})$ are the same. As are $\mathbb{Q}(\sqrt{-8})$ and $\mathbb{Q}(\sqrt{-2})$. Stark's proof of class number involves complicated factoring of high degree polynomials and modular arithmetic. It seems as if the Stark d values are *some* of the UFD d's, but not all. That is, having class number one does not guarantee unique factorization.

An alternate definition of class number involving equivalence classes of *ideals*. Integral domains with the (minimum) class number one had only *one* equivalence class of ideals and thus (by theorem) were PIDs (which implies UFD).

In conclusion, for integral domains $\mathbb{Z}\left[\sqrt{\mathrm{d}}\right]$, the following values of $\mathrm{d} < 0$ form Unique Factorization Domains:

$$\{-1, -2, -3, -7, -11, -19, -43, -67, -163\}.$$

It is an open question as to how many values of $\mathrm{d} > 0$ exist such that unique factorization holds. The first few values include:

$$\{2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 22, 23, 29, \ldots\}.$$

It is conjected that there are infinitely many UFD's for $\mathrm{d} > 0$.

Bibliography

[1] W. W. Rousse Ball *A Short Account on the History of Mathematics* 1960: Dover, NY

[2] H.M. Stark *A Complete Determination of the Complex Quadratic Fields of Class-Number One* The Michigan Mathematical Journal Volume 14, Issue 1 (1967), pages 1-27.

[3] David S. Dummit and Richard M. Foote, *Abstract Algebra, Third Edition* 2004: John Wiley and Sons, Inc., NJ.

[4] Thomas W. Hungerford *Abstract Algebra, An Introduction, Second Edition* 1990: Saunders College Publishing, Harcourt Brace College Publishers, FL.

[5] Kenneth Ireland and Michael Rosen, *A classical Introduction to Modern Number Theory, Second Edition* 1990: Springer-Verlag, NY.

[6] Pete L. Clark *Factorization in Integral Domains*, preprint 2010, University of Georgia, Athens, GA.

[7] Elijah Bunnell *Class Number One Problems* 2009, Oregon State University Masters Paper.

Vita

Susan L. Kirk received her B.S. of Landscape Architecture from Virginia Polytechnic Institute and State University. She practiced Landscape Architecture for several years before returning to her home state of Virginia. She received her M.S. in Mathematical Sciences from Virginia Commonwealth University in 2015.