Unique Factorization in the Rings of Integers of Quadratic Fields

A Method of Proof

Zachary Warren

A Senior Thesis submitted in partial fullfillment
of the requirements for graduation
in the Honors Program
Liberty University
Spring 2023

Acceptance of Senior Honors Thesis

This Senior Honors Thesis is accepted in partial
fullfillment of the requirements for graduation from the
Honors Program of Liberty University.

_____

Daniel Schmidt, Ph.D.
Thesis Chair

_____

Timothy Sprano, Ph.D.
Committee Member

_____

David E. Schweitzer, Ph.D.
Assistant Honors Director

_____

Date

Abstract

It is a well-known property of the integers, that given any nonzero $a \in \mathbb{Z}$, where a is not a unit, we are able to write a as a unique product of prime numbers. This is because the Fundamental Theorem of Arithmetic (FTA) holds in the integers and guarantees (1) that such a factorization exists and (2) that it is unique. As we look at other domains, however, specifically those of the form $\mathbb{O}(\sqrt{D}) = \{a + b\sqrt{D} \mid a, b \in \mathbb{Z},\ D \text{ a negative, squarefree integer}\}$, we find that the FTA does not always hold. For example, in the domain $\mathbb{O}(\sqrt{-5})$, $6 = 2 \cdot 3$ and $6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ are two valid factorizations of 6, with $2,\ 3,\ 1 + \sqrt{-5},\ 1 - \sqrt{-5}$ all irreducible elements in $\mathbb{O}(\sqrt{-5})$. This paper discusses the history and development of the problem of discerning which fields of the form $\mathbb{O}(\sqrt{D})$ are unique factorization domains (UFDs), and concludes by constructing a method of proving unique factorization in some domain using results concerning Euclidean domains and principal ideal domains.

Unique Factorization in the Rings of Integers of Quadratic Fields

A Method of Proof

Introduction

Overview and Statement of Purpose

The purpose of this work is to provide an investigation into the question of which quadratic fields have rings of integers that possess unique factorization. We will first trace the history and development of this question, we will then establish necessary definitions of the concepts and terms involved, and we will conclude by illustrating a process for proving unique factorization in some field $\mathbb{O}(\sqrt{D})$.

What is a Unique Factorization Domain?

Before we can begin this exploration, it is important to first answer a few preliminary questions and provide several examples to ensure a proper understanding of the topic. Firstly, we may begin with the question: What is a unique factorization domain? While a more precise definition will be provided later in this work, for now a helpful illustration of this structure can be found by simply looking at the integers.

It is a very important and well-known property of the integers that every integer that is not 0, 1, or -1 can be factored into a product of prime numbers. This fact is familiar even for middle and high-school students, who often utilize the property for problems such as finding the greatest common divisor of two integers. But while some may find it trivial or unremarkable that this is the case, the property has been deemed to be so important that the theorem which states it has merited the lofty designation “The Fundamental Theorem of Arithmetic” (FTA).

Theorem 1. *For any nonzero $x \in \mathbb{Z}$ $\exists$ irreducibles $p_1, p_2, ..., p_n \in Z$ such that $x = p_1 p_2 \cdots p_n$, and this factorization into irreducible elements is unique up to ordering.*

A proof of this theorem may be found in Rosen (2010). It may be pointed out that the FTA uses the term *irreducible* where we may be used to seeing the term *prime*. Further on, we will provide definitions that will clarify the distinction, but for now, while we are referring to the integers, we may use the terms interchangeably. Notice that the FTA guarantees two important facts about every integer. First, that a factorization of any integer into a product of irreducible elements does exist. Second, there is only one such factorization for every integer. That is, prime factorization in the integers is unique.

Are There Examples of Nonunique Factorization?

The fact that this relatively mundane observation about the integers has been assigned so much importance may cause one to wonder: Is there ever an instance where unique factorization would not be the case? To address this question, we must step outside of the integers and into the more general category of integral domains. Integral domains will be dealt with more thoroughly in following sections, but there is one example that most students have encountered at some point, the Gaussian integers. Gaussian integers are numbers that are formed by conjoining the imaginary number $i = \sqrt{-1}$ to the ordinary integers. Thus, some examples of Gaussian integers would be $1 + 2i$, $5 - 6i$, or $0 + 67i$. The Gaussian integers have many interesting qualities that make them useful in the study of mathematics, and they share many properties with the integers (including, in fact, unique factorization). Suppose, however, that we were to replace -1 in the examples above with another value, perhaps -5. We would then have formed a new integral domain which is

notated as $\mathbb{O}(\sqrt{-5}) = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$ and which contains elements such as $5 - 14\sqrt{-5}$ and $20 + 4\sqrt{-5}$. Since elements of any integral domain having this form can be referred to as *integers*, from this point on to avoid confusion we will use the term *rational integers* to refer to elements of $\mathbb{Z}$. Elements of the domain $\mathbb{O}(\sqrt{-5})$, like the rational integers, can ultimately be factored into irreducibles, but in this particular domain, it can be shown that the factorizations are not guaranteed to be unique. To demonstrate this, first note that any rational integer, such as 6, is contained within $\mathbb{O}(\sqrt{-5})$ since we could write it as $6 - 0\sqrt{-5}$. Now, we can note that $6 = 2 \cdot 3$ is a valid factorization in this domain. However, $6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ is also a factorization of 6 in $\mathbb{O}(\sqrt{-5})$. Thus, since it can be shown that 2, 3, $(1 + \sqrt{-5})$, and $(1 - \sqrt{-5})$ are all *irreducible* elements in $\mathbb{O}(\sqrt{-5})$, we can conclude that the FTA does not hold in this domain.

Is Unique or Nonunique Factorization More Common?

Now that we have demonstrated examples of domains both with and without unique factorization, one may wonder how common a phenomenon these unique factorization domains really are. Is nonunique factorization simply a rare exception, while unique factorization is the norm? Or is the converse true? This question turns out to be a fascinating one that has occupied many mathematicians' minds over the past two centuries, and this work will undertake to shed light on some of the things they have concluded.

Why Should We Care About Unique Factorization?

Before commencing an investigation into the topic of unique factorization, one closing anecdote may help to illustrate what may motivate a mathematician to devote time and attention to this issue. In 1637, renowned mathematician Pierre de Fermat recorded a note in the margins of

a book he was reading that would later become one of the most famously frustrating theorems in the history of mathematics. He stated that he had found a method of proving that there are no solutions to a certain form of equation, but noted "the margin was too narrow to contain" the proof (Gallian, 2016). After his death in 1665, the statement became known as Fermat's Last Theorem, and for hundreds of years mathematicians worked to discover what proof Fermat could have had in mind. Attempt after attempt was made to solve the problem, but each attempt was met with failure, leading some to question whether Fermat's alleged proof might have contained errors that he had failed to notice. Finally, almost 200 years after Fermat's death, a mathematician named Gabriel Lamé excitedly reported that he had finally found a proof of Fermat's Last Theorem. He presented his method at a meeting of the Paris Academy on March 1, 1847. However, it was soon pointed out that Lamé's method rested on assumptions about factorization within a certain ring of numbers, and it had only recently been proven by mathematician Ernest Kummer that in that ring, unique factorization does not hold. This unfortunately invalidated the entire proof, sending a disappointed Lamé back to the drawing board, and painfully illustrating that taking for granted the property of unique factorization in rings of integers can lead to unfortunately flawed results. Fermat's Last Theorem remained an open question for another 150 years until a solution was finally published in 1995 (Fraleigh, 2002).

Preliminaries

What is a Domain?

We will now begin by defining a few terms that will be the basis for our discussion of the issue of unique factorization. The first term we will define is the algebraic structure of a domain.

The most straightforward example of a domain may be found in the rational integers. Without backtracking too deeply into the fundamentals of algebra, we may define a domain as follows:

Definition 1. A domain R is a collection of numbers along with two operations, "addition" and "multiplication," where the following axioms hold (axioms are adapted from Weintraub, 2008):

1. If $a, b \in R$, then $a + b \in R$ also.
2. If $a, b \in R$, $a + b = b + a$.
3. If $a, b, c \in R$, $a + (b + c) = (a + b) + c$.
4. There is some element 0 in R such that for any $a \in R$, $0 + a = a + 0 = a$.
5. For every element $a \in R$ there exists some element $(-a)$ such that $a + (-a) = (-a) + a = 0$.
6. If $a, b \in R$, then $ab \in R$ also.
7. If $a, b \in R$, $ab = ba$.
8. If $a, b, c \in R$, $a(bc) = (ab)c$.
9. There is some element 1 in R such that for any $a \in R$, $1a = a1 = a$.
10. If $a, b, c \in R$, $a(b + c) = ab + ac$ and $(a + b)c = ac + bc$.
11. If $a, b \in R$ and $ab = 0$, then $a = 0$ or $b = 0$.

This last axiom establishes the fact that there are no *zero divisors* in a domain. In other words, the product of two nonzero elements of a domain will always be nonzero as well. This makes it possible to prove a very useful property of domains known as the cancellation property.

Theorem 2. *If a, b, $c \in R$ for some domain R with $a \neq 0$, and we have $ab = ac$, then we may conclude that $b = c$.*

Proof. Suppose we have $ab = bc$ with $a, b, c \in R$ and $a \neq 0$. Then we know $\exists a^{-1} \in R$, so we have $a^{-1}(ab) = a^{-1}(ac) \implies (a^{-1}a)b = (a^{-1}a)c \implies b = c$. □

As we observed above, the rational integers possess all of these properties, and they are therefore the most familiar instance of a domain. For this reason, the terms domain and integral domain are both used to describe this structure.

What is a Field?

If we were to add one more axiom to the sequence we have listed above, the result would be a slightly more restricted structure known as a field. That axiom is

1. For every nonzero element $a \in R$, there exists some element a^{-1} such that
   $a(a^{-1}) = (a^{-1})(a) = 1$.

Note that, while the rational integers do not meet the qualifications to be labeled as a field, there is another familiar set of numbers that do. The rational numbers, denoted as $\mathbb{Q} = \{\frac{a}{b} \mid a, b \in \mathbb{Z}, b \neq 0\}$, make up a field, where the multiplicative inverse of some nonzero number a is simply its reciprocal, $\frac{1}{a}$. It is the case that every integral domain can be used to construct a field that is related to the initial domain in the same way that $\mathbb{Z}$ is related to $\mathbb{Q}$

(Fraleigh, 2002). As indicated in the beginning of this work, we will be concerned with one specific kind of field, known as quadratic fields.

What is a Quadratic Field?

A quadratic field is a type of field in which every element is of the form $a + b\sqrt{D}$ where a and b are rational numbers and D is some squarefree integer, meaning that it does not possess a perfect square as any of its factors. These fields are denoted $\mathbb{Q}(\sqrt{D})$ and are known as quadratic fields because every element will be the solution to some quadratic equation of the form $a_0x^2 + a_1x + a_2 = 0$, where a_0, a_1, and a_2 are integers. Note that depending on whether or not D is a positive value, elements of a quadratic field may be either real or complex. For example, earlier it was demonstrated that 6 possessed two distinct factorizations in the field $\mathbb{Q}(\sqrt{-5})$, which would be an imaginary quadratic field, or complex quadratic field. However, the field $\mathbb{Q}(\sqrt{7})$ would be an example of a real quadratic field.

What is a Ring of Integers?

Note that this paper is not concerned directly with quadratic fields, but with their rings of integers. The ring of integers of some quadratic field $\mathbb{Q}(\sqrt{D})$ is denoted by $\mathbb{O}(\sqrt{D})$, and it will be related to $\mathbb{Q}(\sqrt{D})$ in the same way that the rational integers are related to the rational numbers.

Definition 2. The ring of integers of some quadratic field $\mathbb{Q}(\sqrt{D})$ is $\mathbb{O}(\sqrt{D}) = \{a + b\sqrt{D} \mid a, b \in \mathbb{Z}\}$ if $D \equiv 2$ or $3 \pmod 4$ and $\mathbb{O}(\sqrt{D}) = \{\frac{a+b\sqrt{D}}{2} \mid a, b \in \mathbb{Z}$ and a, b are both even or both odd$\}$ if $D \equiv 1 \pmod 4$ (Weintraub, 2008).

Explaining the rationale for the modular portion of this definition would require a significant detour into the theory of algebraic integers, so, for the purpose of this work, we will

accept it without justification. However, a detailed explanation can be found in Hardy and Wright's (1979) *An Introduction to the Theory of Numbers*.

Just as we may find prime factorizations for rational integers, we can find analogous factorizations for the ring of integers of any quadratic field. However, now that we are dealing with more general cases, it will be helpful to explicitly define what we mean by the terms *factoring* and *unique factorization* in these domains.

What is Factorization?

Every student will be familiar with the process of finding prime factorizations in the rational integers. The process involves beginning with a number and breaking it down into its factors until we are left only with a set of prime numbers that are not able to be broken down any farther. This problem is simple enough to be taught to students in middle school. However, when we begin dealing with other integral domains, a few questions arise that require us to define some of our terms carefully. For example, what does it mean for a number in the domain $\mathbb{O}(\sqrt{-3})$ to be prime? The purpose of this section will be to establish enough of a description of factorization to be helpful for the following proofs and discussions, but not to give an exhaustive investigation into the methods or process of finding factorizations.

The following definitions may be used for any general integral domain R (adapted from Weintraub, 2008):

Definition 3. Given two elements $\alpha, \beta \in R$, we say α *divides* β (written $\alpha|\beta$) if there exists some $\gamma \in R$ such that $\alpha\gamma = \beta$.

Definition 4. An element $\alpha \in R$ is called a *unit* of R if there exists some element $\alpha' \in R$ such

that $\alpha(\alpha') = 1$.

(Note that by the definitions given above, this means that α' is a multiplicative inverse of α. Thus another definition of a field is an integral domain in which every element is a unit).

Definition 5. Two elements $\alpha_1, \alpha_2 \in R$ are called *associates* if $(\alpha_1)\beta = (\alpha_2)$ for some unit $\beta \in R$.

Definition 6. An element $\alpha \in R$ is called *irreducible* in R if $\alpha = \beta\gamma$ implies that β or γ is a unit.

Definition 7. An element $\alpha \in R$ is called a *prime* in R if $\alpha|\beta\gamma$ implies $\alpha|\beta$ or $\alpha|\gamma$.

To demonstrate the process of factorization in some ring of integers $\mathbb{O}(\sqrt{D})$, we will first make an observation from the rational integers. When we say that elements of $\mathbb{Z}$ may be factored into a unique product of primes, we must note that there are a couple of qualifications on this statement. For example, if we were to begin with the integer 10, a valid factorization would be $(2)(5)$. However, $(-2)(-5)$ would be another perfectly valid factorization, as would $(1)(-1)(-1)(5)(2)$. We may recognize that all of these factorizations are essentially the same, but it is still obvious that they are at least different in form, so what exactly do we mean when we talk of the unique factorization of rational integers? Notice that all of the factorizations listed above only differ in the order in which factors are listed and by the number of times the factors (1) and (-1) appear. Also, notice that from definition (2) above, 1 and -1 are the only elements of the integers that can be called units (since $1(1) = (-1)(-1) = 1$). Thus when we say that the rational integers may be factored into a unique product of prime factors, we really mean the factorizations are unique up to multiplication by a unit. Thus, when working within a different integral domain, we must note which elements are units in that domain.

History

Gauss' Introduction of the Class Number One Problem

The problem that this thesis is concerned with has come to be known as the Gauss class number one problem. This is because the question of which quadratic fields contain rings of integers that may be broken into unique factorizations of irreducibles was first formulated by Carl Friedrich Gauss in 1801. Gauss was a German mathematician born in 1777 in Brunswick, Germany (Gray, 2022). He showed incredible ability in mathematics from a very young age, and began making significant contributions to his field beginning at the age of 15 (Gray, 2022). Over the course of his lifetime he made novel discoveries in number theory, astronomy, geometry, geodesy, and other areas that continue to make a significant impact on the progression of the study of mathematics to this day. In 1801, he published an impressive work in Latin entitled *Disquisitiones Arithmeticae* (Mathematical Inquiries). In articles 303-305 of this publication, Gauss is concerned with the problem of finding the class number of some algebraic number field K, that is, the order of the quotient group $(J_K)/(P_K)$, where J_K is the group of fractional ideals of K and P_K is its subgroup of principal ideals (Gauss, 1801). So if a field has class number one, the order of its quotient group $(J_K)/(P_K)$ must be one, so the groups J_K and P_K must be isomorphic to each other. It has been shown that the problem of finding the quadratic fields $\mathbb{Q}(\sqrt{D})$ that have class number one, and the problem of determining which quadratic fields $\mathbb{Q}(\sqrt{D})$ possess unique factorization are equivalent.

Gauss provided a list of nine negative values of D such that $\mathbb{Q}(\sqrt{D})$ has class number one (and thus unique factorization), namely $-1, -2, -3, -7, -11, -19, -43, -67, -163$. He

speculated without proof that this comprised a complete list. However, it was not until much later that this speculation could be proved. He also asserted that it was likely that as D approached negative infinity, the class number of $\mathbb{Q}(\sqrt{D})$ approaches infinity, and that there were possibly an infinite number of positive values for D such that $\mathbb{Q}(\sqrt{D})$ would possess unique factorization.

Hans Heilbronn's Work on the Problem

These speculations of Gauss remained conjectures for more than a century. However, in a 1934 publication entitled *On the Class Number in Imaginary Quadratic Fields*, a mathematician by the name of Hans Heilbronn was able to prove Gauss' conjecture that for any class number h, there are only finitely many fields of the form $\mathbb{Q}(\sqrt{D})$, where D is a negative squarefree integer, such that the class number of $\mathbb{Q}(\sqrt{D}) = h$. This implied that even if Gauss had not been able to list all values of D that result in unique factorization for $\mathbb{O}(\sqrt{D})$, his list only required a finite number of additions to become complete. In the same year, Heilbronn, working together with mathematician Edward Linfoot, was able to demonstrate that there was at most one number that Gauss had missed in his possible solution of the class number one problem. This discovery represented significant headway into the problem, but the question of whether or not Gauss' list was complete remained a mystery that Heilbronn ultimately did not solve.

Kurt Heegner's Work on the Problem

In 1952, the problem was picked back up by a radio engineer named Kurt Heegner who worked with mathematical problems as a hobby (Propp, 2019). In an article titled *Diophantische Analysis und Modulfunktionen* (Diophantine Analysis and Modular Functions), Heegner (1952) claimed to prove that Gauss' list was, in fact, complete. Consequently, there were no other

quadratic fields whose domains of integers would have unique factorization. At the time of its publication, though, it was thought that Heegner's proof contained holes and was incomplete.

Harold Stark's Work on the Problem

Finally in 1963, the problem was settled decisively by Harold Stark and Alan Baker, who determined conclusively that Heegner's conclusion had been correct, that there could be no tenth value for D such that $\mathbb{Q}(\sqrt{D})$ had class number one (Stark, 1967). Stark and Baker were working on the problem independently, but they found their separate solutions the same year. Stark then undertook to show that Heegner's proof needed only to have a couple of holes filled in order to be a completely valid proof (Stark, 1969).

Coining of the Term Heegner Number

In *The Book of Numbers*, published in 1996, authors John Horton Conway and Richard K. Guy were the first to refer to these nine numbers which yielded quadratic fields with class number one as *Heegner Numbers* (Conway & Guy, 1996). This designation has come to be widely used, even though, as one author notes ironically, "naming this set after Heegner is like naming a species not after the naturalist who discovered them, but after the scientist who declared the species extinct!" (Propp, 2019, p. 20).

Proofs

Overview of Section

At this point, we have established the groundwork that is necessary to trace a method through which one might prove that $\mathbb{O}(\sqrt{D})$ is a unique factorization domain for some squarefree integer D. Detailing this method will involve several steps. First, we will give the definition of

two different types of domains, Euclidean domains and principal ideal domains. Once we have established the definitions, we will be able to supply a proof that every Euclidean domain is a principal ideal domain. We will then undertake to prove that every principal ideal domain is a unique factorization domain. Thus, once we have finished these proofs, we will have reduced the task of proving that $\mathbb{O}(\sqrt{D})$ is a unique factorization domain to the task of proving that it is a Euclidean domain. We will conclude by illustrating this process using $\mathbb{O}(\sqrt{-1})$, the Gaussian integers.

Definitions

Euclidean Domain

Roughly speaking, a Euclidean domain is one in which we can always divide one element by another and end up with a quotient and a remainder that is either 0 or strictly less than the divisor. Note that, however, if we are dealing with any domain outside of the rational integers, it quickly becomes apparent that the usual sense of "greater than" and "less than" may no longer carry meaning. For example, what does it mean to say $\rho < \beta$ if $\rho = 3 + 4i$ and $\beta = 6 - 2i$? Thus, in whatever domain we are working with we must establish a definition of what it means for some elements in the domain to be "greater than" or "less than" others. To supply this definition, we will use the mathematical concept of a norm. The first two properties come from Weintraub (2008), the third is commonly used in the definition of a norm.

Definition 8. "Let R be an integral domain. Then N is a norm on R if:

1. for every nonzero element α of R, $N(\alpha)$ is a nonnegative integer;

2. for every two nonzero elements α and β of R, $N(\alpha) \leq N(\alpha\beta)$" (p. 20);

3. $N(\alpha) = 0$ if and only if $\alpha = 0$.

Thus a norm is simply a mapping from a domain R into the nonnegative integers. So to compare the "size" of two different elements of R, we simply compare the norm of each element using the familiar definitions of $<$ and $>$.

Note that we can find an example of a norm by looking at the absolute value function on the rational integers.

Theorem 3. *The absolute value function is a norm on* $\mathbb{Z}$.

Proof. The absolute value function is defined as

$$|x| = \begin{cases} x & x \geq 0 \\ -x & x < 0 \end{cases}$$

. We can clearly see that if we input any element of $\mathbb{Z}$ the output will be a nonnegative integer. To demonstrate the second condition, we will take advantage of the fact that $|ab| = |a||b|$. Let a and b be two nonzero integers, then $|ab| = |a||b| = |a|z$ for some $z \in \mathbb{Z}^+$. So

$$|a||b| = |a|z \geq |a|$$

□

To show that a domain R is a Euclidean domain, one must first define a norm N on R and then demonstrate that given any two elements α and β of R, there exist elements γ and ρ such that $\alpha = \beta\gamma + \rho$ where $\rho = 0$ or $0 < N(\rho) < N(\beta)$. This gives us the following definition of a Euclidean domain.

Definition 9. We say a domain R, along with some norm N, is a Euclidean domain if, given any two elements α and β in R with $\beta \neq 0$, one can write that $\alpha = \beta\gamma + \rho$ for some elements γ and ρ in R where $\rho = 0$ or $0 < N(\rho) < N(\beta)$.

Principal Ideal Domain

To begin our discussion of the second type of domain we will be concerned with, we must first define the algebraic term of an ideal. Gallian (2016) gives the following definition of an ideal.

Definition 10. "A subring A of a ring R is called a (two-sided) ideal of R if for every r in R and every a in A both ra and ar are in A" (p. 249).

Put slightly differently, a collection A of elements of R is an ideal if it is closed under addition, and if it is closed under multiplication by any element of R.

A helpful example can be found once again in the rational integers. If we let $R = \mathbb{Z}_{40}$, the set of all nonnegative integers less than 40, we may show that the set A of all multiples of 5 less than 40 makes up an ideal of R under addition modulo 40. To show this, we first note that A is closed under addition modulo 40 we have $5x_1 + 5x_2 = 5(x_1 + x_2) = 5y$, where $x_1, x_2 \in R$ and $y = x_1 + x_2$. Also, we can see that A is closed under multiplication by any element of R, since, for any r in R and any $a = 5x$ in A, we have $ra = r(5x) = 5(rx)$. Thus A is an ideal of the domain $\mathbb{Z}_{40}$.

Notice that by the same argument shown above, the set of all multiples of 3 would also be an ideal. So, in fact, would the set of multiples of any number in $\mathbb{Z}$. This is true in general, that is, the set A of multiples of any element α of a domain R forms an ideal of R. The proof of this statement would look identical to the proof above that the set of all multiples of 5 is an ideal.

If A is an ideal of R containing only the multiples of some element α, we say that A is a *principal* ideal, *generated by* α, and we write $A = \langle\alpha\rangle$. Thus $\langle 5\rangle = \{0, 5, 10, 15, ..., 35\}$ and $\langle 8\rangle = \{0, 8, 16, 24, 32\}$ would be principal ideals of $\mathbb{Z}_{40}$. At this point, it would possibly be helpful to demonstrate from the rational integers an example of a non-principal ideal, one that is not simply generated by a single element. However, this turns out to be impossible, since there is actually no such ideal in $\mathbb{Z}$ (Fraleigh, 2002). If we were to choose a different domain, such as $\mathbb{O}(\sqrt{-3})$, we could show an example of a non-principal ideal, but that does not lie within the scope of this work.

In fact, this observation about the integers gives the opportunity to introduce a vital new definition.

Definition 11. A domain R is a called a *principal ideal domain* (or PID) if every ideal A in R contains some element α such that A is generated by α.

Now that we have this definition, we may restate our observation about the rational integers in the following theorem.

Theorem 4. *The integers are a principal ideal domain.*

It will be helpful to briefly note that we have now observed that the rational integers are both a Euclidean domain and a principal ideal domain. Over the next few steps, we will demonstrate that it will always be the case that, if R is a Euclidean domain, R will also be a PID.

Unique Factorization Domain

Recall from earlier definitions that we say that an element $\alpha \in R$ is a *unit* if there exists some $\alpha^{-1} \in R$ such that $\alpha(\alpha^{-1}) = 1$. We call two element $\alpha, \beta \in R$ *associates* if $\alpha = \beta\varepsilon$ where ε is some unit in R. Additionally, we call an element $\pi \in R$ an irreducible in R if for $\pi = \alpha\beta$ implies that either α or β is a unit (Gallian, 2016). Finally, we must give a formal definition of a unique factorization domain, or UFD.

Definition 12. A domain D is called a unique factorization domain if the fundamental theorem of arithmetic holds in D. That is, it satisfies the following two conditions:

1. "Every element of D that is neither 0 nor a unit can be factored into a product of a finite number of irreducibles.

2. "If $\pi_1 \cdots \pi_r$ and $\rho_1 \cdots \rho_s$ are two factorizations of the same element of D into irreducibles, then $r = s$ and the ρ_j can be renumbered so that π_i and ρ_i are associates" (Gallian, 2016, p. 312).

Proof That Every Euclidean Domain is a PID

Now that we have formally stated all of the necessary definitions, we will begin to prove that every Euclidean domain is a UFD. We will begin with the following theorem.

Theorem 5. *Every Euclidean domain is a PID.*

Proof. Suppose R is a Euclidean domain with norm N, and let A be an ideal in R such that $A \neq \{0\}$. We define $N(A) = \{N(\alpha) \mid \alpha \in A\}$. By the well-ordering principle, there exists some element $k \in \mathbb{Z}$ such that k is the least element in $N(A)$. Let α be an element in A such that

$N(\alpha) = k$. Then consider an arbitrary element $\kappa \in A$. Since R is a Euclidean domain, $\exists \gamma, \rho \in R$ such that $\kappa = \alpha\gamma + \rho$ with $\rho = 0$ or $0 < N(\rho) < N(\alpha)$. Suppose $\rho \neq 0$. Then note that $\rho = \kappa - \alpha\gamma$. Since A is an ideal, and $\alpha \in A$, $\kappa - \alpha\gamma = \rho \in A$. But then we have $\rho \in A$ with $0 < N(\rho) < N(\alpha)$ which contradicts the fact that $N(\alpha)$ was the least element of $N(A)$. Thus we must have $\rho = 0$, so $\kappa = \alpha\gamma$ for an arbitrary $\kappa \in A$, and therefore $A = \langle\alpha\rangle$. □

Proof That Every PID is a Unique Factorization Domain

Recall that to prove some domain R is a UFD we must show it satisfies two conditions:

1. For any nonzero element of R that is not a unit, a factorization into a finite number of irreducibles exists, and

2. This factorization into irreducibles is essentially unique.

Proof of the Existence of a Factorization

We will first prove that every PID satisfies the first condition. We will begin with a lemma demonstrating that in a PID R, if $A_1, A_2, A_3, ...$ is an arbitrary, possibly infinite, collection of ideals with $A_1 \subseteq A_2 \subseteq A_3 \subseteq \cdots$, then the union $A = A_1 \cup A_2 \cup A_3 \cup \cdots$ is also an ideal.

Lemma 1. *If R is a PID and $A_1 \subseteq A_2 \subseteq A_3 \subseteq \cdots$ with $A_1, A_2, A_3, ...$ ideals in R, the union of $A_1, A_2, A_3, ...$ is also an ideal.*

Proof. Let $A_1, A_2, A_3, ...$ be ideals in a PID R, and suppose $A_1 \subseteq A_2 \subseteq A_3 \subseteq \cdots$. Let $A = A_1 \cup A_2 \cup A_3 \cup \cdots$. Suppose $\alpha, \beta \in A$. Then, $\alpha \in A_i$ and $\beta \in A_j$ for some $i, j \in \mathbb{Z}$, and we may suppose without loss of generality that $0 < i \leq j$. Now $A_i \subseteq A_j$, since $i \leq j$, so we have $\alpha + \beta \in A_j$, which implies that $\alpha + \beta \in A$. Also, given $\alpha \in A$, the fact that α is in some ideal A_i

implies that $\alpha\varepsilon \in A_i$ for all $\varepsilon \in R$, so $\alpha\varepsilon \in A$ for all $\varepsilon \in R$. Thus $A = A_1 \cup A_2 \cup A_3 \cup \cdots$ is an ideal. □

This proof enables us to prove another result for PIDs known as the Ascending Chain Condition, or ACC. Suppose we have $A_1 \subset A_2 \subset \cdots$, for ideals $A_1, A_2, ...$ in R, a PID. We now claim that this chain can only have a finite number of ideals.

Lemma 2. *Any ascending chain of ideals in a PID R contains a finite number of ideals.*

Proof. Let $A_1 \subset A_2 \subset \cdots$ be an ascending chain of ideals in a PID R. First observe from above that $A = A_1 \cup A_2 \cup \cdots$ is an ideal. Since R is a PID, there exists some $\gamma \in R$ such that A is generated by γ, that is $A = \langle\gamma\rangle$. Since $A = A_1 \cup A_2 \cup \cdots$, we know that $\gamma \in A_i$ for some $i \in \mathbf{Z}^+$, so every element of $\langle\gamma\rangle$ will also be in A_i, giving us $\langle\gamma\rangle \subseteq A_i \subseteq A = \langle\gamma\rangle$. Therefore, there exists some $i \in \mathbb{Z}^+$ such that $A_i = A$, where A is the union of all the ideals in the chain, so the chain of strictly ascending ideals must terminate at or before i. □

Finally, having proved these two results, we may now prove the following

Lemma 3. *Given any element $\alpha \in R$, a PID, there exists a factorization of α into irreducibles.*

Proof. We first prove that given any element $\alpha \in R$, α has at least one irreducible factor. If α is an irreducible then we are done, so we suppose not. Then $\alpha = \alpha_1\beta_1$ for some $\alpha_1, \beta_1 \in R$ with neither α_1 nor β_1 a unit. Thus $\langle\alpha\rangle \subset \langle\alpha_1\rangle$. If we assume α_1 is not an irreducible, then $\alpha_1 = \alpha_2\beta_2$ for some $\alpha_2, \beta_2 \in R$ with neither α_2 nor β_2 a unit. So $\langle\alpha\rangle \subset \langle\alpha_1\rangle \subset \langle\alpha_2\rangle$. We observe that if we continue this procedure, we will gain a chain of strictly ascending ideals. Thus, by ACC, there must exist some α_n such that $\langle\alpha\rangle \subset \langle\alpha_1\rangle \subset \langle\alpha_2\rangle \cdots \subset \langle\alpha_n\rangle$, where $\langle\alpha_n\rangle$ is the last ideal in the

chain. If α_n is not an irreducible, then we could write $\alpha_n = \alpha_{n+1}\beta_{n+1}$, hence $\langle\alpha\rangle \subset \langle\alpha_1\rangle \subset \langle\alpha_2\rangle \cdots \subset \langle\alpha_n\rangle \subset \langle\alpha_{n+1}\rangle$. This clearly contradicts the fact that $\langle\alpha_n\rangle$ is the last ideal in the chain, so α_n must be an irreducible (Gallian, 2016).

Now, given any $\alpha \in R$, we know that we can write $\alpha = \pi_1\beta_1$ where π_1 is an irreducible. Now consider β_1. If β_1 is not an irreducible, then we know from above that we can write $\beta_1 = \pi_2\beta_3$ where π_2 is an irreducible. So we have $\langle\alpha\rangle \subset \langle\beta_1\rangle \subset \langle\beta_2\rangle$. If this procedure continues, we can again see that we will gain a chain of strictly ascending ideals, so by the same reasoning as we used above, there must exist some β_m such that $\langle\alpha\rangle \subset \langle\beta_1\rangle \subset \langle\beta_2\rangle \cdots \subset \langle\beta_m\rangle$, where $\langle\beta_m\rangle$ is the last ideal in the chain. Again, if β_m is not an irreducible, then we could write $\beta_m = \pi_{n+1}\beta_{n+1}$, hence $\langle\alpha\rangle \subset \langle\beta_1\rangle \subset \langle\beta_2\rangle \cdots \subset \langle\beta_m\rangle \subset \langle\beta_{m+1}\rangle$. Therefore, β_m is an irreducible, and we may write $\alpha = \pi_1\pi_2 \cdots \beta_m$ where each factor of α is an irreducible (Gallian, 2016). □

Proof of the Uniqueness of a Factorization

Finally, we must prove the following result.

Lemma 4. *Any factorization of an element α into irreducibles in a PID is unique.*

Proof. Suppose that $\alpha = \pi_1\pi_2 \cdots \pi_r$ and $\alpha = \rho_1\rho_2 \cdots \rho_s$ are two factorizations of $\alpha \in R$, a PID, into irreducibles. We must show that it is possible to reorder the ρ_j such that $\pi_i = \rho_i$ or π_i and ρ_i are associates, that is $\pi_i = \rho_i\varepsilon$ for some unit $\varepsilon \in R$. Then we will see that the factorizations are unique up to multiplication by a unit. First, note that we have $\alpha = \pi_1\pi_2 \cdots \pi_r = \rho_1\rho_2 \cdots \rho_s$. So we have $\pi_1|(\rho_1\rho_2 \cdots \rho_s)$. At this point, we must state without proving that any irreducible element in a PID R is also a prime element in R (Gallian, 2016). Thus, by the definition of a prime, $\pi_1|(\rho_1\rho_2 \cdots \rho_s)$ implies that $\pi_1|\rho_i$ for some $i \in \mathbb{Z}, 0 < i \leq s$. Therefore, we have that

$\rho_i = \pi_1\varepsilon_1$ for some $\varepsilon_1 \in R$, and ε_1 must be a unit, since we have assumed ρ_i is an irreducible for every ρ_i. This gives us $\pi_1\pi_2 \cdots \pi_r = (\varepsilon_1\pi_1)\rho_1\rho_2 \cdots \rho_{i-1}\rho_{i+1} \cdots \rho_s$. Since R is a domain, we may cancel and gain $\pi_2 \cdots \pi_r = (\varepsilon_1)\rho_1\rho_2 \cdots \rho_{i-1}\rho_{i+1} \cdots \rho_s$. Now we can continue this process, observing that $\pi_2|(\varepsilon_1\rho_1\rho_2 \cdots \rho_{i-1}\rho_{i+1} \cdots \rho_s)$.

We may suppose without loss of generality that $r \leq s$. So, once we have completed this r times, we will have $1 = (\varepsilon_1\varepsilon_2 \cdots \varepsilon_r)\rho_{r+1}\rho_{r+2} \cdots \rho_s$. But then we $\rho_i|1$ for each ρ_i where $r < i < s$, so each remaining ρ_i is by definition a unit. However, this contradicts our assumption that each ρ_i was an irreducible, so we must have $r = s$. Therefore, we have shown that we must have $\pi_1\pi_2 \cdots \pi_r = \rho_1\rho_2 \cdots \rho_r$ where each $\rho_i = \pi_i\varepsilon_i$ for some unit ε_i. Therefore, factorizations into irreducibles in a PID are unique (Gallian, 2016). □

Combining the previous two theorems we obtain:

Theorem 6. *Every PID is a UFD.*

Demonstrating Uniqueness of Factorization in $\mathbb{O}(\sqrt{D})$

At this point, we have completed a set of proofs that lead us to the following conclusion.

Theorem 7. *For any domain R, if R is Euclidean, then it is a UFD.*

Thus, one possible way of proving that the FTA holds in the nine fields $\mathbb{O}(\sqrt{-1})$, $\mathbb{O}(\sqrt{-2})$, $\mathbb{O}(\sqrt{-3})$, $\mathbb{O}(\sqrt{-7})$, $\mathbb{O}(\sqrt{-11})$, $\mathbb{O}(\sqrt{-19})$, $\mathbb{O}(\sqrt{-43})$, $\mathbb{O}(\sqrt{-67})$, and $\mathbb{O}(\sqrt{-163})$ is to identify a valid norm for each domain and describe a method for satisfying the division algorithm given any two elements from the domain. Interestingly, though, this cannot be done for all nine of these fields. It has been demonstrated that there are some negative values of D for which $\mathbb{O}(\sqrt{D})$

is a UFD but is not a Euclidean domain. Thus, being a Euclidean domain is a sufficient condition for being a UFD, but it is not a necessary condition (Hardy & Wright, 1979).

However, we will conclude this work by demonstrating that, using the results we have obtained at this point, we may prove that $\mathbb{O}(\sqrt{-1})$ and $\mathbb{O}(\sqrt{-2})$ are Euclidean domains and thus UFDs. With slight modifications, the same method could be used to demonstrate the same for $\mathbb{O}(\sqrt{-3})$, $\mathbb{O}(\sqrt{-7})$, and $\mathbb{O}(\sqrt{-11})$.

We begin by considering $\mathbb{O}(\sqrt{D})$ for a negative, squarefree value of D with $D \equiv 2, 3 \pmod 4$. Recall that by definition 2, elements of such domains are of the form $\mathbb{O}(\sqrt{D}) = \{a + b\sqrt{D} \mid a, b \in \mathbb{Z}\}$. Suppose we define the mapping N on $\mathbb{O}(\sqrt{D})$ by

$$N(a + b\sqrt{D}) = (a + b\sqrt{D})(a - b\sqrt{D}) = a^2 - Db^2$$

We will prove that N is a norm on $\mathbb{O}(\sqrt{D})$ after proving the following helpful result.

Theorem 8. *If $\alpha = a + b\sqrt{D}$ and $\beta = c + d\sqrt{D}$ for some $a,\ b,\ c,\ d \in \mathbb{Z}$ then $N(\alpha\beta) = N(\alpha)N(\beta)$.*

Proof. $N(\alpha\beta) = N((a + b\sqrt{D})(c + d\sqrt{D})) = N((ac + bdD) + (ad + bc)\sqrt{D}) =$

$(ac + Dbd)^2 - D(ad + bc)^2 = a^2c^2 - Da^2d^2 + D^2b^2d^2 - Db^2c^2 =$

$a^2(c^2 - Dd^2) - Db^2(c^2 - Dd^2) = (a^2 - Db^2)(c^2 - Dd^2) = N(\alpha)N(\beta)$ □

Theorem 9. *N is a norm on $\mathbb{O}(\sqrt{D})$.*

Proof. First, note that since $x^2 \geq 0\ \forall x \in \mathbb{Z}$, we have $\forall \alpha \in \mathbb{O}(\sqrt{D}),\ N(\alpha) \geq 0$. Now suppose $\alpha, \beta \in \mathbb{O}(\sqrt{D})$ with $\alpha = a + b\sqrt{D}, \beta = c + d\sqrt{D} \neq 0$ for some $a, b, c, d \in \mathbb{Z}$. So

$$N(\alpha\beta) = N(\alpha)N(\beta) = (a^2 - Db^2)(c^2 - Dd^2)$$

Since $D < 0$, and since $(c^2 - Dd^2) \in \mathbb{Z}$ with $c,\ b$ not both zero, we have $N(\alpha\beta) \geq N(\alpha)$. Finally, note that $N(0) = 0$. Therefore N satisfies every necessary condition of a norm. □

Having now defined a norm for this domain, we must prove the following theorem.

Theorem 10. *Given any two elements $\alpha, \beta \in \mathbb{O}(\sqrt{-1}), \beta \neq 0$, there exists $\gamma, \rho \in \mathbb{O}(\sqrt{-1})$ such that $\alpha = \beta\gamma + \rho$ with $0 \leq N(\rho) < N(\beta)$.*

Proof. First consider $\frac{\alpha}{\beta} \in \mathbb{Q}(\sqrt{-1})$ defined as

$$\frac{a + b\sqrt{-1}}{c + d\sqrt{-1}} = \frac{(a + b\sqrt{-1})(c - d\sqrt{-1})}{(c + d\sqrt{-1})(c - d\sqrt{-1})} = \frac{ac + bd}{c^2 + d^2} + \frac{bc - ad}{c^2 + d^2}\sqrt{-1} = x + y\sqrt{-1}$$

for some $x, y \in \mathbb{Q}$. We choose $r, s \in \mathbb{Z}$ such that $|x - r| \leq \frac{1}{2}$ and $|y - s| \leq \frac{1}{2}$, and we let $\gamma = r + s\sqrt{-1}$. Finally, we let $m = (x - r)$, $n = (y - s)$.

Now consider $\rho = \alpha - \beta\gamma$. Note that ρ is in $\mathbb{O}(\sqrt{-1})$ by closure, and

$$\rho = \beta(\frac{\alpha}{\beta} - \gamma) = \beta((x + y\sqrt{-1}) - (r + s\sqrt{-1})) = \beta(m + n\sqrt{-1})$$

Thus it follows that

$$N(\rho) = N(\beta(m + n\sqrt{-1})) = N(\beta)N(m + n\sqrt{-1}) = N(\beta)(m^2 - Dn^2) \leq N(\beta)(\frac{1}{4} - \frac{D}{4})$$

. So if $D = -1$ or $D = -2$, we have $\alpha = \beta\gamma + \rho$ with $\rho = 0$ or $0 < N(\rho) < N(\beta)$. □

Conclusion

It will be helpful now to review what we have proven in this work. We began by defining all of the necessary terms to understand the nature of rings of integers of quadratic fields. We observed that not all domains of the form $\mathbb{O}(\sqrt{D})$ have unique factorization. We then claimed that we would begin a series of proofs that could reduce the problem of proving $\mathbb{O}(\sqrt{D})$ was a UFD, to the problem of proving it was a Euclidean domain. After defining all relevant terms, we first proved that all Euclidean domains are PIDs by showing that any ideal in a Euclidean domain is generated by the element in the ideal whose norm has the smallest value. We then used the properties of ideals to demonstrate that every element in a PID possesses a unique factorization into irreducibles. Thus every Euclidean domain is a PID, and every PID is a UFD. We concluded by using these proofs to demonstrate that $\mathbb{O}(\sqrt{D})$ is a UFD for $D = -1$ and $D = -2$, and we observed that a similar method could be used to show that this is also the case for $D \in \{-3, -7, -11\}$.

References

Chan, W. K. (2013). *Diophantine methods, lattices, and arithmetic theory of quadratic forms*. American Mathematical Society.

Cohen, H. (1993). *A course in computational algebraic number theory*. Springer.

Conway, J., & Guy, R. (1996). *The book of numbers*. Copernicus.

Coykendall, J., & Smith, W. W. (2011). On unique factorization domains. *Journal of Algebra*, *332*(1), 62–70. https://doi.org/10.1016/j.jalgebra.2010.10.024

Fraleigh, J. (2002). *A first course in abstract algebra* (7th ed). Pearson.

Frazer, J. (2014). *Algebraic number theory*. Springer.

Gallian, J. (2016). *Contemporary abstract algebra* (9th ed). Cengage Learning.

Gauss, C. (1801). *Disquisitiones arithmeticae*.

Goldfeld, D. (2004, June 21). The Gauss class number problem for imaginary quadratic fields. In H. Darmon & S.-w. Zhang (Eds.), *Heegner points and Rankin l-series* (1st ed., pp. 25–36). Cambridge University Press. https://doi.org/10.1017/CBO9780511756375.004

Gray, J. (2022). *Carl Friedrich Gauss. Encyclopedia Britannica*. Retrieved January 24, 2023, from https://www.britannica.com/biography/Carl-Friedrich-Gauss

Halter-Koch, F. (2008). Non-unique factorizations of algebraic integers. *Functiones et Approximatio Commentarii Mathematici*, *39*(1), 49–60. https://doi.org/10.7169/facm/1229696553

Hardy, G. H., & Wright, E. M. (1979). *An introduction to the theory of numbers* (5th ed). Oxford University Press.

Heegner, K. (1952). Diophantische analysis und modulfunktionen. *Mathematische Zeitschrift*, *56*, 227–253.

Heilbronn, H. (1934). On the class-number in imaginary quadratic fields. *The Quarterly Journal of Mathematics*, *os-5*(1), 150–160. https://doi.org/10.1093/qmath/os-5.1.150

Pollack, P., & Snyder, N. (2021). A quick route to unique factorization in quadratic orders. *The American Mathematical Monthly*, *128*(6), 554–558. https://doi.org/10.1080/00029890.2021.1898875

Propp, J. (2019). Who mourns the tenth Heegner number? *Math Horizons*, *27*(2), 18–21. https://doi.org/10.1080/10724117.2019.1648929

Rosen, K. (2010). *Elementary number theory and its application* (6th ed). Pearson.

Stark, H. M. (1967). A complete determination of the complex quadratic fields of class-number one. *Michigan Mathematical Journal*, *14*(1), 1–27. https://doi.org/10.1307/mmj/1028999653

Stark, H. M. (1969). On the "gap" in a theorem of Heegner. *Journal of Number Theory*, *1*(1), 16–27. https://doi.org/10.1016/0022-314X(69)90023-7

Stark, H. M. (2007). The Gauss class-number problems. *Clay Mathematics Proceedings*, *7*. https://www.uni-math.gwdg.de/tschinkel/gauss-dirichlet/stark.pdf

Stewart, I., & Tall, D. (2015, October 13). *Algebraic number theory and Fermat's last theorem* (4th ed.). Chapman & Hall/CRC.

Vaskouski, M., Kondratyonok, N., & Prochorov, N. (2016). Primes in quadratic unique factorization domains. *Journal of Number Theory*, *168*, 101–116. https://doi.org/10.1016/j.jnt.2016.04.022

Weintraub, S. H. (2008, May 15). *Factorization: Unique and otherwise*. A K Peters/CRC Press.

Xianke, Z. (2016). *Algebraic number theory* (2nd ed). Alpha Science International.