6-2015

Unique Prime Factorization of Ideals in the Ring of Algebraic Integers of an Imaginary Quadratic Number Field

Nolberto Rezola
California State University - San Bernardino

Unique Prime Factorization of Ideals in the Ring of Algebraic Integers of an Imaginary Quadratic Number Field

---

A Thesis

Presented to the

Faculty of

California State University,

San Bernardino

In Partial Fulfillment

of the Requirements for the Degree

Master of Arts

in

Mathematics

---

by

Nolberto Rezola

June 2015

Unique Prime Factorization of Ideals in the Ring of Algebraic Integers of an Imaginary Quadratic Number Field

---

A Thesis

Presented to the

Faculty of

California State University,

San Bernardino

---

by

Nolberto Rezola

June 2015

Approved by:

Dr. Gary Griffing, Committee Chair	Date
Dr. Paul Vicknair, Committee Member	
Dr. Zahid Hasan, Committee Member	
Dr. Charles Stanton, Chair, Department of Mathematics	Dr. Corey Dunn Graduate Coordinator, Department of Mathematics

Abstract

The ring of integers is a very interesting ring, it has the amazing property that each of its elements may be expressed uniquely, up to order, as a product of prime elements. Unfortunately, not every ring possesses this property for its elements. The work of mathematicians like Kummer and Dedekind lead to the study of a special type of ring, which we now call a Dedekind domain, where even though unique prime factorization of elements may fail, the ideals of a Dedekind domain still enjoy the property of unique prime factorization into a product of prime ideals, up to order of the factors. This thesis seeks to establish the unique prime ideal factorization of ideals in a special type of Dedekind domain: the ring of algebraic integers of an imaginary quadratic number field.

Acknowledgements

I want to thank my advisor Dr. Gary Griffing who has been very supportive and encouraging throughout this tremendous and enchanting experience.

Table of Contents

Abstract **iii**

Acknowledgements **iv**

1 Introduction **1**

2 Rings, Integral Domains, and Fields **3**

3 Integral Elements and Algebraic Elements **6**

4 The Ring of Algebraic Integers and Unique Factorization Domains **15**

5 Integral Closure **18**

6 Algebraic Integers and Lattices **21**

7 Divisibility of Ideals and Unique Prime Ideal Factorization **26**

Bibliography **32**

Chapter 1

Introduction

The notion of a prime rational integer (by rational integer we mean any element belonging to $\mathbb{Z}$) is crucial to the study of number theory. Thanks to Euclid, the notion of a prime element p may be extended to rings other than $\mathbb{Z}$ by defining a prime element in the following way: let p be an element such that $p \neq 0$ and $p \nmid 1$, p is prime if $p \mid ab$ implies that $p \mid a$ or $p \mid b$. By defining a prime element in this way and using the fact that p is a prime rational integer if and only if its only rational integer divisors are ± 1 and $\pm p$, it then follows that any element a of $\mathbb{Z}$ may be expressed uniquely as a product of rational prime integers (it will become apparent why we refer to what are commonly called integers as rational integers later). That is, we may rewrite

$$a = p_1 p_2 \cdots p_n,$$

where each p_i is a rational prime integer. Hence, we see that the ring of rational integers has the special property that each of its elements is expressible as a unique product of prime elements, up to the order of its factors and multiples of ± 1.

Many statements in mathematics have proofs which depend on the notion of unique prime factorization. An example of a problem whose proof depends on the notion of unique prime factorization is the following: 27 is the only perfect cube which is the sum of a square plus 2. This is equivalent to saying that the only integer solution to the equation

$$x^3 = y^2 + 2$$

is when $x = 3$ and $y = 5$. This observation was first mentioned by Diophantus. Euler solved this problem in 1770. Euler's proof is of particular interest because he expresses

$y^2 + 2$ as

$$y^2 + 2 = (y + \sqrt{-2})(y - \sqrt{-2})$$

and then obtains the equation

$$(y + \sqrt{-2})(y - \sqrt{-2}) = 27.$$

Euler then continues his proof by treating the factors $(y+\sqrt{-2})$ and $(y-\sqrt{-2})$ as if they were relatively prime rational integers and then makes arguments which would normally hold in the ring $\mathbb{Z}$. Euler exploits unique prime factorization in $\mathbb{Z}$ to obtain a proof. By approaching the problem from this angle, Euler managed to prove the uniqueness of the solution to the equation. How did Euler know that what he was doing was permissible?

The idea of referring to complex numbers such as $(5 - \sqrt{-2})$ and $(5 + \sqrt{-2})$ as integers may seem a bit strange since they look very distinct from the rational integers we commonly conjure in our heads when we hear the word "integer". The complex numbers $(5 - \sqrt{-2})$ and $(5 + \sqrt{-2})$ are what we call, algebraic integers. In this thesis we will study what are called imaginary quadratic number fields and their corresponding sets of integers. We will show that even though unique prime factorization for elements in the ring of integers of an imaginary quadratic number field may not always hold, the ideals of the ring of integers will always satisfy unique prime factorization.

I would like to acknowledge my use of Şaban Alaca and Kenneth S. Williams text, Introductory Algebraic Number Theory [1], Michael Artin's text, Algebra [2], Richard Dedekind's text, Theory of Algebraic Integers [3], Oscar Zariski and Pierre Samuel's text, Commutative Algebra, volume 1 [5] and the paper by Christina Jamroz titled Ideal Class Group [4]. In comparing this thesis to their texts, one will notice similar arguments for some of the results contained herein.

Chapter 2

Rings, Integral Domains, and Fields

We begin this chapter by defining two very fruitful concepts, the first concept is that of a *ring* and the second concept is that of an *ideal*. It is important that we understand and feel comfortable dealing with these abstract structures since our entire theory depends on them.

Definition 1. ***(Ring)***
A ***ring*** *is a set R with two binary operations, $+$ and $\times$ (called addition and multiplication), which statisfy the following axioms:*

(a) under addition, R is an abelian (commutative) group and we denote the identity element under addition by 0.

(b) Under multiplication, R is associative and commutative and we denote the identity element under multiplication by 1.

(c) Elements in R distribute over addition; that is, if $a, b, c \in R$, then

$$(a+b)c = ac + bc \quad \textit{and} \quad c(a+b) = ca + cb.$$

In general, a ring R is not required to have an identity element under multiplication. This means that R may or may not contain an element e such that for all a in R, the product $ae = a$. In our study of rings we will always assume that a ring R contains an

identity element under multiplication, namely $e = 1$. It should also be mentioned that in general, a ring R is not required to be commutative under multiplication (abelian under multiplication). This means that in general, if a, b are elements in R the product ab does not have to equal the product ba ($ab \neq ba$). In our study of rings we will always assume that our rings are commutative.

A *subring* S of a ring R is a subset of R which is closed under the operations of addition, subtraction, and multiplication and which contains the element 1.

Definition 2. ***(Ideal)***
An ***ideal*** *I of a ring R is a nonempty subset of R which is a subgroup under addition and whenever $a \in I$ and $r \in R$ the product $ar \in I$.*

In our next definition we define an *integral domain.* Although it may sound strange, it is possible for two nonzero elements r and s in a ring R to have a product which equals zero. When this happens we call r and s zero divisors of R. An integral domain is a ring which has no zero divisors other than zero itself.

Definition 3. ***(Integral Domain)***
A ring Δ is called an ***integral domain*** *if for all $\delta \neq 0$, $\gamma \neq 0$ in Δ the product $\delta\gamma \neq 0$.*

Theorem 4. *Let $\delta \neq 0$, γ, and α be elements of Δ. Then Δ is an integral domain if and only if $\delta\gamma = \delta\alpha$ implies $\gamma = \alpha$.*

Proof. Suppose that Δ is an integral domain and $\delta\gamma = \delta\alpha$. By subtracting $\delta\alpha$ from both sides of the equation we obtain

$$\delta\gamma - \delta\alpha = 0.$$

This implies that $\delta(\gamma - \alpha) = 0$. Since $\delta \neq 0$ and Δ is an integral domain we obtain that $\gamma - \alpha = 0$. Hence, $\gamma = \alpha$.

Conversely, suppose that whenever $\delta\gamma = \delta\alpha$ we have that $\gamma = \alpha$. Let $\delta\gamma = 0$. Since $\delta \cdot 0 = 0$ we may rewrite the equation as

$$\delta\gamma = \delta \cdot 0.$$

This then implies that $\gamma = 0$ and therfore Δ is an integral domain. □

We say that b is the multiplicative inverse of $a \neq 0$ if $ab = 1$. A ring R may or may not contain multiplicative inverses for each of its elements. If the multiplicative

inverse of an element exists then it is unique. Elements which have multiplicative inverses are called *units*.

Definition 5. ***(Unit)***
Let R be a ring and let u be a nonzero element of R. If there exists a v in R such that $uv = 1$ we say that u and v are ***units*** *of R.*

Definition 6. ***(Field)***
An integral domain Φ where each of its nonzero elements is a unit is called a ***field****.*

The following examples will help illustrate these notions.

Example 7. *Consider the ring $\mathbb{Z}$. To show that $\mathbb{Z}$ is an integral domain it suffices to show that if a and b are elements of $\mathbb{Z}$ and $ab = 0$, then $a = 0$ or $b = 0$. Suppose that $a \neq 0$, then $ab = 0 = a \cdot 0$. Since $ab = a \cdot 0$ is taking place in $\mathbb{Q}$ and $a \neq 0$ we know that there exists an a^{-1} in $\mathbb{Q}$ such that $a^{-1} \cdot a = 1$. Therefore, if we multiply both sides of the equation $ab = a \cdot 0$ by a^{-1} we obtain that $b = 0$. Hence, $\mathbb{Z}$ is an inetgral domain.*

Example 8. *Consider the ring $\mathbb{Z}_4$. This is the ring of integers modulo 4. Since 2 is an element in this ring and $2 \cdot 2 = 0$, where $2 \neq 0$ we see that $\mathbb{Z}_4$ is not an integral domain.*

Example 9. *If Δ is an integral domain then $\Delta[x]$, the ring of polynomials in x with coefficients from Δ, will also be an integral domain. This follows from the fact that if $f(x) \neq 0$ and $g(x) \neq 0$ are elements of $\Delta[x]$ the product of the leading coefficient of each polynomial will be a product of two nonzero elements of Δ and hence $f(x) \cdot g(x) \neq 0$.*

Example 10. *The sets $\mathbb{C}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{Z}_p$ where p is a prime rational integer, are fields.*

Chapter 3

Integral Elements and Algebraic Elements

The notion of an element being integral will be used extensively throughout this paper. The concept of an integral element will play an essential role in establishing the fact that the set of algebraic integers of an imaginary quadratic number field (a notion we will be talking about further along), forms an integral domain.

Next we define what it means for an element in an integral domain B to be integral over the integral domain A.

Definition 11. ***(Element Integral Over a Domain)***
Let $A \subset B$ where A and B are integral domains. The element $\beta \in B$ is said to be ***integral over*** *A if it satisfies a monic polynomial equation*

$$x^n + \alpha_{n-1}x^{n-1} + \cdots + \alpha_1 x + \alpha_0 = 0,$$

where each of the coefficients $\alpha_0, \alpha_1, ..., \alpha_{n-1}$ are elements of A.

We are now able to define the notion of an *algebraic integer*.

Definition 12. ***(Algebraic Integer)***
A complex number ω which is integral over $\mathbb{Z}$ is called an ***algebraic integer****.*

From this point on if we say "integer" we will mean algebraic integer. When referring to the elements of the set $\mathbb{Z}$ we will say "rational integers" intead of just referring

to them as "integers". We now give an example to illustrate the notion of an algebraic integer.

Example 13. *The complex number $\sqrt{2}$ is an algebraic integer since it satisfies the equation $x^2 - 2 = 0$, where the coefficients of the polynomial are rational integers.*

Next we define what it means for an element of an integral domain to be *algebraic over a field.*

Definition 14. ***(Element Algebraic Over a Field)***
Let $A \subset B$ where A and B are integral domains. Suppose that A is a field and $\beta \in B$ is integral over A; then β is said to be ***algebraic over*** *A.*

If we take $\mathbb{Q}$, the set of rational numbers, to be the set A in the definition above and the set of complex number, $\mathbb{C}$, to be the set B we obtain the following definition.

Definition 15. ***(Algebraic Number)***
A complex number that is algebraic over $\mathbb{Q}$ is called an ***algebraic number****.*

Example 16. *The complex number $\frac{1}{\sqrt{5}}$ is an algebraic number, but not an algebraic integer, as it satisfies the equation $x^2 - \frac{1}{5} = 0$ which has its coefficients in $\mathbb{Q}$ and not in $\mathbb{Z}$.*

Definition 17. ***(Domain Integral Over a Subdomain)***
Let $A \subset B$ where A and B are integral domains. If every $\beta \in B$ is integral over A we say that B is ***integral over*** *A.*

With these definitions we are prepared to prove some useful results which we will need in order to eventually prove that the set of integral elements is closed under: addition, subtraction, and multiplication.

Theorem 18. *Let $A \subset B \subset \Gamma$ where A, B, and Γ are integral domains. If $\gamma \in \Gamma$ is integral over A then γ is integral over B.*

Proof. Since $\gamma \in \Gamma$ is integral over A, we have that γ satisfies a monic equation

$$x^n + \alpha_{n-1}x^{n-1} + \cdots + \alpha_1 x + \alpha_0 = 0$$

with α_{n-1},...,α_1,α_0 in A.

Now, since $A \subset B$ this means that $\alpha_{n-1}, ..., \alpha_1, \alpha_0$ are elements of B. Therefore we see that γ satisfies a monic equation with coefficients in B. Hence γ is integral over B. □

Theorem 19. *Let $A \subset B \subset \Gamma$ where A, B, and Γ are integral domains. If Γ is integral over A then Γ is integral over B.*

Proof. Let γ belong to Γ. Since Γ is integral over A we have that γ satisfies a monic equation

$$x^n + \alpha_{n-1}x^{n-1} + \cdots + \alpha_1 x + \alpha_0 = 0$$

with α_{n-1},...,α_1,α_0 in A.

Since each $\alpha_{n-1}, ..., \alpha_1, \alpha_0$ belongs to A and $A \subset B$, we obtain that each α_{n-1},...,α_1,α_0 belongs to B and therefore γ will be integral over B. Hence, Γ is integral over B. □

We will now define an *R-action*, *R-module*, *submodule*, *submodule generated by a set*, and *finitely generated module.*

Definition 20. ***(R-action)***
*Let R be a ring and M and additive abelian group. A function $\alpha : R \times M \to M$ is called an **R-action** on M if α has the following properties:*

$$\alpha(r + s, m) = \alpha(r, m) + \alpha(s, m),$$
$$\alpha(r, m + n) = \alpha(r, m) + \alpha(r, n),$$
$$\alpha(r, \alpha(s, m)) = \alpha(rs, m),$$
$$\alpha(1, m) = m,$$

for all $r, s \in R$ and all $m, n \in M$. We denote $\alpha(r, m)$ by $r \cdot m$.

Definition 21. ***(R-module)***
*Let R be a ring. An additive abelian group M together with an R-action on M is called an **R-module**.*

Example 22. *Any additive abelian group A can be thought of as a $\mathbb{Z}$-module in a natural way. The $\mathbb{Z}$-action on A is just the map $(n, a) \to n \cdot a$ from $\mathbb{Z} \times A$ to A, where $n \cdot a$ means $a + \cdots + a$ a total of n times.*

Definition 23. *(**Submodule**)*
*Let R be a ring. Let M be an R-module. A subgroup N of M is called a **submodule** of M if $r \cdot n \in N$ for all $r \in R$ and $n \in N$.*

Example 24. *The ideals in any ring R can be thought of as R-modules.*

Definition 25. *(**Submodule Generated by a Set**)*
*If X is a subset of an R-module M then the **submodule generated by a set** X is the smallest submodule of M containing X. By smallest submodule containing X we mean the intersection of all submodules of M which contain X.*

Definition 26. *(**Finitely Generated Module**)*
*An R-module M is called **finitely generated** if M is generated by some finite set of elements of M.*

Now, by the definiton above we see that an R-module M is finitely generated if and only if there exists finitely many elements $x_1, x_2, ..., x_n \in M$ such that if $x \in M$ then x may be expressed as a linear combination of the elements $x_1, x_2, ..., x_n$ with coefficients in R. That is,

$$x = r_1x_1 + r_2x_2 + \cdots \ r_nx_n \quad \text{where each} \ \ r_i \ \ \text{belongs to} \ \ R.$$

Before proving the following theorem we will introduce some new notation. We will let $[\beta]$ denote the set $\{1, \beta, \beta^2, ..., \beta^n, ...\}$. That is,

$$[\beta] = \{1, \beta, \beta^2, ..., \beta^n, ...\}.$$

Theorem 27. *Let $A \subset B$ where A and B are integral domains. Any element β in B which is integral over A will generate a finite A-module $A[\beta] = \{\sum_{i=0}^{n} \alpha_i\beta^i |\ \alpha_i \in A,\ \beta^i \in B\}$, and conversely, if $A[\beta]$ is a finitely generated A-module then β will be integral over A.*

Proof. We begin by supposing that β is integral over A. Therefore, since β is integral over A we obtain that there exists $\alpha_0, \alpha_1, ..., \alpha_{n-2}, \alpha_{n-1} \in A$ such that β satisfies the monic equation

$$x^n + \alpha_{n-1}x^{n-1} + \cdots + \alpha_1x + \alpha_0 = 0.$$

That is,

$$\beta^n + \alpha_{n-1}\beta^{n-1} + \cdots + \alpha_1\beta + \alpha_0 = 0,$$

and therefore we obtain that

$$\beta^n = -\alpha_{n-1}\beta^{n-1} - \alpha_{n-2}\beta^{n-2} - \cdots - \alpha_1\beta - \alpha_0 \in A\beta^{n-1} + A\beta^{n-2} + \cdots + A\beta + A.$$

By multiplying both sides of the equation above by β we obtain that

$$\begin{aligned}\beta^{n+1} &= \alpha_{n-1}\beta^n + \alpha_{n-2}\beta^{n-1} + \cdots + \alpha_1\beta^2 + \alpha_0\beta \\ &\in A\beta^n + A\beta^{n-1} + \cdots + A\beta^2 + A\beta \\ &\subset A\beta^{n-1} + A\beta^{n-2} + \cdots + A\beta + A.\end{aligned}$$

By induction we conclude that

$$\beta^k \in A\beta^{n-1} + A\beta^{n-2} + \cdots + A\beta + A$$

for $k \geq 0$ in $\mathbb{Z}$. Therefore this establishes the fact that the integral domain $A[\beta]$ of "polynomials in β" with coefficients in A is a finitely generated A-module.

Now, suppose that we are given that $A[\beta]$ is a finitely generated A-module. This implies that there exists $\omega_1, \omega_2, \ldots, \omega_n \in A[\beta]$ such that

$$A[\beta] = A\omega_1 + A\omega_2 + \cdots + A\omega_n.$$

Now, since $A[\beta] \neq 0$, not all the ω_i's are zero. Since each $\omega_i, \beta \in A[\beta]$ we obtain that $\beta\omega_i \in A[\beta]$ for $i = 1, 2, ..., n$. Therefore there exists elements $\alpha_{ij} \in A$ where $i, j = 1, 2, ..., n$ such that

$$\begin{aligned}\beta\omega_1 &= \alpha_{11}\omega_1 + \alpha_{12}\omega_2 + \cdots + \alpha_{1n}\omega_n, \\ &\vdots \\ \beta\omega_n &= \alpha_{n1}\omega_1 + \alpha_{1n}\omega_2 + \cdots + \alpha_{nn}\omega_n.\end{aligned}$$

From the equations above we see that the homogeneous system

$$\begin{aligned}(\beta - \alpha_{11})x_1 - \alpha_{12}x_2 - \cdots - \alpha_{1n}x_n &= 0, \\ -\alpha_{21}x_1 + (\beta - \alpha_{22})x_2 - \cdots - \alpha_{2n}x_n &= 0, \\ &\vdots \\ -\alpha_{n1}x_1 - \alpha_{n2}x_2 - \cdots + (\beta - \alpha_{nn})x_n &= 0,\end{aligned}$$

has a nontrivial solution, namely $(x_1, x_2, ..., x_n) = (\omega_1, \omega_2, ..., \omega_n)$, in the integral domain $A[\beta]$ and therefore in its field of quotients. Hence, we obtain that the determinant of its coefficient matrix is zero; that is,

$$\begin{vmatrix} \beta - \alpha_{11} & -\alpha_{12} & \cdots & -\alpha_{1n} \\ -\alpha_{21} & \beta - \alpha_{22} & \cdots & -\alpha_{2n} \\ \vdots & \vdots & & \vdots \\ -\alpha_{n1} & -\alpha_{n2} & \cdots & \beta - \alpha_{nn} \end{vmatrix} = 0.$$

By expanding the determinat above we obtain an equation of the form

$$\beta^n + \alpha_{n-1}\beta^{n-1} + \cdots + \alpha_1\beta + \alpha_0 = 0,$$

where the coefficients $\alpha_0, \alpha_1, ..., \alpha_{n-1} \in A$. Therefore β is integral over A. □

Theorem 27 established a connection between integral elements and finitely generated modules. The proof of Theorem 28 is very similar to the proof of Theorem 27.

Theorem 28. *Let $A \subset B$ where A and B are integral domains. If $\beta \in B$ and there exists an integral domain Γ such that*

$$A[\beta] \subset \Gamma \subset B$$

where Γ is a finitely generated A-module then β is integral over A and therefore $A[\beta]$ is a finitely generated A-module.

Proof. Since Γ is a finitely generated A-module, by Theorem 27, we obtain that there are $\gamma_1, \gamma_2, ..., \gamma_n \in \Gamma$ such that

$$\Gamma = A\gamma_1 + A\gamma_2 + \cdots + A\gamma_n$$

where not all γ_i's are equal to zero. Now, since $\beta \in A[\beta]$ and $A[\beta] \subset \Gamma$ we obtain that $\beta \in \Gamma$.

Since Γ is an integral domain, we obtain that $\beta\gamma_i \in \Gamma$ for $i = 1, 2, ..., n$. We use that fact that Γ is a finitely generated A-module to conclude that there exist $\alpha_{ij} \in A$ where $i, j = 1, 2, ..., n$ such that

$$\begin{aligned} \beta\gamma_1 &= \alpha_{11}\gamma_1 + \alpha_{12}\gamma_2 + \cdots + \alpha_{1n}\gamma_n, \\ \beta\gamma_2 &= \alpha_{21}\gamma_1 + \alpha_{22}\gamma_2 + \cdots + \alpha_{2n}\gamma_n, \\ &\vdots \\ \beta\gamma_n &= \alpha_{n1}\gamma_1 + \alpha_{n2}\gamma_2 + \cdots + \alpha_{nn}\gamma_n. \end{aligned}$$

Therefore the homogeneous system

$$\begin{aligned}(\beta-\alpha_{11})x_1-\alpha_{12}x_2-\cdots-\alpha_{1n}x_n&=0,\\ -\alpha_{21}x_1+(\beta-\alpha_{22})x_2-\cdots-\alpha_{2n}x_n&=0,\\ &\vdots\\ -\alpha_{n1}x_1-\alpha_{n2}x_2-\cdots+(\beta-\alpha_{nn})x_n&=0,\end{aligned}$$

has a nontrivial solution, namely $(x_1,...,x_n)=(\gamma_1,...,\gamma_n)$, in the integral domain Γ and therefore in its field of quotients. Hence, the determinant of its coefficient matrix is zero; that is,

$$\begin{vmatrix}\beta-\alpha_{11} & -\alpha_{12} & \cdots & -\alpha_{1n}\\ -\alpha_{21} & \beta-\alpha_{22} & \cdots & -\alpha_{2n}\\ \vdots & \vdots & & \vdots\\ -\alpha_{n1} & -\alpha_{n2} & \cdots & \beta-a\alpha_{nn}\end{vmatrix}=0.$$

By expanding the determinant above we obtain an equation,

$$\beta^n+\alpha_{n-1}\beta^{n-1}+\cdots+\alpha_1\beta+\alpha_0=0,$$

where $\alpha_0,\alpha_1,...,\alpha_{n-1}\in A$. Hence, β is integral over A and by Theorem 27 we have that $A[\beta]$ is a finitely generated A-module. □

The special case of Theorem 28 where $\Gamma=B$ tells us that if A and B are integral domains such that $A\subset B$ and B is a finitely generated A-module then B is integral over A.

Theorem 29. *Let $A\subset B\subset\Gamma$ where A, B and Γ are integral domains. If B is a finitely generated A-module and Γ is a finitely generated B-module then Γ will also be a finitely generated A-module.*

Proof. If B is a finitely generated A-module we know that there exists $\beta_1,\beta_2,...,\beta_n\in B$ such that

$$B=A\beta_1+A\beta_2+\cdots+A\beta_n$$

Now, since Γ is a finitely generated B-moudle we know that there exists $\gamma_1,\gamma_2,...,\gamma_m\in\Gamma$ such that

$$\Gamma=B\gamma_1+B\gamma_2+\cdots+B\gamma_m.$$

Let $\gamma \in C$. Since Γ is a finitely generated B-module we obtain that

$$\gamma = \sum_{i=1}^{m} \beta_i \gamma_i,$$

where each $\beta_i \in B$. Moreover, since B is a finitely generated A-module we obtain that for $i = 1, ..., m$,

$$\beta_i = \sum_{j=1}^{n} \alpha_{ij} \beta_j,$$

where $a_{ij} \in A$ for $i = 1, ..., m$ and $j = 1, ..., n$. Therefore,

$$\gamma = \sum_{i=1}^{m} \sum_{j=1}^{n} \alpha_{ij} \beta_j \gamma_i.$$

Hence,

$$\Gamma = A\beta_1\gamma_1 + \cdots + A\beta_n\gamma_m$$

is a finitely generated A-module. □

Suppose that M and N are integral domains such that $N \supset M$. Let $\nu_1, ..., \nu_n$ be elements of N which are integral over M. Since ν_1 is integral over M we obtain that $M[\nu_1]$ is a finitely generated M-module. We have that ν_2 is integral over M and therefore ν_2 is integral over $M[\nu_1]$ since $M \subset M[\nu_1]$. Hence, we may conclude that $(M[\nu_1])[\nu_2]$ is a finitely generated $M[\nu_1]$-module.

We now define the module $M[\nu_1, \nu_2] = (M[\nu_1])[\nu_2]$. By induction on n we see that

$$M[\nu_1, ..., \nu_n] = (M[\nu_1, ..., \nu_{n-1}])[\nu_n].$$

Theorem 30 will establish that the set which consists of elements that are integral over another domain is closed under addition, subtraction and multiplication. From the proof of this theorem it will them follow that the ring of algebraic integers of an imaginary quadratic number field forms an integral domain.

Theorem 30. *Let $A \subset B$ where A and B are integral domains. If $\beta_1, \beta_2 \in B$ are elements which integral over A then $\beta_1 + \beta_2$, $\beta_1 - \beta_2$, and $\beta_1\beta_2$ will be integral over A.*

Proof. Since β_1 is integral over A, by Theorem 27, we have that $A[\beta_1]$ is a finitely generated A-module. Now, since β_2 is integral over A we obtain that β_2 is integral over $A[\beta_1]$, since $A \subset A[\beta_1]$. Therefore $A[\beta_1, \beta_2]$ is a finitely generated $A[\beta_1]$-module. Hence,

by Theorem 29, we may conclude that $A[\beta_1, \beta_2]$ is a finitely generated A-module. Let β denote one of the three elements: $\beta_1 + \beta_2$, $\beta_1 - \beta_2$, $\beta_1\beta_2$.

Since

$$A \subset A[\beta] \subset A[\beta_1, \beta_2] \subset B,$$

by Theorem 28 we may conclude that the integral domain $A[\beta]$ is a finitely generated A-module. It then follows that β is integral over A. □

The following result is a direct consequence of Theorem 30.

Theorem 31. *Let $A \subset B$ where A and B are integral domains. The set consisting of all the elements of B which are integral over A forms a subdomain of B containing A.*

Proof. The set of elements which are integral over A is nonempty since 0 is in B and 0 is integral over A. By Theorem 30 we see that this set is closed under sums, differences, and products; therefore, it is a subring. A subring of an integral domain is an integral domain. □

Chapter 4

The Ring of Algebraic Integers and Unique Factorization Domains

We will now point out an important observation. If we let $A = \mathbb{Z}$ and let $B = \mathbb{C}$ in Theorem 31, we obtain the following theorem.

Theorem 32. *The set of all algebraic integers is an integral domain.*

Next we properly define the set of algebraic integers.

Definition 33. ***(The Set of Algebraic Integers Ω)***
The ***set of all algebraic integers*** *is denoted by* Ω.

We are now ready to define *irreducible elements*, *prime elements*, *factorization domains*, and *unique factorization domains*.

Definition 34. ***(Irreducible Element and Reducible Element)***
A nonzero, nonunit element δ of an integral domain Δ is said to be an ***irreducible element*** *if whenever α, β are elements of Δ and $\delta = \alpha\beta$, then either α or β is a unit. A nonzero, nonunit element which is not irreducible is called* ***reducible****.*

Definition 35. ***(Prime Element)***
Let $\alpha, \beta \in \Delta$. A nonzero, nonunit element π of an integral domain Δ is said to be a ***prime element*** *if whenever $\pi \mid \alpha\beta$ then $\pi \mid \alpha$ or $\pi \mid \beta$.*

Definition 36. *(**Factorization Domain**)*
*Let Δ be an integral domain. We say that Δ is a **factorization domain** if every nonzero, nonunit element of Δ can be expressed as a finite product of irreducible elements of Δ.*

Definition 37. *(**Unique Factorization Domain**)*
Let Δ be a factorization domain. Suppose that every nonzero, nonunit element δ of Δ has a unique factorization. By unique factorization we mean if

$$\pi_1\pi_2\cdots\pi_n = \sigma_1\sigma_2\cdots\sigma_m$$

*where each π_i and σ_j are irreducible elements of Δ, then $n = m$ and for each i, $\pi_i = \mu\sigma_j$ for some j and unit μ of Δ. If Δ has this property then Δ is called a **unique factorization domain**.*

It is well known that whenever Δ is a pricipal ideal domain (PID) Δ will be a unique factorization domain (UFD). The converse, however, is not always true. We will give an example to illustrate this.

Example 38. *It can be shown that the ring $\mathbb{Z}[x]$ is a UFD, therefore let us consider the ring $\mathbb{Z}[x]$. This ring is a UFD but not a PID. To show that $\mathbb{Z}[x]$ is not a PID it suffices to find a single ideal I contained in $\mathbb{Z}[x]$ which is not principal. The ideal $\langle 2, x\rangle = \{2r + xs \mid r, s \in \mathbb{Z}[x]\}$ in $\mathbb{Z}[x]$ serves this purpose. The ideal $\langle 2, x\rangle$ is not a principal ideal. One may easily verify that $\langle 2, x\rangle$ is not a principal ideal by supposing that is it and arriving at a contradiction.*

It is also well known that in an integral domain Δ an element π which is prime will always be an irreducible element, but an element δ which is irrudicible will not always be a prime element. However, in a unique factorization domain when one says that an element is irreducible, this implies that it is also a prime element and vice-versa.

Example 39. *Consider the element 3 of $\mathbb{Z} + \mathbb{Z}[\sqrt{-5}]$. It may be shown by consideration of the properties of the norm, that 3 is an irreducible element which is not prime. This is true because $3 \mid (1 - \sqrt{-5})(1 + \sqrt{-5}) = 6$ but 3 does not divide any of the two factors.*

Theorem 40. *Elements in a unique factorization domain D are irreducible if and only if they are prime.*

Proof. Let δ be an irreducible element of Δ and suppose that $\delta \mid \alpha\beta$. This means that $\alpha\beta = \delta\gamma$ for some γ in Δ. Since Δ is a unique factorization domain α, β and γ may be written as $\alpha = \alpha_1 \cdots \alpha_n$, $\beta = \beta_1 \cdots \beta_s$, and $\gamma = \gamma_1 \cdots \gamma_r$ where each α_i, β_j and γ_k are irreducible elements of Δ for $1 \leq i \leq n$, $1 \leq j \leq s$ and $1 \leq k \leq r$. The equation $\alpha\beta = \delta \cdot \gamma$ may then be written as

$$\alpha_1 \cdots \alpha_n \cdot \beta_1 \cdots \beta_s = \delta \cdot \gamma_1 \cdots \gamma_r.$$

Since Δ is a unique factorization domain, the left and right sides of the equation will be the same up to the order of the factors and associates. Therefore we have that δ is an associate of some α_i or β_j. This is equivalent to saying that $\delta \mid \alpha$ or $\delta \mid \beta$. Hence, δ is a prime element of Δ.

Now, suppose that π in Δ is a prime element and that π is a nonirreducible element of Δ. This implies that there exists nonzero, nonunit elements α and β in Δ such that $\pi = \alpha\beta$. Now, since π is a prime element we obtain that $\pi \mid \alpha$ or $\pi \mid \beta$. If $\pi \mid \alpha$ then $\alpha = \pi\delta$ where δ is an element in Δ. After substituting $\alpha = \pi\delta$ in the equation

$$\pi = \alpha\beta$$

and cancelling π from both sides we obtain the equation

$$1 = \delta\beta.$$

Therefore we may conclude that β is a unit. This is a contradiction since we had assumed β and α were not unit elements. Similarly, if $\pi \mid \beta$, by applying the same argument we conclude that α is a unit and hence, another contradiction. Therefore, π is irreducible. $\square$

Chapter 5

Integral Closure

Next we will introduce the notion of an integrally closed set.

Definition 41. *(**Integral Closure**)*
*Let A and B be integral domains with $A \subset B$. The **integral closure** of A in B is the subdomian of B consisting of all elements of B which are integral over A. The integral closure of A in B is denoted by*

$$A^B.$$

Theorem 42. *Let $A \subset B$ where A and B are integral domains. The integral closure A^B of A in B is an integral domain satisfying,*

$$A \subset A^B \subset B.$$

Proof. Let a be an element of A, then $a \in B$. Since a satisfies the monic polynomial equation

$$x - a = 0$$

we see that a belongs to A^B. Hence $A \subset A^B \subset B$. □

The next theorem establishes the fact that the integral closure of a unique factorization domain Δ in its field of quotients Φ is Δ.

Theorem 43. *Let Δ be a unique factorization domain. Let Φ be the field of quotients of Δ. Then $\phi \in \Phi$ is integral over Δ if and only if $\phi \in \Delta$.*

Proof. Let $\phi \in \Phi$, then ϕ may be written in the following way, $\phi = \frac{\alpha}{\beta}$ where $\alpha, \beta \neq 0 \in \Delta$ where α and β have no common irreducible factors. Since ϕ is integral over Δ it will satisfy a monic equation,

$$x^n + \delta_{n-1}x^{n-1} + \cdots + \delta_1 x + \delta_0 = 0.$$

That is,

$$\phi^n + \delta_{n-1}\phi^{n-1} + \cdots + \delta_1\phi + \delta_0 = 0$$

or,

$$\left(\frac{\alpha}{\beta}\right)^n + \delta_{n-1}\left(\frac{\alpha}{\beta}\right)^{n-1} + \cdots + \delta_1\left(\frac{\alpha}{\beta}\right) + \delta_0 = 0.$$

Multiplying both sides of the third equation by β^n we obtain

$$\alpha^n + \delta_{n-1}\beta\alpha^{n-1} + \cdots + \delta_1\beta^{n-1}\alpha + \delta_0\beta^n = 0.$$

Therefore, we obtain

$$\alpha^n = -\delta_{n-1}\beta\alpha^{n-1} - \delta_{n-2}\beta^2\alpha^{n-2} - \cdots - \delta_1\beta^{n-1}\alpha - \delta_0\beta^n$$

If β is not a unit of Δ it may be written as $\beta = \pi_1\pi_2\cdots\pi_n$ where each π_i is an irreducible element of Δ. By Theorem 40, since Δ is a unique factorization domain we obtain that each π_i is also a prime element of Δ. Now, since π_1 divides β, and therefore, each summand on the right of the last equation, we see that π_1 must divide α^n. Therefore, π_1 divides α since it is a prime element. This can't happen because this would imply that α and β have a common irreducible factor, which they don't. Therefore, β is a unit of Δ and consequently $\phi = \alpha\beta^{-1} \in D$.

Now if $\phi \in \Delta$, ϕ is integral over Δ since it satisfies the monic equation $x - \phi = 0$. Hence, ϕ is integral over Δ. □

Next we recall that Ω denotes the set of all algebraic integers in $\mathbb{C}$. The following theorem says that the set of algebraic integers in $\mathbb{Q}$ are the ordinary rational integers, $\mathbb{Z}$.

Theorem 44. $\mathbb{Q} \cap \Omega = \mathbb{Z}$

Proof. Let ω be in $\mathbb{Q} \cap \Omega$. Since ω belongs to $\mathbb{Q}$, this implies that $\omega = \frac{p}{q}$ where p, and $q \neq 0$ belong in $\mathbb{Z}$. We may assume that the greatest common factor of p and q is 1. Also, since ω belongs in Ω it must satisfy a monic equation

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0$$

with the coefficients a_i for $1 \leq i \leq n-1$ in $\mathbb{Z}$. Hence,

$$\left(\frac{p}{q}\right)^n + a_{n-1}\left(\frac{p}{q}\right)^{n-1} + \cdots + a_1\left(\frac{p}{q}\right) + a_0 = 0.$$

Multiplying both sides of the above equation by q^n we obtain

$$p^n + a_{n-1}qp^{n-1} + \cdots + a_1 q^{n-1}p + a_0 q^n = 0,$$

or

$$p^n = -a_{n-1}qp^{n-1} - \cdots - a_1 q^{n-1}p - a_0 q^n.$$

Now, since q divides each of the terms on the right side we may conclude that $q \mid p$. Therefore $p = qr$ for some r in $\mathbb{Z}$. Hence we obtain that $\alpha = \left(\frac{qr}{q}\right) = r$. So we see that ω is an integer. Therefore we may conclude that $\mathbb{Q} \cap \Omega \subset \mathbb{Z}$.

On the other hand if ω is an integer then ω is a rational number, that is, $\omega \in \mathbb{Q}$. Now, since ω satisfies the monic equation

$$x - \omega = 0$$

with integer coefficients we see that ω belongs to Ω. Therefore ω belongs to $\mathbb{Q} \cap \Omega$. This allows us to conclude that $\mathbb{Z} \subset \mathbb{Q} \cap \Omega$. Hence, $\mathbb{Q} \cap \Omega = \mathbb{Z}$. □

Chapter 6

Algebraic Integers and Lattices

Definition 45. *(**Algebraic Number Field**)*
*An **algebraic number field** is a subfield of $\mathbb{C}$ of the form $\mathbb{Q}(\chi_1, \chi_2, ..., \chi_n)$ where each χ_i is an algebraic number. We observe that $\mathbb{Q}(\chi_1, \chi_2, ..., \chi_n)$ is a multiple algebraic extension of $\mathbb{Q}$.*

Using the above definition we may now define what a *quadratic number field* is and what an *imaginary quadratic number field* is.

Definition 46. *(**Quadratic Number Field**)*
*The subfield $\Phi = \mathbb{Q}(\chi) = \mathbb{Q}[\chi]$ of $\mathbb{C}$, where $\chi = \sqrt{d}$, d is a squarefree rational integer is called a **quadratic number field**. If $d < 0$ then $\Phi = \mathbb{Q}[\chi]$ is called an imaginary quadratic number field.*

Definition 47. *(**The Set of Algebraic Integers in an Imaginary Quadratic Number Field**)*
*The **set of algebraic integers in an imaginary quadratic number field** is denoted by Υ, it is the set*

$$\Omega \cap \Phi,$$

where $\Phi = \mathbb{Q}[\chi]$, $\chi = \sqrt{d}$, and d is a negative squarefree rational integer.

The following proposition will tells us the form of the algebraic integers, $\Upsilon = \Omega \cap \Phi$.

Proposition 48. *Let $\chi = \sqrt{d}$. If $\upsilon \in \Upsilon$ then $\upsilon = a + b\chi$, where:*

(a) If $d \equiv 2$ or 3 (modulo 4), then a and b belong to $\mathbb{Z}$.

(b) If $d \equiv 1$ (modulo 4), then either $a,\ b \in \mathbb{Z}$ or $a,\ b \in \mathbb{Z} + \frac{1}{2}$ where $\mathbb{Z} + \frac{1}{2} = \{\frac{r}{2} |\ r = 2k+1,\ k \in \mathbb{Z}\}$.

Proof. Let $\upsilon = a + b\chi$ belong to Υ. Then υ satisfies a monic polynomial equation, namely,

$$0 = x^2 - 2ax + a^2 - b^2 d.$$

Since $2a \in \mathbb{Z}$ we have that $a = \frac{q}{2}$ where $q \in \mathbb{Z}$. Also, since $a^2 - b^2 d \in \mathbb{Z}$ so is $4a^2 - 4b^2 d$. This implies that $4b^2 d \in \mathbb{Z}$. Let $b = \frac{r}{s}$ where r and s are integers with $gcd(r, s) = 1$. Therefore,

$$4b^2 d = 4\frac{r^2}{s^2} d \in \mathbb{Z}$$

which implies that $s^2 | 4d$. Now, if $s \neq \pm 1$ then $s = \pm 2$ and we have that $b = \frac{k}{2}$ for some $k \in \mathbb{Z}$. On the other hand, if $s = \pm 1$ then $b \in \mathbb{Z}$ and therefore so is a. The conclusion that $a \in \mathbb{Z}$ follows from the fact that $a^2 - b^2 d \in \mathbb{Z}$ which implies that $a^2 \in \mathbb{Z}$ and a^2 is in $\mathbb{Z}$ if and only if $a \in \mathbb{Z}$.

Therefore, we have only two possibilities for υ. These two possibilties are the following: either $\upsilon = a + b\chi$ with a and b in $\mathbb{Z}$ or $\upsilon = a + b\chi$ with a and b in $\mathbb{Z} + \frac{1}{2}$.

Now, if $d \equiv 2$ or 3 (modulo 4) and $\upsilon = a + b\chi$ with $a, b \in \mathbb{Z}$ we are done. On the other hand suppose $d \equiv 2$ or 3 (modulo 4) and $\upsilon = a + b\chi$ with $a, b \in \mathbb{Z} + \frac{1}{2}$. We then have that

$$a^2 - b^2 d = \left(\frac{q}{2}\right)^2 - \left(\frac{k}{2}\right)^2 d = \frac{q^2 - k^2 d}{4} \in \mathbb{Z}.$$

Therefore, $q^2 - k^2 d \equiv 0$ (modulo 4) and since $d \equiv 2$ or 3 (modulo 4) we must have that q and k are both even. Thus, a and b are integers in this case too.

Now suppose that $d \equiv 1$ (modulo 4). We have already established that υ is of the form $\upsilon = a + b\chi$ with a and b in $\mathbb{Z}$ or that υ is of the form $\upsilon = a + b\chi$ with a and b in $\mathbb{Z} + \frac{1}{2}$. □

It can be shown that each of the algebraic integers in a quadratic number field $\Phi = \mathbb{Q}[\sqrt{d}]$, where d is congruent to 1 modulo 4, can be expressed in the form

$$a + b\nu \quad \text{where} \quad \nu = \frac{1}{2}(1 + \chi) \quad \text{and} \quad a, b \in \mathbb{Z}.$$

Hence, now we know that if ϕ is an algebraic integer of an imaginary quadratic number field then

$$\phi \in \mathbb{Z} + \mathbb{Z}\chi \quad \text{or} \quad \phi \in \mathbb{Z} + \mathbb{Z}\nu.$$

This is equivalent to saying $\phi = m \cdot 1 + n \cdot \chi$ or $\phi = m \cdot 1 + n \cdot \nu$ for m, n in $\mathbb{Z}$. Next we will define a *lattice*.

Definition 49. *(**Lattice in** $\mathbb{R}^2$)*
*A **lattice** L is a discrete abelian subgroup of $\mathbb{R}^2$ of the form*

$$\mathbb{Z}u + \mathbb{Z}v$$

where u and v are any two noncolinear elements of $\mathbb{R}^2$. By discrete we mean that there is a distance ϵ where $\epsilon > 0$, such that no two elements of the group are less than a distance ϵ apart. We call the set $\{u, v\}$ the basis of the lattice L.

The elements of the lattice $L = \mathbb{Z}u + \mathbb{Z}v$ are of the form,

$$n \cdot u + m \cdot v,$$

where we recall that $n \cdot u$ is $u + u \cdots + u$ (n times) and $m \cdot v$ is $v + v \cdots + v$ (m times) . A lattice is an example of a $\mathbb{Z}$-module which is generated by two elements.

Thus, with this definition we see that the ring of algebraic integers Υ forms a lattice in $\mathbb{R}^2$. After proving the following three lemmas and and introducing the definition of the *fundamental parallelogram* we will be ready to begin proving some results about ideals in the ring of algebraic integers Υ.

Lemma 50. *Let L be a discrete subgroup of $\mathbb{R}^2$.*

(a.) A bounded subset of $\mathbb{R}^2$ contains only finitely many elements of L.

(b.) If $L \neq \{0\}$, then L contains a nonzero vector of minimal length.

Proof. (a.) We let S be a bounded subset of $\mathbb{R}^2$. We recall that a subset of $\mathbb{R}^n$ is bounded if it is contained in a box of $\mathbb{R}^n$, or its elements are not arbitrarily large, meaning that they do not have arbitrarily large coordinates. Therefore if S is bounded then so is $L \cap S$. Now, an infinite bounded set must have elements which are arbitrarily close to one another. This means that the elements cannot be separated by a fixed distance ϵ

from each other. But this does not happen with elements of L since by definition there is a distance ϵ such that L contains no elements which are a distance less than ϵ apart. Hence, since the distance between any two vectors $a, b \in L$ is at least ϵ we obtain that $L \cap S$ is finite.

(b.) A vector v is said to be of minimal length if every vector u in L has a length of at least $|v|$. The vector v is not required to be uniquely determined since $-v$ is also of minimal length. Assume $L \neq \{0\}$. Let u be any nonzero vector of L and let S be the disc of radius $|u|$ about the origin. This disc is a bounded set, so it contains finitely many elements of L. We look through all these elements and choose the one of minimal length. This is the required vector. □

Definition 51. *(**Fundamental Parallelogram**)*
Let u and v be two linearly independent elements of $\mathbb{R}^2$. The set

$$\mathscr{P} = \{ru + sv \mid 0 \leq r \leq 1, 0 \leq s \leq 1; r, s \in \mathbb{R}\}$$

*is called the **fundamental parallelogram** of $\mathbb{R}^2$.*

Lemma 52. *If a plane lattice L has two linear independent generators $u, v \in \mathbb{R}^2$ then for any $x \in \mathbb{R}^2$ there exists an $\ell \in L$ such that $x - l$ is in $\mathscr{P}$.*

Proof. If $x \in \mathbb{R}^2$ then x may be expressed as $x = pu + qv$ where p and q are in $\mathbb{R}$. Choose $\ell \in L$ such that $\ell = \lfloor p \rfloor u + \lfloor q \rfloor v$ where $\lfloor p \rfloor, \lfloor q \rfloor \in \mathbb{Z}$ and $p - 1 < \lfloor p \rfloor \leq p$ and $q - 1 < \lfloor q \rfloor \leq q$. It is a fact that we may express p as $p = \lfloor p \rfloor + r$ and q as $q = \lfloor q \rfloor + s$ where $0 \leq r, s \leq 1$. Hence,

$$x - \ell = ru + sv.$$

This completes the proof. □

Lemma 53. *Let $T \subset U$ be lattices in $\mathbb{R}^2$. There are only finitely many lattices L between T and U.*

Proof. Let (τ_1, τ_2) be a lattice basis for T. Let us consider the parallelogram $\mathscr{P}$ which has vertices 0, τ_1, τ_2, $\tau_1 + \tau_2$. There are finitely many elements of U inside $\mathscr{P}$ by Lemma 50. Now, if L is a lattice such that $T \subset L \subset U$ then there will be finitely many possibilities for the set $L \cap \mathscr{P}$. Let $L \cap \mathscr{P} = S$ and let $\ell \in L$ then there exists an element $\tau \in T$ such

that $\ell - \tau \in \mathscr{P}$, by Lemma 52. Now, since $\ell - \tau$ is in L we see that $\ell - \tau \in S$. Therefore we see that $\ell - \tau = s$ for some $s \in S$. In other words $\ell = s + \tau$. Hence, $L = S + T$ and since there are only finitely many possibilities for S, we see that there will only be finitely many lattices L. $\square$

Chapter 7

Divisibility of Ideals and Unique Prime Ideal Factorization

In this chapter we introduce the notion of the conjugate ideal, $\overline{A}$, of an ideal A in an imaginary quadratic number field.

Definition 54. *(**The conjugate of an Ideal in the Ring** Υ)*
*If A is an ideal of the ring of integers Υ in an imaginary quadratic number field Φ the ideal $\overline{A}$ is called the **conjugate ideal** of A.*

$$\overline{A} = \{\overline{\alpha} |\ \alpha \in A\}$$

where $\overline{\alpha}$ is the complex conjugate of α.

Lemma 55. *Let Υ be the ring of integers in an imaginary quadratic number field Φ. The product of a nonzero ideal and its conjugate is a principal ideal of Υ generated by a rational integer; that is,*

$$A\bar{A} = (d) \quad \text{for some } d \in \mathbb{Z}.$$

Proof. The ideal A may be generated as a lattice by two elements since it may be thought of as a sublattice of the underlying lattice (abelian group) of the ring Υ, call these two elements α and β. Since the elements α and β generate A as a lattice they will generate A as an ideal, moreover, $\overline{\alpha}$ and $\overline{\beta}$ will generate $\overline{A}$. Therefore we see that the elements, $\alpha\overline{\alpha}$, $\beta\overline{\beta}$, $\alpha\overline{\beta}$, and $\beta\overline{\alpha}$ generate the ideal $A\overline{A}$. Now, consider the following three elements $\alpha\overline{\alpha}$, $\beta\overline{\beta}$, and $\alpha\overline{\beta} + \beta\overline{\alpha}$. These elements are equal to their own conjugates, hence they

must be real numbers. Since these three elements are algebraic integers we know that this implies that they must be rational integers by Theorem 44 . Let d be their greatest common divisor in $\mathbb{Z}$. Since d is the greatest common divisor, this means that d will be a linear combination of $\alpha\overline{\alpha}$, $\beta\overline{\beta}$, and $\alpha\overline{\beta} + \beta\overline{\alpha}$. Thus, d is in the product ideal $A\overline{A}$ and therefore $(d) \subset A\overline{A}$.

Next we will show that $A\overline{A} \subset (d)$. To establish this we must show that d divides each of the generators $\alpha\overline{\alpha}$, $\beta\overline{\beta}$, $\alpha\overline{\beta}$, and $\beta\overline{\alpha}$. By construction we already know that $d \mid \alpha\overline{\alpha}$ and $d \mid \beta\overline{\beta}$. Hence all we need to do is show that $d \mid \alpha\overline{\beta}$ and $d \mid \beta\overline{\alpha}$. To establish this it suffices to show that $\frac{\alpha\overline{\beta}}{d}$ and $\frac{\beta\overline{\alpha}}{d}$ are algebraic integers. Now, since $\frac{\alpha\overline{\beta}}{d}$ and $\frac{\beta\overline{\alpha}}{d}$ satisfy the monic equation,

$$x^2 - ax + b = 0,$$

where $a = \frac{\alpha\overline{\beta}+\beta\overline{\alpha}}{d}$ and $b = \frac{\alpha\overline{\alpha}}{d}\frac{\beta\overline{\beta}}{d}$ are rational integers, we may conclude that both $\frac{\alpha\overline{\beta}}{d}$ and $\frac{\beta\overline{\alpha}}{d}$ are algebraic integers. Hence $\frac{\alpha\overline{\beta}}{d}$ and $\frac{\beta\overline{\alpha}}{d}$ belong to Υ. This shows that $d \mid \alpha\overline{\beta}$ and $d \mid \beta\overline{\alpha}$ since $\frac{\alpha\overline{\beta}}{d} = r$ and $\frac{\beta\overline{\alpha}}{d} = s$ for some r and s in Υ which implies that $\alpha\overline{\beta} = dr$ and $\beta\overline{\alpha} = ds$. This is the definition of division. Hence, $A\overline{A} \subset (d)$, thus showing that $A\overline{A} = (d)$ where d is a rational integer. □

We are now prepared to prove the following propositions.

Proposition 56. *Let Υ be the ring of integers in a quadratic number field Φ and Π a proper ideal of Υ. The following are equivalent:*

(a) If $\rho\theta \in \Pi$ where ρ and θ are elements of Υ, then $\rho \in \Pi$ or $\theta \in \Pi$.

(b.) If $AB \subset \Pi$ where A and B are ideals of Υ, then $A \subset \Pi$ or $B \subset \Pi$.

(c.) The quotient ring Υ/Π is an integral domain.

Proof. Let's prove that condition (a) implies condition (b). Suppose that the statement (a) is true. Since Π is a proper ideal of Υ we have that $\Pi \neq \Upsilon$. If $\Pi = \{0\}$ then since $AB \subset \Pi = \{0\}$ we would have that $AB = \{0\}$. Since Υ is an integral domain this would imply that $A = \{0\}$ or $B = \{0\}$ showing that $A \subset \Pi$ or $B \subset \Pi$ ($\alpha \in A$, $\alpha \neq 0$, $\alpha B = \{0\}$). Suppose that $\Pi \neq \{0\}$. Now, if A contains a unit of Υ then since $AB \subset \Pi$ we obtain that $B \subset \Pi$ or if B contains a unit of Υ we obtain $A \subset \Pi$. Suppose that A and B do not contain any units of Υ and that $A \not\subset \Pi$. Since $A \not\subset \Pi$ this means that there exists an α

in A such that α does not belong to Π. Let β be an element of B, then $\alpha\beta \in AB \subset \Pi$. Hence $\alpha\beta \in \Pi$ and therefore by (a) we have that $\alpha \in \Pi$ or $\beta \in \Pi$. Since $\alpha \notin \Pi$ we obtain that $\beta \in \Pi$, therefore $B \subset \Pi$.

Next we show that (b) implies (c). For this we need to establish that $\Upsilon/\Pi \neq \{0\}$, Υ/Π has an identity element under multiplication, and if $\alpha + \Pi$ and $\beta + \Pi$ where $\alpha \in A$ and $\beta \in B$ are elements of Υ/Π such that $(\alpha + \Pi)(\beta + \Pi) = \Pi$ then this implies that $\alpha \in \Pi$ or $\beta \in \Pi$. Now, since $\Upsilon \neq \Pi$ we have that $\Upsilon/\Pi \neq \{0\}$. The element $1 + \Pi$ of Υ/Π serves as the identity element. Finally, since $AB \subset \Pi$ we obtain that $A \subset \Pi$ or $B \subset \Pi$, this implies that if $\alpha\beta + \Pi = \Pi$ where $\alpha \in A$ and $\beta \in B$ then $\alpha + \Pi = \Pi$ or $\beta + \Pi = \Pi$. Therefore, the quotient ring Υ/Π is an integral domain.

Lastly we show that (c) implies (a). Let $\rho\theta \in \Pi$ where ρ and θ are elements of Υ. Then $(\rho + \Pi)(\theta + \Pi) = \rho\theta + \Pi = \Pi$. Since Υ/Π is an integral domain we obtain that $\rho + \Pi = \Pi$ or $\theta + \Pi = \Pi$, that is, $\rho \in \Pi$ or $\theta \in \Pi$. □

Any ideal Π of Υ which satisfies any of the equivalent conditions above in Proposition 56 is called a *prime ideal*.

Proposition 57. *Let Υ be the ring of integers in an imaginary quadratic number field Φ.*

(a.) If A, B, Γ are nonzero ideals of Υ and $AB \subset A\Gamma$ then $B \subset \Gamma$. If $AB = A\Gamma$, then $B = \Gamma$.

(b.) If A and B are two nonzero ideals of Υ, we say $A \subset B$ if and only if B divides A. This is equivalent to saying $A \subset B$ if and only if there exists an ideal Γ of Υ such that $A = B\Gamma$.

(c.) If the nonzero prime ideal Π of Υ divides the product of two ideals AB then it will divide one of its factors A or B.

Proof. (a.) Let A, B, and Γ be nonzero ideals of Υ and suppose that $AB \subset A\Gamma$. If we multiply both sides of $AB \subset A\Gamma$ by the ideal $\overline{A}$ we will obtain $\overline{A}AB \subset \overline{A}A\Gamma$. Therefore, by Lemma 55 we get that $(m)B \subset (m)\Gamma$ for some m is $\mathbb{Z}$. Now, let β be an element of B. Then $m\beta$ belongs to $(m)B$, hence $m\beta$ belongs to $(m)\Gamma$ and thus $m\beta = m\gamma$ for some γ in Γ. It then follows that $\beta = \gamma$ and therefore $B \subset \Gamma$. Now, if $AB = A\Gamma$ we have that

$AB \subset A\Gamma$ and that $A\Gamma \subset AB$ therefore $B \subset \Gamma$ and $\Gamma \subset B$. This establishes that fact that $B = \Gamma$.

(b.) First we prove the statement for when B is a principal ideal. Then we will use Lemma 55 if B is not a principal ideal. Suppose that B is a principal ideal, this means that $B = (\beta)$ for some β in Υ. Hence, we have that $A \subset (\beta)$. Since $A \subset (\beta)$ we see that each element α of A is a multiple of β. Now, let $\Gamma = \beta^{-1}A$ be the set which consists of elements of the form $\beta^{-1}\alpha$ where α belongs to A. The set of quotients $\Gamma = \beta^{-1}A$ is an ideal of Υ and furtheremore, from the above equality we obtain that $B\Gamma = A$. Hence, B divides A in this case. Now, if B is not a principal ideal and $A \subset B$ we may multiply both sides of this set containment by $\overline{B}$ to obtain $\overline{B}A \subset \overline{B}B$; that is, $\overline{B}A \subset (m)$ for some m in $\mathbb{Z}$ by Lemma 55. By now letting Γ equal the set of quotients $m^{-1}\overline{B}A$ which is an ideal of Υ and applying similar reasoning as in the case where B was a principal ideal we obtain that $A = B\Gamma$. Hence B divides A.

(c.) Since Π divides the ideal AB this means that $AB \subset \Pi$. Now since Π is a prime ideal we have that $A \subset \Pi$ or $B \subset \Pi$ by Proposition 56. This is equivalent to saying Π divides A or Π divides B. □

Definition 58. ***(Maximal Ideal)***
Let M be a proper ideal of an integral domain Δ. The ideal M is called a ***maximal ideal*** *of Δ if whenever I is an ideal of Δ such that $M \subset I \subset \Delta$, then $I = M$ or $I = \Delta$.*

The following proposition is a powerful result. The fact that the notion of prime ideal and maximal ideal coincide in the ring of integers of an imaginary quadratic field is truly beautiful. Furthermore, as we will show, if a ring has the property that every prime ideal is maximal and vice-versa, then each ideal may be written as product of prime ideals uniquely, up to the order of each factor.

Proposition 59. *Let Φ be an imaginary quadratic number field and let Υ be its ring of integers.*

(a) The number of ideals between the nonzero ideal A and Υ is finite.

(b) If A is a proper ideal of Υ then it is contained in a maximal ideal.

(c) If Π is a nonzero prime ideal of Υ then it is a maximal ideal.

Proof. (a.) This follows from Lemma 53.

(b.) Since we know that there are finitely many ideals between $B \subset \Upsilon$ we can choose from these a maximal ideal containing B.

(c.) Let Π be a prime ideal. By part (b.) we know that there exists a maximal ideal M of Υ such that $\Pi \subset M$. Since $\Pi \subset M$ we know that there exists an ideal Γ of Υ such that $\Pi = M\Gamma$. Hence we see that $M\Gamma \subset \Pi$. Since Π is a prime ideal we obtain that $M \subset \Pi$ or $\Gamma \subset \Pi$. If $M \subset \Pi$ we obtain that $\Pi = M$ and therefore Π is a maximal ideal. If $\Gamma \subset \Pi$ then Π divides Γ and therefore there exists an ideal I of Υ such that $\Gamma = \Pi I$. Hence we obtain $\Pi = M\Pi I$ and hence $\Upsilon = MI$. Since $\Upsilon \subset M$ we obtain that $M = \Upsilon$ and therefore Π is also a maximal ideal in this case. □

We are now prepared for the main result. Before proving the main result a little background information should be given.

Number theory is a very fascinating subject. In number theory one is concerned about discovering truths about the ring of rational integers. When studying number theory it does not take long for one to realize how crucial the prime rational integers are to the subject. Many results in this field depend on the unique factorization of rational integers into prime factors. Beautiful things happen when a ring possesses unique prime factorization amongst its elements. Unfortuanately for us, the ring of integers in a quadratic number field seldom possesses unique prime factorization at the element level. As we have mentioned before, the ring $\mathbb{Z} + \mathbb{Z}[\sqrt{-5}]$ does not possess unique factorization amongst its elements.

Thanks to the ideas and work of mathematicians such as Ernst Kummer and Richard Dedekind, we now know that eventhough unique prime factorization does not always hold for elements in the ring of integers of an imaginary quadratic number field, unique prime ideal factorization will always hold. This is truly astonishing!

Theorem 60. *Let Υ be the ring of integers in an imaginary quadratic number field Φ. If A is a nonzero proper ideal of Υ then it may be written as a unique product of prime ideals of Υ, this factorization into prime ideals is unique up to the order of the factors.*

Proof. We begin by letting A be a nonzero proper ideal of Υ. By Proposition 59(b) we have that A will be contained in a maximal ideal Π_1, hence A is contained in a prime ideal of Υ. Since $A \subset \Pi_1$, by Proposition 57(b) we obtain that there exists an ideal Γ_1

of Υ such that $A = \Pi_1\Gamma_1$. Now either Γ_1 is a maximal ideal of Υ or it is not. If Γ_1 is a maximal ideal of Υ we are done. If Γ_1 is not a maximal ideal then there exist a maximal ideal Π_2, hence a prime ideal, of Υ which contains it. Therefore, we obtain that $\Gamma_1 \subset \Pi_2$ and therefore, $\Gamma_1 = \Pi_2\Gamma_2$ for some ideal Γ_2 of Υ. Thus, $A = \Pi_1\Pi_2\Gamma_2$. If Γ_2 is a maximal ideal of Υ then we are done with our factorization of A into prime ideals. If Γ_2 is not maximal then there exists a maximal ideal Π_3 which contains it. By Proposition 59(a) we have that there are finitely many ideals containing A and therefore this process will eventually terminate. Once this process has terminated we will be left the the factorization

$$A = \Pi_1\Pi_2 \cdots \Pi_n$$

where each Π_i is a maximal ideal and therefore a prime ideal. Thus, we have shown that a prime factorization for every ideal exists.

We now set out to prove the uniqueness of this factorization. Suppose that

$$A = O_1O_2 \cdots O_m$$

is another factorization of A into prime ideals of Υ. We then obtain the following,

$$O_1O_2 \cdots O_m = \Pi_1\Pi_2 \cdots \Pi_n.$$

Since the right hand side of the equation above is contained in Π_i for each i we get that $O_1O_2 \cdots O_m \subset \Pi_i$ for each i. This implies that each Π_i divides some O_j by Proposition 57(c). Hence, since each O_j and Π_i are maximal ideals of Υ, we obtain that each $\Pi_i = O_j$ for some i and j. If $m > n$, we may use Proposition 57(a) to cancel each of the $\Pi_i = O_j$ from both sides. After we do this we will be left with $O_{n+1} \cdots O_m = \Upsilon$, this equation implies that $\Upsilon \subset O_j$ for $n+1 \leq j \leq m$, and therefore $O_j = \Upsilon$ for $n+1 \leq j \leq m$. This is impossible since each prime ideal O_j is a proper ideal of Υ. If $n > m$, by a similar argument we will obtain that $\Upsilon = \Pi_{m+1} \cdots \Pi_n$ and therefore, each $\Pi_i = \Upsilon$ for $m+1 \leq i \leq n$. This is not possible since each prime ideal Π_i is a proper ideal of Υ. Therefore, $n = m$ and the factorization of A into prime ideals is unique, up to order of the factors. □

Bibliography

[1] Saban Alaca and Kenneth S. Williams. *Introductory Algebraic Number Theory*. Cambridge University Press, 2004.

[2] Michael Artin. *Algebra*. Prentice Hall, 1991.

[3] Richard Dedekind. *Theory of Algebraic Integers*. Cambridge University Press, 1996.

[4] Christina Jamroz. Ideal class group. 2009.

[5] Oscar Zariski and Pierre Samuel. *Commutative Algebra*, volume 1. Springer, 1958.