8-2022

# The HFD Property in Orders of a Number Field

Grant Moles
gmoles@clemson.edu

# The HFD Property in Orders of a Number Field

---

A Thesis
Presented to
the Graduate School of
Clemson University

---

In Partial Fulfillment
of the Requirements for the Degree
Master of Science
Mathematics

---

by
Grant Moles
August 2022

---

Accepted by:
Dr. James Coykendall, Committee Chair
Dr. Hui Xue
Dr. Keri Sather-Wagstaff
Dr. Kevin James

# Abstract

We will examine orders $R$ in a number field $K$. In particular, we will look at how the generalized class number of $R$ relates to the class number of its integral closure $\overline{R}$. We will then apply this to the case when $K$ is a quadratic field to produce a more specific relation. After this, we will focus on orders $R$ which are half-factorial domains (HFDs), in which the irreducible factorization of any element $\alpha \in R$ has fixed length. We will determine two cases in which $R$ is an HFD if and only if its ring of formal power series $R[[x]]$ is an HFD. Finally, we will consider how these strategies may apply (or fail to apply) to more general results.

# Dedication

This thesis is dedicated to those who have supported me in my educational journey: to my parents and siblings, my first teachers, who have always given me love and encouragement; to Dr. Griff Elder, who helped me realize and develop my love for mathematics; and to the countless teachers, friends, and colleagues who are too innumerable to name here, but without whom I never could have made it to this point. You all have my undying gratitude.

# Acknowledgments

I would like to thank Dr. Jim Coykendall for his support and guidance through my research and writing process. His wisdom and advice were invaluable to bringing this thesis to fruition.

# Table of Contents

# Chapter 1

# Introduction

## 1.1 Motivation and Background

When considering the structure of a ring $R$, it is often useful to determine how elements of $R$ factor. For example, in the ring $R = \mathbb{Z}$ of rational integers, it is well-known that the irreducible elements are the prime numbers (along with their negatives), and that any nonzero integer can be represented uniquely as a product of prime numbers (up to a negative sign). Unfortunately, it is also well-known that these nice properties of the integers do not necessarily hold in a general ring. A ring in which these properties hold is called a **unique factorization domain** (UFD), which will be defined more formally in the next section.

Since not every ring has the property of unique factorization, considering rings with weaker forms of factorization is often useful. Such rings include **atomic domains** (in which factorization into irreducibles is possible for every nonzero, nonunit element), **half-factorial domains** (HFDs) (in which any factorization of a given nonzero, nonzero element has a fixed length), and, in a sense, **Dedekind domains** (in which ideals factor uniquely into a product of prime ideals). Again, these concepts will be more formally defined in the next section.

In addition to determining the type of factorization observed in a given ring, it will also be beneficial to consider the relationship between the types of factorization observed in rings which are related to each other. That is, given two rings $R$ and $S$, a relationship between them, and the type of factorization observed in $R$, can we determine the type of factorization which occurs in $S$? The answer, perhaps unsurprisingly, is that we can for certain relationships and factorization types. For

example, in Chapter 4 it will be shown that if $S = R[[x]]$ (the ring of formal power series over $R$) and $S$ is an HFD, then $R$ is an HFD as well; moreover, the major results of this paper will show that in certain circumstances, $R$ is an HFD if and only if $R[[x]]$ is an HFD. By analyzing such relationships, we can in some cases determine the type of factorization that takes place in a relatively complex ring by only considering factorization in a less complicated related ring.

## 1.2 Commutative Ring Structures

This section will introduce definitions of various objects and terms that will be useful for the main results of this thesis. In addition, well-known or minor results which will be used later will be presented here. A basic understanding of abstract algebra concepts, including groups and rings, will be assumed. As promised, some of the terminology used in the introduction will now be presented formally. A fairly thorough treatment of most of the definitions and propositions in this section can be found in [10], though a few items will be drawn from other sources; specific citations for these can be found within the discussion below. Throughout this section, let $R$ be a commutative ring with identity 1.

### 1.2.1 Properties of elements

First, we will focus on the factorization properties of individual elements of $R$.

**Definition 1.2.1.** *Let $a, b \in R$. We say that $a$* **divides** *$b$, written $a \mid b$, if there exists some element $c \in R$ such that $b = ac$. In this case, we also say that $b$ is* **divisible** *by $a$.*

**Definition 1.2.2.** *An element $u \in R$ is called a* **unit** *if $u \mid 1$, i.e. there exists an element $v \in R$ such that $uv = 1$. In this case, $v$ is called the (multiplicative)* **inverse** *of $u$, usually denoted $u^{-1}$. The set of units in $R$ is denoted by $U(R)$ (or $R^\times$). Similarly, an element $a \in R$ is called a* **zero divisor** *if $a \mid 0$, i.e. there exists an element $b \in R$ such that $ab = 0$.*

**Proposition 1.2.3.** *$U(R)$ forms an abelian group under ring multiplication, called the* **group of units** *in $R$.*

*Proof.* Note that ring multiplication is automatically associative, $1 \in U(R)$ is a multiplicative identity, and $U(R)$ contains the (multiplicative) inverse of each of its elements trivially. Furthermore,

for any $u, v \in U(R)$, $(uv)(v^{-1}u^{-1}) = u(vv^{-1})u^{-1} = uu^{-1} = 1$. Then $U(R)$ is closed under ring multiplication. Thus, $U(R)$ is a group; since $R$ is commutative, it is an abelian group. $\square$

**Proposition 1.2.4.** *Let $R$ be finite. Then $\alpha \in R$ is a zero divisor if and only if it is a nonunit.*

*Proof.* Assume that $\alpha \in R$ is a unit. Then if $\beta \in R$ such that $\alpha\beta = 0$, note that $\beta = \alpha^{-1}\alpha\beta = 0$. Then if $\alpha$ is a unit, it is not a zero divisor. Note that this half of the proof does not depend on $R$ being finite.

Now assume that $\alpha$ is not a zero divisor. Then for any $\beta, \gamma \in R$, note that if $\alpha\beta = \alpha\gamma$, then $\alpha(\beta - \gamma) = 0$. Since $\alpha$ is not a zero divisor, then $\beta - \gamma = 0 \implies \beta = \gamma$. In other words, the mapping $\alpha : R \to R$ such that $\alpha(\beta) = \alpha\beta$ is injective. Since $R$ is a finite ring, this mapping must also be surjective. Then there is some $\beta \in R$ such that $\alpha\beta = 1$, i.e. $\alpha$ is a unit. $\square$

**Corollary 1.2.5.** *Let $R$ be a finite integral domain. Then $R$ is a field.*

**Definition 1.2.6.** *Let $R$ be an integral domain and $a, b \in R$. We say that $a$ and $b$ are* **associates** *if $a|b$ and $b|a$; equivalently, if $a = bu$ for some $u \in U(R)$.*

**Definition 1.2.7.** *A nonzero, nonunit element $p \in R$ is called* **prime** *if, whenever $p \mid ab$ for some $a, b \in R$, either $p \mid a$ or $p \mid b$.*

**Definition 1.2.8.** *Let $R$ be an integral domain. A nonzero, nonunit element $r \in R$ is said to be* **irreducible** *if, whenever $r = ab$ for some $a, b \in R$, either $a$ or $b$ is a unit. The set of irreducible elements in $R$ is denoted by* $\mathrm{Irr}(R)$.

**Example 1.2.9.** *In the ring $\mathbb{Z}$ of rational integers, $U(\mathbb{Z}) = \{\pm 1\}$ and $\mathrm{Irr}(\mathbb{Z})$ consists of the prime numbers and their negatives.*

Note that in this particular case, the concepts of prime and irreducible actually coincide. However, this will not always be the case.

**Proposition 1.2.10.** *Let $R$ be an integral domain and $\alpha \in R$ be prime. Then $\alpha$ is irreducible.*

*Proof.* Suppose that $\alpha = \beta\gamma$, with $\beta, \gamma \in R$. Now note that $\alpha|\beta\gamma$, and so by definition of a prime element, either $\alpha|\beta$ or $\alpha|\gamma$. Without loss of generality, assume that $\alpha|\beta$. Then write $\beta = \alpha\delta$ with $\delta \in R$. Then $\alpha = \alpha\delta\gamma \implies \delta\gamma = 1 \implies \gamma$ is a unit. Then whenever $\alpha$ is written as a product, one of the factors must be a unit, so $\alpha$ is irreducible. $\square$

**Example 1.2.11.** *Let $R = \mathbb{Z}[\sqrt{-5}]$. Then 2 is irreducible but not prime. Showing irreducibility of 2 in $R$ will straightforward using the norm, which we will develop later. However, note that $2|6 = (1+\sqrt{-5})(1-\sqrt{-5})$, but 2 does not divide either factor; then 2 is not prime.*

### 1.2.2 Special Types of Ideals

As we are considering factorization, we will need to consider not just the elements of $R$, but the ideals as well. To that end, we define the following.

**Definition 1.2.12.** *Let $I$ be an ideal in $R$. We say that $I$ is a* **principal ideal** *if there exists some $\alpha \in I$ such that $\alpha$ divides every element in $I$. In this case, we say that $\alpha$* **generates** *$I$, and we write $I = (\alpha)$.*

**Proposition 1.2.13.** *Let $R$ be an integral domain. Then $(a) = (b)$ if and only if $a$ and $b$ are associates.*

*Proof.* Note that $(a) = (b)$ if and only if $a \in (b)$ and $b \in (a)$, which is true if and only if $b|a$ and $a|b$, the definition of $a$ and $b$ being associates. □

**Definition 1.2.14.** *Let $P$ be a proper ideal in $R$. We say that $P$ is a* **prime ideal** *if $ab \in P$ for $a, b \in R$ implies that either $a \in P$ or $b \in P$.*

**Proposition 1.2.15.** *A nonzero principal ideal $(\alpha)$ is prime if and only $\alpha$ is a prime element of $R$.*

**Definition 1.2.16.** *Let $M$ be a proper ideal in $R$. We say that $M$ is a* **maximal ideal** *if the only ideal of $R$ strictly containing $M$ is $R$ itself. In other words, if $I$ is an ideal of $R$ such that $M \subseteq I$, either $I = M$ or $I = R$.*

**Proposition 1.2.17.** *Let $I$ be an ideal in $R$. Then $I$ is maximal if and only if $R/I$ is a field. Furthermore, $I$ is prime if and only if $R/I$ is an integral domain.*

*Proof.* First, assume that $I$ is a maximal ideal of $R$, i.e. the only ideal of $R$ strictly containing $I$ is $R$. Now for any ideal $J$ of $R/I$, note that $J'$, the set of all elements of $R$ whose coset in $R/I$ lies in $J$, is an ideal of $R$ (in fact, $J'$ is the preimage of $J$ under the natural projection map from $R$ to $R/I$). Furthermore, since $J$ contains the 0 element of $R/I$, $I \subseteq J'$. Thus, for any ideal $J$ of $R/I$, either $J' = I$ (in which case $J' = \{0\}$) or $J' = R$ (in which case $J = R/I$). Then any nonzero ideal

of $R/I$ is the entirety of $R/I$. Applying this to any nonzero principal ideal $(\alpha)$ of $R/I$, we get that $(\alpha) = R/I \implies \alpha \in U(R/I) \implies R/I$ is a field.

Now if we assume that $R/I$ is a field, note that any ideal $J$ of $R$ strictly containing $I$ has an image $J'$ under the natural projection map from $R$ to $R/I$ which is an ideal of $R/I$. Then since $J$ strictly contains $I$, $J' \neq \{0\}$. Thus, $J' = R/I$, the only nonzero ideal of the field $R/I$. Then necessarily, $J = R$. Then the only ideal of $R$ strictly containing $I$ is $R$, so $I$ is maximal.

Now assume that $I$ is a prime ideal, i.e. for $a, b \in R$, $ab \in I \iff$ either $a \in I$ or $b \in I$. This is equivalent to saying that $(a + I)(b + I) = 0$ in $R/I \iff$ either $a + I = 0$ or $b + I = 0$, i.e. $R/I$ is an integral domain. This shows both directions of this implication. □

**Corollary 1.2.18.** *Any maximal ideal of $R$ is also prime.*

*Proof.* Let $M$ be a maximal ideal of $R$. Then $R/M$ is a field and thus an integral domain. Then $M$ is also prime. □

We will now show an important result regarding maximal ideals. It should be noted that this proposition uses Zorn's Lemma, and thus requires the Axiom of Choice.

**Proposition 1.2.19.** *Let $R$ be a ring and $I$ a proper ideal of $R$. Then $I$ is contained in a maximal ideal of $R$.*

*Proof.* Consider the set $S$ of proper ideals of $R$ which contain $I$. This set is partially ordered by the inclusion relation. Now for any totally ordered subset $T$ of $S$ (i.e. if $I, J \in T$, then either $I \subseteq J$ or $J \subseteq I$), consider $J := \bigcup_{A \in T} A$. Because $T$ is totally ordered, it can easily be seen that $J$ is in fact an ideal of $R$. Furthermore, $I \subseteq A \subseteq J$ for every $A \in T$, so $J$ contains $I$. Finally, note that since each $A \in T$ is a proper ideal of $R$, $1 \notin A$ for every $A \in T$; thus, $1 \notin J$. Then $J$ is a proper ideal of $R$ which contains $I$, so $J \in S$. Then $T$ has upper bound $J$ in $S$, meaning that we can apply Zorn's Lemma. This states that $S$ has at least one maximal element $M$, i.e. there exists a proper ideal $M$ of $R$ which contains $I$ and which is not contained in any proper ideal of $R$ containing $I$. Then $M$ is a maximal ideal of $R$, so $I$ is contained in the maximal ideal $M$. □

**Corollary 1.2.20.** *Let $R$ be a ring and $\alpha \in R$ a nonunit. Then $\alpha$ is contained in a maximal ideal of $R$.*

*Proof.* This is a direct result of the proposition applied to the proper ideal $(\alpha)$. □

### 1.2.3 Special Domains

Now that we have some basic terminology to work with, we are ready to define special types of integral domains. In this subsection, $R$ will be assumed to be an integral domain.

**Definition 1.2.21.** *Consider the following three conditions on $R$:*

*I. Every nonzero, nonunit element $\alpha \in R$ can be written as a product of irreducibles, i.e. $\alpha = \pi_1 \dots \pi_n$ for some $n \in \mathbb{N}$, $\pi_i \in \mathrm{Irr}(R)$ for $1 \leq i \leq n$.*

*II. If $\pi_i, \tau_j \in \mathrm{Irr}(R)$ for $1 \leq i \leq m$, $1 \leq j \leq n$ and $\pi_1 \dots \pi_m = \tau_1 \dots \tau_n$, then $m = n$.*

*III. If $\pi_i, \tau_i \in \mathrm{Irr}(R)$ for $1 \leq i \leq n$ and $\pi_1 \dots \pi_n = \tau_1 \dots \tau_n$, then for every $1 \leq i \leq n$, $\pi_i$ is an associate of $\tau_j$ for some $j$, $1 \leq j \leq n$.*

*$R$ is called an* **atomic domain** *if condition I holds. $R$ is called a* **half-factorial domain** *(HFD) if conditions I and II hold. $R$ is called a* **unique factorization domain** *(UFD) if conditions I, II, and III hold.*

One will note quite trivially from these definitions that $R$ is a UFD $\implies$ $R$ is an HFD $\implies$ $R$ is atomic. However, the reverse implications do not hold, as evidenced by the following examples.

**Example 1.2.22.** *$\mathbb{Z}$, $\mathbb{Z}[i]$, and $\mathbb{Z}[x]$ are all UFDs. If $K$ is a field, then $K[x]$ is a UFD.*

**Example 1.2.23.** *$\mathbb{Z}[\sqrt{-5}]$ is an HFD which is not a UFD. Furthermore, if $K, L$ are fields with $K \subset L$, then $K + xL[x]$ is an HFD which is not a UFD.*

The quintessential example of non-unique factorization is $2 \cdot 3 = 6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$. Each term is irreducible and the elements on the left are not associates of the elements on the right, as we will more clearly be able to see after defining the norm (see Example 1.3.27 at the end of this chapter). However, note that these factorizations are the same length in $\mathbb{Z}[\sqrt{-5}]$. See [7] for a full proof that $\mathbb{Z}[\sqrt{-5}]$ is an HFD.

The half-factorial property in a general factorization is more visible in $K + xL[x]$. Since the group of units is $U(K + xL[x]) = K$, irreducible elements must be of the form $ax$ for some $a \in K$ or $a(1 + xf(x))$ for some $a \in K$, $f(x) \in L[x]$, $1 + xf(x)$ irreducible in $L[x]$. Then factoring any $f \in K + L[x]$ into a product of irreducibles, we can see that each irreducible must be an associate of an irreducible in $L[x]$. Then the number of irreducibles in any factorization of $f$ in $K + xL[x]$

is the same as the number in the corresponding factorization in $L[x]$. Since $L[x]$ is a UFD, these factorizations are of fixed length, and thus $K+xL[x]$ is an HFD. However, note that for any $a \in L\backslash K$, $x^2 = x \cdot x = (ax)(a^{-1}x)$ is an example of non-unique factorization in $K + xL[x]$.

**Example 1.2.24.** **[9]** $\mathbb{Z}[\omega]$*, where* $\omega = e^{\frac{2\pi}{23}}$*, a primitive* $23^{rd}$ *root of* 1*, is an atomic domain which is not an HFD.*

**Example 1.2.25.** $R = \mathbb{Z}+x\mathbb{Q}[x]$ *is an integral domain which is not atomic. In particular,* $x$ *cannot be written as a product of irreducible elements.*

Each of the three types of domains introduced above rely specifically on the type of factorization that we see in its elements. The following domain does not explicitly reference factorization in its definition; nonetheless, we will see that it is intimately connected to the previous discussion.

**Definition 1.2.26.** $R$ *is called a* **principal ideal domain** *(PID) if every ideal* $I$ *of* $R$ *is principal, i.e.* $I = (\alpha)$ *for some* $\alpha \in R$*.*

**Proposition 1.2.27.** *Let* $R$ *be a PID. Then* $R$ *is a UFD.*

*Proof.* First, we will show that $R$ is atomic; then we will show that $R$ is a UFD. Let $\alpha_1 \in R$ be an arbitrary nonzero, nonunit element. If $\alpha_1$ is irreducible, then it trivially factors into irreducibles. Otherwise, we can factor $\alpha_1 = \alpha_2\beta_2$, with neither $\alpha_2$ nor $\beta_2$ a unit. If both $\alpha_2$ and $\beta_2$ factor into irreducibles, then so does $\alpha_1$. Otherwise, one does not (without loss of generality, assume it is $\alpha_2$) and we can further factor $\alpha_2 = \alpha_3\beta_3$, with neither factor a unit. Continue factoring in this way to produce a sequence $\alpha_1, \alpha_2, \ldots$ of elements in $R$ such that $(\alpha_1) \subset (\alpha_2) \subset \ldots$, with these inclusions being strict.

Now consider $I = \bigcup_{i=1}^{\infty}(\alpha_i)$. Because of the inclusion relations above, we can easily confirm that $I$ is actually an ideal in $R$. Then since $R$ is a PID, $I = (\alpha)$ for some $\alpha \in R$. Then $\alpha \in (\alpha_n)$ for some $n \in \mathbb{N}$; moreover, $\alpha_n \in (\alpha)$, so $(\alpha_n) = (\alpha)$. Thus, for any $m \geq n$, $(\alpha_n) \subseteq (\alpha_m) \subseteq (\alpha) \implies (\alpha_n) = (\alpha_m)$, contradicting inclusions being strict by construction. Then $\alpha_1$ must actually factor into irreducibles, meaning that the sequence of strict ideal inclusions above is actually finite. This property of ideals is commonly referred to as the Ascending Chain Condition (ACC), which we will revisit later when defining a Noetherian domain.

We have now shown that $R$ is atomic, i.e. every nonzero, nonunit element factors into irreducibles. Now we need to show that this factorization is unique as in the definition of a UFD.

First, let $\pi \in R$ be irreducible. Then if $I$ is an ideal containing $(\pi)$, we have that $I = (\alpha)$ for some $\alpha \in R$ and thus $\alpha|\pi$. Then either $\alpha$ is a unit, in which case $I = R$, or $\alpha$ is an associate of $\pi$, in which case $I = (\pi)$. Then $(\pi)$ is a maximal ideal, so we know that $(\pi)$ is a prime ideal and $\pi$ is a prime element.

Now consider two equal factorizations $\pi_1 \dots \pi_m = \tau_1 \dots \tau_n$, with each $\pi_i$, $\tau_j$ irreducible in $R$; without loss of generality, assume that $m \geq n$. Since $\pi_1$ is prime and $\pi_1|\tau_1 \dots \tau_n$, we have by repeated application of the definition of primeness that $\pi_1|\tau_j$ for some $j$, $1 \leq j \leq n$. Without loss of generality, assume that $\pi_1|\tau_1$. Then $(\tau_1) \subseteq (\pi_1) \neq R$, so by maximality of $(\tau_1)$, we have $(\tau_1) = (\pi_1)$, i.e. $\pi_1$ and $\tau_1$ are associates. Thus, $\pi_1 = u_1\tau_1$ for some $u_1 \in U(R)$, so $u_1\pi_2 \dots \pi_m = \tau_2 \dots \tau_n$. Note that $u_1\pi_2$ is still irreducible. Then we can continually apply this process to reduce this equality (after reordering, if necessary), to $u\pi_{n+1} \dots \pi_m = 1$, with $u \in U(R)$. However, since each $\pi_i$ is irreducible (and thus a nonunit), we get a contradiction unless $m = n$. Then $m = n$ and each $\pi_i$ is an associate of $\tau_i$ (after potential reordering), meaning that $R$ is in fact a UFD. □

This proof contains an important result that may get lost in the weeds, so we include it here as a corollary:

**Corollary 1.2.28.** *Let $R$ be a PID. Then an element $\alpha \in R$ is prime if and only if it is irreducible. More generally, this will hold when $R$ is a UFD.*

*Proof.* We have already shown in the above proof that this holds for a PID, so we will only show the result when $R$ is a UFD (which will actually imply that it holds for a PID). We already know that any prime element is irreducible. Then we need only show that in a UFD, any irreducible element is prime.

Let $R$ be a UFD, $\pi \in R$ irreducible, and $a, b \in R$ such that $\pi|ab$. Then $ab = c\pi$ for some $c \in R$. Since $R$ is a UFD, we can write each of $a$, $b$, and $c$ as a product of irreducibles: $a = \alpha_1 \dots, \alpha_r$, $b = \beta_1 \dots, \beta_s$, $c = \gamma_1 \dots \gamma_t$. Then by the UFD property, $r + s = t + 1$ and each irreducible on one side of the equation is an associate of an irreducible on the other. In particular, $\pi$ is an associate of some $\alpha_i$ or $\beta_j$; without loss of generality, assume that $\pi$ is an associate of $\alpha_1$. Then $\pi|\alpha_1$ and $\alpha_1|a$, so $\pi|a$. Then if $\pi|ab$ for some $a, b \in R$, $\pi$ must divide either $a$ or $b$; then $\pi$ is prime. □

### 1.2.4 More Domains and Rings

In addition to these more standard types of domains that one might see in an introductory algebra course, we will also need to define some more advanced objects to obtain later results. In this subsection, $R$ is no longer assumed to be an integral domain unless otherwise specified, though $R$ will still be assumed commutative. First, we need some additional terminology.

**Definition 1.2.29.** *Let $P$ be a prime ideal in $R$. The* **height** *of $P$ is defined to be the supremum of all $n \in \mathbb{N}$ such that there exist prime ideals $P_0, P_1, \ldots, P_{n-1}, P_n = P$ with $P_0 \subset P_1 \subset \cdots \subset P_n$, these inclusions being strict (called a* **chain of prime ideals***). This is sometimes denoted* $\mathrm{ht}(P)$.

**Definition 1.2.30.** *The* **Krull dimension** *of $R$, denoted* $\dim(R)$*, is the supremum of the lengths of all chains of prime ideals. In other words,* $\dim(R) := \sup\{\mathrm{ht}(P) : P \text{ prime ideal of } R\}$.

**Definition 1.2.31.** *Let $S$ be a multiplicatively closed subset of $R$ and suppose that $S$ contains no zero divisors. The* **localization** *of $R$ by $S$, denoted $S^{-1}R$, is the smallest ring containing $R$ in which every element of $S$ is a unit. In other words, $S^{-1}R := \{s^{-1}r : s \in S, r \in R\}$.*

**Example 1.2.32.** *Let $P$ be a prime ideal of $R$. Then $R\backslash P$ is a multiplicatively closed set. The localization $(R\backslash P)^{-1}R$ is commonly referred to as the* **localization of $R$ at $P$** *and denoted $R_P$.*

**Example 1.2.33.** *Let $R$ be an integral domain. Then $R\backslash\{0\}$ is a multiplicatively closed set. The localization $(R\backslash\{0\})^{-1}R$ is commonly referred to as the* **field of fractions** *of $R$.*

**Definition 1.2.34.** *$R$ is called a* **local ring** *if $R$ contains a unique maximal ideal.*

A local ring can actually be defined more generally for any ring $R$ with unity, not just commutative $R$. For our purposes, we will only consider commutative local rings. It should also be noted that the definition presented here is sometimes called a **quasi-local ring**. In this case, a local ring is considered to be a quasi-local ring which is also Noetherian (defined later). For the purposes of this thesis, we will opt for the definition presented above.

Now as one might expect, the terms "localization" and "local ring" are related, as the following proposition shows.

**Proposition 1.2.35.** *Let $P$ a prime ideal of $R$. Then $R_P$ is a local ring with maximal ideal $PR_P$.*

*Proof.* Let $S := \{\alpha\beta^{-1} : \alpha \in P, \beta \in R\backslash P\} \subseteq R_P$. Note that for $\alpha_1\beta_1^{-1}, \alpha_2\beta_2^{-1} \in S$, $\alpha_1\beta_1^{-1} + \alpha_2\beta_2^{-1} = (\alpha_1\beta_2 + \alpha_2\beta_1)(\beta_1\beta_2)^{-1}$. Since $P$ is prime, $\beta_1\beta_2 \in R\backslash P$, and so $S$ is closed under addition. Now any

$\alpha\beta^{-1} \in S$ is a product of $\alpha \in P$ and $\beta^{-1} \in R_P$, so $S \subseteq PR_P$. Furthermore, if we take $\alpha \in P$ and $\beta\gamma^{-1} \in R_P$ with $\beta \in R$, $\gamma \in R\backslash P$, note that $\alpha(\beta\gamma^{-1}) = (\alpha\beta)\gamma^{-1} \in S$. Then since $S$ is closed under addition, $PR_P \subseteq S$. Then $PR_P = S$.

Note that $1 \notin PR_P$, so $R_P\backslash PR_P \neq \emptyset$. Now let $\alpha \in R_P\backslash PR_P$. Then by the above argument, $\alpha = \beta\gamma^{-1}$, with $\beta, \gamma \in R\backslash P$. Thus, $\alpha^{-1} = \gamma\beta^{-1} \in R_P$, so $\alpha \in U(R_P)$. Therefore, any ideal strictly containing $PR_P$ must contain a unit and must thus be all of $R_P$. Then $PR_P$ is a maximal ideal. Furthermore, any ideal $I \neq PR_P$ of $R_P$ must either be a subset of $PR_P$ (and is thus not maximal) or must contain an element which is not in $PR_P$, a unit (and is thus $R_P$). Then since any ideal is either contained in $PR_P$ or is the entire ring, $PR_P$ is the unique maximal ideal of $R_P$, so $R_P$ is a local ring. □

**Definition 1.2.36.** *Let $R$ and $S$ be integral domains with $R \subseteq S$. We say that $\alpha \in S$ is* **integral** *over $R$ if $\alpha$ is a root of some monic polynomial $f \in R[x]$. The set of all elements of $S$ which are integral over $R$ is called the* **integral closure** *of $R$ in $S$, denoted $\overline{R}_S$. If $R = \overline{R}_S$, we say that $R$ is* **integrally closed** *in $S$. If $S = \overline{R}_S$, we say that $S$ is an* **integral extension** *of $R$. When $S$ is not specified, it is assumed to be the field of fractions of $R$.*

**Definition 1.2.37.** *Let $R$ and $S$ be integral domains with $R \subseteq S$. We say that $\alpha \in S$ is* **almost integral** *over $R$ if there exists some nonzero $r \in R$ such that $r\alpha^n \in R$ for every $n \in \mathbb{N}$. If the set of elements in $S$ which are almost integral over $R$ is just $R$ itself, we say that $R$ is* **completely integrally closed** *in $S$. Again, if $S$ is not specified, it is assumed to be the field of fractions of $R$.*

**Proposition 1.2.38.** *Let $R$ be an integral domain with field of fractions $K$. If $\alpha \in K$ is integral over $R$, it is also almost integral over $R$.*

*Proof.* Since $\alpha \in K$, we can write $\alpha = \frac{a}{b}$, with $a, b \in R$. Furthermore, since $\alpha$ is integral over $R$, we have that $\alpha^k + a_{k-1}\alpha^{k-1} + \cdots + a_1\alpha + a_0 = 0$ for some $k \in \mathbb{N}$ and $a_i \in R$, $0 \leq i \leq k-1$. With this notation, set $r = b^{k-1}$. Then for $1 \leq n \leq k-1$, note that $r\alpha^n = b^{k-1-n}a^n \in R$. Now for $n \geq k$, assume that $r\alpha^m \in R$ for every $m < n$. Then

$$r\alpha^n = r\alpha^{n-k}\alpha^k = -r\alpha^{n-k}(a_{k-1}\alpha^{k-1}+\cdots+a_1\alpha+a_0) = -r(a_{k-1}\alpha^{n-1}+\cdots+a_1\alpha^{n-k+1}+a_0\alpha^{n-k}) \in R.$$

Then by induction, $r\alpha^m \in R$ for every $n \in \mathbb{N}$, so $\alpha$ is almost integral over $R$. □

**Corollary 1.2.39.** *Let $R$ be an integral domain. If $R$ is completely integrally closed in its field of fractions, then it is also integrally closed in its field of fractions.*

**Proposition 1.2.40.** *Let $R$ and $S$ be integral domains with $R \subseteq S$ and $S$ an integral extension of $R$. Then $U(R) = R \cap U(S)$.*

*Proof.* First, note that if $r \in U(R)$, then $r \in R$ and there exists some $s \in R$ such that $rs = 1$. Then since $r, s \in R \subseteq S$, $r \in R \cap U(S)$. Thus, $U(R) \subseteq R \cap U(S)$.

Now assume that $r \in R \cap U(S)$. Then there is some $s \in S$ such that $rs = 1$. Since $S$ is an integral extension of $R$, we have that $s$ is a root of some monic polynomial $f \in R[x]$. Let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ with $a_i \in R$ for $0 \leq i \leq n-1$. Then $f(s) = s^n + a_{n-1}s^{n-1} + \cdots + a_1s + a_0 = 0 \implies r^{n-1}f(s) = s + a_{n-1} + \cdots + r^{n-2}a_1 + r^{n-1}a_0 = 0$. Thus, $s = -(a_{n-1} + \cdots + r^{n-2}a_1 + r^{n-1}a_0)$, and since $r, a_i \in R$, $s \in R$ as well. Then $r \in U(R)$, so $R \cap U(S) \subseteq U(R)$. Thus, $U(R) = R \cap U(S)$. □

With these definitions, we are now ready to introduce more types of rings.

**Definition 1.2.41.** *$R$ is called a* **Noetherian ring** *if any ascending chain of ideals $I_1 \subseteq I_2 \subseteq \ldots$ is eventually constant; equivalently, if the ascending chain is assumed to be a chain of strict inclusions, it is necessarily finite. This is called the* **ascending chain condition** *(ACC) for ideals of $R$.*

If we assume the Axiom of Choice, we also have the following equivalent definitions of a Noetherian ring.

**Proposition 1.2.42.** *The following conditions are equivalent for $R$:*

*(1) The ACC for ideals of $R$.*

*(2) Every nonempty collection $S$ of ideals of $R$ has a maximal member, i.e. there exists some $M \in S$ such that $M \subseteq I \in S \implies M = I$.*

*(3) Every ideal of $R$ is finitely generated.*

*Then $R$ is a Noetherian ring if it satisfies any one of these conditions.*

*Proof.* First, assume that condition (1) holds for $R$, and let $S$ be any nonempty collection of ideals of $R$. Since $S$ is nonempty, we can pick some ideal from $S$ and call it $I_1$. If $I_1$ is maximal in $S$, then $S$ contains a maximal element. Otherwise, the subset of $S$ consisting of ideals which properly contain

$I_1$ is nonempty. Again, pick one such ideal and call it $I_2$. Repeat this process, which will either terminate at a maximal member $I_n$ of $S$ or produce a strictly ascending chain of ideals $I_1 \subset I_2 \subset \ldots$. However, this contradicts the ascending chain condition for ideals of $R$, meaning that the process must terminate at some maximal member of $S$. Then any nonempty collection $S$ of ideals of $R$ has a maximal member. Thus, (1) $\implies$ (2).

Now assume that condition (2) holds and let $I$ be an arbitrary ideal of $R$. Define $S$ to be the collection of all finitely generated subideals of $I$. Clearly $S$ is nonempty; for instance, $(\alpha) \in S$ for any $\alpha \in I$. Then by condition (2), $S$ has a maximal member $M$. If $M = I$, then $I$ is finitely generated. Otherwise, there exists some $\alpha \in I \backslash M$. However, note that $(\alpha, M)$ is a subideal of $I$ which is finitely generated (by $\alpha$ and the finitely many generators of $M$). However, this means that $(\alpha, M)$ is an element of $S$ which strictly contains $M$, a contradiction. Then $M = I$, so $I$ is finitely generated. Thus, (2) $\implies$ (3).

Now assume that condition (3) holds and let $I_1 \subseteq I_2 \subseteq \ldots$ be an infinite ascending chain of ideals (not necessarily strictly ascending). Then note that because of this chain behavior, $I = \bigcup_{i=1}^{\infty} I_i$ is an ideal of $R$. By condition (3), $I$ is finitely generated, so $I = (\alpha_1, \ldots, \alpha_n)$ for some $\alpha_i \in R$, $1 \leq i \leq n$. For each $i$, $1 \leq i \leq n$, we have that $\alpha_i \in I$, so there exists some $m_i \in \mathbb{N}$ such that $\alpha_i \in I_{m_i}$. Then let $M = \max\{m_i : 1 \leq i \leq n\}$ and note that $\alpha_i \in I_M$ for every $1 \leq i \leq n$. Then $I \subseteq I_M$. Then for any $k \geq M$, $I_M \subseteq I_k \subseteq I \subseteq I_M$, so $I_k = I_M$. Thus, the ascending chain of ideals is eventually constant. Then (3) $\implies$ (1). $\square$

**Proposition 1.2.43.** *Let $R$ be a Noetherian domain. Then $R$ is atomic.*

*Proof.* See the first paragraph of the proof of Proposition 1.2.27 and note that the assumption that $R$ is a PID is not used. Then if any nonzero, nonunit element does not factor into irreducibles, we get an infinite strictly ascending chain of ideals. Since $R$ is Noetherian, we get a contradiction. Then $R$ must be atomic. $\square$

**Definition 1.2.44.** *A Noetherian local ring $R$ is called a* **regular local ring** *if its unique maximal ideal is minimally generated by $\dim(R)$ elements. In other words, if $n = \dim(R)$ is the Krull dimension of $R$ and $M$ is the unique maximal ideal of $R$, then there exist $\alpha_1, \ldots, \alpha_n \in R$ such that $M = (\alpha_1, \ldots, \alpha_n)$, and $M$ cannot be generated by fewer than $n$ elements.*

**Definition 1.2.45.** *A Noetherian ring $R$ is called a* **regular ring** *if, for any prime ideal $P$ of $R$, $R_P$ is a regular local ring.*

**Proposition 1.2.46.** *Let $R$ be a regular local ring. Then $R$ is a UFD.*

*Proof.* See [10], Theorem 20.3. □

**Corollary 1.2.47.** *Let $R$ be a regular ring. Then $R$ is locally factorial, i.e. for every prime ideal $P$ of $R$, $R_P$ is a UFD.*

**Definition 1.2.48.** *An integral domain $R$ is called a* **discrete valuation ring** *(DVR), or* **discrete valuation domain** *(DVD), if it is a local PID which is not a field.*

It should be noted that while this is the standard definition of a DVR in algebraic number theory, a DVR is often defined more generally in commutative algebra. In this case, the definition presented here might more accurately be termed a **Noetherian valuation domain**, though for the purposes of this thesis we will use the terminology presented in Definition 1.2.48.

The term "discrete valuation ring" may at first glance be ill-fitting for the definition provided. However, upon further investigation we find that the name is quite appropriate.

**Proposition 1.2.49.** *Let $R$ be a DVR with unique maximal ideal $M = (\pi)$ and field of fractions $K$. Then any nonzero element $\alpha \in K$ can be expressed uniquely as $\alpha = u\pi^n$ for some $u \in U(R)$ and $n \in \mathbb{Z}$.*

*Proof.* First, note that since $M$ is a maximal principal ideal, we have that $\pi$, a generator of $M$, must be irreducible. Moreover, as shown in the proof of Proposition 1.2.27, $R$ being a PID means that any irreducible element $\tau \in R$ generates a maximal ideal. Then since $M$ is the unique maximal ideal of $R$, $M = (\pi) = (\tau)$, i.e. $\pi$ and $\tau$ are associates.

Now for any nonzero $\alpha \in K$, we can write $\alpha = \frac{\beta}{\gamma}$, with $\beta, \gamma \in R$, both nonzero. Since $R$ is a PID, it is also a UFD, so we can write $\beta = \pi_1 \dots \pi_r$ and $\gamma = \tau_1 \dots \tau_s$ for some irreducible elements $\pi_i$, $\tau_j$ in $R$. Now since each $\pi_i$ and $\tau_j$ is irreducible in $R$, they must each be an associate of $\pi$. Then writing each $\pi_i$ and $\tau_j$ as a unit multiple of $\pi$ and combining units, we get that $\beta = u_1\pi^r$ and $\gamma = u_2\pi^s$, with $u_1, u_2 \in U(R)$ and $r, s \in \mathbb{N} \cup \{0\}$. Then $\alpha = u\pi^n$, with $u = \frac{u_1}{u_2} \in U(R)$ and $n = r - s \in \mathbb{Z}$. Moreover, this representation is unique; if $u\pi^n = v\pi^m$ for some $u, v \in U(R)$ and $n, m \in \mathbb{Z}$, then $\pi^{n-m} = \frac{v}{u} \in U(R) \implies n - m = 0 \implies n = m \implies \frac{v}{u} = 1 \implies u = v$. □

**Definition 1.2.50.** *Let $R$ be a DVR with unique maximal ideal $M = (\pi)$ and field of fractions $K$. Then the function $v : K \to \mathbb{Z} \cup \{\infty\}$ such that $v(u\pi^n) = n$ for any $u \in U(R)$ and $n \in \mathbb{Z}$ and*

$v(0) = \infty$ *is called the* **valuation** *on* $K$ *associated to* $R$*. Since* $v$ *has image* $\mathbb{Z} \cup \{\infty\}$*,* $v$ *is called a* **discrete valuation**.

**Definition 1.2.51.** *Let* $R$ *be an integral domain and define* $\mathcal{P}$ *to be the collection of prime ideals of* $R$ *which have height 1. Then* $R$ *is called a* **Krull domain** *if it has the following properties:*

1. *For every* $P \in \mathcal{P}$*,* $R_P$ *is a DVR.*
2. $R = \bigcap_{P \in \mathcal{P}} R_P$*.*
3. *Any nonzero element of* $R$ *is contained in only finitely many members of* $\mathcal{P}$*.*

**Proposition 1.2.52.** *Let* $R$ *be a Krull domain. Then* $R$ *is completely integrally closed.*

*Proof.* See [5], Theorem 3.6. □

**Definition 1.2.53.** *Let* $R$ *be an integral domain. Then* $R$ *is called a* **Dedekind domain** *if it has the following properties:*

1. $R$ *is Noetherian.*
2. $\dim(R) \leq 1$*; in other words, every nonzero prime ideal is maximal.*
3. $R$ *is integrally closed.*

As we will see in the next chapter, Dedekind domains will be very important to the results we will discuss in this paper. Furthermore, Dedekind domains admit a special type of factorization, namely unique factorization of ideals into products of prime ideals. These discussions and results can be found in Chapter 2.

The last type of ring we will present here is actually a special type of subring.

**Definition 1.2.54.** *Let* $R$ *be a finite-dimensional algebra over* $\mathbb{Q}$*. A subring (with unity)* $\mathcal{O}$ *of* $R$ *is called an* **order** *in* $R$ *if the additive group of* $\mathcal{O}$ *is a free abelian group generated by a basis for* $R$ *over* $\mathbb{Q}$*.*

Although we will later pare this down to a simpler definition specifically in the types of rings we are concerned with, it will help to keep this more general definition in mind.

**Example 1.2.55.** *Let* $R = \mathbb{Q}[\sqrt{2}]$*, a 2-dimensional algebra over* $\mathbb{Q}$*. Then* $\mathbb{Z}[\sqrt{2}]$ *is an order in* $R$*. In fact,* $\mathbb{Z}[n\sqrt{2}]$ *is an order in* $R$ *for any* $n \in \mathbb{N}$*.*

This example is actually a special case of a more general result which we will show and use in later chapters.

### 1.2.5 Two Class Groups

The final piece of commutative algebra we will need to develop before continuing are the two concepts of a class group of ideals. First, we will need to introduce the idea of a fractional ideal. Much of the discussion here will come from [5].

**Definition 1.2.56.** *Let $R$ be an integral domain with field of fractions $K$. A* **fractional ideal** *$I$ of $R$ is an $R$-submodule of $K$ for which there exists some nonzero $\alpha \in R$ such that $\alpha I \subseteq R$.*

With this definition, we can see why the term "fractional" ideal is appropriate; in some sense, this is an ideal of $R$ with fractional parts allowed. In this interpretation, $\alpha$ serves to clear out denominators. In fact, we have the following equivalent definition of a fractional ideal.

**Proposition 1.2.57.** *Let $R$ be an integral domain with field of fractions $K$. Then $I$ is a fractional ideal of $R$ if and only if $I = \alpha^{-1}J$ for some $\alpha \in R$ and ideal $J$ in $R$.*

*Proof.* Let $I$ be a fractional ideal of $R$. Then there is some $\alpha \in R$ such that $J := \alpha I \subseteq R$. Note that $I = \alpha^{-1}J$. Furthermore, since $I$ is closed under addition, contains 0 and additive inverses, and absorbs multiplication from $R$, $J$ inherits those traits. Then since $J \subseteq R$, $J$ is an ideal in $R$.

Now if $I = \alpha^{-1}J$ for some $\alpha \in R$ and ideal $J$ of $R$, note that $I$ is a module by the inverse of the previous argument. Then since $\alpha I = J \subseteq R$, $I$ is a fractional ideal. □

When both ideals in $R$ and fractional ideals of $R$ are being considered, an ideal in $R$ is often referred to as an **integral ideal** to avoid confusion.

**Definition 1.2.58.** *Let $R$ be an integral domain and $I$ a fractional ideal of $R$. The* **inverse** *of $I$, $I^{-1}$ is defined to be the set $I^{-1} := \{\alpha \in K : \alpha I \subseteq R\}$.*

**Proposition 1.2.59.** *Let $I, J$ be nonzero fractional ideals of $R$. Then $I^{-1}$ as defined above and the standard product $IJ := \{\alpha_1\beta_1 + \cdots + \alpha_n\beta_n : n \in \mathbb{N}, \alpha_i \in I, \beta_j \in J\}$ are also a nonzero fractional ideals.*

*Proof.* First, note that $I^{-1}$ as defined above is a subset of $K$ which contains 0, is closed under additive inverses and addition, and absorbs multiplication from $R$. Then $I^{-1}$ is an $R$-submodule of

$K$. Since by definition there is some nonzero $\alpha \in R$ such that $\alpha I \subseteq R$, note that $\alpha \in I^{-1}$, so $I^{-1}$ is a nonzero $R$-submodule of $K$. Furthermore, for any nonzero $\alpha \in I$, note that $\alpha = \frac{a}{b}$, with $a, b \in R$ (both nonzero), and so $b\alpha = a \in I \cap R$. Then $a$ is a nonzero element of $R$ such that for any $\beta \in I^{-1}$, $a\beta \subseteq \beta I \subseteq R \implies aI^{-1} \subseteq R$. Then $I^{-1}$ is a nonzero fractional ideal of $R$.

Now for $IJ$, note that this is again a subset of $K$ which contains 0, is closed under additive inverses and addition, and absorbs multiplication from $R$. Then $IJ$ is an $R$-submodule of $K$, and since both $I$ and $J$ are nonzero, $IJ$ is nonzero as well. Now since $I$ and $J$ are fractional ideals, let $\alpha, \beta \in R$ be such that $\alpha I \subseteq R$ and $\beta J \subseteq R$. Then $\alpha\beta IJ = (\alpha I)(\beta J) \subseteq R$. Thus, $IJ$ is a nonzero fractional ideal of $R$. □

It should be noted here that $I^{-1}$ is not necessarily the multiplicative inverse of $I$. That is, if we assign multiplicative structure to the set of fractional ideals of $I$ as above, we have that $R$ is the identity element, but $II^{-1}$ is not necessarily equal to $R$ (though trivially, $II^{-1} \subseteq R$). This leads us to two important types of fractional ideals.

**Definition 1.2.60.** *Let $R$ be an integral domain and $I$ a fractional ideal of $R$. We say that $I$ is a* **divisorial ideal** *of $R$ if $(I^{-1})^{-1} = I$. We will denote the set of divisorial ideals of $R$ by $D(R)$. The operation defined on $D(R)$ will be $I \cdot J := ((IJ)^{-1})^{-1}$, where $IJ$ is the standard multiplication of fractional ideals.*

**Definition 1.2.61.** *Let $R$ be an integral domain and $I$ a fractional ideal of $R$. We say that $I$ is an* **invertible ideal** *of $R$ if $II^{-1} = R$. We will denote the set of invertible ideals of $R$ by $J(R)$. The operation defined on $J(R)$ will be the standard multiplication of fractional ideals $IJ$.*

In the following propositions, we will see properties of divisorial and invertible ideals. Since these objects are only defined for integral domains, we will assume moving forward that $R$ is an integral domain.

**Proposition 1.2.62.** *Let $I$ be a divisorial ideal of $R$. Then $I^{-1}$ is also a divisorial ideal of $R$. Moreover, for any fractional ideal $I$ of $R$, $(I^{-1})^{-1}$ is a divisorial ideal of $R$, so $D(R)$ is closed under its operation.*

*Proof.* See [5], Lemma 2.4 and Proposition 2.5. □

**Proposition 1.2.63.** *Let $I$ be an invertible ideal of $R$. Then $I^{-1}$ is also an invertible ideal of $R$,*

*and* $(I^{-1})^{-1} = I$*, i.e.* $I$ *is also a divisorial ideal of* $R$*. Moreover,* $J(R)$ *is closed under its operation, and the operation in* $D(R)$ *agrees with the operation in* $J(R)$ *for invertible ideals.*

*Proof.* First, note that if $\alpha \in I$ and $\beta \in I^{-1}$, then $\alpha\beta \in \beta I \subseteq R$, so $\alpha I^{-1} \subseteq R$. Thus, $I \subseteq (I^{-1})^{-1}$. Furthermore,

$$(I^{-1})^{-1} = R(I^{-1})^{-1} = II^{-1}(I^{-1})^{-1} \subseteq IR = I.$$

Thus, for any invertible ideal $I$ of $R$, $(I^{-1})^{-1} = I$, so $I$ is a divisorial ideal and $I^{-1}(I^{-1})^{-1} = II^{-1} = R$. Then $I^{-1}$ is invertible.

Now let $I, J \in J(R)$. We have already seen that $IJ$ is a fractional ideal. Now note that $I^{-1}J^{-1} \subseteq (IJ)^{-1}$ quite trivially (multiply an arbitrary element of $I^{-1}J^{-1}$ by an arbitrary element of $IJ$; it is easy to see that the product is in $R$). Furthermore,

$$(IJ)^{-1} = R(IJ)^{-1} = II^{-1}JJ^{-1}(IJ)^{-1} = IJ(IJ)^{-1}I^{-1}J^{-1} \subseteq RI^{-1}J^{-1} = I^{-1}J^{-1}.$$

Then $(IJ)^{-1} = I^{-1}J^{-1}$. This shows that $IJ(IJ)^{-1} = II^{-1}JJ^{-1} = R$, so $IJ \in J(R)$.

Now for any $I, J \in J(R)$, recall that in $D(R)$, $I \cdot J = ((IJ)^{-1})^{-1}$. Since $IJ$ has been shown to be invertible (and thus divisorial), we have that $((IJ)^{-1})^{-1} = IJ$. Thus, the operations in $D(R)$ and $J(R)$ agree on $J(R)$. □

**Proposition 1.2.64.** *Let* $I, J$ *be fractional ideals of* $R$*. If* $IJ = R$*, then* $J = I^{-1}$*,* $I = J^{-1}$*, and both* $I$ *and* $J$ *are invertible ideals of* $R$*.*

*Proof.* We will show that $J = I^{-1}$; the remaining results will follow immediately. First, note that since $IJ = R$, we have that $J \subseteq I^{-1}$. Furthermore,

$$I^{-1} = I^{-1}R = I^{-1}IJ \subseteq RJ = J.$$

Then $J = I^{-1}$. □

**Proposition 1.2.65.** *Let* $I$ *be an invertible ideal of* $R$ *and* $J$ *a divisorial ideal of* $R$*. Then* $IJ$ *is a divisorial ideal of* $R$*.*

*Proof.* First, note that as before, $I^{-1}J^{-1} \subseteq (IJ)^{-1}$. Furthermore, if $\alpha \in (IJ)^{-1}$, then $\alpha IJ \subseteq R$. Thus, $\alpha I \subseteq J^{-1}$. Then $\alpha \in \alpha R = \alpha II^{-1} \subseteq I^{-1}J^{-1}$. Thus, $(IJ)^{-1} = I^{-1}J^{-1}$ for any invertible

ideal $I$ of $R$ and divisorial ideal $J$ of $R$. Now as shown above, $I^{-1}$ is invertible with inverse $I$ and $J^{-1}$ is divisorial. Then

$$((IJ)^{-1})^{-1} = (I^{-1}J^{-1})^{-1} = (I^{-1})^{-1}(J^{-1})^{-1} = IJ,$$

i.e. $IJ$ is divisorial. □

**Proposition 1.2.66.** *Let $R$ be an integral domain, $K$ its field of fractions, and $I$ a nonzero principal fractional ideal of $R$, i.e. $I = \alpha R$ for some nonzero $\alpha \in K$. Then $I$ is an invertible ideal (and thus a divisorial ideal), and $I^{-1} = \alpha^{-1}R$. We will denote the set of nonzero principal fractional ideals of $R$ by $F(R)$.*

*Proof.* Recall that by definition, $I^{-1} := \{\beta \in K : \beta I \subseteq R\}$. Note that any element of $I$ is expressible as $\alpha r$ for some $r \in R$, so $\alpha^{-1}\alpha r = r \in R$. Then $\alpha^{-1} \in I^{-1}$, so $\alpha^{-1}R \subseteq I^{-1}$. Furthermore, if $\beta \in I^{-1}$, then $\beta\alpha = r \in R \implies \beta = \alpha^{-1}r \in \alpha^{-1}R$. Thus, $I^{-1} = \alpha^{-1}R$. Then it is easy to see that $II^{-1} = (\alpha R)(\alpha^{-1}R) = R$, so $I$ is invertible. □

**Proposition 1.2.67.** *For any integral domain $R$, $J(R)$ is an abelian group, and $F(R)$ is a subgroup. Furthermore, $D(R)$ is a group if and only if $R$ is completely integrally closed. In this case, $D(R)$ is an abelian group with subgroups $J(R)$ and $F(R)$.*

*Proof.* We have shown in the previous results that $J(R)$ contains an identity element ($R$ itself), contains an inverse for each of its elements, and is closed under its operation. Its operation is both associative and commutative because multiplication in $R$ is both associative and commutative. Then $J(R)$ is an abelian group.

As we showed above, $F(R)$ is a subset of $J(R)$ which contains an inverse for each of its elements. Note also that $R \in F(R)$ and $F(R)$ is trivially closed under the operation (with $(\alpha R)(\beta R) = \alpha\beta R$). Then $F(R)$ is a subgroup of $J(R)$; notably, since $J(R)$ is abelian, $F(R)$ is a normal subgroup.

For the proof that $D(R)$ is a group if and only if $R$ is completely integrally closed, see [5], Proposition 3.4. Accepting this result, we note that $D(R)$ must be abelian, since $R$ is commutative. Then since $J(R)$ has been shown to be a subset of $D(R)$ which is a group under the same operation, $J(R)$ (and thus $F(R)$) is a subgroup of $D(R)$. □

Recall from Proposition 1.2.52 that Krull domains are completely integrally closed. $D(R)$ is often considered specifically when $R$ is a Krull domain, and the above results show that in this particular case, $D(R)$ is an abelian group. With this knowledge, we are ready to define the two class groups of fractional ideals, which we will use later.

**Definition 1.2.68.** *Let $R$ be an integral domain. The* **ideal class group** *of $R$ is the quotient group $J(R)/F(R)$, which we will denote $Cl(R)$. We will denote the ideal class containing the invertible ideal $I$ by $[I]$.*

**Definition 1.2.69.** *Let $R$ be a completely integrally closed domain (such as a Krull domain). The* **divisor class group** *of $R$ is the quotient group $D(R)/F(R)$, which we will denote $DivCl(R)$. We will denote the divisor class containing the divisorial ideal $I$ by $[I]$. Alternatively, this is sometimes denoted $C(R)$ or $Cl(R)$, though to keep it distinct from the ideal class group, we will opt for the former notation.*

Using everything we have shown above with these definitions, we can in some sense "simplify" any ideal class or divisorial class to an integral ideal of $R$.

**Proposition 1.2.70.** *Let $[I] \in Cl(R)$ and $[J] \in DivCl(R)$ (for $Cl(R)$, we only need $R$ to be an integral domain; for $DivCl(R)$, we will assume $R$ is completely integrally closed), i.e. $I$ is an invertible ideal and $J$ is a divisorial ideal. Then there are integral ideals $I_0$ and $J_0$ of $R$ such that $[I_0] = [I]$ and $[J_0] = [J]$.*

*Proof.* As we have seen, since $I$ and $J$ are fractional ideals there exist nonzero elements $\alpha, \beta \in R$ such that $\alpha I = I_0$ and $\beta J = J_0$, both $I_0$ and $J_0$ integral ideals of $R$. Then $I_0 = (\alpha R)I$, a product of two invertible ideals, so $I_0$ is also invertible. Moreover, since $I_0$ differs from $I$ by a principal fractional ideal, $[I_0] = [I]$. Similarly, $J_0 = (\beta R)J$, a product of an invertible ideal and a divisorial ideal. Then $J_0$ is divisorial, and since $J_0$ differs from $J$ by a principal fractional ideal, $[J_0] = [J]$. □

## 1.3 Algebraic Number Theory

Later, we will consider factorization in particular types of rings related to algebraic number theory. In order to do so, some background knowledge of this area will be necessary. Most algebraic number theory texts will contain the majority of the information found in this section, an excellent example being [9].

### 1.3.1 Algebraic Numbers and Integers

**Definition 1.3.1.** *Let $K$ be a subfield of $\mathbb{C}$. If $K$ is a finite extension of $\mathbb{Q}$, i.e. if the dimension of $K$ as a vector space over $\mathbb{Q}$ is finite, then we call $K$ a* **number field**.

Many important properties of the rational numbers will generalize to number fields, making number fields in many ways an intuitive context in which to work. Of particular interest will be the generalization of the ring of integers $\mathbb{Z}$, a subring of $\mathbb{Q}$, to a corresponding subring of $K$ (see Definition 1.3.11). To consider this ring, we will appeal to the concept of integrality introduced earlier.

**Definition 1.3.2.** *Let $\alpha \in \mathbb{C}$. We say that $\alpha$ is* **algebraic** *(or an* **algebraic number***) if $\alpha$ is integral over $\mathbb{Q}$, i.e. if $\alpha$ is a root of a monic polynomial $f \in \mathbb{Q}[x]$. If $\alpha$ is not algebraic, $\alpha$ is said to be* **transcendental**.

**Example 1.3.3.** *$\sqrt{2}$ is algebraic, since it is a root of $x^2 - 2$. However, it is well-known that $\pi$ is transcendental.*

**Proposition 1.3.4.** *Let $K$ be a number field. Then every $\alpha \in K$ is algebraic. Specifically, every $\alpha \in K$ is a root of a polynomial of degree no more than $n = [K : L]$.*

*Proof.* Let $\alpha \in K$. Since $K$ is a number field, $n = [K : Q]$ (the degree of $K$ as a vector space over $\mathbb{Q}$) is finite. Then any set of $n + 1$ elements of $K$ must be linearly dependent. Thus, $\{1, \alpha, \alpha^2, \ldots, \alpha^n\}$ is a linearly dependent set, i.e. there exist $a_0, a_1, \ldots, a_n \in \mathbb{Q}$, not all zero, such that

$$a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_n\alpha^n = 0.$$

Let $m \leq n$ be the largest index such that $a_m \neq 0$; note that $m \geq 1$, since $m = 0$ implies that $a_0 = 0$, a contradiction. Then letting $f(x) = x^m + \frac{a_{m-1}}{a_m}x^{m-1} + \cdots + \frac{a_1}{a_m}x + \frac{a_0}{a_m}$, $f$ is a monic polynomial in $\mathbb{Q}[x]$ such that $f(\alpha) = 0$. Then $\alpha$ is algebraic. □

**Definition 1.3.5.** *Let $\alpha \in \mathbb{C}$. We say that $\alpha$ is an* **algebraic integer** *if $\alpha$ is integral over $\mathbb{Z}$, i.e. if $\alpha$ is a root of a monic polynomial in $\mathbb{Z}[x]$.*

One will note that in the definition of an algebraic number, the requirement that the polynomial $f$ of which $\alpha$ is a root does not actually need to be monic: if $\alpha$ is a root of a polynomial

$f \in \mathbb{Q}[x]$ with (nonzero) leading coefficient $a$, then $\alpha$ is also a root of $\frac{1}{a}f$, a monic polynomial in $\mathbb{Q}[x]$. However, $f$ being monic is important when considering an algebraic integer, since $\mathbb{Z}$ is not a field. In each case, we can require $f$ to be monic and irreducible; with these restrictions, $f$ is uniquely determined by the choice of $\alpha$ (see [9], Theorem 1).

**Definition 1.3.6.** *Let $\alpha$ be an algebraic number (or integer). Then the unique monic irreducible polynomial $f \in \mathbb{Q}[x]$ (or $\mathbb{Z}[x]$) of which $\alpha$ is a root is called the* **minimal polynomial** *of $\alpha$.*

**Definition 1.3.7.** *Let $\alpha$ be an algebraic number with minimal polynomial $f$. Then $\beta \in \mathbb{C}$ is called a* **conjugate** *of $\alpha$ if $f(\beta) = 0$. Note that in this case, $\beta$ is also an algebraic number; if $\alpha$ is an algebraic integer, then so is $\beta$.*

Now note that the set of algebraic integers is a subset of the set of algebraic numbers. Since a number field $K$ consists only of algebraic numbers, it is natural, then, to consider the set of algebraic integers in $K$. We will show that this set is actually a subring of $K$ with several nice properties. First, we need the following proposition.

**Proposition 1.3.8.** *For any $\alpha \in \mathbb{C}$, the following are equivalent:*

1. *$\alpha$ is an algebraic integer.*
2. *The additive group of $\mathbb{Z}[\alpha]$ is finitely generated.*
3. *$\alpha$ is contained in some subring of $\mathbb{C}$ having finitely generated additive group.*
4. *$\alpha A \subseteq A$ for some nonzero finitely generated additive subgroup $A \subseteq \mathbb{C}$.*

*Proof.* See [9], Theorem 2. □

**Corollary 1.3.9.** *Let $\alpha, \beta$ be algebraic integers. Then $\alpha \pm \beta$ and $\alpha\beta$ are algebraic integers.*

*Proof.* Since $\alpha$ and $\beta$ are algebraic integers, $\mathbb{Z}[\alpha]$ and $\mathbb{Z}[\beta]$ have finitely generated additive groups. Then $\mathbb{Z}[\alpha, \beta]$ also has a finitely generated additive group. Since $\alpha \pm \beta$ and $\alpha\beta$ are in $\mathbb{Z}[\alpha, \beta]$, $\alpha \pm \beta$ and $\alpha\beta$ are algebraic integers by characterization 3 above. □

This (along with the more obvious properties) shows that the set of algebraic integers actually forms a ring. Furthermore, the following proposition shows that this ring is integrally closed.

**Corollary 1.3.10.** *Let $\alpha \in \mathbb{C}$ be such that $\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$ for some algebraic integers $a_0, \ldots, a_{n-1}$. Then $\alpha$ is an algebraic integer.*

*Proof.* Consider the ring $\mathbb{Z}[a_0, \ldots, a_{n-1}, \alpha]$, the additive group of which is generated by products of the form $a_0^{m_0} \ldots a_{n-1}^{m_{n-1}} \alpha^m$, with $m_i, m \in \mathbb{N} \cup \{0\}$. Now note that if $m \geq n$, we can reduce the exponent of $\alpha$ using the fact that $\alpha^n = -(a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0)$. This substitution will reduce the power of $\alpha$, though it may increase the powers of the $a_i$'s. Furthermore, if any $m_i$ is sufficiently large (in particular, if $m_i$ is at least the degree of the minimal polynomial for $a_i$ over $\mathbb{Z}$), we can similarly reduce the power of $a_i$. Note that since this process substitutes $a_i^{m_i}$ with smaller powers of $a_i$ multiplied by integers, this will not have any effect on the powers of the other $a_j$'s or $\alpha$. Then by first reducing the power of $\alpha$ so that $m < n$, then reducing the powers of each $a_i$ so that $m_i \leq d_i$ for $0 \leq i \leq n-1$, where $d_i$ is the degree of the minimal polynomial for $a_i$, we can see that the additive group of $\mathbb{Z}[a_0, \ldots, a_{n-1}, \alpha]$ is generated by at most $d_0 \ldots d_{n-1} n$ elements. Then $\alpha$ is contained in a subring of $\mathbb{C}$ which has a finitely generated addivite group, so by the proposition, $\alpha$ is an algebraic integer. □

Now since the set of algebraic integers is a ring, then the subset of a number field consisting of algebraic integers is also a ring.

**Definition 1.3.11.** *Let $K$ be a number field. The set of algebraic integers in $K$, denoted $\mathcal{O}_K$, is called the* **number ring** *of $K$. Alternatively, it is often simply referred to as the* **ring of integers in** *$K$.*

**Example 1.3.12.** *The ring of algebraic integers in $\mathbb{Q}$ is the normal set of integers, $\mathbb{Z}$. For this reason, $\mathbb{Z}$ is often referred to as the set of rational integers.*

**Proposition 1.3.13.** *Let $K$ be a number field and $\alpha \in K$. Then there exists some $c \in \mathbb{N}$ such that $c\alpha \in \mathcal{O}_K$.*

*Proof.* Let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ be the minimal polynomial for $\alpha$, with each $a_i \in \mathbb{Q}$. Since there are only finitely many $a_i$, we can find the (positive) least common multiple of their denominators and multiply to get $g(x) = b_n x^n + b_{n-1}x^{n-1} + \cdots + b_1 x + b_0 \in \mathbb{Z}[x]$ which still has $\alpha$ as a root. Then

$$(b_n\alpha)^n + b_{n-1}(b_n\alpha)^{n-1} + \cdots + b_n^{n-2}b_1(b_n\alpha) + b_n^{n-1}b_0 = b_n^{n-1}g(\alpha) = 0.$$

Therefore, letting $c = b_n$, we have that $c\alpha \in \mathcal{O}_K$. □

**Corollary 1.3.14.** *Let $K$ be a number field. Then $\mathcal{O}_K$ is an integral domain with field of fractions $K$.*

*Proof.* First, note that $\mathcal{O}_K$ is trivially an integral domain as a subring of the field $K$ (or of $\mathbb{C}$). Now let $L$ be the field of fractions of $\mathcal{O}_K$. Since $\mathcal{O}_K \subseteq K$ and $L$ is the smallest field containing $\mathcal{O}_K$, then clearly $L \subseteq K$. Furthermore, the proposition shows that any $\alpha \in K$ is representable as $\alpha = \frac{\beta}{c}$, with $\beta \in \mathcal{O}_K$ and $c \in \mathbb{N} \subseteq \mathcal{O}_K$. Then $K \subseteq L$. Thus, $K$ is the field of fractions of $\mathcal{O}_K$. □

**Corollary 1.3.15.** *Let $K$ be a number field. Then there is a basis for $K$ over $\mathbb{Q}$ consisting entirely of algebraic integers.*

*Proof.* Let $\alpha_1, \ldots, \alpha_n$ be an arbitrary basis for $K$ over $\mathbb{Q}$. Then by the proposition, there exist positive integers $c_1, \ldots, c_n$ such that $c_i\alpha_i \in \mathcal{O}_K$ for $1 \leq i \leq n$. Furthermore, each $\alpha_i \in c_i\alpha_i\mathbb{Q}$, so $K$ is spanned by the $n$ elements $c_1\alpha_1, \ldots, c_n\alpha_n$. Then this is a basis for $K$ over $\mathbb{Q}$ consisting of algebraic integers. □

Later, we will be able to develop methods to determine the ring of integers in a number field $K$. First, however, we need to develop some helpful tools.

### 1.3.2 Trace, Norm, and Discriminant

Three of the most important tools we will need to introduce are the trace, norm, and discriminant. For each of these, we will need to use embeddings in $\mathbb{C}$.

**Proposition 1.3.16.** *Let $L$ and $K$ be number fields with $K \subseteq L$ and $[L : K] = n$. Then every embedding of $K$ into $\mathbb{C}$ extends to exactly $n$ distinct embeddings of $L$ into $\mathbb{C}$.*

**Corollary 1.3.17.** *Let $L$ and $K$ be number fields with $K \subseteq L$ and $[L : K] = n$. Then there are exactly $n$ embeddings of $L$ into $\mathbb{C}$ which fix $K$ pointwise.*

**Corollary 1.3.18.** *Let $K$ be a number field with $[K : \mathbb{Q}] = n$. Then there are exactly $n$ embeddings of $K$ into $\mathbb{C}$.*

**Proposition 1.3.19.** *Let $L$ and $K$ be number fields with $K \subseteq L$. Then $L = K[\alpha]$ for some $\alpha \in L$.*

**Corollary 1.3.20.** *Let $K$ be a number field. Then $K = \mathbb{Q}[\alpha]$ for some $\alpha \in K$.*

For proofs of these propositions, see [9], Appendix B. The corollaries follow directly from the propositions which precede them.

**Proposition 1.3.21.** *Let $K$ be a number field and $\alpha, \beta \in K$. Then there is some embedding $\sigma$ of $K$ into $\mathbb{C}$ such that $\sigma(\alpha) = \beta$ if and only if $\beta$ is a conjugate of $\alpha$.*

*Proof.* Let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Q}[x]$ be the minimal polynomial for $\alpha$. Then for any embedding $\sigma$ of $K$ into $\mathbb{C}$,

$$f(\sigma(\alpha)) = \sigma(\alpha)^n + a_{n-1}\sigma(\alpha)^{n-1} + \cdots + a_1\sigma(\alpha) + a_0 = \sigma(f(\alpha)) = \sigma(0) = 0.$$

Now let $\beta$ be a conjugate of $\alpha$ and $L = \mathbb{Q}[\alpha]$. With $f$ as above, we have that $[L : \mathbb{Q}] = n$, so there must be $n$ distinct embeddings of $L$ into $\mathbb{C}$. Since the action of any embedding of $L$ is determined entirely by its action on $\alpha$, these embeddings must act distinctly on $\alpha$, each taking $\alpha$ to one of its $n$ conjugates. Thus, there is exactly one embedding $\tau$ of $L$ into $\mathbb{C}$ such that $\tau(\alpha) = \beta$. Furthermore, we know from above that $\tau$ extends to exactly $[K : L]$ embeddings of $K$ into $\mathbb{C}$; then in fact, $[K : L] = \frac{[K:\mathbb{Q}]}{n}$ embeddings of $K$ into $\mathbb{C}$ map $\alpha$ to $\beta$. □

Now that we have this knowledge, we can define the trace, norm, and discriminant.

**Definition 1.3.22.** *Let $K$ be a number field with $[K : \mathbb{Q}] = n$, and let $\sigma_1, \ldots, \sigma_n$ be the embeddings of $K$ into $\mathbb{C}$. The* **trace** *of some $\alpha \in K$ is*

$$T^K(\alpha) := \sum_{i=1}^{n} \sigma_i(\alpha).$$

*Similarly, the* **norm** *of some $\alpha \in K$ is*

$$N^K(\alpha) := \prod_{i=1}^{n} \sigma_i(\alpha).$$

*Finally, for an $n$-tuple $\alpha_1, \ldots, \alpha_n \in K$, the* **discriminant** *is*

$$\operatorname{disc}^K(\alpha_1, \ldots, \alpha_n) = \begin{vmatrix} \sigma_1(\alpha_1) & \ldots & \sigma_1(\alpha_n) \\ \vdots & \ddots & \vdots \\ \sigma_n(\alpha_1) & \ldots & \sigma_n(\alpha_n) \end{vmatrix}^2.$$

*If $K$ is clear from context, we will often omit it from the notation above.*

**Proposition 1.3.23.** *Let $K$ be a number field with $[K : \mathbb{Q}] = n$, $\alpha, \beta \in K$, and $c \in \mathbb{Q}$. Then we have the following:*

1. $T(\alpha + \beta) = T(\alpha) + T(\beta)$;
2. $N(\alpha\beta) = N(\alpha)N(\beta)$;
3. $T(c) = nc$;
4. $N(c) = c^n$;
5. $T(c\alpha) = cT(\alpha)$;
6. $N(c\alpha) = c^n N(\alpha)$.

*Furthermore, if $K = \mathbb{Q}[\alpha]$, with $\alpha_1, \ldots, \alpha_n$ the conjugates of $\alpha$, $T(\alpha) = \sum_{i=1}^{n} \alpha_i$ and $N(\alpha) = \prod_{i=1}^{n} \alpha_i$.*

*Proof.* These results all follow immediately from the definitions and propositions above. □

**Proposition 1.3.24.** *Let $K$ be a number field, $[K : \mathbb{Q}] = m$, and $\alpha \in K$ with minimal polynomial $f \in \mathbb{Z}[x]$ of degree $n$. Then $T^K(\alpha) = \frac{m}{n} T^{\mathbb{Q}[\alpha]}(\alpha)$ and $N^K(\alpha) = (N^{\mathbb{Q}[\alpha]}(\alpha))^{\frac{m}{n}}$.*

*Proof.* This follows directly from the fact that $T^{\mathbb{Q}[\alpha]}(\alpha)$ is the sum of the conjugates of $\alpha$, $N^{\mathbb{Q}[\alpha]}(\alpha)$ is the product of the conjugates of $\alpha$, and exactly $\frac{m}{n}$ embeddings of $K$ into $\mathbb{C}$ map $\alpha$ to each of its conjugates. □

**Corollary 1.3.25.** *Let $K$ be a number field with $[K : \mathbb{Q}] = m$ and $\alpha \in K$ of degree $n$ over $\mathbb{Q}$. Then $T^K(\alpha)$ and $N^K(\alpha)$ are rational. Moreover, if $\alpha \in \mathcal{O}_K$, then $T^K(\alpha)$ and $N^K(\alpha)$ are rational integers.*

*Proof.* We know that $T^{\mathbb{Q}[\alpha]}(\alpha)$ is the sum of the conjugates of $\alpha$; then $-T^{\mathbb{Q}[\alpha]}(\alpha)$ is the coefficient of the $x^{m-1}$ term in the minimal polynomial of $\alpha$. We also know that $N^{\mathbb{Q}[\alpha]}(\alpha)$ is the product of the conjugates of $\alpha$; then $\pm N^{\mathbb{Q}[\alpha]}(\alpha)$ is the constant term in the minimal polynomial of $\alpha$. Finally, $[K : \mathbb{Q}[\alpha]] = \frac{m}{n} \in \mathbb{Z}$. Then the proposition shows that $T^K(\alpha), N^K(\alpha) \in \mathbb{Q}$, and if $\alpha \in \mathcal{O}_K$, then $T^K(\alpha), N^K(\alpha) \in \mathbb{Z}$. □

**Corollary 1.3.26.** *Let $K$ be a number field with number ring $\mathcal{O}_K$. Then $\alpha \in \mathcal{O}_K$ is a unit in $\mathcal{O}_K$ if and only if $N(\alpha) = \pm 1$.*

*Proof.* First, note that since each embedding of $K$ into $\mathbb{C}$ fixes $\mathbb{Q}$, $N(1) = 1$ (this can also be seen by the proposition). Now assume that $\alpha$ is a unit in $\mathcal{O}_K$. Then $N(\alpha)N(\alpha^{-1}) = N(\alpha\alpha^{-1}) = N(1) = 1$. Since both $\alpha$ and $\alpha^{-1}$ are algebraic integers, their norms are integers. Then either $N(\alpha) = N(\alpha^{-1}) = 1$ or $N(\alpha) = N(\alpha^{-1}) = -1$.

Now assume that $\alpha \in \mathcal{O}_K$ is such that $N(\alpha) = \pm 1$. Then by the proposition, $(N^{\mathbb{Q}[\alpha]}(\alpha))^{\frac{m}{n}} = \pm 1$, with $m$ and $n$ as above. Since $\alpha$ is an algebraic integer, its norm is an integer, and thus $N^{\mathbb{Q}[\alpha]}(\alpha) = \pm 1$. Letting $\alpha_1, \ldots, \alpha_n$ denote the conjugates of $\alpha$ (with $\alpha_1 = \alpha$), this tells us that $\alpha(\alpha_2 \ldots \alpha_n) = \pm 1$, so $\alpha^{-1} = \pm(\alpha_2 \ldots \alpha_n)$. Since each $\alpha_i$ is an algebraic integer (a root of the same minimal polynomial as $\alpha$), their product is as well, so $\alpha^{-1}$ is an algebraic integer. Then since $\alpha^{-1} \in K$, $\alpha^{-1} \in \mathcal{O}_K$. Then $\alpha$ is a unit in $\mathcal{O}_K$. □

**Proposition 1.3.27.** *Let $K$ be a number field with $[K : \mathbb{Q}] = n$ and $\alpha_1, \ldots, \alpha_n \in K$. Then* $\operatorname{disc}(\alpha_1, \ldots, \alpha_n) = \left|T(\alpha_i\alpha_j)\right|$*, the determinant of the matrix of traces of conjugate products.*

*Proof.* Note the following matrix equation:

$$[\sigma_j(\alpha_i)][\sigma_i(\alpha_j)] = [\sigma_1(\alpha_i\alpha_j) + \cdots + \sigma_n(\alpha_i\alpha_j)] = [T(\alpha_i\alpha_j)].$$

This, along with the fact that the determinant is multiplicative and is unchanged by taking the transpose of a matrix, gives the desired result. □

**Corollary 1.3.28.** *Let $K$ be a number field with $[K : \mathbb{Q}] = n$ and $\alpha_1, \ldots, \alpha_n \in K$. Then* $\operatorname{disc}(\alpha_1, \ldots, \alpha_n) \in \mathbb{Q}$*, and if every $\alpha_i \in \mathcal{O}_K$, then* $\operatorname{disc}(\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}$.

*Proof.* This follows directly from the previous proposition and the fact that each $T(\alpha_i\alpha_j) \in \mathbb{Q}$, or $T(\alpha_i\alpha_j) \in \mathbb{Z}$ when every $\alpha_i \in \mathcal{O}_K$. □

**Proposition 1.3.29.** *Let $\alpha_1, \ldots, \alpha_n \in K$. Then* $\operatorname{disc}(\alpha_1, \ldots, \alpha_n) = 0$ *if and only if the $\alpha_i$ are linearly dependent over $\mathbb{Q}$.*

*Proof.* First, assume that the $\alpha_i$ are linearly dependent. Then note that the matrix $\left[\sigma_i(\alpha_j)\right]$ has linearly dependent columns, so $\left|\sigma_i(\alpha_j)\right| = 0$. Then by definition of the discriminant, $\operatorname{disc}(\alpha_1, \ldots, \alpha_n) = 0$.

Now assume that $\text{disc}(\alpha_1, \ldots, \alpha_n) = 0$. Then $\left|\sigma_i(\alpha_j)\right| = 0$, meaning that $\left[\sigma_i(\alpha_j)\right]$ must have linearly independent columns, similar to the argument above. Then there exist $a_1, \ldots, a_n \in \mathbb{Q}$, not all zero, such that $\sigma_i(a_1\alpha_1 + \cdots + a_n\alpha_n) = 0$ for $1 \leq i \leq n$. However, since the $\sigma_i$ are embeddings of $K$ into $\mathbb{C}$, they have trivial kernel. Thus, $a_1\alpha_1 + \cdots + a_n\alpha_n = 0$, so the $\alpha_i$ are linearly dependent. $\square$

**Proposition 1.3.30.** *Let $\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_n \in K$ such that $R := \alpha_1\mathbb{Z} + \cdots + \alpha_n\mathbb{Z} = \beta_1\mathbb{Z} + \cdots + \beta_n\mathbb{Z}$, i.e. the $\alpha_i$ and $\beta_j$ generate the same $\mathbb{Z}$-submodule of $K$. Then $\text{disc}(\alpha_1, \ldots, \alpha_n) = \text{disc}(\beta_1, \ldots, \beta_n)$.*

*Proof.* First, note that if either the $\alpha_i$ or $\beta_j$ are linearly dependent, then the other set must be also. Then if either is linearly dependent, both discriminants are 0 by the previous result.

Now assume that neither the $\alpha_i$ nor the $\beta_j$ are linearly dependent. Then each element in $R$ is uniquely representable as a $\mathbb{Z}$-linear combination of the $\alpha_i$'s and $\beta_j$'s. In particular, each $\alpha_i$ can be written as a linear combination of the $\beta_j$'s, and each $\beta_j$ can be written as a linear combination of the $\alpha_i$'s. Thus, we have matrices $M, N \in \mathbb{Z}^{n\times n}$ such that

$$M\begin{bmatrix}\alpha_1\\ \vdots \\ \alpha_n\end{bmatrix} = \begin{bmatrix}\beta_1\\ \vdots \\ \beta_n\end{bmatrix}, \quad N\begin{bmatrix}\beta_1\\ \vdots \\ \beta_n\end{bmatrix} = \begin{bmatrix}\alpha_1\\ \vdots \\ \alpha_n\end{bmatrix}.$$

Furthermore, since the $\alpha_i$'s and $\beta_j$'s are linearly independent, we know that $M = N^{-1}$. Then since $M$ is an invertible matrix in $\mathbb{Z}^{n\times n}$, $|M| = \pm 1$. Now note that

$$M[\sigma_j(\alpha_i)] = [\sigma_j(\beta_i)].$$

Then taking determinants and squaring, we get that

$$\text{disc}(\beta_1, \ldots, \beta_n) = |M|^2\text{disc}(\alpha_1, \ldots, \alpha_n) = \text{disc}(\alpha_1, \ldots, \alpha_n).$$

$\square$

As we have seen up to this point and will continue to see moving forward, these tools are very useful when working in a number field. Among other things, they can help us determine the

ring of algebraic integers in a number field. This will be discussed more in depth in Chapter 2, but for now we have enough information to find a simple (but important) example.

**Example 1.3.31.** *Let $K$ be a number field with $[K:\mathbb{Q}] = 2$. Then $K = \mathbb{Q}[\sqrt{d}]$ for some squarefree $d \in \mathbb{Z}$. Furthermore, the ring of integers in $K$ is*

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{d}], & d \equiv 2,3 \pmod 4; \\ \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right], & d \equiv 1 \pmod 4. \end{cases}$$

*Proof.* First, recall that $K = \mathbb{Q}[\alpha]$ for some $\alpha \in K$, and that the minimal polynomial for $\alpha$ is of degree 2. Let $f(x) = x^2 + ax + b$ be the minimal polynomial for $\alpha$, with $a, b \in \mathbb{Q}$. Then using the quadratic formula, we know that $\alpha = \frac{-a \pm \sqrt{a^2-4b}}{2}$. Then $\sqrt{a^2-4b} = \pm(2\alpha + a) \in K$. Note that $a^2 - 4b \neq 0$, since $f$ is irreducible. Now multiply by some integer to clear the denominator under the radical, then divide out any square divisors. This produces $\sqrt{d} \in K$, with $d$ an integer. Since all square divisors were removed, either $d$ is squarefree or $d = 1$, in which case $\sqrt{a^2-4b} \in \mathbb{Q}$, and thus $\alpha \in \mathbb{Q}$, a contradiction. Then $\mathbb{Q}[\sqrt{d}] \subseteq K$, and since $d$ is squarefree, both fields are degree 2 extensions of $\mathbb{Q}$, so we must have that $K = \mathbb{Q}[\sqrt{d}]$.

Now let $d$ be a squarefree integer such that $K = \mathbb{Q}[\sqrt{d}]$. For any $\alpha = a + b\sqrt{d} \in K$, note that $T(\alpha) = 2a$ and $N(\alpha) = a^2 - b^2 d$. We already know that if $\alpha$ is an algebraic integer, then $T(\alpha)$ and $N(\alpha)$ are integers. However, note that in this case we also have the reverse implication, since $\alpha$ is a root of $f(x) = x^2 - T(\alpha)x + N(\alpha)$. Then if we determine which $a, b \in \mathbb{Q}$ give rise to $T(\alpha) = 2a \in \mathbb{Z}$ and $N(\alpha) = a^2 - b^2 d \in \mathbb{Z}$, we will have exactly the ring of integers $\mathcal{O}_K$.

Note that since $\sqrt{d}$ is an algebraic integer, $\mathbb{Z}[\sqrt{d}] \subseteq \mathcal{O}_K$. Now suppose that there is some $\alpha = a + b\sqrt{d} \in \mathcal{O}_K$ which does not lie in $\mathbb{Z}[\sqrt{d}]$. First, note that $T(\alpha) = 2a \in \mathbb{Z}$, so $a \in \frac{1}{2}\mathbb{Z}$. If $a \in \mathbb{Z}$, then $N(\alpha) = a^2 - b^2 d \in \mathbb{Z} \implies b^2 d \in \mathbb{Z}$, so if we write $b = \frac{b_1}{b_2}$, a reduced fraction, $b_2^2 | d$. Then since $d$ is squarefree, $b_2 = 1 \implies b \in \mathbb{Z}$. Then if $\alpha \in \mathcal{O}_K$ with $a \in \mathbb{Z}$, $b \in \mathbb{Z}$ as well. Now we need only handle the case when $a = \frac{a_1}{2}$, with $a_1 \in \mathbb{Z}$ odd. Then $N(\alpha) = a^2 - b^2 d = \frac{a_1^2 - 4b^2 d}{4} \in \mathbb{Z} \implies a_1^2 - 4b^2 d \equiv 0 \pmod 4$. If $b \in \mathbb{Z}$, note that then $a_1^2 \equiv 0 \pmod 4$, contradicting the fact that $a_1$ is odd. Again writing $b = \frac{b_1}{b_2}$ with $b_1, b_2$ relatively prime, note that we must have $4b^2 d \in \mathbb{Z}$, so $b_2^2 | 4b_1^2 d$. Since $b_1$ and $b_2$ are relatively prime, $b_2^2 | 4d$. Now if $p$ is a prime divisor of $b_2$, note that $p^2 | 4d$, and since $p^2 \nmid d$, $p | 4$. Then the only prime divisor of $b_2$ is 2, and since $b_2^2 | 4d$, it must be the case that $b_2 = 2$. Furthermore, since $b \notin \mathbb{Z}$, $b_1$ must be odd. Then

$a_1^2 - b_1^2 d \equiv 0 \pmod 4 \implies d \equiv 1 \pmod 4$. Thus, if $d \equiv 2, 3 \pmod 4$, $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$. However, if $d \equiv 1 \pmod 4$, we could have algebraic integers of the form $\beta = \frac{a+b\sqrt{d}}{2}$, with $a, b \in \mathbb{Z}$, $a \equiv b \pmod 2$. Since $T(\beta) = a \in \mathbb{Z}$ and $N(\beta) = \frac{a^2}{4} - \frac{b^2}{4} d \in \mathbb{Z}$ (consider the numerator modulo 4), we have that any element of this form is an algebraic integer when $d \equiv 1 \pmod 4$. Then when $d \equiv 1 \pmod 4$, $\mathcal{O}_K = \left\{ \frac{a+b\sqrt{d}}{2} : a, b \in \mathbb{Z}, a \equiv b \pmod 2 \right\} = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$. □

We can now return to statements made in Examples 1.2.11 and 1.2.23 which are now very straightforward to show.

**Example 1.3.32.** *In $\mathbb{Z}[\sqrt{-5}]$, 2, 3, $1+\sqrt{-5}$, and $1-\sqrt{-5}$ are all irreducible.*

*Proof.* By the previous example, we know that $\mathbb{Z}[\sqrt{-5}]$ is the ring of algebraic integers in $\mathbb{Q}[\sqrt{-5}]$. Then $N(a + b\sqrt{5}) = a^2 + 5b^2$, $N(\alpha) = \pm 1$ if and only if $\alpha$ is a unit, and $N(\alpha) \in \mathbb{Z}$ for every $\alpha \in \mathbb{Z}[\sqrt{-5}]$. Then note that $N(2) = 4$, $N(3) = 9$, and $N(1 + \sqrt{-5}) = N(1 - \sqrt{-5}) = 6$. Then if any of these is reducible, it is a product of two nonunits, i.e. a product of two elements of $\mathbb{Z}[\sqrt{-5}]$, neither of which has norm $\pm 1$. Since the four norms here are a product of exactly two primes, then any of these elements being reducible means that there is an element in $\mathbb{Z}[\sqrt{-5}]$ with norm $\pm 2$ or $\pm 3$. However, since $N(a + b\sqrt{-5}) = a^2 + 5b^2$, with $a, b \in \mathbb{Z}$, we can see that no such elements exist. Then these four elements are irreducible in $\mathbb{Z}[\sqrt{-5}]$. Furthermore, since the norms of 2 and 3 are distinct from the norms of $1+\sqrt{5}$ and $1-\sqrt{5}$, neither 2 nor 3 is an associate of $1+\sqrt{-5}$ or $1-\sqrt{-5}$, so $2 \cdot 3 = 6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ is indeed an example of non-unique factorization. □

# Chapter 2

# Intermediate Results

In the previous chapter, we discussed definitions, examples, and some basic results that will serve as building blocks for the major results in this paper. Here, we will further develop these results and consider their connections. In particular, we will focus on the structures and properties associated with number rings. This will allow us to prove the major results of this paper in the chapters that follow. The discussion in this chapter will largely come from [9], though some results will draw from other sources.

## 2.1 Free Abelian Groups

First, we have a few results regarding finitely generated free abelian groups. As we will see later, this will connect nicely to the discussion of number rings and allow us to build to bigger results. Although it is assumed that the reader is familiar with the concept of a free abelian group, the definition will be presented here for convenience.

**Definition 2.1.1.** *Let $G$ be an abelian group. We say that $G$ is a* **free abelian group** *if there exists a subset $B$ of $G$, called a* **basis** *for $G$, such that every element of $G$ can uniquely be expressed as a finite sum of elements of $B$ and their negatives. That is,*

$$G = \bigoplus_{b \in B} b\mathbb{Z} \cong \bigoplus_{b \in B} \mathbb{Z}.$$

*Any two bases for $G$ have the same cardinality, called the* **rank** *of $G$. If a basis $B$ for $G$ is finite,*

*then we say that $G$ is of finite rank $n = |B|$, or is finitely generated of rank $n$.*

With this definition, we can prove some useful results about finite rank free abelian groups.

**Theorem 2.1.2.** *Let $G$ be a free abelian group of finite rank $n$. Then if $H$ is a subgroup of $G$, $H$ is a free abelian group of rank at most $n$.*

*Proof.* Without loss of generality, we will assume that $G = \bigoplus_{i=1}^{n} \mathbb{Z}$ since we know that $G$ is at least isomorphic to this group. Note that if $n = 1$, then $G = \mathbb{Z}$. We know that every subgroup of $\mathbb{Z}$ is of the form $a\mathbb{Z}$ for some $a \in \mathbb{Z}$, meaning that every subgroup $H$ of $G$ is either a free abelian subgroup of rank 1 (if $a \neq 0$) or $\{0\}$, which is the free abelian group of rank 0.

Now assume that for some $n \in \mathbb{N}$, the result holds for any free abelian group of rank $< n$. Now define $\pi : G \to \mathbb{Z}$ to be the projection of any element of $G$ onto its first coordinate, i.e. $\pi(a_1, \ldots, a_n) = a_1$ for any $a_i \in \mathbb{Z}$, $1 \leq i \leq n$. Note that $\pi$ is a group homomorphism. We know that $\pi(H)$ must be a subgroup of $\mathbb{Z}$, and thus either $\pi(H)$ is a free abelian group of rank 1 or $\pi(H) = \{0\}$. Furthermore, note that $\ker(\pi) \cap H$ consists of all elements of $H$ with first coordinate 0. Thus, $\ker(\pi) \cap H$ is a subgroup of the rank $n-1$ free abelian group consisting of all but the first coordinate of $G$. Thus, $\ker(\pi) \cap H$ is a free abelian group of rank at most $n-1$, by the inductive hypothesis.

If $\pi(H) = \{0\}$, then $H \subseteq \ker(\pi)$; thus, $H = \ker(\pi) \cap H$, a free abelian group of rank at most $n-1$. Otherwise, $\pi(H)$ is a rank 1 free abelian group. Let $h_0 \in H$ such that $\pi(h_0)$ generates $\pi(H)$. Then for any $h \in H$, write $\pi(h) = a\pi(h_0)$ and $h = ah_0 + (h - ah_0)$. We have that $ah_0 \in h_0\mathbb{Z}$ and $\pi(h - ah_0) = \pi(h) - \pi(ah_0) = a\pi(h_0) - a\pi(h_0) = 0$, so $h - ah_0 \in \ker(\pi) \cap H$. Therefore, $H = h_0\mathbb{Z} + \ker(\pi) \cap H$. Finally, note that if $k \in h_0\mathbb{Z} \cap (\ker(\pi) \cap H)$, then the first coordinate of $k$ is $\pi(k) = 0$. However, since $h_0$ has nonzero first coordinate and $k = ah_0$ for some $a \in \mathbb{Z}$, it must be the case that $a = 0 \implies k = 0$. Then since $H = h_0\mathbb{Z} + \ker(\pi) \cap H$ and the two summands have trivial intersection, this sum is direct. Then $H$ is the direct sum of a rank 1 free abelian group and a rank at most $n-1$ free abelian group, so $H$ is a free abelian group of rank at most $n$. □

**Corollary 2.1.3.** *Let $G$ be a group. Suppose that $G$ is a subgroup of $H_1$, a free abelian group of finite rank $n$, and that $G$ also contains a subgroup $H_2$, a free abelian group of rank $n$. Then $G$ is a free abelian group of rank $n$.*

*Proof.* Since $G$ is a subgroup of $H_1$, we have that $G$ is a free abelian group of rank $m \leq n$. Then since $H_2$ is a subgroup of $G$, we must have that $n \leq m$. Thus, $m = n$. □

This "sandwiching" behavior will be important as we discuss number rings and their ideals and orders. For the next result, we require a lemma.

**Lemma 2.1.4.** *Let $G$ be a free abelian group of finite rank $n$, and let $H$ be a subgroup of $G$. Then $G/H$ is a finite group if and only if $H$ is a free abelian group of rank $n$.*

*Proof.* First, assume that $H$ is a free abelian group of rank $n$ and that there is some $g \in G$ such that $g\mathbb{Z} \cap H = \{0\}$. Then $g\mathbb{Z} + H$ is a subgroup of $G$; since $g\mathbb{Z} \cap H = \{0\}$, this sum is direct. Then $G$ has a subgroup $g\mathbb{Z} \oplus H$, a rank $n+1$ free abelian group, contradicting the previous result. Then for every $g \in G$, there is some nonzero $m \in \mathbb{Z}$ such that $mg \in H$. In other words, every element in $G/H$ has finite order. Furthermore, since $H$ contains additive inverses, we can without loss of generality require $m$ to be positive.

Now let $g_1, \ldots, g_n$ be a basis for $G$. Then we have $m_1, \ldots, m_n \in \mathbb{N}$ such that $m_i g_i \in H$ for $1 \leq i \leq n$. Then since every element $g \in G$ is expressible as $g = a_1 g_1 + \ldots a_n g_n$ for some $a_i \in \mathbb{Z}$, note that reducing $a_i$ modulo $m_i$ changes $g$ by an element of $H$. In other words, every coset in $G/H$ has a coset representative such that $0 \leq a_i < m_i$ for $1 \leq i \leq n$. Then $\left|G/H\right| \leq \prod_{i=1}^{n} m_i$, so $G/H$ is finite.

Now assume that $G/H$ is a finite group. Let $g_1, \ldots, g_n$ be a basis for $G$ and note that since $G/H$ is finite, then each $g_i$ has finite order in $G/H$. Then there exist integers $a_1, \ldots, a_n$ such that $a_i g_i \in H$ for $1 \leq i \leq n$. Then $\langle a_1 g_1, \ldots, a_n g_n \rangle \leq H$, and since the $g_i$ are $\mathbb{Z}$-linearly independent, the $a_i g_i$ are as well. Then this is actually a rank $n$ free abelian subgroup of $H$. Then since $H$ is "sandwiched" between two free abelian groups of rank $n$, $H$ is a free abelian group of rank $n$. $\square$

**Theorem 2.1.5.** *Let $G$ and $H$ be free abelian groups of finite rank $n$, with $H \leq G$. Then there exists a basis $\beta_1, \ldots, \beta_n$ for $G$ and positive integers $d_1, \ldots, d_n$ such that $d_n | \ldots | d_1$ and $d_1\beta_1, \ldots, d_n\beta_n$ is a basis for $H$.*

*Proof.* By the lemma, $G/H$ is a finite abelian group. Then by the Fundamental Theorem of Finite abelian groups,

$$G/H \cong \mathbb{Z}_{d_1} \oplus \cdots \oplus \mathbb{Z}_{d_r}$$

for some $r \in \mathbb{N}$ and $d_i \in \mathbb{N}$, $d_r | \ldots | d_1$. Then $\left|G/H\right| = d_1 \ldots d_r$. Now if $\left|G/H\right| = 1$, then $G = H$, in which case any basis for $G$ is a basis for $H$ and the result holds trivially. Then assume that $\left|G/H\right| > 1$. In that case, we can require that $d_r \geq 2$, i.e. there are no trailing trivial groups in

the above representation of $G/H$. Furthermore, we must have that $r \leq n$, since $r$ is the minimal number of cyclic groups in any direct sum representation of $G/H$.

Now define $B_1 := \{\beta \in G : |\beta + H| = d_1\}$, the set of every element of $G$ lying in a coset in $G/H$ of order $d_1$. Since $G/H$ has an element of order $d_1$, $B_1$ is a nonempty set. Now for any basis $g_1, \ldots, g_n$ for $G$, we can write any $\beta \in B_1$ as $\beta = a_1 g_1 + \cdots + a_n g_n$. Since $d_1 \neq 1$, we have that $\beta \notin H$; then there must be some $g_i$ in this basis such that $g_i \notin H$ and $a_i \neq 0$. Thus, the set $N_1 := \{a \in \mathbb{N} : \exists \beta \in B_1, \text{basis } g_1, \ldots, g_n \text{ for } G, g_1 \notin H, a_2, \ldots, a_n \in \mathbb{Z} \text{ s.t. } \beta = ag_1 + a_2 g_2 + \ldots a_n g_n\}$ is nonempty. In other words, $N_1$ is the set of all positive coefficients of $G$-basis elements which do not lie in $H$ in any basis representation of an element of $B_1$, and $N_1$ is nonempty. Then since $N_1$ is a nonempty subset of $\mathbb{N}$, it necessarily contains a least element. Let $a_1$ be that least element, $\beta_1$ the corresponding element of $B_1$, and $g_1 \ldots, g_n$ the corresponding basis for $G$. Then $\beta_1 = a_1 g_1 + \cdots + a_n g_n$ for some $a_2, \ldots, a_n \in \mathbb{Z}$.

Now reorder the basis $g_1, \ldots, g_n$ if necessary so that $g_1$ is as before and for some $s \in \mathbb{N}$, $1 \leq s \leq n$, we have $g_i \notin H$ and $a_i \neq 0$ for $1 \leq i \leq s$, and either $g_i \in H$ or $a_i = 0$ for $s+1 \leq i \leq n$. Now assume that $a_1 \nmid a_i$ for some $i$, $1 \leq i \leq s$. Then using the division algorithm in the integers, there exist some $p, q \in \mathbb{Z}$ with $1 \leq q < a_1$ such that $a_i = pa_1 + q$. Then note that $\{g_1 + pg_i, g_2, \ldots, g_n\}$ forms another basis for $G$ and $\beta_1 = a_1(g_1 + pg_i) + a_2 g_2 + \cdots + a_{i-1} g_{i-1} + q g_i + a_{i+1} g_{i+1} + \cdots + a_n g_n$, where $g_i \notin H$ and $1 \leq q < a_1$. However, this contradicts minimality of $a_1$, so necessarily $a_1 | a_i$ for $1 \leq i \leq s$. Then we can write $\beta_1 + H = a_1 g_1 + \cdots + a_n g_n + H = a_1(g_1 + \frac{a_2}{a_1} g_2 + \cdots + \frac{a_s}{a_1} g_s) + H$. Then since $|\beta_1 + H| = d_1$, $d_1$ must divide $\left| g_1 + \frac{a_2}{a_1} g_2 + \cdots + \frac{a_s}{a_1} g_s + H \right|$. Then since every element of $G/H$ has order dividing $d_1$, we must have that $\left| g_1 + \frac{a_2}{a_1} g_2 + \cdots + \frac{a_s}{a_1} g_s + H \right| = d_1$, i.e. $g_1 + \frac{a_2}{a_1} g_2 + \cdots + \frac{a_s}{a_1} g_s \in B_1$. Then by minimality of $a_1$, it must be the case that $a_1 = 1$. Then $g_1 = \beta_1 - a_2 g_2 - \cdots - a_n g_n$, so $\{\beta_1, g_2, \ldots, g_n\}$ forms a basis for $G$. Importantly, $\beta_1$ is a member of some basis of $G$ and $|\beta_1 + H| = d_1$.

We will now continue inductively. Assume that we have similarly constructed a basis $\beta_1, \ldots, \beta_i, g_{i+1}, \ldots, g_n$ for $G$, where $\left|\beta_j + H\right| = d_j$ and $K = \langle \beta_1 + H \rangle \oplus \cdots \oplus \langle \beta_i + H \rangle \cong \mathbb{Z}_{d_1} \oplus \cdots \oplus \mathbb{Z}_{d_i}$, for some $i$, $1 \leq i < r$. Here, the $g_j$'s are not necessarily the same as above; they are simply an arbitrary completion of $\beta_1, \ldots, \beta_i$ to a basis for $G$. Then note that $(G/H)/K \cong \mathbb{Z}_{d_{i+1}} \oplus \cdots \oplus \mathbb{Z}_{d_r}$. Then as before, define the set $B_{i+1} := \{\beta \in G : |\beta + H + K| = d_{i+1}\}$. For any $\beta \in B_{i+1}$ and completion of $\beta_1, \ldots, \beta_i$ to a basis for $G$, we can write $\beta = a_1 \beta_1 + \cdots + a_i \beta_i + a_{i+1} g_{i+1} + \cdots + a_n g_n$ for some $a_j \in \mathbb{Z}$, $1 \leq j \leq n$. Then similarly to the base case, there must be some $j$, $i+1 \leq j \leq n$

such that $g_j \notin H$ and $a_j \neq 0$ (since otherwise, $|\beta + H + K| = 1$). Then as before, we will pick some $\beta_{i+1} \in B_{i+1}$ and basis $\beta_1, \ldots, \beta_i, g_{i+1} \ldots, g_n$ such that $g_{i+1} \notin H$ and $a_{i+1} \in \mathbb{N}$ is minimal across all such bases and choices of $\beta \in B_{i+1}$.

Again, reorder the basis so that $g_{i+1}, \ldots, g_s \notin H$, $a_{i+1}, \ldots, a_s \neq 0$, and for $s+1 \leq j \leq n$, either $g_j \in H$ or $a_j = 0$. Then by the same argument as in the base case, we can see that $a_{i+1} | a_j$ for $i+1 \leq j \leq s$. Then $\beta_{i+1} + H + K = a_{i+1}(g_{i+1} + \frac{a_{i+2}}{a_{i+1}} g_{i+2} + \cdots + \frac{a_s}{a_{i+1}} g_s) + H + K$. Then $d_{i+1} = |\beta_{i+1} + H + K|$ must divide $\left| g_{i+1} + \frac{a_{i+2}}{a_{i+1}} g_{i+2} + \cdots + \frac{a_s}{a_{i+1}} g_s + H + K \right|$, and since every element of $(G/H)/K$ has order dividing $d_{i+1}$, we have that $\left| g_{i+1} + \frac{a_{i+2}}{a_{i+1}} g_{i+2} + \cdots + \frac{a_s}{a_{i+1}} g_s + H + K \right| = d_{i+1}$. Then by minimality of $a_{i+1}$, we get that $a_{i+1} = 1$. Thus, $\beta_1, \ldots, \beta_{i+1}, g_{i+2}, \ldots, g_n$ is another basis for $G$.

By induction, we can construct a basis $\beta_1, \ldots, \beta_r, g_{r+1}, \ldots, g_n$ for $G$ such that $|\beta_i + H| = d_i$ for $1 \leq i \leq r$ and $\langle \beta_1 + H \rangle \oplus \cdots \oplus \langle \beta_r + H \rangle \cong \mathbb{Z}_{d_1} \oplus \cdots \oplus \mathbb{Z}_{d_r} \cong G/H$. Then the $\beta_i + H$'s generate $G/H$, so for $r+1 \leq i \leq n$, we can write $g_i + H = a_1\beta_1 + \cdots + a_r\beta_r + H$ for some $a_j \in \mathbb{Z}$, $1 \leq j \leq r$. For $r+1 \leq i \leq n$, we will now define $\beta_i = g_i - a_1\beta_1 - \cdots - a_r\beta_r \in H$. Then $\beta_1, \ldots, \beta_n$ form a basis for $G$. Furthermore, setting $d_j = 1$ for $r+1 \leq j \leq n$, we have that $d_i\beta_i \in H$ for $1 \leq i \leq n$.

Finally, take any $h \in H$ and write $h = a_1\beta_1 + \cdots + a_n\beta_n$. Then necessarily $a_1\beta_1 + \cdots + a_r\beta_r \in H$. However, as we have seen from the construction of the $\beta_i$'s, this means that $d_i | a_i$ for $1 \leq i \leq r$. Then keeping in mind that $d_i = 1$ for $r+1 \leq i \leq n$, $d_1\beta_1, \ldots, d_n\beta_n$ is a list of $n$ elements of $H$, a rank $n$ free abelian group, which generates all of $H$. Then this is a basis for $H$. □

**Example 2.1.6.** *Consider $G = \mathbb{Z} \oplus \mathbb{Z}$, a rank 2 free abelian group with subgroup $H = \langle (3,1), (2,3) \rangle$. Then $\left| G/H \right| = 7$ and $(1,0), (3,1)$ is a basis for $G$ such that $7(1,0), (3,1)$ is a basis for $H$.*

## 2.2 Dedekind Domains

We will now move on to results regarding general Dedekind domains that will be of interest to us later. Of note in this section is the proof that ideals in a Dedekind domain factor uniquely into prime ideals, which was one of the forms of factorization we mentioned briefly in the introduction.

**Lemma 2.2.1.** *Let $R$ be a Dedekind domain. Then every ideal of $R$ contains a product of prime ideals.*

*Proof.* Suppose that not every ideal of $R$ contains a product of prime ideals; then letting $S$ be the

set of all ideals of $R$ which do not contains a product of prime ideals, we have that $S$ is nonempty. Then since $R$ is Dedekind (and thus Noetherian), Proposition 1.2.42 tells us that $S$ has a maximal member, i.e. there is some $M \in S$ such that $M \subseteq I \in S \implies M = I$. Note that since $M \in S$, $M$ is neither a prime ideal nor $R$ itself. Then there must exist $\alpha, \beta \in R \backslash M$ such that $\alpha\beta \in M$. Now note that $\alpha R + M$ and $\beta R + M$ strictly contain $M$, so by maximality of $M$ in $S$, neither of these ideals can lie in $S$. Thus, both $\alpha R + M$ and $\beta R + M$ contain a product of prime ideals. However, this means that $(\alpha R + M)(\beta R + M) = \alpha\beta R + \alpha M + \beta M + M^2 \subseteq M$ contains a product of prime ideals, a contradiction. Then $S$ must actually be empty, so every ideal of $R$ contains a product of prime ideals. □

**Lemma 2.2.2.** *Let $R$ be a Dedekind domain which is not a field, $K$ its field of fractions, and $I$ a proper ideal of $R$. Then there exists some element $\gamma \in K \backslash R$ such that $\gamma I \subseteq R$.*

*Proof.* First, note that if $I = \{0\}$, the result holds for any $\gamma \in K \backslash R$. Then assume $I$ is nonzero and let $\alpha \in I$ be nonzero. By the previous lemma, there exist prime ideals $P_1, \ldots, P_r$ of $R$ such that $P_1 \ldots P_r \subseteq (\alpha)$. In particular, we will pick these primes so that $r$ is minimal, i.e. no product of $s$ ideals lies in $(\alpha)$ for $s < r$. Furthermore, since $I$ is a proper ideal, we know that there is some maximal ideal $P$ which contains $I$, which is necessarily prime. Thus, $P_1 \ldots P_r \subseteq (\alpha) \subseteq I \subseteq P$.

Now suppose that $P \neq P_i$ for $1 \leq i \leq r$. Then since $\dim(R) = 1$, we know that $P$ does not even contain any prime $P_i$. Then for $1 \leq i \leq r$, let $\alpha_i \in P_i \backslash P$. Then $\alpha_1 \ldots \alpha_r \in P_1 \ldots P_r \subseteq P$, but no $\alpha_i \in P$, contradicting primeness of $P$. Then it must be the case that $P = P_i$ for some $1 \leq i \leq r$; without loss of generality, assume that $P = P_1$.

Since $(\alpha)$ cannot contain a product of $r - 1$ primes, then $P_2 \ldots P_r \not\subseteq (\alpha)$. Then let $\beta \in P_2 \ldots P_r \backslash (\alpha)$. Since $\beta \notin (\alpha)$, then $\alpha \nmid \beta \implies \gamma = \frac{\beta}{\alpha} \in K \backslash R$. Furthermore, for any $a \in I \subseteq P$, $a\beta \in P_1 \ldots P_r \subseteq (\alpha)$, so $\gamma a = \frac{a\beta}{\alpha} \in R$. Then $\gamma I \subseteq R$. □

**Theorem 2.2.3.** *Let $R$ be a Dedekind domain and $I$ an ideal of $R$. Then there is some ideal $J$ of $R$ such that $IJ$ is principal. In fact, for any $\alpha \in I$, there is some ideal $J$ of $R$ such that $IJ = (\alpha)$.*

*Proof.* First, note that if $I = \{0\}$, then $IJ = (0)$ for any ideal $J$ of $R$. Moreover, if $R$ is a field, then $R$ is a PID and the result holds trivially. Now assuming that $R$ is not a field and $I$ is nonzero, let $\alpha \in I$ be nonzero and consider the set $J := \{\beta \in R : \beta I \subseteq (\alpha)\}$. Note that $J$ is an ideal of $R$. Furthermore, $IJ \subseteq (\alpha)$. Then let $A = \alpha^{-1} IJ$, which can be seen to be another ideal of $R$. Now if

$A = R$, then $1 \in \alpha^{-1}IJ \implies \alpha \in IJ \implies IJ = (\alpha)$. In this case, we are done. Then assume that $A$ is a proper ideal of $R$.

If $A$ is a proper ideal of $R$, then by the second lemma above, there is some $\gamma \in K \backslash R$ such that $\gamma A \subseteq R$. Since $\alpha \in I$, note that $J \subseteq \alpha^{-1}IJ = A$. Then $\gamma J \subseteq \gamma A \subseteq R$. Now let $\beta \in J$ so that $\gamma\beta \in \gamma J$. Then note that $\alpha^{-1}\gamma\beta I \subseteq \gamma\alpha^{-1}IJ = \gamma A \subseteq R$. Thus, $\gamma\beta I \subseteq (\alpha)$, meaning that $\gamma\beta \in J$ by the definition of $J$. Then $\gamma J \subseteq J$.

Since $J$ is an ideal in the Dedekind domain $R$, we know that $J$ is finitely generated; then let $\beta_1, \ldots, \beta_m$ be a generating set for $J$. Then since $\gamma J$ is generated by $\gamma\beta_1, \ldots, \gamma\beta_m$, we can construct a matrix equation

$$M \begin{bmatrix} \beta_1 \\ \vdots \\ \beta_m \end{bmatrix} = \gamma \begin{bmatrix} \beta_1 \\ \vdots \\ \beta_m \end{bmatrix},$$

with $M \in R^{m \times m}$. Then $\gamma$ is an eigenvalue of $M$, i.e. $\gamma$ is a root of the monic polynomial $\det(xI - M) \in R[x]$ (here, I refers to the $m \times m$ identity matrix, not the ideal). However, since $R$ is integrally closed, this implies that $\gamma \in R$, a contradiction. Then it must be the case that $A = R$, i.e. $IJ = (\alpha)$, a principal ideal. □

This is a very powerful statement that will allow us to make several observations about Dedekind domains. First, we have two immediate corollaries that will assist us in these observations.

**Corollary 2.2.4.** *Let $A$, $B$, and $C$ be ideals in a Dedekind domain $R$ with $A$ nonzero. If $AB = AC$, then $B = C$.*

*Proof.* By the theorem, there is some ideal $J$ of $R$ such that $AJ = (\alpha)$, a nonzero principal ideal. Then $\alpha B = JAB = JAC = \alpha C$. For any $b \in B$, note that there is some $c \in C$ such that $\alpha b = \alpha c$, so $b = c \in C$. Then $B \subseteq C$, and by symmetry, $C \subseteq B$. Then $B = C$. □

This property is often referred to as the Cancellation Law in a Dedekind domain.

**Corollary 2.2.5.** *Let $A$ and $B$ be ideals in a Dedekind domain $R$ with $A$ nonzero. Then $A|B \iff B \subseteq A$.*

*Proof.* Assume first that $A|B$, i.e. there is some ideal $C$ of $R$ such that $AC = B$. Then since $AC \subseteq AR = A$, $B \subseteq A$. Note that this part of the proof does not use the theorem, and so will hold in any ring.

Now assume that $B \subseteq A$. By the theorem, there is some ideal $J$ of $R$ such that $JA = (\alpha)$, a nonzero principal ideal. Then consider the set $C = \alpha^{-1}JB$. Since $JB \subseteq JA = (\alpha)$, $C \subseteq R$. Furthermore, it is straightforward to check that $C$ is actually an ideal of $R$. Then $AC = \alpha^{-1}AJB = \alpha^{-1}(\alpha)B = B$, so $A|B$. □

Now before getting to unique factorization of ideals in a Dedekind domain, we have one more result that applies to the two class groups we discussed in the previous chapter.

**Theorem 2.2.6.** *Let $R$ be a Dedekind domain and $I$ a nonzero fractional ideal of $R$. Then $I$ is invertible.*

*Proof.* Recall from the definition of a fractional ideal that there exists some nonzero $\alpha \in R$ such that $\alpha I \subseteq R$. As we have seen, $\alpha I$ is actually an ideal of $R$. Then using the previous theorem, there is some ideal $J$ of $R$ such that $\alpha IJ = (\beta)$ for some nonzero $\beta \in R$. Then $(\frac{\alpha}{\beta}J)I = R$, so by Proposition 1.2.64, $I^{-1} = \frac{\alpha}{\beta}J$ and $I$ is an invertible ideal of $R$. □

**Corollary 2.2.7.** *Let $R$ be a Dedekind domain. Then $DivCl(R) = Cl(R)$.*

*Proof.* This follows directly from the theorem and the fact that any invertible ideal is divisorial. □

These results tell us that if $R$ is a Dedekind domain, we don't need to concern ourselves with the definitions of divisorial or invertible ideals. Any nonzero fractional ideal is both invertible and divisorial, so we only need to consider nonzero fractional ideals. Furthermore, Proposition 1.2.70 tells us that when looking at $DivCl(R) = Cl(R)$, we can actually further restrict ourselves to looking at nonzero integral ideals in $R$, since every class contains an integral ideal of $R$. For this reason, the ideal class group is usually considered when working in a Dedekind domain, since there is a simpler equivalent definition of $Cl(R)$.

**Definition 2.2.8.** *Let $R$ be a Dedekind domain. Then define an equivalence relation $\sim$ on the nonzero ideals of $R$ such that $I \sim J$ if and only if $\alpha I = \beta J$ for some nonzero $\alpha, \beta \in R$ (or equivalently, iff $I = \gamma J$ for some $\gamma \in K$). This separates $R$ into* **ideal classes** *$[I]$, with $[I] = [J]$ if and only if $I \sim J$. The ideal classes in $R$ form a group under the operation $[I][J] = [IJ]$, called the* **ideal class group** *of $R$, denoted $Cl(R)$. In other words, if we let $S$ denote the set of nonzero ideals of $R$, $Cl(R) = S/\sim$.*

We are now ready to prove unique factorization of ideals in a Dedekind domain.

**Theorem 2.2.9.** *Let $R$ be a Dedekind domain. Then the nonzero ideals of $R$ factor uniquely into prime ideals. More precisely, if $I$ is a nonzero ideal in $R$, then $I = P_1 \dots P_r$ for prime ideals $P_1, \dots, P_r$, and if $P_1 \dots P_r = Q_1 \dots Q_s$ are two equal products of nonzero prime ideals, then $r = s$ and (after rearranging, if necessary), $P_i = Q_i$ for $1 \leq i \leq r$.*

*Proof.* We must first show that every nonzero ideal of $R$ can be represented as a product of prime ideals. Let $S$ be the set of nonzero ideals of $R$ which cannot be represented as a product of prime ideals. If $S$ is empty, we are done; otherwise, $S$ is nonempty and thus has a maximal member $M$, since $R$ is Noetherian. By convention, we will say that $R$ is the empty product of ideals, and thus $M$ is a proper ideal of $R$. Then $M$ is contained in some maximal ideal $P$, which must be prime. Corollary 2.2.5 then tells us that there is some ideal $I$ of $R$ such that $M = PI$. Now if $I$ is representable as a product of prime ideals, so is $M$, a contradiction; then $I \in S$. However, note that $I$ divides $M$, so $M \subseteq I$. Furthermore, if $M = I$, then $M = PI = PM \implies R = P$, a contradiction. Then $S$ must actually be empty, so every ideal of $R$ can be written as a product of prime ideals.

Now assume we have two equal factorizations $P_1 \dots P_m = Q_1 \dots Q_n$ of nonzero prime ideals in $R$. Then $Q_1 \dots Q_n \subseteq P_1$. As in the proof of Lemma 2.2.2, we can see that $P_1$ is necessarily equal to one of the primes $Q_i$, so without loss of generality we will assume that $P_1 = Q_1$. Then by the cancellation law, $P_2 \dots P_m = Q_2 \dots Q_n$. Continuing inductively (and assuming without loss of generality that $m \geq n$), we get that (after rearranging), $P_i = Q_i$ for $1 \leq i \leq n$ and $P_{n+1} \dots P_m = R$, so $R \subseteq P_i$ for $n + 1 \leq i \leq m$. Then this must be an empty product, so $m = n$. Thus, factorization into prime ideals is unique. □

The unique factorization of ideals in a Dedekind domain into prime ideals is perhaps one of the most significant properties of this type of domain. As we will see in the next section, this property is especially going to be important to the field of algebraic number theory. For some time, this even gave some significant progress toward proving Fermat's Last Theorem (see [9], Chapter 1 for further discussion).

Now recall that two ideals in a ring are generally considered to be relatively prime if their sum ideal is the entire ring. However, the fact that ideals factor uniquely into prime ideals also suggests a definition of relatively prime. Fortunately, these ideas will coincide in a Dedekind domain, as the following result shows.

**Theorem 2.2.10.** *Let $R$ be a Dedekind domain and $I, J$ nonzero ideals of $R$. Suppose that $I =$*

$P_1^{a_1} \dots P_r^{a_r}$ *and* $J = P_1^{b_1} \dots P_r^{b_r}$*, with* $P_i$ *a prime ideal in* $R$ *and* $a_i, b_i \in \mathbb{N} \cup \{0\}$ *for* $1 \leq i \leq r$*. Then* $I + J = P_1^{m_1} \dots P_r^{m_r}$ *and* $I \cap J = P_1^{M_1} \dots P_r^{M_r}$*, where* $m_i = \min\{a_i, b_i\}$ *and* $M_i = \max\{a_i, b_i\}$*.*

*Proof.* Let $\alpha \in I$ and $\beta \in J$ so that $\alpha + \beta$ is a generic element of $I + J$. Then note that $\alpha, \beta \in P_i^{m_i}$ for $1 \leq i \leq r$, so $\alpha + \beta \in P_i^{m_i}$. Thus, $I + J \subseteq P_1^{m_1} \dots P_r^{m_r}$. Now for any prime $P$ which is not one of the $P_i$, note that $\alpha \in I \subseteq I + J$, but $\alpha \notin P$. Then $P \nmid I + J$. Furthermore, for any of the $P_i$, $1 \leq i \leq r$, note that $m_i = a_i$ or $m_i = b_i$. In the first case, there is some element $\alpha \in I$ such that $\alpha \notin P_i^{a_i+1}$, so $P_i^{m_i+1} = P_i^{a_i+1} \nmid I + J$. Similarly, if $m_i = b_i$, then there is some $\beta \in J$ such that $\beta \notin P_i^{b_i+1}$, so $P_i^{m_i+1} = P_i^{b_i+1} \nmid I + J$. Then by unique factorization of ideals into primes, $I + J = P_1^{m_1} \dots P_r^{m_r}$.

Now note that $I \cap J \subseteq I$ and $I \cap J \subseteq J$, so $I \mid I \cap J$ and $J \mid I \cap J$. Thus, $P_1^{M_1} \dots P_r^{M_r} \mid I \cap J$, so $I \cap J \subseteq P_1^{M_1} \dots P_r^{M_r}$. Furthermore, $P_1^{M_1} \dots P_r^{M_r} \subseteq I$ and $P_1^{M_1} \dots P_r^{M_r} \subseteq J$, so $P_1^{M_1} \dots P_r^{M_r} \subseteq I \cap J$. Then $I \cap J = P_1^{M_1} \dots P_r^{M_r}$. □

**Corollary 2.2.11.** *Let* $R$ *be a Dedekind domain and* $I, J$ *nonzero ideals of* $R$*. Then* $I$ *and* $J$ *are relatively prime, i.e.* $I + J = R$*, if and only if no prime ideal* $P$ *divides both* $I$ *and* $J$*. In other words, if and only if* $I$ *and* $J$ *are not contained within the same prime ideal.*

We will now use unique factorization of ideals to relate Dedekind domains back to the more fundamental types of integral domains and to the topic of factorization of elements.

**Theorem 2.2.12.** *Let* $R$ *be a Dedekind domain. Then* $R$ *is a PID if and only if* $R$ *is a UFD.*

*Proof.* We have already seen that any PID is a UFD; then it remains to show that the converse also holds when $R$ is Dedekind. Let $R$ be a Dedekind UFD and $I$ an ideal of $R$. If $I = \{0\}$, then $I$ is trivially principal. Then assume $I$ is nonzero. By Theorem 2.2.3, $I$ divides some nonzero principal ideal $(\alpha)$ of $R$. Since $R$ is a UFD, $\alpha$ factors uniquely into a product $\alpha = \pi_1 \dots \pi_n$ of irreducible elements of $R$. By Corollary 1.2.28, we can see that each $\pi_i$ is actually prime and thus generates a prime ideal. Then $I|(a) = (\pi_1) \dots (\pi_n)$, and so by unique factorization of ideals in a Dedekind domain (and after some possible rearranging), $I = (\pi_1) \dots (\pi_r)$ for some $0 \leq r \leq n$. Then $I = (\pi_1 \dots \pi_r)$, a principal ideal. Thus, $R$ is a PID. □

**Corollary 2.2.13.** *Let* $R$ *be a Dedekind domain. Then* $\left|Cl(R)\right| = 1$ *if and only if* $R$ *is a UFD.*

*Proof.* Note that since $R$ is Dedekind, then every nonzero ideal of $R$ is invertible and thus belongs to some ideal class in $Cl(R)$. Thus, $\left|Cl(R)\right| = 1$ if and only if every nonzero ideal of $R$ belongs to

the identity class, which is the set of principal fractional ideals of $R$. This is true if and only if $R$ is a PID, which by the theorem is true if and only if $R$ is a UFD. $\square$

This corollary tells us a way to interpret the size of the ideal class group of a Dedekind domain. In some sense, the larger the ideal class group of $R$ is, the farther away $R$ is from having unique factorization.

To finish the discussion of Dedekind domains, we have the following results connecting them to some of the other types of rings discussed in the previous chapter. The results discussed here can be found in [5].

**Lemma 2.2.14.** *Let $R$ be a Dedekind domain and $S$ a multiplicatively closed subset of $R$ which does not contain 0. Then $T := S^{-1}R$, the localization of $R$ by $S$, is also a Dedekind domain.*

*Proof.* By the definition of a Dedekind domain, we must show that $T$ is Noetherian, has Krull dimension 1, and is integrally closed in its field of fractions. Note here that if $K$ is the field of fractions of $R$, then $K$ is also the field of fractions of $T$.

Let $I$ and $J$ be ideals in $T$ with strict containment $I \subset J$. Clearly, $I \cap R$ and $J \cap R$ are ideals in $R$. Because the containment above is strict, there is some $\alpha\beta^{-1} \in J \backslash I$ with $\alpha \in R$ and $\beta \in S$. Then $\alpha = \alpha\beta^{-1}\beta \in J \cap R$. If $\alpha \in I \cap R$, then $\alpha\beta^{-1} \in I$, a contradiction. Then we also have a strict containment $I \cap R \subset J \cap R$.

Now assume that we have an infinite strictly ascending chain of ideals $I_1 \subset I_2 \subset \dots$ in $T$. Then $I_1 \cap R \subset I_2 \cap R \subset \dots$ is an infinite strictly ascending chain of ideals in $R$, contradicting the fact that $R$ is Noetherian. Then no such chain can exist in $T$, so $T$ is also Noetherian.

Now let $P$ be a nonzero prime ideal of $R$ and $I$ an ideal of $T$ strictly containing $P$. Note that if $\alpha, \beta \in R$ such that $\alpha\beta \in P \cap R$, then either $\alpha$ or $\beta$ lies in $P$, by primeness of $P$. Then since each is an element of $R$, one or the other must lie in $P \cap R$, i.e. $P \cap R$ is a nonzero prime ideal of $R$. Since $R$ is a Dedekind domain, then $P \cap R$ is thus a maximal ideal of $R$. Now by the above discussion, $I \cap R$ strictly contains $P \cap R$, meaning that $I \cap R = R$, so $1 \in I$. Then $I = T$, so $P$ is maximal. Then every nonzero prime ideal in $T$ is maximal, so $T$ has Krull dimension 1.

Finally, let $\alpha \in K$ be integral over $T$. Then for some $n \in \mathbb{N}$, $a_i \in R$, and $b_i \in S$, $0 \leq i \leq n-1$, $\alpha^n + \frac{a_{n-1}}{b_{n-1}}\alpha^{n-1} + \dots + \frac{a_1}{b_1}\alpha + \frac{a_0}{b_0} = 0$. Now let $\beta = b_0 \dots b_{n-1} \in S$. Then multiplying the above polynomial by $\beta^n$ and noting that $\frac{\beta}{b_i} \in R$ for $0 \leq i \leq n-1$, we have $(\alpha\beta)^n + \frac{\beta}{b_{n-1}}a_{n-1}(\alpha\beta)^{n-1} + \dots + \frac{\beta^{n-1}}{b_1}a_1(\alpha\beta) + \frac{\beta^n}{b_0}a_0 = 0$. Then $\alpha\beta$ is a root of a polynomial in

$R[x]$; since $R$ is integrally closed in $K$, $\alpha\beta \in R$. Then since $\beta \in S$, $\alpha \in S^{-1}R$, so $T = S^{-1}R$ is integrally closed. Therefore, $T$ is a Dedekind domain. □

**Theorem 2.2.15.** *Let $R$ be a Dedekind domain. Then $R$ is a regular Krull domain.*

*Proof.* First, we will show that $R$ is regular. Note that if $R$ is a field, then $R$ is already a regular local ring with maximal ideal $\{0\}$ generated by $\dim(R) = 0$ elements. Thus, if $R$ is a field, $R$ is regular. Then assume that $R$ is not a field, i.e. $\dim(R) = 1$. By definition of a Dedekind domain, we know that $R$ is Noetherian. Then we need to show that for any prime ideal $P$ of $R$, the localization $R_P$ of $R$ at $P$ is a regular local ring. Since $\dim(R) = 1$, this is equivalent to showing that the maximal ideal $PR_P$ of $R_P$ is principal. By the lemma, we know that $R_P$ is Dedekind; then every ideal in $R_P$ factors uniquely into prime ideals, and every prime ideal of $R_P$ is maximal. Then since there is only one maximal ideal, every ideal $I$ in $R_P$ is $I = (PR_P)^k$ for some $k \in \mathbb{N}$. Then letting $\alpha \in PR_P \backslash (PR_P)^2$ (by cancellation, $PR_P \neq (PR_P)^2$), we have that $(\alpha) \subseteq PR_P$ but $(\alpha) \not\subseteq (PR_P)^2$. Then $(\alpha) = PR_P$, i.e. $PR_P$ is principal. Thus, $R$ is a regular ring.

Now from the definition of a Krull domain, recall that we are concerned with $\mathcal{P}$, the collection of prime ideals of $R$ which have height 1. If $R$ is a field, then $\mathcal{P}$ is empty and we consider $R$ to be vacuously a Krull domain (see the discussion following this proof). Otherwise, $\dim(R) = 1$, so $\mathcal{P}$ consists of all nonzero prime ideals of $R$. We must now show the three conditions for a Krull domain (see Definition 1.2.51).

First, let $P$ be a nonzero prime ideal of $R$. From above, we know that $R_P$ is a local ring with principal maximal ideal. Furthermore, we showed that every ideal of $R_P$ is a power of that principal ideal. Then every ideal $I$ of $R_P$ is $(\alpha^k)$ for some $k \in \mathbb{N}$, where $(\alpha)$ is the unique maximal ideal. Then $R_P$ is a local PID, and since no element of $P$ is invertible (and $P$ is nonzero), $R_P$ is not a field. Then $R_P$ is a DVR for any nonzero prime ideal $P$ of $R$, so $R$ satisfies condition 1 for a Krull domain.

Now note that $R \subseteq R_P$ for every nonzero prime ideal $P$ of $R$. Thus, $R \subseteq \bigcap_{P \in \mathcal{P}} R_P$. Now let $\alpha \in \bigcap_{P \in \mathcal{P}} R_P$, i.e. $\alpha \in R_P$ for every nonzero prime ideal $P$ of $R$. Then let $P$ be any nonzero prime ideal of $R$ and write $\alpha = \beta\gamma^{-1}$, with $\beta \in R$, $\gamma \in R \backslash P$. By unique factorization of ideals in $R$, there exist distinct primes $P_1, \ldots, P_r$ and $k_1, \ldots, k_r \in \mathbb{N}$ such that $(\gamma) = P_1^{k_1} \ldots P_r^{k_r}$. Here, we are simply using the usual factorization into prime ideals and grouping identical primes together. Then for each of these primes, $\alpha \in R_{P_i}$, so $\alpha = \beta_i \gamma_i^{-1}$ for some $\beta \in R$, $\gamma_i \in R \backslash P_i$. Then $\beta_i \gamma = \beta \gamma_i$.

Since the left side of this equation is in $P_i^{k_i}$, then the left side is as well, i.e. $P_i^{k_i}|(\beta\gamma_i) = (\beta)(\gamma_i)$. However, $P_i \nmid (\gamma_i)$, so we must have that $P_i^{k_i}|(\beta)$, i.e. $\beta \in P_i^{k_i}$. Then applying this for $1 \leq i \leq r$, we get that $\beta \in P_1^{k_1} \dots P_r^{k_r} = (\gamma)$, so $\alpha = \beta\gamma^{-1} \in R$. Then $R = \bigcap_{P \in \mathcal{P}} R_P$, so $R$ satisfies condition 2 for a Krull domain.

Finally, let $\alpha \in R$ be nonzero. Then $(\alpha) = P_1 \dots P_n$ for some prime ideals $P_i$ of $R$, $1 \leq i \leq n$. By unique factorization of ideals into primes, $(\alpha)$ is not contained in any primes in $R$ other than $P_1, \dots, P_n$. Then $\alpha$ is in at most $n$ prime ideals of $R$ (not necessarily exactly $n$, since the $P_i$'s are not necessarily distinct), so $R$ satisfies condition 3 for a Krull domain. Then $R$ is a regular Krull domain. □

It should be noted here that some sources do not consider fields to be Krull domains. As in Definition 1.2.51, we can see that the second condition may produce some uncertainty when $\mathcal{P}$ is empty. For the purposes of this thesis, we will consider a field to be vacuously a Krull domain. In either case, the above theorem holds for non-field Krull domains. From this point on, any Krull domains we consider will be non-fields regardless, so this convention will not matter.

## 2.3 Number Rings

We are now ready to produce some important results regarding number rings and their related structures.

**Lemma 2.3.1.** *Let $K$ be a number field with $[K : \mathbb{Q}] = n$, $\alpha_1, \dots, \alpha_n$ a basis for $K$ consisting entirely of algebraic integers, and $d = \operatorname{disc}(\alpha_1, \dots, \alpha_n) \in \mathbb{Z}$. Then every $\alpha \in \mathcal{O}_K$ can be expressed in the form*

$$\alpha = \frac{m_1\alpha_1 + \dots + m_n\alpha_n}{d},$$

*with each $m_i \in \mathbb{Z}$ and each $m_i^2$ divisible by $d$.*

*Proof.* Let $\alpha \in R$ and write $\alpha = a_1\alpha_1 + \dots + a_n\alpha_n$, with $a_i \in \mathbb{Q}$ for $1 \leq i \leq n$. Then applying each embedding of $K$ into $\mathbb{C}$ to $\alpha$, we get that $\sigma_i(\alpha) = a_1\sigma_i(\alpha_1) + \dots + a_n\sigma_i(\alpha_n)$ for $1 \leq i \leq n$. Applying Cramer's rule to this system of $n$ equations gives $a_i = \frac{b_i}{\delta}$, where $\delta = \left|\sigma_i(\alpha_j)\right|$ (so $\delta^2 = d$) and $b_i$ is the discriminant of the matrix obtained by replacing the $i^{th}$ column of $\left[\sigma_i(\alpha_j)\right]$ with the column vector $[\sigma_i(\alpha)]$. Then from these determinants, we can see that $\delta$ and $b_i$ are algebraic integers, $1 \leq i \leq n$. Furthermore, $a_i = \frac{b_i}{\delta} \implies da_i = \delta b_i$. Thus, $da_i \in \mathbb{Q}$ is an algebraic integer, so $da_i \in \mathbb{Z}$. Then letting

$m_i = da_i$ for $1 \leq i \leq n$, we get the desired representation. Moreover, $m_i^2 = (da_i)^2 = (\delta b_i)^2 = db_i^2$. Then $b_i^2$ is an algebraic integer which lies in $\mathbb{Q}$, so $b_i^2 \in \mathbb{Z}$ and $d|m_i^2$ in $\mathbb{Z}$. □

**Theorem 2.3.2.** *Let $K$ be a number field with $[K : \mathbb{Q}] = n$. Then the additive group of $\mathcal{O}_K$ is a rank $n$ free abelian group.*

*Proof.* Let $\alpha_1, \ldots, \alpha_n$ be a basis for $K$ consisting entirely of algebraic integers. Then $\alpha_1\mathbb{Z} + \cdots + \alpha_n\mathbb{Z} \subseteq \mathcal{O}_K$, so $\mathcal{O}_K$ contains a rank $n$ free abelian group. Furthermore, the lemma shows that $\mathcal{O}_K \subseteq \frac{\alpha_1}{d}\mathbb{Z} + \cdots + \frac{\alpha_n}{d}\mathbb{Z}$, so $\mathcal{O}_K$ is contained in a rank $n$ free abelian group. Then by Corollary 2.1.3, $\mathcal{O}_K$ is (additively) a rank $n$ free abelian group. □

**Definition 2.3.3.** *Let $K$ be a number field. Any $\mathbb{Z}$-basis for $\mathcal{O}_K$ is called an* **integral basis**.

**Proposition 2.3.4.** *Let $K$ be a number field with $[K : \mathbb{Q}] = n$ and $\alpha_1, \ldots, \alpha_n$ an integral basis for $R$. Then $\alpha_1, \ldots, \alpha_n$ form a $\mathbb{Q}$-basis for $K$.*

*Proof.* Recall that any $\alpha \in K$ has some $c \in \mathbb{N}$ such that $c\alpha \in R$. Then $c\alpha = a_1\alpha_1 + \cdots + a_n\alpha_n$ for some $a_i \in \mathbb{Z}$, so $\alpha = c^{-1}(a_1\alpha_1 + \cdots + a_n\alpha_n)$. Then the $\alpha_i$'s are a list of $n$ elements of $K$ which span $K$ over $\mathbb{Q}$, so they must form a $\mathbb{Q}$-basis for $K$. □

We will now continue with corollaries to Theorem 2.3.2. Proofs which are omitted are immediate from previous results.

**Corollary 2.3.5.** *Let $K$ be a number field with $[K : \mathbb{Q}] = n$ and $I$ a nonzero ideal of $\mathcal{O}_K$. Then the additive group of $I$ is a rank $n$ free abelian group.*

*Proof.* Let $\alpha \in I$ be nonzero. Then $\alpha^{-1} \in K$, so there is some nonzero $c \in \mathbb{N}$ such that $c\alpha^{-1} \in \mathcal{O}_K$. Then $c = c\alpha^{-1}\alpha \in I$, so $I$ contains a nonzero rational integer. Then $cR \subseteq I \subseteq R$, with both $cR$ and $R$ being (additively) rank $n$ free abelian groups. Then by Corollary 2.1.3, $I$ is (additively) a rank $n$ free abelian group. □

**Corollary 2.3.6.** *Let $K$ be a number field and $I$ an ideal of $\mathcal{O}_K$. Then $R/I$ is finite.*

**Corollary 2.3.7.** *Let $K$ be a number field. Then any integral basis for $\mathcal{O}_K$ has the same discriminant. This allows us to define the* **discriminant of $\mathcal{O}_K$,** $\mathrm{disc}(\mathcal{O}_K)$ *(sometimes written* $\mathrm{disc}(K)$*) as the discriminant of any integral basis of $\mathcal{O}_K$.*

**Proposition 2.3.8.** *Let $K$ be a number field and $R, S$ rank $n$ $\mathbb{Z}$-submodules of $K$ with $R \subseteq S$. Then* $\mathrm{disc}(R) = \left|S/R\right|^2 \mathrm{disc}(S)$*, where* $\mathrm{disc}(S)$ *is the discriminant of any $\mathbb{Z}$-basis for $S$ (and* $\mathrm{disc}(R)$ *similarly defined).*

*Proof.* Since the additive groups of $R$ and $S$ are rank $n$ free abelian subgroups, there exist a basis $\beta_1, \ldots, \beta_n$ for $S$ and integers $d_1, \ldots, d_n$ such that $d_1\beta_1, \ldots, d_n\beta_n$ is a basis for $R$. Then

$$\mathrm{disc}(R) = \left|\sigma_i(d_j\beta_j)\right|^2 = (d_1 \ldots d_n)^2 \left|\sigma_i(\beta_j)\right|^2 = \left|S/R\right|^2 \mathrm{disc}(S).$$

□

**Corollary 2.3.9.** *Let $K$ be a number field with $[K : \mathbb{Q}] = n$ and $\alpha_1, \ldots, \alpha_n \in \mathcal{O}_K$. Then $\alpha_1, \ldots, \alpha_n$ form an integral basis for $\mathcal{O}_K$ if and only if* $\mathrm{disc}(\mathcal{O}_K) = \mathrm{disc}(\alpha_1, \ldots, \alpha_n)$.

*Proof.* As we have just seen, any integral basis for $\mathcal{O}_K$ has the same discriminant. Then assume that $\mathrm{disc}(\alpha_1, \ldots, \alpha_n) = \mathrm{disc}(\mathcal{O}_K)$. Note that the $\alpha_i$'s must be linearly independent; otherwise $\mathrm{disc}(\alpha_1, \ldots, \alpha_n) = 0$, and we know that $\mathrm{disc}(\mathcal{O}_K) \neq 0$ by Proposition 2.3.4 and Proposition 1.3.29. Note that $R = \alpha_1\mathbb{Z} + \cdots + \alpha_n\mathbb{Z}$ is a rank $n$ free abelian subgroup of $\mathcal{O}_K$. Then by the previous corollary, $\mathrm{disc}(\alpha_1, \ldots, \alpha_n) = \left|\mathcal{O}_K/R\right|^2 \mathrm{disc}(\mathcal{O}_K)$. Then $\left|\mathcal{O}_K/R\right| = 1$, so $\alpha_1, \ldots, \alpha_n$ form an integral basis for $\mathcal{O}_K$. □

Already, this gives us a great deal of information about the additive structure of number rings. However, we can do more by directing our attention back to Dedekind domains.

**Theorem 2.3.10.** *Let $K$ be a number field. Then $\mathcal{O}_K$ is a Dedekind domain.*

*Proof.* Let $I$ be an ideal in $\mathcal{O}_K$. If $I = \{0\}$, then $I$ is trivially finitely generated. If $I$ is nonzero, then $I$ is (additively) a rank $n$ free abelian subgroup, where $n = [K : \mathbb{Q}]$. Then since $\mathbb{Z} \subseteq \mathcal{O}_K$, $I$ is generated as an ideal of $\mathcal{O}_K$ by any basis for its additive group. Then any ideal of $\mathcal{O}_K$ is finitely generated, so $\mathcal{O}_K$ is Noetherian.

Now let $P$ be a nonzero prime ideal of $\mathcal{O}_K$. Then $\mathcal{O}_K/P$ is an integral domain, and by Corollary 2.3.6, $\mathcal{O}_K/P$ is finite. Corollary 1.2.5 then tells us that $\mathcal{O}_K/P$ is a field. Thus, $P$ must be a maximal ideal. Then every nonzero prime ideal of $\mathcal{O}_K$ is maximal, i.e. $\dim(\mathcal{O}_K) = 1$.

Finally, let $\alpha \in K$ be integral over $\mathcal{O}_K$. Then $\alpha$ is a root of a monic polynomial whose coefficients are algebraic integers, so Corollary 1.3.10 tells us that $\alpha$ is also an algebraic integer.

Since $\alpha$ is an algebraic integer lying in $K$, we know that $\alpha \in \mathcal{O}_K$. Then $\mathcal{O}_K$ is integrally closed, so $\mathcal{O}_K$ is a Dedekind domain. $\square$

We can now apply all of the previous results about Dedekind domains to number rings. In particular, we know that the ideals in $\mathcal{O}_K$ are all invertible and factor uniquely into a product of prime ideals, $\mathcal{O}_K$ is a PID iff it is a UFD, and $\mathcal{O}_K$ is a regular Krull domain.

Since the ideals in $\mathcal{O}_K$ factor uniquely into prime ideals, it is natural to consider how the principal ideals $(p)$ factor in $\mathcal{O}_K$, where $p$ is a rational prime. Although we will not delve too deeply into this subject, we will need the following definition and theorem later. Both can be found in [9], Chapter 3 along with a more thorough treatment of this phenomena, called the "splitting" of primes.

**Definition 2.3.11.** *Let $K$ be a number field. We say that a prime $p \in \mathbb{Z}$ is* **inert** *in $K$ (or in $\mathcal{O}_K$) if $(p) = p\mathcal{O}_K$ is a prime ideal in $\mathcal{O}_K$.*

**Theorem 2.3.12.** *Let $K = \mathbb{Q}[\sqrt{d}]$ be a quadratic number field for some squarefree $d \in \mathbb{Z}$. Then 2 is inert in $K$ if and only if $d \equiv 5 \pmod 8$, and an odd prime $p$ is inert in $K$ if and only if $\left(\frac{d}{p}\right) = -1$.*

We will now turn our attention to two structures within a number ring which we defined in the previous chapter.

**Theorem 2.3.13. (Dirichlet's Unit Theorem)** *Let $K$ be a number field with $[K : \mathbb{Q}] = n$. Then $U(\mathcal{O}_K)$, the group of units in the number ring $\mathcal{O}_K$, is a direct product $U(\mathcal{O}_K) = W \times V$, where $W$ is a finite cyclic group consisting of the roots of unity in $\mathcal{O}_K$ and $V$ is a free abelian group of rank $r_1 + r_2 - 1$. Here $r_1$ is the number of real embeddings of $K$ into $\mathbb{C}$ (i.e. the number of $\sigma$ such that $\sigma(K) \subseteq \mathbb{R}$) while $r_2$ is the number of complex conjugate pairs of non-real embeddings of $K$ into $\mathbb{C}$, so $n = r_1 + 2r_2$.*

*Proof.* See [9], Theorem 38. $\square$

**Example 2.3.14.** *Let $K = \mathbb{Q}[\sqrt{d}]$, a quadratic number field, for some squarefree $d \in \mathbb{Z}$. If $d < 0$, then $U(\mathcal{O}_K)$ is a finite cyclic group. If $d > 0$, then $U(\mathcal{O}_K) = \pm\{\pm u^k : k \in \mathbb{Z}\} \cong \mathbb{Z}_2 \oplus \mathbb{Z}$ for some $u \in U(\mathcal{O}_K)$, called the* **fundamental unit** *in $\mathcal{O}_K$.*

As we have discussed before, the unit group of a general ring is very important to determining how elements factor. However, we will see later that the unit group is very important to the major

results of this paper. Additionally, we will need to consider orders in a number ring. The following discussion can be seen in greater detail in [11].

**Theorem 2.3.15.** *Let $K$ be a number field with $[K : \mathbb{Q}] = n$. A subring (with unity) $\mathcal{O}$ of $K$ is an order of $K$ if and only if $\mathcal{O}$ is a free $\mathbb{Z}$-submodule of $\mathcal{O}_K$ of rank $n$.*

*Proof.* First, assume that $\mathcal{O}$ is an order of $K$. Then note that by the definition of an order, the additive group of $\mathcal{O}$ must be a free abelian group generated by a basis for $R$ over $\mathbb{Q}$. Then $\mathcal{O}$ must be a free $\mathbb{Z}$-submodule of $K$ of rank $n$. Since $\mathcal{O}$ is a subring of $\mathbb{C}$ having finitely generated additive group, Proposition 1.3.8 tells us that any $\alpha \in \mathcal{O}$ is an algebraic integer, so $\mathcal{O} \subseteq \mathcal{O}_K$. Then $\mathcal{O}$ is a free $\mathbb{Z}$-submodule of $\mathcal{O}_K$ of rank $n$.

Now assume that $\mathcal{O}$ is a free $\mathbb{Z}$-submodule of $\mathcal{O}_K$ of rank $n$. Then $\mathcal{O}$ is (additively) a free abelian group generated by some $\alpha_1, \ldots, \alpha_n \in \mathcal{O}$. Then we know that $\text{disc}(\mathcal{O}) = \text{disc}(\alpha_1, \ldots, \alpha_n)$ is a nonzero multiple of $\text{disc}(\mathcal{O}_K)$, and so the $\alpha_i$ are linearly independent over $\mathbb{Q}$. Since $K$ is an $n$-dimensional vector space over $\mathbb{Q}$, $\alpha_1, \ldots, \alpha_n$ must form a basis for $K$. Then $\mathcal{O}$ is an order in $K$. □

**Corollary 2.3.16.** *Let $K$ be a number field. The the unique maximal order of $K$ is $\mathcal{O}_K$.*

*Proof.* The theorem shows that $\mathcal{O}_K$ is an order of $K$, since it is a free $\mathbb{Z}$-submodule of itself and is of rank $n$. The theorem also shows that every order of $K$ is contained in $\mathcal{O}_K$. Then $\mathcal{O}_K$ is a maximal order, and no other order can be maximal, as it is contained in $\mathcal{O}_K$. □

This equivalent characterization of an order is often used as the definition of an order in a number field, particularly in algebraic number theory, where this is the only context of any interest. We can also determine more about the structure of a general order in a number ring.

**Lemma 2.3.17.** *Let $K$ be a number field and $\mathcal{O}$ an order of $K$. Then for any $\alpha \in K$, there is some $c \in \mathbb{N}$ such that $c\alpha \in \mathcal{O}$.*

*Proof.* For any $\alpha \in K$, recall that there is some $a \in \mathbb{N}$ such that $a\alpha \in \mathcal{O}_K$. Now since the additive group of $\mathcal{O}$ is a rank $n$ free abelian subgroup of $\mathcal{O}_K$, note that $\mathcal{O}_K/\mathcal{O}$ is finite, so every element has finite order. Then there is some $b \in \mathbb{N}$ such that $ab\alpha \in \mathcal{O}$. Then $c = ab \in \mathbb{N}$ is such that $c\alpha \in \mathcal{O}$. □

**Lemma 2.3.18.** *Let $K$ be a number field, $\mathcal{O}$ an order of $K$, and $I$ a nonzero ideal of $\mathcal{O}$. Then the additive group of $I$ is a free abelian group of rank $n$.*

*Proof.* Let $\alpha \in I$ be nonzero. Then $\alpha^{-1} \in K$, so there is some $c \in \mathbb{N}$ such that $c\alpha^{-1} \in \mathcal{O}$. Then $c = c\alpha^{-1}\alpha \in I$. Then $c\mathcal{O} \subseteq I \subseteq \mathcal{O}$, with both $c\mathcal{O}$ and $\mathcal{O}$ being (additively) rank $n$ free abelian groups. Then $I$ is also (additively) a free abelian group of rank $n$. □

**Theorem 2.3.19.** *Let $K$ be a number field and $\mathcal{O}$ an order of $K$. Then $\mathcal{O}$ is a Noetherian domain with* $\dim(\mathcal{O}) = 1$.

*Proof.* This proof will mirror the corresponding parts of the proof that $\mathcal{O}_K$ is Dedekind. By the second lemma above, any nonzero ideal $I$ of $\mathcal{O}$ is (additively) a free abelian group of rank $n$, so $I$ is generated as an ideal of $\mathcal{O}$ by at most $n$ elements, i.e. $I$ is finitely generated. Then $\mathcal{O}$ is Noetherian.

Now let $P$ be a nonzero prime ideal of $\mathcal{O}$. Since the additive group of $P$ is a free abelian subgroup of $\mathcal{O}$ of rank $n$, $\mathcal{O}/P$ is finite; since $P$ is prime, $\mathcal{O}/P$ is an integral domain. Then we know that $\mathcal{O}/P$ is a field, and thus $P$ is maximal. Then every nonzero prime ideal is maximal, so $\dim(\mathcal{O}) = 1$. □

In the context of number rings, we are also interested in the largest ideal contained in both the number ring and the order:

**Definition 2.3.20.** *Let $K$ be a number ring and $\mathcal{O}$ an order of $K$. The* **conductor ideal** *$I$ of $\mathcal{O}$ is the largest ideal of $\mathcal{O}_K$ which is contained in $\mathcal{O}$. Explicitly, $I = \{\alpha \in \mathcal{O} : \alpha\mathcal{O}_K \subseteq \mathcal{O}\}$.*

It should be plain to see that the conductor ideal is an ideal of both $\mathcal{O}_K$ and $\mathcal{O}$, and any ring $J$ which is an ideal of both $\mathcal{O}$ and $\mathcal{O}_K$ must be a subset of the conductor ideal $I$.

**Example 2.3.21.** *Let $K = \mathbb{Q}[\sqrt{d}]$, a quadratic number field, for some squarefree $d \in \mathbb{Z}$. If $d \equiv 1 \pmod 4$, then the orders of $K$ are exactly the rings $\mathbb{Z}\left[n\frac{1+\sqrt{d}}{2}\right]$ for $n \in \mathbb{N}$. If $d \equiv 2, 3 \pmod 4$, then the orders of $K$ are exactly the rings $\mathbb{Z}[n\sqrt{d}]$ for $n \in \mathbb{N}$. In either case, the conductor ideal $I$ of $\mathcal{O}$ is $I = n\mathcal{O}_K$.*

*Proof.* First, note that every ring described here are orders of $K$ by the characterization in Theorem 2.3.15. To show that every order is of this form, let $\alpha = \sqrt{d}$ if $d \equiv 2, 3 \pmod 4$ and $\alpha = \frac{1+\sqrt{d}}{2}$ if $d \equiv 1 \pmod 4$ so that $\mathcal{O}_K = \mathbb{Z}[\alpha]$.

If $\mathcal{O}$ is an order in $K$, then $1 \in \mathcal{O} \implies \mathbb{Z} \subseteq \mathcal{O}$. Now let $n \in \mathbb{N}$ be minimal such that there is some $a \in \mathbb{Z}$ for which $a + n\alpha \in \mathcal{O}$. Then $n\alpha \in \mathcal{O}$, so $\mathbb{Z}[n\alpha] \subseteq \mathcal{O}$. Furthermore, if there is any $a + b\alpha \in \mathcal{O}$ for which $n \nmid b$, $\gcd(n, b) < n$ is a natural number for which $\gcd(n, b)\alpha \in \mathcal{O}$, contradicting minimality of $n$. Then $\mathcal{O} = \mathbb{Z}[n\alpha]$.

Now note that $n\mathcal{O}_K \subseteq \mathcal{O}$, so $n\mathcal{O}_K \subseteq I$. Furthermore, if $a + b\alpha \in I \backslash n\mathcal{O}_K$, then either $n \nmid a$ or $n \nmid b$. In the second case, we immediately get a contradiction, since then $a + b\alpha \notin \mathcal{O}$. Then assume that $n \nmid a$ and $n|b$. In this case, we can add a multiple of $n$ to get $a \in I$, then multiply by $\alpha$ to get $a\alpha \in I$, also a contradiction. Then $I = n\mathcal{O}_K$. □

We will use these characterizations of orders later, particularly the form of an order and its conductor ideal in a quadratic field.

**Theorem 2.3.22.** *Let $K$ be a number field and $\mathcal{O}$ an order of $K$. Then the field of fractions of $\mathcal{O}$ is $K$ and the integral closure of $\mathcal{O}$ in $K$ is $\overline{\mathcal{O}} = \mathcal{O}_K$.*

*Proof.* First, note that $\mathcal{O} \subseteq \mathcal{O}_K$, so the field of fractions of $\mathcal{O}$ is a subfield of $K$, the field of fractions of $\mathcal{O}_K$. Furthermore, $\mathcal{O}$ contains both $\mathbb{Z}$ and a $\mathbb{Q}$-basis $\alpha_1, \ldots, \alpha_n$ for $K$. Then the field of fractions of $\mathcal{O}$ contains $\alpha_1\mathbb{Q} + \cdots + \alpha_n\mathbb{Q} = K$. Then the field of fractions of $\mathcal{O}$ is exactly $K$.

Now note that $\mathbb{Z} \subseteq \mathcal{O} \subseteq \mathcal{O}_K$. Then $\mathcal{O}_K = \overline{\mathbb{Z}}_K \subseteq \overline{\mathcal{O}} \subseteq \overline{\mathcal{O}_K} = \mathcal{O}_K$. Then $\overline{\mathcal{O}} = \mathcal{O}_K$. □

## 2.4 Ideal Class Group in a Number Ring

The final object which we must discuss before getting to the major results of this paper is the ideal class group of a number ring. As we have seen, this group can be thought of as classes of the nonzero integral ideals of the number ring rather than invertible ideals, since every class contains an integral ideal and every nonzero fractional ideal is invertible. We will now consider more facets of this group, as well as an important property of the ideal class group of an order in a number ring. In the interest of brevity, the proofs in this section will be referenced, though not shown here.

**Theorem 2.4.1.** *Let $R$ be a number ring. Then $Cl(R)$ is a finite group. $\left|Cl(R)\right|$ is called the* **class number** *of $R$ (or of $K$), often denoted $h$.*

*Proof.* See [9], Corollary 2 to Theorem 35. □

**Theorem 2.4.2.** *Let $R$ be a Dedekind domain and $I$ an ideal of $R$. Then every ideal class in $Cl(R)$ contains an ideal $J$ of $R$ which is relatively prime to $I$, i.e. for which $I + J = R$.*

*Proof.* See [11], Section I.12. □

As a particular case of this that will be important in a later proof, we have the following corollary.

**Corollary 2.4.3.** *Let $K$ be a number field, $\mathcal{O}$ an order of $K$, and $I$ the conductor ideal of $\mathcal{O}$. Then every ideal class in $Cl(\mathcal{O}_K)$ contains an ideal $J$ of $\mathcal{O}_K$ which is relatively prime to $I$.*

As we have seen, the class number of a Dedekind domain can give us an idea of the factorization of elements. In particular, we know that the ideal class group of $R$ is trivial iff $R$ is a UFD. In a number ring, we get an improved result which tells us how to interpret an ideal class group of order 2.

**Theorem 2.4.4.** *Let $R$ be a number ring. Then $R$ is an HFD if and only if $\left|Cl(R)\right| \leq 2$.*

*Proof.* See [1]. □

Now recall that the ideal class group is defined for a general integral domain, though nicer properties hold in Dedekind domains. As we will explore in the next chapter, we are also interested in the ideal class group of an order in a number ring. We know that such orders are Noetherian domains of Krull dimension 1, though they are not integrally closed in general. Then although we may not have unique factorization of prime ideals or every ideal being invertible, we do have the following property which will help us determine which ideals of an order are invertible.

**Theorem 2.4.5.** *Let $K$ be a number field, $R$ an order of $K$, and $I$ its conductor ideal. Then an ideal $J$ of $R$ is invertible if and only if $J$ is relatively prime to $I$, i.e. $J + I = R$.*

*Proof.* See [11], Section I.12. □

# Chapter 3

# The Generalized Class Number of an Order in a Number Field

In this chapter, we will produce a way to find the generalized class number (order of the ideal class group) of an order $R$ in a number field $K$ with number ring $\mathcal{O}_K = \overline{R}$. The notation of $\overline{R}$ will be primarily used here to reference the fact that $\overline{R}$ is the integral closure of $R$. To do so, we will need to consider a short exact sequence, then exploit the First Isomorphism Theorem to yield the desired result. Then, we will consider the particular case when $K$ is a quadratic number field.

## 3.1 An Exact Sequence

Versions of the exact sequence we will discuss appear in several places in the literature. In particular, we will draw from [11], Proposition 12.9, though for our purposes we will use a slightly altered (though equivalent) version of the exact sequence.

It should be noted that in this source and others which have some version of this sequence, the Picard group of the order $R$ is considered in place of the ideal class group. The Picard group is, in general, different than the ideal class group; in the case of orders in a number ring, however, the two groups will coincide. Thus, we will opt to continue using the class group notation as we have throughout this thesis.

**Theorem 3.1.1.** *Let $R$ be an order in a number field $K$ and $\overline{R} = \mathcal{O}_K$ the integral closure of $R$ in*

*$K$. Let $I$ denote the conductor ideal of $R$. Then we have an exact sequence*

$$1 \to U(R) \to U(\overline{R}) \oplus U(R/I) \to U(\overline{R}/I) \to Cl(R) \to Cl(\overline{R}) \to 1$$

*Proof.* First, we define mappings as follows:

$$\begin{aligned}
&\phi : U(R) \to U(\overline{R}) \oplus U(R/I), && \phi(r) = (r^{-1}, r+I);\\
&\psi : U(\overline{R}) \oplus U(R/I) \to U(\overline{R}/I), && \psi(x, y+I) = xy + I;\\
&\sigma : U(\overline{R}/I) \to Cl(R), && \sigma(s+I) = [s\overline{R} \cap R];\\
&\tau : Cl(R) \to Cl(\overline{R}), && \tau([J]) = [J\overline{R}].
\end{aligned}$$

We need to show that each of these maps is a well-defined homomorphism and that they form an exact sequence.

First, note that if $r \in U(R)$, then $r \in U(\overline{R})$ (and $r^{-1} \in U(\overline{R})$), since $r^{-1} \in R \subseteq \overline{R}$. Moreover, $r \in U(R) \implies r + I \in U(R/I)$, with $(r+I)^{-1} = r^{-1} + I$. Then $\phi$ is a well-defined mapping. Furthermore, note that

$$\phi(rs) = ((rs)^{-1}, rs + I) = (r^{-1}, r+I)(s^{-1}, s+I) = \phi(r)\phi(s).$$

Then in fact, $\phi$ is a homomorphism.

Now for $x \in U(\overline{R})$ and $y + I \in U(R/I)$, note that $xy + I \in U(\overline{R}/I)$, with $(xy+I)^{-1} = (x^{-1}+I)(y+I)^{-1}$ (since $y+I$ is a unit in $R/I$, it is also a unit in $\overline{R}/I$). Moreover, if $y + I = z + I$ for $y, z \in R$, then $y - z \in I$. Then for $x \in U(\overline{R})$, $xy - xz = x(y-z) \in I$, i.e. $xy + I = xz + I$. Then $\psi$ is a well-defined mapping. Now note that

$$\psi(xa, yb + I) = xayb + I = (xy+I)(ab+I) = \psi(x, y+I)\psi(a, b+I).$$

Then $\psi$ is also a homomorphism.

For $s + I \in U(\overline{R}/I)$, note that $s\overline{R} \cap R$ is an ideal in $R$. Furthermore, letting $r \in \overline{R}$ be such that $r + I = (s+I)^{-1}$, there is some $\alpha \in I$ such that $sr + \alpha = 1$. Then since $sr = 1 - \alpha \in R$, $1 = sr + \alpha \in s\overline{R} \cap R + I$, meaning that $s\overline{R} \cap R + I = R$. Then $s\overline{R} \cap R$ is an ideal of $R$ which is relatively prime to the conductor $I$, so $s\overline{R} \cap R$ is an invertible ideal of $R$. Now if $s_1 + I = s_2 + I \in U(\overline{R}/I)$,

note that $s_1 - s_2 \in I$ and so $(s_1 - s_2)\overline{R} \subseteq I \subseteq R$. Then for any $\alpha \in \overline{R}$ such that $s_2\alpha \in R$, $s_1\alpha = s_2\alpha + (s_1 - s_2)\alpha \in R$. By symmetry of $s_1$ and $s_2$, this gives that $s_1\alpha \in R$ if and only if $s_2\alpha \in R$; then $s_1\overline{R} \cap R = \frac{s_1}{s_2}(s_2\overline{R} \cap R)$. Then $[s_1\overline{R} \cap R] = [s_2\overline{R} \cap R]$, so $\sigma$ is a well-defined map. Now to see that $\sigma$ is a homomorphism, note that for $s_1 + I, s_2 + I \in U(\overline{R}/I)$, $(s_1\overline{R} \cap R)(s_2\overline{R} \cap R) \subseteq s_1s_2\overline{R} \cap R$ trivially. For the reverse inclusion, let $\alpha \in \overline{R}$ be such that $s_1s_2\alpha \in R$, i.e. $s_1s_2\alpha$ is a generic element in $s_1s_2\overline{R} \cap R$. By definition of $s_1$ and $s_2$, there exist $r_1, r_2 \in \overline{R}$ and $\beta_1, \beta_2 \in I$ such that $s_1r_1 + \beta_1 = s_2r_2 + \beta_2 = 1$. Then:

$$\begin{aligned} s_1s_2\alpha &= s_1s_2\alpha(s_1r_1 + \beta_1)(s_2r_2 + \beta_2) \\ &= (s_1r_1)(s_2r_2s_1s_2\alpha) + (s_1r_1)(s_1s_2\alpha\beta_2) + (s_2r_2)(s_1s_2\alpha\beta_1) + (s_1\beta_1)(s_2\alpha\beta_2). \end{aligned}$$

Then note that $s_1r_1 \in s_1\overline{R} \cap R$, $s_2r_2 \in s_2\overline{R} \cap R$, and $s_1s_2\alpha \in R$; moreover, $I \subseteq R$ absorbs all multiplication from $\overline{R}$. Then each addend in the above expression is a product of an element of $s_1\overline{R} \cap R$ and an element of $s_2\overline{R} \cap R$. Then $s_1s_2\alpha \in (s_1\overline{R} \cap R)(s_2\overline{R} \cap R)$, so $s_1s_2\overline{R} \cap R = (s_1\overline{R} \cap R)(s_2\overline{R} \cap R)$. Thus, $\sigma$ is a homomorphism.

Finally, for $[J] \in Cl(R)$, $J$ an invertible ideal of $R$, note that $J\overline{R}$ is a fractional ideal of $\overline{R}$, so $\tau([J]) \in Cl(\overline{R})$. Furthermore, if $[J_1] = [J_2]$, then $J_1 = \alpha J_2$ for some $\alpha \in K$. Then $J_1\overline{R} = \alpha J_2\overline{R}$, so $[J_1\overline{R}] = [J_2\overline{R}]$. Thus, $\tau$ is well-defined. Now let $[J_1], [J_2] \in Cl(R)$. Then

$$\tau([J_1J_2]) = [J_1J_2\overline{R}] = [J_1\overline{R}][J_2\overline{R}] = \tau([J_1])\tau([J_2]).$$

Then $\tau$ is a homomorphism.

We have now shown that the four maps comprising the desired sequence are indeed homomorphisms; now we need to show exactness at each group. That is, we need to show the following:

1. $\phi$ is injective;
2. $\phi(U(R)) = \ker(\psi)$;
3. $\psi(U(\overline{R}) \oplus U(R/I)) = \ker(\sigma)$;
4. $\sigma(U(\overline{R}/I)) = \ker(\tau)$;
5. $\tau$ is surjective.

First, let $r \in \ker(\phi)$. Then $\phi(r) = (r^{-1}, r+I) = (1, 1+I)$, so $r^{-1} = 1 \implies r = 1$. Thus, $\ker(\phi) = \{1\}$ and so $\phi$ is injective.

Now let $(r^{-1}, r+I) = \phi(r) \in \phi(U(R))$. Then $\psi(r^{-1}, r+I) = r^{-1}r + I = 1 + I$, so $\phi(U(R)) \subseteq \ker(\psi)$. Furthermore, if $(x, y+I) \in \ker(\psi)$, i.e. $xy + I = 1 + I$, then note that $x + I = (y+I)^{-1} \in U(R/I)$. Therefore, $x \in R$ and $\phi(x^{-1}) = (x, x^{-1} + I) = (x, y+I)$. Then $\phi(U(R)) = \ker(\psi)$.

Now let $xy + I \in \psi(U(\overline{R}) \oplus U(R/I))$, i.e. $x \in U(\overline{R})$ and $y + I \in U(R/I)$. Then $\sigma(xy+I) = xy\overline{R} \cap R = y\overline{R} \cap R$. Now suppose $y\alpha \in R$ for some $\alpha \in \overline{R}$. By definition of $y$, there exists some $z \in R$, $\beta \in I$ such that $yz = 1 + \beta$. Then $\alpha = (1+\beta)\alpha - \alpha\beta = z(y\alpha) - \alpha\beta \in R$. Then since $yR \subseteq R$ trivially, we have that $y\overline{R} \cap R = yR$, a principal ideal in $R$; then $\psi(U(\overline{R}) \oplus U(R/I)) \subseteq \ker(\sigma)$. For the reverse inclusion, let $s + I \in \ker(\sigma)$, i.e. $s + I \in U(\overline{R}/I)$ and $s\overline{R} \cap R = yR$ for some $y \in R$. First, note that since $s + I \in U(\overline{R}/I)$, there exists some $r \in \overline{R}$ and $\beta \in I$ such that $sr = 1 + \beta \in R$. Then $1 + \beta \in s\overline{R} \cap R = yR$, so $1 + \beta = yz$ for some $z \in R$. Thus, $y + I \in U(R/I)$. We now want to show that $s = xy$ for some $x \in U(\overline{R})$, i.e. $s\overline{R} = y\overline{R}$. To do so, note that $y\overline{R} = (s\overline{R} \cap R)\overline{R} \subseteq s\overline{R}$. Furthermore, since $y + I \in U(R/I)$, $1 \in yR + I \implies yR + I = R$. Then:

$$s\overline{R} = s\overline{R}(yR + I) = s\overline{R}(s\overline{R} \cap R) + sI \subseteq (s\overline{R} \cap R)\overline{R} = y\overline{R}.$$

Then $s = xy$ for some $x \in U(\overline{R})$ and $y + I \in U(R/I)$. Then $\psi(x, y+I) = xy + I = s + I$, so $s + I \in \psi(U(\overline{R}) \oplus U(R/I))$. Therefore, $\psi(U(\overline{R}) \oplus U(R/I)) = \ker(\sigma)$.

Now let $[J] \in \sigma(U(\overline{R}/I))$, i.e. $J = s\overline{R} \cap R$ for some $s \in \overline{R}$ such that $s + I \in U(\overline{R}/I)$. Then as shown previously, $J\overline{R} = (s\overline{R} \cap R)\overline{R} = s\overline{R}$, so $J\overline{R}$ is a principal ideal in $\overline{R}$. Then $\sigma(U(\overline{R}/I)) \subseteq \ker(\tau)$. For the reverse inclusion, let $[J] \in \ker(\tau)$, i.e. $J\overline{R} = s\overline{R}$ for some $s \in \overline{R}$. Without loss of generality, assume that $J \subseteq R$; then since $J$ is invertible, $J + I = R$. Then $s\overline{R} + I = J\overline{R} + I = \overline{R}$, so $s + I \in U(\overline{R}/I)$. Now note that quite trivially, $J \subseteq J\overline{R} \cap R$. To show that in fact $J = J\overline{R} \cap R$, note that $J\overline{R} \cap R = (J\overline{R} \cap R)R$. Now let $j \in J$ and $r_1 \in \overline{R}$ such that $jr_1 \in R$, i.e. $jr_1 \in J\overline{R} \cap R$, and $r_2 \in R$. Since $R = J + I$, there exist $\alpha_1, \alpha_2 \in J$ and $\beta_1, \beta_2 \in I$ such that $jr_1 = \alpha_1 + \beta_1$ and $r_2 = \alpha_2 + \beta_2$. Then

$$jr_1r_2 = jr_1(\alpha_2 + \beta_2) = (\alpha_1 + \beta_1)\alpha_2 + jr_1\beta_2 = \alpha_1\alpha_2 + \beta_1\alpha_2 + jr_1\beta_2 \in J^2 + JI = J(J+I) = JR = J.$$

Then since $(J\overline{R}\cap R)R$ is closed under addition, $J\overline{R}\cap R = (J\overline{R}\cap R)R \subseteq J$. Therefore, $J = J\overline{R}\cap R = s\overline{R}\cap R$. Then $[J] = \sigma(s+I) \in \sigma(U(\overline{R}/I))$. Therefore, $\sigma(U(\overline{R}/I)) = \ker(\tau)$.

Finally, we need to show that $\tau$ is surjective. Then let $[A] \in Cl(\overline{R})$. As we have previously seen, we can without loss of generality require that $A$ is an integral ideal of $\overline{R}$ which is relatively prime to the conductor ideal $I$, i.e. $A + I = \overline{R}$. Then there exist $\alpha \in A$ and $\beta \in I$ such that $\alpha+\beta = 1$. Since $I \subseteq R$, note that $\alpha = 1-\beta \in R$. Then $\alpha \in A\cap R$, so $A\cap R + I = R$; that is, $A\cap R$ is an invertible ideal of $R$. Note that $(A\cap R)\overline{R} \subset A$ trivially. For the reverse inclusion, we have that

$$A = AR = A(A\cap R + I) = A(A\cap R) + AI \subseteq (A\cap R)\overline{R}.$$

Then $A = (A\cap R)\overline{R}$, meaning that $[A] = \tau([A\cap R])$. Then $\tau$ is surjective.

□

## 3.2 Class Number of an Order

We will now use the exact sequence proven above to derive a relationship between the generalized class number of an order $R$ of a number field $K$ and the class number of the number ring $\mathcal{O}_K = \overline{R}$. The result here can also be found in [11], Theorem 12.12, though the specifics of the proof are spelled out here in more detail.

**Theorem 3.2.1.** *Let $R$ be an order in a number field $K$ and $\overline{R} = \mathcal{O}_K$, the integral closure of $R$ in $K$. Let $I$ denote the conductor ideal of $R$. Then the class numbers $\left|Cl(R)\right|$ and $\left|Cl(\overline{R})\right|$ are related as follows:*

$$\left|Cl(R)\right| = \left|Cl(\overline{R})\right| \frac{\left|U(\overline{R}/I)\right|}{\left|U(R/I)\right|\left|U(\overline{R})/U(R)\right|}$$

*Proof.* We will use the exact sequence from Theorem 3.1.1 along with repeated use of the First Isomorphism Theorem to construct this equality. This provides the following three isomorphisms:

$$Cl(\overline{R}) \cong Cl(R)/\ker(\tau) = Cl(R)/\sigma(U(\overline{R}/I));$$

$$\sigma(U(\overline{R}/I)) \cong U(\overline{R}/I)/\ker(\sigma) = U(\overline{R}/I)/\psi(U(\overline{R})\oplus U(R/I));$$

$$\psi(U(\overline{R})\oplus U(R/I)) \cong (U(\overline{R})\oplus U(R/I))/\ker(\psi) = (U(\overline{R})\oplus U(R/I))/\phi(U(R)).$$

Recall that $\overline{R}/I$ and $R/I$ are finite quotient rings; then $U(\overline{R}/I)$ and $U(R/I)$ must be finite groups. Then by the first isomorphism and the fact that $Cl(\overline{R})$ is known to be finite, we can immediately conclude that $Cl(R)$ must also be finite. Now note that the first isomorphism gives a cardinality relation between $Cl(\overline{R})$ and $Cl(R)$ based on the second ismorphism, which is further based on the third isomorphism. Then we will first consider the third isomorphism above and work toward the first.

Consider $\Big|(U(\overline{R}) \oplus U(R/I))/\phi(U(R))\Big|$, the cardinality of the groups in the third isomorphism above. Elements in this group are of the form $(a, b+I)\phi(U(R))$, with $a \in U(\overline{R})$ and $b+I \in U(R/I)$. Let $A$ denote a set consisting of one coset representative from each coset in $U(\overline{R})/U(R)$; then $|A| = \Big|U(\overline{R})/U(R)\Big|$ and there is a unique $r \in U(R)$ such that $ar \in A$. Thus, we can represent $(a, b+I)\phi(U(R))$ as $(ar, br^{-1}+I)\phi(U(R))$, and this is the unique representation of this element with the property that the first coordinate is an element of $A$. Furthermore, note that $(ar, c+I)\phi(U(R)) = (ar, d+I)\phi(U(R)) \iff (1, (c+I)(d+I)^{-1}) \in \phi(U(R)) \iff (c+I)(d+I)^{-1} = 1+I \iff c+I = d+I$. Then placing each element $(a, b+I)\phi(U(R))$ into the representation $(ar, br^{-1}+I)\phi(U(R))$, we can see that there are $\Big|U(R/I)\Big|$ choices of $b$ which will produce distinct elements given a particular $ar$. Furthermore, there are $|A| = \Big|U(\overline{R})/U(R)\Big|$ choices for $ar$. Then $\Big|(U(\overline{R}) \oplus U(R/I))/\phi(U(R))\Big| = \Big|U(R/I)\Big|\Big|U(\overline{R})/U(R)\Big|$.

Now using the second isomorphism above and the fact that $U(\overline{R}/I)$ is finite, we have that

$$\Big|\sigma(U(\overline{R}/I))\Big| = \frac{\Big|U(\overline{R}/I)\Big|}{\Big|U(R/I)\Big|\Big|U(\overline{R})/U(R)\Big|}.$$

Notably, this means that $\Big|U(\overline{R}/U(R))\Big|$ must be finite. Finally, we can combine this with the first isomorphism and rearrange to produce the desired equality:

$$\Big|Cl(R)\Big| = \Big|Cl(\overline{R})\Big|\frac{\Big|U(\overline{R}/I)\Big|}{\Big|U(R/I)\Big|\Big|U(\overline{R})/U(R)\Big|}$$

□

Because these results were shown as part of the above proof but are important in and of themselves, we will state them separately here:

**Corollary 3.2.2.** *Let $R$ and $\overline{R}$ be as above. Then $Cl(R)$ and $U(\overline{R})/U(R)$ are both finite groups.*

**Corollary 3.2.3.** *Let $R$ be an order in a number field. Then $U(R) = W \times V$, where $W$ is the finite cyclic group consisting of the roots of unity in $R$ and $V$ is a free abelian group of rank $r_1 + r_2 - 1$, with $r_1, r_2$ as in Dirichlet's Unit Theorem (see Theorem 2.3.13).*

*Proof.* This follows immediately from finiteness of $U(\overline{R})/U(R)$, Dirichlet's Unit Theorem, and Lemma 2.1.4. □

This result allows us to compare the orders of $Cl(R)$ with $Cl(\overline{R})$, provided that we can find the ideal $I$ and determine the relevant unit groups. Thus, a great deal of understanding about the relationship between the class group of a number ring and an order of the number field can be developed by studying units. For example, we have the following corollary.

**Corollary 3.2.4.** *Let $R$ be an order in a number field $K$, $\overline{R}$ its integral closure, and $I$ the conductor ideal, as before. Then the following are equivalent:*

*(1)* $Cl(\overline{R}) \cong Cl(R)$.

*(2)* $\left|Cl(\overline{R})\right| = \left|Cl(R)\right|$.

*(3)* $\left|U(\overline{R})/U(R)\right| = \frac{\left|U(\overline{R}/I)\right|}{\left|U(R/I)\right|}$.

*(4)* $U(\overline{R})/U(R) \cong U(\overline{R}/I)/U(R/I)$.

*(5) Every coset in $U(\overline{R}/I)/U(R/I)$ contains a unit in $\overline{R}$; that is, every coset can be written as $(r + I)U(R/I)$, with $r \in U(\overline{R})$.*

*Proof.* First, note that (1) $\implies$ (2) trivially. Furthermore, since we know by the theorem that there is a surjective homomorphism from $Cl(R)$ onto $Cl(\overline{R})$, both finite groups, (2) $\implies$ (1). Then (1) $\iff$ (2). From the result in the theorem and rearranging terms, we also get (2) $\iff$ (3) trivially.

Clearly (4) $\implies$ (3). Now define a homomorphism $\phi : U(\overline{R}) \to U(\overline{R}/I)/U(R/I)$ by $\phi(r) = (r + I)U(R/I)$. Note that $r \in U(R) \implies r + I \in U(R/I)$, so $U(R) \subseteq \ker(\phi)$. Furthermore, if $r \in U(\overline{R})$ such that $r + I \in U(R/I)$, then $r \in R \cap U(\overline{R}) = U(R)$. Thus, $U(R) = \ker(\phi)$. Then by the first isomorphism theorem, $U(\overline{R})/U(R) \cong \phi(U(\overline{R})) \leq U(\overline{R}/I)/U(R/I)$. Then if the orders of these finite groups are equal, as in (3), they are isomorphic. Then (3) $\iff$ (4).

Now note that, using $\phi$ as above, $\phi(U(\overline{R}))$ is exactly the subgroup of $U(\overline{R}/I)/U(R/I)$ containing units in $U(\overline{R})$. Since $\phi(U(\overline{R}))$ is a subgroup of $U(\overline{R}/I)/U(R/I)$, they are isomorphic

if and only if they are equal. In this case, the isomorphism is equivalent to condition (4) and the equality is equivalent to condition (5). Thus, (4) $\iff$ (5).

□

Now as a particular case of the theorem, we will consider the specifics when $K$ is a quadratic number field, as in [3] Theorem 8.1.4.

**Corollary 3.2.5.** *Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic number field, with $d$ a squarefree integer. Define $\Delta = \text{disc}(K)$, i.e. $\Delta = 4d$ if $d \equiv 2, 3 \pmod 4$ and $\Delta = d$ if $d \equiv 1 \pmod 4$. Let $R$ be an order in $K$ of index $n$, i.e. $R = \mathbb{Z}[n\sqrt{d}]$ if $d \equiv 2, 3 \pmod 4$ or $R = \mathbb{Z}[n\frac{1+\sqrt{d}}{2}]$ if $d \equiv 1 \pmod 4$, and $\overline{R} = \mathcal{O}_K$. Then the class numbers $\left|Cl(R)\right|$ and $\left|Cl(\overline{R})\right|$ are related as follows:*

$$\left|Cl(R)\right| = \frac{n\left|Cl(\overline{R})\right|}{u} \prod_{p|n} \left(1 - \frac{\left(\frac{\Delta}{p}\right)}{p}\right).$$

*Here, $\left(\frac{\Delta}{p}\right)$ is Kronecker's generalization of the Legendre symbol, $u$ is the smallest power of the generator of $U(\overline{R})$ lying in $R$, and the product is taken over all primes $p$ which divide $n$.*

*Proof.* This is a particular case of the result in Theorem 3.2.1 above; then we must determine the sizes of the necessary unit groups. For ease of notation, denote $\alpha = \sqrt{d}$ when $d \equiv 2, 3 \pmod 4$ and $\alpha = \frac{1+\sqrt{d}}{2}$ when $d \equiv 1 \pmod 4$ so that $\overline{R} = \mathbb{Z}[\alpha]$ and $R = \mathbb{Z}[n\alpha]$. As shown in Example 2.3.21, $I = n\overline{R}$.

Note that by applying Dirichlet's Unit Theorem to this quadratic case, $u = \left|U(\overline{R})/U(R)\right|$ trivially; in the real quadratic case, $u$ is an exponent applied to the fundamental unit, while in the imaginary quadratic case, $u$ is an exponent applied to a generator of the finite unit group. Then we need only consider the unit groups $U(\overline{R}/I)$ and $U(R/I)$. First, we have that $\overline{R}/I = \mathbb{Z}[\alpha]/(n) \cong \{a + b\alpha : a, b \in \mathbb{Z}_n\}$ and $R/I \cong \mathbb{Z}_n$. Then $\left|U(R/I)\right| = \left|U(\mathbb{Z}_n)\right| = \phi(n)$. All that remains to find is $\left|U(\overline{R}/I)\right|$; for the desired identity to hold, we need

$$\left|U(\overline{R}/I)\right| = n\phi(n) \prod_{p|n} \left(1 - \frac{\left(\frac{\Delta}{p}\right)}{p}\right).$$

First, let $\beta \in \overline{R}$ and $\overline{\beta}$ be its conjugate (so $\beta\overline{\beta} = N(\beta)$). Since $\overline{R}/I$ is a finite ring, $\beta$ is a unit if and only if it is not a zero divisor. Now let $p$ be a prime factor of $n$. If $p|\beta$, then $\frac{n}{p}\beta \in I$,

meaning that $\beta + I$ is a zero divisor in $\overline{R}/I$, i.e. $\beta + I$ is a nonunit in $\overline{R}/I$. If $p \nmid \beta$ (so $p \nmid \overline{\beta}$) but $p|N(\beta)$, then $\beta(\frac{n}{p}\overline{\beta}) \in I$. However, since $p \nmid \overline{\beta}$, $\frac{n}{p}\overline{\beta} \notin n\overline{R} = I$, so $\beta$ is again a zero divisor. Then if $N(\beta)$ is a nonunit in $Z_n$, i.e. if $N(\beta)$ shares a common factor with $n$, then $\beta + I$ is a nonunit in $\overline{R}/I$. Conversely, if $N(\beta)$ is a unit in $Z_n$ with inverse $a \in \mathbb{Z}_n$, then $a\beta\overline{\beta} \equiv 1 \pmod{I}$, i.e. $\beta + I$ is a unit in $\overline{R}/I$. Therefore, $\beta + I \in U(\overline{R}/I) \iff N(\beta) \in U(\mathbb{Z}_n)$.

Now that we can simplify the argument to considering norms, it will help to note that when $d \equiv 2, 3 \pmod 4$, $N(a + b\alpha) = a^2 - b^2 d$; when $d \equiv 1 \pmod 4$, $N(a + b\alpha) = a^2 + ab + b^2\frac{1-d}{4} = \frac{(2a+b)^2 - b^2 d}{4}$. We will now show the result for $n = p^r$, where $p$ is a prime and $r \in \mathbb{N}$. To do so, we will need to consider several cases. For these arguments, note that $\left|\overline{R}/I\right| = n^2$.

Case 1: Let $p$ be an odd prime, $d \equiv 2, 3 \pmod 4$, and $\left(\frac{\Delta}{p}\right) = \left(\frac{4d}{p}\right) = 1$. Since 4 is a square and $p$ is odd, $\left(\frac{d}{p}\right) = 1$ as well, i.e. $d \equiv m^2 \pmod p$ for some nonzero $m \in \mathbb{Z}_p$. Then $a + b\alpha$ is a unit $\iff p \nmid N(a + b\alpha) = a^2 - b^2 d \iff a^2 \not\equiv b^2 d \equiv (bm)^2 \pmod p$. Of the $n$ choices for $b$, $p^{r-1}$ of them have $b \equiv 0 \pmod p$; for each such $b$, there are $p^{r-1}$ choices of $a$ for which $a^2 \equiv b^2 d \equiv 0 \pmod p$. Meanwhile, there are $\phi(n) = p^{r-1}(p-1)$ choices for $b$ for which $b \not\equiv 0 \pmod p \implies (bm)^2 \not\equiv 0 \pmod p$; for each such $b$, there are $2p^{r-1}$ choices of $a$ for which $a^2 \equiv (bm)^2 \pmod p$. Then

$$\left|U(\overline{R}/I)\right| = n^2 - p^{2(r-1)} - 2p^{2(r-1)}(p-1) = p^{2(r-1)}(p-1)^2 = n\phi(n)\left(1 - \frac{\left(\frac{\Delta}{p}\right)}{p}\right)$$

.

Case 2: Let $p$ be an odd prime, $d \equiv 2, 3 \pmod 4$, and $\left(\frac{\Delta}{p}\right) = -1$. As in the previous case, $\left(\frac{d}{p}\right) = -1$ as well. Then as before we have $p^{2(r-1)}$ nonunits when $b \equiv 0 \pmod p$. However, since $b^2 d$ is a nonsquare modulo $p$ when $b \not\equiv 0 \pmod p$, there are no nonunits when $b \not\equiv 0 \pmod p$. Then

$$\left|U(\overline{R}/I)\right| = n^2 - p^{2(r-1)} = p^{2(r-1)}(p^2-1) = n\phi(n)\left(1 - \frac{\left(\frac{\Delta}{p}\right)}{p}\right).$$

Case 3: Let $p$ be an odd prime, $d \equiv 2, 3 \pmod 4$, and $\left(\frac{\Delta}{p}\right) = 0$, i.e. $p|4d \implies p|d$. Then $N(a + b\alpha) = a^2 - b^2 d \equiv a^2 \pmod p$, so $a + b\alpha$ is a unit if and only if $p \nmid a$. Then there are $n$ valid

choices for $b$ and $\phi(n)$ choices for $a$, so

$$\left|U(\overline{R}/I)\right| = n\phi(n) = n\phi(n)\left(1 - \frac{\left(\frac{\Delta}{p}\right)}{p}\right).$$

Case 4: Let $p$ be an odd prime, $d \equiv 1 \pmod 4$, and $\left(\frac{\Delta}{p}\right) = \left(\frac{d}{p}\right) = 1$, i.e. $d \equiv m^2 \pmod p$ for some nonzero $m \in \mathbb{Z}_p$. Then $a + b\alpha$ is a unit $\iff p \nmid N(a+b\alpha) \iff p \nmid (2a+b)^2 - b^2 d \iff (2a+b)^2 \not\equiv (bm)^2$. Just as in Case 1, we get $p^{2(r-1)}$ nonunits with $b \equiv 0 \pmod p$ and $2p^{2(r-1)}(p-1)$ nonunits with $b \not\equiv 0 \pmod p$. Then the desired equality follows exactly as in Case 1.

Case 5: Let $p$ be an odd prime, $d \equiv 1 \pmod 4$, and $\left(\frac{\Delta}{p}\right) = \left(\frac{d}{p}\right) = -1$. Then as in the previous case, we have $p^{2(r-1)}$ nonunits with $b \equiv 0 \pmod p$. However, since $d$ is a nonsquare modulo $p$, $(2a+b)^2 \equiv b^2 d \pmod p$ has no solutions when $b \not\equiv 0 \pmod p$. Then the result follows exactly as in Case 2.

Case 6: Let $p$ be an odd prime, $d \equiv 1 \pmod 4$, and $\left(\frac{\Delta}{p}\right) = \left(\frac{d}{p}\right) = 0$, i.e. $p|d$. Then $a + b\alpha$ is a unit $\iff p \nmid N(a+b\alpha) \iff p \nmid (2a+b)^2 - b^2 d \iff p \nmid 2a + b \iff 2a \not\equiv -b \pmod p$. Then for each choice of $b$, there are $p^{r-1}$ choices of $a$ which produce nonunits in $\overline{R}/I$. Then

$$\left|U(\overline{R}/I)\right| = n^2 - np^{r-1} = p^{2r-1}(p-1) = n\phi(n) = n\phi(n)\left(1 - \frac{\left(\frac{\Delta}{p}\right)}{p}\right).$$

Case 7: Let $p = 2$, $d \equiv 2 \pmod 4$. Note that in this case, $\left(\frac{\Delta}{p}\right) = \left(\frac{4d}{2}\right) = 0$. Note that $a + b\alpha$ is a unit $\iff 2 \nmid N(a+b\alpha) = a^2 - b^2 d \iff 2 \nmid a$. Then $a + b\alpha$ is a unit iff $a$ is odd. Then there are $\phi(n)$ choices for $a$ and $n$ choices for $b$ which produce a unit in $\overline{R}/I$. Then

$$\left|U(\overline{R}/I)\right| = n\phi(n) = n\phi(n)\left(1 - \frac{\left(\frac{\Delta}{p}\right)}{p}\right).$$

Case 8: Let $p = 2$, $d \equiv 3 \pmod 4$. Note that in this case, $\left(\frac{\Delta}{p}\right) = \left(\frac{4d}{2}\right) = 0$. Note that $a + b\alpha$ is a unit $\iff 2 \nmid N(a+b\alpha) = a^2 - b^2 d \iff a^2 \not\equiv b^2 \pmod 2$. Then $a + b\alpha$ is a unit iff $a$ and $b$ are of opposite parity. Then there are $n$ choices for $a$, and for each choice, $\phi(n)$ choices for $b$

which produce a unit. Then

$$\left|U(\overline{R}/I)\right| = n\phi(n) = n\phi(n)\left(1 - \frac{\left(\frac{\Delta}{p}\right)}{p}\right).$$

Case 9: Let $p = 2$, $d \equiv 1 \pmod 8$. In this case, $\left(\frac{\Delta}{p}\right) = \left(\frac{d}{2}\right) = 1$. Then $a + b\alpha$ is a unit $\iff 2 \nmid N(a + b\alpha) = a^2 + ab + b^2\left(\frac{1-d}{4}\right) \iff 2 \nmid a^2 + ab \iff 2 \nmid a(a + b)$. Then if $a$ is even, any choice of $b$ produces a nonunit; if $a$ is odd, only odd choices of $b$ produce a nonunit. Then

$$\left|U(\overline{R}/I)\right| = n^2 - n\phi(n) - \phi(n)^2 = 2^{2(r-1)} = n\phi(n)\left(1 - \frac{\left(\frac{\Delta}{p}\right)}{p}\right).$$

Case 10: Let $p = 2$, $d \equiv 5 \pmod 8$. In this case, $\left(\frac{\Delta}{p}\right) = \left(\frac{d}{2}\right) = -1$. Then $a + b\alpha$ is a unit $\iff 2 \nmid N(a + b\alpha) = a^2 + ab + b^2\left(\frac{1-d}{4}\right) \iff 2 \nmid a^2 + ab + b^2$. Now note that $2|a^2 + ab + b^2$ if and only if $a$ and $b$ are both even. Then $\phi(n)^2$ choices of $a$ and $b$ produce a nonunit in $\overline{R}/I$, so

$$\left|U(\overline{R}/I)\right| = n^2 - \phi(n)^2 = 2^{2(r-1)} \cdot 3 = n\phi(n)\left(1 - \frac{\left(\frac{\Delta}{p}\right)}{p}\right).$$

We have now shown that the desired equality holds when $n$ is a prime power. Now if $n > 1$ is not a prime power, we can write $n = n_1 n_2$, with $n_1, n_2 > 1$ and $\gcd(n_1, n_2) = 1$. Note by the Chinese Remainder Theorem that $\overline{R}/I = \overline{R}/n\overline{R} \cong (\overline{R}/n_1\overline{R}) \oplus (\overline{R}/n_2\overline{R})$. Then $U(\overline{R}/I) \cong U((\overline{R}/n_1\overline{R}) \oplus (\overline{R}/n_2\overline{R})) \cong U(\overline{R}/n_1\overline{R}) \oplus U(\overline{R}/n_2\overline{R})$. Therefore, $\left|U(\overline{R}/I)\right| = \left|U(\overline{R}/n_1\overline{R})\right|\left|U(\overline{R}/n_2\overline{R})\right|$. Furthermore, since $\phi$ is multiplicative for relatively prime integers and $\gcd(n_1, n_2) = 1$, we have:

$$\left(n_1\phi(n_1)\prod_{p|n_1}\left(1 - \frac{\left(\frac{\Delta}{p}\right)}{p}\right)\right)\left(n_2\phi(n_2)\prod_{p|n_2}\left(1 - \frac{\left(\frac{\Delta}{p}\right)}{p}\right)\right) = \left(n\phi(n)\prod_{p|n}\left(1 - \frac{\left(\frac{\Delta}{p}\right)}{p}\right)\right).$$

Combining the two multiplicative results just shown, we can extend the result to any $n \in \mathbb{N}$. $\square$

# Chapter 4

# Power Series Rings of Half-Factorial Orders in a Number Field

This chapter will present results about orders in a number field $K$ which are half-factorial domains. Of particular interest in the major results of this chapter is the relationship between such an order $R$ and its ring of formal power series $R[[x]]$. We will again primarily use the notation $\overline{R}$ to refer to the integral closure of $R$ in $K$. As before, $\overline{R} = \mathcal{O}_K$, the ring of algebraic integers in $K$.

As one might expect, results for UFDs have been developed more thoroughly than those for HFDs. For example, in [12] it was shown that a general UFD does not necessarily have UFD power series. In particular, it was shown that this failure can occur if the UFD in question is of Krull dimension 2. However, it was also shown that if the UFD has Krull dimension 1, its ring of power series is also a UFD. Since any order in a number field has Krull dimension 1, it follows that any UFD order in a number field (which will necessarily be integrally closed) has a UFD power series ring. However, the corresponding result for HFDs is not known to hold. This leads us to the conjecture that will guide much of the discussion in this chapter and the next.

**Conjecture.** *Let $R$ be an order in a number field $K$. Then $R$ is an HFD if and only if $R[[x]]$ is an HFD.*

It was shown in [8] that a general HFD may have a power series ring which is not an HFD. In particular, they showed that if $R = \mathbb{R} + x\mathbb{C}[x]$, then $R$ and $S := R[[y]]$ are both HFDs; however, $S[[z]]$ is not. However, note that neither $R$ nor $S$ is an order in a number field; when the half-factorial domain in question is an order in a number field, it has yet to be shown that the relationship suggested by this conjecture either holds or fails in general.

## 4.1 The Integrally Closed Case

In order to approach a proof of the above conjecture, it will help to consider particular cases which are simpler to prove and may provide tools and techniques for tackling the broader result. The first such case comes when $R$ is integrally closed, i.e. when $R$ is a number ring. To prove this case, we require a few lemmas. The proofs of these results can be found in their respective source materials.

**Lemma 4.1.1. [10], Theorems 3.3, 12.4, 19.5** *Let $R$ be a ring. Then:*

1. *If $R$ is a Noetherian ring, so is $R[[x]]$.*
2. *If $R$ is a Krull domain, so is $R[[x]]$.*
3. *If $R$ is a regular ring, so is $R[[x]]$.*

**Lemma 4.1.2. [6], Proposition 11.27** *Let $R$ be a locally factorial ring. Then $Cl(R) \cong DivCl(R)$. In particular, this holds when $R$ is a regular ring.*

**Lemma 4.1.3. [2]** *Let $R$ be a regular Noetherian domain. Then the natural mapping $DivCl(R) \to DivCl(R[[x]])$ is a bijection.*

**Lemma 4.1.4. [5], Proposition 6.1.** *Let $R$ be an integral domain. Then $R$ is a Krull domain with $\left|DivCl(R)\right| = 1$ if and only if $R$ is a UFD.*

**Lemma 4.1.5. [13]** *Let $R$ be a Krull domain. If $\left|Cl(R)\right| = 2$, then $R$ is an HFD.*

With these lemmas, we are ready to prove the result for integrally closed $R$.

**Theorem 4.1.6.** *Let $R$ be a number ring. Then $R$ is an HFD if and only if the ring of formal power series $R[[x]]$ is an HFD.*

*Proof.* First, assume that $R[[x]]$ is an HFD. Since $R$ is Noetherian, we know that $R$ is atomic. Then consider two factorizations $\sigma_1 \dots \sigma_m = \tau_1 \dots \tau_n$, with $\sigma_i, \tau_j$ irreducibles in $R$ for $1 \leq i \leq m$, $1 \leq j \leq n$. Each $\sigma_i$ and $\tau_j$ remains irreducible in $R[[x]]$, so $m = n$ by the HFD property of $R[[x]]$. Then $R$ must be an HFD. Note that this half of the proof only depends on the fact that $R$ is atomic, and so holds more generally.

Now assume that $R$ is an HFD. Note that since $R$ is a Dedekind domain, $R$ is Noetherian, regular, and Krull. Then by Lemma 4.1.1 above, $R[[x]]$ shares these properties. Furthermore, since $R$ is an HFD, $\left|Cl(R)\right| \leq 2$ by Theorem 2.4.4. Now since $R$ and $R[[x]]$ are regular, note that they are locally factorial. Then by Lemma 4.1.2, $Cl(R) \cong DivCl(R)$ (which we already knew from $R$ being Dedekind) and $Cl(R[[x]]) \cong DivCl(R[[x]])$. In particular, $\left|DivCl(R)\right| = \left|Cl(R)\right| \leq 2$. Since $R$ is a regular Noetherian domain, Lemma 4.1.3 tells us that $\left|DivCl(R[[x]])\right| = \left|DivCl(R)\right| \leq 2$. Applying Lemma 4.1.2 to $R[[x]]$ now gives us that $\left|Cl(R[[x]])\right| = \left|DivCl(R[[x]])\right| \leq 2$. Then $R[[x]]$ is a Krull domain with $\left|Cl(R[[x]])\right| \leq 2$. If $\left|DivCl(R[[x]])\right| = \left|Cl(R[[x]])\right| = 1$, Lemma 4.1.4 tells us that $R[[x]]$ is a UFD; if $\left|Cl(R[[x]])\right| = 2$, Lemma 4.1.5 tells us that $R[[x]]$ is an HFD. In either case, $R[[x]]$ is an HFD. □

## 4.2 The Quadratic Case

Now that we have a result for number rings, we can move on to more general orders in number fields. Although we are not ready to show the general conjecture for any number field, we can at least approach the simplest case; in this section, we will consider the case when $K$ is a quadratic number field. The conjecture above has not entirely been shown for this case, but we have some useful properties for quadratic orders that can get us very close to the result. We will examine some of those properties here, then see the slightly weaker version of the conjecture which we can prove in the quadratic case.

**Theorem 4.2.1.** **[7]** *Let $R$ be a non-integrally closed order of index $n$ in a quadratic number field $K$. Then $R$ is an HFD if and only if $\overline{R}$ is an HFD, $\overline{R} = RU(\overline{R})$, and $n$ is either a prime or twice an odd prime.*

Furthermore, we have the following result which characterizes the possible primes which can divide the index of an HFD order.

**Theorem 4.2.2.** [7] *Let $R$ be a half-factorial order of index $n$ in a quadratic number field $K$. If $n = p$ for some prime $p$, then $p$ is inert in $K$. If $n = 2p$ for some odd prime $p$, then both 2 and $p$ are inert in $K$, and $p \not\equiv 2 \pmod 3$.*

These theorems provide a useful way to determine if an order in a quadratic number field is an HFD. Alternatively, they can tell us useful information about an order in a number ring if we already know it is an HFD. The following theorem will allow us to use the result for number rings to extend to non-integrally closed orders of number rings. The argument is heavily based on a result from [4]. However, it will help to have the following lemma first.

**Lemma 4.2.3.** *Let $R$ be a commutative ring with unity. Then $f \in R[[x]]$ is a unit if and only if its constant term is a unit in $R$.*

*Proof.* First, assume that $f = a_0 + a_1x + \dots$ is a unit in $R[[x]]$. Then there is some $g = b_0 + b_1x + \dots$ such that $fg = 1$. Note that the constant term of the product $fg$ is $a_0b_0 = 1$. Then $a_0$ is a unit in $R$.

Now assume that $f$ as above is an element in $R[[x]]$ with $a_0 \in U(R)$. Then let $b_0 = a_0^{-1}$, and for $i \in \mathbb{N}$, $b_i = -a_0^{-1} \sum_{j=1}^{i} a_j b_{i-j} \in R$. Define $g(x) := b_0 + b_1x + \dots \in R[[x]]$. Then considering the coefficients of the product $fg = c_0 + c_1x + \dots$, we can see that $c_0 = a_0b_0 = 1$. Furthermore, for $i \in \mathbb{N}$,

$$c_i = \sum_{j=0}^{i} a_j b_{i-j} = a_0(b_i + a_0^{-1} \sum_{j=1}^{i} a_j b_{i-j}) = 0.$$

Then $f \in U(R[[x]])$, with $f^{-1} = g$. □

**Theorem 4.2.4.** *Let $K$ be a number field, $R_1, R_2$ orders in $K$ with $R_2 \subseteq R_1$, and $I_1, I_2$ the corresponding conductor ideals. Also suppose that every nonzero coset in $R_1/I_2$ contains an element of $U(R_1)$. Then if $R_1[[x]]$ is an HFD, $R_2[[x]]$ is also an HFD.*

*Proof.* First, note that $R_2$ is a Noetherian domain; then by Lemma 4.1.1, $R_2[[x]]$ is also Noetherian. Then Proposition 1.2.43 shows that $R_2[[x]]$ is atomic. Now that we know that every element in $R_2[[x]]$ can be expressed as a product of irreducibles, we need only show that every such factorization is of the same length. To do so, we will show that every irreducible element of $R_2[[x]]$ remains irreducible in $R_1[[x]]$.

Let $f \in R_2[[x]]$ be irreducible, and suppose that $f = gh$, with $g, h \in R_1[[x]]$. First, note that if both $g$ and $h$ are in $I_2[[x]]$, then $f = gh$ in $R_2[[x]]$, so either $g$ or $h$ must be a unit. However,

since no element of $I_2[[x]]$ can be a unit, we get a contradiction. Then we have two more cases to consider: one in which neither $g$ nor $h$ is in $I_2[[x]]$, and one in which exactly one of $g$ and $h$ lies in $I_2[[x]]$.

Assume that neither $g$ nor $h$ is in $I_2[[x]]$. Then we can write $g$ and $h$ as follows:

$$g(x) = a_0 + a_1x + \cdots + a_{i-1}x^{i-1} + x^i(a_i + a_{i+1}x + \dots);$$

$$h(x) = b_0 + b_1x + \cdots + b_{j-1}x^{j-1} + x^j(b_j + b_{j+1}x + \dots).$$

Here, $a_i$ is the first coefficient of $g$ which is not in $I_2$, and $b_j$ is the first coefficient of $h$ which is not in $I_2$. Then since $a_i + I_2$ and $b_j + I_2$ are nonzero elements of $R_1/I_2$, each coset contains an element of $U(R_1)$ by assumption. Then by the lemma, we can write $g$ and $h$ as follows:

$$g = \overline{g} + x^i(u_g + I_g); \quad h = \overline{h} + x^j(u_h + I_h).$$

Here, $\overline{g}, \overline{h} \in I_2[[x]]$, $u_g, u_h \in U(R_1[[x]])$, and $I_g, I_h \in I_2$.

Now note that $f = gh = \overline{g}\overline{h} + \overline{g}x^j(u_h + I_h) + \overline{h}x^i(u_g + I_g) + x^{i+j}(u_gu_h + u_gI_h + u_hI_g + I_gI_h)$. Then since $f \in R_2[[x]]$ and $\overline{g}, \overline{h}, I_g, I_h \in I_2[[x]]$, we get that $u_gu_h \in R_2[[x]]$. Thus, $u_hg = u_h\overline{g} + x^i(u_gu_h + u_hI_g) \in R_2[[x]]$ and $u_gh = u_g\overline{h} + x^j(u_gu_h + u_gI_h) \in R_2[[x]]$. Therefore, $f = gh = (u_hg)(u_gh)(u_gu_h)^{-1}$. Since each factor is an element of $R_2[[x]]$ and $f$ is irreducible in $R_2[[x]]$, we must have that either $u_hg$ or $u_gh$ is a unit in $R_2[[x]]$ (we already know that $(u_gu_h)^{-1}$ is a unit). Without loss of generality, assume that $u_hg$ is a unit in $R_2[[x]]$. Then since $u_h$ is a unit in $R_1[[x]]$, we must have that $g$ is a unit in $R_1[[x]]$.

Finally, assume that exactly one of $g$ or $h$ is in $I_2[[x]]$; without loss of generality, we will assume $g \in I_2[[x]]$ and $h \notin I_2[[x]]$. Then we can write $h = \overline{h} + x^j(u_h + I_h)$ exactly as before. Then $u_hg \in I_2[[x]] \subseteq R_2[[x]]$. Furthermore, $u_h^{-1}h = u_h^{-1}\overline{h} + x^j + u_h^{-1}I_h \in R_2[[x]]$. Thus, $f = gh = (u_hg)(u_h^{-1}h)$, so either $u_hg$ or $u_h^{-1}h$ must be a unit in $R_2[[x]]$. Since $u_hg \in I_2[[x]]$, this cannot be a unit; then $u_h^{-1}h \in U(R_2[[x]]) \implies h \in U(R_1[[x]])$. Then in any case, if $f = gh$ with $g, h \in R_1[[x]]$, either $g$ or $h$ is a unit in $U(R_1[[x]])$. Then any irreducible element of $R_2[[x]]$ remains irreducible in $R_1[[x]]$.

Now assume that we have two equal factorizations $\pi_1 \dots \pi_m = \tau_1 \dots \tau_n$, with each $\pi_i$, $\tau_j$ an irreducible element of $R_2[[x]]$. Then as we have seen, each $\pi_i$ and $\tau_j$ is also irreducible in $R_1[[x]]$.

Then since $R_1[[x]]$ is an HFD, $m = n$. Then $R_2[[x]]$ is also an HFD. $\square$

To simplify the arguments we need to make, we will now take note of the following result.

**Theorem 4.2.5.** **[4]** $\mathbb{Z}[\sqrt{-3}]$ *is the unique non-integrally closed order in a non-real quadratic number field which is an HFD. In this case,* $\mathbb{Z}[\sqrt{-3}][[x]]$ *is an HFD as well.*

Since we have already shown that a number ring $R$ is an HFD iff $R[[x]]$ is an HFD, this result allows us to restrict our consideration to real quadratic fields. In other words, if $K = \mathbb{Q}[\sqrt{d}]$, we can restrict only to the cases when $d > 0$. Among other things, this tells us the form of the unit group (see Dirichlet's Unit Theorem, Theorem 2.3.13). This leads us to the major result of this section.

**Theorem 4.2.6.** *Let* $K = \mathbb{Q}[\sqrt{d}]$ *be a real quadratic number field for some squarefree* $d > 0$*,* $R$ *an order in* $K$ *of index* $n \in \mathbb{N}$*, and* $u$ *the fundamental unit in* $U(\overline{R})$*. Also suppose that the order of* $u + I$ *in* $U(\overline{R}/I)$ *is* $|u + I| = \prod_{p|n}(p^2 - 1)$*. Then* $R$ *is an HFD if and only if* $R[[x]]$ *is an HFD.*

*Proof.* The proof that $R[[x]]$ is an HFD $\implies$ $R$ is an HFD will follow exactly as in the proof of Theorem 4.1.6. Then we only need to show the reverse implication. Assume that $R$ is an HFD. If $R$ is integrally closed, i.e. $R = \overline{R}$, then $R[[x]]$ is an HFD by Theorem 4.1.6. Otherwise, either $n$ is a prime or twice an odd prime. For now, we will assume that $n = p$ for some prime $p$. Then $|u + I| = p^2 - 1$. Now recall that $\left|\overline{R}/I\right| = p^2$, so there are $p^2 - 1$ nonzero elements. Then every nonzero coset in $\overline{R}/I$ contains an element of $U(\overline{R})$. Now Theorem 4.2.1 tells us that $\overline{R}$ is an HFD, which tells us by Theorem 4.1.6 that $\overline{R}[[x]]$ is an HFD. Then by Theorem 4.2.4, $R[[x]]$ is an HFD.

Now assume that $n = 2p$ for some odd prime $p$ so that $|u + I| = 3(p^2 - 1)$. We know that both 2 and $p$ are inert in $K$, so by Theorem 2.3.12, $d \equiv 5 \pmod 8$ (notably $d \equiv 1 \pmod 4$) and $\left(\frac{d}{p}\right) = -1$. Now let $R_1 = \mathbb{Z}[\sqrt{d}]$, the index 2 order in $K$ (since $d \equiv 1 \pmod 4$, $\overline{R} = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$), and let $I_1$ be its conductor ideal. By Theorem 4.2.1, we know that $\overline{R}$ is an HFD and $\overline{R} = RU(\overline{R})$. Then $\overline{R} = RU(\overline{R}) \subseteq R_1U(\overline{R}) \subseteq \overline{R}$, so $\overline{R} = R_1U(\overline{R})$. Then since $\overline{R}$ is an HFD, $\overline{R} = R_1U(\overline{R})$, and the index of $R_1$ is 2, Theorem 4.2.1 tells us that $R_1$ is an HFD.

Now by the proof of Corollary 3.2.1, we know that $\left|U(\overline{R}/I)\right| = 3(p^2-1)$ and $\left|U(\overline{R}/I_1)\right| = 3$. Then since $|u + I| = 3(p^2-1)$, $U(\overline{R}/I)$ is cyclic, generated by $u+I$. Then $U(\overline{R}/I_1)$ is also generated by $u + I_1$, so $|u + I_1| = 3$. Then $R_1$ satisfies the conditions of this theorem, so since it is of prime index, the first case we showed shows that $R_1[[x]]$ is an HFD.

Now consider the unit group $U(R_1/I)$. Any element here is also a unit in $\overline{R}/I$, and so is a power of $u+I$. Note that since $\left|U(\overline{R}/I_1)\right| = 3$, we have that $u^3 + I_1 = 1 + I_1$, so $u^3 \in R_1$. However, note that if $u \in R_1$, then $u + I_1 = 1 + I_1$ (the only nonzero element of $R_1/I_1$), so $|u + I_1| = 1 \implies \left|U(\overline{R}/I_1)\right| = 1$, a contradiction. Then $U(R_1/I)$ must be generated by $u^3 + I = (u+I)^3$, so $\left|U(R_1/I)\right| = \left|u^3 + I\right| = \frac{3(p^2-1)}{3} = p^2 - 1$. Then since $\left|R_1/I\right| = p^2$, every nonzero coset in $R_1/I$ contains an element of $U(R_1)$ (namely, $u^{3k}$ for some $k \in \mathbb{N}$). Then by Theorem 4.2.4 and the fact that $R_1[[x]]$ is an HFD, $R_2[[x]]$ is an HFD. □

**Example 4.2.7.** *Let $K = \mathbb{Q}[\sqrt{5}]$ and $R = \mathbb{Z}[\sqrt{5}]$. Then $\overline{R} = \mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$, $n = 2$, and $I = 2\overline{R}$. $R$ as described here is an HFD (but not a UFD) such that $R[[x]]$ is an HFD.*

*Proof.* See [7] to see that $R$ is an HFD which is not a UFD. Then note that $N\left(\frac{1+\sqrt{5}}{2}\right) = -1$, so $\frac{1+\sqrt{5}}{2}$ is a unit in $\overline{R}$. Moreover, it is straightforward to show that this element cannot be expressed as a positive power of any other element of $\overline{R}$, and so must be the fundamental unit $u$ in $\overline{R}$. Then note that $|u + I| = 3$, since $u^3 = 2 + \sqrt{5} = 1 + 2\frac{1+\sqrt{5}}{2}$ is the first power of $u$ lying in $R$. Therefore, $R$ satisfies the assumptions of the theorem, so $R[[x]]$ is an HFD. □

**Example 4.2.8.** *Let $K$ be as in the previous example, but now let $R = \mathbb{Z}[3\sqrt{5}]$ so that $n = 6$. Then $R$ as described here is also an HFD such that $R[[x]]$ is an HFD.*

*Proof.* From the previous example, we know that $\overline{R} = \left[\frac{1+\sqrt{5}}{2}\right]$ is an HFD (in fact, it is a UFD) and that $n = 6 = 2 \cdot 3$. Then to show that $R$ is an HFD, Theorem 4.2.1 tells us that we need only know that $\overline{R} = RU(\overline{R})$. Letting $R_1 = \mathbb{Z}[\sqrt{5}]$, we already know that $\overline{R} = R_1U(\overline{R})$. Then if we instead show that $R_1 = RU(R_1)$, then $RU(\overline{R}) = RU(R_1)U(\overline{R}) = R_1U(\overline{R}) = \overline{R}$ and $R$ is an HFD. Since $RU(R_1) \subseteq R_1$ trivially, we only need to show the reverse inclusion.

As before, the fundamental unit in $\overline{R}$ is $\frac{1+\sqrt{5}}{2}$ and the fundamental unit in $R_1$ is $2 + \sqrt{5}$. Now let $a + b\sqrt{5} \in R_1$. We will consider four cases. If $b \equiv 0 \pmod 3$, then $a + b\sqrt{5} \in R \subseteq RU(R_1)$. If $a \equiv -b \pmod 3$, then $a + b\sqrt{5} = \left((-2a + 5b) + (a - 2b)\sqrt{5}\right)(2 + \sqrt{5}) \in RU(R_1)$. If $a \equiv 0 \pmod 3$, then $\left((9a - 20b) + (-4a + 9b)\sqrt{5}\right)(2 + \sqrt{5})^2 \in RU(R_1)$. If $a \equiv b \pmod 3$, then $\left((2a + 5b) + (a + 2b)\sqrt{5}\right)(2 + \sqrt{5})^{-1} \in RU(R_1)$. Since this covers all cases of elements in $R_1$, then $R_1 = RU(\overline{R_1})$. Then $R$ is an HFD.

Finally, we leave it as an exercise to the reader to verify that $u^{24}$ is the first power of $u$ which is congruent to 1 modulo $I$, i.e. that $|u + I| = 24 = (2^2 - 1)(3^2 - 1)$ in $U(\overline{R}/I)$. Then $R$ satisfies the assumptions of Theorem 4.2.6, and thus $R[[x]]$ is an HFD. □

# Chapter 5

# Conclusions and Conjectures

The results of this paper give us a glimpse of how orders in a number field are related to their integral closures and their power series rings. We have seen that the class number of such an order can be determined by finding the class number of its integral closure and examining units. Furthermore, we have seen that in some cases, the HFD property exists in an order $R$ if and only if it exists in $R[[x]]$. However, the power series results were somewhat incomplete, only having been shown to hold in the integrally closed case or in certain quadratic cases. That being said, no HFD order $R$ in any number field has been found for which $R[[x]]$ has been shown to not have the HFD property. This brings us to some conjectures that warrant further research.

## 5.1 Conjectures

This first conjecture is a repeat of the general case presented in the previous chapter.

**Conjecture.** *Let $R$ be an order in a number field $K$. Then $R$ is an HFD if and only if $R[[x]]$ is an HFD.*

As should be apparent from the previous chapter, the techniques used to show the integrally closed and quadratic cases require specific knowledge about the case at hand. For example, in the integrally closed case, we used that $R$ was a Krull domain. Since Krull domains are necessarily completely integrally closed, this will not hold in any non-integrally closed order. In the quadratic case, we leaned heavily on Theorems 4.2.1 and 4.2.2, which told us that $\overline{R} = RU(\overline{R})$ and the index

$n$ is either an inert prime or twice an inert prime, with 2 also inert in the second case. Moreover, we needed to know the structure of the order based on $n$, the representation of the conductor ideal, and the sizes and structures of the unit groups discussed in the results of Chapter 3. Even with this information, we have yet to show the quadratic case in general.

From this, it should be clear that the techniques used here will have to be heavily altered, supplemented, or replaced entirely to approach the general case. However, the quadratic case seems much more attainable in the immediate future, needing only to either show that $u + I$ has the necessary order in $U(\overline{R}/I)$ (see the statement of Theorem 4.2.6) for any quadratic HFD order, that some weaker statement holds which gives the desired result, or that this requirement is unnecessary in the first place. In any case, the quadratic case gives a more approachable conjecture than the general case.

**Conjecture.** *Let $R$ be an order in a quadratic number field $K$. Then $R$ is an HFD if and only if $R[[x]]$ is an HFD.*

That being said, the general case is certainly not a lost cause. In fact, it is certainly possible that developing the quadratic techniques further could provide a road map for the more general strategy. For example, the following conjecture would provide a huge step forward.

**Conjecture.** *Let $R, T$ be orders in a number field $K$ with $R \subseteq T$. Then if $R$ is an HFD, $T$ is an HFD as well.*

As we saw in the quadratic case, the fact that the index 2 order was an HFD whenever the index $2n$ order was an HFD allowed to use a sort of "stairstepping" behavior, first showing that $R_1[[x]]$ was an HFD, then using that to show that $R[[x]]$ was an HFD (in the notation of Theorem 4.2.6). If we can also show this conjecture in a general order, it could allow for a similar strategy.

Based on the quadratic case, we also saw that it helped to have information about the prime factorization of the index $n$ of the order. In the general case, such information could be very useful, though not much is currently known. However, it might be more useful to consider the factorization of the conductor ideal $I$. In the quadratic case, we know that $I = n\overline{R}$ and any prime factors of $n$ were necessarily inert in $K$. Then in addition to the factorization of $n$ in $\mathbb{Z}$, this actually told us the prime factorization of $I$ as an ideal in $\overline{R}$. This leads us to several questions, the answers to which could assist in proving the general case.

**Questions.** *Let $R$ be an HFD order in a number field $K$ with conductor ideal $I$. Are there any restrictions we can determine on the prime factors of $n = \left|\overline{R}/R\right|$? Are there any restrictions we can determine on the prime factors of $I$? Are these prime factors necessarily inert or distinct? Using the notation of Theorem 2.1.5 and the knowledge that $\overline{R}$, $R$, and $I$ are rank $[K : \mathbb{Q}]$ free abelian groups, what restrictions can we determine on the $d_i$ values involved in $\overline{R}/R$, $\overline{R}/I$, or $R/I$?*

Answering any or all of these questions could provide insight on how to approach the general case.

# Bibliography


[1] L. Carlitz. A characterization of algebraic number fields with class number two. *Proceedings of the American Mathematical Society*, 11(3):391, 1960.

[2] Luther Claborn. Note generalizing a result of Samuel's. *Pacific Journal of Mathematics*, 15(3):805–808, 1965.

[3] Harvey Cohn. *Introduction to the construction of class fields.* Dover Publications, 1994.

[4] Jim Coykendall. Extensions of half-factorial domains: A survey. *Arithmetical Properties of Commutative Rings and Monoids*, page 46–70, 2005.

[5] Robert M. Fossum. *The divisor class group of a Krull domain.* Springer, 1973.

[6] Ulrich Görtz and Torsten Wedhorn. *Algebraic geometry.* Vieweg+Teubner, 2010.

[7] Franz Halter-Koch. Factorization of algebraic integrers. *Ber. Math. Stat. Sektion Forschung*, 191, 1983.

[8] Peter Malcolmson and Frank Okoh. Power series extensions of half-factorial domains. *Journal of Pure and Applied Algebra*, 213(4):493–495, 2009.

[9] Daniel A. Marcus. *Number fields.* Springer, second edition, 2018.

[10] Hideyuki Matsumura. *Commutative ring theory.* Cambridge Univ. Press, 2008.

[11] Jürgen Neukirch. *Algebraic number theory.* Springer, 1999.

[12] Pierre Samuel. On unique factorization domains. *Illinois Journal of Mathematics*, 5(1), 1961.

[13] Abraham Zaks. Half factorial domains. *Bulletin of the American Mathematical Society*, 82(5):721–723, Sep 1976.