8-2024

Relating Elasticity and Other Multiplicative Properties Among Orders in Number Fields and Related Rings

Grant Moles
gmoles@clemson.edu

Relating Elasticity and other Multiplicative Properties among Orders in Number Fields and Related Rings

A Dissertation
Presented to
the Graduate School of
Clemson University

In Partial Fulfillment
of the Requirements for the Degree
Doctor of Philosophy
Mathematical Sciences

by
Grant Moles
August 2024

Accepted by:
Dr. James Coykendall, Committee Chair
Dr. Michael Burr
Dr. Ryann Cartor
Dr. Robert Dicks
Dr. Hui Xue

Abstract

This dissertation will explore factorization within orders in a number ring. By far the most well-understood of these orders are rings of algebraic integers. We will begin by examining how certain types of subrings may relate to the larger rings in which they are contained. We will then apply this knowledge, along with additional techniques, to determine how the elasticity in an order relates to the elasticity of the full ring of algebraic integers. Using many of the same strategies, we will develop a corresponding result in the rings of formal power series. Finally, we will explore a number of additional cases, including several explicit examples of orders of interest.

Dedication

This dissertation is dedicated to all those who have made it possible: to my family, whose support, love, and encouragement I have never had to question; to my teachers who helped me discover and develop my love of mathematics, especially Drs. Griff Elder and James Coykendall; to ¿306?, Aluminum Peanut Butter, and my Clemson Math Peeps, whose friendship and adventures have given my life so much joy; to the wonderful people in and around Cook, NE, the village that helped raise me into the man I am today; and to the countless others not named here whose lives have touched mine in innumerable ways. You have my undying gratitude.

Acknowledgments

I would like to thank my advisor, Dr. James Coykendall, for his advice, guidance, and support throughout my time at Clemson. This work would not have been possible without him, and I will be forever grateful for his constant positivity and seemingly endless patience.

I would also like to acknowledge the late Dr. Franz Halter-Koch, one of the giants on whose shoulders my work stands. Although I never had the chance to meet him, his work (and those which followed from it) formed a large part of the foundation for this dissertation.

Table of Contents

List of Tables

Chapter 1

Introduction

1.1 Motivation and Background

Given a ring R, one can consider the structure of R under either its addition operation or its multiplication operation. Under addition, the elements of R form an abelian group. Under multiplication, the (nonzero) elements of R form a semigroup; when R has multiplicative identity, this semigroup is actually a monoid. Broadly speaking, the goal of this dissertation is to understand the structure of the multiplicative monoid of certain types of rings. In particular, we will consider how elements in these rings factor into irreducibles and how we might glean information about their multiplicative structures from more well-understood related rings. In this chapter, we will compile the background knowledge necessary to understand the theorems that will be presented in later chapters. Much of this discussion will be drawn from [14], but it will be presented here for completeness.

Fundamental to the discussion presented here is the idea that much more is known about the structures of certain types of rings than others. For instance, fields have relatively simple structures because of the tight restrictions placed on their definition; thus, their properties are generally well known. Rings of algebraic integers, which are of particular interest to this dissertation, have, in some sense, more complex multiplicative structures. Even so, the study of these rings and their multitude of "nice" properties has a great deal of historical importance and forms the basis for the field of algebraic number theory. Since so much more is known when working in these and other similarly well-understood rings, it makes sense to leverage this knowledge to better understand rings that are closely related. As we will discuss in Chapter 2, certain types of subrings may retain some multiplicative properties of the larger rings in which they are contained. This will allow us to draw conclusions about the properties and structures of subrings within more familiar rings.

One method by which we may try to understand the multiplicative structure of a ring is how its elements may factor into irreducibles. For instance, it is well-known that the ring of integers $\mathbb{Z}$ has unique factorization, i.e. every integer (other than 0, 1, and -1) decomposes uniquely (up to sign) into a product of prime numbers. As we will see, not every ring exhibits such nice factorization properties (and in fact, some rings do not permit factorization into irreducibles at all). In Chapter 3, we will explore the idea of elasticity, one metric by which we measure how "badly" unique factorization may fail. In particular, we will focus on elasticity within orders in algebraic number fields using what is known about factorization in the corresponding ring of algebraic integers, as discussed above. We will also see how these results may be extended to the rings of formal power series over such orders. Chapter 4 will compile a few more specific cases of what is known, including explicitly determining which orders possess certain properties. Finally, Chapter 5 will outline directions in which this work may continue, as well as conjectures based on the results outlined throughout this paper.

The definitions and results in this first chapter are not original and are drawn from other sources in order to provide necessary background. In the remaining chapters, definitions and results are original to this dissertation unless otherwise indicated.

1.2 Commutative Algebra

This section will discuss definitions, theorems, and examples relating to the structures of elements, ideals, and properties present in a commutative ring. A basic understanding of abstract algebra concepts, including groups and rings, will be assumed. The definitions and results presented here can, for the most part, be found in a typical algebra text, such as [13], though some will be drawn from other sources; these additional sources will be identified as needed. As mentioned previously, this discussion will proceed much as in the first two chapters of [14], though some items will be omitted, added, or rearranged, as appropriate. Most proofs will not be presented here and will be left to the source materials. Throughout this section, we will let R be a commutative ring with identity 1.

1.2.1 Properties of Elements

First, we will consider certain properties that an element of R may have.

Definition 1.2.1. Let $\alpha, \beta \in R$. We say that α **divides** β if there exists some element $\gamma \in R$ such that $\beta = \alpha\gamma$. In this case, we also say that β is **divisible** by α.

Definition 1.2.2. Let $\alpha \in R$. We say that α is a **zero divisor** if $\alpha | 0$ nontrivially, i.e. if there exists some nonzero $\beta \in R$ such that $\alpha\beta = 0$.

Definition 1.2.3. Let $\alpha \in R$. We say that α is a **unit** if $\alpha | 1$, i.e. if there exists some $\beta \in R$ such that $\alpha\beta = 1$. In this case, the element β is called the **inverse** of α and denoted α^{-1}. The set of all units in R is denoted $U(R)$ (or $R^{\times}$).

As we will see in later sections, the set of units $U(R)$ will be very important to the major results of this dissertation. Thus, it will help to know the structure of this set.

Proposition 1.2.4. *$U(R)$ forms an abelian group under the ring multiplication from R, called the* **unit group** *(or* **group of units***) of R.*

Definition 1.2.5. Let R be a commutative ring with identity. We say R is an **integral domain** if $0 \in R$ is the only zero divisor in R, i.e. $\alpha\beta = 0 \implies \alpha = 0$ or $\beta = 0$.

Definition 1.2.6. Let R be a commutative ring with identity. We say R is a **field** if $0 \in R$ is the only nonunit in R, i.e. $U(R) = R\backslash\{0\}$.

The following result shows a relation between units and zero divisors that we will use frequently.

Proposition 1.2.7. *Let $\alpha \in R$ be a zero divisor. Then $\alpha \notin U(R)$. Moreover, if R is finite, the converse holds, i.e. $\alpha \notin U(R) \implies \alpha$ is a zero divisor when R is finite.*

Corollary 1.2.8. *If R is a field, then R is also an integral domain. Moreover, if R is finite, the converse holds, i.e. any finite integral domain is a field.*

In addition to these two types of elements, we can also consider a special type of zero divisor.

Definition 1.2.9. Let $\alpha \in R$. We say that α is **nilpotent** if there exists some $n \in \mathbb{N}$ such that $\alpha^n = 0$.

Especially important to some of the objects presented in Chapter 2 is the idea of elements in a ring being associated.

Definition 1.2.10. Let $\alpha, \beta \in R$. We say that α is an **associate** of β if there exists $u \in U(R)$ such that $\alpha = \beta u$.

Proposition 1.2.11. *Let $\sim$ be the relation on elements of R defined by $\alpha \sim \beta$ if and only if α is an associate of β. Then $\sim$ is an equivalence relation on the elements of R, i.e. it is reflexive, symmetric, and transitive.*

We will often choose to say that a set of elements $\{\alpha_i\}_{i\in\Gamma}$ are associates, rather than that one element is an associate of one other element. One will note that this usage make sense precisely because of the above proposition.

Proposition 1.2.12. *Let R be an integral domain. Then $\alpha, \beta \in R$ are associates if and only if $\alpha|\beta$ and $\beta|\alpha$.*

We will now consider the two types of elements which will be of primary interest when considering factorization in the ring R.

Definition 1.2.13. Let $\pi \in R$ be a nonunit. We say that π is **prime** if, for any $\alpha, \beta \in R$ such that $\pi|\alpha\beta$, either $\pi|\alpha$ or $\pi|\beta$.

Definition 1.2.14. Let R be an integral domain and $\pi \in R$ a nonzero, nonunit. We say that π is **irreducible** if, for any $\alpha, \beta \in R$ such that $\pi = \alpha\beta$, either $\alpha \in U(R)$ or $\beta \in U(R)$. The set of irreducible elements in R is denoted $\text{Irr}(R)$.

Example 1.2.15. Consider $\mathbb{Z}$, the ring of rational integers. Then $U(\mathbb{Z}) = \pm 1$, and $\text{Irr}(\mathbb{Z})$ is the set of prime numbers and their negatives. The set of prime elements in $\mathbb{Z}$ is exactly $\text{Irr}(\mathbb{Z}) \cup \{0\}$.

In this case, note that the concepts of (nonzero) prime and irreducible are actually equivalent. However, this will not always be the case.

Proposition 1.2.16. *Let R be an integral domain and $\alpha \in R$ be a nonzero prime. Then α is irreducible in R.*

Example 1.2.17. Let $R = \mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$. Then 2 is irreducible but not prime. Showing irreducibility will be easier after developing the idea of a norm on R, which we will see later. However, note that $2|6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$, but 2 does not divide either factor. Thus, 2 is not prime in R.

It should also be noted that these definitions rely heavily not just on the element(s) in question, but also on the ring R itself. This will be an important concept to keep in mind, especially in the major results presented in Chapter 3.

Example 1.2.18. Consider the rings $\mathbb{Z} \subseteq \mathbb{Q}$. Note that 2 lies in both $\mathbb{Z}$ and $\mathbb{Q}$, but is only a unit in $\mathbb{Q}$. On the other hand, 2 is only an irreducible in $\mathbb{Z}$. Moreover, 2 and 3 are associates in $\mathbb{Q}$, but not in $\mathbb{Z}$.

1.2.2 Properties of Ideals

On its face, factorization deals only with individual elements. However, considering the ideals of R will often be equally, if not more, informative. We start with the definitions of three special types of ideals.

Definition 1.2.19. Let I be an ideal in R. We say that I is a **principal ideal** if there exists some $\alpha \in R$ such that $I = \{\alpha\beta | \beta \in R\}$. In this case, we say that α **generates** I, and we write $I = (\alpha)$ (or $I = \alpha R$, particularly when R may not be clear from context).

Proposition 1.2.20. *Let R be an integral domain. Then $(a) = (b)$ if and only if a and b are associates.*

Definition 1.2.21. Let P be a proper ideal in R. We say that P is a **prime ideal** if, for any $\alpha, \beta \in R$, $\alpha\beta \in P$ implies that either $\alpha \in P$ or $\beta \in P$. The collection of all prime ideals in a ring R is called the **spectrum** of R, denoted $\operatorname{Spec}(R)$.

Proposition 1.2.22. *A principal ideal (α) in R is prime if and only if α is a prime element of R.*

Definition 1.2.23. Let M be a proper ideal in R. We say that M is a **maximal ideal** if the only ideal of R which strictly contains M is R itself. That is, if I is an R-ideal with $M \subseteq I \subsetneq R$, then $M = I$.

The following proposition gives an alternate characterization of prime and maximal ideals that will frequently be of great utility. Among other things, it will provide insight into the relationship between these two properties.

Proposition 1.2.24. *Let I be an ideal in R. Then I is maximal if and only if R/I is a field. Similarly, I is prime if and only if R/I is an integral domain.*

Corollary 1.2.25. *Any maximal ideal of R is also prime.*

While these three types of ideals are more foundational and typically of greater use and interest, we also want to consider two more types of ideals. As we will see in a moment, these are closely related to prime ideals.

Definition 1.2.26. Let I be an ideal in R. The **radical** of I is

$$\sqrt{I} := \{\alpha \in R \mid \exists\, n \in \mathbb{N} \text{ s.t. } \alpha^n \in I\} \supseteq I.$$

If $I = \sqrt{I}$, we say that I is a **radical ideal**.

Definition 1.2.27. Let I be a proper ideal in R. We say that I is a **primary ideal** if, for any $\alpha, \beta \in R$, $\alpha\beta \in I$ implies that either $\alpha \in I$ or $\beta^n \in I$ for some $n \in \mathbb{N}$.

Proposition 1.2.28. *Let I be an ideal in R. Then I is a prime ideal if and only if I is both radical and primary.*

As before, we can characterize these two types of ideals by their quotient rings.

Proposition 1.2.29. *Let I be an ideal in R. Then I is a radical ideal if and only if $^{R}\!/_{I}$ has no nonzero nilpotent elements. Similarly, a proper ideal I is primary if and only if every zero divisor in $^{R}\!/_{I}$ is nilpotent.*

The final type of ideal we will define here is actually an object associated with a ring extension.

Definition 1.2.30. Let T be a commutative ring with identity and $R \subseteq T$ a subring. The **conductor** from T into R is $(R : T) := \{\alpha \in R \,|\, \alpha T \subseteq R\}$. For any $\alpha \in (R : T)$, we say that α **conducts** T into R.

Proposition 1.2.31. *Let T be a commutative ring with identity and R a subring. Then $(R : T)$ is an ideal of both R and T. Moreover, $(R : T)$ is the largest T-ideal contained in R (i.e. it is the union of all T-ideals contained in R). For this reason, $(R : T)$ is often called the* **conductor ideal** *from T into R.*

The conductor ideal of a ring extension is one of the most important objects of study in this dissertation. As we will see in Chapters 2, 3, and 4, the structure of this ideal can often tell us a great deal about the rings R and T, especially which properties of T are "inherited" by its subring R.

It is worth noting that in this dissertation, we will assume the Axiom of Choice. In the field of commutative algebra, this is necessary to prove many well-known and interesting results, including the next proposition and its corollaries. In the interest of completeness, we will include here a statement of Zorn's Lemma, which is equivalent to the Axiom of Choice and is quite often a more useful statement in commutative algebra.

Axiom 1.2.32. Zorn's Lemma. *Let S be a partially ordered set. If every chain (totally ordered subset) in S has an upper bound in S, then S contains a maximal element.*

Proposition 1.2.33. *Let I be a proper ideal of R. Then I is contained in some maximal ideal of R.*

Corollary 1.2.34. *Let $\alpha \in R$ be a nonunit. Then α is contained in some maximal ideal of R.*

Corollary 1.2.35. *Every commutative ring with identity contains a maximal ideal.*

Finally, we conclude our discussion of ideals with a famous result that will be of particular use to us in the results presented in Chapter 2. As this result can often be found in a number of different forms throughout the literature (and was not part of the discussion in [14]), we will present this result with proof for the convenience of the reader.

Proposition 1.2.36. Prime Avoidance Lemma. *Let $\{I_i\}_{i=1}^{n}$ be a finite collection of ideals in R, with I_i prime for $i \geq 3$. Then for any ideal J of R, $J \subseteq \bigcup_{i=1}^{n} I_i \implies J \subseteq I_i$ for some $1 \leq i \leq n$.*

Proof. First, note that if $n = 1$, then the result is trivial. Now assume that $n = 2$ and $J \subseteq I_1 \cup I_2$. If we assume that J is not a subset of either I_1 or I_2, then there exist $\alpha_1 \in J \backslash I_2$ and $\alpha_2 \in J \backslash I_1$. Note that since J is in the union of these two ideals, $\alpha_1 \in I_1$ and $\alpha_2 \in I_2$. Since J is closed under addition, $\alpha_1 + \alpha_2 \in J$, and thus must be in either I_1 or I_2 (without loss of generality, assume $\alpha_1 + \alpha_2 \in I_1$). Then $(\alpha_1 + \alpha_2) - \alpha_1 = \alpha_2 \in I_1$, a contradiction. Then the result holds when $n = 2$.

Now working toward induction, assume that we have shown the result for any $n < m$ for some $m \geq 3$. Let $\{I_i\}_{i=1}^m$ be a collection of R-ideals such that I_i is prime for $i \geq 3$ and $J \subseteq \bigcup_{i=1}^m I_i$. Namely, I_m is a prime ideal. Then if J is contained in the union of any sub-collection of $m-1$ of the ideals $\{I_i\}_{i=1}^m$, the inductive hypothesis shows that J must be contained in one of the ideals I_i. Otherwise, for each $1 \leq j \leq m$, there exists some $\alpha_j \in J \backslash \bigcup_{i \neq j} I_i$; note that $\alpha_j \in I_j$ for every $1 \leq j \leq m$. Then consider the element $\alpha := \alpha_m + \alpha_1\alpha_2 \ldots \alpha_{m-1} \in J$. Since J is contained in the union of the I_i's, there is some $1 \leq i \leq m$ such that $\alpha \in I_i$. If $i < m$, then note that $\alpha - (\alpha_1\alpha_2 \ldots \alpha_{m-1}) = \alpha_m \in I_i$, a contradiction. On the other hand, if $i = m$, then $\alpha - \alpha_n = \alpha_1\alpha_2 \ldots \alpha_{m-1} \in I_m$. However, I_m is a prime ideal, and $\alpha_j \notin I_m$ for $1 \leq j < m$. Then this is also a contradiction. Then by induction, the result holds for any $n \in \mathbb{N}$. □

1.2.3 Properties of Rings

With this terminology and toolset, we can now consider properties of an entire ring R. To begin, we introduce three types of integral domains that will be of special interest to the later discussion of factorization.

Definition 1.2.37. Let R be an integral domain. We say that R is an **atomic domain** if for any nonzero, nonunit $\alpha \in R$, there exist $\pi_1, \ldots, \pi_n \in \text{Irr}(R)$ for some $n \in \mathbb{N}$ such that $\alpha = \pi_1 \ldots \pi_n$. Such an expression is called an **irreducible factorization** of the element α.

In other words, an atomic domain is an integral domain in which every nonzero, nonunit can be factored into a product of irreducibles. This should seem familiar; after all, it is well-known that integers (other than 0 and ±1) can be factored into a product of prime numbers. However, note that in this definition, we don't assume that such an irreducible factorization of $\alpha \in R$ is unique, as prime factorizations in $\mathbb{Z}$ are. This brings us to our next definition.

Definition 1.2.38. Let R be an atomic domain. We say that R is a **unique factorization domain** (UFD) if the following conditions hold:

1. If $\pi_1 \dots \pi_m = \tau_1 \dots \tau_n$ with $\pi_i, \tau_j \in \operatorname{Irr}(R)$ for $1 \leq i \leq m$, $1 \leq j \leq n$, then $m = n$; in other words, the two factorizations are of the same length.

2. If $\pi_1 \dots \pi_n = \tau_1 \dots \tau_n$ with $\pi_i, \tau_j \in \operatorname{Irr}(R)$ for $1 \leq i, j \leq n$, then there is some permutation $\sigma \in S_n$ such that π_i is an associate of $\tau_{\sigma(i)}$ for every $1 \leq i \leq n$; in other words, the two factorizations are the same up to reordering and multiplication by units.

In this sense, UFDs are the domains with the "nicest" factorization properties: every element breaks down into irreducibles, and any two irreducible factorizations of the same element are the same up to reordering and associates. Note the importance of allowing the irreducibles in two factorizations to be reordered and to be associates of one another rather than strictly the same element. In $\mathbb{Z}$, for example, one could write $6 = 2 \cdot 3 = (-3) \cdot (-2)$; under this definition, these factorizations would be considered equivalent. As it turns out, the irreducibles in UFDs have an additional nice property that is not immediately obvious.

Proposition 1.2.39. *Let R be a UFD. If $\pi \in \operatorname{Irr}(R)$, then π is a prime element of R.*

Recall that in general, any nonzero prime element is irreducible. This proposition tells us that in a UFD, the converse holds as well. This is why in the ring of rational integers $\mathbb{Z}$, which is a UFD, we generally make no distinction between (nonzero) primes and irreducibles.

However, as we will see in a moment, not every atomic domain exhibits unique factorization. One might then ask: can we create a metric by which we can measure how "badly" an atomic domain fails to be a UFD? Although it is certainly not the only such metric, one measurement we may use is called elasticity.

Definition 1.2.40. Let R be an atomic domain. For any nonzero, nonunit $\alpha \in R$, denote $\ell(\alpha) := \{n \in \mathbb{N} \mid \exists\, \pi_1, \ldots, \pi_n \in \mathrm{Irr}(R) \text{ s.t. } \alpha = \pi_1 \ldots, \pi_n\}$, the set of lengths of irreducible factorizations of α in R. The **elasticity** of α in R is

$$\rho_R(\alpha) = \frac{\sup(\ell(\alpha))}{\inf(\ell(\alpha))}.$$

The elasticity of R is $\rho(R) = \sup\{\rho_R(\alpha) | \alpha \in R \backslash (U(R) \cup \{0\})\}$.

Elasticity as a concept was first introduced in [21]. Fittingly, the elasticity of an element describes how far one can "stretch" the lengths of its irreducible factorizations. Similarly, the elasticity of an atomic domain is a measure of how stretchy its stretchiest element is. One will note that the elasticity of any element or any atomic domain must be at least one. Immediately from the definition, it should be clear that any UFD has an elasticity of exactly one. However, this feature alone does not fully characterize a UFD. This brings us to the next type of domain we will consider. Along with elasticity as a whole, this type of domain will be one of the chief objects of interest in Chapters 3 and 4.

Definition 1.2.41. Let R be an atomic domain. We say that R is a **half-factorial domain** (HFD) if $\rho(R) = 1$. In other words, if $\pi_1 \ldots \pi_m = \tau_1 \ldots \tau_n$ for $\pi_i, \tau_j \in \mathrm{Irr}(R)$, then $m = n$, i.e. any two irreducible factorizations of the same element must be of the same length.

It is worth noting that historically, elasticity was originally introduced to generalize observations that had been made about HFDs. In fact, HFDs were originally studied thirty years prior by Carlitz in [2]. In this paper, the term half-factorial domain is not used, and the study of such a domain is restricted only to rings of algebraic integers (which we will discuss later). It was Zaks who coined the phrase half-factorial domain and broadened their study in [23] and [24]. Study into these concepts, as well as into factorization as a whole, really picked up steam in the 1990s; since then, this has been a vast and vibrant field of study.

From the definition of a UFD, one can see that an HFD is simply an atomic domain that satisfies "half" of the conditions to be a UFD. Unsurprisingly, this was the original motivation behind Zaks' terminology. Clearly, any UFD is an HFD, and any HFD is an atomic domain. However, as the following examples will show, the converses of these implications do not hold in general.

Example 1.2.42. $\mathbb{Z}$, $\mathbb{Z}[i]$, and $\mathbb{Z}[x]$ are all UFDs. In general, if R is a UFD, then $R[x]$ is a UFD.

Example 1.2.43. $\mathbb{Z}[\sqrt{-5}]$ is an HFD which is not a UFD; in particular, the two irreducible factorizations $2 \cdot 3 = 6 = (1+\sqrt{-5})(1-\sqrt{-5})$ of 6 are of the same length, but not equivalent. Furthermore, if $K \subsetneq L$ are fields, then $K + xL[x]$ is an HFD which is not a UFD [22].

Example 1.2.44. $\mathbb{Z}[\omega]$, where $\omega = e^{\frac{2\pi i}{23}}$ is a primitive 23^{rd} root of of 1, is an atomic domain which is not an HFD [12]. For any squarefree $d \in \mathbb{Z}$ and $n \in \mathbb{N}$, with n neither a prime number nor twice an odd prime number, $\mathbb{Z}[n\sqrt{d}]$ is an atomic domain which is not an HFD [10].

Example 1.2.45. $R = \mathbb{Z} + x\mathbb{Q}[x]$ is an integral domain which is not atomic. In particular, the element $x \in R$ cannot be written as a product of irreducibles. $\mathbb{A}$, the ring of all algebraic integers (which we will define later) is also an integral domain which is not atomic; in fact, $\mathbb{A}$ has no irreducible elements at all.

The three types of domains presented here are defined based on their factorization behavior. Although there are more ways that we could categorize domains based on their factorization (BFDs, FFDs, etc.), these will not be discussed here. However, we will discuss another type of domain which may at first glance seem unrelated to the previous discussion. As we will see in a moment, this type of domain is actually intimately connected to the idea of unique factorization, especially in contexts of interest that we will discuss later.

Definition 1.2.46. Let R be an integral domain. We say that R is a **principal ideal domain** (PID) if every ideal I of R is principal, i.e. $I = (\alpha)$ for some $\alpha \in R$.

Proposition 1.2.47. *If R is a PID, then R is also a UFD.*

Even though the definition of a PID does not directly mention factorization at all, this proposition shows that any PID necessarily has unique factorization. The following example shows that the converse does not hold in general.

Example 1.2.48. As noted eariler, if R is a UFD, then $R[x]$ is a UFD as well. $R[x]$ is a PID if and only if R is a field. In particular, this means that if R is a UFD when is not a field (such as when $R = \mathbb{Z}$), then $R[x]$ is a UFD which is not a PID.

Although the concepts of a PID and UFD are not equivalent, they actually will be in a particular context of great interest that we will discuss later. In order to build up to the discussion of this context, we must first introduce some additional concepts and definitions.

Definition 1.2.49. Let P be a prime ideal in R. The **height** of P is

$$\mathrm{ht}(P) = \sup\{n \in \mathbb{N} \mid \exists\, P_i \in \mathrm{Spec}(R), 0 \leq i \leq n \text{ s.t. } P_0 \subseteq P_1 \subseteq \cdots \subseteq P_n = P\}.$$

In other words, the height of P is a measure of how many prime ideals could be "stacked" under P.

Definition 1.2.50. The **Krull dimension** of R is $\dim(R) = \sup\{\mathrm{ht}(P) \mid P \in \mathrm{Spec}(R)\}$. In other words, $\dim(R)$ is a measure of the highest possible "stack" of primes in R.

The Krull dimension is a very important tool in the field of commutative algebra. In the types of rings of interest to the major results of this dissertation, the Krull dimension will be well-behaved, as we will see later.

Definition 1.2.51. 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. Explicitly, $S^{-1}R = \{\frac{r}{s} \mid s \in S, r \in R, \frac{r_1}{s_1} = \frac{r_2}{s_2} \iff r_1s_2 = r_2s_1\}$.

It should be noted here that this definition is often adjusted to allow for S to contain zero divisors (or even zero itself). For our purposes, this simpler definition will suffice. Two types of localizations that are particularly useful are given in the following examples.

Example 1.2.52. 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 1.2.53. Let R be an integral domain. Then $R \backslash \{0\}$ is a multiplicatively closed set (in fact, $\{0\}$ is a prime ideal). The localization $(R\backslash\{0\})^{-1}R$ is commonly referred to as the **field of fractions** (or **quotient field**) of R.

The localizations of a ring R at its prime ideals are often studied instead of R itself, as they are often simpler to work with and can give useful information about R. We will return to this concept later. Fields of fractions are also important, and serve as a larger context in which to consider certain features of R. The next two definitions give examples of when it is useful to consider R within this (or another) larger context.

Definition 1.2.54. Let R and T be integral domains with R a subring of T. We say that $\alpha \in T$ is **integral** over R if α is a root of some monic polynomial $f \in R[x]$ (i.e. the leading coefficient of f is 1). The set of all elements of T which are integral over R is called the **integral closure** of R in T, denoted $\overline{R}_T$. If $R = \overline{R}_T$, we say that R is **integrally closed** in T. If $T = \overline{R}_T$, we say that T is an **integral extension** of R. When T is not specified, it is assumed to be the field of fractions of R.

Definition 1.2.55. Let R and T be integral domains with $R \subseteq T$. We say that $\alpha \in T$ is **almost integral** over R if there is some nonzero $r \in R$ such that $r\alpha^n \in R$ for every $n \in \mathbb{N}$. The set of all elements of T which are almost integral over R is called the **complete integral closure** of R in T, denoted R'_T. If $R = R'_T$, we say that R is **completely integrally closed** in T. If $T = R'_T$, we say that T is an **almost integral extension** of R. When T is not specified, it is assumed to be the field of fractions of R.

As the names might suggest, integrality is closely related to almost integrality, as the following proposition will show.

Proposition 1.2.56. *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.*

Corollary 1.2.57. *Let R be an integral domain. Then $\overline{R} \subseteq R'$, and if R is completely integrally closed, it is also integrally closed.*

It is also worth noting the following.

Proposition 1.2.58. *Let R and T be integral domains with $R \subseteq T$. Then $\overline{R}_T$ and R'_T are both closed under addition and multiplication. Thus, $\overline{R}_T$ and R'_T are integral domains.*

Although integrality tends to have nicer properties than almost integrality (and has historically been more studied), both properties are important. Even when working in a context in which integrality is more useful, understanding almost integrality can still be helpful. For one thing, it is sometimes easier to check if an element is almost integral over a ring than it is to check if the element is integral. Likewise, when a ring is completely integrally closed, it is often easier to show this than that the ring is integrally closed (despite the former being a stronger property). One important class of domains in which we will be particularly interested will always be completely integrally closed, so we will be able to take advantage of this relationship.

Before continuing to the next definition, we will note the following useful characteristic of integral extensions.

Proposition 1.2.59. *Let R and T be integral domains with $R \subseteq T$ and T an integral extension of R. Then $U(R) = R \cap U(T)$, i.e. any $\alpha \in R$ which has a multiplicative inverse $\alpha^{-1} \in T$ actually has $\alpha^{-1} \in R$.*

We now turn our attention to a type of ring whose ideals have useful finiteness conditions.

Definition 1.2.60. Let R be a commutative ring with identity. We say that R is a **Noetherian ring** if any ascending chain of ideals $I_1 \subseteq I_2 \subseteq \ldots$ is eventually constant, i.e. there exists $n \in \mathbb{N}$ such that $I_m = I_n$ for every $m \geq n$. Equivalently, any strictly ascending chain of ideals must be finite.

The following proposition provides useful equivalent characterizations of a Noetherian ring. It is worth mentioning again that we are assuming the Axiom of Choice; without this additional axiom, this equivalence does not hold.

Proposition 1.2.61. *Let R be a commutative ring with identity. The following are equivalent:*

1. *R is Noetherian;*
2. *Every ideal I of R is finitely generated, i.e. there exist $\alpha_1, \ldots, \alpha_n \in R$ such that $I = (\alpha_1, \ldots, \alpha_n)$;*
3. *Every nonempty collection S of ideals of R has a maximal member, i.e. there exists some $M \in S$ such that $M \subseteq I \in S \implies M = I$.*

The following result relates Noetherian rings back to our earlier discussion about factorization.

Proposition 1.2.62. *Let R be a Noetherian domain. Then R is atomic.*

With this terminology in hand, we are finally ready to define one of the most important classes of domains to the results in this dissertation.

Definition 1.2.63. Let R be an integral domain. We say that R is a **Dedekind domain** if the following conditions hold:

1. R is Noetherian;
2. $\dim(R) \leq 1$, i.e. every nonzero prime ideal in R is maximal;

3. R is integrally closed.

It is worth noting here that under this definition, a field is a Dedekind domain. Under certain conventions in the literature, a field may not be considered to be Dedekind. In this case, we would only need to change the second condition above to require $\dim(R) = 1$, i.e. disallow $\dim(R) = 0$. For our purposes, we will consider a field to act as a trivial example of a Dedekind domain.

Proposition 1.2.64. *Let R be an integral domain. The following are equivalent:*

1. *R is Dedekind;*

2. *R is Noetherian, and R_M is a PID for every maximal ideal M of R;*

3. *Every nonzero ideal I of R can be (uniquely) expressed as a product of prime ideals in R under the standard ideal multiplication*

$$I \cdot J = \{\alpha_1\beta_1 + \cdots + \alpha_n\beta_n | n \in \mathbb{N}, \alpha_i \in I, \beta_i \in I\}.$$

Here, R itself is considered to be an empty product of primes.

Dedekind domains are a very nice context in which to work, and as we will see later, are very significant in the field of algebraic number theory. Especially useful is the fact that every nonzero ideal in a Dedekind domain can be expressed uniquely as a product of primes. This will allow us to easily determine properties of ideals. Furthermore, this means that once we understand the structure of the prime ideals in a Dedekind domain, we can extend this knowledge to understand any ideal. We will now collect a number of useful properties of Dedekind domains.

Proposition 1.2.65. Ideal Cancellation. *Let R be a Dedekind domain and I, J_1, and J_2 ideals in R, with I nonzero. If $IJ_1 = IJ_2$, then $J_1 = J_2$.*

Proposition 1.2.66. *Let R be a Dedekind domain and I and J ideals in R. Then $I|J$ if and only if $I \supseteq J$.*

Proposition 1.2.67. *Let R be a Dedekind domain and I and J nonzero ideals in R. Let $I = P_1^{a_1} \dots P_k^{a_k}$ and $J = P_1^{b_1} \dots P_k^{b_k}$ be the unique factorizations of I and J into prime ideals in R. That is, $P_i \in \operatorname{Spec}(R)$ and $a_i, b_i \in \mathbb{N}_0$ for $1 \leq i \leq k$. Then $I + J = P_1^{m_1} \dots P_k^{m_k}$ and $I \cap J = P_1^{M_1} \dots P_k^{M_k}$, where $m_i = \min\{a_i, b_i\}$ and $M_i = \max\{a_i, b_i\}$ for $1 \leq i \leq k$.*

Corollary 1.2.68. *Let R be a Dedekind domain and I and J nonzero ideals in R. Then I and J are relatively prime, i.e. $R = I + J$, if and only if no prime ideal P of R divides both I and J.*

Proposition 1.2.69. *Let R be a Dedekind domain and I a nonzero ideal in R. Let $I = P_1^{a_1} \dots P_k^{a_k}$ be the unique factorization of I into prime ideals of R. Then I is a primary ideal if and only if $k = 1$, i.e. if and only if I is a power of a prime ideal. I is a radical ideal if and only if $a_i = 1$ for every $1 \leq i \leq k$, i.e. if and only if I is a product of distinct prime ideals.*

Proposition 1.2.70. *Let R be a Dedekind domain. Then R is a UFD if and only if R is a PID.*

Proposition 1.2.71. *Let R be a Dedekind domain. Then R is completely integrally closed.*

1.2.4 The Ideal Class Group

Thus far, for commutative rings with identity, we have considered properties of the elements, the ideals, and the rings themselves. In an integral domain, and in particular in a Dedekind domain, there is an additional structure on the ideals which we can consider. First, we will define a more general concept of an ideal which will help us to define this structure.

Definition 1.2.72. 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 $\alpha I \subseteq R$. Equivalently, $I = \alpha^{-1}J$ for some $\alpha \in R$ and ideal J of R. The collection of all fractional ideals of R will be denoted $\operatorname{Frac}(R)$.

From this definition, one can see why the term "fractional ideal" may be appropriate for such an object. In some sense, a fractional ideal I is simply an ideal of R which is allowed to have denominators, so long as the denominator of every element in I can be cleared by the same element $\alpha \in R$. When discussing both ideals of R (under the standard definition) and fractional ideals of R, we will often refer to ideals in R as **integral ideals** to avoid confusion. One will note that any integral ideal I of R is also a fractional ideal of R, since $\alpha I \subseteq R$ for any $\alpha \in R$.

Now to determine what additional structure is present in $\operatorname{Frac}(R)$, we will define inverses and an operation on this set.

Definition 1.2.73. Let R be an integral domain and $I \in \operatorname{Frac}(R)$. The **inverse** of I, denoted I^{-1}, is defined to be $I^{-1} = \{\alpha \in K \mid \alpha I \subseteq R\}$.

Proposition 1.2.74. *Let R be an integral domain and I, J nonzero fractional ideals of R. Then I^{-1} and $IJ := \{\alpha_1\beta_1 + \cdots + \alpha_n\beta_n \mid n \in \mathbb{N}, \alpha_i \in I, \beta_i \in J\}$ are also nonzero fractional ideals of R.*

With this, we now have a way to multiply two fractional ideals and a way to find the inverse of a fractional ideal. Furthermore, we have an identity fractional ideal, R itself, with the property that $IR = I$ for any fractional ideal I of R. One might expect that the inverse of a fractional ideal will be the inverse with respect to the multiplication defined here, i.e. that $II^{-1} = R$. However, this is not true in general.

Proposition 1.2.75. *Let R be an integral domain and I a fractional ideal of R. Then $II^{-1} \subseteq R$ and $I \subseteq (I^{-1})^{-1}$. Moreover, if there is some fractional ideal J of R for which $IJ = R$, then $J = I^{-1}$. However, it is not always true that $II^{-1} = R$.*

Example 1.2.76. Let $R = \mathbb{Z}[x]$ and $I = (2, x)$. Since I is an integral ideal of R, it is also a fractional ideal of R. Upon inspection, one will note that $I^{-1} = R$. Then $II^{-1} = IR = I \neq R$.

Since Frac(R) has an associative and commutative multiplication operation (note that it inherits these properties from multiplication in R) and a multiplicative identity, Frac(R) is a commutative monoid under this operation. However, this proposition and example show that Frac(R) may not be a group, since fractional ideals may not have an inverse with respect to this operation. In order to impose this additional structure, we must restrict our choices of fractional ideals to ensure that inverses exist.

Definition 1.2.77. Let R be an integral domain and I a fractional ideal of R. We say that I is an **invertible ideal** if $II^{-1} = R$. We denote the collection of all invertible ideals of R by Inv(R).

Proposition 1.2.78. *Let R be an integral domain and $I, J \in$ Inv(R). Then I^{-1} and IJ are also invertible ideals, with $(I^{-1})^{-1} = I$ and $(IJ)^{-1} = I^{-1}J^{-1}$. Thus,* Inv(R) *forms an abelian group under multiplication with identity R.*

With this, we have constructed a group consisting of the invertible fractional ideals of R. Although this group can certainly be useful, its structure actually carries a great deal of redundant information. In order to filter out the noise and make best use of this group, we will first want to identify a large class of invertible ideals.

Proposition 1.2.79. *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 of R with inverse $I^{-1} = \alpha^{-1}R$. Moreover,* $\text{Prin}(R)$*, the set of all principal fractional ideals of R, is a subgroup of* $\text{Inv}(R)$*.*

Now since $\text{Inv}(R)$ is an abelian group with subgroup $\text{Prin}(R)$, $\text{Prin}(R)$ is actually a normal subgroup. Then we can consider the quotient of $\text{Inv}(R)$ by this normal subgroup. In essence, this will give us an idea of how the invertible ideals of R behave after we have removed the redundant information carried by the nonzero elements of K themselves (the principal fractional ideals).

Definition 1.2.80. Let R be an integral domain. The quotient group ${}^{\text{Inv}(R)}\!/_{\text{Prin}(R)}$ is called the **ideal class group** (or just class group) of R, denoted $\text{Cl}(R)$. We call elements of $\text{Cl}(R)$ **ideal classes**, and we will denote by $[I]$ the ideal class containing the fractional ideal I.

Proposition 1.2.81. *Let R be an integral domain and I an invertible ideal of R. Then the ideal class $[I]$ contains some integral ideal J, i.e. there is an integral ideal $J \subseteq R$ such that $[J] = [I]$. Namely, given any nonzero $\alpha \in R$ such that $\alpha I \subseteq R$ (which must exist by definition of a fractional ideal), $J = \alpha I$ is an integral ideal such that $[J] = [\alpha I] = [I]$.*

This result shows that when considering the ideal class group $\text{Cl}(R)$, it actually suffices to only consider ideal classes containing invertible integral ideals. In other words, we need not concern ourselves with fractional ideals which are not contained in R.

The ideal class group will be of particular interest in the field of algebraic number theory, as we will discuss later. However, Dedekind domains in general have a very nice characterization in terms of fractional ideals which will make their class groups particularly easy to work with.

Proposition 1.2.82. *Let R be an integral domain. The following are equivalent:*

1. *R is Dedekind;*

2. *Every nonzero fractional ideal of R is invertible.*

In other words, to construct the ideal class group of a Dedekind domain, we do not need to first determine which ideals are invertible. Since every fractional ideal is invertible and every ideal class contains an integral ideal, the ideal class group of a Dedekind domain really provides a structure on all the integral ideals. This allows us to construct the ideal class group of a Dedekind domain in a different manner that does not reference fractional ideals (or even the field of fractions).

Proposition 1.2.83. *Let R be a Dedekind domain, and let S denote the set of all nonzero (integral) ideals of R. Define an equivalence relation $\sim$ on S by $I \sim J \iff \alpha I = \beta J$ for some nonzero $\alpha, \beta \in R$. Then $\mathrm{Cl}(R) \cong {}^{S}\big/{\sim}$.*

Now from the definition of a class group, note that $\mathrm{Cl}(R)$ is trivial if and only if every invertible ideal of R is principal. Then in the case of a Dedekind domain, in which every fractional ideal is invertible, we immediately get the following corollary to Proposition 1.2.70.

Corollary 1.2.84. *Let R be a Dedekind domain. Then $\big|Cl(R)\big| = 1$ if and only if R is a UFD.*

1.2.5 Orders and Free Abelian Groups

To understand the major results of this paper, there is one more type of ring (more precisely, a type of subring) which we must define.

Definition 1.2.85. 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 $\mathcal{O}$ is a $\mathbb{Z}$-module generated by a basis for R over $\mathbb{Q}$.

Example 1.2.86. Let $d \in \mathbb{Z}$ be a squarefree integer and $R = \mathbb{Q}[\sqrt{d}]$. Then $\mathcal{O} = \mathbb{Z}[n\sqrt{d}]$ is an order in R for any $n \in \mathbb{N}$. Note that $\{1, n\sqrt{d}\}$ is a $\mathbb{Z}$-basis for $\mathcal{O}$ and a $\mathbb{Q}$-basis for R.

As we will see in Chapters 2, 3, and 4, orders are the primary focus of the main results of this dissertation. In order to fully understand orders (as well as certain additional objects which we will discuss in the next section), we will need to make a detour through group theory. In particular, we will need some results regarding the structure of free abelian groups. For convenience, we recall the definition of a free abelian group.

Definition 1.2.87. 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 be uniquely expressed as a finite sum of elements of B and their negatives. That is,

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

Proposition 1.2.88. *Let G be a free abelian group and B_1, B_2 two bases for G. Then $|B_1| = |B_2|$. The cardinality of any basis for G is called the* **rank** *of G.*

Note that by definition, the additive group of an order is a free abelian group of finite rank. Examining how such groups interact with their subgroups will be helpful when moving through the rest of this dissertation. For full proofs of the following statements, see [14].

Proposition 1.2.89. *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.*

Corollary 1.2.90. *Let G be a group. Suppose that G is a subgroup of H_1 and contains a subgroup H_2, with both H_1 and H_2 free abelian groups of finite rank n. Then G is a free abelian group of rank n.*

Lemma 1.2.91. *Let G be a free abelian group of finite rank n, and let H be a subgroup of G. Then the quotient ${}^{G}\!/_{H}$ is a finite group if and only if H is a free abelian group of rank n.*

Proposition 1.2.92. *Let G be a free abelian group of finite rank n and H a free abelian subgroup of G of rank n. Then there exists a basis $\beta_1, \ldots, \beta_n$ for G and positive integers $d_1, \ldots, d_n$ such that $d_n | d_{n-1} | \ldots | d_2 | d_1$ and $d_1\beta_1, \ldots, d_n\beta_n$ forms a basis for H.*

It should be noted in this proposition that although such a basis must exist, it may not always be the most obvious basis for G, as the following example illustrates.

Example 1.2.93. Let $G = \mathbb{Z}\oplus\mathbb{Z}$, a rank 2 free abelian group, and $H = \langle(3,1),(2,3)\rangle \leq G$. 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. Note that with $\{(1,0),(0,1)\}$, the typical basis for G, we cannot choose integer multiples of the basis elements to serve as a basis for H.

1.3 Algebraic Number Theory

Although the methods and results of this dissertation will largely fall under the umbrella of commutative algebra, many of the particular objects of interest come from the realm of algebraic number theory. Thus, in order to understand the statements and proofs of the major results in Chapters 2, 3, and 4, one needs to have some familiarity with algebraic number theory. The results presented in this section can mostly be found in [12]; for proofs, see [12] or [14].

1.3.1 Algebraic Numbers and Integers

We start with the definitions of the fundamental objects of algebraic number theory.

Definition 1.3.1. Let K be a subfield of $\mathbb{C}$. If K is a field extension of $\mathbb{Q}$ of finite degree, i.e. if $[K : \mathbb{Q}] < \infty$, then we call K a **number field**.

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

Example 1.3.3. $\sqrt{2}$ and $\frac{1}{\sqrt{2}}$ are both algebraic, as they are roots of $x^2 - 2$ and $x^2 - \frac{1}{2}$, respectively. However, it is well-known that π and e are transcendental.

As the following proposition will show, the concepts of number fields and algebraic numbers are intimately related.

Proposition 1.3.4. *Let K be a number field. Then we have the following:*

1. *Any $\alpha \in K$ is a root of some monic polynomial $f \in \mathbb{Q}[x]$, with $\deg(f) \leq [K : \mathbb{Q}]$; thus, α is an algebraic number.*

2. *$K = \mathbb{Q}[\alpha]$ for some algebraic number α.*

While algebraic numbers and number fields are certainly important, they are not particularly interesting in and of themselves from a factorization standpoint.

After all, fields exhibit a form of trivial factorization, in that every nonzero element is a unit. However, just as the field of rational numbers has a very important subring with nice factorization properties, namely the ring of integers, so too do number fields.

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

Definition 1.3.6. Let K be a number field. The set of all algebraic integers in K is called the **ring of algebraic integers** in K (or the **number ring** corresponding to K), denoted $\mathcal{O}_K$. Since $\mathcal{O}_K = \overline{\mathbb{Z}}_K$, Proposition 1.2.58 tells us that $\mathcal{O}_K$ is an integral domain.

Example 1.3.7. Let $K = \mathbb{Q}$, the field of rational numbers. Then $\mathcal{O}_K = \mathbb{Z}$; thus, $\mathbb{Z}$ is often referred to as the ring of rational integers. If $K = \mathbb{Q}[\sqrt{2}]$, then $\mathcal{O}_K = \mathbb{Z}[\sqrt{2}]$.

Rings of algebraic integers are another very important object to the major results of this dissertation. As it turns out, these rings also have a number of properties that make them a particularly nice type of ring to work in, especially with regards to factorization. Before examining the structure of number rings themselves, we will first look into the relationship between a number field and its ring of algebraic integers.

Proposition 1.3.8. *Let K be a number field and $\mathcal{O}_K$ its ring of algebraic integers. Then we have the following:*

1. *K is the field of fractions of $\mathcal{O}_K$.*

2. *For any $\alpha \in K$, there is some $c \in \mathbb{N}$ such that $c\alpha \in \mathcal{O}_K$.*

3. *$K = \mathbb{Q}[\alpha]$ for some $\alpha \in \mathcal{O}_K$.*

In this proposition, note that item 1 tells us that any $\alpha \in K$ has some $\beta \in \mathcal{O}_K$ such that $\beta\alpha \in \mathcal{O}_K$. Item 2 simply states that we can be more selective in choosing β. Finally, item 3 actually follows as an application of item 2.

1.3.2 Structure of a Number Ring

We will now describe the structure of rings of algebraic integers using the terminology and results we developed in the previous section. To start, we have the following result regarding the additive structure of number rings.

Proposition 1.3.9. *Let K be a number field and $\mathcal{O}_K$ its ring of algebraic integers. Then $\mathcal{O}_K$ is an order in K, i.e. the additive group of $\mathcal{O}_K$ is a free abelian group of rank $n = [K : \mathbb{Q}]$.*

Definition 1.3.10. Let K be a number field, $\mathcal{O}_K$ its ring of algebraic integers, and $n = [K : \mathbb{Q}]$. Any $\mathbb{Z}$-basis for $\mathcal{O}_K$, i.e. any $\alpha_1, \ldots, \alpha_n \in \mathcal{O}_K$ such that $\mathcal{O}_K = \alpha_1\mathbb{Z} + \cdots + \alpha_n\mathbb{Z}$, is called an **integral basis** for $\mathcal{O}_K$.

Proposition 1.3.11. *Let K be a number field and $\mathcal{O}_K$ its ring of algebraic integers. Then any integral basis for $\mathcal{O}_K$ is also a $\mathbb{Q}$-basis for K. In particular, this means that K has a basis over $\mathbb{Q}$ consisting only of algebraic integers.*

As we discussed previously, free abelian groups have many useful properties. In particular, their subgroups, especially those of the same rank, are well-structured. The following result should suggest why these properties are useful in the field of algebraic number theory.

Proposition 1.3.12. *Let K be a number field, $\mathcal{O}_K$ its ring of algebraic integers, and I a nonzero ideal of $\mathcal{O}_K$. Then the additive group of I is a free abelian group of rank $n = [K : \mathbb{Q}]$.*

Thus, we can apply the results of our previous discussion of free abelian groups to ideals in a number ring.

Corollary 1.3.13. *Let K be a number field, $\mathcal{O}_K$ its ring of algebraic integers, I an ideal of $\mathcal{O}_K$, and $n = [K : \mathbb{Q}]$. Then ${}^{\mathcal{O}_K}/_{I}$ is a finite quotient ring. Moreover, there* *exists an integral basis $\{\alpha_1, \dots, \alpha_n\}$ for $\mathcal{O}_K$ and $d_1, \dots, d_n \in \mathbb{N}$ with $d_1 | \dots | d_n$ such that $\{d_1\alpha_1, \dots, d_n\alpha_n\}$ forms a $\mathbb{Z}$-basis for I. Also note that $\left|{}^{\mathcal{O}_K}/_{I}\right| = d_1 \dots d_n$. We will often refer to $\left|{}^{\mathcal{O}_K}/_{I}\right|$ as the* **norm** *of the ideal I.*

The next major structural result about rings of algebraic integers is arguably more important. However, much of the proof for the following statement actually follows from this discussion of the free abelian additive group.

Proposition 1.3.14. *Let K be a number field and $\mathcal{O}_K$ its ring of algebraic integers. Then $\mathcal{O}_K$ is a Dedekind domain.*

This result is incredibly significant to the field of algebraic number theory. It tell us that any number ring is Noetherian, has Krull dimension 1 (i.e. any nonzero prime ideal is maximal), and is integrally closed. As we have discussed previously, it also tells us that ideals can be factored into products of prime ideals and that every fractional ideal is invertible. We will discuss these properties in more detail later.

1.3.3 Trace, Norm, and Discriminant

The fact that any number ring is Dedekind is very important to understanding its structure. However, this alone is not enough to fully understand how factorization works in a given number ring. After all, a domain being Dedekind only tells us that the ideals factor uniquely into a product of prime ideals; that is, if we understand the prime ideals, we understand all the ideals. How, then, do we determine the structure and properties of the prime ideals? Moreover, how do the elements themselves factor? In order to tackle these questions, we will need to develop three useful tools to help us describe the properties of the elements of R. First, we must discuss minimal polynomials and embeddings.

Definition 1.3.15. Let α be an algebraic number. The **minimal polynomial** of α is the unique monic polynomial of minimal degree in $\mathbb{Q}[x]$ of which α is a root. If $f \in \mathbb{Q}[x]$ is the minimal polynomial of α, then any algebraic number β for which $f(\beta) = 0$ is called a **conjugate** of α.

Proposition 1.3.16. *Let α be an algebraic number with minimal polynomial f, with $n = \deg(f)$. Then α has exactly n distinct conjugates (including itself) and $n = [\mathbb{Q}[\alpha] : \mathbb{Q}]$.*

Corollary 1.3.17. *Let K be a number field, $\alpha \in K$, and f the minimal polynomial for α. Then $\deg(f) \leq [K : \mathbb{Q}]$.*

Proposition 1.3.18. *Let α be an algebraic integer. Then the minimal polynomial for α (as an algebraic number) lies in $\mathbb{Z}[x]$. Thus, every conjugate of α is an algebraic integer as well.*

Related to the idea of conjugates (though perhaps not on the surface) are embeddings of a number field in $\mathbb{C}$.

Proposition 1.3.19. *Let K and L be number fields with $L \subseteq K$. Then there are exactly $n = [K : L]$ embeddings of K into $\mathbb{C}$ which fix L pointwise.*

Corollary 1.3.20. *Let K be a number field. Then there are exactly $n = [K : \mathbb{Q}]$ embeddings of K into $\mathbb{C}$.*

Definition 1.3.21. Let K and L be number fields with $L \subseteq K$. If the embeddings of K into $\mathbb{C}$ which fix L pointwise are actually automorphisms of K, we say that the extension K/L is **Galois** (or **normal**). In this case, the group of automorphisms of K which fix L pointwise is called the **Galois group** of the extension K/L, denoted $\mathrm{Gal}(K/L)$.

Proposition 1.3.22. *Let K be a number field and $\alpha \in K$. Then $\beta \in \mathbb{C}$ is a conjugate of α if and only if there exists an embedding σ of K into $\mathbb{C}$ such that $\sigma(\alpha) = \beta$.*

Example 1.3.23. Let $d \in \mathbb{Z}$ be a squarefree integer and $K = \mathbb{Q}[\sqrt{d}]$. Because $[K : \mathbb{Q}] = 2$, there are exactly 2 embeddings of K into $\mathbb{C}$: σ_1, the identity on K; and σ_2 defined by $\sigma_2(a + b\sqrt{d}) = a - b\sqrt{d}$ for all $a, b \in \mathbb{Q}$.

Example 1.3.24. Let $d \in \mathbb{Z}$ be a cube-free integer, $K = \mathbb{Q}[\sqrt[3]{d}]$, and $\omega = e^{\frac{2\pi i}{3}}$, a primitive cube root of 1. Since $[K : \mathbb{Q}] = 3$, there are exactly 3 embeddings of K into $\mathbb{C}$: σ_1, the identity on K; σ_2 defined by $\sigma_2(\sqrt[3]{d}) = \omega\sqrt[3]{d}$; and σ_3 defined by $\sigma_3(\sqrt[3]{d}) = \omega^2\sqrt[3]{d}$.

With these tools in hand, we are ready to define the trace, norm, and discriminant.

Definition 1.3.25. Let K be a number field with $n = [K : \mathbb{Q}]$, and let $\sigma_1, \ldots, \sigma_n$ be the n embeddings of K into $\mathbb{C}$. For any $\alpha \in K$, the **trace** of α is defined by

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

Then **norm** of α is defined by

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

For an n-tuple $(\alpha_1, \ldots, \alpha_n) \in K^n$, the **discriminant** is defined by the square determinant

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

For convenience, given $\alpha \in K$, we will denote $\mathrm{disc}^K(\alpha) := \mathrm{disc}^K(1, \alpha, \ldots, \alpha^{n-1})$. If K is clear from context, we will often omit K from the above notation.

Proposition 1.3.26. *Let K be a number field with $n = [K : \mathbb{Q}]$, $\alpha, \beta \in K$, 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. *$N(c\alpha) = c^n N(\alpha)$;*

7. *Let $\alpha_1, \ldots, \alpha_m$ be the distinct conjugates of α, so $m = [\mathbb{Q}[\alpha] : \mathbb{Q}]$. Then $T(\alpha) = [K : \mathbb{Q}[\alpha]] \left(\sum_{i=1}^m \alpha_i\right)$ and $N(\alpha) = \left(\prod_{i=1}^m \alpha_i\right)^{[K:\mathbb{Q}[\alpha]]}$.*

8. *$N(\alpha) = \left|\mathcal{O}_K/(\alpha)\right|$; that is, the norm of a principal ideal is equal to the norm of its generator.*

One will note that, as a sum (respectively, a product) of algebraic integers, the trace (respectively, the norm) of an algebraic number must be an algebraic number. However, close inspection of item 7 above will show that in fact, the trace and norm of some α are coefficients in the minimal polynomial for α (potentially multiplied by an integer or raised to an integer power). This gives the following result.

Corollary 1.3.27. *Let K be a number field and $\alpha \in K$. Then $T(\alpha)$ and $N(\alpha)$ lie in $\mathbb{Q}$. Furthermore, if $\alpha \in \mathcal{O}_K$, then $T(\alpha)$ and $N(\alpha)$ lie in $\mathbb{Z}$.*

Corollary 1.3.28. *Let K be a number field and $\alpha \in \mathcal{O}_K$. Then $\alpha \in U(\mathcal{O}_K)$ if and only if $N(\alpha) = \pm 1$.*

These results, particularly those regarding the norm, are very important when considering factorization in a number ring. For instance, we claimed in Example 1.2.43 that the elements 2, 3, and $1 \pm \sqrt{-5}$ are irreducible in $\mathbb{Z}[\sqrt{-5}]$. The norm provides a way to prove this in an easier manner than the naïve approach.

Example 1.3.29. Let $K = \mathbb{Q}[\sqrt{-5}]$. Then $n = [K : \mathbb{Q}] = 2$ and $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$. Note that for any $\alpha = a + b\sqrt{-5} \in \mathcal{O}_K$, we have $N(\alpha) = (a+b\sqrt{-5})(a-b\sqrt{-5}) = a^2+5b^2$. Then $N(2) = 4$, $N(3) = 9$, and $N(1 \pm \sqrt{-5}) = 6$. However, one will note that there are no elements in $\mathcal{O}_K$ of norm ± 2 or ± 3. Then if $1 \pm \sqrt{-5} = \beta\gamma$, with $\beta, \gamma \in \mathcal{O}_K$, we must have that $6 = N(1 \pm \sqrt{-5}) = N(\beta)N(\gamma)$. Since $N(\beta)$ and $N(\gamma)$ must both be integers, but neither can be 2 or 3, then one of these norms must be ± 1, meaning that either β or γ must be a unit in $\mathcal{O}_K$. Then $1 \pm \sqrt{-5}$ is irreducible in $\mathcal{O}_K$; the proof that 2 and 3 are irreducible follows similarly.

This discussion shows that the trace and norm are not only more well-behaved than one might initially suspect, but also more useful. The same can be said about the discriminant.

Proposition 1.3.30. *Let K be a number field with $n = [K : \mathbb{Q}]$, and let $\alpha_1, \ldots, \alpha_n \in K$. Then $\operatorname{disc}(\alpha_1, \ldots, \alpha_n) \in \mathbb{Q}$. Furthermore, if each $\alpha_i \in \mathcal{O}_K$, then $\operatorname{disc}(\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}$.*

Proposition 1.3.31. *Let K be a number field and $\alpha_1, \ldots, \alpha_n \in K$. Then we have that $\operatorname{disc}(\alpha_1, \ldots, \alpha_n) = 0$ if and only if the α_i are linearly dependent over $\mathbb{Q}$.*

Proposition 1.3.32. *Let K be a number field and R a free $\mathbb{Z}$-submodule of K of rank $n = [K : \mathbb{Q}]$. If $\alpha_1, \ldots, \alpha_n$ and $\beta_1, \ldots, \beta_n$ are bases for R over $\mathbb{Z}$, then*

$\mathrm{disc}(\alpha_1, \ldots, \alpha_n) = \mathrm{disc}(\beta_1, \ldots, \beta_n)$. *In other words, any two n-tuples in K which generate the same R-module have the same discriminant.*

In this sense, the discriminant can be seen as a property of rank $n = [K : \mathbb{Q}]$ $\mathbb{Z}$-submodules of K, rather than of n-tuples in K. This gives us another way to define the discriminant.

Definition 1.3.33. Let K be a number field and R a free $\mathbb{Z}$-submodule of K of rank $n = [K : \mathbb{Q}]$. The **discriminant** of R is $\mathrm{disc}(R) := \mathrm{disc}(\alpha_1, \ldots, \alpha_n)$, where $\alpha_1, \ldots, \alpha_n$ form a basis for R over $\mathbb{Z}$ and the discriminant of this n-tuple is as defined above. When $R = \mathcal{O}_K$, we will often denote $\mathrm{disc}(\mathcal{O}_K)$ as $\mathrm{disc}(K)$ or Δ_K.

Proposition 1.3.34. *Let K be a number field and R, S be free $\mathbb{Z}$-submodules of K, both of rank $n = [K : \mathbb{Q}]$, with $R \subseteq S$. Then* $\mathrm{disc}(R) = \left|{}^{S}\!/_{R}\right|^2 \mathrm{disc}(S)$.

Corollary 1.3.35. *Let K be a number field and $\alpha_1, \ldots, \alpha_n \in \mathcal{O}_K$. Then the α_i form an integral basis for $\mathcal{O}_K$ if and only if* $\mathrm{disc}(\mathcal{O}_K) = \mathrm{disc}(\alpha_1, \ldots, \alpha_n)$.

Then among other things, the discriminant can help us determine when a given n-tuple is an integral basis for $\mathcal{O}_K$. Although a ring of algebraic integers cannot always be written in this form, it is often easiest to work with number rings of the form $\mathcal{O}_K = \mathbb{Z}[\alpha]$ for some $\alpha \in \mathcal{O}_K$. This corollary shows us that this is possible if and only if there is some $\alpha \in \mathcal{O}_K$ such that $\mathrm{disc}(\mathcal{O}_K) = \mathrm{disc}(\alpha)$. We conclude this discussion with the following result on integral bases, along with an explicit construction in the simplest case.

Proposition 1.3.36. *Let K be a number field and $\alpha \in \mathcal{O}_K$ such that $K = \mathbb{Q}[\alpha]$. Then there exist integers $d_1 | d_2 | \ldots | d_{n-1}$ and monic polynomials $f_1, \ldots, f_{n-1} \in \mathbb{Z}[x]$, with* $\deg(f_i) = i$ *for $1 \leq i \leq n-1$, such that $\{1, \frac{f_1(\alpha)}{d_1}, \ldots, \frac{f_{n-1}(\alpha)}{d_{n-1}}\}$ forms an integral basis for $\mathcal{O}_K$. Moreover, the d_i are uniquely determined by α, and* $\mathrm{disc}(\alpha) = (d_1 \ldots d_{n-1})^2 \mathrm{disc}(\mathcal{O}_K)$.

Proposition 1.3.37. *Let K be a quadratic number field, i.e. $[K:\mathbb{Q}]=2$. Then $K=\mathbb{Q}[\sqrt{d}]$ for some squarefree $d\in\mathbb{Z}$. The ring of integers of K is*

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

Furthermore, the discriminant of $\mathcal{O}_K$ is

$$\Delta_K=\begin{cases}4d, & d\equiv 2,3 \pmod 4;\\ d, & d\equiv 1 \pmod 4.\end{cases}$$

Before moving on to discuss prime and irreducibles in a number ring, we should take this moment to mention the units. As mentioned before, an algebraic integer is a unit if and only if its norm is ±1. Large unit groups mean large associate classes of the elements of a ring, which provides some degree of "freedom" to the irreducibles. This will especially be something we are concerned about in Chapter 2, when discussing a particular type of interesting subring. The structure of the unit group in a ring of algebraic integers is described in the following result.

Proposition 1.3.38. Dirichlet's Unit Theorem. *Let K be a number field with $n=[K:\mathbb{Q}]$. Then $U(\mathcal{O}_K)$, the group of units in the ring of algebraic integers $\mathcal{O}_K$, can be expressed as a direct product $U(\mathcal{O}_K)\cong W\times V$, where W is a finite cyclic group consisting of the roots of 1 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 embeddings σ of K into $\mathbb{C}$ such that $\sigma(K)\subseteq\mathbb{R}$), and r_2 is the number of complex conjugate pairs of non-real embeddings of K into $\mathbb{C}$, i.e. $n=r_1+2r_2$.*

Definition 1.3.39. Let K be a number field. In the notation of Dirichlet's Unit

Theorem above, if the rank of V as a free abelian group is 1, we call any generator of V a **fundamental unit** of $\mathcal{O}_K$. Note that a fundamental unit exists if and only if $n = r_1 = 2$; $n = 3$ and $r_1 = r_2 = 1$; or $n = 4$ and $r_2 = 2$.

Example 1.3.40. Let $K = \mathbb{Q}[i]$. Both embeddings of K into $\mathbb{C}$ are non-real embeddings, so $r_1 = 0$ and $r_2 = 1$. Then the rank of V is $0 + 1 - 1 = 0$, i.e. $U(\mathcal{O}_K)$ is a finite cyclic group, $U(\mathcal{O}_K) = \langle i \rangle$.

Example 1.3.41. Let $K = \mathbb{Q}[\sqrt{2}]$. This time, both embeddings of K into $\mathbb{C}$ are real, so $r_1 = 2$ and $r_2 = 0$. Then the only roots of unity in $\mathcal{O}_K$ are ± 1 and the rank of V is $2 + 0 - 1 = 1$, i.e. $U(\mathcal{O}_K) \cong \mathbb{Z}_2 \times \mathbb{Z}$. A fundamental unit of $\mathcal{O}_K$ is $1 + \sqrt{2}$ (note that $N(1 + \sqrt{2}) = 1 - 2 = -1$, so this is a unit), so $U(\mathcal{O}_K) = \{\pm(1 + \sqrt{2})^k | k \in \mathbb{Z}\}$.

1.3.4 Prime Decomposition

In the ring of rational integers, we know how prime and irreducible elements behave. Namely, every irreducible element is prime, and the prime elements are exactly the prime numbers and zero. Furthermore, since any ring of algebraic integers is a Dedekind domain, we know that any ideal factors uniquely into a product of prime ideals. The question, then, is how we may describe the prime ideals and irreducible elements in a number ring. As it turns out, we can leverage our knowledge of the rational primes to understand prime ideals in a generic ring of algebraic integers.

Definition 1.3.42. Let K be a number field and $p \in \mathbb{Z}$ a rational prime. Let $p\mathcal{O}_K = P_1^{e_1} \dots P_r^{e_r}$ be the factorization of the ideal $p\mathcal{O}_K$ into prime $\mathcal{O}_K$-ideals. We define the following.

1. For each $1 \leq i \leq r$, we say that P_i is a prime **lying over** p and note that $p\mathbb{Z} = P_i \cap \mathbb{Z}$.

2. For each $1 \leq i \leq r$, we call the exponent e_i the **ramification index** of P_i over p, denoted $e(P_i|p)$.

3. For each $1 \leq i \leq r$, we call $f_i \in \mathbb{N}$ such that $\left|{}^{\mathcal{O}_K}\!/_{P_i}\right| = p^{f_i}$ the **inertial degree** of P_i over p, denoted $f(P_i|p)$.

4. If $r > 1$, we say that p **splits** in K (or in $\mathcal{O}_K$). If $e(P_i|p) = f(P_i|p) = 1$ for every $1 \leq i \leq r$, we say that p **splits completely** in K (or in $\mathcal{O}_K$).

5. If $e(P_i|p) > 1$ for some $1 \leq i \leq r$, we say that p **ramifies** in K (or in $\mathcal{O}_K$). If $r = 1$ and $f(P_1|p) = 1$, we say that p is **totally ramified** in K (or in $\mathcal{O}_K$).

6. If $p\mathcal{O}_K$ is a prime $\mathcal{O}_K$ ideal (i.e. $r = 1$ and $e(P_1|p) = 1$), we say that p is **inert** in K (or in $\mathcal{O}_K$).

Proposition 1.3.43. *Let K be a number field and $p \in \mathbb{Z}$ a rational prime. Let $p\mathcal{O}_K = P_1^{e_1} \ldots P_r^{e_r}$ be the factorization of the ideal $p\mathcal{O}_K$ into prime $\mathcal{O}_K$-ideals and f_i denote the inertial degree $f(P_i|p)$ for $1 \leq i \leq r$. Then $[K : \mathbb{Q}] = \sum_{i=1}^{r} e_i f_i$.*

Proposition 1.3.44. *Let K be a number field and $p \in \mathbb{Z}$ a rational prime. If K is Galois over $\mathbb{Q}$, then every prime $\mathcal{O}_K$-ideal lying over p has the same ramification index and inertial degree.*

This gives us terminology to use to describe the way in which a rational prime decomposes into prime ideals in a number ring. However, it fails to actually tell us how to produce these factorizations. The following proposition describes how we might derive such a factorization.

Proposition 1.3.45. *Let $K = \mathbb{Q}[\alpha]$ be a number field with $\alpha \in \mathcal{O}_K$, f the minimal polynomial of α in $\mathbb{Z}[x]$, and $p \in \mathbb{Z}$ a rational prime which does not divide $\left|{}^{\mathcal{O}_K}\!/_{\mathbb{Z}[\alpha]}\right|$. Let $\overline{f}$ be the the polynomial in $\mathbb{Z}_p[x]$ found by reducing the coefficients of f modulo p,* *and* $\overline{f} = \overline{g_1}^{e_1}\overline{g_2}^{e_2}\ldots\overline{g_r}^{e_r}$ *the unique factorization of* $\overline{f}$ *into irreducible polynomials in* $\mathbb{Z}_p[x]$ *(here each* g_i *is a polynomial in* $\mathbb{Z}[x]$*). Then the factorization of* $p\mathcal{O}_K$ *into prime* $\mathcal{O}_K$*-ideals is given by* $p\mathcal{O}_K = P_1^{e_1}\ldots P_r^{e_r}$*, with* $P_i = (p, g_i(\alpha))$ *and* $f(P_i|p) = \deg(g_i)$ *for* $1 \leq i \leq r$*.*

Thus, the decomposition of all but finitely many rational primes in a number field K can be determined by factoring a degree $n = [K : \mathbb{Q}]$ polynomial modulo p. If we apply this proposition to the case of a quadratic number field, we get the following corollary.

Corollary 1.3.46. *Let* $K = \mathbb{Q}[\sqrt{d}]$ *be a quadratic number field,* $p \in \mathbb{Z}$ *a rational prime, and* $\left(\frac{d}{p}\right)$ *the Legendre symbol. Since* $[K : \mathbb{Q}] = 2$*,* p *must either split completely, totally ramify, or be inert in* K*. If* p *is odd, then* p *splits completely if and only if* $\left(\frac{d}{p}\right) = 1$*,* p *is inert if and only if* $\left(\frac{d}{p}\right) = -1$*, and* p *ramifies if and only if* $\left(\frac{d}{p}\right) = 0$ *(i.e. if and only if* $p|d$*). For* $p = 2$*,* 2 *splits completely if and only if* $d \equiv 1 \pmod 8$*,* 2 *is inert if and only if* $d \equiv 5 \pmod 8$*, and* 2 *ramifies otherwise.*

From the quadratic case, one might notice a pattern with the primes that ramify, especially after considering Proposition 1.3.37. The following shows that this pattern is not a coincidence, and actually holds for any number field.

Proposition 1.3.47. *Let* K *be a number field,* Δ_K *its discriminant, and* p *a rational prime. Then* p *ramifies in* K *if and only if* $p|\Delta_K$*.*

With this, we can decompose each rational prime into prime ideals to fully determine the ideal structure of a number ring. We will use these methods of prime factorization a great deal in Chapter 4.

1.3.5 The Ideal Class Group of a Number Ring

Recall that any ring of algebraic integers is a Dedekind domain. Furthermore, every (fractional) ideal in a Dedekind domain is invertible, making their ideal class groups particularly informative. In the case of a ring of algebraic integers, the class group is even nicer, carrying additional properties that tell us a great deal about the structure of the ring. In particular, it actually tells us about how well factorization behaves. To start, we have the following basic result.

Proposition 1.3.48. *Let K be a number field. Then $\mathrm{Cl}(\mathcal{O}_K)$, often also denoted $\mathrm{Cl}(K)$, is a finite group.*

Definition 1.3.49. Let K be a number field. We call $\left|\mathrm{Cl}(\mathcal{O}_K)\right|$ the **class number** of K, often denoted h_K. When K is clear from context, it may be omitted from this notation.

This result tells us that there are only finitely many ideal classes which the ideals of a number ring can fall into. Furthermore, since we already know that $\mathrm{Cl}(\mathcal{O}_K)$ is an abelian group, we know that $\mathrm{Cl}(\mathcal{O}_K)$ can be expressed as a finite direct product of finite cyclic groups.

In addition to the structure of the class group $\mathrm{Cl}(\mathcal{O}_K)$ itself, we may also ask how the ideals are distributed amongst these ideal classes. The following result shows again that rings of algebraic integers have particularly nice class groups.

Proposition 1.3.50. *Let K be a number field and $[I] \in \mathrm{Cl}(\mathcal{O}_K)$. Then there are infinitely many prime ideals in the ideal class $[I]$.*

Regardless of how nice these properties are, they do us little good unless we can reliably construct the class group of a number ring. One might reasonably ask at this point if such a thing is even possible. Even though there are only finitely many ideal classes, how might we tell when we have identified every class? The following result addresses exactly this concern.

Proposition 1.3.51. Minkowski's Bound. *Let K be a number field. Then every ideal class in $\mathrm{Cl}(\mathcal{O}_K)$ contains an ideal I such that:*

$$\left|{}^{\mathcal{O}_K}\!/_{I}\right| \leq \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2}\sqrt{|\Delta_K|}.$$

Here, $n = [K : \mathbb{Q}]$, r_2 refers to the number of complex conjugate pairs of embeddings of K into $\mathbb{C}$, and Δ_K refers to the discriminant of K.

Using this theorem along with what we know about prime decomposition in a ring of algebraic integers, we can see that Minkowski's Bound allows us to check only finitely many ideals to produce all the ideal classes in $\mathrm{Cl}(\mathcal{O}_K)$. In particular, we should factor each rational prime $p \in \mathbb{Z}$ which is less than or equal to this bound, determine from this all the ideals I in R which have norm less than or equal to the bound, then determine which ideal classes these ideals belong to. Once we have done so, we have determined the class group of $\mathcal{O}_K$.

Example 1.3.52. Let $K = \mathbb{Q}[\sqrt{-5}]$; then $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$. In this case, note that in the notation above, $n = 2$, $r_2 = 1$, and $\Delta_K = -20$. Plugging into the formula for Minkowski's Bound, this tells us that every ideal class in $\mathrm{Cl}(\mathcal{O}_K)$ must contain an ideal I such that $\left|{}^{\mathcal{O}_K}\!/_{I}\right| \leq \frac{4\sqrt{5}}{\pi} < 3$, so we should consider the ideals of norm 1 or 2. $\mathcal{O}_K$ itself is the only ideal of norm 1, which belongs to the principal (identity) class of $\mathrm{Cl}(\mathcal{O}_K)$. Corollary 1.3.46 tells us that $2\mathcal{O}_K$ is ramified; Proposition 1.3.45 tells us that $2\mathcal{O}_K = (2, 1 + \sqrt{-5})^2$. This ideal has norm 2, and since no elements in $\mathcal{O}_K$ have norm 2, it is a non-principal ideal (and thus is not in the identity class). These two ideals must cover every ideal class in $\mathrm{Cl}(\mathcal{O}_K)$. Thus, $h_K = 2$, so $\mathrm{Cl}(\mathcal{O}_K) \cong \mathbb{Z}_2$.

Now that we can construct the ideal class group of a ring of algebraic integers, we can use it to discuss factorization. First, we note that an irreducible element in an integral domain can equivalently be defined as an element generating a proper principal ideal which is maximal among the proper principal ideals of the domain. Then in a number ring, we might ask how such proper principal ideals can be constructed. If we multiply a number of prime ideals together and the result is a principal ideal (i.e. lies in the identity class of $\mathrm{Cl}(\mathcal{O}_K)$), but no (nontrivial) proper sub-product of these prime ideals multiply to be a principal ideal, then any generator of that principal ideal is irreducible in $\mathcal{O}_K$.

Example 1.3.53. Let $K = \mathbb{Q}[\sqrt{-5}]$, as above. We know that $(2, 1+\sqrt{-5})$, a prime ideal, is non-principal. If we square this ideal, we get $(2, 1+\sqrt{-5}) = (2)$. Since this ideal is principal, but no (nontrivial) proper sub-product of $(2, 1+\sqrt{-5})^2$ is principal, we can conclude that 2 is irreducible in $\mathcal{O}_K$.

This discussion motivates us to consider the Davenport constant.

Definition 1.3.54. Let G be a finite abelian group and $\{g_1, \ldots, g_n\} \subseteq G$ a sequence of elements of G (we do not require the g_i to be distinct). We say that $\{g_1, \ldots, g_n\}$ is a **0-sequence** of G if $g_1 + \cdots + g_n = 0$. Similarly, we say that $\{g_1, \ldots, g_n\}$ has a **0-subsequence** if there exist $1 \leq i_1 < i_2 < \cdots < i_m \leq n$ such that $g_{i_1} + \cdots + g_{i_m} = 0$. The **Davenport constant** of G is

$$D(G) := \min\{n \in \mathbb{N} \mid \{g_1, \ldots, g_n\} \subseteq G \implies \exists \text{ a 0-subsequence of } \{g_1, \ldots, g_n\}\}.$$

In other words, the Davenport constant is the smallest number such that any sequence of elements of G of that length is guaranteed to have a 0-subsequence. Equivalently, $D(G)$ is the length of the longest 0-sequence in G which has no proper 0-subsequence.

Proposition 1.3.55. *Let G be a finite abelian group. Then $D(G) \leq |G|$. If $G \cong \mathbb{Z}_n$ is cyclic, then $D(G) = n$. If $G \cong \mathbb{Z}_m \times \mathbb{Z}_n$ with $n|m$, then $D(G) = m + n - 1$ [18]. If $G \cong \mathbb{Z}_{p^{a_1}} \times \cdots \times \mathbb{Z}_{p^{a_n}}$ is a p-group for some prime $p \in \mathbb{N}$, then $D(G) = \left(\sum_{i=1}^{n} p^{a_i}\right) - n + 1$ [17].*

The concept of 0-sequences and 0-subsequences should look familiar from our earlier discussion of how to construct irreducible elements in $\mathcal{O}_K$. In particular, any 0-sequence in $\mathrm{Cl}(\mathcal{O}_K)$ with no proper 0-subsequences can be used to find an irreducible element by multiplying a prime ideal from each class in the 0-subsequence, then finding a generator for the resulting principal ideal. Then it may come as no surprise that we can use the Davenport constant of the class group to give us information about factorization (in particular, elasticity) in a ring of algebraic integers. The following result comes from [15] and demonstrates just how well-understood factorization is in rings of algebraic integers.

Proposition 1.3.56. *Let K be a number field. If $h_K = 1$, we know that $\mathcal{O}_K$ is a UFD, so $\rho(\mathcal{O}_K) = 1$. If $h_K > 1$, then $\rho(\mathcal{O}_K) = \frac{D(\mathcal{O}_K)}{2}$.*

Corollary 1.3.57. *Let K be a number field. Then $\mathcal{O}_K$ is an HFD if and only if $\left|\mathrm{Cl}(\mathcal{O}_K)\right| \leq 2$.*

Although this corollary follows immediately from the proposition, it is worth noting that it was originally shown by Carlitz in [2] and predates the proposition by over 30 years. In fact, this is generally considered the first description of an HFD that is not a UFD in the literature, before such a ring would even have been called half-factorial.

Example 1.3.58. Let $K = \mathbb{Z}[\sqrt{-5}]$. We determined above that $\mathrm{Cl}(\mathcal{O}_K) \cong \mathbb{Z}_2$. Then $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$ is an HFD.

Thus, the elasticity of a number ring is determined entirely by its class group. Since we can determine the class group of a number ring using Minkowski's bound, we can determine the elasticity of any given ring of algebraic integers in finitely many steps. We will make heavy use of these results throughout the rest of this dissertation.

1.3.6 Orders in a Number Field

The final object which we need to discuss before getting to the main results of this dissertation is actually the primary object of interest. We have already seen the definition of an order; we will specifically be interested in orders which lie in number fields. The following gives an alternate characterization of an order in this context.

Proposition 1.3.59. *Let K be a number field and $\mathcal{O}$ a subring (with unity) of K. Then $\mathcal{O}$ is an order in K if and only if $\mathcal{O} \subseteq \mathcal{O}_K$ and the additive group of $\mathcal{O}$ is a rank $n = [K : \mathbb{Q}]$ free abelian group.*

Corollary 1.3.60. *Let K be a number field. Then $\mathcal{O}_K$ is the maximal order in K, i.e. $\mathcal{O}_K$ is an order of K, and for any order $\mathcal{O}$ in K, $\mathcal{O} \subseteq \mathcal{O}_K$.*

Corollary 1.3.61. *Let K be a number field and $\mathcal{O}$ an order in K. Then there exists some $c \in \mathbb{N}$ such that $c\alpha \in \mathcal{O}$ for every $\alpha \in \mathcal{O}_K$. Moreover, for any $\alpha \in K$, there exists some $d \in \mathbb{N}$ such that $d\alpha \in \mathcal{O}$.*

Corollary 1.3.62. *Let K be a number field and $\mathcal{O}$ an order in K. Then the conductor ideal $(\mathcal{O} : \mathcal{O}_K)$ is nonzero. We will often refer to $(\mathcal{O} : \mathcal{O}_K)$ as the* **conductor ideal** *of $\mathcal{O}$ without specifying $\mathcal{O}_K$.*

As we will see in later chapters, the conductor ideal of an order in a number field can actually tell us a great deal about the order itself. In particular, we will see that when this conductor ideal is radical, we can often relate the factorization properties of the order more intimately to those of the ring of algebraic integers.

Recall that a number ring is Dedekind; that is, it is Noetherian, has Krull dimension 1, and is integrally closed. However, this structure will not be maintained for a general order in a number field. The following result outlines which of these three properties carry over.

Proposition 1.3.63. *Let K be a number field and $\mathcal{O}$ an order in K. Then $\mathcal{O}$ is Noetherian and* $\dim(\mathcal{O}) = 1$*. The field of fractions of $\mathcal{O}$ is K, and $\overline{\mathcal{O}} = \mathcal{O}_K$. In particular, this means that $\mathcal{O}$ is integrally closed if and only if it is Dedekind, which holds if and only if $\mathcal{O} = \mathcal{O}_K$.*

Although the main results of this dissertation pertain to orders in any number field, it will help to more fully understand orders in quadratic number fields. Not only are these fields relatively simple and can thus be used to construct helpful and illustrative examples, they connect to a prior result that served as a foundation for those found in this dissertation.

Proposition 1.3.64. *Let $d \in \mathbb{Z}$ be squarefree, $K = \mathbb{Q}[\sqrt{d}]$ and $\mathcal{O}_K = \mathbb{Z}[\alpha]$, where α is the generator from Proposition 1.3.37. Then any order in K is of the form $\mathcal{O} = \mathbb{Z}[n\alpha]$ for some $n \in \mathbb{N}$. Moreover, the conductor ideal of $\mathcal{O}$ is the principal ideal $n\mathcal{O}_K$. We will often refer to such $n \in \mathbb{N}$ as the* **index** *of $\mathcal{O}$.*

Note that in the quadratic case, an order can be determined solely by its conductor ideal. However, this will not be true in general.

Example 1.3.65. Let $K = \mathbb{Q}[\sqrt[3]{2}]$. Then $\mathcal{O}_K = \mathbb{Z}[\sqrt[3]{2}]$, and the orders $\mathcal{O}_1 = \mathbb{Z} + n\sqrt[3]{2}\mathbb{Z} + n^2\sqrt[3]{4}\mathbb{Z}$, $\mathcal{O}_2 = \mathbb{Z} + n^2\sqrt[3]{2}\mathbb{Z} + n\sqrt[3]{4}\mathbb{Z}$, and $\mathcal{O}_3 = \mathbb{Z} + n^2\sqrt[3]{2}\mathbb{Z} + n^2\sqrt[3]{4}\mathbb{Z}$ in K all have the same conductor ideal, namely $n^2\mathcal{O}_K$.

To conclude this discussion, we present the following theorem of Halter-Koch [10], which serves as a basis for much of the work presented in the following chapters. This result demonstrates how we may use what we know about factorization in a ring of algebraic integers and extend that knowledge to orders, which we know comparatively little about. It should be noted that in this theorem, we will use the notation that will be used throughout the rest of this dissertation; namely, we will denote an order in a number field by R and the ring of algebraic integers $\mathcal{O}_K$ by $\overline{R}$.

Theorem 1.3.66. *Let $d \in \mathbb{Z}$ be squarefree and $K = \mathbb{Q}[\sqrt{d}]$ the quadratic number field defined by d. Let $R = \mathbb{Z}[n\alpha]$ be the index $n \in \mathbb{N}\backslash\{1\}$ order in K, where $\alpha = \sqrt{d}$ if $d \equiv 2, 3 \pmod 4$ or $\alpha = \frac{1+\sqrt{d}}{2}$ if $d \equiv 1 \pmod 4$ so that $\overline{R} = \mathbb{Z}[\alpha]$. Then R is an HFD if and only if the following properties hold:*

1. *$\overline{R}$ is an HFD;*

2. *$\overline{R} = R \cdot U(\overline{R})$;*

3. *$n = p$ for some prime $p \in \mathbb{N}$, or $n = 2p$ for some odd prime $p \in \mathbb{N}$.*

Chapter 2

Associated Subrings and Related Properties

As explored throughout the introduction, certain mathematical objects are much more well understood than others. For instance, the structure in a ring of algebraic integers has been studied in great detail. We know that such a ring is Dedekind, has a free abelian additive group of known rank, and admits algorithms for explicitly finding the prime ideals and elasticity, among other nice properties. However, there are other types of rings about which we know relatively little of the factorization properties. Even orders in an algebraic number field, which possess a great deal of structure themselves and are closely related to number rings, do not have a simple, known algorithm for determining elasticity. One might ask, then, if we can leverage our knowledge about these well-understood rings to grant insight into the properties of their subrings. This chapter will explore this question, first exploring the relationships that might be present between a ring and its subring, then seeing how these relationships can be leveraged to provide information. In the next chapter, we will specifically apply these results to the question of elasticity.

2.1 Associated and Ideal-Preserving Subrings

Recall Theorem 1.3.66 from the previous chapter [10]:

Theorem 1.3.66. *Let $d \in \mathbb{Z}$ be squarefree and $K = \mathbb{Q}[\sqrt{d}]$ the quadratic number field defined by d. Let $R = \mathbb{Z}[n\alpha]$ be the index $n \in \mathbb{N}\backslash\{1\}$ order in K, where $\alpha = \sqrt{d}$ if $d \equiv 2, 3 \pmod 4$ or $\alpha = \frac{1+\sqrt{d}}{2}$ if $d \equiv 1 \pmod 4$ so that $\overline{R} = \mathbb{Z}[\alpha]$. Then R is an HFD if and only if the following properties hold:*

1. *$\overline{R}$ is an HFD;*

2. *$\overline{R} = R \cdot U(\overline{R})$;*

3. *$n = p$ for some prime $p \in \mathbb{N}$, or $n = 2p$ for some odd prime $p \in \mathbb{N}$.*

Among these three properties, easily the least explored is the second, $\overline{R} = R \cdot U(\overline{R})$. In fact, it is difficult to find any mention of this property or anything similar before the work of Halter-Koch. In the years since, this property has largely only been explored within the context of HFD orders in algebraic number fields, and not in-depth as a standalone property. In this chapter, we will explore a more general version of this property. We will also consider related properties and how they may apply in particular settings.

We start with the following definition:

Definition 2.1.1. Let T be a commutative ring with unity and $R \subseteq T$ a subring (not necessarily with unity). We say that R is an **associated subring** of T if $T = R{\cdot}U(T)$; that is, if for any $t \in T$, there exist $r \in R$ and $u \in U(T)$ such that $t = ru$.

The following examples illustrate what such rings may look like. To start, we have three trivial examples.

Example 2.1.2. Any commutative ring with identity T is an associated subring of itself. Let T be any field and R any nonzero subring of T. Then R is an associated subring of T. Let R be an associated subring of a ring T, and let S be any subring of T containing R. Then S is an associated subring of T.

Example 2.1.3. Let $R = \mathbb{Z}[\sqrt{5}]$ and $T = \overline{R} = \mathbb{Z}[\frac{1+\sqrt{5}}{2}]$. Then $u = \frac{1+\sqrt{5}}{2} \in U(T)$, and any element of T is of the form $t = a + b\frac{1+\sqrt{5}}{2}$. If b is even, then $t \in R$; if a is even, then $t = ru$ for some $r \in R$; if a and b are of the same parity, then $t = ru^2$ for some $r \in R$. Then R is an associated subring of T. Note that in this case, R is actually an HFD by Theorem 1.3.66.

Example 2.1.4. Let $m, n \in \mathbb{N}$ with $m|n^i$ for some $i \in \mathbb{N}$, and let $T = \mathbb{Z}[\frac{1}{n}]$ and $R = m\mathbb{Z} \subseteq T$. Note that any element of T is of the form $t = \frac{a}{n^k}$ for some $a \in \mathbb{Z}$ and $k \in \mathbb{N}$ (this form not necessarily reduced). Then $t = (n^i a) \cdot \frac{1}{n^{i+k}}$, with $n^i a \in R$ and $\frac{1}{n^{i+k}} \in U(T)$. Then R is an associated subring of T. Note that in this case, for $m \neq 1$, R is a subring without identity.

As the term "associate" is used to refer to a unit multiple of an element in a ring, it should be clear why the term "associated subring" is appropriate for such a subring. It is also worth noting that there are two ways to think of this property. First, as stated above, one can think of "decomposing" an element $t \in T$ into $t = ru$, with $r \in R$ and $u \in U(T)$. On the other hand (and clearly equivalently), one can think of finding an associate $ut \in R$ for any $t \in T$. Though it is immediately obvious that these are equivalent (if $t = ru$, then $u^{-1}t = r \in R$, and vice versa), it will at times be convenient to frame this property in one way or the other.

We now introduce another definition that at first glance seems totally unrelated to the concept of an associated subring. However, we will see in a moment that these concepts are naturally connected.

Definition 2.1.5. Let T be a commutative ring and R a subring (neither assumed to have identity). We say that R is an **ideal-preserving subring** of T if, for any T-ideals $J_1 \not\subseteq J_2$, $R \cap J_1 \not\subseteq J_2$ (equivalently, $R \cap J_1 \not\subseteq R \cap J_2$).

Example 2.1.6. Any commutative ring T is an ideal-preserving subring of itself. Let T be any field and R any nonzero subring of T. Then R is an ideal-preserving subring of T. Let R be an ideal-preserving subring of a ring T, and let S be any subring of T containing R. Then S is an ideal-preserving subring of T.

Again, the term "ideal-preserving" is quite appropriate for such a subring. What this property really says is that two distinct T-ideals will remain distinct (are preserved) when they are restricted to R (and in fact, incomparable ideals remain incomparable).

Proposition 2.1.7. *Let T be a commutative ring with identity and R an associated subring of T. Then R is an ideal-preserving subring of T.*

Proof. Let $J_1 \not\subseteq J_2$ be two T-ideals (note that we can always select two such ideals, since $J_1 = T$ and $J_2 = \{0\}$ will always satisfy this relationship) and take any $t \in J_1 \backslash J_2$. Since R is an associated subring of T, there must be some $u \in U(T)$ such that $ut \in R$. Then note that $ut \in R \cap J_1$. Furthermore, if $ut \in J_2$, then $u^{-1}(ut) = t \in J_2$, a contradiction. Then $R \cap J_1 \not\subseteq J_2$, so R is ideal-preserving. □

As the following example illustrates, the converse of this statement is not necessarily true.

Example 2.1.8. Let $T = \mathbb{Z}[\sqrt{2}]$ and $R = \mathbb{Z}[5\sqrt{2}]$. Then R is not an associated subring of T (in particular, $U(T) = \{\pm(1+\sqrt{2})^k \mid k \in \mathbb{N}\}$, so $1 + 2\sqrt{2} \notin R \cdot U(T)$), but R is an ideal-preserving subring of T. These facts will both be easier to see after developing these ideas further.

2.2 Equivalent Characterizations

Now that the concepts of associated subrings and ideal-preserving subrings have been defined, we will explore some of their equivalent characterizations. For many of these characterizations, we will require additional assumptions about the rings T and R. Throughout this discussion, one should keep in mind Proposition 2.1.7, i.e. that any of the equivalent characterizations of an associated subring implies any of the equivalent characterizations of an ideal-preserving subring.

First, we will see how these properties can be characterized in an integral domain. As we will see, this will illustrate how closely related associated subrings are to ideal-preserving subrings.

Proposition 2.2.1. *Let T be an integral domain and R a subring (possibly without identity) of T. The following are equivalent:*

1. *R is an ideal-preserving subring of T.*
2. *For any T-ideal J and $x \in T$, $x \notin J \implies R \cap (x) \not\subseteq J$.*

Proof. Since T is an integral domain, note that $x \notin J$ is equivalent to $(x) \not\subseteq J$. Then Condition 2 above is simply the standard definition of an ideal-preserving subring, but where J_1 is restricted to being a principal ideal. Then $1 \implies 2$ trivially. To show the converse, let J_1 and J_2 be T-ideals such that $J_1 \not\subseteq J_2$. Then there exists some $x \in J_1 \backslash J_2$. Since $x \notin J_2$, Condition 2 tells us that $R \cap (x) \not\subseteq J_2$. Then there exists $y \in R \cap (x) \subseteq R \cap J_1$ which is not contained in J_2, so $R \cap J_1 \not\subseteq J_2$. Thus, $2 \implies 1$. □

We will now see two equivalent ways to characterize associated subrings of an integral domain. These characterizations will give us an idea of what “extra” we need to produce the converse of Proposition 2.1.7.

Proposition 2.2.2. *Let T be an integral domain and R a subring (possibly without identity) of T. The following are equivalent:*

1. *R is an associated subring of T.*

2. *R is an ideal-preserving subring of T, and for any principal ideal (x) of T and collection of T-ideals $\{I_\alpha\}_{\alpha\in\Gamma}$,*

$$R\cap(x)\subseteq\bigcup_{\alpha\in\Gamma}I_\alpha\iff\exists\,\alpha\in\Gamma\text{ s.t. }R\cap(x)\subseteq I_\alpha.$$

3. *For any $x\in T$ and collection of T-ideals $\{I_\alpha\}_{\alpha\in\Gamma}$,*

$$R\cap(x)\subseteq\bigcup_{\alpha\in\Gamma}I_\alpha\iff\exists\,\alpha\in\Gamma\text{ s.t. }x\in I_\alpha.$$

Proof. We have already seen that any associated subring is ideal-preserving. To complete the proof of $1\implies 2$, assume that R is an associated subring of T. Let (x) be a principal ideal of T and $\{I_\alpha\}_{\alpha\in\Gamma}$ be an arbitrary collection of T-ideals. Then note that if $R\cap(x)\subseteq I_\alpha$ for some $\alpha\in\Gamma$, $R\cap(x)\subseteq\bigcup_{\alpha\in\Gamma}I_\alpha$ trivially. To show the converse, note that since R is an associated subring of T, there is some $u\in U(T)$ such that $ux\in R$. Then $ux\in R\cap(x)\subseteq\bigcup_{\alpha\in\Gamma}I_\alpha$, so $ux\in I_\alpha$ for some $\alpha\in\Gamma$. Then $(x)=(ux)\subseteq I_\alpha$, so $R\cap(ux)\subseteq I_\alpha$. Then $1\implies 2$ (in fact, we have shown that $1\implies 3$ in the process).

We will now show that $2\implies 3$. Let $x\in T$ and $\{I_\alpha\}_{\alpha\in\Gamma}$ be a collection of T-ideals such that $R\cap(x)\subseteq\bigcup_{\alpha\in\Gamma}I_\alpha$. Then Condition 2 tells us that there is some $\alpha\in\Gamma$ such that $R\cap(x)\subseteq I_\alpha$. Then since R is ideal-preserving, $(x)\subseteq I_\alpha$, so $x\in I_\alpha$. Then $2\implies 3$.

All that remains to show is that $3\implies 1$. Let $x\in T$; we want to show that there is some $u \in U(T)$ such that $ux \in R$. Let $\{I_\alpha\}_{\alpha\in\Gamma}$ be the collection of all T-ideals which do not contain x. Then by Condition 3, we have $R \cap (x) \not\subseteq \bigcup_{\alpha\in\Gamma} I_\alpha$. Then there must be some $y \in R \cap (x)$ which is not contained in any I_α. Then since (y) is a T-ideal which contains y, (y) cannot be any of the I_α, i.e. (y) must contain (x). Then $(y) = (x)$, and since T is an integral domain, $y = ux \in R$ for some $u \in U(T)$. Then $3 \implies 1$, completing the proof. □

Note a few things about these conditions. First, if the principal ideal (x) is replaced with a non-principal ideal J, neither Condition 2 nor 3 can ever hold; indeed, we can take the collection $\{(\alpha)\}_{\alpha\in J}$. The union of these ideals will always contain $R \cap J$, but J is not contained in any individual (α). In that sense, the use of principal ideals is not an arbitrary choice, and in fact these are the only ideals with any chance of satisfying these conditions. Next, Condition 2 is primarily presented here to show the relationship between associated subrings and ideal-preserving subrings. It is also presented in a way to illustrate that, just like ideal-preserving subrings, associated subrings can be characterized from a purely ideal-theoretic standpoint. Finally, Condition 3 illustrates that associated subrings are, in a sense, “strongly” ideal-preserving, as Condition 2 from Proposition 2.2.1 is exactly the same statement but without allowing for an arbitrary union.

We will now consider these properties in the realm of Dedekind domains. Since ideals in Dedekind domains can be expressed (uniquely) as a product of prime ideals, we will see in both cases that the ideal-theoretic characterizations can be put in terms of only prime ideals.

Proposition 2.2.3. *Let T be a Dedekind domain and R a subring (possibly without identity) of T. The following are equivalent:*

1. *R is an ideal-preserving subring of T.*

2. *For any nonzero prime T-ideals $P_1 \neq P_2$, $R \cap P_1 \not\subseteq R \cap P_2$ and $R \cap P_1 \neq R \cap P_1^2$.*

Proof. First, note that since T is a Dedekind domain, any two nonzero prime ideals P_1 and P_2 are incomparable and $P_1 \not\subseteq P_1^2$. Then Condition 2 follows immediately from the definition of ideal-preserving subrings, i.e. $1 \implies 2$.

Now assume that condition 2 holds and let $J_1 \not\subseteq J_2$ be two T-ideals. Since T is a Dedekind domain, we can factor these ideals into prime ideals, $J_1 = P_1^{a_1} \dots P_k^{a_k}$ and $J_2 = P_1^{b_1} \dots P_k^{b_k}$. Since $J_1 \not\subseteq J_2$, i.e. $J_2 \nmid J_1$, then $a_i < b_i$ for some $1 \leq i \leq k$. Now note that for $j \neq i$, $R \cap P_j \not\subseteq P_i$; furthermore, $R \cap P_i \not\subseteq P_i^2$. Then select $\alpha_i \in R \cap P_i \backslash P_i^2$, and for $j \neq i$, select $\alpha_j \in R \cap P_j \backslash P_i$. Then $\alpha := \alpha_1^{a_1} \dots \alpha_k^{a_k} \in R \cap P_1^{a_1} \dots P_k^{a_k} = R \cap J_1$. However, $\alpha \notin P_i^{a_i+1} \supseteq P_i^{b_i} \supseteq J_2$, so $\alpha \in R \cap J_1 \backslash J_2$, and thus $R \cap J_1 \not\subseteq J_2$. Then R is ideal-preserving, i.e. $2 \implies 1$. □

Proposition 2.2.4. *Let T be a Dedekind domain and R a subring (possibly without identity) of T. The following are equivalent:*

1. *R is an associated subring of T.*

2. *For any nonzero principal T-ideal $(x) = P_1^{a_1} \dots P_k^{a_k}$,*

$$R \cap (x) \not\subseteq \left(\bigcup_{i=1}^{k} P_i^{a_i+1} \right) \cup \left(\bigcup_{Q \in \operatorname{Spec}(T), Q \nmid (x)} Q \right).$$

Proof. First, assume that R is an associated subring. We will be using the third characterization of associated subrings from Proposition 2.2.2. Note that since x is not contained in any of the prime ideals $Q \nmid (x)$ or $P_i^{a_i+1}$, then $R \cap (x)$ is not contained in the union of these ideals. Then $1 \implies 2$.

Now assume that condition 2 holds. Then let $\{I_\alpha\}_{\alpha \in \Gamma}$ be an arbitrary collection of ideals such that $x \notin I_\alpha$ for every $\alpha \in \Gamma$. Then $I_\alpha \nmid (x)$, so either I_α has too many factors of P_i for some $1 \leq i \leq k$ (i.e. $P_i^{a_i+1}|I_\alpha$) or I_α has a prime divisor which does not divide (x) (i.e. there is some $Q \nmid (x)$ such that $Q|I_\alpha$). In either case, each I_α is contained in the union of ideals in the statement of condition 2. Then

$$R \cap (x) \not\subseteq \left(\bigcup_{i=1}^{k} P_i^{a_i+1} \right) \cup \left(\bigcup_{Q \in \operatorname{Spec}(T), Q \nmid (x)} Q \right) \supseteq \bigcup_{\alpha \in \Gamma} I_\alpha,$$

so $R \cap (x) \not\subseteq \bigcup_{\alpha \in \Gamma} I_\alpha$. Then by Proposition 2.2.2, R is an associated subring of T, so $2 \implies 1$. □

These equivalent conditions allow us to only work with prime ideals in the case of a Dedekind domain. Now, we will see that if the conductor ideal $(R : T)$ is nonzero and R contains 1, we can restrict our consideration to a finite set of prime ideals for ideal-preserving subrings.

Proposition 2.2.5. *Let T be a Dedekind domain and R a subring (with identity) of T such that the conductor ideal $I = (R : T)$ is nonzero. The following are equivalent:*

1. *R is an ideal-preserving subring of T.*

2. *For any prime T-ideals $P_1 \neq P_2$ dividing I, $R \cap P_1 \not\subseteq R \cap P_2$ and $R \cap P_1 \neq R \cap P_1^2$.*

Proof. First, note that Proposition 2.2.3 gives us that any ideal-preserving subring of T satisfies condition 2 for any nonzero prime ideals, not just those dividing I. Then $1 \implies 2$.

For the converse, we will show that condition 2 from Proposition 2.2.3 is always satisfied if either P_1, P_2, or both do not divide I. First, suppose that $P_2 \nmid I$. Then since $I \not\subseteq P_2$, there must exist some $\beta \in I \backslash P_2$. Then letting $\alpha \in P_1 \backslash P_2$, we have that $\alpha\beta \in R \cap P_1 \backslash P_2$, so $R \cap P_1 \not\subseteq R \cap P_2$.

Now assume that $P_1 \nmid I$ but $P_2 \mid I$. Note that P_1 and I are relatively prime in T. Then there must be some $\alpha \in P_1$ and $\beta \in I$ such that $1 = \alpha + \beta$. Then $\alpha = 1 - \beta \in R \cap P_1$. Since $\beta \in I \subseteq P_2$, then $\alpha = 1 - \beta \notin P_2$, i.e. $\alpha \in R \cap P_1 \backslash P_2$. Then $R \cap P_1 \nsubseteq P_2$.

All that remains to show is that if $P_1 \nmid I$, then $R \cap P_1 \neq R \cap P_1^2$. To see this, let $\alpha \in P_1 \backslash P_1^2$ and $\beta \in I \backslash P_1$. Then $\alpha\beta \in R \cap P_1 \backslash P_1^2$, i.e. $R \cap P_1 \neq R \cap P_1^2$. Then $2 \implies 1$. □

Note that with this characterization, it is possible to check only finitely many prime ideals to check whether R is an ideal-preserving subring of T. Returning to Example 2.1.8, one can see that the conductor ideal $I = (R : T) = 5T$, which is prime in T. Then we only need to check that $R \cap 5T = 5T \neq 25T = R \cap (5T)^2$. Then by this new equivalent characterization, R is an ideal-preserving subring of T. This characterization also allows us to easily produce a large class of ideal-preserving subrings of a Dedekind domain T.

Corollary 2.2.6. *Let T be a Dedekind domain and R a subring (with identity) of T such that the conductor ideal $I = (R : T)$ is a nonzero prime ideal of T. Then R is an ideal-preserving subring of T.*

Proof. By the proposition, note that since I only has a single prime divisor, the only check that must be made is that $R \cap I \neq R \cap I^2$. Since $I^2 \subsetneq I \subsetneq R$, then $R \cap I^2 = I^2 \subsetneq I = R \cap I$. Then R is ideal-preserving. □

Under the assumption that the conductor ideal $I = (R : T)$ is nonzero, we can similarly make it easier to check whether a subring is associated.

Proposition 2.2.7. *Let T be a commutative ring with identity and R a subring (with identity) of T such that the conductor ideal $I = (R : T)$ is nonzero. The following are equivalent:*

1. *R is an associated subring of T.*

2. *For any subset $\{u_\alpha\}_{\alpha \in U(T)/U(R)}$ of $U(T)$ such that u_α is a representative of the coset $\alpha \in {}^{U(T)}\!/_{U(R)}$ and $t \in T$, there exists $\alpha \in {}^{U(T)}\!/_{U(R)}$ and $\beta \in I$ such that $u_\alpha(t+\beta) \in R$. That is, in a slight abuse of notation, ${}^{T}\!/_{I} = {}^{R}\!/_{I} \cdot {}^{U(T)}\!/_{U(R)}$.*

Proof. First, note that if R is an associated subring of T, i.e. $T = R{\cdot}U(T)$, then every $t \in T$ has some $u \in U(T)$ such that $ut \in R$. Then there is some $\alpha \in {}^{U(T)}\!/_{U(R)}$ such that $uv = u_\alpha$ for some $v \in U(R)$. Letting $\beta = 0$, this gives $u_\alpha(t+\beta) = (ut)v \in R$, so $1 \implies 2$.

Now assume that condition 2 holds, and let $t \in T$. Then given any set of coset representatives $\{u_\alpha\}_{\alpha \in U(T)/U(R)}$, there is some u_α and $\beta \in I$ such that $u_\alpha(t+\beta) = r \in R$. Note that since $\beta \in I = (R : T)$, $u_\alpha\beta \in R$ as well. Then $u_\alpha t = r - u_\alpha\beta \in R$, so R is an associated subring. Thus, $2 \implies 1$. □

Although this characterization is not always one which can be checked in finitely many steps, as in Proposition 2.2.5, when R is an order in a number field and $T = \overline{R}$ is the corresponding number ring, ${}^{T}\!/_{I}$, ${}^{R}\!/_{I}$, and ${}^{U(T)}\!/_{U(R)}$ are all finite. Thus, this characterization is able to be finitely checked in this particular case. This can be used to check that the subring in Example 2.1.8 is indeed associated. In this case, we can pick three coset representatives $\{1, 1+\sqrt{2}, 3+2\sqrt{2}\} \subseteq U(T)$ and the element $t = 1+2\sqrt{2}$ and verify that none of these units multiply t into R. Then R is not an associated subring of T, since $1+2\sqrt{2} \in T \backslash R \cdot U(T)$.

It is also worth noting that the last two propositions, which assume that $I = (R : T)$ is a nonzero ideal, technically hold when $I = \{0\}$ as well. However, if $I = \{0\}$, then every nonzero prime T-ideal divides (contains I) and ${}^{T}\!/_{I} \cong T$, so nothing new is really being presented.

Since the primary context of interest for this dissertation is still in the realm of orders in algebraic number fields, we note that all of these results will hold when R is an order in a number field and $T = \overline{R}$. Then we combine these propositions to get the following theorems. For ease, we will also include an additional characterization of ideal-preserving subrings, the discussion and proof of which fits better in the following section.

Theorem 2.2.8. *Let R be an order in a number field K with conductor ideal I. The following are equivalent:*

1. *For any $\overline{R}$-ideals $J_1 \not\subseteq J_2$, $R \cap J_1 \not\subseteq J_2$; that is, R is an ideal-preserving subring of $\overline{R}$.*
2. *For any $\overline{R}$-ideal J and $x \in \overline{R}$, $x \notin J \implies R \cap (x) \not\subseteq J$.*
3. *For any nonzero prime $\overline{R}$-ideals $P_1 \neq P_2$, $R \cap P_1 \not\subseteq P_2$ and $R \cap P_1 \neq R \cap P_1^2$.*
4. *For any prime $\overline{R}$-ideals $P_1 \neq P_2$ dividing I, $R \cap P_1 \not\subseteq R \cap P_2$ and $R \cap P_1 \neq R \cap P_1^2$.*
5. *If $I = P_1^{a_1} \dots P_k^{a_k}$ is the factorization of I into prime $\overline{R}$-ideals, then $R \cap P_i \neq R \cap P_i^2$ for $1 \leq i \leq k$ and*

$$R/I \cong R/R \cap P_1^{a_1} \times \cdots \times R/R \cap P_k^{a_k} \cong R + P_1^{a_1}/P_1^{a_1} \times \cdots \times R + P_k^{a_k}/P_k^{a_k}.$$

For simplicity, we will refer to any such order as an **ideal-preserving order***.*

Theorem 2.2.9. *Let R be an order in a number field K. The following are equivalent:*

1. *$\overline{R} = R \cdot U(\overline{R})$; that is, R is an associated subring of $\overline{R}$.*

2. *R is an ideal-preserving order, and for any principal ideal (x) of $\overline{R}$ and collection of $\overline{R}$-ideals $\{I_\alpha\}_{\alpha\in\Gamma}$,*

$$R \cap (x) \subseteq \bigcup_{\alpha\in\Gamma} I_\alpha \iff \exists\, \alpha \in \Gamma \text{ s.t. } R \cap (x) \subseteq I_\alpha.$$

3. *For any $x \in \overline{R}$ and collection of $\overline{R}$-ideals $\{I_\alpha\}_{\alpha\in\Gamma}$,*

$$R \cap (x) \subseteq \bigcup_{\alpha\in\Gamma} I_\alpha \iff \exists\, \alpha \in \Gamma \text{ s.t. } x \in I_\alpha.$$

4. *For any nonzero principal $\overline{R}$-ideal $(x) = P_1^{a_1} \dots P_k^{a_k}$,*

$$R \cap (x) \not\subseteq \left(\bigcup_{i=1}^{k} P_i^{a_i+1}\right) \cup \left(\bigcup_{Q\in\operatorname{Spec}(\overline{R}),\, Q\nmid(x)} Q\right).$$

5. *For any subset $\{u_\alpha\}_{\alpha\in U(\overline{R})/U(R)}$ of $U(\overline{R})$ such that u_α is a representative of the coset $\alpha \in {}^{U(\overline{R})}\big/_{U(R)}$ and $t \in \overline{R}$, there exists $\alpha \in {}^{U(\overline{R})}\big/_{U(R)}$ and $\beta \in I$ such that $u_\alpha(t+\beta) \in R$. That is, in a slight abuse of notation, ${}^{\overline{R}}\big/_{I} = {}^{R}\big/_{I} \cdot {}^{U(\overline{R})}\big/_{U(R)}$.*

For simplicity, we will refer to any such order as an **associated order***.*

2.3 Related Rings

In many of the results we will show in the next chapter, it will be necessary to understand how properties of an order R in a number field K can inform us about properties of related orders. To this end, we will now examine how associated or ideal-preserving subrings of a ring T can tell us information about related subrings of T. Throughout this discussion, one should keep in mind Proposition 2.1.7, i.e. that any associated subring is also ideal-preserving. Furthermore, the results presented here will all apply to orders in an algebraic number field.

To start, we will see how a subring $R \subseteq T$ can be built into a larger subring.

Theorem 2.3.1. *Let T be a Dedekind domain and R an ideal-preserving subring (with identity) of T. Let $I = (R : T)$. Then for any T-ideal J, $(R + J : T) = I + J$.*

Proof. First, note that $I + J$ is a T-ideal which divides J, and $R + J = R + (I + J)$. Then it will suffice to show that for any T-ideal J which divides I, the ring $R + J$ has conductor ideal $(R + J : T) = J$.

Now assume that J is a T-ideal dividing I and consider the subring $R + J$ of T. First, note that $J \subseteq R + J$ trivially. Then letting $A = (R + J : T)$, we have that $J \subseteq A$. If $A = J$, then we are done. Otherwise, assume that $J \subsetneq A$. Then $R + J \subseteq R + A \subseteq R + (R + J) = R + J$, so $R + J = R + A$.

Since T is a Dedekind domain, we can now factor ideals into products of prime ideals. Let $I = P_1^{a_1} \dots P_k^{a_k}$. Then $J = P_1^{b_1} \dots P_k^{b_k}$ for some $b_i \leq a_i$ for $1 \leq i \leq k$. Now since R is an ideal-preserving subring of T, we have that for each $1 \leq i \leq k$, $R \cap P_i \not\subseteq R \cap P_i^2$, and for $i \neq j$, $R \cap P_i \not\subseteq R \cap P_j$. Since R has identity, each $R \cap P_i$ remains prime in R, so prime avoidance tells us that for each $1 \leq i \leq k$, there exists some $r_i \in R \cap P_i \backslash \left(P_i^2 \cup \bigcup_{j \neq i} P_j \right)$. Then letting $\beta = \prod_{i=1}^k r_i^{a_i - b_i}$, we have that $\beta \in R$ and $\beta T + I = P_1^{a_1 - b_1} \dots P_k^{a_k - b_k} = (I : J)$.

Now note that $\beta(R + A) = \beta(R + J) = \beta R + \beta J$. Since $\beta \in R$, $\beta R \subseteq R$; since $\beta \in (I : J)$, $\beta J \subseteq I$. Then $\beta(R + A) = \beta R + \beta J \subseteq R + I = R$. Then β conducts any element of $R + A$ into R, i.e. $\beta \in (R : R + A)$. Now since $J \subseteq A$, and $J \neq A$, this means that $A \not\subseteq J$. Since R is an ideal-preserving subring of T, $R \cap A \not\subseteq J$. Then let $\alpha \in R \cap A \backslash J$. Since $(\alpha) \not\subseteq J$, there must be some $1 \leq i \leq k$ such that $P_i^{b_i} \nmid (\alpha)$. Now consider the element $\alpha\beta$. Note that for any $t \in T$, $\alpha t \in A \subseteq R + A$, so $\alpha\beta t = \beta(\alpha t) \in R$. Then $\alpha\beta \in (R : T) = I$, i.e. $I|(\alpha\beta)$. However, note that as there is some $1 \leq i \leq k$ such that $P_i^{b_i} \nmid (\alpha)$ and the exact power of P_i dividing (β) is $P_i^{a_i - b_i}$, $P_i^{a_i} \nmid (\alpha\beta)$, a contradiction. Then the conductor ideal $(R + J : T)$ must be exactly J. □

With this result, we can start by considering a particular ideal-preserving subring R of T and construct intermediate subrings of the form $R + J$ of T, which will still be ideal-preserving. As we will see, especially in the next chapter, breaking down a subring R into these "simpler" components will be very useful when trying to determine the properties of R itself. The following result shows how this "breaking down" process works.

Theorem 2.3.2. *Let R be an order in a number field K and $I = (R : \overline{R})$ its conductor ideal. Let $I = P_1^{a_1} \dots P_k^{a_k}$ be the factorization of I into prime $\overline{R}$ ideals. The following are equivalent:*

1. *R is an ideal-preserving order.*

2. *If $I = P_1^{a_1} \dots P_k^{a_k}$ is the factorization of I into prime $\overline{R}$-ideals, $R \cap P_i \neq R \cap P_i^2$ for $1 \leq i \leq k$ and*

$$R/I \cong R/R \cap P_1^{a_1} \times \cdots \times R/R \cap P_k^{a_k} \cong R + P_1^{a_1}/P_1^{a_1} \times \cdots \times R + P_k^{a_k}/P_k^{a_k}.$$

Proof. Note that when R is ideal-preserving, then $R \cap P_i \neq R \cap P_i^2$ for $1 \leq i \leq k$ by definition. Then for the implication $1 \implies 2$, we only need to show the isomorphism.

First, we will note that the second isomorphism in the statement of condition 2 will always hold. The mapping $f(r + R \cap P_1^{a_1}, \dots, r + R \cap P_k^{a_k}) = (r + P_1^{a_1}, \dots, r + P_k^{a_k})$ makes this straightforward to see. For the first isomorphism, recall by the Chinese

Remainder Theorem that

$$\overline{R}/I \cong \overline{R}/P_1^{a_1} \times \cdots \times \overline{R}/P_k^{a_k}.$$

Now let π be the canonical projection isomorphism $\pi : \overline{R}/I \to \overline{R}/P_1^{a_1} \times \cdots \times \overline{R}/P_k^{a_k}$, and define $\tau : R/I \to R + P_1^{a_1}/P_1^{a_1} \times \cdots \times R + P_k^{a_k}/P_k^{a_k}$ by $\tau(r + I) = \pi(r + I)$. Since τ is defined as a restriction of an isomorphism, we immediately have that τ is an injective homomorphism; then we need only show that τ is also surjective. To show this, we will show that for each $1 \leq i \leq k$, there is some $r_i \in R$ such that $\tau(r_i + I)$ is 0 in every coordinate except the i^{th}, in which it is $1 + P_i^{a_i}$. Since R is ideal-preserving, we have that $R \cap \prod_{j \neq i} P_j^{a_j} \not\subseteq P_i$, so let $x_i \in R \cap \prod_{j \neq i} P_j^{a_j} \backslash P_i$. Note that $\tau(x_i + I)$ is 0 in every coordinate except the i^{th}, though it may not be $1 + P_i^{a_i}$ in the i^{th} coordinate as desired. However, since $\overline{R}/P_i^{a_i}$ is a finite quotient ring and $P_i^{a_i}$ is primary, every element is either a unit or nilpotent. Then since $x_i \notin P_i$, $x_i + P_i^{a_i} \in R + P_i^{a_i}/P_i^{a_i} \cap U(\overline{R}/P_i^{a_i}) = U(R + P_i^{a_i}/P_i^{a_i})$. Then there is some $y_i \in R$ such that $x_i y_i + P_i^{a_i} = 1 + P_i^{a_i}$. Then letting $r_i = x_i y_i$, we have that $\tau(r_i + I)$ is 0 in every coordinate except the i^{th}, in which it is $1 + P_i^{a_i}$. Then τ is surjective, so $1 \implies 2$.

Now assume Condition 2 holds. By Proposition 2.2.5, it will suffice to show that for $i \neq j$, $R \cap P_j \not\subseteq P_i$. Then letting $\tau : R/I \to R/R \cap P_1^{a_1} \times \cdots \times R/R \cap P_k^{a_k}$ be the canonical isomorphism such that $\tau(r + I) = (r_1 + R \cap P_1^{a_1}, \ldots, r_k + R \cap P_k^{a_k})$. Since this is an isomorphism (and is thus surjective), there exists some $r_i \in R$ for each $1 \leq i \leq k$ such that $r_1 + P_i^{a_i} = 1 + P_i^{a_i}$ and $r \in R \cap P_j^{a_j} = 0$ for $j \neq i$. Then this r_i lies in $R \cap P_j \backslash P_i$ for every $j \neq i$. Then for any $i \neq j$, $R \cap P_j \not\subseteq R \cap P_i$, so $2 \implies 1$. □

The above result gives the final characterization of ideal-preserving orders presented in Theorem 2.2.8. This will allow us to utilize techniques similar to the Chinese Remainder Theorem when working with ideal-preserving subrings, which will be very useful to the major results of this dissertation. This will also allow us to show the following result, which gives a view of how we might bring together multiple intermediate orders of the form $R + J$, where J is a T-ideal.

Theorem 2.3.3. *Let T be a Dedekind domain and R an ideal-preserving subring (with identity) of T. Let J_1 and J_2 be two T-ideals dividing $I = (R : T)$, and define $R_1 := R + J_1$ and $R_2 := R + J_2$. Then $R_1 \cap R_2$ is a subring of T such that $R \subseteq R + J_1 \cap J_2 \subseteq R_1 \cap R_2$ and the conductor ideal $(R_1 \cap R_2 : T) = J_1 \cap J_2$. Moreover, if R is an order in a number field and $T = \overline{R}$, $R_1 \cap R_2 = R + J_1 \cap J_2$.*

Proof. First, note that the inclusions $R \subseteq R + J_1 \cap J_2 \subseteq R_1 \cap R_2$ are trivial. This also gives us that $J_1 \cap J_2 \subseteq R_1 \cap R_2$, so $J_1 \cap J_2 \subseteq (R_1 \cap R_2 : T)$. Now from Theorem 2.3.1, we have that $(R_1 : T) = J_1$ and $(R_2 : T) = J_2$. Then for any $\alpha \in (R_1 \cap R_2 : T)$, note that $\alpha T \subseteq R_1 \cap R_2$. Then by definition of the conductor ideal, $\alpha \in J_1$ and $\alpha \in J_2$. Then $\alpha \in J_1 \cap J_2$, so $(R_1 \cap R_2 : T) \subseteq J_1 \cap J_2$. Then $(R_1 \cap R_2 : T) = J_1 \cap J_2$.

All that remains to show is that when R is an order in a number field and $T = \overline{R}$, $R_1 \cap R_2 \subseteq R + J_1 \cap J_2$. To start, note that $R + J_1 \cap J_2$ is an ideal-preserving order with conductor ideal $J_1 \cap J_2$, and $R_i = R + J_i = (R + J_1 \cap J_2) + J_i$ for $i \in \{1, 2\}$. Then without loss of generality, we can assume that $J_1 \cap J_2 = I$.

For now, we will also assume that J_1 and J_2 are relatively prime and show that $R_1 \cap R_2 \subseteq R$. Applying Theorem 2.3.2 first to R, then R_1 and R_2, we get that ${}^{R}\!/_{I} \cong {}^{R_1}\!/_{J_1} \times {}^{R_2}\!/_{J_2}$. Then letting $t \in R_1 \cap R_2$ and $\tau : {}^{R}\!/_{I} \to {}^{R_1}\!/_{J_1} \times {}^{R_2}\!/_{J_2}$, there must be some $r \in I$ such that $\tau(r + I) = (r + J_1, r + J_2) = (t + J_1, t + J_2)$. Then $r - t \in J_1 \cap J_2 = I$, so $t = r + \beta \in R$ for some $\beta \in I$. Then $R_1 \cap R_2 \subseteq R$.

We will now show that when $J_1 \cap J_2 = I$, $R_1 \cap R_2 \subseteq R$ even when J_1 and

J_2 are not relatively prime. Write $I = P_1^{a_1} \dots P_k^{a_k}$, where each P_i is a prime $\overline{R}$-ideal. Then since $J_1 \cap J_2 = I$, we can write $J_1 = P_1^{b_1} \dots P_k^{b_k}$ and $J_2 = P_1^{c_1} \dots P_k^{c_k}$, with $a_i = \max\{b_i, c_i\}$ for $1 \leq i \leq k$. Now let $t \in R_1 \cap R_2$. Since $R_1 \subseteq R + P_i^{b_i}$ and $R_2 \subseteq R + P_i^{c_i}$ for each $1 \leq i \leq k$, we have that $t \in (R + P_i^{b_i}) \cap (R + P_i^{c_i}) = R + P_i^{a_i}$ for each $1 \leq i \leq k$. Then by the relatively prime case above, $t \in \bigcap_{i=1}^{k}(R + P_i^{a_i}) = R$. Then $R_1 \cap R_2 \subseteq R$, completing the proof. $\square$

The results thus far show how an ideal-preserving subring R of a Dedekind domain T (or more specifically, an order in a number field) relate to rings of the form $R + J$, with J an ideal of T. In other words, we are constructing intermediate subrings S with $R \subseteq S \subseteq T$. However, we can also examine how properties might be "inherited" when moving to a smaller subring $S \subseteq R \subseteq T$, as the following results will demonstrate.

Theorem 2.3.4. *Let R_1 and R_2 be two subrings of the same commutative ring with unity T, and let $J_1 = (R_1 : T)$ and $J_2 = (R_2 : T)$. Then $R := R_1 \cap R_2$ is a subring of T with conductor ideal $I = (R : T) = J_1 \cap J_2$. Moreover, if R_1 and R_2 are orders in a number field, $T = \overline{R_1} = \overline{R_2} = \overline{R}$, and J_1 and J_2 are relatively prime as $\overline{R}$-ideals, then $R_1 = R + J_1$, $R_2 = R + J_2$, and*

$$R/I \cong R_1/J_1 \times R_2/J_2.$$

Proof. Let $I = (R : T)$. Then $I \subseteq R = R_1 \cap R_2$, so I is contained in both R_1 and R_2. Then since I is a T-ideal contained in these subrings, it is contained in the conductor ideals $J_1 = (R_1 : T)$ and $J_2 = (R_2 : T)$, i.e. $I \subseteq J_1 \cap J_2$. On the other hand, $J_1 \cap J_2 \subseteq R_1 \cap R_2 = R$, so $J_1 \cap J_2$ must be contained in $(R : T) = I$. Then $J_1 \cap J_2 \subseteq I$, so $I = J_1 \cap J_2$.

We will now assume that R_1 and R_2 are orders in the same number field K, and T is the ring of algebraic integers; equivalently, $T = \overline{R_1} = \overline{R_2} = \overline{R}$. Furthermore, we will assume that J_1 and J_2 are relatively prime $\overline{R}$-ideals. Now consider $\tau : {}^{R}\!/\!{}_{I} \to {}^{R_1}\!/\!{}_{J_1} \times {}^{R_2}\!/\!{}_{J_2}$ defined by $\tau(r+I) = (r+J_1, r+J_2)$. Since $R = R_1 \cap R_2$ and $I = J_1 \cap J_2$, this is a well-defined homomorphism. Furthermore, if $\tau(r+I) = (0+J_1, 0+J_2)$, then $r \in J_1 \cap J_2 = I$, i.e. $r + I = 0 + I$. Then τ is an injective homomorphism. Now let $r_1 \in R_1$ and $r_2 \in R_2$. By the Chinese Remainder Theorem, we know that there must exist some $r \in \overline{R}$ such that $r \equiv r_1 \pmod{J_1}$ and $r \equiv r_2 \pmod{J_2}$, i.e. $r - r_1 \in J_1$ and $r - r_2 \in J_2$. Then $r \in R_1 \cap R_2 = R$, so $r + I \in {}^{R}\!/\!{}_{I}$ is such that $\tau(r+I) = (r_1+J_1, r_2+J_2)$. Therefore, τ is surjective and thus an isomorphism. Note that this also tells us that for any $r_1 \in R_1$, there is some $r \in R$ such that $r_1 = r + \beta_1$ for some $\beta_1 \in J_1$, i.e. $R_1 \subseteq R + J_1$ (and by a similar argument, $R_2 \subseteq R + J_2$). The reverse inclusions are immediate, so $R_1 = R + J_1$, $R_2 = R + J_2$, and ${}^{R}\!/\!{}_{I} \cong {}^{R_1}\!/\!{}_{J_1} \times {}^{R_2}\!/\!{}_{J_2}$. □

In this result, the assumption that J_1 and J_2 are relatively prime is actually important to showing that descending in this manner is possible. The following example illustrates how this may fail in general.

Example 2.3.5. Let $K = \mathbb{Q}[\sqrt[3]{2}]$. Since the polynomial $x^3 - 2$ has no roots modulo 7, note that 7 is an inert prime in K, i.e. (7) is a prime ideal in the ring of integers $\mathcal{O}_K = \mathbb{Z}[\sqrt[3]{2}]$ of K. Then let $R_1 = \mathbb{Z} + 7\sqrt[3]{2}\mathbb{Z} + \sqrt[3]{4}\mathbb{Z}$ and $R_2 = \mathbb{Z} + \sqrt[3]{2}\mathbb{Z} + 7\sqrt[3]{4}\mathbb{Z}$; these are both orders in K. Note that since these are properly contained inside $\mathcal{O}_K$ and (7) is contained in both of these orders, then $J_1 = J_2 = (7)$ (since (7) is prime and therefore maximal in $\mathcal{O}_K$). By the theorem, $R := R_1 \cap R_2 = \mathbb{Z} + 7\sqrt[3]{2}\mathbb{Z} + 7\sqrt[3]{4}\mathbb{Z}$ is an order in K with conductor ideal $I = J_1 \cap J_2 = (7)$ (this is also easy to verify independently of the result). However, $R + J_1 = R \neq R_1$ and $R + J_2 = R \neq R_2$. Furthermore, $\left|{}^{R}\!/\!{}_{I}\right| = 7$ and $\left|{}^{R_1}\!/\!{}_{J_1}\right| = \left|{}^{R_2}\!/\!{}_{J_2}\right| = 49$, so $\left|{}^{R}\!/\!{}_{I}\right| = 7 \neq 49^2 = \left|{}^{R_1}\!/\!{}_{J_1} \times {}^{R_2}\!/\!{}_{J_2}\right|$. In particular, this means that these rings are not isomorphic.

Using these results, we can now start with two subrings of a commutative ring and determine properties of their intersection. In the case of orders in a number field, these larger orders will often be easier to work with, allowing us to start with large, simple orders, then extend their properties to their intersections, which may be more complex. A natural question to ask, then, is which properties will be "inherited" when such an intersection is considered. As the following result shows, the property of being an ideal-preserving subring is "nice" in the sense that it is easily inherited in this way.

Theorem 2.3.6. *Let R_1 and R_2 be two ideal-preserving subrings (with unity) of the same Dedekind domain T, and let $J_1 = (R_1 : T)$ and $J_2 = (R_2 : T)$ be relatively prime as T-ideals. Then $R = R_1 \cap R_2$ is an ideal-preserving subring of T.*

Proof. First, note by Theorem 2.3.4, R is a subring of T with conductor ideal $I = (R : T) = J_1 \cap J_2 = J_1 J_2$. If either J_1 or J_2 is the zero ideal, then note that the other must be T, as $J_1 + J_2 = T$. Without loss of generality, assume $R_2 = T$. Then $R = R_1 \cap R_2 = R_1$, which is an ideal-preserving subring of T. From this point, we will assume that J_1 and J_2 are relatively prime nonzero T-ideals. Thus, we can factor J_1 and J_2 into products of prime T-ideals, and any prime dividing J_1 cannot divide J_2 (and vice versa).

Since $R = R_1 \cap R_2$ is contained in both R_1 and R_2, then if R is an ideal-preserving subring of T, R_1 and R_2 will both be ideal-preserving trivially. On the other hand, suppose that R_1 and R_2 are both ideal-preserving. To show that R is ideal-preserving, Proposition 2.2.5 tells us that it will suffice to show that any distinct prime T-ideals dividing $I = J_1 J_2$ remain distinct from each other and from their squares when restricting to R.

Let P be a prime T-ideal dividing I. Then P must divide exactly one of J_1 or J_2; without loss of generality, suppose $P|J_1$. Then since R_1 is ideal-preserving, select $\alpha \in R_1 \cap P\backslash P^2$ and $\beta \in R_1 \cap J_2\backslash P$. Then $\alpha\beta \in R_1 \cap J_2 \subseteq R_1 \cap R_2 = R$, and $\alpha\beta \in P\backslash P^2$. Then $R \cap P \not\subseteq R \cap P^2$.

Now suppose that we have distinct prime T-ideals $P_1 \neq P_2$, both of which divide I. Again, each of these primes must divide either J_1 or J_2 but not both. Without loss of generality, assume that $P_1|J_1$. If $P_2|J_1$, then we can proceed similarly to the previous case. Since R_1 is ideal preserving, we can select $\alpha \in R_1 \cap P_1\backslash P_2$ and $\beta \in R_1 \cap J_2\backslash P_2$. Then $\alpha\beta \in R_1 \cap J_2 \subseteq R$ and $\alpha\beta \in P_1\backslash P_2$, so $R \cap P_1 \not\subseteq P_2$. If $P_2|J_2$, we will instead make use of the fact that R_2 is ideal-preserving. In this case, select $\alpha \in R_2 \cap P_1\backslash P_2$ and $\beta \in R_2 \cap J_1\backslash P_2$. Then $\alpha\beta \in R_2 \cap J_1 \subseteq R$ and $\alpha\beta \in P_1\backslash P_2$, so $R \cap P_1 \not\subseteq P_2$. Thus, R is an ideal-preserving subring of T. □

This result shows that the property of being an ideal-preserving subring is "inherited" when intersecting subrings in a Dedekind domain with relatively prime conductor ideals. While this may seem like a very specific case, this will be very useful when looking for ideal-preserving orders in a number field. The following example shows that the property of being an associated subring is not so nicely inherited, even within the context of orders in a number field.

Example 2.3.7. Let $R_1 = \mathbb{Z}[3\sqrt{2}]$, $R_2 = \mathbb{Z}[11\sqrt{2}]$, and $T = \overline{R} = \mathbb{Z}[\sqrt{2}]$. It can be verified that R_1 and R_2 are both associated subrings of T (in particular, one can use the characterization from Proposition 2.2.7). However, $R = R_1 \cap R_2 = \mathbb{Z}[33\sqrt{2}]$ is not an associated subring. This can be verified by finding an element of $T\backslash R \cdot U(T)$, but an easier method of showing this will be developed later.

2.4 Locally Associated Subrings

The final property that we will explore in this section is also closely related to the idea of an associated subring. This property is presented here, separately from the others, primarily since its utility at present is largely restricted to the context of orders in a number ring.

Definition 2.4.1. Let T be a commutative ring with identity, $R \subseteq T$ a subring (with identity) of T, and $I := (R : T)$. We say that R is a **locally associated subring** of T if

$$U(T)\big/U(R) \cong U(T/I)\big/U(R/I).$$

Note that as with some alternate characterizations of associated or ideal-preserving subrings, this property only really makes sense to consider when $I = (R : T) \neq \{0\}$ (from the definition, any subring R with $I = (R : T) = \{0\}$ is immediately locally associated). As the name suggests, locally associated subrings are very closely related to associated subrings. While this may not be immediately obvious from the definition presented here, it will become apparent after the following discussion.

First, we present an equivalent characterization of a locally associated subring that will help to illustrate the relation to associated subrings.

Proposition 2.4.2. *Let T be a commutative ring with unity, $R \subseteq T$ a subring (with unity) of T, and $I := (R : T)$. The following are equivalent:*

1. *R is a locally associated subring of T.*

2. *Every coset in $U(T/I)\big/U(R/I)$ contains a unit in T; that is, for any $t + I \in U(T/I)$, there exists some $r + I \in U(R/I)$ and $\beta \in I$ such that $tr + \beta \in U(T)$.*

3. If $t \in T$ is relatively prime to I, i.e. $tT + I = T$, then there exists $r \in R$ relatively prime to I, i.e. $rR + I = R$, and $u \in U(T)$ such that $t = ru$.

Proof. First, we will consider in general the map $\phi : U(T) \to {}^{U(T/I)}/_{U(R/I)}$ defined by $\phi(u) = (u + I)U({}^{R}/I)$. It is trivial to see that ϕ is a well-defined (multiplicative group) homomorphism. Suppose that $u \in U(R)$; then note that $u + I \in U({}^{R}/I)$, so $\phi(u) = (1 + I)U({}^{R}/I)$. Then $U(R) \subseteq \ker(\phi)$. On the other hand, suppose that $u \in \ker(\phi)$, i.e. $\phi(u) = (1 + I)U({}^{R}/I)$. Then there is some $r + I \in U({}^{R}/I)$ such that $u+I = r+I$, so $u \in R$. Furthermore, note that since $u \in U(T)$, then u^{-1} exists in T, and thus $\phi(u^{-1}) = \phi(u^{-1})\phi(u) = \phi(uu^{-1}) = \phi(1) = (1 + I)U({}^{R}/I)$. Then as before, $u^{-1} \in R$, so $u \in U(R)$. Then $\ker(\phi) = U(R)$, so by the first isomorphism theorem, ${}^{U(T)}/_{U(R)} \cong \phi(U(T))$.

Since $\phi(U(T))$ is a subgroup of ${}^{U(T/I)}/_{U(R/I)}$, the above discussion tells us that R is a locally associated subring of T if and only if ϕ is onto. Furthermore, condition 2 above is equivalent to ϕ being onto; to illustrate this, suppose that ϕ is onto. Then for every $t + I \in U({}^{T}/I)$, there is some $u \in U(T)$ such that $\phi(u) = (u + I)U({}^{R}/I) = (t+I)U({}^{R}/I)$. Then there exists $r+I \in U({}^{R}/I)$ such that $u+I = (t+I)(r+I) = tr+I$, and thus there is some $\beta \in I$ such that $tr + \beta = u \in U(T)$. The converse follows by reversing this same argument. Then $1 \iff 2$.

Now to show that $2 \iff 3$, note that $t \in T$ is relatively prime to I, i.e. $tT + I = T$, if and only if $t + I \in U({}^{T}/I)$ (similarly, $rR + I = R$ if and only if $r + I \in U({}^{R}/I)$). Then assuming Condition 2, let $t \in T$ be relatively prime to I. Condition 2 tells us that there is some $r + I \in U({}^{R}/I)$ and $\beta \in I$ such that $tr + \beta = u \in U(T)$. Letting $s \in R$ such that $s + I = (r + I)^{-1} \in U({}^{R}/I)$, this gives us that $t = us + \beta'$ for some $\beta' \in I$, and thus $t = (s + \beta' u^{-1})u$. Then $2 \implies 3$.

Finally, assume that Condition 3 holds and let $t + I \in U({}^{T}/I)$. Since $t \in T$

is relatively prime to I, Condition 3 tells us that there exist $s \in R$ relatively prime to I and $u \in U(T)$ such that $t = su$. Then letting $r + I = (s + I)^{-1} \in U({}^{R}\!/_{I})$, we have $tr + I = u + I$, i.e. there is some $\beta \in I$ such that $tr + \beta = u \in U(T)$. Then $3 \implies 2$. $\square$

Note that this third characterization of locally associated subrings shows the relationship to associated subrings. Namely, rather than every element of T having an associate which lies in R, every element of T relatively prime to I has an an associate which lies in R and remains relatively prime to I. Interestingly, this leaves open the possibility of a subring being associated without being locally associated, as the following example shows.

Example 2.4.3. Let $T = \mathbb{Q}[x]$ and $R = \mathbb{Z} + \mathbb{Z}x + x^2\mathbb{Q}[x] \subseteq T$. Note that in this case, $I = (R : T) = x^2T$. Now let $t = \frac{r_0}{s_0} + \frac{r_1}{s_1}x + \cdots + \frac{r_n}{s_n}x^n \in T$, with $r_i, s_i \in \mathbb{Z}$, $s_i \neq 0$ for $0 \leq i \leq n$. Then we have that

$$t = (r_0s_1 + r_1s_0x + \cdots + \frac{r_ns_0s_1}{s_n}x^n) \cdot \frac{1}{s_0s_1} \in R \cdot U(T).$$

Then R is an associated subring of T. However, R is not a locally associated subring of T. To see this, let $t = 2+3x \in R \subseteq T$ and note that $(2+3x)(\frac{1}{2} - \frac{3}{4}x) \equiv 1 \pmod{I}$, so $t + I \in U({}^{T}\!/_{I})$. However, note that any element of $U({}^{R}\!/_{I})$ must have a constant term of ± 1. Then for any $u \in U(T) = \mathbb{Q}$, $ut = 2u + 3ux \in U({}^{R}\!/_{I}) \implies u = \pm\frac{1}{2}$, but $3u = \pm\frac{3}{2} \notin \mathbb{Z}$. Then $t \in T$ is relatively prime to I, but has no associates which lie in R and are relatively prime to I, so R is not a locally associated subring of T.

Despite this example, in many cases (in particular, when R is an order in a number field and $T = \overline{R}$), a subring being associated will imply that it is also locally associated. In fact, an immediate result follows from the characterizations presented in Proposition 2.4.2.

Corollary 2.4.4. *Let T be a commutative ring with unity, $R \subseteq T$ a subring (with unity) of T, and $I := (R : T)$. Also assume that $U(R/I) = R/I \cap U(T/I)$, i.e. any element of R which has an inverse modulo I in T has that inverse also lying in R. Then if R is an associated subring of T, it is a locally associated subring of T. In particular, this will hold when T is integral over R.*

Proof. Let $R \subseteq T$ be as described above, and assume that R is an associated subring of T. Then for any $t + I \in U(T/I)$, there is some $u \in U(T)$ such that $tu \in R$. Then since $tu + I \in R/I \cap U(T/I) = U(R/I)$, there is some $r + I \in U(R/I)$ such that $tur \equiv 1 \pmod{I}$. Then for some $\beta \in I$, $tr + \beta = u^{-1} \in U(T)$. Then R is a locally associated subring.

Note that when T is integral over R, T/I is integral over R/I. Then in this case, $U(R/I) = R \cap U(T/I)$, as discussed in Proposition 1.2.59. □

It will often be the case that it will be easier to check that a subring is locally associated than to check if it is associated (this will be especially true in the case of orders in a number field, as we will see in a moment). The following result shows that in some cases, it is sufficient to show that a subring is locally associated to show that it is also associated.

Proposition 2.4.5. *Let T be a commutative ring with unity, $R \subseteq T$ a subring (with unity) of T, and $I := (R : T)$. Also assume that I is a maximal T-ideal. Then if R is a locally associated subring of T, it is also an associated subring of T.*

Proof. Let $t \in T$. If $t \notin I$, then I being maximal means that t is relatively prime to I. Then since R is a locally associated subring of T, there is some $u \in U(T)$ such that $ut \in R$. Otherwise, $t \in I$, in which case $ut \in I \subseteq R$ for every $u \in U(T)$. Then $t \in R \cdot U(T)$, so R is an associated subring of T. □

We will now turn our attention to this property in orders of algebraic number fields. In this context, we have the following well-known result found in [16] that provided the original motivation for the definition of locally associated subrings.

Proposition 2.4.6. *Let R be an order in a number field K with conductor ideal I. Then there is an exact sequence*

$$1 \to U(R) \to U(\overline{R}) \times U({}^{R}/_{I}) \to U({}^{\overline{R}}/_{I}) \to \mathrm{Cl}(R) \to \mathrm{Cl}(\overline{R}) \to 1.$$

Thus, the class numbers $\left|\mathrm{Cl}(R)\right|$ and $\left|\mathrm{Cl}(\overline{R})\right|$ are related as follows:

$$\left|\mathrm{Cl}(R)\right| = \left|\mathrm{Cl}(\overline{R})\right| \frac{\left|U({}^{\overline{R}}/_{I})\right|}{\left|U({}^{R}/_{I})\right| \cdot \left|{}^{U(\overline{R})}/_{U(R)}\right|}.$$

A detailed proof of this result can be found in [14]. It should be noted that since R is an order in a number field, ${}^{\overline{R}}/_{I}$, ${}^{R}/_{I}$, and $\mathrm{Cl}(\overline{R})$ are finite; from this result, we also get that $\mathrm{Cl}(R)$ and ${}^{U(\overline{R})}/_{U(R)}$ are finite as well. This exact sequence and subsequent relation between the sizes of $\mathrm{Cl}(R)$ and $\mathrm{Cl}(\overline{R})$ have been used a great deal, including in [4] and [20]; we will discuss this latter paper in greater detail in the subsequent chapters.

From this result, we get the following equivalent definitions of locally associated subrings in the context of orders in a number field.

Corollary 2.4.7. *Let R be an order in a number field K with conductor ideal I. The following are equivalent:*

1. *R is a locally associated subring of $\overline{R}$.*
2. $\left|{}^{U(\overline{R})}/_{U(R)}\right| = \frac{\left|U({}^{\overline{R}}/_{I})\right|}{\left|U({}^{R}/_{I})\right|}$.
3. $\left|\mathrm{Cl}(\overline{R})\right| = \left|\mathrm{Cl}(R)\right|$.

4. $\mathrm{Cl}(\overline{R}) \cong \mathrm{Cl}(R)$.

For convenience, we will call any order satisfying these properties a **locally associated order**.

Proof. Recall from the proof of Proposition 2.4.2 that there is an injective homomorphism $\phi : {}^{U(\overline{R})}\!/_{U(R)} \to {}^{U(\overline{R}/I)}\!/_{U(R/I)}$. Furthermore, from the exact sequence above, we know that there is a surjective homomorphism $\tau : \mathrm{Cl}(R) \to \mathrm{Cl}(\overline{R})$. Since the domains and codomains of ϕ and τ are all finite groups, ϕ and τ are isomorphisms if and only if the orders of their domains and codomains are equal. Thus, $1 \iff 2$ and $3 \iff 4$. Finally, $2 \iff 3$ follows immediately from the proposition. □

These equivalent characterizations of locally associated orders, particularly condition 2, make this a useful type of order to study. First, the structures of orders in a number field make this second condition particularly simple to check, as everything involved is a well-understood finite quantity. Moreover, it gives us a way to count units and determine how they must be distributed modulo I, which will be useful in some of the arguments found in Chapter 4.

Finally, we present some concluding results on locally associated subrings, which will, in part, describe how this property interacts with related subrings and the other two properties discussed earlier.

Theorem 2.4.8. *Let T be a commutative ring with unity, $R \subseteq T$ a subring (with unity) of T, and $I = (R : T)$. Also assume that I is contained in some unique maximal T-ideal M. Then if R is a locally associated subring of T, any subring S of T with $R \subseteq S \subseteq T$ is also a locally associated subring of T. In particular, this will hold when T is Dedekind and $I = P^n$ for some prime T-ideal P and $n \in \mathbb{N}$.*

Proof. First, let $J = (S : T)$ and note that $I \subseteq J$. Then if J is contained in a maximal ideal N, $I \subseteq J \subseteq N \implies N = M$. Then either $J = S = T$, in which case S is trivially a locally associated subring of T, or J is also contained in only the maximal ideal M. Then note that an element $t \in T$ is relatively prime to I if and only if it is relatively prime to J if and only if it lies outside M. Then for any $t \in T$, we know that there is some $u \in U(T)$ and $r \in R$ relatively prime to I for which $t = ru$. Then since $r \in R \subseteq S$ and is also relatively prime to J, we have that S is also a locally associated subring of T. □

Unlike associated and ideal-preserving subrings, locally associated subrings do not pass on their defining property in general to intermediate subrings, as the following example illustrates.

Example 2.4.9. Let $T = \mathbb{Q}[x]$ and $R = \mathbb{Z}[x]$. Note that $I = (R : T) = \{0\}$, so R is trivially a locally associated subring of T. Let $S = \mathbb{Z} + \mathbb{Z}x + x^2\mathbb{Q}[x]$, and note that $R \subseteq S \subseteq T$. However, recall from Example 2.4.3 that S is not a locally associated subring of T.

Even though this property is not inherited by intermediate subrings in general, we can use Corollary 2.4.7 to show that such inheritance does hold in the realm of orders in a number field. First, we require the following lemmas, both from [4].

Lemma 2.4.10. *Let R be an order in a number field K with conductor ideal I. Then any R-ideal which is relatively prime to I is invertible. That is, if J is an ideal in R such that $J + I = R$, then $JJ^{-1} = R$, with $J^{-1} = \{\alpha \in K | \alpha J \subseteq R\}$.*

Lemma 2.4.11. *Let R be an order in a number field K and J an ideal in R. Then every ideal class in $\mathrm{Cl}(R)$ contains a representative which is an integral ideal of R that is relatively prime to J. That is, for any invertible $A \in \mathrm{Inv}(R)$, there exists $\alpha \in K$ such that $\alpha A \subseteq R$ and $\alpha A + J = R$.*

Theorem 2.4.12. *Let R be an order in a number field K with conductor ideal I, and let S be an intermediate order, $R \subseteq S \subseteq \overline{R}$. Then the mapping $\phi : \mathrm{Cl}(R) \to \mathrm{Cl}(S)$ such that $\phi([J]) = [JS]$ is a surjective homomorphism.*

Proof. First, note that ϕ is well-defined. If $[J_1] = [J_2]$ for two invertible fractional R-ideals J_1 and J_2, then $J_1 = \alpha J_2$ for some $\alpha \in K$. Thus, $J_1S = \alpha J_2S$, so $\phi([J_1]) = [J_1S] = [J_2S] = \phi([J_2])$. Furthermore, ϕ is a homomorphism, since for any invertible fractional R-ideals J_1 and J_2, $\phi([J_1J_2]) = [J_1J_2S] = [J_1S][J_2S] = \phi([J_1])\phi([J_2])$. All that remains to show is that ϕ is surjective.

Let $[A] \in \mathrm{Cl}(S)$. Since $I \subseteq S$, we can use the second lemma above to assume without loss of generality that A is an integral ideal of S which is relatively prime to I. Then let $J = R \cap A$. Since A is relatively prime to I, we know that there is some $\alpha \in A$ and $\beta \in I$ such that $\alpha + \beta = 1$. Then $\alpha = 1 - \beta \in R$, so in fact $\alpha \in J$. Then J is relatively prime to I as an R-ideal. The first lemma above tells us that $J \in \mathrm{Inv}(R)$. Moreover, note the following:

$$A = AR = A(J + I) = AJ + AI \subseteq JS \subseteq A.$$

Then $A = JS$, so $\phi([J]) = [JS] = [A]$. Thus, ϕ is a surjective homomorphism. □

Corollary 2.4.13. *Let R be a locally associated order in a number field K. Then if S is an intermediate order to R, i.e. $R \subseteq S \subseteq \overline{R}$, S is also locally associated.*

Proof. By Corollary 2.4.7, we know that since R is locally associated, $\left|\mathrm{Cl}(R)\right| = \left|\mathrm{Cl}(\overline{R})\right|$. By the theorem, $\left|\mathrm{Cl}(R)\right| \geq \left|\mathrm{Cl}(S)\right|$; by Proposition 2.4.6, $\left|\mathrm{Cl}(S)\right| \geq \left|\mathrm{Cl}(\overline{R})\right|$. Then $\left|\mathrm{Cl}(S)\right| \geq \left|\mathrm{Cl}(\overline{R})\right| = \left|\mathrm{Cl}(R)\right| \geq \left|\mathrm{Cl}(S)\right|$, so $\left|\mathrm{Cl}(S)\right| = \left|\mathrm{Cl}(\overline{R})\right|$. Then again using Corollary 2.4.7, we have that S is locally associated. □

Recall that in the case of orders in a number field, any associated order is also locally associated. An important question to ask, then, is how far locally associated orders are from being associated; in other words, what additional properties must be present to conclude that a locally associated order is associated. While this question does not seem to have a simple answer in general, when the conductor ideal I of the order R is radical, this question is much more manageable. As we will see in the following chapter, orders with radical conductor ideal are an important subclass when studying elasticity.

Theorem 2.4.14. *Let R be an order in a number field K with radical conductor ideal I. Then R is an associated order if and only if the following hold:*

1. *R is locally associated;*

2. *For any $\overline{R}$-ideals J_1 and J_2 such that $I = J_1 J_2$, $(R + J_1) \cap (R + J_2) = R$.*

Proof. We have already seen throughout this chapter that the forward direction holds. What remains to show is that if R is a locally associated order and $(R+J_1)\cap(R+J_2) = R$ for $\overline{R}$-ideals J_1 and J_2 such that $I = J_1 J_2$, then R is associated. To show this direction, let $t \in \overline{R}$ and define $J_1 := t\overline{R} + I$ and $J_2 = I J_1^{-1}$. Note that since I is radical, t is relatively prime to J_2. By prime avoidance, there also exists some $s \in J_2$ which is relatively prime to J_1 (i.e. is not contained in any of the prime ideals dividing J_1). Then note that $t + s$ is not contained in any prime ideals containing I, i.e. $t + s$ is relatively prime to I. Then since R is locally associated, there is some $u \in U(\overline{R})$ such that $(t + s)u = r \in R$. Then $tu = r - su \in R + J_2$, and so $tu \in J_1 \cap (R + J_2) \subseteq (R + J_1) \cap (R + J_2) = R$. Then R is an associated order. □

From this result and Theorem 2.3.3, we immediately get the following corollary.

Corollary 2.4.15. *Let R be an order in a number field K with radical conductor ideal I. Then R is an associated order if and only if it is both locally associated and ideal-preserving.*

Chapter 3

Elasticity of Orders in a Number Field and Their Power Series Rings

As in the previous chapter, we begin by recalling Theorem 1.3.66 from Halter-Koch [10].

Theorem 1.3.66. *Let $d \in \mathbb{Z}$ be squarefree and $K = \mathbb{Q}[\sqrt{d}]$ the quadratic number field defined by d. Let $R = \mathbb{Z}[n\alpha]$ be the index $n \in \mathbb{N}\backslash\{1\}$ order in K, where $\alpha = \sqrt{d}$ if $d \equiv 2, 3 \pmod 4$ or $\alpha = \frac{1+\sqrt{d}}{2}$ if $d \equiv 1 \pmod 4$ so that $\overline{R} = \mathbb{Z}[\alpha]$. Then R is an HFD if and only if the following properties hold:*

1. *$\overline{R}$ is an HFD;*

2. *R is an associated order, i.e. $\overline{R} = R \cdot U(\overline{R})$;*

3. *$n = p$ for some prime $p \in \mathbb{N}$, or $n = 2p$ for some odd prime $p \in \mathbb{N}$.*

This theorem gives a full characterization of half-factorial orders in quadratic number fields. From this result, some natural questions may arise. For instance, recall that a half-factorial domain is really just an atomic domain with elasticity 1;

are there similar characterizations for orders with other elasticities? One might also ask what happens when R is allowed to be an order in a general number ring (not just quadratic). The results presented in this section will serve to address these questions. Furthermore, they will examine how these results can be extended to the power series ring $R[[x]]$ over such orders R.

Throughout this section, one might want to keep in mind previous work describing how HFDs pass (or more accurately, fail to pass) their elasticity to extension rings in general. For instance, [7] and [6] demonstrate that for a general HFD R, any of $R[x]$, $R[[x]]$, $\overline{R}$, or R' can fail to be an HFD. However, number rings are much nicer in this sense. It has been shown that if R is a ring of algebraic integers which is an HFD, then all of $R[x]$ ([1]), $R[[x]]$ ([14]), $\overline{R}$, and R' (both trivial) must be HFDs as well. In the case of a half-factorial order R in a number field, $\overline{R}$ and R' (which are both equal to the corresponding number ring) must be HFDs as well, though $R[x]$ need not be [1]. The results of this section serve to expand these ideas into larger elasticities as well as tackle the question of whether $R[[x]]$ must be an HFD when R is a half-factorial order in a number field.

It is worth noting here that recent work, found in [20], has provided a characterization of HFD orders in a general number field. We will state this result later in this chapter. As we will discuss later, this result is important and may prove to be quite useful moving forward in this field. Although the original results presented in this section will be closely related to those in [20], neither this dissertation nor the paper in question will imply the results of the other.

3.1 Elasticity of an Order

We begin with considering the elasticity of an order R in a number field K. In particular, we are interested when the elasticity of R will be equal to the elasticity of the ring of integers $\overline{R}$, since the elasticity of $\overline{R}$ is already well understood. Throughout this discussion, we will be using the concepts of associated, ideal-preserving, and locally associated orders as developed in the previous chapter. To start, we need a few lemmas leading toward an inequality which will hold in general and will serve as a jumping-off point for the following discussion. The first comes from [4].

Lemma 3.1.1. *Let R be an order in a number field with conductor ideal I. Any R-ideal relatively prime to I has unique factorization into prime R-ideals relatively prime to I. Moreover, all but finitely many prime ideals in R are relatively prime to I.*

The next lemma comes from [19] and generalizes a result we have already seen for number rings.

Lemma 3.1.2. *Let R be an order in a number field. Every ideal class in* $\mathrm{Cl}(R)$ *contains infinitely many prime ideals.*

One will note that together, these lemmas tell us that each ideal class in $\mathrm{Cl}(R)$ actually contains infinitely many prime ideals which are relatively prime to I. The last lemma we need relates the Davenport constants of the ideal class groups for two orders in a number field.

Lemma 3.1.3. *Let R and T be orders in the same number field K with $R \subseteq T$. Then $D(\mathrm{Cl}(R)) \geq D(\mathrm{Cl}(T))$.*

Proof. Recall by Theorem 2.4.12 that there exists a surjective homomorphism τ from $\mathrm{Cl}(R)$ onto $\mathrm{Cl}(T)$. Then let $k = D(\mathrm{Cl}(T))$ and $\{g_1, \ldots, g_k\} \subseteq \mathrm{Cl}(T)$ be a 0-sequence with no proper 0-subsequence. Since τ is surjective, there must exist $h_i \in \mathrm{Cl}(R)$ such that $\tau(h_i) = g_i$ for each $1 \leq i \leq k$. Since $\{g_1, \dots, g_k\}$ does not have any proper 0-subsequence, neither can the sequence $\{h_1, \dots, h_k\} \subseteq \mathrm{Cl}(R)$. If $\{h_1, \dots, h_k\}$ is a 0-sequence, then $\mathrm{Cl}(R)$ has a 0-sequence of length k with no proper 0-subsequence. If not, then note that (using additive notation) $\{h_1, \dots, h_k, -(h_1 + \dots + h_k)\}$ is a 0-sequence of length $k+1$ in $\mathrm{Cl}(R)$. Moreover, it is clear that this 0-sequence cannot have any proper 0-subsequence, since this would force $\{h_1, \dots, h_k\}$ to have a 0-subsequence. Then in this case, $\mathrm{Cl}(R)$ has a 0-sequence of length $k+1$ with no proper 0-subsequence. Since $D(\mathrm{Cl}(R))$ gives the length of the longest 0-sequence in $\mathrm{Cl}(R)$ with no proper 0-subsequence, $D(\mathrm{Cl}(R)) \geq k = D(\mathrm{Cl}(T))$. □

In particular, this result will be useful to us in the case that $T = \overline{R}$. The following theorem displays this utility.

Theorem 3.1.4. *Let R be an order in a number field. Then $\rho(R) \geq \rho(\overline{R})$.*

Proof. First, note that if $\rho(\overline{R}) = 1$, then the result is trivial. Otherwise, recall from Proposition 1.3.56 that $\rho(\overline{R}) = \frac{D(\mathrm{Cl}(\overline{R}))}{2}$.

Now let $k = D(\mathrm{Cl}(R))$ and $\{[I_1], \dots, [I_k]\}$ be a 0-sequence in $\mathrm{Cl}(R)$ with no 0-subsequence. As we saw from the above lemmas, we can now pick a prime ideal $P_i \in [I_i]$ relatively prime to the conductor ideal I of R for each $1 \leq i \leq k$. Furthermore, we can pick a prime ideal $Q_i \in [I_i]^{-1}$ relatively prime to I for each $1 \leq i \leq k$. Then let $\alpha \in R$ be a generator of the principal ideal $P_1 \dots P_k$; $\beta \in R$ be a generator of the principal ideal $Q_1 \dots Q_k$; and for each $1 \leq i \leq k$, $\gamma_i \in R$ be a generator of the principal ideal $P_i Q_i$. Also assume without loss of generality that $\alpha\beta = \gamma_1 \dots \gamma_k$ (if not, these elements are associates; we can absorb the unit into one of the generators). Now note that α, β, and each γ_i are relatively prime to I; then any divisor of these elements must also be relatively prime to I.

Suppose $\alpha = ab$ for some $a, b \in R$. Then the principal ideals aR and bR are relatively prime to I and must thus factor uniquely into products of prime R-ideals relatively prime to I by Lemma 3.1.1. Since $\alpha R = P_1 \dots P_k = aR \cdot bR$, we must have (after possible reordering) that $aR = P_1 \dots P_i$ and $bR = P_{i+1} \dots P_k$ for some $1 \leq i \leq k$. Then $\{[P_1], \dots, [P_i]\}$ is a 0-subsequence of $\{[I_1], \dots, [I_k]\}$ in $\mathrm{Cl}(R)$. Then since this 0-sequence has no proper 0-subsequence, either $aR = R$, an empty product of prime ideals, or $aR = \alpha R$. In either case, either a or b must be a unit, so α is irreducible. By similar arguments, β and each γ_i must be irreducible.

We now have $\alpha\beta = \gamma_1 \dots \gamma_k$, with α, β, and each γ_i an irreducible element of R. Then by definition of elasticity and using Lemma 3.1.3, $\rho(R) \geq \frac{k}{2} = \frac{D(\mathrm{Cl}(R))}{2} \geq \frac{D(\mathrm{Cl}(\overline{R}))}{2} = \rho(\overline{R})$. □

This result tells us that in general, factorization will only get "worse" when passing from a ring of algebraic integers to an order contained within. In particular, it tells us that if an order in a number field is half-factorial, i.e. has elasticity one, then so does its integral closure. However, it does nothing to tell us about the reverse inequality. The following results will serve to show under what circumstances these elasticities may actually be equal. To start, we need the following result regarding the distribution of units in an associated order.

Theorem 3.1.5. *Let R be an associated order in a number field K with conductor ideal I. Let J_1, J_2 be $\overline{R}$-ideals containing I such that J_1, J_2, and $J_3 = I(J_1J_2)^{-1}$ are pairwise relatively prime. Denote $R_1 = R + IJ_1^{-1} = R + J_2J_3$, $R_2 = R + IJ_2^{-1} = R + J_1J_3$, and $R_3 = R + J_3$. Then $U(R_3) = U(R_1) \cdot U(R_2)$, i.e. for every unit $u \in U(R_3)$, there exist $u_1 \in U(R_1)$ and $u_2 \in U(R_2)$ such that $u = u_1u_2$.*

Proof. First, note that from their definitions, R_1 and R_2 are both contained in R_3. Then $U(R_1) \cdot U(R_2) \subseteq U(R_3)$ trivially. We must show the reverse inclusion. In order to show this, we will first simplify the problem. To start, note that if every coset of ${}^{U(R_3)}\!/_{U(R)}$ contains an element of $U(R_1) \cdot U(R_2)$, then we are done. This is because then every element $u \in U(R_3)$ can be written as $u = u_1 u_2 v$, with $u_1 \in U(R_1)$, $u_2 \in U(R_2)$, and $v \in U(R)$. Since $R \subseteq R_2$, then $u = u_1(u_2 v) \in U(R_1) \cdot U(R_2)$. Then it will suffice to show the result modulo $U(R)$, i.e.

$$ {}^{U(R_3)}\!/_{U(R)} = {}^{U(R_1)}\!/_{U(R)} \cdot {}^{U(R_2)}\!/_{U(R)}. $$

Now suppose that we have $u_1, v_1 \in U(R_1)$ and $u_2, v_2 \in U(R_2)$ such that $u_1 u_2 \equiv v_1 v_2 \pmod{U(R)}$, i.e. there exists some $w \in U(R)$ such that $u_1 u_2 = v_1 v_2 w$. Then $u_1 v_1^{-1} = u_2^{-1} v_2 w$, with the left-hand side of this identity lying in $U(R_1)$ and the right-hand side lying in $U(R_2)$. Then in fact, both sides lie in $U(R_1) \cap U(R_2)$. Since both R_1 and R_2 are integral over R, and $R_1 \cap R_2 = R$ by Theorem 2.3.3, $U(R_1) \cap U(R_2) = U(R)$, and so $u_1 \equiv v_1 \pmod{U(R)}$ and $u_2 \equiv v_2 \pmod{U(R)}$. This means that for each distinct choice of cosets $u_1 U(R) \in {}^{U(R_1)}\!/_{U(R)}$ and $u_2 U(R) \in {}^{U(R_2)}\!/_{U(R)}$, we will get a unique product coset $u_1 u_2 U(R) \in {}^{U(R_3)}\!/_{U(R)}$. Then since ${}^{U(R_i)}\!/_{U(R)}$ is finite for $i = 1, 2, 3$, it will suffice to show that

$$ \left| {}^{U(R_3)}\!/_{U(R)} \right| = \left| {}^{U(R_1)}\!/_{U(R)} \right| \cdot \left| {}^{U(R_2)}\!/_{U(R)} \right|. $$

Now recall from Corollary 2.4.4 that R, R_1, R_2, and R_3 are all locally associated orders. In particular, this means that

$$ \left| {}^{U(\overline{R})}\!/_{U(R)} \right| = \frac{\left| U({}^{\overline{R}}\!/_{I}) \right|}{\left| U({}^{R}\!/_{I}) \right|}, $$

and similarly for R_1, R_2, and R_3. We will make extensive use of this property.

Note the following:

$$\begin{aligned}
\left|U(R_3)/U(R)\right| &= \frac{\left|U(\overline{R})/U(R)\right|}{\left|U(\overline{R})/U(R_3)\right|} = \frac{\left|U(\overline{R}/I)\right| \cdot \left|U(R_3/J_3)\right|}{\left|U(\overline{R}/J_3)\right| \cdot \left|U(R/I)\right|} \\
&= \frac{\left|U(\overline{R}/J_1)\right| \cdot \left|U(\overline{R}/J_2)\right| \cdot \left|U(\overline{R}/J_3)\right| \cdot \left|U(R_3/J_3)\right|}{\left|U(\overline{R}/J_3)\right| \cdot \left|U(R/I)\right|} \\
&= \frac{\left|U(\overline{R}/J_1)\right| \cdot \left|U(\overline{R}/J_2)\right| \cdot \left|U(R_3/J_3)\right|}{\left|U(R/I)\right|}.
\end{aligned}$$

The identities in the first line come from a simple quotient group property and the fact that R and R_3 are locally associated orders. The second line follows from applying the Chinese Remainder Theorem to $\overline{R}/I$. The final line comes from canceling out the common factor of $\left|U(\overline{R}/J_3)\right|$. By applying largely the same process to R_1 and R_2, we get:

$$\begin{aligned}
\left|U(R_1)/U(R)\right| &= \frac{\left|U(\overline{R}/J_1)\right| \cdot \left|U(R_1/IJ_1^{-1})\right|}{\left|U(R/I)\right|}, \\
\left|U(R_2)/U(R)\right| &= \frac{\left|U(\overline{R}/J_2)\right| \cdot \left|U(R_2/IJ_2^{-1})\right|}{\left|U(R/I)\right|}.
\end{aligned}$$

Finally, we can multiply these last two identities and simplify to obtain:

$$\left|U(R_1/U(R))\right| \cdot \left|U(R_2/U(R))\right| = \left|U(R_3)/U(R)\right| \cdot \frac{\left|U(R_1/IJ_1^{-1})\right| \cdot \left|U(R_2/IJ_2^{-1})\right|}{\left|U(R_3/J_3)\right| \cdot \left|U(R/I)\right|}.$$

Note that this gives us the desired identity, but with an additional fraction multiplied on the right-hand side. To show the desired identity, we simply need to show that this fraction is equal to 1. To do so, note from Theorem 2.2.8 that

$$R_1/IJ_1^{-1} \cong R+J_2/J_2 \times R_3/J_3,$$

$$R_2/IJ_2^{-1} \cong R+J_1/J_1 \times R_3/J_3,$$

$$R/I \cong R+J_1/J_1 \times R+J_2/J_2 \times R_3/J_3.$$

Thus,

$$R_1/IJ_1^{-1} \times R_2/IJ_2^{-1} \cong R/I \times R_3/J_3,$$

so in particular,

$$\left|U(R_1/IJ_1^{-1})\right| \cdot \left|U(R_2/IJ_2^{-1})\right| = \left|U(R/I)\right| \cdot \left|U(R_3/J_3)\right|$$

Then this gives the desired identity above, completing the proof. □

With this result, we can now consider how factorization in $\overline{R}$ will influence factorization in R. For the arguments presented here, we will need to assume that R has a radical conductor ideal. Among other things, this assumption will allow us to apply the above theorem quite frequently, since it will be much easier to produce relatively prime ideals J_1, J_2, and J_3 as in the statement of the theorem. We will discuss this assumption more following the presentation of the following results.

Theorem 3.1.6. *Let R be an associated order in a number field K with radical conductor ideal I. Then any irreducible element in R remains irreducible in $\overline{R}$.*

Proof. Let α be an irreducible element in R, and write $\alpha = \beta\gamma$ for some $\beta, \gamma \in \overline{R}$. To show that α remains irreducible in $\overline{R}$, we want to show that either β or γ must be a unit in $\overline{R}$. Since R is an associated order, we can pick some $u, v \in U(\overline{R})$ such that $u\beta, v\gamma \in R$. We will use this notation throughout the proof.

First, assume that α is relatively prime to I, i.e. $\alpha + I \in U(R/I)$. Then $uv + I = ((u\beta)(v\gamma) + I)(\alpha + I)^{-1} \in R/I$. Then $uv \in U(R)$, so $(uv)\alpha$ is an associate of α in R and thus must also be irreducible in R. Then either $u\beta$ or $v\gamma$ must be a unit in R, and thus either β or γ must be a unit in $\overline{R}$. Then α remains irreducible in $\overline{R}$.

Now removing the assumption that α is relatively prime to I, write $I = J_1J_2J_3$ as follows: let $J_1 = \beta\overline{R} + I$, the minimal divisor of I which contains β; let $J_2 = \gamma\overline{R} + IJ_1^{-1}$, the minimal divisor of I which contains γ and is relatively prime to J_1; and let $J_3 = I(J_1J_2)^{-1}$. Note that as I is radical, J_1, J_2, and J_3 are pairwise relatively prime. As in the previous theorem, we will write $R_1 = R + IJ_1^{-1}$, $R_2 = R + IJ_2^{-1}$, and $R_3 = R + J_3$. Then note that α is relatively prime to J_3. By the previous case, this tells us that $uv \in U(R_3)$. We can now use the previous theorem to conclude that there must exist $w_1 \in U(R_1)$ and $w_2 \in U(R_2)$ such that $(uv)^{-1} = w_1w_2$. Then $\alpha = (w_1w_2)(uv)\alpha = (w_1u\beta)(w_2v\gamma)$. Now note that $w_1u\beta \in R_1 \cap J_1 \subseteq R$ and $w_2v\gamma \in R_2 \cap J_2 \subseteq R$. Then $\alpha = (w_1u\beta)(w_2v\gamma)$ is a factorization of α into two elements of R, so either $w_1u\beta$ or $w_2v\gamma$ is a unit in R. Thus, either β or γ must be a unit in $\overline{R}$, so α remains irreducible in $\overline{R}$. □

We can now build on this result to relate the elasticity of R to that of $\overline{R}$. The definition of elasticity can be found in Definition 1.2.40.

Theorem 3.1.7. *Let R be an associated order in a number field K with radical conductor ideal I. Then for any nonzero, nonunit $\alpha \in R$, $\rho_R(\alpha) = \rho_{\overline{R}}(\alpha)$. Moreover, $\rho(R) = \rho(\overline{R})$.*

Proof. By the previous theorem, any irreducible in R will remain irreducible in $\overline{R}$. Then for any nonzero, nonunit $\alpha \in R$, any factorization of α into irreducibles in R is also a factorization of α into irreducibles in $\overline{R}$. Then $\ell_R(\alpha) \subseteq \ell_{\overline{R}}(\alpha)$, so $\rho_R(\alpha) \leq \rho_{\overline{R}}(\alpha)$ for every nonzero, nonunit $\alpha \in R$. Note that since $R \subseteq \overline{R}$, this also gives $\rho(R) \leq \rho(\overline{R})$. By Theorem 3.1.4, $\rho(R) = \rho(\overline{R})$.

Now let $\alpha = \pi_1 \ldots \pi_k$ be a factorization of $\alpha \in R$ into irreducibles $\pi_i \in \mathrm{Irr}(\overline{R})$. As in the proof of the previous theorem, we can find $u_1, \ldots, u_k \in U(\overline{R})$ such that $u_i\pi_i \in R$ for each $1 \leq i \leq k$. Now define ideals $J_1 := \pi_1\overline{R} + I$, the minimal ideal dividing I which contains π_1, and for $2 \leq i \leq k$, define $J_i := \pi_i\overline{R} + I(J_1 \ldots J_{i-1})^{-1}$, the minimal ideal dividing I which contains π_i and is relatively prime to each J_j for $1 \leq j \leq i-1$. Finally, define $J_{k+1} := I(J_1 \ldots J_k)^{-1}$ so that $I = J_1 \ldots J_{k+1}$. Since I is radical, these J_i's are pairwise relatively prime. For ease of notation, we will also define $R_{k+1} := R + J_{k+1}$, and for $1 \leq i \leq k$, $R_i := R + IJ_i^{-1}$. As seen in the previous proof, since α is relatively prime to J_{k+1}, $u_1 \ldots u_k \in U(R_{k+1})$. Furthermore, we can repeatedly apply Theorem 3.1.5 to get

$$U(R_{k+1}) = U(R_1) \ldots U(R_k).$$

Then there exist $v_i \in U(R_i)$ for $1 \leq i \leq k$ such that $(u_1 \ldots u_k)^{-1} = v_1 \ldots v_k$, and so $\alpha = (v_1u_1\pi_1) \ldots (v_ku_k\pi_k)$. Each $v_iu_i\pi_i \in R_i \cap J_i \subseteq R$, so this is a factorization of α in R. Furthermore, each $v_iu_i\pi_i$ is an associate of π_i in $\overline{R}$, and so is also irreducible in $\overline{R}$ (and must thus be irreducible in R). Then any irreducible factorization $\alpha = \pi_1 \ldots \pi_k$ in $\overline{R}$ gives rise in this way to an irreducible factorization $\alpha = (v_1u_1\pi_1) \ldots (v_ku_k\pi_k)$ in R of the same length. Then for any nonzero, nonunit $\alpha \in R$, $\ell_{\overline{R}}(\alpha) \subseteq \ell_R(\alpha)$, so $\rho_{\overline{R}}(\alpha) \leq \rho_R(\alpha)$. Thus, $\rho_{\overline{R}}(\alpha) = \rho_R(\alpha)$. □

From these results, we know that any associated order in a number field K with radical conductor ideal will inherit its elasticity from its integral closure (the full ring of integers in K). In particular, this gives us a large class of half-factorial orders:

associated orders with radical conductor ideal whose integral closures are HFDs. For the proofs presented here, one will note that the assumption that the conductor ideal is radical is a vital component. However, this condition is not necessary for an order to be an HFD. As we will discuss in the next chapter, examples exist of half-factorial orders with non-radical conductor ideal. One such example is presented in [20]; work independently producing another example can be found in the next chapter. It is worth noting, however, that it is not enough just to assume that R is an associated order. Indeed, it is not particularly difficult to find examples of an associated order which does not have the same elasticity as its integral closure, though any such order must have non-radical conductor ideal.

Example 3.1.8. Let $R = \mathbb{Z}[9\sqrt{2}]$. Note that $\overline{R} = \mathbb{Z}[\sqrt{2}]$ is a UFD (and thus an HFD). Furthermore, one can verify that R is an associated order (in particular, the characterization given in Proposition 2.2.7 can be checked in finite steps). However, note that $I = (R : \overline{R}) = 9\overline{R} = (3\overline{R})^2$ is a non-radical conductor ideal. Moreover, by Theorem 1.3.66, R is not an HFD, i.e. its elasticity does not match that of its integral closure.

Several additional examples of such orders in number fields have been found. These examples, along with methods by which such examples may be produced, can be found in the next chapter.

3.2 Extending to Power Series

In the previous section, we discussed how to relate the elasticity of an order R in a number field to that of its integral closure. In particular, we say that these elasticities agree when R is an associated order with radical conductor ideal. In this section, we will see how these results may be extended to study the elasticity of the ring of formal power series $R[[x]]$. First, it will help to consider a similar result to Theorem 3.1.5, which we will do in two parts.

Lemma 3.2.1. *Let R be an associated order in a number field K. Let I be the conductor ideal of R and J_1, J_2 be relatively prime $\overline{R}$-ideals such that $I = J_1J_2$. Denote $R_1 = R + J_1$ and $R_2 = R + J_2$. Then $U(\overline{R}[[x]]) = U(R_1[[x]]) \cdot U(R_2[[x]])$.*

Proof. Recall that a power series over a commutative ring with unity T is a unit if and only if its constant term is a unit. Then an arbitrary element of $U(\overline{R}[[x]])$ looks like $u(x) = u_0 + b_1x + b_2x^2 + \dots$, with $b_i \in \overline{R}$ for $i \in \mathbb{N}$ and $u_0 \in U(\overline{R})$. To prove the lemma, we would like to construct $v_1(x) = u_1 + c_1x + c_2x^2 + \cdots \in U(R_1[[x]])$ and $v_2(x) = u_2 + d_1x + d_2x^2 + \cdots \in U(R_2[[x]])$ such that $u = v_1v_2$. By Theorem 3.1.5, we know that we can pick constant terms $u_1 \in U(R_1)$ and $u_2 \in U(R_2)$ such that $u_0 = u_1u_2$. Then we need to find $c_i \in R_1$ and $d_i \in R_2$ for $i \geq 1$ such that the equation

$$b_k = c_ku_2 + \sum_{i=1}^{k-1} c_id_{k-i} + d_ku_1$$

is satisfied for each $k \geq 1$. Note that this equation can equivalently be stated as

$$c_ku_2 + d_ku_1 = b_k - \sum_{i=1}^{k-1} c_id_{k-i}.$$

If we assume for some $k \geq 1$ that we have constructed c_i, d_i for $1 \leq i < k$ such that each previous equation is satisfied, this becomes a problem of finding $c_k \in R_1$ and $d_k \in R_2$ such that $c_ku_2 + d_ku_1$ is equal to some fixed element of $\overline{R}$. Then note that $\overline{R} \supseteq u_2R_1 + u_1R_2 \supseteq u_2J_1 + u_1J_2 = J_1 + J_2 = \overline{R}$. Then finding such c_k and d_k is possible for every $k \geq 1$ (in fact, we could select $c_k \in J_1$ and $d_k \in J_2$ if we so wished), so we can indeed construct $v_1 \in U(R_1[[x]])$ and $v_2 \in U(R_2[[x]])$ such that $u = v_1v_2$.

Then $U(\overline{R}[[x]]) = U(R_1[[x]]) \cdot U(R_2[[x]])$. □

Theorem 3.2.2. *Let R be an associated order in a number field K with conductor ideal I. Let J_1, J_2 be $\overline{R}$-ideals containing I such that J_1, J_2, and $J_3 = I(J_1J_2)^{-1}$ are pairwise relatively prime. Denote $R_1 = R + IJ_1^{-1}$, $R_2 = R + IJ_2^{-1}$, and $R_3 = R + J_3$. Then $U(R_3[[x]]) = U(R_1[[x]]) \cdot U(R_2[[x]])$.*

Proof. Let $u \in U(R_3[[x]])$. Since this is an element in $U(\overline{R}[[x]])$, we can use the lemma to construct $v_1 \in U((R+J_1)[[x]])$ and $v_2 \in U((R+J_2)[[x]])$ such that $u = v_1v_2$ (the lemma would actually give $v_2 \in U((R+J_2J_3)[[x]]) \subseteq U((R+J_2)[[x]])$, but we do not need this added specificity). Now note that since $J_1[[x]]$, $J_2[[x]]$, and $J_3[[x]]$ are pairwise relatively prime ideals of $\overline{R}[[x]]$, we can use the Chinese Remainder Theorem to decompose:

$$\overline{R}/I[[x]] \cong \overline{R}/J_1[[x]] \times \overline{R}/J_2[[x]] \times \overline{R}/J_3[[x]].$$

Then we will pick some coset representative $w \in \overline{R}[[x]]$ of the congruence class modulo $I[[x]]$ such that $w \equiv 1 \pmod{J_1[[x]]}$, $w \equiv 1 \pmod{J_2[[x]]}$, and $w \equiv v_1^{-1} \pmod{J_3[[x]]}$. Note that although w itself is not necessarily a unit in $\overline{R}[[x]]$, its constant term, say w_0, is congruent to a unit modulo J_1, J_2, and J_3, so $w_0 + I \in U(\overline{R}/I)$. Since R is a locally associated order, there exists $r + I \in U(R/I)$ and $\beta \in I$ such that $w_0r + \beta \in U(\overline{R})$. Define $w' = wr + \beta \in U(\overline{R}[[x]])$ and $s \in R$ such that $s + I = (r+I)^{-1} \in U(R/I)$.

Now note that $u = v_1v_2 = (v_1w')(v_2w'^{-1})$. Moreover:

$$v_1w' \equiv v_1(wr+\beta) \equiv v_1r \pmod{J_1[[x]]} \implies v_1w' \in (R+J_1)[[x]];$$

$$v_1w' \equiv v_1(wr+\beta) \equiv v_1v_1^{-1}r \equiv r \pmod{J_3[[x]]} \implies v_1w' \in R_3[[x]];$$

$$v_2w'^{-1} \equiv v_2(wr+\beta)^{-1} \equiv v_2s \pmod{J_2[[x]]} \implies v_2w'^{-1} \in (R+J_2)[[x]];$$

$$v_2 w'^{-1} \equiv v_2(wr+\beta)^{-1} \equiv v_2 v_1 s \equiv us \pmod{J_3[[x]]} \implies v_2 w'^{-1} \in R_3[[x]].$$

Then since R is an ideal-preserving order and J_1, J_2, and J_3 are relatively prime, $v_1 w' \in (R+J_1)[[x]] \cap R_3[[x]] = R_2[[x]]$ and $v_2 w'^{-1} \in (R+J_2)[[x]] \cap R_3[[x]] = R_1[[x]]$. Furthermore, since v_1, v_2, and w' are all units in $\overline{R}[[x]]$, then $v_1 w' \in U(R_2[[x]])$ and $v_2 w'^{-1} \in U(R_1[[x]])$, completing the proof. □

This result shows us that, when R is an associated order, we can "break down" units in the power series rings over intermediate orders just like we could in the intermediate orders themselves. As before, this result will be easiest to use when the conductor ideal I is radical.

Now working toward an analogous elasticity result to Theorem 3.1.7 for the ring of formal power series $R[[x]]$, we first take note the following important lemma dealing with associated subrings.

Lemma 3.2.3. *Let R be an associated order in a number field K with radical conductor ideal I. Then $R[[x]]$ is an associated subring of $\overline{R}[[x]]$.*

Proof. Let $a(x) = a_0 + a_1 x + a_2 x^2 + \cdots \in \overline{R}[[x]]$. We want to show that there exist $r(x) = r_0 + r_1 x + r_2 x^2 + \cdots \in R[[x]]$ and $u(x) = u_0 + b_1 x + b_2 x^2 + \cdots \in U(\overline{R}[[x]])$ such that $a = ru$. First, note that since R is an associated order, we can find constant terms r_0 and u_0 such that $a_0 = r_0 u_0$.

Working toward an inductive argument, we will start by assuming that I is prime. If $a \in I[[x]]$, then we could choose $r = a$ and $u = 1$. Otherwise, $a \notin I[[x]]$; for now, we will also assume that $a_0 \notin I$. Since $a_0 = r_0 u_0$, this means that $r_0 \notin I$; since I is prime, $r_0 + I \in U(\overline{R}/I)$. We now need to construct $r_i \in R$ and $b_i \in \overline{R}$ for $i \in \mathbb{N}$

such that for each $k \in \mathbb{N}$,

$$a_k = r_0 b_k + \sum_{i=1}^{k-1} r_i b_{k-i} + r_k u_0;$$

equivalently,

$$r_0 b_k + r_k u_0 = a_k - \sum_{i=1}^{k-1} r_i b_{k-i}.$$

Assume that for some $k \in \mathbb{N}$, we have selected r_i and b_i for every $1 \leq i < k$ such that all previous equations are satisfied. Then note that $\overline{R} \supseteq r_0\overline{R} + u_0 R \supseteq r_0\overline{R} + I = \overline{R}$. Then selecting $r_k \in R$ and $b_k \in \overline{R}$ to satisfy the k^{th} such equation is always possible, so we can construct $r \in R[[x]]$ and $u \in U(\overline{R}[[x]])$ such that $a = ru$.

Now assume that I is prime and $a \notin I[[x]]$, but $a_0 \in I$. Since $a \notin I[[x]]$, there is some minimal $j \in \mathbb{N}$ such that $a_j \notin I$ (i.e. $a_i \in I$ for all $0 \leq i < j$). Then write $a(x) = (a_0 + a_1 x + \cdots + a_{j-1}x^{j-1}) + x^j(a_j + a_{j+1}x + \ldots) = b + cx^j$, with $b \in I[x]$ and $c \in \overline{R}[[x]]$ having constant term $a_j \notin I$. By the previous case, there must exist $r \in R[[x]]$ and $u \in U(\overline{R}[[x]])$ such that $c = ru$. Then $a = b + cx^j = (bu^{-1} + rx^j)u$, with $bu^{-1} + rx^j \in R[[x]]$ and $u \in U(\overline{R}[[x]])$. This completes the case when I is prime.

Now assume that I is not prime (but is still radical), and for the inductive argument, assume that for every $\overline{R}$-ideal J properly dividing I, $(R + J)[[x]]$ is an associated subring of $\overline{R}[[x]]$ (note that any such $R + J$ is an associated order with radical conductor ideal J). Since I is not prime, we can write $I = J_1 J_2$, with neither J_1 nor J_2 equal to I; since I is radical, J_1 and J_2 are relatively prime. For ease of notation, denote $R_1 = R + J_1$ and $R_2 = R + J_2$. By the inductive hypothesis, we can select $r_1 \in R_1[[x]]$ and $u \in U(\overline{R}[[x]])$ such that $a = r_1 u$. Furthermore, we can select $r_2 \in R_2[[x]]$ and $v \in U(\overline{R}[[x]])$ such that $r_1 = r_2 v$. Finally, by Lemma 3.2.1, we can select $w_1 \in U(R_1[[x]])$ and $w_2 \in U(R_2[[x]])$ such that $v = w_1 w_2$. Then note that $r_1 = r_2 v = r_2 w_1 w_2 \implies r_1 w_1^{-1} = r_2 w_2$. Since the left-hand side of this equality lies in $R_1[[x]]$ and the right-hand side lies in $R_2[[x]]$, both must actually lie in $R_1[[x]] \cap R_2[[x]] = R[[x]]$. Then $a = r_1 u = r_2 v u = (r_2 w_2)(w_1 u) \in R[[x]] \cdot U(\overline{R}[[x]])$. Then $R[[x]]$ is an associated subring of $\overline{R}[[x]]$. □

With these tools in hand, we are now ready to tackle the questions of irreducibility and elasticity in $R[[x]]$.

Theorem 3.2.4. *Let R be an associated order in a number field K with radical conductor ideal I. Then any irreducible element in $R[[x]]$ remains irreducible in $\overline{R}[[x]]$.*

Proof. Let f be an irreducible power series in $R[[x]]$, and write $f = gh$ for $g, h \in \overline{R}[[x]]$. To show that f remains irreducible in $\overline{R}[[x]]$, we want to show that either g or h is a unit. The previous theorem tells us that $R[[x]]$ is an associated subring of $\overline{R}[[x]]$, so there exist $u, v \in U(\overline{R}[[x]])$ such that $ug, vh \in R[[x]]$. We will use this notation throughout the rest of the proof.

First, we will consider the case when $f \notin I[[x]]$ and I is a prime $\overline{R}$-ideal. We write $uv = u_0 + b_1 x + b_2 x^2 + \cdots \in U(\overline{R}[[x]])$, $f = r_0 + r_1 x + r_2 x^2 + \cdots \in R[[x]]$, and $(uv)f = a_0 + a_1 x + a_2 x^2 + \cdots \in R[[x]]$ (note that $(uv)f$ must lie in $R[[x]]$ as the product of ug and vh, both of which lie in $R[[x]]$). Since $f \notin I[[x]]$, there is some minimal $n \in \mathbb{N}_0$ such that $r_n \notin I$ (i.e. $r_i \in I$ for $0 \leq i < n$). Then

$$a_n = u_0 r_n + \sum_{i=1}^{n} b_i r_{n-i} \implies u_0 r_n = a_n - \sum_{i=1}^{n} b_i r_{n-i}.$$

Note that $a_n \in R$ and $r_{n-i} \in I$ for $1 \leq i \leq n$, so the right-hand side of this equation lies in R. Furthermore, since I is prime and $r_n \notin I$, $r_n + I \in U({}^{R}/_{I})$, so

$$u_0 + I = \left(a_n - \sum_{i=1}^{n} b_i r_{n-i} + I \right) (r_n + I)^{-1} \in {}^{R}/_{I}.$$

then $u_0 \in U(R)$.

Now for some $k > n$, we will assume that $u_0 \in U(R)$ and $b_i \in R$ for $1 \leq i < k - n$. Similarly to before, we write

$$a_k = u_0 r_k + \sum_{i=1}^{k-n-1} b_i r_{k-i} + b_{k-n} r_n + \sum_{i=k-n+1}^{k} b_i r_{k-i};$$

rearranging, this gives

$$b_{k-n} r_n = a_k - u_0 r_k - \sum_{i=1}^{k-n-1} b_i r_{k-i} - \sum_{i=k-n+1}^{k} b_i r_{k-i}.$$

On the right-hand side of this equation, note that $a_k \in R$, $u_0 r_k \in R$, $b_i r_{k-i} \in R$ for $1 \leq i \leq k-n-1$, and $r_{k-i} \in I$ for $i \geq k-n+1$. Then the right-hand side of this equation is in R, so we can proceed as before to multiply by the inverse of r_n modulo I to get

$$b_{k-n} + I = \left(a_k - u_0 r_k - \sum_{i=1}^{k-n-1} b_i r_{k-i} - \sum_{i=k-n+1}^{k} b_i r_{k-i} + I \right) (r_n + I)^{-1} \in {}^{R}\!/_{I}.$$

Then $b_i \in R$ for every $i \in \mathbb{N}$, so $uv \in U(R[[x]])$. Then uvf is an associate of f in $R[[x]]$, and must thus remain irreducible in $R[[x]]$. Therefore, either ug or vh must be a unit in $R[[x]]$, meaning that either g or h must be a unit in $\overline{R}[[x]]$. Thus, f remains irreducible in $\overline{R}[[x]]$.

Now removing the assumption that I is prime, we will split I into relatively prime factors much as in the proof of Theorem 3.1.6: let J_1 be the minimal divisor of I such that $J_1[[x]]$ contains g; let J_2 be the minimal divisor of IJ_1^{-1} such that $J_2[[x]]$ contains h; and let $J_3 = I(J_1J_2)^{-1}$. As before, we will denote $R_1 = R + IJ_1^{-1}$, $R_2 = R + IJ_2^{-1}$, and $R_3 = R + J_3$. Since $P[[x]]$ is a prime $\overline{R}[[x]]$-ideal for any prime ideal P, note that α is not contained in $P[[x]]$ for any prime divisor P of J_3. By the previous case, this tells us that $uv \in (R+P)[[x]]$ for every prime divisor P of J_3, and thus $uv \in \bigcap_{P|J_3}(R+P)[[x]] = R_3[[x]]$. Then since $uv \in U(R_3[[x]])$, we can use Theorem 3.2.2 to conclude that there must exist $w_1 \in U(R_1[[x]])$ and $w_2 \in U(R_2[[x]])$ such that $(uv)^{-1} = w_1w_2$. Then $f = (uv)^{-1}(ug)(vh) = (w_1ug)(w_2vh)$, with $w_1ug \in R_1[[x]] \cap J_1[[x]] \subseteq R[[x]]$ and $w_2vh \in R_2[[x]] \cap J_2[[x]] \subseteq R[[x]]$. Then $f = (w_1ug)(w_2vh)$ is a factorization of f in $R[[x]]$, so either w_1ug or w_2vh is a unit in $R[[x]]$. Then either g or h must be a unit in $\overline{R}[[x]]$, meaning that f is irreducible in $\overline{R}[[x]]$. □

Theorem 3.2.5. *Let R be an associated order in a number field K with radical conductor ideal I. Then for any nonzero, nonunit $f \in R[[x]]$, $\rho_{R[[x]]}(f) = \rho_{\overline{R}[[x]]}(f)$. Moreover, $\rho(R[[x]]) = \rho(\overline{R}[[x]])$.*

Proof. By the previous theorem, any irreducible in $R[[x]]$ remains irreducible in $\overline{R}[[x]]$. Then for any nonzero, nonunit $f \in R[[x]]$, any factorization of f into $R[[x]]$-irreducibles is also a factorization of f into $\overline{R}[[x]]$-irreducibles. Then $\ell_{R[[x]]}(f) \subseteq \ell_{\overline{R}[[x]]}(f)$, so $\rho_{R[[x]]}(f) \leq \rho_{\overline{R}[[x]]}(f)$ for every nonzero, nonunit $f \in R[[x]]$. Note that this also gives $\rho(R[[x]]) \leq \rho(\overline{R}[[x]])$.

Now let $f = g_1 \dots g_k$ be a factorization of some nonzero, nonunit $f \in R[[x]]$ into irreducibles $g_i \in \mathrm{Irr}(\overline{R}[[x]])$. By Lemma 3.2.3, we can find $u_1, \dots, u_k \in U(\overline{R}[[x]])$ such that $u_ig_i \in R[[x]]$ for every $1 \leq i \leq k$. Now let J_1 be the minimal divisor of I such that $J_1[[x]]$ contains g_1, and for $2 \leq i \leq k$, let J_i be the minimal divisor of $I(J_1 \dots J_{i-1})^{-1}$ such that $J_i[[x]]$ contains g_i. Finally, let $J_{k+1} = I(J_1 \dots J_k)^{-1}$ so that $J_1, \dots, J_{k+1}$ are pairwise relatively prime ideals such that $I = J_1 \dots J_{k+1}$ and $g_i \in J_i[[x]]$ for $1 \leq i \leq k$. For ease of notation, we will denote $R_{k+1} = R + J_{k+1}$ and $R_i = R + IJ_i^{-1}$ for $1 \leq i \leq k$. Then as in the proof of the previous theorem, since f is not contained in $P[[x]]$ for any prime $\overline{R}$-ideal P dividing J_{k+1}, $u_1 \dots u_k \in U(R_{k+1}[[x]])$.

By repeatedly applying Theorem 3.2.2, we have that

$$U(R_{k+1}[[x]]) = U(R_1[[x]]) \dots U(R_k[[x]]).$$

Then there exist $v_i \in U(R_i[[x]])$ for $1 \leq i \leq k$ such that $(u_1 \dots u_k)^{-1} = v_1 \dots v_k$. Thus, $f = (v_1 u_1 g_1) \dots (v_k u_k g_k)$. Note that each $v_i u_i g_i \in R_i[[x]] \cap J_i[[x]] \subseteq R[[x]]$; furthermore, since each $v_i u_i g_i$ is an associate of $g_i \in \operatorname{Irr}(\overline{R}[[x]])$, each of these elements is irreducible in $\overline{R}[[x]]$ (and thus also irreducible in $R[[x]]$). Then the irreducible factorization $f = g_1 \dots g_k$ in $\overline{R}[[x]]$ gave rise to an irreducible factorization $f = (v_1 u_1 g_1) \dots (v_k u_k g_k)$ in $R[[x]]$ of the same length. Then $\ell_{\overline{R}[[x]]}(f) \subseteq \ell_{R[[x]]}(f)$, so $\rho_{\overline{R}[[x]]}(f) \leq \rho_{R[[x]]}(f)$ for every nonzero, nonunit $f \in R[[x]]$. Thus, $\rho_{\overline{R}[[x]]}(f) = \rho_{R[[x]]}(f)$.

All that remains to show is that $\rho(R[[x]]) = \rho(\overline{R}[[x]])$. We already know that $\rho(R[[x]]) \leq \rho(\overline{R}[[x]])$; furthermore, for any nonzero, nonunit $f \in R[[x]]$, we know that $\rho_{\overline{R}[[x]]}(f) = \rho_{R[[x]]}(f)$. Then if we can show that for any nonzero $f \in \overline{R}[[x]]$, there exists $g \in R[[x]]$ such that $\rho_{\overline{R}[[x]]}(f) = \rho_{R[[x]]}(g)$, this would complete the proof. To do so, recall that by Lemma 3.2.3, there exists $u \in U(\overline{R}[[x]])$ such that $uf \in R[[x]]$. Then since f and uf are associates in $\overline{R}[[x]]$, we know that $\rho_{\overline{R}[[x]]}(uf) = \rho_{\overline{R}[[x]]}(f)$. Furthermore, the previous argument tells us that since $uf \in R[[x]]$, $\rho_{R[[x]]}(uf) = \rho_{\overline{R}[[x]]}(uf)$. Then for any nonzero, nonunit $f \in \overline{R}[[x]]$, there is some $g \in R[[x]]$ (in this construction, $g = uf$) such that $\rho_{\overline{R}[[x]]}(f) = \rho_{R[[x]]}(g)$. Then $\rho(\overline{R}[[x]]) \leq \rho(R[[x]])$, so $\rho(\overline{R}[[x]]) = \rho(R[[x]])$. □

3.3 Half-Factorial Orders

Recall that a half-factorial domain is characterized by being an atomic domain with elasticity 1, i.e. any two factorizations of the same nonzero, nonunit element into irreducibles must have the same length. Then naturally, the results from this chapter will apply very nicely to the half-factorial property for orders in a number field. First, it will help to consider the recent characterization of half-factorial orders in a number field from [20]. We will present this characterization in the notation of this dissertation, rather than that used in the original paper.

Theorem 3.3.1. *Let K be a number field and R an order in K with conductor ideal I. Let $I = P_1^{a_1} \dots P_k^{a_k}$ be the factorization of I into prime $\overline{R}$-ideals, and denote $Q_i := R \cap P_i$ for each $1 \leq i \leq k$. Then R is an HFD if and only if the following properties hold:*

1. *$\overline{R}$ is an HFD;*
2. *R is an associated order;*
3. *For each $1 \leq i \leq k$, $a_i \leq 4$, and letting π_i be an arbitrary prime element of $\overline{R}_{Q_i}$, $v_{\pi_i}(\mathrm{Irr}(R_{Q_i})) \subseteq \{1, 2\}$. If P_i is a principal ideal, then $a_i \leq 2$ and $v_{\pi_i}(\mathrm{Irr}(R_{Q_i})) = \{1\}$.*

Here, R_{Q_i} refers to the localization of R at the prime ideal Q_i (with $\overline{R}_{Q_i}$ analogously defined) and v_{π_i} is the valuation associated with the element π_i.

One will note that the first two conditions in this characterization are the same as those for quadratic HFD orders from Theorem 1.3.66. Although the third condition does not in general require R to have a radical conductor ideal, it does restrict the prime powers which can divide the conductor. It is also worth noting the relationship between this result and the previously discussed results. First, note that this characterization shows what is needed for the converse to Theorem 3.1.7 in the case that $\overline{R}$ is an HFD. As we have alluded to (and will show in the next chapter), not every HFD order in a number field will necessarily have radical conductor ideal. On the other hand, Theorem 3.1.7 applies more generally to orders in a number field with elasticities other than 1 (and more explicitly gives a large class of ideals which satisfy Condition 3 above).

Two of the features that make HFD orders particularly nice to work with are given in the above characterization: their integral closures are HFDs (i.e. $\mathrm{Cl}(K) \leq 2$), and they are associated orders. Another fact that makes half-factorial orders especially nice to work with in the context of this dissertation comes from [14] using a handful of results found in [13], [9], [3], [8], and [23]. We will include here an additional equivalent condition not present in [14] which follows immediately from the proof.

Theorem 3.3.2. *Let R be an integrally closed order in a number field K, i.e. $R = \overline{R} = \mathcal{O}_K$. The following are equivalent:*

1. *R is an HFD.*
2. *$R[[x_1, \ldots, x_n]]$ is an HFD for some $n \in \mathbb{N}$.*
3. *$R[[x_1, \ldots, x_n]]$ is an HFD for all $n \in \mathbb{N}$.*

While it is currently unknown whether the elasticity of a ring of integers carries over to its ring of formal power series in general, this tells us that this relationship holds at least when this elasticity is 1. From this and the previous results in this chapter, we get the following.

Corollary 3.3.3. *Let R be an order in a number field K with radical conductor ideal I. Then R is an HFD if and only if $R[[x]]$ is an HFD.*

Proof. First, assume that $R[[x]]$ is an HFD. Since R is Noetherian, we know that R must be atomic. Then consider two factorizations $\pi_1 \ldots \pi_m = \tau_1 \ldots \tau_n$, with σ_i and τ_j irreducibles in R for $1 \leq i \leq m$, $1 \leq j \leq n$. By considering just the constant terms of any potential factorizations of π_i or τ_j in $R[[x]]$, one can clearly see that these elements must remain irreducible in $R[[x]]$. Then since $R[[x]]$ is an HFD, we must have that $m = n$, so R is an HFD.

Now assume that R is an HFD. From Theorem 3.3.1, we know that R must be an associated order and $\overline{R}$ must be an HFD. From Theorem 3.2.5, we know that $R[[x]]$ must have the same elasticity as $\overline{R}[[x]]$. Finally, the previous theorem tells us that $\overline{R}[[x]]$ is an HFD. Then $R[[x]]$ must be an HFD. □

One might ask following this result whether the same holds even when I is non-radical; this question is not yet answered. As mentioned before, examples of half-factorial orders in a number field have been found which have non-radical conductor - the rings of formal power series over these orders have not yet been explored in detail. The methods used in the proofs presented here are not sufficient to conclude that the $R[[x]]$ must also be an HFD for such orders R (though we will still know that $\overline{R}$ and $\overline{R}[[x]]$ are HFDs). Moreover, one might ask if the same conclusion holds for elasticities other than 1. In particular, can we always conclude that $\rho(\overline{R}[[x]]) = \rho(\overline{R})$? Again, this question is yet unanswered, but will require a different argument than that found in [14] for Theorem 3.3.2.

We will now turn our attention even more specifically to the context of HFD orders in quadratic number fields. As mentioned several times, this context was of particular interest to Halter-Koch, and such orders were completely characterized in

[10]. We restate this characterization here for convenience.

Theorem 1.3.66. *Let $d \in \mathbb{Z}$ be squarefree and $K = \mathbb{Q}[\sqrt{d}]$ the quadratic number field defined by d. Let $R = \mathbb{Z}[n\alpha]$ be the index $n \in \mathbb{N}\backslash\{1\}$ order in K, where $\alpha = \sqrt{d}$ if $d \equiv 2, 3 \pmod 4$ or $\alpha = \frac{1+\sqrt{d}}{2}$ if $d \equiv 1 \pmod 4$ so that $\overline{R} = \mathbb{Z}[\alpha]$. Then R is an HFD if and only if the following properties hold:*

1. *$\overline{R}$ is an HFD;*

2. *R is an associated order, i.e. $\overline{R} = R \cdot U(\overline{R})$;*

3. *$n = p$ for some prime $p \in \mathbb{N}$, or $n = 2p$ for some odd prime $p \in \mathbb{N}$.*

Additionally, it is well-known that for an order R of index n (i.e. $R = \mathbb{Z}[n\alpha]$), the conductor ideal of R is $I = n\overline{R}$, and any prime $p \in \mathbb{Z}$ dividing n must be inert in K. The fact that $I = n\overline{R}$ is easy to see; the fact that the primes dividing n must be inert follows almost immediately from results in this dissertation.

Proposition 3.3.4. *Let $R = \mathbb{Z}[n\alpha]$ be an HFD order in a quadratic ring of integers K, with notation as in Theorem 1.3.66. Then any prime $p \in \mathbb{Z}$ dividing n must be inert in K.*

Proof. Assume that n has a prime divisor $p \in \mathbb{Z}$ which is not inert in K. Then $p\overline{R}$ has some proper prime ideal divisor P, so $\left|{}^{\overline{R}}/_{P}\right| = p$. Since R is an HFD order, it must be an associated (and therefore ideal-preserving) order. Then $R + P$ must be an order in K with conductor ideal P. However, this means that

$$\left|{}^{\overline{R}}/_{P}\right| = \left|{}^{\overline{R}}/_{R}\right| \cdot \left|{}^{R}/_{P}\right| = p.$$

Since p is prime in $\mathbb{Z}$, this means that either $\overline{R} = R$, a contradiction, or $R = P$, a contradiction (since $1 \in R\backslash P$). Then p must be inert. $\square$

This gives a corollary that is particularly interesting after seeing the main results of this chapter.

Corollary 3.3.5. *Let R be an HFD order in a quadratic ring of integers K. Then R has a radical conductor ideal.*

Proof. From Theorem 1.3.66, we know that the conductor ideal of R must be $I = n\overline{R}$, with n either prime in $\mathbb{Z}$ or twice an odd prime. In either case, the proposition gives us that the primes dividing n must be inert, and thus $I = n\overline{R}$ is a product of distinct prime ideals in $\overline{R}$. Then I is radical. □

This, along with Corollary 3.3.3, gives another immediate corollary.

Corollary 3.3.6. *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.*

Now recall that from Theorem 3.1.7, we know in general that an order R in any number field K is an HFD if $\overline{R}$ is an HFD, R is an associated order, and the conductor ideal I is radical. Theorem 1.3.66 actually tells us that in the case of orders in a quadratic number field, we can actually restrict the possible conductor ideals even further. This gives the following interesting result regarding associated orders.

Proposition 3.3.7. *Let R be the order of index n (i.e. $I = n\overline{R}$) in a quadratic number field K such that $\overline{R}$ is an HFD. If n has two distinct odd prime divisors in $\mathbb{Z}$, then R is not an associated order.*

Proof. Assume that n has two distinct odd prime divisors $p, q \in \mathbb{Z}$. First, note that as in the proof of Proposition 3.3.4, if either p or q are not inert, then R cannot be an associated order. This is because in this case, I has a prime ideal divisor P with

$\left|{}^{\overline{R}}/_{P}\right|$ a prime integer, so $R + P$ cannot have conductor ideal P. If p and q are both inert primes, then we can consider the order $S = R + pq\overline{R}$. If R is an associated order, then S is also an associated order. Furthermore, S has radical conductor ideal $pq\overline{R}$, since $p\overline{R}$ and $q\overline{R}$ are prime $\overline{R}$-ideals. Then since $\overline{S} = \overline{R}$ is an HFD, S is an HFD. However, this contradicts Theorem 1.3.66, since pq is neither an odd prime nor twice an odd prime. Then R cannot be an associated order. □

Example 3.3.8. Let $R = \mathbb{Z}[33\sqrt{2}]$. Since $\overline{R} = \mathbb{Z}[\sqrt{2}]$ is an HFD and 33 has two distinct prime divisors (3 and 11), the proposition tells us that R cannot be an associated order. Note that this holds despite the fact that both $\mathbb{Z}[3\sqrt{2}]$ and $\mathbb{Z}[11\sqrt{2}]$ are both associated subrings (and thus HFDs), which can easily be checked using Proposition 2.4.5.

Finally, we present an alternative characterization of HFD orders in a quadratic number field. One will note from Theorem 1.3.66 that to show that an order R in a quadratic number field is an HFD, one needs to show that R is an associated order. This condition can often be time-consuming to check. However, as the following characterization will show, one can simplify the process considerably.

Theorem 3.3.9. *Let R be an order in a quadratic number field K with conductor ideal I. Then R is an HFD if and only if the following properties hold:*

1. *$\overline{R}$ is an HFD;*
2. *R is a locally associated order, i.e. $\left|{}^{U(\overline{R})}/_{U(R)}\right| = \frac{\left|U({}^{\overline{R}}/_{I})\right|}{\left|U({}^{R}/_{I})\right|}$;*
3. *$I = n\overline{R}$, where $n \in \mathbb{Z}$ is either $n = p$, with p an inert prime in K, or $n = 2p$, with 2 and p inert primes in K.*

Proof. We already know from Theorem 1.3.66, Corollary 2.4.4, and Proposition 3.3.4 that if R is an HFD, then these three conditions hold. We simply need to show the converse. Suppose that R is an order satisfying the above three conditions. From Theorem 1.3.66, to show that R is an HFD, it will be sufficient to show that R is an associated order. If $n = p$, then I is a prime (and thus maximal) ideal. Then Proposition 2.4.5 immediately gives us that R is an associated order and thus an HFD. If $n = 2p$, then note that $2 \in (2\overline{R} \cap R)\backslash p\overline{R}$ and $p \in (p\overline{R} \cap R)\backslash 2\overline{R}$. Then R is an ideal-preserving order, so Theorem 2.4.15 tells us that R is an associated order and thus an HFD. $\square$

In general, checking that an order is locally associated is easier than checking that it is associated. For the former, one really only needs to find the order of ${}^{U(\overline{R})}\big/_{U(R)}$; For the latter, one needs to pick a coset representative from each coset of ${}^{U(\overline{R})}\big/_{U(R)}$ (which requires knowing the order of this group), then perform a number of multiplications. Furthermore, checking that a prime $p \in \mathbb{Z}$ is inert in a quadratic number field only requires use of the Legendre symbol. Then this alternate characterization will often make checking that an order in a quadratic number field is an HFD easier.

Chapter 4

Examples and Additional Cases

Up to this point, most of the results that we have seen have been abstracted for generality with a few examples sprinkled throughout. In Chapter 2, we explored properties of associated, ideal-preserving, and locally associated subrings. In Chapter 3, we explored elasticity in orders of algebraic number fields and their rings of formal power series. In both cases, we focused more on proving general results and less on explicitly determining when a specific order in a number field possessed the properties we were interested in. This chapter will examine these orders more closely, first using the knowledge we have developed to determine large swaths of orders which either must be or cannot be locally associated, ideal-preserving, associated, or half-factorial. Then, we will make use of MATLAB to explicitly find orders which possess these properties. Finally, we will use what we have found to produce an example of particular interest to this dissertation.

4.1 Summary of Results

Before getting into specific cases and explicitly stating examples, it will help to present a summary of useful results. Many of these results come from Chapter 2, though they will be restated here in terms specific to orders in a number field. Such results will be presented without proof; those presented with proof are new.

Theorem 4.1.1. *Let R be an order in a number field K and S a subring of $\overline{R}$ containing R. Then S is an order in K. If R is an associated order, then so is S; if R is an ideal-preserving order, then so is S; finally, if R is a locally associated order, then so is S.*

When searching for orders with these three properties, this will be one of the most important results to keep in mind. For instance, we noted in Example 2.1.8 that the order $R = \mathbb{Z}[5\sqrt{2}]$ in the number field $K = \mathbb{Q}[\sqrt{2}]$ is not associated. This theorem tells us that any order contained in R cannot be associated; thus, we would have no need to check if $\mathbb{Z}[25\sqrt{2}]$ is associated.

Theorem 4.1.2. *Let R be an ideal-preserving order in a number field K with conductor ideal I. Then for any T-ideal J, $R + J$ is an order in K with conductor ideal $I + J$. In particular, if $J|I$, then $R + J$ has conductor ideal J.*

Lemma 4.1.3. *Let R be an order in a number field with conductor ideal I. Then $\left|{}^{\overline{R}}\!/\!_{I}\right|$ is not a rational prime.*

Proof. Assume that there exists some number field K with order R such that the conductor ideal I of R has prime norm in $\overline{R}$; that is, $\left|{}^{\overline{R}}\!/\!_{I}\right| = p$ for some rational prime p. One will note that if $R = \overline{R}$, then $I = \overline{R}$, i.e. I would have norm 1. Thus, R is a non-maximal order. Now considering the additive groups of $\overline{R}$, R, and I, we have that $p = \left|{}^{\overline{R}}\!/\!_{I}\right| = \left|{}^{\overline{R}}\!/\!_{R}\right| \cdot \left|{}^{R}\!/\!_{I}\right|$. Since both factors on the right-hand side of this equality must be positive integers which multiply to be the prime integer p, it must be the case that one of these factors is equal to 1. However, we have already established that $\overline{R} \neq R$, so we must have $R = I$. However, note that $1 \in R \backslash I$, a contradiction. Then $\left|\overline{R}/I\right|$ cannot be prime. $\square$

Theorem 4.1.4. *Let R be an ideal-preserving order in a number field K with conductor ideal I, and let P be a prime divisor of I which lies over the rational prime p. Then the inertial degree $f(P|p) > 1$.*

Proof. Suppose that I has a prime divisor P which lies over $p \in \mathbb{Z}$ and $f(P|p) = 1$. This means that $\left|\overline{R}/I\right| = p$. By the above results, we know that $R + P$ is an order in K with conductor ideal P. However, the lemma tells us that this is impossible, since P has prime norm. Then any prime divisor P of I must have $f(P|p) > 1$. $\square$

This result will allow us to rule out the possibility of many orders being ideal-preserving. For instance, we know that $\mathbb{Z}[2\sqrt{2}]$ is not an ideal-preserving order. This is because its conductor ideal is $I = (2) = (\sqrt{2})^2$, with $f((\sqrt{2})|2) = 1$.

Theorem 4.1.5. *Let R be an order in a number field with conductor ideal I. If every prime divisor of I is principal in $\overline{R}$ and can be generated (as an $\overline{R}$-ideal) by an element of R, then R is ideal-preserving.*

Proof. Assume that I is as described in the theorem statement. Recall that to show that R is ideal-preserving, we simply need to show that for any primes P_1 and P_2 dividing I, $R \cap P_1 \neq R \cap P_2$ and $R \cap P_1 \neq R \cap P_1^2$. By the assumption, such P_1 and P_2 are principal and generated by an element of R. Let $\pi_1 \in R$ such that $P_1 = \pi_1 \overline{R}$. Then $\pi_1 \in R \cap P_1$. However, if $\pi_1 \in P_2$ or $\pi_1 \in P_1^2$, that would imply that P_1 itself is contained in one of these ideals, a contradiction. Then $R \cap P_1 \neq R \cap P_2$ and $R \cap P_1 \neq R \cap P_1^2$, meaning that R is ideal-preserving. $\square$

Although this theorem has a strong assumption associated with it, it will actually be very useful to us in one scenario in particular. Recalling that $\mathbb{Z} \subseteq R$ for any order R in a number field, we get the following immediate corollary.

Corollary 4.1.6. *Let R be an order in a number field with conductor ideal $I = n\overline{R}$ for some $n \in \mathbb{Z}$. If every rational prime divisor of n is an inert prime in R, then R is ideal-preserving.*

Theorem 4.1.7. *Let R_1 and R_2 be orders in a number field K with conductor ideals J_1 and J_2, respectively. Then $R_1 \cap R_2$ is an order in K with conductor ideal $J_1 \cap J_2$. If J_1 and J_2 are relatively prime, then $R_1 = R + J_1$, $R_2 = R + J_2$, and ${}^{R}\!/_{I} \cong {}^{R_1}\!/_{J_1} \times {}^{R_2}\!/_{J_2}$. If we also assume that R_1 and R_2 are ideal-preserving orders, then so is $R_1 \cap R_2$.*

Whereas the previous results largely helped us to rule out the possibility of an order being associated or ideal-preserving, this result can actually save us a lot of work in determining which orders are ideal-preserving. For instance, $\mathbb{Z}[3\sqrt{2}]$ and $\mathbb{Z}[11\sqrt{2}]$ are both ideal-preserving orders; from this, we know that their intersection, $\mathbb{Z}[33\sqrt{2}]$, must also be ideal-preserving.

Theorem 4.1.8. *Let R be an order in a number field with conductor ideal I. If I is prime, then R is ideal-preserving.*

The applications of this result are obvious. We mentioned in the previous paragraph that $\mathbb{Z}[3\sqrt{2}]$ and $\mathbb{Z}[11\sqrt{2}]$ are ideal-preserving; this result tells us this immediately given the knowledge that 3 and 11 are inert primes in $\mathbb{Z}[\sqrt{2}]$. Note that in this specific case, we can also use Corollary 4.1.6, though the theorem can be applied more generally.

Theorem 4.1.9. *Let R be an order in a number field with conductor ideal I. If R is an associated order, then R is both ideal-preserving and locally associated. If I is* *radical, i.e. if I is a product of distinct prime $\overline{R}$-ideals, then R is an associated order if and only if R is both ideal-preserving and locally associated.*

As a bidirectional statement, this result actually helps us in two ways. In some cases, checking whether an order is ideal-preserving is actually quite simple. Similarly, checking that an order is locally associated is almost universally easier than checking that the order is associated. On the one hand, if either of these conditions fail, then there is no need to check if the order is associated. On the other, if the order happens to have radical conductor ideal, we only need to check these two simpler conditions; if both hold, the order must be associated.

Finally, we have another result with a similar bidirectional statement. When reading this statement, one should keep in mind Theorem 4.1.5.

Theorem 4.1.10. *Let R be an order in a number field with conductor ideal I. Also assume that every prime divisor of I is a principal ideal which can be generated (as an $\overline{R}$-ideal) by an element of R. Then R is an associated order if and only if R is locally associated.*

Proof. First, note that as before, any associated order R is locally associated. Then we will only need to show that any locally associated order R with conductor ideal I as described above is associated. Suppose that R is such an order, and let $\alpha \in \overline{R}$. Let $I = P_1^{a_1} \dots P_k^{a_k}$ be the prime factorization of I into prime $\overline{R}$-ideals, and for each $1 \leq i \leq k$, let b_i be the exact power of P_i dividing (α) (note that some or all of the b_i's may be zero). Since each P_i is a principal $\overline{R}$-ideal generated by an element of R, then so is $P_1^{b_1} \dots P_k^{b_k} | (\alpha)$. Let $\beta \in R$ be a generator of this ideal, and note that $\alpha = \beta\gamma$ for some $\gamma \in \overline{R}$ relatively prime to I. Now since R is a locally associated order, there must exist some $r \in R$ and $u \in U(\overline{R})$ such that $\gamma = ru$. Then $\alpha = \beta\gamma = (\beta r)u \in R \cdot U(\overline{R})$, so R is an associated order. □

Recall from Theorem 4.1.5 that any order whose conductor ideal satisfies the hypothesis of this theorem must be ideal-preserving. Then much like Theorem 4.1.9, this result gives us a case in which showing an order is both ideal-preserving and locally associated suffices to show that the order is associated. We will make use of this result in the following section.

4.2 Quadratic Orders

We will now apply these findings to the simplest types of orders: those found in quadratic number fields. Recall the following statement about orders in a quadratic number field:

Proposition 4.2.1. *Let $d \in \mathbb{Z}$ be squarefree, $K = \mathbb{Q}[\sqrt{d}]$ and $\mathcal{O}_K = \mathbb{Z}[\alpha]$, where $\alpha = \sqrt{d}$ if $d \equiv 2, 3 \pmod 4$ or $\alpha = \frac{1+\sqrt{d}}{2}$ if $d \equiv 1 \pmod 4$. Then any order in K is of the form $\mathcal{O} = \mathbb{Z}[n\alpha]$ for some $n \in \mathbb{N}$. Moreover, the conductor ideal of $\mathcal{O}$ is the principal ideal $n\mathcal{O}_K$. We will often refer to such $n \in \mathbb{N}$ as the* **index** *of $\mathcal{O}$.*

This result tells us exactly the form of an order in a quadratic number field; in particular, an order in a given quadratic number field is completely determined by the index (equivalently, by the conductor ideal). Thus, an order in any quadratic number field will be totally determined by two integer values: d, the squarefree integer determining the number field in which the order is contained; and n, the index of the order in that number field. Now using the results we discussed above, we get the following regarding ideal-preserving quadratic orders.

Theorem 4.2.2. *Let $K = \mathbb{Q}[\sqrt{d}]$ for some squarefree $d \in \mathbb{Z}$ and R the index n order in K. Then R is ideal-preserving if and only if every rational prime divisor of n is inert in K.*

Proof. First, we will note that Corollary 4.1.6 tells us that if every rational prime divisor of n is inert in K, R is ideal-preserving. Now assume that R is ideal-preserving and let p be a divisor of n. Since K is a quadratic number field, p must either be inert or be a product of two (not necessarily distinct) prime $\overline{R}$-ideals of norm p. Since R is ideal-preserving, then its conductor ideal $n\overline{R}$ cannot have any prime divisors of prime norm. Thus, every rational prime dividing n must be inert. □

With this theorem, we have completely characterized which orders in a quadratic number field are ideal-preserving. For each squarefree $d \in \mathbb{Z}$ and $n \in \mathbb{N}$, we simply need to consider the Legendre symbols $\left(\frac{d}{p}\right)$ for each odd $p|n$ to determine if p is inert (recall: for odd p this happens when $\left(\frac{d}{p}\right) = -1$); for $p = 2$, we simply need to check that $d \equiv 5 \pmod 8$. Thus, we can focus on determining which orders are locally associated, keeping in mind our previous results. Once we have done so, we immediately get the following corollary from the previous theorem and Theorem 4.1.10.

Corollary 4.2.3. *Let R be an order in a quadratic number field. Then R is associated if and only if it is both ideal-preserving and locally associated.*

This corollary will allow us to check two much simpler conditions to determine whether a given order in a number field is associated. Finally, we can use Theorems 1.3.66 and 3.1.7 to find the elasticities of any associated orders with radical conductor ideals.

4.2.1 Non-Real Quadratic Orders

We will start by restricting our interest to non-real quadratic fields, i.e. $\mathbb{Q}[\sqrt{d}]$ such that $d < 0$. By Dirichlet's Unit Theorem, note that in this case, the unit group of the ring of algebraic integers is a finite cyclic group consisting of the roots of 1. In particular, when $d = -1$, the unit group is generated by i; when $d = -3$, the unit group is generated by $\frac{1+\sqrt{-3}}{2}$; otherwise, the unit group is generated by -1. Note further that for any order $R = \mathbb{Z}[n\alpha]$ in these rings with $n > 1$, $U(R) = \{\pm 1\}$ (since no non-maximal order in $\mathbb{Q}[i]$ or $\mathbb{Q}[\sqrt{-3}]$ will contain i or $\frac{1+\sqrt{-3}}{2}$, respectively). Then in any case, we know the value of $\left| {}^{U(\overline{R})}\!/\!{}_{U(R)} \right|$ and can use this to determine when R is locally associated.

Theorem 4.2.4. *Let R be the order of index $n > 1$ in the quadratic number field $K = \mathbb{Q}[\sqrt{d}]$, where $d < 0$ is squarefree. Then R is locally associated if and only if one of the following conditions holds:*

1. *$d \equiv 1 \pmod 8$ and $n = 2$;*

2. *$d = -1$ and $n = 2$;*

3. *$d = -3$ and $n \in \{2, 3\}$.*

Proof. To check if an order is locally associated, we will check the equivalent condition

$$\left| {}^{U(\overline{R})}\!/\!{}_{U(R)} \right| = \frac{\left| U({}^{\overline{R}}\!/\!{}_{I}) \right|}{\left| U({}^{R}\!/\!{}_{I}) \right|}.$$

From the above discussion, we will always know the value of the left-hand side of this equation:

$$\left| {}^{U(\overline{R})}\!/\!{}_{U(R)} \right| = \begin{cases} 2, & d = -1; \\ 3, & d = -3; \\ 1, & \text{otherwise.} \end{cases}$$

Then if we choose n such that the right-hand side of the equation matches the left, R will be locally associated. For convenience, we will denote $n = p_1^{a_1} \dots p_k^{a_k}$.

First, note that since $R = \mathbb{Z}[n\alpha]$ and $I = n\mathbb{Z}[\alpha]$, the cosets in ${}^{R}\!/_{I}$ can each be represented by an integer modulo n. Thus, a coset in ${}^{R}\!/_{I}$ will be a unit if and only if its integer coset representative is relatively prime to n. Then $\left|U({}^{R}\!/_{I})\right| = \phi(n) = \prod_{i=1}^{k} p_i^{a_i-1}(p_i - 1)$. Tackling $\left|U({}^{\overline{R}}\!/_{I})\right|$ is slightly more complicated. Using the Chinese Remainder Theorem, we can separate this into

$$\left|U({}^{\overline{R}}\!/_{I})\right| = \prod_{i=1}^{k} \left|U({}^{\overline{R}}\!/_{(p_i)^{a_i}})\right|.$$

Thus, we can determine the size of this unit group for prime-power n, then use the fact that it is multiplicative. We will need to consider three cases: when p_i is inert; when p_i is split; and when p_i is ramified.

If p_i is inert, i.e. (p_i) is a prime ideal:

$$\left|U({}^{\overline{R}}\!/_{(p_i)^{a_i}})\right| = \left|{}^{\overline{R}}\!/_{(p_i)^{a_i}}\right| - \left|{}^{(p_i)}\!/_{(p_i)^{a_i}}\right| = p_i^{2a_i} - p_i^{2(a_i-1)} = p_i^{2(a_i-1)}(p_i^2 - 1).$$

If p_i is split, i.e. $(p_i) = PQ$ for two distinct prime $\overline{R}$-ideals P and Q:

$$\left|U({}^{\overline{R}}\!/_{(p_i)^{a_i}})\right| = \left|U({}^{\overline{R}}\!/_{P^{a_i}})\right| \cdot \left|U({}^{\overline{R}}\!/_{Q^{a_i}})\right| = \left(\left|{}^{\overline{R}}\!/_{P^{a_i}}\right| - \left|{}^{P}\!/_{P^{a_i}}\right|\right)^2 = p_i^{2(a_i-1)}(p_i - 1)^2.$$

If p_i is ramified, i.e. $(p_i) = P^2$ for some prime $\overline{R}$-ideal P:

$$\left|U({}^{\overline{R}}\!/_{(p_i)^{a_i}})\right| = \left|{}^{\overline{R}}\!/_{P^{2a_i}}\right| - \left|{}^{P}\!/_{P^{2a_i}}\right| = p_i^{2a_i} - p_i^{2a_i-1} = p_i^{2a_i-1}(p_i - 1).$$

Now since both $\left|U({}^{\overline{R}}\!/_{I})\right|$ and $\left|U({}^{R}\!/_{I})\right|$ are multiplicative, their ratio will be as well. This again allows us to consider this ratio for only the prime-power factors of

n. If p_i is inert:

$$\frac{\left|U\left(\overline{R}/(p_i)^{a_i}\right)\right|}{\left|U\left(R+(p_i)^{a_i}/(p_i)^{a_i}\right)\right|}=\frac{p_i^{2(a_i-1)}(p_i^2-1)}{p_i^{a_i-1}(p_i-1)}=p_i^{a_i-1}(p_i+1).$$

If p_i is split:

$$\frac{\left|U\left(\overline{R}/(p_i)^{a_i}\right)\right|}{\left|U\left(R+(p_i)^{a_i}/(p_i)^{a_i}\right)\right|}=\frac{p_i^{2(a_i-1)}(p_i-1)^2}{p_i^{a_i-1}(p_i-1)}=p_i^{a_i-1}(p_i-1).$$

If p_i is ramified:

$$\frac{\left|U\left(\overline{R}/(p_i)^{a_i}\right)\right|}{\left|U\left(R+(p_i)^{a_i}/(p_i)^{a_i}\right)\right|}=\frac{p_i^{2a_i-1}(p_i-1)}{p_i^{a_i-1}(p_i-1)}=p_i^{a_i}.$$

By inspection, the only one of these which could possibly be equal to 1 is when p_i is split, which is equal to 1 if and only if $p_i=2$ and $a_i=1$. Then the order R of index $n>1$ in $\mathbb{Q}[\sqrt{d}]$, with d a negative squarefree integer other than -1 and -3, is locally associated if and only if $n=2$ and 2 is split, which happens if and only if $d\equiv 1 \pmod 8$.

Now we can focus on the cases when $d=-1$ and $d=-3$. In both cases, note that we are looking for the above fraction equal to a prime number, and no prime-power yields this fraction being equal to 1. Then for R to be locally associated, n must be a prime power. When $d=-1$, we are looking for the above fraction to be equal to 2. Note that this is only possible when $n=2$, with 2 ramified; $n=3$ with 3 split; or $n=4$ with 2 split. Since 2 is ramified and 3 is inert in $\mathbb{Z}[i]$, the only locally associated order in $\mathbb{Q}[i]$ is $\mathbb{Z}[2i]$. When $d=-3$, we are looking for the fraction equal to 3. This is only possible when $n=2$ with 2 inert or $n=3$ with 3 ramified. Since 2 is inert and 3 is ramified in $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$, the only locally associated orders in $\mathbb{Q}[\sqrt{-3}]$

are $\mathbb{Z}[\sqrt{-3}]$ and $\mathbb{Z}[\frac{3+3\sqrt{-3}}{2}]$. This completes the proof. $\square$

Keeping in mind our previous results, this immediately yields the following corollary.

Corollary 4.2.5. *Let R be the order of index $n > 1$ in the quadratic number field $K = \mathbb{Q}[\sqrt{d}]$, where $d < 0$ is squarefree. Then R is associated if and only if $d = -3$ and $n = 2$.*

Note in this case, $\overline{R} = \mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$ is an HFD (in fact, a UFD), R is associated, and $n = 2$ is prime. This gives an alternate proof of a result originally from [5].

Corollary 4.2.6. *Let $R = \mathbb{Z}[\sqrt{-3}]$, the index 2 order in the number field $K = \mathbb{Q}[\sqrt{-3}]$. Then R is an HFD. Moreover, this is the only non-integrally closed half-factorial order in a non-real quadratic number field.*

4.2.2 Real Quadratic Orders

We can now focus our attention on orders contained in real quadratic number fields, i.e. orders in fields of the form $\mathbb{Q}[\sqrt{d}]$ for d a squarefree positive integer. In the rings of integers of such fields, Dirichlet's Unit Theorem states that the unit group will be of the form $W \times V$, with W finite cyclic and V free abelian of rank 1. In this case, the only roots of unity will be ± 1, so the unit group will be of the form $\{\pm u^k | k \in \mathbb{Z}\}$ for some unit u, called the fundamental unit. Since $\pm 1 \in \mathbb{Z} \subseteq R$ for any order R, we can determine $\left| U(\overline{R}) / U(R) \right|$ by finding the minimal power of u which lies in R. Unfortunately, this means that the process of finding whether an order in a real quadratic field is locally associated will be more difficult than the process for non-real quadratic fields. Fortunately, many of the results from the non-real case will still hold for $\left| U(\overline{R}/I) \right|$ and $\left| U(R/I) \right|$.

In order to determine when orders in real quadratic number fields are locally associated and associated, we will make use of the MATLAB program `quadLA.m`; this code can be found in the appendix. Also included are the programs `primePowers.m`, `polyMult.m`, `quadFundUnit.m`, and `isSquare.m`, which are utilized by this program. To make use of this code, one will need to input `n`, the index of the desired order, and `d`, the squarefree integer defining the field. The output of this program is a vector `[lao ao]`, where `lao` and `ao` are Boolean values stating whether the order is locally associated and associated, respectively. Table 4.1 summarizes the output of this program for selected values of n and d. In this table, '-' indicates that an order is not locally associated; 'L' indicates that it is locally associated but not associated; and 'A' indicates that it is associated (and thus locally associated).

Looking through Table 4.1, one might notice that several patterns emerge in both the rows and columns. For instance, in columns 3, 7, 11, 19, and 23 (the prime numbers congruent to 3 modulo 4), no orders are associated, and the orders which are locally associated seem to be exactly those of the form d^k or $2d^k$ for some $k \in \mathbb{N}_0$. Furthermore, columns 6, 14, and 22 (twice the primes we just discussed) seem to have only a single locally associated order: that of index $\frac{d}{2}$. In the rows, one may notice that no order listed here of index $n = 4k$ for $k \geq 2$ is associated, and even the locally associated orders of these indices seem to be sparser than those of many other indices. Although these patterns could certainly be products of the fact that only a limited number of cases have been considered here, they are certainly interesting in their own right. Looking further into these patterns could also illuminate structures among such orders that might lead to a general characterization of locally associated or associated orders in quadratic number fields.

Now recall Theorem 1.3.66, which gave a characterization of orders in quadratic number fields which are HFDs. Using the database of algebraic number fields (in-

Table 4.1: Real Quadratic (Locally) Associated Orders

d n	2	3	5	6	7	10	11	13	14	15	17	19	21	22	23	26	29	30
2	L	L	A	-	L	L	L	A	-	L	L	L	A	-	L	L	A	-
3	A	L	A	L	-	L	-	L	-	L	A	-	L	-	-	A	A	L
4	L	-	A	-	-	L	-	A	-	-	L	-	-	-	-	L	A	-
5	-	-	L	-	-	L	-	-	-	L	-	-	-	-	-	-	-	L
6	-	L	A	-	-	-	-	L	-	L	L	-	-	-	-	-	A	-
7	L	-	A	-	L	A	-	A	L	-	A	-	L	-	-	A	L	-
8	L	-	-	-	-	L	-	-	-	-	-	-	-	-	-	L	-	-
9	A	L	A	-	-	L	-	L	-	-	A	-	L	-	-	A	-	L
10	-	-	L	-	-	L	-	-	-	L	-	-	-	-	-	-	-	-
11	A	-	L	-	-	A	L	-	-	-	-	-	-	L	-	L	A	-
12	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
13	-	-	-	-	-	-	-	L	-	-	-	-	-	-	-	L	-	-
14	-	-	A	-	L	-	-	A	-	-	L	-	L	-	-	-	-	-
15	-	-	L	-	-	L	-	-	-	L	-	-	-	-	-	-	-	L
16	L	-	-	-	-	L	-	-	-	-	-	-	-	-	-	L	-	-
17	-	-	-	-	-	-	-	-	-	-	L	-	-	-	-	-	-	-
18	-	L	-	-	-	-	-	-	-	-	L	-	-	-	-	-	-	-
19	A	-	L	-	-	-	-	A	-	-	L	L	-	-	-	L	A	-
20	-	-	L	-	-	L	-	-	-	-	-	-	-	-	-	-	-	-
21	-	-	-	-	-	-	-	-	-	-	-	-	L	-	-	-	-	-
22	-	-	L	-	-	-	L	-	-	-	-	-	-	-	-	-	-	-
23	L	-	A	-	-	A	-	L	-	-	A	-	-	-	L	L	L	-
24	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
25	-	-	L	-	-	L	-	-	-	L	-	-	-	-	-	-	-	L
26	-	-	-	-	-	-	-	L	-	-	-	-	-	-	-	L	-	-
27	A	L	A	-	-	L	-	L	-	-	A	-	L	-	-	A	-	L
28	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
29	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	L	-
30	-	-	L	-	-	-	-	-	-	L	-	-	-	-	-	-	-	-

cluding their class groups) found at [11], we note that $\left|\mathrm{Cl}(\mathbb{Q}[\sqrt{d}])\right| \leq 2$ for every $d \leq 30$. This tells us that the integral closure of every order in Table 4.1 is an HFD. Thus, the associated orders in this table whose index n is either prime or twice an odd prime are exactly the HFD orders in this table. Therefore, there are exactly 27 half-factorial orders of index $2 \leq n \leq 30$ in real quadratic number fields of the form $\mathbb{Q}[\sqrt{d}]$ for squarefree $d \leq 30$.

More generally, for an order in a quadratic number field whose integral closure is not an HFD, we could use Theorem 3.1.7 to determine when the elasticity of the order might match that of its integral closure. Specifically, any associated order with radical conductor ideal (that is, any order which outputs `ao = true` from `quadLA.m` whose index n is squarefree) must have the same elasticity as its integral closure. Again, we can check the elasticity of such a number field using the class group; the database at [11] can provide these class groups for many number fields.

4.3 Other Orders

Moving beyond quadratic number fields, the situation gets decidedly more complicated. For instance, orders are no longer uniquely defined by their conductor ideal, and these conductor ideals need not be principal, let alone generated by an integer. Furthermore, the prime decomposition of rational primes may be more nuanced than simply inert, split completely, or totally ramified. Integral bases for the rings of algebraic integers may be more difficult to find, especially bases which interact nicely with the order, as in Proposition 1.2.92. Perhaps most troubling, especially when trying to determine if a given order is (locally) associated, is that the group of units may have a free abelian part of rank greater than 1.

In some cases, we can rely on the same results from the quadratic case. For instance, if every prime ideal dividing the conductor is principal and generated by an element of R (such as when the prime ideal is generated by an inert rational prime), we know that R is ideal-preserving. Similarly, if any prime divisors of the conductor ideal have prime norm, the order is not ideal-preserving. Beyond these results, we will not explore ideal-preserving orders in depth beyond the quadratic case.

In order to simplify the process of determining whether an order is (locally) associated, we will be making three big assumptions about the ring of algebraic integers, then explaining in loose terms how one might extend to a more general case. First, given an order R, we will assume that $\overline{R} = \mathbb{Z}[\alpha]$ for some $\alpha \in \overline{R}$. While this is certainly always true in the quadratic case, it can fail even in a cubic extension. To check that this assumption holds, we will rely on the database found at [11]; among other features of a number field, this database includes an integral basis for the ring of algebraic integers.

The second assumption we will make is even more limiting; we will assume that $\overline{R}$ admits a fundamental unit. As discussed in the introduction, this limits us to quadratic number fields (which we have already discussed), cubic number fields with exactly one real embedding (such as pure cubic extensions, $\mathbb{Q}[\sqrt[3]{d}]$), and quartic number fields with no real embeddings. This will make it much easier to determine whether an order is locally associated, as then $\left| U(\overline{R}) / U(R) \right|$ is simply the smallest power of the fundamental unit which lies in R, perhaps multiplied by the smallest power of the generating root of 1 which lies in R. This will also make storing units in order to determine if an order is associated easier. Again, we will use the database at [11] to check this assumption.

Note that these two assumptions only restrict the number field in which the order is contained, not the order itself within any number field. The final assumption we will make is specific to the order. We will assume that an integral basis $\{\beta_1, \ldots, \beta_n\}$

for $\overline{R}$ and integers $c_1, \ldots, c_n, d_1, \ldots, d_n$ exist such that $\{c_1\beta_1, \ldots, c_n\beta_n\}$ is a basis for R and $\{d_1\beta_1, \ldots, d_n\beta_n\}$ is a basis for I. Recall by Proposition 1.2.92 that choosing such a basis and such integers is always possible for any free abelian group with a free abelian subgroup of the same (finite) rank. However, it may not always be possible to do this for three nested free abelian groups of the same rank. Whether it is always possible to do this specifically for an order in a number field, its conductor ideal, and its integral closure is unknown. In the cases we will consider, it will be possible.

With these assumptions laid out, we will examine orders in the number field $K = \mathbb{Q}[\alpha]$, with α a root of the polynomial $f(x) = x^3 - x^2 + 1$. Pulling from the database at [11], we note that this is a cubic number field with class number $\left|\mathrm{Cl}(K)\right| = 1$ and exactly one real embedding. Moreover, the ring of algebraic integers in this number field is $\mathbb{Z}[\alpha]$. As the ring of integers in a cubic number field with exactly one real embedding, $\mathbb{Z}[\alpha]$ admits a fundamental unit - in this case, α itself. Thus, this number field will satisfy the first two assumptions stated above.

When selecting an order to consider, we will start by selecting the conductor ideal. To find prime ideals in the number ring, we will use the MATLAB program `polyFactor.m` (included in the appendix) to factor $f(x)$ modulo a rational prime p. By Proposition 1.3.45, this will determine how p decomposes into prime ideals in the number ring. After choosing a conductor ideal, we will select one or more orders with that conductor ideal (if such orders exist) to test. Then, we will determine a basis for $\overline{R}$, R, and I as described above (if such a basis exists) and find $\left|U(\overline{R}/I)\right|$ and $\left|U(R/I)\right|$. Finally, we will make use of the MATLAB program `polyLA.m` (included in the appendix) to determine whether the order is (locally) associated. As in the quadratic case, the output of this program is a Boolean vector `[lao ao]` which indicates whether the order is locally associated and associated.

Rather than pass arguments as inputs to the program, we will edit the first few lines of `polyLA.m` directly. This is primarily because of the large amount of information we will need to input to the program. To test whether an order is (locally) associated, we will change the values on the first six lines. The following procedure shows how we would carry out this process for one such order.

1. First, we choose a conductor ideal. Using `polyFactor.m` to factor $x^3 - x^2 + 1$ modulo 5 tells us that $(5) = (5, 3 + \alpha)(5, 2 + \alpha + \alpha^2)$. Using `polyNorm.m` (included in the appendix) and the knowledge that $\mathcal{O}_K$ is a UFD, we find principal generators for these ideals to get $(5) = (-2 + \alpha)(2 + \alpha + \alpha^2)$. The ideal $(-2 + \alpha)$ has prime norm 5, and so cannot be the conductor ideal of an order. We will choose our conductor ideal to be $I = (2 + \alpha + \alpha^2)$.

2. Next, we choose an order R which has conductor ideal I. Note that $\mathbb{Z} + I$ must be contained in any such order, $\mathbb{Z} + I$ is closed under multiplication (and is thus an order in K), and $\left| {}^{\mathcal{O}_K}\!/_{\mathbb{Z}+I} \right| = 5$, a prime. Then in fact, $R = \mathbb{Z} + I$ is the only order in K with conductor ideal I.

3. We now want to select an integral basis for $\overline{R}$ following the conditions of our assumption above. In this case, we note that $\{1, \alpha, 2 + \alpha + \alpha^2\}$ is a basis for $\overline{R}$. Furthermore, $\mathbb{Z} + 5\alpha\mathbb{Z} + (2 + \alpha + \alpha^2)\mathbb{Z}$ is an index 5 additive subgroup of $\overline{R}$ which is contained in R, and thus must be the additive group of R itself. Then $\{1, 5\alpha, 2 + \alpha + \alpha^2\}$ is a basis for R. Similarly, we find that $\{5, 5\alpha, 2 + \alpha + \alpha^2\}$ is a basis for I.

4. Noting that I is a prime ideal in $\overline{R}$ of norm 25, we get that $\left| U({}^{\overline{R}}\!/_{I}) \right| = 24$. Furthermore, since the classes in ${}^{R}\!/_{I}$ can be represented by the integers modulo 5, we know that $\left| U({}^{R}\!/_{I}) \right| = 4$.

5. We are now ready to use `polyLA.m`. First, we input the minimal polynomial

for α, $f(x) = x^3 - x^2 + 1$, by setting `poly = [1 0 -1]`. Then, we enter the fundamental unit $u = \alpha$ by setting `u = [0 1 0]`. Together, these indicate the important features of K.

6. We now indicate the structure of R and I by setting `R = [1 5 1]` (the multiples of the basis elements above that form a basis for R), `I = [5 5 1]` (the multiples of the basis elements above that form a basis for I), and `basis = [1 0 0; 0 1 0; 2 1 1]` (the elements of the basis above encoded as rows of a matrix). Finally, we set `goal = 6`, which indicates how large $\left|U(\overline{R})/U(R)\right|$ needs to be for R to be locally associated.

7. Running the program, we get an output vector of `[1 1]`. The first 1 indicates that R is locally associated; the second indicates that R is associated.

Table 4.3 below gives the results from running this program on a number of orders in this same number field. We could also use this code to test orders in other number fields which satisfy the three assumptions stated earlier, though we will reserve this for only a few key examples that we will explore later.

Of course, there is room to improve this MATLAB code. We will not discuss the efficiency of the program here, but it is worth noting that there are certainly potential improvements to be made in this aspect. Instead, we will focus on the assumptions that were made and discuss briefly how the code might be altered to relax these requirements.

First, recall that we assumed that there existed some $\alpha \in \overline{R}$ such that $\overline{R} = \mathbb{Z}[\alpha]$. While this is not always the case, we know by Proposition 1.3.36 that we can create an integral basis for $\overline{R}$ using polynomials in α of a particular form. As stated previously, we can draw such an integral basis for many number rings from the database at [11]. If one first indicated the polynomials in such an integral basis, one

Table 4.2: (Locally) Associated Orders in $\mathbb{Q}[\alpha]$, where $\alpha^3 - \alpha^2 + 1 = 0$

R	I	basis	goal	Locally Associated?	Associated?
[1 2 2]	[2 2 2]	$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$	7	Yes	Yes
[1 3 3]	[3 3 3]	$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$	13	Yes	Yes
[1 4 4]	[4 4 4]	$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$	28	No	No
[1 2 4]	[4 4 4]	$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$	14	Yes	Yes
[1 4 2]	[4 4 4]	$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$	14	No	No
[1 5 1]	[5 5 1]	$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 2 & 1 & 1 \end{bmatrix}$	6	Yes	Yes
[1 6 6]	[6 6 6]	$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$	91	Yes	Yes
[1 7 1]	[7 7 1]	$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -2 & 3 & 1 \end{bmatrix}$	8	Yes	Yes
[1 11 1]	[11 11 1]	$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 6 & 8 & 1 \end{bmatrix}$	12	Yes	Yes
[1 11 11]	[11 11 11]	$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$	120	Yes	No
[1 23 23]	[23 23 23]	$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$	506	Yes	No
[1 35 1]	[35 35 1]	$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 12 & -4 & 1 \end{bmatrix}$	48	No	No

could use this to convert among relevant bases.

Second, we assumed that $\overline{R}$ admitted a fundamental unit, which greatly restricted our choices of number fields that we could consider here. However, recall that $U(\overline{R})/U(R)$ is a finite abelian group. By choosing representative units in each of the generating cosets of $U(\overline{R})/U(R)$, one could store these units and use them to determine whether R is associated. However, it should be noted that such an implementation would require prior knowledge of $\left|U(\overline{R})/U(R)\right|$. Thus, this would only be relevant if one could determine first whether such an order were locally associated, then find the generating units as described here, and finally use this to decide whether R is associated.

Finally, we assumed that an integral basis for $\overline{R}$ existed which had integer multiples that served as bases for R and I. As mentioned previously, it is unclear whether this assumption will always hold for any order R. If such a basis always exists, we certainly would not need to make the additional assumption. In the case that such a basis does not exist, one might store two separate bases which are of the form in Proposition 1.2.92: one for $\overline{R}$ over R, and one for R over I (depending on the implementation, it may be more convenient to substitute one of these bases with a basis for $\overline{R}$ over I). For the various checks that need to be made in this code, one would then need to convert among the various bases used.

4.4 HFD Orders with Non-Radical Conductor

Recall the major result from the previous section regarding the elasticity of an order in a number field.

Theorem 3.1.7. *Let R be an associated order in a number field K with radical conductor ideal I. Then for any nonzero, nonunit $\alpha \in R$, $\rho_R(\alpha) = \rho_{\overline{R}}(\alpha)$. Moreover,*

$\rho(R) = \rho(\overline{R})$.

This allows us to determine when the elasticity of an order is equal to the elasticity of its integral closure. In particular, when $\overline{R}$ is an HFD, this theorem tells us when we can also conclude that R is an HFD. Now also recall from Theorem 1.3.66 (with some of the discussion from the previous section) that when R is an order in a quadratic number field, the converse holds as well. That is, an order R in a quadratic number field is an HFD if and only if $\overline{R}$ is an HFD, R is associated, and the conductor ideal of R is radical. The question that remains, then, is whether this holds in a more general number field.

Recall the following characterization of a half-factorial order in a number field from [20]:

Theorem 3.3.1. *Let K be a number field and R an order in K with conductor ideal I. Let $I = P_1^{a_1} \dots P_k^{a_k}$ be the factorization of I into prime $\overline{R}$-ideals, and denote $Q_i := R \cap P_i$ for each $1 \leq i \leq k$. Then R is an HFD if and only if the following properties hold:*

1. *$\overline{R}$ is an HFD;*

2. *R is an associated order;*

3. *For each $1 \leq i \leq k$, $a_i \leq 4$, and letting π_i be an arbitrary prime element of $\overline{R}_{Q_i}$, $v_{\pi_i}(\mathrm{Irr}(R_{Q_i})) \subseteq \{1, 2\}$. If P_i is a principal ideal, then $a_i \leq 2$ and $v_{\pi_i}(\mathrm{Irr}(R_{Q_i})) = \{1\}$.*

Here, R_{Q_i} refers to the localization of R at the prime ideal Q_i (with $\overline{R}_{Q_i}$ analogously defined) and v_{π_i} is the valuation associated with the element π_i.

In particular, we can see that any half-factorial order in a number field must have half-factorial integral closure and must be associated. However, we will note that in this theorem, it is not explicitly required that the conductor ideal be radical for the order to be an HFD. That being said, it is also not immediately obvious that a half-factorial order in a number field with non-radical conductor ideal must exist. Throughout the remainder of this chapter, we will discuss a number of results that came to light as a result of the search for such an order. These results will narrow down where such orders might exist, making them easier to find. Finally, we will present two examples of such orders: one which is presented in [20]; and one which was discovered independently using the results presented here.

To simplify this process, we will make use of a lemma from [20]. It will be presented here in the notation used in this dissertation and in a statement that makes use of the theorem above.

Lemma 4.4.1. *Let R be an order in a number field K. Then R is an HFD if and only if the following properties hold:*

1. *$\overline{R}$ is an HFD;*

2. *R is an associated order;*

3. $\mathrm{Irr}(R) \subseteq \mathrm{Irr}(\overline{R})$*, i.e. every irreducible in R remains irreducible in $\overline{R}$.*

This result tells us that if R is an associated order in a number field whose integral closure is an HFD, we can conclude that R is an HFD if the irreducible elements of R remain irreducible in $\overline{R}$. Moreover, if any irreducible in R becomes reducible when extending to $\overline{R}$, we can conclude that R is not an HFD. We will use both of these facts to our advantage.

In the following results, we will primarily focus on orders in a number field with conductor ideal $I = P^2$ for some prime $\overline{R}$-ideal P. As we will see throughout this discussion, the cases for such orders will be dramatically different depending on whether the prime ideal P in question is principal or non-principal. We will also carefully examine the behavior of the units in $\overline{R}$. Since any half-factorial order R must be associated, i.e. $\overline{R} = R \cdot U(\overline{R})$, it will help to consider which units might multiply a given element $\alpha \in \overline{R}$ into R. We begin with the following results regarding these units.

Lemma 4.4.2. *Let R be an order in a number field K with conductor ideal $I = P^2$ for some prime $\overline{R}$-ideal P. Define $R_1 := R + P$, and for any $\alpha \in \overline{R}$, $U_\alpha := \{u \in U(\overline{R}) | u\alpha \in R\}$. Then for any $\alpha \in P$ and $u \in U(\overline{R})$, $u \in U_\alpha$ if and only if $uv \in U_\alpha$ for every $v \in U(R_1)$. In particular, $U(R_1) \subseteq U_\alpha$ for every $\alpha \in R \cap P$.*

Proof. Let $\alpha \in P$ and $u \in U(\overline{R})$, and suppose that $uv \in U_\alpha$ for every $v \in U(R_1)$. Since $1 \in U(R_1)$, this means that $u \in U_\alpha$. For the converse, suppose that $u \in U_\alpha$, i.e. $u\alpha \in R$. Then for any $v \in U(R_1)$, write $v = r + \beta$, with $r \in R$ and $\beta \in P$. Then $uv\alpha = u\alpha(r + \beta) = u\alpha r + u\alpha\beta$. Since $u\alpha$ and r are both element of R, so is their product $u\alpha r$. Since α and β are both in P, then $\alpha\beta \in P^2 = I$. Then $uv\alpha \in R+I = R$, so $uv \in U_\alpha$. □

One will note from this lemma that for any $\alpha \in R \cap P$, U_α is a subset of $U(\overline{R})$ which contains $U(R_1)$. Moreover, $U(\overline{R})/U(R_1)$ can be neatly divided into two disjoint subsets: the cosets which only contain elements of U_α; and the cosets which contain no elements of U_α. This leads us into the following theorem.

Theorem 4.4.3. *Let R be an associated order in a number field K with conductor ideal $I = P^2$ for some principal prime $\overline{R}$-ideal $P = \pi\overline{R}$ with $\pi \in R$. Let R_1 and U_α be defined as before. Then letting $U_\pi/U(R_1)$ denote the subset of $U(\overline{R})/U(R_1)$ whose cosets* *consist of elements in U_π,*

$$\left|{}^{U_\pi}\!\big/_{U(R_1)}\right| = \frac{\left|{}^{R\cap P}\!\big/_{I}\right| - 1}{\left|{}^{R_1}\!\big/_{P}\right| - 1}.$$

Proof. First, note that the assumption that $\pi \in R$ can be made without loss of generality. For any $\pi \in \overline{R}$ such that $P = (\pi)$, the fact that R is associated tells us that there is some $u \in U(\overline{R})$ such that $u\pi \in R$. Then $P = (\pi) = (u\pi)$, and thus P is generated by an element of R. Also note by the lemma that since $\pi \in R \cap P$, $U(R_1) \subseteq U_\pi$, and every coset of ${}^{U(\overline{R})}\!\big/_{U(R_1)}$ which contains an element of U_π consists entirely of elements of U_π.

Now since R and R_1 are both associated, we know they are locally associated as well. Furthermore, R is ideal-preserving, so we know that $R_1 = R + P$ has conductor ideal P, a prime $\overline{R}$-ideal. Then

$$\left|{}^{U(\overline{R})}\!\big/_{U(R_1)}\right| = \frac{\left|U\left({}^{\overline{R}}\!\big/_{P}\right)\right|}{\left|U\left({}^{R_1}\!\big/_{P}\right)\right|} = \frac{\left|{}^{\overline{R}}\!\big/_{P}\right| - 1}{\left|{}^{R_1}\!\big/_{P}\right| - 1}.$$

Using the fact that $\left|{}^{\overline{R}}\!\big/_{P}\right| = \left|{}^{P}\!\big/_{I}\right|$ and $\left|{}^{R_1}\!\big/_{P}\right| = \left|{}^{R}\!\big/_{R\cap P}\right|$, this gives

$$\left|{}^{P}\!\big/_{I}\right| - 1 = \left(\left|{}^{R}\!\big/_{R\cap P}\right| - 1\right) \cdot \left|{}^{U(\overline{R})}\!\big/_{U(R_1)}\right|.$$

We will now make use of the fact that R is an associated order and consider elements of $P \backslash I$. Since P is principal and generated by π, we know that any such element can be written as $\alpha\pi$ for some $\alpha \in \overline{R}\backslash P$. Furthermore, since R is associated, we can write each $\alpha \in \overline{R}\backslash P$ as $\alpha = ru$ for some $r \in R\backslash P$ and $u \in U(\overline{R})$. Then every element of $P\backslash I$ is expressible as $ru\pi$ for some $r \in R\backslash P$ and $u \in U(\overline{R})$.

Now consider the nonzero cosets of ${}^{P}\!/_{I}$, which must all be of the form $ru\pi + I$, as above. First, note that if $v \equiv u \pmod{U(R_1)}$, i.e. $v^{-1}u \in U(R_1)$, then we can write $u^{-1}v = s + \beta$, with $s \in R\backslash P$ and $\beta \in P$. Then $ru\pi + I = rv(v^{-1}u)\pi + I = rv(s+\beta)\pi + I = (rs)v\pi + I$, with $rs \in R\backslash P$ and $v \in U(\overline{R})$. Then we could instead choose to represent this nonzero coset using the unit $v \in U(\overline{R})$ rather than u. Thus, when selecting the unit in the representation of a nonzero coset $ru\pi + I$, we can limit our choice of u to only one coset representative from each coset in ${}^{U(\overline{R})}\!/_{U(R_1)}$.

Now suppose that we have written some nonzero coset of ${}^{P}\!/_{I}$ as $ru\pi + I$, with u chosen from one of the $\left|{}^{U(\overline{R})}\!/_{U(R_1)}\right|$ coset representatives we selected, as outlined above. Suppose also that $s \in R\backslash P$ with $s \equiv r \pmod{P}$, i.e. $r - s \in P$. Then $ru\pi + I = su\pi + (r-s)u\pi + I = su\pi + I$. Thus, without changing the coset representative u, we can limit our selection of r to only a single coset representative from each nonzero coset of ${}^{R}\!/_{R \cap P}$.

In this way, we know that we can represent each of the $\left|{}^{P}\!/_{I}\right| - 1$ nonzero cosets in ${}^{P}\!/_{I}$ by first selecting one of the $\left|{}^{U(\overline{R})}\!/_{U(R_1)}\right|$ cosets in ${}^{U(\overline{R})}\!/_{U(R_1)}$, then selecting one of the $\left|{}^{R}\!/_{R \cap P}\right| - 1$ nonzero cosets in ${}^{R}\!/_{R \cap P}$. However, recall from above that

$$\left|{}^{P}\!/_{I}\right| - 1 = \left(\left|{}^{R}\!/_{R \cap P}\right| - 1\right) \cdot \left|{}^{U(\overline{R})}\!/_{U(R_1)}\right|.$$

Then in fact, each distinct choice of coset $uU(R_1) \in {}^{U(\overline{R})}\!/_{U(R_1)}$ and nonzero coset $r + I \in {}^{R}\!/_{R \cap P}$ must produce a distinct nonzero coset $ru\pi + I \in {}^{P}\!/_{I}$.

Finally, we will make the observation that if $u \in U_\pi$, then $r(u\pi) \in R$ for any $r \in R$. Moreover, if $r \in R\backslash P$, then $r + I \in U({}^{R}\!/_{I})$. Then for any $u \in U(\overline{R})$ such that $ru\pi \in R$, we have $u\pi + I = (r+I)^{-1}(ru\pi + I) \in {}^{R}\!/_{I}$, so $u\pi \in R$ and thus $u \in U_\pi$. Then a nonzero coset $ru\pi + I \in {}^{P}\!/_{I}$ is in ${}^{R \cap P}\!/_{I}$ if and only if $u \in U_\pi$. The number of nonzero cosets in ${}^{R \cap P}\!/_{I}$ is $\left|{}^{R \cap P}\!/_{I}\right| - 1$, and each of these cosets can be expressed uniquely as $ru\pi + I$, with r a coset representative of one of the $\left|{}^{R}\!/\!_{R\cap P}\right| - 1$ nonzero cosets of ${}^{R}\!/\!_{R\cap P}$ and u a coset representative of one of the $\left|{}^{U_\pi}\!/\!_{U(R_1)}\right|$ cosets in ${}^{U(\overline{R})}\!/\!_{U(R_1)}$ consisting of elements of U_π. Then

$$\left|{}^{R\cap P}\!/\!_{I}\right| - 1 = \left(\left|{}^{R}\!/\!_{R\cap P}\right| - 1\right)\left|{}^{U_\pi}\!/\!_{U(R_1)}\right| \implies \left|{}^{U_\pi}\!/\!_{U(R_1)}\right| = \frac{\left|{}^{R\cap P}\!/\!_{I}\right| - 1}{\left|{}^{R}\!/\!_{R\cap P}\right| - 1} = \frac{\left|{}^{R\cap P}\!/\!_{I}\right| - 1}{\left|{}^{R_1}\!/\!_{P}\right| - 1}.$$

□

With these tools in hand, we will now examine how the behavior of these units may force irreducibles in R to reduce in $\overline{R}$. Throughout this discussion, we will keep in mind Lemma 4.4.1.

Lemma 4.4.4. *Let R be an associated order in a number field K with conductor ideal $I = P^2$ for some principal prime $\overline{R}$-ideal $P = \pi\overline{R}$ with $\pi \in R$. Let U_π be as before. If $U_\pi \cdot U_\pi = \{uv | u, v \in U_\pi\} \neq U(\overline{R})$, then R is not an HFD.*

Proof. By Lemma 4.4.1, it will suffice to show that there is some irreducible element of R which reduces in $\overline{R}$. Assume that $U_\pi \cdot U_\pi \neq U(\overline{R})$. Then there is some $u \in U(\overline{R})$ which cannot be written as a product of two elements in U_π. Then let $\alpha = u\pi^2$, and note that $\alpha = u\pi \cdot \pi$. Since neither $u\pi$ nor π is a unit in $\overline{R}$, α is reducible in $\overline{R}$. We will now show that α is irreducible in R.

Suppose that $\alpha = \beta\gamma$ for some $\beta, \gamma \in R$. Then $u\pi^2 = \beta\gamma$, with π a prime element of $\overline{R}$, so one of three cases must hold: $\pi^2 | \beta$ and γ is a unit; $\pi^2 | \gamma$ and β is a unit; or $\pi | \beta$ and $\pi | \gamma$. In either of the first two cases, we are done. Then suppose that $\pi | \beta$ and $\pi | \gamma$, and write $\beta = c\pi$ and $\gamma = d\pi$ for some $c, d \in \overline{R}$. Then $\alpha = u\pi^2 = \beta\gamma = (cd)\pi^2$, so $u = cd$. Then necessarily, $c = uv$ and $d = v^{-1}$ for some $v \in U(\overline{R})$. Then note that since $\beta = uv\pi \in R$, $uv \in U_\pi$. On the other hand, since $\gamma = v^{-1}\pi \in R$, $v^{-1} \in U_\pi$. Then $u = (uv)v^{-1} \in U_\pi \cdot U_\pi$, a contradiction. Then α must be irreducible in R. Since an irreducible element of R exists which reduces in $\overline{R}$, R is not an HFD. $\square$

Lemma 4.4.5. *Let R be an associated order in a number field K with conductor ideal $I = P^2$ for some principal prime $\overline{R}$-ideal $P = \pi\overline{R}$ with $\pi \in R$. Let R_1, U_π and ${}^{U_\pi}\!/_{U(R_1)}$ be as above, and let $m = \left|{}^{U_\pi}\!/_{U(R_1)}\right|$. If*

$$\frac{m(m+1)}{2} < \left|{}^{U(\overline{R})}\!/_{U(R_1)}\right|,$$

then R is not an HFD.

Proof. From the previous lemma note that if $U_\pi \cdot U_\pi \neq U(\overline{R})$, then R is not an HFD. Then considering these units modulo $U(R_1)$, R will not be an HFD in the case that ${}^{U_\pi}\!/_{U(R_1)} \cdot {}^{U_\pi}\!/_{U(R_1)} \neq {}^{U(\overline{R})}\!/_{U(R_1)}$. Now since ${}^{U_\pi}\!/_{U(R_1)}$ is a finite set with m elements, the number of possible products of two elements from this set is m^2. However, since $\overline{R}$ is commutative, the number of distinct products in ${}^{U_\pi}\!/_{U(R_1)} \cdot {}^{U_\pi}\!/_{U(R_1)}$ is at most the m^{th} triangular number, $\frac{m(m+1)}{2}$. Then if

$$\frac{m(m+1)}{2} < \left|{}^{U(\overline{R})}\!/_{U(R_1)}\right|,$$

there are not enough distinct products to cover every element in ${}^{U(\overline{R})}\!/_{U(R_1)}$, so R cannot be an HFD. $\square$

Using these lemmas, we can now show the following result, which will rule out the possibility of certain orders from being half-factorial.

Theorem 4.4.6. *Let R be an order in a number field K with conductor ideal $I = P^2$ for some principal prime $\overline{R}$-ideal $P = \pi\overline{R}$ with $\pi \in R$, and let $p \in \mathbb{N}$ be the rational prime lying under P. If the inertial degree $f := f(P|p) \leq 3$, then R is not an HFD.*

Proof. First, note that if R is not an associated order, then R is not an HFD by Theorem 3.3.1. Then we will focus on the case when R is associated. Recall that $\left|\overline{R}/P\right| = p^f$, with f being the inertial degree of P over p. We will show the result in three cases: when $f = 1$; when $f = 2$; and when $f = 3$.

First assume $f = 1$. Since R is associated (and thus ideal-preserving), $R_1 := R + P$ must be an order with conductor ideal P. However, Lemma 4.1.3 tells us that the norm of the conductor ideal of an order cannot be a rational prime. Then this case is impossible.

Now assume $f = 2$, i.e. $\left|\overline{R}/P\right| = \left|P/I\right| = p^2$. Then since $I \subsetneq R \cap P \subsetneq P \subsetneq R_1 \subsetneq \overline{R}$, it must be the case that $\left|\overline{R}/R_1\right| = \left|R_1/P\right| = \left|P/R \cap P\right| = \left|R \cap P/I\right| = p$. By Theorem 4.4.3, this means that $m := \left|U_\pi/U(R_1)\right| = 1$. Then

$$\left|U(\overline{R})/U(R_1)\right| = \frac{\left|U(\overline{R}/P)\right|}{\left|U(R_1/P)\right|} = \frac{p^2-1}{p-1} = p + 1 > 1 = \frac{m(m+1)}{2},$$

so by Lemma 4.4.5, R is not an HFD.

Finally, assume $f = 3$, i.e. $\left|\overline{R}/P\right| = \left|P/I\right| = p^3$. As before, $I \subsetneq R \cap P \subsetneq P \subsetneq R_1 \subsetneq \overline{R}$, so $\left|R_1/P\right|$ and $\left|R \cap P/I\right|$ must be either p or p^2. Note from Theorem 4.4.3 that $\left|R \cap P/I\right| \geq \left|R_1/P\right|$, so we can consider this in two cases. If $\left|R \cap P/I\right| = \left|R_1/P\right|$, then Theorem 4.4.3 tells us that $\left|U_\pi/U(R_1)\right| = 1$. As before, Lemma 4.4.5 will show us that R cannot be an HFD. If $\left|R \cap P/I\right| = p^2$ and $\left|R_1/P\right| = p$, then $m := \left|U_\pi/U(R_1)\right| = p+1$, so $\frac{m(m+1)}{2} = \frac{p^2+3p+2}{2}$. On the other hand,

$$\left|U(\overline{R})/U(R_1)\right| = \frac{\left|U(\overline{R}/P)\right|}{\left|U(R_1/P)\right|} = \frac{p^3-1}{p-1} = p^2 + p + 1.$$

One can easily verify that for $p > 2$, $p^2 + p + 1 > \frac{p^2+3p+2}{2}$. Once again, Lemma 4.4.5

gives us that R is not an HFD. □

Immediately from this theorem, we get the following corollary.

Corollary 4.4.7. *Let R be an order in a cubic number field K with conductor ideal $I = P^2$ for some principal prime $\overline{R}$-ideal P. Then R is not an HFD.*

These results serve to tell us when a particular order in a number field cannot be an HFD. Similarly, we can examine the irreducible elements in an order to see when it must be an HFD. First, we need the following lemma.

Lemma 4.4.8. *Let R be an associated order in a number field K with conductor ideal $I = P^2$ for some prime $\overline{R}$-ideal P. Then any irreducible element in R which lies outside of I remains irreducible in $\overline{R}$.*

Proof. Let $\alpha \in R\backslash I$ be irreducible, and write $\alpha = \beta\gamma$ for some $\beta, \gamma \in \overline{R}$. Since $\alpha \notin I = P^2$, we know that either β or γ must lie outside P. Without loss of generality, assume that $\gamma \notin P$. We will also let U_α, U_β, and U_γ be as above. Since R is an associated order, we know that none of these three sets are empty.

Let $v \in U_\gamma$, i.e. $v\gamma \in R$. Then if $u \in U_\beta$, note that $(uv)\alpha = (u\beta)(v\gamma) \in R$. Then $uv \in U_\alpha$, so $vU_\beta \subseteq U_\alpha$. Similarly, if $u \in U_\alpha$, then $u\alpha = u\beta\gamma = (uv^{-1}\beta)(v\gamma) \in R$. Since $v\gamma \in R\backslash P$, we know that $v\gamma + I \in U({}^{R}\!/\!{}_{I})$. Then $uv^{-1}\beta + I = (u\alpha + I)(v\gamma + I)^{-1} \in {}^{R}\!/\!{}_{I}$, so $uv^{-1} \in U_\beta$. Thus, $v^{-1}U_\alpha \subseteq U_\beta \implies U_\alpha \subseteq vU_\beta$. Therefore, $U_\alpha = vU_\beta$ for any $v \in U_\gamma$.

Now note that since $\alpha \in R$, $1 \in U_\alpha$. Then $v^{-1} \in U_\beta$, so $\alpha = (v^{-1}\beta)(v\gamma)$, with both $v^{-1}\beta$ and $v\gamma$ lying in R. Since α is irreducible in R, this means that either $v^{-1}\beta$ or $v\gamma$ must be a unit in R. Then either β or γ is a unit in $\overline{R}$, meaning that α remains irreducible in $\overline{R}$. □

From Lemma 4.4.1, we know that half-factorial orders are intrinsically linked to irreducible elements which reduce in the integral closure. The lemma we have just shown tells us that to find such an element (or prove such an element cannot exist), we only need to consider irreducible elements in the conductor ideal. This gives the following result.

Theorem 4.4.9. *Let R be an associated order in a number field K such that $\left|\mathrm{Cl}(K)\right| = 2$, i.e. $\overline{R}$ is an HFD which is not a UFD. Let $I = P^2$ be the conductor ideal of R for some non-principal $\overline{R}$-ideal P. Then R is an HFD.*

Proof. Since $\overline{R}$ is an HFD and R is an associated order, Lemma 4.4.1 tells us that it will suffice to show that every irreducible in R remains irreducible in $\overline{R}$. By Lemma 4.4.8, we only need to check the irreducibles which lie in I. Note that since $I = P^2$ for a non-principal prime $\overline{R}$-ideal P, it must be the case that I is principal and generated by an irreducible element $\pi \in \mathrm{Irr}(\overline{R})$.

Now let $\alpha \in I$ be irreducible in R. Since $I = (\pi)$, we know that $\alpha = \beta\pi$ for some $\beta \in \overline{R}$. Since R is an associated order, we can write $\beta = ru$ for some $r \in R$ and $u \in U(\overline{R})$. Then $\alpha = (u^{-1}\beta)(u\pi)$, with $u^{-1}\beta, u\pi \in R$. Since α is irreducible in R, this means that either β or π is a unit; since $\pi \in I$, it must be the case that β is the unit. Then the only elements of I which are irreducible in R are associates of π, which are also irreducible in $\overline{R}$. Then every irreducible in R remains irreducible in $\overline{R}$, so R is an HFD. □

We can now use this result to produce an example of a half-factorial order in a number field whose conductor ideal is non-radical.

Example 4.4.10. Let $K = \mathbb{Q}[\alpha]$, with α a root of $x^3 + 4x - 1$. From the database at [11], we get that the ring of algebraic integers in K is $\mathcal{O}_K = \mathbb{Z}[\alpha]$, $\left|\mathrm{Cl}(K)\right| = 2$, and

$\mathcal{O}_K$ admits the fundamental unit α. Using Proposition 1.3.45 and `polyFactor.m`, we can see that the rational prime 3 factors as $3\overline{R} = (3, 1+\alpha)(3, 2+2\alpha+\alpha^2)$, with both of these prime factors being non-principal. Then let $I = (3, 2+2\alpha+\alpha^2)^2 = (2-4\alpha+\alpha^2)$ and $R = \mathbb{Z} + I$, an order in K with conductor ideal I. Then R is an order in a number field whose integral closure is an HFD and whose conductor ideal is $I = P^2$, with P a non-principal prime $\overline{R}$-ideal. Noting that $\overline{R} = \mathbb{Z} + \alpha\mathbb{Z} + (2 - 4\alpha + \alpha^2)\mathbb{Z}$, $R = \mathbb{Z} + 9\alpha\mathbb{Z} + (2-4\alpha+\alpha^2)\mathbb{Z}$, and $I = 9\mathbb{Z} + 9\alpha\mathbb{Z} + (2-4\alpha+\alpha^2)\mathbb{Z}$, we can once again use the MATLAB program `polyLA.m` to see that R is an associated order. Then by the theorem, R is an HFD.

Another similar example comes from [20].

Example 4.4.11. Let $K = \mathbb{Q}[\alpha]$, with α a root of $x^3 - 8x - 19$. Letting $P = (2, 1+\alpha+\alpha^2)$ (one of the non-principal primes lying over 2), $I = P^2$, and $R = \mathbb{Z} + I$, we have that R is a half-factorial order in K with non-radical conductor ideal I. This is shown in [20] and can also be verified using the process from the previous example.

Chapter 5

Conclusion and Future Work

Throughout this dissertation, we have explored the properties of orders in a number field. We began by defining associated, ideal-preserving, and locally associated subrings and exploring how these properties can give us insight into the structure of an order in a number field. Then, we examined elasticity in orders of a number field; in particular, we looked at when an order might have the same elasticity as its integral closure or its ring of formal power series. In both cases, we are motivated by a desire to use what is known about a simpler or more well-studied type of ring to provide information about the ring we are interested in. Finally, we used what we had found to explicitly construct examples of associated, ideal-preserving, locally associated, and half-factorial orders in number fields.

In this chapter, we will conclude this discussion by first restating the major original results from this dissertation. Then, we will state a handful of conjectures, questions, and directions for future work in this area.

5.1 Major Results

Arguably the two most important original results from this dissertation are the following elasticity results from Chapter 3.

Theorem 3.1.7. *Let R be an associated order in a number field K with radical conductor ideal I. Then for any nonzero, nonunit $\alpha \in R$, $\rho_R(\alpha) = \rho_{\overline{R}}(\alpha)$. Moreover, $\rho(R) = \rho(\overline{R})$.*

Theorem 3.2.5. *Let R be an associated order in a number field K with radical conductor ideal I. Then for any nonzero, nonunit $f \in R[[x]]$, $\rho_{R[[x]]}(f) = \rho_{\overline{R}[[x]]}(f)$. Moreover, $\rho(R[[x]]) = \rho(\overline{R}[[x]])$.*

Throughout this dissertation, we concerned ourselves with the relationships that may arise between two rings which satisfy certain properties. The two results stated here apply this knowledge to the realm of factorization, describing how we might apply our knowledge of elasticity in one ring to find the elasticity of another ring.

Recall that HFDs are defined as atomic domains with elasticity one. Then as we have seen, these results naturally apply to the study of half-factorial orders in a number field. Although these results rely on the fact that the conductor ideal I is radical, we saw from the characterization of half-factorial orders in [20] that a half-factorial order in a number field does not necessarily need to have radical conductor ideal. In the previous chapter, we provided two examples of such orders, one drawn from [20], the other found using the methods developed in this dissertation.

One significant application of the previous results to the specific case that the order in question is an HFD was the following result.

Theorem 3.3.3. *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.

5.2 Conjectures and Future Work

In the interest of developing this field further and encouraging future work, we will now discuss questions that remain open, conjectures to the answers of those questions, and additional directions that may naturally follow from the work done here. First, we will explore how the major results of this paper may be expanded upon.

Conjecture 5.2.1. *Let R be an order in a number field K. Then $\rho(R[[x]]) = \rho(R)$.*

This conjecture would be a vast generalization of Theorem 3.3.3. It is worth noting that the work done thus far in determining the elasticity of such a ring of power series $R[[x]]$ has depended on relating it to the elasticities of $\overline{R}[[x]]$ and $\overline{R}$. Thus, tackling this conjecture in full generality would be quite difficult, especially when the elasticity of R and $\overline{R}$ are not the same. Instead, we might focus on some particular cases first.

Conjecture 5.2.2. *Let R be a ring of algebraic integers, i.e. an integrally closed order in a number field. Then $\rho(R[[x]]) = \rho(R)$.*

As we have discussed previously, rings of algebraic integers are much more well-structured and well-understood than more general orders in a number field. Thus, this case might be easier to prove than the more general case above. In fact, we know from Theorem 3.3.2 that this conjecture holds in the case that R is an HFD. However, as we have stated previously, the techniques used in the original proof of Theorem 3.3.2, found in [14], will not apply to this more general statement.

Similarly, we might consider the following conjecture which initially served as the motivation for this research project.

Conjecture 5.2.3. *Let R be an order in a number field. Then R is an HFD if and only if $R[[x]]$ is an HFD.*

Again, this serves as a more specific, easier to consider version of Conjecture 5.2.1. By Theorems 3.2.5, 3.3.1, and 3.3.2, it would actually suffice to consider this conjecture for half-factorial orders which have non-radical conductor ideal. Moreover, it is already known that if R is an HFD, then $\overline{R}$ and $\overline{R}[[x]]$ are HFDs as well; a proof of this conjecture would likely benefit from leveraging this knowledge. A good first step toward this will be to check whether the rings of formal power series over the orders from Examples 4.4.10 and 4.4.11 are half-factorial.

It would seem at this point that Conjectures 5.2.2 and 5.2.3 are more likely to hold than Conjecture 5.2.1. If the general conjecture does not hold, we might consider the following question.

Question 5.2.4. Let R be an order in a number field. Can we in general use properties of R to determine the elasticity of $R[[x]]$?

A good first step toward answering this question may be to first consider the following.

Question 5.2.5. Let R be an order in a number field. If we know the elasticity of $\overline{R}$, what additional information do we need to know to find the elasticity of R? For instance, can we determine some multiplier $m \in \mathbb{Q}$, perhaps based on the prime factorization of the conductor ideal I of R and the set $R \cdot U(\overline{R}) \subseteq \overline{R}$, such that $\rho(R) = m\rho(\overline{R})$? Can we similarly determine $\rho(R[[x]])$ from $\rho(\overline{R}[[x]])$?

Related to these questions is the following conjecture which would go a long way toward understanding how the elasticity in orders in a number field might evolve.

Conjecture 5.2.6. *Let R be an order in a number field and T an intermediate order, i.e. $R \subseteq T \subseteq \overline{R}$. Then $\rho(T) \leq \rho(R)$; in particular, if R is an HFD, then T is an HFD as well.*

This conjecture is actually a generalization of Theorem 3.1.4, which states that this inequality holds when $T = \overline{R}$. The theorem tells us that factorization can only get "worse" when moving from a ring of algebraic integers to an order contained within. This conjecture plays off of that same idea: that factorization should not "improve" by then passing to an order even further removed from $\overline{R}$. However, the techniques used to prove Theorem 3.1.4 relied on the Davenport constant, which only tell us the elasticity of a ring of algebraic integers, not a more general order in a number field; thus, the proof will not immediately generalize.

For the HFD portion of this conjecture, one will note that if R is an HFD order with radical conductor ideal, then any intermediate order will automatically also be an HFD by Theorem 3.1.7. Furthermore, since any intermediate order strictly containing the orders from Examples 4.4.10 and 4.4.11 are either integrally closed or have prime conductor ideal, the conjecture holds for these orders as well. Whether this will hold in general is still open.

We will now consider questions related to Theorem 3.3.1 from [20].

Question 5.2.7. Can the characterization of half-factorial orders in [20] be stated in an easier-to-check way or solely ideal-theoretic manner? Are any of the allowances in this characterization extraneous? For instance, do there exist any half-factorial orders whose conductor ideal has divisor P^2 for principal prime ideal P or divisor P^4 for non-principal prime ideal P?

The following conjecture generalizes one of the conditions from Theorem 3.3.1 to the case when the order in question may not be an HFD.

Conjecture 5.2.8. *Let R be an order in a number field such that $\rho(R) = \rho(\overline{R})$. Then R is an associated order.*

One will note that this question naturally arises from Theorem 3.3.1, since the condition that R is a half-factorial order can equivalently be stated as $\rho(R) = \rho(\overline{R}) = 1$. Finally, we have some conjectures and questions related to associated, locally associated, and ideal-preserving orders.

Conjecture 5.2.9. *Let R be an order in a number field. Then R is associated if and only if R is both ideal-preserving and locally associated.*

Recall from Corollaries 2.4.15 and 4.2.3 that this bidirectional statement will hold if we also assume that R either has radical conductor ideal or lies in a quadratic number field. Moreover, if R is associated, then we know that R is both ideal-preserving and locally associated without any additional assumptions. Whether an example exists of an ideal-preserving and locally associated order which is not associated is still open.

The last set of questions arises from Table 4.1 in the previous chapter.

Question 5.2.10. Consider Table 4.1. Can we describe the patterns that arise in a way that will provide a characterization of locally associated (or associated) orders in quadratic number fields? If such a characterization exists, can it be generalized to orders in higher-degree number fields? Can we also find a simple characterization of ideal-preserving orders in higher-degree number fields?

Recall that any half-factorial order in a number field must be associated (and thus locally associated and ideal-preserving). By finding an easy characterization of any of these properties, we will therefore be making it easier to find orders with the potential of being half-factorial.

Appendices

Appendix A MATLAB Code

quadLA.m

```
function [lao,ao] = quadLA(n,d)
    %determines whether the index n array in Q[sqrt(d)] is (locally)
        associated
    %fu is the fundamental unit
    %lao will indicate whether R is LA
    %ao will indicate whether R is associated
pf = primePowers(n);    %factors n into prime numbers
a = size(pf);
a = a(1);       %the number of distinct prime factors of n
ao = true;
fu = quadFundUnit(d);   %finds the fundamental unit in Rbar

%first, we will calculate the sizes of U(Rbar/I) and U(R/I)
num = 1;    %this will hold the size of U(Rbar/I)
for i=1:a
    if pf(i,1) == 2
        if mod(d,8) == 5        %if p is inert
            num = num*2^(2*(pf(i,2)-1))*3;
        else
            ao = false;
            if mod(d,8) == 1    %if p splits
                num = num*2^(2*(pf(i,2)-1));
            else                %if p ramifies
                num = num*2^(2*pf(i,2)-1);
            end
        end
    else
```

```
        if jacobiSymbol(d,pf(i,1))==-1      %if p is inert
            num = num*pf(i,1)^(2*(pf(i,2)-1))*(pf(i,1)^2-1);
        else
            ao = false;
            if jacobiSymbol(d,pf(i))==1     %if p is split
                num = num*(pf(i,1)^(pf(i,2)-1)*(pf(i,1)-1))^2;
            else                            %if p is ramified
                num = num*pf(i,1)^(2*pf(i,2)-1)*(pf(i,1)-1);
            end
        end
    end
end
%now, ao actually tells us if R is ideal-preserving

den = eulerPhi(n);  %this will always be the size of U(R/I)
goal = num/den;     %if this is the minimal power of fu that lands in R, R is locally associated

b = [mod(fu,n)];      %this will hold powers of fu mod n to determine if they lie in R
for i=1:goal-1
    if b(i,2)==0
        lao = false;    %if too small a power of fu lies in R, not LA
        ao = false;     %if not LA, certainly not associated
        return;
    end
    if i==goal-1
        break;      %we don't need to calculate fu^goal
    end
    %now calculate next power of fu
    if mod(d,4)==1
        b = [b; mod(polyMult(b(i,:),fu,[(1-d)/4,-1]),n)];
    else
        b = [b; mod(polyMult(b(i,:),fu,[-d,0]),n)];
    end
end

lao = true; %if we make it this far, R is locally associated
%R is associated iff it is locally assocaited and ideal-preserving
%thus, we don't need to check anything more to determine associated
```

primePowers.m

```
function p = primePowers(n)     %factors n into prime powers
                                %each row of p is [q a], where q^a
                                   divides n

pf = factor(n);     %find the prime factorization of n
p = [pf(1) 1];      %this will encode pf more usefully
j = 1;              %counter for the following loop

for i=2:length(pf)
    if pf(i)==pf(i-1)
        p(j,2) = p(j,2)+1;
    else
        p = [p; pf(i) 1];
        j = j+1;
    end
end
```

polyMult.m

```
function M = polyMult(a,b,p)
    %multiplies a*b in Q[alpha], where alpha is a root of the
       polynomial p
    %a=a1+a2*alpha+...+an*alpha^(n-1)
    %b=b1+b2*alpha+...+bn*alpha^(n-1)
    %p(x)=p1+p2*x+...+pn*x^(n-1)+x^n
n = size(a);
n = n(2);   %n = the degree [Q[alpha]:Q], also the length of a,b,p
A = zeros(n,n,n);
B = zeros(n,2*n-1);
p=-p;       %now, p encodes alpha^n=p1+p2*alpha+...+pn*alpha^(n-1)

B(1:n,1:n)=eye(n);
B(1:n,n+1)=p;       %the i^th column of B will encode alpha^i

for i=n+2:2*n-1
    q = [zeros(1,i-n-1),p(1:n-(i-n-1))];
    B(1:n,i)=q;
    for j=n+1:i-1       %fills in the columns of B
        B(1:n,i)=B(1:n,i)+B(1:n,j)*p(n-(i-j)+1);
    end
end

for i=1:n
    for j=1:n
        for k=1:n
            A(i,j,k)=B(k,i+j-1);    %forms an n by n by n matrix,
               where A(i,j) encodes alpha^(i-1)*alpha^(j-1)
        end
    end
end

M=basisMult(a,b,A);
    %carries out the multiplication a*b; M=a*b=M1+M2*alpha+...+Mn*
       alpha^(n-1)
```

quadFundUnit.m

```
function u = quadFundUnit(d)
    %determines the fundemantal unit in Q[sqrt(d)]

if mod(d,4)==1      %determines the denominator of the integers
    c = 2;
else
    c = 1;
end

b = 1;
while true      %searches for units; unit with smallest b is fu
    if isSquare(d*b^2-c^2)
        a = sqrt(d*b^2-c^2);
        break;
    end
    if isSquare(d*b^2+c^2)
        a = sqrt(d*b^2+c^2);
        break;
    end
    b = b+1;
end

if mod(d,4)==1          %outputs in form u=[a b]=a+b*\alpha
    u = [(a-b)/2 b];
        %alpha = sqrt(d) if d=2,3 mod 4, (1+sqrt(d))/2 if d=1 mod 4
else
    u = [a b];
end
```

isSquare.m

```
function y = isSquare(n)
    %determines if the positive integer n is a square
    %outputs true if square, false if not
if n==1
    y = 1;      %1 is a square
    return;
end

pf = primePowers(n);    %factor n into primes
a = size(pf);
a = a(1);               %the number of distinct prime factors of n
y = true;

for i=1:a
    if mod(pf(i,2),2)== 1
        y = false;
        %n is square iff every prime divides an even number of times
        return;
    end
end
```

polyFactor.m

```
function M = polyFactor(poly,p)
    %factors the polynomial poly modulo the prime p
    %poly=poly(1)+poly(2)*x+...+poly(n)*x^(n-1)+x^n
n = size(poly);
n = n(2);        %n is the degree of the polynomial to be factored
poly = [poly,1];    %appends 1 onto poly to represent the x^n term
boom = false;
    %a Boolean variable that will indicate when we find a factor

if mod(poly(1),p)==0
    N = polyFactor(poly(2:n),p);
    s = size(N);
    M = [0,1,zeros(1,n-1);N zeros(s(1),n+1-s(2))];
    %if poly has a factor of x, pull it out and factor what remains
    return;
end

for i=1:floor(n/2)
    %searches for factors of degree <n/2 to determine if poly
       factors
    a = [1,zeros(1,i-1),1];
        %initializes potential factor of degree i, starts as x^i+1
    b = [zeros(1,n-i),1];
        %initializes other factor st poly = a*b, starts as x^(n-i)
    a = [a,zeros(1,n-i)];
    b = [b,zeros(1,i)];     %fills in remaining coeffients with 0
    done = false;
        %boolean variable to determine when we are done with a
           certain degree i
```

```
while ~done

    for j=1:n-i
        boom = false;       %resets boom to false
        goal = mod(poly(j),p);
        for k=1:j-1
            goal = mod(goal-b(k)*a(j+1-k),p);
        end
        %after this loop if a*b=poly mod p, goal=a(1)*b(j) mod p
        for c=1:p-1
            if mod(c*a(1),p)==goal
                b(j)=c;
                %sets b(j) to the value needed to make poly=a*b,
                    if one exists
                boom = true;
                break;
            end
        end
        if ~boom
            break;
            %if no b(j) value is possible, moves to the next
               potential factor a
        end
    end

    if boom
        for j=n-i+1:n
            goal = 0;
            for k=1:j
                goal = mod(goal+b(k)*a(j+1-k),p);
        end
        %after this loop, goal is the coefficient of x^(j-1)
            in a*b
        if goal~=mod(poly(j),p)
            boom = false;
            break;
            %if this value doesn't match the coefficient of
               x^(j-1) in poly, try another a
        end
    end
end
if boom
    break;
    %exits the process if a factorization poly=a*b has been
       found
end
a(1) = mod(a(1)+1,p);
%this line and the loop moves to the next potential factor a
for j=2:i
    if a(j-1)==0
        a(j) = mod(a(j)+1,p);
    else
        break;
    end
end
done = true;
for j=1:i
    done = done&&(a(j)==0);
end
if a(1)==0
    a(1)=1;
```

```
            %we know at this point that poly has no factors of x, so
                a shouldn't either
        end
    end
    if boom
        break;
            %exits the process if a factorization poly=a*b has been
               found
    end
end

if boom
    N = polyFactor(b(1:n-i),p);
        %if poly=a*b, factor b further; a is already irreducible
    s = size(N);
    M = [a;N zeros(s(1),n+1-s(2))];
        %output is a matrix whose rows encode the factors of poly
else
    M = mod(poly,p);
        %if no factorization was found, return the original poly
end
```

polyNorm.m

```
function N = polyNorm(a,roots)
    %finds the norm in Q[alpha] of the element a
    %a = a1+a2*alpha+...+an*alpha^(n-1)
    %roots are the n conjugates of alpha
n = length(a);  %n is the degree [Q[alpha]:Q], also the length of a
evals = zeros(1,n);
    %this will hold the values of sigma(a) for each embedding sigma
       of Q[alpha] into C

for i=1:n
    for j = 1:n
        evals(i) = evals(i)+a(j)*roots(i)^(j-1);
            %fills in the values of evals
    end
end

N = round(prod(evals));
    %multiplies the values of the embeddings to give norm
```

polyLA.m

```
poly = [1 0 -1];
%the minimal polynomial for alpha, working in Q[alpha]
u = [0 1 0];
%fundamental unit of Rbar in standard basis 1,alpha,...,alpha^(n-1)

%values above this line are specific only to the number field
%values below this line are specific to the order within that field
R = [1 5 1];
    %integer multiples of the basis that serve as basis for R
I = [5 5 1];
    %integer multiples of the basis that serve as basis for I
basis = [1 0 0; 0 1 0; 2 1 1];
    %a basis for Rbar, each row is b1+b2*alpha+...+bn*alpha^(n-1)
    %integer multiples of this basis should work as bases for R, I
goal = 6;   %|U(Rbar/I)|/|U(R/I)|

%values ABOVE this line should be changed; everything else stays
basisi = round(inv(basis));
    %inverse of basis to allow for change of basis
n = length(poly);   %the degree [Q[alpha]:Q]
b = [mod(u*basisi,I)*basis;zeros(goal-2,n)];
    %this will hold powers of generating units to determine whether
       they lie in R
for i=1:goal-1
    if ~any(mod(b(i,:)*basisi,R))
        [false, false]  %if too small a power lies in R, not locally
            associated or associated
        return;
    else
```

```
        if i~=goal-1
            b(i+1,:) = mod(polyMult(b(i,:),u,poly)*basisi,I)*basis;
                %find next power if necessary
        end
    end
end

a = zeros(1,n); %this will count through elements of Rbar/I
                %a is stored in terms of the non-standard basis
while true
    %will verify that every element Rbar has an associate in R
    a(1) = a(1)+1;
    for i=2:n
        if a(i-1)==R(i-1)
            a(i) = a(i)+1;
        else
            break;
        end
    end
    a = mod(a,R);
    if ~any(a)
        break;
    end

    done = false;
    for i=1:goal-1
        if ~any(mod(polyMult(a*basis,b(i,:),poly)*basisi,R))
            done = true;
            break;
        end
    end
    if ~done
        [true, false]   %locally associated, but not associated
        return;
    end
end

[true true]   %both locally associated and associated
```

Bibliography

[1] Mark Thomas Batell and Jim Coykendall. Elasticity in polynomial-type extensions. *Proceedings of the Edinburgh Mathematical Society*, 59:581 – 590, 2013.

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

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

[4] Keith Conrad. The conductor ideal of an order. *Expository Paper*, 2019. `https://kconrad.math.uconn.edu/blurbs/gradnumthy/conductor.pdf`.

[5] Jim Coykendall. Half-factorial domains in quadratic fields. *Journal of Algebra*, 235(2):417–430, 2001.

[6] Jim Coykendall. On the integral closure of a half-factorial domain. *Journal of Pure and Applied Algebra*, 180:25–34, 2003.

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

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

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

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

[11] The LMFDB Collaboration. The L-functions and modular forms database. `https://www.lmfdb.org`, 2024. [Online; accessed 16 April 2024].

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

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

[14] Grant Moles. The HFD property in orders of a number field. *All Theses*, 3851, 2022. `https://tigerprints.clemson.edu/all_theses/3851/`.

[15] Władysław Narkiewicz. A note on elasticity of factorizations. *Journal of Number Theory*, 51:46–47, 1995.

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

[17] John E. Olson. A combinatorial problem on finite abelian groups, i. *Journal of Number Theory*, 1(1):8–10, 1969.

[18] John E. Olson. A combinatorial problem on finite abelian groups, ii. *Journal of Number Theory*, 1(2):195–199, 1969.

[19] Martine Picavet-L'Hermitte. Some remarks on half-factorial orders. *Rendiconti del Circolo Matematico di Palermo*, 52:297–307, 2003.

[20] Balint Rago. A characterization of half-factorial orders in algebraic number fields. *arXiv preprint arXiv:2304.08099*, 2024.

[21] Robert J. Valenza. Elasticity of factorization in number fields. *Journal of Number Theory*, 36:212–218, 1990.

[22] Muhammad Zafrullah. Rings between d [x] and k [x]. *Houston J. Math*, 17(1):109–129, 1991.

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

[24] Abraham Zaks. Half-factorial-domains. *Israel Journal of Mathematics*, 37:281–302, 1980.