NTNU – Trondheim
Norwegian University of
Science and Technology

Unique Factorization of Ideals

Eirik Holteberg Vold

Master of Science in Mathematics
Submission date: November 2013
Supervisor: Petter Andreas Bergh, MATH

Norwegian University of Science and Technology
Department of Mathematical Sciences

Abstract

We study Dedekind domains, where ideals factorize uniquely into a product of prime ideals. This subject is of interest as general elements in these rings do not necessarily factorize uniquely.

Norsk sammendrag:
Vi studerer hvordan idealer faktoriseres til et unikt produkt av primidealer i et Dedekind-område. Dette er av interesse siden et generelt element i en slik ring ikke nødvendigvis fakoriseres unikt.

Preface

This Master's thesis is the product of my final semester as a student at the Natural Science with Teacher Education programme at NTNU. There have been some great years with hard work, long nights, and many moments to remember. I am very grateful for forcing myself throughout several hard courses in mathematics and science to come to the place where I am today. Working with the thesis has been very rewarding, and definitely the part of my studies which I have enjoyed the most.

There are some acknowledgements to be made. Most of all, I would like to thank my supervisor Professor Petter Andreas Bergh for his suggestion of topic, and for all his help during the months of writing. Thanks to my study friends and room-mates; over the years in Trondheim there have been many great moments. Last but not least, I would like to thank my friends back home and my ever-supportive family.

Eirik Holteberg Vold
Trondheim, November 2013

Contents

1

Introduction

The ring of integers consists of elements that factorize uniquely into prime numbers, but if we extend the ring with the square root of an integer there is no guarantee that factorization of elements remains unique. For this reason we will study the behaviour of ideals in these rings instead. It turns out that ideals in such rings as described, at least when the ring is a *Dedekind domain*, eventually factorize into prime ideals. In addition, this factorization is unique. Consider the following theorem:

Theorem: Unique Factorization into Prime Ideals. *In a Dedekind domain D every proper nonzero ideal I is a product of prime ideals in D, and this factorization is unique in the sense that if*

$$I = P_1 P_2 \cdots P_k = Q_1 Q_2 \cdots Q_n,$$

where P_i and Q_j are prime ideals, then $k = n$, and after relabelling (if necessary)

$$P_i = Q_i, \ i \in \{1, 2, \ldots, k\}.$$

Our motivation for the study is to prove this theorem. As this will be a study in algebraic number theory we will focus on rings, and especially *integral domains*, which are generalizations of the integers and provide a natural setting for studying divisibility. Furthermore, we will study the following chain of class inclusions:

$$\left\{\text{Fields}\right\} \subsetneq \left\{\begin{matrix}\text{Euclidean}\\ \text{domains}\end{matrix}\right\} \subsetneq \left\{\begin{matrix}\text{Principal ideal}\\ \text{domains}\end{matrix}\right\} \subsetneq \left\{\begin{matrix}\text{Dedekind}\\ \text{domains}\end{matrix}\right\} \subsetneq \left\{\begin{matrix}\text{Noetherian}\\ \text{domains}\end{matrix}\right\}$$

These rings, or domains if you like, are all integral domains by definition. During the text we will prove that each inclusion holds. The reason for listing the completed chain, already in the introduction, is to give the reader an early overview of the integral domains in question. That is, we will also study *unique factorization domains*, which we will see is not included in the chain.

2

Integral Domains and Ideals

2.1 Commutative Rings

We start off by defining a *ring*, explicitly remarking that all rings in this Master's thesis will be rings with **unity**, which means that every ring contain the multiplicative identity element 1. Although we assume the reader to be familiar with the concepts of group theory, rings, fields, and terms concerning these algebraic subjects, it is important to point out this definition; several authors of mathematical publications may not necessarily define a ring to be with unity.

Definition. A **ring** R is a nonempty set with two binary operations, $+$ and $\cdot$, such that for all $a, b, c \in R$ we have the following:

i) $(R, +)$ is an abelian group, that is, R is abelian under addition.

ii) Multiplication is associative: $(ab)c = a(bc)$.

iii) The distributive laws hold: $a(b + c) = ab + ac$ and $(a + b)c = ac + bc$.

iv) $1 \in R$ is the multiplicative identity such that $1 \cdot a = a \cdot 1 = a$.

Remark. In algebraic number theory we are only interested in **commutative rings**, that is, $ab = ba$ for all $a, b \in R$. We need to state the following for further reading:

NB! Whenever we write "ring" we always mean a commutative ring.

Next, we define a *subring*. More often than not it is easier to show that a set is a subring of an already known ring to ensure that the set is a ring.

DEFINITION. A **subring** S is a nonempty subset of a ring R, where S itself is a ring with multiplicative identity $1_S = 1_R$.

REMARK. When S is a subset of a ring R, denoted $S \subseteq R$, we can also state the definition as the following:

$$S \text{ is a subring } \Leftrightarrow \ a - b, ab, 1_R \in S \text{ for all } a, b \in S.$$

DEFINITION. Let R be a ring with a nonzero element $r \in R$. If there exists an inverse $r^{-1} \in R$ such that $r^{-1}r = 1$, then r is called a **unit**.

REMARK. It is equivalent saying $r \in R$ is a unit if $r \mid 1$, that is, r divides 1 as we have $1 = r^{-1}r$.

EXAMPLE. In the ring of integers, denoted by $\mathbb{Z}$, we have 1 and -1 as the only units; there are no other elements with an inverse.

2.2 Integral Domains

This study will focus on *integral domains*. It is most common to define integral domains to be commutative. As we only work with commutative rings it is obviously the definition we will use as well.

DEFINITION. An **integral domain** D is a (commutative) ring with no zero-divisors, that is, if $ab = 0$ for any $a, b \in D$, then either $a = 0$ or $b = 0$.

EXAMPLE. The ring $\mathbb{Z}$ is an integral domain as multiplication of elements is commutative and 0 is a factor whenever a product is 0.

From the integral domain we can derive a **field**, which is a integral domain where every nonzero element has an inverse, that is, every nonzero element is a unit. A field that is a subring of another field we refer to as a **subfield**.

Later we will see what consequence the inclusion of a new element to integral domains causes. For instance, we can extend the ring of integers with a new element, say $\sqrt{n}$, where n is either a positive or a negative integer, such that we obtain a set, denoted

$$\mathbb{Z}[\sqrt{n}] = \{a + b\sqrt{n} \mid a, b \in \mathbb{Z}\},$$

which is another example of an integral domain.

EXAMPLE. The ring $\mathbb{Z}[\sqrt{n}]$ is an integral domain. First of all, we need to ensure that $\mathbb{Z}[\sqrt{n}]$ is a ring. We have $\mathbb{Z}[\sqrt{n}] \subseteq \mathbb{C}$, that is, $\mathbb{Z}[\sqrt{n}]$ is a subset of the field of complex numbers. Hence $\mathbb{Z}[\sqrt{n}]$ is a subset of a ring. We take two arbitrary elements $(a + b\sqrt{n}), (c + d\sqrt{n}) \in \mathbb{Z}[\sqrt{n}]$, hence $a, b, c, d \in \mathbb{Z}$, and observe that

$$(a + b\sqrt{n}) - (c + d\sqrt{n}) = \big((a - c) + (b - d)\sqrt{n}\big) \in \mathbb{Z}[\sqrt{n}],$$

and

$$(a + b\sqrt{n}) \cdot (c + d\sqrt{n}) = \big((ac + nbd) + (ad + bc)\sqrt{n}\big) \in \mathbb{Z}[\sqrt{n}].$$

The multiplicative identity $1 \in \mathbb{C}$ is also an element in $\mathbb{Z}[\sqrt{n}]$. Hence $\mathbb{Z}[\sqrt{n}]$ is a subring of $\mathbb{C}$, and $\mathbb{C}$ is an integral domain as it is a field. Any subring of an integral domain is also an integral domain.

As $\sqrt{n}$ always is a root of the quadratic polynomial $x^2 - n$ we call $\mathbb{Z}[\sqrt{n}]$ a **quadratic domain**. Note that we always consider n to be **squarefree**, which means that we will not work with $\mathbb{Z}[\sqrt{n}]$ where n is divisible by a squared prime number. For instance, $\pm1, \pm2, \pm3, \pm5, \pm6, \pm7, \pm10$ are all squarefree numbers, whereas $\pm4, \pm8, \pm9, \pm16, \pm18$ are not squarefree as every number have a squared prime as a factor. An extension finds place whenever we add a new element, which is not part of the ring from before, to the ring. When n is a squarefree integer then $\sqrt{n}$ is not a element in $\mathbb{Z}$, except when $n = 1$, which would imply $\mathbb{Z}[\sqrt{n}] = \mathbb{Z}$. Consider another example, let $n = 18$, which is not a squarefree number. We get $\mathbb{Z}[\sqrt{18}] = \mathbb{Z}[3\sqrt{2}] \subseteq \mathbb{Z}[\sqrt{2}]$, that is, $\mathbb{Z}[\sqrt{18}]$ is a subring of $\mathbb{Z}[\sqrt{2}]$. In fact, for every n that is not squarefree we have that $\mathbb{Z}[\sqrt{n}]$ is a subring of another quadratic domain where the integer under the square root *is* squarefree.

An integral domain D is not necessarily a field, but we can always construct a field from an integral domain. If we invert every nonzero element $b \in D$, then the set of products $a \cdot b^{-1}$, where $a \in D$, contains a inverse for every nonzero element ab^{-1} in that set. Hence we have a field, called the *quotient field* of D.

DEFINITION. The **quotient field** of an integral domain D is defined by the set

$$\mathrm{Quot}(D) = \{a \cdot b^{-1} \mid a, b \in D,\ b \neq 0\}.$$

EXAMPLE. The field of rational numbers, denoted by $\mathbb{Q}$, is the quotient field of $\mathbb{Z}$ since $\mathrm{Quot}(\mathbb{Z}) = \{a \cdot b^{-1} \mid a, b \in \mathbb{Z},\ b \neq 0\} = \{\frac{a}{b} \mid a, b \in \mathbb{Z},\ b \neq 0\} = \mathbb{Q}$.

REMARK. If we let $b = b^{-1} = 1 \in D$, then clearly $D \subseteq \mathrm{Quot}(D)$ as we still have every $a \in D$ left in the set. It follows that D is a subring of $\mathrm{Quot}(D)$.

2.3 Ideals

A central subject of the thesis is, as its title suggests, *ideals*. We define ideals as subsets of rings closed under multiplication with elements from the ring, that is, every product is again an element in the ideal.

DEFINITION. An **ideal** I is a nonempty subset of a ring R where the following conditions are satisfied:

i) $a, b \in I \;\Rightarrow\; a - b \in I$.

ii) $r \in R,\ a \in I \;\Rightarrow\; ra \in I$.

REMARK. As R is a commutative ring we only need to define *left* ideals since every left ideal is also a *right* ideal. Hence every ideal is a *two-sided ideal*.

EXAMPLE. In a ring R any element $r \in R$ generates an ideal. We denote the ideal generated by r as $\langle r \rangle$. Define the subset

$$I = \langle r \rangle = rR = \{ra \mid a \in R\}.$$

We show the following:

i) If $ra, rb \in I$, then $ra - rb = r(a - b) \in I$.

ii) If $b \in R$ and $ra \in I$, then $(ra)b = r(ab) \in I$.

We see that $ra - rb \in I$ and $(ra)b \in I$, hence I is an ideal in R.

EXAMPLE. Every ideal in $\mathbb{Z}$ is of the form $n\mathbb{Z}$, where n is a nonnegative integer. This follows from the previous example, letting $r = n$ and $R = \mathbb{Z}$. If an ideal in $\mathbb{Z}$ is generated by more than one element, say $a, b \in \mathbb{Z}$, then the element $(a - b) \in \mathbb{Z}$ is also a generator. Therefore, every ideal in $\mathbb{Z}$ is of the form $n\mathbb{Z}$, where n is a nonnegative integer; we do not need to include negative integers as $-n\mathbb{Z} = n\mathbb{Z}$ for all $n \in \mathbb{Z}$.

In any ring R we always have 0 as an element. The ideal generated by 0, denoted (0), is the subset of R that contains 0 and no other element. Also, we notice that R itself always satisfy the conditions of being an ideal. Therefore, R and (0) are the **trivial ideals** in R. Furthermore, we call every ideal I that is a proper subset of R, denoted $I \subsetneq R$, a **proper ideal**.

The majority of the theorems in the thesis concern ideals, but before we start proving any theorems we will state three important propositions, which will be used frequently in many proofs to follow.

Proposition 2.1. *If I is an ideal in a ring R, then $RI = I$.*

Proof: Let $a \in I$. Since I is an ideal we have $Ra \subseteq I$. As $Ra \subseteq I$ for all $a \in I$, then $RI \subseteq I$.

Conversely, we have that $1 \in R$, so it follows that $1 \cdot a = a \in Ra \subseteq RI$. The fact that $a \in RI$ for all $a \in I$ implies $I \subseteq RI$. Hence $RI = I$. □

Proposition 2.2. *If I is an ideal in a ring R, then*

$$I = R \;\Leftrightarrow\; 1 \in I.$$

Proof: Suppose $I = R$. Every ring R contains the identity element 1, thus $1 \in I$.

Conversely, suppose $1 \in I$. Take any element $r \in R$. As I is an ideal we have $1 \cdot r = r \in I$. Hence $I = R$. □

REMARK. It follows that $\langle 1 \rangle = R$, where $\langle 1 \rangle$ is the ideal generated by 1.

Proposition 2.3. *If R is a ring with an element $u \in R$, then*

$$\langle u \rangle = R \;\Leftrightarrow\; u \text{ is a unit.}$$

Proof: Suppose $R = \langle u \rangle = \{ur \mid r \in R\}$. As $1 \in R$ we have $ur = 1$ for some $r \in R$. Hence u is a unit.

Conversely, suppose u is a unit. We have that $\langle u \rangle = \{ur \mid r \in R\}$, and since u is a unit we have $u^{-1} \in R$. It follows that $u \cdot u^{-1} = 1 \in \langle u \rangle$, hence $\langle u \rangle = R$ by Proposition 2.2. □

DEFINITION. An ideal M is a **maximal ideal** in a ring R if we have the following:

i) $M \subsetneq R$.

ii) For every ideal I in R, where $M \subseteq I$, either $I = M$ or $I = R$.

EXAMPLE. In the ring $\mathbb{Z}$ every ideal of the form $p\mathbb{Z}$, where $p \in \mathbb{Z}$ is a prime number, is a maximal ideal. As $p \neq 1$ we have that $p\mathbb{Z}$ is a proper ideal in $\mathbb{Z}$. If $p\mathbb{Z} \subseteq n\mathbb{Z}$, where n is a positive integer, then $n \mid p$. Since p is a prime the only two options are $n = p$ or $n = 1$. It follows that either $n\mathbb{Z} = p\mathbb{Z}$ or $n\mathbb{Z} = \mathbb{Z}$. Hence $p\mathbb{Z}$ is a maximal ideal.

Theorem 2.4. *If I is an ideal in a ring R, then*

$$R/I \text{ is a field} \;\Leftrightarrow\; I \text{ is a maximal ideal.}$$

Proof: Suppose R/I is a field and let J be an ideal in R such that

$$I \subsetneq J \subseteq D.$$

There exists some $a \in J$ where $a \notin I$, thus $a + I \in R/I$ is a nonzero element, and as R/I is a field there exists an element $b + I \in R/I$ such that

$$(a + I)(b + I) = ab + I = 1 + I.$$

Hence

$$ab - 1 \in I \subsetneq J.$$

We have $a \in J$ and $b \in R$, and as J is an ideal we get $ab \in J$. Hence

$$1 = ab - (ab - 1) \in J,$$

and $J = R$ by Proposition 2.2. Thus I is a maximal ideal.

Conversely, we suppose I is a maximal ideal and that R/I is not a field. There must exist a nonzero element that is not a unit, say $r + I \in R/I$, hence $1 + I \notin \langle r \rangle + I$, which implies that $\langle r \rangle + I \subsetneq R$. Since $r + I \neq 0 + I$ we have $r \notin I$. Hence $I \subsetneq \langle r \rangle + I$, and

$$I \subsetneq \langle r \rangle + I \subsetneq R,$$

which contradicts I being maximal. Thus R/I is a field. □

Definition. An integral domain D is called a **PID** (principal ideal domain) if all ideals are **principal**, that is, for each ideal I in D there exists an element $r \in D$ that generates I.

Remark. If D is a PID, then every ideal is of the form $rD = \langle r \rangle$ for some $r \in D$.

Example. The ring $\mathbb{Z}$ is a PID; every ideal is of the form $n\mathbb{Z}$, where $n \in \mathbb{Z}$. Let I be an ideal in $\mathbb{Z}$. If I is either equal to (0) or $\mathbb{Z}$, then I is generated by the element 0 or 1, respectively. Hence it is a principal ideal. Therefore, suppose I is a proper nonzero ideal, thus there exists a nonzero element $a \in I$. Both a and 0 are elements in I, hence $-a = (0 - a) \in I$, thus we may assume that a is a positive integer. Let n denote the least positive integer in I. We can write a as

$$a = nq + r$$

for some $q, r \in \mathbb{Z}$, where $0 \leq r < n$. As I is an ideal we have $nq \in I$, hence $r = (a - nq) \in I$. It follows that $r = 0$, otherwise $r \in I$ contradicts the minimality of n. Hence $a = nq$, thus

$$I = \langle n \rangle = n\mathbb{Z}.$$

2.4 Prime Ideals

We dedicate the last section in this chapter to *prime ideals*; as they are central to our main theorem we need to study prime ideals closely. There are different definitions of prime ideals, like whether or not a prime ideal needs to be a proper ideal. We see some authors that define the ring itself as a prime ideal [3, p. 206], but in this text we define a prime ideal to be a proper ideal.

DEFINITION. If P is a proper ideal in a ring R, then P is a **prime ideal** if

$$a, b \in R \text{ and } ab \in P \;\Rightarrow\; a \in P \text{ or } b \in P.$$

EXAMPLE. The ideal $p\mathbb{Z}$ is a prime ideal in $\mathbb{Z}$ for any prime number $p \in \mathbb{Z}$.

EXAMPLE. The ideal $6\mathbb{Z}$ is not a prime ideal in $\mathbb{Z}$. We have that $6\mathbb{Z}$ is a proper ideal, and both $2, 3 \in \mathbb{Z}$, where $2 \cdot 3 = 6 \in 6\mathbb{Z}$, but $2, 3 \notin 6\mathbb{Z}$. We can show the same for any $n\mathbb{Z}$ where n is not a prime, the only exception is $n = 0$.

REMARK. If D is a ring, then

$$(0) \text{ is a prime ideal } \Leftrightarrow \; D \text{ is an integral domain.}$$

Suppose (0) is a prime ideal. Let $a, b \in D$ be such that $ab \in (0)$, hence $ab = 0$. Either $a \in (0)$ or $b \in (0)$, which implies either $a = 0$ or $b = 0$. Hence D is an integral domain.

Conversely, suppose D is an integral domain. If $ab = 0$, then either $a = 0$ or $b = 0$. If $ab \in (0)$, then $ab = 0$, and either $a \in (0)$ or $b \in (0)$. Hence (0) is a prime ideal.

In the following example we will see how number theory can be used to ensure that an ideal is a prime ideal. The prime ideal in the following example will be used in an example following the main theorem in Section 6.3.

EXAMPLE. The ideal generated by 2 and $(1+\sqrt{-5})$, denoted $P = \langle 2, (1+\sqrt{-5})\rangle$, is a prime ideal in $\mathbb{Z}[\sqrt{-5}]$. We have that

$$P = \langle 2, (1+\sqrt{-5})\rangle = \{2r + (1+\sqrt{-5})s \mid r, s \in \mathbb{Z}[\sqrt{-5}]\}.$$

We first show what a general element in P looks like. Suppose $(a + b\sqrt{-5}) \in P$, where $a, b \in \mathbb{Z}$, then the linear combination

$$a + b\sqrt{-5} = 2r + (1+\sqrt{-5})s$$

is fulfilled for some $r, s \in \mathbb{Z}[\sqrt{-5}]$, say $r = (e + f\sqrt{-5})$ and $s = (g + h\sqrt{-5})$, where $e, f, g, h \in \mathbb{Z}$. Hence

$$\begin{aligned} a + b\sqrt{-5} &= 2(e + f\sqrt{-5}) + (1 + \sqrt{-5})(g + h\sqrt{-5}) \\ &= (2e + g - 5h) + (2f + g + h)\sqrt{-5}. \end{aligned}$$

It is clear that $a = (2e + g - 5h)$ and $b = (2f + g + h)$. Suppose g is an even number, then both $(2e+g)$ and $(2f+g)$ are even as well, and they are both odd numbers whenever g is odd. We say $(2e+g)$ and $(2f+g)$ have the same **parity** as they are both even or both odd at the same time. It follows that $a = (2e+g-5h)$ and $b = (2f + g + h)$ have the same parity whenever $(a + b\sqrt{-5}) \in P$. Now, we assume there exist some $a, b \in \mathbb{Z}$ of same parity such that $(a+b\sqrt{-5}) \notin P$. Hence the linear combination above is not satisfied for any $e, f, g, h \in \mathbb{Z}$. We rewrite $a = (2e + g - 5h)$ and $b = (2f + g + h)$ as

$$a - 2e = g - 5h \quad \text{and} \quad b - 2f - 6h = g - 5h.$$

It follows that

$$a - 2e = b - 2(f + 3h),$$

where $-2e$ and $-2(f + 3h)$ is always even. Therefore, the only restriction such that this linear combination does not have an solution is if a and b is of different parity, but that contradicts the assumption. Hence, if a and b have the same parity, then $(a + b\sqrt{-5}) \in P$.

Next, we show that P is a prime ideal. We choose two arbitrary elements $(a + b\sqrt{-5}), (c + d\sqrt{-5}) \in \mathbb{Z}[\sqrt{-5}]$ such that

$$(a + b\sqrt{-5})(c + d\sqrt{-5}) \in P.$$

We have to show that if, say $(a+b\sqrt{-5}) \notin P$, then we must have $(c+d\sqrt{-5}) \in P$. If $(a + b\sqrt{-5}) \notin P$, then either a is odd and b even or vice versa, that is to say, different parity. We have that

$$(a + b\sqrt{-5})(c + d\sqrt{-5}) = (ac - 5bd) + (ad + bc)\sqrt{-5} \in P,$$

which means $(ac - 5bd)$ and $(ad + bc)$ have the same parity. If a is odd, then b is even, and so $5bd$ and bc are even. It follows that ac and ad have the same parity, and since a is odd, c and d have the same parity. Hence $(c + d\sqrt{-5}) \in P$. If a is even, then ac and ad is even, and $5bd$ and bc have the same parity. As b now is odd, c and d must have the same parity, hence $(c + d\sqrt{-5}) \in P$. Thus P is a prime ideal in $\mathbb{Z}[\sqrt{-5}]$.

Theorem 2.5. *If I is an ideal in a ring R, then*

$$R/I \text{ is an integral domain } \Leftrightarrow \text{ } I \text{ is a prime ideal.}$$

Proof: Suppose R/I is an integral domain. Let $a, b \in R$ be such that $ab \in I$. We have that $ab + I$ is the zero-element of R/I, hence

$$(a + I)(b + I) = ab + I = 0 + I \in R/I.$$

As R/I is an integral domain either $(a + I) = 0 + I$ or $(b + I) = 0 + I$, which again implies that $a \in I$ or $b \in I$. Hence I is a prime ideal.

Conversely, assume that I is a prime ideal. I is a proper ideal of R, hence $1 \notin I$, and $1 + I \in R/I$, thus R/I is a ring with identity $1 + I$. Next, we let $(a + I), (b + I) \in R/I$ be such that $(a + I)(b + I) = 0 + I$, which implies $ab + I = 0 + I$. Thus $ab \in I$. It follows that either $a \in I$ or $b \in I$, hence $(a + I) = 0 + I$ or $(b + I) = 0 + I$. Hence we have shown that R/I has no zero-divisors. Thus R/I is an integral domain. □

Theorem 2.6. *In any ring every maximal ideal is a prime ideal.*

Proof: Let I be a maximal ideal in a ring R. We have that R/I is a field by Theorem 2.4. Therefore, R/I is also an integral domain, and I is a prime ideal by Theorem 2.5. □

Theorem 2.7. *If D is a PID with a proper nonzero ideal P, then*

$$P \text{ is a maximal ideal } \Leftrightarrow \ P \text{ is a prime ideal.}$$

Proof: We have by Theorem 2.6 that a maximal ideal in any ring is a prime ideal.

Conversely, we assume that P is a prime ideal in D that is *not* maximal. There must exist some ideal I in D such that

$$P \subsetneq I \subsetneq D.$$

Since D is a PID we have $P = \langle a \rangle$ and $I = \langle b \rangle$ for some nonzero $a, b \in D$. We have $\langle a \rangle \subsetneq \langle b \rangle$, hence $a = rb$ for some $r \in D$. We have $rb = a \in P$, thus either $r \in P$ or $b \in P$ as P is a prime ideal. If $b \in P$, then $I = \langle b \rangle \subseteq P \subsetneq I$, which is clearly a contradiction, thus $r \in P$. We have $r = sa$ for some $s \in D$, hence $a = (sa)b = a(sb)$, where $sb = 1$ since a is nonzero. Thus b is a unit, and $I = \langle b \rangle = D$ by Proposition 2.3. This contradicts $I \subsetneq D$, hence P is a maximal ideal. □

From our basic number theory we know that any prime number $p \in \mathbb{Z}$ that divides a product ab, where $a, b \in \mathbb{Z}$, must also divide either a or b. We are not restricted to integers while working with primes; a *prime* can be defined for any ring by the following generalized definition.

DEFINITION. A nonzero element $p \in R$ is a **prime** in the ring R if the following conditions are satisfied:

i) p is not a unit.

ii) If $p \mid ab$ for some $a, b \in R$, then either $p \mid a$ or $p \mid b$.

Theorem 2.8. *If R is a ring with a nonzero element $p \in R$, that is not a unit, then*

$$\langle p \rangle \text{ is a prime ideal } \Leftrightarrow \text{ } p \text{ is a prime in } R.$$

Proof: Assume $\langle p \rangle$ is a prime ideal in R. Let $a, b \in R$ be such that $p \mid ab$, hence $ab \in \langle p \rangle$. Thus either $a \in \langle p \rangle$ or $b \in \langle p \rangle$. It follows that either $p \mid a$ or $p \mid b$, hence p is a prime.

Conversely, let p is a prime in R. We let $a, b \in R$ be such that $ab \in \langle p \rangle$. There must exist some $r \in R$ such that $rp = ab$, thus $p \mid ab$. Since p is a prime we have that $p \mid a$ or $p \mid b$. Suppose $p \mid a$, then there exists some $s \in R$ such that $sp = a$. Hence $a \in \langle p \rangle$, and $\langle p \rangle$ is a prime ideal. If $p \nmid a$, then $p \mid b$, and we are left with the same result. □

Theorem 2.9. *If P is a proper ideal in a ring R, then*

$$P \text{ is a prime ideal } \Leftrightarrow \text{ for all ideals } A \text{ and } B \text{ where } AB \subseteq P, \text{ either } A \subseteq P \text{ or } B \subseteq P.$$

Proof: Let P be a proper ideal in a ring R. We need to show that P is a prime ideal if the following holds for all ideals A and B in R:

$$AB \subseteq P \text{ } \Rightarrow \text{ } A \subseteq P \text{ or } B \subseteq P.$$

Let $a, b \in R$ be such that $ab \in P$. We let $A = \langle a \rangle$ and $B = \langle b \rangle$ such that $AB = \langle a \rangle \langle b \rangle = \langle ab \rangle \subseteq P$. Following the implication we must have that either $\langle a \rangle \subseteq P$ or $\langle b \rangle \subseteq P$, but then $a \in P$ or $b \in P$, and P is by the definition a prime ideal.

To show the converse, we first assume that there exists a proper ideal P that does *not* satisfy the right-implication above. We need to show that P is not a prime in this case. We have

$$AB \subseteq P \text{ } \not\Rightarrow \text{ } A \subseteq P \text{ or } B \subseteq P,$$

where A and B are ideals in R. Hence there exists some ideals A and B such that $A \nsubseteq P$ and $B \nsubseteq P$, while $AB \subseteq P$. There must exist some $a \in A$ and $b \in B$, where $a, b \notin P$, but we have that $ab \in AB \subseteq P$, and by the definition P is not a prime ideal. □

Theorem 2.10. *Let A and D be integral domains such that $D \subseteq A$. If P is a prime ideal in A, then $P \cap D$ is a prime ideal in D.*

Proof: Obviously $P \cap D \subseteq D$, and we will first show that $P \cap D$ is an ideal in D. Let $a, b \in P \cap D$, hence $a, b \in P$ and $a, b \in D$. We have that $(a-b) \in P$ since P is an ideal. We also have $(a - b) \in D$ as a ring is closed under subtraction, thus $(a - b) \in P \cap D$. Next, suppose $a \in P \cap D$ and $r \in D \subseteq A$. As P is an ideal in A, we have $ra \in P$. We also have $ra \in D$ as both $a \in D$ and $r \in D$, thus $ra \in P \cap D$. Hence $P \cap D$ is an ideal in D.

Next, we will show that $P \cap D$ is a prime ideal. As P is a prime ideal in A it is a proper ideal, hence $1 \notin P$, which implies $1 \notin P \cap D$. As $1 \in D$ we have that $P \cap D \subsetneq D$. Let $a, b \in D \subseteq A$ be such that $ab \in P \cap D$, hence either $a \in P$ or $b \in P$ as P is a prime ideal in A. Thus either $a \in P \cap D$ or $b \in P \cap D$, hence $P \cap D$ is a prime ideal in D. □

3

Noetherian Domains

3.1 Modules

In this chapter we will define a *Noetherian domain*, but first we define the term *module*, which is a generalization of a vector space. A module over a specific ring R is referred to as an "R-module". When type of ring is insignificant we will frequently just write "module".

Definition. Let R be a ring and let $(M, +)$ be an abelian group. M is an **R-module** if there exists a function $f : R \times M \to M$, with $(r, m) \mapsto rm$, such that the following hold for all $r, r_1, r_2 \in R$ and $m, m_1, m_2 \in M$:

i) $r(m_1 + m_2) = rm_1 + rm_2$.

ii) $(r_1 + r_2)m = r_1m + r_2m$.

iii) $(r_1r_2)m = r_1(r_2m)$.

iv) $1_R \cdot m = m$.

Remark. This is in fact the definition of a *left* R-module, but every left module is also a *right* module over a commutative ring.

Example. A ring R is actually an R-module over itself as $(R, +)$ is an abelian group. We often regard the ring as a module; if R has a property as a module, then R has that very same property as a ring.

DEFINITION. If R is a ring and M an R-module, then N is a **submodule** of M if the following hold:

i) N is a subgroup of M.

ii) $r \in R,\ n \in N \ \Rightarrow\ rn \in N$.

EXAMPLE. Since every ideal I in a ring R also is a subgroup of $(R, +)$, and in addition, every $r \in R$ and $a \in I$ are such that $ra \in I$, then clearly every ideal in R is a submodule of R, that is, whenever we regard R as a module.

3.2 Noetherian Modules and Rings

We have our definition of a module; we proceed by defining a *Noetherian module* and a *Noetherian ring*.

DEFINITION. If R is a ring and M an R-module, then M is a **Noetherian module** if there for each ascending chain of submodules,

$$N_1 \subseteq N_2 \subseteq N_3 \subseteq \cdots,$$

exists a positive integer k such that $N_k = N_{k+1} = N_{k+2} = \cdots$.

We follow up this definition of a Noetherian module by defining a Noetherian ring, using the fact that we can regard it as a module.

DEFINITION. A ring R is a **Noetherian ring** if it is Noetherian as an R-module.

REMARK. If R is a Noetherian ring, then for each ascending chain of ideals,

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots,$$

there exists a positive integer $k \in \mathbb{Z}$ such that $I_k = I_{k+1} = I_{k+2} = \cdots$.

Knowing that a ring is Noetherian is important as it has a very useful property – namely, every set of ideals in a ring contains a maximal element. In other words, there is at least one set that contains an element that is a maximal ideal in the ring. Similarly for modules, we have that every set of submodules contains a maximal element. In order to prove this fact we first need to know the following definition.

DEFINITION. Let R be a ring and M an R-module. If M contains some finite set of elements that generates M, then M is **finitely generated**.

As the matter of fact, if a module M is Noetherian, then each submodule of M is a finitely generated module, which we will see in the following theorem, where we will prove three equivalent statements.

Theorem 3.1. *If R is a ring and M an R-module, then the following are equivalent:*

a) M is Noetherian.

b) Each submodule of M is finitely generated.

c) Each nonempty set of submodules of M contains a maximal element.

Proof:

$a) \Rightarrow b)$: Let M be a Noetherian R-module. Assume that there exists some submodule N that is not finitely generated. Choose some $x_1 \in N$ and let $N_1 = Rx_1$, which is a submodule of M. Since N is not finitely generated we have $N_1 \subsetneq N$. We now choose some $x_2 \in N$, where $x_2 \notin N_1$, and let $N_2 = Rx_1 + Rx_2$. Thus $N_1 \subsetneq N_2$, and as N is not finitely generated we have $N_2 \subsetneq N$. If we continue in the same fashion, then we obtain submodules $N_i = Rx_1 + Rx_2 + \cdots + Rx_i$ for all $i \geq 1$. It follows that

$$N_1 \subsetneq N_2 \subsetneq \cdots \subsetneq N_k \subsetneq N_{k+1} \subsetneq \cdots ,$$

which is an infinite properly ascending chain of submodules of M. This contradicts the fact that M is Noetherian. Hence N is finitely generated.

$b) \Rightarrow c)$: Let M be an R-module where every submodule is finitely generated. Let S be a nonempty set of submodules of M. Suppose N_1 is an element in S. If N_1 is not a maximal element in S, then N_1 is properly contained in another submodule, say N_2, which also is an element in S. If N_2 is not a maximal element in S, then N_2 is properly contained in N_3, and so on. We assume that there exists no maximal element in S, and we obtain an infinite properly ascending chain of elements in S:

$$N_1 \subsetneq N_2 \subsetneq N_3 \subsetneq \cdots .$$

Now let $N = N_1 \cup N_2 \cup N_3 \cup \cdots$, indexed by the set $\Lambda = \{1, 2, 3, \ldots\}$. We take two elements $x, y \in N$ and let $r \in R$, hence $x \in N_\alpha$ and $y \in N_\beta$ for some $\alpha, \beta \in \Lambda$. We have that either $N_\alpha \subseteq N_\beta$ or $N_\beta \subseteq N_\alpha$, meaning that both x and y lie in one submodule N_α or N_β. Hence $(x - y)$ and rx lie in the same submodule. This implies $(x - y) \in N$ and $rx \in N$, thus N is a submodule of M. It follows that N is finitely generated. In other words, there exist elements $a_1, a_2, \ldots, a_k \in N$ that generates N, that is, $N = \langle a_1, a_2, \ldots, a_k \rangle$. There exists a submodule N_k containing every a_i, and it follows that $N_k = N$. Hence

$$N_k = N_{k+1} = N_{k+2} = \cdots ,$$

which contradicts the infinite chain we obtained above. Thus S must have a maximal element.

$c) \Rightarrow a)$: Suppose we have an ascending sequence of submodules of M,

$$N_1 \subseteq N_2 \subseteq N_3 \subseteq \cdots .$$

As it is a nonempty set of submodules we have that this sequence contains a maximal element, say N_k. Thus $N_k = N_{k+1} = \cdots$, hence M is Noetherian. □

As our main focus is rings, rather than modules, we now rewrite Theorem 3.1 for rings.

Theorem 3.2. *If R is a ring, then the following are equivalent:*

a) R is Noetherian.

b) Each ideal in R is finitely generated.

c) Each nonempty set of ideals in R contains a maximal element.

DEFINITION. A **Noetherian domain** D is an integral domain which is Noetherian.

EXAMPLE. The ring $\mathbb{Z}$ is a Noetherian domain. We have earlier shown that $\mathbb{Z}$ is an integral domain where every ideal is of the form $n\mathbb{Z}$ for some positive integer n. Assume there exists an ascending chain of ideals

$$n_1\mathbb{Z} \subsetneq n_2\mathbb{Z} \subsetneq n_3\mathbb{Z} \subsetneq \cdots .$$

We have that $n_2 \mid n_1,\ n_3 \mid n_2,\ \ldots$, hence every $n_i \mid n_1$ for $i \in \{1, 2, 3, \ldots\}$. Since n_1 is a finite number the chain eventually stabilises, hence there exists a $k \in \mathbb{Z}$ such that $n_k\mathbb{Z} = n_{k+1}\mathbb{Z} = n_{k+2}\mathbb{Z} = \cdots$. Thus $\mathbb{Z}$ is Noetherian.

EXAMPLE. The ring $\mathbb{Z}[\sqrt{n}]$, where n is a squarefree integer, is a Noetherian domain. In Section 2.2 we showed that $\mathbb{Z}[\sqrt{n}]$ is an integral domain. We define a function

$$\phi :\ \mathbb{Z}[\sqrt{n}] \longrightarrow \mathbb{Z}[x]/\langle x^2 - n\rangle$$

with the map $(a + b\sqrt{n}) \longmapsto (a + bx)$. We check that ϕ is a homomorphism:

$$\begin{aligned}
\phi\big((a + b\sqrt{n}) + (c + d\sqrt{n})\big) &= \phi\big((a + c) + (b + d)\sqrt{n})\big) \\
&= (a + c) + (b + d)x \\
&= (a + bx) + (c + dx) \\
&= \phi(a + b\sqrt{n}) + \phi(c + d\sqrt{n}),
\end{aligned}$$

$$\begin{aligned}\phi\big((a+b\sqrt{n})\cdot(c+d\sqrt{n})\big) &= \phi\big((ac+nbd)+(ad+bc)\sqrt{n}\big)\\ &= (ac+nbd)+(ad+bc)x\\ &= (ac+nbd)+(ad+bc)x+bd(x^2-n)\\ &= ac+(ad+bc)x+bdx^2-nbd+nbd\\ &= (a+bx)\cdot(c+dx)\\ &= \phi(a+b\sqrt{n})\cdot\phi(c+d\sqrt{n}),\end{aligned}$$

$$\begin{aligned}\phi(1) &= \phi(1+0\cdot\sqrt{n})\\ &= 1+0\cdot x\\ &= 1.\end{aligned}$$

We see that ϕ is an homomorphism, and ϕ is clearly a surjective map. The only element that maps to 0 is $(0+0\sqrt{n})=0$, hence the kernel of ϕ is 0. Thus ϕ is an isomorphism:

$$\mathbb{Z}[\sqrt{n}] \simeq \mathbb{Z}[x]/\langle x^2-n\rangle.$$

In the previous example we saw that $\mathbb{Z}$ is a Noetherian ring, and by Hilbert's Basis Theorem, which for instance is proven in [3, Theorem 2.14], we have that $\mathbb{Z}[x]$ is also Noetherian. In any ring R with an ideal I the ideals in the factor ring R/I correspond precisely to the ideals in R containing I. As $\mathbb{Z}[x]$ is Noetherian every ideal is finitely generated by Theorem 3.2, and every ideal in $\mathbb{Z}[x]/\langle x^2-n\rangle$ is finitely generated as well. Hence $\mathbb{Z}[x]/\langle x^2-n\rangle$ is Noetherian. Thus $\mathbb{Z}[\sqrt{n}]$ is a Noetherian domain.

We have earlier stated that $\mathbb{Z}$ is a PID; in fact, we can show that every PID is Noetherian.

Theorem 3.3. *Every PID is a Noetherian domain.*

Proof: Let D be a PID. Every ideal in D is principal, hence finitely generated. Thus D is Noetherian by Theorem 3.2. □

Remark. As a Noetherian domain may contain ideals generated by more than one element the converse is not true. Thus we have shown the inclusion

$$\left\{\begin{matrix}\text{Principal ideal}\\ \text{domains}\end{matrix}\right\} \subsetneq \left\{\begin{matrix}\text{Noetherian}\\ \text{domains}\end{matrix}\right\},$$

which is part of our motivation in proving the chain of class inclusions, as presented in the introduction. We will inspect the chain closer and extend it further in the upcoming chapter.

4

Euclidean Domains and UFDs

4.1 Norms

Factorization of elements is the central part of this chapter. We are going to define both a *unique factorization domain*, abbreviated "UFD", and a *Euclidean domain*. We will start looking at *norms* of elements in $\mathbb{Z}[\sqrt{n}]$. Norms will become helpful when we later in the chapter discuss irreducibility of elements in $\mathbb{Z}[\sqrt{n}]$. We first present the definition and follow up with two important theorems.

DEFINITION. The **norm** of an element $x \in \mathbb{Z}[\sqrt{n}]$, where n is a squarefree integer and $x = (a + b\sqrt{n})$ for some $a, b \in \mathbb{Z}$, is the integer defined by

$$\mathcal{N}(x) = |x \cdot \overline{x}| = |(a + b\sqrt{n})(a - b\sqrt{n})| = |a^2 - nb^2|.$$

REMARK. We observe that $(a - b\sqrt{n})$ is equal to $\overline{x}$, called the **conjugate** of x; *not* the "complex conjugate" as x is not a complex number when n is positive. We define the norm to be a nonnegative integer, thus the absolute value signs. Also, notice that the norm of any integer $a \in \mathbb{Z} \subseteq \mathbb{Z}[\sqrt{n}]$, the case when $b = 0$, is always $\mathcal{N}(a) = a^2$.

As the norm is a function that maps elements to $\mathbb{Z}^+$ it can sometimes be used as a *Euclidean function* for integral domains of the form $\mathbb{Z}[\sqrt{n}]$, which we will see in the next section. In this Master's thesis we only intend to use norms as a tool. For further details about the subject we refer to [5, Section 2.5] and [4, Section 14.4], respectively.

Theorem 4.1. *If $x, y \in \mathbb{Z}[\sqrt{n}]$, where n is a squarefree integer, then*

$$\mathcal{N}(xy) = \mathcal{N}(x) \cdot \mathcal{N}(y).$$

Proof: Let $x = (a + b\sqrt{n})$ and $y = (c + d\sqrt{n})$ where $a, b, c, d \in \mathbb{Z}$. We get that

$$\mathcal{N}(x) \cdot N(y) = |a^2 - nb^2| \cdot |c^2 - nd^2|,$$

and since both $(a^2 - nb^2)$ and $(c^2 - nd^2)$ are integers we have that

$$|a^2 - nb^2| \cdot |c^2 - nd^2| = |(a^2 - nb^2)(c^2 - nd^2)|.$$

Hence

$$\mathcal{N}(x) \cdot N(y) = |(ac)^2 - n(ad)^2 - n(bc)^2 + (nbd)^2|.$$

We need to show that $\mathcal{N}(xy)$ is the same. We calculate

$$xy = (a + b\sqrt{n})(c + d\sqrt{n}) = (ac + nbd) + (ad + bc)\sqrt{n},$$

and get that

$$\overline{xy} = (ac + nbd) - (ad + bc)\sqrt{n}.$$

We finally see that

$$\begin{aligned}\mathcal{N}(xy) &= |xy \cdot \overline{xy}| = |(ac + nbd)^2 - n(ad + bc)^2| \\ &= |(ac)^2 + n \cdot 2abcd + (nbd)^2 - n(ad)^2 - n \cdot 2abcd - n(bc)^2| \\ &= |(ac)^2 - n(ad)^2 - n(bc)^2 + (nbd)^2| = \mathcal{N}(x) \cdot \mathcal{N}(y).\end{aligned}$$

This finishes the proof. □

The property we just proved is essential for the definition of $\mathcal{N}(x)$ being a norm, as is the property of the next theorem.

Theorem 4.2. *If $u \in \mathbb{Z}[\sqrt{n}]$, where n is a squarefree integer, then*

$$u \text{ is a unit } \Leftrightarrow \mathcal{N}(u) = 1.$$

Proof: Suppose $u = (a + b\sqrt{n}) \in \mathbb{Z}[\sqrt{n}]$ is a unit. There must exist some inverse $u^{-1} \in \mathbb{Z}[\sqrt{n}]$ such that $u^{-1}u = 1$. By Theorem 4.1 we have that

$$\mathcal{N}(1) = \mathcal{N}(u^{-1}u) = \mathcal{N}(u^{-1}) \cdot \mathcal{N}(u),$$

but since $\mathcal{N}(1) = 1^2 = 1$ we get that $\mathcal{N}(u^{-1}) \cdot \mathcal{N}(u) = 1$. We have that $\mathcal{N}(u^{-1})$ and $\mathcal{N}(u)$ both are nonnegative integers; the only option is $\mathcal{N}(u^{-1}) = \mathcal{N}(u) = 1$.

Conversely, we let $u = (a + b\sqrt{n})$ and suppose $\mathcal{N}(u) = 1$. We get

$$\mathcal{N}(u) = |(a + b\sqrt{n})(a - b\sqrt{n})| = 1.$$

It follows that $(a + b\sqrt{n})(a - b\sqrt{n}) = \pm 1$, hence $\pm(a - b\sqrt{n})$ is the inverse of $u = (a + b\sqrt{n})$, which clearly is an element in $\mathbb{Z}[\sqrt{n}]$. Hence u is a unit. □

REMARK. Whenever $x = (a + b\sqrt{n})$ is such that $x \cdot \overline{x} = (a + b\sqrt{n})(a - b\sqrt{n}) = 1$ then $\overline{x} = (a - b\sqrt{n})$ is the inverse. Likewise, whenever $x = (a + b\sqrt{n})$ is such that $x \cdot \overline{x} = (a + b\sqrt{n})(a - b\sqrt{n}) = -1$, it is equivalent to say $(a + b\sqrt{n})(-a + b\sqrt{n}) = 1$, and the inverse is then $-\overline{x} = (-a + b\sqrt{n})$.

EXAMPLE. The element $x = (5 + 2\sqrt{6})$ is a unit in $\mathbb{Z}[\sqrt{6}]$ as we calculate the norm to be $\mathcal{N}(x) = |5^2 - 6 \cdot 2^2| = |25 - 24| = 1$. We can find that the inverse of x is $(5 - 2\sqrt{6})$, and we see that $(5 + 2\sqrt{6})(5 - 2\sqrt{6}) = 1$.

4.2 Euclidean Domains

In this section we let S^* denote every nonzero element in a set S, and $\mathbb{Z}^+$ is the set of every nonnegative integer.

DEFINITION. An integral domain D is a **Euclidean domain** if there exists a map $\phi : D \to \mathbb{Z}^+$ such that the following hold for all $a, b \in D^*$:

i) $\phi(a) \leq \phi(ab)$.

ii) There exist some $q, r \in D$ such that $a = qb + r$ and $\phi(r) < \phi(b)$.

REMARK. Note that the function ϕ, the **Euclidean function**, is not itself a part of the Euclidean domain. A single Euclidean domain may possess several Euclidean functions, although we only require the existence of one map. The two points does also hold for any function $\phi(a)$ if $a = 0$. This is why we have excluded $a = 0$ from the definition. In fact, by letting $a = 0$ we can show that the Euclidean function is bounded below. In the second point of the definition it follows that $0 = qb + r$. Suppose $r \neq 0$, then we have $r = b \cdot (-q) \neq 0$. We get $\phi(b \cdot (-q)) < \phi(b)$, but from the first point we have $\phi(b) \leq \phi(b \cdot (-q))$, which is a contradiction. It follows that $r = 0$, and we get $\phi(0) < \phi(b)$ for all nonzero $b \in D$.

EXAMPLE. The ring $\mathbb{Z}$ is a Euclidean domain with the function $\phi(n) = |n|$, where $n \in \mathbb{Z}^*$.

EXAMPLE. Any field F is a Euclidean domain. We first define the function $\phi(a) = a^{-1}a = 1$ for all $a \in F^*$. For every $b \in F^*$ we have $ab \in F^*$, and the first part of the definition is satisfied as

$$\phi(a) = 1 = \phi(ab).$$

We need to show that any element $a \in F^*$ can be expressed as $a = qb + r$, where $\phi(r) < \phi(b)$, for some $q, r \in F$ and $b \in F^*$. We choose $r = 0$ and get

that $a = qb$, hence $q = b^{-1}a$, which clearly is an element in F. We also have $\phi(r) = \phi(0) < \phi(b)$ for all $b \in F^*$. Thus the second part of the definition is satisfied.

As $\mathbb{Z}$ is not a field the previous two examples are enough to show that the inclusion

$$\left\{\text{Fields}\right\} \subsetneq \left\{\begin{matrix}\text{Euclidean}\\ \text{domains}\end{matrix}\right\},$$

holds.

EXAMPLE. The ring $\mathbb{Z}[\sqrt{2}]$ is a Euclidean domain. Let $x = (a + b\sqrt{2})$ and $y = (c + d\sqrt{2})$, where $y \neq 0$, be two elements in $\mathbb{Z}[\sqrt{2}]$, where $a, b, c, d \in \mathbb{Z}$. We then write

$$\frac{x}{y} = \frac{a + b\sqrt{2}}{c + d\sqrt{2}} = \alpha + \beta\sqrt{2}$$

such that $\alpha, \beta \in \mathbb{Q}$. We choose $\alpha_0, \beta_0 \in \mathbb{Z}$ such that

$$|\alpha - \alpha_0| \leq \frac{1}{2} \quad \text{and} \quad |\beta - \beta_0| \leq \frac{1}{2}.$$

We now have

$$\begin{aligned} x &= (\alpha + \beta\sqrt{2}) \cdot y \\ &= (\alpha + \beta\sqrt{2}) \cdot y + \underbrace{(\alpha_0 - \alpha_0 + \beta_0\sqrt{2} - \beta_0\sqrt{2})}_{=0} \cdot y \\ &= (\alpha_0 + \beta_0\sqrt{2}) \cdot y + \Big((\alpha - \alpha_0) + (\beta - \beta_0)\sqrt{2}\Big) \cdot y. \end{aligned}$$

We let $r = \Big((\alpha - \alpha_0) + (\beta - \beta_0)\sqrt{2}\Big) \cdot y$, hence

$$x = (\alpha_0 + \beta_0\sqrt{2}) \cdot y + r,$$

where x, y, and $(\alpha_0 + \beta_0\sqrt{2})$ all are elements in $\mathbb{Z}[\sqrt{2}]$. Now, as r is a sum of elements in $\mathbb{Z}[\sqrt{2}]$, and $\mathbb{Z}[\sqrt{2}]$ is closed under addition, we have $r \in \mathbb{Z}[\sqrt{2}]$. We let $q = (\alpha_0 + \beta_0\sqrt{2})$, hence we have written x of the form

$$x = qy + r.$$

It remains to find a Euclidean function ϕ such that

i) $\phi(x) \leq \phi(x \cdot y)$, and

ii) $\phi(r) < \phi(y)$.

We can use the norm as a function from $\mathbb{Z}[\sqrt{2}]$ to $\mathbb{Z}^+$, hence the first point is satisfied as

$$\begin{aligned} 1 &\leq \mathcal{N}(y) \\ \mathcal{N}(x) &\leq \mathcal{N}(x) \cdot \mathcal{N}(y) \\ \mathcal{N}(x) &\leq \mathcal{N}(x \cdot y), \end{aligned}$$

when $y \neq 0$. We recall that we chose α_0 and β_0 such that $|\alpha - \alpha_0| \leq \frac{1}{2}$ and $|\beta - \beta_0| \leq \frac{1}{2}$. Thus

$$|\alpha - \alpha_0|^2 \leq (\frac{1}{2})^2 = \frac{1}{4},$$

and

$$2 \cdot |\beta - \beta_0|^2 \leq 2 \cdot (\frac{1}{2})^2 = \frac{1}{2}.$$

We may remove the absolute value signs as they now are squared; we get that

$$(\alpha - \alpha_0)^2 \leq \frac{1}{4},$$

and

$$2(\beta - \beta_0)^2 \leq \frac{1}{2}.$$

We use the triangular inequality to obtain

$$\begin{aligned} |(\alpha - \alpha_0)^2 + (-2(\beta - \beta_0)^2)| &\leq |(\alpha - \alpha_0)^2| + |-2(\beta - \beta_0)^2| \\ |(\alpha - \alpha_0)^2 - 2(\beta - \beta_0)^2| &\leq |(\alpha - \alpha_0)^2| + |2(\beta - \beta_0)^2| \leq \frac{1}{4} + \frac{1}{2} \\ \mathcal{N}(\Big((\alpha - \alpha_0) + (\beta - \beta_0)\sqrt{2})\Big)) &\leq \frac{3}{4} < 1 \\ \mathcal{N}(\Big((\alpha - \alpha_0) + (\beta - \beta_0)\sqrt{2})\Big)) \cdot \mathcal{N}(y) &< 1 \cdot \mathcal{N}(y) \\ \mathcal{N}(\Big((\alpha - \alpha_0) + (\beta - \beta_0)\sqrt{2}\Big) \cdot y) &< \mathcal{N}(y) \\ \mathcal{N}(r) &< \mathcal{N}(y). \end{aligned}$$

Thus the second point is also satisfied.

Theorem 4.3. *Every Euclidean domain is a PID.*

Proof: Let D be a Euclidean domain. Thus there exists a Euclidean function, say ϕ. Let I be an ideal in D. If $I = (0)$, then it is a principal ideal. We suppose $I \neq (0)$. Consider the set of integers $\Omega \subseteq \mathbb{Z}^+$ defined by

$$\Omega = \{\phi(x) \mid x \in I,\ x \neq 0\}.$$

The set Ω is nonempty as $I \neq (0)$. From the remark following the definition of a Euclidean domain we have that $\phi(0) < \phi(b)$ for all $b \in D$, where $b \neq 0$, thus also when $b \in I$. Hence there is a "least element" in Ω. Choose $b \in I$ such that $\phi(b)$ is the least element in Ω. Now, let $a \in I$, thus there exist some $q, r \in D$ such that

$$a = qb + r \quad \text{and} \quad \phi(r) < \phi(b).$$

Since I is an ideal we have $qb \in I$, hence $r = (a - qb) \in I$. As $\phi(r) < \phi(b)$, and $\phi(b)$ is the least element in Ω, we get $r = 0$. It follows that $a = qb$, thus $I = \langle b \rangle$. Hence every ideal in D is principal. □

Remark. The converse is not true as there exist PIDs which are not Euclidean domains. For instance, Jack C. Wilson showed, in 1973, that $\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$ is a PID, but that it is not a Euclidean domain [6]. Hence we have the following inclusion satisfied:

$$\left\{ \begin{matrix} \text{Euclidean} \\ \text{domains} \end{matrix} \right\} \subsetneq \left\{ \begin{matrix} \text{Principal ideal} \\ \text{domains} \end{matrix} \right\}$$

4.3 Unique Factorization Domains

A UFD is, as its name suggests, an integral domain where elements factorize uniquely. Before we state the definition of a UFD we first need to define *irreducible elements*, which is what all elements in a ring eventually factorize into.

Definition. Let R be a ring with a nonzero element $r \in R$. If r is not a unit and $r = ab$, for some $a, b \in R$, implies that either a or b is a unit, then r is an **irreducible element**.

Remark. A **reducible element** is an element that is not irreducible.

Example. In $\mathbb{Z}$ all prime numbers p are irreducible elements. The only units are ± 1 as no other elements have inverses, and as $p \neq 0, \pm 1$ it is a nonzero and nonunit element. If $p = ab$ for some $a, b \in \mathbb{Z}$, then either a or b is equal to ± 1, hence a or b is a unit. Thus p is irreducible. Every element in $\mathbb{Z}$ that is not a prime or not a unit is a reducible element.

We will now present two examples of irreducible elements in $\mathbb{Z}[\sqrt{-5}]$ where the results are used in the example following our main theorem in Section 6.3.

Example. The element $2 \in \mathbb{Z}[\sqrt{-5}]$ is irreducible. If we assume that 2 is reducible, then

$$2 = (a + b\sqrt{-5})(c + d\sqrt{-5})$$

for some $a, b, c, d \in \mathbb{Z}$. We use the norm function on each side of the equation,

$$\begin{aligned}\mathcal{N}(2) &= \mathcal{N}(a + b\sqrt{-5}) \cdot \mathcal{N}(c + d\sqrt{-5}) \\ 2^2 &= (a^2 + 5b^2)(c^2 + 5d^2).\end{aligned}$$

We get that $(a^2 + 5b^2)$ must divide $2^2 = 4$, hence

$$(a^2 + 5b^2) = 1, 2, \text{ or } 4.$$

We rule out the option of $(a^2 + 5b^2) = 1$ as $(a + b\sqrt{-5})$ then must be a unit by Theorem 4.2. In either case we need $b = 0$, and we rule out the option of 2 as it is not a square. This leaves us with $a = \pm 2$ such that $(a^2 + 5b^2) = 4$, but then $(c^2 + 5d^2) = 1$, and $(c + d\sqrt{-5})$ is a unit. Hence 2 is irreducible.

Example. The element $(1 + \sqrt{-5}) \in \mathbb{Z}[\sqrt{-5}]$ is irreducible. If $(1 + \sqrt{-5})$ is reducible, then

$$(1 + \sqrt{-5}) = (a + b\sqrt{-5})(c + d\sqrt{-5})$$

for some $a, b, c, d \in \mathbb{Z}$. We take the norm of each side

$$\begin{aligned}\mathcal{N}(1 + \sqrt{-5}) &= \mathcal{N}(a + b\sqrt{-5}) \cdot \mathcal{N}(c + d\sqrt{-5}) \\ 6 &= (a^2 + 5b^2)(c^2 + 5d^2).\end{aligned}$$

We get that $(a^2 + 5b^2)$ must divide 6, hence

$$(a^2 + 5b^2) = 1, 2, 3, \text{ or } 6.$$

Again we rule out the option of 1, otherwise $(a + b\sqrt{-5})$ is a unit. We cannot have $b = 0$ since none of 2, 3, or 6 are squares. It follows that $b = \pm 1$ which leaves us with the only option that $a = \pm 1$. We get $(a^2 + 5b^2) = 6$, but then $(c^2 + 5d^2) = 1$, and $(c + d\sqrt{-5})$ is a unit. Hence $(1 + \sqrt{-5})$ is irreducible.

Remark. Since $\mathcal{N}(1 + \sqrt{-5}) = (1 + \sqrt{-5})(1 - \sqrt{-5}) = \mathcal{N}(1 - \sqrt{-5})$ it follows that $(1 - \sqrt{-5})$ is also irreducible in $\mathbb{Z}[\sqrt{-5}]$.

Definition. An integral domain D is a **UFD** (unique factorization domain) if every nonzero element $r \in D$, that is not a unit, factorizes into a finite product of irreducible elements in D, where the product is unique up to units.

Example. The ring $\mathbb{Z}$ is a UFD. Every integer, other than 0 and ± 1, factorizes into a finite product of prime numbers, which are the irreducible elements of $\mathbb{Z}$. The product is unique up to units.

REMARK. When we say "unique up to units" we mean that the order of the elements is insignificant and that if an element $r \in D$ is multiplied with a unit $u \in D$, then ur is considered the same element as r. For instance,

$$2 \cdot 3 = 3 \cdot 2 = (-3) \cdot (-2) = (-2) \cdot (-3)$$

are all the same factorization of the element $6 \in \mathbb{Z}$. Elements that differ by being multiplied by a unit we refer to as *associates*.

DEFINITION. Let R be a ring with two nonzero elements $a, b \in R$. If $a \mid b$ and $b \mid a$, that is, both elements divide the other, then a and b are called **associates**, denoted $a \sim b$.

REMARK. Equivalently, if $a = bu$ for some $a, b, u \in R$, then

$$a \sim b \;\Leftrightarrow\; u \text{ is a unit.}$$

EXAMPLE. In $\mathbb{Z}$, $a \sim b$ if and only if $a = \pm b$.

EXAMPLE. In $\mathbb{Z}(\sqrt{-1})$ we have $(1 + i) = (1 - i) \cdot i$, and furthermore, we also have $(1 - i) = (1 + i) \cdot (-i)$. Hence $(1 + i) \mid (1 - i)$ and $(1 - i) \mid (1 + i)$, thus $(1 + i) \sim (1 - i)$.

In both examples we see that $a = b \cdot (\pm 1)$ and $(1 + i) = (1 - i) \cdot i$, where (± 1) and i are units in their respective rings. We see even clearer why associated elements are important in the next example.

EXAMPLE. In Section 4.2 we showed that $\mathbb{Z}[\sqrt{2}]$ is a Euclidean domain. We will later see, by Corollary 4.7, it implies that $\mathbb{Z}[\sqrt{2}]$ is also a UFD. We have that the element $(8 - 3\sqrt{2}) \in \mathbb{Z}[\sqrt{2}]$ factorizes into the two following products:

$$(5 + \sqrt{2})(2 - \sqrt{2}) = (11 - 7\sqrt{2})(2 + \sqrt{2}).$$

Following the procedure using norms we can show that each of these four factors are irreducible elements in $\mathbb{Z}[\sqrt{2}]$, where neither is a unit. Therefore, the only explanation is that the factors are associates. We observe that $(3+2\sqrt{2})$ is a unit in $\mathbb{Z}[\sqrt{2}]$ since $\mathcal{N}(3 + 2\sqrt{2}) = 3^2 - 2 \cdot 2^2 = 1$. We calculate $(2 - \sqrt{2})(3 + 2\sqrt{2}) = (2 + \sqrt{2})$, and since $(3 + 2\sqrt{2})$ is a unit,

$$(2 - \sqrt{2}) \sim (2 + \sqrt{2}).$$

Similarly, $(11 - 7\sqrt{2})(3 + 2\sqrt{2}) = (5 + \sqrt{2})$, hence

$$(11 - 7\sqrt{2}) \sim (5 + \sqrt{2}).$$

We present one final example of associates, where we need the result for later in the example following the main theorem in Section 6.3.

EXAMPLE. In $\mathbb{Z}[\sqrt{-5}]$ neither of the elements $2, 3, (1+\sqrt{-5}), (1-\sqrt{-5})$ are associates. We will make use of the norm of each element,

$$\begin{aligned}
&\mathcal{N}(2) = 2^2 = 4,\\
&\mathcal{N}(3) = 3^2 = 9,\\
&\mathcal{N}(1+\sqrt{-5}) = 1^2 + 5\cdot 1^2 = 6,\\
&\mathcal{N}(1-\sqrt{-5}) = 1^2 + 5\cdot (-1)^2 = 6.
\end{aligned}$$

In general, if a and b are associates, then $a \mid b$ implies $b = ac$ for some c, and we also have $\mathcal{N}(b) = \mathcal{N}(a)\cdot\mathcal{N}(c)$. As norms are positive integers then none of the elements above are associated with 2 or 3. Hence $4 = \mathcal{N}(a)\cdot\mathcal{N}(c)$ and $9 = \mathcal{N}(a)\cdot\mathcal{N}(c)$ are impossible when using one of the other norms above. It remains to check if $(1+\sqrt{-5})$ and $(1-\sqrt{-5})$ are associates. Suppose they are associates, then $(1+\sqrt{-5}) \mid (1-\sqrt{-5})$, and for some $(c+d\sqrt{-5}) \in \mathbb{Z}[\sqrt{-5}]$, where $c, d \in \mathbb{Z}$, we have that

$$\begin{aligned}
(1+\sqrt{-5}) &= (1-\sqrt{-5})(c+d\sqrt{-5})\\
&= (c+5d) + (d-c)\sqrt{-5}.
\end{aligned}$$

We get that $(d-c) = 1$ and $(c+5d) = 1$, which implies $\big(c+5(c+1)\big) = 1$. Hence $c = -\frac{2}{3}$, which contradicts the fact that $c \in \mathbb{Z}$. Thus $(1+\sqrt{-5})$ and $(1-\sqrt{-5})$ are not associates.

Theorem 4.4. *If D is a UFD with an element $p \in D$, then*

$$p \text{ is irreducible } \Leftrightarrow \text{ } p \text{ is a prime.}$$

Proof: Suppose $p \in D$ is an irreducible element. Assume that $p \mid ab$, for some $a, b \in D$. There exists an element $c \in D$ such that $ab = pc$. Since D is a UFD we have

$$a = p_1 \cdots p_k,\ b = q_1 \cdots q_m,\ c = r_1 \cdots r_n,$$

where $p_1, \ldots, p_k, q_1, \ldots, q_m, r_1, \ldots, r_n$ all are irreducible elements in D, not necessarily distinct. We get

$$(p_1 \cdots p_k)(q_1 \cdots q_m) = p(r_1 \cdots r_n).$$

Since D is an UFD, and we only have irreducible elements, every element on the left is an associate to an element on the right, including p. Hence

$$p = p_i \text{ or } p = q_j$$

for $i \in \{1, 2, \ldots, k\}$ and $j \in \{1, 2, \ldots, m\}$. Hence

$$p \mid a \quad \text{or} \quad p \mid b,$$

and p is by definition a prime.

For the converse, let $p \in D$ be a prime. Assume that $p = ab$ for some nonzero $a, b \in D$. As $p = ab$ implies $p \mid ab$, and since p is a prime we have that

$$p \mid a \quad \text{or} \quad p \mid b.$$

It follows that

$$px = a \quad \text{or} \quad py = b,$$

for some $x, y \in D$. We can rewrite $p = ab$ as both $a = b^{-1}p$ and $b = a^{-1}p$, where $a^{-1}, b^{-1} \in \text{Quot}(D)$ are the inverses of the nonzero elements $a, b \in D$. To complete the proof we need to show that one of the inverses is an element in D. We have

$$px = b^{-1}p \quad \text{or} \quad py = a^{-1}p,$$

thus

$$x = b^{-1} \quad \text{or} \quad y = a^{-1}.$$

We get that either a^{-1} or b^{-1} is an element in D. Hence either a or b is a unit, thus p is an irreducible element. □

Lemma 4.5. *Every irreducible element in a PID is a prime.*

Proof: Let D be a PID with an irreducible element $p \in D$. Suppose $p \mid ab$ for some $a, b \in D$. We assume that $p \nmid a$, otherwise p is a prime. Hence we need to show that $p \mid b$. We let $I = \langle p, a \rangle$. As I is an ideal in D there exists an element $r \in D$ such that $I = \langle r \rangle$. Since we have $p, a \in I$ both $r \mid p$ and $r \mid a$. We have that r and p are not associates, denoted $r \not\sim p$, otherwise it contradicts $p \nmid a$. As p is irreducible we must have that r is a unit. Thus there exists an element $c \in D$ such that $rc = 1$. We have $r \in I = \langle p, a \rangle$, hence there exists some $x, y \in D$ such that $r = px + ay$. Thus we also have

$$rc = (px + ay)c = pxc + ayc = 1.$$

Hence

$$b = b \cdot 1 = b \cdot (pxc + ayc) = p(bcx) + ab(cy).$$

As $p \mid ab$ we get $p \mid ab(cy)$. It follows that p is a divisor in both terms, thus $p \mid b$. Hence p is a prime. □

Theorem 4.6. *Every PID is a UFD.*

Proof: Let D be a PID. From Theorem 3.3 we have that D is Noetherian. We let $a_0 \in D$ be a nonzero and nonunit element. Assume that a_0 is *not* a finite product of irreducible elements in D. It follows that $a_0 = a_1 b_1$ for some $a_1, b_1 \in D$, where a_1 is not a finite product of irreducible elements and b_1 is not a unit. If $a_1 \in \langle a_0 \rangle$, then $a_1 = r a_0$ for some $r \in R$, but then $a_1 = r(a_1 b_1)$ which implies $1 = r b_1$. It contradicts the fact that b_1 is not a unit, and so $a_1 \notin \langle a_0 \rangle$. Next, we let $a_1 = a_2 b_2$, where a_2 is not a finite product of irreducible elements, and b_2 is not a unit. We follow the same procedure and obtain an infinite chain of ideals

$$\langle a_0 \rangle \subsetneq \langle a_1 \rangle \subsetneq \langle a_2 \rangle \subsetneq \langle a_3 \rangle \subsetneq \cdots,$$

which contradicts D being Noetherian. Hence a_0 is a finite product of irreducible elements in D.

We need to show that the factorization is unique up to units. We assume that there exists at least one nonzero element $r \in D$ that is not a unit, which factorizes into at least two different products of irreducible elements. We let Ω denote the set containing all such elements, and furthermore, let

$$S = \{\langle r \rangle \mid r \in \Omega\}.$$

It follows that S is a nonempty set of ideals in D, which is Noetherian, and must contain a maximal element, say $\langle m \rangle$, by Theorem 3.2. Therefore, $m \in S$ factorizes into at least two different products of irreducible elements, say

$$m = u_a \cdot a_1^{c_1} \cdots a_k^{c_k} = u_b \cdot b_1^{d_1} \cdots b_n^{d_n},$$

where $u_a, u_b \in D$ are units, $a_1, \ldots, a_k, b_1, \ldots, b_n \in D$ are irreducible elements, and the exponents $c_1, \ldots, c_k, d_1, \ldots, d_n$ are positive integers. We also assume that $a_i \not\sim a_j$ and $b_i \not\sim b_j$ for all $i \neq j$, with $i \in \{1, 2, \ldots, k\}$ and $j \in \{1, 2, \ldots, n\}$. By Lemma 4.5 every a_i is a prime since they all are irreducible. Thus $a_1 \mid b_j$ for some j. We may, without loss of generality, choose $j = 1$, hence $a_1 \mid b_1$, but since b_1 also is irreducible we have that $a_1 \sim b_1$. Hence $a_1 = b_1 u_1$ for some unit $u_1 \in D$. Thus

$$m = u_a \cdot (b_1 u_1)^{c_1} \cdots a_k^{c_k} = u_b \cdot b_1^{d_1} \cdots b_n^{d_n}.$$

If we multiply with ${b_1}^{-1} \in \text{Quot}(D)$ we obtain the equality

$$m {b_1}^{-1} = u_a {u_1}^{c_1} \cdot b_1^{c_1 - 1} a_2^{c_2} \cdots a_k^{c_k} = u_b \cdot b_1^{d_1 - 1} b_2^{d_2} \cdots b_n^{d_n}$$

in Quot(D). As b_1 is not a unit in D we have $\langle m \rangle \subsetneq \langle m {b_1}^{-1} \rangle$. It follows that $\langle m {b_1}^{-1} \rangle \notin S$ since $\langle m \rangle$ is maximal, and then after some suitable rearrangement we have that

$$c_1 - 1 = d_1 - 1,\ c_2 = d_2,\ \ldots,\ c_k = d_k,$$

where $k = n$, and

$$a_2 \sim b_2, \ \ldots, \ a_k \sim b_k.$$

From this we deduce that $c_1 = d_1$, and we already have that $a_1 \sim b_1$, which all together contradicts the fact that m factorizes into at least two different products of irreducible elements. This finishes the proof. □

Corollary 4.7. *Every Euclidean domain is a UFD.*

In the example to follow we will present a UFD that is not a PID. Therefore, we have that

$$\left\{ \begin{matrix} \text{Euclidean} \\ \text{domains} \end{matrix} \right\} \subsetneq \Big\{ \text{PIDs} \Big\} \subsetneq \Big\{ \text{UFDs} \Big\},$$

but in light of the same example, we will not include UFDs in our chain of class inclusions as a UFD is not necessarily a Noetherian domain.

Example. A UFD is not necessarily a Noetherian domain. We let $F[[x]]$ denote the ring of power series over a field F with indeterminate x. We have that

$$a_0 + a_1 x + a_2 x^2 + \ldots,$$

where $a_i \in F$, is a general element in $F[[x]]$. A power series ring of two indeterminates, say $F[[x_1, x_2]]$, consists of elements such as

$$a_{00} + a_{10}x_1 + a_{01}x_2 + a_{11}x_1x_2 + a_{20}{x_1}^2 + a_{02}{x_2}^2 + a_{21}{x_1}^2x_2 + \cdots,$$

where $a_{ij} \in F$. We let $D = F[[x_1, x_2, x_3, \ldots]]$ denote the power series ring of infinitely many indeterminates. This is a known *regular local ring*, and by the Auslander-Buchsbaum Theorem every regular local ring is a UFD [2]. Hence D is a UFD where

$$\langle x_1 \rangle \subsetneq \langle x_1, x_2 \rangle \subsetneq \langle x_1, x_2, x_3 \rangle \subsetneq \cdots$$

is an infinite chain of ideals. Thus D is not Noetherian, and the inclusion

$$\Big\{ \text{UFDs} \Big\} \subsetneq \left\{ \begin{matrix} \text{Noetherian} \\ \text{domains} \end{matrix} \right\}$$

does *not* hold. As D is not a Noetherian domain it is neither a PID by Theorem 3.3.

5

Algebraic Number Fields

5.1 Integral Over a Domain

Our motivation for the following chapter is to study algebraic number fields and what properties the subset of algebraic integers contained in those fields possesses. First we need an understanding of what it means for an element or a domain to be *integral over a domain.*

DEFINITION. Let A and D be integral domains such that $A \subseteq D$. If $r \in D$ is such that $r^n + a_{n-1}r^{n-1} + \cdots + a_1 r + a_0 = 0$ for some $a_0, a_1, \ldots, a_{n-1} \in A$, then **the element r is integral over A.**

REMARK. This means that if r is integral over A, then there exists some polynomial $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ in $A[x]$, where $r \in D$ is a root and $A[x]$ is the polynomial ring over A with indeterminate x; a ring containing all polynomials with elements in A as coefficients. We have that $f(x)$ is a **monic polynomial**, that is, the leading coefficient, which is the one in front of x^n, is equal to 1. If r is a complex number, which is integral over $\mathbb{Z}$, then r is an **algebraic integer**.

Proposition 5.1. *Let $A \subseteq B \subseteq D$ be a tower of integral domains. If an element $r \in D$ is integral over A, then r is integral over B.*

Proof: Let $r \in D$ be integral over A. There exist $a_0, a_1, \ldots, a_{n-1} \in A$ such that

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

As $A \subseteq B$ we have $a_0, a_1, \ldots, a_{n-1} \in B$, thus r is integral over B. □

Theorem 5.2. *Let A and D be integral domains such that $A \subseteq D$. If $r \in D$, then*

$$r \text{ is integral over } A \;\Leftrightarrow\; A[r] \text{ is a finitely generated } A\text{-module.}$$

Proof: Suppose r is integral over A. There exist $a_0, a_1, \ldots, a_{n-1} \in A$ such that

$$r^n - a_{n-1}r^{n-1} - a_{n-2}r^{n-2} - \cdots - a_1 r - a_0 = 0.$$

It follows that

$$r^n = a_{n-1}r^{n-1} + a_{n-2}r^{n-2} + \cdots + a_1 r + a_0,$$

and we multiply with r to obtain

$$r^{n+1} = a_{n-1}r^n + a_{n-2}r^{n-1} + \cdots + a_1 r^2 + a_0 r.$$

Now, let

$$\Omega = Ar^{n-1} + Ar^{n-2} + \cdots + Ar + A,$$

such that $r^n \in \Omega$. Since $A \subseteq \Omega$ we also have $Ar^n \subseteq \Omega$, hence

$$r^{n+1} \in \underbrace{Ar^n}_{\subseteq\Omega} + \underbrace{Ar^{n-1} + \cdots + Ar^2 + Ar}_{\subseteq\Omega} \subseteq \Omega.$$

By induction we see that

$$r^k \in \Omega$$

for all positive integers k. Thus $A[r]$ is an A-module generated by Ω, and since Ω is generated by a finite number of elements we have that $A[r]$ is a finitely generated A-module.

Conversely, suppose $A[r]$ is a finitely generated A-module. There exists a finite number of nonzero elements $m_1, m_2, \ldots, m_k \in A[r]$ such that

$$A[r] = Am_1 + Am_2 + \cdots + Am_k.$$

As each $m_i \in A[r]$, and $r \in A[r]$, we have that $rm_i \in A[r]$ for $i \in \{1, 2, \ldots, k\}$, thus rm_i can be expressed as

$$rm_i = a_{i1}m_1 + a_{i2}m_2 + \cdots + a_{ik}m_k,$$

for some $a_{i1}, a_{i2}, \ldots, a_{ik} \in A$. Hence we can derive the following linear system:

$$\begin{aligned}
rm_1 &= a_{11}m_1 + a_{12}m_2 + \cdots + a_{1k}m_k \\
rm_2 &= a_{21}m_1 + a_{22}m_2 + \cdots + a_{2k}m_k \\
&\vdots \\
rm_k &= a_{k1}m_1 + a_{k2}m_2 + \cdots + a_{kk}m_k.
\end{aligned}$$

We first rewrite it as

$$\begin{aligned}(a_{11}-r)m_1 + a_{12}m_2 + \cdots + a_{1k}m_k &= 0\\ a_{21}m_1 + (a_{22}-r)m_2 + \cdots + a_{2k}m_k &= 0\\ &\vdots\\ a_{k1}m_1 + a_{k2}m_2 + \cdots + (a_{kk}-r)m_k &= 0,\end{aligned}$$

and then represent it as a matrix system $M\mathbf{x} = 0$:

$$M\mathbf{x} = \begin{pmatrix}(a_{11}-r) & a_{12} & \dots & a_{1k}\\ a_{21} & (a_{22}-r) & \dots & a_{2k}\\ \vdots & \vdots & \ddots & \\ a_{k1} & a_{k2} & \dots & (a_{kk}-r)\end{pmatrix}\begin{pmatrix}m_1\\ m_2\\ \vdots\\ m_k\end{pmatrix} = 0.$$

From linear algebra we have that this homogeneous system has a nontrivial solution if and only if the matrix M is not invertible, that is, the determinant of M is equal to 0. When computing the determinant, $\det(M)$, we will get

$$\det(M) = r^k + a^*_{k-1}r^{k-1} + \cdots + a^*_2 r^2 + a^*_1 r + a^*_0 = 0,$$

where $a^*_0, a^*_1, \dots, a^*_{k-1}$ are sums and products of a_{ij} for $i, j \in \{1, 2, \dots, k\}$ in different constellations. As $a_{ij} \in A$ we have $a^*_0, a^*_1, \dots, a^*_{k-1} \in A$. Hence r is integral over A. □

Definition. Let A and D be integral domains such that $A \subseteq D$. If every $r \in D$ is integral over A, then **the domain D is integral over A.**

The proof following the next theorem is very similar to the proof of the previous theorem.

Theorem 5.3. *Let A and D be integral domains such that $A \subseteq D$, and let $r \in D$. If there exists an integral domain B such that*

$$A[r] \subseteq B \subseteq D,$$

and B is a finitely generated A-module, then r is integral over A, and $A[r]$ is a finitely generated A-module.

Proof: As B is a finitely generated A-module there exists a finite number of nonzero elements $b_1, b_2, \dots, b_k \in B$ such that

$$B = Ab_1 + Ab_2 + \cdots + Ab_k.$$

We have that $r \in A[r] \subseteq B$, hence $rb_i \in B$ for $i \in \{1, 2, \ldots, k\}$, which again can be expressed as

$$rb_i = a_{i1}b_1 + a_{i2}b_2 + \cdots + a_{ik}b_k,$$

for some $a_{i1}, a_{i2}, \ldots, a_{ik} \in A$. Hence we obtain a linear system like the one in the proof of Theorem 5.2:

$$\begin{aligned} rb_1 &= a_{11}b_1 + b_{12}m_2 + \cdots + b_{1k}m_k \\ rb_2 &= a_{21}b_1 + b_{22}m_2 + \cdots + b_{2k}m_k \\ &\vdots \\ rb_k &= a_{k1}b_1 + b_{k2}m_2 + \cdots + b_{kk}m_k. \end{aligned}$$

We represent it as a matrix system $M\mathbf{x} = 0$:

$$M\mathbf{x} = \begin{pmatrix} (a_{11} - r) & a_{12} & \ldots & a_{1k} \\ a_{21} & (a_{22} - r) & \ldots & a_{2k} \\ \vdots & \vdots & \ddots & \\ a_{k1} & a_{k2} & \ldots & (a_{kk} - r) \end{pmatrix} \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_k \end{pmatrix} = 0.$$

There is a nontrivial solution of $M\mathbf{x} = 0$ if and only if $\det(M) = 0$. We get

$$\det(M) = r^k + a^*_{k-1}r^{k-1} + \cdots + a^*_2 r^2 + a^*_1 r + a^*_0 = 0,$$

where $a^*_0, a^*_1, \ldots, a^*_{k-1} \in A$. Hence r is integral over A, and by Theorem 5.2 $A[r]$ is a finitely generated A-module. □

Corollary 5.4. *Let A and D be integral domains such that $A \subseteq D$. If D is a finitely generated A-module, then D is integral over A.*

Proof: This follows from the special case of Theorem 5.3 when have

$$A[r] \subseteq B = D,$$

thus any $r \in D$ is integral over A. □

The following theorem introduces polynomial rings with with more than one indeterminate. For instance, the polynomial ring $A[r_1, r_2]$ consists of sums and products of its two indeterminates r_1 and r_2 in all possible constellations, with elements in A as coefficients. Thus a general element in $A[r_1, r_2]$ is of the form

$$\begin{aligned} &a_{00} + a_{10}r_1 + a_{11}r_1r_2 + a_{12}r_1{r_2}^2 + \cdots + a_{1n}r_1{r_2}^n \\ &\quad + a_{20}{r_1}^2 + a_{21}{r_1}^2r_2 + a_{22}{r_1}^2{r_2}^2 + \cdots + a_{2n}{r_1}^2{r_2}^n \\ &\quad + \cdots \\ &\cdots + a_{n0}{r_1}^n + a_{n1}{r_1}^nr_2 + a_{n2}{r_1}^n{r_2}^2 + \cdots + a_{nn}{r_1}^n{r_2}^n, \end{aligned}$$

where $a_{00}, a_{10}, a_{11}, \ldots, a_{nn} \in A$.

Theorem 5.5. *Let A and D be integral domains such that $A \subseteq D$. If the elements $r_1, r_2, \ldots, r_n \in D$ are integral over A, then $A[r_1, r_2, \ldots, r_n]$ is a finitely generated A-module.*

Proof: We will deduce the proof by induction on n. First, if $n = 1$, then $r_1 \in D$ is integral over A. From Theorem 5.2 we get that $A[r_1]$ is a finitely generated A-module.

Next, we let $n \geq 2$ and assume that $A[r_1, r_2, \ldots, r_{n-1}]$ is is a finitely generated A-module, where $r_1, r_2, \ldots, r_{n-1} \in D$ are integral over A. Let r_n be integral over A. Since $A \subseteq A[r_1, r_2, \ldots, r_{n-1}] \subseteq D$ we have that r_n is integral over $A[r_1, r_2, \ldots, r_{n-1}]$ by Proposition 5.1. Hence

$$(A[r_1, r_2, \ldots, r_{n-1}])[r_n] = A[r_1, r_2, \ldots, r_n]$$

is a finitely generated A-module by Theorem 5.2. □

Theorem 5.6. *Let $A \subseteq B \subseteq D$ be a tower of integral domains. If an element $r \in D$ is integral over B, and B is integral over A, then r is integral over A.*

Proof: As $r \in D$ is integral over B there exist $b_0, b_1, \ldots, b_{n-1} \in B$ such that

$$r^n + b_{n-1}r^{n-1} + \cdots + b_1 r + b_0 = 0.$$

Hence r is also integral over $A[b_0, b_1, \ldots, b_{n-1}]$. As B is integral over A each element $b_i \in B$, where $i \in \{0, 1, \ldots, n-1\}$, is integral over A. We have that $A[b_0, b_1, \ldots, b_{n-1}]$ is a finitely generated A-module by Theorem 5.5. Next, we regard $A[b_0, b_1, \ldots, b_{n-1}]$ as an integral domain, where $A[b_0, b_1, \ldots, b_{n-1}] \subseteq D$. Since r is integral over $A[b_0, b_1, \ldots, b_{n-1}]$ we have that $(A[b_0, b_1, \ldots, b_{n-1}])[r]$ is a finitely generated A-module by Theorem 5.2. Thus the integral domain $(A[b_0, b_1, \ldots, b_{n-1}])[r] = A[b_0, b_1, \ldots, b_{n-1}, r]$ is a finitely generated A-module such that

$$A[r] \subseteq A[b_0, b_1, \ldots, b_{n-1}, r] \subseteq D.$$

Hence r is integral over A by Theorem 5.3. □

5.2 Integral Closure

Definition. An integral domain D is **integrally closed** if whenever an element $\alpha \in \mathrm{Quot}(D)$ is integral over D, then $\alpha \in D$.

Example. The ring $\mathbb{Z}$ is integrally closed. We need to show that if an element $\alpha \in \mathbb{Q} = \mathrm{Quot}(\mathbb{Z})$ is integral over $\mathbb{Z}$, then $\alpha \in \mathbb{Z}$. We have that

$$\alpha^n + c_{n-1}\alpha^{n-1} + \cdots + c_1\alpha + c_0 = 0,$$

where $c_0, c_1, \ldots, c_{n-1} \in \mathbb{Z}$. We let $\alpha = \frac{a}{b}$ for some $a, b \in \mathbb{Z}$, where $b \neq 0$ and a and b do not have any common factors, that is, their greatest common divisor, $\gcd(a, b)$, is equal to 1. Hence

$$(\frac{a}{b})^n + c_{n-1}(\frac{a}{b})^{n-1} + \cdots + c_1(\frac{a}{b}) + c_0 = 0,$$

and when we multiply by b^{n-1} we obtain

$$\frac{a^n}{b} + \underbrace{c_{n-1}(a^{n-1})}_{\in\mathbb{Z}} + \cdots + \underbrace{c_1(a \cdot b^{n-2})}_{\in\mathbb{Z}} + \underbrace{c_0(b^{n-1})}_{\in\mathbb{Z}} = 0.$$

It follows that $\frac{a^n}{b} \in \mathbb{Z}$, and as $\gcd(a, b) = 1$ we have $b = \pm 1$. Thus $\alpha = \pm a \in \mathbb{Z}$.

EXAMPLE. The ring $\mathbb{Z}[\sqrt{-3}]$ is *not* integrally closed. We have the quotient field $\text{Quot}(\mathbb{Z}[\sqrt{-3}]) = \{a + b\sqrt{-3} \mid a, b \in \mathbb{Q}\}$. Let $\alpha = (\frac{1}{2} + \frac{1}{2}\sqrt{-3}) \in \text{Quot}(\mathbb{Z}[\sqrt{-3}])$ such that $\alpha \notin \mathbb{Z}[\sqrt{-3}]$, but α is integral over $\mathbb{Z}$ as it is a root of the polynomial $f(x) = x^2 - x + 1 \in \mathbb{Z}[x]$. Hence $f(x) \in (\mathbb{Z}[\sqrt{-3}])[x]$, and α is also integral over $\mathbb{Z}[\sqrt{-3}]$. Thus $\mathbb{Z}[\sqrt{-3}]$ is *not* integrally closed.

The next theorem and corollary deduce that every UFD, and hence PID, is integrally closed.

Theorem 5.7. *Every UFD is integrally closed.*

Proof: Let D be a UFD. Suppose $\alpha \in D$. Clearly α satisfies the equation $x - \alpha = 0$, and is therefore integral over D.

Conversely, suppose that $\alpha \in \text{Quot}(D)$ is integral over D. It follows that α is a root in a polynomial equation

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

where $a_0, a_1, \ldots, a_{n-1} \in D$. As $\alpha \in \text{Quot}(D)$ we can express it as $\alpha = ab^{-1}$, where $a, b \in D$, $b \neq 0$, and $\gcd(a, b) = 1$. Hence

$$\begin{aligned}
(ab^{-1})^n + a_{n-1}(ab^{-1})^{n-1} + \cdots + a_1(ab^{-1}) + a_0 &= 0 \\
a^n \cdot (b^{-1})^n + a_{n-1}(a^{n-1} \cdot (b^{-1})^{n-1}) + \cdots + a_1(a \cdot b^{-1}) + a_0 &= 0 \\
a^n + a_{n-1}(a^{n-1} \cdot b) + \cdots + a_1(a \cdot b^{n-1}) + a_0 \cdot b^n &= 0.
\end{aligned}$$

Suppose now that b is *not* a unit in D. In light of the definition of a UFD and Theorem 4.4 there exists a prime $p \in D$ such that $p \mid b$. As

$$a^n = -a_{n-1}(a^{n-1} \cdot b) - \cdots - a_1(a \cdot b^{n-1}) - a_0 \cdot b^n,$$

where b is a factor in every term, we have $p \mid a^n$. Since p is a prime we have that $p \mid a$. Hence p is a factor in both a and b, which contradicts the fact that $\gcd(a, b) = 1$. We have that b is a unit, hence $b^{-1} \in D$. Thus $\alpha = ab^{-1} \in D$. □

Corollary 5.8. *Every PID is integrally closed.*

5.3 Algebraic Numbers

DEFINITION. Let F be a field and D an integral domain such that $F \subseteq D$. If $r \in D$ is integral over F, then **the element r is algebraic over F**.

REMARK. If r is a complex number which is algebraic over $\mathbb{Q}$, then r is an **algebraic number**.

EXAMPLE. An algebraic integer is an algebraic number. Let D be an integral domain. An algebraic integer, say $r \in D$, is by definition integral over $\mathbb{Z}$. As $\mathbb{Z} \subseteq \mathbb{Q}$ it follows that r is integral over $\mathbb{Q}$ by Proposition 5.1.

Theorem 5.9. *Every algebraic number $r \in \mathbb{C}$ is of the form $r = a \cdot b^{-1}$ for some algebraic integer $a \in \mathbb{C}$ and some nonzero $b \in \mathbb{Z}$.*

Proof: As $r \in \mathbb{C}$ is an algebraic number there exist $a_0, a_1, \ldots, a_{n-1} \in \mathbb{Q}$ such that we have satisfied an equation

$$r^n + a_{n-1}r^{n-1} + a_{n-2}r^{n-2} + \cdots + a_1 r + a_0 = 0.$$

We have that every a_i, where $i \in \{0, 1, \ldots, n-1\}$, is of the form $\frac{c_i}{b_i}$ for some $b_i, c_i \in \mathbb{Z}$, with $b_i \neq 0$. Let $b = \operatorname{lcm}(b_0, b_1, \ldots, b_{n-1})$, that is, b is the least common multiple of the denominators of $a_0, a_1, \ldots, a_{n-1}$. Thus $b \in \mathbb{Z}$, and we also have that $ba_i \in \mathbb{Z}$. If we multiply the same equation with b^n, then

$$(br)^n + (ba_{n-1})(br)^{n-1} + (b^2 a_{n-2})(br)^{n-2} + \ldots + (b^{n-1}a_1)(br) + (b^n a_0) = 0.$$

Here we have a monic polynomial equation with coefficients in $\mathbb{Z}$, where $br \in \mathbb{C}$ is a root. Thus br is an algebraic integer, say a. Therefore, as $a = br$ we obtain $r = ab^{-1}$, where a is an algebraic integer and $b \in \mathbb{Z}$. □

DEFINITION. An **algebraic number field** K is a subfield of $\mathbb{C}$ of the form $\mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_n)$, where $\alpha_1, \alpha_2, \ldots, \alpha_n$ are algebraic numbers.

REMARK. By $\mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_n)$ we mean the smallest subfield of $\mathbb{C}$ containing all the elements $\alpha_1, \alpha_2, \ldots, \alpha_n$, and every element in $\mathbb{Q}$.

DEFINITION. Let K be an algebraic number field and let $\mathcal{O}_K$ be the subset of all algebraic integers in K. The subset $\mathcal{O}_K$ is the **ring of integers of the algebraic number field** K.

REMARK. As every element in $\mathcal{O}_K$ is an algebraic integer we have that $\mathcal{O}_K$ is integral over $\mathbb{Z}$.

For the rest of the chapter we will show some properties of $\mathcal{O}_K$. We will see that the ring is integrally closed, that it is a Noetherian ring, and finally, that every nonzero prime ideal in $\mathcal{O}_K$ is a maximal ideal.

Proposition 5.10. *If K is an algebraic number field, then $\mathcal{O}_K$ is an integral domain.*

Proof: From the definition we have that $\mathcal{O}_K \subseteq K$, where K is an integral domain (field) and $\mathcal{O}_K$ is a subring. Any subring of an integral domain is also an integral domain. □

Theorem 5.11. *If K is an algebraic number field, then* $\text{Quot}(\mathcal{O}_K) = K$.

Proof: Let $F = \text{Quot}(\mathcal{O}_K)$ denote the quotient field of $\mathcal{O}_K$. Take any element $\alpha = ab^{-1} \in F$, where $a, b \in \mathcal{O}_K$ and $b \neq 0$. Since $\mathcal{O}_K \subseteq K$ we have that $a, b \in K$, thus $b^{-1} \in K$ since K is a field. Hence $\alpha \in K$, and we have $F \subseteq K$.

For the converse, let $\alpha \in K$. From Theorem 5.9 we have that $\alpha = ab^{-1}$ for some algebraic integer $a \in \mathbb{C}$ and some nonzero $b \in \mathbb{Z} \subseteq K$. Hence $a = b\alpha \in K$, and as a is an algebraic integer in K we have $a \in \mathcal{O}_K$. As $b \in \mathbb{Z}$ we have $b \in \mathcal{O}_K$. Therefore, a and b are also elements in the quotient field of $\mathcal{O}_K$, hence $b^{-1} \in F$. Thus $\alpha = ab^{-1} \in F$, which implies that $K \subseteq F$. Therefore, $K = F = \text{Quot}(\mathcal{O}_K)$. □

Theorem 5.12. *If K is an algebraic number field, then $\mathcal{O}_K$ is integrally closed.*

Proof: We have from Theorem 5.11 that $\text{Quot}(\mathcal{O}_K) = K$. Let $\alpha \in K$ be integral over $\mathcal{O}_K$. We have that $\mathbb{Z} \subseteq \mathcal{O}_K \subseteq K$, where $\mathcal{O}_K$ is integral over $\mathbb{Z}$. By Theorem 5.6 we have that α is integral over $\mathbb{Z}$, hence α is an algebraic integer in K. It follows that $\alpha \in \mathcal{O}_K$, and that $\mathcal{O}_K$ is integrally closed. □

Theorem 5.13. *If K is an algebraic number field, then $\mathcal{O}_K$ is Noetherian.*

Proof: We have $\mathbb{Z} \subseteq \mathcal{O}_K$, and $\mathcal{O}_K$ is an integral domain as stated in Theorem 5.10. We have seen that $\mathbb{Z}$ is both an integral domain and a Noetherian

domain. Next, $\langle 1 \rangle = \mathcal{O}_K$ is a nonzero ideal of $\mathcal{O}_K$, hence by [1, Theorem 6.5.2] there exist elements $a_1, \ldots, a_n \in \mathcal{O}_K$ such that any $r \in \mathcal{O}_K$ can be expressed as

$$r = a_1 m_1 + \ldots + a_n m_n,$$

where $m_1, \ldots, m_n \in \mathbb{Z}$. Hence $\mathcal{O}_K$ is a finitely generated $\mathbb{Z}$-module. Next, we let I be another ideal in $\mathcal{O}_K$. If $I = (0)$, then it is finitely generated. It is also finitely generated when $I \neq (0)$, using the arguments from the same theorem. Hence every ideal of $\mathcal{O}_K$ is finitely generated, and by Theorem 3.2 we have that $\mathcal{O}_K$ is Noetherian. □

Theorem 5.14. *If K is an algebraic number field, then every nonzero prime ideal P in $\mathcal{O}_K$ is a maximal ideal.*

Proof: Assume that there exists a nonzero prime ideal P in $\mathcal{O}_K$ which is *not* a maximal ideal. We define the set

$$\Omega = \{I \text{ proper nonzero ideal in } \mathcal{O}_K \mid P \subsetneq I\}.$$

As P is not a maximal ideal there is at least one ideal $I \in \Omega$, hence it is nonempty. By Theorem 5.13 we have that $\mathcal{O}_K$ is Noetherian, thus there exists a maximal element in Ω by Theorem 3.2. It follows that there exists a maximal ideal, say M, in $\mathcal{O}_K$ such that

$$P \subsetneq M \subsetneq \mathcal{O}_K.$$

By Theorem 2.6 we have that M is a prime ideal, and [1, Theorem 6.1.7] states that every nonzero ideal in $\mathcal{O}_K$ contains a nonzero (rational) integer. Hence the intersection of P and $\mathbb{Z}$ contains at least one integer, that is, $P \cap \mathbb{Z} \neq (0)$. Hence $P \cap \mathbb{Z}$ is a prime ideal in $\mathbb{Z}$ by Theorem 2.10. As $\mathbb{Z}$ is a PID there exists some $p \in \mathbb{Z}$ that generates $P \cap \mathbb{Z}$. We have $P \cap \mathbb{Z} = \langle p \rangle$, and by Theorem 2.8 we have that p is a prime in $\mathbb{Z}$. Thus

$$\langle p \rangle = P \cap \mathbb{Z} \subseteq M \cap \mathbb{Z} \subseteq \mathbb{Z}.$$

As M is a proper ideal in $\mathcal{O}_K$ we have $1 \notin M$, and it follows that $M \cap \mathbb{Z} \neq \mathbb{Z}$. In addition, $P \cap \mathbb{Z}$ is a maximal ideal by Theorem 2.7. Thus

$$\langle p \rangle = P \cap \mathbb{Z} = M \cap \mathbb{Z} \subsetneq \mathbb{Z}.$$

As $P \subsetneq M$ there exists some $r \in M$ where $r \notin P$. As $r \in \mathcal{O}_K$ it is an algebraic integer, and so r is integral over $\mathbb{Z}$. Hence there exists some positive integer n such that

$$r^n + a_{n-1} r^{n-1} + \ldots + a_1 r + a_0 = 0,$$

for some $a_0, a_1, \ldots, a_{n-1} \in \mathbb{Z}$. As $0 \in P$ we have

$$r^n + a_{n-1}r^{n-1} + \ldots + a_1 r + a_0 \in P.$$

We let k be the least positive integer for which there exist $b_0, b_1, \ldots, b_{k-1} \in \mathbb{Z}$ such that

$$r^k + b_{k-1}r^{k-1} + \ldots + b_1 r + b_0 \in P.$$

Since M is an ideal in $\mathcal{O}_K$, with $r \in M$, and $b_0, b_1, \ldots, b_{k-1} \in \mathbb{Z} \subseteq \mathcal{O}_K$, we have that

$$r^k + b_{k-1}r^{k-1} + \ldots + b_1 r \in M.$$

Thus

$$b_0 = \underbrace{(r^k + b_{k-1}r^{k-1} + \ldots + b_1 r + b_0)}_{\in P \subsetneq M} - \underbrace{(r^k + b_{k-1}r^{k-1} + \ldots + b_1 r)}_{\in M} \in M.$$

As $b_0 \in \mathbb{Z}$ we have $b_0 \in M \cap \mathbb{Z} = P \cap \mathbb{Z}$. Hence $b_0 \in P$, and it follows that

$$r^k + b_{k-1}r^{k-1} + \cdots + b_1 r = (r^k + b_{k-1}r^{k-1} + \cdots + b_1 r + b_0) - b_0 \in P.$$

If $k = 1$, then $(r^1 + b_0) - b_0 \in P$ which implies $r \in P$, but that is a contradiction as $r \notin P$. Hence $k \geq 2$, and we write

$$r \cdot (r^{k-1} + b_{k-1}r^{k-2} + \ldots + b_1) \in P.$$

Since $r \notin P$ and P is a prime ideal we get that

$$r^{k-1} + b_{k-1}r^{k-2} + \ldots + b_1 \in P.$$

This contradicts the minimality of k as there now exist $k-1$ elements in $\mathbb{Z}$, where $r^{k-1} + b_{k-1}r^{k-2} + \ldots + b_1 \in P$. The assumption that P is not a maximal ideal is proven wrong. □

6

Dedekind Domains

6.1 Dedekind Domains

Now we have come to the closing chapter of the Master's thesis, where we will prove the theorem stated in the introduction, and the chain of class inclusions will completed as we now define a *Dedekind domain*.

Definition. A **Dedekind domain** D is an integral domain that satisfies the following properties:

i) D is Noetherian.

ii) D is integrally closed.

iii) Each nonzero prime ideal in D is a maximal ideal.

Example. The ring $\mathbb{Z}$ is a Dedekind domain. We have earlier shown that $\mathbb{Z}$ is both Noetherian and integrally closed. We have also seen that nonzero prime ideals in $\mathbb{Z}$ are of the form $p\mathbb{Z}$, where $p \in \mathbb{Z}$ is a prime, and that $p\mathbb{Z}$ is a maximal ideal in $\mathbb{Z}$.

Example. Every PID is a Dedekind domain. If D is a PID, then D is Noetherian by Theorem 3.3, integrally closed by Corollary 5.8, and each nonzero prime ideal in D is a maximal ideal by Theorem 2.7. The converse is not true. We will later in the chapter see that $\mathbb{Z}[\sqrt{-5}]$ is a Dedekind domain, but it is not a UFD, hence neither a PID by Theorem 4.6.

It follows from the definition that every Dedekind domain is a Noetherian domain. In Section 3.2 we showed that $\mathbb{Z}[\sqrt{n}]$ is a Noetherian domain for any squarefree integer n, but in an example from Section 5.2 we saw $\mathbb{Z}[\sqrt{-3}]$ is not integrally closed, hence there is a Noetherian domain that is not a Dedekind domain. Using this fact and the previous example we deduce that

$$\left\{\begin{matrix}\text{Principal ideal}\\ \text{domains}\end{matrix}\right\} \subsetneq \left\{\begin{matrix}\text{Dedekind}\\ \text{domains}\end{matrix}\right\} \subsetneq \left\{\begin{matrix}\text{Noetherian}\\ \text{domains}\end{matrix}\right\},$$

thus our chain of class inclusions is completed.

Theorem 6.1. *If K is an algebraic number field, then $\mathcal{O}_K$ is a Dedekind domain.*

Proof: By Theorem 5.10 we have that $\mathcal{O}_K$ is an integral domain, and we have earlier shown that

i) $\mathcal{O}_K$ is Noetherian by Theorem 5.13,

ii) $\mathcal{O}_K$ is integrally closed by Theorem 5.12, and

iii) each nonzero prime ideal in $\mathcal{O}_K$ is a maximal ideal by Theorem 5.14.

Thus $\mathcal{O}_K$ is a Dedekind domain. □

In the introduction of the thesis we stated that ideals in $\mathbb{Z}[\sqrt{n}]$ factorize uniquely into prime ideals, at least when $\mathbb{Z}[\sqrt{n}]$ is a Dedekind domain. We will not go into the theory of how to decide whether or not $\mathbb{Z}[\sqrt{n}]$ is a Dedekind domain; we refer to [1, Section 5.4] for details about the topic. In the same section, by [1, Theorem 5.4.2], we have that if K is an algebraic number field with $K = \mathbb{Q}(\sqrt{n})$, then

$$\mathcal{O}_K = \mathbb{Z}[\sqrt{n}],$$

whenever n is a squarefree integer with $n \not\equiv 1 \pmod 4$. We have that $\mathbb{Q}(\sqrt{n})$ is an algebraic number field as $\sqrt{n}$ is algebraic over $\mathbb{Q}$, being a root of the polynomial $x^2 - n \in \mathbb{Q}[x]$. Recall that $\mathbb{Z}[\sqrt{n}]$ is called a *quadratic domain*; similarly, $\mathbb{Q}(\sqrt{n})$ is called a **quadratic field**. We use the fact that $\mathcal{O}_K = \mathbb{Z}[\sqrt{n}]$ to state the following proposition.

Proposition 6.2. *If n is a squarefree integer with $n \not\equiv 1 \pmod 4$, then $\mathbb{Z}[\sqrt{n}]$ is a Dedekind domain.*

Proof: If K is an algebraic number field, then $\mathcal{O}_K = \mathbb{Z}[\sqrt{n}]$ is a Dedekind domain by Theorem 6.1. □

REMARK. We cannot rule out the option of $\mathbb{Z}[\sqrt{n}]$ being a Dedekind domain for every $n \equiv 1 \pmod 4$, but we have already seen that $\mathbb{Z}[\sqrt{-3}]$, for instance, is not a Dedekind domain.

6.2 Prime Ideals in Dedekind Domains

In order to complete the proof of the main theorem, we first need a few more theorems concerning the behaviour of prime ideals in Dedekind domains.

Theorem 6.3. *In a Noetherian ring every nonzero ideal contains a product of one or more nonzero prime ideals.*

Proof: Let R be a Noetherian ring with a proper nonzero ideal I. Assume that I does *not* contain a product of one or more nonzero prime ideals. Let Ω be the set of all ideals in R with the same property, that is, Ω is set of all nonzero ideals which do not contain a product of one or more nonzero prime ideals. Obviously $I \in \Omega$, and so Ω is nonempty, and by Theorem 3.2 we have that Ω contains a maximal element, say M. No ideals in Ω are prime ideals, hence M it is not a prime ideal. By Theorem 2.9 there exist ideals A and B in R satisfying $AB \subseteq M$, where both $A \nsubseteq M$ and $B \nsubseteq M$. Next, we define the ideals A_1 and B_1 in R by

$$A_1 = M + A \quad \text{and} \quad B_1 = M + B$$

such that

$$M \subsetneq A_1 \quad \text{and} \quad M \subsetneq B_1.$$

Neither A_1 nor B_1 is contained in Ω as M is a maximal ideal in Ω. Thus there exist some prime ideals $P_1, \ldots, P_k$ such that the product of one or more P_i, where $i \in \{1, \ldots, k\}$, are contained in A_1 and B_1, say

$$P_1 \cdots P_h \subseteq A_1 \quad \text{and} \quad P_{h+1} \cdots P_k \subseteq B_1.$$

We have

$$A_1 B_1 = (M + A)(M + B) = MM + MB + AM + AB \subseteq M.$$

It follows that

$$P_1 \cdots P_k = (P_1 \cdots P_h)(P_{h+1} \cdots P_k) \subseteq A_1 B_1 \subseteq M,$$

but then M is not an element in Ω, which is a contradiction. Hence I contains a product of one or more nonzero prime ideals. □

Corollary 6.4. *In a Dedekind domain every nonzero ideal contains a product of one or more nonzero prime ideals.*

In the proofs to follow we need the notion of *fractional ideals* of an integral domain. We will see that in an integral domain D any ideal in the ordinary sense is also a fractional ideal, but that the converse is not true.

DEFINITION. Let D be an integral domain with the quotient field $\mathrm{Quot}(D)$. For each prime ideal P in D we define the set $\tilde{P}$ as

$$\tilde{P} = \{\alpha \in \mathrm{Quot}(D) \mid \alpha P \subseteq D\}.$$

EXAMPLE. The ring $\mathbb{Z}$ is an integral domain and $\mathbb{Q}$ is its quotient field. For each prime ideal $P = p\mathbb{Z}$ in $\mathbb{Z}$, where p is a prime number, we have that

$$\tilde{P} = \{\alpha \in \mathbb{Q} \mid \alpha p\mathbb{Z} \subseteq \mathbb{Z}\} = \{\alpha \in \mathbb{Q} \mid \alpha p \in \mathbb{Z}\}.$$

REMARK. If $P = (0)$, then $\tilde{P} = \mathrm{Quot}(D)$ since $\alpha P = \alpha \cdot (0) = (0) \subseteq D$ for all $\alpha \in \mathrm{Quot}(D)$.

DEFINITION. If D is an integral domain with quotient field $\mathrm{Quot}(D)$, then a nonempty subset $I_f \subseteq \mathrm{Quot}(D)$ is a **fractional ideal** of D if the following conditions are satisfied:

i) $\alpha, \beta \in I_f \;\Rightarrow\; \alpha - \beta \in I_f$.

ii) $r \in D,\ \alpha \in I_f \;\Rightarrow\; r\alpha \in I_f$.

iii) There exists a nonzero $r \in D$ such that $rI_f \subseteq D$.

REMARK. It follows from the definition that any ideal I in D, in the ordinary sense, is also a fractional ideal of D. On the other hand, if a fractional ideal I_f of D is fully contained in D, then I_f is also an ideal in D, in the ordinary sense.

EXAMPLE. If P is a prime ideal in an integral domain D, then $\tilde{P}$ is a fractional ideal of D. We have by definition that $\tilde{P}$ is a nonempty subset of $\mathrm{Quot}(D)$.

i) If $\alpha, \beta \in \tilde{P}$, then $\alpha P \subseteq D$ and $\beta P \subseteq D$. Hence $\alpha P - \beta P \subseteq D$ which implies that $(\alpha - \beta)P \subseteq D$, and we have $\alpha - \beta \in \tilde{P}$.

ii) If $\alpha \in \tilde{P}$, then $\alpha P \subseteq D$, and $r(\alpha P) \subseteq rD \subseteq D$ for some $r \in D$. We get $(r\alpha)P \subseteq D$, thus $r\alpha \in \tilde{P}$.

iii) If P is a nonzero ideal there exists some nonzero $r \in D$ such that $r \in P$. For all $\alpha \in \tilde{P}$ we have that $\alpha P \subseteq D$, in particular $\alpha r \in D$. We have $\alpha r = r\alpha$

since D is commutative, hence $r\alpha \in D$ for all $\alpha \in \tilde{P}$, which implies that $r\tilde{P} \subseteq D$. From the remark following the definition of $\tilde{P}$ we see that $r\tilde{P} \subseteq D$ also holds for $P = (0)$.

Theorem 6.5. *In a Noetherian domain D every fractional ideal is a finitely generated D-module.*

Proof: Let I_f be a fractional ideal of a Noetherian domain D. From the definition of fractional ideals there exists a nonzero $r \in D$ such that $rI_f \subseteq D$. We have that $r^{-1} \in \mathrm{Quot}(D)$ is the inverse of r, and we write $I_f \subseteq r^{-1}D$. There must exist some subset $I \subseteq D$ such that $I_f = r^{-1}I$. We have that $r^{-1}I$ is a fractional ideal of D, hence the three conditions in the definition are fulfilled, especially the two first. We choose two general elements $(r^{-1}a), (r^{-1}b) \in r^{-1}I$, for some $a, b \in I$, and get that

i) $(r^{-1}a) - (r^{-1}b) = r^{-1}(a-b) \in r^{-1}I$ implies that $a - b \in I$, and

ii) $s(r^{-1}a) \in r^{-1}I$ for all $s \in D$ implies that $r^{-1}(sa) \in r^{-1}I$, hence $sa \in I$.

Thus I is an ideal in D. As D is Noetherian we have that I is finitely generated by Theorem 3.2, hence

$$I = \langle a_1, a_2, \ldots, a_k \rangle,$$

for some $a_1, a_2, \ldots, a_k \in D$. Therefore, I is also a finitely generated D-module as it is a submodule of D. We get that

$$I_f = r^{-1}I = r^{-1}\langle a_1, a_2, \ldots, a_k \rangle = \langle r^{-1}a_1, r^{-1}a_2, \ldots, r^{-1}a_k \rangle$$

is a finitely generated D-module as well. Hence every fractional ideal in a Noetherian domain is a finitely generated D-module. □

Lemma 6.6. *If P is a prime ideal in a Dedekind domain D, then $D \subsetneq \tilde{P}$.*

Proof: As P is a prime ideal it is a proper ideal in D. From the remark following the defintion of $\tilde{P}$ we have that if $P = (0)$, then $\tilde{P} = \mathrm{Quot}(D)$. Hence $D \subsetneq \tilde{P}$ if $P = (0)$.

We now suppose $P \neq (0)$. For any $r \in D$ we have $rP \subseteq D$, thus $r \in \tilde{P}$, and $D \subseteq \tilde{P}$. If $D \subsetneq \tilde{P}$, then there must exist an element $\alpha \in \tilde{P}$ where $\alpha \notin D$. We let $b \in P$ be a nonzero element such that $\langle b \rangle \subseteq P$. By Corollary 6.4 there exists a product of one or more nonzero prime ideals contained in $\langle b \rangle$. Let k be the smallest integer possible such that the following inclusion holds:

$$P_1 \cdots P_k \subseteq \langle b \rangle \subseteq P,$$

where $P_1, \ldots, P_k$ are nonzero prime ideals. Since P is a prime ideal we have that

$$P_i \subseteq P, \text{ for some } i \in \{1, \ldots, k\},$$

by Theorem 2.9. As we are dealing with commutative rings we are free to relabel any P_i. We may, without loss of generality, choose P_1 to be such that

$$P_1 \subseteq P.$$

As P_1 is a nonzero prime ideal in a Dedekind domain it is a maximal ideal, hence

$$P_1 = P.$$

We first look at the case when $k = 1$, where

$$P_1 \subseteq \langle b \rangle \subseteq P \;\Rightarrow\; P_1 = \langle b \rangle = P.$$

Define the element $\alpha \in \tilde{P}$ as b^{-1}, which one can do since $b \neq 0$. Now, assume that $\alpha \in D$, that is, $b^{-1} \in D$, it follows that $b \in D$ is a unit. Hence $\langle b \rangle = D$ by Proposition 2.3. It follows that

$$P = \langle b \rangle = D,$$

but this contradicts the fact that P is a proper ideal in D. Hence we have shown that $\alpha \notin D$. We have

$$\alpha P = b^{-1}P = b^{-1}\langle b \rangle = \langle 1 \rangle = D,$$

and since $\alpha P = D$ implies that $\alpha P \subseteq D$ we get

$$\alpha \in \tilde{P}.$$

Therefore, when $k = 1$ we have that

$$\alpha \in \tilde{P} \text{ and } \alpha \notin D \;\Rightarrow\; D \subsetneq \tilde{P}.$$

It remains to show that $D \subsetneq \tilde{P}$ for $k \geq 2$. Recall that we chose k to be the smallest number of prime ideal factors such that $P_1 \cdots P_k \subseteq \langle b \rangle$. This implies that

$$P_2 \cdots P_k \nsubseteq \langle b \rangle$$

as there are $k - 1$ prime ideals. If there were an inclusion like this it would contradict the minimality of k. In other words, there exists some nonzero element $a \in P_2 \cdots P_k$ such that $a \notin \langle b \rangle$. It follows that $\langle a \rangle \subseteq P_2 \cdots P_k$. Since $b \neq 0$ we may now define α to be

$$\alpha = ab^{-1} \in \text{Quot}(D),$$

which implies that $a = b\alpha$. Since $a \notin \langle b\rangle = \{br \mid r \in D\}$ we have that $a \neq br$, and we get $r \neq ab^{-1}$ for all $r \in D$. Thus $\alpha = ab^{-1} \notin D$. However,

$$\langle a\rangle P = \langle a\rangle P_1 \subseteq (P_2 \cdots P_k)P_1 = P_1 \cdots P_k \subseteq \langle b\rangle,$$

and we have

$$\alpha P = \{\alpha p \mid p \in P\} = \{(ab^{-1})p \mid p \in P\} = \{b^{-1}(ap) \mid p \in P\}.$$

Especially we have $ap \in \langle b\rangle$, hence

$$\alpha P \subseteq \{b^{-1}x \mid x \in \langle b\rangle\} = \{b^{-1}(br) \mid r \in D\} = D.$$

Thus

$$\alpha P \subseteq D \;\Rightarrow\; \alpha \in \tilde{P}.$$

Hence for $k \geq 2$ we have that

$$\alpha \in \tilde{P} \text{ and } \alpha \notin D \;\Rightarrow\; D \subsetneq \tilde{P},$$

which completes the proof that $D \subsetneq \tilde{P}$. □

Lemma 6.7. *If P is a nonzero prime ideal in a Dedekind domain D, then $\tilde{P}P = D$.*

Proof: We first show that either $\tilde{P}P = D$ or $\tilde{P}P = P$. We have earlier shown that both P and $\tilde{P}$ are fractional ideals in D and hence $\tilde{P}P$ is also a fractional ideal of D. Since we obviously have that $\tilde{P}P \subseteq D$ then $\tilde{P}P$ is not only a fractional ideal, but also an ideal in the ordinary sense. We have that P is a nonzero prime ideal in a Dedekind domain, hence P is maximal. Next, if $\alpha \in \tilde{P}$, then $\alpha P \subseteq D$. Hence $D \subseteq \tilde{P}$. By Proposition 2.1 we have $P = DP$, hence $P \subseteq \tilde{P}P$. Thus $\tilde{P}P = D$ or $\tilde{P}P = P$.

Suppose that $\tilde{P}P = P$. We let $\alpha, \beta \in \tilde{P}$. It follows that $\alpha P \subseteq \tilde{P}P = P$ and $\beta P \subseteq \tilde{P}P = P$. We have $(\alpha - \beta)P = \alpha P - \beta P \subseteq P$, hence $\alpha - \beta \in \tilde{P}$. Since $\beta P \subseteq P$ we have $\alpha(\beta P) \subseteq \alpha P$, thus $(\alpha\beta)P \subseteq P$. It follows that $\alpha\beta \in \tilde{P}$, and $\tilde{P}$ is closed under multiplication. We also have that $1 \in \mathrm{Quot}(D)$ and $1 \in \tilde{P}$. Hence $\tilde{P}$ is a subring of $\mathrm{Quot}(D)$. As $\mathrm{Quot}(D)$ is a field, it is also an integral domain, which again implies that $\tilde{P}$ is an integral domain. As D is a Dedekind domain it is also a Noetherian domain, and as $\tilde{P}$ is a fractional ideal of D it is, by Theorem 6.5, a finitely generated D-module. From Lemma 6.6 we have that $D \subsetneq \tilde{P}$. So to sum up, we have two integral domains D and $\tilde{P}$ such that $D \subseteq \tilde{P}$, and $\tilde{P}$ is a finitely generated D-module. Thus $\tilde{P}$ is integral over D by Corollary 5.4. Hence every element $\alpha \in \tilde{P}$ is integral over D, but since D is a Dedekind domain it is integrally closed. It follows that every element that is integral over D is itself an element in D. Hence $\alpha \in D$ for all $\alpha \in \tilde{P}$, thus $D = \tilde{P}$. This contradicts the fact that $D \subsetneq \tilde{P}$, hence $\tilde{P}P = D$. □

6.3 Main Theorem

Last but not least, we will finally prove the main theorem.

Theorem 6.8. *In a Dedekind domain D every proper nonzero ideal I is a product of prime ideals in D, and this factorization is unique in the sense that if*

$$I = P_1P_2\cdots P_k = Q_1Q_2\cdots Q_n,$$

where P_i and Q_j are prime ideals, then $k = n$, and after relabelling (if necessary)

$$P_i = Q_i,\ i \in \{1, 2, \ldots, k\}.$$

Proof: Assume there exists some proper nonzero ideal M in D that is *not* a product of prime ideals. We let Ω denote the set containing all such ideals, that is, Ω is the set containing all proper nonzero ideals in D that are not a product of one or more prime ideals. As $M \in \Omega$ we have a nonempty set. As D is a Dedekind domain it is Noetherian by definition, and by Theorem 3.2 there exists a maximal element in Ω. We let M be our maximal element in Ω. By Corollary 6.4 every nonzero ideal in a Dedekind domain contains a product of one or more nonzero prime ideals. Therefore, we have that

$$P_1\cdots P_k \subseteq M,$$

where $P_1, \ldots, P_k$ are nonzero prime ideals in D. We now let k be the smallest integer possible for such a product to exist. If $k = 1$, then $P_1 \subseteq M \subsetneq D$. Since P_1 is a nonzero prime ideal in a Dedekind domain it is by definition a maximal ideal. Hence $M = P_1$, but as M is not a product of prime ideals this cannot be true, hence $k \geq 2$. Next, let P denote a maximal ideal in D such that

$$P_1\cdots P_k \subseteq M \subseteq P.$$

Since P is also a prime ideal we have that

$$P_i \subseteq P, \text{ for some } i \in \{1, \ldots, k\},$$

by Theorem 2.9. Without loss of generality we choose P_1 to be such that

$$P_1 \subseteq P.$$

As P_1 is a prime ideal it is maximal, hence

$$P_1 = P.$$

It follows from $M \subseteq P$ that

$$M \subseteq P_1.$$

By Lemma 6.7 we have that $\tilde{P_1}P_1 = D$, thus

$$\tilde{P_1}P_1(P_2 \cdots P_k) = D(P_2 \cdots P_k) \;\Rightarrow\; \tilde{P_1}P_1 \cdots P_k = DP_2 \cdots P_k.$$

Notice that since P_i is an ideal in D we get that $DP_i = P_i$ by Proposition 2.1, and so $DP_2 \cdots P_k = P_2 \cdots P_k$. Thus

$$P_2 \cdots P_k = \tilde{P_1}P_1 \cdots P_k \subseteq \tilde{P_1}M.$$

As M is an ideal in D we have $M \subseteq DM$. By Lemma 6.6 we have that $D \subsetneq \tilde{P_1}$, that is, every $r \in D$ is also an element in $\tilde{P}$, and we have the inclusion

$$M \subseteq \tilde{P_1}M.$$

If we assume that $M = \tilde{P_1}M$, then

$$P_2 \cdots P_k \subseteq M,$$

which contradicts the minimality of k. This shows that there is a proper inclusion

$$M \subsetneq \tilde{P_1}M.$$

We have that both $\tilde{P_1}$ and M are fractional ideals of D, hence $\tilde{P_1}M$ is also a fractional ideal. As $M \subseteq P_1$ we have $\tilde{P_1}M \subseteq \tilde{P_1}P_1 = D$. Thus $\tilde{P_1}M$ is also an ideal in the ordinary sense. Since we have $M \subsetneq \tilde{P_1}M$, and the fact that M is maximal in Ω, we get $\tilde{P_1}M \notin \Omega$. It follows that $\tilde{P_1}M$ is a product of one or more nonzero prime ideals, say $Q_1, \ldots, Q_m$, such that

$$\tilde{P_1}M = Q_1 \cdots Q_m.$$

Since $DM = M$ and $\tilde{P_1}P_1 = D$ we have that $(\tilde{P_1}P_1)M = M$. Hence

$$M = P_1(\tilde{P_1}M) = P_1Q_1 \cdots Q_m,$$

but this contradicts the fact that M is not a product of prime ideals, so this assumption cannot be true. Hence we have proven that every proper nonzero ideal in D is a product of prime ideals.

It remains to show that the factorization of ideals as a product of prime ideals is unique. Let $k \in \mathbb{Z}$ be minimal with the property that there exists a proper nonzero ideal I in D with two distinct factorizations such that

$$I = P_1 \cdots P_k = Q_1 \cdots Q_n,$$

where P_i and Q_j are nonzero prime ideals in D. We let Λ denote the set containing all nonzero ideals in D that have at least two distinct factorizations as a product of nonzero prime ideals. As $I \in \Lambda$ it is a nonempty set, and as D is Noetherian there exists a maximal element in Λ by Theorem 3.2. We choose I to be our maximal element. Next, as Q_1 is an ideal we have $Q_1 D = Q_1$, and as $Q_2 \cdots Q_n \subseteq D$ we get $Q_1(Q_2 \cdots Q_n) \subseteq Q_1$. It follows that that

$$P_1 \cdots P_k \subseteq Q_1,$$

and since Q_1 is a prime ideal we have

$$P_i \subseteq Q_1, \text{ for some } i \in \{1, 2, \ldots, k\},$$

by Theorem 2.9. We are free to relabel any P_i. We may, without loss of generality, choose P_1 to be such that

$$P_1 \subseteq Q_1.$$

We have that P_1 is a maximal ideal since it is a prime ideal in a Dedekind domain, and thus

$$P_1 = Q_1.$$

Hence

$$P_2 \cdots P_k = Q_2 \cdots Q_n,$$

which clearly is an ideal, say J, in D. Thus have that

$$J = P_2 \cdots P_k = Q_2 \cdots Q_n$$

is a product of two distinct factorizations, otherwise it contradicts the assumptions of I being a product of two factorizations. We have that J is a product of $k-1$ nonzero prime ideals, which contradicts the minimality of k. Hence there does not exist a proper nonzero ideal in D with two distinct factorizations. This finishes the proof. □

We will end the thesis with two examples that illustrate the theorem. We have already, during the text, done most of the hard work of the first example, which will be presented in depth.

Example. Let $D = \mathbb{Z}[\sqrt{-5}]$. From examples in Section 4.3 we have seen that $2, (1 + \sqrt{-5})$, and $(1 - \sqrt{-5})$ are irreducible elements in $\mathbb{Z}[\sqrt{-5}]$. Similarly, we can show that $3 \in \mathbb{Z}[\sqrt{-5}]$ is irreducible as well. In the same section we showed that neither of the elements are associates. From this we deduce that D is not a UFD as we have

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}),$$

which are two different factorizations of the same element. However, by Proposition 6.2 we have that $D = \mathbb{Z}[\sqrt{-5}]$ is a Dedekind domain, thus there exists a unique factorization of the ideals in D into prime ideals, and hence we will show that the factorization

$$\langle 6\rangle = \langle 2\rangle \cdot \langle 3\rangle = \langle (1+\sqrt{-5})\rangle \cdot \langle (1-\sqrt{-5})\rangle$$

will induce the same factorization of prime ideals.

We start by forming prime ideals generated by the four elements. Note that any ideal I where both 2 and 3 are elements will generate the whole ring D as the difference $3-2=1 \in I$ implies $I = D$ by Proposition 2.2. Hence I is not a prime ideal. Ruling out those alternatives we are left we the following candidates for prime ideals:

$$\begin{aligned}
&a)\ \langle 2, (1+\sqrt{-5})\rangle \\
&b)\ \langle 2, (1-\sqrt{-5})\rangle \\
&c)\ \langle 2, (1+\sqrt{-5}), (1-\sqrt{-5})\rangle \\
&d)\ \langle 3, (1+\sqrt{-5})\rangle \\
&e)\ \langle 3, (1-\sqrt{-5})\rangle \\
&f)\ \langle 3, (1+\sqrt{-5}), (1-\sqrt{-5})\rangle \\
&g)\ \langle (1+\sqrt{-5}), (1-\sqrt{-5})\rangle
\end{aligned}$$

We use the fact that the sum or the difference between generators is also a generator, hence

$$\begin{aligned}
\langle 2, (1+\sqrt{-5})\rangle &= \langle 2, (1+\sqrt{-5}), 2-(1+\sqrt{-5})\rangle \\
&= \langle 2, (1+\sqrt{-5}), (1-\sqrt{-5})\rangle \\
&= \langle 2, 2-(1-\sqrt{-5}), (1-\sqrt{-5})\rangle \\
&= \langle 2, (1-\sqrt{-5})\rangle.
\end{aligned}$$

It follows that $a)$, $b)$, and $c)$ are the same ideal. Next, we see that

$$\begin{aligned}
\langle (1+\sqrt{-5}), (1-\sqrt{-5})\rangle &= \langle (1+\sqrt{-5}), (1-\sqrt{-5}), (1+\sqrt{-5})+(1-\sqrt{-5})\rangle \\
&= \langle (1+\sqrt{-5}), (1-\sqrt{-5}), 2\rangle,
\end{aligned}$$

hence $g) = c)$. Similar inspections will show that $d) \neq e) \neq a)$. Finally

$$\begin{aligned}
\langle 3, (1+\sqrt{-5}), (1-\sqrt{-5})\rangle &= \langle 3, (1+\sqrt{-5}), (1-\sqrt{-5}), (1+\sqrt{-5})+(1-\sqrt{-5})\rangle \\
&= \langle 3, (1+\sqrt{-5}), (1-\sqrt{-5}), 2\rangle
\end{aligned}$$

shows us that $f)$ contains both 2 and 3, thus $3-2=1$, and is equal to $\langle 1\rangle = D$. We name our remaining ideals

$$\begin{aligned} P_1 &= \langle 2, (1+\sqrt{-5})\rangle = \langle 2, (1-\sqrt{-5})\rangle, \\ P_2 &= \langle 3, (1+\sqrt{-5})\rangle, \\ P_3 &= \langle 3, (1-\sqrt{-5})\rangle. \end{aligned}$$

In an example in Section 2.4 we showed that the ideal $P_1 = \langle 2, (1+\sqrt{-5})\rangle$ was a prime ideal in $\mathbb{Z}[\sqrt{-5}]$. Similarly, we can show that P_2 and P_3 also are prime ideals in $\mathbb{Z}[\sqrt{-5}]$. Now, consider the following:

$$\begin{aligned} P_1P_1 &= \langle 2, (1+\sqrt{-5})\rangle \cdot \langle 2, (1-\sqrt{-5})\rangle \\ &= \langle 4, 2(1+\sqrt{-5}), 2(1-\sqrt{-5}), 6\rangle \\ &= \langle 2\rangle \cdot \langle 2, (1+\sqrt{-5}), (1-\sqrt{-5}), 3\rangle \\ &= \langle 2\rangle \cdot \langle 1\rangle = \langle 2\rangle, \end{aligned}$$

$$\begin{aligned} P_2P_3 &= \langle 3, (1+\sqrt{-5})\rangle \cdot \langle 3, (1-\sqrt{-5})\rangle \\ &= \langle 9, 3(1+\sqrt{-5}), 3(1-\sqrt{-5}), 6\rangle \\ &= \langle 3\rangle \cdot \langle 3, (1+\sqrt{-5}), (1-\sqrt{-5}), 2\rangle \\ &= \langle 3\rangle \cdot \langle 1\rangle = \langle 3\rangle, \end{aligned}$$

$$\begin{aligned} P_1P_2 &= \langle 2, (1+\sqrt{-5})\rangle \cdot \langle 3, (1+\sqrt{-5})\rangle \\ &= \langle 6, 2(1+\sqrt{-5}), 3(1+\sqrt{-5}), (1+\sqrt{-5})^2\rangle \\ &= \langle (1+\sqrt{-5})\rangle \cdot \langle (1-\sqrt{-5}), 2, 3, (1+\sqrt{-5})\rangle \\ &= \langle (1+\sqrt{-5})\rangle \cdot \langle 1\rangle = \langle (1+\sqrt{-5})\rangle, \end{aligned}$$

$$\begin{aligned} P_1P_3 &= \langle 2, (1-\sqrt{-5})\rangle \cdot \langle 3, (1-\sqrt{-5})\rangle \\ &= \langle 6, 2(1-\sqrt{-5}), 3(1-\sqrt{-5}), (1-\sqrt{-5})^2\rangle \\ &= \langle (1-\sqrt{-5})\rangle \cdot \langle (1+\sqrt{-5}), 2, 3, (1-\sqrt{-5})\rangle \\ &= \langle (1-\sqrt{-5})\rangle \cdot \langle 1\rangle = \langle (1-\sqrt{-5})\rangle. \end{aligned}$$

We see that

$$\langle 6\rangle = \langle 2\rangle \cdot \langle 3\rangle = P_1P_1 \cdot P_2P_3 = (P_1)^2P_2P_3,$$

and

$$\langle 6\rangle = \langle (1+\sqrt{-5})\rangle \cdot \langle (1-\sqrt{-5})\rangle = P_1P_2 \cdot P_1P_3 = (P_1)^2P_2P_3.$$

Thus $6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$ induces the same the factorization of prime ideals for the ideal $\langle 6 \rangle$. By Theorem 6.8 we have that this is the only factorization of the ideal $\langle 6 \rangle$ into prime ideals.

EXAMPLE. A similar example is $\mathbb{Z}[\sqrt{-17}]$, which is not a UFD as

$$18 = 2 \cdot 3 \cdot 3 = (1 + \sqrt{-17})(1 - \sqrt{-17}),$$

where all factors are irreducible and not associated elements. By Proposition 6.2 $\mathbb{Z}[\sqrt{-17}]$ is a Dedekind domain, hence the ideal generated by 18 factorizes uniquely into prime ideals by Theorem 6.8; in this case

$$\langle 18 \rangle = (P_1)^2 (P_2)^2 (P_3)^2,$$

where $P_1 = \langle 2, (1 + \sqrt{-17}) \rangle, P_2 = \langle 3, (1 + \sqrt{-17}) \rangle$, and $P_3 = \langle 3, (1 - \sqrt{-17}) \rangle$. For detailed calculations, see [5, Section 5.2].

Bibliography

[1] Ş. Alaca and K. S. Williams. *Introductory Algebraic Number Theory.* Cambridge University Press: Cambridge, UK / New York, NY / Port Melbourne, AU-VIC / Madrid / Cape Town, 1st edition, 2004.

[2] M. Auslander and D. A. Buchsbaum. Unique Factorization in Regular Local Rings. *Proceedings of the National Academy of Sciences of the United States of America*, (Volume 45, Issue 5):733–734, 1959.

[3] P. B. Bhattacharya, S. K. Jain, and S. R. Nagpaul. *Basic Abstract Algebra.* Cambridge University Press: Cambridge, UK / New York, NY / Oakleigh, AU-VIC, 2nd edition, 1994.

[4] G. H. Hardy and E. M. Wright. *An Introduction to the Theory of Numbers.* Oxford Univerity Press: London W.1, UK, 4th edition, 1960.

[5] I. N . Stewart and D. O. Tall. *Algebraic Number Theory.* Champman and Hall Ltd: Londonm UK, 1st edition, 1979.

[6] J. C. Wilson. A Principal Ideal Ring That Is Not a Euclidean Ring. *Mathematics Magazine*, (Volume 46, No. 1, Jan. 1973):34–38, 1973.