Summary

In this thesis we study ideals in Dedekind domains, which factorize uniquely into a product of prime ideals. Since not every Dedekind domain is a unique factorization domain, a general element in these domains does not necessarily factorize uniquely, so it is interesting that ideals has this property.

Norsk sammendrag:
I denne teksten studerer vi idealer i Dedekind-områder, som faktoriseres til et unikt produkt av primidealer. I et Dedekind-område er det ikke nødvendigvis slik at et generelt element faktoriseres unikt, så det er interessant at idealer har denne egenskapen.

Preface

Before you lies the work that concludes my time as a student at the Department of Mathematical Science and at the Teacher Education program at NTNU. I have found working with this thesis to be very educative, and it has allowed me to focus on the parts of mathematics that I have come to enjoy the most. Of all the different parts of my study program that I have been through, this semester has been the most rewarding.

I would like to thank my supervisor Petter Andreas Bergh for all his guidance and help during the months of writing. Thank you for helping me making this time much less stressful than it could have been.

Also, a big thanks to my friends here in Trondheim, who have made these years very memorable, and the studies that much easier. Finally, thank you to my family for always supporting me and building me up.

Simen Einmo Engdal
Trondheim, 01.12.16

Table of Contents

Chapter 1

Introduction

It is well known that in $\mathbb{Z}$, the ring of integers, elements factorize uniquely into a product of prime numbers. If we extend this ring with an element of the form $\sqrt{n}$ where $n \in \mathbb{Z}$, we obtain a ring which does not necessarily have the property of its elements factorizing uniquely. However, these rings will be Dedekind domains for certain values of n, and in Dedekind domains nonzero proper ideals factorize uniquely into a product of nonzero prime ideals. The main objective of this thesis is to prove this fact. This was first done by the German mathematician Julius Wilhelm Richard Dedekind, in connection with his work on algebraic number theory.

To that end, we start by looking at integral domains along with the aforementioned ideals and prime ideals in Chapter 2. In Chapter 3 we present the notion of Noetherian domains, which is of importance as it is part of both the definition of Dedekind domains, and the proof of our main theorem. We move on to discuss additional types of domains in Chapter 4, namely Euclidean domains, principal ideal domains and unique factorization domains, before we define an algebraic number field in Chapter 5, and its associated ring of integers. In Chapter 6 we prove that this ring is in fact a Dedekind domain, and we give the proof of our main theorem.

Chapter 2

Integral domains and ideals

2.1 Commutative rings

Assuming the reader to be familiar with basic algebraic concepts and group theory, we start by defining a ring. It needs to be pointed out that all rings in this thesis will be rings with unity, i.e. rings containing a multiplicative identity element 1.

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

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

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 $1 \cdot a = a \cdot 1 = a$

From here we immediately define a commutative ring.

Definition. A *commutative ring* R is a ring in which multiplication is commutative, that is $ab = ba$ for all a, $b \in R$.

Example 2.1.1. The set of integers $\mathbb{Z}$ is clearly a ring. As multiplication by integers is known to be commutative, $\mathbb{Z}$ is also a commutative ring.

In this thesis we are only interested in commutative rings, and from this point on every ring stated is a commutative ring. In order to simplify the method of concluding that a given set is in fact a ring, we give the definition of a subring.

Definition. Let $(R,+,\cdot)$ be a ring and S a nonempty subset of R. Then S is called a *subring* if $(S,+,\cdot)$ is itself a ring.

Example 2.1.2. Trivially, $\mathbb{Z}$ is a subring of $\mathbb{Q}$, the ring of rational numbers.

Theorem 2.1.3. *A nonempty subset S of a ring R is a subring if and only if S contains the multiplicative identity 1 of R, and for all $a,b \in S$ we have $a - b \in S$ and $ab \in S$.*

Example 2.1.4. Let R be a ring and $R[x]$ the polynomial ring over R. Let S be a set consisting of polynomials of the form

$$a_0 + a_2x^2 + \cdots + a_nx^n$$

where $n = 0$ or $n \geq 2$ and $a_i \in R$, i.e. polynomials over R for which the coefficient of x is zero. Then S is a subset of $R[x]$, contains the multiplicative identity, and is closed under multiplication and subtraction, making it a subring of $R[x]$ by Theorem 2.1.3.

Next, we move on to a special class of rings which gives us a natural setting for studying divisibility.

2.2 Integral domains

As every ring will be a commutative ring, every integral domain will be a commutative integral domain, as stated in the following definition:

Definition. An *integral domain* D is a ring that has no divisors of zero, that is, if $ab = 0$ either $a = 0$ or $b = 0$.

Furthermore, if for every $a \in D$ where $a \neq 0$, there exits $b \in D$ with $ab = 1$, every nonzero element in D has an inverse. In this case D is called a *field*. If a field is a subring of another field, it is called a subfield.

Theorem 2.2.1. *Every subring of a field that contains the identity, is an integral domain.*

Proof. Let $R \subseteq F$ be a subring of a field F. Assume that for $x, y \in R$ we have $xy = 0$. Now, since $x, y \in F$ and R and F has the same zero element, either $x = 0$ or $y = 0$, and so R has no divisors of zero. Since all our rings contain 1, R is an integral domain. □

Note that an integral domain need not be a field, but from every integral domain we may construct a field by inverting all the nonzero elements, obtaining the *quotient field* of the integral domain.

Definition. Let D be an integral domain. The *quotient field* of D, denoted $\mathrm{Quot}(D)$ is defined as

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

Example 2.2.2. In the ring $\mathbb{Q}$, elements can be written as fractions a/b where a and $b \neq 0$ are integers. The additive inverse of such fractions are $-a/b$, and the multiplicative inverse is b/a for $a \neq 0$. It is clear that $\mathbb{Q}$ contains no divisors of zero, and so $\mathbb{Q}$ is a field.

In example 2.1.2 we stated that $\mathbb{Z}$ is subring of $\mathbb{Q}$, hence, by Theorem 2.2.1, $\mathbb{Z}$ is an integral domain. Also, we observe that

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

so $\mathbb{Q}$ is in fact the quotient field of $\mathbb{Z}$.

At this point we have already seen that $\mathbb{Z}$ is both a ring and an integral domain. Throughout this thesis we will show several more properties of $\mathbb{Z}$ as we go along. Also, we will see the consequences of extending $\mathbb{Z}$ with an element which is not part of the ring already. We will look at elements of the form $\sqrt{n}$, where $n \in \mathbb{Z}$, and obtain the set

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

$\mathbb{Z}[\sqrt{n}]$ is an integral domain, as it is a subset of $\mathbb{C}$, which is a field. Then, since $\mathbb{Z}[\sqrt{n}]$ is closed under subtraction and multiplication, and contains 1, it is a subring of $\mathbb{C}$, thus an integral domain by Theorem 2.2.1.

In order for $\sqrt{n}$ not to be in $\mathbb{Z}$ already, we consider n to be *squarefree*, meaning that in the prime factorization of n, no prime number occurs more than once. As an example of n *not* being squarefree, look at $n = 4 = 2 \cdot 2$. Then

$$\mathbb{Z}[\sqrt{4}] = \mathbb{Z}[2] = \mathbb{Z},$$

and we have not extended $\mathbb{Z}$ at all. Now, there are integers n that are *not* squarefree for which $\sqrt{n}$ is not in $\mathbb{Z}$, but in this case $\mathbb{Z}[\sqrt{n}]$ will always be a subring of a domain $\mathbb{Z}[\sqrt{m}]$ where m is a squarefree integer. For example, in the case where $n = 24$, which is not squarefree, we obtain

$$\mathbb{Z}[\sqrt{24}] = \mathbb{Z}[2\sqrt{6}] \subseteq \mathbb{Z}[\sqrt{6}],$$

and $m = 6$ is squarefree. Also, note that $\mathbb{Z}[\sqrt{n}]$ will not be an extension of $\mathbb{Z}$ in the case where $n = 1$, as

$$\mathbb{Z}[\sqrt{1}] = \mathbb{Z}[1] = \mathbb{Z}.$$

We now turn to a special class of subsets of rings, called *ideals*, which have the property of being closed under addition and multiplication by elements of the ring.

2.3 Ideals

Definition. A nonempty subset I of a ring R is called an *ideal* of R if

i) $a, b \in I$ implies $a - b \in I$.

ii) $a \in I$ and $r \in R$ imply $ra \in I$.

Actually, the definition above gives only a left ideal, but recalling that all rings stated here are commutative, all left (and right) ideals are two-sided. We state that every ring R has at least two ideals, namely the trivial ideals R and $\langle 0 \rangle$.

Definition. An ideal I of a ring R is called a *proper ideal* of R if $I \neq \langle 1 \rangle$.

This means that a proper ideal of a ring R is an ideal I such that $I \subsetneq R$, as $\langle 1 \rangle$ generates the whole ring.

Proposition 2.3.1. *If I is an ideal in a ring R, then $I = R$ if and only if $1 \in I$.*

Proof. Suppose $I = R$. Every ring R contains the identity element, hence $1 \in I$.
Now assume $1 \in I$, and let $r \in R$. As I is an ideal we have $1 \cdot r = r \in I$, hence $I = R$. $\square$

Example 2.3.2. Let $I \neq \langle 0 \rangle$ be an ideal of a field F, and let $a \in I$. Then $a \in F$. We know that $ra \in F$ for any $r \in F$. Since F is a field, a has an inverse a^{-1}, and so $a^{-1}a = 1 \in I$. With the identity element of F in I we must have that $I = F$, making $\langle 0 \rangle$ and F the only ideals of F.

To move on, we look at some additional examples of ideals.

Example 2.3.3. Let R be a ring and $r \in R$. Then $rR = (ra \mid a \in R)$ is the ideal of R generated by r. We then denote $\langle r \rangle$ to be the *principal ideal* of R generated by r.

Definition. A *principal ideal ring* is a ring R in which every ideal is principal.

Example 2.3.4. We want to show that $\mathbb{Z}$ is a principal ideal ring. Let I be an ideal of $\mathbb{Z}$. If $I = \{0\}$ then $I = \langle 0 \rangle$ is a principal ideal, so we assume $I \neq \{0\}$. Then we have an element $a \in I$, where $a \neq 0$. Since also $-a \in \mathbb{Z}$, we may suppose $a > 0$, and hence I has at least one positive integer. Now let n denote the least positive integer in I. By dividing a by n we can express a as

$$a = nq + r$$

for some $q, r \in \mathbb{Z}$, where $0 \leq r < n$. Since a and n are elements of the ideal I, so is $r = a - nq$. To avoid a contradiction with the fact that n is the least positive integer in I, we must have that $r = 0$, making $a = nq$. Hence $I = \langle n \rangle = n\mathbb{Z}$. This shows that every ideal in $\mathbb{Z}$ is principal, making $\mathbb{Z}$ is a principal ideal ring.

In chapter 4 we will revisit the above example, and see that $\mathbb{Z}$ is an example of what we call a principal ideal domain. The next section of this chapter, we dedicate to prime ideals, which play a central role in this thesis.

2.4 Prime ideals

Definition. An ideal $P \subsetneq R$ of a ring R is called a *prime ideal* if a, $b \in R$ and $ab \in P$ implies $a \in P$ or $b \in P$.

Example 2.4.1. For each prime integer p, the ideal $\langle p \rangle$ in $\mathbb{Z}$ is a prime ideal.

Actually, the above holds *only* for prime integers, and for each $n \in \mathbb{Z}$ not a prime integer, we can show that $\langle n \rangle$ is not a prime ideal.

Example 2.4.2. For $8\mathbb{Z}$ we have $2, 4 \in \mathbb{Z}$ and $2 \cdot 4 \in 8\mathbb{Z}$, but $2, 4 \notin 8\mathbb{Z}$, so $8\mathbb{Z}$ is a proper ideal of $\mathbb{Z}$, but not a prime ideal.

Going back to integral domains, it is now clear that $\langle 0 \rangle$ is a prime ideal in any integral domain D. In fact, if $\langle 0 \rangle$ is a prime ideal in a ring D, and we let a, $b \in D$ be elements such that $ab \in \langle 0 \rangle$, then either $a \in \langle 0 \rangle$ or $b \in \langle 0 \rangle$. Now $ab = 0$ which implies that $a = 0$ or $b = 0$, hence D is an integral domain. We end up with the equivalence:

$$\text{A ring } D \text{ is an integral domain } \iff \langle 0 \rangle \text{ is a prime ideal in } D.$$

Closely related to prime ideals we have maximal ideals.

Definition. A proper ideal M of a ring R is called a *maximal ideal* if for an ideal I of R such that $M \subseteq I \subseteq R$, either $I = M$ or $I = R$.

Now that we have defined both a prime ideal and a maximal ideal, we will move on with some results regarding the two.

Theorem 2.4.3. *Let I be an ideal of the ring R. Then we have that*

$$R/I \text{ is a field} \iff I \text{ is maximal.}$$

Proof. Suppose R/I is a field and that J is an ideal of R with

$$I \subsetneq J \subseteq R.$$

Thus there exists $b \in J$ such that $b \notin I$. Then $b + I$ is a nonzero element of R/I and therefore, as R/I is a field, there exists an element $c + I \in R/I$ such that

$$(b + I)(c + I) = bc + I = 1 + I,$$

and so

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

Since $b \in J$ and $c \in R$ we have

$$bc \in J.$$

Hence

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

so that $J = \langle 1 \rangle = R$. Thus I is a maximal ideal. Conversely, let I be a maximal ideal, and assume R/I is not a field. Then there exists an element $r + I \in R/I$ not a unit, hence $1 + I \notin \langle r \rangle + I$, which implies $\langle r \rangle \subsetneq R$. Since $r + I \neq 0 + I$, $r \notin I$ and then

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

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

For our next result we need to define *prime elements*. We are familiar with the fact that a prime number can not be factorized into a product of two integers other than itself and 1. More generally, for a prime p where $p = ab$, a or b must be a unit. In $\mathbb{Z}$ the only units are ± 1, and the prime elements are exactly the prime numbers. There is a second property of prime elements though, stating that if $p|ab$, then either $p|a$ or $p|b$. These two properties of a prime element are equivalent in $\mathbb{Z}$, but not in general. However, the second one can be shown to always imply the first one, and so we define prime elements as follows.

Definition. A nonzero element $p \in R$ is a *prime* in the ring R if p is not a unit, and if $p|ab$ for some $a, b \in R$, then either $p|a$ or $p|b$.

Theorem 2.4.4. *Let R be a ring. Let $p \in R$ be such that $p \neq 0$ and not a unit. Then*

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

Proof. Let $\langle p \rangle$ be a prime ideal of R, and let $a, b \in R$ be such that $p|ab$, i.e. $ab \in \langle p \rangle$. As $\langle p \rangle$ is a prime ideal, $a \in \langle p \rangle$ or $b \in \langle p \rangle$, leading to $p|a$ or $p|b$. Hence p is prime in R.

Conversely, assume that p is a prime in R, and let $a \in R$ and $b \in R$ such that $ab \in \langle p \rangle$. Then there exists $c \in R$ such that $ab = pc$, and then $p|ac$. Since p is a prime we have that $p|a$ or $p|b$. Suppose now $p|a$. Then there exists $d \in R$ such that $a = pd$ and so $a \in \langle p \rangle$, hence $\langle p \rangle$ is a prime ideal. In the same way, if $p|b$ there exists an element $e \in R$ such that $b = pe$, and so $b \in \langle p \rangle$, making $\langle p \rangle$ a prime ideal in this case as well. □

Theorem 2.4.5. *For a ring R and an ideal I of R we have that*

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

Proof. Assume R/I to be an integral domain. Let $a, b \in R$ such that $ab \in I$. Then

$$(a + I)(b + I) = ab + I = 0 + I$$

is the zero element of R/I. Since an integral domain has no zero divisors, we must have $a + I = 0 + I$ or $b + I = 0 + I$. This means that $a \in I$ or $b \in I$, so I is a prime ideal.

Conversely, suppose that I is a prime ideal of R. As I then is a proper ideal of R, R/I is a ring with identity $1 + I$. Now let $a + I \in R/I$ and $b + I \in R/I$ such that

$$(a + I)(b + I) = 0 + I.$$

Then $ab+I = I$ so that $ab \in I$. Since I is prime either $a \in I$ or $b \in I$, that is, $a+I = 0+I$ or $b + I = 0 + I$, hence R/I has no zero divisors, and so R/I is an integral domain. □

Theorem 2.4.6. *For a ring R a maximal ideal I is also a prime ideal.*

Proof. For I a maximal ideal of R, we have by Theorem 2.4.3 that R/I is a field, which is always an integral domain. By Theorem 2.4.5 I is then also a prime ideal of R. □

Before giving two additional results, we define multiplication of ideals.

Definition. Let I and J be ideals in a ring R. Then the *product of I and J*, denoted IJ is defined by

$$IJ = \{x \in R \mid x = i_1 j_1 + \cdots + i_r j_r \text{ for some } r \in \mathbb{N}, \\ \text{some } i_1, ..., i_r \in I, \text{ and some } j_1, ..., j_r \in J\}.$$

If $I = \langle i \rangle$ and $J = \langle j \rangle$ are principal ideals, then $IJ = \langle ij \rangle$. In addition, we state the following properties for ideals I, J and K of a ring R:

1. IJ is itself an ideal of R.
2. $IJ = JI$.
3. $(IJ)K = I(JK)$.
4. $I\langle 0 \rangle = \langle 0 \rangle$.
5. $I\langle 1 \rangle = I$.

We end this chapter with our two last results concerning prime ideals.

Theorem 2.4.7. *Let P be a proper ideal of a ring R. Then we have that*

$$P \text{ is prime} \iff \text{for ideals } A,B \text{ of } R \text{ satisfying } AB \subseteq P, \text{ either } A \subseteq P \text{ or } B \subseteq P.$$

Proof. Assume P to be a proper ideal of R meeting the requirement of ideals A, B of R

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

Let a, $b \in R$ such that $ab \in P$. Now let $A = \langle a \rangle$ and $B = \langle b \rangle$, making $AB = \langle ab \rangle \subseteq P$. From here we obtain that $\langle a \rangle \subseteq P$ or $\langle b \rangle \subseteq P$, and so $a \in P$ or $b \in P$, making P a prime ideal. For the converse, let P not meet the requirement above. Then there exist ideals A and B of R, such that $A \nsubseteq P$, $B \nsubseteq P$ and $AB \subseteq P$. Next, let $a \in A$, $a \notin P$ and $b \in B$, $b \notin P$. Then $ab \in AB \subseteq P$, but $a \notin P$, $b \notin P$, so P is not a prime ideal, and this completes the proof. □

Theorem 2.4.8. *Let D and E be rings where $D \subseteq E$. Let P be a prime ideal of E. Then $P \cap D$ is a prime ideal of D.*

Proof. First we must verify that $P \cap D$ is in fact an ideal of D. For elements $a, b \in P \cap D$ we have $a, b \in P$ and $a, b \in D$. Now, since P is an ideal, $a + b \in P$ and $a + b \in D$. Hence $a + b \in P \cap D$. Now let $a \in P \cap D$ and $d \in D$. Then, since P is an ideal of E, $a \in P$ and $d \in D$, $da \in P$, and as $a \in D$ and $d \in D$, $da \in D$ as well, since D is closed under multiplication. Hence $da \in P \cap D$, and $P \cap D$ is an ideal of D.

Now it only remains to show that $P \cap D$ is a prime ideal. Let $a, b \in D$ and $ab \in P \cap D$. Then $a, b \in E$ and $ab \in P$. Since P is a prime ideal of E, $a \in P$ or $b \in P$, showing that $P \cap D$ is a prime ideal, and thus completing the proof. □

Chapter 3

Noetherian domains

In this chapter we will define *Noetherian domains*, which will reappear in our definition of a Dedekind domain in the final chapter. We start by defining modules, and see how they give rise to Noetherian rings.

3.1 Modules

Definition. Let R be a ring, M an additive abelian group and $(r, m) \mapsto rm$ a mapping of $R \times M \mapsto M$ such that

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) $1m = m$,

for all $r, r_1, r_2 \in R$ and $m, m_1, m_2 \in M$. Then M is called a left R-*module*.

Again, considering only commutative rings saves us the trouble of distinguishing between left and right, and we consider a left and right R-module to be the same thing, simply denoting them R-modules.

Example 3.1.1. A ring R becomes itself an R-module by defining am for $a, m \in R$ to be the product of a and m as elements of the ring R.

Definition. For a ring R and an R-module M, a subgroup N of M is called a *submodule* of M if $rn \in N$ for all $r \in R$ and $n \in N$.

Example 3.1.2. If, like in the previous example, the ring R is considered an R-module, the submodules of R are the ideals of R.

Before moving on to Noetherian and Artinian modules, we define a *finitely generated module*.

Definition. An R-module M is *finitely generated* if M is generated by some finite set of elements of M.

This means that in order to be a finitely generated R-module, M need to have finitely many elements $x_1, ..., x_n \in M$ such that each $x \in M$ can be expressed as $\sum_{i=1}^{n} r_i x_i$ with coefficients $r_i \in R$.

3.2 Noetherian and Artinian rings

In order to avoid giving basically the same definition twice, we define a Noetherian and an Artinian module simultaneously, presenting the conditions of an Artinian module in brackets, as our main concern will be the Noetherian case.

Definition. An R-module is called *Noetherian* (*Artinian*) if for every ascending (descending) chain of submodules of M,

$$M_1 \subseteq M_2 \subseteq M_3 \subseteq \cdots \qquad (M_1 \supseteq M_2 \supseteq M_3 \supseteq \cdots)$$

there exists a positive integer k such that $M_k = M_{k+1} = M_{k+2} = \cdots$.

Example 3.2.1. We have shown that in the ring $\mathbb{Z}$ every ideal is principal, making any ascending chain of ideals of $\mathbb{Z}$ of the form

$$\langle n_1 \rangle \subseteq \langle n_2 \rangle \subseteq \langle n_3 \rangle \subseteq \cdots$$

for $n_1, n_2, n_3, ... \in \mathbb{Z}$. Since $\langle n_i \rangle \subseteq \langle n_{i+1} \rangle$ implies $n_{i+1} | n_i$, any ascending chain of ideals in $\mathbb{Z}$ starting with n_1 will have a finite number of distinct terms, making $\mathbb{Z}$ as a $\mathbb{Z}$-module Noetherian. On the other hand, the descending chain

$$\langle n \rangle \supseteq \langle n^2 \rangle \supseteq \langle n^3 \rangle \supseteq \cdots$$

is infinite, showing that $\mathbb{Z}$ as a $\mathbb{Z}$-module is *not* Artinian.

Definition. A ring R is a *Noetherian (Artinian)* ring if R regarded as an R-module is Noetherian (Artinian).

Now that we have defined what it means for both a module and a ring to be Noetherian (Artinian), we will present one of the main results for Noetherian (Artinian) modules with a proof for the Noetherian case, and then rewrite the result for Noetherian (Artinian) rings.

Theorem 3.2.2. *For M an R-module, the following are equivalent:*

i) M is Noetherian (Artinian).

ii) Every submodule (quotient module) of M is finitely generated (cogenerated).

iii) Every nonempty set S of submodules of M has a maximal (minimal) element.

Proof. $(i) \implies (ii)$: Let M be a Noetherian module and N a submodule of M, where N is assumed not to be finitely generated. For a positive integer k let $n_1, ..., n_k \in N$. Then $(n_1, ..., n_k) \neq N$, and we choose $n_{k+1} \in N$ such that $n_{k+1} \notin (n_1, ..., n_k)$. This gives an infinite ascending chain of submodules of M

$$(n_1) \subsetneq (n_1, n_2) \subsetneq \cdots \subsetneq (n_1, ..., n_k) \subsetneq (n_1, ..., n_{k+1}) \subsetneq \cdots,$$

contradicting with M being Noetherian. Hence N is finitely generated.

$(ii) \implies (iii)$: Let M be an R-module where every submodule is finitely generated, and let S be a nonempty set of submodules of M. Then, if an element $N_1 \in S$ is not maximal, it is contained in another submodule $N_2 \in S$. If S has no maximal elements, we obtain an infinite ascending chain of submodules

$$N_1 \subsetneq N_2 \subsetneq \cdots$$

of M. Let $N = N_1 \cup N_2 \cup \cdots$, and let $x, y \in N$ and $r \in R$. Then $x \in N_i$ and $y \in N_j$ for $i, j \in \{1, 2, ...\}$ and $i \neq j$. Now, since either $N_i \subseteq N_j$ or $N_j \subseteq N_i$, both x and y lie in N_i or N_j, hence $x - y$ and rx lie in the same submodule. This again implies $x - y \in N$ and $rx \in N$, making N a submodule of M. From (ii) N is finitely generated, i.e. there exist elements $a_1, a_2, ..., a_n \in N$ such that $N = (a_1, a_2, ..., a_n)$. There exists a submodule N_k such that all $a_l \in N_k$ for $l = 1, 2, ..., n$. Since $N_k \subseteq N$ and N is the smallest submodule containing all a_l, we must have that $N_k = N$. Then $N_k = N_{k+1} = \cdots$, contradicting with S not having a maximal element, hence S has a maximal element.

$(iii) \implies (i)$: Assume we have an ascending chain of submodules of M

$$M_1 \subseteq M_2 \subseteq M_3 \subseteq \cdots.$$

By (iii) this chain has a maximal element M_k, implying $M_k = M_{k+1} = \cdots$. Hence M is Noetherian. □

Theorem 3.2.3. *Let R be a ring. Then the following are equivalent:*

i) R is Noetherian (Artinian).

ii) For I an ideal of R, we have that I (R/I) is finitely generated (cogenerated).

iii) Every nonempty set S of ideals of R has a maximal (minimal) element.

We see that Noetherian (Artinian) rings provides us with the useful property that every set of ideals of the ring has a maximal (minimal) element. The same holds for Noetherian (Artinian) modules and the set of their submodules, as we just proved. Obviously it is desirable to be able to determine whenever a ring or a module is Noetherian (Artinian). From [1, section 19.2] we make the following remarks.

Remark. 1. If R is an Artinian ring it is also Noetherian.

2. Every principal ideal ring is a Noetherian ring.

Theorem 3.2.4. *Every submodule of a Noetherian (Artinian) module is Noetherian (Artinian).*

Proof. The result follows immediately from Theorem 3.2.2. □

Example 3.2.5. Consider $\mathbb{Q}$. In example 2.2.2 we saw that $\mathbb{Q}$ is a field, and so by example 2.3.2 the only ideals of $\mathbb{Q}$ are $\langle 0 \rangle$ and $\mathbb{Q}$ itself. Clearly the chain $\mathbb{Q} \supseteq \langle 0 \rangle$ has a minimal element, and so $\mathbb{Q}$ is Artinian. Then we know that $\mathbb{Q}$ is also Noetherian.

Now look at $\mathbb{Z}$ which is a subring of $\mathbb{Q}$, as we have seen earlier. In example 3.2.1 we saw that $\mathbb{Z}$ as a $\mathbb{Z}$-module is Noetherian, but not Artinian. Then, from the definition of an Artinian ring we can conclude that $\mathbb{Z}$ is *not* an Artinian ring, even though it is a subring of an Artinian ring.

We finish this chapter by defining Noetherian domains.

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

Example 3.2.6. We have shown earlier that $\mathbb{Z}$ is an integral domain, and that it is Noetherian. Hence $\mathbb{Z}$ is a Noetherian domain.

In the following chapter we will define three more domains, namely Euclidean domains, principal ideal domains, and unique factorization domains.

Chapter 4

Euclidean domains, PIDs and UFDs

4.1 Norms

Leading up to defining Euclidean domains, principal ideal domains and unique factorization domains, we start by defining the norm of elements in $\mathbb{Z}[\sqrt{n}]$.

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

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

Notice that $\overline{x}$ represents the *conjugate* of x, and not the complex conjugate, as x is not a complex number when $n > 0$. Also, in the case where $b = 0$, we have $x \in \mathbb{Z}$, and the norm simply becomes $\mathcal{N}(x) = a^2$. If both $a = 0$ and $b = 0$, that is $x = 0$, we obviously obtain $\mathcal{N}(x) = 0$, but since n is a squarefree integer the implication goes the other way as well. For $\mathcal{N}(x) = 0$ we have

$$|a^2 - nb^2| = 0,$$

implying $a^2 = nb^2$. Since n is squarefree it factorizes into k distinct primes, that is $n = p_1 \cdots p_k$, where $p_i \neq p_j$ for $i \neq j$ and $i, j \in \{1, ..., k\}$. We write

$$a^2 = p_1 \cdots p_k \cdot b^2.$$

Now, if $b = 0$ we get $a = 0$ and so $x = 0$. Therefore, assume that $b \neq 0$. Then we may write

$$\frac{a^2}{b^2} = p_1 \cdots p_k,$$

which after taking the square root of each side yields

$$\frac{a}{b} = \sqrt{p_1 \cdots p_k}.$$

This however, is a contradiction as $a/b \in \mathbb{Q}$, but $\sqrt{p_1 \cdots p_k} \notin \mathbb{Q}$. Hence the only conclusion is that $a = b = 0$, making $x = 0$. This shows that

$$\mathcal{N}(x) = 0 \iff x = 0.$$

We will make use of the norm later, when we look at elements of $\mathbb{Z}[\sqrt{n}]$ being irreducible, but first we present two results regarding the norm.

Theorem 4.1.1. *For $x, y \in \mathbb{Z}[\sqrt{n}]$, where n is a squarefree integer, we have that*

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

Proof. Let $x = (a + b\sqrt{n})$ and $y = (c + d\sqrt{n})$, where $a, b, c, d \in \mathbb{Z}$. Then we obtain

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

so that

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

The norm then becomes

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

Now we look at the norm of x and y, and multiply them together.

$$\begin{aligned}\mathcal{N}(x) \cdot \mathcal{N}(y) &= |a^2 - nb^2| \cdot |c^2 - nd^2| \\ &= |(a^2 - nb^2)(c^2 - nd^2)| \\ &= |(ac)^2 - n(ad)^2 - n(bc)^2 + (nbd)^2|.\end{aligned}$$

We see that $\mathcal{N}(xy) = \mathcal{N}(x) \cdot \mathcal{N}(y)$. □

Theorem 4.1.2. *For $u \in \mathbb{Z}[\sqrt{n}]$, and n a squarefree integer, we have that*

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

Proof. Let $u = (a + b\sqrt{n}) \in \mathbb{Z}[\sqrt{n}]$ and assume u is a unit. Then u has an inverse $u^{-1} \in \mathbb{Z}[\sqrt{n}]$ such that $uu^{-1} = 1$. This means that $\mathcal{N}(1) = \mathcal{N}(uu^{-1})$, and we obtain $\mathcal{N}(uu^{-1}) = \mathcal{N}(u) \cdot \mathcal{N}(u^{-1})$ from Theorem 4.1.1. Now, since $\mathcal{N}(1) = 1^2 = 1$, also $\mathcal{N}(u) \cdot \mathcal{N}(u^{-1}) = 1$, which implies $\mathcal{N}(u) = \mathcal{N}(u^{-1}) = 1$, since they are both nonnegative integers. For the converse we assume that $\mathcal{N}(u) = 1$. Then

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

This implies that $(a + b\sqrt{n})(a - b\sqrt{n}) = \pm 1$, and so $\pm(a - b\sqrt{n})$ is the inverse of $u = (a + b\sqrt{n})$. Hence u is a unit. □

Example 4.1.3. Look at $\mathbb{Z}[\sqrt{10}]$ and consider the element $x = (19 + 6\sqrt{10})$. Then the norm becomes $\mathcal{N}(x) = |19^2 - 10 \cdot 6^2| = |361 - 360| = 1$, and we conclude that x is a unit in $\mathbb{Z}[\sqrt{10}]$.

Now we turn to our different types of domains, starting with Euclidean domains.

4.2 Euclidean domains

Definition. An integral domain E is called a *Euclidean domain* if there exists a function $\phi : E \to \mathbb{Z}$ such that:

i) for all $a, b \in E^* = E \setminus \{0\}$, we have $\phi(ab) \geq \phi(a)$, and

ii) for each pair of elements $a, b \in E$, $b \neq 0$, there exist $q, r \in E$ such that $a = bq + r$ and $\phi(r) < \phi(q)$.

The function ϕ in the the definition of a Euclidean domain is central. As ϕ satisfies the axioms in the definition, it is called the *Euclidean function*, but note that it is not part of the Euclidean domain itself. Actually, a single integral domain may be a Euclidean domain given several different Euclidean functions, but as we see, we only demand that there exists at least one. Next we present two examples.

Example 4.2.1. $\mathbb{Z}$ is a Euclidean domain for $\phi(a) = |a|$, where $a \in \mathbb{Z}$. It is clear that $\phi(ab) \geq \phi(a)$ when both a and b are nonzero integers. Also, for any two integers a and b where b is different from zero, it is known that the ordinary division algorithm yields integers q and r satisfying (ii) in the definition of a Euclidean domain.

Example 4.2.2. We want to show that $\mathbb{Z}[\sqrt{2}]$ is a Euclidean domain given the norm defined in the previous section,

$$\mathcal{N}(a + b\sqrt{2}) = |a^2 - 2b^2|.$$

Let $x, y \in \mathbb{Z}[\sqrt{2}]$, where $x = a_1 + b_1\sqrt{2}$ and $y = a_2 + b_2\sqrt{2} \neq 0$. Then, $y \neq 0$ implies $\mathcal{N}(y) \neq 0$, and so $1 \leq \mathcal{N}(y)$. Also

$$\mathcal{N}(x) \leq \mathcal{N}(x)\mathcal{N}(y) = \mathcal{N}(xy),$$

and so (i) is verified. Next we want to verify (ii). Note that in $\mathbb{Q}[\sqrt{2}]$ we have

$$\frac{x}{y} = c_1 + c_2\sqrt{2}$$

where

$$c_1 = \frac{a_1b_1 - 2a_2b_2}{b_1^2 - 2b_2^2}, \qquad c_2 = \frac{a_2b_1 - a_1b_2}{b_1^2 - 2b_2^2}.$$

Now let q_1 be the integer closest to c_1, and q_2 the integer closest to c_1, i.e. $|c_1 - q_1| \leq 1/2$ and $|c_2 - q_2| \leq 1/2$. Next, let $r = q_1 + q_2\sqrt{2}$. Certainly $r \in \mathbb{Z}[\sqrt{2}]$. Let

$$s = (c_1 - q_1) + (c_2 - q_2)\sqrt{2}.$$

Then we have

$$s = \frac{x}{y} - r$$

so that $sy = x - r$. Denote $sy = u$, and we obtain $x = ry + u$, as required of (ii) in the definition. We now need to show that $\mathcal{N}(u) < \mathcal{N}(y)$. Note that by the triangle inequality we have

$$\mathcal{N}(s) = |(c_1 - q_1)^2 - 2(c_2 - q_2)^2| \leq |(c_1 - q_1)^2| + |-2(c_2 - q_2)^2|.$$

Thus we have that

$$\mathcal{N}(s) \leq (c_1 - q_1)^2 + 2(c_2 - q_2)^2 \leq (1/2)^2 + 2(1/2)^2 = 3/4,$$

and in particular $\mathcal{N}(u) \leq \frac{3}{4}\mathcal{N}(y)$, making (ii) satisfied. Hence $\mathbb{Z}[\sqrt{2}]$ is a Euclidean domain with respect to the norm.

Next we look at principal ideal domains, or PIDs. We will also see the relation between Euclidean domains and PIDs, and later also unique factorization domains.

4.3 Principal ideal domains

In section 2.4 we looked at principal ideal rings. Now, similarly we will define a principal ideal domain, denoted PID, and present several results that the property of PIDs provides us.

Definition. An integral domain D is called a *principal ideal domain*, denoted *PID*, if every ideal in D is principal.

Now, recalling our definition of a Noetherian domain and how finitely generated ideals relates to Noetherian rings provides us with the following result.

Theorem 4.3.1. *Every PID is a Noetherian domain.*

Proof. Let D be a PID, making every ideal of D principal. Then every ideal is finitely generated, and so, by Theorem 3.2.3, D is Noetherian. □

Note that the converse of Theorem 4.3.1 is not true, as Noetherian domains may contain ideals generated by more than one element. Next, we look at an example of a PID.

Example 4.3.2. Recall that we in example 2.3.4 showed that in $\mathbb{Z}$, all ideals are of the form $n\mathbb{Z}$, which are all principal, making $\mathbb{Z}$ a principal ideal ring. In example 2.2.2 we concluded that $\mathbb{Z}$ is an integral domain. Hence $\mathbb{Z}$ is a PID.

We now revisit maximal and prime ideals, and state the following result.

Theorem 4.3.3. *For D a PID, and a proper ideal I of D, the following holds:*

$$I \text{ is a maximal ideal} \iff I \text{ is a prime ideal.}$$

Proof. The right implication is Theorem 2.4.6. Now for the left implication assume I is a prime ideal in D that is not maximal, meaning there exists an ideal J of D such that

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

Since I and J are both ideals of a PID, we have that $I = \langle a \rangle$ and $J = \langle b \rangle$, for $a, b \in D$ both nonzero. Since $\langle a \rangle \subsetneq \langle b \rangle$, there must exist an element $r \in D$ such that $rb = a \in I$. Now, from I being a prime ideal we must have that either $r \in I$ or $b \in I$. For $b \in I$ we obtain the chain

$$\langle b \rangle = J \subseteq I \subsetneq J$$

which does not hold, and we must have $r \in I$. Then $r = sa$ for some $s \in D$, hence $a = (sa)b = a(sb)$, and since $a \neq 0$, we get $sb = 1$. This makes b a unit, i.e.

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

contradicting $J \subsetneq D$ and so the assumption of I not being maximal. We conclude that I must be maximal. □

It is also possible to determine a PID by knowing a domain is Euclidean.

Theorem 4.3.4. *Every Euclidean domain is a PID.*

Proof. Let E be a Euclidean domain, and let I be an ideal in E. If $I = \{0\}$ then $I = \langle 0 \rangle$ and I is principal. Assume $I \neq \{0\}$. For all $a \in I$ we have that $1|a$, and so $\phi(a) \geq \phi(1)$. Then the set $S = \{\phi(a) \mid a \in I, a \neq 0\}$ is a nonempty set with $\phi(1)$ as a lower bound. Then there exists an element $b \in I$ such that $\phi(b)$ is the smallest element in this set. If $a \in I$, we have $a = qb + r$ for $q, r \in E$ and $\phi(r) < \phi(b)$. But $r = a - qb \in I$ and $\phi(r) \geq \phi(b)$ by the choice of b, so we must have $r = 0$, so $a \in \langle b \rangle$, hence $I = \langle b \rangle$. Every ideal is principal and so E is a PID. □

We dedicate the next and final section of this chapter to unique factorization domains, and we will see how these relate to our other types of domains.

4.4 Unique factorization domains

In a unique factorization domain, or UFD, elements can be factorized in a unique way. In order to define what we mean by unique factorization precisely, we start by looking at elements in a domain being irreducible.

Definition. For R a ring, a nonzero nonunit element $r \in R$ is *irreducible* if for $r = ab$ where $a, b \in R$, either a or b is a unit.

Theorem 4.4.1. *In an integral domain D, every prime element is irreducible.*

Proof. Let $p \in D$ be a prime element, and let $p = ab$, where $a, b \in D$. Now $ab = p \cdot 1$, and so $p|ab$. Since p is prime we must have that $p|a$ or $p|b$, i.e. $a/p \in D$ or $b/p \in D$. Since $1 = (a/p)b$ or $1 = a(b/p)$, we conclude that either a or b is a unit of D, making p an irreducible element of D. □

In a general ring, an element with the property of being irreducible is the equivalent of an integer in $\mathbb{Z}$ being prime. In the same way that every (nonzero nonunit) integer has a unique prime factorization, every (nonzero nonunit) element in a UFD has a unique factorization into irreducible elements.

Note that an element which is irreducible in one ring, may be reducible in another. It is therefore essential to specify in which ring the factorization of an element is to be carried out. Before giving the precise definition of a UFD, we take a closer look at irreducible elements.

Example 4.4.2. Look at the integral domain $\mathbb{Z}[\sqrt{-5}]$, where an element r is of the form

$$r = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}.$$

The norm is defined as earlier, that is

$$\mathcal{N}(r) = a^2 + 5b^2.$$

From the properties of the norm we get that the only units are $r = \pm 1$. Now consider the element $9 \in \mathbb{Z}[\sqrt{-5}]$, and look at the factorization

$$9 = (2 + \sqrt{-5})(2 - \sqrt{-5}).$$

We want to check that $(2 + \sqrt{-5})$ and $(2 - \sqrt{-5})$ are irreducible factors. To reach our objective, let $(2 + \sqrt{-5}) = rs$. Then we obtain

$$\mathcal{N}(2 + \sqrt{-5}) = \mathcal{N}(r)\mathcal{N}(s),$$

which gives $9 = \mathcal{N}(r)\mathcal{N}(s)$. Now we must have that $\mathcal{N}(r)$ or $\mathcal{N}(s)$, let us choose $\mathcal{N}(r)$, is equal to $1, 3$ or 9. For $\mathcal{N}(r) = 3$ we get

$$a^2 + 5b^2 = 3,$$

which is not solvable for integers a and b. This leaves us with the two situations where $\{\mathcal{N}(r) = 1, \mathcal{N}(s) = 9\}$ or $\{\mathcal{N}(r) = 9, \mathcal{N}(s) = 1\}$. In either case $(2 + \sqrt{-5})$ is a product of two elements where one of them is a unit, hence $(2 + \sqrt{-5})$ is irreducible. Doing the corresponding calculations for $(2 - \sqrt{-5})$ shows that it also is an irreducible factor.

While we for an integral domain showed that every prime element is also irreducible, we can prove the converse implication for a PID.

Theorem 4.4.3. *An irreducible element in a principal ideal domain is always prime.*

Proof. Let R be a PID, and consider $p \in R$ to be an irreducible element with $p|ab$, for $a, b \in R$. Look at $\langle p \rangle + \langle a \rangle$. This is an ideal in R, so there exists an element $c \in R$ with

$$\langle p \rangle + \langle a \rangle = \langle c \rangle.$$

Then $p \in \langle c \rangle$, i.e. $p = cd$ for some $d \in R$. Since p is irreducible, either c or d is a unit. If c is a unit, then $\langle c \rangle = R$, so

$$\langle p \rangle + \langle a \rangle = R.$$

Then, for some $x, y \in R$ we have that

$$1 = px + ay,$$

and so

$$b = pbx + aby.$$

Since $p|ab$, we get that $p|b$. Now, if d is a unit, since $p = cd$, we have $\langle p \rangle = \langle c \rangle$, so

$$\langle p \rangle + \langle a \rangle = \langle p \rangle.$$

Then $a \in \langle p \rangle$ and so $p|a$. We conclude that p is a prime element. □

Now we turn to unique factorization domains.

Definition. An integral domain R is called a *unique factorization domain* if the following hold:

i) For $a \in R \setminus \{0\}$ not a unit, $a = p_1 p_2 \cdots p_m$ for some irreducible elements $p_i \in R$.

ii) If $p_1, ..., p_m$ and $q_1, ..., q_n$ are irreducible elements in R and $p_1 p_2 \cdots p_m = q_1 q_2 \cdots q_n$, then $m = n$ and for all $1 \leq i \leq n$ there exists a unit $u_i \in R$ with $p_i = u_i q_i$.

Remark. Elements of the form $p_i = u_i q_i$, as in the definition of a UFD, are called *associates*. These are elements that differ by multiplication of a unit. This means that since p_i and q_i are associates, denoted $p_i \sim q_i$, we have that $p_i | q_i$ and $q_i | p_i$. In a commutative integral domain the converse is also true.

What the definition tells us is, as mentioned before, that every nonzero nonunit element in a UFD factorizes *uniquely* into irreducible elements. With that in mind we revisit our previous example.

Example 4.4.4. We have seen that the element $9 \in \mathbb{Z}[\sqrt{-5}]$ factorizes into a product of irreducible factors, namely

$$9 = (2 + \sqrt{-5})(2 - \sqrt{-5}).$$

But we also have that $9 = 3 \cdot 3$. As before, we now let $3 = rs$, where $r, s \in \mathbb{Z}[\sqrt{-5}]$. We obtain

$$\mathcal{N}(3) = \mathcal{N}(r)\mathcal{N}(s),$$

which gives $9 = \mathcal{N}(r)\mathcal{N}(s)$, the same as in the previous example. Then we know that 3 is irreducible. This means that 9 can be factorized into two products of different irreducible factors, namely

$$9 = 3 \cdot 3 = (2 + \sqrt{-5})(2 - \sqrt{-5}).$$

Since the only units in $\mathbb{Z}[\sqrt{-5}]$ are 1 and -1, we deduce that the factors are not associates, and so the factorization from before is not unique. We conclude that $\mathbb{Z}[\sqrt{-5}]$ is *not* a UFD.

Before we eventually give an example of a ring that is in fact a UFD, we give a result connecting PIDs and UFDs.

Theorem 4.4.5. *Every principal ideal domain is a unique factorization domain.*

Proof. Let R be a a PID. Then we know from Theorem 4.3.1 that R is Noetherian, and so it does not have any infinite properly ascending chain of ideals. Now let $a \neq 0$ be an element of R that is not a unit. In order for R to be a UFD, a must factorize uniquely into a finite product of irreducible elements. Assume a is not irreducible, that is, it can be written as $a = a_1 b$ where neither a_1 nor b are units. Assume now that a_1 is not a product of irreducible elements, and that $a_1 = a_2 c$ where we let a_2 be a product of reducible elements. Repeating this process gives an ascending chain of ideals

$$\langle a \rangle \subsetneq \langle a_1 \rangle \subsetneq \langle a_2 \rangle \subsetneq \cdots$$

which in the case of a not being a finite product of irreducible elements will be infinite. But with R being Noetherian we deduce that the chain must be finite, hence a is a finite product of irreducible elements.

Next we need to show that this product is unique. Assume there exists a nonzero element $a \in R$ not a unit, that factorizes into two different products of irreducible elements. Suppose

$$a = p_1 p_2 \cdots p_m \text{ and } a = q_1 q_2 \cdots q_n$$

where p_i for $i = 1, ..., m$ and q_j for $j = 1, ..., n$ are all irreducible in R, and $n \geq m$. Then p_1 divides the product $q_1 \cdots q_n$. Since p_1 is irreducible it is also prime by Theorem 4.4.3, and so p_1 divides q_j for some j. Without loss of generality we may suppose $p_1 | q_1$. Then, since p_1 and q_1 are both irreducibles, $q_1 = u_1 p_1$ for some unit u_1 of R. Thus

$$p_1 p_2 \cdots p_m = u_1 p_1 q_2 \cdots q_n$$

and

$$p_2 \cdots p_m = u_1 q_2 \cdots q_n.$$

By continuing this process we reach

$$1 = u_1 u_2 \cdots u_m q_{m+1} \cdots q_n.$$

As q_j is not a unit for any j we have $m = n$, and $p_1, ..., p_m$ are associates of $q_1, ..., q_n$ in some order. This contradicts with the assumption that a has two different factorizations, and we may conclude that a factorizes into a finite and unique product of irreducible elements, making every PID a UFD, and thus the proof is complete. □

Next we give the relation between prime elements and irreducible elements in a UFD, just as we did for integral domains and PIDs.

Theorem 4.4.6. *For an element $p \in R$, where R is a UFD, we have that*

$$p \text{ is irreducible } \iff p \text{ is prime.}$$

Proof. The left implication follows from Theorem 4.4.1. For the right implication let $p \in R$ be an irreducible element and suppose $p | ab$ for $ab \in R$. Then there exists an element $c \in R$ such that $ab = pc$. Since R is a UFD, we have that

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

where $p_1 \cdots p_k$, $q_1 \cdots q_m$ and $r_1 \cdots r_n$ are irreducible elements of R, not necessarily distinct. We obtain

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

Now, since R is a UFD, p must be an associate of one of the p_i's or q_j's, implying that $p | a$ or $p | b$. Hence p is prime. □

For the final result of this section, we combine Theorem 4.3.4 and Theorem 4.4.5 to obtain the following Corollary.

Corollary 4.4.7. *Every Euclidean domain is a unique factorization domain.*

In light of this corollary, we summarize as follows for a ring R:

R Euclidean domain $\Rightarrow$ R principal ideal domain $\Rightarrow$ R unique factorization domain.

Or as inclusions:

$$\Big\{\text{Euclidean domains}\Big\} \subsetneq \Big\{\text{PIDs}\Big\} \subsetneq \Big\{\text{UFDs}\Big\}.$$

We note that the inclusions are proper, and look at an example.

Example 4.4.8. Let R be a polynomial ring over a field F in variables x and y, that is $R = F[x, y]$. As shown in [1, Theorem 4.3, page 222-223], R is then a UFD. Consider the ideal $I = \langle x\rangle + \langle y\rangle$ of R. I can not be of the form $\langle f(x, y)\rangle$ for any polynomial $f(x, y) \in R$ since

$$\langle x\rangle + \langle y\rangle = \langle f(x, y)\rangle \Rightarrow x = cf(x, y),\ y = df(x, y)$$

for some nonzero elements $c, d \in F$. This gives

$$\frac{x}{c} = \frac{y}{d},$$

and so $dx - cy = 0$, which can not be the case as x and y are independent variables over F. Hence $R = F[x, y]$ is not a PID. This stresses the fact that a UFD need not be a PID. Also, in [2] there are given several PIDs that are not Euclidean domains, for example $\mathbb{Z}[\sqrt{-19}]$.

We finish this chapter with two additional examples regarding UFDs.

Example 4.4.9. In section 4.2 we concluded that $\mathbb{Z}[\sqrt{2}]$ is a Euclidean domain. Then, by Corollary 4.4.7 it follows immediately that $\mathbb{Z}[\sqrt{2}]$ is also a UFD. We can emphasize this fact by taking associates into account. Look at the element $(8 - 3\sqrt{2}) \in \mathbb{Z}[\sqrt{2}]$. We may factorize it into two products as follows:

$$(8 - 3\sqrt{2}) = (5 + \sqrt{2})(2 - \sqrt{2}) = (11 - 7\sqrt{2})(2 + \sqrt{2}).$$

By the same procedure as in the previous examples in this section, we can use the norm to show that none of these four factors are units in $\mathbb{Z}[\sqrt{2}]$, and that all of them are irreducible. Then, as we know $\mathbb{Z}[\sqrt{2}]$ is a UFD, we must have that the two products differ only by a unit, in order to satisfy the second condition of the definition of a UFD. In other words, the factors have to be associates. Look at $u = (3 + 2\sqrt{2}) \in \mathbb{Z}[\sqrt{2}]$. We have that

$$\mathcal{N}(u) = 3^2 - 2 \cdot 2^2 = 1,$$

hence u is a unit of $\mathbb{Z}[\sqrt{2}]$. By using u we can verify that the factors are associates.

$$(2 - \sqrt{2})u = (2 + \sqrt{2}) \Rightarrow (2 - \sqrt{2}) \sim (2 + \sqrt{2}),$$

$$(11 - 7\sqrt{2})u = (5 + \sqrt{2}) \Rightarrow (11 - 7\sqrt{2}) \sim (5 + \sqrt{2}),$$

and so the conditions of a UFD are satisfied for $(8 - 3\sqrt{2})$.

Example 4.4.10. Consider the integral domain $\mathbb{Z}[\sqrt{-p}] = \{a + b\sqrt{-p} \mid a, b \in \mathbb{Z}\}$ where p is a prime number. Using the norm we can verify that its only units are 1 and -1, and that both elements $(1 + \sqrt{-p})$ and $(1 - \sqrt{-p})$ are irreducible in $\mathbb{Z}[\sqrt{-p}]$. We can now show that this domain is *not* a UFD when p is an odd prime number, that is $p > 2$. Look at the element $2 \in \mathbb{Z}[\sqrt{-p}]$. We can show that neither $(1 + \sqrt{-p})$ nor $(1 - \sqrt{-p})$ divides 2. Assume the contrary, that is $(1 + \sqrt{-p})|2$, which gives

$$2 = (a + b\sqrt{-p})(1 + \sqrt{-p}).$$

Calculating the norm on each side of the equation yields

$$4 = (a^2 + b^2 p)(1 + p).$$

By inspection we see that the only solutions to the last equation are $\{a = b = p = 1\}$, $\{a = 2, b = p = 0\}$ and $\{a = 1, b = 0, p = 3\}$. Both $p = 1$ and $p = 0$ contradicts with p being a prime number, and from the last solution we obtain

$$2 = 1 + \sqrt{-3}$$

which is not true. Hence $(1 + \sqrt{-p}) \nmid 2$. By the same procedure we conclude that $(1 - \sqrt{-p}) \nmid 2$. Now, the element $(1 + p) \in \mathbb{Z}[\sqrt{-p}]$ can be factorized into irreducible elements as

$$1 + p = (1 + \sqrt{-p})(1 - \sqrt{-p}),$$

and since p is an odd prime, $1 + p$ has to be even, i.e. $2|(p + 1)$. Then 2 is a factor of $(p + 1)$. As $(1 \pm \sqrt{-p}) \nmid 2$ they are not associates, and so $(1 + p)$ does not have a unique factorization, hence $\mathbb{Z}[\sqrt{-p}]$ is not a UFD when p is an odd prime.

Chapter 5

Algebraic number fields

In this chapter we will study algebraic number fields, focusing on the set of algebraic integers contained in these fields, and their properties. More specifically, we will look at the algebraic integers in a finite extension field of $\mathbb{Q}$. If we name this extension field K, the algebraic integers form a subring of K, which we will define as the ring of integers of K. To that end, we start by defining the term *integral over a domain*.

5.1 Integral elements

Definition. Let A and B be two integral domains such that $A \subseteq B$. Then the element $b \in B$ is *integral over* A if there are $a_i \in A$ and $n \geq 1$ such that

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

That is, b is a root of a monic polynomial with all its coefficients in A.

In the special case where $A = \mathbb{Z}$ and $B = \mathbb{C}$, making $b \in \mathbb{C}$ a complex number, b is called an *algebraic integer*. As a simple example of this case, let $b = \sqrt{2}$. As $\sqrt{2}$ is a solution to the equation $x^2 - 2 = 0$, which is monic and has both its coefficients in $\mathbb{Z}$, $\sqrt{2}$ is an algebraic integer. Leading up to the definition of algebraic number fields, we will later look at the case where A is assumed to be a field, making b not only integral over A, but also what we will call *algebraic over* A. For now, we focus on elements being integral over a domain, and prove the following results.

Theorem 5.1.1. *Let $A \subseteq B \subseteq C$ be a tower of integral domains. If $c \in C$ is integral over A then c is integral over B.*

Proof. Since $c \in C$ is integral over A there exists a polynomial

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

where $a_i \in A$ for $i = 0, 1, ..., n-1$. Now, since $A \subseteq B$ we have that $a_i \in B$, making c integral over B. □

Before our next theorem we note that $A[b]$ denotes the polynomial ring in b over A, that is, the set of polynomials of the form

$$a_n b^n + a_{b-1} b^{n-1} + \cdots + a_1 b + a_0$$

where $a_i \in A$ for $i = 0, ..., n$.

Theorem 5.1.2. *For integral domains A and B where $A \subseteq B$ and $b \in B$, we have that*

$$b \text{ is integral over } A \iff A[b] \text{ is a finitely generated } A\text{-module.}$$

Proof. Assume that b is integral over A. Then we have that

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

for $a_i \in A$ where $i = 0, 1, ..., n-1$. From here we obtain

$$\begin{aligned} b^n &= a_{n-1} b^{n-1} + a_{n-2} b^{n-2} + \cdots + a_1 b + a_0, \\ b^{n+1} &= a_{n-1} b^n + a_{n-2} b^{n-1} + \cdots + a_1 b^2 + a_0 b. \end{aligned}$$

Now,

$$b^n \in Ab^{n-1} + Ab^{n-2} + \cdots + Ab + A$$

while

$$b^{n+1} \in Ab^n + Ab^{n-1} + \cdots + Ab^2 + Ab \subseteq Ab^{n-1} + \cdots Ab + A.$$

From here we obtain by induction on n, that for all integers $k \geq 0$ we have

$$b^k \in Ab^{n-1} + \cdots + Ab + A.$$

Hence $A[b]$ is a finitely generated A-module, as it is generated by $b^{n-1} + \cdots + b + 1$.

For the converse, assume that $A[b]$ is a finitely generated A-module. Then we have

$$A[b] = Au_1 + \cdots + Au_n$$

for $u_i \in A[b]$ where $i = 1, 2, ..., n$, which can not all be zero. We have that $bu_i \in A[b]$, implying that there exist $a_{ij} \in A$ such that

$$\begin{aligned} bu_1 &= a_{11} u_1 + \cdots + a_{1n} u_n, \\ &\vdots \\ bu_n &= a_{n1} u_1 + \cdots + a_{nn} u_n. \end{aligned}$$

We rewrite the equations and obtain for unknowns $x_1, ..., x_n$

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

Now, from linear algebra we know that this system of equations has a solution if and only if its coefficient matrix is not invertible, meaning its determinant is equal to zero, i.e.

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

By computation of the determinant we obtain an equation

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

for some $a_0, a_1, ..., a_{n-1} \in A$, making b integral over A. □

The proof of the next theorem follows the last one closely, and we abstain from showing all the details.

Theorem 5.1.3. *Let A and B be two integral domains such that $A \subseteq B$ and $b \in B$. If there exists an integral domain C such that*

$$A[b] \subseteq C \subseteq B$$

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

Proof. Since C is a finitely generated A-module we have that $C = Ac_1 + \cdots + Ac_n$ for $c_i \in C$ nonzero, where $i = 1, 2, ..., n$. We have $b \in A[b]$ and $A[b] \subseteq C$, which gives $b \in C$. Since C is an integral domain we have $bc_i \in C$. Then, for $a_{ij} \in A$ we obtain a linear system as the one in the proof of Theorem 5.1.2. Following the same procedure, computing the determinant of the coefficient matrix, we reach the conclusion that b is integral over A, making $A[b]$ a finitely generated A-module by Theorem 5.1.2. □

Theorem 5.1.4. *Let $A \subseteq B \subseteq C$ be a tower of integral domains. If B is a finitely generated A-module and C a finitely generated B-module, then C is a finitely generated A-module.*

Proof. By assumption we have that $B = Ab_1 + \cdots + Ab_m$ and $C = Bc_1 + \cdots + Bc_n$ for $b_i \in B$ and $c_j \in C$ where $i = 1, ..., m$ and $j = 1, ..., n$. Let $c \in C$. Then we have

$$c = \sum_{j=1}^{n} x_j c_j$$

where $x_j \in B$. For $a_{ij} \in A$ we have

$$x_j = \sum_{i=1}^{m} a_{ij} b_i.$$

Combining the two sums yields

$$c = \sum_{j=1}^{n} \sum_{i=1}^{m} a_{ij} b_i c_j$$

making $C = Ab_1c_1 + \cdots + Ab_mc_n$ a finitely generated A-module. □

Theorem 5.1.5. *Let A and B be two integral domains such that $A \subseteq B$, and let $b_i \in B$ be integral over A for $i = 1, ..., n$. Then $A[b_1, ..., b_n]$ is a finitely generated $A - module$.*

Proof. We prove the statement by induction on n. First, if $b_1 \in B$ is integral over A then $A[b_1]$ is a finitely generated A-module by Theorem 5.1.2, and so the theorem is true for $n = 1$, completing the base case.

Next, assume that $A[b_1, ..., b_{n-1}]$ is a finitely generated A-module, where $b_i \in B$ is integral over A, and $i = 1, ..., n-1$ for $n \geq 2$. Also, let $b_n \in B$ be integral over A. Then, by Theorem 5.1.1, b_n is integral over $A[b_1, ..., b_{n-1}]$, and so by Theorem 5.1.2, we have that $(A[b_1, ..., b_{n-1}])[b_n] = A[b_1, ..., b_n]$ is a finitely generated A-module, which completes the inductive step, thus verifying the theorem by induction. □

There are not only elements that may have the property of being integral over a domain, but also domains themselves.

Definition. Let A and B be two integral domains such that $A \subseteq B$. Then, if every element $b \in B$ is integral over A, *B is integral over A.*

We go on by presenting a result combining both elements and domains being integral.

Theorem 5.1.6. *Let $A \subseteq B \subseteq C$ be a tower of integral domains. If B is integral over A and $c \in C$ is integral over B, then c is integral over A.*

Proof. Since $c \in C$ is integral over B, we have that

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

for $b_i \in B$, where $i = 0, ..., n-1$, thus c is integral over $A[b_0, ..., b_{n-1}]$. Now, since every $b_i \in B$ and B is integral over A, every b_i is also integral over A, and so $A[b_0, ..., b_{n-1}]$ is a finitely generated A-module by Theorem 5.1.5. By Theorem 5.1.2 and the fact that c is integral over $A[b_0, ..., b_{n-1}]$, we deduce that $(A[b_0, ..., b_{n-1}])[c] = A[b_0, ..., b_{n-1}, c]$ is a finitely generated A-module. Then finally, by Theorem 5.1.3 c is integral over A. □

Now we will circle back to the special case of the definition of integral elements where we let $A = \mathbb{Z}$ and $B = \mathbb{C}$.

Theorem 5.1.7. *Let A and B be integral domains such that $A \subseteq B$. If $b_1, b_2 \in B$ are integral over A, then $b_1 + b_2$, $b_1 - b_2$ and $b_1 b_2$ are also integral over A.*

Proof. Since b_1 is integral over A we have by Theorem 5.1.2 that $A[b_1]$ is a finitely generated A-module. We have $A \subseteq A[b_1] \subseteq B$, and since b_2 is integral over A we have by Theorem 5.1.1 that b_2 is integral over $A[b_1]$. Then $(A[b_1])[b_2] = A[b_1, b_2]$ is a finitely generated $A[b_1]$-module by Theorem 5.1.2, making $A[b_1, b_2]$ a finitely generated A-module by Theorem 5.1.4. Next, let x denote any one of the elements $b_1 + b_2$, $b_1 - b_2$, $b_1 b_2$. Hence $A \subseteq A[x] \subseteq A[b_1, b_2] \subseteq B$ where the integral domain $A[b_1, b_2]$ is a finitely generated A-module. Then, by Theorem 5.1.3, x is integral over A. □

This theorem allows us to conclude that in the situation where $A \subseteq B$, the set of all elements of B that are integral over A is a subdomain of B containing A. For $A = \mathbb{Z}$ and $B = \mathbb{C}$ we are left with the fact that *the set of all algebraic integers is an integral domain.*

5.2 Integral closure

As we just mentioned, in the situation $A \subseteq B$ where A and B are integral domains, the set of all elements in B that are integral over A is a subdomain of B containing A. We provide notation for this domain in the next definition.

Definition. Let A and B be two integral domains such that $A \subseteq B$. Then the *integral closure* of A in B, denoted A^B is the subdomain of B consisting of all elements of B that are integral over A.

Theorem 5.2.1. *For R a UFD let F be its field of quotients, that is $F = \mathrm{Quot}(R)$. Then for an element $f \in F$ we have that*

$$f \text{ is integral over } R \iff f \in R.$$

Proof. In the case where $f \in R$, f satisfies the equation $x - f = 0$ and so f is integral over R, proving the left implication.

For the converse, assume that $f \in F$ is integral over R, hence satisfying an equation

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

for $a_i \in R$ where $i = 0, ..., n-1$. Since $f \in F$ we write $f = rs^{-1}$ for $s \neq 0$ where $r, s \in R$ and $\gcd(r, s) = 1$. We insert the new expression for f in the equation above and obtain

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

Multiplying by s^n on both sides yields

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

We need to show that s is a unit in R. To that end, assume that s is not a unit. Then there exists an irreducible element $p \in R$ such that $p|s$. We have that

$$r^n = -a_{n-1}r^{n-1}s - \cdots - a_1 rs^{n-1} - a_0 s^n$$

where s is a factor in every term, and so we deduce that $p|r^n$. Since p is prime (by Theorem 4.4.6) $p|r$. This contradicts with the fact that $\gcd(r, s) = 1$, hence s is a unit in R and $f = rs^{-1} \in R$. □

In light of this theorem, we look at the situation where $R = \mathbb{Z}$. We know that $\mathbb{Z}$ is in fact a UFD, as we showed in example 4.2.1 that it is a Euclidean domain. In example 2.2.2 we concluded that $\mathrm{Quot}(\mathbb{Z}) = \mathbb{Q}$. Now, for the integral domains $\mathbb{Z}$ and $\mathbb{C}$, we get that $\mathbb{Z}^{\mathbb{C}}$ denotes the set of all algebraic integers. Then $\mathbb{Q} \cap \mathbb{Z}^{\mathbb{C}}$ denotes all rational algebraic integers. By our last theorem, an element a is in $\mathbb{Q} \cap \mathbb{Z}^{\mathbb{C}}$, i.e. a is integral over $\mathbb{Z}$, if and only if $a \in \mathbb{Z}$, making $\mathbb{Q} \cap \mathbb{Z}^{\mathbb{C}} = \mathbb{Z}$. In other words: *a rational algebraic integer must be an ordinary integer*.

To move on we look at the situation where the integral closure of an integral domain R, makes R *integrally closed*.

Definition. Let R be an integral domain. Then R is said to be *integrally closed* if for all elements $a \in \mathrm{Quot}(R)$ that are integral over R, we have $a \in R$.

We observe the connection between our last definition and Theorem 5.2.1, and conclude that *every UFD is integrally closed*.

Example 5.2.2. Consider the ring $\mathbb{Z}$. We have seen that $\mathbb{Z}$ is a UFD, hence $\mathbb{Z}$ is integrally closed.

As we know every PID is also a UFD we get the following corollary.

Corollary 5.2.3. *Every PID is integrally closed.*

Up till now we have defined what it means for an element in an integral domain to be integral over a domain, and to be an algebraic integer. In the upcoming section we will start by looking at elements being algebraic over a domain and algebraic numbers, leading up to the definition of an algebraic number field and its ring of integers.

5.3 The ring of integers

We have earlier considered integral domains A and B where $A \subseteq B$. Now, we will look at the case where A is not only an integral domain, but also a field.

Definition. Let A and B be two integral domains such that $A \subseteq B$. If A is a field and an element $b \in B$ is integral over A, then b is *algebraic over A*.

Just as we in the previous section obtained algebraic integers by looking at $\mathbb{Z}$ and $\mathbb{C}$, we know look at the situation where, in our definition, $A = \mathbb{Q}$ and $B = \mathbb{C}$. Then we name an element $b \in \mathbb{C}$ that is integral over the field $\mathbb{Q}$, an *algebraic number*. As $\mathbb{Z} \subseteq \mathbb{Q}$, an element $c \in \mathbb{C}$ that is integral over $\mathbb{Z}$, will also be integral over $\mathbb{Q}$ by Theorem 5.1.1. In other words: *every algebraic integer is an algebraic number*.

Theorem 5.3.1. *Every algebraic number b is of the form r/s where $r \in \mathbb{C}$ is an algebraic integer and $s \neq 0$ is an integer.*

Proof. Let b be an algebraic number. Then for $a_i \in \mathbb{Q}$ where $i = 0, ..., n-1$ we have

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

Let s be the least common multiple of the denominators a_i. Then $0 \neq s \in \mathbb{Z}$ and $sa_i \in \mathbb{Z}$. Now, multiplying the above equation by s^n yields

$$(sb)^n + (sa_{n-1})(sb)^{n-1} + \cdots + (s^{n-1}a_1)(sb) + (s^n a_0) = 0,$$

which is a monic polynomial with coefficients in $\mathbb{Z}$ and sb as a root. Hence sb is an algebraic integer which we denote r. Then $b = r/s$ where r is an algebraic integer and s is a nonzero integer. □

As we now know what it means for an element to be an algebraic number, we define an algebraic number field. Afterwards, we will look at what we call *the ring of integers of an algebraic number field*, and study it further.

Definition. An *algebraic number field* K is a subfield of $\mathbb{C}$ of the form $\mathbb{Q}(\alpha_1, ..., \alpha_n)$, where α_i for $i = 1, ..., n$, are algebraic numbers.

Example 5.3.2. $K = \mathbb{Q}(\sqrt{2})$ is an algebraic number field, as we have shown that $\sqrt{2}$ is an algebraic integer, hence an algebraic number.

We may also express an algebraic number field by saying that $K = \mathbb{Q}(\alpha_1, ..., \alpha_n)$ is the smallest subfield of $\mathbb{C}$ containing the whole of $\mathbb{Q}$ and all the elements $\alpha_1, ..., \alpha_n$. Now, in the case where $K = \mathbb{Q}(\alpha)$ and $\alpha \in \mathbb{C}$ is a root of an irreducible quadratic polynomial $x^2 + ax + b \in \mathbb{Q}[x]$, we name $\mathbb{Q}(\alpha)$ a *quadratic field*, or a *quadratic field extension* of $\mathbb{Q}$. We want to be able to determine these fields in a unique way.

Theorem 5.3.3. *If K is a quadratic field, then there exists a unique squarefree integer d such that $K = \mathbb{Q}(\sqrt{d})$.*

Proof. Let $K = \mathbb{Q}(\alpha)$ where α is a root of the irreducible polynomial $x^2 + ax + b \in \mathbb{Q}[x]$. Thus

$$\alpha = \frac{-a \pm \sqrt{a^2 - 4b}}{2}.$$

We may write, without loss of generality that

$$\alpha = \frac{-a + \sqrt{a^2 - 4b}}{2}$$

and so

$$K = \mathbb{Q}(\alpha) = \mathbb{Q}\left(\frac{-a + \sqrt{a^2 - 4b}}{2}\right) = \mathbb{Q}(\sqrt{c})$$

where $c = a^2 - 4b \in \mathbb{Q}$. Since $x^2 + ax + b$ is irreducible in $\mathbb{Q}[x]$, c is not the square of a rational number. Let $c = p/q$ where $p, q \in \mathbb{Z}$ are such that $q > 0$ and $\gcd(p, q) = 1$. Now for pq let m^2 be the biggest square such that $m^2 | pq$. Then we have that $pq = m^2 d$ for a squarefree integer $d \neq 1$. Furthermore

$$K = \mathbb{Q}(\sqrt{c}) = \mathbb{Q}\left(\sqrt{\frac{p}{q}}\right) = \mathbb{Q}(\sqrt{pq}) = \mathbb{Q}(\sqrt{m^2 d}) = \mathbb{Q}(m\sqrt{d}) = \mathbb{Q}(\sqrt{d}).$$

Let n be another squarefree integer such that $K = \mathbb{Q}(\sqrt{n})$. Then $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{n})$, and so

$$\sqrt{d} = x + y\sqrt{n}$$

for some $x, y \in \mathbb{Q}$. After squaring we obtain

$$d = x^2 + ny^2 + 2xy\sqrt{n}.$$

Assume $xy \neq 0$. Then

$$\sqrt{n} = \frac{d - x^2 - ny^2}{2xy}$$

which contradicts with $\sqrt{n} \notin \mathbb{Q}$ since n is chosen to be a squarefree integer. Hence $xy = 0$. For $y = 0$ we have $\sqrt{d} = x$, but as d is squarefree this contradicts with $\sqrt{d} \notin \mathbb{Q}$, and so we must have $x = 0$, making $\sqrt{d} = y\sqrt{n}$ and finally

$$d = y^2 n.$$

This implies $y^2 = 1$, as d is squarefree, and so $d = n$. This proves that d is uniquely determined by K. □

For any algebraic number field we may obtain the subset containing all its algebraic integers. We will define this subset for a general algebraic number field, and then determine it for the quadratic extensions of $\mathbb{Q}$.

Definition. For K an algebraic number field, the subset of all algebraic integers in K, denoted $\mathcal{O}_K$, is called *the ring of integers of the algebraic number field* K.

Note that since every element of $\mathcal{O}_K$ is an algebraic integer, $\mathcal{O}_K$ is integral over $\mathbb{Z}$. Also, in the case where $K = \mathbb{Q}$, we have that $\mathcal{O}_K = \mathbb{Z}$. Before giving several properties of the ring of integers for a general algebraic number field K, we look at the special case where K is a quadratic field.

Theorem 5.3.4. *Let $K = \mathbb{Q}(\sqrt{d})$ where d is a squarefree integer. Then $\mathcal{O}_K$ is given by*

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{d}] & \text{if } d \not\equiv 1 \pmod 4, \\ \mathbb{Z}\left[\frac{1}{2} + \frac{\sqrt{d}}{2}\right] & \text{if } d \equiv 1 \pmod 4. \end{cases}$$

Proof. Let α be an element of $\mathbb{Q}(\sqrt{d})$, which we then express as $\alpha = r + s\sqrt{d}$, where $r, s \in \mathbb{Q}$. Then we can write

$$\alpha = \frac{a + b\sqrt{d}}{c}$$

where $a, b, c \in \mathbb{Z}$, $c > 0$ and a, b, c have no common prime factor. Then $\alpha \in \mathcal{O}_K$ if and only if the coefficients of the minimal polynomial

$$\begin{aligned} \left(x - \frac{a + b\sqrt{d}}{c}\right)\left(x - \frac{a - b\sqrt{d}}{c}\right) &= x^2 - \frac{xa - xb\sqrt{d}}{c} - \frac{xa + xb\sqrt{d}}{c} + \frac{a^2 - b^2 d}{c^2} \\ &= x^2 - \frac{xa - xb\sqrt{d} + xa + xb\sqrt{d}}{c} + \frac{a^2 - b^2 d}{c^2} \\ &= x^2 - \frac{2a}{c}x + \frac{a^2 - b^2 d}{c^2} \end{aligned}$$

are integers, that is

$$\frac{a^2 - b^2 d}{c^2}, \frac{2a}{c} \in \mathbb{Z}.$$

Now, if a and c have a common prime factor p, then $(a^2 - b^2 d)/c^2 \in \mathbb{Z}$ implies that p divides b, as d is squarefree. This contradicts with the assumption that a, b, c have no common prime factor. Hence, since $2a/c \in \mathbb{Z}$, we must have $c = 1$ or $c = 2$. For $c = 1$, $\alpha \in \mathcal{O}_K$ independent of d. Consider $c = 2$. Then we must have $(a^2 - b^2 d)/4 \in \mathbb{Z}$, that is

$$a^2 - b^2 d \equiv 0 \pmod 4.$$

Also, in order for a, b, c to have no common prime factor, a and b must be odd, i.e. of the form $2n + 1$. As a, b are both squared, they are of the form

$$(2n + 1)^2 = 4n^2 + 4n + 1 \equiv 1 \pmod 4,$$

and so $a^2 \equiv 1 \pmod 4$ and $b^2 \equiv 1 \pmod 4$, leading to the conclusion that $d \equiv 1 \pmod 4$. Conversely, let $d \equiv 1 \pmod 4$. Then for odd a, b we have $(a^2 - b^2 d)/c^2 \in \mathbb{Z}$ and $(2a)/c \in \mathbb{Z}$ by the same argument, and so $\alpha \in \mathcal{O}_K$.

To sum up: if $d \not\equiv 1 \pmod 4$, then $c = 1$ and so $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$. If $d \equiv 1 \pmod 4$ we can also have $c = 2$ and a, b odd, and so $\mathcal{O}_K = \mathbb{Z}\left[\frac{1}{2} + \frac{\sqrt{d}}{2}\right]$. □

Example 5.3.5. Consider the quadratic fields $K_1 = \mathbb{Q}(\sqrt{13})$ and $K_2 = \mathbb{Q}(\sqrt{-1})$. We want to determine their ring of integers by using Theorem 5.3.4. Since $13 \equiv 1 \pmod 4$ we have

$$\mathcal{O}_{K_1} = \mathbb{Z}\left[\tfrac{1}{2} + \tfrac{\sqrt{13}}{2}\right].$$

As $-1 \not\equiv 1 \pmod 4$ we have

$$\mathcal{O}_{K_2} = \mathbb{Z}[\sqrt{-1}].$$

Actually, $\mathcal{O}_{K_2}$ and the ring of integers of $\mathbb{Q}(\sqrt{d})$ where $d = -2, -3, -7, -11$, are all Euclidean domains with respect to the norm, as proven in [3, Theorem 4.17].

For the remainder of this chapter, we will prove the properties of $\mathcal{O}_K$ that we will use in our next chapter, considering Dedekind domains.

Theorem 5.3.6. *For K an algebraic number field, $\mathcal{O}_K$ is an integral domain.*

Proof. As K is a field, and $\mathcal{O}_K \subseteq K$, we conclude that $\mathcal{O}_K$ is an integral domain. □

Theorem 5.3.7. *For K an algebraic number field we have that $\mathrm{Quot}(\mathcal{O}_K) = K$.*

Proof. For $F = \mathrm{Quot}(\mathcal{O}_K)$ and $\alpha \in F$ we have $\alpha = b/c$ where $b, c \in \mathcal{O}_K$ and $c \neq 0$. Since $\mathcal{O}_K \subseteq K$ we also have $b, c \in K$, and then $\alpha \in K$ as K is a field. Hence $F \subseteq K$. Next, let $\beta \in K$. By Theorem 5.3.1 we can write $\beta = r/s$ where r is an algebraic integer and s is a nonzero integer. Then $r = \beta s \in K$ and since r is an algebraic integer in K we have $r \in \mathcal{O}_K$. Hence $\beta = r/s \in F$ and so $K \subseteq F$. As we have also shown $F \subseteq K$ we conclude that $F = K$. □

Theorem 5.3.8. *For K an algebraic number field, $\mathcal{O}_K$ is integrally closed.*

Proof. Let K be an algebraic number field. By Theorem 5.3.7 we have $\mathrm{Quot}(\mathcal{O}_K) = K$. An element $\alpha \in K$ that is integral over $\mathcal{O}_K$, will also be integral over $\mathbb{Z}$ by Theorem 5.1.6, as $\mathcal{O}_K$ is integral over $\mathbb{Z}$. Then α is an algebraic integer in K, and so $\alpha \in \mathcal{O}_K$, making $\mathcal{O}_K$ integrally closed. □

Theorem 5.3.9. *For K an algebraic number field, $\mathcal{O}_K$ is a Noetherian domain.*

Proof. Let I be an ideal of $\mathcal{O}_K$. For $I = \{0\}$ we have that $I = \langle 0 \rangle$ is finitely generated. For $I \neq \{0\}$ we have that I is finitely generated by [4, Theorem 6.5.2]. Thus every ideal of $\mathbb{O}_K$ is finitely generated, and so, by Theorem 3.2.3, $\mathcal{O}_K$ is a Noetherian domain. □

Theorem 5.3.10. *Let K be an algebraic number field and P a nonzero prime ideal of $\mathcal{O}_K$. Then P is a maximal ideal of $\mathcal{O}_K$.*

Proof. We will prove this theorem by assuming the contrary of what it states, and find that the assumption does not hold. To that end, let K be an algebraic number field, and assume there exists a prime ideal P_1 of $\mathcal{O}_K$ that is not maximal. Define the set

$$S = \{I \text{ proper ideal of } \mathcal{O}_K | P_1 \subsetneq I\}$$

which is not empty as P_1 is not a maximal ideal. By Theorem 5.3.9 $\mathcal{O}_K$ is a Noetherian domain. Then, by Theorem 3.2.3, S contains a maximal element. This means that there exists a maximal ideal P_2 such that

$$P_1 \subsetneq P_2 \subsetneq \mathcal{O}_K.$$

By Theorem 2.4.6 P_2 is then also a prime ideal. As by [4, Theorem 6.1.7] every nonzero ideal in $\mathcal{O}_K$ contains a rational integer, we must have $P_1 \cap \mathbb{Z} \neq \{0\}$, and so $P_1 \cap \mathbb{Z}$ is a prime ideal of $\mathbb{Z}$ by Theorem 2.4.8. But we saw in example 4.3.2 that $\mathbb{Z}$ is a PID, meaning $P_1 \cap \mathbb{Z} = \langle p \rangle$ for some $p \in \mathbb{Z}$. This element p is prime by Theorem 2.4.4, and so we obtain

$$\langle p \rangle = P_1 \cap \mathbb{Z} \subseteq P_2 \cap \mathbb{Z} \subseteq \mathbb{Z}.$$

P_2 is a proper ideal of $\mathcal{O}_K$, and so $1 \notin P_2$, making $P_2 \cap \mathbb{Z} \neq \mathbb{Z}$. Also, $\langle p \rangle$ is a maximal ideal by Theorem 4.3.3, thus

$$\langle p \rangle = P_1 \cap \mathbb{Z} = P_2 \cap \mathbb{Z}.$$

Now, $P_1 \subsetneq P_2$, so there exists an element $b \in P_2$ that is not in P_1. Since $b \in \mathcal{O}_K$, b is an algebraic integer, and then integral over $\mathbb{Z}$. Thus we have that

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

for $a_i \in \mathbb{Z}$ where $i = 0, ..., n-1$, and so, since $0 \in P_1$

$$b^n + a_{n-1}b^{n-1} + \cdots + a_1 b + a_0 \in P_1.$$

Let k be the least positive integer for which there exist $c_i \in \mathbb{Z}$ where $i = 0, ..., k-1$, such that

$$b^k + c_{k-1}b^{k-1} + \cdots + c_1 b + c_0 \in P_1.$$

Since $b \in P_2$ we have that

$$b^k + c_{k-1}b^{k-1} + \cdots + c_1 b = b(b^{k-1} + c_{k-1}b^{k-2} + \cdots + c_1) \in P_2.$$

Now, as $P_1 \subsetneq P_2$ and P_2 is an ideal of $\mathcal{O}_K$

$$c_0 = (b^k + \cdots + c_1 b + c_0) - (b^k + \cdots + c_1 b) \in P_2,$$

but $c_0 \in \mathbb{Z}$, and so $c_0 \in P_2 \cap \mathbb{Z} = P_1 \cap \mathbb{Z}$, making c_0 an element of P_1. Then

$$b^k + c_{k-1}b^{k-1} + \cdots + c_1 b = (b^k + c_{k-1}b^{k-1} + \cdots + c_1 b + c_0) - c_0 \in P_1.$$

In the case where $k = 1$ we will have $b \in P_1$, clearly contradicting with $b \notin P_1$, so $k \geq 2$ and

$$b(b^{k-1} + \cdots + c_1) \in P_1.$$

Finally, since P_1 is a prime ideal and $b \notin P_1$, we must have

$$b^{k-1} + \cdots + c_1 \in P_1$$

which contradicts with k being the least positive integer, as $(k-1)$ is positive when $k \geq 2$. Hence the assumption of P_1 not being maximal does not hold, and we conclude that every prime ideal of $\mathcal{O}_K$ is maximal. $\square$

Chapter 6

Ideal factorization in Dedekind domains

We have arrived at the final chapter of this thesis. Here we will define a *Dedekind domain*, and at the end we will prove our main theorem.

6.1 Dedekind domains

Definition. An integral domain D is called a *Dedekind domain* if it satisfies the following conditions:

i) D is a Noetherian domain.

ii) D is integrally closed.

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

Throughout this thesis we have shown several properties of the domain $\mathbb{Z}$. It will also be our first example of a Dedekind domain.

Example 6.1.1. Consider the integral domain $\mathbb{Z}$. We check for the properties of a Dedekind domain.

i) $\mathbb{Z}$ is Noetherian by example 3.2.6.

ii) $\mathbb{Z}$ is integrally closed by example 5.2.2.

iii) $\mathbb{Z}$ is a PID by example 4.3.2, and so every nonzero prime ideal in $\mathbb{Z}$ is a maximal ideal by Theorem 4.3.3.

Hence $\mathbb{Z}$ is a Dedekind domain.

We now know that $\mathbb{Z}$ is both a principal ideal domain and a Dedekind domain. In fact, this is an example of a general rule.

Theorem 6.1.2. *Every PID is a Dedekind domain.*

Proof. Assume D to be a PID. Then by Theorem 4.3.1 D is Noetherian. D is integrally closed by Corollary 5.2.3, and finally, by Theorem 4.3.3 every nonzero prime ideal in D is a maximal ideal. Hence D is a Dedekind domain. □

We now turn to the ring of integers of an algebraic number field. As mentioned in the previous chapter, we will make use of the properties of $\mathcal{O}_K$ that we have already proven.

Theorem 6.1.3. *For K an algebraic number field, $\mathcal{O}_K$ is a Dedekind domain.*

Proof. Let K be an algebraic number field and $\mathcal{O}_K$ its ring of integers. Then we know that $\mathcal{O}_K$ is Noetherian by Theorem 5.3.9, integrally closed by Theorem 5.3.8 and that every nonzero prime ideal of $\mathcal{O}_K$ is a maximal ideal by Theorem 5.3.10. Hence $\mathcal{O}_K$ is a Dedekind domain. □

We have seen that the quadratic domain $\mathbb{Z}[\sqrt{n}]$ where n is a squarefree integer, is the ring of integers of the algebraic number field $K = \mathbb{Q}(\sqrt{n})$ when $n \not\equiv 1 \pmod 4$. Then, by our last theorem, we conclude that $\mathbb{Z}[\sqrt{n}]$ is a Dedekind domain when $n \not\equiv 1 \pmod 4$. For $n \equiv 1 \pmod 4$ however, we know that $\mathcal{O}_K \neq \mathbb{Z}[\sqrt{n}]$, so we can not as easily jump to any conclusions. Actually, in this case, $\mathbb{Z}[\sqrt{n}]$ is not a Dedekind domain.

Proposition 6.1.4. *If n is a squarefree integer such that $n \equiv 1 \pmod 4$, then $\mathbb{Z}[\sqrt{n}]$ is not a Dedekind domain.*

Proof. We want to show that $\mathbb{Z}[\sqrt{n}]$ is not integrally closed when n is a squarefree integer such that $n \equiv 1 \pmod 4$. For such values we may express n as $n = 4k + 1$ for $k \in \mathbb{Z}$. Let

$$\alpha = \left(\frac{1}{2} + \frac{\sqrt{n}}{2}\right) \in \mathrm{Quot}(\mathbb{Z}[\sqrt{n}]).$$

Then $\alpha \notin \mathbb{Z}[\sqrt{n}]$. Look at the polynomial

$$x^2 - x - k$$

which has all its coefficients in $\mathbb{Z}[\sqrt{n}]$. For $x = \alpha$ we obtain

$$\begin{aligned}
\alpha^2 - \alpha - k &= \left(\frac{1}{2} + \frac{\sqrt{n}}{2}\right)\left(\frac{1}{2} + \frac{\sqrt{n}}{2}\right) - \left(\frac{1}{2} + \frac{\sqrt{n}}{2}\right) - k \\
&= \frac{1}{4} + \frac{\sqrt{n}}{2} + \frac{n}{4} - \frac{1}{2} - \frac{\sqrt{n}}{2} - k \\
&= \frac{n-1}{4} - k.
\end{aligned}$$

And so, replacing n yields

$$\frac{(4k+1)-1}{4} - k = \frac{4k}{4} - k = k - k = 0.$$

This makes α integral over $\mathbb{Z}[\sqrt{n}]$, and so we have an integral element in the quotient field of $\mathbb{Z}[\sqrt{n}]$, not in $\mathbb{Z}[\sqrt{n}]$. Hence, when $n \equiv 1 \pmod 4$, $\mathbb{Z}[\sqrt{n}]$ is not integrally closed, thus not a Dedekind domain. Since every UFD is integrally closed, it is not a UFD either. □

In order to provide the proof of our main theorem, we must first consider ideals in Dedekind domains, and look at how they contain a product of prime ideals.

6.2 Ideals in Dedekind domains

We start with a theorem concerning Noetherian domains. As every Dedekind domain is also a Noetherian domain by definition, it follows immediately that the result also holds for Dedekind domains.

Theorem 6.2.1. *For a Noetherian domain D, every nonzero ideal $I \in D$ contains a product of one or more nonzero prime ideals.*

Proof. Let D be a Noetherian domain. Assume that there exists a nonzero ideal $I \in D$ that does not contain a product of one or more nonzero prime ideals. Denote the set containing all such ideals by S. Then S is nonempty, and since D is Noetherian S contains a maximal element by Theorem 3.2.3, say J. Now J is not a prime ideal, and so by Theorem 2.4.7 there exist ideals A and B such that

$$AB \subseteq J,\ A \nsubseteq J,\ B \nsubseteq J.$$

Next we define two ideals A_1 and B_1 as

$$A_1 = J + A,\ B_1 = J + B,$$

and so $J \subsetneq A_1$ and $J \subsetneq B_1$. Then $A_1 \notin S$ and $B_1 \notin S$, hence there exist nonzero prime ideals $P_1, ..., P_n$ such that

$$P_1 \cdots P_i \subseteq A_1,\ P_{i+1} \cdots P_n \subseteq B_1.$$

Then finally, as

$$A_1 B_1 = (J + A)(J + B) = JJ + JB + AJ + AB \subseteq J$$

we have that

$$(P_1 \cdots P_i)(P_{i+1} \cdots P_n) = P_1 \cdots P_n \subseteq A_1 B_1 \subseteq J,$$

contradicting with $J \in S$. This leads to the conclusion that every nonzero ideal in D contains a product of one or more nonzero prime ideals. □

As mentioned, this result provides us with the following corollary.

Corollary 6.2.2. *For a Dedekind domain D, every nonzero ideal $I \in D$ contains a product of one or more nonzero prime ideals.*

To move on, we define a *fractional ideal*, which we will use in our upcoming theorems.

Definition. Let D be an integral domain. A nonempty subset I of its quotient field $\mathrm{Quot}(D)$, is called a *fractional ideal* of D if it has the following properties:

i) $\alpha \in I, \beta \in I \Rightarrow \alpha + \beta \in I$.

ii) $\alpha \in I, r \in D \Rightarrow r\alpha \in I$.

iii) There exists a nonzero $\gamma \in D$ such that $\gamma I \subseteq D$.

Note that a fractional ideal of D that is a subset of D is an ideal just as we have defined it earlier. Also, any ideal of D is a fractional ideal.

Example 6.2.3. Consider $\mathbb{Z}$ and its quotient field $\mathrm{Quot}(\mathbb{Z}) = \mathbb{Q}$. Define the subset I of $\mathbb{Q}$ as

$$I = \Big\{ \frac{n}{15} \mid n \in \mathbb{Z} \Big\}.$$

Clearly I has property (i) and (ii) of a fractional ideal. Also, we see that $15I = \mathbb{Z}$, and so (iii) holds. We conclude that I is a fractional ideal of $\mathbb{Z}$.

Definition. Let D be an integral domain, and $K = \mathrm{Quot}(D)$. For a prime ideal P in D the set $\tilde{P}$ is defined as $\tilde{P} = \{\alpha \in K \mid \alpha P \subseteq D\}$.

Theorem 6.2.4. *For a prime ideal P of an integral domain D, the set $\tilde{P}$ is a fractional ideal of D.*

Proof. For $\alpha \in \tilde{P}$ and $\beta \in \tilde{P}$ we have $\alpha P \subseteq D$ and $\beta P \subseteq D$. Thus

$$(\alpha + \beta)P \subseteq \alpha P + \beta P \subseteq D,$$

and so $\alpha + \beta \in \tilde{P}$. For another element $r \in D$ we have that $\alpha P \subseteq D$, making $r\alpha P \subseteq D$, and so $r\alpha \in \tilde{P}$. Finally let $\gamma \in P$ be nonzero. Then $\alpha\gamma \in D$, hence $\gamma\tilde{P} \subseteq D$. Thus $\tilde{P}$ is a fractional ideal of D. □

The following theorem will be used in the proof of our main theorem, in the upcoming and final section of this thesis.

Theorem 6.2.5. *For a nonzero prime ideal P in a Dedekind domain D, we have that $P\tilde{P} = D$.*

Proof. The first step to proving this theorem is to show that $P\tilde{P} = D$ or $P\tilde{P} = P$. To that end, we start by observing that P and $\tilde{P}$ are both fractional ideals of D, making $P\tilde{P}$ a fractional ideal of D. Obviously $P\tilde{P} \subseteq D$, and so it is also an ideal of D in the ordinary sense. As P is a nonzero prime ideal and D is a Dedekind domain, P is a maximal ideal by definition. Now, since $1 \in \tilde{P}$ we have $P \subseteq P\tilde{P}$, hence $P\tilde{P} = D$ or $P\tilde{P} = P$.

The next step is to show that $D \subsetneq \tilde{P}$. For an element $\alpha \in D$ we have $\alpha P \subseteq D$, hence $\alpha \in \tilde{P}$, and so $D \subseteq \tilde{P}$. In order to prove that $D \subsetneq \tilde{P}$ we must have that $\tilde{P}$ contains an element γ of $\mathrm{Quot}(D)$ that is not in D. Let $\beta \in P$ be a nonzero element, and $\langle\beta\rangle$ the ideal generated by $\langle\beta\rangle$. Then by Corollary 6.2.2 we have that

$$P_1 \cdots P_n \subseteq \langle\beta\rangle$$

for nonzero prime ideals $P_1, ..., P_n$ where $n \geq 1$. Let n be the least positive integer for which this inclusion holds. Then, since

$$P_1 \cdots P_n \subseteq \langle\beta\rangle \subseteq P$$

and P is a prime ideal we have $P_i \subseteq P$ for some $i = 1, ..., n$. We may now assume that $P_1 \subseteq P$, but as D is a Dedekind domain we obtain $P_1 = P$, since P_1 is a maximal ideal. Next, assume that $n = 1$. Then

$$P = P_1 = \langle\beta\rangle.$$

The element β is defined to be nonzero, so we can define $\gamma = 1/\beta \in \mathrm{Quot}(D)$. Assume $\gamma \in D$, making β a unit in D and

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

contradicting with P being a prime ideal. Thus $\gamma \notin D$. Furthermore,

$$\gamma P = \frac{1}{\beta}\langle \beta \rangle = \langle 1 \rangle = D,$$

so $\gamma \in \tilde{P}$, that is $\gamma \in \tilde{P} \setminus D$ for $n = 1$. Suppose next that $n \geq 2$. By the minimality of n we have that

$$P_2 \cdots P_n \not\subseteq \langle \beta \rangle.$$

Thus there exists $\delta \in P_2 \cdots P_n$ such that $\delta \notin \langle \beta \rangle$. We may now express γ as $\gamma = \delta/\beta$ which lies in $\mathrm{Quot}(D)$, but $\gamma \notin D$ as $\delta \notin \langle \beta \rangle$. However, $\gamma \in \tilde{P}$ since

$$P\langle \delta \rangle = P_1\langle \delta \rangle \subseteq P_1 \cdots P_n \subseteq \langle \beta \rangle$$

and so

$$P\gamma = P\delta/\beta \subseteq D.$$

Then $\gamma \in \tilde{P} \setminus D$ for $n \geq 2$ as well. Hence $D \subsetneq \tilde{P}$.

The final step is to show that $P\tilde{P} = D$. As we have already shown that $P\tilde{P} = P$ or $P\tilde{P} = D$, we assume the contrary, that $P\tilde{P} = P$. For $\alpha, \beta \in \tilde{P}$ we have

$$\alpha P \subseteq P\tilde{P} = P$$

and

$$\beta P \subseteq P\tilde{P} = P$$

and

$$\alpha\beta P \subseteq \alpha P \subseteq P,$$

thus $\alpha\beta \in \tilde{P}$. This shows that $\tilde{P}$ is closed under multiplication, and so $\tilde{P}$ is an integral domain strictly containing D. Now, D is a Noetherian domain, hence all its ideals are finitely generated by Theorem 3.2.3. This makes $\tilde{P}$ a finitely generated fractional ideal of D, thus $\tilde{P}$ is a finitely generated D-module. Then, by Theorem 5.1.3, in the case where $B = C$, $\tilde{P}$ is integral over D. But as D is a Dedekind domain, it is integrally closed in its quotient field, and so we must have $\tilde{P} = D$. This contradicts with $D \subsetneq \tilde{P}$, hence $P\tilde{P} \neq P$, and we are left with the conclusion that $P\tilde{P} = D$. □

6.3 Unique factorization into prime ideals

Finally we are ready to prove our main theorem.

Theorem 6.3.1. *For a Dedekind domain D every proper nonzero ideal I is a product of nonzero prime ideals, and this factorization is unique in the sense that if*

$$P_1P_2\cdots P_n = Q_1Q_2\cdots Q_m,$$

where P_i and Q_j are nonzero prime ideals, then $n = m$, and after relabeling (if necessary)

$$P_i = Q_i,\ i = 1, 2, ..., n.$$

Proof. Let S denote the set of proper nonzero ideals of a Dedekind domain D that are not products of nonzero prime ideals. Assume that there exists a proper nonzero ideal $I \in D$ that is not a product of nonzero prime ideals. Then as $I \in S$, we have that S is nonempty by assumption. Since D is a Dedekind domain, it is also Noetherian, and so by Theorem 3.2.3 S has a maximal element, say I. By Corollary 6.2.2 I contains a product of one or more nonzero prime ideals, that is

$$P_1\cdots P_n \subseteq I$$

for nonzero prime ideals $P_1, ..., P_n \in D$. Let n be the smallest positive integer for which such a product exists, and assume first that $n = 1$. Then

$$P_1 \subseteq I \subseteq D.$$

Since D is a Dedekind domain and P_1 is a nonzero prime ideal, P_1 will also be a maximal ideal of D, and so $P_1 = I$. This contradicts with I not being a product of nonzero prime ideals, and so $n \neq 1$. Then we must have $n \geq 2$. By Theorem 6.2.5 we have $\tilde{P}_1P_1 = D$, and so

$$\tilde{P}_1P_1P_2\cdots P_n = DP_2\cdots P_n.$$

Then

$$\tilde{P}_1I \supseteq \tilde{P}_1P_1\cdots P_n = P_2\cdots P_n.$$

Now, as shown in the proof of Theorem 6.2.5, we have $D \subsetneq \tilde{P}_1$, and then $I \subseteq \tilde{P}_1I$. Suppose that $I = \tilde{P}_1I$. Then

$$P_2\cdots P_n \subseteq I,$$

contradicting with n being the smallest positive integer, since $n - 1 \geq 1$, and we are left with the conclusion that $I \subsetneq \tilde{P}_1I$. Since $\tilde{P}_1I$ is an ideal of D, by the fact that I is the maximal element in S, we have that for nonzero prime ideals $Q_2, ..., Q_m$,

$$\tilde{P}_1I = Q_2\cdots Q_m.$$

Hence

$$I = ID = I\tilde{P}_1P_1 = P_1Q_2\cdots Q_m$$

is a product of nonzero prime ideals, contradicting with the fact that $I \in S$ by assumption. Thus every proper nonzero ideal of D is a product of nonzero prime ideals.

Next, as we have proven that a factorization into a product of nonzero prime ideals always exists for a proper nonzero ideal in D, we want to show that this factorization is unique. To reach this objective, assume the contrary, that the factorization is not always unique. Let S^* denote the set of all proper nonzero ideals of D that has at least two distinct factorizations into products of nonzero prime ideals. Assume that there exists a proper nonzero ideal $J \in D$ with two distinct factorizations into nonzero prime ideals, that is

$$J = P_1 \cdots P_n = Q_1 \cdots Q_m$$

for nonzero prime ideals P_i and Q_j, where $i = 1, ..., n$, $j = 1, ..., m$, and n is the smallest positive integer for which such a factorization exists. Then $J \in S^*$, and so S^* is nonempty. Since D is Noetherian, S^* has a maximal element by Theorem 3.2.3, say J. Now, as Q_1 is an ideal of D we have that $Q_1 D = Q_1$, and as $Q_2 \cdots Q_m \subseteq D$, we obtain $Q_1(Q_2 \cdots Q_m) \subseteq Q_1$. We deduce that

$$P_1 \cdots P_n \subseteq Q_1.$$

Then, since Q_1 is a prime ideal, we apply Theorem 2.4.7 and obtain $P_i \subseteq Q_1$, which after relabeling allows us to suppose that $P_1 \subseteq Q_1$. P_1 is prime and nonzero, and as D is a Dedekind domain, P_1 is a maximal ideal, hence $P_1 = Q_1$. From here we obtain

$$J\tilde{P_1} = \tilde{P_1} P_1 P_2 \cdots P_n = P_2 \cdots P_n$$

and

$$J\tilde{P_1} = J\tilde{Q_1} = \tilde{Q_1} Q_1 \cdots Q_m = Q_2 \cdots Q_m.$$

That is

$$P_2 \cdots P_n = Q_2 \cdots Q_m.$$

In the case where $J\tilde{P_1} = J$ we have $J\tilde{P_1}P_1 = JP_1$, and so $J = JP_1$. Next we define the fractional ideal $\tilde{J}$ of J as

$$\tilde{J} = \tilde{P_1} \cdots \tilde{P_n},$$

and so

$$J\tilde{J} = P_1 \cdots P_n \tilde{P_1} \cdots \tilde{P_n} = P_1 \tilde{P_1} \cdots P_n \tilde{P_n} = D,$$

from where we deduce that

$$D = J\tilde{P_1}\tilde{J} = P_1.$$

But P_1 is a prime ideal, and so $P_1 \neq D$, hence $J\tilde{P_1} \neq J$. Then, since $D \subsetneq \tilde{P_1}$, we have $J \subsetneq J\tilde{P_1}$. As $J\tilde{P_1}$ is an ideal of D strictly containing J, and J is the maximal element of S^*, we have that $J\tilde{P_1}$ has exactly one factorization into a product of nonzero prime ideals. Then, since $P_2 \cdots P_n = Q_2 \cdots Q_m$, we must have $n = m$, and after relabeling $P_i = Q_i$ for $i = 2, ..., n$. In other words the two factorizations of J are the same, contradicting with our assumption. We conclude that the factorization of an ideal into nonzero prime ideals is always unique, which completes the proof. □

Now as our main theorem has been proved, we end this thesis with an example.

Example 6.3.2. Consider the algebraic number field $K = \mathbb{Q}(\sqrt{-5})$. Since

$$-5 \not\equiv 1 \pmod 4,$$

we have by Theorem 5.3.4 that its ring of integers is $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$. Then we have by Theorem 6.1.3 that $\mathbb{Z}[\sqrt{-5}]$ is a Dedekind domain, and so every proper nonzero ideal in $\mathbb{Z}[\sqrt{-5}]$ has a unique factorization into a product of nonzero prime ideals. However, in example 4.4.4 we showed that $\mathbb{Z}[\sqrt{-5}]$ is not a UFD, from the fact that

$$9 = 3 \cdot 3 = (2 + \sqrt{-5})(2 - \sqrt{-5}),$$

where 3, $(2 + \sqrt{-5})$ and $(2 - \sqrt{-5})$ are all irreducibles and nonassociates in $\mathbb{Z}[\sqrt{-5}]$. Now we want to restore unique factorization by using prime ideals. Let

$$P_1 = \langle 3, 2 + \sqrt{-5} \rangle,$$
$$P_2 = \langle 3, 2 - \sqrt{-5} \rangle.$$

By the notion of the norm of an ideal and [4, Theorem 7.1.5 and Theorem 10.1.6], it can be shown that these two are distinct prime ideals in $\mathbb{Z}[\sqrt{-5}]$. We calculate the following products for these two ideals:

$$\begin{aligned} P_1^2 &= \langle 3, 2 + \sqrt{-5} \rangle^2 = \langle 3, 2 + \sqrt{-5} \rangle \langle 3, 2 + \sqrt{-5} \rangle \\ &= \langle 9, 3(2 + \sqrt{-5}), 3(2 + \sqrt{-5}), (2 + \sqrt{-5})^2 \rangle \\ &= \langle 2 + \sqrt{-5} \rangle \langle 2 - \sqrt{-5}, 3, 3, 2 + \sqrt{-5} \rangle \\ &= \langle 2 + \sqrt{-5} \rangle \langle 1 \rangle = \langle 2 + \sqrt{-5} \rangle, \end{aligned}$$

$$\begin{aligned} P_2^2 &= \langle 3, 2 - \sqrt{-5} \rangle^2 = \langle 3, 2 - \sqrt{-5} \rangle \langle 3, 2 - \sqrt{-5} \rangle \\ &= \langle 9, 3(2 - \sqrt{-5}), 3(2 - \sqrt{-5}), (2 - \sqrt{-5})^2 \rangle \\ &= \langle 2 - \sqrt{-5} \rangle \langle 2 + \sqrt{-5}, 3, 3, 2 - \sqrt{-5} \rangle \\ &= \langle 2 - \sqrt{-5} \rangle \langle 1 \rangle = \langle 2 - \sqrt{-5} \rangle, \end{aligned}$$

$$\begin{aligned} P_1 P_2 &= \langle 3, 2 + \sqrt{-5} \rangle \langle 3, 2 - \sqrt{-5} \rangle \\ &= \langle 9, 3(2 - \sqrt{-5}), 3(2 + \sqrt{-5}), 9 \rangle \\ &= \langle 3 \rangle \langle 3, 2 - \sqrt{5}, 2 + \sqrt{-5}, 3 \rangle \\ &= \langle 3 \rangle \langle 1 \rangle = \langle 3 \rangle. \end{aligned}$$

Thus the factorization $9 = 3 \cdot 3 = (2 + \sqrt{-5})(2 - \sqrt{-5})$ becomes, in terms of ideals,

$$\langle 9 \rangle = \langle 3 \rangle \cdot \langle 3 \rangle = P_1 P_2 \cdot P_1 P_2 = P_1^2 P_2^2,$$
$$\langle 9 \rangle = \langle 2 + \sqrt{-5} \rangle \langle 2 - \sqrt{-5} \rangle = P_1^2 P_2^2.$$

By Theorem 6.3.1 we have that the factorization $\langle 9 \rangle = P_1^2 P_2^2$ is unique.

Bibliography

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

[2] K. S. Williams. Note on non-euclidean principal ideal domains. *Math. Mag.*, 48(3):176–177, 1975.

[3] I. Stewart and D. Tall. *Algebraic Number Theory and Fermat's Last Theorem*. A K Peters, Ltd: Natick, MA, 3. edition, 2002.

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