SJÄLVSTÄNDIGA ARBETEN I MATEMATIK

MATEMATISKA INSTITUTIONEN, STOCKHOLMS UNIVERSITET

Primary Decomposition

av

Emmi Arwidsson

2013 - No 14

Primary Decomposition

Emmi Arwidsson

Självständigt arbete i matematik 15 högskolepoäng, Grundnivå

Handledare: Karl Rökaeus och Gwyn Bellamy

2013

Primary decomposition

Emmi Arwidsson

June 10, 2013

UNIVERSITY OF STOCKHOLM

BACHELOR THESIS

Emmi ARWIDSSON

SUPERVISORS
Glasgow University, Gwyn BELLAMY
Stockholm University, Karl RÖKAEUS

MATHEMATICS

Abstract

This paper concerns primary decomposition in Noetherian rings, a subject in commutative algebra with its origins in number theory. One of the first rings of interest to mathematicians after the study of $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ could be said to be the ring of Gaussian integers $\mathbb{Z}[i]$ introduced by Gauss in 1828. This ring was found to have many similarities with the ring $\mathbb{Z}$, in particular $\mathbb{Z}[i]$ is an Euclidean domain and hence as such, a unique factorization domain. The process of adjoining roots to polynomials in $\mathbb{Z}[X]$ to the ring $\mathbb{Z}$ was further studied by, amongst others, Euler, Gauss, Dirichlet and Kummer. Of particular interest was the ring of cyclotomatic integers $\mathbb{Z}[\zeta]$, where ζ is a primitive nth root of unity. The study of these rings was interlinked with the search for a proof of Fermats last theorem. Fermat last theorem is the conjecture made by Fermat that the equation $x^n + y^n = z^n$ has no positive integer solutions for $n \geq 3$. The mathematician Lamé addressed a meeting on March 1, 1847 where he announced that he had proved Fermat last theorem. Lamés proof was using the factorization $x^n+y^n = (x+y)(x+\zeta y)\dots(x+\zeta^{n-1}y)$ for ζ a primitive nth root of unity and n a odd prime. His proof was relying on the assumption that if x, y where chosen such that the n factors $(x+y), (x+\zeta y), \dots, (x+\zeta^{n-1}y)$ had no common factors for $1 \leq i < j \leq n-1$ then $(x+y)(x+\zeta y)\dots(x+\zeta^{n-1}y) = z^n$ could only hold if each one of the factors where itself a nth power. For a product of n integers with no common prime divisors this argument clearly holds. However one major flaw of Lamés argument was to assume that unique factorization which holds in $\mathbb{Z}$ also holds in the ring of cyclotomatic integers for each n. As a response to Lamés meeting Liouville asked the question: Do cyclotomatic integers have unique factorization for all n? [7][Query 1.12] It soon became clear that the answer was no. And that $\mathbb{Z}[\alpha]$, for α an algebraic integer, need not be an unique factorization domain. As a consequence of the failure of these rings to satisfy unique factorization of elements Kummer developed the theory of "ideal numbers" for which unique factorization would hold. These "ideal numbers" are precisely what we today call ideals. Dedekind proved that for rings fulfilling certain conditions, today called Dedekind domains, there exists a unique factorization of every ideal into the product of prime ideals. He proved that the ring of algebraic integers in any number field satisfies these conditions and so he developed a theory that in a way "saved" unique factorization in some of the above mentioned rings. In 1905 the mathematician Lasker generalized the concepts developed by Dedekind into the concept of primary decomposition. Primary decomposition holds for a bigger class of rings, called Noetherian rings and is a (not unique) decomposition of ideals as the intersection of primary ideals. Emmy Noether reformulated and axiomatized the theories of Dedekind and Lasker in 1920 and hence initiated the modern development of commutative algebra [5][Section 1.1].

This paper concerns the theory of primary decomposition in Noetherian rings and will prove the results obtained by Dedekind as a consequence of the general theory. This paper will also introduce the concept of Noetherian modules and prove the corresponding results on primary decomposition in this context. Hence this paper is within the field of commutative algebra but will also include results normally covered in number theory.

Contents

1 Introduction

In this paper we will focus on a class of rings, called Noetherian rings, which could be said to fulfill certain "finiteness conditions". Noetherian rings are characterized by the *ascending chain condition* on ideals. That is, if $I_1 \subseteq I_2 \subseteq ... \subseteq I_m \subseteq ...$ is an increasing sequence of ideals in a ring R, then there exists $r \in \mathbb{N}$ such that $I_n = I_r$ whenever $n \geq r$. Emmy Noether was one of the first to study the consequences of the ascending chain condition and these rings are named Noetherian in her honour. In 1921 she gave an elegant proof showing that every ideal in a ring, which satisfies the ascending chain condition, may be expressed as a finite intersection of *irreducible ideals* [5][Chapter 3]. Irreducible ideals are ideals that cannot themselves be written as the intersection of any two strictly larger ideals. Hence irreducible ideals may be viewed as "the smallest building blocks" for ideals in Noetherian rings. Generally it is not true that an irreducible ideal needs to be prime, but it will be proved that an irreducible ideal in a Noetherian ring is always *primary*. Therefore every ideal I in a Noetherian ring R may be expressed as the finite intersection of *primary ideals*. We say that I has a *primary decomposition*. In general this primary decomposition is not unique. In Sections 4 and 5 we will explore what uniqueness properties there are. In Section 7 we will discuss the factorization of ideals in a Dedekind domain as the product of prime ideals. It is worth noting, as mentioned in the abstract, that the results obtained on Dedekind domains in Section 7 historically preceded the idea of primary decomposition in Noetherian rings and may therefore be proven without these results.

This thesis has four major parts. Section 2 discusses ring and ideal theory for commutative rings. The results in this section will be used repeatedly in the rest of the text. Sections 3, 4 and 5 are the main sections of this paper and here the theory of primary decomposition in Noetherian rings is developed. In Section 6 we turn our attention to Noetherian modules. In the last section we consider the factorization of ideals in Dedekind domains. We will end with a discussion of the *ring of integers in a number field*. It was the failure of these rings to be unique factorization domains that motivated much of the development of the present theory. The aim is that the results on modules in section 6 and on Dedekind domains in section 7 will naturally relate to the results obtained in earlier sections.

Throughout this paper the ring R is assumed to be commutative with unity 1. The reader is assumed to be familiar with the content of a first course in abstract algebra, see [10]. I will use basic results from such an earlier course without further explanations, for results that may not always be covered in similar courses I refer the reader to the relevant sections in [2], which is the course literature used in [10]. All results and terminology beyond a first course in abstract algebra, i.e. beyond the scope of [10], will however be introduced gradually in the following text. References will be given in connection to most proofs. These references indicate that either the statement, or the proof of the given statement, is inspired by, or in different degrees resembles, the given reference.

2 Rings and ideals

This section concerns ring and ideal theory. In this section, as in the rest of the text, the ring R is assumed to be commutative with unity 1. We will start with a discussion of Zorn's Lemma. Zorn's Lemma is a set theoretical axiom which one uses to prove the existence of subsets that are maximal with respect to certain properties in some certain infinite sets. In

this context the relevant application of Zorn's Lemma is to conclude that every ring R with unity has a maximal ideal.

Definition 2.1. A partial order on a non empty set Σ is a relation $\leq$ on Σ satisfying the following three properties:

i) $x \leq x$ for all $x \in \Sigma$ (reflexive)

ii) if $x \leq y$ and $y \leq x$ then $x = y$ for all $x, y \in \Sigma$ (antisymmetric)

iii) if $x \leq y$ and $y \leq z$ then $x \leq z$ for all $x, y, z \in \Sigma$ (transitive)

Definition 2.2.

i) A non-empty set Σ together with a partial order $\leq$ is called a partially ordered set. A subset T of Σ is called a totally ordered (sub)set if for all $x, y \in T$ either $x \leq y$ or $y \leq x$.

ii) An upper bound for a subset T of a partially ordered set Σ is an element $a \in \Sigma$ such that $x \leq a$ for all $x \in T$.

iii) A maximal element of a partially ordered set Σ is an element $a \in \Sigma$ such that if $a \leq x$ for any $x \in \Sigma$ then this implies that $x = a$.

The partially ordered set Σ that concerns us in the current paper is the set of proper ideals of a ring R, ordered under set inclusion. This set is what is called an *inductive system* as will be shown in example 2.6.

Definition 2.3. An inductive system is a set Σ together with a partial order on Σ with the property that every totally ordered subset has an upper bound in Σ.

Zorn's Lemma. *Every non-empty inductive system possesses at least one maximal element.*

Zorn's Lemma may be proved to be equivalent to the axiom of choice and the well ordering principle, so is therefore treated as an axiom in the present context.

Even though the reader is assumed to be familiar with the definitions of maximal and prime ideals we will repeat them here as a reminder:

Definition 2.4. An ideal I in a ring R is prime if $I \neq (1)$ and if $ab \in I$ implies that $a \in I$ or $b \in I$

Definition 2.5. An ideal I in a ring R is maximal if $I \neq (1)$ and for each proper ideal J of R, we have that $I \subseteq J$ implies $I = J$

Note that I is a maximal ideal of R if and only if I is a maximal element of the set Σ of proper ideals of R ordered under set inclusion.

Example 2.6. *Every ring R with 1 has a maximal ideal.* Let Σ be the set of proper ideals of R ordered under set inclusion. Let T be a totally ordered subset of Σ, that is, for all elements I, J of T either $I \subseteq J$ or $J \subseteq I$. We will show that T has an upper bound. Let $K = \bigcup_{I \subseteq T} I$. We have that $I \subseteq K$ for all $I \subset T$ and hence K is an upper bound for T if $K \subseteq \Sigma$. We will show that K is a proper ideal of R and hence that T has an upper bound. Let $a, b \in K$ and $r \in R$ then for some ideals I, J in R we have that $a \in I$ and $b \in J$. Now

since T is totally ordered we may assume without loss of generality that $I \subseteq J$, meaning that $a, b \in J$ and therefore $a+b \in J$ hence $a+b \in K$. Furthermore, since $a \in I$ we have that $ra \in I$ and hence $ra \in K$. Therefore K is an ideal. Since all ideals in Σ are proper there is no ideal in Σ that contains 1 and hence K, being a union of elements in Σ, do not contain 1 and is therefore a proper ideal. This shows that Σ is a non-empty inductive system. By Zorn's Lemma we conclude that Σ has a maximal element. [8][Chapter 2, Lemma 4]

Lemma 2.7. *Every proper ideal I of a ring R is contained in a maximal ideal.*

Proof. Apply example 2.6 to the ring R/I. □

2.1 Operations on ideals

In this section we will discuss the sum, product and intersection of a family of ideals in a commutative ring R. By using these operations we may construct new ideals of R from old ones.

Definition 2.8. Let $\{I_i\}$ be a (possibly infinite) set of ideals in a commutative ring R:

1. We define the sum of a family of ideals $\sum_i I_i$ as the set $\{\text{all finite sums } \sum_i x_i : x_i \in I_i\}$.
2. We define the product of a finite family of ideals $\prod_{i=1}^n I_i$ as the set

$$\{\text{all finite sums } \sum_j (x_{1j}x_{2j}...x_{nj}) : x_{ij} \in I_i \text{ for each j}\}.$$

Lemma 2.9. *The sum and intersection of any family of ideals is an ideal and the product of a finite family of ideals is an ideal. Furthermore $\prod_{i=1}^n I_i \subseteq \bigcap_{i=1}^n I_i$.*

Proof. The construction immediately gives that $\sum_i I_i$ and $\prod_{i=1}^n I_i$ is closed under sums and multiplication by R. If $a, b \in \bigcap_i I_i$ and $r \in R$ then $a, b \in I_i$ for each i and hence $a+b$, ra belongs to $\bigcap_i I_i$. Let $x \in \prod_{i=1}^n I_i$ then $x = \sum_j (x_{1j}x_{2j}\dots x_{nj})$ for $x_{ij} \in I_i$ for all j. For each j $(x_{1j}x_{2j}\dots x_{nj})$ is an element of I_i, $1 \leq i \leq n$ and hence $x \in \bigcap_{i=1}^n I_i$. □

Example 2.10. Let I, J be two ideals in a commutative ring R. Consider the ideal product $(I+J)(I \bigcap J)$, this is a well defined ideal by Lemma 2.9. Let $x \in (I+J)(I \bigcap J)$. For some $n \in \mathbb{N}$ we have that $x = \sum_{i=1}^n a_i b_i$, with $a_i \in I \bigcap J$ and $b_i \in (I+J)$. Write $b_i = \sum_{j=1}^m x_j + y_j$ for $m \in \mathbb{N}$, $x_j \in I$ and $y_j \in J$. Since $a_i x_j$, $a_i y_j$ are elements of IJ for every $j \in \{1, 2, \dots, m\}$ and every $i \in \{1, 2, \cdots, n\}$, it is clear that $x = \sum_{i=1}^n a_i b_i \in IJ$. Therefore $(I+J)(I \bigcap J) \subseteq IJ$.[1][Chapter 1, Operations on ideals]

Proposition 2.11. *Let $I_1, I_2, ..., I_n$ be ideals in a ring R and let $P \subset R$ be a prime ideal such that $\bigcap_{i=1}^n I_i \subseteq P$, then $I_i \subseteq P$ for some i. Furthermore if $\bigcap_{i=1}^n I_i = P$, then $P = I_i$ for some i.*

Proof. Let $\bigcap_{i=1}^n I_i \subseteq P$ and assume that I_i is not contained in P for $1 \leq i \leq n$. Then for every i there exists $x_i \in I_i$ such that $x_i \notin P$. Consider the product $x = \prod_{i=1}^n x_i$, by construction and using the fact that P is prime this product is not in P. Clearly $x \in \prod_{i=1}^n I_i$ and hence by Lemma 2.9 this implies that $x \in \bigcap_{i=1}^n I_i$. By assumption $\bigcap_{i=1}^n I_i \subseteq P$ and therefore $x \in P$, resulting in a contradiction. We conclude that $I_i \subseteq P$ for some i. Now assume that $\bigcap_{i=1}^n I_i = P$, then clearly $P \subseteq I_i$ for every i, and since we already have shown that there exists an ideal I_i with $I_i \subseteq P$ we may conclude that $I_i = P$. [1][Proposition 1.11 ii)]. □

Proposition 2.12. *Let $P_1, P_2, ..., P_n$ be prime ideals and let I be an ideal which is not wholly contained in any one of them. Then there exists an element $\alpha \in I$ such that α does not belong to any P_i.*

Proof. We may assume that $P_i \nsubseteq P_j$ for all $i \neq j$, $1 \leq i \leq n$. Since if, for example $P_1 \subset P_2$ and we have proven the proposition for the set $P_2, P_3, ..., P_n$, then $\alpha \notin P_2$ implies that $\alpha \notin P_1$. Hence the proposition is also true for the original set of primes. Supposing that this extra condition is satisfied, for each i we have that none of $I, P_1, P_2, ..., P_{i-1}, P_{i+1}, ..., P_n$ is wholly contained in P_i. Since P_i is prime we may use the same argument as in the proof of Proposition 2.11 to conclude that the ideal product $IP_1P_2...P_{i-1}P_{i+1}...P_n$ is not contained in P_i, $1 \leq i \leq n$. Choose

$$\alpha_i \in IP_1P_2...P_{i-1}P_{i+1}...P_n \subseteq I \bigcap P_1 \bigcap P_2 \bigcap ... \bigcap P_{i-1} \bigcap P_{i+1} \bigcap ... \bigcap P_n$$

such that $\alpha_i \notin P_i$, $1 \leq i \leq n$. Set $\alpha = \sum_{i=1}^{n} \alpha_i$. Clearly α belongs to I. We will prove that α does not belong to any P_i. We have that $\alpha_i = \alpha - \sum_{i \neq j} \alpha_j$. By construction $\sum_{i \neq j} \alpha_j$ belongs to P_i, hence if α belongs to P_i this would imply that $\alpha_i \in P_i$. This is clearly not the case. We conclude that $\alpha \notin P_i$, $1 \leq i \leq n$. [8][Chapter 2, Proposition 5] □

Definition 2.13. Let E be a non-empty indexing set and let R_i be a family of rings for each $i \in E$. The direct product $\prod_{i \in E} R_i$ is defined as the Cartesian product $\prod_{i \in E} R_i = \{(r_1, r_2, r_3, ...) : r_i \in R_i\}$ equipped with component-wise addition and multiplication.

Lemma 2.14. *The direct product of a family of rings $\prod_{i \in E} R_i$ is a ring.*

Proof. Since addition and multiplication are defined component-wise the ring axioms are satisfied by the ring properties of each R_i, the element $(1_1, 1_2, 1_3, ...)$ where 1_i is the identity of R_i serves as the identity element of the direct product. □

Definition 2.15. We say that two ideals I and J of R are coprime if $I + J = (1)$.

Note that I, J are coprime if and only if there exist elements $x \in I$, $y \in J$ such that $x + y = 1$.

Theorem 2.16. *The Chinese Remainder Theorem.*
Let $I_1, I_2, ..., I_n$ be ideals of R. The map

$$R \to R/I_1 \times R/I_2 \times ... \times R/I_n \text{ defined by } r \to (r + I_1, r + I_2, ..., r + I_n)$$

is a ring homomorphism with kernel $I_1 \bigcap I_2 \bigcap ... \bigcap I_n$. If for each $i, j \in \{1, 2, ..., n\}$ with $i \neq j$ the ideals I_i and I_j are coprime, then this map is surjective and $I_1 \bigcap I_2 \bigcap ... \bigcap I_n = I_1I_2...I_n$, so

$$R/I_1I_2...I_n \cong R/I_1 \times R/I_2 \times ... \times R/I_n.$$

Proof. We first prove this for $k = 2$, the general case will follow by induction. Let
$\Phi : R \to R/I_1 \times R/I_2$ be defined by $\Phi(r) = (r + I_1, r + I_2)$. Since Φ is the natural projection of R into R/I_i, for $i = 1, 2$, on each component, it is a ring homomorphism. The kernel of Φ contains precisely those elements of R which are sent to the element $(0 \bmod I_1, 0 \bmod I_2)$, hence the elements $r \in R$ such that $r \in I_1 \bigcap I_2$. We need to show that if the ideals I_1 and I_2 are coprime, then Φ is surjective and $I_1 \bigcap I_2 = I_1I_2$. We will first prove that Φ is surjective. Since $I_1 + I_2 = R$ there exist $x \in I_1$, $y \in I_2$ such that $x + y = 1$. Hence $x = 1 - y$, consider $\Phi(x) = (x + I_1, 1 - y + I_2) = (0 \bmod I_1, 1 \bmod I_2)$. The same argument shows that $\Phi(y) =$

$(1 \bmod I_1, 0 \bmod I_2)$. Let $(r_1 \bmod I_1, r_2 \bmod I_2)$ be an arbitrary element of $R/I_1 \times R/I_2$. We have that $\Phi(r_2x + r_1y) = \Phi(r_2)\Phi(x) + \Phi(r_1)\Phi(y) = (r_2 \bmod I_1, r_2 \bmod I_2)(0,1) + (r_1 \bmod I_1, r_1 \bmod I_2)(1,0) = (r_1 \bmod I_1, r_2 \bmod I_2)$. Consequently, we have proven that Φ is surjective.

We will now prove that $I_1 \bigcap I_2 = I_1 I_2$. By Lemma 2.9 we always have that $I_1 I_2 \subseteq I_1 \bigcap I_2$. By Example 2.10 we have that $(I_1 + I_2)(I_1 \bigcap I_2) \subseteq I_1 I_2$. By assumption $I_1 + I_2 = (1)$ and hence we have proven that $(I_1 \bigcap I_2) \subseteq I_1 I_2$. We conclude that $I_1 \bigcap I_2 = I_1 I_2$. We will now prove the general case by induction. Assume that the assertion is true for $i = n-1$, consider the two ideals $I = I_n$, $J = I_1 I_2 ... I_{n-1}$. By the induction hypothesis $J = I_1 \bigcap I_2 \bigcap ... \bigcap I_{n-1}$, hence by the previous case it is sufficient to prove that I, J are coprime. Since by assumption I and I_i are coprime for all $i \in \{1, 2, ..., n-1\}$ there exists $x_i \in I$, $y_i \in I_i$ such that $x_i + y_i = 1$, $1 \leq i \leq n-1$. Hence $(x_1 + y_1)(x_2 + y_2)...(x_{n-1} + y_{n-1}) = 1$, writing this product as a sum there is only one way of choosing elements from each parenthesis so that their product doesn't contain any x_i, $1 \leq i \leq n-1$. Hence the only term in the sum which is not an element of I is the term $y_1 y_2 ... y_{n-1}$. By construction $y_1 y_2 ... y_{n-1} \in J$ and since every other term in the sum is in I, we have that $1 \in I + J$. Therefor I and J are coprime. Applying the already covered case of $i = 2$ to the ideals I and J proves the Theorem. [4][Section 7.6, Theorem 17]. □

Note that the homomorphism Φ defined as in Theorem 2.16 is not in general surjective. For example, let $R = \mathbb{Z}$ and $I_1 = 2\mathbb{Z}$, $I_2 = 4\mathbb{Z}$. Consider the element $(1, 2)$ in $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. There is no integer solution to the system of congruences $x \equiv 1 \bmod 2, x \equiv 2 \bmod 4$ since $x \equiv 2 \bmod 4$ implies that $x \equiv 0 \bmod 2$. Hence Φ is NOT generally surjective when the ideals I_i are not pairwise coprime.

Example 2.17. In a first abstract algebra course Theorem 2.16 is often proven in the special case of the ring $\mathbb{Z}_n$ of integers modulo n. That is, it is proven that $\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{\alpha_1}} \times \mathbb{Z}_{p_2^{\alpha_2}} \times ... \times \mathbb{Z}_{p_n^{\alpha_n}}$ where $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_n^{\alpha_n}$ is the prime factorization of the integer n into powers of distinct primes. The proof given in that context relies on the fact that the $GCD(p_i^{\alpha_i}, p_j^{\alpha_j}) = 1$ whenever $i \neq j$ which is equivalent to the statement that the principal ideals $(p_i^{\alpha_i})$ and $(p_j^{\alpha_j})$ are coprime whenever $i \neq j$.

2.2 The nilradical and radical ideals

Definition 2.18. An element x in a ring R is said to be *nilpotent* if there exists $n > 0$ such that $x^n = 0$.

Lemma 2.19. *The set of all nilpotent elements of a ring R is an ideal η called the nilradical of R.*

Proof. If $a \in \eta$ then there exists $n \in \mathbb{N}$ such that $a^n = 0$ hence $(ra)^n = r^n a^n = 0$, for all $r \in R$. Therefore $ra \in \eta$. Now, if $a, b \in \eta$ then for some $m, n > 0$ we have $a^m = b^n = 0$. Consider:

$$(a+b)^{m+n-1} = c_0 a^{m+n-1} + c_1 a^{m+n-2} b + ... + c_{n-1} a^m b^{n-1} + c_n a^{m-1} b^n + ... + c_{m+n-1} b^{m+n-1}$$

where $c_i \in R$, $0 \leq i \leq m+n-1$. It is clear that every term in the above expression consists of a product where at least one of the elements is zero and hence each term of the sum is zero. Hence $a + b \in \eta$. [1][Proposition 1.7] □

Proposition 2.20. *The nilradical η of R is the intersection of all prime ideals of R.*

Proof. Let η' denote the intersection of all prime ideals of R. Let $a \in \eta$ and let P be any prime ideal in R. Then for some $n > 0$ we have that $a^n = 0 \in P$. Since P is prime this implies that $a \in P$. Hence $\eta \subseteq \eta'$. Conversely we will show that $\eta' \subseteq \eta$. Suppose that $a \in R - \eta$, i.e. a is not nilpotent. Let Σ denote the set of ideals:

$$\Sigma = \{I \subset R : a^n \notin I, \forall n > 0\}$$

We want to show that there is some prime ideal of R that belongs to Σ. Since a is not nilpotent the zero ideal belongs to Σ, hence Σ is non-empty. We may prove that Σ is an inductive system in the same way as in Example 2.6. Hence may use Zorn's lemma to conclude that Σ has a maximal element, say P. We will show that P is prime. Let $x, y \notin P$ then both the ideals $(x) + P$ and $(y) + P$ strictly contain P and hence (since P is maximal in Σ) do not belong to Σ. Consequently, $a^n \in (x) + P$ and $a^m \in (y) + P$ for some $m, n > 0$. It follows that $a^{m+n} \in (xy) + P$ hence $(xy) + P \notin \Sigma$. Therefore $xy \notin P$ and so P is prime. Hence $a \notin \eta \Rightarrow a \notin \eta'$ and so $\eta' \subseteq \eta$. We conclude that $\eta = \eta'$. [1][Proposition 1.8] □

Definition 2.21. The radical of an ideal I of R is the set:

$$rad(I) = \{x \in R : x^n \in I \text{ for some } n > 0\}$$

Let $\pi : R \to R/I$ be the natural projection of R by I, then there is a one to one correspondence between the ideals of R/I and the ideals of R which contain I and hence under this correspondence $\pi^{-1}(\eta_{R/I}) = \{r \in R : r^n \in I\} = rad(I)$ and hence by Lemma 2.19 $rad(I)$ is an ideal of R. Furthermore, $I \subset rad(I)$ and $rad(I)$ is the intersection of all prime ideals of R which contain I.

Proposition 2.22. *Let I be an ideal of a ring R then:*
i) $rad(I)$ is an ideal of R. ii) $I \subset rad(I)$ and iii) $rad(I)$ is the intersection of all prime ideals of R which contain I.

Proof. i) and ii) follows from the definition of $rad(I)$ and the text preceding the Proposition. iii) follows from Proposition 2.20 and the fact that the one to one correspondence of ideals induced by the natural projection π preserves prime ideals. [1][Proposition 1.14] □

Lemma 2.23.

i) $rad(I \bigcap J) = rad(I) \bigcap rad(J)$

ii) rad(I)=(1) $\Leftrightarrow$ I=(1)

iii) rad(I+J)=rad(rad(I)+rad(J))

Proof. i) Let $x \in rad(I \bigcap J)$. Then for some $m > 0$ we have that $x^m \in I \bigcap J$, hence $x^m \in I$ and $x^m \in J$. Consequently $x \in rad(I) \bigcap rad(J)$. Conversely, let $x \in rad(I) \bigcap rad(J)$ then $x \in rad(I)$ and $x \in rad(J)$ hence there exists $m, n > 0$ such that $x^m \in I$ and $x^n \in J$ hence $x \in rad(I \bigcap J)$. ii) The implication $I = (1) \Rightarrow rad(I) = (1)$ is obvious. Conversely, if $rad(I) = (1)$ then by Proposition 2.22 there is no prime ideal which contains I. Since every proper ideal is contained in a maximal ideal and every maximal ideal is prime this results in a contradiction. Hence (I) is not a proper ideal, that is $(I) = (1)$. iii) Let $x \in rad(I + J)$. Then for some $m > 0$ we have that $x^m \in I + J$, hence $x^m = y + z$, for some $y \in I, z \in J$. Since $y \in rad(I), z \in rad(J)$ we have that $x^m \in rad(I) + rad(J)$. Consequently, $x \in$

$rad(rad(I)+rad(J))$. Conversely, let $x \in rad(rad(I)+rad(J))$ then $x^m \in rad(I)+rad(J)$ for some $m > 0$. Let $x^m = y+z$ for some $y \in rad(I)$, $z \in rad(J)$. Then there exists $k, n > 0$ such that $y^k \in I$ and $z^n \in J$. This implies that $y^k, z^n \in I+J$ and hence $y, z \in rad(I+J)$. Therefore $y+z = x^m \in rad(I+J)$. Consequently, $x \in rad(rad(I+J)) = rad(I+J)$. [1][Exercise 1.13] □

Definition 2.24. We say that an ideal I is radical if $I = rad(I)$

It is clear that $rad(rad(I)) = rad(I)$ and hence the radical of an ideal is a radical ideal.

2.3 Unique factorization domains

The reader is probably familiar with the basic properties of unique factorization domains [2][Sections 9.1, 9.2], but since this paper concerns the failure of unique factorization it is important that we remember the properties of domains that do have unique factorization.

Definition 2.25. Let R be a ring and let $x, y \in R$. We say that two elements x, y are associates if $x = uy$ for a unit $u \in R$. Clearly $y = u^{-1}x$ in this case. A non-unit $x \in R$ is said to be irreducible if $x = yz$ implies that either y or z is a unit in R. We say that an irreducible element x has no nontrivial factorization. We say that a domain D is a unique factorization domain if every non-zero non-unit $x \in D$ has a unique factorization into a finite product of irreducible elements in D. I.e $x = p_1 p_2 \dots p_m$, where p_i is irreducible for $1 \leq i \leq m$ and if $x = p_1 p_2 \dots p_m = q_1 q_2 \dots q_r$ is another such factorization then $m = r$ and it is possible to rearrange the factors such that q_i is an associate of p_i. Hence unique factorization means unique factorization up to order and multiplication by units.

If D is a domain then $x, y \in D$ are associates if and only if $x|y$ and $y|x$. Assume that $x|y$ and $y|x$, say $y = xa$ and $x = yb$ for $a, b \in D$. Then $y = yba$ which since D is a domain implies that $ab = 1$ and hence b is a unit in D. The other direction holds by definition.

Definition 2.26. An element $p \in R$ is said to be prime if whenever $p|ab$ we have that $p|a$ or $p|b$

Lemma 2.27. *In a domain D every prime element p is irreducible.*

Proof. Let p be prime and assume $p = ab$, then $p|a$ or $p|b$. Without loss of generality assume $p|a$, say $a = pc$, then $p = pcb$. Since D is a domain this implies that $cb = 1$ and hence b is a unit which shows that p is irreducible. □

Proposition 2.28. *In a unique factorization domain D every irreducible element is prime.*

Proof. Let p be irreducible in D and let $p|yz$. Let $a \in D$ be such that $yz = ap$. Let $y = \prod_{i=1}^{r} p_i$, $z = \prod_{i=1}^{s} q_i$, $a = \prod_{i=1}^{m} r_i$ be a factorization of $y, z, a \in D$ into irreducibles. Since D is a unique factorization domain p is an associate of p_i or q_j for some i or j, in particular p divides either a or b. □

Example 2.29. Let K be a field. In this example we will show that the ring $R = K[x_1, x_2, \dots]$ is a unique factorization domain. It is known that the ring of polynomials in a finite number of variables over a field is a UFD, i.e. $R_n = K[x_1, x_2, \cdots, x_n]$ is a unique factorization domain [2][Corollary 9.28], for all n. Note that $R = \bigcap_{n \in \mathbb{N}} R_n$. For any $f \in R$, f has only finitely many non-zero coefficients and is a polynomial in finitely many indeterminants, hence f belongs to R_n for some $n > 0$. Let $p \in R_n$ be irreducible, we will show

that p is irreducible in R_m for all $m \geq n$. Assume that $p = ab$ for $a, b \in R_m$, evaluating p at $x_1 = x_2 = \cdots = x_n = 1$ gives the equation $\lambda = \overline{ab}(x_{n+1}, \ldots x_m)$ where λ is a constant and $\overline{ab}$ is a polynomial in R_{m-n}, this implies that $\overline{ab}$ is constant and therefore $ab \in R_n$. Since p is irreducible in R_n we conclude that a or b is a unit. Therefore p is irreducible in R_m. This proves that there exists a factorization of f into irreducibles in R, since the factorization of f in the polynomial ring R_n is still irreducible in R by the argument above. Let $q_1 q_2 \ldots q_r$ be another factorization of f in R and let R_k be a subring of R containing the indeterminants occurring in this factorization, then there exists two irreducible factorizations of f in R_{k+n}, contradicting that R_{k+n} is a UFD. We conclude that R is a UFD. Note that the sequence $(x_1) \subset (x_1, x_2) \subset (x_1, x_2, x_3) \subset \ldots$ of ideals in R is strictly increasing. There is no $n \in \mathbb{N}$ such that $(x_1, \cdots, x_n) = (x_1, x_2, \cdots, x_r)$ whenever $r \geq n$. If there would exist such a n then this would imply that there exists polynomials $f_1, f_2, \cdots, f_n \in R$ such that $x_{n+1} = f_1 x_1 + f_2 x_2 + \cdots + f_n x_n$. If we set $x_{n+1} = 1, x_i = 0, 1 \leq i \leq n$ this implies that $1 = 0$ leading to a contradiction. We say that R does not satisfy the *ascending chain condition*, in particular R is not a Noetherian ring, see Definition 3.10. Hence a unique factorization domain is not always Noetherian.

3 Primary ideals and primary decomposition

Proposition 2.22 shows that, even though it is generally not possible to express an ideal of an arbitrary ring as the intersection of prime ideals, there exists such a decomposition of the radical ideals in an arbitrary ring. This will prove to be a useful fact. We will now introduce primary ideals, which in a sense are a generalization of prime ideals since every prime ideal is primary but not every primary ideal is prime.

3.1 Primary ideals

Definition 3.1. An ideal Q in a ring R is primary if one of the two equivalent conditions hold:

1) $Q \neq R$ and $ab \in Q$ implies that either $a \in Q$ or $b^n \in Q$ for some $n \in \mathbb{N}$

2) $R/Q \neq 0$ and every zero-divisor in R/Q is nilpotent.

To see that the conditions given above are equivalent, first assume Q fulfills 1). Let b be a zero divisor in R/Q. Then $ab \in Q$ for some $a \notin Q$, by assumption on Q we have that this implies that $b^n \in Q$, for some $n \in \mathbb{N}$ and hence b is nilpotent. Conversely, assume that every zero divisor in R/Q is nilpotent. Let $ab \in Q$ for some $a \notin Q$. Since b is a zero divisor in R/Q this implies that $b^n \in Q$, for some $n \in \mathbb{N}$. Hence 1) and 2) are equivalent.

Proposition 3.2. *Let Q be a primary ideal of a ring R. Then $rad(Q)$ is the smallest prime ideal containing Q. In particular $rad(Q)$ is a prime ideal.*

Proof. Let $P = rad(Q)$. By Proposition 2.22 we only need to show that P is prime. Let $xy \in P$ then $(xy)^n \in Q$ for some $n > 0$. Using that Q is primary we conclude that $x^n \in Q$ or $y^{nm} \in Q$, for some $m > 0$. Therefore $x \in P$ or $y \in P$. [1][Proposition 4.1]. □

Definition 3.3. Let Q be a primary ideal of the ring R. We say that Q is *P-primary* if $rad(Q) = P$.

It is well known that the prime ideals in $\mathbb{Z}$ are those principal ideals which are generated by a prime p. In Example 3.7 we will show that the primary ideals in $\mathbb{Z}$ are power of prime ideals, hence of the form $(p)^\alpha$. The primary ideal $(p)^\alpha$ in $\mathbb{Z}$ is hence (p)-primary, as one would intuitively expect. It is important to note that the general case is not quite as simple. In general a primary ideal doesn't need to be a power of a prime ideal and a power of a prime ideal doesn't need to be primary. Example 3.4 provides an example of a primary ideal that is not a power of a prime ideal.

Example 3.4. Let $R = K[x, y, z]$ where K is a field, and consider the ideal $I = (x, y, z^2)$. Then $R/I \cong K[z]/(z^2)$ under the homomorphism $\Phi(f(x, y, z)) = f(0, 0, z)$ modulo (z^2). Since every zero-divisor in $K[z]/(z^2)$ is nilpotent I is primary. Furthermore $K[z]/(z^2)$ is obviously not a domain and hence I is not prime. We have that $rad(I) = (x, y, z)$, note that $(x, y, z)^2 \subset (x, y, z^2) \subset (x, y, z)$ and hence this is an example of a primary ideal that is not a prime power. (Since the ideal I lies strictly between the minimal prime ideal $rad(I)$ that contains I and $(rad(I))^2$ and is itself not prime.) [1][Section 4, Example 2]

Example 3.5. It is important to note that the converse of Proposition 3.2 is not in general true. I.e. if $rad(I)$ is a prime ideal this does not generally imply that I is primary. For example, consider the ideal $I = (xy, y^3)$ in $K[x, y]$ for a field K. We may write $(xy, y^3) = (y) \bigcap (x, y^3)$. By Proposition 2.23 we have that $rad(xy, y^3) = rad(y) \bigcap rad(x, y^3) = (y) \bigcap (x, y) = (y)$. We conclude that $rad(I) = (y)$ and hence prime. Consider the quotient ring $K[x, y]/(xy, y^3)$. Not every zero-divisor in this ring is nilpotent and therefore I is not primary.

Example 3.5 shows that $rad(I)$ is prime is a necessary but not sufficient condition for I to be primary. Proposition 3.6 shows that if $rad(I)$ is maximal, then this is sufficient to conclude that I is a primary ideal.

Proposition 3.6. *If $rad(I)$ is a maximal ideal then I is primary. In particular every power of $rad(I)$ is in this case primary.*

Proof. Consider the natural projection $\pi : R \to R/I$. Let $rad(I) = M$, for M a maximal ideal of R. By definition $\pi(M)$ is the nilradical of R/I. Hence by Proposition 2.20 every prime ideal of R/I contains $\pi(M)$. The maximality of M therefore implies that $\pi(M)$ is the only prime ideal in R/I. Therefore there is only one maximal ideal of R/I. Let $\overline{u} = u + I$ be a non-unit of R/I, the ideal generated by $\overline{u}$ is a proper ideal. By Zorn's Lemma this ideal is contained in a maximal ideal, hence contained in $\pi(M)$. Therefore every non-unit has to be contained in $\pi(M)$ since every ideal generated by a non unit of R/I has to be contained in $\pi(M)$. We conclude that every non-unit is nilpotent in R/I. Since a unit can't be a zero-divisor this proves the proposition. (Let $u \in R$ be a unit, if $uv = 0$ for some $v \in R$, then this implies that $v = 0$ by left cancellation) [1][Proposition 4.2] □

Example 3.7. In this Example we will show that every primary ideal in $\mathbb{Z}$ is a power of a prime ideal and hence is generated by a power of a prime. First note that the ideal (p^α) and the ideal product $(p)^\alpha$ are the same ideal in $\mathbb{Z}$. Let $I = (n)$ be any ideal in $\mathbb{Z}$, with $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$, for primes p_i, $1 \leq i \leq k$. Consider $rad(I) = \{m \in \mathbb{Z} : m^r \in (n) \text{ for some } r \in \mathbb{Z}\}$. If $m \in rad(I)$, then there exists $r \in \mathbb{Z}$ such that $n \mid m^r$. Using the prime factorization of n we have that $m \in rad(I)$ iff $p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k} \mid m^r$ for some $r \in \mathbb{Z}$. Since p_i is prime for $1 \leq i \leq k$ it follows that $p_1 p_2 ... p_k \mid m$ and hence that $m \in (p_1 p_2 ... p_k)$. Conversely, if $m \in (p_1 p_2 ... p_k)$, let $r = max(\alpha_1, \alpha_2, ..., \alpha_k)$ then $m^r \in I$. Consequently, $rad(I) = (p_1 p_2 ... p_k)$. This ideal is prime if and only if it is of the form (p) for a prime $p \in \mathbb{Z}$.

Hence, any primary ideal in $\mathbb{Z}$ has to be of the form (p^α). Conversely, since $\mathbb{Z}$ is a Principal Ideal Domain every prime ideal is maximal and hence by Proposition 3.6 every power of a prime ideal is primary. Since the ideal (p^α) and the ideal product $(p)^\alpha$ are the same ideal in $\mathbb{Z}$ we conclude that every primary ideal in $\mathbb{Z}$ is of this form.

We will now introduce some further notation.

Definition 3.8. Let I and J be ideals in a ring R, their *ideal quotient* is: $(I : J) = \{r \in R : rJ \subseteq I\}$

This is a proper ideal of R if and only if $J \nsubseteq I$. If $J \subseteq I$ we have that $(I : J) = R$. Assume that $J \nsubseteq I$. For $x, y \in (I : J)$ and $r \in R$ we have that $rx \in (I : J)$ and $x+y \in (I : J)$ using the ideal properties of I. Furthermore, if $1 \in (I : J)$ then this implies that $J \subseteq I$. In particular $(0 : I)$ is called the *annihilator* of I and is denoted $Ann(I)$. $Ann(I)$ is the set of all elements $r \in R$ such that $rI = 0$. For an element $x \in R$ and a principal ideal (x) we have that $(I : (x)) = \{r \in R : r(x) \subseteq I\} = \{r \in R : rx \in I\}$ and we write $(I : (x)) = (I : x)$. In this notation the set of zero divisors in a ring R together with the element zero is:

$$\{r \in R : \exists x \neq 0 \in R \text{ such that } rx = 0\} = \bigcup_{x \neq 0} (0 : x) = \bigcup_{x \neq 0} Ann(x).$$

Lemma 3.9. *Let J be an ideal in R and let I_i be a family of ideals in R, for $1 \leq i \leq n$. Then $(\bigcap_{i=1}^n I_i : J) = \bigcap_{i=1}^n (I_i : J)$.*

Proof. See Lemma 6.13 and consider R as a module over itself. □

3.2 Noetherian rings

Definition 3.10. A Noetherian ring is a ring which satisfies the following three equivalent conditions:

i) *The ascending chain condition.* Whenever

$$I_1 \subseteq I_2 \subseteq ... \subseteq I_m \subseteq ...$$

is an increasing sequence of ideals in R there exists $r \in \mathbb{N}$ such that $I_n = I_r$ whenever $n \geq r$.

ii) *Maximal condition.* Every non-empty collection of ideals in R has a maximal element under inclusion.

iii) Every ideal of R is finitely generated

The proof that *i*), *ii*), *iii*) are equivalent is postponed to section 6 and follows Definition 6.7.

Note that for R Noetherian we do not have to use Zorn's lemma on the inductive system Σ of proper ideals of R ordered under set inclusion to come to the conclusions of Example 2.6 and Lemma 2.7. By *ii*) in Definition 3.10 every non-empty collection of ideals in R has a maximal element and therefore it is clear that every ideal is contained in a maximal ideal. Therefore, it might be worth noting that this paper does not depend on Zorn's lemma in order to derive the desired results on Noetherian rings that we are ultimately heading towards. The reason for including Zorn's Lemma in this essay is that it has allowed us to state all of the results in Section 2 for arbitrary commutative rings with 1. See Proposition

2.20, where Zorn's lemma was used. We will now explore the consequences of assuming that a ring satisfies the equal conditions $i), ii), iii)$ above. The next proposition illustrates one consequence of $iii)$.

Proposition 3.11. *In a Noetherian ring every ideal contains a power of its radical.*

Proof. Let $rad(I)$ be generated by $x_1, x_2, \cdots, x_r$. Let n_i, $1 \leq i \leq k$ be such that $x_i^{n_i}$ is in I. Let $m = 1 + \sum_{i=1}^{k}(n_i - 1)$. Consider $(rad(I))^m$, this ideal is generated by all elements of the form $x_1^{r_1}x_2^{r_2}...x_k^{r_k}$, where $\sum_i r_i = m$. From the choice of m it follows that $r_i \geq n_i$ for at least one i, hence every generator $x_1^{r_1}x_2^{r_2}...x_k^{r_k}$ of $(rad(I))^m$ belongs to I. We conclude that $rad(I)^m \subseteq I$. [1][Proposition 7.14] □

Definition 3.12. A primary decomposition of an ideal I in R is a finite expression $I = \bigcap_{i=1}^{n} Q_i$ where Q_i is a primary ideal in R.

It is possible to prove our existence theorem 3.13 within the framework we have already developed, but we will instead postpone the proof until we introduced the concepts of modules in section 6. The reason for this is to avoid a repetition of considerably similar arguments.

Theorem 3.13. *Every ideal I of a Noetherian ring R admits a primary decomposition.*

Proof. This theorem is proven in Section 6 as a special case of Theorem 6.10. However the first half of the proof is given in the text below. □

The proof of Theorem 3.13 uses what is called the *Noetherian argument* to conclude that every ideal in a Noetherian ring may be decomposed into the intersection of *irreducible ideals*. An irreducible ideal is an ideal which itself may not be written as an intersection of strictly larger ideals. The argument is simple and beautiful. Consider the set Σ of all ideals in a Noetherian ring R which may not be decomposed into an intersection of irreducible ideals. Assume, by way of contradiction, that Σ is non-empty. Since R is Noetherian there exists a maximal ideal I in Σ. By assumption I is not itself irreducible and hence there exists ideals properly containing I such that I is the intersection of these ideals. Since I is a maximal ideal in Σ these ideals have a decomposition into irreducible ideals. Therefore also I has a decomposition into irreducible ideals. This proves that every ideal in a Noetherian ring has a decomposition into irreducible ideals. To prove Theorem 3.13 it remains to show that every irreducible ideal in a Noetherian ring is a primary ideal. For this we refer to Theorem 6.10. The above illustrates the power of the Noetherian argument and the next proposition is yet another example of the same. Proposition 3.14 proves that every non-zero non-unit in a Noetherian domain has a factorization into irreducible elements.

Proposition 3.14. *Every non-zero non-unit in a Noetherian domain R may be factored into a product of irreducible elements.*

Proof. Let x be a non-unit in R, we will consider the principal ideal (x). Since the elements in (x) are those elements which are multiples of x, the ideal $(y) \subseteq (x)$ if and only if $x|y$. If $(x) = (y)$ then $x = yr$, $y = xs$ for some $s, r \in R$ which implies that $x = xsr$. Since R by assumption is a domain $x = xsr$ implies that $sr = 1$ and hence that both s, r are units. Let Σ be the set of all principal ideals (x) of R such that x may not be written as a product of irreducible elements. By way of contradiction, assume that Σ is non-empty. Using that R is Noetherian we let (y) be a maximal ideal in Σ. Then y is not irreducible and hence $y = ab$

where neither a nor b is a unit. Therefore $(y) \subset (a)$ and $(y) \subset (b)$ where the inclusion is proper because otherwise a or b would be a unit. Since (y) is a maximal ideal in Σ this implies that both a and b may be factored into a product of irreducibles. In particular this implies that $y = ab$ has a factorization into irreducible elements. □

One of the reason that we are interested with the construction of primary decomposition in Noetherian rings (and therefore in particular in Noetherian domains) is that the factorization of elements discussed in the theorem above may not be *unique*. There may be *different factorizations of the same element into irreducible elements*. In fact this is often the case, see the next example.

Example 3.15. Consider the ring $\mathbb{Z}[\sqrt{-5}] = \{a+b\sqrt{-5} : a, b \in \mathbb{Z}\}$, this ring is a Noetherian domain (see Proposition 6.8), but does not satisfy unique factorization. The element 6 has two *different* factorization into a product of irreducible elements. We have that $6 = 3 \times 2 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ in $\mathbb{Z}[\sqrt{-5}]$. We will show in Example 7.24 that the four elements $3, 2, (1 + \sqrt{-5}), (1 - \sqrt{-5})$ really are irreducible in $\mathbb{Z}[\sqrt{-5}]$, a result that acquires some knowledge about number fields. Note that it is not sufficient that 6 has to seemingly different factorization, for example $12 = 3 \times 4 = 6 \times 2$ is two seemingly different factorizations of the element $12 \in \mathbb{Z}$. This however is not two different factorizations of 12 into irreducibles, since they are just different ways of writing the unique factorization $12 = 3 \times 2 \times 2$. As already mentioned, we will show in Example 7.24 that 2 is irreducible in $\mathbb{Z}[\sqrt{-5}]$. Note that 2 divides $6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$, but is not a factor of $(1 \pm \sqrt{-5})$. Hence 2 is an *irreducible element which is not prime* in $\mathbb{Z}$. In fact, the failure of irreducible elements to be prime is the reason for the failure of unique factorization in Noetherian domains.

Proposition 3.16. *A Noetherian domain D is a unique factorization domain if and only if every irreducible element in D is prime*

Proof. If D is a UFD then every irreducible element in D is prime by Proposition 2.28. Conversely, let $x \in D$ and let $x = \prod_{i=1}^{m} p_i = \prod_{j=1}^{n} q_i$, for $m \leq n$, be two factorizations of x into a product of irreducibles. Since p_1 is prime, p_1 divides q_i for some i, wlofg assume $i = 1$. Since q_1 is irreducible this implies that q_1 is an associate of p_1. We will proceed by induction on m, since p_1 and q_1 are associates we may cancel p_1 to obtain $\prod_{i=2}^{m} p_i = \prod_{j=2}^{n} uq_i$ for u a unit in D. By induction $m - 1 = n - 1$ and we may rearrange such that p_i is an associate of q_i. □

Now is the right time to note that neither the factorization of elements in a Noetherian domain nor the primary decomposition of ideals in a Noetherian ring (nor a domain) is unique. Theorem 3.13 only states that there exist at least one decomposition of every ideal into a finite intersection of primary ideals and, in fact, there are in general many such decompositions. The following example illustrates this. Let $R = K[x, y]$, for K a field (the result that this ring is Noetherian is called Hilbert Basis Theorem and will not be proven in this text, for a proof of this result see for example [1, Theorem 7.5]). Let $I = (x^2, xy)$. Two different primary decompositions of I are given by $(x^2, xy) = (x) \bigcap (x, y)^2$ and $(x^2, xy) = (x) \bigcap (x^2, y)$. It might help to write $(x, y)^2 = (x^2, xy, y^2)$ to see that $(x^2, xy, y^2) \bigcap (x)$ is really the ideal (x^2, xy). To see that the ideals occurring in the two decompositions are actually primary ideals, note that $K[x, y]/(x, y) \cong K$ which is a field and $K[x, y]/(x) \cong K[y]$ which is a domain. Hence (x, y) is a maximal ideal and (x) is a prime (and hence primary) ideal. Since $(x, y) = rad(x^2, y) = rad((x, y)^2)$ we may conclude (by Proposition 3.6) that the ideals occurring in the two different decompositions of I are really primary ideals. This gives us two different primary decompositions of (x^2, xy) in $K[x, y]$.

Example 3.17. A primary ideal does not need to be irreducible. Consider the ideal $(x, y)^2$ in the ring $K[x, y]$, we have that $(x, y)^2 = (x^2, xy, y^2)) = (x^2, y) \cap (x, y^2)$.

Example 3.18. Let $R = K[x, y]$ and $I = (x^2, xy)$ as above, then there are even more primary decompositions of I. Actually, for every $a \in K$ we have that $(x) \bigcap (x^2, y - ax)$ is a primary decomposition of I. To prove this, we will first show that $(x^2, xy) = (x^2, xy - ax^2)$ for all $a \in K$. The elements in (x^2, yx) are of the form $g(x, y)x^2 + f(x, y)yx$ for some $g(x, y), f(x, y) \in K[x, y]$. For any $a \in K$ we may write this as $(g(x, y) + af(x, y))x^2 + f(x, y)(yx - ax^2)$, hence $(x^2, xy) \subseteq (x^2, xy - ax^2)$. A similar argument shows that $(x^2, xy - ax^2) \subseteq (x^2, xy)$, hence the two ideals are the same. We may therefor search for a primary decomposition of $(x^2, yx - ax^2)$. We have that $(x^2, yx - ax^2) = (x^2, x(y - ax)) = (x^2, y - ax) \bigcap (x)$. For K infinite, for example $K = \mathbb{Q}$, there are therefore infinite many primary decompositions of I. [3][Section 4.7, exercise 6]

The examples above shows that a primary decomposition of an ideal I in a Noetherian ring R can not be expected to be unique. Therefore it may seam like we have not reached much further in our search for an alternative to unique factorization in these rings. But our work has not been in vain, because as we will see, the primary decomposition of an ideal I, after being slightly modified, will have some "uniqueness properties". This will be the subject of the next two sections.

4 The first uniqueness theorem

4.1 Associated primes

In this section we will associate a uniquely determined set of prime ideals to any ideal I of R. The set of primes which we associate to I in this certain way will be called the *associated primes of* I and will be denoted $Ass(I)$. In the first uniqueness theorem 4.7 we will show that for a primary decomposition fulfilling certain conditions (see Definition 4.5) the radicals of the primary ideals occurring in the primary decomposition of I equal the set $Ass(I)$. Hence the prime ideals related to a primary decomposition in this way are always the same. Our first step towards this result will be to define the set of associated primes of an ideal I.

Definition 4.1. Let I be an ideal of a ring R. The set of *associated primes of* I denoted $Ass(I)$ is the set of prime ideals occurring in the set of ideals $(I : x)$, $x \in R$.

The definition of associated primes of an ideal I differ between authors. In [1] the set of associated primes of an ideal is introduced after the first uniqueness theorem. The set of associated primes as defined there is proven to be equal to the set we have chosen above in a much later section of the same book [1][Proposition 7.17]. In [9], associated primes are defined in the context of modules, the following lemma gives another way of thinking about the set $Ass(I)$.

Lemma 4.2. *Let $\pi : R \to R/I$ be the natural projection of R by I. The elements of $Ass(I)$ are in one to one correspondence with the prime ideals $\overline{P} \in R/I$ such that $\overline{P} = ann(\overline{x})$, $\overline{x} \in R/I$. The correspondence is the natural one $P \to \pi(P)$, $\overline{P} \to \pi^{-1}(\overline{P})$.*

Proof. It is clear that there is a one to one correspondence between the ideals of R/I and the ideals of R which contain I and that this correspondence preserves prime ideals. Let

$\overline{P}$ be prime in R/I. Let π be the natural projection of R by I. If $\overline{P} = (0 : \overline{x})$, then $\pi^{-1}(\overline{P}) = \{r \in R : (r+I)(x+I) = I\} = (I : x)$. Choose any other representative of $\overline{r}$ say r', then $r - r' \in I$ and hence $rx \in I \Leftrightarrow r'x \in I$, hence $r' \in (I : x)$. Choose any other representative of $\overline{x}$ say x', then $x - x' \in I$ and hence $rx \in I \Leftrightarrow rx' \in I$, hence $(I : x) = (I : x')$. Conversely if $(I : x) = P$ is prime, then $\pi(P)$ is prime in R/I. And $\pi(P) = \{r + I : (r+I)(x+I) = I\} = (0 : \overline{x})$. If $(I : x) = (I : y)$ then $rx \in I \leftrightarrow ry \in I$ and hence $(r+I)(x+I) = I$ if and only if $(r+I)(y+I) = I$, hence $(0 : \overline{x}) = (0 : \overline{y})$. □

Our definition of the associated primes of I is equivalent to the way that the set $Ass(R/I)$ has been defined in [9]. There they consider R/I as an R-module and the set $Ass(R/I)$ to be the set of primes $P \in R$ such that $P = ann(\overline{x})$, for some $\overline{x} \in R/I$. After reading about modules in Section 6 it will be easy for the reader to verify that $P \in Ass(R/I)_{[9]}$ if and only if P is prime and $P = \{r \in R : r(x+I) = I\} = (I : x)$, for some $x \in R$. Where $Ass(R/I)_{[9]}$ denotes the definition given in [9] as described above. Therefore, considering R/I as a R-module, we have that $Ass(I)$ is the set of prime ideals $P \subset R$ such that $P = ann(\overline{x})$ for some $\overline{x} \in R/I$ and our definition of the set $Ass(I)$ corresponds to the set $Ass(R/I)$ as defined in [9].

4.2 The first uniqueness theorem

Let R be a Noetherian ring and let I be an ideal of R. By Theorem 3.13 the ideal I has a primary decomposition. We will now examine which uniqueness properties there are.

Definition 4.3. Let R be a Noetherian ring and I an ideal of R. We say that the primary decomposition $I = \bigcap_{i=1}^{n} Q_i$ is irredundant if: i) the primes $rad(Q_i)$ are all distinct, and ii) we have $\bigcap_{j \neq i} Q_j \nsubseteq Q_i$, $1 \leq i \leq n$.

We will see that a given primary decomposition may easily be reduced to an irredundant primary decomposition. First we will need the following lemma:

Lemma 4.4. *Let Q_i be P-primary, for $1 \leq i \leq n$. Then $Q = \bigcap_{i=1}^{n} Q_i$ is a P-primary ideal.*

Proof. By Proposition 2.23 we have that $rad(Q) = rad(\bigcap_{i=1}^{m} Q_i) = \bigcap_{i=1}^{m}(rad(Q_i)) = P$. We will now prove that Q is primary. Let $ab \in Q$, $a \notin Q$. Then $ab \in Q_i$, $1 \leq i \leq n$ and for some $i \in \{1, 2, \cdots, n\}$ we have that $a \notin Q_i$. Since $ab \in Q_i$, $a \notin Q_i$, where Q_i is a P-primary ideal, this implies that $b \in P$. Since $rad(Q) = P$ it follows that $b^n \in Q$ for some $n \in \mathbb{N}$. [1][Lemma 4.3] □

Lemma 4.5. *Any primary decomposition of an ideal I may be reduced to an irredundant primary decomposition.*

Proof. By Lemma 4.4 we may achieve i) by replacing all P-primary ideals with their intersection. Thereafter we may achieve ii) by simply removing superfluous terms one after the other. I.e. if $\bigcap_{j \neq i} Q_j \subseteq Q_i$ then $\bigcap_{j \neq i} Q_j \cap Q_i = \bigcap_{j \neq i} Q_j$ and hence Q_i is superfluous. □

Lemma 4.6. *Let Q be a P-primary ideal of the ring R.*
i) If $x \in Q$ then $(Q : x) = R$, ii) If $x \notin Q$ then $rad(Q : x) = P$

Proof. i) is immediate. ii) Consider $x \notin Q$. Let $y \in (Q : x)$. Then $yx \in Q$ and hence since $x \notin Q$ this implies that $y \in P$ since Q is primary. Consequently $(Q : x) \subseteq P$. Since $Q \subseteq (Q : x)$ by definition we have the following containment: $Q \subseteq (Q : x) \subseteq P$ taking radicals shows that $rad(Q : x) = P$. [1][Lemma 4.4] □

Theorem 4.7. *The first uniqueness theorem. Let I be an ideal of a Noetherian ring R. Let $I = \bigcap_{i=1}^{n} Q_i$ be an irredundant primary decomposition of I. Let $P_i = rad(Q_i)$, $1 \leq i \leq n$. Then $\{P_1, P_2, \cdots, P_n\} = Ass(I)$ and hence independent of the particular decomposition of I.*

Proof. We will first show that the prime ideals that occur in the set of ideals $rad(I : x)$, $(x \in R)$ are the set $\{P_1, P_2, ..., P_n\}$. We will then prove that the prime ideals in the set of ideals $rad(I : x)$ are the same as the prime ideals occurring in the set of ideals $(I : x)$.

1. For any $x \in R$ we have (by Lemma 3.9 and Lemma 2.23) that $rad(I : x) = rad(\bigcap_{i=1}^{n} Q_i : x) = rad(\bigcap_{i=1}^{n}(Q_i : x)) = \bigcap_{i=1}^{n} rad(Q_i : x)$. Combining the two cases described in Lemma 4.6, we have that $\bigcap_{i=1}^{n} rad(Q_i : x) = \bigcap_{x \notin Q_i} rad(Q_i : x) = \bigcap_{x \notin Q_i} P_i$. If $rad(I : x)$ is a prime ideal P, then $P = \bigcap_{x \notin Q_i} P_i$. By Proposition 2.11 this implies that $P = P_i$ for some i, $1 \leq i \leq n$. Therefore each prime ideal occurring in the set of ideals $rad(I : x)$, $(x \in R)$ is one of the $P_i s$. Conversely, we will show that every P_i is of the form $rad(I : x)$ for some $x \in R$. Since the decomposition of I is irredundant, we have that $\bigcap_{j \neq i} Q_j \nsubseteq Q_i$ for all i, $1 \leq i \leq n$. Therefore there exists $x_i \in \bigcap_{j \neq i} Q_j$ such that $x_i \notin Q_i$ and hence $rad(I : x_i) = P_i$.

2. By passing to R/I and using the correspondence developed in Lemma 4.2, we may assume that $I = 0$. Using this extra assumption, we will prove that if $0 = \bigcap_{i=1}^{n} Q_i$ is an irredundant primary decomposition of the zero ideal where Q_i is P_i-primary then $Ass(0) = \{P_1, P_2, ..., P_n\}$. If $(0 : x)$ is a prime ideal P then $rad(0 : x) = P$ and hence by part 1, P is one of the $P_i s$. Conversely, we will show that there exists $x_i \in R$ such that $(0 : x_i) = P_i$, $1 \leq i \leq n$. Let $I_i = \bigcap_{i \neq j} Q_i$. For any $x_i \neq 0 \in I_i$ the discussion in part 1 of this proof shows that $rad(0 : x_i) = P_i$, hence $(0 : x_i) \subseteq P_i$ for any such x_i. Conversely, since Q_i is P_i-primary there exists $m \in \mathbb{N}$ (by Proposition 3.11) such that $P_i^m \subseteq Q_i$. Hence the following containment holds: $P_i^m I_i \subseteq P_i^m \bigcap I_i \subseteq Q_i \bigcap I_i = 0$. We conclude that $P_i^m I_i = 0$. Let m be the smallest integer for which this equality holds. Let $x_i \neq 0 \in P_i^{m-1} I_i$, for such an x_i we have that $P_i x_i = 0$. Therefore $P_i \subseteq ann(x_i)$, note that $x_i \subseteq I_i$ and hence there exists $x_i \in R$ such that $(0 : x_i) = P_i$, $1 \leq i \leq n$. Therefore the prime ideals in the set of ideals $rad(I : x)$ are the same as the prime ideals in the set of ideals $(I : x)$, $(x \in R)$. We conclude that $Ass(I) = \{P_1, P_2, ..., P_n\}$. □

Our proof of the first uniqueness theorem follows the arguments given in [1][Theorem 4.5, Proposition 7.17], where part 1 of the given proof corresponds to [1][Theorem 4.5] and part 2 corresponds to [1][Proposition 7.17]. Note that part one of the proof is sufficient to prove that the set of primes $\{P_1, P_2, ..., P_n\}$ as described in the theorem is uniquely determined by I, since the set treated in 1 does not depend on the given primary decomposition of I. The reason for including part 2 of the theorem is that the theorem then corresponds to the first uniqueness theorem as stated in for example [9], see [9][Section 7.12, 1st uniqueness theorem].

Definition 4.8. We say that an ideal I_i in R is a minimal element of the set $\Sigma = \{I_1, I_2, ...\}$ of ideals of R, if for any ideal I_j in Σ such that $I_j \subseteq I_i$, we have that $I_j = I_i$. If P_i is a minimal element of the set $Ass(I) = \{P_1, P_2, ..., P_n\}$ then P_i is said to be a minimal prime of I, otherwise P_i is said to be an embedded prime of I.

Lemma 4.9. *Let $I = \bigcap_{i=1}^{n} Q_i$ be an irredundant primary decomposition of I. Let $Ass(I) = \{P_1, P_2, \cdots, P_n\}$. Let P be a prime ideal in R, then P contains I if and only if $P_i \subseteq P$ for*

at least one $i \in \{1, 2, \cdots, n\}$. Hence there are only finitely many minimal primes among the primes which contain I and all of these occur as minimal primes of the set $\{P_1, P_2, \cdots, P_n\}$.

Proof. Assume that $P_i \subseteq P$ for some i. We have that $I \subseteq rad(I) = \bigcap_{i=1}^{n} P_i$, hence $I \subseteq P_i$, $(1 \leq i \leq n)$, therefore $I \subseteq P$. Conversely, let $I \subseteq P$ then $\bigcap_{i=1}^{n} Q_i \subseteq P$. We will prove that this implies that $\bigcap_{i=1}^{n} P_i \subseteq P$. Assume the contrary, let $x \in (\bigcap_{i=1}^{n} P_i) - P$. For some large enough integer $m \in \mathbb{N}$, $x^m \in \bigcap_{i=1}^{n} Q_i \subseteq P$. This contradicts the assumption that P is prime. Consequently, $\bigcap_{i=1}^{n} P_i \subseteq P$, by Proposition 2.11 this implies that $P_i \subseteq P$ for some i. □

Example 4.10. Let $R = K[x, y]$ and let $I = (x^2, xy)$ as in Example 3.18. We have seen that $(x^2, xy) = (x^2, y - ax) \bigcap (x)$ for any $a \in K$. The associated primes of I are $rad(x^2, y - ax) = (x, y)$ and $rad(x) = (x)$. In this example $(x) \subseteq (x, y)$. Therefore (x) is a minimal prime of the primary decomposition and (x, y) is an embedded prime of the primary decomposition.

5 The second uniqueness theorem

In the previous sections we gave examples to show that an irredundant primary decomposition of an ideal I in a Noetherian ring R, $I = \bigcap_{i=1}^{n} Q_i$ is not uniquely determined. I.e. the primary ideals Q_i, $1 \leq i \leq n$ are in general not unique. However, we did show in Theorem 4.7 that the set of *associated primes of* I is equal to the set $\{rad(Q_i), 1 \leq i \leq n\}$ and hence that this set of prime ideals is independent of the chosen decomposition. In this section we will go further and prove that some of the primary ideals Q_i occurring in a primary decomposition of I actually are uniquely determined and hence have to occur in any primary decomposition of I. These are the P_i-primary ideals for which the prime ideal P_i is a minimal prime of I.

To prove this result we will consider a bigger ring R_{P_i}, which we construct from R by adjoining inverses to some of the elements of R. The construction of this ring is very similar to the construction of the field of fractions when R is an integral domain. In both cases we are creating inverses for some elements in the ring R. The difference to the latter construction being that we don't necessary want to create inverses for every non-zero element and that we don't assume the ring R to be a domain. For these two reasons we generally don't end up with a field but instead a ring, called a ring of fractions.

5.1 Ring of fractions

I assume that the reader is familiar with the construction of the field of fractions for an integral domain D as the quotient $D \times D^* / \sim$, where D^* is the set of non zero elements of D and $\sim$ denotes the equivalence relation $(a, b) \sim (c, d)$ iff $ad - bc = 0$. To prove that $\sim$ is transitive the assumption that D is a domain is used for cancellation. Hence, we will have to do some slight modifications when considering an arbitrary ring R.

Definition 5.1. A multiplicative set S of R is a subset of R such that $1 \in S$ and S is closed under multiplication. Further, we will follow the convention and assume that $0 \notin S$.

Let R be a ring and let S be a multiplicative set. Define the relation $\sim$ on $R \times S$ by $(a, b) \sim (c, d)$ if and only if there exists $s \in S$ such that $s(ad - bc) = 0$. Then $\sim$ is an equivalence

relation. We will leave the proof that $\sim$ is reflexive and symmetric to the reader and only show transitivity. Let $(a,s) \sim (b,t)$ and $(b,t) \sim (c,u)$ then there exists $v, w \in S$ such that $v(at-sb) = 0$ and $w(bu-ct) = 0$. Therefore $vwt(au-cs) = vuw(at-bs)+wsv(bu-ct) = 0$. Since $vwt \in S$ this shows that $(a,s) \sim (c,u)$.

We usually write $\frac{a}{s}$ to denote the equivalence class $\overline{(a,s)}$. As in the case of the domain D we may induce a ring structure on the set $S^{-1}R = R \times S/\sim$ given by:

$$\frac{a}{s} + \frac{b}{t} = \frac{at+bs}{st},$$

$$\frac{a}{s}\frac{b}{t} = \frac{ab}{st}$$

Both $+$ and $\times$ are independent of representatives and hence the operations stated above are well-defined. Furthermore $S^{-1}R$ is a ring under these two operations. We will not show any of these results here, since we assume that the reader has seen very similar verifications when considering the field of fractions of a domain.

Example 5.2. Let R be a ring and S be the set $R - P$ for a prime ideal P of R. By definition of prime ideals S is a multiplicative set. We denote $S^{-1}R$ by R_P.

5.2 Extended and contracted ideals

The results in this section mainly correspond to [1][Proposition 3.11]. Let $\Phi : R \to R'$ be any ring homomorphism. Let J be any ideal of R', the set $\Phi^{-1}(J) = \{r \in R : \Phi(r) \in J\}$ is always an ideal of R, called the contraction of J, denoted J^c. If J is a prime ideal of R' then J^c is easily seen to be prime in R. Consider the set $\Phi(I)$ for an ideal I of R, in general $\Phi(I)$ is not an ideal of R'. Let $y = \Phi(x) \in \Phi(I)$ and $r' \in R'$, consider the product yr', this product may not be an element in $\Phi(I)$. If however Φ is an epimorphism, then $r' = \Phi(r)$ for some $r \in R$ and hence $yr' = \Phi(x)\Phi(r) = \Phi(xr)$ which by the ideal property of I is in $\Phi(I)$. With this motivation it is easy to see that the smallest ideal in R' which contains the set $\Phi(I)$ is the ideal generated by the same set. I.e. the set of all finite sums $\sum_i \Phi(x_i)r'_i$ where $x_i \in I$, $r'_i \in R'$. This ideal is called the extension of I and is denoted by I^e. Hence, for any epimorphism $I^e = \Phi(I)$.

In general we can factor Φ as follows, $R \xrightarrow{\rho} \Phi(R) \xrightarrow{i} R'$. For ρ the situation is easy, we know that there is a one to one correspondence between the ideals of R witch contain $ker(\Phi)$ and the ideals of $\Phi(R)$. In particular, under this correspondence prime ideals correspond to prime ideals. For the embedding i the situation is more complicated. To give an example, consider $R = \mathbb{Q}[x]$, $I = (x^2 - 3)$, $R' = \mathbb{R}[x]$ and Φ the embedding of $\mathbb{Q}[x]$ into $\mathbb{R}[x]$. We have that I is prime in $\mathbb{Q}[x]$ but I^e is not prime in $\mathbb{R}[x]$.

Lemma 5.3. *Let $\Phi : R \to R'$ be a ring homomorphism. Let I, I_1, I_2 be ideals of R and J, J_1, J_2 be ideals of R', then:*

i) $I \subseteq I^{ec}$, $J \supseteq J^{ce}$ and $I^e = I^{ece}$, $J^c = J^{cec}$

ii) $(I_1 \bigcap I_2)^e \subseteq I_1^e \bigcap I_2^e$ and $(J_1 \bigcap J_2)^c = J_1^c \bigcap J_2^c$

iii) $(I_1 I_2)^e = I_1^e I_2^e$ and $(J_1 J_2)^c \supseteq J_1^c J_2^c$

iiii) $(rad(I))^e \subseteq rad(I^e)$ and $(rad(J))^c = rad(J^c)$

Proof. i) $I \subseteq I^{ec}$, $J \supseteq J^{ce}$ follows from the definition. Considering the set I^e and the set I^{ece}, $I \subseteq I^{ec}$ implies that $I^e \subseteq I^{ece}$. In the same manner $J \supseteq J^{ce}$ implies that $J^{cec} \subseteq J^c$. For the other direction $J \supseteq J^{ce}$ implies that $I^e \supseteq I^{ece}$ and $I \subseteq I^{ec}$ implies that $J^c \subseteq J^{cec}$. ii) $(I_1 \bigcap I_2)^e \subseteq I_1^e \bigcap I_2^e$ is immediate. Let $x \in (J_1 \bigcap J_2)^c$, then $\Phi(x) \in J_1 \bigcap J_2$, hence $x \in J_1^c \bigcap J_2^c$. Conversely, let $x \in J_1^c \bigcap J_2^c$, then $\Phi(x) \in J_1 \bigcap J_2$, hence $x \in (J_1 \bigcap J_2)^c$. iii) Let $y \in (I_1 I_2)^e$. For $x_1 \in I_1, x_2 \in I_2$ and $r_i' \in R'$ we have that $y = \sum_i \Phi(x_{1i}x_{2i})r_i' = \sum_i \Phi(x_{1i})\Phi(x_{2i})r_i'$. It is clear that $y \in I_1^e I_2^e$. Conversely, let $y \in I_1^e I_2^e$, $y = \sum_i r_{1i}'\Phi(x_{1i})\Phi(x_{2i})r_{2i}' = \sum_i r_{1i}'r_{2i}'\Phi(x_{1i}x_{2i})$, therefore $y \in (I_1 I_2)^e$. Let $x \in J_1^c J_2^c$. For some $x_{1i} \in J_1^c$, $x_{2i} \in J_2^c$ we have that $\Phi(x) = \sum_i \Phi(x_{1i}x_{2i}) = \sum_i \Phi(x_{1i})\Phi(x_{2i})$. Therefore $\Phi(x) \in J_1^{ce} J_2^{ce} \subseteq J_1 J_2$, hence $x \in (J_1 J_2)^c$. iiii) Let $y \in (rad(I))^e$. Choose $m \in \mathbb{N}$, $x_i \in rad(I)$ and $r' \in R'$ such that $y = \sum_{i=1}^m r_i'\Phi(x_i)$. Then there exists $n_i \in \mathbb{N}$ such that $x_i^{n_i} \in I$, $1 \leq i \leq m$. Set $k = 1 + \sum_{i=1}^m (n_i - 1)$. Then $y^k = (\sum_{i=1}^m r_i'\Phi(x_i))^k = \sum r'_{k_1,k_2,\ldots,k_m}\Phi(x_1^{k_1})\Phi(x_2^{k_2})\ldots\Phi(x_m^{k_m})$, where the sum ranges over all possible combinations k_i such that $k_1 + k_2 + \cdots + k_m = k$ and where $r'_{k_1,k_2,\ldots,k_m} \in R'$. By construction $k_i \geq n_i$ for some i, hence for such an i we have that $x_i^{k_i} \in I$. Therefore $y^k \in I^e$ and hence $y \in rad(I^e)$. Let $x \in (rad(J))^c$. We have $\Phi(x) \in rad(J) \Rightarrow (\Phi(x))^n \in J$, for some $n \in \mathbb{N}$. Since $(\Phi(x))^n = \Phi(x^n)$ we have that $x^n \in J^c$ hence $x \in rad(J^c)$. Conversely, let $x \in rad(J^c)$. Then there exists $m \in \mathbb{N}$ such that $x^m \in J^c$ which implies that $(\Phi(x))^m \in J$, hence $(\Phi(x)) \in rad(J)$. Therefore $x \in (rad(J))^c$. [1][Exercise 1.18] □

Let $\Phi : R \to S^{-1}R$ be given by $\Phi(r) = \frac{r}{1}$. Then Φ is clearly a homomorphism. For the rest of this section we will consider this homomorphism and examine the relationship between the ideals I, J^c of R and the ideals I^e, J of $S^{-1}R$. We will come to the conclusion, that even though there is no one to one correspondence between the general ideals of these rings, there is such a correspondence if we restrict our attention to a certain subset of ideals. In particular, there is a one to one correspondence between the prime ideals which do not meet S in R and the prime ideals in $S^{-1}R$, given by $P \leftrightarrow P^e$. Note that for Φ defined as above and for an ideal I of R, we have that $I^e = S^{-1}I$. This can be seen as follows, let $x \in I^e$ for $a_i \in I$, $r' \in S^{-1}R$, $r_i \in R$ and $s_i \in S$, we have that:

$$x = \sum_{i=1}^n \Phi(a_i)r_i' = \sum_{i=1}^n \frac{a_i}{1}\frac{r_i}{s_i} = \frac{1}{s_1 s_2 \ldots s_n}\sum_{i=1}^n \frac{s_1 s_2 \ldots s_n}{s_i} a_i r_i$$

for some $n \in \mathbb{N}$. It is clear that the last sum is in I hence $x = \frac{a}{s}$ for some $a \in I$, $s \in S$. The reverse inclusion is immediate. We will use the notation $S^{-1}I$ and I^e interchangeably.

Lemma 5.4. *Let R be a ring and let S be a multiplicative set. i) For any ideal I of R with $I \bigcap S \neq \emptyset$ we have that $I^e = S^{-1}R$. ii) Every ideal J of $S^{-1}R$ is equal to I^e for some ideal I of R which does not meet S; conversely, for every proper ideal I of R that does not meet S, I^e is a proper ideal of $S^{-1}R$.*

Proof. i) Let $x \in I \bigcap S$ then $\frac{x}{1} \in I^e$, since $x \in S$ by assumption this is a unit in $S^{-1}R$. ii) Let I be an ideal of R which does not meet S. By definition I^e is an ideal in $S^{-1}R$. It is clear that $I^e = S^{-1}I \neq S^{-1}R$ since it does not contain any units of $S^{-1}R$. Conversely, let J be any ideal of $S^{-1}R$, if $\frac{x}{s} \in J$, then $\frac{x}{1} \in J$, therefore $x \in J^c$. This shows that $\frac{x}{s} \in J^{ce}$, hence $J \subseteq J^{ce}$. By Lemma 5.3 it is always true that $J \supseteq J^{ce}$. Hence $J = J^{ce}$. Since $J^c = I$ for some ideal I of R we have that $J = S^{-1}I$. □

Example 5.5. Consider the ring R_P, the elements $\frac{p}{s}$ for $p \in P$ form the ideal P^e in R_P. By the previous proposition, it is clear that any ideal in R_P has to be of the form I^e for

some ideal I contained in P. It is easy to see that $I^e \subseteq P^e$ for all such I. Hence the ideal P^e is the only maximal ideal of R_P. We say that a ring with only one maximal ideal is a *local ring*. The process of passing R to R_P is called *localization*.

Proposition 5.6. *Let I be an ideal of R and let J be an ideal of $S^{-1}R$, then i) $J^{ce} = J$, and ii) $I^{ec} = \bigcup_{s\in S}(I : s)$*

Proof. i) Follows directly from the proof of Lemma 5.4. To prove ii) note that for any ideal I of R, we have that $x \in I^{ec} = (S^{-1}I)^c$ iff $\frac{x}{1} = \frac{a}{s}$ for some $s \in S$ and some $a \in I$. That is, there exists $t \in S$ such that $t(sx - a) = 0$. Since $0 \in I$ and $at \in I$ by construction, this implies that $s'x \in I$, for $s' = st \in S$. Therefore $x \in \bigcup_{s\in S}(I : s)$. Conversely, if $sx \in I$ for some $s \in S$ then $\frac{sx}{s} \in I^e$ and hence $x \in I^{ec}$. □

Consider two ideals I_1 and I_2 of R which do not meet S. In general it is false that $S^{-1}I_1 = S^{-1}I_2$ in $S^{-1}R$ implies that $I_1 = I_2$ in R. For example, consider the ring $R = \mathbb{Q}[x]$ and the irreducible ideal $P = (x^2 - 2)$. Let $S^{-1}R$ be the localization of R by P. Consider the ideal $I = (x - 9)(x^2 - 2)$ in R. We have that $I \subsetneq P$. Since $(x - 9)$ is in S, we have that $S^{-1}(x-9) = S^{-1}R$. By Lemma 5.3 iii), we have that $((x-9)(x^2-2))^e = (x-9)^e(x^2-2)^e = S^{-1}RS^{-1}P = S^{-1}P$. We conclude that we have found ideals $P \neq I$ that do not meet S such that $S^{-1}I = S^{-1}P$. Hence there is no one to one correspondence between general ideals of R that doesn't meet S and the ideals of $S^{-1}R$, but as stated in the beginning of this section, we will show that such a correspondence exists for ideals of R with certain properties (5.7) and especially for primary and prime ideals (5.10).

Corollary 5.7. *Let M be the set of ideals $M = \{I \subset R - S : I^{ec} = I\}$, then there is a one to one correspondence $(I \leftrightarrow I^e)$ between the elements of M and the ideals of $S^{-1}R$.*

Proof. First note that by Lemma 5.4 we have that every ideal in $S^{-1}R$ is equal to $I^e = I^{ece}$ for some ideal I of R that doesn't meet S, hence equal to $(I^{ec})^e$. It is easy to see that I^{ec} is an element of M. Secondly, let I be an ideal in M with $I^e = I'^e$ for some ideal $I' \neq I$ in R. Then we must have that $I^{ec} = I'^{ec}$. Since I is in M we have that $I = I^{ec} = I'^{ec}$. By assumption $I' \neq I$, hence $I' \neq I'^{ec}$ and therefor $I' \notin M$. □

Example 5.8. Let Q be a P-primary ideal of R, we will show that $Q^{ec} = Q$ if $P \bigcap S = \emptyset$. For a primary ideal Q, $rs \in Q$, $s \notin P$ implies that $r \in Q$ since if $r \notin Q$ this would imply (since Q is primary) that $s^n \in Q$, contradicting the assumption on P. Hence $Q^{ec} = \bigcup_{s\in S}(Q : s) \subseteq Q$, by Lemma 5.3 $Q \subseteq Q^{ec}$ and therefore $Q^{ec} = Q$ in this case.

Proposition 5.9. *S^{-1} commutes with the formation of intersections, radicals and products.*

Proof. i) By Lemma 5.3 we only need to prove that $S^{-1}I_1 \bigcap S^{-1}I_2 \subseteq S^{-1}(I_1 \bigcap I_2)$. Let $x \in S^{-1}I_1 \bigcap S^{-1}I_2$. Then $x = \frac{a}{s} = \frac{b}{t}$ for $a \in I_1, b \in I_2, s, t \in S$. Hence there exists $u \in S$ such that $u(at-sb) = 0$ and therefore $uat = usb = w$. Consequently, $x = \frac{w}{stu} \in S^{-1}(I_1 \bigcap I_2)$. ii) By Lemma 5.3 we only need to prove that $rad(S^{-1}I) \subseteq S^{-1}(rad(I))$. Let $x = \frac{x_i}{s_i} \in rad(S^{-1}I)$. For some $n \in \mathbb{N}$ we have that $x^n = \frac{x_i^n}{s_i^n} \in S^{-1}I$. This implies that $\frac{x_i^n}{1} \in S^{-1}I$, hence $x_i^n \in I^{ec}$. By Proposition 5.6 there exists $s \in S$ such that $x_i^n s \in I$. Therefore $x_i^n s^n \in I$, hence $x_i s \in rad(I)$. Considering $S^{-1}(rad(I))$ we have that: $\frac{x_i s}{s s_i} = \frac{x_i}{s_i} = x \in S^{-1}(rad(I))$. *iii*) follows from Lemma 5.3 □

Corollary 5.10. *Let Q be a P-primary ideal of R. If $P \bigcap S \neq \emptyset$ then $S^{-1}Q = S^{-1}R$. If $P \bigcap S = \emptyset$ then $S^{-1}P$ is a prime ideal of $S^{-1}R$, furthermore $S^{-1}Q$ is a $S^{-1}P$-primary ideal of $S^{-1}R$.*

Proof. If $S \bigcap P \neq \emptyset$, we may choose $s \in S \bigcap P$ and $n \in \mathbb{N}$ such that $s^n \in S \bigcap Q$, therefore $Q \bigcap S \neq \emptyset$. By Lemma 5.4 this implies that $S^{-1}Q = S^{-1}R$. Assume that $S \bigcap P = \emptyset$, we will first prove that $S^{-1}P$ is prime. Let $\frac{x}{s}\frac{y}{t} \in S^{-1}P$, then $xy \in P^{ec}$. By Example 5.8 we have that $P^{ec} = P$. Since P is prime by assumption either $x \in P$ or $y \in P$. Consequently $\frac{x}{s}$ or $\frac{y}{t}$ belongs to $S^{-1}P$. We conclude that $S^{-1}P$ is in this case prime. By Proposition 5.9 we have that $rad(S^{-1}Q) = S^{-1}rad(Q) = S^{-1}P$. Let $\frac{xy}{st} \in S^{-1}Q$ and $\frac{x}{s} \notin S^{-1}Q$, then $xy \in Q^{ec} = Q$ and $x \notin Q$ by Example 5.8. Therefore $y \in P$ and hence $\frac{y}{t} \in S^{-1}P$. Showing that $S^{-1}Q$ is primary.[1][Proposition 4.8] □

5.3 The second uniqueness theorem

Given a primary decomposition of an ideal I in a Noetherian ring R we will consider the ideal $S^{-1}I$ in the ring $S^{-1}R$ and a corresponding primary decomposition in this ring. In this fashion we will find that the primary ideals Q_i corresponding to minimal prime ideals P_i of I are uniquely determined.

Theorem 5.11. *Let R be a Noetherian ring, and let S be a multiplicative set. Let $I = \bigcap_{i=1}^{n} Q_i$ be an irredundant primary decomposition of an ideal I of R, with $P_i = rad(Q_i)$. Renumber the Q_is such that $S \bigcap P_i = \emptyset$ for $1 \leq i \leq m$ and $S \bigcap P_j \neq \emptyset$ for $m < j \leq n$. Then:*

$$i)\ S^{-1}I = \bigcap_{i=1}^{m} S^{-1}Q_i \text{ and } ii)\ (S^{-1}I)^c = \bigcap_{i=1}^{m} Q_i$$

Proof. i) follows from Proposition 5.9 and Corollary 5.10. ii) We have that $(S^{-1}I)^c = (\bigcap_{i=1}^{m} S^{-1}Q_i)^c = \bigcap_{i=1}^{m}(S^{-1}Q_i)^c$ by Proposition 5.9 and Lemma 5.3. By Example 5.8 we have that $(S^{-1}Q_i)^c = Q_i$. [1][Proposition 4.9] □

Corollary 5.12. *The Second Uniqueness Theorem. Let $I = \bigcap_{i=1}^{n} Q_i$ be an irredundant primary decomposition of I with $rad(Q_i) = P_i$ for $1 \leq i \leq n$. Suppose that P_i is an minimal element of $\{P_1, P_2, .., P_n\}$. Let S be the multiplicative set $R - P_i$, Then:*

$$Q_i = (S^{-1}I)^c$$

In particular, Q_i is uniquely determined by I and P_i

Proof. Since P_i is minimal there is no $j \neq i$ such that P_j is contained in P_i and hence $S \bigcap P_j \neq \emptyset$ for all $j \neq i$ and hence $(S^{-1}I)^c = Q_i$ by Theorem 5.11. [9][Section 7.13, 2nd uniqueness theorem] □

Example 5.13. Consider the ideal (x^2y, y^2x) in $K[x, y]$. One irredundant primary decomposition is $(x^2y, y^2x) = (x) \bigcap (y) \bigcap (x^2, y^2)$. The associated primes are $\{(x), (y), (x, y)\}$, we have that (x) and (y) are minimal prime ideals and that (x, y) is an embedded prime ideal. Note that the fact that $(x), (y)$ are minimal implies that the corresponding primary ideals (in this special case the same ideals) are *uniquely* determined and hence have to be a part of *any* primary decomposition of (x^2y, y^2x). Furthermore, since the set of associated primes is uniquely determined any other primary decomposition of (x^2y, y^2x) has to include a third component that is (x, y)-primary. Note that any ideal I with $rad(I) = (x, y)$ is primary by Proposition 3.6 since (x, y) is a maximal ideal. Hence we may find another irredundant primary decomposition by finding some ideal I with $rad(I) = (x, y)$ and $I \bigcap (x) \bigcap (y) = (x^2y, y^2x)$, and every irredundant primary decomposition must be of exactly

this form. As in Example 3.18 we have that $(x^2y, y^2x) = (x^2y - y^2x, y^2x)$. We find a decomposition in the following way:

$$(x^2y - y^2x, y^2x) = (xy(x-y), y^2x) = (y) \bigcap (x) \bigcap (x-y, y^2).$$

Since $rad(x-y, y^2) = (x-y, y) = (x, y)$, this is really a primary decomposition.

6 Modules

Definition 6.1. Let R be a commutative ring (as always). A R-module M is an abelian group together with a mapping μ from $R \times M$ into M satisfying the following properties:

i) $\mu(r, x+y) = \mu(r, x) + \mu(r, y)$

ii) $\mu(r+s, x) = \mu(r, x) + \mu(s, x)$

iii) $\mu(rs, x) = \mu(r, \mu(s, x))$

iiii) $\mu(1, x) = x$

We often write rx for $\mu(r, x)$.

Definition 6.2. A subset N of a R-module M is a *submodule* of M if N is a subgroup of M that is closed under multiplication by R.

The concept of modules generalizes many familiar concepts, here are some examples:

Example 6.3. Any ring R is a module over itself. Furthermore any ideal I of R is a submodule of R since an ideal by definition is an abelian subgroup of R closed under multiplication by R. Conversely, every submodule of the module R over itself is an ideal of R.

Example 6.4. For R a field a R-module is a R-vector space. In this sense modules are a generalization of vector spaces, that allow the "scalars" to come from an arbitrary ring and not only a field.

Example 6.5. Let G be an abelian group. Define $\mu : \mathbb{Z} \times G \to G$ as $\mu(n, g) = g + g + \cdots + g$ (n times), it is easy to see that μ fulfills i)-iiii) in definition 6.1, hence every abelian group is a $\mathbb{Z}$-module.

Definition 6.6. Let E be an indexing set. A set $X = \{x_i\}$ for $i \in E$ is a set of generators for the R-module M if $M = \sum_{i \in E} Rx_i$. This means that every element of M can be expressed as a finite linear combination of elements in R and elements in X. A finitely generated module is a module with a finite set of generators.

Most of the operations defined in 2.1 have their counterparts for modules. Let M be a R-module and let N_i be a family of submodules in M. Then $\sum_i N_i$ is the submodule consisting of all elements $x \in M$ which are finite sums $\sum_i x_i$ where $x_i \in N_i$. Generally we cannot define the product of two submodules of M. If I however is an ideal in R we can define the product IM as all finite sums $\sum_i a_i x_i$, where $a_i \in I$ and $x_i \in M$. This is a submodule of M.

6.1 Noetherian modules

Similarly to definition 3.10 we define a Noetherian module in the following way:

Definition 6.7. A Noetherian R-module M is a module satisfying the following three equivalent conditions:

i) *The ascending chain condition.* Whenever

$$N_1 \subseteq N_2 \subseteq ... \subseteq N_m \subseteq ...$$

is an increasing sequence of submodules of M there exists $r \in \mathbb{N}$ such that $N_n = N_r$ whenever $n \geq r$.

ii) *Maximal condition.* Every non-empty collection of submodules of M has a maximal element under inclusion.

iii) Every submodule of M is finitely generated.

We will now prove the equivalence of *i*), *ii*), *iii*) and hence as a consequence prove the equivalence of the conditions in Definition 3.10. Assume that *i*) holds, we will prove *ii*). Let Σ be any non-empty collection of submodules of M. Choose $N_i \in \Sigma$. If N_i is a maximal element of Σ we are done. Assume N_i is not maximal, then there exists $N_{i+1} \in \Sigma$ such that $N_i \subset N_{i+1}$. Assume that Σ doesn't have any maximal element, then for each $m \in \mathbb{N}$ we have a proper containment $N_{i+m} \subset N_{i+m+1}$ of submodules of M, this contradicts *i*). Hence Σ has a maximal element. Now, assume that *ii*) holds, we will prove *iii*). Let N be any submodule of M. Let Σ be the collection of all finitely generated submodules of N. Σ is non-empty since the zero module is contained in any submodule N and is finitely generated, hence by *ii*) Σ contains a maximal element say N'. If $N = N'$ we are done. Assume $N \neq N'$. Let $y \in N - N'$. Consider the submodule $Ry + N'$, by assumption N' is finitely generated and Ry is obviously finitely generated by y, this shows that $Ry + N'$ is finitely generated. Since $Ry + N'$ by construction is a submodule of N which properly contains N' this contradicts the maximality of N'. We conclude that $N - N'$ is empty and that $N = N'$, hence N is finitely generated. Finally, assume that *iii*) holds, we will prove *i*). Let $N_1 \subseteq N_2 \subseteq ... \subseteq N_m \subseteq ...$ be an infinite increasing sequence of submodules of M. Let $N = \bigcup_{i=1}^{\infty} N_i$. Obviously N is a submodule of M and therefore by *iii*), N is finitely generated. Let $\{x_i\}_{i=1}^n$ be a minimal set of generators of N. Let N_{j_i} be a submodule in the chain above such that $x_i \in N_{j_i}$ for $1 \leq i \leq n$. Let $m = max\{j_1, j_2, ..., j_n\}$, that is, m is the maximal index for which the generators of N is contained. We conclude that $\{x_i\}_{i=1}^n \subseteq N_m$ by construction and hence $N \subseteq N_m$, hence $N = N_m = N_k$ for all $k \geq m$. This proves *i*). [4][Section 12.1, Theorem 1].

Note that not every finitely generated module is Noetherian, in particular every submodule of a finitely generated module doesn't need to be finitely generated. Consider the ring $R = K[x_1, x_2, \dots]$ discussed in example 2.29 as a module over itself. It is finitely generated as a R-module with generator 1, but the ideal consisting of all polynomials with zero constant term is not finitely generated, since any finite set of elements in I could only span a subset of polynomials in finitely many variables, since each polynomial only has finitely many non-zero coefficients. As a consequence of *iii*) in Definition 6.7 the converse is always true, i.e. a Noetherian module is always finitely generated. Proposition 6.8 gives the sufficient conditions for a finitely generated module to be Noetherian.

Proposition 6.8. *If M is a finitely generated R-module over a Noetherian ring R then M is a Noetherian module.*

Proof. Let N be a submodule of M, we will show that N is finitely generated and hence that M is Noetherian. Since M is finitely generated it has a finite set of generators say $\{f_1, f_2, ..., f_t\}$ we will give a proof by induction on the number t of generators of M. Consider the case $t = 1$, say M is generated by f_1. Consider the epimorphism $\Phi : R \to M$ defined by $\Phi(1) = f_1$. Consider the set $\Phi^{-1}(N) = \{r \in R : \Phi(r) \in N\}$ this is an ideal of R. Hence by assumption on R it is finitely generated, say by $\{b_1, b_2, ..., b_k\}$, hence $\{\Phi(b_1), \Phi(b_2), ..\Phi(b_k)\}$ is a set of generators of N. Consider the case $t > 1$ and the submodule $Rf_1 \subset M$. Let π be the natural projection $\pi : M \to M/Rf_1$, let $\overline{N}$ be the image of N under π. Now, consider M/Rf_1 as a R-module in the following way: define $\mu : R \times M/Rf_1 \to M/Rf_1$ by $\mu(r, a+Rf_1) = ra+Rf_1$, (addition is of course given by $(a+Rf_1)+(b+Rf_1) = (a+b)+Rf_1$) it is left to the reader to verify that these operations are well defined and that M/Rf_1 is indeed a R-module under the same. M/Rf_1 is generated by $t-1$ generators, hence by the induction hypothesis the submodule $\overline{N} \in M/Rf_1$ is finitely generated. Since π is onto we may assume that $\overline{N}$ is generated by $\{\pi(g_1), \pi(g_2), ..., \pi(g_k)\}$ for $g_i \in M$, $1 \leq i \leq k$. For any $x \in N$ we have that $\overline{x} = \pi(x)$ is a linear combination of the generators of $\overline{N}$, say $\overline{x} = a_1\pi(g_1) + a_2\pi(g_2) + ... + a_k\pi(g_k)$ for $a_i \in R$, $1 \leq i \leq k$. Consider $n = x - (a_1g_1 + a_2g_2 + ... + a_kg_k) \in M$ this is by construction an element of $N \bigcap ker(\pi) = N \bigcap Rf_1$. Since $M \bigcap Rf_1$ is finitely generated by one element the submodule $N \bigcap Rf_1 \subseteq M \bigcap Rf_1$ is finitely generated, by the case $t = 1$ already considered in the beginning of this proof. Let $\{h_1, h_2, ..., h_m\}$ be a minimal set of generators of $N \bigcap Rf_1$. Write the element $n \in N \bigcap Rf_1$ as $n = b_1h_1+b_2h_2+...+b_mh_m$, for $b_i \in R$. This shows that $x = n+a_1g_1+a_2g_2+...+a_kg_k = b_1h_1 + b_2h_2 + ... + b_mh_m + a_1g_1 + a_2g_2 + ... + a_kg_k$, for $b_i, a_j \in R$, $1 \leq i \leq m$ and $1 \leq j \leq k$. In particular $\{h_1, h_2, ..., h_m\} \bigcup \{g_1, g_2, ..., g_m\}$ is a set of generators of N. We conclude that M is Noetherian. [5][Proposition 1.4] □

It is important to note that in general the converse of Theorem 6.8 is not true. That is, if the R-module M is Noetherian this doesn't imply that R is. For example, consider the zero module, which is clearly Noetherian over every ring R.

6.2 Primary decomposition in Noetherian modules

Definition 6.9. A submodule N of a R-module M is called primary if:

i) N is a proper submodule

ii) if for $r \in R$ and $e \in M$ we have $re \in N$ and $e \notin N$, then this implies that $r^mM \subseteq N$ for some $m \in \mathbb{N}$

Theorem 6.10. *Let M be a Noetherian R-module over a commutative ring R. Then any proper submodule N of M has a primary decomposition; that is, N is a finite intersection of primary submodules.*

Proof. We will prove the theorem in two parts. We say that a submodule N_i is irreducible if it cannot be written as the intersection of any two strictly larger submodules. We will first show that every submodule of a Noetherian module M may be written as a finite intersection of irreducible submodules. Thereafter we will show that every irreducible submodule of M is a primary submodule.

1. Every submodule N of M may be written as a finite intersection of irreducible submodules. We will give a proof by contradiction. Let Σ be the set of all submodules N_i of M such that N_i is not an intersection of irreducible submodules. Assume that Σ is non empty, since M is Noetherian there is a maximal submodule N in Σ. N is not an intersection of irreducible submodules, in particular N is not irreducible. Hence N is the intersection of two strictly larger submodules. By the maximality of N these are not in Σ and hence may be written as the intersection of irreducible submodules. It follows that N is also an intersection of irreducible submodules.
2. Every irreducible submodule N of M is primary. Let $rx \in N$ for $r \in R$, $x \in M - N$. Consider $N_i = \{y \in M : r^i y \in N\}$. N_i is clearly a submodule of M. Consider the ascending chain of submodules given by:

$$N_1 \subseteq N_2 \subseteq ... \subseteq N_i \subseteq N_{i+1}....$$

Since M is Noetherian there exists $n \in \mathbb{N}$ such that $N_r = N_n$ for all $r \geq n$. Consider the submodules $T = Rx + N$, $S = r^n M + N$ of M, it is clear that $N \subseteq T$, $N \subseteq S$ and in particular $T \bigcap S$ is non-empty. Let $y \in T \bigcap S$, then $y \in S$ and hence $y = r^n z + q$ for some $z \in M$, $q \in N$. Since by assumption $rx \in N$ we have that $rT \subseteq N$ and in particular $ry = r^{n+1}z + rq$ is in N. This implies that $r^{n+1}z \in N$. Therefore $z \in N_{n+1} = N_n$ which means that $r^n z \in N$. We conclude that $y = r^n z + q \in N$ and therefore $S \bigcap T \subseteq N$. Since $N \subseteq S \bigcap T$ we have proven that $N = S \bigcap T$. We now use the assumption that N is irreducible, hence $T = N$ or $S = N$. By assumption $x \notin N$ and hence $N \neq T$, this implies that $N = S$. Therefore $r^n M \subseteq N$ and we conclude that N is primary. The above proof is a modification of the proof given for Noetherian rings in [4][Proposition 15, Section 15.2], into the language of Modules. □

6.3 Uniqueness properties of primary decomposition in Noetherian modules

In Theorem 6.10 we proved the existence of a primary decomposition of every submodule N of a Noetherian module M. In general this decomposition is not unique, in this section we will examine what uniqueness properties there are.

Definition 6.11. Let M be a R-module. Let N be a submodule and let U be a subset of M. Let T be a subset of R. We define

$(N : U)$ to be the set of $r \in R$ such that $rx \in N$ for all $x \in U$.

$(N : T)_M$ to be the set of $x \in M$ such that $rx \in N$ for all $r \in T$.

Lemma 6.12. *Let M be a R-module. Let N be a submodule, let U be a subset of M and let T be a subset of R. The set $(N : U)$ is an ideal of R and the set $(N : T)_M$ is a submodule of M. If $U \subset N$ then $(N : U) = R$ and if $T \subset (N : M)$ then $(N : T)_M = M$.*

Proof. Let $s, t \in (N : U)$ and $r \in R$. For any $x \in U$ $sx, tx \in N$ and hence $sx+tx = (s+t)x \in N$. Therefore $(s + t) \in (N : U)$. Furthermore, since N is closed under multiplication of R we have that $rt \in (N : U)$. Hence $(N : U)$ is an ideal of R. Similarly, let $x, y \in (N : T)_M$ and $r \in R$, then we have that $tx, ty \in N$, for all $t \in T$. Since N is a submodule of M, this implies that $tx + ty = t(x + y) \in N$ for all $t \in T$, hence $(N : T)_M$ is closed under addition. Since $tx \in N$, this implies that $rtx \in N$ and hence $rx \in (N : T)_M$. Hence $(N : T)_M$ is a submodule of M. The last two statements are immediate. □

Lemma 6.13. *Let $\{N_i\}$ for $1 \leq i \leq n$ be a family of submodules of the R-module M, let U be a subset of M and let T be a subset of R, then $((\bigcap_{i=1}^n N_i) : U) = \bigcap_{i=1}^n (N_i : U)$ and $((\bigcap_{i=1}^n N_i) : T)_M = \bigcap_{i=1}^n (N_i : T)_M$.*

Proof. Let $r \in R$ for each $u \in U$, $ru \in \bigcap_{i=1}^n N_i$ iff $ru \in N_i$, $1 \leq i \leq n$. Hence for each u we have that $r \in (\bigcap_{i=1}^n N_i : u) \Leftrightarrow r \in \bigcap_{i=1}^n (N_i : u)$. Varying u shows that $r \in ((\bigcap_{i=1}^n N_i) : U)$ iff $r \in \bigcap_{i=1}^n (N_i : U)$. Similarly, let $x \in M$, for each $t \in T$, $tx \in \bigcap_{i=1}^n N_i$ iff $tx \in N_i$, $1 \leq i \leq n$. Varying t shows that $x \in ((\bigcap_{i=1}^n N_i) : T)_M$ iff $x \in \bigcap_{i=1}^n (N_i : T)_M$. □

Proposition 6.14. *Let N be a primary submodule of a R-module M. Then $(N : M)$ is a primary ideal of R.*

Proof: By lemma 6.12 we only need to show that $(N : M)$ is primary. Let $ab \in (N : M)$ such that $b \notin (N : M)$. Then there exists some $x \in M$ such that $bx \notin N$, since $ab \in (N : M)$ we have that $abx \in N$. Since N is a primary submodule this implies that $a^n M \subseteq N$ for some $n > 0$, hence $a^n \in (N : M)$. [8][Chapter 2, Proposition 18.].

Definition 6.15. We say that a primary submodule $N \subset M$ is P-primary if $rad(N : M) = P$.

Note that if N is a P-primary submodule of a R-module M, then if $rx \in N$, where $r \in R$ and $x \in M$, we must have that either $r \in P$ or $x \in N$. Since if $x \notin N$, then by definition $r^n M \subseteq N$, for some $n \in \mathbb{N}$. Accordingly $r \in rad(N : M)$.

Definition 6.16. Let S be a multiplicative set of R, for the submodule N of the R-module M, let N^S denote the set of all elements $x \in M$ such that there exists $s \in S$ such that $sx \in N$.

Lemma 6.17. *N^S is a submodule of M.*

Proof. Let $x, y \in N^S$. Then there exists $s, s' \in S$ such that $sx, s'y \in N$. Set $ss' = t$, then we have that $t \in S$ and that $t(x + y) \in N$. Hence $x + y \in N^S$. Let $r \in R$, then $rsx \in N$ and hence $rx \in N^S$. □

Proposition 6.18. *Let $N = \bigcap_{i=1}^n N_i$ be a primary decomposition of the submodule N of the R-module M, where N_i is a P_i-primary submodule. Let S be a non-empty multiplicative set of R. Renumber the N_is such that $S \bigcap P_i = \emptyset$, for $1 \leq i \leq m$, and $S \bigcap P_i \neq \emptyset$, for $m + 1 \leq i \leq n$. Then:*

$$N^S = \bigcap_{i=1}^m N_i$$

Proof. For each i satisfying $m + 1 \leq i \leq n$, choose $s_i \in S$ such that $s_i \in P_i$. Put $\sigma = s_{m+1} s_{m+2} ... s_n$. Then $\sigma \in S$ and $\sigma \in P_i$, for $m + 1 \leq i \leq n$. Since $P_i = Rad(N_i : M)$ there exists some large enough $k > 0$ such that σ^k belongs to $(N_i : M)$ for all $i = m+1, m+2, ..., n$. If we therefore choose $s = \sigma^k$, we have that $s \in S$ and $sM \subseteq \bigcap_{i=m+1}^n N_i$. We will use this to prove that $\bigcap_{i=1}^m N_i \subseteq N^S$. Let $x \in \bigcap_{i=1}^m N_i$, for the $s \in S$ described in the previous sentence, we have that $sx \in \bigcap_{i=1}^n N_i = N$. Therefore, $x \in N^S$ and hence $\bigcap_{i=1}^m N_i \subseteq N^S$. Conversely, let $y \in N^S$. Then there exists $s' \in S$ such that $s'y \in N$, hence $s'y \in \bigcap_{i=1}^n N_i$. Since $S \bigcap P_i = \emptyset$, $1 \leq i \leq m$, the fact that $s'y \in N_i$ and the fact that N_i is primary imply that $y \in \bigcap_{i=1}^m N_i$. Therefore $N^S \subseteq \bigcap_{i=1}^m N_i$. [8][Chapter 2, Proposition 27] □

Definition 6.19. We say that a primary decomposition of a submodule $N = \bigcap_{i=1}^n N_i$, where N_i is P_i-primary is *irredundant* if $\bigcap_{j \neq i} N_j \nsubseteq N_i$ and all the P_is are distinct, for $1 \leq i \leq n$.

6.3.1 The uniqueness theorems

Lemma 6.20. *Every primary decomposition of a submodule N of the R-module M may be turned into an irredundant primary decomposition.*

Proof. The idea is the same as in Lemma 4.5. First we group the P_i-primary submodules together and replace them with their intersection, thereafter we remove all superfluous terms one by one. Hence we need to prove that if $\{N_1, N_2, \cdots, N_m\}$ are all P-primary submodules then so is $N = \bigcap_{i=1}^{m} N_i$. By Lemma 6.13 and Lemma 2.23 $rad(N : M) = \bigcap_{i=1}^{m} rad(N_i : M) = P$. Let $rx \in N$, for $r \in R$ and $x \in M - N$. Then for some i we have that $rx \in N_i$ for $x \notin N_i$. This implies that $r \in P$, hence for a large enough integer k we have that $r^k M \subseteq N$. Hence N is primary. □

Theorem 6.21. *The first uniqueness theorem. Let N be a submodule of the Noetherian R-module M. Let $N = \bigcap_{i=1}^{n} N_i$ and $N = \bigcap_{j=1}^{k} N'_j$ be two irredundant primary decompositions of N. Suppose that N_i is P_i-primary and that N'_j is P'_j-primary. Then $k = n$ and the prime ideals $P_1, P_2, .., P_n$ are the same as the prime ideals $P'_1, P'_2, ..., P'_k$ though their order may be different.*

Proof. Let P be any one of $P_1, P_2, .., P_n$. It is sufficient to show that P occurs amongst $P'_1, P'_2, ..., P'_k$ because the roles of the two set of prime ideals can then be interchanged to prove the other direction. Without loss of generality renumber the $P_i s$ and the $P'_j s$ such that: $P = P_m$,

$$P_i \subseteq P \text{ for } 1 \leq i \leq m-1 \text{ and } P_i \nsubseteq P \text{ for } m+1 \leq i \leq n$$

And such that

$$P'_j \subseteq P \text{ for } 1 \leq j \leq r \text{ and } P'_j \nsubseteq P \text{ for } r+1 \leq j \leq k.$$

Let $S = R - P$ and consider N^S. By Theorem 6.18, $N^S = \bigcap_{i=1}^{m} N_i = \bigcap_{i=1}^{r} N'_j$. Now assume that $P \neq P'_j$, $1 \leq j \leq r$, we will derive a contradiction. Since the primes in each of the given primary decompositions are all distinct, P is not contained in any of $P_1, P_2, ..., P_{m-1}$. By assumption P is not equal to any of $P'_1, P'_2, ..., P'_r$, hence P is not contained in any one of these prime ideals either. Since P is not contained in any of $P_1, P_2, ..., P_{m-1}$ or $P'_1, P'_2, ..., P'_r$ there exists an element $\alpha \in P$ (by Proposition 2.12) such that α does not belong to a single one of $P_1, P_2, ..., P_{m-1}, P'_1, P'_2, ..., P'_r$. Since $P = rad(N_m : M)$, we have that α^v belongs to $(N_m : M)$ provided that v is a large enough positive integer. Since α^v belongs to $(N_m : M)$ we have that $(N_m : \alpha^v) = M$. On the other hand, since $\alpha \notin P_i$, $1 \leq i \leq m-1$, if $x\alpha^v \in N_i$ for any $x \in M$ we must have that $x \in N_i$, hence $(N_i : \alpha^v) = N_i$, $1 \leq i \leq m-1$. Similarly, $(N'_j : \alpha^v) = N'_j$, $1 \leq j \leq r$. Thus

$$(N^S : \alpha^v) = (N_1 : \alpha^v) \bigcap (N_2 : \alpha^v) \bigcap ... \bigcap (N_m : \alpha^v) = N_1 \bigcap N_2 ... \bigcap N_{m-1}$$

And

$$(N^S : \alpha^v) = (N'_1 : \alpha^v) \bigcap (N'_2 : \alpha^v) \bigcap ... \bigcap (N'_r : \alpha^v) = N'_1 \bigcap N'_2 ... \bigcap N'_r$$

But $N'_1 \bigcap N'_2 ... \bigcap N'_r = N_1 \bigcap N_2 ... \bigcap N_m$ and hence the calculations above show that $N_1 \bigcap N_2 ... \bigcap N_{m-1} = N_1 \bigcap N_2 ... \bigcap N_m$. This contradicts the assumption that the primary decomposition was irredundant. Therefore we have derived a contradiction and we conclude that $P = P'_j$ for some $j \in \{1, 2, \cdots, r\}$. [8][Chapter 2, Theorem 13] □

The set $\{P_1, P_2, ..., P_n\}$ of prime ideals in Theorem 6.21 is hence uniquely determined by N and M. We say that the prime ideals in this set *belong to the submodule* N of M. Similarly to the earlier discussion of associated primes of an ideal, we say that a prime ideal P_i belonging to N is *minimal* if $P_j \subseteq P_i$ implies that $P_i = P_j$ for all $j \in \{1, 2, ..., n\}$. The prime ideals belonging to N which are not minimal are called *embedded* prime ideals of N.

Corollary 6.22. *The second uniqueness theorem. Let $N = \bigcap_{i=1}^{n} N_i$ be an irredundant primary decomposition of the submodule N of the Noetherian module M, where N_i is P_i-primary. Suppose that P_i is a minimal prime belonging to N. Let S be the multiplicative set $R - P_i$, Then:*

$$N^S = N_i$$

and hence N_i is uniquely determined by P_i and N.

Proof. Since P_i is minimal in the set $\{P_1, P_2, \cdots, P_n\}$, S meets P_j for all $j \neq i$, hence the proposition follows directly from Proposition 6.18. □

Theorem 6.23. *Let N be a proper submodule of a finitely generated R-module M over a Noetherian ring R. Let $N = \bigcap_{i=1}^{n} N_i$ be an irredundant primary decomposition of N, where N_i is P_i-primary. Let $Ass(N : M)$ denote the associated primes of the ideal $(N : M)$ in R, then:*

$$Ass(N : M) \subseteq \{P_1, P_2, ..., P_n\}$$

And the minimal prime ideals of $(N : M)$ are the same as the minimal prime ideals belonging to N.

Proof. First note that M is Noetherian by Proposition 6.8 and hence N admits a primary decomposition. By assumption and by Lemma 6.13 we have that $(N : M) = (\bigcap_{i=1}^{n} N_i : M) = \bigcap_{i=1}^{n} (N_i : M)$. This is a primary decomposition of the ideal $(N : M)$ in the Noetherian ring R. By removing superfluous terms, this may be turned into an irredundant primary decomposition. In this process we might lose some of the $P_i s$ so it follows from Theorem 4.7 that the associated primes of $(N : M)$ are a subset of $\{P_1, P_2, ..., P_n\}$. By Lemma 4.9 a minimal prime P_i containing $(N : M)$ will always be an element of $Ass(N : M)$. □

7 Dedekind domains

In this section we will consider a special kind of Noetherian rings which admit some nicer properties in their primary decomposition than the general case we have so far considered. We will find that every ideal in a Dedekind domain has a *unique factorization into prime ideals*, a result that is far stronger than the primary decompositions we have so far discussed. First, we will state the unique factorization theorem in a slightly more general form. We will prove that for a Noetherian domain with the property that every non-zero prime ideal is maximal, there exists a unique factorization of every ideal into primary ideals. Such a ring is called a Noetherian domain of (Krull-) dimension one.

Definition 7.1. A ring R where every non-zero prime ideal P is maximal is said to be of (Krull-) dimension one.

Theorem 7.2. *The unique factorization theorem. Let R be a Noetherian domain of dimension one. Then every non-zero ideal I in R can be uniquely expressed as a product of primary ideals which radicals are all distinct.*

Proof. Since R is Noetherian there exists an irredundant primary decomposition of I. Say $I = \bigcap_{i=1}^{n} Q_i$, where $rad(Q_i) = P_i$ and all the $P_i s$ are distinct.

Since P_i is prime for all i it is maximal by assumption. Since P_i and P_j are distinct maximal ideals for $i \neq j$ we must have that they are pairwise co-prime, since for any i, j with $i \neq j$ we have that $P_i \subset P_i + P_j$ which by the maximality of P_i implies that $P_i + P_j = (1)$. Furthermore, by Lemma 2.23 we have that $rad(Q_i + Q_j) = rad(rad(Q_i) + rad(Q_j)) = rad(P_i + P_j) = (1)$ this implies that $Q_i + Q_j = (1)$. By Theorem 2.16 we therefore have that $\bigcap_{i=1}^{n} Q_i = \prod_{i=1}^{n} Q_i$.

To show uniqueness note that since all the $P_i s$ are distinct *maximal* ideals, we have for each i that there is no $j \neq i$ such that P_j is contained in P_i. Therefore considering $\prod_{i=1}^{n} Q_i = \bigcap_{i=1}^{n} Q_i$, the maximality of the associated primes allows us to repeat the arguments given in the proof of the second uniqueness theorem 5.12. Explicitly, for every i choose $S = R - P_i$, then $S \bigcap P_j \neq \emptyset$ since $P_j \nsubseteq P_i$, for all $j \neq i$ and hence $(S^{-1}I)^c = Q_i$ by the proof of Theorem 5.11. This shows that the factorization is unique. [1][Proposition 9.1] □

7.1 Integrally closed domains

In this and following sections we assume that reader is familiar with the basics of field theory as given in a first course in abstract algebra, see [2][Chapters 6.1-6.4].

Definition 7.3. Let R be a subring of a commutative ring S.

An element $s \in S$ is integral over R if s satisfies a monic polynomial in R.

The ring S is said to be an integral extension of R if every element in S is integral over R.

An integral closure of R in S is the set of all elements in S which are integral over R.

The ring R is said to be integrally closed in S if R is equal to its integral closure in S.

We say that an integral domain is integrally closed if it is integrally closed in its field of fractions.

Proposition 7.4. *Let R be a subring of the field F. Let $\alpha \in F$ then the following are equivalent:*

i) α is integral over R

ii) $R[\alpha]$ is finitely generated as a R-module.

iii) $\alpha \in S$ where $S \subseteq F$ is a ring that is finitely generated as a R-module.

iiii) There exist a non-zero module M such that $\alpha M \subseteq M$, where $M \subseteq F$ is finitely generated as a R-module.

Proof. *i)* $\Rightarrow$ *ii)* since α is integral over R there exists $a_i \in R$ and $n \in \mathbb{N}$ such that $\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$ therefore $\alpha^n = -(a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0)$. Hence α^n and therefore all higher powers of α may be expressed as R-linear combinations of $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ which shows that $R[\alpha]$ is a finitely generated R-module. *ii)* $\Rightarrow$ *iii)* take $S = R[\alpha]$. *iii)* $\Rightarrow$ *iiii)* take $M = S$. *iiii)* $\Rightarrow$ *i)* Let $\{x_1, x_2, \cdots, x_r\}$ be a generating set for M. By assumption there exists $a_{ij} \in R$ such that $\alpha x_j = \sum_{i=1}^{r} a_{ij} x_i$ for all $j \in \{1, 2, \cdots, r\}$. Therefore, for each $j \in \{1, 2, \cdots, r\}$, we have that $\sum_{i=1}^{r} (a_{ij} - \alpha\delta_{ij}) x_i = 0$, where $\delta_{ij} = 1$

whenever $i = j$ and $\delta_{ij} = 0$ otherwise. Writing this equation in matrix form we get

$$\begin{bmatrix} a_{11} - \alpha & a_{21} & \dots & a_{r1} \\ a_{12} & a_{22} - \alpha & \dots & a_{r2} \\ \vdots & \vdots & \vdots & \vdots \\ a_{1r} & a_{2r} & \dots & a_{rr} - \alpha \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_r \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

In linear algebra *Cramers rule* states that if A is an $n \times n$ matrix and X, B are $1 \times n$ column matrices over a ring R then the equation $AX = B$ implies that $det(A)x_j = det(A_j)$ where x_j is the $j : th$ entry of X and (A_j) is the matrix obtained from A by replacing the elements in the $j : th$ column of A with the column matrix B. If we set $A = (a_{ij} - \alpha\delta_{i1})$ and use Cramers rule on the the equation above we get that $det(A)x_i = 0$ for $1 \leq i \leq r$. Since R is a domain this implies that $det(A) = 0$. We have that $det(A)$ is a monic polynomial in α with coefficients in R, hence this implies that α is integral over R. [7][Theorem 1.51] □

Corollary 7.5. *Let $R \subset S$ be rings. Let A be the integral closure of R in S. Then A is a subring of S.*

Proof. Let $\alpha, \beta \in A$ by Proposition 7.4 we have that $R[\alpha]$ and $R[\beta]$ are both finitely generated as R-modules, therefore $R[\alpha, \beta]$ is finitely generated. Since $\alpha \pm \beta$, $\alpha\beta$ belongs to $R[\alpha, \beta]$ the same Proposition implies that these are integral over R and hence belongs to A. This shows that A is a ring. □

Lemma 7.6. *Let $R \subset S \subset T$ be rings. If T is finitely generated as a S-module and S is finitely generated as a R-module then T is finitely generated as a R-module.*

Proof. Let $\{x_1, x_2 \cdots x_l\}$ generate S as a R-module and $\{y_1, y_2, \cdots, y_r\}$ generate T as a S-module. Let $t \in T$ and $b_i \in S$ be such that $t = \sum_{i=1}^{r} b_i y_i$. For each i let $a_{ij} \in R$ be such that $b_i = \sum_{j=1}^{l} a_{ij} x_j$, clearly this implies that $t = \sum_{i=1}^{r} \sum_{j=1}^{l} a_{ij} x_j y_i$ and hence $\{x_j y_i\}$, $1 \leq j \leq l, 1 \leq i \leq r$ is a generating set for T as a R-module. [6][Lemma 2.14] □

Lemma 7.7. *Let $R \subset S \subset T$ be integral domains such that T is an integral extension of S and S is an integral extension of R. Then T is an integral extension of R.*

Proof. Let $t \in T$. Since T is integral over S there exists $a_i \in S$ such that $t^n + a_{n-1}t^{n-1} + \cdots + a_1 t + a_0 = 0$. Since S is integral over R we have that $R_1 = R[a_1, a_2, \dots, a_n]$ is a finitely generated R-module. By construction t is integral over R_1 and hence $R_1[t]$ is finitely generated as a R_1-module, by Lemma 7.6 $R_1[t]$ is finitely generated as a R-module. This proves that t is integral over R. We have been using Proposition 7.4 repeatedly. [6][Proposition 2.15] □

Definition 7.8. A finite field extension K of $\mathbb{Q}$ is called a number field. An element α in $\mathbb{C}$ is called an algebraic number if α is algebraic over $\mathbb{Q}$. The set of all algebraic numbers in $\mathbb{C}$ will be denoted by $\overline{\mathbb{Q}}$. An element α in $\mathbb{C}$ is called an algebraic integer if α is integral over $\mathbb{Z}$. The ring of algebraic integers in a number field K (i.e the integral closure of $\mathbb{Z}$ in K) is denoted by $\mathcal{O}_K$.

Recall from a first course in Algebra that every finite field extension is an algebraic extension [2][Proposition 6.2.4]. Hence every element in a number field K is an algebraic number. However, every algebraic number is not an algebraic integer. In particular every algebraic number is algebraic over $\mathbb{Z}$, (multiply the minimal polynomial of α over $\mathbb{Q}$ with

the least common multiple of the denominators of the coefficients to get a polynomial over $\mathbb{Z}$ which satisfies α) but it might not satisfy any *monic* polynomial over $\mathbb{Z}$. Hence the difference between algebraic numbers and algebraic integers are that the later necessarily satisfies *monic* polynomials over $\mathbb{Z}$.

Proposition 7.9. *Let K be a number field. The ring $\mathcal{O}_K$ is integrally closed.*

Proof. Let $\alpha \in K$ be integral over $\mathcal{O}_K$, by Lemma 7.7 α is integral over $\mathbb{Z}$ hence this implies that $\alpha \in \mathcal{O}_K$. □

Proposition 7.10. *Let K be a number field. Then $\alpha \in K$ is an algebraic integer if and only if the minimal polynomial of α over $\mathbb{Q}$ has integer coefficients. In particular the algebraic integers in $\mathbb{Q}$ is equal to $\mathbb{Z}$.*

Proof. If the minimal polynomial of α over $\mathbb{Q}$ has integer coefficients then clearly α is an algebraic integer. Conversely, let $\alpha \in K$ be an algebraic integer and let $f(x) \in \mathbb{Z}[x]$ be the monic polynomial of least degree which satisfies α. If $f(x)$ is reducible over $\mathbb{Q}$ then $f(x)$ is reducible over $\mathbb{Z}$ by Gauss lemma [2][Theorem 4.4.5]. If $f(x) = g(x)h(x)$ over $\mathbb{Z}$ then this implies that α is a root of either $h(x)$ or $g(x)$, since $f(x)$ is monic any factor of $f(x)$ has to be monic as well, leading to a contradiction of the choice of $f(x)$ as the monic polynomial of minimal degree satisfying α. Hence $f(x)$ is irreducible over $\mathbb{Q}[x]$, showing that the minimal polynomial of α over $\mathbb{Q}$ has coefficients in $\mathbb{Z}$. Now, let $\beta \in \mathbb{Q}$, the minimal polynomial of β over $\mathbb{Q}$ is $x - \beta$ this polynomial has integer coefficients if and only if $\beta \in \mathbb{Z}$ which proves that the set of algebraic integers in $\mathbb{Q}$ is equal to $\mathbb{Z}$. [4][Section 15.3, Proposition 23] □

We have seen that the algebraic integers in $\mathbb{Q}$ are just the ordinary integers. In fact, this results holds for general number fields, i.e. if K is a number field then K is the field of fractions of the domain $\mathcal{O}_K$.

Proposition 7.11. *Let K be a number field. For every $\alpha \in K$ there exists some non-zero $n \in \mathbb{Z}$ such that $n\alpha$ belongs to $\mathcal{O}_K$. Hence K is the field of fractions of $\mathcal{O}_K$.*

Proof. Since α is algebraic over $\mathbb{Q}$ there exist $a_i \in \mathbb{Q}$ and $k > 0$ such that $\alpha^k + a_{k-1}\alpha^{k-1} + a_{k-2}\alpha^{k-2} + \cdots + a_1\alpha + a_0 = 0$. Let $n \in \mathbb{Z}$ be a common denominator of the coefficients a_i, then $(\alpha n)^k + a_{k-1}n(\alpha n)^{k-1} + a_{k-2}n^2(\alpha n)^{k-2} + \cdots + a_1 n^{k-1}(\alpha n) + a_0 n^k = 0$. Since all the coefficients above is in $\mathbb{Z}$ this proves the proposition. □

7.2 Dedekind domains

Definition 7.12. A Dedekind domain is a Noetherian, integrally closed domain of Krull dimension one.

Recall that we showed in Theorem 7.2 that in every Noetherian domain of dimension one there exists a unique factorization of every ideal into a product of primary ideals. Hence, in particular Theorem 7.2 applies to Dedekind domains. Further on we will prove that the ring $\mathcal{O}_K$ is a Dedekind domain for every number field K. As already noted this will have promising implications for unique factorization on the level of ideals in these rings. Actually, for Dedekind domains a stronger version of Theorem 7.2 holds, in Theorem 7.15 we will see that every primary ideal is a power of a prime ideal in a Dedekind domain. This implies that in these rings every ideal has a unique factorization into the product of prime ideals. To prove these results we will need to pass to the local ring D_P, hence the following lemma will be of importance.

Lemma 7.13. *Let S be a multiplicative set of the Dedekind domain D then $S^{-1}D$ is a Dedekind domain.*

Proof. Let J be a an ideal in $S^{-1}D$. By Proposition 5.4 we have that $J = S^{-1}I$ for some ideal I of R such that $I \cap S = \emptyset$, hence J is finitely generated whenever I is. If $S^{-1}P$ is a prime ideal in $S^{-1}D$ that is not maximal, then $S^{-1}P$ is properly contained in a prime ideal $S^{-1}Q$. The one to one correspondence between prime ideals in D and $S^{-1}D$ developed in Corollary 5.10 implies that P is a prime ideal properly contained in Q in D, leading to a contradiction. Hence every prime ideal of $S^{-1}D$ is maximal. Let $Q(D)$ be the field of fractions of D, then $Q(D)$ is the field of fractions of $S^{-1}D$. Let $\alpha \in Q(D)$ be integral over $S^{-1}D$. Let $a_i \in S^{-1}D$ be such that $\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$. Let $d \in D$ be a common multiple of the denominators of the a_i, then $d\alpha$ is integral over D and hence $d\alpha \in D$ by the assumption that D is integrally closed. By construction $\frac{1}{d} \in S^{-1}D$ and hence $\alpha = \frac{d\alpha}{d}$ belongs to $S^{-1}D$. Therefore $S^{-1}D$ is integrally closed. [6][Proposition 3.4] □

Proposition 7.14. *Let D be a Noetherian integrally closed domain with exactly one non-zero prime ideal P, i.e. D is a local Dedekind domain.* [1] *Then D is a principal ideal domain and every ideal in D is a power of P.*

Proof. Choose a non-zero non-unit $c \in D$. Consider $M = D/(c)$ as a D-module. Let $m \neq 0 \in M$. Consider the ideal $ann(m) = \{a \in D : am = 0\}$. For each nonzero $m \in M$ this is a proper ideal of D. Since D is Noetherian we may choose a $m \in M$ such that $ann(m)$ is maximal among the ideals of this form. Let $m = b + (c)$ and $P = ann(b + (c))$. Since $c \in P$, we have that P is non-zero. We will use the Noetherian argument to establish that P is prime. Assume that P is not prime, then there exists $x \notin P$, $y \notin P$ such that $xy \in P$. We have that $P = \{a \in D : c|ab\}$ and hence $x \notin P$ implies that $xb + (c) \neq 0 \in M$. Consider the ideal $I = ann(xb + (c))$, clearly $P \subseteq I$ and by construction $y \in I$, therefore P is properly contained in I, leading to a contradiction. We conclude that P is prime. We will now establish that P is principal by the following two observations:

i) $\frac{b}{c} \notin D$ since $b = \frac{b}{c}c$. And this would imply that $m = 0 \in M$

ii) $\frac{c}{b} \in D$ and $P = (\frac{c}{b})$. By definition $Pb \subseteq (c)$ and therefore $P\frac{b}{c} \subseteq D$ and this is an ideal in D, by the maximality of P we either have $P\frac{b}{c} \subseteq P$ or $P\frac{b}{c} = D$. If $P\frac{b}{c} \subseteq P$ then Proposition 7.4 implies that $\frac{b}{c}$ is integral over D, since P is finitely generated by the assumption that D is Noetherian. Since D is integrally closed in its field of fractions (to which the element $\frac{b}{c}$ clearly belongs) this implies that $\frac{b}{c} \in D$. By *i)* this results in a contradiction. Therefore $P\frac{b}{c} = D$, hence $(\frac{c}{b}) = P$. We have now proven that P is principal, set $\frac{c}{b} = \pi$, we will show that every ideal I of D is a power of $P = (\pi)$. Let I be a proper ideal of D, consider the sequence

$$I \subset I\pi^{-1} \subset I\pi^{-2} \subset I\pi^{-3} \subset \dots$$

If $I\pi^{-m} = I\pi^{-m-1}$ for some $m \in \mathbb{N}$ then $I\pi^{-m} = \pi^{-1}I\pi^{-m}$, since I is finitely generated $I\pi^{-m}$ is finitely generated as a D-module and hence Proposition 7.4 again implies that $\pi^{-1} \in D$ which again results in a contradiction by *i)* or simply because π is not a unit in D. Therefore the inclusion in the above sequence is strict and for the same reason this sequence can not be contained in D, since this would contradict the assumption that D is Noetherian. Let $n \in \mathbb{N}$ be such that $I\pi^{-n} \subseteq D$ but $I\pi^{-n-1} \nsubseteq D$. We have that $I\pi^{-n} \nsubseteq P$

[1] A local Dedekind domain is one of several equivalent definitions of a discrete valuation ring. A concept of great importance in algebraic geometry.

since otherwise each element in $I\pi^{-n}$ would be of the form $d\pi$, for some $d \in D$, which would imply that $I\pi^{-n-1} \subseteq D$. Hence $I\pi^{-n} = D$ which implies that $I = (\pi)^n$. [6][Proposition 3.2]

□

Theorem 7.15. *In a Dedekind domain D every primary ideal is a power of a prime ideal. Hence every ideal I in a Dedekind domain has a unique factorization into the product of prime ideals.*

Proof. Let Q be a P-primary ideal of D and consider the localization of D by P. Remember that $D_P = S^{-1}D$ where S is the multiplicative set $D - P$. In D_P the only maximal ideal is $S^{-1}P$ and by Lemma 7.13 we have that D_P is a Dedekind domain. Hence D_P is a Noetherian integrally closed domain with exactly one non-zero prime ideal, we may therefore use Proposition 7.14 to conclude that every ideal in D_P is of the form $(S^{-1}P)^n$. By Proposition 5.9 we know that S^{-1} commutes with products, hence we have that $(S^{-1}P)^n = S^{-1}(P^n)$. By Example 5.8 we have that $Q = Q^{ec}$. Since Q^e is an ideal of D_P, $Q^e = (S^{-1}P)^m$ for some $m > 0$, hence $Q = Q^{ec} = ((P^e)^m)^c = (P^m)^{ec} = P^m$ which proves the Theorem. The last equality follows from the fact that P^m is a primary ideal in D, which follows from Proposition 3.6 and the fact that P is a maximal ideal of D. The second statement in the theorem is now an immediate consequence of Theorem 7.2. □

In fact, historically, the property that every ideal in a Dedekind domain admits a unique factorization into prime ideals where taken as the defining property for these rings. It was Emmy Noether who first proved the equivalence of the existence of such a factorization and our definition 7.12. We have now learned about the existence of prime factorization of ideals in Dedekind domains, a result that we wish to apply to some specific rings fulfilling these conditions. Hence, our next task will be to prove that the ring of integers in a number field is a Dedekind domain. A result which requires some effort, but we will also gain some insight about the structure of number fields and their integers on the way.

7.3 Number fields

We will now discuss number fields a bit more, first we will remind the reader of the concepts of characteristic of a field and its prime subfield. Let $\Phi : \mathbb{Z} \to F$ be the homomorphism defined by $\Phi(1) = 1$. I.e. $\Phi(n) = 1 + 1 + \cdots + 1$ where the sum has n terms. If the additive group of F has infinite order then the kernel of Φ is trivial, otherwise the kernel is an ideal of $\mathbb{Z}$ and hence of the form $n\mathbb{Z}$ for some $n \in \mathbb{Z}$. Since the image of Φ is a subring of F, it is a integral domain. This implies that $n = p$ for a prime number p whenever Φ is not injective. We define the characteristic of the field F, denoted $Char(F)$ as $|ker(\Phi)|$, which by the discussion above is either zero or prime. The smallest subfield of F that contains 1 is called the prime subfield of F. Clearly the image of the homomorphism Φ is contained in the prime subfield of F. In the case where $Char(F)$ is equal to a prime number p the first isomorphism theorem implies that the prime subfield of F is isomorphic to $\mathbb{Z}/p\mathbb{Z}$. When the characteristic of F is equal to zero $\Phi(\mathbb{Z}) \cong \mathbb{Z}$ and hence the smallest field containing $\Phi(\mathbb{Z})$ is equal to the field of fractions of this domain and therefore, by the above isomorphism, isomorphic to $\mathbb{Q}$. If F and K are fields of the same characteristic then any homomorphism $\Phi : F \to K$ induces an isomorphism of the prime subfields of F and K. Hence if K is a number field then any homomorphism $\Phi : K \to \mathbb{C}$ has to be such that $\Phi(a) = a$ for all $a \in \mathbb{Q}$, we say that Φ fixes $\mathbb{Q}$ point vise.

Definition 7.16. Let K be a number field. A monomorphism $\Phi : K \to \mathbb{C}$ is called an embedding of K.

Note that any homomorphism of fields is a monomorphism since a field has no nontrivial ideal. The reader should recall some results about polynomials over $\mathbb{Q}$, see [2][Chapter 4.1-4.2], before continuing. In particular we shall use Proposition [2][4.2.11] which states that a polynomial $f(x)$ over $\mathbb{Q}$ has no repeated roots in $\mathbb{C}$ if and only if $GCD(f(x), f'(x)) = 1$, where $f'(x)$ denotes the derivative of $f(x)$. This result implies that an irreducible polynomial $p(x)$ over $\mathbb{Q}$ has no repeated roots.

Proposition 7.17. *Every irreducible polynomial $p(x)$ in $\mathbb{Q}[x]$ has only simple roots.*

Proof. Let $p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$, then $p'(x) = nx^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + a_1$, since $p(x)$ is irreducible it has no non-constant factor, hence $GCD(p(x), p'(x))$ is either one or zero, since $p'(x)$ is non-zero this implies that $GCD(p(x), p'(x)) = 1$. □

We will now show that number fields have a particular easy structure. We will show that every number field K is a simple extension of $\mathbb{Q}$, i.e. $K = \mathbb{Q}(\alpha)$ for some $\alpha \in K$. We will state a slightly more general result.

Definition 7.18. We say that an algebraic field extension F of E is separable over E if for each $\alpha \in F$ the minimal polynomial of α in E has no multiple roots.

Theorem 7.19. *Primitive element theorem. If F is a finite separable field extension of a field E of characteristic 0 then there exists an $\alpha \in F$ such that $F = E(\alpha)$. In particular, every number field K is a simple extension of $\mathbb{Q}$.*

Proof. It is sufficent to prove that the result holds for $F = E(u, v)$ since it then holds for $F = E(u_1, u_2, \cdots, u_n)$ by induction. Let $g(x), f(x)$ be the minimal polynomial of u, v over E respectively. Let $\{u = u_1, u_2, \cdots, u_r\}$ be the roots of $g(x)$ and $\{v = v_1, v_2, \cdots, v_s\}$ be the roots of $f(x)$. Let L be a field over which both $g(x)$ and $f(x)$ splits. Let $j \neq 1$ and consider the equation $u_i + av_j = u + av$, it has the unique solution $a = \frac{u-u_i}{v_j-v}$. Since E has characteristic 0, E has infinitely many elements and hence there exists an element $a \in E$ such that $u_i + av_j \neq u + av$, for all i and all $j \neq 1$, choose a as such. Let $\alpha = u + av$, clearly $E(\alpha) \subseteq E(u, v)$. We will prove the converse by proving that $v \in E(\alpha)$ from which it follows that $u = \alpha - av \in E(\alpha)$. Let $p(x)$ be the minimal polynomial of v over $E(\alpha)$, we will show that $p(x)$ is linear. Let $h(x) = g(\alpha - ax)$, then $h(x)$ has coefficients in $E(\alpha)$ and $h(v) = g(\alpha - av) = g(u) = 0$. By assumption $f(v) = 0$ and hence $p(x)$ is a common divisor of $h(x), f(x)$ over $E(\alpha)$. In L we have the factorization $f(x) = \prod_{j=1}^{s}(x - v_j)$. Since $u_i + av_j \neq u + av$ we have that $u_i \neq u + av - av_j$ for all $i, j \neq 1$, and therefore v_j is not a root of $h(x)$ for $j > 1$. Hence $(x - v)$ is the only common factor of $f(x)$ and $h(x)$ in L. Since $p(x)$ is a common factor of $f(x), h(x)$ in $E(\alpha)$, it is a common factor of the same in the extension L. This implies that $p(x)$ is linear and hence proves the Theorem. [2][Theorem 8.2.8] □

The above theorem is also true when the characteristic of E is non-zero, but the argument is different. Since we are concerned with number fields we have excluded this case.

Example 7.20. In this example we show that if K is a quadratic field extension of $\mathbb{Q}$, i.e. $[K : \mathbb{Q}] = 2$, then $K = \mathbb{Q}(\sqrt{D})$ for some square free integer D. Let $K = \mathbb{Q}(\alpha)$ be an extension of degree two over $\mathbb{Q}$. Let $p(x) = x^2 + bx + c$ be the minimal polynomial of α over

$\mathbb{Q}$. The roots of $p(x)$ are $\frac{1}{2}(\pm\sqrt{b^2-4c}-b)$. Set $D=b^2-4c$, clearly D is an integer since b,c are integers by Proposition 7.10, furthermore D is square free since $p(x)$ has no roots in $\mathbb{Q}$. Clearly $\mathbb{Q}(\alpha)\subseteq\mathbb{Q}(\sqrt{D})$. The minimal polynomial of D over $\mathbb{Q}$ is x^2-D and hence a degree argument proves that $\mathbb{Q}(\alpha)=\mathbb{Q}(\sqrt{D})$

Proposition 7.21. *If $K=\mathbb{Q}(\alpha)$ is a number field of degree d over $\mathbb{Q}$ then there exists d embeddings $\{\theta_1,\theta_2,\cdots,\theta_d\}$ of K in C. These are completely determined by there action on α. If the roots of the minimal polynomial $p(x)$ of α are $\{\alpha=\alpha_1,\alpha_2,\cdots,\alpha_d\}$ then for each $j\in\{1,2,\cdots,d\}$ we have $\theta_j(\alpha)=\alpha_j$.*

Proof. Suppose θ is an embedding of K in $\mathbb{C}$ with $\theta(\alpha)=\beta$. Let $p(\alpha)=\sum_{i=1}^{d}a_i\alpha^i$, $a_i\in\mathbb{Q}$. Since θ fixes $\mathbb{Q}$ point vise we have that $0=\theta(0)=\theta(\sum_{i=1}^{n}a_i\alpha^i)=\sum_{i=1}^{n}a_i\theta(\alpha)^i=\sum_{i=1}^{n}a_i\beta^i$. Which proves $\beta=\alpha_j$ for some $j\in\{1,2,\cdots,d\}$. Clearly θ is uniquely determined by its action on α, there are exactly d such choices by Proposition 7.17, hence there exists d embeddings of K in $\mathbb{C}$. Define $\theta_j:K\to\mathbb{C}$ by $\theta_j(f(\alpha))=f(\alpha_j)$, for all $f(x)\in K[x]$, it is sufficient to show that θ_j is well defined. If $f(\alpha)=g(\alpha)$ for $f,g\in K[x]$ then $f(\alpha)-g(\alpha)=0$ and hence $p(x)|f(x)-g(x)$. Since $p(\alpha_j)=0$, $1\le j\le d$ we have that $f(\alpha_j)-g(\alpha_j)=0$, i.e. $f(\alpha_j)=g(\alpha_j)$. [7][Theorem 1.29] □

Let $p(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0\in\mathbb{Q}[x]$ be the minimal polynomial of an algebraic number α_1. Let $\prod_{i=1}^{n}(x-\alpha_i)$ be a factorization of $p(x)$ in a splitting field of $p(x)$ over $\mathbb{Q}$. Expanding the terms in this product we see that $a_{n-1}=\pm\sum_{i=1}^{n}\alpha_i$ and $a_0=\pm\prod_{i=1}^{n}\alpha_i$. If α is an algebraic integer then $p(x)\in\mathbb{Z}[x]$ by Proposition 7.10 and in particular we have that $a_{n-1}=\pm\sum_{i=1}^{n}\alpha_i$ and $a_0=\pm\prod_{i=1}^{n}\alpha_i$ are elements in $\mathbb{Z}$.

Definition 7.22. Let K be a number field of degree d over $\mathbb{Q}$ and let θ_j, $1\le j\le d$, be the embeddings of K in $\mathbb{C}$. For each element $\alpha\in K$ we define the trace and the norm of α over K:

The trace of α over K is $T_K(\alpha)=\sum_{j=1}^{d}\theta_j(\alpha)$

The norm of α over K is $N_K(\alpha)=\prod_{j=1}^{d}\theta_j(\alpha)$

Since each embedding of K in $\mathbb{C}$ is a homomorphism the norm is multiplicative. I.e for any $\alpha,\beta\in K$ we have that $N_K(\alpha\beta)=N_K(\alpha)N_K(\beta)$. We will show that if $\alpha\in\mathcal{O}_K$ then $T_K(\alpha)$ and $N_K(\alpha)$ are both integers. Note that if $K=\mathbb{Q}(\alpha)$ then this follows from the discussion preceding the definition.

Proposition 7.23. *Let K be a number field of degree n over $\mathbb{Q}$, and $\alpha\in K$ with the degree $[\mathbb{Q}(\alpha):\mathbb{Q}]=d$. Let θ_j, $1\le j\le d$ be the embeddings of $\mathbb{Q}(\alpha)$ in $\mathbb{C}$. Let $p(x)$ be the minimal polynomial of α over $\mathbb{Q}$ with roots $\{\alpha=\alpha_1,\alpha_2,\cdots,\alpha_d\}$ Then $p(x)=x^d\pm T_{\mathbb{Q}(\alpha)}(\alpha)x^{d-1}+\cdots\pm N_{\mathbb{Q}(\alpha)}(\alpha)$ and $T_K(\alpha)=\sum_{j=1}^{d}\frac{n}{d}\alpha_j=\frac{n}{d}T_{\mathbb{Q}(\alpha)}(\alpha)$ and $N_K(\alpha)=\prod_{j=1}^{d}\alpha_j^{\frac{n}{d}}=(N_{\mathbb{Q}(\alpha)}(\alpha))^{\frac{n}{d}}$. In particular if $\alpha\in\mathcal{O}_K$ then $T_K(\alpha)$ and $N_K(\alpha)$ are both integers.*

Proof. Let $\theta(\alpha)=\alpha_j$, $1\le j\le d$. Since K is a simple extension of $\mathbb{Q}$ in particular it is a simple extension of $\mathbb{Q}(\alpha)$, say $K=\mathbb{Q}(\alpha)(\beta)$. Since any embedding ϕ of K in $\mathbb{C}$ permutes the roots of $p(x)$ the restriction $\phi\restriction_{\mathbb{Q}(\alpha)}=\theta_j$ for some $j\in\{1,2,\cdots,d\}$. Hence ϕ is an extension of θ_j. Let $q(x)$ be the minimal polynomial of β over $\mathbb{Q}(\alpha)$, then the degree of $q(x)$ is $\frac{n}{d}$ [2][Theorem 6.25]. Let $\{\beta=\beta_1,\beta_2,\cdots,\beta_{\frac{n}{d}}\}$ be the roots of $q(x)$. Let ϕ_{ij} be the embedding $\phi_{ij}\restriction_{\mathbb{Q}(\alpha)}=\theta_j$ and $\phi_{ij}(\beta)=\beta_i$, all embeddings of K in $\mathbb{C}$ are of this form. We have that $T_K(\alpha)=\sum_{j=1}^{d}\sum_{i=1}^{\frac{n}{d}}\phi_{ij}(\alpha)=\sum_{j=1}^{d}\frac{n}{d}\theta_j(\alpha)=\sum_{j=1}^{d}\frac{n}{d}\alpha_j=\frac{n}{d}T_{\mathbb{Q}(\alpha)}(\alpha)$

and $N_K(\alpha) = \prod_{j=1}^{d} \prod_{i=1}^{\frac{n}{d}} \phi_{ij}(\alpha) = \prod_{j=1}^{d} \theta_j(\alpha)^{\frac{n}{d}} \prod_{j=1}^{d} \alpha_j^{\frac{n}{d}} = (N_{\mathbb{Q}(\alpha)}(\alpha))^{\frac{n}{d}}$. By the remarks before the proposition we have that $p(x) = x^d \pm T_{\mathbb{Q}(\alpha)}(\alpha)x^{d-1} + \cdots \pm N_{\mathbb{Q}(\alpha)}(\alpha)$. If $\alpha \in \mathcal{O}_K$ then $p(x)$ has integer coefficients, hence $T_{\mathbb{Q}(\alpha)}(\alpha)$ and $N_{\mathbb{Q}(\alpha)}(\alpha)$ are integers which implies that $N_K(\alpha), T_K(\alpha)$ are integers (since $\frac{n}{d}$ is an integer). [7][Theorem 1.41] □

Example 7.24. Consider the ring $\mathbb{Z}[\sqrt{-5}]$, in example 3.15 we stated that this ring does not satisfy unique factorization. We have that $6 = 3 \times 2 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ in $\mathbb{Z}[\sqrt{-5}]$. We are now ready to show that this really is two different factorizations of 6 into irreducible elements. Since $\mathbb{Z}[\sqrt{-5}]$ is a subring of the number field $K = \mathbb{Q}(\sqrt{-5})$ we may use the multiplicativity of the norm of elements in this number field to easily prove that all of the elements which occur in the above factorization are really irreducible. Note that any element $\alpha = a+b\sqrt{-5}$ in $\mathbb{Z}[\sqrt{-5}]$ is an algebraic integer in K since $(x-(a+b\sqrt{-5})(x-(a-b\sqrt{-5}) = x^2 - 2ax + a^2 + 5b^2$ and this clearly is a monic polynomial satisfied by α over $\mathbb{Z}$. By the previous discussion we therefore have that $N_K(\alpha)$ is an integer for every $\alpha \in \mathbb{Z}[\sqrt{-5}]$. Assume that 2 has a non-trivial factorization in the ring $\mathbb{Z}[\sqrt{-5}]$, i.e. $2 = (a + b\sqrt{-5})(c + d\sqrt{-5})$ then $N_K(2) = 4 = N_K(a + b\sqrt{-5})N_K(c + d\sqrt{-5}) = (a^2 + 5b^2)(c^2 + 5d^2)$, where both factors are integers. Clearly $(a^2 + 5b^2) \neq 2$ for $a, b \in \mathbb{Z}$ since this would contradict the irrationality of $\sqrt{2}$. Hence either $(a^2 + 5b^2) = 1$ or $(c^2 + 5d^2) = 1$ this implies that one of the factors above is trivial, since the equation $(a^2 + 5b^2) = 1$ only has two integral solutions, $a = \pm 1, b = 0$, hence any factorization of 2 is trivial, that is, if $2 = pq$ then this implies that either p or q is a unit. The same argument applies to the element 3, since $(a^2 + 5b^2) = 3$ for $a, b \in \mathbb{Z}$ would contradict the irrationality of $\sqrt{3}$. Furthermore, we have that $N_K(1+\sqrt{-5}) = N_K(1-\sqrt{-5}) = 6$ and hence any non trivial factorization of $(1 \pm \sqrt{-5})$ in $\mathbb{Z}[\sqrt{-5}]$ would result in the contradictions $(a^2 + 5b^2) = 3$ and $(c^2 + 5d^2) = 2$, hence the two factorizations above really yields different factorization of 6 into irreducibles in this ring. We conclude that $\mathbb{Z}[\sqrt{-5}]$ is not a UFD.

Definition 7.25. Let K be a number field of degree d over $\mathbb{Q}$ and let θ_j, $1 \leq j \leq d$, be the embeddings of K in $\mathbb{C}$. Let $\Omega = \{\beta_1, \beta_2, \cdots \beta_{d-1}\}$ be a basis for K over $\mathbb{Q}$. We define the discriminant of Ω denoted $disc(\Omega)$ as the square of the determinant of the matrix $(\theta_j(\beta_i))$, which has $\theta_j(\beta_i)$ on the $i : th$ row and the $j : th$ column.

Recall from linear algebra that the determinant of a matrix is multiplicative and that the determinant of a matrix B equal the determinant of the transpose of the same matrix B^t. That is, for matrices A and B we have $det(AB) = det(A)det(B)$ and $det(B) = det(B^t)$. Using this fact we can characterize the discriminant of the basis Ω in the following way.

Lemma 7.26. *Let K be a number field of degree d over $\mathbb{Q}$ and let θ_j, $1 \leq j \leq d$, be the embeddings of K in $\mathbb{C}$. Let $\Omega = \{\beta_1, \beta_2, \cdots \beta_{d-1}\}$ be a basis for K over $\mathbb{Q}$. Then $disc(\Omega)$ is equal to the determinant of the matrix $(T_K(\beta_i\beta_j))$, which has $T_K(\beta_i\beta_j)$ on the $i : th$ row, $j : th$ column. In particular, if $\Omega \subset \mathcal{O}_K$ then $disc(\Omega)$ is an integer.*

Proof. Let B denote the matrix $(\theta_j(\beta_i))$. We have that $disc(\Omega) = (det(B))^2 = det(B)det(B^t) = det(BB^t) = det((\sum_{n=1}^{d} \theta_n(\beta_i\beta_j)) = det(T_K(\beta_i\beta_j))$. By earlier remarks $T_K(\beta_i\beta_j)$ is an integer whenever $\beta_i\beta_j \in \mathcal{O}_K$. This proves the lemma. [7][Theorem 1.65] □

Lemma 7.27. *Let $A = \{\alpha_1, \alpha_2, \ldots, \alpha_d\}$ be a basis for K over $\mathbb{Q}$. If $B = \{\beta_1, \beta_2, \cdots, \beta_d\}$ is another basis for K over $\mathbb{Q}$ such that $\beta_i = \sum_{k=1}^{d} q_{ik}\alpha_k$, for $1 \leq i \leq d$, then $disc(B) = D^2 disc(A)$. Where D is the determinant of the matrix (q_{ik}).*

Proof. Let θ_j denote the embeddings of K in $\mathbb{C}$ for $1 \leq j \leq d$. We have that $\theta_j(\beta_i) = \sum_{k=1}^{d} q_{ik}\theta_j(\alpha_k)$. Hence the matrix $(\theta_j(\beta_i))$ is equal to the product of the matrix (q_{ik}) with the matrix $(\theta_j(\alpha_i))$. Hence $disc(B) = (det((\theta_j(\beta_i))))^2 = (det((q_{ik})(\theta_j(\alpha_i))))^2 = D^2 disc(A)$ where the last equality follows from that the determinant function is multiplicative.[7][Theorem 1.63] □

Using the two lemmas above we are now ready to prove that $\mathcal{O}_K$ is a Noetherian ring for every number field K.

Theorem 7.28. *Let $K = \mathbb{Q}(\alpha)$ be a number field of degree d over $\mathbb{Q}$. Then $\mathcal{O}_K$ is a finitely generated $\mathbb{Z}$-module with a basis consisting of d elements. In particular $\mathcal{O}_K$ is a Noetherian ring.*

Proof. The set $\{1, \alpha, \alpha^2, \cdots, \alpha^{d-1}\}$ is a basis for K over $\mathbb{Q}$. By Proposition 7.11 there exists an integer n such that $n\alpha$ is an element of $\mathcal{O}_K$. Clearly the set $\{n^{d-1}, n^{d-1}\alpha, n^{d-1}\alpha^2, \cdots, n^{d-1}\alpha^{d-1}\}$ is linearly independent over $\mathbb{Q}$ and hence a basis for K over $\mathbb{Q}$. This establishes the existence of a basis for K over $\mathbb{Q}$ consisting of elements in $\mathcal{O}_K$. Consider all basis Ω of K such that $\Omega \subset \mathcal{O}_K$. All such basis have an integer discriminant by lemma 7.26, choose a basis $B = \{b_1, b_2, \cdots, b_d\}$ with $|disc(B)|$ minimal. Since B is a basis of K over Q it is in particular a basis for $\mathcal{O}_K$, it is left to prove that there exists such a basis as a $\mathbb{Z}$-module. Assume B is not a $\mathbb{Z}$ basis for $\mathcal{O}_K$, then there exists $\gamma \in \mathcal{O}_K$ such that $\gamma = \sum_{i=1}^{d} q_i b_i$ and at least one $q_i \notin \mathbb{Z}$, assume $q_1 \notin \mathbb{Z}$. Thus $q_1 = \lfloor q_1 \rfloor + r$, $0 < r < 1$, where $\lfloor q_1 \rfloor$ denotes the greatest integer less than or equal to q_1. Set $\delta = \gamma - \lfloor q_1 \rfloor b_1 = rb_1 + \sum_{i=2}^{d} q_i b_i$. We will show that $B_1 = \{\gamma, b_2, \cdots, b_d\}$ is a basis for K. The matrix

$$A = \begin{bmatrix} r & q_1 & \dots & q_d \\ 0 & 1 & \dots & 0 \\ \vdots & & \vdots & \vdots \\ 0 & 0 & \dots & 1 \end{bmatrix}$$

has determinant $r \neq 0$. Since A is the matrix given by the coefficients of $\{\gamma, b_2, \cdots, b_d\}$ in the basis B, the elements $\{\gamma, b_2, \cdots, b_d\}$ are linearly independent and hence B_1 is a basis for K. Clearly $\gamma \in \mathcal{O}_K$, hence $B_1 \subset \mathcal{O}_K$. We have that $disc(B_1) = (det(A))^2 disc(B) = r^2 disc(B)$. Since $0 < r < 1$ this contradicts the minimality of $|disc(B)|$. Therefore $q_i \in \mathbb{Z}$, $1 \leq i \leq d$, and B is a basis for $\mathcal{O}_K$ as a $\mathbb{Z}$-module. Since $\mathcal{O}_K$ is a finitely generated $\mathbb{Z}$-module, Proposition 6.8 implies that every submodule of $\mathcal{O}_K$ is finitely generated as a $\mathbb{Z}$-module. In particular, this implies that every submodule is finitely generated as a $\mathcal{O}_K$-module and that $\mathcal{O}_K$ is Noetherian as a module over itself, i.e. $\mathcal{O}_K$ is a Noetherian ring. [7][Theorem 1.69] □

Example 7.29. Let $K = \mathbb{Q}(\sqrt{D})$, for a square free integer D. In this example we will find a basis for the ring $\mathcal{O}_K$ as a $\mathbb{Z}$-module. Define

$$\omega = \begin{cases} \sqrt{D} & \text{if } D \equiv 2, 3 \bmod 4 \\ \frac{1+\sqrt{D}}{2} & \text{if } D \equiv 1 \bmod 4 \end{cases}$$

We will prove that $\mathcal{O}_K = \mathbb{Z}[w]$, i.e $\{1, w\}$ is a basis for $\mathcal{O}_K$ as a $\mathbb{Z}$-module. If $D \equiv 2, 3 \bmod 4$ then $x^2 - D$ is a monic polynomial with integer coefficients that satisfy ω. If $D \equiv 1 \bmod 4$ then $\frac{1-D}{4} \in \mathbb{Z}$ and $x^2 - x - \frac{1-D}{4}$ is a monic polynomial in $\mathbb{Z}[x]$ witch satisfies ω. Therefore $\mathbb{Z}[w] \subseteq \mathcal{O}_K$. Conversely, let $\alpha \in \mathcal{O}_K$ then $\alpha = a + b\sqrt{D}$, $a, b \in \mathbb{Q}$, has a minimal polynomial

over $\mathbb{Q}$ with integer coefficients. If $b = 0$ then this implies $a \in \mathbb{Z}$. Assume $b \neq 0$, then we have that $x^2 - 2ax + a^2 - b^2D$ is the minimal polynomial of α over $\mathbb{Q}$. This implies that $2a \in \mathbb{Z}$ and $a^2 - b^2D \in \mathbb{Z}$, therefore $4(a^2 - b^2D) = (2a)^2 - (2b)^2D \in \mathbb{Z}$. Since $2a \in \mathbb{Z}$ this implies that $(2b)^2D \in \mathbb{Z}$, if $2b \in \mathbb{Q} - \mathbb{Z}$ then this would contradict the assumption that D is square free, hence $2b \in \mathbb{Z}$. Therefore $2a, 2b \in \mathbb{Z}$. Set $a = \frac{x}{2}$, $b = \frac{y}{2}$, $x, y \in \mathbb{Z}$. Then $a^2 - b^2D \in \mathbb{Z}$ implies that $\frac{x^2 - y^2D}{4} \in \mathbb{Z}$, i.e. $x^2 - y^2D \equiv 0 \bmod 4$. The only squares modulo 4 are 0 and 1. Assume that $D \equiv 2 \bmod 4$, then $x^2 - y^2D \equiv 0 \bmod 4$ implies $x^2 - 2y^2 \equiv 0 \bmod 4$, which happens if and only if $x^2 \equiv y^2 \equiv 0 \bmod 4$. This can only happen if x and y are both even. The same is true when $D \equiv 3 \bmod 4$ since this implies, by the same argument, that $x^2 - 3y^2 \equiv 0 \bmod 4$, which is true if and only if $x^2 \equiv y^2 \equiv 0 \bmod 4$. Hence $D \equiv 2, 3 \bmod 4$ implies that x, y are both divisible by 2 and hence that $a, b \in \mathbb{Z}$, which means that $\alpha \in \mathbb{Z}[\sqrt{\omega}]$ and therefore $\mathcal{O}_K \subseteq \mathbb{Z}[\sqrt{\omega}]$ in this case. Assume $D \equiv 1 \bmod 4$ then $x^2 - y^2D \equiv 0 \bmod 4$ implies $x^2 - y^2 \equiv 0 \bmod 4$ which is true if and only if $x^2 \equiv y^2 \equiv 1 \bmod 4$ or $x^2 \equiv y^2 \equiv 0 \bmod 4$. This holds whenever x and y are both odd or both even. This implies that a, b are either both integers or both half integers. In any case $\alpha \in \mathbb{Z}[\sqrt{\omega}]$. We conclude that $\mathcal{O}_K = \mathbb{Z}[\sqrt{\omega}]$.

Proposition 7.30. *Let S be a domain and let $R \subset S$ be a subring of S such that S is an integral extension of R. Then S is a field if and only if R is a field.*

Proof. Assume that R is a field. Let $s \neq 0 \in S$, since S is integral over R there exists $a_i \in R$ such that $s^n + a_{n-1}s^{n-1} + \cdots + a_1 s + a_0 = 0$. By assumption S is a domain and we may therefore assume $a_0 \neq 0$ because otherwise we may cancel s until we get a non-zero constant term. Since R is a field $-a_0$ has an inverse, therefore $s((-a_0)^{-1}(s^{n-1} + an - 1s^{n-2} + \cdots + a_1)) = 1$ and hence s is invertible. Assume that S is a field and let $r \neq 0 \in R$ then $r^{-1} \in S$. Since S is an integral extension of R there exist $a_i \in R$ and $m \in \mathbb{N}$ such that $r^{-m} + a_{m-1}r^{-m+1} + \cdots + a_1 r^{-1} + a_0 = 0$. Multiplying this equation by r^{m-1} gives that $r^{-1} = -(a_{m-1} + a_{m-2}r + \cdots + a_1 r^{m-2} + a_0 r^{m-1})$. Hence $r^{-1} \in R$ since the right hand side clearly is an element in R. [4][Section 15.3, Theorem 21 (1)] □

Corollary 7.31. *Let $R \subset S$ be rings such that S is an integral extension of R. Then a prime ideal $Q \subset S$ is a maximal ideal of S if and only if $P = R \bigcap Q$ is a maximal ideal of R.*

Proof. We will prove that S/Q is an integral extension of R/P and the result will then follow from Proposition 7.30. Consider the following diagram, where π denotes natural projections and i denotes embeddings:

$$\begin{array}{ccc} R & \xrightarrow{\pi_1} & R/P \\ i\downarrow & & i\downarrow \\ S & \xrightarrow{\pi_2} & S/Q \end{array}$$

For any $r \in R$ we have that $i(\pi_1(r)) = \pi_2(i(r))$. Let $\overline{s} \in S/Q$, since S is integral over R there exists a monic polynomial $p(x)$ with coefficients in R such that $p(s) = 0$, clearly this implies that $\pi_1(p(s)) = 0$ in R/P. Furthermore $\pi_1(p(x))$ is monic. Since $p(x)$ has coefficients in R we have that $i(\pi_1(p(x))) = \pi_2(i(p(x)))$. Let $\overline{p(x)} = \pi_2(i(p(x)))$ be the image of $p(x) \in S/Q$ then $\overline{p(\overline{s})} = \pi_2(i(p(s))) = i(\pi_1(p(s))) = 0$ and hence $\overline{s}$ is a root of $\pi_1(p(x))$. [4][Section 15.3, Theorem 21 (2)] □

Theorem 7.32. *The ring $\mathcal{O}_K$ of integers in a number field K is a Dedekind domain.*

Proof. By the discussion so far it is sufficient to prove that every prime ideal is a maximal ideal in $\mathcal{O}_K$. Let Q be a prime ideal in $\mathcal{O}_K$, consider the embedding $i : \mathbb{Z} \to \mathcal{O}_K$. Then $\mathbb{Q}^c = \mathbb{Z} \bigcap Q$ is a prime ideal $P \subset \mathbb{Z}$. Assume that Q is non-zero, and let $\alpha \neq 0 \in Q$, then $N_K(\alpha) \in \mathbb{Z} \bigcap Q$ since $\mathcal{O}_K$ is integral over $\mathbb{Z}$. Furthermore $N_K(\alpha)$ is non-zero, since α being non-zero implies that 0 is not a root of the minimal polynomial $p(x)$ of α. If $p(0) = 0$ then this implies that x divides $p(x)$ which contradicts that $p(x)$ is irreducible. This proves that P is non-zero and hence $P = p\mathbb{Z}$ for some prime p. By Corollary 7.31 Q is a maximal ideal of $\mathcal{O}_K$ if and only if P is maximal in $\mathbb{Z}$. Since P is a non-zero prime ideal in $\mathbb{Z}$ we have that P is a maximal ideal in $\mathbb{Z}$ and hence it follows that every prime ideal Q in $\mathcal{O}_K$ is maximal. [4][Section 16.3, Proposition 14 (2)] □

Example 7.33. We return in this example to the ring $\mathbb{Z}[\sqrt{-5}]$. Since $-5 \equiv 3 \bmod 4$ we have that $\mathbb{Z}[\sqrt{-5}] = \mathcal{O}_K$, for $K = \mathbb{Q}(\sqrt{-5})$. By Theorem 7.32 $\mathbb{Z}[\sqrt{-5}]$ is a Dedekind domain and therefore there exists an unique decomposition of the ideal $(6) = (3)(2) = (1-\sqrt{-5})(1+\sqrt{-5})$ into prime ideals. In particular $(2), (3), (1-\sqrt{-5}), (1+\sqrt{-5})$ are not prime ideals in this ring. In this example we will find the unique prime factorization of the ideal (6) in $\mathbb{Z}[\sqrt{-5}]$. Consider the ideals:

$$P_1 = (2, 1-\sqrt{-5}), P_2 = (2, 1+\sqrt{-5}), Q_1 = (3, 1-\sqrt{-5}), Q_2 = (3, 1+\sqrt{-5})$$

We have that $P_1P_2 = (2, 1-\sqrt{-5})(2, 1+\sqrt{-5}) = (4, 2(1-\sqrt{-5}), 2(1+\sqrt{-5}), 6) = (2)$ and similarly that $Q_1Q_2 = (3, 1-\sqrt{-5})(3, 1+\sqrt{-5}) = (3)$. Furthermore $P_1Q_1 = (2, 1-\sqrt{-5})(3, 1-\sqrt{-5}) = (6, 2(1-\sqrt{-5}), 3(1-\sqrt{-5})) = (1-\sqrt{-5})$ and similarly $P_2Q_2 = (1+\sqrt{-5})$. Therefore the seemingly different factorizations of the ideal (6) are not different, $(6) = (3)(2) = Q_1Q_2P_1P_2 = P_2Q_2P_1Q_1 = (1-\sqrt{-5})(1+\sqrt{-5})$. It is time to show that P_i, Q_i are prime ideals for $i = 1, 2$. Consider $\mathbb{Z}[\sqrt{-5}]/P_i$, for $i = 1, 2$. For any $\alpha = a + b\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$, we have that $a + b\sqrt{-5} = a \pm b \pm b(1 \pm \sqrt{-5})$. Therefore the image of $a + b\sqrt{-5}$ under the natural projection $\Phi : \mathbb{Z}[\sqrt{-5}] \to \mathbb{Z}[\sqrt{-5}]/P_i$ is $a \pm b + (2, 1 \pm \sqrt{-5})$. We conclude that $\mathbb{Z}[\sqrt{-5}]/P_i \cong \mathbb{Z}_2$ for $i = 1, 2$. In particular P_1, P_2 are prime ideals. Similarly we consider $\mathbb{Z}[\sqrt{-5}]/Q_i$, for $i = 1, 2$. Using the same argument as above we find that $\mathbb{Z}[\sqrt{-5}]/Q_i \cong \mathbb{Z}_3$ and hence Q_1, Q_2 are prime ideals.

We will end this paper with some indications on how to develop a divisibility theory for ideals in a Dedekind Domain similarly to the divisibility theory that exists for elements in $\mathbb{Z}$.

Definition 7.34. Let D be a domain and I, J ideals, we say that I divides J (we write $I|J$) if there exists an ideal $A \subset D$ such that $J = IA$. We say that an ideal J is unfactorable if it has no no non-trivial factorization, i.e. $J = IA$ implies $I = R$ or $A = R$.

Proposition 7.35. *Suppose that D is a Dedekind domain and I, J are two non-zero ideals in D, with prime factorization $I = P_1^{\alpha_1}P_2^{\alpha_2}\dots P_k^{\alpha_k}$ and $J = P_1^{\beta_1}P_2^{\beta_2}\dots P_k^{\beta_k}$, for $\alpha_i, \beta_i \geq 0$, $1 \leq i \leq k$. Then*

i) $J \subseteq I$ iff $I|J$ iff $\alpha_i \leq \beta_i$, for $1 \leq i \leq k$.

ii) $I+J = P_1^{min(\alpha_1,\beta_1)}P_2^{min(\alpha_2,\beta_2)}\dots P_k^{min(\alpha_k,\beta_k)}$ and in particular I, J are coprime ($I+J = R$), if and only if I, J have no common divisors.

iii) P is a prime ideal iff $P|IJ$ implies that $P|I$ or $P|J$

Proof. *i*) If $I|J$ then there exists an ideal $A \subset D$ such that $J = IA$, looking at the prime factorization of J it is evident that this implies $\alpha_i \leq \beta_i$, for $1 \leq i \leq k$. Converserly, if $\alpha_i \leq \beta_i$, for $1 \leq i \leq k$ let A be the ideal $P_1^{\beta_1-\alpha_1}P_2^{\beta_2-\alpha_2}\dots P_k^{\beta_k-\alpha_k}$ then $J = IA$. It is also evident that $\alpha_i \leq \beta_i$, for $1 \leq i \leq k$ if and only if $J \subseteq I$. This proves *i*). *ii*) Since $I + J$ is the smallest ideal containing both I and J *ii*) follows from *i*). *iii*) By *i*) an equivalent statement is that P is prime if and only if $IJ \subset P$ implies that $I \subset P$ or $J \subset P$. Assume that $IJ \subset P$ does not imply that $I \subset P$ or $J \subset P$. Let $x \in P - I$, $y \in P - J$ then $xy \in IJ$ which implies that P is not prime. Conversely, assume that P is not prime. Then there exists $xy \in P$ with $x \notin P$, $y \notin P$ and hence $(x)(y) \subseteq P$ but $(x) \nsubseteq P$, $(y) \nsubseteq P$. This proves the Proposition. [4][Section 16.3, Proposition 17] □

Definition 7.36. Let D be a dedekind domain and let I, J be ideals. We define $GCD(I, J)$ to be the ideal $I + J$. That is $GCD(I, J)$ is a divisor of I and J and is such that any common divisor of I, J is a divisor of $GCD(I, J)$

Proposition 7.35 implies that $GCD(I, J) = I + J = 1$ if and only if I and J have no common divisors.

References

[1] Atiyah, M.F., and Macdonald, I.G. 1969.

Introduction to commutative Algebra

Reading, Massachusetts. Menlo Park, California, London-Don Mills, Ontario, Addison-Wesley publishing company.

[2] Beachy, J.A and Blair, D.W. 3rd edn. 2006.

Abstract Algebra

United States, Long Grove, Waveland Press, Inc.

[3] Cox, D., Little, J., and O'Shea, D. 2nd edn. 1997

IDEALS, VARIETIES, AND ALGORITHMS- An Introduction to Computational Algebraic Geometry and Commutative Algebra

United States, Springer-Verlag New York, Inc.

[4] Dummit, D.S, and Foote, R.M. 2nd edn. 1999

ABSTRACT ALGEBRA

United States, Library of Congress Cataloging-in-Publication Data.

[5] Eisenbud, D., 1995

Commutative Algebra with a view towards algebraic geometry

New York, Graduate Texts in Mathematics, Springer-Verlag.

[6] Milne, J.S, 2013

Algebraic Number Theory (v3.05)

Available at www.jmilne.org/math/

[7] Mollin, R.A, 1999

Algebraic number theory

United states, Florida, CRC Press LLC.

[8] Northcott, D.G. 1968

Lessons on rings, modules and multiplicities

Cambridge, Cambridge University Press.

[9] Reid, M. 1995

Undergraduate Commutative Algebra

Cambridge, Cambridge University Press.

[10] Algebra 3, 7.5 ECTS, University of Stockholm

Including [2][Sections; 1.1-6.5 and 9.1-9.2]