Algebra I:
Commutative Algebra

Alexander Schmitt

Berlin, Winter 2012/2013

Table of Contents

Preface

The present text contains notes on my course "Algebra I" at Freie Universität Berlin during the winter term 2012/2013. The course "Algebra I" is part of a cycle of three courses providing an introduction to algebraic geometry. It is also meant as a continuation of my course "Algebra und Zahlentheorie" (see [30]).

The basic objects we will be studying are commutative rings and their ideals. There are many different motivations for looking at these objects. A ring can be, for example, viewed as a domain of numbers with which we would like to compute. In certain situations, ideals are valuable generalizations of numbers.[1] A ring can also consist of regular functions on an affine algebraic variety. If we consider algebraic varieties over an algebraically closed field such as the field of complex numbers, then this algebra completely determines the variety. Ideals in the algebra correspond to subvarieties, e.g., points of the variety. It is one of the merits of commutative algebra that it provides a unified framework for, among other things, arithmetic and algebro-geometric investigations.

The first chapter presents the language of rings and their ideals. Many operations on rings and ideals which will be used throughout the text are presented. I would like to highlight two topics: The first one is the section on factorial rings. It shows how we may generalize the main theorem of elementary number theory, i.e., the unique factorization of natural numbers into powers of prime numbers, to other settings and problems which will usually occur. The second one is the spectrum of a ring. It attaches to a commutative ring a geometric object. This is a fundamental construction of modern algebraic geometry.

Noetherian rings are rings which satisfy a crucial finiteness condition. This condition is fulfilled by important rings occuring in number theory and algebraic geometry, such as orders in number fields and coordinate algebras of algebraic varieties. A central result is the decomposition of ideals in noetherian rings into primary ideals and its uniqueness properties. This is a vast generalization of the main theorem of elementary number theory and has also an important geometric interpretation.

As the main topic of the courses "Algebra I-III" is algebraic geometry, the remaining two chapters deal with subjects of a more geometric nature. The third chapter focusses on Hilbert's Nullstellensatz. The Nullstellensatz provides the dictionary between finitely generated algebras over an algebraically closed field k and their (radical) ideals on the one hand and algebraic varieties defined over k and their subvarieties on the other hand. It explains the fundamental role of commutative algebra in algebraic geometry. We present an elementary proof due to Munshi. Another central topic is Noether's normalization

[1] This is an idea of Kummer.

theorem which supplies important information on the structure of algebraic varieties and will be used over and over again in the fourth chapter. The third chapter also develops the notion of modules over a ring.

The fourth chapter begins the study of the geometry of algebraic varieties. The Krull dimension of a ring is introduced and investigated. If the ring in question is the coordinate algebra of an affine algebraic variety, this provides a basic geometric invariant. We will check various properties which we intuitively expect from the notion of dimension. Finally, we will study singularities of algebraic varieties. In this context, we will also discuss the relation between the intricate notion of normality of rings and affine algebraic varieties and singularities.

Dr. Juan Pons Llopis and Anna Wißdorf proofread the manuscript and suggested various corrections and improvements. The biographical data of mathematicians were taken from WIKIPEDIA. These notes are heavily based on the books [1] and [14]. Other important sources are [4], [8], and [11].

Alexander Schmitt
Berlin, March 2013

I

Basic Theory of Rings and their Ideals

In an introductory course on linear algebra, one usually works over fields. In commutative algebra, fields are replaced by more general objects, namely commutative rings with identity element. In linear algebra, you rarely talk about the fields themselves. Certainly, you can do some explicit computations over the field of rational numbers or finite fields, and, for the theory of the Jordan normal form, you need the ground field to be algebraically closed. Apart from that, you don't worry much about the "internal" structure of the field. In various respects, rings have a much richer structure than fields. To begin with, you should think of the ring of integers $\mathbb{Z}$ or the polynomial ring $k[x]$ over a field k. In these rings, you may investigate when a number or a polynomial divides another one. This leads you to certain "indivisible" objects which you call prime numbers or irreducible polynomials. In fields, there are no counterparts to these concepts, because any non-zero element is a unit. During the development of algebra, it turned out that it is more useful to work with ideals than with the ring elements themselves.[1] In this section, we will first define rings and look at some basic examples. Then, we will develop the notion of ideals and explain how to compute with them. As a motivation in Kummer's[2] spirit, we will also look at prime factorization. In that context, we will see its failure in some rings and the class of factorial rings in which prime factorizations do exist.

I.1 Rings

A *ring* is a tuple $(R, 0, +, \cdot)$ which consists of an abelian group $(R, 0, +)$ (see [30], Definition II.1.1 and II.1.4) and a map

$$\begin{array}{rcl} \cdot\colon R \times R & \longrightarrow & R \\ (a, b) & \longmapsto & a \cdot b \end{array}$$

[1] The term ideal goes back to Kummer's notion of "ideale Zahl", an extension of the concept of number or ring element that permits to generalize the prime factorization in the ring of integers to some rings such as $\mathbb{Z}[\sqrt{-5}]$ (see Section I.5).

[2] Ernst Eduard Kummer (1810 - 1893) was a German mathematician.

which is **associative**, i.e.,

$$\forall a, b, c \in R: \quad a \cdot (b \cdot c) = (a \cdot b) \cdot c,$$

such that the **distributive laws** hold, i.e.,

$$\begin{aligned} \forall a, b, c \in R: \quad a \cdot (b + c) &= a \cdot b + a \cdot c, \\ (a + b) \cdot c &= a \cdot c + b \cdot c. \end{aligned}$$

We will refer to "+" as the *addition* and to "$\cdot$" as the *multiplication*. In the sequel, we will write R rather than $(R, 0, +, \cdot)$ for the datum of a ring.

A ring R is called *commutative*, if

$$\forall a, b \in R: \quad a \cdot b = b \cdot a.$$

An element 1 in a ring R is an *identity element*, if

$$\forall a \in R: \quad 1 \cdot a = a = a \cdot 1.$$

I.1.1 Note. A ring R can have at most one identity element. For, if $1, 1' \in R$ are identity elements, we have

$$1 = 1 \cdot 1' = 1'.$$

Let R be a ring. For $a \in R$, we let $-a$ be the additive inverse of a, i.e., the element for which $a + (-a) = 0$ holds.

I.1.2 Properties. *Let R be a ring.*

i) *For $a \in R$, we have $a \cdot 0 = 0 \cdot a = 0$.*

ii) *For $a, b \in R$, we have $(-a) \cdot b = -(a \cdot b) = a \cdot (-b)$. In particular, $(-a) \cdot (-b) = a \cdot b$.*

Proof. i) We use $0 = 0 + 0$, so that

$$0 \cdot a = (0 + 0) \cdot a = 0 \cdot a + 0 \cdot a.$$

Add $-(0 \cdot a)$ to both sides to get

$$0 = 0 + 0 \cdot a = 0 \cdot a.$$

Similarly, one shows $a \cdot 0 = 0$.

ii) Using i), we see

$$a \cdot (-b) + a \cdot b = a \cdot (-b + b) = a \cdot 0 = 0.$$

Thus, $a \cdot (-b) = -(a \cdot b)$. In the same vein, one shows $(-a) \cdot b = -(a \cdot b)$. □

I.1.3 Examples. i) $R = \{0\}$ with the only possible addition and multiplication is a ring with identity element $1 = 0$. (It is not a field (compare [30], Definition III.1.1.)!) Note that R is the only ring with identity element in which $1 = 0$ holds. Indeed, let $R \neq \{0\}$ be a ring with identity element 1 and pick $a \in R \setminus \{0\}$. Then,

$$1 \cdot a = a \neq 0 = 0 \cdot a.$$

Hence, $1 \neq 0$.

ii) Let $(R, 0, +)$ be an abelian group and define

$$\begin{array}{rcl} \cdot\colon R \times R & \longrightarrow & R \\ (a, b) & \longmapsto & 0 \end{array}$$

Then, $(R, 0, +, \cdot)$ is a ring. If $R \neq \{0\}$, then R has no identity element.

iii) The integers form the ring $\mathbb{Z}$.

iv) Fields are rings, e.g., $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{F}_q$, $q = p^n$, $n \geq 1$ and p a prime number.

v) Suppose R is a ring and X is a set. We introduce

$$\mathrm{Map}(X, R) := \{\, f\colon X \longrightarrow R \mid f \text{ is a set theoretic map} \,\}.$$

For $f, g \in \mathrm{Map}(X, R)$, we form

$$\begin{array}{rcl} f + g\colon X & \longrightarrow & R \\ x & \longmapsto & f(x) + g(x) \end{array}$$

and

$$\begin{array}{rcl} f \cdot g\colon X & \longrightarrow & R \\ x & \longmapsto & f(x) \cdot g(x). \end{array}$$

Moreover, we set

$$\begin{array}{rcl} 0\colon X & \longrightarrow & R \\ x & \longmapsto & 0. \end{array}$$

The tuple $(\mathrm{Map}(X, R), 0, +, \cdot)$ is a ring. Observe that $\mathrm{Map}(X, R)$ is commutative if R is so and that $\mathrm{Map}(X, R)$ possesses an identity element if R does. In fact, if $1 \in R$ is the identity element of R, then

$$\begin{array}{rcl} 1\colon X & \longrightarrow & R \\ x & \longmapsto & 1 \end{array}$$

is the identity element in $\mathrm{Map}(X, R)$. Note, however, that $\mathrm{Map}(X, R)$ will, in general, not be a field, even if R is one (see Example I.3.1, iv).

vi) Suppose X is a topological space. Then,

$$\mathscr{C}(X, \mathbb{R}) := \{\, f\colon X \longrightarrow \mathbb{R} \mid f \text{ is continuous} \,\}$$

together with 0, 1, +, $\cdot$ as in v) is a commutative ring with identity element.

vii) Suppose $X \subset \mathbb{C}$ is an open subset (compare [31], Definition III.2.1, ii), and III.3.10, i). Then,

$$\mathscr{O}(X) := \{\, f\colon X \longrightarrow \mathbb{C} \mid f \text{ is holomorphic} \,\}$$

together with 0, 1, +, $\cdot$ as in v) is a commuative ring with identity element.

viii) Let $(G, 0, +)$ be an abelian group. We look at

$$\mathrm{End}(G) := \{\, f\colon G \longrightarrow G \mid f \text{ is a group homomorphism} \,\}$$

and define

$$\begin{aligned} 0\colon G &\longrightarrow G \\ g &\longmapsto 0 \end{aligned}$$

and, for $f, h \in \mathrm{End}(G)$,

$$\begin{aligned} f+h\colon G &\longrightarrow G \\ g &\longmapsto f(g)+h(g). \end{aligned}$$

Composition of maps provides us with the multiplication: For $f, h \in \mathrm{End}(G)$, we set

$$\begin{aligned} f\circ h\colon G &\longrightarrow G \\ g &\longmapsto f(h(g)). \end{aligned}$$

We leave it to the reader to verify that $(\mathrm{End}(G), 0, +, \cdot)$ is a ring with identity element id_G. It is, in general, not a commutative ring (see Exercise I.1.4).

ix) Let k be a field. The vector space $M_n(k)$ of $(n\times n)$-matrices with entries in k forms a ring with respect to componentwise addition and matrix multiplication (see [33], Kapitel III). The unit matrix $\mathbb{E}_n$ is the identity element. Note that $M_n(k)$ is non-commutative if and only if $n \geq 2$.

x) Suppose R_1, ..., R_n are rings. The cartesian product $R_1 \times \cdots \times R_n$ equipped with componentwise addition and multiplication is again a ring. It is called the *direct product* of the rings R_1, ..., R_n.

I.1.4 Exercise. Describe $\mathrm{End}(\mathbb{Z}\times\mathbb{Z})$ in terms of (2×2)-matrices and give two elements of that ring which do not commute with each other.

Let R be a ring with identity element. A subset $S \subset R$ is a *subring*, if S is a subgroup of $(R, +, 0)$ (see [30], Definition II.4.1), $1 \in S$ and $a \cdot b \in S$, if $a, b \in S$.

> From now on, all rings are supposed to be **commutative** and to possess an **identity element**.

Let R, S be two rings. A *homomorphism* from R to S is a map $f\colon R \longrightarrow S$, such that

- ⋆ $\forall a, b \in R : f(a+b) = f(a) + f(b)$, i.e., f is a homomorphism of the underlying abelian groups,
- ⋆ $\forall a, b \in R : f(a\cdot b) = f(a)\cdot f(b)$,
- ⋆ $f(1) = 1$.

I.1.5 Remark. One may be tempted to believe that the third condition is a consequence of the second. However, the proof for the analogous statement in group theory ([30], Lemma II.3.4, i) requires the existence of inverse elements. This cannot be assumed for multiplication. Indeed, choosing $R = \{0\}$ and $S \neq \{0\}$, we see that it may be false. A more sophisticated example, using the construction in Example I.1.3, x), is the following:

$$\begin{aligned} \varphi\colon \mathbb{Z} &\longrightarrow \mathbb{Z}\times\mathbb{Z} \\ k &\longmapsto (k, 0). \end{aligned}$$

I.1.6 Exercise. Let $f\colon R \longrightarrow S$ be a homomorphism of rings. Check that

$$\mathrm{Im}(f) := \{\, b \in S \mid \exists a \in R : b = f(a) \,\}$$

is a subring of S.

Is

$$\mathrm{Ker}(f) := \{\, a \in R \mid f(a) = 0 \,\}$$

a subring of R?

Suppose R is a ring and $a \in R$. We set

- $a^0 := 1$,
- $a^{n+1} := a \cdot a^n$, $n \in \mathbb{N}$.

As usual, the **exponential rule**

$$\forall a \in R \forall m, n \in \mathbb{N} : \quad a^{m+n} = a^m \cdot a^n$$

holds true.

Polynomial Rings

Let R be a ring. A *polynomial* over R in the indeterminate x should be an expression of the form

$$p = a_0 + a_1 \cdot x + \cdots + a_n \cdot x^n \quad \text{with} \quad a_0, ..., a_n \in R.$$

We have natural rules for adding and multiplying two polynomials. They are based on the multiplication in R, the distributive laws and

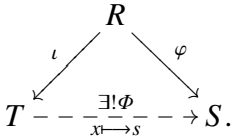
$$\forall m, n \in \mathbb{N} : \quad x^m \cdot x^n = x^{m+n}.$$

In this way, we obtain the **polynomial ring** $R[x]$. This description is not satisfactory, because it uses the mathematically undefined terms “indeterminate” and “formal expression”. In the following definition, we will characterize the polynomial ring by its (universal) property rather than by a construction. We advise the reader to pay special attention to this procedure as this kind of approach will become more and more important during the course.

A *polynomial ring* over R in the indeterminate x is a triple (T, x, ι) which consists of a ring T, an element $x \in T$, and a homomorphism $\iota\colon R \longrightarrow T$, such that the following **universal property** holds: For every ring S, every element $s \in S$, and every homomorphism $\varphi\colon R \longrightarrow S$, there exists a **unique** homomorphism $\Phi\colon T \longrightarrow S$, such that

- $\Phi \circ \iota = \varphi$,
- $\Phi(x) = s$.

The stated property may be best remembered by the diagram



Notation. We set $R[x] := T$.

I.1.7 Remark. Given two polynomial rings (T, x, ι) and (T', x', ι'), there are, by definition, uniquely determined homomorphisms

- ⋆ $\Phi\colon T \longrightarrow T'$ with a) $\Phi \circ \iota = \iota'$ and b) $\Phi(x) = x'$;
- ⋆ $\Phi'\colon T' \longrightarrow T$ with a) $\Phi' \circ \iota' = \iota$ and b) $\Phi'(x') = x$.

Observe that, for $\Phi' \circ \Phi$, we have

- ⋆ $(\Phi' \circ \Phi) \circ \iota = \iota$,
- ⋆ $(\Phi' \circ \Phi)(x) = x$.

The uniqueness statement in the definition of a polynomial ring, applied to $S = T$, $\varphi = \iota$ and $s = x$ shows

$$\Phi' \circ \Phi = \mathrm{id}_T.$$

Similarly, we verify

$$\Phi \circ \Phi' = \mathrm{id}_{T'}.$$

We do not only see that T and T' are isomorphic, there is also a distinguished isomorphism between T and T' that respects the extra data x, ι and x', ι', respectively. One says

*The tuples (T, x, ι) and (T', x', ι') are **canonically** isomorphic.*

This means that, in dealing with a polynomial ring, we need just to remember its universal property as it is completely determined by it. This aspect will be very useful in other situations, e.g., the tensor product ([1], p. 24f) or the fibered product of schemes ([11], Chapter II.3) are usually remembered by their universal properties and not by their (involved) constructions.

I.1.8 Theorem. *Let R be a ring. Then, there exists a polynomial ring (T, x, ι) over R. Furthermore, the homomorphism ι is injective.*

Proof. We define

$$T := \{\, f\colon \mathbb{N} \longrightarrow R \mid f(n) = 0 \text{ for all but finitely many } n \in \mathbb{N} \,\},$$

$$\begin{array}{rcl} x\colon \mathbb{N} & \longrightarrow & R \\ n & \longmapsto & \begin{cases} 0, & \text{if } n \neq 1 \\ 1, & \text{if } n = 1 \end{cases}, \end{array}$$

and

$$\begin{array}{rcl} \iota\colon R & \longrightarrow & T \\ a & \longmapsto & \left(n \longmapsto \begin{cases} 0, & \text{if } n \neq 0 \\ a, & \text{if } n = 0 \end{cases} \right). \end{array}$$

We define addition as before, i.e., for $f, g \in T$, we set

$$\begin{array}{rcl} f + g\colon \mathbb{N} & \longrightarrow & R \\ n & \longmapsto & f(n) + g(n). \end{array}$$

The product of $f, g \in T$ is defined in the following way:

$$\begin{aligned} f \cdot g \colon \mathbb{N} &\longrightarrow R \\ n &\longmapsto \sum_{k=0}^{n} f(k) \cdot g(n-k). \end{aligned}$$

The reader should verify that $f + g$ and $f \cdot g$ do belong to T, i.e., vanish in all but finitely many points, $f, g \in T$. Furthermore, the following properties are readily verified:

- ⋆ T is a commutative ring with identity element $\iota(1)$.
- ⋆ ι is an injective ring homomorphism.

Let us write a map $f \colon \mathbb{N} \longrightarrow R$ as a sequence $(a_0, a_1, a_2, ...)$ with $a_k = f(k)$, $k \in \mathbb{N}$. Then,

- ⋆ $x = (0, 1, 0, ...)$,
- ⋆ $\iota(a) = (a, 0, 0, ...)$, $a \in R$,
- ⋆ $(a_0, a_1, a_2, ...) + (b_0, b_1, b_2, ...) = (a_0 + b_0, a_1 + b_1, a_2 + b_2, ...)$,
- ⋆ $(a_0, a_1, a_2, ...) \cdot (b_0, b_1, b_2, ...) = (a_0 \cdot b_0, a_0 \cdot b_1 + a_1 \cdot b_0, ...)$,
- ⋆ $x^k = (0, ..., 0, 1, 0, ...)$ with 1 at the $(k + 1)$-st place, $k \in \mathbb{N}$, i.e.,

$$\begin{aligned} x^k \colon \mathbb{N} &\longrightarrow R \\ n &\longmapsto \begin{cases} 0, & \text{if } n \neq k \\ 1, & \text{if } n = k \end{cases} . \end{aligned}$$

Let $f = (a_0, a_1, a_2, ...) \in T$. If $a_k = 0$ for all $k \in \mathbb{N}$, we simply write $f = 0$. Otherwise, let

$$n := \max\{\, k \in \mathbb{N} \mid a_k \neq 0 \,\}.$$

Then, using the above formulae, we have the identity

$$f = a_0 + a_1 \cdot x + a_2 \cdot x^2 + \cdots + a_n \cdot x^n.$$

This representation is unique.

Using the above notation, we find, for a given homomorphism $\varphi \colon R \longrightarrow S$, $s \in S$, and a homomorphism $\Phi \colon T \longrightarrow S$, satisfying $\Phi \circ \iota = \varphi$ and $\Phi(x) = s$, that

$$\Phi(a_0 + a_1 \cdot x + \cdots + a_n \cdot x^n) = \varphi(a_0) + \varphi(a_1) \cdot s + \cdots + \varphi(a_n) \cdot s^n, \quad n \in \mathbb{N},\ a_0, ..., a_n \in R. \tag{I.1}$$

This shows that Φ is uniquely determined, if it exists. On the other hand, for given $\varphi \colon R \longrightarrow S$ and $s \in S$, Equation (I.1) defines a set theoretic map $\Phi \colon T \longrightarrow S$, and it is readily checked that it is a ring homomorphism with $\Phi(x) = s$ and $\Phi \circ \iota = \varphi$. □

We can now recursively define the polynomial ring in the indeterminates $x_1, ..., x_{n+1}$ as

$$R[x_1, ..., x_{n+1}] = R[x_1, ..., x_n][x_{n+1}]. \tag{I.2}$$

I.1.9 Exercise. Characterize $R[x_1, ..., x_{n+1}]$ by a universal property which is not recursive.

Let S be a ring, $R \subset S$ a subring, and $y_1, ..., y_n \in S$. By the universal property of the polynomial ring, there is a unique homomorphism

$$\begin{array}{rcl} R[x_1, ..., x_n] & \longrightarrow & S \\ x_i & \longmapsto & y_i, \quad i = 1, ..., n. \end{array}$$

We say that $y_1, ..., y_n$ are *algebraically independent* over R, if this homomorphism is injective.

I.2 Ideals and Quotient Rings

Let R be a ring. A subset $I \subset R$ is called an *ideal*, if

- ⋆ I is a subgroup of $(R, 0, +)$,
- ⋆ $\forall a \in I \forall r \in R : r \cdot a \in I$, or, for short, $R \cdot I \subset I$.

The role of ideals in ring theory is somewhat similar to the role of **normal subgroups** in group theory (see [30], Abschnitt II.9). We will come back to this below.

I.2.1 Examples and properties. i) For any ring R, the subsets $\{0\}$ and R are ideals.

ii) Let R be a ring and $I \subset R$ an ideal. Then,

$$I = R \quad \Longleftrightarrow \quad 1 \in I.$$

The implication "$\Longrightarrow$" is clear. For "$\Longleftarrow$", let $a \in R$. Since $a = a \cdot 1$, it follows that a belows to I.

iii) Suppose k is a field. Then, the only ideals are $\{0\}$ and k. For, if $I \neq \{0\}$ is an ideal of k, there exists an element $a \in I \setminus \{0\} \subset k \setminus \{0\}$. Since $1 = a^{-1} \cdot a$, we see that $1 \in I$, and ii) implies $I = k$.

iv) If R is a ring and $a \in R$ an element, then

$$\langle a \rangle := \{ r \cdot a \,|\, r \in R \}$$

is an ideal of R. It is called the *principal ideal* generated by a and is the smallest ideal of R which contains a.

v) Suppose $R = \mathbb{Z}$. We first recall that, for integers $k, m \in \mathbb{Z}$, the relation $m|k$ means that there is an integer $l \in \mathbb{Z}$ with $k = l \cdot m$ which is equivalent to $k \in \langle m \rangle$. Now, suppose $I \subset \mathbb{Z}$ is an ideal. The zero ideal is the principal ideal $\langle 0 \rangle$. If I is a nonzero ideal, it contains some integer $k \neq 0$. By the definition of an ideal, it also contains $-k = (-1) \cdot k$. It follows that I contains a positive integer. By the least element principle ([27], Satz 1.3.22), we can define

$$m := \min\{ n \in \mathbb{N} \,|\, n > 0 \wedge n \in I \}.$$

We claim $I = \langle m \rangle$. Suppose $k \in I$ is a nonzero element. There are integers $x, y \in \mathbb{Z}$ (see [30], Satz I.4.4, ii), such that

$$x \cdot k + y \cdot m = \gcd(k, m).$$

This shows $\gcd(k, m) \in I$. By definition of m, we have $m \leq \gcd(k, m)$. This means $m = \gcd(k, m)$ and is equivalent to $m|k$, i.e., $k \in \langle m \rangle$.

vi) Let R be a ring and X a set. In Example I.1.3, v), we introduced the ring $\mathrm{Map}(X, R)$. Let $Y \subset X$ be a subset. Then,

$$I := \{ f \colon X \longrightarrow R \,|\, \forall y \in Y : \ f(y) = 0 \}$$

is an ideal of $\mathrm{Map}(X, R)$.

vii) Let R, S be rings and $\varphi \colon R \longrightarrow S$ a homomorphism. Then, the **kernel**

$$\mathrm{Ker}(\varphi) := \{ x \in R \,|\, \varphi(x) = 0 \}$$

is an ideal of R. More generally, for every ideal $J \subset S$, the preimage $\varphi^{-1}(J) \subset R$ is an ideal. (Note $\mathrm{Ker}(\varphi) = \varphi^{-1}(\{0\})$.)

viii) The inclusion $\mathbb{Z} \subset \mathbb{Q}$ is a ring homomorphism. Its image is not an ideal, i.e., the image of an ideal is, in general, not an ideal.

ix) Let R, S be rings and $\varphi \colon R \longrightarrow S$ a **surjective** homomorphism. Then, the image of an ideal in R is an ideal in S. In fact, let $I \subset R$ be an ideal. Then, $\varphi(I)$ is a subgroup of $(S, 0, +)$ ([30], Lemma II.4.4). Now, let $s \in S$ and $b \in \varphi(I)$. Then, there exist elements $r \in R$ and $a \in I$ with $\varphi(r) = s$ and $\varphi(a) = b$. We see

$$s \cdot b = \varphi(r) \cdot \varphi(a) = \varphi(r \cdot a) \in \varphi(I).$$

x) If $I, J \subset R$ are ideals, then $I \cap J$ and

$$I + J = \{ a + b \,|\, a \in I \wedge b \in J \}$$

are ideals, too. In particular, we have, for elements $a_1, ..., a_s \in R$ the ideal

$$\langle a_1, ..., a_s \rangle = \langle a_1 \rangle + \cdots + \langle a_s \rangle.$$

It is the smallest ideal of R which contains $a_1, ..., a_s$.

Part iii) and v) illustrate how ideals reflect the algebraic structure of the respective ring. We will see many more examples of this kind.

Let us spend a few words why ideals are important. For this, let R be a ring and $I \subset R$ an ideal. Then, the set R/I of residue classes inherits the structure of an abelian group (see [30], Satz II.9.4).

Notation. Write $[a]$ for the class

$$a + I = \{ a + r \,|\, r \in I \} \in R/I, \quad a \in R.$$

Now, we try the following multiplication on R/I:

$$\begin{array}{rcl} \cdot \colon R/I \times R/I & \longrightarrow & R/I \\ ([a], [b]) & \longmapsto & [a \cdot b]. \end{array}$$

We need to verify that this is well-defined. Given $a, a', b, b' \in R$, such that $[a] = [a']$ and $[b] = [b']$, there exist elements $x, y \in I$ with

$$a' = a + x \quad \text{and} \quad b' = b + y.$$

We get

$$a' \cdot b' = a \cdot b + a \cdot y + b \cdot x + x \cdot y.$$

By definition of an ideal, we have

$$a \cdot y + b \cdot x + x \cdot y \in I \quad \text{and} \quad [a' \cdot b'] = [a \cdot b].$$

Note that

$$\begin{aligned} \pi \colon R &\longrightarrow R/I \\ a &\longmapsto [a] \end{aligned}$$

is a group homomorphism which satisfies

$$\forall a, b \in R: \quad \pi(a \cdot b) = [a \cdot b] = [a] \cdot [b] = \pi(a) \cdot \pi(b).$$

This shows that the multiplication in R/I satisfies associativity and that the distributive laws hold. So, R/I inherits a ring structure, such that π is a surjective ring homomorphism.

I.2.2 Lemma. *The assignment $J \longmapsto \pi^{-1}(J)$ induces an inclusion preserving bijection between the set of ideals of R/I and the set of ideals of R that contain I.*

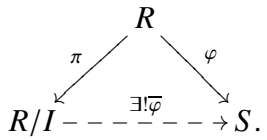
I.2.3 Exercise. Prove this lemma. In particular, give the map from the set of ideals in R that contain I to the set of ideals of S that is inverse to the map described in the lemma.

I.2.4 Exercises. i) Let R be a ring and $I \subset R$ an ideal. Show that the pair $(R/I, \pi)$, consisting of the quotient ring R/I and the surjection $\pi \colon R \longrightarrow R/I$, $a \longmapsto [a]$, has the following universal property (compare [30], Satz II.9.7): For every ring S and every homomorphism $\varphi \colon R \longrightarrow S$, such that

$$I \subset \operatorname{Ker}(\varphi),$$

there is a unique homomorphism $\overline{\varphi} \colon R/I \longrightarrow S$ with

$$\varphi = \overline{\varphi} \circ \pi;$$



ii) Let $f \colon R \longrightarrow S$ be a homomorphism of rings. Prove the **first isomorphism theorem** (compare [30], II.10.1): We have $\operatorname{Im}(\overline{f}) = \operatorname{Im}(f)$ (compare Exercise I.1.6), $\overline{f}$ being the induced homomorphism from Part i), and

$$\overline{f} \colon R/\operatorname{Ker}(f) \longrightarrow \operatorname{Im}(f)$$

is an isomorphism.

I.3 Zero Divisors, Nilpotent Elements, and Units

Let R be a ring. An element $a \in R$ is called a *zero divisor*, if there exists an element $b \neq 0$, such that $a \cdot b = 0$. The ring R is called an *integral domain*, if $R \neq \{0\}$ and 0 is its only zero divisor.

I.3.1 Examples. i) The ring $\mathbb{Z}$ of integers is an integral domain.

ii) Fields are integral domains.

iii) If R is an integral domain, then the polynomial ring $R[x]$ is also an integral domain. In particular, if R is a field, then the polynomial ring $k[x_1, ..., x_n]$ in n variables is an integral domain.

iv) Assume that X contains at least two distinct elements $x_1 \neq x_2$ and $R \neq \{0\}$ is a ring. Then, $\mathrm{Map}(X, R)$ contains non-trivial zero-divisors. For example, we look at

$$\begin{array}{rcl} f_i \colon X & \longrightarrow & R \\ x & \longmapsto & \begin{cases} 0, & \text{if } x \neq x_i \\ 1, & \text{if } x = x_i \end{cases}, \quad i = 1, 2. \end{array}$$

Then, $f_i \neq 0$, $i = 1, 2$, but $f_1 \cdot f_2 = 0$.

Let R be a ring. An element $a \in R$ is *nilpotent*, if there exists a natural number n with $a^n = 0$.

I.3.2 Remark. Obviously, a nilpotent element is a zero divisor. The converse does not hold. E.g., f_1 and f_2 in Example I.3.1, iv), are zero divisors but not nilpotent.

I.3.3 Example. Let k be a field and $n \geq 2$ a natural number. We look at the principal ideal $\langle x^n \rangle \subset k[x]$ and the quotient ring $R := k[x]/\langle x^n \rangle$. Then, $[x]^k = [x^k] \neq 0$, for $1 \leq k < n$, but $[x]^n = [x^n] = 0$, i.e., $[x]$ is a nilpotent element of R.

I.3.4 Exercise. Let $n \geq 2$ be a natural number. Describe the zero divisors and nilpotent elements in the residue ring $\mathbb{Z}/\langle n \rangle$ in terms of the prime factorization (see [30], Kapitel I) of n.

Let R be a ring. An element $a \in R$ is called a *unit*, if there exists an element $b \in R$, such that $a \cdot b = 1$. Observe that the element b is uniquely determined. (Indeed, for $b, b' \in R$ with $a \cdot b = 1 = a \cdot b'$, we find $b = b \cdot 1 = b \cdot (a \cdot b') = (b \cdot a) \cdot b' = 1 \cdot b' = b'$.)

Notation. We write $a^{-1} := b$.

I.3.5 Remarks. i) The set

$$R^\star := \{\, a \in R \mid a \text{ is a unit of } R \,\}$$

of units in the ring R is an abelian group with respect to multiplication in R with identity element 1.

ii) An element $a \in R$ is a unit if and only if $\langle a \rangle = R$.

I.3.6 Examples. i) The units of the ring $\mathbb{Z}$ of integers form the group $\mathbb{Z}^\star = \{\pm 1\}$.

ii) Let R be an integral domain, then $(R[x])^\star = R^\star$ (compare Exercise I.3.10).

I.3.7 Exercise. Describe the units of $\mathbb{Z}/\langle n \rangle$ for $n \geq 1$ (compare [30], Abschnitt III.2).

I.3.8 Exercises (Units and nilpotent elements). i) Let R be a ring and $n \in R$ a nilpotent element. Show that $1 + n$ is a unit.

ii) Deduce that the sum $u + n$ of a unit $u \in R$ and a nilpotent element $n \in R$ is a unit.

I.3.9 Lemma. *Let $R \neq \{0\}$ be a ring. The following conditions are equivalent:*

i) *R is a field.*

ii) *The subsets $\{0\}$ and R are the only ideals of R.*

iii) *Every homomorphism $\varphi\colon R \longrightarrow S$ to a nonzero ring $S \neq \{0\}$ is injective.*

Proof. For the implication "i)$\Longrightarrow$ii)", see Example I.2.1, iii).

"ii)$\Longrightarrow$iii)": If $S \neq \{0\}$, then $1 \notin \mathrm{Ker}(\varphi)$ (see Example I.2.1). So, $\mathrm{Ker}(\varphi)$ is a proper ideal of R. The assumption yields $\mathrm{Ker}(\varphi) = \{0\}$. As for group homomorphisms (see [30], Lemma II.4.5), this implies that φ is injective.

"iii)$\Longrightarrow$i)": For an element $a \in R \setminus \{0\}$, we define $S := R/\langle a\rangle$. Then, $\pi\colon R \longrightarrow S$ is a surjective ring homomorphism with $\pi(a) = \pi(0) = 0$. So, π is not injective. This implies $S = \{0\}$ or, equivalently, $\langle a\rangle = R$. In view of Remark I.3.5, ii), this shows that a is a unit. □

I.3.10 Exercise (Units in polynomial rings). Let R be a ring and $f = a_0 + a_1 x + \cdots + a_n x^n \in R[x]$ a polynomial. Show that f is a unit if and only if a_0 is a unit and $a_1, \ldots, a_n$ are nilpotent elements.

Instructions.

- For "$\Longrightarrow$", use Exercise I.3.8.
- For "$\Longleftarrow$", let $g = b_0 + b_1 x + \cdots + b_m x^m \in R[x]$ be a polynomial with $f \cdot g = 1$. Prove by induction on r that

$$a_n^{r+1} \cdot b_{m-r} = 0, \quad r = 0, ..., m. \tag{I.3}$$

  To this end write $f \cdot g = c_0 + c_1 \cdot x + \cdots + c_{m+n} \cdot x^{m+n}$ and look at $a_n^{r+1} \cdot c_{m+n-r-1}$. Finally, deduce from (I.3) that a_n is nilpotent and conclude by induction on n.

I.4 Prime Ideals and Maximal Ideals

Let R be a ring. An ideal $I \subset R$ is called a *prime ideal*, if $I \neq R$ and

$$\forall a, b \in R: \quad a \cdot b \in I \quad \Longrightarrow \quad (a \in I \vee b \in I),$$

and a *maximal ideal*, if $I \neq R$ and there is no ideal J of R with $I \subsetneq J \subsetneq R$.

Notation. It is customary to use gothic letters for prime and maximal ideals, e.g., $\mathfrak{p}$, $\mathfrak{m}$.

I.4.1 Proposition. *Let R be a ring and $I \subset R$ an ideal, then*

i) *I is a prime ideal if and only if R/I is an integral domain.*

ii) *I is a maximal ideal if and only if R/I is a field.*

Proof. i) This is immediate from the definitions.

ii) "$\Longrightarrow$": Let $I \neq R$ be a maximal ideal. According to Lemma I.2.2, the ideals of R/I correspond to the ideals in R which contain I. These are I and R. So, $\{0\}$ and R/I are the only ideals of R/I. By Lemma I.3.9, R/I is a field. The converse implication "$\Longleftarrow$" is obtained by a similar reasoning. □

I.4.2 Corollary. *A maximal ideal is a prime ideal.*

I.4.3 Remarks. i) Let R be a ring. The zero ideal $\{0\}$ is a prime ideal if and only if R is an integral domain.

ii) Let $\varphi\colon R \longrightarrow S$ be a homomorphism of rings. If $\mathfrak{q} \subset S$ is a prime ideal, then $\mathfrak{p} := \varphi^{-1}(\mathfrak{q})$ is a prime ideal of R. Indeed, we have

$$1 \notin \mathfrak{q} \quad \Longrightarrow \quad 1 \notin \mathfrak{p},$$

so that $\mathfrak{p}$ is a proper ideal. By Exercise I.2.4, ii), there is the induced **injective** homomorphism $\overline{\varphi}\colon R/\mathfrak{p} \longrightarrow S/\mathfrak{q}$, $[r] \longmapsto [\varphi(r)]$. Since $S/\mathfrak{q}$ is an integral domain, the same holds for $R/\mathfrak{p}$. Now, apply Proposition I.4.1, i).

iii) Let $\varphi\colon R \longrightarrow S$ be, as before, a ring homomorphism. If $\mathfrak{m} \subset S$ is a maximal ideal, then $\mathfrak{q} := f^{-1}(\mathfrak{m})$ needs **not** be maximal. Look for example at the inclusion $\varphi\colon \mathbb{Z} \subset \mathbb{Q}$. Then, $\{0\} \subset \mathbb{Q}$ is a maximal ideal, because $\mathbb{Q}$ is a field, but $\{0\} = \varphi^{-1}(\{0\})$ is not a maximal ideal of $\mathbb{Z}$.

I.4.4 Theorem. *In every ring $R \neq \{0\}$, there exist maximal ideals.*

I.4.5 Remark (The axiom of choice). i) The proof of this theorem requires the **axiom of choice**. Like the theorem that every vector space has a basis, this theorem is actually **equivalent** to the axiom of choice (see, e.g., [3]).

ii) Since, by Corollary I.4.2, maximal ideals are prime ideals, Theorem I.4.4 shows that every non-zero ring contains a prime ideal. It might be interesting to know that the statement "Every ring $R \neq \{0\}$ possesses a prime ideal." is actually **weaker** than the axiom of choice. It is equivalent to the axiom (BPI) that every non-zero boolean ring (see Exercise I.4.16) contains a prime ideal. We refer the reader to the paper [25] for more details and references.

The axiom of choice, in turn, is equivalent to **Zorn's**[3] **lemma** that we shall now formulate. Let $(S, \leq)$ be a **partially ordered set**. This means that S is a set and "$\leq$" a relation on S which satisfies the following properties:

- ⋆ **Reflexivity:** $\forall s \in S : s \leq s$.
- ⋆ **Antisymmetry:** $\forall s_1, s_2 \in S : (s_1 \leq s_2 \wedge s_2 \leq s_1) \Longleftrightarrow s_1 = s_2$.
- ⋆ **Transitivity:** $\forall s_1, s_2, s_3 \in S : s_1 \leq s_2 \wedge s_2 \leq s_3 \Longrightarrow s_1 \leq s_3$.

I.4.6 Note. The relation "$\leq$" corresponds to a subset $U \subset S \times S$, such that

$$\forall s_1, s_2 \in S : \quad s_1 \leq s_2 \quad \Longleftrightarrow \quad (s_1, s_2) \in U.$$

[3] Max August Zorn (1906 - 1993) was a German mathematician who emigrated to the USA because of the Nazi policies.

A *chain* in S is a subset $T \subset S$, such that, for $t_1, t_2 \in T$, one has $t_1 \leq t_2$ or $t_2 \leq t_1$, i.e., "$\leq$" induces a **total ordering** on T.

An *upper bound* for a chain T is an element $u \in S$, such that $t \leq u$ holds for all $t \in T$. Observe that it is **not** required that u belongs to T.

A *maximal element* of S is an element $m \in S$, such that, for $s \in S$, $m \leq s$ implies $m = s$.

I.4.7 Zorn's lemma. *Let $(S, \leq)$ be a nonempty partially ordered set, such that every chain T in S has an upper bound. Then, S contains at least one maximal element.*

Proof. See [35], Satz 5.13. □

Proof of Theorem I.4.4. We look at the set

$$S := \{\, I \subset R \mid I \neq R \text{ and } I \text{ is an ideal} \,\}.$$

This set contains $\{0\}$ and is therefore nonempty, and it is partially ordered by inclusion "$\subset$". Let T be a chain in S and define

$$J := \bigcup_{I \in T} I.$$

Claim. *The set J is an upper bound for T, i.e., $J \in S$.*

We first verify that $J \neq R$. This follows, because $1 \notin I$, $I \in T$. Next, we show that J is an ideal. To see that J is a subgroup of R, note first that $0 \in J$, because $0 \in I$ for all $I \in T$. Next, assume $a_1, a_2 \in J$. Then, there are ideals $I_1, I_2 \in T$ with $a_1 \in I_1$ and $a_2 \in I_2$. Since T is a chain, we have $I_2 \subset I_1$ or $I_1 \subset I_2$. We assume the latter. Then, $a_1 + a_2 \in I_2 \subset J$. Finally, let $a \in J$ and $r \in R$. Then, there is an ideal $I \in T$ with $a \in I$. Since I is an ideal, $r \cdot a \in I$ and, thus, $r \cdot a \in J$. For $r = -1$, this gives $-a \in J$ (see Property I.1.2, ii) and completes the proof. ✓

By Zorn's lemma I.4.7, S contains a maximal element $\mathfrak{m}$. By definition, $\mathfrak{m}$ is a maximal ideal. □

I.4.8 Corollary. i) *Every ideal $I \subset R$ is contained in a maximal ideal.*

ii) *Every element $a \in R$ which is not a unit is contained in a maximal ideal.*

Proof. i) We may apply the theorem to the ring R/I and use Lemma I.2.2 or modify the above proof.

ii) If a is not a unit, then $\langle a \rangle \subsetneq R$. Hence, we may conclude by i). □

A ring R with exactly one maximal ideal is called a *local ring*. In this case, the field $R/\mathfrak{m}$ is called the *residue field*. A ring with only finitely many maximal ideals is a *semilocal ring*.

I.4.9 Example. A field is a local ring with maximal ideal $\{0\}$.

I.4.10 Proposition. i) *Let $R \neq \{0\}$ be a ring and $\mathfrak{m} \subsetneq R$ an ideal, such that every element $a \in R \setminus \mathfrak{m}$ is a unit. Then, R is a local ring with maximal ideal $\mathfrak{m}$.*

ii) *Let $R \neq \{0\}$ be a ring and $\mathfrak{m} \subset R$ a maximal ideal, such that $1 + \mathfrak{m} \subset R^\star$. Then, R is a local ring.*

Proof. i) Let $I \subsetneq R$ be an ideal. Then, no element of $a \in I$ is a unit. By assumption, $I \subset \mathfrak{m}$.

ii) Let $a \in R \setminus \mathfrak{m}$. Then, $\langle a \rangle + \mathfrak{m} = R$, because $\mathfrak{m}$ is a maximal ideal. So, there exist $r \in R$ and $b \in \mathfrak{m}$, such that

$$r \cdot a + b = 1.$$

We see that $r \cdot a \in 1 + \mathfrak{m}$, so that $r \cdot a$ is a unit. It follows that a is a unit. (To see this, note $((r \cdot a)^{-1} \cdot r) \cdot a = 1$.) We now conclude by i). □

I.4.11 Examples. i) In $\mathbb{Z}$, every ideal is principal, i.e., of the form $\langle m \rangle$ for some integer $m \in \mathbb{Z}$. Here, $\langle m \rangle$ is a prime ideal if and only if $m = 0$ or m is a prime number. For a prime number p, $\mathbb{F}_p = \mathbb{Z}/\langle p \rangle$ is the field with p elements. In particular, every non-zero prime ideal in $\mathbb{Z}$ is a maximal ideal.

ii) An integral domain R in which every ideal is principal is called a *principal ideal domain*. Examples for principal ideal domains include the ring of integers $\mathbb{Z}$ and the polynomial ring $k[x]$ over a field k (see Exercise I.4.15, i). In a principal ideal domain, every **nonzero** prime ideal is maximal. Indeed, let $\langle a \rangle$ be a nonzero prime ideal, i.e., $a \neq 0$, and $\langle b \rangle$ be an ideal with

$$\langle a \rangle \subsetneq \langle b \rangle.$$

Thus, there exists an element $r \in R$ with $r \cdot b = a$. If $b \notin \langle a \rangle$, we must have $r \in \langle a \rangle$. Choose $s \in R$ with $r = s \cdot a$. So, $b \cdot s \cdot a = a$, i.e., $(b \cdot s - 1) \cdot a = 0$. Since $a \neq 0$ and R is an integral domain, we infer $b \cdot s = 1$. So, b is a unit and $\langle b \rangle = R$.

iii) **Power series rings**. Let R be a ring. We look again at

$$\mathrm{Map}(\mathbb{N}, R) = \{ \text{Sequences } (a_0, a_1, a_2, ...) \,|\, a_k \in R, k \in \mathbb{N} \}.$$

The arithmetic operations are as follows:

- ⋆ As addition, we use again componentwise addition:

$$(a_0, a_1, a_2, ...) + (b_0, b_1, b_2, ...) = (a_0 + b_0, a_1 + b_1, a_2 + b_2, ...).$$

- ⋆ As multiplication, we use, as for polynomial rings, the **Cauchy**[4] **product**:

$$(a_0, a_1, a_2, ...) \cdot (b_0, b_1, b_2, ...) = (c_0, c_1, c_2, ...)$$

with

$$c_n := \sum_{k=0}^{n} a_k \cdot b_{n-k}, \quad n \in \mathbb{N}. \tag{I.4}$$

Notation. We write a sequence $(a_0, a_1, a_2, ...)$ in $\mathrm{Map}(\mathbb{N}, R)$ as $\sum_{k=0}^{\infty} a_k \cdot x^k$. Such an expression is called a *formal power series* over R. The ring of all formal power series over R is denoted by $R[\![x]\!]$.

Remark. Note that the polynomial ring $R[x]$ is a subring (see Page 4) of $R[\![x]\!]$.

[4] Augustin-Louis Cauchy (1789 - 1857), French mathematician.

Proposition. *A formal power series* $\sum_{k=0}^{\infty} a_k \cdot x^k$ *is a unit in* $R[[x]]$ *if and only if* a_0 *is a unit in* R.

We leave it to the reader to verify this easy consequence of (I.4).

Corollary. *If* k *is a field, then* $k[[x]]$ *is a local ring with maximal ideal*

$$\langle x \rangle = \left\{ \sum_{i=1}^{\infty} a_i \cdot x^i \,\middle|\, a_i \in k, i = 1, 2, 3, \ldots \right\}.$$

Assume $k = \mathbb{C}$. A formal power series $\sum_{i=0}^{\infty} a_i \cdot x^i$ is *convergent*, if its radius of convergence (see [31], Definition II.3.8) is positive. We set

$$\mathbb{C}\{x\} := \left\{ p = \sum_{i=0}^{\infty} a_i \cdot x^i \in \mathbb{C}[[x]] \,\middle|\, p \text{ is convergent} \right\}.$$

Proposition. i) $\mathbb{C}\{x\} \subset \mathbb{C}[[x]]$ *is a subring.*
ii) $\mathbb{C}[x] \subset \mathbb{C}\{x\}$.
iii) $\mathbb{C}\{x\}$ *is a local ring with maximal ideal* $\langle x \rangle$.

iv) Let k be a field. For $a \in k$, the principal ideal $\langle x - a \rangle$ is a maximal ideal of $k[x]$. If $a_1 \neq a_2$, then $\langle x - a_1 \rangle \neq \langle x - a_2 \rangle$. This means that $k[x]$ is not a local ring. If k is **algebraically closed** (see [31], Satz IV.5.11), then all maximal ideals are of the form $\langle x - a \rangle$, $a \in k$.

Note. If k is algebraically closed, a non-constant polynomial $p \in k[x]$ is irreducible[5] if and only if its degree is 1.

I.4.12 Exercises[6]. The ring $\mathbb{C}\{x\}$ may be interpreted in terms of complex functions. Let

$$\mathfrak{S} := \{ (U, f) \,|\, U \subset \mathbb{C} \text{ open}, 0 \in U, f \colon U \longrightarrow \mathbb{C} \text{ holomorphic} \}.$$

We introduce the following relation on $\mathfrak{S}$:

$$(U, f) \sim (V, g) \quad :\Longleftrightarrow \quad \exists 0 \in W \subset U \cap V \text{ open} : \; f_{|W} \equiv g_{|W}.$$

i) Prove that "$\sim$" is an equivalence relation on $\mathfrak{S}$.

The equivalence classes are *germs* of holomorphic functions at 0. We write the equivalence class of $(U, f) \in \mathfrak{S}$ as $[U, f]$.

ii) Show that addition and multiplication of complex functions endow the set $\overline{\mathfrak{S}}$ of germs of holomorphic functions at 0 with the structure of a ring and that

$$\begin{array}{rcl} \mathrm{ev} \colon \overline{\mathfrak{S}} & \longrightarrow & \mathbb{C} \\ [U, f] & \longmapsto & f(0) \end{array}$$

is a ring homomorphism.[7]

[5] See Page 20 for the definition of an irreducible element in an integral domain.
[6] The necessary prerequisites for these exercises are contained [31], especially Kapitel IV
[7] Note that 0 is the only point at which it makes sense to evaluate a germ.

iii) For a germ $[U, f] \in \overline{\mathfrak{S}}$, let $T_{f,0}$ be its Taylor series with expansion point 0. Show that

$$\begin{array}{rcl} T : \overline{\mathfrak{S}} & \longrightarrow & \mathbb{C}\{x\} \\ [U, f] & \longmapsto & T_{f,0} \end{array}$$

is an isomorphism of rings, such that

$$T^{-1}(\langle x \rangle) = \{\, [U, f] \in \overline{\mathfrak{S}} \,|\, \mathrm{ev}(f) = 0 \,\}.$$

This exercise illustrates the name "local": It comes exactly from the context of such rings of germs of functions at a point, here the origin. Germs are, roughly speaking, the local functions at the given point.

I.4.13 Exercises (Prime ideals). Determine all prime and maximal ideals of the following rings: i) $\mathbb{R}$, ii) $\mathbb{Z}$, iii) $\mathbb{C}[x]$, and iv) $\mathbb{R}[x]$.

I.4.14 Exercise. Let $R \neq \{0\}$ be a ring. Show that the set Σ of prime ideals of R has a minimal element with respect to inclusion.

I.4.15 Exercises. Let k be a field.

i) Prove that the polynomial ring $k[x]$ over k is a principal ideal domain.

ii) Prove that k is algebraically closed if and only if, for every maximal ideal $\mathfrak{m} \subset k[x]$, there exists an element $a \in k$ with $\mathfrak{m} = \langle x - a \rangle$.

I.4.16 Exercises (Boolean rings). i) Let R be a ring such that every element $x \in R$ satisfies $x^n = x$ for some $n > 1$. Show that every prime ideal $\mathfrak{p}$ of R is a maximal ideal.

ii) A ring R is called *boolean*[8], if every element $x \in R$ verifies $x^2 = x$. Show that $2x = x + x = 0$ holds true for every element x in a boolean ring R.

iii) Let $R \neq \{0\}$ be a boolean ring and $\mathfrak{p} \subset R$ a prime ideal. Show that $\mathfrak{p}$ is a maximal ideal and that $R/\mathfrak{p}$ is a field of two elements.

The Spectrum of a Ring

The following set of exercises contains the first steps of associating with a ring a geometric object which contains all the information about the ring.

I.4.17 Exercises (The spectrum of a ring). Let $R \neq \{0\}$ be a ring. We define

$$\mathrm{Spec}(R) := \{\, \mathfrak{p} \subset R \,|\, \mathfrak{p} \text{ is a prime ideal} \,\}.$$

For an ideal $I \subset R$, we set

$$V(I) := \{\, \mathfrak{p} \in \mathrm{Spec}(R) \,|\, I \subset \mathfrak{p} \,\}.$$

Establish the following properties:

i) $V(0) = \mathrm{Spec}(R)$, $V(R) = \emptyset$.

ii) Let I_k, $k \in K$, be a family of ideals in R. Their *sum* $\sum\limits_{k\in K} I_k$ is the ideal of all linear combinations $\sum\limits_{k\in K} a_k$ with $a_k \in I_k$, $k \in K$, almost all zero (see also Page 33). Then,

$$V\Big(\sum_{k\in K} I_k\Big) = \bigcap_{k\in K} V(I_k).$$

[8] George Boole (1815 - 1864), English mathematician, philosopher and logician.

iii) For two ideals I and J of R,

$$V(I \cap J) = V(I) \cup V(J).$$

Remark. Call a subset $Z \subset \mathrm{Spec}(R)$ *Zariski*[9] *closed*, if there is an ideal $I \subset R$ with $Z = V(I)$ and a subset $U \subset \mathrm{Spec}(R)$ *Zariski open*, if the complement $Z = \mathrm{Spec}(R) \setminus U$ is Zariski closed. The above properties say:

i') The empty set and $\mathrm{Spec}(R)$ are Zariski open.

ii') The union of an arbitrary family of Zariski open subsets is Zariski open.

iii') The intersection of two Zariski open subsets is Zariski open.

So,

$$\mathscr{T} := \{\, U \subset \mathrm{Spec}(R) \mid U \text{ is Zariski open} \,\}$$

is a topology (see [18], Section 1.2) on $\mathrm{Spec}(R)$, the *Zariski topology*.

iv) Let $f\colon R \longrightarrow S$ be a homomorphism of rings. Define

$$\begin{array}{rcl} f^{\#}\colon \mathrm{Spec}(S) & \longrightarrow & \mathrm{Spec}(R) \\ \mathfrak{p} & \longmapsto & f^{-1}(\mathfrak{p}). \end{array}$$

Show that $f^{\#}$ is continuous in the Zariski topology.

I.4.18 Exercises (Principal open subsets). Let R be a ring and $X := \mathrm{Spec}(R)$. For $f \in R$, set $X_f := X \setminus V(\langle f \rangle)$.

i) Show that the X_f, $f \in R$, form a *basis* for the Zariski topology, i.e., for every Zariski open subset $U \subset X$, there is a subset $F \subset R$, such that

$$U = \bigcup_{f \in F} X_f.$$

Hint: For an ideal $I \subset R$, one has $I = \sum_{f \in I} \langle f \rangle$.

ii) Prove that $X_f \cap X_g = X_{f \cdot g}$, $f, g \in R$.

iii) Check that $X_f = X$ holds if and only if f is a unit.

iv) Show that X is *quasi-compact*, i.e., every open covering of X possesses a **finite** subcovering.

I.4.19 Exercises. Let R be a ring and $X := \mathrm{Spec}(R)$.

i) Show that, for an ideal $I \in R$, one has $V(I) = V(\sqrt{I})$.

ii) For a subset $Z \subset X$, define the ideal

$$I(Z) := \bigcap_{\mathfrak{p} \in Z} \mathfrak{p}.$$

Show that

$$I(V(I)) = \sqrt{I}$$

holds for every ideal $I \subset R$.

iii) Let $Z \subset X$ be a closed subset. Prove that

$$V(I(Z)) = Z.$$

[9] Oscar Zariski (1899 - 1986), was an American mathematician of Russian origin.

I.4.20 Exercises (Boolean rings). Let R be a boolean ring (see Exercise I.4.16). Set $X := \mathrm{Spec}(R)$.

i) Show that, for $f \in R$, the set X_f is both open and closed (in the Zariski topology).

ii) Let $f_1,...,f_n \in R$ and

$$I := \langle f_1, ..., f_n \rangle := \langle f_1 \rangle + \cdots + \langle f_n \rangle.$$

Prove that I is a principal ideal.

iii) Suppose $f_1,...,f_n \in R$. Demonstrate that there is an element $f \in R$, such that

$$X_f := X_{f_1} \cup \cdots \cup X_{f_n}.$$

I.4.21 Exercises (The spectrum of $\mathbb{Z}[x]$). The aim of this exercise is to determine all prime and maximal ideals of $\mathbb{Z}[x]$.

i) Show that a prime ideal $\mathfrak{p}$ which is **not** principal contains two **irreducible** polynomials f_1 and f_2 with $f_1 \nmid f_2$ and $f_2 \nmid f_1$.

ii) Explain why the greatest common divisor of f_1 and f_2 in $\mathbb{Q}[x]$ is 1, so that there are polynomials $g_1, g_2 \in \mathbb{Q}[x]$ with $f_1 \cdot g_1 + f_2 \cdot g_2 = 1$.

iii) Deduce from ii) that the intersection $\mathbb{Z} \cap \mathfrak{p}$ is non-zero and therefore of the form $\langle p \rangle$ for some prime number $p \in \mathbb{Z}$.

iv) Infer that a non-principal prime ideal $\mathfrak{p} \subset \mathbb{Z}[x]$ is of the form $\langle p, f \rangle$ where $p \in \mathbb{Z}$ is a prime number and $f \in \mathbb{Z}[x]$ is a primitive polynomial (see Page 28) of positive degree, such that its class $\overline{f} \in \mathbb{F}_p[x]$ is irreducible. Is such an ideal maximal?

v) Now, describe all prime and all maximal ideals of $\mathbb{Z}[x]$.

Remark. A picture of $\mathrm{Spec}(\mathbb{Z}[x])$ may be found in the books [21], Example H, page 74f, and [6], Section II.4.3.

I.4.22 Exercise (The spectrum of a product). Let R_1, R_2 be non-zero rings. Describe the spectrum of $R_1 \times R_2$ in terms of the spectra of R_1 and R_2. (Don't forget to think about the topology of the respective spaces.)

I.5 Irreducible Elements and Prime Elements

In this section, R is assumed to be an **integral domain**. The prime factorization in the ring of integers ([30], Kapitel I) is the most important tool of elementary number theory. To state it, we just need the relation of divisibility among two integers. This can equally well be defined and studied in any integral domain.

I.5.1 Question. Is there a prime factorization in R?

We will see that the answer is **no**, in general. This motivates two developments. First, we may single out the class of rings for which the answer is yes, so-called **factorial rings**, and study some examples and properties of these rings. Second, we can generalize the concept of prime factorization by allowing also ideals in the factorization. This will lead to the **primary decomposition** of ideals (see Section II.4).

Let $a, b \in R$. We say that *b divides a*, if there exists an element $c \in R$, such that

$$a = b \cdot c.$$

I.5.2 Notation. $b|a$.

The reader may check the following properties of the divisibility relation (see [30], Eigenschaften I.2.2, for the corresponding statements in the ring $\mathbb{Z}$.)

I.5.3 Properties. i) *Let $a \in R$. Then,* $1|a$ *and* $a|a$.

ii) *Let $a, b, c \in R$. If $c|b$ and $b|a$, then also $c|a$.*

iii) *Let $a_1, ..., a_n, b \in R$ be elements with $b|a_i$, $i = 1, ..., n$. For all $r_1, ..., r_n \in R$, we have*

$$b \Big| (r_1 \cdot a_1 + \cdots + r_n \cdot a_n).$$

iv) *Let $b \in R$ be an element with $b|1$. Then, b is a unit of R.*

v) *Let $a \in R$ and $u \in R^\star$ be a unit. For every $b \in R$, the relation $b|a$ implies $(b \cdot u)|a$ and $b|(a \cdot u)$.*

vi) *Let $a, b \in R$. Then,*

$$b|a \quad \Longleftrightarrow \quad \langle a \rangle \subset \langle b \rangle.$$

Two elements $a, b \in R$ are *associated*, if there exists a unit $u \in R^\star$, such that

$$a = b \cdot u.$$

I.5.4 Notation. $a \sim b$.

I.5.5 Lemma. i) *The relation "$\sim$" is an equivalence relation.*

ii) *Let $a, b \in R$. Then, the following conditions are equivalent: $\star$) $a \sim b$, $\star\star$) $a|b \wedge b|a$, and $\star \star \star$) $\langle a \rangle = \langle b \rangle$.*

Proof. i) This is very easy to check directly. It is also an immediate consequence of ii).

ii) Condition $\star$) clearly implies $\star\star$). Condition $\star\star$) and $\star \star \star$) are equivalent by Property I.5.3, vi). So, assume that $a|b$ and $b|a$ and let $r, s \in R$ be such that $a = b \cdot r$ and $b = a \cdot s$. Then,

$$a = (r \cdot s) \cdot a.$$

This is equivalent to

$$(1 - r \cdot s) \cdot a = 0.$$

Since R is an integral domain,[10] we have $a = 0$ or $1 = r \cdot s$. In the first case, $b = a \cdot s = 0$. In the second case, r and s are units of R. In both cases, a and b are associated. □

We have now two options to generalize the notion of a prime number in the ring of integers (compare [30], Definition I.3.1 and Satz I.4.5): An element $p \in R$ is called a *prime element*, if $p \neq 0$, $p \notin R^\star$, and

$$\forall a, b \in R: \quad p|(a \cdot b) \Longrightarrow p|a \text{ or } p|b.$$

An element $q \in R$ is *irreducible*, if$p \neq 0$, $p \notin R^\star$, and

$$\forall a, b \in R: \quad q = a \cdot b \Longrightarrow a \in R^\star \text{ or } b \in R^\star.$$

In other words, the only divisors of q are units or associated elements.

[10] Here, our general assumption becomes important.

I.5.6 Examples. i) Let k be a field. Then, there are no prime or irreducible elements in k.

ii) An integer $m \in \mathbb{Z}$ is an irreducible element if and only if it is a prime number. A prime number is a prime element, by [30], Satz I.4.5. Since a prime element is irreducible (Proposition I.5.7, i), every prime element in $\mathbb{Z}$ is a prime number.

I.5.7 Proposition. *Let $p \in R$ be an element.*

i) *If p is a prime element, then p is irreducible.*

ii) *The element p is a prime element if and only if $\langle p\rangle$ is a prime ideal*

iii) *The element p is irreducible if and only if there is no element $a \in R$ with*

$$\langle p\rangle \subsetneq \langle a\rangle \subsetneq R,$$

*i.e., if $\langle p\rangle$ is maximal among the proper **principal** ideals of R.*

Proof. i) Let $a, b \in R$ be such that $p = a \cdot b$. Since $p|p$, we have $p|(a \cdot b)$ and $p|a$ or $p|b$. Let us assume $p|a$ and let $c \in R$ be such that $a = p \cdot c$. We find $p = (b \cdot c) \cdot p$. Since $p \neq 0$ and R is an integral domain, it follows that $b \cdot c = 1$ and that b is a unit.

ii) "$\Longrightarrow$": For a, b with $a \cdot b \in \langle p\rangle$, we have $p|(a \cdot b)$. Since p is a prime element, this implies $p|a$ or $p|b$, i.e., $a \in \langle p\rangle$ or $b \in \langle p\rangle$. The converse is similar.

iii) "$\Longrightarrow$": Suppose $a \in R$ is an element with $\langle p\rangle \subset \langle a\rangle$, i.e., $a|p$. Let $b \in R$ be such that $a \cdot b = p$. Then, $a \in R^\star$ or $b \in R^\star$, that is $\langle a\rangle = R$ or $\langle a\rangle = \langle p\rangle$.

"$\Longleftarrow$": For $a, b \in R$ with $p = a \cdot b$, we have $\langle p\rangle \subset \langle a\rangle$. By assumption, $\langle a\rangle = \langle p\rangle$ or $\langle a\rangle = R$. In the first case $b \in R^\star$, and, in the second case, $a \in R^\star$. □

I.5.8 Corollary. *Suppose R is a principal ideal domain. Then, any irreducible element $p \in R$ is a prime element.*

I.5.9 Important example. We look at the ring

$$R := \mathbb{Z}\left[\sqrt{-5}\right] := \left\{ k + l \cdot \sqrt{-5} \in \mathbb{C} \,\middle|\, k, l \in \mathbb{Z} \right\}.$$

It is a subring of the field $\mathbb{C}$ of complex numbers and therefore an integral domain. In order to study divisibility among elements in R, we introduce the *norm map*

$$\begin{array}{rcl} N\colon R & \longrightarrow & \mathbb{Z} \\ k + l \cdot \sqrt{-5} & \longmapsto & k^2 + 5 \cdot l^2. \end{array}$$

It satisfies

$$\forall a, b \in R: \quad N(a \cdot b) = N(a) \cdot N(b). \tag{I.5}$$

We can list elements of small norm:

- ⋆ An element of $a \in R$ has norm 1 if and only if $a = \pm 1$.
- ⋆ There are no elements $a \in R$ of norm 2 or 3.
- ⋆ The elements of norm 9 are ± 3 and $\pm(2 \pm \sqrt{-5})$.

This has already several interesting consequences:

Claim. *The units of R are ± 1.*

The elements ± 1 are clearly units of R. Conversely, (I.5) shows that a unit $u \in R$ satisfies $N(u) = 1$. Our previous observation says that this is equivalent to $u = \pm 1$. ✓

Claim. *The elements* ± 3 *and* $\pm(2 \pm \sqrt{-5})$ *are irreducible.*

We explain the argument for 3. Equation (I.5) shows that a divisor a of 3 has norm 1 or 9, because there is no element of norm 3. If $N(a) = \pm 1$, then $a = \pm 1$. If $N(a) = 9$, then $a = \pm 3$ or $a = \pm(2 \pm \sqrt{-5})$. The elements $\pm(2 \pm \sqrt{-5})$ do not divide 3. ✓

Claim. *The elements* ± 3 *and* $\pm(2 \pm \sqrt{-5})$ *are not prime.*

Again, we show the assertion for 3. We use the equation

$$9 = 3 \cdot 3 = (2 - \sqrt{-5}) \cdot (2 + \sqrt{-5}). \tag{I.6}$$

It shows $3|9$. By our previous discussion, $3 \nmid (2 \pm \sqrt{-5})$. ✓

I.5.10 Exercise. Prove that every element $a \in R$ which is neither zero nor a unit can be written as a product of irreducible elements.

I.5.11 Remark. i) There are several related observations resulting from our discussion, in particular, Equation (I.6). Every element in R may be written as a product of irreducible elements, but this factorization is, in general, not unique up to associated element. For example, 9 has two essentially distinct factorizations. Not every irreducible element is a prime element. There are elements such as 9 which cannot be written as products of prime elements. We will clarify these matters in the following section.

ii) The fact that there are numbers which cannot be written as products of prime elements led to the idea of "ideal numbers" and eventually of ideals which may be used to obtain such a factorization nevertheless. An example looks as follows (see Exercise I.8.9): The ideals

$$\mathfrak{p}_1 := \langle\, 3, 2 + \sqrt{-5} \,\rangle \quad \text{and} \quad \mathfrak{p}_2 := \langle\, 3, 2 - \sqrt{-5} \,\rangle$$

are prime ideals in R with

$$\langle 9 \rangle = \mathfrak{p}_1^2 \cdot \mathfrak{p}_2^2 = \mathfrak{p}_1^2 \cap \mathfrak{p}_2^2.$$

iii) The ring R is the **ring of integers** in the **number field** $\mathbb{Q}(\sqrt{-5})$. Every number field K has such a ring of integers $\mathcal{O}_K$. The question whether there is a prime factorization or not in $\mathcal{O}_K$ is of great importance for algebraic number theory. It is, for example, related to the famous equation $x^p + y^p = z^p$, p a prime number, of Fermat.[11] Chapter I of [23] contains detailed information on these topics.

I.6 Factorial Rings

In this section, R will be an **integral domain**. We will study the following properties:

(F1) For every element $a \in R \backslash (\{0\} \cup R^\star)$, there are a natural number $r \geq 1$ and **irreducible** elements $q_1, ..., q_r \in R$ with

$$a = q_1 \cdot \cdots \cdot q_r.$$

[11] Pierre de Fermat (1601 or 1607/8 - 1665) was a French lawyer and mathematician.

(F2) For every element $a \in R \setminus (\{0\} \cup R^\star)$, there are a natural number $r \geq 1$ and **prime** elements $p_1, ..., p_r \in R$ with

$$a = p_1 \cdot \dots \cdot p_r.$$

(F3) If we are given natural numbers $r, t \geq 1$ and irreducible elements $q_1, ..., q_r, s_1, ..., s_t \in R$ with

$$q_1 \cdot \dots \cdot q_r = s_1 \cdot \dots \cdot s_t,$$

then $r = t$ and there is a permutation $\sigma\colon \{1, ..., r\} \longrightarrow \{1, ..., r\}$, such that

$$\forall i \in \{1, ..., r\}: \quad q_i \sim s_{\sigma(i)}.$$

(F4) Every irreducible element of R is a prime element.

I.6.1 Theorem. *The following conditions on the integral domain R are equivalent:*
i) *The properties* (F1) *and* (F3) *hold in R.*
ii) *The properties* (F1) *and* (F4) *hold in R.*
iii) *Property* (F2) *holds in R.*

Proof. "i)$\Longrightarrow$ii)". Let q be an irreducible element and $a, b \in R$ ring elements with $q|a \cdot b$. If $a = 0$ or $b = 0$, there is nothing to show. If $a \in R^\star$, it follows that $q|b$, and, if $b \in R^\star$, we have $q|a$. So, we may assume $a, b \in R \setminus (\{0\} \cup R^\star)$. Let $c \in R$ be such that

$$a \cdot b = q \cdot c.$$

Since q is irreducible, we must have $c \notin R^\star$ and, obviously, $c \neq 0$. By (F1), there are natural numbers $r, t, v \geq 1$ and irreducible elements $q_1, ..., q_r, s_1, ..., s_t, u_1, ..., u_v \in R$ with

$$a = q_1 \cdot \dots \cdot q_r, \quad b = s_1 \cdot \dots \cdot s_t, \quad \text{and} \quad c = u_1 \cdot \dots \cdot u_v.$$

The identity

$$q_1 \cdot \dots \cdot q_r \cdot s_1 \cdot \dots \cdot s_t = q \cdot u_1 \cdot \dots \cdot u_v$$

and (F3) show that there is an index $i_0 \in \{1, ..., r\}$ or an index $j_0 \in \{1, ..., t\}$ with

$$q \sim q_{i_0} \quad \text{or} \quad q \sim s_{j_0},$$

so that

$$q|a \quad \text{or} \quad q|b.$$

"ii)$\Longrightarrow$iii)". This is trivial.

"iii)$\Longrightarrow$i)". By Proposition I.5.7, i), every prime element of R is irreducible. This implies that (F1) holds true in R.

Claim. *Property* (F4) *is verified by R.*

In fact, let $q \in R$ be an irreducible element. There are a natural number $r \geq 1$ and prime elements $p_1, ..., p_r$ with

$$q = p_1 \cdot \dots \cdot p_r.$$

Since prime elements aren't units, the irreducibility of q implies $r = 1$ and $q = p_1$. ✓

Now, let $q_1, ..., q_r, s_1, ..., s_t \in R$ be irreducible elements with

$$q_1 \cdot \cdots \cdot q_r = s_1 \cdot \cdots \cdot s_t.$$

We proceed by induction on r. If $r = 1$, then $t = 1$, because q_1 is irreducible. In general, there is an index $i \in \{1, ..., r\}$ with $s_1 | q_i$, because, according to (F4), s_1 is a prime element. Since q_i is irreducible, this implies $s_1 \sim q_i$. We may clearly assume $i = 1$. There is a unit $u \in R$ with $s_1 = u \cdot q_1$. We infer

$$q_1 \cdot q_2 \cdot \cdots \cdot q_r = q_1 \cdot (u \cdot s_2) \cdot s_3 \cdot \cdots \cdot s_t.$$

Using the fact that R is an integral domain, this equation implies

$$q_2 \cdot \cdots \cdot q_r = (u \cdot s_2) \cdot s_3 \cdot \cdots \cdot s_t,$$

and we may conclude by induction. □

A *factorial ring* is an integral domain which satisfies Conditions (F1) - (F4).

I.6.2 Exercise (Chains of ideals in principal ideal domains). Let R be a principal ideal domain.

i) Let

$$\langle r_1 \rangle \subset \langle r_2 \rangle \subset \cdots \subset \langle r_k \rangle \subset \langle r_{k+1} \rangle \subset \cdots$$

be an ascending chain of (principal) ideals. Show that this sequence becomes *stationary*,[12] i.e., there is an index $k_0 \in \mathbb{N}$, such that

$$\langle r_k \rangle = \langle r_{k_0} \rangle \quad \text{for all } k \geq k_0.$$

ii) Use Part i) to show that (F1) (see Page 22) holds in a principal domain (compare [8], Chapter II, Lemma 4.3.4) and conclude that a principal ideal domain is factorial.

I.6.3 Example. Let k be a field. By Exercise I.4.15, i), the polynomial ring $k[x]$ is a principal ideal domain and, therefore, by the previous exercise a factorial ring.

The next aim is to prove the existence of more factorial rings.

I.6.4 Theorem (Gauß)**.** *Let R be a factorial ring. Then, the polynomial ring $R[x]$ is factorial, too.*

By Example I.6.3, the theorem is true, if R is a field. We would like to use this result. This is possible, because we may associate with any **integral domain** in a canonical way a field.

Quotient Fields

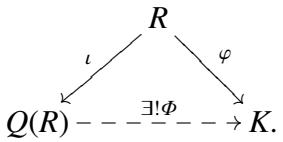
In order to define what a quotient field is, we will recur again to a universal property. Let R be an integral domain. A *quotient field* of R is a pair $(Q(R), \iota)$ which consists of a field $Q(R)$ and an injective homomorphism $\iota\colon R \longrightarrow Q(R)$ and satisfies the following

[12] This property will be studied in detail in Chapter II.1.

property: For every field K and every injective homomorphism $\varphi\colon R \longrightarrow K$, there is a unique homomorphism $\Phi\colon Q(R) \longrightarrow K$ with

$$\Phi \circ \iota = \varphi.$$

The corresponding diagram looks as follows:



The universal property expresses that $Q(R)$ is the smallest field that contains R. In order to construct it, we obviously have to invert the elements of $R \setminus \{0\}$. The formal construction proceeds along the lines of the construction of the field $\mathbb{Q}$ of rational numbers from the ring $\mathbb{Z}$ of integers ([27], Abschnitt 1.5).

For $(a, b), (c, d) \in R \times (R \setminus \{0\})$, we write

$$(a, b) \sim (c, d) \quad :\Longleftrightarrow \quad a \cdot d = b \cdot c.$$

I.6.5 Proposition. *The relation "$\sim$" is an equivalence relation on $R \times (R \setminus \{0\})$.*

Proof. We leave this as an exercise. □

In the following, we write

$$\frac{a}{b}$$

for the equivalence class $[a, b]$ of $(a, b) \in R \times (R \setminus \{0\})$. We will also abusively write a for the class $a/1$, $a \in R$. In this notation, we declare the *addition*

$$\begin{array}{rcl} +\colon Q(R) \times Q(R) & \longrightarrow & Q(R) \\ \left(\frac{a}{b}, \frac{c}{d}\right) & \longmapsto & \frac{a \cdot d + b \cdot c}{b \cdot d} \end{array}$$

and the *multiplication*

$$\begin{array}{rcl} \cdot\colon Q(R) \times Q(R) & \longrightarrow & Q(R) \\ \left(\frac{a}{b}, \frac{c}{d}\right) & \longmapsto & \frac{a \cdot c}{b \cdot d}. \end{array}$$

I.6.6 Theorem. i) *The tuple $(Q, 0, +, \cdot, 1)$ is a field.*

ii) *The map*

$$\begin{array}{rcl} \iota\colon R & \longrightarrow & Q(R) \\ a & \longmapsto & a = \frac{a}{1} \end{array}$$

is an injective ring homomorphism.[13]

iii) *The pair $(Q(R), \iota)$ is a quotient field of R.*

Proof. Everything works as for $\mathbb{Z}$ and $\mathbb{Q}$. So, we leave the proof as an exercise. □

[13] This justifies our abusive notation.

Greatest Common Divisors

We need some more concepts in factorial rings which generalize their counterparts in the ring $\mathbb{Z}$ of integers in order to compare factorizations in the rings $R[x]$ and $Q(R)[x]$.

For ring elements $a_1, ..., a_n \in R$, a *common divisor* of $a_1, ..., a_n$ is an element $d \in R$ with

$$d|a_i, \quad i = 1, ..., n,$$

and

$$\mathrm{cd}(a_1, ..., a_n) := \{\, d \in R \,|\, d \text{ is a common divisor of } a_1, ..., a_n \,\}$$

is the *set of common divisors* of $a_1, ..., a_n$.

I.6.7 Properties. *Let $n \geq 1$ be a positive natural number, $a_1, ..., a_n \in R$ ring elements and $u \in R^\star$ a unit.*

i) *For every ring element $d \in R$ we have*

$$d \in \mathrm{cd}(a_1, ..., a_n) \quad \Longleftrightarrow \quad \langle d \rangle \supset \langle a_1 \rangle + \cdots + \langle a_n \rangle.$$

ii) *It is always true that $R^\star \subset \mathrm{cd}(a_1, ..., a_n)$.*
iii) *We have $\mathrm{cd}(a_1, ..., a_n, u) = R^\star$.*
iv) *We have $\mathrm{cd}(a_1, ..., a_n, 0) = \mathrm{cd}(a_1, ..., a_n)$.*
v) *The property $0 \in \mathrm{cd}(a_1, ..., a_n)$ holds if and only if $a_1 = \cdots = a_n = 0$.*

Proof. For i), observe that, for $a \in R$, $d|a$ holds if and only if $\langle d \rangle \supset \langle a \rangle$ (Property I.5.3, vi). So,

$$d \in \mathrm{cd}(a_1, ..., a_n) \quad \Longleftrightarrow \quad \langle d \rangle \supset (\langle a_1 \rangle \cup \cdots \cup \langle a_n \rangle).$$

The fact that $\langle d \rangle$ is an ideal implies

$$\langle d \rangle \supset (\langle a_1 \rangle \cup \cdots \cup \langle a_n \rangle) \quad \Longleftrightarrow \quad \langle d \rangle \supset \langle a_1 \rangle + \cdots + \langle a_n \rangle.$$

The rest of the asserted properties is straightforward to verify, and we leave the proofs to the reader. □

The elements $a_1, ..., a_n \in R$ are *coprime*, if

$$\mathrm{cd}(a_1, ..., a_n) \subset R^\star.$$

By Property I.6.7, ii), this condition is equivalent to $\mathrm{cd}(a_1, ..., a_n) = R^\star$.

Given $a_1, ..., a_n \in R$, a *greatest common divisor* of $a_1, ..., a_n$ is an element $d \in \mathrm{cd}(a_1, ..., a_n)$ with the property

$$\forall d' \in \mathrm{cd}(a_1, ..., a_n): \quad d'|d.$$

We let

$$\mathrm{gcd}(a_1, ..., a_n) = \{\, d \in R \,|\, d \text{ is a greatest common divisor of } a_1, ..., a_n \,\}$$

be the *set of greatest common divisors* of $a_1, ..., a_n$.

I.6.8 Properties. *Let $a_1, ..., a_n \in R$ be ring elements.*

i) *Let $d, d' \in R$ be elements with $d \in \gcd(a_1, ..., a_n)$ and $d \sim d'$. Then, $d' \in \gcd(a_1, ..., a_n)$.*

ii) *If $d, d' \in \gcd(a_1, ..., a_n)$ are greatest common divisors of $a_1, ..., a_n$, then $d \sim d'$, i.e., a greatest common divisor is determined up to units.*

iii) *Suppose there is an index $i_0 \in \{1, ..., n\}$ with $a_{i_0} \neq 0$ and $d \in \gcd(a_1, ..., a_n)$. Then, the elements $a'_1, ..., a'_n \in R$ with $a_i = d \cdot a'_i$ are coprime.*

Proof. i) This is obvious. ii) This is a direct consequence of Property I.5.3, v). iii) Let $t \in \mathrm{cd}(a'_1, ..., a'_n)$ and write $a'_i = a''_i \cdot t$ for a suitable ring element $a''_i \in R$, $i = 1, ..., n$. It follows that $d \cdot t \in \mathrm{cd}(a_1, ..., a_n)$. By definition of a greatest common divisor, $(d \cdot t)|d$. As usual, we infer that $t \in R^\star$ is a unit. So, we have shown $\mathrm{cd}(a'_1, ..., a'_n) \subset R^\star$ as required. □

The concept of a greatest common divisor has been defined in any integral domain. In general, it need not exist.

I.6.9 Example. We look again at the ring $\mathbb{Z}[\sqrt{-5}]$. The element $a = 9$ has the divisors ± 1, ± 3, $\pm(2 \pm \sqrt{-5})$, ± 9, and the element $b := 3 \cdot (2 + \sqrt{-5})$ has the divisors ± 1, ± 3, $\pm(2 + \sqrt{-5})$ and $\pm 3 \cdot (2 + \sqrt{-5})$. Since the elements 3 and $(2 + \sqrt{-5})$ are not associated, it follows that the elements a and b do not have a greatest common divisor.

I.6.10 Proposition. *Assume that R is a **factorial** ring. Then, for $n \geq 1$, ring elements $a_1, ..., a_n$ which are not all zero do have a greatest common divisor.*

Proof. By Property I.6.7, iv) and v), we may suppose $a_i \neq 0$, $i = 1, ..., n$, and by Property I.6.7, iii), we may assume $a_i \notin R^\star$, $i = 1, ..., n$. Since R is factorial, we may find prime elements $p_1, ..., p_r$ with $p_i \not\sim p_j$ for $1 \leq i < j \leq r$ and natural numbers $k_j(a_i)$, $j = 1, ..., r$, $i = 1, ..., n$, with

$$a_i \sim p_1^{k_1(a_i)} \cdot \cdots \cdot p_r^{k_r(a_i)}, \quad i = 1, ..., n.$$

Now, set

$$m_j := \min\{ k_j(a_i) \mid i = 1, ..., n \}, \quad j = 1, ..., r.$$

It is readily verified that

$$d := p_1^{m_1} \cdot \cdots \cdot p_r^{m_r}$$

is a greatest common divisor of $a_1, ..., a_n$. □

I.6.11 Lemma. *Let R be a **factorial ring**. Then, every element $x \in Q(R)$ can be written as $x = a/b$ with $a \in R$ and $b \in R \setminus \{0\}$ coprime.*

Proof. We pick $\alpha \in R$ and $\beta \in R \setminus \{0\}$. By Proposition I.6.10, α and β have a greatest common divisor. Let d be one, $a \in R$ and $b \in R \setminus \{0\}$ be elements with $\alpha = a \cdot d$ and $\beta = b \cdot d$. According to Property I.6.8, iii), a and b are coprime. It is also clear that $x = \alpha/\beta = a/b$. □

Primitive Polynomials

For the rest of this section, we assume that R is a **factorial ring**. We need to compare irreducible elements in the rings $R[x]$ and $Q(R)[x]$. The key concept for doing so is the one of a **primitive polynomial**: A polynomial $f \in R[x]$ is *primitive*, if its coefficients are coprime.

I.6.12 Example. If k is a field, then every polynomial $f \in k[x] \setminus \{0\}$ is primitive.

I.6.13 Lemma. i) *Let $f \in R[x]$ be a polynomial of positive degree. If f is irreducible, then f is primitive.*

ii) *If $f \in R[x]$ is a primitive polynomial and f is irreducible in $Q(R)[x]$, then f is irreducible in $R[x]$.*

In i), we need to assume that f is non-constant, because the element $2 \in \mathbb{Z}[x]$ is irreducible but not primitive. Part ii) does not work, if we don't assume that f is primitive. In fact, the polynomial $2x+2 \in \mathbb{Q}[x]$ is irreducible. In $\mathbb{Z}[x]$, the equation $2\cdot(x+1) = 2x+2$ expresses $2x+2$ as a product of two non-units, so that $2x+2$ is not an irreducible element of $\mathbb{Z}[x]$. (This is the only subtlety of the lemma.)

Proof of Lemma I.6.13. i) Let d be a greatest common divisor of the coefficients of f. (This exists by Proposition I.6.10.) By Property I.6.8, iii), there is a primitive polynomial $g \in R[x]$ with $f = d \cdot g$. Since f is irreducible and $g \in R[x]$ is not a unit, because $\deg(g) = \deg(f) > 0$, d must be a unit.

ii) Let $g, h \in R[x]$ polynomials with $f = g \cdot h$. This is also an equation in $Q(R)[x]$. By assumption, $g \in Q(R)[x]^\star = Q(R) \setminus \{0\}$ or $h \in Q(R)^\star$. It suffices to treat the first case. We have $g \in R \setminus \{0\}$, and g clearly is a common divisor of the coefficients of f. Since f is primitive, we have $g \in R^\star = R[x]^\star$ as required. □

I.6.14 Lemma (Gauß)**.** *Let $f, g \in R[x]$ be primitive polynomials. Then, $f \cdot g \in R[x]$ is primitive, too.*

Proof. For every prime element $p \in R$, we have the surjection

$$\begin{aligned} \varrho_p \colon R[x] &\longrightarrow (R/\langle p\rangle)[x] \\ a_0 + a_1 \cdot x + \cdots + a_n \cdot x^n &\longmapsto [a_0] + [a_1] \cdot x + \cdots + [a_n] \cdot x^n. \end{aligned}$$

Formally, it is associated with the homomorphism $\pi_p \colon R \longrightarrow R/\langle p\rangle$ and the element $x \in (R/\langle p\rangle)[x]$ (see Page 5). Using prime factorization in R, we have the following:

$$\forall f \in R[x]: \quad f \text{ is primitive} \iff \forall \text{ prime elements } p \in R: \quad \varrho_p(f) \neq 0. \tag{I.7}$$

By assumption, we have $\varrho_p(f) \neq 0$ and $\varrho_p(g) \neq 0$, $p \in R$ a prime element. Now, $\langle p\rangle$ is a prime ideal (Proposition I.5.7, ii). So, $R/\langle p\rangle$ and $(R/\langle p\rangle)[x]$ are integral domains. The inequality

$$\forall \text{ prime elements } p \in R: \quad \varrho_p(f \cdot g) = \varrho_p(f) \cdot \varrho_p(g) \neq 0$$

gives the result. □

I.6.15 Remark. We can rephrase the above proof also in terms of ideals. The kernel $\mathfrak{p}$ of ϱ_p is a prime ideal (see Proposition I.4.1, i), $p \in R$ a prime element. In the proof, we have exploited the property

$$f \notin \mathfrak{p} \wedge g \notin \mathfrak{p} \quad \Longrightarrow \quad f \cdot g \notin \mathfrak{p}$$

of the prime ideal $\mathfrak{p}$.

I.6.16 Lemma. i) *For every polynomial $g \in Q(R)[x] \setminus \{0\}$, there is a number $a \in Q(R)$, such that the polynomial $a \cdot g$ belongs to $R[x]$ and is primitive.*

ii) *If $f, g \in R[x]$ are polynomials, g is primitive, and $a \in Q(R)$ is a number with $f = a \cdot g$, then $a \in R$.*

Proof. i) We write $g = \alpha_0 + \alpha_1 \cdot x + \cdots + \alpha_n \cdot x^n$ with $\alpha_0, ..., \alpha_n \in Q(R)$ and pick elements $r_i \in R$, $s_i \in R \setminus \{0\}$ with $\alpha_i = r_i/s_i$, $i = 0, ..., n$. Set $s := s_0 \cdot \cdots \cdot s_n$. Then, we obviously have $s \cdot g \in R[x] \setminus \{0\}$. Since R is factorial, we may find a greatest common divisor d of the coefficients of $s \cdot g$. There exists a polynomial $f \in R[x]$ with $s \cdot g = d \cdot f$. By Property I.6.8, iii), f is primitive. Altogether, we may choose $a = s/d$.

ii) The case $f = 0$ is trivial. Otherwise, we may write $a = r/s$ with $r, s \in R$ coprime (see Lemma I.6.11). The equation $f = a \cdot g$ may be rewritten as

$$s \cdot f = r \cdot g.$$

This shows that s divides all the coefficients of $r \cdot g$. Since s is coprime to r, prime factorization in R implies that s divides all the coefficients of g. The primitivity of g implies that s is a unit. So, $a = r/s \in R$ as asserted. □

The following result finally relates the irreducible elements of $R[x]$ and $Q(R)[x]$.

I.6.17 Proposition. i) *Let $f \in R[x]$ be a non-constant primitive polynomial and $g \in R[x]$. If the relation $f|g$ holds in $Q(R)[x]$, then it holds in $R[x]$, too.*

ii) *If $f \in R[x]$ is a non-constant irreducible polynomial, then f is irreducible as an element of $Q(R)[x]$.*

Proof. i) If $g = 0$, there is nothing to show. Otherwise, there is a polynomial $h \in Q(R)[x] \setminus \{0\}$ with $g = f \cdot h$. By Lemma I.6.16, i), there is a number $a \in Q(R)$, such that $a \cdot h$ is a primitive polynomial in $R[x]$. Now, we look at the equation

$$g = \frac{1}{a} \cdot f \cdot (a \cdot h).$$

By Lemma I.6.14, $f \cdot (a \cdot h)$ is primitive. According to Lemma I.6.16, ii), $1/a \in R$, so that $h = (1/a) \cdot (a \cdot h) \in R[x]$.

ii) Suppose we could write $f = g \cdot h$ with $g, h \in Q(R)[x]$. We pick $a \in Q(R)$, such that $a \cdot h \in R[x]$ is a primitive polynomial, and look at the equation

$$f = \left(\frac{1}{a} \cdot g\right) \cdot (a \cdot h).$$

By Part i), we have $(1/a) \cdot g \in R[x]$. Since f is irreducible as an element of $R[x]$, we conclude that $(1/a) \cdot g \in R^\star$ or $a \cdot h \in R^\star$. This implies $g \in Q(R)^\star$ or $h \in Q(R)^\star$. □

Proof of Theorem I.6.4. We will verify Conditions (F1) and (F3) (see Page 22f).

Step 1. We show that (F1) holds, i.e., that every element of $R[x] \setminus (\{0\} \cup R^\star)$ may be written as a product of irreducible elements. We do this by induction on the degree n.

***n* = 0.** Let $f \in R[x] \setminus (\{0\} \cup R^\star)$ be a non-zero constant. Since R is factorial, f can be written as a product of irreducible elements in R. Finally, every irreducible element of R is an irreducible element of $R[x]$.

***n* ⟶ *n* + 1.** Let $f \in R[x]$ be a polynomial of degree $n+1$. There are a ring element $a \in R$ and a primitive polynomial $g \in R[x]$ with $f = a \cdot g$. Since the assertion holds for a, it suffices to factorize g. If g is irreducible, there is nothing to show. If g is not irreducible, there exist elements $g_1, g_2 \in R[x] \setminus (\{0\} \cup R^\star)$ with $g = g_1 \cdot g_2$. Since g is primitive and g_1, g_2 aren't units, g_1 and g_2 cannot be constant. It follows $\deg(g_1) < \deg(g)$ and $\deg(g_2) < \deg(g)$. By induction hypothesis, g_1 and g_2 may be written as products of irreducible polynomials. The same is true for $g = g_1 \cdot g_2$.

Step 2. Here, we check (F3). Let $c_1, ..., c_m, d_1, ..., d_n \in R$ be irreducible elements and $p_1, ..., p_s, q_1, ..., q_t \in R[x] \setminus R$ be irreducible polynomials of positive degree, such that

$$c_1 \cdot \dots \cdot c_m \cdot p_1 \cdot \dots \cdot p_s = d_1 \cdot \dots \cdot d_n \cdot q_1 \cdot \dots \cdot q_t. \tag{I.8}$$

By Lemma I.6.13, i), the polynomials $p_1, ..., p_s$ and $q_1, ..., q_t$ are primitive. By Lemma I.6.14, the polynomials $p_1 \cdot \dots \cdot p_s$ and $q_1 \cdot \dots \cdot q_t$ are primitive, too. It is easy to infer from Equation (I.8) that

$$c_1 \cdot \dots \cdot c_m \sim d_1 \cdot \dots \cdot d_n.$$

Since R is a factorial ring, $m = n$ and there is a permutation $\sigma\colon \{1, ..., n\} \longrightarrow \{1, ..., n\}$ with

$$c_i \sim d_{\sigma(i)}, \quad i = 1, ..., n.$$

We conclude

$$p_1 \cdot \dots \cdot p_s \sim q_1 \cdot \dots \cdot q_t. \tag{I.9}$$

Now, we look at this relation in the ring $Q(R)[x]$. By Proposition I.6.17, ii), the polynomials $p_1, ..., p_s, q_1, ..., q_t$ are irreducible in $Q(R)[x]$. We already know that $Q(R)[x]$ is factorial (see Example I.6.3). From (I.9), we now infer that $s = t$ and that there is a permutation $\tau\colon \{1, ..., t\} \longrightarrow \{1, ..., t\}$ with

$$p_i \sim q_{\tau(i)} \text{ in } Q(R)[x], \quad i = 1, ..., t.$$

With Lemma I.5.5, ii), we rewrite this as

$$p_i | q_{\tau(i)} \text{ and } q_{\tau(i)} | p_i \text{ in } Q(R)[x], \quad i = 1, ..., t.$$

Next, Proposition I.6.17 shows

$$p_i | q_{\tau(i)} \text{ and } q_{\tau(i)} | p_i \text{ in } R[x],$$

and, thus, by Lemma I.5.5, ii),

$$p_i \sim q_{\tau(i)} \text{ in } R[x], \quad i = 1, ..., t.$$

This gives the assertion and concludes the proof. □

I.7 The Nilradical

I.7.1 Proposition. *Let R be a ring and*

$$\mathfrak{N} := \{\, a \in R \mid a \text{ is nilpotent} \,\}.$$

i) *The subset $\mathfrak{N}$ of R is an ideal.*
ii) *The quotient ring $R/\mathfrak{N}$ has no nilpotent element other than* 0.

Proof. i) Clearly, $0 \in \mathfrak{N}$. Suppose $a, b \in \mathfrak{N}$ and choose exponents $m \geq 1$ and $n \geq 1$ with $a^m = 0$ and $b^n = 0$. For $0 \leq i < m$, we have $m + n - 1 - i \geq n$. This shows that every summand of the right hand sum in

$$(a+b)^{m+n-1} = \sum_{i=0}^{m+n-1} \binom{m+n-1}{i} \cdot a^i \cdot b^{m+n-1-i}$$

is zero, so that $(a+b)^{m+n-1} = 0$ and $a + b \in \mathfrak{N}$. Assume $r \in R$ and $a \in \mathfrak{N}$ and let $n \geq 1$ be an exponent with $a^n = 0$. Then, $(r \cdot a)^n = r^n \cdot a^n = 0$ and $r \cdot a \in \mathfrak{N}$. In the special case $r = -1$, we get $-a \in \mathfrak{N}$.

ii) Let $a \in R$ be such that $[a] \in R/\mathfrak{N}$ is nilpotent. Let $n \geq 1$ be such that $[a^n] = [a]^n = 0$. This means $a^n \in \mathfrak{N}$. Hence, we may find an exponent $m \geq 1$ with

$$a^{m \cdot n} = (a^n)^m = 0.$$

This shows $a \in \mathfrak{N}$ and $[a] = 0$. □

The ideal $\mathfrak{N}$ is called the *nilradical* of R.

I.7.2 Proposition. *Let $R \neq \{0\}$ be a ring. Then, the nilradical is the intersection of all prime ideals in R:*

$$\mathfrak{N} = \bigcap_{\substack{\mathfrak{p} \subset R \\ \text{prime ideal}}} \mathfrak{p}.$$

Proof. We first show that the nilradical is contained in every prime ideal. To this end, let $a \in \mathfrak{N}$ be a nilpotent element, $n \geq 1$ an exponent with $a^n = 0$, and $\mathfrak{p} \subset R$ a prime ideal. We obviously have $a^n \in \mathfrak{p}$. So, we may define

$$l := \min\{\, m \geq 1 \mid a^m \in \mathfrak{p} \,\}.$$

Assume $l > 1$. Then, $a^l = a \cdot a^{l-1} \in \mathfrak{p}$. By definition, $a \in \mathfrak{p}$ or $a^{l-1} \in \mathfrak{p}$. Both conclusions contradict the choice of l. The only way out is $l = 1$ and $a \in \mathfrak{p}$.

Now, let $a \in R$ be an element which is not nilpotent. We will prove the existence of a prime ideal which does not contain a. Denote by Σ the set of ideals $I \subset R$ with the property that $a^n \notin I$ for all $n \geq 1$. This set contains the zero ideal $\{0\}$ and is, therefore, non-empty. By Zorn's lemma I.4.7 (compare the proof of Theorem I.4.4), it contains a maximal element. Let $\mathfrak{p} \in \Sigma$ be a maximal element. If we can show that $\mathfrak{p}$ is a prime ideal, we are clearly done. Suppose $b, c \in R \setminus \mathfrak{p}$. Then, $\mathfrak{p} \subsetneq \mathfrak{p} + \langle b \rangle$ and $\mathfrak{p} \subsetneq \mathfrak{p} + \langle c \rangle$. By definition of $\mathfrak{p}$, there are exponents $m \geq 1$ and $n \geq 1$ with $a^m \in \mathfrak{p} + \langle b \rangle$ and $a^n \in \mathfrak{p} + \langle c \rangle$. We infer

$$a^{m+n} \in \mathfrak{p} + \langle b \cdot c \rangle.$$

So, $\mathfrak{p} + \langle b \cdot c \rangle \notin \Sigma$ and $\mathfrak{p} \subsetneq \mathfrak{p} + \langle b \cdot c \rangle$. This shows $b \cdot c \notin \mathfrak{p}$ as required. □

I.7.3 Remark. In the above proof, we have used Zorn's lemma, i.e., the axiom of choice in its full strength. In Section II.3, we will see that the statement that Proposition I.7.2 holds for every non-zero ring is equivalent to the fact that every non-zero ring has a prime ideal (compare Remark I.4.5). Note the fact that, in a non-zero ring, $1 \notin \mathfrak{N}$, so that R must contain a prime ideal, if Proposition I.7.2 holds.[14]

I.8 Operations on Ideals

Here, we will discuss various ways to construct new ideals from given ones. These constructions and their properties will be used throughout the following text.

Intersections, Sums, and Products

Let R be a ring, S an index set and $(I_s)_{s\in S}$ a family of ideals in R indexed by the set S. Then, it is a straightforward task to verify that the intersection

$$\bigcap_{s\in S} I_s$$

is also an ideal. This basic observation makes possible the following important construction:

I.8.1 Lemma. *Let R be a ring and $X \subset R$. The ring R possesses one and only one ideal $I(X)$ which contains X and is contained in any ideal containing X.*

Proof. Obviously, the ideal

$$I(X) := \bigcap_{\substack{I\subset R \text{ ideal}\\ X\subset I}} I$$

does the trick. □

The reader should compare this to the corresponding construction in group theory ([30], Satz II.4.10). The ideal $I(X)$ is the *ideal generated by X*.

Definition. We will often write $\langle X\rangle$ for $I(X)$.

I.8.2 Remark. The ideal $I(X)$ is identical to the ideal of all finite R-linear combinations of elements in X:

$$I(X) = \left\{ \sum_{a\in X} r_a \cdot a \,\middle|\, r_a \in R, a \in X, \text{all but finitely many are zero} \right\}.$$

I.8.3 Examples. i) The ideal generated by the empty set is the zero ideal, $\langle\varnothing\rangle = \{0\}$.

ii) For $a \in R$, the ideal $I(\{a\})$ agrees with the principal ideal $\langle a\rangle$ generated by a (see Example I.2.1, iv).

iii) More generally, for finitely many elements $a_1, ..., a_n \in R$, we have (compare Example I.2.1, x)

$$I(\{\, a_1, ..., a_n \,\}) = \langle\, a_1, ..., a_n \,\rangle = \langle a_1\rangle + \cdots + \langle a_n\rangle.$$

[14] The intersection over an empty index set is, by definition, the whole ring R.

We say that an ideal $I \subset R$ is *finitely generated*, if there are a natural number n and elements $a_1, ..., a_n \in R$ with $I = \langle a_1, ..., a_n \rangle$.

The above construction has an important special case: For S an index set and a family of ideals $(I_s)_{s\in S}$ in R indexed by the set S, the *sum* is the ideal

$$\sum_{s\in S} I_s := \left\langle \bigcup_{s\in S} I_s \right\rangle = \left\{ \sum_{s\in S} a_s \,|\, a_s \in I_s, s \in S, \text{ all but finitely many zero} \right\}.$$

I.8.4 Examples. i) For a subset $X \subset R$, we find $I(X) = \sum_{a\in X} \langle a \rangle$.

ii) The union of ideals is, in general, not an ideal. This means that we get, in general,

$$\bigcup_{s\in S} I_s \subsetneq \sum_{s\in S} I_s.$$

For example, $\langle 2\rangle \cup \langle 3\rangle \subset \mathbb{Z}$ is not an ideal. We have $2 \in (\langle 2\rangle \cup \langle 3\rangle)$ and $3 \in (\langle 2\rangle \cup \langle 3\rangle)$, but $5 \notin (\langle 2\rangle \cup \langle 3\rangle)$. Note also that

$$\langle 2\rangle + \langle 3\rangle = \mathbb{Z},$$

because $1 = -2 + 3 \in \langle 2\rangle + \langle 3\rangle$.

For ideals $I, J \subset R$, the *product* is the ideal

$$I \cdot J = I(\{ a \cdot b \,|\, a \in I, b \in J \}) = \left\{ \sum_{i=1}^{n} a_i \cdot b_i \,\middle|\, n \in \mathbb{N}, a_i \in I, b_i \in J, i = 1, ..., n \right\}.$$

The *powers* of an ideal $I \subset R$ are defined recursively via

- $I^0 := R$,
- $I^{n+1} := I \cdot I^n$, $n \in \mathbb{N}$.

I.8.5 Examples. i) Let $R = \mathbb{Z}$ and $a, b \in \mathbb{Z}$ integers. We find the following description of the above constructions:

- $\langle a\rangle + \langle b\rangle = \langle c\rangle$ with c the **greatest common divisor** of a and b.
- $\langle a\rangle \cap \langle b\rangle = \langle c\rangle$ with c the **least common multiple** of a and b (see [30], Definition I.4.12).
- $\langle a\rangle \cdot \langle b\rangle = \langle a \cdot b\rangle$.

ii) Let k be a field, $k[x_1, ..., x_n]$ the polynomial ring in n variables (see Equation (I.2) and the following exercise) and $I := \langle x_1, ..., x_n \rangle$. Then, for $m \geq 1$,

$$\begin{aligned} I^m &= \{ \text{polynomials which contain only monomials of degree at least } m \} \\ &= \left\{ \sum_{\substack{(i_1,...,i_n)\in\mathbb{N}^{\times n}: \\ i_1+\cdots+i_n \geq m}} a_{i_1,...,i_n} \cdot x_1^{i_1} \cdot \cdots \cdot x_n^{i_n} \,\middle|\, a_{i_1,...,i_n} \in R, (i_1, ..., i_n) \in \mathbb{N}^{\times n} : i_1 + \cdots + i_n \geq m \right\}. \end{aligned}$$

Note that R/I^m contains nilpotent elements different from zero, if $m \geq 2$.

I.8.6 Example. Let R be a ring and $I, J \subset R$ ideals. We always have

$$I \cdot J \subset I \cap J.$$

In general, this inclusion is strict. For example, the discussion in Example I.8.5, i), shows that, for integers $a, b \in \mathbb{Z}$, the equation

$$\langle a \rangle \cdot \langle b \rangle = \langle a \rangle \cap \langle b \rangle$$

holds if and only if a and b are coprime.

We say that I and J are *coprime*, if $I + J = R$, and claim that, for coprime ideals $I, J \subset R$, we have

$$I \cdot J = I \cap J.$$

We have to verify the inclusion "$\supset$". Pick $r \in I$ and $s \in J$ with $r + s = 1$ and let $a \in I \cap J$. Then, the equations

$$a = a \cdot 1 = a \cdot (r + s) = \underbrace{a \cdot r}_{\in I \cdot J} + \underbrace{a \cdot s}_{\in I \cdot J}$$

shows that a is an element of $I \cdot J$.

I.8.7 Remarks. i) The operations of taking intersections, sums, and products of ideals are commutative and associative, and the following **distributive law** holds:

$$\text{For ideals } I, J, K \subset R: \quad I \cdot (J + K) = I \cdot J + I \cdot K.$$

The reader may verify this as an exercise.

ii) Let I, J, K be ideals of the ring R and assume $J \subset I$ or $K \subset I$. Then, we also have

$$I \cap (J + K) = (I \cap J) + (I \cap K).$$

Here, the inclusion "$\supset$" is obvious. For the converse inclusion, we assume $J \subset I$. Let $b \in J$ and $c \in K$ be elements with $b + c \in I$. Together with $b \in I$, this implies $c \in I$.

I.8.8 Examples. i) Let k be a field and $R = k[x, y, z]$ the polynomial ring in three variables over k. We assert

$$\langle\, x \cdot y, x \cdot z, y \cdot z \,\rangle = \langle\, x, y \,\rangle \cap \langle\, x, z \,\rangle \cap \langle\, y, z \,\rangle.$$

The inclusion "$\subset$" is immediate. For the converse, we apply the rules from Remark I.8.7. We have

$$\begin{aligned} \langle\, x, y \,\rangle \cap \langle\, x, z \,\rangle &= (\langle x \rangle + \langle y \rangle) \cap \langle\, x, z \,\rangle \\ &= (\langle x \rangle \cap \langle\, x, z \,\rangle) + (\langle y \rangle \cap \langle\, x, z \,\rangle). \end{aligned}$$

Since $\langle y \rangle$ and $\langle\, x, z \,\rangle$ are not coprime, the rules do not give the intersection $\langle y \rangle \cap \langle\, x, z \,\rangle$. Here, we apply prime factorization. Let $f \in \langle\, x, z \,\rangle$. Write f as a product of irreducible factors. Since y is irreducible, it must be associated with one of these irreducible factors, provided $f \in \langle y \rangle$. We see $f \in \langle\, x \cdot y, y \cdot z \,\rangle$ and, thus, $\langle y \rangle \cap \langle\, x, z \,\rangle \subset \langle\, x \cdot y, y \cdot z \,\rangle$. The converse inclusion is obvious. We continue as follows:

$$(\langle x \rangle \cap \langle\, x, z \,\rangle) + (\langle y \rangle \cap \langle\, x, z \,\rangle) = \langle x \rangle + \langle\, x \cdot y, y \cdot z \,\rangle = \langle\, x, y \cdot z \,\rangle.$$

Next

$$\begin{aligned}\langle\, x, y\cdot z\,\rangle \cap \langle\, y, z\,\rangle &= (\langle x\rangle + \langle y\cdot z\rangle) \cap \langle\, y, z\,\rangle \\ &= (\langle x\rangle \cap \langle\, y, z\,\rangle) + (\langle y\cdot z\rangle \cap \langle\, y, z\,\rangle) \\ &= \langle x\cdot y, x\cdot z\rangle + \langle\, y\cdot z\,\rangle \\ &= \langle\, x\cdot y, x\cdot z, y\cdot z\,\rangle.\end{aligned}$$

ii) If we have two finitely generated ideals $I = \langle\, f_1, ..., f_s\,\rangle$ and $J = \langle\, g_1, ..., g_t\,\rangle$ in a ring R, then one easily sees

$$I\cdot J = \langle\, f_1\cdot g_1, ..., f_1\cdot g_t, ..., f_s\cdot g_1, ..., f_s\cdot g_t\,\rangle.$$

A similar result holds, if the ideals are specified by possibly infinite sets of generators.

We may apply this to the setting of the previous example:

$$\langle\, x, y\,\rangle\cdot\langle\, x, z\,\rangle\cdot\langle\, y, z\,\rangle = \langle\, x^2\cdot y, x^2\cdot z, x\cdot y^2, x\cdot y\cdot z, x\cdot z^2, y^2\cdot z, y\cdot z^2\,\rangle.$$

We infer

$$\langle\, x, y\,\rangle\cdot\langle\, x, z\,\rangle\cdot\langle\, y, z\,\rangle \subsetneq \langle\, x, y\,\rangle \cap \langle\, x, z\,\rangle \cap \langle\, y, z\,\rangle.$$

I.8.9 Exercise (A primary decomposition in $\mathbb{Z}[\sqrt{-5}]$). Define

$$\mathfrak{p}_1 := \langle\, 3, 2+\sqrt{-5}\,\rangle \quad \text{and} \quad \mathfrak{p}_2 := \langle\, 3, 2-\sqrt{-5}\,\rangle$$

i) Show that $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are prime ideals.
ii) Verify that the ideals $\mathfrak{p}_1^2$ and $\mathfrak{p}_2^2$ are coprime.
iii) Demonstrate that $\langle 9\rangle = \mathfrak{p}_1^2\cdot\mathfrak{p}_2^2 = \mathfrak{p}_1^2\cap\mathfrak{p}_2^2$.

The Chinese Remainder Theorem

We generalize Example I.8.6.

I.8.10 Lemma. *Let R be a ring and $I_1, ..., I_n \subset R$ ideals, such that I_k and I_l are coprime for $1 \le k < l \le n$. Then,*[15]

$$\prod_{k=1}^{n} I_k := I_1\cdot\dots\cdot I_n = \bigcap_{k=1}^{n} I_k.$$

Proof. We proceed by induction on n. The case $n = 2$ has already been dealt with in Example I.8.6.

***n* − 1 ⟶ *n*.** We set

$$J := \prod_{k=1}^{n-1} I_k.$$

By induction hypothesis, we have

$$J = \bigcap_{k=1}^{n-1} I_k.$$

[15]The associativity of the product shows that the definition is independent of the brackets one implicitly has to insert into the middle term, or, in other words, grants that the middle term is well-defined.

It suffices to show that J and I_n are coprime. By assumption, there are elements $r_k \in I_k$ and $s_k \in I_n$ with

$$r_k + s_k = 1, \quad k = 1, ..., n-1.$$

There is an element $s \in I_n$ with

$$\prod_{k=1}^{n-1} r_k = \prod_{k=1}^{n-1}(1 - s_k) = 1 - s.$$

Since the element on the left hand side belongs to J, we see that $1 \in J + I_n$. □

Now, we would like to generalize the Chinese remainder theorem from elementary number theory in the formulation [30], III.1.4. We place ourselves in the situation of the lemma. To make the notation more precise, we denote the class of $a \in R$ in the quotient ring R/I_k by $[a]_k$, $k = 1, ..., n$. For $k = 1, ..., n$, there is the canonical surjection

$$\begin{aligned} \pi_k \colon R &\longrightarrow R/I_k \\ a &\longmapsto [a]_k. \end{aligned}$$

Using the cartesian product of rings (Example I.1.3, x), we define

$$\begin{aligned} \varphi \colon R &\longrightarrow \bigtimes_{k=1}^{n} R/I_k \\ a &\longmapsto ([a]_1, ..., [a]_n). \end{aligned}$$

Note that

$$\ker(\varphi) = \bigcap_{k=1}^{n} I_k.$$

By the isomorphism theorem, we get an induced injective homomorphism

$$\overline{\varphi} \colon R/\bigcap_{k=1}^{n} I_k \longrightarrow \bigtimes_{k=1}^{n} R/I_k.$$

Next, we would like to study when φ or, equivalently, $\overline{\varphi}$ is surjective. Let

$$e_i := (0, ..., 0, 1, 0, ..., 0) \in \bigtimes_{k=1}^{n} R/I_k$$

be the element which has the entry 1 at the i-th place, $i = 1, ..., n$. Then, it is readily checked that

$$\varphi \text{ is surjective} \quad \Longleftrightarrow \quad \forall i \in \{1, ..., n\} : e_i \in \operatorname{im}(\varphi).$$

Let us look at the condition $e_1 \in \operatorname{im}(\varphi)$ in more detail. If it is satisfied, then there is an element $a \in R$ with $[a]_1 = 1$, i.e., $1 - a \in I_1$, and $[a]_k = 0$, that is $a \in I_k$, for $k = 2, ..., n$. In particular, we have

$$1 = (1 - a) + a \in I_1 + I_k, \quad k = 2, ..., n.$$

Conversely, assume that I_1 and I_k are coprime, for $k = 2, ..., n$. Then, there are elements $r_k \in I_1$ and $s_k \in I_k$ with

$$1 = r_k + s_k, \quad k = 2, ..., n.$$

Set

$$a := \prod_{k=2}^{n} s_k = \prod_{k=2}^{n}(1 - r_k).$$

The second description of a shows $[a]_1 = 1$ and the first $[a]_k = 0$, $k = 2, ..., n$. It follows $\varphi(a) = e_1$. Our discussion shows:

I.8.11 Lemma. *The homomorphism φ is surjective if and only if the ideals I_k and I_l are coprime, for $1 \leq k < l \leq n$.*

We combine this observation with Lemma I.8.10:

I.8.12 Chinese remainder theorem. *Let R be a ring and $I_1, ..., I_n \subset R$ ideals, such that I_k and I_l are coprime for $1 \leq k < l \leq n$. Then,*

$$R/\bigcap_{k=1}^{n} I_k = R/\prod_{k=1}^{n} I_k \cong \bigtimes_{k=1}^{n} R/I_k.$$

I.8.13 Example. Let $a \in \mathbb{Z}$ be an integer and

$$a = p_1^{\nu_1} \cdot \cdots \cdot p_n^{\nu_n}$$

its prime factorization. Then,

$$\mathbb{Z}/\langle a\rangle \cong \mathbb{Z}/\langle p_1^{\nu_1}\rangle \times \cdots \times \mathbb{Z}/\langle p_n^{\nu_n}\rangle.$$

I.8.14 Exercise (The Chinese remainder theorem). i) What is the smallest (positive) multiple of 10 which has remainder 2 when divided by 3, and remainder 3 when divided by 7?

ii) Let k be a field. Describe the ring $k[x]/\langle x^2 - 1\rangle$.

Ideal Quotients

Let R be a ring and $I, J \subset R$ ideals. Then, the *ideal quotient* of I by J is set to be

$$(I : J) := \{\, a \in R \,|\, a \cdot J \subset I \,\}.$$

It is straightforward to check that $(I : J)$ is an ideal. For an ideal $I \subset R$, we call $(\langle 0\rangle : I)$ the *annihilator* of I.

Notation. ⋆ $\mathrm{Ann}(I) := (\langle 0\rangle : I)$.

⋆ For $a \in R$, we set $\mathrm{Ann}(a) := \mathrm{Ann}(\langle a\rangle)$.

I.8.15 Remark. The union

$$D := \bigcup_{a \in R\setminus\{0\}} \mathrm{Ann}(a)$$

is the set of zero divisors of the ring R.

I.8.16 Example. Let $R = \mathbb{Z}$ and $a, b \in \mathbb{Z}$ be integers. We look at the prime factorizations

$$a = \prod_{p \text{ prime number}} p^{\mu_p} \quad \text{and} \quad b = \prod_{p \text{ prime number}} p^{\nu_p}.$$

There exists a positive integer c with

$$(\langle a\rangle : \langle b\rangle) = \langle c\rangle.$$

Its prime factorization

$$c = \prod_{p \text{ prime number}} p^{\gamma_p}$$

is determined by

$$\gamma_p = \max\{\mu_p - \nu_p, 0\} = \mu_p - \min\{\mu_p, \nu_p\}, \quad p \text{ a prime number.}$$

We see

$$c = \frac{a}{\gcd(a, b)}.$$

I.8.17 Properties. *Let R be a ring, S and T index sets, and I, J, K, I_s, $s \in S$, and J_t, $t \in T$, ideals in R. Then, the following properties are verified:*

i) $I \subset (I : J)$.

ii) $(I : J) \cdot J \subset I$.

iii) $\big((I : J) : K\big) = \big(I : (J \cdot K)\big) = \big((I : K) : J\big)$.

iv) $\left(\bigcap_{s\in S}(I_s : J)\right) = \bigcap_{s\in S}(I_s : J)$.

v) $\left(I : \sum_{t\in T} J_t\right) = \bigcap_{t\in T}(I : J_t)$.

The verifications are left as an exercise to the reader.

Radicals of Ideals

Let R be a ring and $I \subset R$ an ideal. The *radical* of I is

$$\sqrt{I} := \{\, a \in R \mid \exists k \geq 1 : a^k \in I \,\}.$$

Note that $\sqrt{I}$ is the preimage of the nilradical $\overline{\mathfrak{N}}$ of the ring R/I under the canonical projection $\pi\colon R \longrightarrow R/I$. Proposition I.7.2, therefore, gives the following

I.8.18 Corollary. *The radical $\sqrt{I}$ is the intersection of all prime ideals which contain I.*

I.8.19 Properties. *Let R be a ring, $I, J \subset R$ ideals, and $\mathfrak{p} \subset R$ a prime ideal of R. Then, we have the following properties:*

i) $I \subset \sqrt{I}$.

ii) $\sqrt{\sqrt{I}} = \sqrt{I}$.

iii) $\sqrt{I} = R$ *if and only if* $I = R$.

iv) $\sqrt{I \cdot J} = \sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$.

v) $\sqrt{I + J} = \sqrt{\sqrt{I} + \sqrt{J}}$.

vi) *For every $n > 0$, one has* $\sqrt{\mathfrak{p}^n} = \mathfrak{p}$.

The proof is again left to the reader.

I.8.20 Examples. i) Let $R = \mathbb{Z}$ and $a \in \mathbb{Z}$ an integer. As usual, we look at the prime factorization

$$a = p_1^{\nu_1} \cdot \cdots \cdot p_n^{\nu_n}.$$

This means, in particular, that $\nu_i > 0$, $i = 1, ..., n$. Then, it is readily checked that

$$\sqrt{\langle a \rangle} = \langle p_1 \cdot \cdots \cdot p_n \rangle.$$

ii) We return to Example I.8.8, ii). More precisely, we look at the ideal

$$I = \langle\, x^2 \cdot y, x^2 \cdot z, x \cdot y^2, x \cdot y \cdot z, y^2 \cdot z, y \cdot z^2 \,\rangle.$$

Note $x \cdot y \notin I$, but $(x \cdot y)^2 = x \cdot (x \cdot y^2) \in I$.

An ideal $I \subset R$ which is its own radical, $I = \sqrt{I}$, is a *radical ideal*. Radical ideals play an important role in algebraic geometry (see Section I.9).

Extension and Contraction of Ideals

Let R, S be rings and $\varphi\colon R \longrightarrow S$ a homomorphism. It is important to compare the ideals of R and S.[16] Recall from Example I.2.1, viii), that the image $\varphi(I)$ of an ideal $I \subset R$ need not be an ideal. For this reason, we have to resort to the construction in Lemma I.8.1: Let $I \subset R$. Then, the ideal

$$I^{\mathrm{e}} := I(\varphi(I))$$

of S generated by the image $\varphi(I)$ of I is the *extension* of I via φ. We have

$$I^{\mathrm{e}} = \left\{ \sum_{i=1}^{n} s_i \cdot f(a_i) \,\middle|\, n \in \mathbb{N}, s_i \in S, a_i \in I, i = 1, ..., n \right\}.$$

I.8.21 Remarks. If $\mathfrak{p} \subset R$ is a prime ideal, then $\mathfrak{p}^{\mathrm{e}} \subset S$ need not be a prime ideal.[17] For example, for the inclusion $\iota\colon \mathbb{Z} \longrightarrow \mathbb{Q}$, the extension of $\langle p \rangle$, p a prime number, is always $\mathbb{Q}$ which is not a prime ideal. Another example is the canonical projection $\pi\colon k[x, y] \longrightarrow k[x, y]/\langle x \cdot y \rangle$, k a field. Since $k[x, y]$ is an integral domain, $\langle 0 \rangle$ is a prime ideal of $k[x, y]$. Obviously, $\langle 0 \rangle^{\mathrm{e}} = \langle 0 \rangle$. But the quotient ring $k[x, y]/\langle x \cdot y \rangle$ has zero divisors, e.g., $[x]$ and $[y]$. Therefore, $\langle 0 \rangle \subset k[x, y]/\langle x \cdot y \rangle$ is not a prime ideal.

In the above setting, let $J \subset S$ be an ideal. Then,

$$J^{\mathrm{c}} := \varphi^{-1}(J)$$

is always an ideal of S. It is called the *contraction* of J via φ. Recall that $\mathfrak{q}^{\mathrm{c}}$ is a prime ideal of R, if $\mathfrak{q}$ is a prime ideal of S.

[16] In Exercise I.4.17, iv), you have already encountered the induced continuous map $\varphi^{\#}\colon \mathrm{Spec}(S) \longrightarrow \mathrm{Spec}(R)$.

[17] So, there is, in general, no induced map $\varphi_\star\colon \mathrm{Spec}(R) \longrightarrow \mathrm{Spec}(S)$.

I.8.22 Remark. By Exercise I.2.4, we can factorize $\varphi\colon R \longrightarrow S$ as

$$R \xrightarrow{\pi} T := R/\ker(\varphi) \xhookrightarrow{\iota} S.$$

Here, π is the canonical projection and $\iota := \overline{\varphi}$ is injective. Regarding the surjection

$$\pi\colon R \longrightarrow T,$$

we have

- ⋆ If $I \subset R$ is an ideal, then $\pi(I) \subset T$ is an ideal (Example I.2.1).
- ⋆ The map $K \subset R/\ker(\varphi) \longmapsto \pi^{-1}(K) \subset R$ induces an inclusion preserving bijection between the set of ideals of $R/\ker(\varphi)$ and the set of ideals of R containing $\ker(\varphi)$.[18]

The above discussion reveals that most of the complications encountered in the extension and contraction of ideals show up for injective ring homomorphisms. Here is a nice classical example from number theory.

I.8.23 Example. We look at the ring of **Gaußian integers**:

$$\mathbb{Z}[i] = \{\, k + l \cdot i \in \mathbb{C} \mid k, l \in \mathbb{Z} \,\}.$$

This ring is euclidean (see [8], Chapter II, Definition 2.2.4, for the definition of a euclidean ring and [8], Beispiel 2.2.5, 3), or [23], I.(1.2), for the proof of the above-mentioned fact). In particular, it is a principal ideal domain ([8], Satz 2.2.6). The prime elements of $\mathbb{Z}[i]$ are described in [23], I.(1.4).

Let $\varphi\colon \mathbb{Z} \longrightarrow \mathbb{Z}[i]$ be the natural inclusion. Using the classification of prime elements in $\mathbb{Z}[i]$, one finds the following:

- ⋆ $\langle 2\rangle^{\mathrm{e}} = \langle (1+i)^2\rangle$.
- ⋆ If $p \equiv 1 \bmod 4$, then $\langle p\rangle^{\mathrm{e}}$ is the product of two prime ideals. For example, $\langle 5\rangle^{\mathrm{e}} = \langle 2+i\rangle \cdot \langle 2-i\rangle$.
- ⋆ If $p \equiv 3 \bmod 4$, then $\langle p\rangle^{\mathrm{e}}$ is a prime ideal.

This is just the ideal theoretic description of the classical result of number theory that an odd prime number can be written as the sum of two squares if and only if it is congruent to 1 modulo 4 (see [23], Chapter I, §1).

We list further rules for the extension and contraction of ideals which the reader should prove on her or his own.

I.8.24 Properties. *Let R, S be rings, I, I_1, I_2 be ideals in R, J, J_1, J_2 ideals in S, and $f\colon R \longrightarrow S$ a ring homomorphism. Then:*

i) $I \subset I^{\mathrm{ec}}$, $J \supset J^{\mathrm{ce}}$.
ii) $I^{\mathrm{e}} = I^{\mathrm{ece}}$, $J^{\mathrm{c}} = J^{\mathrm{cec}}$.
iii) $(I_1 + I_2)^{\mathrm{e}} = I_1^{\mathrm{e}} + I_2^{\mathrm{e}}$, $(J_1 + J_2)^{\mathrm{c}} \supset J_1^{\mathrm{c}} + J_2^{\mathrm{c}}$.
iv) $(I_1 \cap I_2)^{\mathrm{e}} \subset I_1^{\mathrm{e}} \cap I_2^{\mathrm{e}}$, $(J_1 \cap J_2)^{\mathrm{c}} = J_1^{\mathrm{c}} \cap J_2^{\mathrm{c}}$.
v) $(I_1 \cdot I_2)^{\mathrm{e}} = I_1^{\mathrm{e}} \cdot I_2^{\mathrm{e}}$, $(J_1 \cdot J_2)^{\mathrm{c}} \supset J_1^{\mathrm{c}} \cdot J_2^{\mathrm{c}}$.
vi) $(I_1 : I_2)^{\mathrm{e}} \subset (I_1^{\mathrm{e}} : I_2^{\mathrm{e}})$, $(J_1 : J_2)^{\mathrm{c}} \subset (J_1^{\mathrm{c}} : J_2^{\mathrm{c}})$.
vii) $(\sqrt{I})^{\mathrm{e}} \subset \sqrt{I^{\mathrm{e}}}$, $(\sqrt{J})^{\mathrm{c}} = \sqrt{J^{\mathrm{c}}}$.

[18] Be aware that, for distinct ideals I and I' which do not both contain $\ker(\varphi)$, it may very well happen that $\varphi(I) = \varphi(I')$. Can you think of an easy example?

I.9 Algebraic Sets

So far, we have developed the calculus of ideals. In addition, we studied the problem of prime factorizations in integral domains. The failure of it led to Kummer's idea that ideals are generalizations of numbers which should help to save the prime factorization. This is a strong motivation for introducing ideals. The main motivation to study ideals in this course comes, however, from algebraic geometry. We will now illustrate how basic notions concerning systems of polynomial equations may be elegantly treated in the language of ideals. To do this, we will need some of the operations on ideals that we have discussed. This is why we treat this material at such a late stage.

Roughly speaking, algebraic geometry is the study of solutions of systems of polynomial equations over a field or even a ring. Let us formalize this. Let k be a field. The *n-dimensional affine space over k* is[19]

$$\mathbb{A}_k^n := \{\, (a_1, ..., a_n) \,|\, a_i \in k, i = 1, ..., n \,\}.$$

Let $F \subset k[x_1, ..., x_n]$ be a subset. The set

$$V(F) := \{\, p = (a_1, ..., a_n) \in \mathbb{A}_k^n \,|\, \forall f \in F : f(p) = f(a_1, ..., a_n) = 0 \,\}$$

is the *vanishing locus of* F. Its points are those which simultaneously solve all the polynomial equations $f = 0$, $f \in F$. Note that F may be an infinite set.

A subset $Z \subset \mathbb{A}_k^n$ is *algebraic*, if there is a subset $F \subset k[x_1, ..., x_n]$ with

$$Z = V(F).$$

For a subset $S \subset \mathbb{A}_k^n$, we introduce

$$I(S) := \{\, f \in k[x_1, ..., x_n] \,|\, \forall p \in S : f(p) = 0 \,\}.$$

Note that $I(S)$ is an ideal (compare Example I.2.1, vi). It is the *ideal of regular functions vanishing on* S or simply the *ideal of* S.

I.9.1 Properties. *Let* $S, Y, Z \subset \mathbb{A}_k^n$ *and* $F, G, H \subset k[x_1, ..., x_n]$ *be subsets. Then, one has:*

i) *The ideal* $I(S)$ *of* S *is a radical ideal.*

ii) $I(Y \cup Z) = I(Y) \cap I(Z)$.

iii) *If* $Y \subset Z$, *then* $I(Y) \supset I(Z)$.

iv) *If* $G \subset H$, *then* $V(G) \supset V(H)$.

v) *Let* $\langle F \rangle$ *be the ideal generated by* F *(see Lemma* I.8.1*). Then,*

$$V(\langle F \rangle) = V(F).$$

Proof. i) Let $f \in k[x_1, ..., x_n]$ and $l \geq 1$ be such that $f^l \in I(S)$. This means that $f^l(p) = (f(p))^l = 0$ for all $p \in S$. Since the field k has no nilpotent element besides 0, this condition is equivalent to $f(p) = 0$ for all $p \in S$, i.e., to $f \in I(S)$.

ii), iii), and iv) are trivial.

[19] One uses this notation rather than k^n to indicate that we are not interested in the k-vector space structure of that set.

v) Since $F \subset \langle F \rangle$, we have $V(F) \supset V(\langle F \rangle)$. Now, let $p \in V(F)$ and $h \in \langle F \rangle$. We have to show that $h(p) = 0$. There are a natural number s, elements $f_1, ..., f_s \in F$ and $r_1, ..., r_s \in k[x_1, ..., x_n]$ with

$$h = \sum_{i=1}^{s} r_i \cdot f_i.$$

It follows that

$$h(p) = \sum_{i=1}^{s} r_i(p) \cdot f_i(p) = 0,$$

because $f_i(p) = 0$, $i = 1, ..., s$. □

Property I.9.1, v), tells us that, when dealing with algebraic sets, we may restrict to vanishing loci of ideals. The set theoretic operations on algebraic sets reflect very nicely in the operations on ideals.

I.9.2 Properties. i) *The empty set* $\varnothing$ *and the affine space* $\mathbb{A}_k^n$ *are algebraic sets.*

ii) *Let* $I, J \subset k[x_1, ..., x_n]$ *be ideals. Then,*

$$V(I) \cup V(J) = V(I \cap J) = V(I \cdot J).$$

iii) *Let* K *be an index set and* $(I_k)_{k \in K}$ *be a family of ideals in* $k[x_1, ..., x_n]$*. Then,*

$$\bigcap_{k \in K} V(I_k) = V\Big(\sum_{k \in K} I_k\Big).$$

Proof. i) We have $\varnothing = V(\langle 1 \rangle)$ and $\mathbb{A}_k^n = V(\langle 0 \rangle)$.

ii) Since $I \cap J \subset I$ and $I \cap J \subset J$, we have $V(I \cap J) \supset V(I) \cup V(J)$, by Property I.9.1, iv). We also have $I \cdot J \subset I \cap J$, so that $V(I \cdot J) \supset V(I \cap J)$. Let us show that $V(I \cdot J) \subset V(I) \cup V(J)$. To this end, let $p \in V(I \cdot J)$ and assume $p \notin V(I)$. Then, we find a polynomial $f \in I$ with $f(p) \neq 0$. For every $g \in J$, we obviously have $f \cdot g \in I \cdot J$, so that

$$\forall g \in J : \quad f(p) \cdot g(p) = (f \cdot g)(p) = 0.$$

Since $f(p) \neq 0$ and k is a field, this means

$$\forall g \in J : \quad g(p) = 0$$

and shows that $p \in V(J)$.

iii) It is readily verified that

$$\bigcap_{k \in K} V(I_k) = V\Big(\bigcup_{k \in K} I_k\Big).$$

By definition (see Page I.8), $\sum_{k \in K} I_k$ is the ideal generated by $\bigcup_{k \in K} I_k$. So, we conclude by Property I.9.1, v). □

Property I.9.2 tells us that the algebraic subsets of $\mathbb{A}_k^n$ fullfil the axioms of the closed subsets of a topological space (see [18], Abschnitt 1.3). Therefore, we say that a subset $Z \subset \mathbb{A}_k^n$ is *Zariski closed*, if it is algebraic. A subset $U \subset \mathbb{A}_k^n$ is *Zariski open*, if its complement $\mathbb{A}_k^n \setminus U$ is Zariski closed.

By Property I.9.2

$$\mathcal{T} := \{\, U \subset \mathbb{A}_k^n \mid U \text{ is Zariski open} \,\}$$

is a topology on $\mathbb{A}_k^n$, the *Zariski topology*.

I.9.3 Remark. i) We already see some of the nice features of algebraic geometry emerge: the subtle interplay of topological, geometric and algebraic tools. The reader should be careful about the topology. It is very distinct from, e.g., the usual topology on $\mathbb{R}^n$ or $\mathbb{C}^n$ (see the following exercise).

ii) In Property I.9.2, ii), we give two ideals which yield the union $V(I) \cup V(J)$, $I, J \subset k[x_1, ..., x_n]$ ideals, namely, $I \cap J$ and $I \cdot J$. The first description has the advantage that $I \cap J$ will be a radical ideal, if I and J are radical ideals (Property I.8.19, iv). The second description allows to determine easily equations for $V(I) \cup V(J)$ from known generators for I and J. In fact, if $(f_k)_{k\in K}$ generate I and $(g_l)_{l\in L}$ generate J, then $(f_k \cdot g_l)_{(k,l)\in K\times L}$ generate $I \cdot J$ (compare Example I.8.8, ii).

I.9.4 Exercises. i) Describe the Zariski open subsets of $\mathbb{A}^1_k$. (Recall that $k[x]$ is a principal ideal domain.)

ii) Check that the Zariski topology on $\mathbb{A}^2_k$ is not the product topology (see [18], Section 2.1) on $\mathbb{A}^1_k \times \mathbb{A}^1_k$, the factors being endowed with the Zariski topology.

Let $(X, \mathcal{T})$ be a topological space and $S \subset X$ a subset. Recall ([18], Definition, p. 11) that the *closure* $\overline{S}$ *of* S is the smallest closed subset of X that contains S, i.e.,

$$\overline{S} = \bigcap_{\substack{Z\subset X \text{ closed:}\\ S\subset Z}} Z.$$

I.9.5 Lemma. i) *For every ideal* $I \subset k[x_1, ..., x_n]$*, one has*

$$\sqrt{I} \subset I(V(I)).$$

ii) *Let* $S \subset \mathbb{A}^n_k$ *be a subset. Then,*

$$\overline{S} = V(I(S)).$$

Proof. i) Clearly, $I \subset I(V(I))$. Hence,

$$\sqrt{I} \subset \sqrt{I(V(I))} = I(V(I)).$$

For the last equation, we used Property I.9.1, i).

ii) We clearly have $S \subset V(I(S))$. Since $V(I(S))$ is closed, we also find $\overline{S} \subset V(I(S))$. Let $S \subset Z \subset \mathbb{A}^n_k$ be a closed subset. There is an ideal $I \subset k[x_1, ..., x_n]$ with $Z = V(I)$. We see

$$Z = V(I) \supset V(I(Z)) \supset V(I(S)).$$

The first inclusion is a consequence of $I \subset I(Z)$ and the second one of $I(Z) \subset I(S)$ which, in turn, follows from $Z \supset S$. □

We have maps

$$\begin{array}{rccl} \Phi\colon & \left\{\text{Algebraic sets in } \mathbb{A}^n_k\right\} & \longrightarrow & \left\{\text{Radical ideals in } k[x_1, ..., x_n]\right\} \\ & Z & \longmapsto & I(Z) \end{array}$$

and

$$\begin{array}{rccl} \Psi\colon & \left\{\text{Radical ideals in } k[x_1, ..., x_n]\right\} & \longrightarrow & \left\{\text{Algebraic sets in } \mathbb{A}^n_k\right\} \\ & I & \longmapsto & V(I). \end{array}$$

Lemma I.9.5, ii), shows

$$\Psi \circ \Phi = \mathrm{id}\,.$$

In particular, Φ is injective and Ψ is surjective.

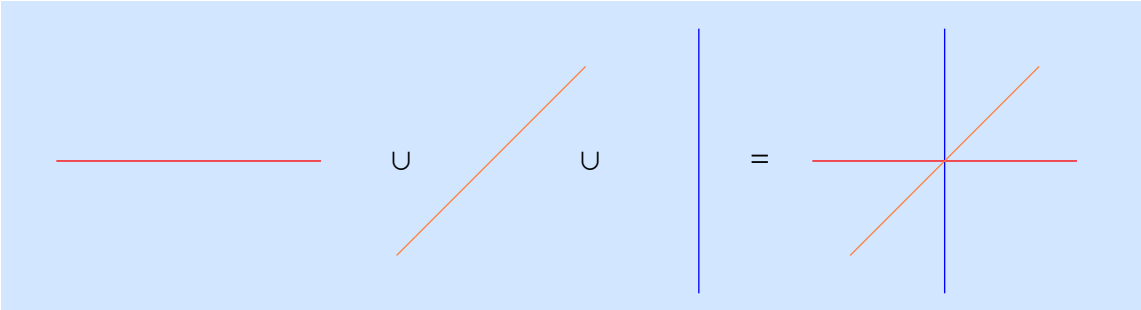
Hilbert's[20] Nullstellensatz III.3.4 asserts that, if k is **algebraically closed**, then also

$$\Phi \circ \Psi = \mathrm{id}\,.$$

Then, we have translated the theory of algebraic sets into the theory of ideals in rings.

If k is **not algebraically closed**, we cannot expect such a result. Look, for example, at the prime ideal[21] $I := \langle x^2 + y^2 + 1\rangle \subset k[x, y]$. Obviously, $V(I) = \varnothing$ and $I(V(I)) = \langle 1\rangle$.

I.9.6 Examples. i) We look at the ideals $I_x = \langle\, y, z\,\rangle$, $I_y = \langle\, x, z\,\rangle$, and $I_z = \langle\, x, y\,\rangle$ inside $k[x, y, z]$. Then, $V(I_x)$ is the x-axis, $V(I_y)$ the y-axis, and $V(I_z)$ the z-axis. The ideals $I_x \cdot I_y \cdot I_z$ and $I_x \cap I_y \cap I_z$ were computed in Example I.8.8. By Property I.9.2, ii), both $V(I_x \cdot I_y \cdot I_z)$ and $V(I_x \cap I_y \cap I_z)$ consist of the union of the coordinate axes.



Note that

$$I_x \cdot I_y \cdot I_z \subsetneq I_x \cap I_y \cap I_z \subset I(V(I_x \cap I_y \cap I_z)) = I(V(I_x \cdot I_y \cdot I_z)).$$

We remark that $I_x \cdot I_y \cdot I_z \neq I(V(I_x \cdot I_y \cdot I_z))$ is already implied by the fact that $I_x \cdot I_y \cdot I_z$ is not a radical ideal (see Example I.8.20, ii).

ii) We look at the ideals $I_1 := \langle\, y^2 - x^3, z\,\rangle$ and $I_2 := \langle\, x, y\,\rangle$ in the ring $k[x, y, z]$. The vanishing locus $V(I_1)$ is Neil's parabola ([28], Beispiel 4.1.2, iv) inside the (x, y)-plane and $V(I_2)$ is, as before, the z-axis. The union of these two objects is $V(I_1 \cdot I_2)$. By Example I.8.8, ii),

$$I_1 \cdot I_2 = \langle\, x \cdot z, y \cdot z, x \cdot y^2 - x^4, y^3 - x^3 \cdot y\,\rangle.$$

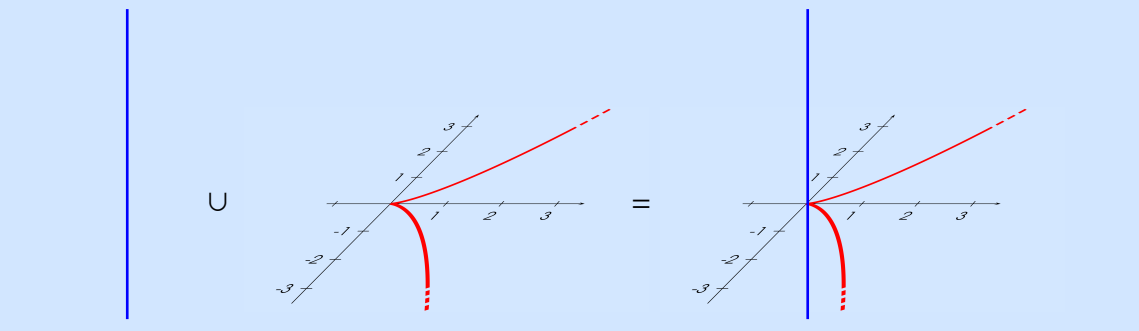
Again, $I_1 \cdot I_2$ is not a radical ideal. For example, $y^2 - x^3 \notin I_1 \cdot I_2$ but

$$(y^2 - x^3)^2 = y \cdot y \cdot (y^2 - x^3) - x^2 \cdot x \cdot (y^2 - x^3) = y \cdot (y^3 - x^3 \cdot y) - x^2 \cdot (x \cdot y^2 - x^4) \in I_1 \cdot I_2.$$

We see $I_1 \cdot I_2 \subsetneq I(V(I_1 \cdot I_2))$.

[20] David Hilbert (1862 - 1943), German mathematician.

[21] $x^2 + y^2 + 1$ is an irreducible polynomial, because, if it could be written as the product of two linear polynomials, it would have zeroes.



I.9.7 Remark. Let $Z \subset \mathbb{A}_k^n$ be an algebraic set and $I(Z) \subset k[x_1, ..., x_n]$ its ideal. The ring

$$k[Z] := k[x_1, ..., x_n]/I(Z)$$

is called the *coordinate algebra* of Z. It describes Z as an "abstract object", i.e., without reference to the inclusion $\iota\colon Z \hookrightarrow \mathbb{A}_k^n$. We will elaborate on this later (see, e.g., the following exercise).

I.9.8 Exercises (Maps between algebraic sets). Let k be a field and $Z \subset \mathbb{A}_k^n$ an algebraic set. Its *algebra of regular functions* is

$$k[Z] := k[x_1, ..., x_n]/I(Z).$$

Note that an element $f \in k[Z]$ defines indeed a function $f\colon Z \longrightarrow k$. Let $W \subset \mathbb{A}_k^m$ and $Z \subset \mathbb{A}_k^n$ be algebraic sets and $F\colon W \longrightarrow Z$ a map. Write the induced map $F\colon W \longrightarrow Z \subset \mathbb{A}_k^n$ as $w \longmapsto (f_1(w), ..., f_n(w))$. We say that F is *regular*, if f_i is a regular function on W, $i = 1, ..., n$.

i) Show that a regular map $F\colon W \longrightarrow Z$ induces a homomorphism

$$F^\star\colon k[Z] \longrightarrow k[W]$$

of k-algebras.

ii) Suppose $\varphi\colon k[Z] \longrightarrow k[W]$ is a homomorphism of k-algebras. Show that there is a unique regular map $F\colon W \longrightarrow Z$ with $F^\star = \varphi$.

Let $I \subset k[x_1, ..., x_n]$ be an ideal. Then, we have its vanishing locus $V(I)$. As a subset of $\mathbb{A}_k^n$, it is endowed with an induced Zariski topology. On the other hand, we introduced $\mathrm{Spec}(k[x_1, ..., x_n]/I)$. It carries a topology that was also called the Zariski topology. It is important not to confuse these two objects.

I.9.9 Remark. By Lemma I.2.2 and Exercise I.2.3, the surjection

$$\pi\colon k[x_1, ..., x_n] \longrightarrow k[x_1, ..., x_n]/I$$

induces an injective map

$$\pi^\#\colon \mathrm{Spec}(k[x_1, ..., x_n]/I) \hookrightarrow \mathrm{Spec}(k[x_1, ..., x_n]),$$

and the Zariski topology on $\mathrm{Spec}(k[x_1, ..., x_n]/I)$ agrees with the subspace topology (see [18], Section 2.1).

In order to get an idea about the difference of these two objects, let us first relate them to each other. First, note that, for a point $p = (a_1, ..., a_n) \in \mathbb{A}^n_k$,

$$\mathfrak{m}_p := \langle\, x_1 - a_1, ..., x_n - a_n \,\rangle$$

is a maximal ideal.[22] This provides us with the map

$$\begin{aligned} \Phi\colon \mathbb{A}^n_k &\longrightarrow \operatorname{Spec}(k[x_1, ..., x_n]) \\ p &\longmapsto \mathfrak{m}_p. \end{aligned}$$

I.9.10 Lemma. *For every point $p = (a_1, ..., a_n)$ and every ideal $I \subset k[x_1, ..., x_n]$, we have*

$$p \in V(I) \quad \Longleftrightarrow \quad I \subset \langle\, x_1 - a_1, ..., x_n - a_n \,\rangle.$$

Proof. Let $p \in V(I)$. Then, $\langle\, x_1 - a_1, ..., x_n - a_n \,\rangle \subset I(\{p\}) \subsetneq \langle 1 \rangle$. Since $\langle\, x_1 - a_1, ..., x_n - a_n \,\rangle$ is a maximal ideal, we must have equality. Thus, we see

$$\langle\, x_1 - a_1, ..., x_n - a_n \,\rangle = I(\{p\}) \supset I(V(I)) \supset I.$$

Conversely, $I \subset \langle\, x_1 - a_1, ..., x_n - a_n \,\rangle$ yields

$$\{p\} = V(\langle\, x_1 - a_1, ..., x_n - a_n \,\rangle) \subset V(I).$$

This completes the proof. □

For any ideal $I \subset k[x_1, ..., x_n]$, the sets $V(I) \subset \mathbb{A}^n_k$ and $V(I) \subset \operatorname{Spec}(k[x_1, ..., x_n])$ are, thus, related by

$$V(I) = \Phi^{-1}(V(I)). \tag{I.10}$$

In particular, Φ is continuous in the Zariski topology.

I.9.11 Exercise. Let R be a ring. A point $\mathfrak{p} \in \operatorname{Spec}(R)$ is *closed*, if $\{\mathfrak{p}\}$ is a Zariski closed subset of $\operatorname{Spec}(R)$. Show that $\mathfrak{p} \in \operatorname{Spec}(R)$ is a closed point if and only if $\mathfrak{p}$ is a maximal ideal.

In order to get a precise understanding of Φ and, therefore, of the relation between $\mathbb{A}^n_k$ and $\operatorname{Spec}(k[x_1, ..., x_n])$, we need to understand the maximal ideals of $k[x_1, ..., x_n]$.

If k is **algebraically closed**, Hilbert's Nullstellensatz III.3.4 shows that all maximal ideals of $k[x_1, ..., x_n]$ are of the form $\langle\, x_1 - a_1, ..., x_n - a_n \,\rangle$, $(a_1, ..., a_n) \in \mathbb{A}^n_k$. So, Φ identifies $\mathbb{A}^n_k$ with the set of closed points of $\operatorname{Spec}(k[x_1, ..., x_n])$. Note that $\operatorname{Spec}(k[x_1, ..., x_n])$ contains non-closed points, e.g., $\langle 0 \rangle$, and, if $n \geq 2$, $\langle x_i \rangle$, $i = 1, ..., n$ and, more generally, $\langle\, f \,\rangle$, $f \in k[x_1, ..., x_n]$ an irreducible polynomial.

If k is **not algebraically closed**, then $\operatorname{Spec}(k[x_1, ..., x_n])$ contains in some way the points of $\mathbb{A}^n_K$, K/k a finite extension field. Let us look at the extension $\mathbb{C}/\mathbb{R}$. The set $\{\, (\pm i, 1) \in \mathbb{A}^2_{\mathbb{C}} \,\}$ corresponds to the maximal ideal $\langle\, x^2 + 1, y - 1 \,\rangle \subset \mathbb{R}[x, y]$. Indeed,

$$\mathbb{R}[x, y]/\langle\, x^2 + 1, y - 1 \,\rangle \cong \mathbb{R}[x]/\langle x^2 + 1 \rangle \cong \mathbb{C}.$$

[22] The canonical map (see Page 5 and Exercise I.1.9) $k[x_1, ..., x_n] \longrightarrow k$ that sends x_i to a_i, $i = 1, ..., n$, factorizes over an isomorphism $k[x_1, ..., x_n]/\langle\, x_1 - a_1, ..., x_n - a_n \,\rangle \longrightarrow k$.

The fact that $\langle\, x^2 + 1, y - 1 \,\rangle$ gives two points is reflected by the fact that we have two $\mathbb{R}$-linear isomorphisms between $\mathbb{R}[x]/\langle x^2 + 1\rangle$ and $\mathbb{C}$, namely, we may map x either to i or to $-i$.

The above discussion carries over to $V(I)$ and $\mathrm{Spec}(k[x_1, ..., x_n]/I)$, $I \subset k[x_1, ..., x_n]$ an ideal. If k is not algebraically closed, it may happen that $V(I)$ is empty (see Page 44). For a non-zero ring R, the set $\mathrm{Spec}(R)$ is not empty, because R contains a prime ideal (Theorem I.4.4).

II

Noetherian Rings

In this chapter, we present the concept of a noetherian ring.[1] Noetherian rings are characterized by a finiteness condition which may be phrased in several ways. Each of the characterizations is given in terms of ideals of the ring. These rings are the most important ones appearing in algebraic geometry. For example, all coordinate algebras of algebraic varieties are noetherian rings. We also introduce a major tool for constructing new rings, namely localization. The main theorem of this chapter is the existence of primary decompositions of ideals in noetherian rings which has already been alluded to several times. It vastly generalizes prime factorizations and has also a geometric flavour: It is closely related to the decomposition of an algebraic set into its irreducible components. Primary decompositions are not unique, in general, but many important ingredients in a primary decomposition are determined by the respective ideal. In order to prove these uniqueness statements, we carefully investigate the extension and contraction of ideals under localization.

II.1 Chain Conditions

A ring R is *noetherian*, if every ideal $I \subset R$ is finitely generated, i.e., there are a natural number $n \geq 1$ and elements $a_1, ..., a_n \in I$, such that

$$I = \langle\, a_1, ..., a_n \,\rangle.$$

Let R be a ring. An *ascending chain* in R is a sequence $(I_k)_{k\in\mathbb{N}}$ of ideals with the property

$$\forall k \in \mathbb{N}: \quad I_k \subset I_{k+1}.$$

Likewise, a *descending chain* in R is a sequence $(I_k)_{k\in\mathbb{N}}$ of ideals, such that

$$\forall k \in \mathbb{N}: \quad I_k \supset I_{k+1}.$$

[1] Emmy Noether (1882 - 1935), German mathematician.

Let $(I_k)_{k\in\mathbb{N}}$ be an ascending or descending chain in R. It is *stationary*, if there is an index k_0 with

$$\forall k \geq k_0 : \quad I_k = I_{k_0}.$$

Here are two alternative characterizations of noetherian rings.

II.1.1 Theorem. *Let R be a ring. Then, the following conditions on R are equivalent:*

i) *The ring R is noetherian.*

ii) *The ring R satisfies the* ***ascending chain condition*** *(ACC), that is, every ascending chain in R is stationary.*

iii) *Every non-empty subset Σ of ideals in R contains an element which is maximal with respect to inclusion.*

Let $R \neq \{0\}$ be a notherian ring. Then, we can define Σ as the set of all proper ideals of R. Thus, the theorem asserts, in particular, that every non-zero noetherian ring has a maximal ideal. This statement is weaker than Theorem I.4.4 which asserts that every non-zero ring has a maximal ideal. In the proof of Theorem II.1.1, we use the following:

II.1.2 Axiom of dependent choice. Let X be a non-empty set and $R \subset X \times X$ a relation, satisfying the following property:

$$\forall x \in X \exists y \in X : \quad (x, y) \in R.$$

Then, there is a sequence $(x_k)_{k\in\mathbb{N}}$, such that

$$\forall k \in \mathbb{N} : \quad (x_k, x_{k+1}) \in R.$$

If we do not assume the axiom of choice, this is really an axiom: One might try to define the sequence $(x_k)_{k\in\mathbb{N}}$ by recursion. Having already constructed $x_0, ..., x_k$, there is an element $y \in X$ with $(x_k, y) \in R$. But y is, in general, not uniquely defined. We have to **choose** one. The choice, of course, depends on the previous element. So, the construction of $(x_k)_{k\in\mathbb{N}}$ requires countably many choices and these are not possible without some axiom. For a deeper discussion of this axiom, we refer the reader to [12], Chapter 2.

Proof of Theorem II.1.1. "i)$\Longrightarrow$ii)". Let $(I_k)_{k\in\mathbb{N}}$ be an ascending chain of ideals. Then,

$$I := \bigcup_{k\in\mathbb{N}} I_k$$

is also an ideal. By assumption, it is finitely generated. Pick $n \geq 1$ and $a_1, ..., a_n \in I$ with $\langle a_1, ..., a_n \rangle = I$. There are natural numbers $k_1, ..., k_n$ with $a_i \in I_{k_i}$, $i = 1, ..., n$. Set

$$k_0 := \max\{ k_1, ..., k_n \}.$$

Then, $a_i \in I_{k_0}$, $i = 1, ..., n$. We see:

$$\forall k \geq k_0 : \quad I_{k_0} \subset I_k \subset I \subset I_{k_0}.$$

This shows that $I_{k_0} = I_k$, $k \geq k_0$.

"ii)$\Longrightarrow$iii)". Suppose that iii) does not hold, and let Σ be a non-empty set of ideals in R without maximal element. Then, there exists an ascending chain $(I_k)_{k\in\mathbb{N}}$ with

$$\forall k \in \mathbb{N}: \quad I_k \in \Sigma \quad \wedge \quad I_k \subsetneq I_{k+1}.$$

We found an ascending chain in R which is not stationary, a contradiction.

"iii)$\Longrightarrow$i)". Let $I \subset R$ be an ideal. We define Σ as the set of all finitely generated ideals of R which are contained in I. Note that $\langle 0\rangle \in \Sigma$, so that $\Sigma \neq \emptyset$. Let $J \in \Sigma$ be a maximal element. We have $J \subset I$, and J is finitely generated. We have to show that $J = I$. If this were wrong, we could pick an element $a \in I \setminus J$. Then,

$$J \subsetneq J + \langle a\rangle.$$

This implies that $J + \langle a\rangle$ is **not** finitely generated. On the other hand, there exist $n \geq 1$ and $a_1, ..., a_n \in J$ with $\langle a_1, ..., a_n\rangle = J$. But then

$$J + \langle a\rangle = \langle a_1, ..., a_n, a\rangle,$$

a contradiction. □

II.1.3 Exercise. Where was the axiom of dependent choice used in the above proof? Specify the set X and the relation R to which it was applied.

II.1.4 Corollary. *Let R, S be rings and $\varphi\colon R \longrightarrow S$ a **surjective** ring homomorphism. If R is noetherian, then so is S.*

Proof. Let $J \subset S$ be an ideal of S. Then,

$$J = \varphi(I), \quad I := \varphi^{-1}(J).$$

Since I is an ideal of R and R is noetherian, there exists a natural number $n \geq 1$ and elements $a_1, ..., a_n \in I$ with $I = \langle a_1, ..., a_n\rangle$. Obviously, J is generated by the images $\varphi(a_1), ..., \varphi(a_n)$.

We can also argue by using ACC: By Exercise I.2.4, ii),

$$S \cong R/\ker(\varphi).$$

The ideals of S are in inclusion preserving bijection to the ideals of R containing $\ker(\varphi)$ (Lemma I.2.2). So, the ascending chain condition in R clearly implies the ascending chain condition in S. □

II.1.5 Examples. i) Fields are noetherian rings.

ii) Principal ideal domains are noetherian rings. Recall that $\mathbb{Z}$ and the polynomial ring $k[x]$ over a field k are examples for principal ideal domains and, thus, for noetherian rings.

iii) We let $R := \mathscr{C}^0([0,1])$ be the ring of continuous functions on the interval $[0,1]$ (compare Example I.1.3, vi). Set

$$I_k := \left\{ f \in R \,\middle|\, f_{|[0,1/k]} \equiv 0 \right\}, \quad k \geq 1.$$

Then, $(I_k)_{k\geq 1}$ is an ascending chain which is not stationary. In particular, R is **not** a noetherian ring.

II.1.6 Hilbert's basis theorem. *If R is a noetherian ring, then the polynomial ring $R[x]$ is also a noetherian ring.*

Proof. Assume that $R[x]$ is not noetherian. Let $I \subset R[x]$ be an ideal which is not finitely generated and X the set of all finite subsets of I. It is obviously non-empty. For $x, y \in X$, we write $x < y$, if $x \subset y$, $\#y = \#x + 1$, and the unique element $f \in y \setminus x$ satisfies

$$f \notin \langle x \rangle \quad \wedge \quad \forall g \in I \setminus \langle x \rangle : \quad \deg(g) \geq \deg(f).$$

Since I is not finitely generated, it is clear that we find for each $x \in X$ an element $y \in X$ with $x < y$. By the axiom of dependent choice II.1.2, there is a sequence $(x_k)_{k\in\mathbb{N}}$ with $x_k \in X$ and $x_k < x_{k+1}$, $k \in \mathbb{N}$. This defines the sequence $(f_k)_{k\geq 1}$ with

$$\{f_k\} = x_k \setminus x_{k-1}, \quad k \geq 1.$$

Finally, we obtain the sequence $(a_k)_{k\geq 1}$ in R in which a_k is the leading coefficient of f_k, i.e., the coefficient of $x^{\deg(f_k)}$ in f_k, $k \geq 1$.

Claim. $\forall k \geq 1 : \langle\, a_1, ..., a_k \,\rangle \subsetneq \langle\, a_1, ..., a_k, a_{k+1} \,\rangle$.

If we had $\langle\, a_1, ..., a_k \,\rangle = \langle\, a_1, ..., a_k, a_{k+1} \,\rangle$, then there were elements $r_1, ..., r_k \in R$ with

$$a_{k+1} = \sum_{i=1}^{k} r_i \cdot a_i.$$

The definition of the relation "<" implies

$$\forall k : \quad \deg(f_k) \leq \deg(f_{k+1}).$$

Therefore, we can define

$$g := f_{k+1} - \sum_{i=1}^{k} r_i \cdot x^{\deg(f_{k+1})-\deg(f_i)} \cdot f_i. \tag{II.1}$$

But then,

$$\deg(g) < \deg(f_{k+1}).$$

By construction of "<", f_{k+1} has the least degree among all elements of I that are not contained in $\langle x_0 \rangle + \langle\, f_1, ..., f_k \,\rangle$. So, we must have $g \in \langle x_0 \rangle + \langle\, f_1, ..., f_k \,\rangle$. Now, (II.1) shows $f_{k+1} \in \langle x_0 \rangle + \langle\, f_1, ..., f_k \,\rangle$, and this is a contradiction. ✓

This claim shows that $(\langle\, a_1, ..., a_k \,\rangle)_{k\geq 1}$ is a non-stationary ascending chain in R. This contradicts the assumption that R is noetherian. □

II.1.7 Corollary. *Let R be a noetherian ring, e.g., a field. Then, the polynomial ring $R[x_1, ..., x_n]$ is noetherian, $n \geq 1$.*

II.1.8 Remark (An application to algebraic sets). Let k be a field, $n \geq 1$ a natural number, $k[x_1, ..., x_n]$ the polynomial ring in n variables, and $F \subset k[x_1, ..., x_n]$ a possibly infinite subset. We claim that there are a natural number $m \geq 1$ and elements $f_1, ..., f_m \in F$ with

$$V(F) = V(\{\, f_1, ..., f_m \,\}).$$

In particular, every algebraic set may be defined by finitely many equations. According to Property I.9.1, v),

$$V(F) = V(\langle F \rangle).$$

Now, $k[x_1, ..., x_n]$ is a noetherian ring, so that $\langle F \rangle$ is finitely generated. Pick a natural number $s \geq 1$ and elements $g_1, ..., g_s$ with

$$\langle F \rangle = \langle\, g_1, ..., g_s \,\rangle.$$

Then,

$$V(F) = V(\{\, g_1, ..., g_s \,\}),$$

but the elements $g_1, ..., g_s$ need not belong to F. However, there are elements

$$a_{ij} \in R \quad \text{and} \quad f_{ij} \in F, \quad j = 1, ..., m_i, i = 1, ..., s,$$

such that

$$g_i = \sum_{j=1}^{m_i} a_{ij} \cdot f_{ij}, \quad i = 1, ..., s.$$

We obviously have

$$\langle F \rangle = \langle\, f_{11}, ..., f_{1m_1}, ..., f_{s1}, ..., f_{sm_s} \,\rangle$$

and, consequently,

$$V(F) = V(\langle F \rangle) = V(\langle\, f_{11}, ..., f_{1m_1}, ..., f_{s1}, ..., f_{sm_s} \,\rangle) = V(\{\, f_{11}, ..., f_{1m_1}, ..., f_{s1}, ..., f_{sm_s} \,\}).$$

Let R be a ring. An *R-algebra* is a ring S together with a ring homomorphism $\varphi\colon R \longrightarrow S$. An R-algebra S is *finitely generated*, if there are elements $f_1, ..., f_n \in S$, such that the homomorphism

$$R[x_1, ..., x_n] \longrightarrow S$$

that is associated with φ and the assignment $x_i \longmapsto f_i$, $i = 1, ..., n$, is surjective (compare Exercise I.1.9). One writes abusively

$$S = R[f_1, ..., f_n].$$

II.1.9 Proposition. *If R is a noetherian ring and S is a finitely generated R-algebra, then S is also a noetherian ring.*

II.1.10 Example. Let k be a field, $n \geq 1$ a natural number, and $Z \subset \mathbb{A}^n_k$ an algebraic set. Then, the coordinate algebra

$$k[x_1, ..., x_n]/I(Z)$$

is a finitely generated k-algebra and, hence, a noetherian ring.

II.1.11 Exercise (Noetherian rings and spaces). i) Let k be a field. Then, one may define the polynomial ring $R := k[x_1, x_2, x_3, ...]$ in the infinitely many variables x_i, $i \geq 1$. Is R noetherian?

ii) A topological space X is called *noetherian*, if it satisfies the descending chain condition for closed subsets, i.e., for any sequence

$$Z_1 \supset Z_2 \supset \cdots$$

of closed subsets of X, there is an index k_0, such that $Z_k = Z_{k_0}$, for every $k \geq k_0$. Let R be a noetherian ring. Show that $\mathrm{Spec}(R)$ is a noetherian topological space.

iii) Give an example of a **non**-noetherian ring R, such that $\mathrm{Spec}(R)$ consists of just one point (and is, therefore, noetherian).

II.2 Artinian Rings

A ring satisfies the *descending chain condition* (DCC), if every descending chain of ideals in R is stationary. A ring which satisfies the descending chain condition is called an *artinian*[2] ring. It might be surprising that the descending chain condition is much more restrictive than the ascending chain condition. In fact, it turns out that artinian rings are very special noetherian rings (see [1], Theorem 8.5). We will not discuss this in full detail. Instead we give some indications.

II.2.1 Proposition. *In an artinian ring, every prime ideal is maximal.*

Proof. Let R be an artinian ring and $\mathfrak{p} \subset R$ a prime ideal. Then, $R/\mathfrak{p}$ is an integral domain. Lemma I.2.2 shows that $R/\mathfrak{p}$ satisfies the descending chain condition (compare the proof of Corollary II.1.4). Let $x \in R/\mathfrak{p}$ be a non-zero element. Consider the descending chain

$$(\langle x^k \rangle)_{k\in\mathbb{N}}.$$

For some $k_0 \geq 0$,

$$\langle x^{k_0} \rangle = \langle x^{k_0+1} \rangle.$$

Thus, there exists an element $a \in R/\mathfrak{p}$ with $x^{k_0} = a \cdot x^{k_0+1}$. In other words,

$$x^{k_0} \cdot (1 - a \cdot x) = 0.$$

Since $R/\mathfrak{p}$ is an integral domain, $x^{k_0} \neq 0$ and, so, $1 - a \cdot x = 0$ and x is a unit.

Every element $x \in (R/\mathfrak{p}) \setminus \{0\}$ is a unit. This shows that $R/\mathfrak{p}$ is a field and $\mathfrak{p}$ is a maximal ideal. □

II.2.2 Examples. Let k be a field.

i) Let R be a k-algebra which is finite dimensional as a k-vector space. Then, R satisfies the ascending and descending chain condition for dimension reasons. (Ideals in R are, in particular, sub vector spaces.) So, R is both noetherian and artinian.

ii) For $n \geq 1$, $k[x]/\langle x^n \rangle$ is a k-algebra which has dimension n as k-vector space. By i), it is an artinian ring.

II.3 Localization

Let R be a ring. A subset $S \subset R$ is *multiplicatively closed*, if

- ⋆ $1 \in S$,
- ⋆ $\forall s, t \in S\colon\ s \cdot t \in S$.

II.3.1 Example. Let R be a ring, $f \in R$, and $\mathfrak{p} \subset R$ a prime ideal. Then, the following subsets of R are multiplicatively closed:

- ⋆ $S := \{\, a \in R \mid a \text{ is not a zero divisor } \}$.
- ⋆ $S := \{\, f^k \mid k \in \mathbb{N} \,\} = \{\, 1, f, f^2, \ldots \}$.

[2] Emil Artin (1898 - 1962), Austrian mathematician.

★ $S := R \setminus \mathfrak{p}$.

Let R be a ring and $S \subset R$ a multiplicatively closed subset. We define a relation "$\sim$" on $R \times S$ by:

$$\forall (a,s),(b,t) \in R \times S : \quad (a,s) \sim (b,t) \quad :\Longleftrightarrow \quad \exists u \in S : \; u \cdot (a \cdot t - b \cdot s) = 0.$$

II.3.2 Lemma. *The relation "$\sim$" is an equivalence relation on $R \times S$.*

Proof. Reflexivity and symmetry follow easily from $1 \in S$. For transitivity, let (a,s), $(b,t),(c,u) \in R \times S$ with $(a,s) \sim (b,t)$ and $(b,t) \sim (c,u)$. This means that there exist elements $v, w \in S$ with

$$v \cdot (a \cdot t - b \cdot s) = 0 \quad \text{and} \quad w \cdot (b \cdot u - c \cdot t) = 0.$$

We multiply the first equation by $u \cdot w$, the second by $v \cdot s$ and find

$$\begin{aligned} u \cdot v \cdot w \cdot a \cdot t - u \cdot v \cdot w \cdot b \cdot s &= 0 \\ u \cdot v \cdot w \cdot b \cdot s - v \cdot w \cdot c \cdot t \cdot s &= 0. \end{aligned}$$

Adding these two yields

$$t \cdot v \cdot w \cdot (a \cdot u - c \cdot s) = u \cdot v \cdot w \cdot a \cdot t - v \cdot w \cdot c \cdot t \cdot s = 0.$$

Since S is multiplicatively closed, $t \cdot v \cdot w \in S$, and we see $(a,s) \sim (c,u)$. □

II.3.3 Remarks. Assume that R is an integral domain and $0 \notin S$. Then,[3]

$$\forall (a,s),(b,t) \in R \times S : \quad (a,s) \sim (b,t) \quad \Longleftrightarrow \quad a \cdot t - b \cdot s = 0.$$

If R does contain zero divisors, it is necessary to formulate the relation "$\sim$" as above in order to get an equivalence relation.

In the following, we write

$$\frac{a}{s}$$

for the equivalence class of (a,s), $a \in R$, $s \in S$, and set

$$R_S := \left\{ \frac{a}{s} \,\middle|\, a \in R, s \in S \right\}.$$

II.3.4 Notation. i) Other common symbols for R_S are $S^{-1}R$ and $R[S^{-1}]$.
ii) Let $f \in R$ and $S = \{ f^k \mid k \in \mathbb{N} \}$. Then, we write R_f for R_S.
iii) Let $\mathfrak{p} \subset R$ be a prime ideal and $S := R \setminus \mathfrak{p}$. We will write $R_\mathfrak{p}$ instead of R_S.

Next, we equip R_S with the structure of a ring. The *addition* is defined via

$$\begin{aligned} +\colon R_S \times R_S &\longrightarrow R_S \\ \left(\frac{a}{s}, \frac{b}{t}\right) &\longmapsto \frac{a \cdot t + b \cdot s}{s \cdot t}. \end{aligned}$$

[3] Compare Page 25.

We first check that this is well-defined. Let $(a, s), (a', s'), (b, t) \in R \times S$ with

$$(a, s) \sim (a', s').$$

We need to show

$$(a \cdot t + b \cdot s, s \cdot t) \sim (a' \cdot t + b \cdot s', s' \cdot t). \tag{II.2}$$

For this, we observe

$$\Delta := (a \cdot t + b \cdot s) \cdot s' \cdot t - (a' \cdot t + b \cdot s') \cdot s \cdot t = a \cdot s' \cdot t^2 - a' \cdot s \cdot t^2 = (a \cdot s' - a' \cdot s) \cdot t^2.$$

If $u \in S$ annihilates $a \cdot s' - a' \cdot s$, then u also annihilates Δ. This establishes (II.2). ✓

The addition is clearly commutative, and

$$0 := \frac{0}{1}$$

is the neutral element. Finally, we check associativity: Let a/s, b/t, and $c/u \in R_S$. We compute

$$\begin{aligned}\left(\frac{a}{s} + \frac{b}{t}\right) + \frac{c}{u} &= \frac{a \cdot t + b \cdot s}{s \cdot t} + \frac{c}{u} \\ &= \frac{a \cdot t \cdot u + b \cdot s \cdot u + c \cdot s \cdot t}{s \cdot t \cdot u} \\ &= \frac{a}{s} + \frac{b \cdot u + c \cdot t}{t \cdot u} \\ &= \frac{a}{s} + \left(\frac{b}{t} + \frac{c}{u}\right).\end{aligned}$$

The *multiplication* is defined as

$$\begin{aligned}\cdot \colon R_S \times R_S &\longrightarrow R_S \\ \left(\frac{a}{s}, \frac{b}{t}\right) &\longmapsto \frac{a \cdot b}{s \cdot t}.\end{aligned}$$

Again, we verify that this is well-defined. For $(a, s), (a', s'), (b, t) \in R \times S$ with

$$(a, s) \sim (a', s'),$$

we have to establish

$$(a \cdot b, s \cdot t) \sim (a' \cdot b, s' \cdot t). \tag{II.3}$$

We form

$$\Delta := a \cdot b \cdot s' \cdot t - a' \cdot b \cdot s \cdot t = (a \cdot s' - a' \cdot s) \cdot b \cdot t.$$

If $u \in S$ annihilates $a \cdot s' - a' \cdot s$, then u also annihilates Δ. We infer (II.3). ✓

It is immediate that multiplication is commutative and associative and that

$$1 := \frac{1}{1}$$

is the neutral element.

The last thing we verify is the distributive law. For a/s, b/t, and $c/u \in R_S$, we find

$$\begin{aligned}\frac{a}{s}\cdot\left(\frac{b}{t}+\frac{c}{u}\right) &= \frac{a}{s}\cdot\frac{b\cdot u+c\cdot t}{t\cdot u}\\ &= \frac{a\cdot b\cdot u+a\cdot c\cdot t}{s\cdot t\cdot u}\\ &= \frac{a\cdot b\cdot s\cdot u+a\cdot c\cdot s\cdot t}{s^2\cdot t\cdot u}\\ &= \frac{a\cdot b}{s\cdot t}+\frac{a\cdot c}{s\cdot u}\\ &= \frac{a}{s}\cdot\frac{b}{t}+\frac{a}{s}\cdot\frac{c}{u}.\end{aligned}$$

So, $(R_S, +, \cdot, 0, 1)$ is a ring.

II.3.5 Example. i) If R is an integral domain and $S := R \setminus \{0\}$, then R_S is the quotient field of R that was already considered in Section I.6.

ii) In an arbitrary ring R,

$$S := \{\, s \in R \mid s \text{ is not a zero divisor} \,\}$$

is a multiplicatively closed subset. In this case, $Q(R) := R_S$ is the *total ring of fractions of* R.

iii) The ring R_S is the zero ring if and only if $0 \in S$. In fact, $0/1 = 1/1$ is equivalent to the existence of an element $s \in S$ with $s \cdot 1 = 0$. Multiplicatively closed subsets of R which contain zero are, e.g., $\{0, 1\}$, R.

We look at the homomorphism

$$\begin{aligned}\varphi\colon R &\longrightarrow R_S\\ a &\longmapsto \frac{a}{1}.\end{aligned}$$

Note that

$$\frac{a}{1} = \varphi(a) = 0 \quad\Longleftrightarrow\quad \exists s \in S : \quad s\cdot a = 0.$$

This shows

$$\ker(\varphi) = \bigcup_{s\in S} \operatorname{Ann}(s).$$

In particular, if R is an integral domain, φ is injective.

II.3.6 Proposition. i) *For every ideal $I \subset R$, the extension of I via φ is*

$$I^{\mathrm{e}} = J := \left\{ \frac{a}{s} \,\middle|\, a \in I, s \in S \right\}.$$

ii) *For an ideal $I \subset R$,*

$$I^{\mathrm{e}} = R_S \quad\Longleftrightarrow\quad I \cap S \neq \varnothing.$$

iii) *Every ideal $J \subset R_S$ is an extended ideal.*

iv) *For an ideal $I \subset R$, we have*

$$I^{\mathrm{ec}} = \bigcup_{s \in S} (I : \langle s \rangle)$$

v) *An ideal $I \subset R$ is a contracted ideal if and only if, for all $s \in S$, $[s]$ is not a zero divisor in R/I.*

Proof. i) It is clear that $\varphi(I) \subset J \subset I^{\mathrm{e}}$. Since I^{e} is the smallest ideal of R_S which contains $\varphi(I)$, it suffices to show that J is an ideal. But this is immediate.

ii) "$\Longleftarrow$". If $s \in I \cap S$, then

$$1 = \frac{s}{s} \in I^{\mathrm{e}}.$$

"$\Longrightarrow$". For $a \in I$ and $s \in S$, the equation

$$\frac{a}{s} = 1$$

implies that there is element $t \in S$ with

$$t \cdot a - s \cdot t = t \cdot (a - s) = 0.$$

So, $s \cdot t \in I \cap S$.

iii) By Property I.8.24, i), $J^{\mathrm{ce}} \subset J$. So, we have to show $J \subset J^{\mathrm{ce}}$. Let $a/s \in J$. Then,

$$\frac{a}{1} = \frac{s}{1} \cdot \frac{a}{s} \in J.$$

This shows $a \in J^{\mathrm{c}}$ and $a/s \in J^{\mathrm{ce}}$.

iv) "$\subset$". Let $a \in I^{\mathrm{ec}}$. This means that there exist $b \in I$ and $s \in S$ with

$$\frac{a}{1} = \frac{b}{s}.$$

So, there exists an element $t \in S$ with

$$t \cdot (a \cdot s - b) = 0.$$

For $u := s \cdot t \in S$, we obtain

$$u \cdot a \in I, \quad \text{i.e.,} \quad a \in (I : \langle u \rangle).$$

"$\supset$". Let $s \in S$ and $a \in (I : \langle s \rangle)$. Then, $b := a \cdot s \in I$, so that

$$\frac{a}{1} = \frac{b}{s} \in I^{\mathrm{e}}.$$

This shows $a \in I^{\mathrm{ec}}$.

v) Since $I \subset I^{\mathrm{ec}}$ (Property I.8.24, i), we have to investigate the condition $I^{\mathrm{ec}} \subset I$. By iv), it is equivalent to

$$\forall s \in S : \quad (I : \langle s \rangle) \subset I.$$

This condition is, in turn, equivalent to

$$\forall s \in S \, \forall a \in R : \quad a \cdot s \in I \quad \Longrightarrow \quad a \in I.$$

This is equivalent to the condition that $[s] \in R/I$ is not a zero divisor, $s \in S$. □

II.3.7 Corollary. *Let R, S, and $\varphi\colon R \longrightarrow R_S$ be as in the proposition.*

i) *The assignment $\mathfrak{p} \longmapsto \mathfrak{p}^e$ gives an inclusion preserving bijection between the prime ideals of R with $\mathfrak{p} \cap S = \emptyset$ and the prime ideals of R_S.*

ii) *Let $\mathfrak{p} \subset R$ be a prime ideal. Then, $R_\mathfrak{p}$ is a local ring with maximal ideal $\mathfrak{p}^e$.*

Proof. i) Let $\mathfrak{p} \subset R$ be a prime ideal with $\mathfrak{p} \cap S = \emptyset$. By Part ii) of the proposition, $\mathfrak{p}^e$ is a proper ideal of R. We show that it is a prime ideal. Let $a, b \in R$ and $s, t \in S$ with

$$\frac{a \cdot b}{s \cdot t} = \frac{a}{s} \cdot \frac{b}{t} \in \mathfrak{p}^e.$$

So, there exist $c \in \mathfrak{p}$ and $u \in S$ with

$$\frac{a \cdot b}{s \cdot t} = \frac{c}{u},$$

i.e.,

$$\exists v \in S : \quad v \cdot (a \cdot b \cdot u - c \cdot s \cdot t) = 0.$$

We see

$$(a \cdot b) \cdot (u \cdot v) = (s \cdot t \cdot v) \cdot c \in \mathfrak{p}.$$

Since $u, v \notin \mathfrak{p}$, we have $u \cdot v \notin \mathfrak{p}$ and $a \cdot b \in \mathfrak{p}$. This means $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$ and

$$\frac{a}{s} \in \mathfrak{p}^e \quad \text{or} \quad \frac{b}{t} \in \mathfrak{p}^e.$$

Finally, $R/\mathfrak{p}$ is an integral domain (Proposition I.4.1, i). Since $\mathfrak{p} \cap S = \emptyset$, we have $0 \neq [s] \in R/\mathfrak{p}$, i.e., $[s]$ is not a zero divisor, $s \in S$. Proposition II.3.6, v), shows $\mathfrak{p}^{ec} = \mathfrak{p}$.

ii) This follows immediately from i): For a prime ideal $\mathfrak{q} \subset R$, $\mathfrak{q} \cap (R \setminus \mathfrak{p}) = \emptyset$ is equivalent to $\mathfrak{q} \subset \mathfrak{p}$. □

II.3.8 Exercise (The universal property of localization). Let R be a ring, $S \subset R$ a multiplicatively closed subset, and $\varphi\colon R \longrightarrow R_S$, $x \longmapsto x/1$, the canonical homomorphism to the localization. Show that the pair (R_S, φ) has the following universal property: For any ring T and any homomorphism $\psi\colon R \longrightarrow T$, such that $\psi(S) \subset T^\star$, there is a unique homomorphism $\psi_S : R_S \longrightarrow T$ with $\psi = \psi_S \circ \varphi$.

To conclude this section, we will give another proof of Proposition I.7.2 which only uses the axiom that every non-zero ring possesses a prime ideal. This axiom is weaker than the axiom of choice (see Remark I.4.5, ii).

Alternative proof of Proposition I.7.2. The inclusion "$\subset$" is obtained as before. For the converse inclusion, let $f \in R \setminus \mathfrak{N}$. Then, the multiplicatively closed subset $S = \{ f^k \mid k \in \mathbb{N} \}$ does not contain 0, so that $R_f \neq \{0\}$, by Example II.3.5, iii). Let $\mathfrak{q} \subset R_f$ be a prime ideal. Then, $\mathfrak{p} := \mathfrak{q}^c$ is a prime ideal of R with

$$\mathfrak{p} \cap \{ f^k \mid k \in \mathbb{N} \} = \emptyset,$$

i.e., $f \notin \mathfrak{p}$. □

II.4 Primary Decomposition

In the ring of integers, we need powers of prime numbers in order to factorize all positive integers. We now need the ideal theoretic analogs for powers of prime numbers. It turns out that these are quite subtle.

Let R be a ring. An ideal $\mathfrak{q} \subset R$ is *primary*, if the following property holds:

$$\forall a, b \in R: \quad a \cdot b \in \mathfrak{q} \quad \Longrightarrow \quad a \in \mathfrak{q} \quad \vee \quad \exists k \geq 1: \quad b^k \in \mathfrak{q}.$$

II.4.1 Lemma. *An ideal $\mathfrak{q} \subset R$ is a primary ideal if and only if every zero divisor in the ring $R/\mathfrak{q}$ is nilpotent.*

Proof. Assume that $\mathfrak{q}$ is a primary ideal and that $b \in R$ is an element, such that $[b] \in R/\mathfrak{q}$ is a zero divisor. Then, there is an element $a \in R$ with $[a] \neq 0$ and $[a \cdot b] = [a] \cdot [b] = 0$. This means that $a \cdot b \in \mathfrak{q}$ but $a \notin \mathfrak{q}$. By assumption, there is an exponent $k \geq 1$ with $b^k \in \mathfrak{q}$, i.e., $[b]^k = 0$.

Now, assume that every zero divisor in $R/\mathfrak{q}$ is nilpotent. Let $a, b \in R$ with $a \cdot b \in \mathfrak{q}$. This means $[a] \cdot [b] = [a \cdot b] = 0$ in $R/\mathfrak{q}$. So, $[a] = 0$ or $[b]$ is a zero divisor and there exists a natural number $k \geq 1$ with $[b^k] = [b]^k = 0$. This shows $a \in \mathfrak{q}$ or there is a natural number $k \geq 1$ with $b^k \in \mathfrak{q}$. □

II.4.2 Examples. i) A prime ideal is a primary ideal.

ii) If $\varphi\colon R \longrightarrow S$ is a ring homomorphism and $\mathfrak{q} \subset S$ is a primary ideal, then $\mathfrak{q}^c \subset R$ is a primary ideal. In fact, by Exercise I.2.4, ii), we have an injective homomorphism

$$\overline{\varphi}\colon R/\mathfrak{q}^c \longrightarrow S/\mathfrak{q},$$

so that we may apply Lemma II.4.1.

II.4.3 Lemma. *Let R be a ring and $\mathfrak{q} \subset R$ a primary ideal, then the radical $\sqrt{\mathfrak{q}}$ is a prime ideal.*

Proof. Let $a, b \in R$ be elements with $a \cdot b \in \sqrt{\mathfrak{q}}$. There is an exponent $k \geq 1$ with

$$a^k \cdot b^k = (a \cdot b)^k \in \mathfrak{q}.$$

Then, $a^k \in \mathfrak{q}$ or there is an exponent $l \geq 1$ with

$$b^{k \cdot l} = (b^k)^l \in \mathfrak{q}.$$

This shows $a \in \sqrt{\mathfrak{q}}$ or $b \in \sqrt{\mathfrak{q}}$ as asserted. □

Let $\mathfrak{q} \subset R$ be an ideal and $\mathfrak{p}$ a prime ideal. We say that $\mathfrak{q}$ is a $\mathfrak{p}$-*primary ideal*, if it is a primary ideal with $\sqrt{\mathfrak{q}} = \mathfrak{p}$.

II.4.4 Examples. i) The primary ideals of $\mathbb{Z}$ are exactly the ideals of the form $\langle p^k \rangle$, p a prime number, $k \geq 1$ a natural number. First, let $\mathfrak{q} \subset \mathbb{Z}$ be a primary ideal. According to Lemma II.4.3, $\sqrt{\mathfrak{q}}$ is a prime ideal, i.e., of the form $\langle p \rangle$, for some prime number p. By Example I.8.20, i), $\mathfrak{q} = \langle p^k \rangle$, for some natural number $k \geq 1$. Second, let $k \geq 1$ be a natural number and p a prime number. For integers $a, b \in \mathbb{Z}$, $a \cdot b \in \langle p^k \rangle$ means $p^k | (a \cdot b)$.

Then, p^k divides a or p divides b and, then, p^k divides b^k. It follows that $a \in \langle p^k \rangle$ or $b^k \in \langle p^k \rangle$.

ii) Let k be a field, $R = k[x, y]$, and $\mathfrak{q} := \langle x, y^2 \rangle$. Then,

$$R/\mathfrak{q} \cong k[y]/\langle y^2 \rangle.$$

The zero divisors in that ring form the ideal $\langle y \rangle$. The elements of that ideal are all nilpotent. So, $\mathfrak{q}$ is a primary ideal. Its radical is

$$\sqrt{\mathfrak{q}} = \langle x, y \rangle =: \mathfrak{p}.$$

Observe

$$\mathfrak{p}^2 = \langle x^2, x \cdot y, y^2 \rangle \subsetneq \mathfrak{q} = \langle x, y^2 \rangle \subsetneq \mathfrak{p} = \langle x, y \rangle.$$

This shows:

Not every primary ideal is the power of a prime ideal.

iii) Let k be a field and

$$R := k[x, y, z]/\langle x \cdot y - z^2 \rangle.$$

We look at

$$\mathfrak{p} := \langle [x], [z] \rangle.$$

Since

$$R/\mathfrak{p} = k[y],$$

the ideal $\mathfrak{p}$ is a prime ideal. We claim that the ideal $\mathfrak{p}^2$ is not primary. We have

$$[x] \cdot [y] = [z]^2 \in \mathfrak{p}^2.$$

Here, $[x] \notin \mathfrak{p}^2$ and, for all $k \geq 1$, $[y]^k \notin \mathfrak{p}^2$. We note:

Not every power of a prime ideal is a primary ideal.

The phenomenon in Example II.4.4, iii), cannot be observed in rings in which every non-zero prime ideal is a maximal ideal, such as principal ideal domains. More generally, the following holds true:

II.4.5 Lemma. *Let R be a ring and $\mathfrak{q} \subset R$ an ideal, such that $\mathfrak{m} = \sqrt{\mathfrak{q}}$ is a maximal ideal. Then, $\mathfrak{q}$ is an $\mathfrak{m}$-primary ideal.*

Proof. By Corollary I.8.18, $\sqrt{\mathfrak{q}}$ is the intersection of all prime ideals which contain $\mathfrak{q}$. The assumption implies that $\mathfrak{m}$ is the only prime ideal which contains $\mathfrak{q}$, i.e., $R/\mathfrak{q}$ is a local ring. Let $\overline{\mathfrak{m}}$ be the image of $\mathfrak{m}$ in $R/\mathfrak{q}$. The elements of $\overline{\mathfrak{m}}$ are nilpotent, and the elements of $(R/\mathfrak{q}) \setminus \overline{\mathfrak{m}}$ are units. In particular, every zero divisor in $R/\mathfrak{q}$ is nilpotent. By Lemma II.4.1, $\mathfrak{q}$ is an $\mathfrak{m}$-primary ideal. □

II.4.6 Primary decomposition in noetherian rings. *Let R be a **noetherian** ring and $I \subsetneq R$ a proper ideal. Then, there exist a natural number $m \geq 1$ and primary ideals $\mathfrak{q}_1, ..., \mathfrak{q}_m$, such that*

$$I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_m.$$

Proof. **Step 1.** An ideal $\mathfrak{q} \subset R$ is *irreducible*, if, for ideals $I, J \subset R$, the equality

$$\mathfrak{q} = I \cap J$$

implies $\mathfrak{q} = I$ or $\mathfrak{q} = J$.

Claim. *For every proper ideal $I \subsetneq R$, there exist a natural number $m \geq 1$ and **irreducible** ideals $\mathfrak{q}_1, ..., \mathfrak{q}_m$, such that*

$$I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_m.$$

Let Σ be the set of proper ideals in R which cannot be written as the intersection of finitely many irreducible ideals. Assume that Σ is non-empty. By Theorem II.1.1, this set contains a maximal element $\mathfrak{a}$. The ideal $\mathfrak{a}$ is not irreducible. So, there exist ideals $\mathfrak{a} \subsetneq I$ and $\mathfrak{a} \subsetneq J$ with

$$\mathfrak{a} = I \cap J.$$

Note that this implies $I \subsetneq R$ and $J \subsetneq R$, By definition of $\mathfrak{a}$, the ideals I and J are finite intersections of irreducible ideals. But then, $\mathfrak{a}$ is also an intersection of finitely many irreducible ideals, a contradiction. ✓

Step 2. By Step 1, it remains to be shown that every irreducible ideal is primary. Let $\mathfrak{q} \subset R$ be an irreducible ideal. In view of Lemma I.2.2, we may replace R by $R/\mathfrak{q}$. So, without loss of generality, we may assume $\mathfrak{q} = \langle 0 \rangle$. Let $a, b \in R$ with $a \cdot b = 0$ and $a \neq 0$. We look at the ascending chain

$$(\mathrm{Ann}(b^k))_{k \in \mathbb{N}}.$$

Since R is noetherian, there exists a natural number $k_0 \in \mathbb{N}$ with

$$\mathrm{Ann}(b^{k_0}) = \mathrm{Ann}(b^{k_0+1}).$$

Claim. $\langle a \rangle \cap \langle b^{k_0} \rangle = \langle 0 \rangle$.

Let $c \in \langle a \rangle \cap \langle b^{k_0} \rangle$. We write $c = r \cdot b^{k_0}$ for a suitable element $r \in R$. Since $c \in \langle a \rangle$, we have

$$0 = c \cdot b = r \cdot b^{k_0+1}.$$

This means

$$r \in \mathrm{Ann}(b^{k_0+1}) = \mathrm{Ann}(b^{k_0}),$$

so that $c = r \cdot b^{k_0} = 0$. ✓

Since $\langle 0 \rangle$ is irreducible and $\langle 0 \rangle \neq \langle a \rangle$, we have $\langle 0 \rangle = \langle b^{k_0} \rangle$, i.e., $b^{k_0} = 0$. □

The first step of the above proof bears strong resemblance to the proof of the existence of a prime factorization in the ring of integers ([30], Satz I.3.2).

II.4.7 Corollary. *Let R be a noetherian ring and $I \subset R$ a **radical** ideal. Then, there exist **prime** ideals $\mathfrak{p}_1, ..., \mathfrak{p}_m$ with*

$$I = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_m.$$

Proof. Let

$$I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_m$$

be a primary decomposition. According to our assumption and Property I.8.19, iv), we have

$$I = \sqrt{I} = \sqrt{\mathfrak{q}_1} \cap \cdots \cap \sqrt{\mathfrak{q}_m}.$$

By Lemma II.4.3, the radical ideal $\mathfrak{p}_i := \sqrt{\mathfrak{q}_i}$ is a prime ideal, $i = 1, ..., m$. □

II.4.8 Remarks. i) The theorem is also known as the **Lasker**[4]**–Noether theorem**.

ii) A ring in which every ideal can be written as a **finite** intersection of primary ideals is called a *laskerian ring*. The above theorem states that every noetherian ring is laskerian. However, there exist laskerian rings which are not noetherian. An example is contained in [9].

iii) The zero ideal in the ring $\mathscr{C}^0([0,1])$ of continuous functions on the unit interval does not admit a primary decomposition (Exercise II.4.11).

II.4.9 Caution. In the proof of the Lasker–Noether theorem II.4.6, we showed that every irreducible ideal in a noetherian ring is a primary ideal. The converse does not hold: Let k be a field and $R := k[x,y]$.[5] We have

$$\langle\, x^2, x\cdot y, y^2 \,\rangle = \langle\, x, y^2 \,\rangle \cap \langle\, y, x^2 \rangle.$$

All occurring ideals have the maximal ideal $\mathfrak{m} = \langle\, x, y \,\rangle$ as radical, so they are all $\mathfrak{m}$-primary, by Lemma II.4.5.

The reader should also look at the proof of Lemma II.4.12. There, several primary ideals are intersected to obtain a new, non-irreducible, primary ideal. In order to obtain uniqueness statements, we have to include primary ideals which are not irreducible. This explains, in particular, why we work with primary ideals rather than with irreducible ones.

II.4.10 Exercise (Maximal ideals in rings of continuous functions). In this exercise, we work in the ring $R := \mathscr{C}^0([0,1])$ of continuous functions on the interval $[0,1] \subset \mathbb{R}$.

i) Show that, for a point $x \in [0,1]$,

$$\mathfrak{m}_x := \{\, f \in R \mid f(x) = 0 \,\}$$

is a maximal ideal in R.

ii) Let $\mathfrak{m} \subset R$ be a maximal ideal of R. Show that there exists a point $x \in [0,1]$ with $\mathfrak{m} = \mathfrak{m}_x$. (**Hint.** Use the compactness of $[0,1]$.)

II.4.11 Exercise (An ideal without primary decomposition). Let R be as in the previous exercise.

i) Let $\mathfrak{q} \subset R$ be a primary ideal. Show that there is a unique point $x \in [0,1]$ with $\mathfrak{q} \subset \mathfrak{m}_x$.

ii) Conclude that the zero ideal $\langle 0 \rangle \subset R$ cannot be written as the intersection of finitely many primary ideals.

The First Uniqueness Theorem

For the considerations in this part, we do not need to assume that the ring R is noetherian.

Unfortunately, primary decompositions are, in general, not unique. First, there are some stupid reasons for non-uniqueness which we will eliminate first. A primary decomposition

$$I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_m$$

is *minimal* or *irredundant*, if the following two properties hold:

[4] Emanuel Lasker (1868 - 1941), German chess player, mathematician, and philosopher.

[5] Example taken from `http://math.stackexchange.com/questions/28620/primary-ideals-of-noetherian-rings-which-are-not-irreducible`

i) $\forall i \in \{1, ..., m\}$: $\bigcap_{j \in \{1,...,m\} \setminus \{i\}} \mathfrak{q}_j \not\subset \mathfrak{q}_i$.

ii) For $1 \leq i < j \leq m$: $\sqrt{\mathfrak{q}_i} \neq \sqrt{\mathfrak{q}_j}$.

II.4.12 Lemma. *Let R be a ring, $I \subset R$ an ideal, and*

$$I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_m$$

a primary decomposition. Then, the ideal possesses also a minimal primary decomposition

$$I = \mathfrak{s}_1 \cap \cdots \cap \mathfrak{s}_n.$$

Proof. **Step 1.** Given any primary decomposition, one gets a primary decomposition satisfying Condition i), by just removing some of the primary components.

Step 2. The idea is to collect the primary components with the same radical in one primary component. For this, we need the following result:

Claim. *Let $\mathfrak{p} \subset R$ a prime ideal and $\mathfrak{r}_1, \mathfrak{r}_2 \subset R$ two $\mathfrak{p}$-primary ideals. Then, the intersection*

$$\mathfrak{r} := \mathfrak{r}_1 \cap \mathfrak{r}_2$$

is also a $\mathfrak{p}$-primary ideal.

We first compute the radical with the help of Property I.8.19, iv):

$$\sqrt{\mathfrak{r}_1 \cap \mathfrak{r}_2} = \sqrt{\mathfrak{r}_1} \cap \sqrt{\mathfrak{r}_2} = \mathfrak{p} \cap \mathfrak{p} = \mathfrak{p}.$$

Now, we show that $\mathfrak{r}_1 \cap \mathfrak{r}_2$ is a primary ideal. Let $a, b \in R$ with $a \cdot b \in \mathfrak{r}_1 \cap \mathfrak{r}_2$ and $a \notin \mathfrak{r}_1 \cap \mathfrak{r}_2$. We may assume without loss of generality that $a \notin \mathfrak{r}_1$. Then, there exists an exponent $k \geq 1$ with $b^k \in \mathfrak{r}_1$. So,

$$b \in \sqrt{\mathfrak{r}_1} = \sqrt{\mathfrak{r}_1 \cap \mathfrak{r}_2}.$$

This means that there is also an exponent $l \geq 1$ with $b^l \in \mathfrak{r}_1 \cap \mathfrak{r}_2$. ✓

Let $\mathfrak{p}_1, ..., \mathfrak{p}_n$ be the distinct prime ideals with

$$\{\mathfrak{p}_1, ..., \mathfrak{p}_n\} = \{\sqrt{\mathfrak{q}_1}, ..., \sqrt{\mathfrak{q}_m}\}.$$

Set

$$I_j := \{i \in \{1, ..., m\} \mid \sqrt{\mathfrak{q}_i} = \mathfrak{p}_j\} \quad \text{and} \quad \mathfrak{r}_j = \bigcap_{i \in I_j} \mathfrak{q}_i, \quad j = 1, ..., n.$$

By the claim,

$$I = \mathfrak{r}_1 \cap \cdots \cap \mathfrak{r}_n \tag{II.4}$$

is a primary decomposition with satisfies Condition ii). If the primary decomposition we started with satisfied Condition i), (II.4) will also satisfy Condition i). Otherwise we apply Step 1 to (II.4). □

II.4.13 Example. Let k be a field and $R = k[x, y]$. Here, we have

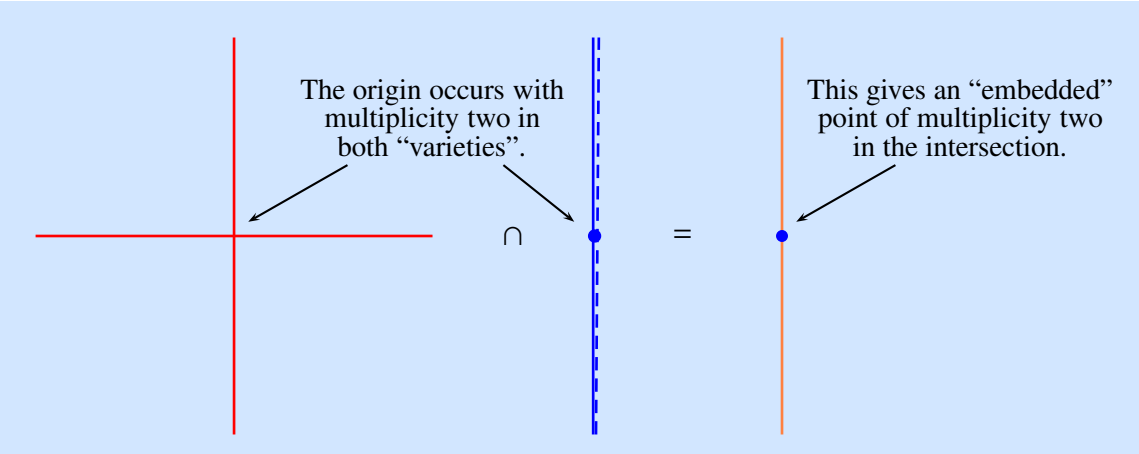
$$\langle\, x^2, x \cdot y \,\rangle = \langle x \rangle \cap \langle\, x, y \,\rangle^2 = \langle x \rangle \cap \langle\, x^2, y \,\rangle. \tag{II.5}$$

The ideal $\langle x \rangle$ is a prime ideal, and

$$\langle\, x, y \,\rangle = \sqrt{\langle\, x^2, y \,\rangle} = \sqrt{\langle\, x, y \,\rangle^2}.$$

This is a maximal ideal, so $\langle\, x^2, y \,\rangle$ and $\langle\, x, y \,\rangle^2$ are primary ideals. Therefore, (II.5) contains two distinct minimal primary decompositions of the same ideal.

We can understand the underlying geometry at a heuristic level. The algebraic set $V(x^2)$ is the y-axis in $\mathbb{A}^2_k$. We should count it twice. The set $V(x \cdot y)$ is the union of the coordinate axes. The intersection $V(x^2) \cap V(x \cdot y)$ consists of the y-axis. But the origin occurs with multiplicity 2, because it occurs both in $V(x^2)$ and in $V(x \cdot y)$ with multiplicity 2. This fact is reflected by the above primary decompositions.



II.4.14 First uniqueness theorem. *Let R be a ring, $I \subset R$ an ideal,*

$$I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_m$$

*a **minimal** primary decomposition, and $\mathfrak{p}_i := \sqrt{\mathfrak{q}_i}$, $i = 1, ..., m$. Then,*

$$\{\, \mathfrak{p}_1, ..., \mathfrak{p}_m \,\} = \left\{\, \mathfrak{p} \subset R \mid \mathfrak{p} \text{ is a prime ideal} : \exists r \in R \text{ with } \mathfrak{p} = \sqrt{(I : \langle r \rangle)} \,\right\}.$$

In particular, the set $\{\, \mathfrak{p}_1, ..., \mathfrak{p}_m \,\}$ depends only on I and not on the primary decomposition.

II.4.15 Corollary. *Let R be a **noetherian** ring. For every **radical** ideal $I \subset R$, there exist uniquely determined distinct prime ideals $\mathfrak{p}_1, ..., \mathfrak{p}_m$ with*

$$I = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_m.$$

Let $I \subsetneq R$ be a proper ideal. A prime ideal $\mathfrak{p} \subset R$ is *associated* with I, if there is an element $r \in R$ with

$$\mathfrak{p} = \sqrt{(I : \langle r \rangle)}.$$

The set of prime ideals associated with I is denoted by

$$\mathrm{Ass}(I).$$

The prime ideals in $\mathrm{Ass}(I)$ which are minimal with respect to inclusion among the ideals in $\mathrm{Ass}(I)$ are called *isolated*. The remaining ones are called *embedded*.

II.4.16 Example. We return to Example II.4.13 and the primary decomposition

$$\langle\, x^2, x \cdot y \,\rangle = \langle x \rangle \cap \langle\, x, y \,\rangle^2.$$

The associated prime ideals are $\langle x \rangle$ and $\langle\, x, y \,\rangle$, and we have

$$\langle x \rangle \subset \langle\, x, y \,\rangle.$$

So, $\langle x \rangle$ is an isolated associated prime ideal and $\langle\, x, y \,\rangle$ an embedded one. The corresponding geometric objects are the y-axis $V(\langle x \rangle)$ and the origin $V(\langle\, x, y \,\rangle)$. The origin is embedded into the y-axis. This explains the terminology.

We need some preparations for the proof of Theorem II.4.14.

II.4.17 Prime avoidance. *Let R be a ring.*

i) *Suppose $\mathfrak{p}_1, ..., \mathfrak{p}_m \subset R$ are prime ideals and $I \subset R$ an ideal with*

$$I \subset \bigcup_{i=1}^{m} \mathfrak{p}_i.$$

Then, there exists an index $i_0 \in \{\, 1, ..., m \,\}$ with

$$I \subset \mathfrak{p}_{i_0}.$$

ii) *Let $I_1, ..., I_m \subset R$ be ideals and $\mathfrak{p} \subset R$ a prime ideal. If*

$$\mathfrak{p} \supset \bigcap_{j=1}^{m} I_j,$$

then, there exists an index $j_0 \in \{\, 1, ..., m \,\}$ with

$$\mathfrak{p} \supset I_{j_0}.$$

Moreover, if

$$\mathfrak{p} = \bigcap_{j=1}^{m} I_j,$$

then, there exists an index $j_0 \in \{\, 1, ..., m \,\}$ with

$$\mathfrak{p} = I_{j_0},$$

i.e., prime ideals are irreducible.

Proof. i) We prove the following statement[6] by induction on m:

$$\forall i \in \{\, 1, ..., m \,\}: \quad I \not\subset \mathfrak{p}_i \quad \Longrightarrow \quad I \not\subset \bigcup_{i=1}^{m} \mathfrak{p}_i.$$

[6] This explains the name "prime avoidance": If I avoids the prime ideals $\mathfrak{p}_1$, ..., $\mathfrak{p}_m$, then it also avoids their union.

The case $m = 1$ is trivial. For the induction step "$m \longrightarrow m+1$", we may choose elements $a_1, ..., a_{m+1} \in I$ with

$$a_i \notin \mathfrak{p}_j, \quad j \in \{1, ..., m+1\} \setminus \{i\}, \quad i = 1, ..., m+1.$$

If there is an index $i_0 \in \{1, ..., m+1\}$ with $a_{i_0} \notin \mathfrak{p}_{i_0}$, we are done. Thus, we need to consider the case $a_i \in \mathfrak{p}_i$, $i = 1, ..., m+1$. We then form

$$b := \sum_{i=1}^{m+1} a_1 \cdot \cdots \cdot a_{i-1} \cdot a_{i+1} \cdot \cdots \cdot a_{m+1} \in I.$$

Let $i \in \{1, ..., m+1\}$. The i-th summand of b is not contained in $\mathfrak{p}_i$, but all the other summands are. It follows $b \notin \mathfrak{p}_i$, $i = 1, ..., m+1$.

ii) Suppose that $\mathfrak{p} \not\supset I_j$, $j = 1, ..., m$. Choose elements $a_j \in I_j \setminus \mathfrak{p}$, $j = 1, ..., m$. Then,

$$a_1 \cdot \cdots \cdot a_m \in \prod_{j=1}^{m} I_j \subset \bigcap_{j=1}^{m} I_j,$$

but

$$a_1 \cdot \cdots \cdot a_m \notin \mathfrak{p}.$$

This is a contradiction.

Assume

$$\mathfrak{p} = \bigcap_{j=1}^{m} I_j.$$

By what has already been proved, there is an index $j_0 \in \{1, ..., m\}$ with $\mathfrak{p} \supset I_{j_0}$. We clearly have $\mathfrak{p} \subset I_{j_0}$ and, thus, $\mathfrak{p} = I_{j_0}$. □

II.4.18 Lemma. *Let R be a ring, $\mathfrak{p} \subset R$ a prime ideal, $\mathfrak{q}$ a $\mathfrak{p}$-primary ideal, and $a \in R$. Then,*

$$(\mathfrak{q} : \langle a \rangle) = \begin{cases} R, & \text{if } a \in \mathfrak{q} \\ a\ \mathfrak{p}\text{-primary ideal}, & \text{if } a \notin \mathfrak{q} \\ \mathfrak{q}, & \text{if } a \notin \mathfrak{p} \end{cases}.$$

Proof. The assertion for $a \in \mathfrak{q}$ is clear. Next, let us assume $a \notin \mathfrak{p}$. If $r \in (\mathfrak{q} : \langle a \rangle)$, we have $r \cdot a \in \mathfrak{q}$. Since $a \notin \mathfrak{p} = \sqrt{\mathfrak{q}}$, we have $r \in \mathfrak{q}$. This shows $(\mathfrak{q} : \langle a \rangle) \subset \mathfrak{q}$. The other inclusion is trivial.

Next, we just assume $a \notin \mathfrak{q}$. Let us first determine the radical of $(\mathfrak{q} : \langle a \rangle)$. For $r \in (\mathfrak{q} : \langle a \rangle)$, we have $r \cdot a \in \mathfrak{q}$. Since $a \notin \mathfrak{q}$, we have $r \in \sqrt{\mathfrak{q}} = \mathfrak{p}$. This implies

$$\mathfrak{q} \subset (\mathfrak{q} : \langle a \rangle) \subset \mathfrak{p}.$$

Taking radicals yields $\sqrt{(\mathfrak{q} : \langle a \rangle)} = \mathfrak{p}$.

Finally, assume that $r, s \in R$ are elements with $r \cdot s \in (\mathfrak{q} : \langle a \rangle)$ and $s \notin \mathfrak{p} = \sqrt{(\mathfrak{q} : \langle a \rangle)}$. We have to check that $r \in (\mathfrak{q} : \langle a \rangle)$. With $a \cdot r \cdot s \in \mathfrak{q}$ and $s \notin \mathfrak{p}$, we find $a \cdot r \in \mathfrak{q}$, i.e., $r \in (\mathfrak{q} : \langle a \rangle)$. □

Proof of Theorem II.4.14. Let $I \subset R$ be an ideal and

$$I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_m$$

a minimal primary decomposition. By Property I.8.17, iv),

$$\forall a \in R: \quad (I : \langle a \rangle) = \left(\bigcap_{i=1}^{m} \mathfrak{q}_i : \langle a \rangle \right) = \bigcap_{i=1}^{m} (\mathfrak{q}_i : \langle a \rangle).$$

With Lemma II.4.18, this gives

$$\forall a \in R: \quad \sqrt{(I : \langle a \rangle)} = \bigcap_{i=1}^{m} \sqrt{(\mathfrak{q}_i : \langle a \rangle)} = \bigcap_{i \in \{ 1,\ldots,m \,|\, a \notin \mathfrak{q}_i \}} \mathfrak{p}_i. \tag{II.6}$$

a) Let $a \in R$ be an element, such that $\sqrt{(I : \langle a \rangle)}$ is a prime ideal. By (II.6) and Proposition II.4.17, ii), there is an index $i_0 \in \{ 1, ..., m \,|\, a \notin \mathfrak{q}_i \}$ with $\mathfrak{p}_{i_0} = \sqrt{(I : \langle a \rangle)}$.

b) Let $i_0 \in \{ 1, ..., m \}$. By the minimality of the primary decomposition, there is an element

$$a_{i_0} \in \left(\bigcap_{j \in \{ 1,\ldots,m \} \setminus \{ i_0 \}} \mathfrak{q}_j \right) \setminus \mathfrak{q}_{i_0}.$$

Lemma II.4.18 and (II.6) show

$$\sqrt{(I : \langle a_{i_0} \rangle)} = \mathfrak{p}_{i_0}.$$

This concludes the proof. □

II.4.19 Exercise (Irreducible sets). A topological space X is called *irreducible*, if it is nonempty, and, if X_1 and X_2 are closed subsets, such that $X = X_1 \cup X_2$, then $X_1 = X$ or $X_2 = X$. Let X be a topological space and Y a subset of X. Then, Y inherits a topology as follows: A subset $U \subset Y$ is said to be *open*, if there is an open subset $\widetilde{U} \subset X$ with $U = Y \cap \widetilde{U}$. We call a subset $Y \subset X$ *irreducible*, if it is irreducible with respect to the induced topology.

i) Let X be a noetherian topological space and Z a **closed** subset. Show that there are irreducible closed subsets Z_1,...,Z_r, such that

- ⋆ $Z = Z_1 \cup \cdots \cup Z_r$,
- ⋆ $Z_i \not\subset Z_j$, for $i \neq j$.

Show also that these closed subsets are uniquely determined. The sets Z_i, $i = 1, ..., r$, are called the *irreducible components* of Z.

ii) Let R be a noetherian ring and $I \subset R$ an ideal. What is the relation between the primary decomposition of I and the above decomposition of the closed subset $V(I) \subset \mathrm{Spec}(R)$ into irreducible components?

II.4.20 Exercise (Primary ideals). Show the following: In the polynomial ring $\mathbb{Z}[t]$, a) the ideal $\mathfrak{m} = \langle 2, t \rangle$ is maximal and b) the ideal $\mathfrak{q} = \langle 4, t \rangle$ is $\mathfrak{m}$-primary, but c) $\mathfrak{q}$ is not a power of $\mathfrak{m}$.

II.4.21 Exercise (A primary decomposition). Let k be a field and $R := k[x, y, z]$. Set $\mathfrak{p}_1 := \langle x, y \rangle$, $\mathfrak{p}_2 := \langle x, z \rangle$, and $\mathfrak{m} := \langle x, y, z \rangle$.

i) Show that $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are prime ideals, while $\mathfrak{m}$ is maximal.

ii) Let $I := \mathfrak{p}_1 \cdot \mathfrak{p}_2$. Show that

$$I = \mathfrak{p}_1 \cap \mathfrak{p}_2 \cap \mathfrak{m}^2$$

and that this a minimal primary decomposition of I.

iii) Which components are isolated and which are embedded?

II.4.22 Exercise (A primary decomposition). We work in the ring $R = k[x_1, x_2, x_3, x_4]$, k a field. Show that

$$\begin{aligned} &\langle\, x_1x_2 - x_4, x_1x_3 - x_4, x_2x_3 - x_4 \,\rangle = \\ &= \langle\, x_1, x_2, x_4 \,\rangle \cap \langle\, x_1, x_3, x_4 \,\rangle \cap \langle\, x_2, x_3, x_4 \,\rangle \cap \langle\, x_1 - x_2, x_2 - x_3, x_1^2 - x_4 \,\rangle \end{aligned}$$

is a minimal primary decomposition.

The Second Uniqueness Theorem

II.4.23 Proposition. *Let R be a ring, $S \subset R$ a multiplicatively closed subset, $\mathfrak{p} \subset R$ a prime ideal, $\mathfrak{q} \subset R$ a $\mathfrak{p}$-primary ideal, and*

$$\varphi\colon R \longrightarrow R_S$$

the natural localization homomorphism. Then:

i) *The assertion $S \cap \mathfrak{p} \neq \emptyset$ is equivalent to the assertion $\mathfrak{q}^e = R_S$.*

ii) *If $S \cap \mathfrak{p} = \emptyset$, then $\mathfrak{q}^e$ is a $\mathfrak{p}^e$-primary ideal and $\mathfrak{q}^{ec} = \mathfrak{q}$.*

Proof. i) By Proposition II.3.6, ii), the extended ideal $\mathfrak{q}^e$ equals R_S if and only if $S \cap \mathfrak{q} \neq \emptyset$. Thus, we have to prove:

Claim. $S \cap \mathfrak{p} \neq \emptyset \Longleftrightarrow S \cap \mathfrak{q} \neq \emptyset$.

"$\Longleftarrow$". This is clear, because $\mathfrak{q} \subset \mathfrak{p}$.

"$\Longrightarrow$". Let $s \in S \cap \mathfrak{p}$. Since $\mathfrak{p}$ is the radical of $\mathfrak{q}$, there is an exponent $k \geq 1$ with $s^k \in \mathfrak{q}$. Furthermore, S is a multiplicatively closed subset, so that $s^k \in S$. ✓

ii) We use the description

$$\mathfrak{q}^{ec} = \bigcup_{s \in S} (\mathfrak{q} : \langle s \rangle)$$

from Proposition II.3.6, iv). Suppose $s \in S$ and $r \in (\mathfrak{q} : \langle s \rangle)$. Then, $r \cdot s \in \mathfrak{q}$. Since $s^k \notin \mathfrak{q}$, $k \geq 1$, we must have $r \in \mathfrak{q}$. This shows $\mathfrak{q}^{ec} \subset \mathfrak{q}$. The other inclusion is contained in Property I.8.24, i), so that

$$\mathfrak{q}^{ec} = \mathfrak{q}.$$

By Proposition II.3.6, iii), $J^{ce} = J$ holds for every ideal $J \subset R_S$. So, in order to verify $\sqrt{\mathfrak{q}^e} = \mathfrak{p}^e$, it suffices to check

$$\left(\sqrt{\mathfrak{q}^e}\right)^c = \mathfrak{p}^{ec}.$$

With Property I.8.19, iv), we verify this as follows:

$$\left(\sqrt{\mathfrak{q}^e}\right)^c = \sqrt{\mathfrak{q}^{ec}} = \sqrt{\mathfrak{q}} = \mathfrak{p} = \mathfrak{p}^{ec}.$$

Finally, we check that $\mathfrak{q}^{\mathrm{e}}$ is a primary ideal. Suppose we are given $a, b \in R$ and $s, t \in R$ with

$$\frac{a \cdot b}{s \cdot t} = \frac{a}{s} \cdot \frac{b}{t} \in \mathfrak{q}^{\mathrm{e}}.$$

Then, $a \cdot b \in \mathfrak{q}^{\mathrm{ec}} = \mathfrak{q}$, so that $a \in \mathfrak{q}$ or $b^k \in \mathfrak{q}$, for some $k \geq 1$. This implies $a/s \in \mathfrak{q}^{\mathrm{e}}$ or $(b/t)^k = b^k/t^k \in \mathfrak{q}^{\mathrm{e}}$, for some $k \geq 1$. □

II.4.24 Proposition. *Let R be a ring, $S \subset R$ a multiplicatively closed subset, $I \subset R$ an ideal, and*

$$I = \bigcap_{i=1}^{m} \mathfrak{q}_i$$

a minimal primary decomposition. Set $\mathfrak{p}_i := \sqrt{\mathfrak{q}_i}$, $i = 1, ..., m$, and suppose that the numbering is such that

$$\exists m_0 \in \{0, ..., m\} \forall i \in \{1, ..., m\} : \quad S \cap \mathfrak{p}_i \neq \emptyset \quad \Longleftrightarrow \quad i > m_0.$$

Then,

$$I^{\mathrm{e}} = \bigcap_{i=1}^{m_0} \mathfrak{q}_i^{\mathrm{e}} \quad \textit{and} \quad I^{\mathrm{ec}} = \bigcap_{i=1}^{m_0} \mathfrak{q}_i, \tag{II.7}$$

and these are both minimal primary decompositions.

Proof. Using Proposition II.3.6, iii), and Property I.8.24, iv), it is enough to check the second equality in (II.7). We first apply Proposition II.3.6, iv), and Property I.8.17, iv), to see

$$I^{\mathrm{ec}} = \bigcup_{s \in S} (I : \langle s \rangle) = \bigcup_{s \in S} \left(\bigcap_{i=1}^{m} \mathfrak{q}_i : \langle s \rangle \right) = \bigcup_{s \in S} \bigcap_{i=1}^{m} (\mathfrak{q}_i : \langle s \rangle).$$

Our assertion amounts to

$$\bigcup_{s \in S} \bigcap_{i=1}^{m} (\mathfrak{q}_i : \langle s \rangle) = \bigcap_{i=1}^{m_0} \mathfrak{q}_i.$$

"$\subset$". For $s \in S$ and $1 \leq i \leq m_0$, we have $s \notin \mathfrak{p}_i$. This inclusion, therefore, follows from Lemma II.4.18.

"$\supset$". For $m_0 + 1 \leq i \leq m$, $S \cap \mathfrak{p}_i \neq \emptyset$. By Proposition II.4.23, i), we may pick an element $s_i \in S \cap \mathfrak{q}_i$. Then,

$$\forall i \in \{m_0 + 1, ..., m\} : \quad s := s_{m_0+1} \cdot \cdots \cdot s_m \in \mathfrak{q}_i.$$

Lemma II.4.18 shows

$$\forall i \in \{m_0 + 1, ..., m\} : \quad (\mathfrak{q}_i : \langle s \rangle) = R.$$

The second equation in (II.7) is a minimal primary decomposition, because $I = \bigcap_{i=1}^{m} \mathfrak{q}_i$ is one. By Proposition II.4.23, ii), $\mathfrak{q}_i^{\mathrm{e}}$ is a $\mathfrak{p}_i^{\mathrm{e}}$-primary ideal, $i = 1, ..., m_0$. This shows that the first equation in (II.7) is also a primary decomposition. To check that it is minimal, we may contract it to R. This is the second equation in (II.7) which is minimal. □

II.4.25 Second uniqueness theorem. *Let R be a ring, $I \subset R$ an ideal,*

$$I = \bigcap_{i=1}^{m} \mathfrak{q}_i \tag{II.8}$$

a minimal primary decomposition, and

$$\mathrm{Ass}(I) = \{\, \mathfrak{p}_1, ..., \mathfrak{p}_m \,\}.$$

i) *Let $\{\, i_1, ..., i_n \,\} \subset \{\, 1, ..., m \,\}$ be a subset, such that $\mathfrak{p}_{i_j}$ is an **isolated** associated prime ideal of I, $j = 1, ..., n$. Then, the **intersection***

$$\bigcap_{j=1}^{n} \mathfrak{q}_{i_j}$$

does not depend on (II.8).

ii) *Let $\mathfrak{p} \in \mathrm{Ass}(I)$ be an associated prime ideal and set*

$$M(I, \mathfrak{p}) = \{\, \mathfrak{r} \in \mathrm{Ass}(I) \,|\, \mathfrak{r} \subset \mathfrak{p} \,\}.$$

Let

$$\{\, i_1, ..., i_n \,\} = \{\, i \in \{\, 1, ..., m \,\} \,|\, \sqrt{\mathfrak{q}_i} \in M(I, \mathfrak{p}) \,\}.$$

*Then, the **intersection***

$$\bigcap_{j=1}^{n} \mathfrak{q}_{i_j}$$

does not depend on (II.8).

Proof. For i), we define

$$S := R \setminus (\mathfrak{p}_{i_1} \cup \cdots \cup \mathfrak{p}_{i_n})$$

and, for ii),

$$S := R \setminus \mathfrak{p},$$

and look at the localization map $\varphi \colon R \longrightarrow R_S$. In both cases,

$$I^{\mathrm{ec}} = \bigcap_{j=1}^{n} \mathfrak{q}_{i_j},$$

by Proposition II.4.24. □

II.4.26 Remark. In general, we may associate with any subset $\{\, \mathfrak{p}_{i_1}, ..., \mathfrak{p}_{i_m} \,\} \subset \mathrm{Ass}(I)$ an ideal which is the intersection of some of the primary ideals in (II.8) and which does not depend on I.

II.4.27 Corollary. *The primary ideals in a minimal primary decomposition of I which correspond to the **isolated** associated prime ideals are uniquely determined by I.*

Proof. Let $\mathfrak{p} \subset R$ be an isolated associated prime ideal. We apply i) to $\{\mathfrak{p}\} \subset \mathrm{Ass}(I)$ or ii), noting $M(I, \mathfrak{p}) = \{\mathfrak{p}\}$. □

To further familiarize us with primary decompositions, we study the primary decomposition of the zero ideal.

II.4.28 Theorem. *Let R be a noetherian ring. Write*

$$\{ \mathfrak{p}_{i_1}, ..., \mathfrak{p}_k \} = \mathrm{Ass}(\langle 0 \rangle)$$

and let

$$\{ \mathfrak{p}_{i_1}, ..., \mathfrak{p}_{i_m} \} \subset \mathrm{Ass}(\langle 0 \rangle)$$

*be the subset of **isolated** prime ideals associated with $\langle 0 \rangle$. Then:*

i) *The nilradical of R is*

$$\mathfrak{N} = \sqrt{\langle 0 \rangle} = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_k = \mathfrak{p}_{i_1} \cap \cdots \cap \mathfrak{p}_{i_m}.$$

ii) *Let $\mathfrak{p} \subset R$ be a prime ideal. Then, there exists an index $j \in \{ 1, ..., m \}$ with*

$$\mathfrak{p}_{i_j} \subset \mathfrak{p},$$

i.e., the isolated prime ideals associated with $\langle 0 \rangle$ are the minimal prime ideals of R.

iii) *The zero divisors of R are exactly the elements of the set*

$$\bigcup_{i=1}^{k} \mathfrak{p}_i.$$

Proof. i) Let

$$\langle 0 \rangle = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_k$$

be a minimal primary decomposition with $\mathfrak{p}_i = \sqrt{\mathfrak{q}_i}$, $i = 1, ..., k$. Then,

$$\sqrt{\langle 0 \rangle} = \sqrt{\mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_k} = \sqrt{\mathfrak{q}_1} \cap \cdots \cap \sqrt{\mathfrak{q}_k} = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_k = \mathfrak{p}_{i_1} \cap \cdots \cap \mathfrak{p}_{i_m}.$$

ii) By Proposition I.7.2, $\sqrt{\langle 0 \rangle} \subset \mathfrak{p}$, so that

$$\mathfrak{p}_{i_1} \cap \cdots \cap \mathfrak{p}_{i_m} \subset \mathfrak{p}.$$

By prime avoidance (Proposition II.4.17), there is an index $j \in \{ 1, ..., m \}$ with $\mathfrak{p}_{i_j} \subset \mathfrak{p}$.

iii) Assume first that $a \in R$ is a zero divisor. There is an element $b \in R \setminus \{0\}$ with $a \cdot b = 0$. Since $\langle 0 \rangle = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_k$, there is an index $i_0 \in \{ 1, ..., k \}$ with $b \notin \mathfrak{q}_{i_0}$. Since $\mathfrak{q}_{i_0}$ is a primary ideal, it follows that $a \in \sqrt{\mathfrak{q}_{i_0}} = \mathfrak{p}_{i_0}$.

Next, let

$$a \in \mathfrak{p}_1 \cup \cdots \cup \mathfrak{p}_k.$$

If a is nilpotent, then a is a zero divisor and we are done. Otherwise, we may choose an index $i_0 \in \{ 1, ..., k \}$ and an exponent $l \geq 1$ with $a^l \in \mathfrak{q}_{i_0}$. Note that the existence of non-nilpotent zero divisors implies $k \geq 2$. We have

$$\mathfrak{q}_{i_0} \cdot (\mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_{i_0 - 1} \cap \mathfrak{q}_{i_0 + 1} \cap \cdots \cap \mathfrak{q}_k) \subset \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_k = \langle 0 \rangle.$$

Since the primary decomposition is minimal, we infer

$$J := \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_{i_0 - 1} \cap \mathfrak{q}_{i_0 + 1} \cap \cdots \cap \mathfrak{q}_k \neq \langle 0 \rangle.$$

Choose $b \in J \setminus \{0\}$. Then, $a^l \cdot b = 0$. Let $n \geq 0$ be the largest natural number with $a^n \cdot b \neq 0$. We see that $a \cdot (a^n \cdot b) = a^{n+1} \cdot b = 0$ and that a is a zero divisor. □

III

The Nullstellensatz

We prove here Hilbert's famous Nullstellensatz. It completes our discussion from Section I.9: Over an algebraically closed ground field k, there is a correspondence between algebraic sets in $\mathbb{A}^n_k$ and radical ideals in $k[x_1, ..., x_n]$. This result, therefore, translates algebraic geometry in affine spaces into commutative algebra and establishes the close ties between these two areas of mathematics. There are many proofs of the Nullstellensatz. We will present a very elementary one which is a variant of an argument due to Munshi. The proof uses some basic facts about integral ring extensions. In order to speak about integral ring extensions, we need the language of modules. For these reasons, we take the opportunity to develop the language of modules and the formalism of finite ring extensions in some detail. We will also discuss normal rings and (Noether) normalization.

III.1 Modules

Let R be a ring. An *R-module* is an abelian group $(M, +, 0)$ together with a *scalar multiplication*

$$\cdot\colon R \times M \longmapsto M,$$

such that the following conditions are satisfied:

- ⋆ $\forall a \in R \forall x, y \in M\colon a \cdot (x + y) = a \cdot x + a \cdot y.$
- ⋆ $\forall a, b \in R \forall x \in M\colon (a + b) \cdot x = a \cdot x + b \cdot x.$
- ⋆ $\forall a, b \in R \forall x \in M\colon (a \cdot b) \cdot x = a \cdot (b \cdot x).$
- ⋆ $\forall x \in M\colon 1 \cdot x = x.$

III.1.1 Remark. Let $(M, +, 0)$ be an abelian group. The datum of a scalar multiplication $\cdot\colon R \times M \longrightarrow M$ is equivalent to the datum of a ring homomorphism[1]

$$\varphi\colon R \longrightarrow \mathrm{End}(M).$$

[1] The ring $\mathrm{End}(M)$, which is, in general, non-commutative, was described in Example I.1.3, viii).

In fact, let a scalar multiplication $\cdot\colon R \times M \longrightarrow M$ be given. The first property states that

$$\begin{array}{rcl} \mu_a\colon M & \longrightarrow & M \\ x & \longmapsto & a \cdot x \end{array}$$

is an endomorphism of the abelian group M. So, we can define

$$\begin{array}{rcl} \varphi\colon R & \longrightarrow & \mathrm{End}(M) \\ a & \longmapsto & \mu_a. \end{array}$$

The fourth property says that $\varphi(1) = \mathrm{id}_M$, the second and third property express that φ is compatible with addition and multiplication.

If we are give a ring homomorphism[2]

$$\varphi\colon R \longrightarrow \mathrm{End}(M),$$

then it is easy to check that

$$\begin{array}{rcl} \cdot\colon R \times M & \longrightarrow & M \\ (a, x) & \longmapsto & \varphi(a)(x) \end{array}$$

is a scalar multiplication.

III.1.2 Examples. i) If k is a field, a k-module is the same as a k-vector space (see [33], §7).

ii) A $\mathbb{Z}$-module is the same as an abelian group. In fact, the endomorphisms $\mu_n\colon M \longrightarrow M$ (see Remark III.1.1), $n \in \mathbb{N}$, satisfy the recursion formula

$$\forall n \in \mathbb{N} \forall x \in M: \quad \mu_{n+1}(x) = (n+1) \cdot x = n \cdot x + 1 \cdot x = n \cdot x + x = \mu_n(x) + x. \quad \text{(III.1)}$$

Furthermore, it is easy to see that $\mu_{-1}(x) = -x$ (compare Property I.1.2, ii). Thus, $\mu_0 = 0$ and

$$\forall n \in \mathbb{N} \forall x \in M: \ \mu_{-n}(x) = (-n) \cdot x = \big((-1) \cdot n\big) \cdot x = n \cdot \big((-1) \cdot x\big) = n \cdot (-x) = \mu_n(-x). \quad \text{(III.2)}$$

So, the μ_k, $k \in \mathbb{Z}$, or, equivalently, the scalar multiplication "$\cdot$" are completely determined by the condition $\mu_1 = \mathrm{id}_M$. In particular, on every abelian group, there exists at most one scalar multiplication $\cdot\colon \mathbb{Z} \times M \longrightarrow M$.

On the other hand, given an abelian group M, we can start with the constant map $\mu_0\colon M \longrightarrow M$, $x \longmapsto 0$, and define μ_n by recursion (see [27], Satz 1.3.8) via (III.1) for all natural numbers and, using (III.2), for all integers. It is then checked with various inductions (compare [27], Satz 1.3.12) that

$$\begin{array}{rcl} \cdot\colon \mathbb{Z} \times M & \longrightarrow & M \\ (k, x) & \longmapsto & \mu_k(x) \end{array}$$

is a scalar multiplication.

[2] This implies that $\varphi(1) = \mathrm{id}_M$.

iii) Let k be a field and $R = k[t]$ the polynomial ring in one variable over k. Any R-module M is, in particular, a k-vector space, and

$$\begin{aligned} f := \mu_t \colon M &\longrightarrow M \\ x &\longmapsto t \cdot x \end{aligned}$$

is a k-linear map. So, an R-module determines a pair (M, f) which consists of a k-vector space M and a k-linear map $f \colon M \longrightarrow M$.

Suppose, conversely, that M is a k-vector space and $f \colon M \longrightarrow M$ is a k-linear map. Set

$$k[f] := \left\{ \sum_{i=0}^{n} \lambda_i \cdot f^i \,\middle|\, n \in \mathbb{N}, \lambda_i \in k, i = 0, ..., n \right\} \subset \mathrm{End}(M).$$

This is a commutative subring of $\mathrm{End}(M)$. By the universal property of the polynomial ring (Page 5), id_k and $f \in k[f]$ define a (surjective) homomorphism $k[t] \longrightarrow k[f]$ and, thus, a homomorphism

$$\varphi \colon k[t] \longrightarrow \mathrm{End}(M).$$

In this way, we get an R-module structure on M. It satisfies $\mu_t = f$.

Altogether, we can say that R-modules identify with pairs (M, f) composed of a k-vector space M and a k-linear endomorphism f of M. Such objects are intensely studied in any introduction to linear algebra, especially in the situation when M is finite dimensional.

iv) Let R, S be rings and $\varphi \colon R \longrightarrow S$ a ring homomorphism. Then,

$$\begin{aligned} \cdot \colon R \times S &\longrightarrow S \\ (a, b) &\longmapsto \varphi(a) \cdot b \end{aligned}$$

equips S with the structure of an R-module. In particular, we can use $\mathrm{id}_R \colon R \longrightarrow R$ to view R as an R-module.

Let R be a ring and M, N R-modules. An *R-module homomorphism* is a map $\varphi \colon M \longrightarrow N$, such that

- ⋆ $\forall x, y \in M \colon \varphi(x + y) = \varphi(x) + \varphi(y)$.
- ⋆ $\forall a \in R \forall x \in M \colon \varphi(a \cdot x) = a \cdot \varphi(x)$.

Module homomorphisms are the maps that are compatible with the given group structures and scalar multiplications on the modules and, therefore, allow to compare different modules. As usual, there are different modules which are in a certain sense "indistinguishable". These are modules which are related by an **isomorphism**. The "categorical" definition of an isomorphism reads as follows: Let R be a ring and M, N R-modules. A map $\varphi \colon M \longrightarrow N$ is an *isomorphism of R-modules*, if

- ⋆ φ is an R-module homomorphism,
- ⋆ there exists an R-module homomorphism $\psi \colon N \longrightarrow M$ with $\varphi \circ \psi = \mathrm{id}_M$ and $\psi \circ \varphi = \mathrm{id}_N$.

III.1.3 Exercise. Let R be a ring, M, N R-Modules, and $\varphi \colon M \longrightarrow N$ an R-module homomorphism. Show that φ is an isomorphism if and only if φ is bijective.

III.1.4 Example and Exercise. Let k be a field, $R = k[x]$, and (M, f) and (N, g) k-vector spaces endowed with k-linear endomorphisms. According to Example III.1.2, iii), they define R-modules. A map $\varphi\colon M \longrightarrow N$ is a homomorphism of R-modules if and only if it is k-linear and verifies

$$\varphi \circ f = g \circ \varphi,$$

i.e., the diagram

$$\begin{array}{ccc} M & \xrightarrow{\varphi} & N \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle g} \\ M & \xrightarrow{\varphi} & N \end{array}$$

commutes.

The classification of finite dimensional $\mathbb{C}[x]$-modules is provided by the theory of the Jordan[3] normal form (see [33], §54; compare Page 87ff).

Constructions

Let R be a ring and M an R-module. A *submodule* is a subset $N \subset M$, such that

- ⋆ $N \neq \emptyset$.
- ⋆ $\forall x, y \in N\colon\ x + y \in N$.
- ⋆ $\forall a \in R \forall x \in N\colon\ a \cdot x \in N$.

Note that, for $x \in N$, we have $-x = (-1) \cdot x \in N$. Let $x_0 \in N$ (N is non-empty). Then, $0 = x_0 - x_0 \in N$. This proves that N is a subgroup of M. By the third property, N is also equipped with a scalar multiplication. So, N inherits the structure of an R-module.

III.1.5 Example. Let R be a ring. According to Example III.1.2, iv), we may view R as an R-module. The submodules of R are the ideals.

Suppose that M is an R-module and that $N \subset M$ is a submodule. Then, we can form the group M/N (see [30], Satz II.9.4). We set

$$\begin{array}{rcl} \cdot\colon R \times M/N & \longrightarrow & M/N \\ (a, [x]) & \longrightarrow & [a \cdot x]. \end{array}$$

The reader should verify that this is well-defined and equips M/N with the structure of an R-module. It is the *quotient module of M by N*.

III.1.6 Example and Exercise. Let R be a ring, M, N R-modules, and $\varphi\colon M \longrightarrow N$ a homomorphism.

i) Then,

- ⋆ $\mathrm{im}(\varphi)$ is a submodule of N.
- ⋆ $\ker(\varphi)$ is a submodule of M.
- ⋆ The module $N/\mathrm{im}(\varphi)$ is called the *cokernel* of φ.

[3] Marie Ennemond Camille Jordan (1838 - 1922), french mathematician.

ii) The first isomorphism theorem holds, i.e.,

$$M/\ker(\varphi) \cong \operatorname{im}(\varphi).$$

Let $I \neq \emptyset$ be a possibly infinite index set and $(M_i)_{i\in I}$ a family of R-modules indexed by I. The cartesian product

$$\bigtimes_{i\in I} M_i$$

together with componentwise addition and scalar multiplication is an R-module. It is called the *direct product* of $(M_i)_{i\in I}$.

The set

$$\bigoplus_{i\in I} M_i := \left\{ (x_i)_{i\in I} \in \bigtimes_{i\in I} M_i \,\middle|\, x_i = 0 \text{ for all but finitely many } i \in I \right\}$$

is a submodule of $\bigtimes_{i\in I} M_i$. It is referred to as the *direct sum* of $(M_i)_{i\in I}$. Note that the direct sum $\bigoplus_{i\in I} M_i$ equals the direct product $\bigtimes_{i\in I} M_i$ if and only if I is finite.

If M is an R-module and $I \neq \emptyset$ an index set, we may define $M_i := M$, $i \in I$. In this case, we set

$$\bigoplus_{i\in I} M := \bigoplus_{i\in I} M_i.$$

For convenience, we also define

$$\bigoplus_{i\in\emptyset} M := \{0\}.$$

Let M, N be R-modules, then

$$\operatorname{Hom}_R(M,N) := \{\, \varphi\colon M \longrightarrow N \,|\, \varphi \text{ is a homomorphism of } R\text{-modules} \,\}$$

together with the **addition**

$$\forall \varphi, \psi \in \operatorname{Hom}_R(M,N): \quad \varphi + \psi\colon M \longrightarrow N, \quad x \longmapsto \varphi(x) + \psi(x),$$

and the **scalar multiplication**

$$\forall a \in R \forall \varphi \in \operatorname{Hom}_R(M,N): \quad a \cdot \varphi\colon M \longrightarrow N, \quad x \longmapsto a \cdot \varphi(x),$$

is an R-module, too. The neutral element for the addition is the **zero homomorphism** $0\colon M \longrightarrow N$, $x \longmapsto 0$.

III.1.7 Exercises (The universal properties of the direct sum and the direct product). i) Let R be a ring, $(M_i)_{i\in I}$ a family of R-modules, and $\bigoplus_{i\in I} M_i$ its direct sum. Define, for $k \in I$,

$$\begin{array}{rcl} j_k\colon M_k & \longrightarrow & \displaystyle\bigoplus_{i\in I} M_i \\ m & \longmapsto & (m_i)_{i\in I} \text{ with } m_i = \begin{cases} m, & \text{if } i = k \\ 0, & \text{if } i \neq k \end{cases}. \end{array}$$

Prove that $\bigoplus_{i\in I} M_i$ has the following universal property: Given an R-module N and a collection of homomorphisms $f_k\colon M_k \longrightarrow N$, $k \in I$, there is a unique homomorphism $f\colon \bigoplus_{i\in I} M_i \longrightarrow N$ with $f \circ j_k = f_k$, $k \in I$. In other words,

$$\mathrm{Hom}_R\Big(\bigoplus_{i\in I} M_i, N\Big) \cong \bigtimes_{i\in I} \mathrm{Hom}_R(M_i, N).$$

ii) Let R be a ring, $(M_i)_{i\in I}$ a family of R-modules, and $\bigtimes_{i\in I} M_i$ its direct product. Define, for $k \in I$,

$$\begin{aligned} p_k\colon \bigtimes_{i\in I} M_i &\longrightarrow M_k \\ (m_i)_{i\in I} &\longmapsto m_k. \end{aligned}$$

Show that $\bigtimes_{i\in I} M_i$ has the following universal property: Given an R-module N and a collection of homomorphisms $f_k\colon N \longrightarrow M_k$, $k \in I$, there is a unique homomorphism $f\colon N \longrightarrow \bigtimes_{i\in I} M_i$ with $p_k \circ f = f_k$, $k \in I$. In other words,

$$\mathrm{Hom}_R\Big(N, \bigtimes_{i\in I} M_i\Big) \cong \bigtimes_{i\in I} \mathrm{Hom}_R(N, M_i).$$

Let R be a ring, M an R-module, and $S \subset M$ a **subset**. The *submodule generated by* S is

$$\langle S\rangle := \bigcap_{\substack{N\subset M \text{ submodule} \\ S\subset N}} N = \left\{ \sum_{i=1}^{n} a_i \cdot x_i \,\middle|\, n \geq 1, a_i \in R, x_i \in S, i = 1, ..., n \right\}.$$

We say that the R-module M is *finitely generated*, if the there is a **finite** subset $S \subset M$ with

$$M = \langle S\rangle.$$

An R-module M is *free*, if there are an index set I and an isomorphism

$$\varphi\colon \bigoplus_{i\in I} R \longrightarrow M.$$

If $I = \{1, ..., n\}$, we write

$$R^{\oplus n} := \bigoplus_{i=1}^{n} R.$$

III.1.8 Exercise (Finitely generated modules). Show that an R-module M is finitely generated if and only if there exist a natural number $n \in \mathbb{N}$ and a surjection

$$\varphi\colon R^{\oplus n} \longrightarrow M$$

of R-modules.

III.1.9 Exercise (The rank of a free module). Let R be a ring, $s, t \in \mathbb{N}$ natural numbers, and $\varphi\colon R^{\oplus s} \longrightarrow R^{\oplus t}$ a **surjective map**. Prove that $s \geq t$. In particular, $R^{\oplus s} \cong R^{\oplus t}$ if and only if $s = t$.

If M is an R-module and there are a **finite** index set I and an isomorphism $\varphi\colon \bigoplus_{i\in I} R \longrightarrow M$, we call the number $\#I$ the *rank* of M. By the last exercise, this is well-defined.

If k is a field, then every vector space has a basis[4] (see [33], §28) and, so, every k-module is free. Many concepts of linear algebra, such as the matrix formalism, may be extended to free modules. However, the condition of freeness is rather restrictive, in general. The following lemma gives a first illustration for this.

III.1.10 Lemma. *Let R be an integral domain and $I \subset R$ an ideal. Then, I is a free R-module if and only if it is a **principal ideal**.*

Proof. Let I be a principal ideal. If $I = \langle 0\rangle$, there is nothing to show. Otherwise, $I = \langle a\rangle$ with $a \neq 0$. Consider

$$\begin{array}{rccc} \varphi\colon & R & \longrightarrow & R \\ & r & \longmapsto & r\cdot a \end{array}$$

Since R is an integral domain, φ is injective. The image of φ is $\langle a\rangle$, so that $\langle a\rangle \cong R$ as R-module.

Assume I is a free R-module. If it is of rank 0 or 1, then I is a principal ideal. Otherwise, there is an injective homomorphism $\varphi\colon R^{\oplus 2} \longrightarrow I$. Set $f := \varphi(1,0)$ and $g := \varphi(0,1)$. The elements f and g are non-zero, because φ is injective. Observe

$$\varphi(g,-f) = g\cdot\varphi(1,0) - f\cdot\varphi(0,1) = g\cdot f - f\cdot g = 0.$$

Since $(g,-f) \neq 0$, this contradicts the injectivity of φ. □

Let M be an R-module. The *torsion submodule* of M is

$$\mathrm{Tors}(M) := \{\, x\in M \mid \exists \text{ non-zero divisor } a\in R : a\cdot x = 0\,\}.$$

If $\mathrm{Tors}(M) = \{0\}$, then M is said to be *torsion free*. If $M = \mathrm{Tors}(M)$, then M is said to be a *torsion module*.

III.1.11 Remark. Let us briefly verify that $\mathrm{Tors}(M)$ is indeed a submodule. Clearly, $0 \in \mathrm{Tors}(M)$. Let $x \in \mathrm{Tors}(M)$, $a \in R$, and $b \in R$ a non-zero divisor with $b\cdot x = 0$. Then, $b\cdot(a\cdot x) = a\cdot(b\cdot x) = a\cdot 0 = 0$, so that $a\cdot x \in \mathrm{Tors}(M)$. If $x, y \in \mathrm{Tors}(M)$ and $a, b \in R$ are non-zero divisors with $a\cdot x = 0$ and $b\cdot y = 0$. Then, $a\cdot b$ is not a zero divisor and

$$(a\cdot b)\cdot(x+y) = (a\cdot b)\cdot x + (a\cdot b)\cdot y = b\cdot(a\cdot x) + a\cdot(b\cdot y) = 0.$$

This illustrates the appearance of non-zero divisors in the definition of the torsion submodule.

III.1.12 Examples. i) A free R-module is torsion free.

ii) If k is a field, then every k-module is free and, in particular, torsion free.

iii) If A is an abelian group, i.e., a $\mathbb{Z}$-module (Example III.1.2, ii), then $x \in A$ lies in $\mathrm{Tors}(A)$ if and only it is an element of finite order.

iv) Let k be a field and (M, f) a $k[x]$-module (see Example III.1.2, iii). If M is a **finite dimensional** k-vector space, then (M, f) is a torsion module. In fact, since the

[4] if and only if the axiom of choice is admitted ([12], Theorem 4.44)

vector space $\mathrm{End}_k(M) = \mathrm{Hom}_k(M, M)$ is also finite dimensional, the powers f^k, $k \in \mathbb{N}$, are linearly dependent. So, there is a polynomial $p \in k[x]$ with $p(f) = 0$,[5] and, for every $x \in M$,

$$p \cdot x = p(f)(x) = 0.$$

Let M be an R-module and $x \in M$, then

$$\mathrm{Ann}(x) := \mathrm{Ann}_R(x) := \{\, a \in R \mid a \cdot x = 0 \,\}$$

is an ideal in R. It is the *annihilator* of x.

If $N \subset M$ is a submodule, we set

$$\mathrm{Ann}(N) := \mathrm{Ann}_R(N) := \{\, a \in R \mid \forall x \in N : a \cdot x = 0 \,\} = \bigcap_{x \in N} \mathrm{Ann}(x).$$

This is the *annihilator* of N.

III.1.13 Remark. Let M be an R-module. Note that M is in a natural way a module over the ring $R/\mathrm{Ann}(M)$.

Modules over Principal Ideal Domains

The main theorem on finite abelian groups (see [30], II.13.5) classifies all finitely generated $\mathbb{Z}$-modules. It generalizes to modules over a principal ideal domain R. We start with the following

III.1.14 Theorem. *Let R be a **principal ideal domain** and M a **finitely generated** R-module. Then,*

- ⋆ *$M/\mathrm{Tors}(M)$ is a free R-module.*
- ⋆ *The map*

$$\begin{aligned} \varphi\colon M/\mathrm{Tors}(M) \oplus \mathrm{Tors}(M) &\longrightarrow M \\ (x, y) &\longmapsto x + y \end{aligned}$$

is an isomorphism.

The rank of the free R-module $M/\mathrm{Tors}(M)$ is called the *rank* of M and is denoted by $\mathrm{rk}(M)$.

III.1.15 Remark. Let M, N be finitely generated R-modules and $\varphi\colon M \longrightarrow N$ a homomorphism. It induces a homomorphism

$$\overline{\varphi}\colon M/\mathrm{Tors}(M) \longrightarrow N/\mathrm{Tors}(N).$$

If φ is surjective, then so is $\overline{\varphi}$. In particular, $\mathrm{rk}(M) \geq \mathrm{rk}(N)$ in that case (see Exercise III.1.9).

We need several preparations to prove this result.

[5] The theorem of Cayley–Hamilton ([33], §36) asserts that we may take p to be the characteristic polynomial of f.

III.1.16 Proposition. *Let R be a **principal ideal domain**, $m \in \mathbb{N}$ a natural number, and M a free module of rank m. Then, every submodule N of M is free of rank n for some $n \in \{0, ..., m\}$.*

Proof. Without loss of generality, we may assume $M = R^{\oplus m}$. We set

$$M_k := \{(a_1, ..., a_k, 0, ..., 0) \in R^{\oplus m} \mid a_i \in R, i = 1, ..., k\}$$

and

$$N_k := N \cap M_k, \quad k = 1, ..., m.$$

We will prove inductively that N_k is a free module, $k = 1, ..., m$. Obviously, M_1 is isomorphic to R (as R-module). Thus, N_1 is isomorphic to a submodule of R, i.e., to an ideal of R (Example III.1.5). Lemma III.1.10 shows that N_1 is free of rank 0 or 1.

For $k \geq 2$, we set

$$I := \{b \in R \mid \exists b_1, ..., b_{k-1} \in R : (b_1, ..., b_{k-1}, b, 0, ..., 0) \in N_k\}.$$

This is an ideal in R. Pick an element $a \in R$ with $I = \langle a \rangle$ and elements $a_1, ..., a_{k-1} \in R$ with

$$x_0 := (a_1, ..., a_{k-1}, a, 0, ..., 0) \in N_k.$$

If $a = 0$, then $N_k = N_{k-1}$ and N_k is free by induction hypothesis. For the rest of the argument, we assume $a \neq 0$. For every element $x \in N_k$, there exists an element $r \in R$ with $x - r \cdot x_0 \in N_{k-1}$. This shows that the homomorphism

$$\begin{aligned} \varphi_k \colon N_{k-1} \oplus R &\longrightarrow N_k \\ (x, r) &\longmapsto x + r \cdot x_0 \end{aligned}$$

is surjective. It is also injective, because

$$N_{k-1} \cap \langle x_0 \rangle = \{0\}.$$

So, N_k is free of rank $\mathrm{rk}(N_{k-1}) + 1$. Note that the rank of N_k is at most k. □

III.1.17 Remark. The proposition is false, if R is not a principal ideal domain. In fact, R is a free module of rank 1. If R contains an ideal which is not principal, we may use the argument given in the proof of Lemma III.1.10. If R is not an integral domain, then we pick a non-trivial zero divisor b. Then,

$$\mathrm{Ann}(\langle b \rangle) = \mathrm{Ann}(b) \neq \{0\}.$$

But, for a non-zero free module, the annihilator is clearly $\{0\}$.

III.1.18 Corollary. *Let R be a principal ideal domain and M a finitely generated R-module. Then, every submodule N of M is finitely generated.*

Proof. The assumption means that there exist a natural number $m \in \mathbb{N}$ and a surjection

$$\varphi \colon R^{\oplus m} \longrightarrow M.$$

Now, $\varphi^{-1}(N)$ is a submodule of M and, therefore, free. Let $n \in \{1, ..., m\}$ be its rank and choose an isomorphism $\psi \colon R^{\oplus n} \longrightarrow \varphi^{-1}(N)$. Then,

$$R^{\oplus n} \xrightarrow{\psi} \varphi^{-1}(N) \xrightarrow{\varphi_{|\varphi^{-1}(N)}} N$$

is a surjection, and N is finitely generated. □

III.1.19 Remark. The corollary is true for every **noetherian** ring (see Proposition III.1.30 and Lemma III.1.29).

III.1.20 Proposition. *Let R be a **principal ideal domain** and M a finitely generated **torsion free** R-module. Then, M is free.*

Proof. We may clearly assume $M \neq \{0\}$. Let us start with a surjection (see Exercise III.1.8)

$$\varphi\colon R^{\oplus m} \longrightarrow M.$$

Let $e_i := (0, ..., 0, 1, 0, ..., 0)$, 1 being the i-th entry, and $x_i := \varphi(e_i)$, $i = 1, ..., m$. A subset $X \subset M$ is *linearly independent*, if

$$\lambda_1 \cdot x_1 + \cdots + \lambda_n \cdot x_n = 0 \quad \Longrightarrow \quad \lambda_1 = \cdots = \lambda_n = 0$$

holds for all $n \geq 1$, for all pairwise distinct $x_1, ..., x_n \in X$, and for all $\lambda_1, ..., \lambda_n \in R$. Note that, in a non-zero torsion free module, any set of cardinality 1 is linearly independent. Let $n \in \{1, ..., m\}$ be the maximal cardinality of a linearly independent subset of $\{x_1, ..., x_m\}$ and fix a linearly independent subset $\{x_{i_1}, ..., x_{i_n}\}$ of $\{x_1, ..., x_m\}$ with n elements. For $i = 1, ..., m$, there exist ring elements $a_i, a_{i1}, ..., a_{in} \in R$ with

$$a_i \cdot x_i + a_{i1} \cdot x_{i_1} + \cdots + a_{in} \cdot x_{i_n} = 0.$$

Note that $a_i \neq 0$, because $\{x_{i_1}, ..., x_{i_n}\}$ is linearly independent, $i = 1, ..., m$. So,

$$a := a_1 \cdot \cdots \cdot a_m \neq 0.$$

For $i = 1, ..., m$, we have

$$a \cdot x_i \in N := \langle x_{i_1}, ..., x_{i_n} \rangle$$

and, thus,

$$a \cdot M \subset N.$$

Note that N is a free module of rank n. By Proposition III.1.16, $a \cdot M$ is also free. Finally,

$$\begin{array}{rcl} \mu_a\colon M & \longrightarrow & M \\ x & \longmapsto & a \cdot x \end{array}$$

is injective, because $a \neq 0$ and M is torsion free. Since μ_a maps M onto $a \cdot M$, the module M is free. □

III.1.21 Proposition. *Let R be an **arbitrary ring**, M an R-module, N a **free** R-module, and $\varphi\colon M \longrightarrow N$ a surjection. Then, there exists a submodule $P \subset M$, such that*

- ⋆ *$\varphi_{|P}\colon P \longrightarrow N$ is an isomorphism,*
- ⋆ *the homomorphism*

$$\begin{array}{rcl} \psi\colon P \oplus \ker(\varphi) & \longrightarrow & N \\ (x, y) & \longmapsto & x + y \end{array}$$

is an isomorphism.

Proof. Let I be an index set, such that

$$N \cong \bigoplus_{i \in I} R.$$

Let $e_i = (e_{ij})_{j \in I}$ be the tuple with $e_{ii} = 1$ and $e_{ij} = 0$, $j \in I \setminus \{i\}$. We pick elements $x_i \in M$ with

$$\varphi(x_i) = e_i, \quad i \in I.$$

By the universal property of the direct sum (Exercise III.1.7, i), there is a unique homomorphism $\varrho\colon N \longrightarrow M$ that maps e_i to x_i, $i \in I$. We set

$$P := \operatorname{im}(\varrho).$$

Clearly, $\varphi \circ \varrho = \mathrm{id}_N$. In particular, ϱ is injective and, therefore, maps N isomorphically to P. It also follows that $\varphi_{|P}$ is inverse to ϱ.

For $x \in M$, we have

$$\varphi\big(x - (\varrho \circ \varphi)(x)\big) = \varphi(x) - (\varphi \circ \varrho)\big(\varphi(x)\big) = \varphi(x) - \varphi(x) = 0$$

and

$$x = \underbrace{(\varrho \circ \varphi)(x)}_{\in P} + \underbrace{\big(x - (\varrho \circ \varphi)(x)\big)}_{\in \ker(\varphi)}.$$

It follows that ψ is surjective. It is also injective, because $P \cap \ker(\varphi) = \{0\}$. □

Proof of Theorem III.1.14. We first show that $M/\mathrm{Tors}(M)$ is free. By Proposition III.1.14, it is enough to verify that this module is torsion free. Let $[x] \in M/\mathrm{Tors}(M)$ be a torsion element. There exists a non-zero divisor b with $[b \cdot x] = b \cdot [x] = 0$. This means $b \cdot x \in \mathrm{Tors}(M)$. So, there is a non-zero divisor $a \in R$ with

$$(a \cdot b) \cdot x = a \cdot (b \cdot x) = 0.$$

Since $a \cdot b$ is a non-zero divisor, $x \in \mathrm{Tors}(M)$ and $[x] = 0$. To conclude, we apply Proposition III.1.21 to the surjection $M \longrightarrow M/\mathrm{Tors}(M)$. □

Let R be a principal ideal domain. In order to understand all finitely generated modules over R, we need to understand the finitely generated torsion modules. This we will do now. Let $\mathbb{P} \subset R$ be a subset, such that for every prime element $q \in R$, there exists one and only one element $p \in \mathbb{P}$ with $q \sim p$, i.e., $\mathbb{P}$ is a set of representatives for the equivalence classes of prime elements in R with respect to the equivalence relation "being associated".

Let $M \neq \{0\}$ be a non-trivial torsion module over R. In this case, $\mathrm{Ann}(M)$ is a non-zero proper ideal of R. Pick a generator $a \in R \setminus (R^\star \cup \{0\})$ for $\mathrm{Ann}(M)$. The idea is to use the prime factorization of a to decompose M further.

For any ring element $b \in R$, let

$$\begin{array}{rccc} \mu_b\colon & M & \longrightarrow & M \\ & x & \longmapsto & b \cdot x \end{array}$$

and

$$M_b := \ker(\mu_b).$$

III.1.22 Proposition. *Let $c, d \in R$ be **coprime** elements and $b = c \cdot d$. Then,*

$$M_b \cong M_c \oplus M_d.$$

Proof. It is evident that $M_c \subset M_b$ and $M_d \subset M_c$. Note that $\langle c \rangle + \langle d \rangle = \langle 1 \rangle$. So, let $r, s \in R$ with

$$r \cdot c + s \cdot d = 1. \tag{III.3}$$

With this equation, we see that $M_c \cap M_d = \{0\}$.

Next, let $x \in M_b$. By (III.3), we have

$$x = 1 \cdot x = r \cdot (c \cdot x) + s \cdot (d \cdot x).$$

Now, $d \cdot x \in M_c$ and $c \cdot x \in M_d$. □

There are distinct elements $p_1, ..., p_s \in \mathbb{P}$ and positive integers $k_1, ..., k_s$ with

$$\langle a \rangle = \langle\, p_1^{k_1} \cdot \cdots \cdot p_s^{k_s} \,\rangle.$$

By Proposition III.1.22,

$$M \cong M_{p_1^{k_1}} \oplus \cdots \oplus M_{p_s^{k_s}}.$$

III.1.23 Proposition. *Suppose there are an element $p \in \mathbb{P}$ and a natural number $k \geq 1$ with*

$$M = M_{p^k}.$$

Then, there exist positive integers $l_1, ..., l_t$, such that

$$M \cong R/\langle p^{l_1} \rangle \oplus \cdots \oplus R/\langle p^{l_t} \rangle.$$

We need some preparations for the proof. Let M be any R-mdoule. We call elements $x_1, ..., x_u \in M$ *independent*, if

$$\forall \lambda_1, ..., \lambda_u \in R: \quad \lambda_1 \cdot x_1 + \cdots + \lambda_u \cdot x_u = 0 \quad \Longrightarrow \quad \lambda_1 \cdot x_1 = \cdots = \lambda_u \cdot x_u = 0.$$

This condition is weaker than linear independence. In fact, independent elements can exist in torsion modules whereas linearly independent elements can't.

In the set-up of Proposition III.1.23, M is said to be a *p-torsion module*. The number

$$e := \min\{\, k \in \mathbb{N} \mid M = M_{p^k} \,\}$$

is the *exponent* $\exp_p(M)$ of M. In the following, M is assumed to be a p-torsion module.

Let $x \in M \setminus \{0\}$. We call

$$s := \min\{\, t \in \mathbb{N} \mid p^t \cdot x = 0 \,\}$$

the *order* $\mathrm{ord}_p(x)$ of x. Clearly,

$$s \geq 1, \quad \mathrm{ord}_p(x) \leq \exp_p(M),$$

and there is an element $x_0 \in M$ for which equality is achieved.

III.1.24 Lemma. *In the above setting, let $b \in R$ be an element with $b \cdot x = 0$. Then,*

$$p^{\mathrm{ord}_p(x)} | b.$$

Proof. We may write $b = p^s \cdot m$ with p and m coprime. Assume $s < o := \mathrm{ord}_p(x)$. As in the proof of Proposition III.1.22, we find $r, s \in R$ with

$$1 = r \cdot p^{o-s} + s \cdot m.$$

Now,

$$x = r \cdot p^{o-s} \cdot x + s \cdot m \cdot x$$

has order at most s. This is a contradiction to the definition of the order. □

III.1.25 Lemma. *Let M be a p-torsion module of exponent e and $x_0 \in M$ an element of order e. Assume $y_1, ..., y_n \in M/\langle x_0 \rangle$ are non-zero independent elements. Then, there exist elements $x_1, ..., x_n \in M$, such that*

- ⋆ $[x_i] = y_i$, $i = 1, ..., n$,
- ⋆ $\mathrm{ord}_p(x_i) = \mathrm{ord}_p(y_i)$, $i = 1, ..., n$,
- ⋆ *$x_0, x_1, ..., x_n$ are independent.*

Proof. Let $y \in M/\langle x_0 \rangle$, $o := \mathrm{ord}_p(y)$, and $x' \in M$ an element with $[x'] = y$. Obviously,

$$\mathrm{ord}_p(x') \geq \mathrm{ord}_p(y).$$

There exist $0 \leq s \leq e$ and an element $m \in R$ which is coprime to m, such that

$$p^o \cdot x' = p^s \cdot m \cdot x_0.$$

If $s = e$, then $p^o \cdot x' = 0$, and $\mathrm{ord}_p(x') \leq \mathrm{ord}_p(y)$, so that finally $\mathrm{ord}_p(x') = \mathrm{ord}_p(y)$.

If $s < e$, then $p^s \cdot m \cdot x_0$ has order $e - s$, by Lemma III.1.24. This means that x' has order $o + e - s$. But, we also know

$$o + e - s \leq e, \quad \text{i.e.,} \quad o \leq s.$$

In this case,

$$x := x' - p^{s-o} \cdot m \cdot x_0$$

has order o and $[x] = y$.

These considerations show that we may find $x_1, ..., x_n \in M$, satisfying the first two properties. Finally, let $a_0, a_1, ..., a_n \in R$ with

$$a_0 \cdot x_0 + a_1 \cdot x_1 + \cdots + a_n \cdot x_n = 0.$$

Then,

$$a_1 \cdot y_1 + \cdots + a_n \cdot y_n = 0.$$

By assumption, $a_i \cdot y_i = 0$, $i = 1, ..., n$. According to Lemma III.1.24,

$$p^{\mathrm{ord}_p(y_i)} | a_i, \quad i = 1, ..., n.$$

But then

$$a_i \cdot x_i = 0, \quad i = 1, ..., n,$$

and also $a \cdot x_0 = 0$. □

From now on, we assume that M is **finitely generated**. Let $p \in \mathbb{P}$ and suppose M is a p-torsion module. By Corollary III.1.18, M_p is finitely generated. According to Remark III.1.13, M_p is a module over $R/\langle p\rangle$. The latter is a field. We shall denote it by $K(p)$. So, we may associate with M the number

$$\dim_{K(p)}(M_p) \in \mathbb{N}.$$

Proof of Proposition III.1.23. Let $x_0 \in M$ be an element of order r and $\overline{M} = M/\langle x_0\rangle$. We prove

$$\dim_{K(p)}(\overline{M}_p) < \dim_{K(p)}(M_p).$$

Note that elements $x_1, ..., x_n \in M_p$ or elements $y_1, ..., y_n \in \overline{M}_p$ are independent if and only if they are $K(p)$-linearly independent (Lemma III.1.24).

Let $y_1, ..., y_n \in \overline{M}_p$ form a $K(p)$-basis. By Lemma III.1.25, we can lift these elements to $K(p)$-linear independent elements $x_1, ..., x_n \in M_p$. The elements $x_0, x_1, ..., x_n \in M$ are independent. Then, $p^{r-1} \cdot x_0, x_1, ..., x_n$ are also independent. Observe that $p^{r-1} \cdot x_0 \in M_p$. We see

$$\dim_{K(p)}(M_p) \geq n + 1 = \dim_{K(p)}(\overline{M}_p) + 1.$$

We now prove the result by induction on $d := \dim_{K(p)}(M)$. If $d = 0$, we claim that $M = \{0\}$. Indeed, if $M \neq \{0\}$ and $x \in M \setminus \{0\}$, then $o := \mathrm{ord}_p(x) \geq 1$ and $p^{o-1} \cdot x$ is an element of order 1, i.e., a non-zero element in M_p.

Now, suppose the result holds for all natural numbers $< \dim_{K(p)}(M_p)$. Pick an element $x_0 \in M$ of order $e = \exp_0(M)$. Then,

$$\dim_{K(p)}\Big(\big(M/\langle x_0\rangle\big)_p\Big) < \dim_{K(p)}(M_p).$$

By induction hypothesis, $M/\langle x_0\rangle$ is generated by independent elements $y_1, ..., y_n$. We construct $x_1, ..., x_n \in M$ as in Lemma III.1.25. Then, $x_0, x_1, ..., x_n$ generate M and are independent. This means

$$M = \langle x_0\rangle \oplus \langle x_1\rangle \oplus \cdots \oplus \langle x_n\rangle.$$

Furthermore,

$$\langle x_i\rangle \cong R/\langle p^{\mathrm{ord}_p(x_i)}\rangle, \quad i = 0, 1, ..., n.$$

This finishes the proof. □

III.1.26 Theorem (Torsion modules over principal ideal domains)**.** *Let M be a finitely generated torsion module. Then, there are positive integers $s, t_1, ..., t_s$, s distinct prime elements $p_1, ..., p_s \in \mathbb{P}$, and positive integers $1 \leq k_{i1} \leq \cdots \leq k_{it_i}$, $i = 1, ..., s$, such that*

$$M \cong R/\langle p_1^{k_{11}}\rangle \oplus \cdots \oplus R/\langle p_1^{k_{1t_1}}\rangle \oplus \cdots \oplus R/\langle p_s^{k_{s1}}\rangle \oplus \cdots \oplus R/\langle p_s^{k_{st_s}}\rangle. \tag{III.4}$$

The integers $s, t_1, ..., t_s$, k_{ij}, $j = 1, ..., t_i$, $i = 1, ..., s$, and the prime elements[6] *$p_1, ..., p_s \in \mathbb{P}$ are uniquely determined by M.*

[6] They depend, of course, on the choice of $\mathbb{P}$.

Proof. The existence follows from the previous discussion. The uniqueness follows from a careful look at submodules of the form N_p where N is constructed in some way from M and $p \in \mathbb{P}$ is a prime element.

First, we observe

$$\{ p_1, ..., p_s \} = \{ p \in \mathbb{P} \mid M_p \neq \{0\} \}.$$

Hence, s and $p_1, ..., p_s$ are uniquely determined.

Next, we point out that

$$\big(\mathbb{Z}/\langle p^k \rangle\big)_p = \langle p^{k-1} \rangle / \langle p^k \rangle, \quad p \in \mathbb{P}, k \geq 1.$$

This shows

$$t_i = \dim_{K(p_i)}(M_{p_i}), \quad i = 1, ..., s.$$

Likewise one sees

$$\#\{ j \in \{1, ..., t_s\} \mid k_{ij} \geq l \} = \dim_{K(p_i)}\Big(\big(M/p_i^{l-1} \cdot M\big)_{p_i}\Big), \quad l \geq 1, i = 1, ..., s.$$

From these numbers, one may clearly determine $k_{11}, ..., k_{st_s}$. □

As an application of this result, let us derive the theorem on the Jordan normal form. Let $R = \mathbb{C}[x]$ and let (M, f) be a pair in which M is a finite dimensional complex vector space and $f\colon M \longrightarrow M$ is an endomorphism. By Example III.1.2, ii), and Exercise III.1.12, iv), this defines a torsion module over $\mathbb{C}[x]$.

We decompose it according to Theorem III.1.26. Since $\mathbb{C}$ is algebraically closed, a polynomial $p \in \mathbb{C}[x]$ is irreducible if and only if it is linear, i.e., of the form $c \cdot (x - \lambda)$, for some $c \in \mathbb{C}^\star$, $\lambda \in \mathbb{C}$. We need to understand the $\mathbb{C}[x]$-modules

$$M_{\lambda,k} = \mathbb{C}[x]/\big\langle (x - \lambda)^k \big\rangle, \quad \lambda \in \mathbb{C}, k \geq 1.$$

The elements

$$v_i := \big[(x - \lambda)^{k+1-i}\big], \quad i = 1, ..., k,$$

form a $\mathbb{C}$-basis for $M_{\lambda,k}$. Set $v_0 := 0$. We have, for $i = 1, ..., k$,

$$x \cdot v_i = \lambda \cdot v_i + (x-\lambda) \cdot v_i = \lambda \cdot v_i + (x-\lambda) \cdot \big[(x-\lambda)^{k+1-i}\big] = \lambda \cdot v_i + \big[(x-\lambda)^{k+1-(i-1)}\big] = \lambda \cdot v_i + v_{i-1}.$$

Thus, with respect to the ordered $\mathbb{C}$-basis $(v_1, ..., v_k)$ of $M_{\lambda,k}$, multiplication by x is described by the matrix

$$\begin{pmatrix} \lambda & 1 & 0 & \cdots & 0 \\ 0 & \lambda & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ \vdots & & \ddots & \lambda & 1 \\ 0 & \cdots & \cdots & 0 & \lambda \end{pmatrix}, \quad \lambda \in \mathbb{C}.$$

III.1.27 Theorem (Finitely generated modules over principal ideal domains)**.** *Let R be a principal ideal domain and M a finitely generated R-module. Then, there are a positive integer t and elements $a_1, ..., a_t \in R \setminus \{0\}$ with*

$$\langle a_1 \rangle \supset \cdots \supset \langle a_t \rangle$$

and

$$M \cong R^{\oplus \mathrm{rk}(M)} \oplus R/\langle a_1\rangle \oplus \cdots \oplus R/\langle a_t\rangle. \tag{III.5}$$

Moreover, if $a'_1, ..., a'_u$ are other elements with these properties, then $t = u$ and $a_i \sim a'_i$, $i = 1, ..., t$.

Proof. By Theorem III.1.14, it suffices to look at the case $\mathrm{rk}(M) = 0$, i.e., that M is a torsion module. We use Theorem III.1.26. Let $t := \max\{\, t_i \mid i = 1, ..., s \,\}$. Define

$$l_{i1} := \cdots := l_{i(t-t_i)} := 0 \quad \text{and} \quad l_{i(t-t_i+j)} := k_{ij}, \quad j = 1, ..., t_i, i = 1, ..., s,$$

and

$$a_\nu = p_1^{l_{1\nu}} \cdot \cdots \cdot p_s^{l_{s\nu}}, \quad \nu = 1, ..., t.$$

By the Chinese remainder theorem I.8.12, these elements clearly have the required properties.

Since we recover the decomposition (III.4) from (III.5), the asserted uniqueness follows from the corresponding statement in Theorem III.1.26. □

Note that this theorem includes the main theorem on finitely generated abelian groups ([30], Satz II.13.5).

Noetherian Modules

Let R be a ring and M an R-module. We say that M is *noetherian*, if every submodule N of M is finitely generated.

III.1.28 Remark. i) We may view R as an R-module (Example III.1.2, iv). Then, the submodules of R are the ideals of R (see Example III.1.5). So, R is noetherian as R-module if and only if R is noetherian as ring.

ii) If R is not noetherian, then there exist finitely generated R-modules which are not noetherian. In fact, R itself is such an example. It is free of rank 1 as R-module and contains an ideal I which is not finitely generated.

III.1.29 Lemma. *Let M be an R-module and $N \subset M$ a submodule. Then, M is noetherian if and only if N and M/N are noetherian.*

Proof. We will use the canonical surjection

$$\pi\colon M \longrightarrow M/N.$$

Assume first that M is noetherian. Every submodule of N is also a submodule of M. Therefore, N is also noetherian. The fact that any submodule of M/N is finitely generated is shown with an argument similar to the one in the proof Corollary III.1.18.

Next, assume that N and M/N are noetherian and P is a submodule of M. Let $x_1, ..., x_m \in P$ be generators of the module $N \cap P$, $y_1, ..., y_n \in M/N$ generators for $\pi(P) \subset M/N$, and $x_{m+i} \in P$ with $\pi(x_{m+i}) = y_i$, $i = 1, ..., n$. Then, one easily checks that $x_1, ..., x_{m+n}$ generate P. □

III.1.30 Proposition. *Let R be a **noetherian** ring, M a **finitely generated** R-module. Then, M is a noetherian R-module.*

Proof. There exist a natural number $m \geq 0$ and a surjection $\varphi\colon R^{\oplus m} \longrightarrow M$. By Lemma III.1.29, it suffices to show that $R^{\oplus m}$ is noetherian. This will be done by induction on m.

***m* = 1.** This was explained in Remark III.1.28.

***m* ⟶ *m* + 1.** Let

$$N := \{\, (0, ..., 0, r) \in R^{\oplus(n+1)} \mid r \in R \,\}.$$

This is a submodule of $R^{\oplus m}$. It is evidently isomorphic to R. The quotient $R^{\oplus(m+1)}/N$ is isomorphic to $R^{\oplus m}$. In fact,

$$\begin{array}{rcccc} \varphi\colon R^{\oplus m} & \longrightarrow & R^{\oplus(m+1)} & \longrightarrow & R^{\oplus(m+1)}/M \\ (a_1, ..., a_m) & \longmapsto & (a_1, ..., a_m, 0) & & \\ & & (a_1, ..., a_m, a_{m+1}) & \longmapsto & [a_1, ..., a_m, a_{m+1}] \end{array}$$

is an isomorphism. By the induction hypothesis, N and $R^{\oplus(m+1)}/N$ are noetherian. By Lemma III.1.29, $R^{\oplus(m+1)}$ is noetherian, too. □

III.1.31 The Nakayama[7] lemma. *Let R be a **local** ring with maximal ideal $\mathfrak{m}$. Let M be a **finitely generated** R-module, such that*

$$\mathfrak{m} \cdot M = M.$$

Then,

$$M = \{0\}.$$

Proof. Assume $M \neq \{0\}$ and let $m \geq 1$ be minimal, such that there is a surjection $\varphi\colon R^{\oplus m} \longrightarrow M$. Define e_i as in the proof of Proposition III.1.21 and set $x_i := \varphi(e_i)$, $i = 1, ..., m$. Since $\mathfrak{m} \cdot M = M$, there are elements $a_1, ..., a_t \in \mathfrak{m}$, such that

$$x_m = a_1 \cdot x_1 + \cdots + a_m \cdot x_m,$$

i.e.,

$$(1 - a_m) \cdot x_m = a_1 \cdot x_1 + \cdots + a_{m-1} \cdot x_{m-1}.$$

Since $a_m \in \mathfrak{m}$ and R is a local ring, $(1 - a_m)$ is a unit. This shows that x_m is a linear combination of $x_1, ..., x_{m-1}$, so that M is generated by $x_1, ..., x_{m-1}$. This contradicts the choice of m. □

We will discuss two applications of this result.

III.1.32 Krull's[8] intersection theorem. *Let R be a **noetherian** local ring with maximal ideal $\mathfrak{m}$. Then,*

$$I := \bigcap_{k \in \mathbb{N}} \mathfrak{m}^k = \{0\}.$$

Proof. The intersection I is an ideal. Set

$$\Sigma := \{\, J \subseteq R \mid J \text{ is an ideal with } J \cap I = \mathfrak{m} \cdot I \,\}.$$

Note that $\mathfrak{m} \cdot I \in \Sigma$, so that $\Sigma \neq \emptyset$. Let J_0 be a maximal element of Σ (see Theorem II.1.1). By definition, $\mathfrak{m} \cdot I \subset J_0$.

[7] Tadashi Nakayama (1912 - 1964), japanese mathematician.

[8] Wolfgang Krull (1899 - 1971), german mathematician.

Claim. *There is a natural number $k \in \mathbb{N}$, such that $\mathfrak{m}^k \subseteq J_0$.*

If the claim is correct, we have

$$I \subset \mathfrak{m}^k \subset J_0,$$

so that

$$I \subset J_0 \cap I = \mathfrak{m} \cdot I.$$

We see

$$I = \mathfrak{m} \cdot I.$$

Hence, $I = \{0\}$, by the Nakayama lemma III.1.31. ✓

Let us prove the claim. Since $\mathfrak{m}$ is finitely generated, it suffices to check:

$$\forall f \in \mathfrak{m} \exists l \geq 1 : \quad f^l \in J_0.$$

In fact, let $f_1, ..., f_n$ generate $\mathfrak{m}$ and assume $f_i^{l_i} \in J_0$, $i = 1, ..., n$. For $k \geq 1$, $\mathfrak{m}^k$ is generated by the monomials (compare Example I.8.8, ii)

$$f_1^{k_1} \cdot \cdots \cdot f_n^{k_n} \quad \text{with} \quad k_1 + \cdots + k_n = k. \tag{III.6}$$

If $k \geq l_1 + \cdots + l_n$, there is an index $i_0 \in \{1, ..., n\}$ with $k_{i_0} \geq l_{i_0}$, and then the monomial in (III.6) belongs to J_0.

Let $f \in \mathfrak{m}$ and look at the ascending chain

$$(J_0 : \langle f^k \rangle)_{k \in \mathbb{N}}.$$

There is an exponent $k_0 \geq 1$, such that

$$(J_0 : \langle f^{k_0} \rangle) = (J_0 : \langle f^{k_0+1} \rangle).$$

Choose $x \in (J_0 + \langle f^{k_0} \rangle) \cap I$. This means

$$\exists y \in J_0 \exists a \in R : \quad x = y + a \cdot f^{k_0}.$$

We see

$$f^{k_0+1} \cdot a = f \cdot x - f \cdot y \in \mathfrak{m} \cdot I + J_0 = J_0$$

and conclude $a \in (J_0 : \langle f^{k_0+1} \rangle) = (J_0 : \langle f^{k_0} \rangle)$. Consequently, $a \cdot f^{k_0} \in J_0$ and $x \in J_0$. This implies

$$(J_0 + \langle f^{k_0} \rangle) \cap I = J_0 \cap I = \mathfrak{m} \cdot I \quad \text{and} \quad (J_0 + \langle f^{k_0} \rangle) \in \Sigma.$$

Since J_0 is maximal in Σ and $J_0 \subset J_0 + \langle f^{k_0} \rangle$, we infer $J_0 = J_0 + \langle f^{k_0} \rangle$, that is $f^{k_0} \in J_0$. □

Let M and N be finitely generated R-modules and $\varphi \colon M \longrightarrow N$ a homomorphism of R-modules. We also have the natural quotient map

$$\pi \colon N \longrightarrow C := \operatorname{coker}(\varphi) = N/\operatorname{im}(\varphi).$$

Note that we get induced homomorphisms

$$\overline{\varphi} \colon \overline{M} := M/(\mathfrak{m} \cdot M) \longrightarrow \overline{N} := M/(\mathfrak{m} \cdot N)$$

and

$$\overline{\pi} \colon \overline{N} \longrightarrow \overline{C} := C/(\mathfrak{m} \cdot C).$$

III.1.33 Lemma. i) *We have* $\overline{C} \cong \operatorname{coker}(\overline{\varphi})$.

ii) *The homomorphism* φ *is surjective if and only if* $\overline{\varphi}$ *is surjective.*

Proof. ii) If φ is surjective, then $\overline{\varphi}$ is obviously surjective, too. If $\overline{\varphi}$ is surjective, then $\operatorname{coker}(\overline{\varphi}) = \{0\}$. By i), $\overline{C} = \{0\}$. The Nakayama lemma III.1.31 implies $C = \{0\}$, i.e., the surjectivity of φ.

i) We have to show that

$$\ker(\overline{\pi}) = \operatorname{im}(\overline{\varphi}).$$

The inclusion "$\supset$" is clear. For "$\subset$", let $y \in N$ be such that $\overline{\pi}([y]) = [\pi(y)] = 0$. So, there are an element $m \in \mathfrak{m}$ and an element $z \in N$ with $\pi(y) = m \cdot [z]$ in C. This, in turn, means that there is an element $u \in \operatorname{im}(\varphi)$ with

$$y = u + m \cdot z.$$

We see that, in $\overline{N}$, we have

$$[y] = [u],$$

and this element belongs to $\operatorname{im}(\overline{\varphi})$. □

III.1.34 Remark. The proof actually shows that the kernel of the induced surjection

$$N \longrightarrow \overline{C}$$

is

$$\operatorname{im}(\varphi) + \mathfrak{m} \cdot N.$$

III.1.35 Exercise. Let R be a local ring with maximal ideal $\mathfrak{m}$, M a finitely generated R-module, and $N \subset M$ a submodule. Prove that, if

$$M = \mathfrak{m} \cdot M + N,$$

then

$$M = N.$$

III.2 Finite Ring Extensions

Let R, S be rings and $\varphi\colon R \longrightarrow S$ a ring homomorphism. We say that φ is a *finite ring extension*, if φ is injective and S is finitely generated as an R-module.

III.2.1 Example. If K and L are **fields**, then a finite field extension $K \subset L$, i.e., $\dim_K(L) < \infty$, is an example for a finite ring extension.

For the following definitions, we assume that φ is **injective**. An element $s \in S$ is *integral over* R, if there are a positive integer $n > 0$ and elements $a_1, ..., a_n \in R$ with[9]

$$s^n + a_1 \cdot s^{n-1} + \cdots + a_{n-1} \cdot s + a_n = 0.$$

III.2.2 Example. Let $K \subset L$ a field extension. Then, $y \in L$ is integral over K if and only if it is algebraic over K (see [8], Satz III.1.6.2, i). If R and S aren't fields, it is important to keep in mind that the coefficient of the highest occurring power of s is 1.

[9] The symbol "$\cdot$" refers to the R-module structure of S (Example III.1.2, iv).

The ring R is *integrally closed in* S, if

$$\forall s \in S : \quad s \text{ is integral over } R \quad \Longleftrightarrow \quad s \in R.$$

We say that R is *integrally closed*, if R is integrally closed in its total ring of fractions (see Example II.3.5, ii). A ring R is *reduced*, if $\sqrt{\langle 0 \rangle} = \{0\}$, i.e., R does not contain non-trivial nilpotent elements. It is *normal*, if it is integrally closed and reduced.

III.2.3 Examples. i) We define

$$R := \mathbb{C}[x, y]/\langle x^2 - y^3 \rangle.$$

One readily checks that the polynomial $x^2 - y^3$ is irreducible, so that R is an integral domain.

We will show that R is not normal. For this, we look at the element

$$t := \frac{x}{y} \in Q(R)$$

in the quotient field of R. We have

$$t^2 = \frac{x^2}{y^2} = \frac{y^3}{y^2} = y \quad \text{and} \quad t^3 = t \cdot y = x.$$

In particular, t is integral over R, but is is not contained in R. This shows that R is not normal.

To conclude this example, let us compute the **normalization** of R, i.e., its integral closure in $Q(R)$. We look at

$$S := R[t] \subset Q(R).$$

We see that

$$S \cong \mathbb{C}[x, y, t]/\langle\, x^2 - y^3, t^2 - y, t^3 - x \,\rangle.$$

Moreover, one checks that

$$\begin{array}{rccc} \varphi\colon & \mathbb{C}[\vartheta] & \longrightarrow & S \\ & \vartheta & \longmapsto & t \end{array}$$

and

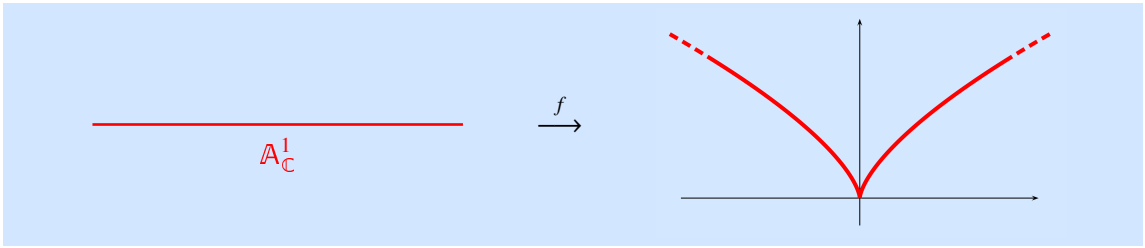
$$\begin{array}{rccc} \psi\colon & S & \longrightarrow & \mathbb{C}[\vartheta] \\ & t & \longmapsto & \vartheta \\ & x & \longmapsto & \vartheta^3 \\ & y & \longmapsto & \vartheta^2 \end{array}$$

are homomorphisms which are inverse to each other. It is easy to verify that the polynomial ring $\mathbb{C}[\vartheta]$ is a normal ring. Hence, so is S. The integral extension $\nu\colon R \subset S$ is, therefore, called the *normalization*. Using the isomorphism $S \cong \mathbb{C}[\vartheta]$ just described, it is given as

$$\begin{array}{rccc} \nu\colon & S & \longrightarrow & \mathbb{C}[\vartheta] \\ & x & \longmapsto & t^3 \\ & y & \longmapsto & t^2. \end{array}$$

Its geometric counterpart is the map

$$\begin{array}{rcl} f\colon \mathbb{A}^1_{\mathbb{C}} & \longrightarrow & V(x^2-y^3)\subset \mathbb{A}^2_k \\ t & \longmapsto & (t^3,t^2). \end{array}$$



ii) Set

$$R := \mathbb{C}[x,y]/\langle\, x\cdot y\,\rangle.$$

We write abusively x, y for $[x], [y] \in R$. Note that R is not an integral domain but reduced and that

$$\langle 0\rangle = \langle x\rangle \cap \langle y\rangle$$

is a minimal primary decomposition. By Theorem II.4.28, iii), we have

$$\{\text{ zero divisors of } R\,\} = \langle x\rangle \cup \langle y\rangle.$$

This shows that $x + y$ is not a zero divisor, so that we may form the non-zero element

$$u := \frac{x}{x+y} \in Q(R)$$

in the total ring of fractions of R. It is not contained in R, but satisfies the integrality condition

$$u^2 - u = \frac{x^2}{(x+y)^2} - \frac{x}{x+y} \overset{x\cdot y=0}{=} \frac{x\cdot(x+y)}{(x+y)^2} - \frac{x}{x+y} = \frac{x}{x+y} - \frac{x}{x+y} = 0.$$

This shows that R is not normal.

iii) Set $R := \mathbb{C}[x]/\langle x^2\rangle$. An element $a + b\cdot[x]$ is a unit if and only if $a \neq 0$, $a, b \in \mathbb{C}$. Otherwise, it is nilpotent. We see that $Q(R) = R$. The ring R is integrally closed, but not normal, because it is not reduced.

The notion of normality is an important concept in commutative algebra and algebraic geometry. The above examples already suggest that the notion of normality is related to **singularities**. We will study normal rings and normalizations in more detail in Section III.5 and IV.8.

Let $K \subset L$ be a field extension. If it is finite, then every element of L is algebraic over K. Conversely, if $\alpha \in L$ is algebraic over K, then the subfield $K(\alpha) \subset L$ it generates is a finite extension of K. The sum and product of algebraic elements are algebraic, and so on. The reader may consult, e.g., [8], Satz III.1.6.2, ii), for this. We will now prove similar results in the realm of commutative rings.

III.2.4 Proposition. *Let $\varphi\colon R \longrightarrow S$ be an **injective** ring homomorphism and $s \in S$. The following conditions are equivalent:*

i) *The element s is integral over R.*

ii) *The R-module $R[s] \subset S$ is finitely generated.*

iii) *There is a finitely generated R-module $T \subset S$ which contains $R[s]$.*

iv) *There exists an $R[s]$-module M, such that*

- ⋆ *M is finitely generated as R-module,*
- ⋆ $\mathrm{Ann}_{R[s]}(M) = \{\, y \in R[s] \,|\, y \cdot M = \{0\} \,\} = \{0\}$.

Proof. "i)⟹ii)". Let $n \geq 1$ and $a_1, ..., a_n \in R$, such that

$$s^n + a_1 \cdot s^{n-1} + \cdots + a_{n-1} \cdot s + a_n = 0.$$

Then, $R[s]$ is generated as an R-module by $1, s, ..., s^{n-1}$. In fact, set

$$p(x) := x^n + a_1 \cdot x^{n-1} + \cdots + a_{n-1} \cdot x + a_n \in R[x].$$

For $u \in R[s]$, there is a polynomial $g \in R[x]$ with $u = g(s)$. Since the leading coefficient of p is a unit in R, polynomial division is possible. This implies that there are polynomials $q, r \in R[x]$, such that

$$g = q \cdot p + r$$

and $\deg(r) < n$. Then,

$$u = g(s) = r(s) \in \langle\, 1, s, ..., s^{n-1} \,\rangle.$$

"ii)⟹iii)". We may take $T = R[s]$.

"iii)⟹iv)". Set $M := T$. For $y \in \mathrm{Ann}_{R[s]}(M) \subset S$, we have $y \cdot 1 = 0$ and, thus, $y = 0$.

"iv)⟹i)". Let M be generated as an R-module by the elements $x_1, ..., x_m$. There are elements $a_{ij} \in R$, $i, j = 1, ..., m$, such that

$$\forall i \in \{\, 1, ..., m \,\}: \quad s \cdot x_i = a_{i1} \cdot x_1 + \cdots + a_{im} \cdot x_m.$$

We form the $(m \times m)$-matrix

$$B := s \cdot \mathbb{E}_m - (a_{ij})_{i,j=1,...,m} \in \mathrm{Mat}_m(R[s])$$

with entries in the ring $R[s]$. By definition

$$B \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix} = 0. \tag{III.7}$$

We note that the theory of determinants works over every commutative ring. In particular, we have Cramer's rule[10] ([33], §27): For $i, j = \{\, 1, ..., m \,\}$, let $B_{ij} \in \mathrm{Mat}_{m-1}(R[s])$ be the matrix that is obtained from B by deleting the i-th column and the j-th row and $b_{ij} := (-1)^{i+j} \cdot \det(B_{ij})$. The matrix $B^{\mathrm{ad}} := (b_{ij})_{i,j=1,...,m}$ is the *adjoint matrix of B* and satisfies

$$B^{\mathrm{ad}} \cdot B = \det(B).$$

[10] Gabriel Cramer (1704 - 1752), swiss mathematician.

Multiplying Equation (III.7) by B^{ad} yields the conclusion

$$\forall i \in \{1, ..., m\}: \quad \det(B) \cdot x_i = 0, \quad \text{i.e.,} \quad \det(B) \in \mathrm{Ann}_{R[s]}(M).$$

By assumption, $\det(B) = 0$. Expanding the determinant of B provides us with an integrality equation for s. □

This proposition has several important consequences.

III.2.5 Corollary. *Let R, S be rings and $\varphi: R \longrightarrow S$ an injective ring homomorphism.*

i) *Suppose $n \geq 1$ and $s_1, ..., s_n \in S$ are integral over R. Then, the R-subalgebra $R[s_1, ..., s_n] \subset S$ is finitely generated as R-module.*

ii) *If $s, t \in S$ are integral over R, then so are $s + t$ and $s \cdot t$. In particular,*

$$T := \{ s \in S \mid s \text{ is integral over } R \}$$

is a subring of S.

The subring T in Part ii) of the corollary is called the *integral closure of R in S*. In the proof of the above corollary, we use the following

III.2.6 Lemma. *Suppose A, B, C are rings and $f: A \longrightarrow B$ and $g: B \longrightarrow C$ are homomorphisms. If B is finitely generated as A-module and C is finitely generated as B-module, then C is also finitely generated as A-module.*

Proof. Suppose $x_1, ..., x_m \in B$ generate B as A-module and that $y_1, ..., y_n \in C$ generate C as B-module. Using the B-module structure of C, we introduce the elements

$$x_i \cdot y_j, \quad i = 1, ..., m, j = 1, ..., n.$$

It is readily checked that these elements generate C as A-module. □

Proof of Corollary III.2.5. i) We prove this result by induction on n. The case $\boldsymbol{n = 1}$ is Part ii) of Proposition III.2.4, ii).

$\boldsymbol{n \longrightarrow n + 1}$**.** For the induction step, we write (compare (I.2))

$$R[s_1, ..., s_{n+1}] = R[s_1, ..., s_n][s_{n+1}].$$

By induction hypothesis, $R[s_1, ..., s_n]$ is finitely generated as R-module. Since s_{n+1} is integral over R, it is also integral over $R[s_1, ..., s_n]$. By Part ii) of Proposition III.2.4, $R[s_1, ..., s_n, s_{n+1}]$ is a finitely generated $R[s_1, ..., s_n]$-module. Lemma III.2.6 shows that $R[s_1, ..., s_n, s_{n+1}]$ is also finitely generated as R-module.

ii) By Part i), we know that the R-module $R[s, t] \subset S$ is finitely generated. Note $R[s + t] \subset R[s, t]$ and $R[s \cdot t] \subset R[s, t]$. Part iii) of Proposition III.2.4, iii), says that $s + t$ and $s \cdot t$ are integral over R. □

III.2.7 Corollary. *Let R, S, T be rings and $\varphi: R \longrightarrow S$ and $\psi: S \longrightarrow T$ **injective** ring homomorphisms. If S is integral over R and T is integral over S, then T is also integral over R.*

Proof. Let $t \in T$. There exist a natural number $n \geq 1$ and elements $b_1, ..., b_n \in S$ with

$$t^n + b_1 \cdot t^{n-1} + \cdots + b_{n-1} \cdot t + b_n = 0.$$

Set $S' := R[b_1, ..., b_n]$. The elements $b_1, ..., b_n$ are integral over R. By Corollary III.2.5, S' is a finitely generated R-module. The element t is integral over S'. So,

$$S'[t] = R[b_1, ..., b_n, t]$$

is a finitely generated S'-module. Lemma III.2.6 proves that $R[b_1, ..., b_n, t]$ is a finitely generated R-module. It contains $R[t]$. By Part iii) of Proposition III.2.4, t is integral over R. □

III.2.8 Corollary. *Let R, S be rings, $\varphi\colon R \longrightarrow S$ an **injective** homomorphism, and $T \subset S$ the integral closure of R in S. Then, T is integrally closed in S.*

III.2.9 Example. This corollary can be applied to the homomorphism $\varphi\colon R \longrightarrow Q(R)$. If T is the integral closure of R in $Q(R)$, then $Q(T) = Q(R)$ (Exercise III.2.11, ii). This means that T is an integrally closed ring.

III.2.10 Exercise (Integral ring extensions). Let R, S_1,...,S_n be rings and $f_i\colon R \longrightarrow S_i$, $i = 1, ..., n$, integral ring extensions. Show that

$$\begin{array}{rcl} f\colon R & \longrightarrow & \bigtimes_{i=1}^{n} S_i \\ x & \longmapsto & (f_1(x), ..., f_n(x)) \end{array}$$

is also an integral ring extension.

III.2.11 Exercises (Total rings of fractions and integral ring extensions). Let R be a ring and $Q(R)$ its total ring of fractions.

i) Show that the homomorphism

$$\begin{array}{rcl} \lambda_R\colon R & \longrightarrow & Q(R) \\ a & \longmapsto & \dfrac{a}{1} \end{array}$$

is injective.

ii) Let $S \subset Q(R)$ be a subring, containing $\lambda_R(R)$. Prove that

$$\begin{array}{rcl} \psi\colon Q(R) & \longrightarrow & Q(S) \\ \dfrac{a}{s} & \longmapsto & \dfrac{\lambda_R(a)}{\lambda_R(s)} \end{array}$$

is an isomorphism, so that, in particular, $Q(Q(R)) = Q(R)$.

iii) Give an example of rings R, S, an injective ring homomorphism $\varphi\colon R \longrightarrow S$, and an element $a \in R$, such that

- ⋆ $a \in R$ is not a zero divisor,
- ⋆ $\varphi(a) \in S$ is a zero divisor.

Conclude that there is no ring homomorphism $\psi\colon Q(R) \longrightarrow Q(S)$, such that the diagram

$$\begin{array}{ccc} R & \xrightarrow{\varphi} & S \\ {\scriptstyle \lambda_R}\downarrow & & \downarrow{\scriptstyle \lambda_S} \\ Q(R) & \xrightarrow{\psi} & Q(S) \end{array}$$

commutes.

iv) Let R be a ring and $S \subset Q(R)$ the integral closure of R in $Q(R)$. Demonstrate that S is an integrally closed ring with $Q(R) = Q(S)$.

III.2.12 Exercise (Normal rings). i) Let R be an integral domain and $S \subset R$ a multiplicatively closed subset. Note that one may interpret the localization R_S as a subring of the quotient field $Q(R)$. Using this interpretation, show that the following identity holds in $Q(R)$:

$$R = \bigcap_{\substack{\mathfrak{m}\subset R \\ \text{maximal ideal}}} R_{\mathfrak{m}}.$$

Hint. Let s be an element of the right hand intersection. Look at $\{\, r \in R \mid r \cdot s \in R \,\}$.

ii) Prove that an integral domain R is normal if and only if $R_{\mathfrak{m}}$ is normal for every maximal ideal $\mathfrak{m} \subset R$.

III.3 The Nullstellensatz

In this section, we will present a fairly elementary proof of Hilbert's Nullstellensatz, following Swan[11] [34]. It is due to Munshi [22]. The next section contains a more geometric proof, based on Noether's normalization theorem.

III.3.1 Nullstellensatz — Field theoretic version. *Let k be a field and R a finitely generated k-algebra. If R is a field, then $k \subset R$ is a finite field extension.*

III.3.2 Exercise (Maximal ideals). Suppose that k is an **algebraically closed** field and that $\mathfrak{m} \subset k[x_1, ..., x_n]$ is a maximal ideal. Prove that there exists a point $(a_1, ..., a_n) \in \mathbb{A}^n_k$ with

$$\mathfrak{m} = \langle\, x_1 - a_1, ..., x_n - a_n \,\rangle.$$

III.3.3 Weak Nullstellensatz. *Let k be an **algebraically closed** field, $n \geq 1$ a natural number, and $I \subsetneq k[x_1, ..., x_n]$ a proper ideal. Then,*

$$V(I) \neq \varnothing.$$

Proof. There is a maximal ideal $\mathfrak{m}$ with $I \subset \mathfrak{m}$ (Corollary I.4.8, i). By Exercise III.3.2, there is a point $(a_1, ..., a_n) \in \mathbb{A}^n_k$, such that

$$\mathfrak{m} = \langle\, x_1 - a_1, ..., x_n - a_n \,\rangle.$$

Then,

$$(a_1, ..., a_n) \in V(I).$$

This proves the claim. □

[11] Richard Gordon Swan (* 1933), US mathematician.

III.3.4 Strong Nullstellensatz. *Let k be an **algebraically closed** field, $n \geq 1$ a natural number, and $I \subset k[x_1, ..., x_n]$ an ideal. Then,*

$$I(V(I)) = \sqrt{I}.$$

Proof. We apply the **trick of Rabinovich**. Let $I = \langle f_1, ..., f_m \rangle \subset k[x_1, ..., x_n]$ and $f \in I(V(I)) \setminus \{0\}$. This means

$$\forall a = (a_1, ..., a_n) \in \mathbb{A}_k^n : \quad (\forall i \in \{1, ..., m\} : \ f_i(a) = 0) \quad \Longrightarrow \quad f(a) = 0.$$

We infer that the polynomials $f_1, ..., f_m, (1 - x_0 \cdot f) \in k[x_0, x_1, ..., x_n]$ do not have a common zero in $\mathbb{A}_k^{n+1}$. By the weak Nullstellensatz III.3.3, there exist polynomials $b_0, ..., b_m \in k[x_0, ..., x_m]$ with

$$b_0 \cdot (1 - x_0 \cdot f) + b_1 \cdot f_1 + \cdots + b_m \cdot f_m = 1. \tag{III.8}$$

Define

$$\begin{array}{rcl} \varphi \colon k[x_0, ..., x_m] & \longrightarrow & k[x_1, ..., x_n]_f \\ x_0 & \longmapsto & \dfrac{1}{f} \\ x_i & \longmapsto & x_i, \quad i = 1, ..., n. \end{array}$$

With $c_i := \varphi(b_i)$, $i = 1, ..., m$, Equation (III.8) yields

$$c_1 \cdot f_1 + \cdots + c_m \cdot f_m = 1. \tag{III.9}$$

By construction of the localization $R[x_1, ..., x_n]_f$, there exists a natural number $s \in \mathbb{N}$ with

$$d_i := f^s \cdot c_i \in R[x_1, ..., x_n], \quad i = 1, ..., m.$$

Multiplying Equation (III.9) by f^s gives

$$d_1 \cdot f_1 + \cdots + d_m \cdot f_m = f^s$$

and shows $f^s \in I$ and $f \in \sqrt{I}$. □

III.3.5 Corollary. *Let k be an **algebraically closed** field, $n \geq 1$ a natural number. Then, the maps Φ and Ψ defined on Page 43 are bijections which are inverse to each other.*

Next, we will prepare the proof of Theorem III.3.1.

III.3.6 Lemma. *Let R be an integral domain and $R[x]$ the polynomial ring in one variable over R. Then, there does not exist an element $f \in R[x]$, such that the localization $R[x]_f$ is a field.*

Proof. Assume to the contrary that $f \in R[x]$ is an element, such that $R[x]_f$ is a field. Obviously, we must have $\deg(f) \geq 1$. In particular, $1 + f \neq 0$. There are a polynomial $g \in R[x]$ and an exponent $k \in \mathbb{N}$, such that the equation

$$\frac{1}{1 + f} = \frac{g}{f^k}$$

holds in $R(x) := Q(R[x])$. It implies the equation

$$f^k = (1 + f) \cdot g \tag{III.10}$$

in $R[x]$. We pass to the ring $S := R[x]/\langle 1 + f\rangle$. Then, $[f] = -1$ in S and (III.10) gives $[f]^k = 0$. We find

$$(-1)^k = 0$$

in S. This means $S = \{0\}$ and $\langle 1 + f\rangle = R[x]$. So, $1 + f$ is a unit in $R[x]$. But this is impossible, because $\deg(1 + f) > 0$ (Exercise I.3.10). □

III.3.7 Lemma. *Let $\varphi\colon R \longrightarrow S$ be an **integral** ring extension. Then,*

$$R \cap S^\star = R^\star.$$

Proof. The inclusion "$\supset$" is obvious. For the converse inclusion, let $a \in R \cap S^\star$. Then, there is an element $b \in S$ with $a \cdot b = 1$. Since b is integral over R, there are a positive integer $n \geq 1$ and elements $a_1, ..., a_n \in R$ with

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

We multiply this by a^{n-1} and find

$$b = -a_1 - a_2 \cdot a - \cdots - a_{n-1} \cdot a^{n-2} - a_n \cdot a^{n-1}.$$

This shows $b \in R$ and $a \in R^\star$. □

III.3.8 Exercise. Let R and S be integral domains, $\varphi\colon R \longrightarrow S$ an integral ring extension, and $\mathfrak{n} \subset S$ be a maximal ideal and $\mathfrak{m} := \mathfrak{n} \cap R$. Show that $\mathfrak{m}$ is a maximal ideal in R.

III.3.9 Lemma. *Let $\varphi\colon R \longrightarrow S$ be an **integral** ring extension. If S is a field, then so is R.*

Proof. This is a direct consequence of Lemma III.3.7: $R \setminus \{0\} = R \cap (S \setminus \{0\}) = R \cap S^\star = R^\star$. □

The central ingredient in the proof of the Nullstellensatz is

III.3.10 Proposition. *Let R be an integral domain, $n \geq 1$ a positive integer, and $\mathfrak{m} \subset R[x_1, ..., x_n]$ a maximal ideal with*

$$\mathfrak{m} \cap R = \{0\}.$$

Then, there exists an element $a \in R$, such that

- ⋆ *R_a is a field,*
- ⋆ *$R_a \subset R[x_1, ..., x_n]/\mathfrak{m}$ is a finite field extension.*

Proof. We prove the result by induction on n.

$n = 1$. Let $f \in \mathfrak{m} \setminus \{0\}$ be a non-constant element and $l \geq 1$ be its degree. Write

$$f = a_0 \cdot x^l + a_1 \cdot x^{l-1} + \cdots + a_{l-1} \cdot x + a_l.$$

Since $R \cap \mathfrak{m} = 0$, by assumption, we have $a_0 \notin \mathfrak{m}$. Thus, we obtain the injective homomorphism (compare Exercise II.3.8)

$$\varphi \colon R_{a_0} \longrightarrow R[x]/\mathfrak{m} = R[\xi], \quad \xi := [x].$$

Observe that

$$g := \frac{1}{a_0} \cdot f = x^l + b_1 \cdot x^{l-1} + \cdots + b_{l-1} \cdot x + b_l, \quad b_i := \frac{a_i}{a_0}, \quad i = 1, ..., l,$$

is a polynomial in $R_{a_0}[x]$ with

$$g(\xi) = 0.$$

This shows that φ is an **integral** ring extension. By Lemma III.3.9, R_{a_0} is a field. Obviously, φ is a field extension of degree at most l.

$n \longrightarrow n + 1$. Set $S_i := R[x_i]$, $i = 1, ..., n + 1$. We apply the induction hypothesis to S_i and the polynomial ring

$$S_i[x_1, ..., x_{i-1}, x_{i+1}, ..., x_{n+1}], \quad i = 1, ..., n + 1.$$

We infer from Proposition III.3.10 that

$$S_i \cap \mathfrak{m} \neq \{0\}, \quad i = 1, ..., n + 1.$$

Pick non-zero elements

$$f_i \in S_i \cap \mathfrak{m}$$

and write

$$f_i = a_0^i \cdot x_i^l + a_1^i \cdot x_i^{l-1} + \cdots + a_{l-1}^i \cdot x_i + a_l^i, \quad i = 1, ..., n + 1.$$

As before, we may assume that $a_0^i \notin \mathfrak{m}$, $i = 1, ..., n + 1$, and

$$a := a_0^1 \cdot \cdots \cdot a_0^{l+1} \notin \mathfrak{m}.$$

We get the injective homomorphism

$$\varphi \colon R_a \longrightarrow R[x_1, ..., x_{n+1}]/\mathfrak{m} = R[\xi_1, ..., \xi_{n+1}], \quad \xi_i := [x_i], \quad i = 1, ..., n + 1.$$

Note that

$$\frac{1}{a_0^i} = \frac{a_0^1 \cdot \cdots \cdot a_0^{i-1} \cdot a_0^{i+1} \cdot \cdots \cdot a_i^{n+1}}{a} \in R_a, \quad i = 1, ..., n + 1,$$

so that we can form the polynomial

$$g_i := \frac{1}{a_0^i} \cdot f = x_i^l + b_1^i \cdot x_i^{l-1} + \cdots + b_{l-1}^i \cdot x_i + b_l^i, \quad b_j^i := \frac{b_j^i}{a_0^i}, \quad j = 1, ..., l,$$

in $R_a[x_i]$, $i = 1, ..., n$. We have

$$g_i(\xi_i) = 0, \quad i = 1, ..., n.$$

We see that φ is an **integral** ring extension. As before, we conclude that R_a is a field and φ is a finite field extension. □

Proof of Theorem III.3.1. We find a positive integer $n \geq 1$ and a surjection

$$\varphi\colon k[x_1, ..., x_n] \longrightarrow R.$$

Its kernel is a maximal ideal $\mathfrak{m} \subset k[x_1, ..., x_n]$. Since the elements of $k^\star$ are units in $k[x_1, ..., x_n]$, we have

$$k \cap \mathfrak{m} = \{0\}.$$

In Proposition III.3.10, we must have $R_a = k$, so that this proposition immediately yields the claim. □

III.3.11 Exercise (Study's lemma[12]). Deduce the following result from the Nullstellensatz: Let k be an algebraically closed field and $f, g \in k[x_1, ..., x_n]$ polynomials. Assume that f is **irreducible** and $V(f) \subset V(g)$. Show that f divides g in $k[x_1, ..., x_n]$.

III.4 Noether Normalization

Let k be an **infinite** field, e.g., an algebraically closed field. We first collect some elementary facts on the polynomial ring $k[x_1, ..., x_n]$.

III.4.1 Lemma. *Let $f \in k[x_1, ..., x_n] \setminus \{0\}$ be a non-zero polynomial. Then, there exists a point $(a_1, ..., a_n) \in \mathbb{A}^n_k$ with*

$$f(a_1, ..., a_n) \neq 0.$$

Proof. We prove this result by induction on n. For $\boldsymbol{n = 1}$, observe that a polynomial $f \in k[x_1]$ has at most $\deg(f)$ zeroes and k is infinite.

$\boldsymbol{n \longrightarrow n + 1}$**.** For the induction step, set $S := k[x_1, ..., x_n]$ and let $f \in S[x_{n+1}]$ be a non-trivial polynomial and $d \in \mathbb{N}$ its degree. There are polynomials $g_0, ..., g_d \in S$ with $g_d \neq 0$, such that

$$f = g_d \cdot x_{n+1}^d + \cdots + g_1 \cdot x_{n+1} + g_0.$$

By the induction hypothesis, there is a point $(a_1, ..., a_n) \in \mathbb{A}^n_k$ with $g_d(a_1, ..., a_n) \neq 0$. Then,

$$f(a_1, ..., a_n, x_{n+1}) = g_d(a_1, ..., a_n) \cdot x_{n+1}^d + \cdots + g_1(a_1, ..., a_n) \cdot x_{n+1} + g_0(a_1, ..., a_n)$$

is a non-trivial polynomial in $k[x_{n+1}]$. There exists an element $a \in k$ with

$$f(a_1, ..., a_n, a) \neq 0,$$

and this finishes the proof. □

III.4.2 Exercises (Dominant regular maps). Let k be an algebraically closed field. An *affine algebraic variety* is an **irreducible** algebraic set $X \subset \mathbb{A}^n_k$. Recall that an algebraic set $Z \subset \mathbb{A}^n_k$ is irreducible if and only if its coordinate algebra

$$k[Z] := k[x_1, ..., x_n]/I(Z)$$

is an integral domain. A regular map (see Exercise I.9.8) $f\colon X \longrightarrow Y$ between algebraic varieties is *dominant*, if $f(X)$ is dense in Y.

[12] Christian Hugo Eduard Study (1862 - 1930), German mathematician.

i) Let $F\colon X \longrightarrow Y$ be a regular map between algebraic varieties and $F^\star\colon k[Y] \longrightarrow k[X]$ the corresponding homomorphism of algebras. Show that F is dominant if and only if $F^\star$ is injective.

ii) Let X be an algebraic variety. The *function field* of X is the quotient field

$$k(X) := Q(k[X])$$

of the coordinate algebra $k[X]$ of X. Show that a dominant morphism $F\colon X \longrightarrow Y$ induces a field extension $F^\#\colon k(Y) \longrightarrow k(X)$, such that the diagram

$$\begin{array}{ccc} k[Y] & \xrightarrow{F^\star} & k[X] \\ \big\downarrow & & \big\downarrow \\ k(Y) & \xrightarrow{F^\#} & k(X) \end{array}$$

commutes.

An element $m \in k[x_1, ..., x_n]$ is a *monomial*, if there are natural numbers $k_1, ..., k_n \in \mathbb{N}$ with

$$m = x_1^{k_1} \cdot \cdots \cdot x_n^{k_n}.$$

The number

$$\deg(m) = k_1 + \cdots + k_n$$

is the *degree* of m. The set of monomials is a k-basis for $k[x_1, ..., x_n]$. Let $d \geq 1$ be a natural number. A polynomial $f \in k[x_1, ..., x_n]$ is *homogeneous of degree d*, if it is a linear combination of monomials of degree d.

III.4.3 Remark. Lemma III.4.1 shows that a polynomial $f \in k[x_1, ..., x_n]$ is homogeneous of degree d if and only if

$$\forall (a_1, ..., a_n) \in \mathbb{A}_k^n \forall \lambda \in k: \quad f(\lambda \cdot a_1, ..., \lambda \cdot a_n) = \lambda^d \cdot f(a_1, ..., a_n).$$

The *degree* of a not necessarily homogeneous non-zero polynomial $f \in k[x_1, ..., x_n] \setminus \{0\}$ is the maximal degree of a monomial occuring with non-zero coefficient in f.

III.4.4 Noether normalization for hypersurfaces. *Let $d \geq 1$ be a natural number and $f \in k[x_1, ..., x_n]$ a polynomial of degree d. Then, there are linear polynomials $y_1, ..., y_n \in k[x_1, ..., x_n]$, polynomials $g_1, ..., g_d \in k[x_1, ..., x_{n-1}]$, and a non-zero constant $c \in k^\star$, such that*

$$\begin{array}{rccl} \varphi\colon k[x_1, ..., x_n] & \longrightarrow & k[x_1, ..., x_n] \\ x_i & \longmapsto & y_i, \quad i = 1, ..., n, \end{array}$$

is an isomorphism and

$$\varphi(f) = f(y_1, ..., y_n) = c \cdot (x_n^d + g_1 \cdot x_n^{d-1} + \cdots + g_{d-1} \cdot x_n + g_d). \tag{III.11}$$

Proof. There are uniquely determined **homogeneous** polynomials $f_0, ..., f_d \in k[x_1, ..., x_n]$ with

$\star$ $\deg(f_i) = i$, $i = 0, ..., d$,

- ⋆ $f = f_d + f_{d-1} + \cdots + f_1 + f_0$,
- ⋆ $f_d \neq 0$.

By Lemma III.4.1, there is an element $(b_1, ..., b_n) \in \mathbb{A}_k^n$ with $c := f_d(b_1, ..., b_n) \neq 0$. Note that $(b_1, ..., b_n) \neq 0$, because $d \geq 1$ and f_d is homogeneous of degree d, so that $f_d(0, ..., 0) = 0$. After renumbering, we may assume $b_n \neq 0$. Set

$$\begin{aligned} y_n &:= b_n \cdot x_n, \\ y_i &:= b_i \cdot x_n + x_i, \quad i = 1, ..., n-1. \end{aligned}$$

We leave it to the reader to check that the homomorphism $\varphi\colon k[x_1, .., x_n] \longrightarrow k[x_1, ..., x_n]$, $x_i \longmapsto y_i$, $i = 1, ..., n$, is an isomorphism. Let $h := \varphi(f)$. We compute (compare Remark III.4.3)

$$h(0, ..., 0, x_n) = f_d(b_1, ..., b_n) \cdot x_n^d + f_{d-1}(b_1, .., b_n) \cdot x_n^{d-1} + \cdots + f_1(b_1, ..., b_n) \cdot x_n + f_0(b_1, ..., b_n).$$

This implies that there are polynomials $g_1, ..., g_d \in k[x_1, ..., x_{n-1}]$, such that Equation (III.11) holds. □

III.4.5 Remarks. i) Let f be a polynomial as in (III.11). Then,

$$k[x_1, ..., x_n]/\langle f \rangle$$

is a finitely generated $k[x_1, ..., x_{n-1}]$-module. Indeed, it is generated by 1, $[x_n]$, ..., $[x_n^{d-1}]$ (see the proof of Proposition III.2.4).

ii) Assume that k is algebraically closed. There is a geometric interpretation of the lemma. We let f be a polynomial as in (III.11) and look at the projection

$$\begin{aligned} \pi\colon \mathbb{A}_k^n &\longrightarrow \mathbb{A}_k^{n-1} \\ (a_1, ..., a_n) &\longmapsto (a_1, ..., a_{n-1}) \end{aligned}$$

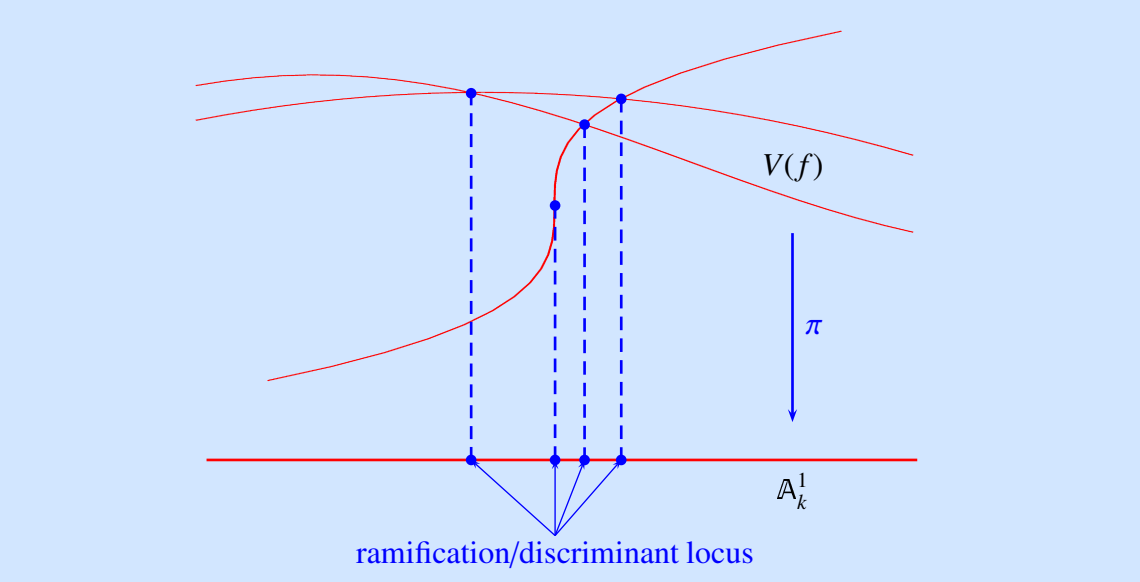
and its restriction

$$\widetilde{\pi} := \pi_{|V(f)}\colon V(f) \longrightarrow \mathbb{A}_k^{n-1}$$

to the zero set of f. Then,

- ⋆ $\widetilde{\pi}$ is surjective,
- ⋆ any fiber of $\widetilde{\pi}$ consists of at most d points, or exactly d points when counted with multiplicity.

This means that the hypersurface $V(f) \subset \mathbb{A}_k^n$ may be presented as a **ramified** covering of degree d of affine $(n-1)$-space $\mathbb{A}_k^{n-1}$. This suggests also that the dimension of $V(f)$ is $n-1$. We will develop this in Chapter IV.



III.4.6 The projection theorem. *Let k be an **algebraically closed** field, $I \subset k[x_1, .., x_n]$ an ideal, and $f_0 \in I$ an element for which there exist a natural number $d \geq 1$ and elements $g_1, ..., g_d \in k[x_1, ..., x_{n-1}]$, such that*

$$f_0 = x_n^d + g_1 \cdot x_n^{d-1} + \cdots + g_{d-1} \cdot x_n + g_d.$$

Set

- ⋆ $X := V(I) \subset \mathbb{A}^n_k$,
- ⋆ $I' := I \cap k[x_1, ..., x_{n-1}]$,
- ⋆ $X' := V(I') \subset \mathbb{A}^{n-1}_k$.

Then, the projection

$$\begin{array}{rcl} \pi\colon \mathbb{A}^n_k & \longrightarrow & \mathbb{A}^{n-1}_k \\ (a_1, ..., a_n) & \longmapsto & (a_1, ..., a_{n-1}) \end{array}$$

satisfies

$$\pi(X) = X'.$$

Proof. "$\subset$". Let $a = (a_1, ..., a_{n-1}) \in \pi(X)$. There, there exists an element $b \in k$ with

$$(a, b) = (a_1, ..., a_{n-1}, b) \in X.$$

For $f \in I' \subset I$, we have $f(a, b) = 0$. Since $f \in k[x_1, ..., x_{n-1}]$, this means $f(a) = 0$. We conclude $a \in V(I')$.

"$\supset$". Suppose $a = (a_1, ..., a_{n-1}) \notin \pi(X)$. We will construct an element $g \in I'$ with $g(a) \neq 0$, so that $a \notin X'$.

Claim. *Let $f \in k[x_1, ..., x_n]$. Then, there exist an element $h_f \in I$ and polynomials $p_0, ..., p_{d-1} \in k[x_1, ..., x_{n-1}]$ with $p_i(a) = 0$, $i = 0, ..., d-1$, such that*

$$f = p_0 + p_1 \cdot x_n + \cdots + p_{d-1} \cdot x_n^{d-1} + h_f.$$

We look at the homomorphism

$$\begin{aligned} \varphi\colon k[x_1,...,x_n] &\longrightarrow k[x_n] \\ x_i &\longmapsto a_i, \quad i = 1,...,n-1, \\ x_n &\longmapsto x_n, \end{aligned}$$

i.e.,

$$\varphi(f) = f(a, x_n).$$

Since φ is surjective, the image $\varphi(I)$ of I is an ideal. Note:

$$\exists b \in k:\ b \in V(\varphi(I)) \iff \exists b \in k \forall f \in I:\ f(a,b) = 0 \iff a \in \pi(X).$$

Since we assumed $a \notin \pi(X)$, we see $V(\varphi(I)) = \varnothing$. By the "Nullstellensatz in one variable", i.e., the definition of an algebraically closed field, $\varphi(I) = k[x_n]$. So, there exists an element $h'_f \in I$ with

$$\varphi(h'_f) = \varphi(f).$$

We set

$$g_f := f - h'_f.$$

We perform polynomial division by f_0 (in $k[x_1,...,x_{n-1}][x_n]$). There are a polynomial $q \in k[x_1,...,x_n]$ and polynomials $p_0,...,p_{d-1} \in k[x_1,...,x_{n-1}]$, such that

$$g_f = q \cdot f_0 + \sum_{i=0}^{d-1} p_i \cdot x_n^i.$$

We look at the equation

$$0 = g_f(a, x_n) = q(a, x_n) \cdot f_0(a, x_n) + \sum_{i=0}^{d-1} p_i(a) \cdot x_n^i.$$

Now, $\deg(f_0(a, x_n)) = d$. This implies $q(a, x_n) = 0$ and $p_i(a) = 0$, $i = 0,...,d-1$. With

$$h_f := h'_f + q \cdot f_0 \in I,$$

we find

$$f = h_f + \sum_{i=0}^{d-1} p_i \cdot x_n^i$$

as asserted. ✓

Using this claim, we find polynomials $p_{ij} \in k[x_1,...,x_{n-1}]$ with $p_{ij}(a) = 0$, $i,j = 0,...,d-1$, and $h_i \in I$, $i = 0,...,d-1$, with

$$\begin{aligned} 1 &= p_{0,0} + p_{0,1} \cdot x_n + \cdots + p_{0,d-1} \cdot x_n^{d-1} + h_0 \\ x_n &= p_{1,0} + p_{1,1} \cdot x_n + \cdots + p_{1,d-1} \cdot x_n^{d-1} + h_1 \\ &\vdots \\ x_n^{d-1} &= p_{d-1,0} + p_{d-1,1} \cdot x_n + \cdots + p_{d-1,d-1} \cdot x_n^{d-1} + h_{d-1}. \end{aligned}$$

Define

$$A := \mathbb{E}_d - (p_{ij})_{i,j=0,...,d-1} \in \mathrm{Mat}_d(k[x_1, ..., x_{n-1}]).$$

The above system of equations can be rewritten as

$$A \cdot \begin{pmatrix} 1 \\ \vdots \\ x_n^{d-1} \end{pmatrix} = \begin{pmatrix} h_0 \\ \vdots \\ h_{d-1} \end{pmatrix}.$$

Multiplying by the adjoint matrix (compare Page 94) A^{ad}, we infer

$$\det(A) \cdot \begin{pmatrix} 1 \\ \vdots \\ x_n^{d-1} \end{pmatrix} = \begin{pmatrix} h'_0 \\ \vdots \\ h'_{d-1} \end{pmatrix}, \tag{III.12}$$

for appropriate polynomials $h'_0, ..., h'_n \in I$. We would like to show that $g := \det(A) \in k[x_1, ..., x_{n-1}]$ is the polynomial we are looking for. The first row in (III.12) shows $g \in I$ and, consequently, $g \in I'$. Finally, $p_{ij}(a) = 0$, $i, j = 0, ..., d-1$. This gives $g(a) = 1$. □

We pause a minute to give an alternative proof of the weak Nullstellensatz III.3.3.

Proof of Theorem III.3.3. We perform induction on n. For $n = 0, 1$, the theorem is true. Since an algebraically closed field is infinite, we can apply Noether normalization for hypersurfaces III.4.4 and assume without loss of generality that I contains an element f_0 as in the projection theorem. If $I \subset k[x_1, ..., x_n]$ is a proper ideal, so is $I' \subset k[x_1, ..., x_{n-1}]$. By induction hypothesis, $V(I') \neq \emptyset$. Since

$$\pi(V(I)) = V(I'),$$

we also have $V(I) \neq \emptyset$. □

III.4.7 Noether's normalization theorem. *Let k be an **infinite** field and $I \subset k[x_1, ..., x_n]$ a proper ideal. Then, there are linear polynomials $z_1, ..., z_n \in k[x_1, ..., x_n]$ and a natural number $r \leq n$, such that*

$$\begin{aligned} \psi\colon k[x_1, ..., x_n] &\longrightarrow k[x_1, ..., x_n] \\ x_i &\longmapsto z_i, \quad i = 1, ..., n, \end{aligned}$$

is an isomorphism,

$$\begin{aligned} k[x_1, ..., x_r] &\longrightarrow k[x_1, ..., x_n]/\psi(I) \\ x_i &\longmapsto [x_i], \quad i = 1, ..., r, \end{aligned}$$

is a finite ring extension. If $I \neq \langle 0 \rangle$, then $r < n$.

Proof. We perform induction on n. Note that the case $I = \langle 0 \rangle$ is trivial.

$\boldsymbol{n = 1}$. Let $f \in k[x] \setminus \{0\}$ be a polynomial with $I = \langle f \rangle$. Then, $k[x]/I$ is a finite dimensional k-vector space of dimension at most $\deg(f)$ (compare Remark III.4.5, i).

$\boldsymbol{n \longrightarrow n+1}$. Again, we may assume $I \neq \langle 0 \rangle$. We let $y_1, ..., y_n$ and φ be as in Theorem III.4.4, i.e., such that $\varphi(I)$ contains an element f_0 of the form given in (III.11). As was

explained in Remark III.4.5, i), $k[x_1, ..., x_n]/\langle f_0\rangle$ is a finite module over $k[x_1, ..., x_{n-1}]$. Set $J := \varphi(I)$ and

$$J' := J \cap k[x_1, ..., x_{n-1}].$$

Since $f_0 \in \varphi(I)$, we have the commutative diagram

$$\begin{array}{ccc} k[x_1, ..., x_{n-1}] & \longrightarrow & k[x_1, ..., x_n]/\langle f_0\rangle \\ \downarrow & & \downarrow \\ k[x_1, ..., x_{n-1}]/J' & \longrightarrow & k[x_1, ..., x_n]/J \end{array}$$

in which the vertical maps are surjective and the horizontal ones injective. So, the ring $k[x_1, ..., x_n]/J$ is a finite module over $k[x_1, ..., x_{n-1}]/J'$. Now, we apply the induction hypothesis to $J' \subset k[x_1, ..., x_{n-1}]$. (The reader should pay attention how to combine the choice of $y_1, ..., y_n$ and the choice of elements in $k[x_1, ..., x_{n-1}]$ hidden in the application of the induction hypotheses to J' to a single choice of elements $z_1, ..., z_n \in k[x_1, ..., x_n]$.) □

III.4.8 Lemma. *Assume that k is **algebraically closed**, and let $I \subset k[x_1, ..., x_n]$ be an ideal and $r \leq n$ an integer, such that*

$$k[x_1, ..., x_r] \longrightarrow k[x_1, ..., x_n]/I$$

is injective and $k[x_1, ..., x_n]/I$ is a finite $k[x_1, ..., x_r]$-module. Then, the restriction

$$\widetilde{\pi} := \pi_{|V(I)} \colon V(I) \longrightarrow \mathbb{A}^r_k$$

of the projection

$$\begin{array}{rcl} \pi \colon \mathbb{A}^n_k & \longrightarrow & \mathbb{A}^r_k \\ (a_1, ..., a_n) & \longmapsto & (a_1, ..., a_r) \end{array}$$

to the algebraic set $V(I)$ is surjective.

Proof. Set $s_i := [x_i] \in k[x_1, ..., x_n]/I$, $i = r+1, ..., n$. Since s_i is integral over $S := k[x_1, ..., x_r]$, there are a positive integer $d_i \in \mathbb{Z}$ and a polynomial

$$f_i(x_i) = x_i^{d_i} + g_1 \cdot x_i^{d_i-1} + \cdots + g_{d_i-1} \cdot x_i + g_{d_i} \in S[x_i] \tag{III.13}$$

with

$$f_i(s_i) = 0,$$

i.e.,

$$f_i \in I \cap k[x_1, ..., x_i], \quad i = r+1, ..., n.$$

Define, for $i = r+1, ..., n$,

$$J_i := I \cap k[x_1, ..., x_i]$$

and

$$\begin{array}{rcl} \pi_i \colon \mathbb{A}^i_k & \longrightarrow & \mathbb{A}^{i-1}_k \\ (a_1, ..., a_i) & \longmapsto & (a_1, ..., a_{i-1}). \end{array}$$

Due to (III.13), the projection theorem III.4.6 implies that π_i maps $V(J_i)$ surjectively onto $V(J_{i-1})$, $i = r+2, ..., n$, and $V(J_{r+1})$ surjectively onto $\mathbb{A}^r_k$. Since

$$\pi = \pi_{r+1} \circ \cdots \circ \pi_n,$$

this gives the assertion. We will see in Remark IV.2.5, ii), a more conceptual proof of this statement. □

III.4.9 Exercises (Noether normalization). We study the map

$$\begin{array}{rccc} \nu\colon & \mathbb{C} & \longrightarrow & \mathbb{C}^3 \\ & t & \longmapsto & (t^3, t^4, t^5). \end{array}$$

i) Show that the image of ν is the set $V(\mathfrak{a})$ with

$$\mathfrak{a} := \langle\, z_2^2 - z_1 \cdot z_3, z_1^3 - z_2 \cdot z_3, z_3^2 - z_1^2 \cdot z_2 \,\rangle.$$

ii) Prove that the projection $\pi\colon \mathbb{C}^3 \longrightarrow \mathbb{C}$, $(z_1, z_2, z_3) \longmapsto z_1$, gives a Noether normalization of $V(\mathfrak{a})$, such that $\overline{z}_2$ is a primitive element for the corresponding field extension. Determine the discriminant locus.

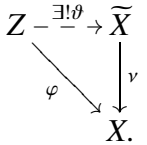
III.4.10 Exercise (Noether normalization). Let S be an integral domain and $R \subset S$ a subring, such that S is finitely generated as R-algebra. Prove that there are a non-zero element $f \in R \setminus \{0\}$, a natural number n, and elements $y_1, ..., y_n \in S$, such that

- ⋆ $y_1, ..., y_n$ are algebraically independent over R,[13]
- ⋆ the induced homomorphism $\varphi\colon R_f[y_1, ..., y_n] \longrightarrow S_f$ is an integral ring extension.

III.4.11 Exercise (Universal property of normalization). An affine algebraic variety X is said to be *normal*, if its coordinate algebra $k[X]$ is normal (compare Exercise III.4.2). Let k be an algebraically closed field and X an affine algebraic variety over k. Show that there are a **normal** affine algebraic variety $\widetilde{X}$ and a **dominant** regular map

$$\nu\colon \widetilde{X} \longrightarrow X$$

which are **universal**, i.e., for every normal algebraic variety Z and every dominant regular map $\varphi\colon Z \longrightarrow X$, there is a unique regular map $\vartheta\colon Z \longrightarrow \widetilde{X}$ with $\varphi = \nu \circ \vartheta$:



The pair $(\widetilde{X}, \nu)$ is the *normalization* of X.

[13] See Page 8 for the definition of algebraically independent elements.

III.5 Normal Rings

III.5.1 Lemma. *Let R be a **factorial** ring.*[14] *Then, R is a normal ring.*

Proof. Recall that a factorial ring is an integral domain. Let $Q(R)$ be the quotient field of R and $s \in Q(R) \setminus \{0\}$ a non-zero element which is integral over R. Pick $d \geq 1$ and $a_1, ..., a_d \in R$ with

$$s^d + a_1 \cdot s^{d-1} + \cdots + a_{d-1} \cdot s + a_d = 0. \tag{III.14}$$

According to Lemma I.6.11, there are elements $q, r \in R \setminus \{0\}$ which are coprime and satisfy

$$s = \frac{q}{r}.$$

By Equation (III.14),

$$r^{d-1} \cdot s^d \in R.$$

Therefore,

$$q^d = r^d \cdot s^d \in \langle r \rangle.$$

Since q and r are coprime, this is possible if and only if r is a unit of R. This implies $s \in R$. □

III.5.2 Proposition. *Let R be a normal noetherian local ring. Then, R is an integral domain.*

Proof (compare Example III.2.3, ii). By definition, a normal ring is reduced, i.e., $\sqrt{\langle 0 \rangle} = \langle 0 \rangle$. According to Corollary II.4.7, there are a natural number $r \geq 1$ and prime ideals $\mathfrak{p}_1$, ..., $\mathfrak{p}_r$ with

$$\langle 0 \rangle = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_r.$$

We have to prove that $r = 1$. So, let us assume $r \geq 2$. We choose elements

- $f \in \mathfrak{p}_1 \setminus (\mathfrak{p}_2 \cup \cdots \cup \mathfrak{p}_r)$ (compare Proposition II.4.17, i),
- $g \in (\mathfrak{p}_2 \cap \cdots \cap \mathfrak{p}_r) \setminus \mathfrak{p}_1$.

Then,

- $f + g \notin \mathfrak{p}_1 \cup \cdots \cup \mathfrak{p}_r$, i.e., $f + g$ is not a zero-divisor (Theorem II.4.28, iii),
- $f \cdot g \in \mathfrak{p}_1 \cdot (\mathfrak{p}_2 \cap \cdots \cap \mathfrak{p}_r) \subset \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_r = \langle 0 \rangle$.

We look at the element (compare Example III.2.3)

$$u := \frac{f}{f+g} \in Q(R).$$

It satisfies

$$u^2 = \frac{f^2}{(f+g)^2} \overset{f \cdot g = 0}{=} \frac{f \cdot (f+g)}{(f+g)^2} = \frac{f}{f+g} = u, \quad \text{i.e.,} \quad u \cdot (u-1) = 0.$$

[14] See Page 24.

This shows that u is integral over R. Since R is assumed to be integrally closed in $Q(R)$, this means that $u \in R$. Note $u \neq 0$, because $f \neq 0$, and $u \neq 1$, because $g \neq 0$. Hence, u and $(1-u)$ are zero divisors in R. Thus, they are both contained in the maximal ideal $\mathfrak{m}$ of R. But then $1 = u + (1-u) \in \mathfrak{m}$, and this is impossible. □

III.5.3 Exercises[15]. i) Let R_1 and R_2 be integral domains. Describe the total ring of fractions $Q(R_1 \times R_2)$ in terms of the quotient fields $Q(R_1)$ and $Q(R_2)$.

ii) Use Part i) to construct a normal ring which is not an integral domain.

We look at **integral domains** R, S, and at an injective ring extension $\varphi\colon R \longrightarrow S$. By the universal property of a quotient field (Page 25), it induces a field extension

$$\widetilde{\varphi}\colon Q(R) \longrightarrow Q(S).$$

III.5.4 Remark. If φ is a finite ring extension, then $\widetilde{\varphi}$ is a finite field extension.

We need to recall some results from the theory of fields. Let K be a field, $n \geq 1$, and

$$f(x) = x^n + a_1 \cdot x^{n-1} + \cdots + a_{n-1} \cdot x + a_n$$

a **monic polynomial** in $K[x]$, i.e., a polynomial with leading coefficient one. Let $K \subset L$ be a field extension, such that f **splits** in L, i.e., there are elements $\alpha_1, ..., \alpha_n \in L$, such that

$$f(x) = (x - \alpha_1) \cdot \cdots \cdot (x - \alpha_n) \quad \text{in} \quad L[x].$$

The *discriminant* of f is

$$\Delta(f) := \prod_{\substack{i,j \in \{1,...,n\}: \\ i \neq j}} (\alpha_i - \alpha_j).$$

By the theory of **symmetric functions** ([17], Chapter IV, §6), $\Delta(f)$ is a polynomial in $a_1, ..., a_n$ with **integral** coefficients and does not depend on L. In particular,

$$\Delta(f) \in K.$$

III.5.5 Remark. We have $\Delta(f) = 0$ if and only if f has a multiple root in L.

An **irreducible** monic polynomial $f \in K[x]$ is *separable*, if $\Delta(f) \neq 0$. An arbitrary non-constant monic polynomial $f \in K[x]$ is *separable*, if its irreducible factors, normalized to have leading coefficient one, are separable. A field k is *perfect*, if every non-constant monic polynomial $f \in K[x]$ is separable.

III.5.6 Examples. i) Every field of characteristic zero is perfect ([8], Korollar III.3.4.8; Exercise III.5.7, ii).

ii) Every finite field is perfect ([8], Korollar III.4.1.9; Exercise III.5.8, ii).

iii) Every algebraically closed field is perfect. (This is trivial, because the only irreducible polynomials are those of degree one.)

iv) Let k be a field of characteristic $p > 0$ and $k(t) := Q(k[t])$ the quotient field of the polynomial ring in one variable over k. Then, $k(t)$ is not perfect. In fact, the polynomial $x^p - t$ is not separable, because

$$x^p - t = (x - \vartheta)^p$$

for every field extension $k(t) \subset L$ and every element $\vartheta \in L$ with $\vartheta^p = t$.

[15] It might be good to recall Exercise I.4.22

III.5.7 Exercises (Separable polynomials). Let K be a field and $f \in K[x]$ an irreducible monic polynomial. Define the derivative f' of f by the usual rules of analysis ([27], Page 127).

i) Let $K \subset L$ be a field extension, such that f and f' split over L. Show that f is separable if and only if f and f' do not have a common zero in L.

ii) Prove that f is inseparable, i.e., not separable, if and only if $f' = 0$.

III.5.8 Exercises (Perfect fields). i) Let k be a **perfect** field of characteristic $p > 0$. Show that, for every element $a \in k$ and every $s \geq 1$, there is an element $b \in k$ with

$$b^{p^s} = a.$$

ii) Prove that a field k with the property that, for every element $a \in k$, there is an element $b \in k$ with $b^p = a$ is perfect.

Hint. Use Exercise III.5.7, ii), to show that an inseparable polynomial $f \in k[x]$ lies in the subring $k[x^p]$.

Let $K \subset L$ be a finite field extension and $\alpha \in L$. Then,

$$\begin{array}{rcl} m_\alpha \colon L & \longrightarrow & L \\ v & \longmapsto & \alpha \cdot v \end{array}$$

is a K-linear automorphism. The *minimal polynomial* of α is the minimal polynomial $\mu_\alpha \in K[x]$ of the linear map m_α (see [33], §36). It is, by definition, monic and irreducible. We say that $\alpha \in L$ is *separable* over K, if $\mu_\alpha \in K[x]$ is a separable polynomial. The field extension $K \subset L$ is *separable*, if every element $\alpha \in L$ is separable over K.

Let $K \subset L$ be a field extension. An element $\alpha \in L$ is *primitive* for this field extension, if $L = K(\alpha)$. Here, $K(\alpha)$ is the smallest subfield of L that contains K and α.

III.5.9 Remark. If the primitive element $\alpha \in L$ is algebraic over K, then $K \subset L$ is a finite extension and every element can be written as a polynomial in α with coefficients in K. The degree of this polynomial can be chosen to be smaller than the degree of the minimal polynomial μ_α of α. In fact, if $r = \deg(\mu_\alpha)$, then $1, \alpha, ..., \alpha^{r-1}$ is a K-basis for L.

III.5.10 Theorem of the primitive element. *Let $K \subset L$ be a **finite separable** field extension. Then, it has a primitive element.*

Proof. [8], III.4.2.3; [17], Theorem V.4.6. □

III.5.11 Lemma. *Let R be an integral domain, $K := Q(R)$ its quotient field, and $K \subset L$ a **finite** field extension.*

i) *If there exists a primitive element for the field extension, then there exists also a primitive element which is **integral** over R.*

ii) *Assume that R is also **normal**, and let $\alpha \in L$ be an element which is integral over R. Then, the minimal polynomial of α lies in $R[x]$.*

Proof. i) Let $\alpha \in L$ be a primitive element. Then, there are a natural number $r \geq 1$ and elements $a_1, ..., a_r \in K$ with

$$\alpha^r + a_1 \cdot \alpha^{r-1} + \cdots + a_{r-1} \cdot \alpha + a_r = 0.$$

Since K is the quotient field of R, we may find an element $s \in R \setminus \{0\}$ with $s \cdot a_i \in R$, $i = 1, ..., r$. We multiply the above equation by s^r and find

$$(\alpha \cdot s)^r + (a_1 \cdot s) \cdot (\alpha \cdot s)^{r-1} + \cdots + (a_{r-1} \cdot s^{r-1}) \cdot (\alpha \cdot s) + (a_r \cdot s^r) = 0.$$

This shows that the element $\alpha \cdot s$ is integral over R. Finally, $K(\alpha \cdot s) = K(\alpha)$, because $s \in K^\star$.

ii) Let $L \subset \overline{L}$ be a field extension, such that μ_α splits in $\overline{L}$, and write

$$\mu_\alpha = (x - \alpha_1) \cdot \cdots \cdot (x - \alpha_r) \quad \text{in} \quad \overline{L}[x],$$

for suitable elements $\alpha_1, ..., \alpha_r \in \overline{L}$. We may assume that the numbering is such that $\alpha = \alpha_1$. Note that μ_α is also the minimal polynomial for α_i, $i = 2, ..., r$. Thus, there are K-linear isomorphisms

$$\psi_i \colon K[x]/\langle \mu_\alpha \rangle \longrightarrow K(\alpha_i) \tag{III.15}$$

sending x to α_i, $i = 1, ..., r$. We deduce that α_i is integral over R, $i = 1, ..., r$. The coefficients of μ_α are polynomials in $\alpha_1, ..., \alpha_r$ with integer coefficients. By Corollary III.2.5, ii), they are integral over R. Since R is integrally closed in K, they must actually belong to R, and this concludes the argument. □

III.5.12 Finiteness of integral closure I. *Let R be a normal integral domain with quotient field $K := Q(R)$, $K \subset L$ a finite **separable** field extension, and S the integral closure of R in L.*[16] *Pick a primitive element*[17] *$\alpha \in S$ for the given field extension, and let $\Delta \in R \setminus \{0\}$ be the discriminant of the minimal polynomial $\mu_\alpha \in R[x]$.*[18] *Then, the following properties hold true:*

i) *If $r = \deg(\mu_\alpha)$, then S is contained in the R-submodule of L that is generated by the elements*

$$\frac{1}{\Delta}, \frac{\alpha}{\Delta}, ..., \frac{\alpha^{r-1}}{\Delta}.$$

In particular, for $f \in S$, there exists a polynomial $q \in R[x]$ with $0 \leq \deg(q) < \deg(\mu_\alpha)$, such that

$$\Delta \cdot f = q(\alpha).$$

ii) *We have*

$$S_\Delta = R_\Delta[\alpha].$$

In particular, $R_\Delta[\alpha]$ is normal.

III.5.13 Remark. Assume that R is noetherian. Since the R-module $(1/\Delta) \cdot R[\alpha]$ is finitely generated, the R-submodule S is also finitely generated (Proposition III.1.30), i.e., $R \subset S$ is a finite ring extension. The theorem does not necessarily hold, if $K \subset L$ is not separable! See [15], Theorem 100, for a counterexample. In the case of an inseparable extension, we have to add additional assumptions on R for the theorem to remain true (see Theorem III.5.14).

[16] See Page 95.
[17] See Theorem III.5.10 and Lemma III.5.11, i).
[18] See Lemma III.5.11, ii)

Proof of Theorem III.5.12. i) We fix a finite field extension $K \subset M$, such that μ_α splits in M. Let $\alpha_1, ..., \alpha_r \in M$ be such that

$$\mu_\alpha(x) = (x - \alpha_1) \cdot \cdots \cdot (x - \alpha_r) \in M[x].$$

We may assume $\alpha = \alpha_1$. Since μ_α belongs to $R[x]$ and is monic, the equation $\mu_\alpha(\alpha_i) = 0$ shows that α_i is integral over R, $i = 1, ..., r$.

Next, let $f \in S$ be an element of the integral closure of R in L. There are elements $q_0, ..., q_{r-1} \in K$ with

$$f = q_0 + q_1 \cdot \alpha + \cdots + q_{r-1} \cdot \alpha^{r-1}.$$

We define

$$f_i = q_0 + q_1 \cdot \alpha_i + \cdots + q_{r-1} \cdot \alpha_i^{r-1}, \quad i = 1, ..., r.$$

Note that $f = f_1$. By (III.15), there is a K-linear isomorphism $K(\alpha) \longrightarrow K(\alpha_i)$ which maps α to α_i and, therefore, f to f_i, so that f_i is integral over R, $i = 1, ..., r$. We form the matrix

$$A := \begin{pmatrix} 1 & \alpha_1 & \cdots & \alpha_1^{r-1} \\ \vdots & \vdots & & \vdots \\ 1 & \alpha_r & \cdots & \alpha_r^{r-1} \end{pmatrix} \in \mathrm{Mat}_r(M).$$

By definition,

$$A \cdot \begin{pmatrix} q_0 \\ \vdots \\ q_{r-1} \end{pmatrix} = \begin{pmatrix} f_1 \\ \vdots \\ f_r \end{pmatrix}$$

We multiply this equation by the adjoint matrix A^{ad} of A (see Page 94) and find

$$\det(A) \cdot \begin{pmatrix} q_0 \\ \vdots \\ q_{r-1} \end{pmatrix} = \begin{pmatrix} p_1 \\ \vdots \\ p_r \end{pmatrix}.$$

The entries of A^{ad} are polynomials in the elements $\alpha_i^j \in M$, $i = 1, ..., r$, $j = 0, ..., r-1$, with integer coefficients. This implies that they are integral over R (see Corollary III.2.5, ii). Since $f_1, ..., f_r$ are also integral over R, we infer that $p_1, ..., p_r$ are integral over R. Note that $\det(A)$ is a **Vandermonde**[19] determinant (see [19], Kapitel IV, §3, Beispiel 3). Hence,

$$\det(A) = \prod_{r \geq i > j \geq 1} (\alpha_i - \alpha_j).$$

This implies that $\det(A)$ is integral over R. We finally see that

$$\Delta \cdot q_i = \pm \det(A) \cdot p_i$$

is integral over R, $i = 1, ..., r$. Furthermore, $\Delta \cdot q_i \in K$ and R is normal, so that $\Delta \cdot q_i \in R$, $i = 1, ..., r$. We infer

$$\Delta \cdot f \in R[\alpha].$$

[19] Alexandre-Théophile Vandermonde (1735 - 1796), French musician, mathematician, and chemist.

ii) We clearly have

$$R[\alpha] \subset S,$$

and Part i) shows

$$S \subset R_{\Delta}[\alpha].$$

This yields the assertion. □

III.5.14 Finiteness of integral closure II. *Let k be an **infinite perfect** field,[20] R a finitely generated k-algebra and integral domain with quotient field $K := Q(R)$, $K \subset L$ a finite field extension. Then, the integral closure S of R in L is a finitely generated R-module.*

Proof. Let $n \in \mathbb{N}$ be a natural number, such that R may be generated over k by n elements. By the Noether normalization theorem III.4.7, there are a natural number $0 \leq r \leq n$ and a finite ring extension

$$\varphi\colon k[t_1, ..., t_r] \longrightarrow R.$$

This means that we may assume without loss of generality that $R = k[t_1, ..., t_r]$. In particular, the theorem of Gauß I.6.4 and Lemma III.5.1 show that R is normal.

By Theorem III.5.12, we only have to treat the case that $K \subset L$ is an inseparable extension. We explain how we may reduce to the separable case. We fix an algebraically closed extension $L \subset \overline{K}$ ([8], Theorem III.2.1.8). Let $p > 0$ be the characteristic of the field k. Let $i = 1, ..., r$, $s \geq 1$, and $\vartheta_{i,s} \in \overline{K}$ a root of the polynomial

$$x^{p^s} - t_i \in K[x].$$

Then,

$$x^{p^s} - t_i = (x - \vartheta_{i,s})^{p^s} \in \overline{K}[x].$$

In other words, t_i has a unique p^s-th root in $\overline{K}$, $i = 1, ..., r$, $s \geq 1$. Thus, we write

$$t_i^{1/p^s} := \vartheta_{i,s}, \quad i = 1, ..., r, \quad s \geq 1.$$

Define[21]

$$K_s := k(t_1^{1/p^s}, ..., t_r^{1/p^s}), \quad s \geq 1.$$

Note

$$\forall s \geq 1 : \quad K_s \subset K_{s+1}.$$

Therefore, we may form

$$K_\infty := \bigcup_{s \geq 1} K_s.$$

This is a subfield of $\overline{K}$. For every element $a \in K_\infty$, there is an index $s_0 \geq 1$ with $a \in K_{s_0}$, so that we may define

$$s(a) := \min\{\, s \geq 1 \,|\, a \in K_s \,\}. \tag{III.16}$$

Claim. *The field K_∞ is perfect.*

[20] e.g., an algebraically closed field as in Example III.5.6, iii)

[21] By definition, this is the smallest subfield of $\overline{K}$ that contains k, t_1^{1/p^s}, ..., t_r^{1/p^s}.

We apply Exercise III.5.8, ii). The fact that k is perfect (Exercise III.5.8) gives

$$K_s = \{\, b \in \overline{K} \mid b^{p^s} \in K \,\}, \quad s \geq 1, \tag{III.17}$$

i.e., K_s consists of the p^s-th roots of elements of K, $s \geq 1$. Now, let $a \in K_\infty$. Since $\overline{K}$ is algebraically closed, there is an element $b \in \overline{K}$ with $b^p = a$. By Equation (III.17), $b \in K_{s(a)+1} \subset K_\infty$. ✓

The *composite* $L \cdot K_\infty$ of L and K_∞ in $\overline{K}$ is the smallest subfield of $\overline{K}$ that contains both L and K_∞. The extension $K_\infty \subset L \cdot K_\infty$ is finite and, by the claim, separable. Let $\beta \in L \cdot K_\infty$ be a primitive element (Theorem III.5.10) and $\mu_\beta \in K_\infty[x]$ its minimal polynomial.

Claim. *There is an index $s_0 \geq 1$ with $L \subset K_{s_0}[\beta]$ and $\mu_\beta \in K_{s_0}[x]$. In particular, $K_{s_0}[\beta] = K_{s_0}(\beta)$.*

We have $L \subset K_\infty[\beta]$. Let $b \in L$, $m \in \mathbb{N}$, and $\lambda_0, ..., \lambda_m \in K_\infty$ with

$$b = \lambda_0 + \lambda_1 \cdot \beta + \cdots + \lambda_m \cdot \beta^m.$$

Then, in the notation of (III.16),

$$b \in K_s[\beta], \quad s := \max\{\, s(\lambda_0), ..., s(\lambda_m) \,\}.$$

Now, let $(b_1, ..., b_n)$ be a K-basis for L. The previous discussion shows that there is an index $s_0 \geq 1$ with $b_i \in K_{s_0}[\beta]$, $i = 1, ..., n$. This clearly implies $L \subset K_{s_0}[\beta]$. Likewise, the fact that $\mu_\beta \in K_\infty[x]$ has only finitely many coefficients implies that we may suppose $\mu_\beta \in K_{s_0}[x]$. ✓

We choose s_0 so large that $K_{s_0}[x]$ contains the minimal polynomial μ_β of β. The field extension $K_{s_0} \subset K_{s_0}[\beta]$ is separable, because the μ_β is a separable polynomial ([8], Korollar III.3.4.13).

Since $L \subset K_{s_0}[\beta]$ is a finite field extension, we may replace L by $K_{s_0}[\beta]$. In fact, the integral closure S of R in L is an R-submodule of the integral closure T of R in $K_{s_0}[\beta]$. If T is finitely generated as R-module, then so is S (Proposition III.1.30).

For the field extension $K_{s_0} \subset K_{s_0}[\beta]$, we may apply Theorem III.5.12. It remains to investigate the extension $K \subset K_{s_0}$. Recall that $R = k[t_1, ..., t_r]$.

Claim. *The elements $t_1^{1/p^{s_0}}, ..., t_r^{1/p^{s_0}}$ are algebraically independent over k.*

Indeed, if $q \in k[x_1, ..., x_r]$ is a polynomial with

$$q(t_1^{1/p^{s_0}}, ..., t_r^{1/p^{s_0}}) = 0,$$

then $u := q^{p^{s_0}}$ is a polynomial in the subring $k[x_1^{p^{s_0}}, ..., x_r^{p^{s_0}}] \subset k[x_1, ..., x_r]$. So, $u(t_1^{1/p^{s_0}}, ..., t_r^{1/p^{s_0}})$ is actually a polynomial in $t_1, ..., t_r$, i.e., there exists a polynomial $u' \in k[x_1, ..., x_r]$ with

$$u'(t_1, ..., t_r) = u(t_1^{1/p^{s_0}}, ..., t_r^{1/p^{s_0}}).$$

Since $t_1, ..., t_r$ are algebraically independent over k, $u' = 0$. Using the injective map

$$\begin{array}{ccc} \mathbb{N}^{\times r} & \longrightarrow & \mathbb{N}^{\times r} \\ (\nu_1, ..., \nu_r) & \longmapsto & (p^{s_0} \cdot \nu_1, ..., p^{s_0} \cdot \nu_r), \end{array}$$

we find a bijection between the monomials in u and the monomials in u'. We infer $u = 0$ and $q = 0$. ✓

By this claim,

$$\begin{aligned} \iota\colon k[x_1, ..., x_r] &\longrightarrow K_{s_0} \\ x_i &\longmapsto t_i^{1/p^{s_0}}, \quad i = 1, ..., r, \end{aligned}$$

is an injective homomorphism, and K_{s_0} is isomorphic to the quotient field of $k[x_1, ..., x_r]$. The polynomial ring $k[x_1, ..., x_r]$ is normal (Theorem I.6.4 and Lemma III.5.1), so that $k[t_1^{1/p^{s_0}}, ..., t_r^{1/p^{s_0}}]$ is integrally closed in K_{s_0}. It remains to show that

$$k[t_1, ..., t_r] \longrightarrow k[t_1^{1/p^{s_0}}, ..., t_r^{1/p^{s_0}}]$$

is a finite ring extension. By Corollary III.2.5, i), it is enough to show that $\tau_i := t_i^{1/p^{s_0}}$ is integral over $k[t_1, ..., t_r]$, $i = 1, ..., r$. Finally, τ_i satisfies the integrality equation $\tau_i^{p^{s_0}} - t_i = 0$, $i = 1, ..., r$. □

III.5.15 Corollary (Finiteness of normalization)**.** *Let k be an **infinite perfect** field, R a finitely generated k-algebra and integral domain, and $R \subset S$ the **normalization** of R, i.e., the integral closure of the ring R in its quotient field $Q(R)$.*[22] *Then, the integral closure S is a finitely generated R-module and, in particular, a finitely generated k-algebra.*

Proof. By Theorem III.4.7, there are $r \in \mathbb{N}$ and a finite ring extension

$$\varphi\colon k[x_1, ..., x_r] \longrightarrow R.$$

By Corollary III.2.7, the integral closure of $k[x_1, ..., x_r]$ in $Q(R)$ equals the integral closure of R in $Q(R)$. So, we may apply Theorem III.5.14 to $k[x_1, ..., x_r]$ and $L := Q(R)$. □

III.5.16 Remark. Not every noetherian ring has a finite normalization. We refer to [24] for a survey on counterexamples.

[22] See Example III.2.9.

IV

Dimension Theory

The concept of dimension is very important in many areas of mathematics. That might be partially due to the fact that we have a good intuition for dimension. It is our impression that we live in a three-dimensional world, so that, adding time, we may visualize up to four real dimensions. Now, it becomes an important task to introduce in a mathematically rigid way a concept of dimension that matches our intuitive expectations. In commutative algebra, this concept is the Krull dimension of a ring. It will be defined and discussed in this chapter. For integral domains which are finitely generated over a field, it is possible to identify the Krull dimension with the transcendence degree of the quotient field. Another important concept is the embedding dimension of a local ring. In the geometric context, the embedding dimension is the dimension of the tangent space at a point.[1] With the embedding dimension, we may define regular and singular points of algebraic varieties. Working over the complex numbers, a point of a variety is regular if and only if the variety looks locally[2] around that point like an open subset of $\mathbb{C}^k$, k the dimension of the variety, i.e., is a complex manifold around that point. So, near regular points, the local geometry is very easy, whereas, at singular points, it can become very intricate. We will see some basic examples for this. We will also highlight some algebraic consequences of regularity.

IV.1 Krull Dimension

Let R be a ring. Its *Krull dimension* is

$$\dim(R) := \sup\{\, k \in \mathbb{N} \mid \exists \text{ prime ideals } \mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_k \,\} \in \mathbb{N} \cup \{\infty\}.$$

IV.1.1 Examples. i) A field has Krull dimension zero. Geometrically, a field is the coordinate algebra of a point. So, this matches our expectation that a point should be zero-dimensional.

[1] We recall that, for varieties over algebraically closed ground fields, we have a correspondence between points of the variety and maximal ideals in the coordinate algebra. The local ring attached to a point of the variety is the localization of the coordinate algebra of the variety at the corresponding maximal ideal.

[2] in the euclidean topology of $\mathbb{A}^n_{\mathbb{C}}$

ii) A principal ideal domain is either a field or has Krull dimension one. For example, let k be a field. Then, $k[x]$ is one-dimensional as ring. It is the coordinate algebra of the affine line $\mathbb{A}^1_k$. Again, our feeling that the affine line should be one-dimensional is confirmed. It is worthwhile noting that $\mathbb{Z}$ also has Krull dimension one. For this reason, one draws Spec($\mathbb{Z}$) in a fashion which supports this fact (see [21], Chapter II.1, Example C).[3] It is, indeed, one of the big achievements of modern algebraic geometry that rings such as $\mathbb{Z}$ and $k[x]$ may be described on an equal footing.

IV.1.2 Remarks. i) Let k be a field, $n \in \mathbb{N}$, $I \subset k[x_1, ..., x_n]$ an ideal, and

$$R := k[x_1, ..., x_n]/I.$$

Then, the Krull dimension of R is the supremum of all natural numbers s for which there exist **irreducible** algebraic sets

$$V(I) \supset V_0 \supsetneq \cdots \supsetneq V_s$$

in the affine n-space $\mathbb{A}^n_k$. This illustrates the idea behind Krull dimension: Given two irreducible subsets $Y, Z \subset \mathbb{A}^n_k$, an inclusion $Y \subset Z$ is only possible, if $Y = Z$ or the dimension of Z is larger than the one of Y. For example, an irreducible zero-dimensional algebraic set is just a point. Any irreducible algebraic set properly containing it has to be at least one-dimensional, and so on.

ii) Let k be a field, $n \in \mathbb{N}$, and $R := k[x_1, ..., x_n]$. We have the chain of prime ideals

$$\langle 0 \rangle \subsetneq \langle x_1 \rangle \subsetneq \cdots \subsetneq \langle x_1, ..., x_n \rangle.$$

This shows

$$\dim(k[x_1, ..., x_n]) \geq n.$$

IV.1.3 Theorem. *Assume that the field k is infinite. For any natural number $n \in \mathbb{N}$, we have* $\dim(k[x_1, ..., x_n]) = n$.

The proof will be given on Page 121f.

IV.2 The Going-Up Theorem

We now investigate how dimension behaves under integral ring extensions.

IV.2.1 Lemma. *Let R and S be **integral domains** and $\varphi\colon R \longrightarrow S$ an **integral ring extension**. Then, R is a field if and only if S is one.*

Proof. We have already seen that R is a field, if S is one (Lemma III.3.9). Now, assume that R is a field. Let $y \in S \setminus \{0\}$ be a non-zero element. Choose $n \geq 1$ minimal, such that there exist elements $a_1, ..., a_n \in R$ with

$$y^n + a_1 \cdot y^{n-1} + \cdots + a_{n-1} \cdot y + a_n = 0. \tag{IV.1}$$

[3] Accordingly, $\mathbb{Z}[x]$ should be two-dimensional. Here, you should consult your picture of the spectrum of that ring (Exercise I.4.21). You will also find it in [21], Chapter II.1, Example H.

Since we chose n to be minimal and S is an integral domain, we have $a_n \neq 0$. Equation (IV.1) can be read as

$$a_n = -y \cdot (y^{n-1} + a_1 \cdot y^{n-2} + \cdots + a_{n-1}).$$

This shows that

$$y^{-1} = -\frac{1}{a_n} \cdot (y^{n-1} + a_1 \cdot y^{n-2} + \cdots + a_{n-1})$$

is an element of S. □

IV.2.2 Lemma. *Let R, S be rings, $\varphi\colon R \longrightarrow S$ an **integral ring extension**, $\mathfrak{q} \subset S$ a prime ideal, and*

$$\mathfrak{p} := \mathfrak{q} \cap R.$$

Then, $\mathfrak{q}$ is a maximal ideal in S if and only if $\mathfrak{p}$ is a maximal ideal in R.[4]

Proof. The homomorphism φ induces the homomorphism

$$\overline{\varphi}\colon R/\mathfrak{p} \longrightarrow S/\mathfrak{q}.$$

Here, $R/\mathfrak{p}$ and $S/\mathfrak{q}$ are integral domains, and $\overline{\varphi}$ is also an integral ring extension.

By Proposition I.4.1, ii), $\mathfrak{q}$ is a maximal ideal in S if and only if $S/\mathfrak{q}$ is a field. The previous lemma says that $S/\mathfrak{q}$ is a field if and only if $R/\mathfrak{p}$ is a field. Using Proposition I.4.1, ii), again, $R/\mathfrak{p}$ is a field if and only if $\mathfrak{p}$ is a maximal ideal in R. This completes the proof. □

IV.2.3 Lemma. *Let R, S be rings, $\varphi\colon R \longrightarrow S$ an **integral ring extension**, and $\mathfrak{q} \subset \mathfrak{q}' \subset S$ prime ideals. If*

$$\mathfrak{p} := R \cap \mathfrak{q} = R \cap \mathfrak{q}',$$

then

$$\mathfrak{q} = \mathfrak{q}'.$$

Proof. The set $T := R \setminus \mathfrak{p}$ is a multiplicatively closed subset of both R and S. By Exercise II.3.8, the homomorphism φ induces a homomorphism

$$\varphi_T\colon R_T \longrightarrow S_T.$$

It is readily verified that φ_T is an integral ring extension, too. We use the commutative diagram

$$\begin{array}{ccc} R & \xrightarrow{\varphi} & S \\ \downarrow & & \downarrow \\ R_T & \xrightarrow{\varphi_T} & S_T. \end{array} \tag{IV.2}$$

Define

$$\mathfrak{n} := \mathfrak{q}^e \subset S_T \quad \text{and} \quad \mathfrak{n}' := \mathfrak{q}'^e \subset S_T.$$

Note that[5]

$$\mathfrak{q} \cap T = \varnothing = \mathfrak{q}' \cap T.$$

[4] Compare Exercise III.3.8.

[5] We use φ to view R as a subring of S and write intersections instead of preimages.

Thus, Proposition II.3.6, v), shows

$$\mathfrak{n}^c = \mathfrak{q} \quad \text{and} \quad \mathfrak{n}'^c = \mathfrak{q}'. \tag{IV.3}$$

Next,

$$\mathfrak{m} := \mathfrak{p}^e \subset R_T.$$

By Corollary II.3.7, ii), it is the maximal ideal of R_T. Using Proposition II.3.6, i), and the maximality of $\mathfrak{m}$, our assumption gives

$$\mathfrak{n} \cap R_T = \mathfrak{m} = \mathfrak{n}' \cap R_T.$$

We apply Lemma IV.2.2 to φ_T. It shows that $\mathfrak{n}$ and $\mathfrak{n}'$ are maximal ideals in S_T. Since $\mathfrak{n} \subset \mathfrak{n}'$, we infer $\mathfrak{n} = \mathfrak{n}'$. So, Equation (IV.3) yields our claim. □

IV.2.4 Lying-over theorem. *Let R, S be rings, $\varphi\colon R \longrightarrow S$ an **integral ring extension**, and $\mathfrak{p} \subset R$ a prime ideal. Then, there is a prime ideal $\mathfrak{q} \subset S$ with*

$$\mathfrak{p} = \mathfrak{q} \cap R.$$

IV.2.5 Remarks. i) The theorem says that the induced map

$$\varphi^{\#}\colon \operatorname{Spec}(S) \longrightarrow \operatorname{Spec}(R)$$

is surjective.

ii) Note that, by Lemma IV.2.2, $\varphi^{\#}$ maps maximal ideals to maximal ideals, i.e., $\varphi^{\#}$ is also surjective on the level of maximal ideals. Together with the correspondence between the points of an algebraic set and the maximal ideals of its coordinate algebra provided by the Nullstellensatz (Exercise III.3.2), we find a nice conceptual proof for Lemma III.4.8.

Proof of the lying-over theorem. As in the proof of Lemma IV.2.3, we localize at the multiplicatively closed subset $T := R \setminus \mathfrak{p}$ and look at Diagram (IV.2). Let $\mathfrak{n} \subset S_T$ be a maximal ideal (Theorem I.4.4). Since φ_T is an integral ring extension, we conclude by Lemma IV.2.2 that

$$\mathfrak{m} := \mathfrak{n} \cap R_T$$

is a maximal ideal of R_T. Now, R_T is a local ring (Corollary II.3.7, ii). So, $\mathfrak{m} = \mathfrak{p}^e$ and $\mathfrak{m}^c = \mathfrak{p}$. Finally,

$$\mathfrak{q} := \mathfrak{n}^c \subset S$$

is a prime ideal. By construction, $\mathfrak{q} \cap R = \mathfrak{p}$. □

IV.2.6 The going-up theorem. *Let R, S be rings, $\varphi\colon R \longrightarrow S$ an **integral ring extension**, $k > l$ natural numbers,*

$$\mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_k$$

prime ideals in R, and

$$\mathfrak{q}_0 \subsetneq \cdots \subsetneq \mathfrak{q}_l$$

prime ideals in S, such that

$$\forall i \in \{0, ..., l\}: \quad \mathfrak{q}_i \cap R = \mathfrak{p}_i.$$

Then, one finds prime ideals

$$\mathfrak{q}_{l+1} \subsetneq \cdots \subsetneq \mathfrak{q}_k$$

in S with

- ★ $\mathfrak{q}_l \subsetneq \mathfrak{q}_{l+1}$,
- ★ $\mathfrak{q}_i \cap R = \mathfrak{p}_i$, $i = l+1, ..., k$.

Proof. It clearly suffices to treat the case $k = l + 1$. This case follows from applying the lying-over theorem to the integral ring extension

$$\overline{\varphi}_l \colon R/\mathfrak{p}_l \longrightarrow S/\mathfrak{q}_l$$

and the prime ideal $\overline{\mathfrak{p}}_k$ of $R/\mathfrak{p}_l$ (Lemma I.2.2). □

IV.2.7 Theorem. *Let R, S be rings and $\varphi \colon R \longrightarrow S$ an **integral ring extension**. Then, the Krull dimensions of R and S are equal:*

$$\dim(R) = \dim(S).$$

Proof. The lying-over theorem and the going-up theorem clearly show that

$$\dim(R) \leq \dim(S).$$

Conversely, let

$$\mathfrak{q}_0 \subsetneq \cdots \subsetneq \mathfrak{q}_k$$

be prime ideals in S and

$$\mathfrak{p}_i := \mathfrak{q}_i \cap R.$$

By Lemma IV.2.3,

$$\mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_k.$$

This implies

$$\dim(R) \geq \dim(S)$$

and, therefore, the assertion of the theorem. □

Proof of Theorem IV.1.3. We proceed by induction on n. For $n = 0$, we are dealing with the field k. It has Krull dimension 0 (Example IV.1.1).

Now, assume that the theorem is true for n, and let

$$\mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_k$$

be prime ideals in the polynomial ring $k[x_1, ..., x_{n+1}]$. Since $k[x_1, ..., x_{n+1}]$ is an integral domain, we may assume $\mathfrak{p}_0 = \langle 0 \rangle$. Moreover, we may suppose $k \geq 1$ (see Remark IV.1.2, ii). Let $f \in \mathfrak{p}_1 \setminus \{0\}$. Recall that $k[x_1, ..., x_{n+1}]$ is a factorial ring (Theorem I.6.4). Thus, there are pairwise non-associated irreducible polynomials $f_1, ..., f_s \in k[x_1, ..., x_{n+1}]$ and positive integers $k_1, ..., k_s$, such that

$$f \sim f_1^{k_1} \cdot \cdots \cdot f_s^{k_s}.$$

Since $\mathfrak{p}_1$ is a prime ideal, there is an index $i_0 \in \{1, ..., s\}$ with $f_{i_0} \in \mathfrak{p}_1$. We get the prime ideals

$$\mathfrak{p}_0 \subsetneq \langle f_{i_0} \rangle \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_k.$$

This shows that we may assume without loss of generality that $\mathfrak{p}_1$ is a principal ideal, say, $\mathfrak{p}_1 = \langle g \rangle$ with $g \in k[x_1, ..., x_{n+1}]$ an irreducible polynomial. By the Noether normalization theorem for hypersurfaces III.4.4, there is an integral ring extension

$$\varphi\colon k[x_1, ..., x_n] \longrightarrow k[x_1, ..., x_{n+1}]/\langle g \rangle$$

By Theorem IV.2.7 and the induction hypothesis,

$$\dim(k[x_1, ..., x_{n+1}]/\langle g \rangle) = n.$$

This shows that $k \leq n + 1$ and, consequently,

$$\dim(k[x_1, ..., x_{n+1}]) \leq n + 1.$$

Together with Remark IV.1.2, ii), we obtain the desired equality. □

IV.3 The Transcendence Degree of a Field

Let $k \subset K$ be a field extension. A subset $S \subset K$ is said to be *algebraically independent* over k, if every **finite** subset $S' \subset S$ is algebraically independent over k (in the sense of Page 8). The algebraically independent subsets of K are partially ordered by inclusion, and $\varnothing$ is an algebraically independent subset. Zorn's lemma I.4.7 gives:

IV.3.1 Lemma. *The field K contains maximal algebraically independent subsets.*

A maximal algebraically independent subset $S \subset K$ is called a *transcendence basis* for K over k. We say that K has *finite transcendence degree* over k, if there exists a finite transcendence basis for K over k.

IV.3.2 Remark. The field extension $k \subset K$ is algebraic if and only if $\varnothing$ is a transcendence basis of K over k.

IV.3.3 Proposition. *Assume that K has finite transcendence degree over k. Let $S \subset K$ be a transcendence basis and $m := \#S$. Then, every transcendence basis of K over k has m elements.*

If K has finite transcendence degree over k and $S \subset K$ is a transcendence basis, we call

$$\operatorname{trdeg}_k(K) := \#S$$

the *transcendence degree* of K over k. By Proposition IV.3.3, this is well-defined. If K does not have finite transcendence degree, we say that it has *infinite transcendence degree* and write

$$\operatorname{trdeg}_k(K) := \infty.$$

Proof of Proposition IV.3.3. We may assume that S has the minimal number of elements among all transcendence bases for K. Write $S = \{ s_1, ..., s_m \}$ and let $T = \{ t_1, ..., t_n \} \subset K$ be an algebraically independent subset with $m \leq n$. We will then prove that there is a subset $T' \subset T$ with m elements, such that K is algebraic over $k(T')$. This implies that $T \setminus T'$ is empty and, thus, $m = n$, and that T is a transcendence basis. The strategy is to exchange elements of S by elements of T.

We set

$$r := \max\{\varrho \in \{0, ..., m\} \mid \exists i_{\varrho+1}, ..., i_m \in \{1, ..., m\}: K \text{ is algebraic over } k(t_1, ..., t_\varrho, s_{i_{\varrho+1}}, ..., s_{i_m})\}.$$

We will lead the assumption $r < m$ to a contradiction. After renumbering, we may assume $\{i_{r+1}, ..., i_m\} = \{r+1, ..., m\}$. There exists a non-zero polynomial $f \in k[x_1, ..., x_{m+1}]$ with

$$f(t_1, ..., t_r, s_{r+1}, ..., s_m, t_{r+1}) = 0 \quad (\text{in } K).$$

Since $t_1, ..., t_{r+1}$ are algebraically independent over k, there is an index $i_0 \in \{r+1, ..., m\}$, such that x_{i_0} occurs in f, i.e., $f \notin k[x_1, ..., x_r, x_{r+1}, ..., x_{i_0-1}, x_{i_0+1}, ..., x_{m+1}]$. After renumbering, if necessary, we may assume that $r+1$ is such an index. This means that s_{r+1} is algebraic over $k(t_1, ..., t_{r+1}, s_{r+2}, ..., s_m)$ and, therefore, K is an algebraic extension of $k(t_1, ..., t_{r+1}, s_{r+2}, ..., s_m)$, contradicting the definition of r. □

IV.3.4 Example. Let k be a field. For $n \in \mathbb{N}$, it follows readily that

$$\operatorname{trdeg}_k(k(x_1, ..., x_n)) = n, \quad k(x_1, ..., x_n) := Q(k[x_1, ..., x_n]).$$

IV.4 The Dimension of an Algebraic Variety

IV.4.1 Theorem. *Let k be an **infinite** field, $n \geq 1$, and $\mathfrak{p} \subset k[x_1, ..., x_n]$ a **prime ideal**. Then,*

$$\dim(k[x_1, ..., x_n]/\mathfrak{p}) = \operatorname{trdeg}_k(Q(k[x_1, ..., x_n]/\mathfrak{p})).$$

Proof. By Noether normalization III.4.7, there are a natural number $0 \leq m \leq n$ and a finite ring extension

$$\varphi\colon k[x_1, ..., x_m] \longrightarrow k[x_1, ..., x_n]/\mathfrak{p}.$$

The homomorphism φ induces a **finite** field extension (see Page 25)

$$\widetilde{\varphi}\colon k(x_1, ..., x_m) = Q(k[x_1, ..., x_m]) \longrightarrow Q(k[x_1, ..., x_n]/\mathfrak{p}).$$

Since every finite field extension is algebraic ([8], Satz III.1.6.2, 1), we have

$$\operatorname{trdeg}_k(Q(k[x_1, ..., x_n]/\mathfrak{p})) = \operatorname{trdeg}_k(k(x_1, ..., x_m)) = m.$$

On the other hand, Theorem IV.2.7 gives

$$\dim(k[x_1, ..., x_n]/\mathfrak{p}) = \dim(k[x_1, ..., x_m]) = m.$$

This settles the theorem. □

The Going-Down Theorem

Let R, T be rings, $\psi\colon R \longrightarrow T$ an injective homomorphism, and $I \subset R$ an ideal. We say that $\alpha \in T$ is *integral* over I, if there exist a positive natural number $n \geq 1$ and elements $a_1, ..., a_n \in I$ with

$$\alpha^n + a_1 \cdot \alpha^{n-1} + \cdots + a_{n-1} \cdot \alpha + a_n = 0. \tag{IV.4}$$

IV.4.2 Lemma. *Let R, S be integral domains, $\varphi\colon R \longrightarrow S$ an integral ring extension, $\widetilde{\varphi}\colon K \longrightarrow L$ the corresponding algebraic field extension, $K := Q(R)$, $L := Q(S)$, and $I \subset R$ an ideal.*

i) *An element $\alpha \in S$ is integral over I if and only if $\alpha \in \sqrt{I^e}$.*

ii) *Assume that R is normal. Let $\alpha \in L$ be an element which is integral over I. Then, the minimal polynomial $\mu_\alpha \in K[x]$ of α has coefficients in $\sqrt{I}$.*

Proof. i) If $\alpha \in S$ is integral over I, then an integrality equation like (IV.4) shows $\alpha^n \in I^e$, so that $\alpha \in \sqrt{I^e}$.

Conversely, suppose that $\alpha \in \sqrt{I^e}$ and pick $s \geq 1$ with $\alpha^s \in I^e$. There are $m \geq 1$, $r_1, ..., r_m \in I$, and $a_1, ..., a_m \in S$ with

$$\alpha^s = a_1 \cdot r_1 + \cdots + a_m \cdot r_m.$$

Now, let $M \subset S$ be the finitely generated R-submodule generated by $a_1, ..., a_m$, and set

$$\begin{array}{rcl} \varphi\colon M & \longrightarrow & M \\ x & \longmapsto & \alpha^s \cdot x. \end{array}$$

This is an endomorphism with $\varphi(M) \subset I \cdot M$. As in the proof of "iv)$\Longrightarrow$i)" of Proposition III.2.4, we construct a monic polynomial $p \in R[x]$ with coefficients in I, such that $p(\alpha^s)$ annihilates M. If $\alpha \neq 0$, then $M \neq \{0\}$. Since S is an integral domain, this implies that $p(\alpha^s) = 0$. Therefore, α^s and α are integral over I.

ii) By Equation (IV.4) and the definition of a minimal polynomial, the minimal polynomial μ_α of α divides $p(x) := x^n + a_1 \cdot x^{n-1} + \cdots + a_{n-1} \cdot x + a_n$. Therefore, the roots $\alpha_1, ..., \alpha_r$ of μ_α are integral over I. The arguments in the proof of Lemma III.5.11, ii), show that the coefficients of μ_α belong to R, and Part i) yields that they lie in $\sqrt{I}$. □

IV.4.3 The going-down theorem. *Let R, S be integral domains, $\varphi\colon R \longrightarrow S$ an **integral ring extension**, $k > l$ natural numbers,*

$$\mathfrak{p}_0 \supsetneq \cdots \supsetneq \mathfrak{p}_k$$

prime ideals in R, and

$$\mathfrak{q}_0 \supsetneq \cdots \supsetneq \mathfrak{q}_l$$

prime ideals in S, such that

$$\forall i \in \{0, ..., l\}: \quad \mathfrak{q}_i \cap R = \mathfrak{p}_i.$$

*If R is **normal**, one finds prime ideals*

$$\mathfrak{q}_{l+1} \supsetneq \cdots \supsetneq \mathfrak{q}_k$$

in S with

- ★ $\mathfrak{q}_l \supsetneq \mathfrak{q}_{l+1}$,
- ★ $\mathfrak{q}_i \cap R = \mathfrak{p}_i$, $i = l+1, ..., k$.

Proof. Again, it suffices to treat the case $k = l + 1$. We look at the localization[6] $S_{\mathfrak{q}_l}$ and the homomorphism $R \longrightarrow S_{\mathfrak{q}_l}$. It is sufficient to show that, with respect to this homomorphism,

$$\mathfrak{p}_{l+1}^{ec} = \mathfrak{p}_{l+1}.$$

In fact, by Corollary II.3.7, $\mathfrak{p}_{l+1}^{e}$, the extension being taken with respect to φ, will do the trick.

Let $\beta \in \mathfrak{p}_{l+1}^{e}$. Then, we may write $\beta = \alpha/s$ with $\alpha \in S \cdot \mathfrak{p}_{l+1}$ and $s \in S \setminus \mathfrak{q}_l$. Since S is integral over R, it is clear that α is integral over $\mathfrak{p}_{l+1}$, and Lemma IV.4.2, ii), shows that we may find $n \geq 1$ and $a_1, ..., a_n \in \mathfrak{p}_{l+1}$ with

$$\alpha^n + a_1 \cdot \alpha^{n-1} + \cdots + a_{n-1} \cdot \alpha + a_n = 0. \tag{IV.5}$$

In fact, we may assume that $x^n + a_1 \cdot x^{n-1} + \cdots + a_{n-1} \cdot x + a_n$ is the minimal polynomial of α. Now, assume that $\beta \in \mathfrak{p}_{l+1}^{ec} \setminus \{0\}$. Recall that $s = \alpha/\beta$. We divide (IV.5) by β^n and find the integrality equation

$$s^n + b_1 \cdot s^{n-1} + \cdots + b_{n-1} \cdot s + b_n = 0, \quad b_i := \frac{a_i}{\beta^i}, \quad i = 1, ..., n, \tag{IV.6}$$

for s over K. We claim that $q(x) := x^n + b_1 \cdot x^{n-1} + \cdots + b_{n-1} \cdot x + b_n$ is the minimal polynomial of s. Indeed, if there were a polynomial $r(x) \in K[X]$ of degree, say, $l < n$, with $r(s) = 0$, then $(\beta^l \cdot r)(\alpha) = 0$ and $\beta^l \cdot r \in K[x]$. This contradicts the choice of n. By Lemma III.5.11, $q(x)$ is a polynomial in $R[x]$, i.e., $b_i \in R$, and

$$\beta^i \cdot b_i = a_i \in \mathfrak{p}_{l+1}, \quad i = 1, ..., n.$$

If $\beta \notin \mathfrak{p}_{l+1}$, then $b_i \in \mathfrak{p}_{l+1}$, $i = 1, ..., n$. Equation (IV.6) proves that $s^n \in S \cdot \mathfrak{p}_{l+1} \subset \mathfrak{q}_l$, and this is impossible. So, after all, $\beta \in \mathfrak{p}_{l+1}$. □

A Refined Version of Noether Normalization

IV.4.4 Theorem. *Let k be an infinite field, R a finitely generated k-algebra, $n := \dim(R)$, and*

$$I_0 \subsetneq \cdots \subsetneq I_l$$

a chain of ideals in R. Then, there exist a finite ring extension

$$\varphi\colon k[t_1, ..., t_n] \longrightarrow R$$

and natural numbers

$$0 \leq k_0 \leq \cdots \leq k_l \leq n$$

with

$$\varphi^{-1}(I_j) = \langle\, t_1, ..., t_{k_j} \,\rangle, \quad j = 0, ..., l.$$

[6] Corollary II.3.7 explains why this is natural.

Proof. **Step 1.** We first reduce to the case when R is a polynomial ring. By definition, there are a natural number $m \geq 1$ and an ideal $J \subset k[x_1, ..., x_m]$, such that

$$R = k[x_1, ..., x_m]/J.$$

By Theorem III.4.7, there is an integral ring extension

$$\psi\colon k[x_1, ..., x_n] \longrightarrow R.$$

We get the chain

$$J_0 \subset \cdots \subset J_l, \quad J_k := \psi^{-1}(I_k), \quad k = 0, ..., l.$$

Since the composition of finite ring extensions is a finite ring extension (Lemma III.2.6), we may assume without loss of generality that $R = k[x_1, ..., x_n]$.

Step 2. We first consider the case $l = 0$. Here, we will use several inductions. To start with, we look at the case $I = \langle f \rangle$ with $f \neq 0$.

Claim. *The element f is transcendent over k.*

According to the proof of Theorem III.4.4, we may assume that there are polynomials $g_1, ..., g_r \in k[x_2, ..., x_n]$, such that

$$f = x_1^r + g_1 \cdot x_1^{r-1} + \cdots + g_{r-1} \cdot x_1 + g_r. \tag{IV.7}$$

For a non-zero polynomial $p(t) = t^l + a_1 \cdot t^{l-1} + \cdots + a_{l-1} \cdot t + a_l \in k[t]$, we have

$$p(f) = x_1^{r \cdot l} + \text{terms involving } x_2, ..., x_n + \text{lower order terms.}$$

This is not zero. ✓

A similar argument shows that the elements $f, x_2, ..., x_n$ are algebraically independent over k (compare Section IV.3). The inclusion

$$k[f, x_2, ..., x_n] \subset k[x_1, x_2, ..., x_n]$$

is a finite ring extension,

$$x_1^r + g_1 \cdot x_1^{r-1} + \cdots + g_{r-1} \cdot x_1 + g_r - f = 0$$

being an integrality equation for x_1. Together with the isomorphism

$$\begin{array}{rcl} k[t_1, t_2, ..., t_n] & \longrightarrow & k[f, x_2, ..., x_n] \\ t_1 & \longmapsto & f \\ t_i & \longmapsto & x_i, \quad i = 2, ..., n, \end{array}$$

we obtain the integral ring extension ϑ with

$$\vartheta^{-1}(\langle f \rangle) = \langle t_1 \rangle.$$

Now, we are ready to prove the case $l = 0$ by induction on n. The case $n = 1$ is clear by the foregoing discussion.

Next, assume that $I \subset k[x_1, x_2, ..., x_n]$ is a non-trivial ideal. We let $f \in I \setminus \{0\}$. Suppose that it has the form given in (IV.7) and construct an integral ring extension

$$\vartheta\colon k[u_1, ..., u_n] \longrightarrow k[x_1, ..., x_n]$$

with $\vartheta^{-1}(\langle f\rangle) = \langle u_1\rangle$. So, we have an induced finite ring extension

$$\overline{\vartheta}\colon k[u_2, ..., u_n] = k[u_1, ..., u_n]/\langle u_1\rangle \longrightarrow k[x_1, ..., x_n]/\langle f\rangle.$$

Define I' as the image of I in the ring $k[x_1, ..., x_n]/\langle f\rangle$ and $I'' := \overline{\vartheta}^{-1}(I')$. By induction, there are a natural number $2 \leq k_0 \leq n$ and a finite ring extension

$$\psi\colon k[t_2, ..., t_n] \longrightarrow k[u_2, ..., u_n]$$

with

$$\psi^{-1}(I'') = \langle\, t_2, ..., t_{k_0}\,\rangle.$$

Define φ as the composition of ϑ and the homomorphism

$$\begin{array}{rcl} k[t_1, ..., t_n] & \longrightarrow & k[u_1, ..., u_n] \\ t_1 & \longmapsto & u_1 \\ t_i & \longmapsto & \psi(t_i), \quad i = 2, ..., n. \end{array}$$

It is an integral ring extension with

$$\varphi^{-1}(I) = \langle\, t_1, ..., t_{k_0}\,\rangle.$$

Step 3. Now, we can prove the general statement by induction on l. The case $l = 0$ has been settled in the previous step. Let $I_0 \subset \cdots \subset I_{l+1}$ be a chain of ideals in $k[x_1, ..., x_n]$. By induction hypothesis, there are natural numbers $0 \leq k_0 \leq \cdots \leq k_l \leq n$ and a finite ring extension

$$\vartheta\colon k[u_1, ..., u_n] \longrightarrow k[x_1, ..., x_n]$$

with

$$\vartheta^{-1}(I_j) = \langle\, u_1, ..., u_{k_j}\,\rangle, \quad j = 0, ..., l.$$

It induces a finite ring extension

$$\overline{\vartheta}\colon k[u_{k_l+1}, ..., u_n] = k[u_1, ..., u_n]/\langle\, u_1, ..., u_{k_l}\,\rangle \longrightarrow k[x_1, ..., x_n]/I_l.$$

We conclude as in Step 2. □

IV.4.5 Remark. Assume in the statement of Theorem IV.4.4 that

$$\mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_l$$

is a chain of prime ideals. Then, by Lemma IV.2.3,

$$\varphi^{-1}(\mathfrak{p}_{i-1}) \subsetneq \varphi^{-1}(\mathfrak{p}_i), \quad i = 1, ..., l,$$

i.e.,

$$0 \leq k_0 < \cdots < k_l \leq n,$$

and $k_0 = 0$ holds if and only if $\mathfrak{p}_0 = \langle 0\rangle$.

IV.4.6 The chain theorem. *Let k be an infinite field, $n \geq 1$ a natural number, R a finitely generated k-algebra and an integral domain, and $n = \dim(R)$. Every finite chain*

$$\mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_l \tag{IV.8}$$

of prime ideals in R can be completed to a finite chain of length n, i.e., there are prime ideals

$$\mathfrak{p}'_0 \subsetneq \cdots \subsetneq \mathfrak{p}'_n$$

such that

$$\{ \mathfrak{p}_0, ..., \mathfrak{p}_l \} \subset \{ \mathfrak{p}'_0, ..., \mathfrak{p}'_n \}.$$

Proof. We apply Theorem IV.4.4 to (IV.8). Let $0 \leq k_0 < \cdots < k_l \leq n$ be natural numbers and

$$\varphi\colon k[t_1, ..., t_n] \longrightarrow R$$

be an integral ring extension with

$$\varphi^{-1}(\mathfrak{p}_i) = \langle t_1, ..., t_{k_i} \rangle, \quad i = 0, ..., l.$$

Note that we may assume $k_l = n$, because otherwise, by the going-up theorem IV.2.6, there is an ideal $\mathfrak{p}_l \subsetneq \mathfrak{p}_{l+1}$ with $\varphi^{-1}(\mathfrak{p}_{l+1}) = \langle t_1, ..., t_n \rangle$. This assumption and Remark IV.4.5 imply that, if $l < n$, there must be an index $i_0 \in \{ 1, ..., l \}$ with

$$k_{i_0} - k_{i_0-1} > 1.$$

We pass to the finite ring extension

$$\overline{\varphi}\colon k[t_{\varkappa+1}, ..., t_n] := k[t_1, ..., t_n]/\langle t_1, ..., t_\varkappa \rangle \longrightarrow R/\mathfrak{p}_{i_0-1} \quad \varkappa := k_{i_0-1},$$

and look at the image $\overline{\mathfrak{p}}$ of $\mathfrak{p}_{i_0}$ in $R/\mathfrak{p}_{i_0-1}$. By construction,

$$\overline{\varphi}^{-1}(\overline{\mathfrak{p}}) = \langle t_{\varkappa+1}, ..., t_{k_{i_0}} \rangle.$$

The assumption $k_{i_0} > \varkappa + 1$ implies

$$\langle t_{\varkappa+1} \rangle \subsetneq \langle t_{\varkappa+1}, ..., t_{k_{i_0}} \rangle$$

Since $k[t_{\varkappa+1}, ..., t_n]$ is a normal ring (Theorem I.6.4 and Lemma III.5.1), we may apply the going-down theorem IV.4.3. So, there exists an ideal

$$\overline{\mathfrak{q}} \subsetneq \overline{\mathfrak{p}}$$

with

$$\overline{\varphi}^{-1}(\overline{\mathfrak{q}}) = \langle t_{\varkappa+1} \rangle.$$

The preimage $\mathfrak{q}$ of $\overline{\mathfrak{q}}$ in $k[x_1, ..., x_n]$ satisfies

$$\mathfrak{p}_{i_0-1} \subsetneq \mathfrak{q} \subsetneq \mathfrak{p}_{i_0}.$$

So, we have increased the length of the given chain by one. Iterating the argument, if necessary, we arrive at a chain of length n. □

Heights

Let R be a ring and $\mathfrak{p} \subset R$ a **prime ideal**. The *height* of $\mathfrak{p}$ is

$$\mathrm{ht}(\mathfrak{p}) = \sup\{\, k \mid \exists \text{ prime ideals } \mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_k = \mathfrak{p} \,\}.$$

IV.4.7 Remark. By Corollary II.3.7, i), we have

$$\mathrm{ht}(\mathfrak{p}) = \dim(R_{\mathfrak{p}}).$$

IV.4.8 Corollary to the chain theorem. *Let k be an infinite field, $n \geq 1$ a natural number, $\mathfrak{q} \subset k[x_1, ..., x_n]$ a **prime** ideal, and*

$$R := k[x_1, ..., x_n]/\mathfrak{q}.$$

Then, for every prime ideal $\mathfrak{p} \subset R$, we have

$$\dim(R) = \dim(R/\mathfrak{p}) + \mathrm{ht}(\mathfrak{p}).$$

*In particular, if $\mathfrak{m} \subset R$ is a **maximal** ideal, then*

$$\dim(R) = \dim(R_{\mathfrak{m}}).$$

We now prove a variant of **Krull's principal ideal theorem** (see Theorem IV.5.6) for $k[x_1, ..., x_n]$. If $Z \subset \mathbb{A}^n_k$ is an algebraic set, we define

$$\dim(Z) := \dim(k[Z])$$

to be the *dimension* of Z.

IV.4.9 Proposition. *Let k be an algebraically closed field, $n \geq 1$ a natural number, $I \subset k[x_1, ..., x_n]$ a radical ideal, and*

$$V(I) = V_1 \cup \cdots \cup V_s$$

the decomposition into irreducible components. Then, the following conditions are equivalent:

i) *The ideal I is a principal ideal.*

ii) *For $i = 1, ..., s$, one has $\dim(V_i) = n - 1$.*

Proof. One reduces immediately to $s = 1$, i.e., to the case when I is a prime ideal.

"i)$\Longrightarrow$ii)". This is again an application of Noether normalization for hypersurfaces III.4.4.

"ii)$\Longrightarrow$i)". Since I is a prime ideal, we may apply Corollary IV.4.8. The assumption is equivalent to $\mathrm{ht}(I) = 1$, i.e., $\langle 0 \rangle \subsetneq I$ is the maximal chain ending in I. As explained in the proof of Theorem IV.1.3, we may always insert a non-zero principal ideal into that chain. Therefore, I has to be a principal ideal. □

IV.4.10 Exercise (Dimension). Let k be a field, R a finitely generated k-algebra, and $\mathfrak{p}_1, ..., \mathfrak{p}_s$ the minimal prime ideals of R (see Theorem II.4.28, ii).

i) Assume that k is algebraically closed and that R is reduced. Write $R = k[x_1, ..., x_n]/I$ for a suitable natural number n and a suitable radical ideal $I \subset k[x_1, ..., x_n]$, and set $Z := V(I) \subset \mathbb{A}^n_k$. Define $\widetilde{\mathfrak{p}}_i \subset k[x_1, ..., x_n]$ as the preimage of $\mathfrak{p}_i$ under the projection $k[x_1, ..., x_n] \longrightarrow k[x_1, ..., x_n]/I$, $i = 1, ..., n$. What is the geometric significance of the varieties $V(\widetilde{\mathfrak{p}}_i) \subset \mathbb{A}^n_k$, $i = 1, ..., s$?

ii) Set $R_i := R/\mathfrak{p}_i$, $i = 1, ..., s$. Prove that

$$\dim(R) = \max\Big\{ \operatorname{trdeg}_k(Q(R_i)) \,\Big|\, i = 1, ..., s \Big\}.$$

iii) Let $S \subset R$ be a subalgebra. Prove that $\dim(S) \leq \dim(R)$.

Hint. If $p_1, ..., p_s \in R$ are algebraically independent over k, then $k[p_1, ..., p_s] \subset R$ is an integral domain.

IV.5 Krull's Principal Ideal Theorem

Let R be a ring and M an R-module. The number

$$l(M) := \sup\{\, l \in \mathbb{N} \mid \exists \text{ submodules } M_0 \subsetneq \cdots \subsetneq M_l \,\} \in \mathbb{N} \cup \{\infty\}$$

is called the *length* of M.

IV.5.1 Remarks. i) Let R be a ring. We may view R as an R-module. Then, $l(R)$ is **not** the same as $\dim(R)$. In fact, in the definition of $l(R)$, **all** ideals are used, not just the prime ideals.

ii) As Part i) already suggests, an R-module M, even a noetherian one, will usually have infinite length. In other words, modules of finite length are quite special.

IV.5.2 Example. Let k be a field and V a k-vector space. Then, $l(V) = \dim_k(V)$.

IV.5.3 Lemma. *Let R be a ring, M an R-module, and $M_0 \subsetneq \cdots \subsetneq M_l$ a **maximal** chain of submodules. Then, $l(M) = l$.*

Proof. Note that the maximality of the chain implies $M_0 = \{0\}$ and $M_l = M$. We proceed by induction on l. The case $\boldsymbol{l = 0}$ is trivial.

$\boldsymbol{l - 1 \longrightarrow l}$. Let $l' \in \mathbb{N}$ and $M'_0 \subsetneq \cdots \subsetneq M'_{l'}$ be a chain of submodules of M with $M'_0 = \{0\}$. Set

$$r := \max\Big\{ t \in \{\, 0, ..., l' \,\} \,\Big|\, M'_t \subset M_{l-1} \Big\}.$$

Then,

$$M_{l-1} + M'_i = M, \quad i = r + 1, ..., l'.$$

Observe that

$$M'_{i+1} = M'_{i+1} \cap M = M'_{i+1} \cap (M_{l-1} + M'_i) = M'_i + (M_{l-1} \cap M'_{i+1}), \quad i = r + 1, ..., l' - 1.$$

Since $M'_i \subsetneq M'_{i+1}$, we have

$$(M_{l-1} \cap M'_i) \subsetneq (M_{l-1} \cap M'_{i+1}), \quad i = r + 1, ..., l' - 1.$$

We form

$$M'_0 \subsetneq \cdots \subsetneq M'_r \subset (M_{l-1} \cap M'_{r+1}) \subsetneq (M_{l-1} \cap M'_{r+2}) \subsetneq \cdots \subsetneq (M_{l-1} \cap M'_{l'}).$$

This is a chain of length at least $l' - 1$. Since $M_0 \subsetneq \cdots \subsetneq M_{l-1}$ is a maximal chain in M_{l-1}, the induction hypothesis gives $l' - 1 \leq l - 1$, i.e., $l' \leq l$, and we are done. □

IV.5.4 Lemma. *Let R be a ring, M an R-module, and $N \subset M$ a submodule. Then,*

$$l(M) = l(N) + l(M/N).$$

Proof. If N or M/N has infinite length, then it is easy to check that M has infinite length, too. So, assume that N and M/N have finite length. Then, we have maximal sequences

$$\{0\} = N_0 \subsetneq \cdots \subsetneq N_{l(N)} = N \quad \text{and} \quad \{0\} = \overline{M}_0 \subsetneq \cdots \subsetneq \overline{M}_{l(M/N)} = M/N$$

of submodules of N and M/N, respectively. With the preimage M_i of $\overline{M}_i$ under the projection $M \longrightarrow M/N$, $i = 0, ..., l(M/N)$, we get the maximal chain

$$\{0\} = N_0 \subsetneq \cdots \subsetneq N_{l(N)} = N = M_0 \subsetneq \cdots \subsetneq M_{l(M/N)}$$

of submodules of M. Lemma IV.5.3 shows $l(M) = l(N) + l(M/N)$. □

IV.5.5 Lemma. *Let R be a noetherian local ring and M a finitely generated R-module. Then, the following holds:*

$$\dim(R/\mathrm{Ann}(M)) = 0 \quad \Longrightarrow \quad l(M) < \infty.$$

Proof. We suppose $M \neq 0$.

Step 1. Let $\mathfrak{m}$ be the maximal ideal of R and $k := R/\mathfrak{m}$. Since R and M are noetherian, $\mathfrak{m}$ is finitely generated, and, for every natural number $s \in \mathbb{N}$, $(\mathfrak{m}^s \cdot M)/(\mathfrak{m}^{s+1} \cdot M)$ is a finite dimensional k-vector space. Note, for $s \in \mathbb{N}$,

$$l((\mathfrak{m}^s \cdot M)/(\mathfrak{m}^{s+1} \cdot M)) = \dim_k((\mathfrak{m}^s \cdot M)/(\mathfrak{m}^{s+1} \cdot M))$$

and

$$l(M/(\mathfrak{m}^s \cdot M)) = \sum_{i=0}^{s-1} \dim_k((\mathfrak{m}^i \cdot M)/(\mathfrak{m}^{i+1} \cdot M)).$$

The second formula results from Lemma IV.5.4.

Step 2. Let $\overline{R} := R/\mathrm{Ann}(M)$ and $\overline{\mathfrak{m}} \subset \overline{R}$ the image of $\mathfrak{m}$ under the surjection $R \longrightarrow \overline{R}$. Then, $\overline{R}$ is a local ring with maximal ideal $\overline{\mathfrak{m}}$. The assumption $\dim(\overline{R}) = 0$ implies that $\overline{\mathfrak{m}}$ is also a minimal prime ideal of R. Therefore, it equals the radical of $\overline{R}$ (see Proposition I.7.2). Since $\overline{\mathfrak{m}}$ is finitely generated, there is a power $s \geq 1$ with $\overline{\mathfrak{m}}^s = \langle 0 \rangle$ (compare Example I.8.8, ii), i.e.,

$$\mathfrak{m}^s \subset \mathrm{Ann}(M) \quad \text{and} \quad \mathfrak{m}^s \cdot M = \langle 0 \rangle.$$

Together with Step 1, we find our claim. □

Let R be a noetherian ring and $x \in R \setminus R^\star$. A *minimal prime ideal containing x* is a prime ideal $x \in \mathfrak{p} \subset R$ whose image $\overline{\mathfrak{p}} \subset R/\langle x \rangle$ is a minimal prime ideal.

IV.5.6 Krull's principal ideal theorem. *Let R be a noetherian ring, $x \in R \setminus R^\star$ and $\mathfrak{p} \subset R$ a minimal prime ideal containing x. Then,* $\operatorname{ht}(\mathfrak{p}) \leq 1$.

Proof. We look at the localization $R_\mathfrak{p}$. In view of Remark IV.4.7, we have to show that $\dim(R_\mathfrak{p}) \leq 1$. So, we have reduced to the case that R is a local ring and the minimal prime ideal $\mathfrak{p}$ containing x is the maximal ideal of R.

Suppose we have a chain $\mathfrak{r} \subsetneq \mathfrak{q} \subsetneq \mathfrak{p}$ of prime ideals in R. We may pass to the quotient $R/\mathfrak{r}$ and, therefore, assume that $\mathfrak{r} = \langle 0 \rangle$ and that R is an **integral domain**.

Now, we work with the localization $R \longrightarrow R_\mathfrak{q}$. We form the descending chain

$$\mathfrak{q}^{n\mathrm{ec}} + \langle x \rangle \subset R, \quad n \in \mathbb{N}, \tag{IV.9}$$

of ideals in R. We claim that this sequence becomes stationary. It gives rise to a descending chain $(\overline{\mathfrak{p}}_n)_{n\in\mathbb{N}}$ in $\overline{R} := R/\langle x \rangle$. Note that our construction implies that $\overline{R}$ is zero-dimensional and, therefore, has finite length as $\overline{R}$-module, by Lemma IV.5.5. For this reason, the sequence $(\overline{\mathfrak{p}}_n)_{n\in\mathbb{N}}$ becomes stationary. By Lemma I.2.2, this is also true for the sequence (IV.9).

Pick a natural number n_0 with

$$\mathfrak{q}^{n_0\mathrm{ec}} + \langle x \rangle = \mathfrak{q}^{n_0+1\mathrm{ec}} + \langle x \rangle.$$

In particular,

$$\mathfrak{q}^{n_0\mathrm{ec}} \subset \mathfrak{q}^{n_0+1\mathrm{ec}} + \langle x \rangle.$$

Let $r \in \mathfrak{q}^{n_0\mathrm{ec}}$. There are elements $s \in \mathfrak{q}^{n_0+1\mathrm{ec}}$ and $a \in R$ with

$$r = s + a \cdot x.$$

We infer

$$a \cdot x = r - s.$$

Since $x \notin \mathfrak{q}$, we find, using Property I.8.24, ii),

$$a = \frac{r-s}{x} \in \mathfrak{q}^{n_0\mathrm{ece}} \cap R = \mathfrak{q}^{n_0\mathrm{e}} \cap R = \mathfrak{q}^{n_0\mathrm{ec}}.$$

Our discussion shows

$$\mathfrak{q}^{n_0\mathrm{ec}} = \mathfrak{q}^{n_0+1\mathrm{ec}} + \mathfrak{p} \cdot \mathfrak{q}^{n_0\mathrm{ec}}.$$

Using Exercise III.1.35, we find

$$\mathfrak{q}^{n_0\mathrm{ec}} = \mathfrak{q}^{n_0+1\mathrm{ec}}.$$

This yields

$$\mathfrak{q}^{n_0\mathrm{e}} = \mathfrak{q}^{n_0\mathrm{ece}} = \mathfrak{q}^{n_0+1\mathrm{ece}} = \mathfrak{q}^{n_0+1\mathrm{e}} = \mathfrak{q}^{n_0\mathrm{e}} \cdot \mathfrak{q}^{\mathrm{e}}$$

in $R_\mathfrak{q}$. Note that $\mathfrak{q}^\mathrm{e}$ is the maximal ideal of $R_\mathfrak{q}$ (Corollary II.4.7). We apply the Nakayama lemma III.1.31 once more. It gives

$$\mathfrak{q}^{n_0\mathrm{e}} = \langle 0 \rangle.$$

Since R is an integral domain, this implies that $\mathfrak{q}^{n_0} = \langle 0 \rangle$ (see Page 57) and, thus, $\mathfrak{q} = \langle 0 \rangle$. This contradicts our assumption on $\mathfrak{q}$. □

IV.5.7 Exercise (Krull's Höhensatz). Let R be a noetherian ring and $I \subsetneq R$ a proper ideal. We say that $I \subset \mathfrak{p}$ is a *minimal prime ideal containing* I, if the image $\overline{\mathfrak{p}}$ of $\mathfrak{p}$ in R/I is a minimal prime ideal of R/I.

Assume that there are $s \in \mathbb{N}$ and $a_1, ..., a_s \in R$ with $\langle a_1, ..., a_s \rangle = I$. Prove that

$$\mathrm{ht}(\mathfrak{p}) \leq s$$

for every minimal prime ideal $\mathfrak{p} \subset R$ containing I. What is the geometric interpretation of this statement?

IV.6 Embedding Dimension

Let R be a **local notherian** ring and $\mathfrak{m} \subset R$ its maximal ideal. Then,

$$\mathfrak{m}/\mathfrak{m}^2$$

is a vector space over the field $R/\mathfrak{m}$.

IV.6.1 Remark. The ideal $\mathfrak{m}$ is finitely generated, because R is a noetherian ring. Let $s \geq 1$ and $a_1, ..., a_s \in \mathfrak{m}$ be such that

$$\langle a_1, ..., a_s \rangle = \mathfrak{m}.$$

Then, the classes $[a_1], ..., [a_s] \in \mathfrak{m}/\mathfrak{m}^2$ generate $\mathfrak{m}/\mathfrak{m}^2$ as a vector space over $R/\mathfrak{m}$, i.e.,

$$\dim_{R/\mathfrak{m}}(\mathfrak{m}/\mathfrak{m}^2) \leq s.$$

The natural number

$$\mathrm{edim}(R) := \dim_{R/\mathfrak{m}}(\mathfrak{m}/\mathfrak{m}^2)$$

is called the *embedding* or *tangential dimension* of R.

IV.6.2 Proposition. *Let $a_1, ..., a_s \in \mathfrak{m}$ be elements, such that the classes $[a_1], ..., [a_s] \in \mathfrak{m}/\mathfrak{m}^2$ generate $\mathfrak{m}/\mathfrak{m}^2$ as a vector space over $R/\mathfrak{m}$. Then,*

$$\langle a_1, ..., a_s \rangle = \mathfrak{m}.$$

In particular, the embedding dimension of R equals the minimal number of generators for the maximal ideal $\mathfrak{m}$.

Proof. We look at the homomorphism

$$\begin{array}{rcl} \varphi\colon R^{\oplus s} & \longrightarrow & \mathfrak{m} \\ (r_1, ..., r_s) & \longmapsto & r_1 \cdot a_1 + \cdots + r_s \cdot a_s \end{array}$$

of R-modules. The assumption states that the induced homomorphism

$$\overline{\varphi}\colon (R/\mathfrak{m})^{\oplus s} \longrightarrow \mathfrak{m}/\mathfrak{m}^2$$

is surjective. By Lemma III.1.33, ii), φ is surjective. □

A noetherian local ring R is *regular*, if

$$\dim(R) = \operatorname{edim}(R).$$

IV.6.3 Remarks. i) Let R, S be not necessarily local rings and $\varphi\colon R \longrightarrow S$ a **surjective** homomorphism. If $\mathfrak{n} \subset S$ is a maximal ideal in S, then $\mathfrak{m} = \varphi^{-1}(\mathfrak{n})$ is a maximal ideal in R, and we have an induced surjection

$$\overline{\varphi}\colon \mathfrak{m}/\mathfrak{m}^2 \longrightarrow \mathfrak{n}/\mathfrak{n}^2.$$

ii) Let R be a not necessarily local ring, $\mathfrak{m} \subset R$ a maximal ideal, and $\varphi\colon R \longrightarrow R_{\mathfrak{m}}$ the localization. Then, $R_{\mathfrak{m}}$ is a local ring with maximal ideal $\mathfrak{n} = \mathfrak{m}^{\mathrm{e}}$. Then, by Corollary II.3.7, i),

$$\mathfrak{n}^{\mathrm{c}} = \mathfrak{m}^{\mathrm{ec}} = \mathfrak{m} \quad \text{and} \quad (\mathfrak{m}^2)^{\mathrm{ec}} = \mathfrak{m}^2.$$

It is also evident (Proposition II.3.6) that

$$(\mathfrak{m}^2)^{\mathrm{e}} = \mathfrak{n}^2.$$

Thus, we have an induced injective homomorphism

$$\overline{\varphi}\colon \mathfrak{m}/\mathfrak{m}^2 \longrightarrow \mathfrak{n}/\mathfrak{n}^2.$$

It is also clear that $\overline{\varphi}$ is surjective and, therefore, an isomorphism.

IV.6.4 Examples. i) Let k be an algebraically closed field, $n \geq 1$ a natural number, $R := k[x_1, ..., x_n]$ and $\mathfrak{m} \subset R$ a maximal ideal. Then,

$$\dim_k(\mathfrak{m}/\mathfrak{m}^2) = n.$$

This is obvious for $\mathfrak{m} = \langle\, x_1, ..., x_n \,\rangle$. In general, there is a point $(a_1, ..., a_n) \in \mathbb{A}^n_k$ with

$$\mathfrak{m} = \langle\, x_1 - a_1, ..., x_n - a_n \,\rangle,$$

and

$$\begin{array}{rcl} \varphi\colon k[x_1, ..., x_n] & \longrightarrow & k[x_1, ..., x_n] \\ x_i & \longmapsto & x_i - a_i, \quad i = 1, ..., n, \end{array}$$

is an automorphism which maps $\langle\, x_1, ..., x_n \,\rangle$ to $\mathfrak{m}$. Corollary IV.4.8 and Remark IV.6.3, ii), show that $R_{\mathfrak{m}}$ is a regular local ring of dimension n.

ii) Let k be an algebraically closed field, $n \geq 1$ a natural number, $I \subset k[x_1, ..., x_n]$ an ideal, $R := k[x_1, ..., x_n]/I$, and $\mathfrak{m} \subset R$ a maximal ideal. Then,

$$\operatorname{edim}(R_{\mathfrak{m}}) \leq n.$$

In fact, let

$$\pi\colon k[x_1, ..., x_n] \longrightarrow R$$

be the canonical surjection. There is a point $(a_1, ..., a_n) \in \mathbb{A}^n_k$ with

$$\pi(\langle\, x_1 - a_1, ..., x_n - a_n \,\rangle) = \mathfrak{m}.$$

By Remark IV.6.1,

$$\dim(\mathfrak{m}/\mathfrak{m}^2) \leq n.$$

The contention follows now from Remark IV.6.3, ii). This gives (a partial) explanation for the name embedding dimension: Given an affine variety X with coordinate algebra $R := k[X]$, k an algebraically closed field. Then, the maximum[7] of the embedding dimensions of the localizations of R at all maximal ideals is a lower bound for the minimal number n, such that X can be embedded into $\mathbb{A}^n_k$.

IV.7 Singular Points of Algebraic Varieties

We now work over an **algebraically closed field** k. Fix a natural number $n \geq 1$, and a **radical** ideal $I \subset k[x_1, ..., x_n]$. Define

$$Z := V(I) \subset \mathbb{A}^n_k$$

as the corresponding algebraic set and

$$R := k[x_1, ..., x_n]/I$$

as its coordinate algebra. According to Exercise III.3.2, the assignment

$$a \longmapsto \mathfrak{m}_a := \{\, f \in R \mid f(a) = 0 \,\}$$

establishes a bijection between $V(I)$ and the set of maximal ideals of the k-algebra R.

We say that $a \in Z$ is a *regular point* of Z or that Z is *non-singular* at a, if $R_{\mathfrak{m}_a}$ is a regular local ring. Otherwise, we say that a is a *singular point* of Z or that Z is *singular* at a. The k-vector space

$$T_a Z := \mathrm{Hom}_k(\mathfrak{m}_a/\mathfrak{m}_a^2, k)$$

is the *Zariski tangent space* of Z at a. Observe that it is defined intrinsically in terms of the coordinate algebra of Z, i.e., without reference to the embedding $Z \subset \mathbb{A}^n_k$.

A *derivation* of R at a is a ***k*-linear** map

$$t\colon R \longrightarrow k$$

which satisfies the **Leibniz**[8] **rule**

$$\forall f, g \in R: \quad t(f \cdot g) = t(f) \cdot g(a) + f(a) \cdot t(g).$$

The space

$$\mathrm{Der}_a(R) := \{\, t \in \mathrm{Hom}_k(R, k) \mid t \text{ is a derivation at } a \,\}$$

of all derivations of R at a is a sub vector space of $\mathrm{Hom}_k(R, k)$.

Now, suppose $t\colon R \longrightarrow k$ is a derivation of R at a. We find

$$t(1) = t(1 \cdot 1) = 2 \cdot t(1).$$

[7] The above discussion shows that this maximum exists. In fact, it is bounded by m, if $X \subset \mathbb{A}^m_k$.

[8] Gottfried Wilhelm von Leibniz (1646 - 1716), German mathematician and philosopher.

This implies $t(1) = 0$ and, by k-linearity,

$$\forall \lambda \in k: \quad t(\lambda) = 0. \tag{IV.10}$$

Note that

$$\begin{array}{rcl} F: R & \longrightarrow & k \oplus \mathfrak{m}_a \\ f & \longmapsto & \big(f(a), f - f(a)\big) \end{array}$$

is an isomorphism of k-vector spaces. By (IV.10), t is determined by its restriction to $\mathfrak{m}_a$. Next, let $f, g \in \mathfrak{m}_a$. Then,

$$t(f \cdot g) = t(f) \cdot g(a) + f(a) \cdot t(g) = 0.$$

Thus, $t_{|\mathfrak{m}_a}$ factorizes over a k-linear map

$$\overline{t}: \mathfrak{m}_a/\mathfrak{m}_a^2 \longrightarrow k.$$

IV.7.1 Proposition. *The map*

$$\begin{array}{rcl} H: \mathrm{Der}_a(R) & \longrightarrow & T_aZ = \mathrm{Hom}_k(\mathfrak{m}_a/\mathfrak{m}_a^2, k) \\ t & \longmapsto & \overline{t} \end{array}$$

is an isomorphism of k-vector spaces.

Proof. The injectivity and k-linearity are clear from the definition and the above discussion. Now, suppose we are given $l \in \mathrm{Hom}_k(\mathfrak{m}_a/\mathfrak{m}_a^2, k)$. We set

$$\begin{array}{rcl} t: R & \longrightarrow & k \\ f & \longmapsto & l\Big(\big[f - f(a)\big]\Big). \end{array}$$

Now, let $f, g \in R$. Then,

$$(f - f(a)) \cdot (g - g(a)) \in \mathfrak{m}_a^2.$$

We now compute

$$\begin{array}{rcl} t(f \cdot g) & = & t\Big(f \cdot g - (f - f(a)) \cdot (g - g(a))\Big) \\ & = & t(f \cdot g(a) + f(a) \cdot g - f(a) \cdot g(a)) \\ & = & t(f) \cdot g(a) + f(a) \cdot t(g) - f(a) \cdot g(a) \cdot t(1) \\ & = & t(f) \cdot g(a) + f(a) \cdot t(g). \end{array}$$

So, t is a derivation of R at a with $\overline{t} = l$, i.e., H is also surjective. □

IV.7.2 Example (Taylor[9] expansion). Let $a = (a_1, ..., a_n) \in \mathbb{A}_k^n$ be a point and $\mathfrak{m} := \langle\, x_1 - a_1, ..., x_n - a_n \,\rangle \subset k[x_1, ..., x_n]$ the corresponding maximal ideal. The homomorphism

$$\begin{array}{rcl} \tau_a: k[x_1, ..., x_n] & \longrightarrow & k[x_1, ..., x_n] \\ x_i & \longmapsto & x_i - a_i, \quad i = 1, ..., n, \end{array}$$

[9] Brook Taylor (1685 - 1731), English mathematician.

is a k-linear isomorphism. So, for a polynomial $f \in k[x_1, ..., x_n]$, there exists a polynomial $T_a f \in k[x_1, ..., x_n]$ with

$$f(x_1, ..., x_n) = T_a f(x_1 - a_1, ..., x_n - a_n).$$

We call $T_a f$ the *Taylor expansion* of f at a. We have

$$T_a f(x_1 - a_1, ..., x_n - a_n) = f(a) + \sum_{i=1}^{n} \delta_{f,i}(a) \cdot (x_i - a_i) + \text{higher order terms.}$$

The vector space $\mathfrak{m}_a/\mathfrak{m}_a^2$ has the basis $[x_1 - a_1]$, ..., $[x_n - a_n]$. Let $l_1, ..., l_n$ be the dual basis of $\mathrm{Hom}_k(\mathfrak{m}_a/\mathfrak{m}_a^2, k)$. Then,

$$\forall f \in k[x_1, ..., x_n]: \quad l_i(f) = \delta_{f,i}(a).$$

On the other hand, we may define the **partial derivatives**

$$\frac{\partial f}{\partial x_i} \in k[x_1, ..., x_n], \quad i = 1, ..., n,$$

by formally applying the rules we know from analysis ([28], Kapitel 5). Then, one finds

$$\delta_{f,i}(a) = \frac{\partial f}{\partial x_i}(a), \quad i = 1, ..., n. \tag{IV.11}$$

In fact, for $i \in \{1, ..., n\}$, the operators $\delta_{\cdot,i}(a)$ and $(\partial/\partial x_i)(a)$ are both k-linear and satisfy the **Leibniz rule**, i.e., for $f, g \in k[x_1, ..., x_n]$,

$$\delta_{f\cdot g,i}(a) = \delta_{f,i}(a) \cdot g(a) + f(a) \cdot \delta_{g,i}(a) \quad \text{and} \quad \frac{\partial(f \cdot g)}{\partial x_i}(a) = \frac{\partial f}{\partial x_i}(a) \cdot g(a) + f(a) \cdot \frac{\partial g}{\partial x_i}(a).$$

For this reason, it is enough to check (IV.11) for constant polynomials and the polynomials $x_1, ..., x_n$. For all of these, (IV.11) is trivial.

IV.7.3 Remark. In principle, we could try to compute the Taylor expansion also up to higher orders. Here, we have to be a little cautious: The usual Taylor formula ([28], Satz 7.2.2, [4], Kapitel I, Satz (2.9)) requires division by natural numbers of the form $l_1! \cdot \cdots \cdot l_n!$ with $l_1 + \cdots + l_n = l$ in the term of order l. So, the characteristic of our base field k must be larger than l, if we would like to have the usual formula for the term of order l in the Taylor expansion. If we allow, as we do, fields of characteristic 2, it makes only sense to look at the linear terms of the Taylor expansion.

Now, let $g_1, ..., g_s \in k[x_1, ..., x_n]$ be such that $I = \langle g_1, ..., g_s \rangle$. For every derivation $D\colon R \longrightarrow k$ at a, the composition

$$\widetilde{D}\colon k[x_1, ..., x_n] \xrightarrow{\pi} R \xrightarrow{D} k$$

is a derivation of $k[x_1, ..., x_n]$ at a.

IV.7.4 Lemma. *A derivation $\widetilde{D}\colon k[x_1, ..., x_n] \longrightarrow k$ at a factorizes over a derivation $D\colon R \longrightarrow k$ of R at a if and only if*

$$\forall i \in \{1, ..., s\}: \quad \widetilde{D}(g_i) = 0.$$

Proof. The implication "$\Longrightarrow$" is trivial. For the converse, we have to show that $\widetilde{D}$ vanishes on all elements of I. An element of I has the form $f_1 \cdot g_1 + \cdots + f_s \cdot g_s$ for suitable polynomials $f_1, ..., f_s \in k[x_1, ..., x_n]$. Since a derivation is a k-linear, it suffices to look at elements of the shape $f \cdot g_i$, $f \in k[x_1, ..., x_n]$, $i \in \{1, ..., s\}$. For such an element we have

$$\widetilde{D}(f \cdot g_i) = \widetilde{D}(f) \cdot g_i(a) + f(a) \cdot \widetilde{D}(g_i) = 0.$$

Indeed, the first summand vanishes, because $a \in V(I) \subset V(g_i)$ and the second one by assumption. □

Example IV.7.2 and Lemma IV.7.4 give the following description of the tangent space of a variety at a point.

IV.7.5 Proposition. *Let $I = \langle g_1, ..., g_s \rangle \subset k[x_1, ..., x_n]$ be an ideal, $R := k[x_1, ..., x_n]/I$, $Z := V(I)$, and $a = (a_1, ..., a_n) \in Z$. Then,*

$$T_a Z \cong \left\{ (t_1, ..., t_n) \in k^n \;\middle|\; \sum_{j=1}^{n} t_j \cdot \frac{\partial g_i}{\partial x_j}(a) = 0,\ i = 1, ..., s \right\}.$$

In the situation of Proposition IV.7.5, set $G := (g_1, ..., g_s)$. The matrix

$$J_G := \left(\frac{\partial g_i}{\partial x_j} \right)_{\substack{i=1,...,s \\ j=1,...,n}} \in \mathrm{Mat}(s, n, k[x_1, ..., x_n])$$

is the *Jacobian matrix* of the ordered tuple G of polynomials. Putting everything together, we find the following result.

IV.7.6 Proposition (Jacobian criterion)**.** *Let $I = \langle g_1, ..., g_s \rangle \subset k[x_1, ..., x_n]$ be an ideal, $R := k[x_1, ..., x_n]/I$, $Z := V(I)$, and $a = (a_1, ..., a_n) \in Z$. Then,*

$$\mathrm{edim}(R_{\mathfrak{m}_a}) = n - \mathrm{rk}(J_G(a)), \quad J_G(a) := \left(\frac{\partial g_i}{\partial x_j}(a) \right)_{\substack{i=1,...,s \\ j=1,...,n}} \in \mathrm{Mat}(s, n, k).$$

Moreover, if all the irreducible components of Z have the same dimension, $R_{\mathfrak{m}_a}$ is a regular local ring if and only if

$$\mathrm{rk}(J_G(a)) = n - \dim(Z).$$

The reader should compare this with the corresponding result in real analysis ([28], Abschnitt 11.2). Given a set of elements $g_1, ..., g_s \in k[x_1, ..., x_n]$, it is not obvious what the dimension of $V(g_1, ..., g_s)$ is. However, if $s = 1$, we know from Proposition IV.4.9 that it is $n - 1$. In this case, the Jacobian criterion is easy to check. For $g \in k[x_1, ..., x_n] \setminus \{0\}$, the hypersurface $V(g)$ is non-singular at $a \in V(g)$ if and only if there is at least one index $j \in \{1, ..., n\}$ with $(\partial g/\partial x_j)(a) \neq 0$.

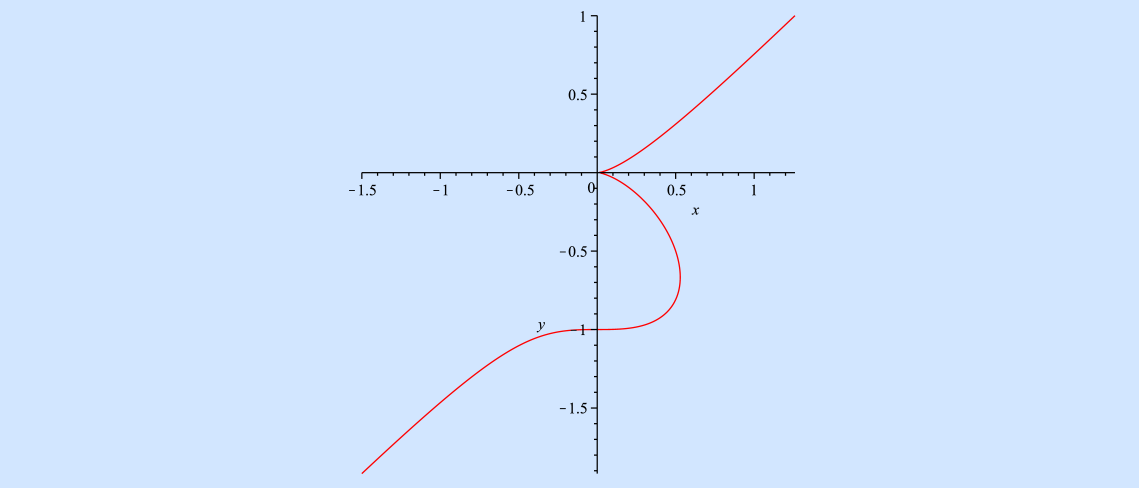
IV.7.7 Examples. i) We define the curve

$$Z := V(x^3 - y^2 - y^3) \subset \mathbb{A}^2_{\mathbb{C}}$$

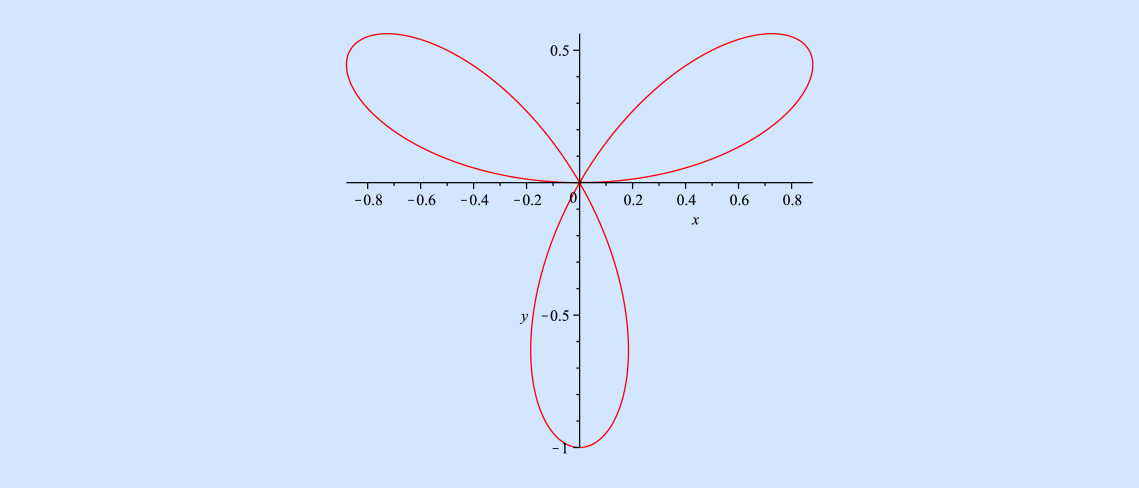
and compute the partial derivatives of $f := x^3 - y^2 - y^3$:

$$\frac{\partial f}{\partial x} = 3x^2, \quad \frac{\partial f}{\partial y} = -y \cdot (2 + 3y).$$

They both vanish at $(0, 0)$ and $(0, -2/3)$. The second point does not lie on Z. So, Z has exactly one singular point at the origin.



ii) Set $f := y \cdot (3x^2 - y^2) - (x^2 + y^2)^2$ and $Z := V(f) \subset \mathbb{A}^2_{\mathbb{C}}$. This is a **clover leaf**.



The partial derivatives are

$$\frac{\partial f}{\partial x} = 6xy - 4x \cdot (x^2 + y^2), \quad \frac{\partial f}{\partial y} = 3x^2 - 3y^2 - 4y \cdot (x^2 + y^2).$$

We look at points where both partial derivatives vanish. These points verify the equation

$$0 = 3x^3 - 3xy^2 - 6xy^2 = 3x \cdot (x^2 - 3y^2).$$

This gives $x = 0$ or $x = \pm\sqrt{3} \cdot y$. In the first case, we must also have $-y^2 \cdot (3 + 4y) = 0$, that is, $y = 0$ or $y = -3/4$. The origin $(0, 0)$ is a singular point of Z, but $(0, -3/4)$ does not belong to the curve. In the second case, we plug the result into the second derivative:

$$0 = 9y^2 - 3y^2 - 4y \cdot 4y^2 = 2y^2 \cdot (3 - 8y).$$

So, $y = 0$ and $x = 0$, or $y = 3/8$ and $x = 3 \cdot \sqrt{3}/8$. The point $(3 \cdot \sqrt{3}/8, 3/8)$ does not lie on the curve.

iii) We look at **Cayley's ruled surface**

$$Z := V(x_1^2 x_3 + x_2^3 + x_1 x_2) \subset \mathbb{A}^3_{\mathbb{C}}.$$

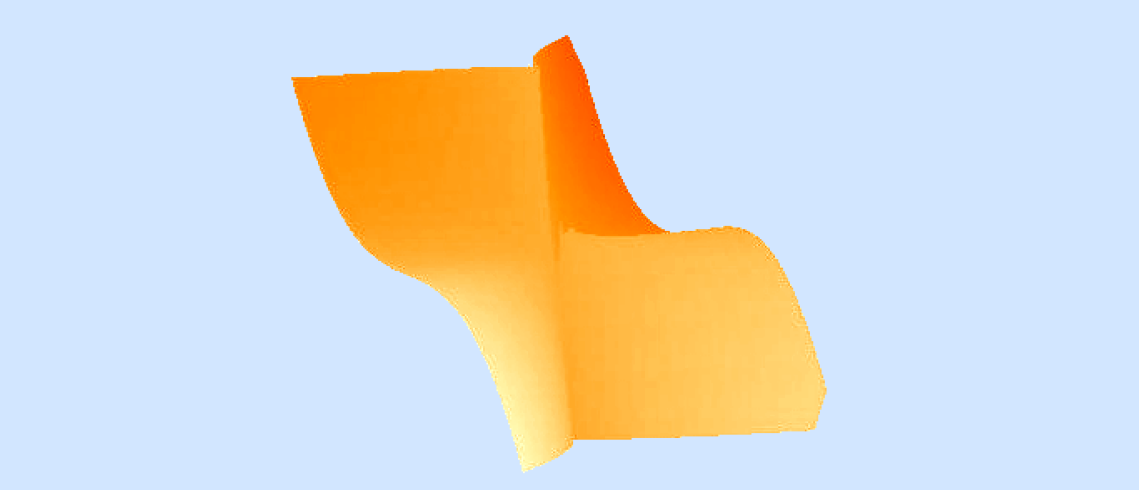
The partial derivatives of $f := x_1^2 x_3 + x_2^3 + x_1 x_2$ are

$$\frac{\partial f}{\partial x_1} = 2x_1 x_3 + x_2, \quad \frac{\partial f}{\partial x_2} = 3x_2^2 + x_1, \quad \frac{\partial f}{\partial x_3} = x_1^2.$$

They all vanish on the line

$$l := \{\, x_1 = 0 = x_2 \,\} \subset Z.$$

In other words, Z is singular along the line l.



Let us add a simple example which is not a hypersurface.

IV.7.8 Example (The twisted cubic[10]). We look at the regular map

$$\begin{array}{rcl} \varphi\colon \mathbb{A}^1_k & \longrightarrow & \mathbb{A}^3_k \\ t & \longmapsto & (t, t^2, t^3). \end{array}$$

The points in the image clearly satisfy the equations[11]

$$x^2 - y = 0, \quad x^3 - z = 0, \quad y^3 - z^2 = 0.$$

Set $g_1 := x^2 - y$, $g_2 := x^3 - z$, $g_3 := y^3 - z^2$, $I := \langle\, g_1, g_2, g_3 \,\rangle$, and $Z := V(I)$. The map

$$\begin{array}{rcl} \psi\colon Z & \longrightarrow & \mathbb{A}^1_k \\ (x, y, z) & \longmapsto & x \end{array}$$

[10] In this example, we will slightly abuse notation, by not distinguishing between coordinate functions and coordinates.

[11] The third one being redundant.

is inverse to φ. Let us determine the corresponding homomorphisms of algebras (Exercise I.9.8):

$$\begin{array}{rcl} \varphi^{\#}\colon k[x,y,z]/I & \longrightarrow & k[t] \\ [x] & \longmapsto & t \\ [y] & \longmapsto & t^2 \\ [z] & \longmapsto & t^3 \end{array}$$

and

$$\begin{array}{rcl} \psi^{\#}\colon k[t] & \longrightarrow & k[x,y,z]/I \\ t & \longmapsto & [x]. \end{array}$$

So, the varieties $\mathbb{A}^1_k$ and Z are isomorphic and one dimensional. In particular, Z is non-singular. Let us check this with the Jacobian criterion:

$$J_G = \begin{pmatrix} 2x & -1 & 0 \\ 3x^2 & 0 & -1 \\ 0 & 3y^2 & -2z \end{pmatrix}.$$

This matrix has everywhere rank at least two. We add $(3y^2)\times$ the first line and $(-2z)\times$ the second line to the last line and find

$$(6x \cdot (y^2 - xz)\ 0\ 0).$$

This vanishes at every point of Z. So, the matrix has, in fact, rank two at every point of Z.[12]

IV.7.9 Lemma. *Let k be an algebraically closed field, $n \geq 1$, $f \in k[x_1, ..., x_n]$ an **irreducible** polynomial, and $Z := V(f) \subset \mathbb{A}^n_k$. Then,*

$$\mathrm{Sing}(Z) := \{\, a \in Z \mid Z \text{ is singular at } a \,\}$$

*is a **proper** Zariski closed subset of Z.*

Proof. By the Jacobian criterion IV.7.6, we have

$$\mathrm{Sing}(Z) = V\left(f, \frac{\partial f}{\partial x_1}, ..., \frac{\partial f}{\partial x_n}\right).$$

This shows that $\mathrm{Sing}(Z)$ is Zariski closed in Z. Assume $Z = \mathrm{Sing}(Z)$. This means

$$V(f) \subset V\left(\frac{\partial f}{\partial x_i}\right),$$

i.e.,

$$f \Big| \frac{\partial f}{\partial x_i}, \quad i = 1, ..., n,$$

[12] The fact that the rank of J_G can never be three at a point of Z follows, indeed, from Theorem IV.7.16, ii).

by the lemma of Study III.3.11. Since $\deg(\partial f/\partial x_i) < \deg(f)$, this is only possible if

$$\frac{\partial f}{\partial x_i} = 0, \quad i = 1, ..., n. \tag{IV.12}$$

In characteristic zero, it follows that f is constant. But, this is ruled out by the assumption that f be irreducible.

If $\mathrm{char}(k) = p > 0$, then (IV.12) implies that f is a polynomial in $x_1^p, ..., x_n^p$. The field k is perfect, because it is algebraically closed (Example III.5.6, iii). So, we may find a polynomial $g \in k[x_1, ..., x_n]$ with

$$f = g^p.$$

Again, this contradicts the assumption that f be irreducible. □

We would like to extend this result to arbitrary varieties. For this, we need some preparations.

Semicontinuity of the embedding dimension

Let R be a ring, $r, s \in \mathbb{N}$, $M \in \mathrm{Mat}(r, s, R)$ an $(r \times s)$-matrix with coefficients in R, and $1 \leq t \leq \min\{ r, s \}$. A *$t$-minor* of M is the determinant of a $(t \times t)$-matrix which is obtained from M by deleting $r-t$ rows and $s-t$ columns. It is an element of R and can be expressed as a polynomial with integer coefficients in the entries of M. Recall the following basic result from linear algebra ([7], 3.3.6, Satz):

IV.7.10 Lemma. *Let K be a field, $r, s \in \mathbb{N}$, $M \in \mathrm{Mat}(r, s, K)$, and $1 \leq t \leq \min\{ r, s \}$. Then, the rank of the matrix M is at least t if and only if it has a non-vanishing t-minor.*

Now, let k be an algebraically closed field, $n \geq 1$, $I \subset k[x_1, ..., x_n]$ a radical ideal, $R := k[x_1, ..., x_n]/I$, $Z := V(I) \subset \mathbb{A}_k^n$, and

$$M = (f_{ij})_{\substack{i=1,...,r \\ j=1,...,s}} \in \mathrm{Mat}(r, s, R).$$

For every point $a \in Z$, we obtain the matrix

$$M(a) := (f_{ij}(a))_{\substack{i=1,...,r \\ j=1,...,s}} \in \mathrm{Mat}(r, s, k).$$

For $t \in \{ 1, ..., \min\{ r, s \} \}$, a t-minor of M is a regular function on Z, i.e., an element of R.

IV.7.11 Exercises. i) Let $a \in Z$ be a point and $t := \mathrm{rk}(M(a))$. Show that there is a Zariski open subset $a \in U \subset Z$, such that

$$\forall a \in U : \quad \mathrm{rk}(M(a)) \geq t.$$

ii) Show that there are a non-empty Zariski open subset $\emptyset \neq U \subset Z$ and a natural number $t \in \{ 0, ..., \min\{ r, s \} \}$, such that

$$\forall a \in U : \quad \mathrm{rk}(M(a)) = t$$

and

$$\forall a \in Z : \quad \mathrm{rk}(M(a)) \leq t.$$

Suppose $g_1, ..., g_l \in k[x_1, ..., x_n]$ generate I and set $G := (g_1, ..., g_l)$. Then, the above discussion can be applied to the Jacobian matrix J_G. An immediate consequence of Exercise IV.7.11 is:

IV.7.12 Proposition. *There are a non-empty Zariski open subset $\emptyset \neq U \subset Z$ and a natural number $t \in \{ n - \min\{ l, n \}, ..., n \}$, such that*

$$\forall a \in U : \quad \operatorname{edim}(R_{\mathfrak{m}_a}) = t, \quad \mathfrak{m}_a = \{ f \in R \mid f(a) = 0 \},$$

and

$$\forall a \in Z : \quad \operatorname{edim}(R_{\mathfrak{m}_a}) \geq t.$$

We will see later (Theorem IV.7.16) that $t = \dim(Z)$.

Principal open subsets

Let k be an algebraically closed field, $n \geq 1$, and $f \in k[x_1, ..., x_n] \setminus \{0\}$. Then, we call

$$D(f) := \mathbb{A}^n_k \setminus V(f)$$

the *principal open subset associated with f* (compare Exercise I.4.18).

IV.7.13 Remark. Let $U \subset \mathbb{A}^n_k$ be a non-empty Zariski open subset. Then, there is a non-zero ideal $I \subset k[x_1, ..., x_n]$ with $\mathbb{A}^n_k \setminus U = V(I)$. Pick $f \in I \setminus \{0\}$. According to Property I.9.1, iv), $V(I) \subset V(f)$, and, therefore,

$$D(f) \subset U.$$

IV.7.14 Exercise. Let $U \subset \mathbb{A}^n_k$ be a non-empty Zariski open subset. Prove that there are finitely many elements $f_1, ..., f_s \in k[x_1, ..., x_n] \setminus \{0\}$ with

$$U = D(f_1) \cup \cdots \cup D(f_s).$$

The regular function f doesn't vanish anywhere on $D(f)$. For this reason, we consider

$$k[x_1, ..., x_n]_f$$

as the **algebra of regular functions** on $D(f)$. There is an even better justification for doing this: The homomorphisms

$$\begin{aligned} \varphi \colon k[x_1, ..., x_{n+1}]/\langle x_{n+1} \cdot f - 1 \rangle &\longrightarrow k[x_1, ..., x_n]_f \\ x_i &\longmapsto x_i, \quad i = 1, ..., n \\ x_{n+1} &\longmapsto \frac{1}{f} \end{aligned}$$

and

$$\begin{aligned} \psi \colon k[x_1, ..., x_n]_f &\longrightarrow k[x_1, ..., x_{n+1}]/\langle x_{n+1} \cdot f - 1 \rangle \\ x_i &\longmapsto x_i, \quad i = 1, ..., n \\ \frac{1}{f} &\longmapsto x_{n+1} \end{aligned}$$

are inverse to each other. Now, the algebra $k[x_1, ..., x_{n+1}]/\langle x_{n+1} \cdot f - 1\rangle$ is attached to the hypersurface

$$V(x_{n+1} \cdot f - 1) \subset \mathbb{A}_k^{n+1}.$$

This hypersurface is the graph of the function

$$\begin{array}{rcl} D(f) & \longrightarrow & \mathbb{A}_k^1 \\ a & \longmapsto & \dfrac{1}{f(a)}. \end{array}$$

The projection

$$\begin{array}{rcl} \pi\colon \mathbb{A}_k^{n+1} & \longrightarrow & \mathbb{A}_k^n \\ (a_1, ..., a_{n+1}) & \longmapsto & (a_1, ..., a_n) \end{array}$$

induces a homeomorphism between $V(x_{n+1} \cdot f - 1)$ and $D(f)$. In this way, we may view $D(f)$ as an affine algebraic variety. The inclusion

$$D(f) \subset \mathbb{A}_k^n$$

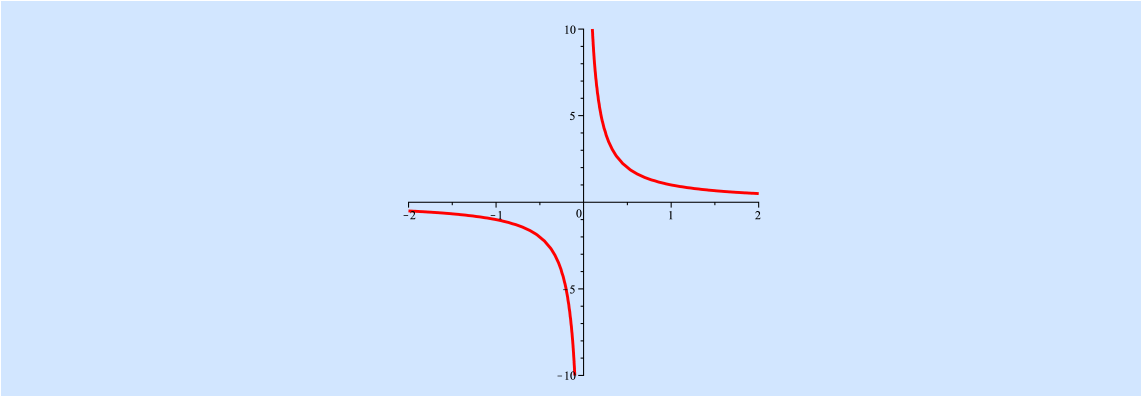
corresponds to the localization homomorphism

$$k[x_1, ..., x_n] \longrightarrow k[x_1, ..., x_n]_f.$$

IV.7.15 Example. Look at

$$D(x) = \mathbb{A}_k^1 \setminus \{0\} \subset \mathbb{A}_k^1.$$

The above construction embeds $\mathbb{A}_k^1 \setminus \{0\}$ as a hyperbola into $\mathbb{A}_k^2$.



The same thing can be done for every algebraic variety. Indeed, let $\mathfrak{p} \subset k[x_1, ..., x_n]$ be a prime ideal, $R := k[x_1, ..., x_n]/\mathfrak{p}$, and $Z = V(\mathfrak{p})$. For $f \in R \setminus \{0\}$,

$$D(f) := Z \setminus V(f)$$

is a non-empty open subset. By Property I.9.1, iv), and Exercise III.3.2, its points are in one-to-one correspondence with the maximal ideals $\mathfrak{m} \subset R$, such that

$$f \notin \mathfrak{m}. \tag{IV.13}$$

The set $D(f)$ inherits a topology from the Zariski topology of Z (compare [18], Section 2.1). On the other hand, R_f is a finitely generated k-algebra, and thus defines an affine algebraic variety Z_f. By Corollary II.3.7, ii), the points of Z_f correspond to the maximal ideals of R, satisfying (IV.13). Again, Z_f comes with a topology. The reader should check that both topologies on the set of maximal ideals of R, satisfying (IV.13), thus obtained do agree and that the localization $R \longrightarrow R_f$ gives (via Exercise I.9.8) rise to the inclusion $D(f) \subset Z$.

The singular locus of an algebraic variety

IV.7.16 Theorem. *Let k be an algebraically closed field, $n \geq 1$, $\mathfrak{p} \subset k[x_1, ..., x_n]$ a **prime** ideal, $S := k[x_1, ..., x_n]/\mathfrak{p}$, and $Z := V(\mathfrak{p})$.*

i) *The singular locus*

$$\mathrm{Sing}(Z) := \{\, a \in Z \mid Z \text{ is singular at } a \,\}$$

is a proper Zariski closed subset of Z.

ii) *For every point $a \in Z$, we have*

$$\mathrm{edim}(S_{\mathfrak{m}_a}) \geq \dim(Z).$$

Proof. We will reduce to the case of a hypersurface (Lemma IV.7.9). In fact, we will show that Z looks almost everywhere like a hypersurface. This is basically a consequence of the theorem of the primitive element III.5.10.

Let $L := Q(S)$ be the quotient field of S. The proof of Theorem III.5.14 shows that there is an injective homomorphism

$$\varphi\colon k[t_1, ..., t_s] \longrightarrow L,$$

such that the induced field extension

$$\widetilde{\varphi}\colon K := k(t_1, ..., t_s) \longrightarrow L$$

is separable. Now, there are elements $g_1, ..., g_s, h_1, ..., h_s \in S \setminus \{0\}$ with

$$\varphi(t_i) = \frac{g_i}{h_i}, \quad i = 1, ..., s.$$

By the theorem of the primitive element III.5.10, we may find $g_{s+1}, h_{s+1} \in S \setminus \{0\}$, such that

$$\alpha := \frac{g_{s+1}}{h_{s+1}}$$

is a primitive element for the field extension $K \subset L$. Set $h := h_1 \cdot \cdots \cdot h_s \cdot h_{s+1}$. Then, we may view φ as a homomorphism:

$$\varphi\colon k[t_1, ..., t_s] \longrightarrow S_h.$$

As a k-algebra, S_h is generated by $\xi_1 := [x_1], ..., \xi_n := [x_n]$, and $\xi_{n+1} := 1/h$. Since $K \longrightarrow L$ is a finite ring extension, these elements are integral over K, i.e., we find natural numbers $s_i \geq 1$ and elements $\varkappa_1^i, ..., \varkappa_{s_i}^i \in K$ with

$$\xi_i^{s_i} + \varkappa_1^i \cdot \xi_i^{s_i - 1} + \cdots + \varkappa_{s_i - 1}^i \cdot \xi_i + \varkappa_{s_i}^i = 0, \quad i = 1, ..., n + 1.$$

Now, there are elements $\alpha^i_j \in k[t_1, ..., t_s]$ and $\beta^i_j \in k[t_1, ..., t_s] \setminus \{0\}$ with

$$\varkappa^i_j = \frac{\alpha^i_j}{\beta^i_j}, \quad j = 1, ..., s_i,\ i = 1, ..., n+1.$$

Setting

$$g := \prod_{i=1}^{n+1} \prod_{j=1}^{s_i} \beta^i_j,$$

we find a **finite** ring extension

$$\widehat{\varphi}\colon k[t_1, ..., t_s]_g \longrightarrow (S_h)_g = S_{g\cdot h}$$

which induces $K \longrightarrow L$.[13] Recall that, by our construction, there is a primitive element $\alpha \in S_{g\cdot h}$. Let $\Delta \in k[t_1, ..., t_s]_g$ be as in Theorem III.5.12. We find a natural number $t \in \mathbb{N}$ and an element $\Delta' \in k[t_1, ..., t_s]$, such that

$$\Delta = \frac{\Delta'}{g^t}.$$

We see that

$$S_{g\cdot h\cdot \Delta'} = (S_{g\cdot h})_{\Delta'} = k[t_1, ..., t_s]_{g\cdot\Delta}[\alpha] = k[t_1, ..., t_s]_{g\cdot\Delta}[t_{s+1}]/\langle \mu_\alpha \rangle.$$

The minimal polynomial μ_α of α has coefficients in $k[t_1, ..., t_s]_g$ (see Lemma III.5.11, ii). We may find a polynomial $\gamma \in k[t_1, ..., t_s]$ whose irreducible factors are among those of g and Δ', such that $f := \gamma \cdot \mu_\alpha \in k[t_1, ..., t_s, t_{s+1}]$ is an irreducible polynomial (compare Lemma I.6.16, i). Let

$$H := V(f) \subset \mathbb{A}^{s+1}_k.$$

This is an irreducible hypersurface, and

$$H_0 := H \setminus V(g \cdot \Delta')$$

is a dense open subset of H. By construction, H_0 is isomorphic to the dense open subset

$$Z_0 := Z \setminus V(g \cdot h \cdot \Delta')$$

of Z. Lemma IV.7.9 yields that there is a dense open subset $U \subset Z$ with

$$\mathrm{Sing}(Z) \subset Z \setminus U.$$

By the previous discussion, the rank of the Jacobian is everywhere at most

$$t := n - \dim(Z),$$

and the locus where it is strictly less than t is the vanishing locus of all $(t \times t)$-minors of the Jacobian. But this is also the singular locus of Z. This proves all the claims about the singular locus. The statement on the embedding dimension follows from this and the Jacobian criterion IV.7.6. □

[13] By Exercise III.4.10, you should be familiar with this argument.

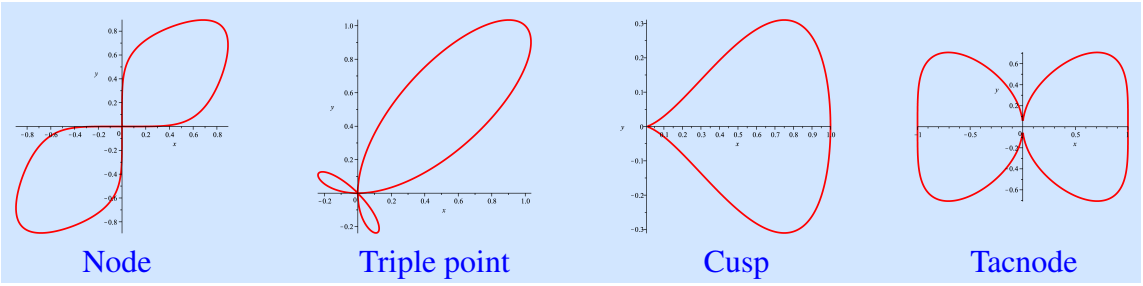
IV.7.17 Remark. In the above proof, we have shown that any algebraic variety has an open subset which is isomorphic to an open subset of an irreducible hypersurface. You will usually find this result in the form (see, e.g., [11], Proposition I.4.9)

Any algebraic variety is birationally equivalent to a hypersurface.

IV.7.18 Exercise (Singular and non-singular points I). i) Compute the Jacobian for the following regular functions $f\colon \mathbb{C}^2 \longrightarrow \mathbb{C}$. Which points are non-singular by the "Jacobian criterion"? Find out which equation gives which curve in the following picture. Try to explain why the remaining points really are singular.

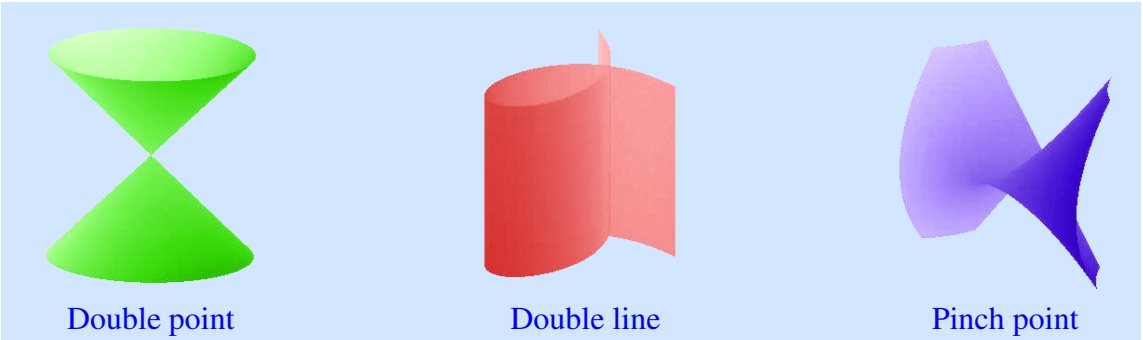
a) $f(x,y) = x^2 - x^4 - y^4$, b) $f(x,y) = xy - x^6 - y^6$, c) $f(x,y) = x^3 - y^2 - x^4 - y^4$,

d) $f(x,y) = x^2y + xy^2 - x^4 - y^4$.



ii) Do the same as in i) for the following regular functions $f\colon \mathbb{C}^3 \longrightarrow \mathbb{C}$.

a) $f(x,y,z) = xy^2 - z^2$, b) $f(x,y,z) = x^2 + y^2 - z^2$, c) $f(x,y,z) = xy + x^3 + y^3$.



IV.7.19 Exercise (Singular and non-singular points II). Let k be an algebraically closed field and $R := k[x,y,z]/\langle xyz, z^2\rangle$.

i) Is the ring R reduced?

ii) Sketch the "variety" associated with R.

iii) Determine $\dim(R)$.

iv) For which maximal ideals $\mathfrak{m} \subset R$ is $R_{\mathfrak{m}}$ a regular local ring?

IV.8 Regularity and Normality

IV.8.1 Lemma. *Let R be a noetherian ring, $l \in \mathbb{N}$ a natural number, $\mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_l$ a chain of prime ideals, $\mathfrak{q} \supset \mathfrak{p}_l$ a prime ideal, and $x \in \mathfrak{q}$. There exists a chain*

$$\mathfrak{p}'_0 \subsetneq \cdots \subsetneq \mathfrak{p}'_{l-1} \subset \mathfrak{q}$$

of prime ideals with $x \in \mathfrak{p}'_0$.

Proof. ***l* = 1.** Here, we simply take $\mathfrak{p}'_0 := \mathfrak{q}$.

***l* − 1 ⟶ *l*.** If $x \in \mathfrak{p}_{l-1}$, we may apply the induction hypothesis with $\mathfrak{p}_{l-1}$ instead of $\mathfrak{q}$ to get

$$\mathfrak{p}'_0 \subsetneq \cdots \subsetneq \mathfrak{p}'_{l-2} \subset \mathfrak{p}_{l-1} \subsetneq \mathfrak{p}'_{l-1} := \mathfrak{p}_l \subset \mathfrak{q}.$$

If $x \notin \mathfrak{p}_{l-1}$, then we look at $\langle x\rangle + \mathfrak{p}_{l-2} \not\subset \mathfrak{p}_{l-1}$. Let $\overline{\mathfrak{q}} \subset R/(\langle x\rangle + \mathfrak{p}_{l-2})$ be the image of $\mathfrak{q}$ in this ring. The ring $(R/(\langle x\rangle + \mathfrak{p}_{l-2}))_{\overline{\mathfrak{q}}}$ contains a minimal prime ideal $\mathfrak{s}$ (Exercise I.4.14 or Theorem II.4.28). The ideal $\mathfrak{s}$ corresponds to a prime ideal $\mathfrak{r} \subset R$ with

$$\mathfrak{p}_{l-2} \subsetneq \langle x\rangle + \mathfrak{p}_{l-2} \subset \mathfrak{r} \subset \mathfrak{q}.$$

We apply the induction hypothesis once more,[14] and find a chain

$$\mathfrak{p}'_0 \subsetneq \cdots \subsetneq \mathfrak{p}'_{l-2} \subset \mathfrak{r}$$

with $x \in \mathfrak{p}'_0$. It suffices to show that $\mathfrak{r} \subsetneq \mathfrak{q}$.

For this, we look at the integral domain $\overline{R} := R/\mathfrak{p}_{l-2}$. As usual, for an ideal $I \subset R$, we denote by $\overline{I}$ its image in $\overline{R}$. If $\mathfrak{r} = \mathfrak{q}$, then the chain

$$\langle 0\rangle \subsetneq \overline{\mathfrak{p}}_{l-1} \subsetneq \overline{\mathfrak{r}}$$

of prime ideal in $\overline{R}$ shows

$$\operatorname{ht}(\overline{\mathfrak{r}}) \geq 2.$$

By contruction, $\overline{\mathfrak{r}}$ is a minimal prime ideal containing $[x]$, the class of x in $\overline{R}$. Krull's principal ideal theorem requires $\operatorname{ht}(\overline{\mathfrak{r}}) \leq 1$. This contradiction shows that, indeed, $\mathfrak{r} \subsetneq \mathfrak{q}$. □

The following lemma provides an important tool for carrying out inductions on the Krull dimension of a ring.

IV.8.2 Lemma. *Let R be a noetherian local ring with maximal ideal $\mathfrak{m}$ and $x \in \mathfrak{m}$ not a zero divisor. Then,*

$$\dim(R/\langle x\rangle) = \dim(R) - 1.$$

Proof. We may apply Lemma IV.8.1 to a maximal chain $\mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_n = \mathfrak{m}$, $n = \dim(R)$, of prime ideals in R, and $\mathfrak{q} = \mathfrak{m}$. It shows

$$\dim(R/\langle x\rangle) \geq \dim(R) - 1.$$

[14] namely to the chain $\mathfrak{u}_0 \subsetneq \cdots \subsetneq \mathfrak{u}_{l-1}$ with $\mathfrak{u}_i = \mathfrak{p}_i$, $i = 1, ..., l-1$, $\mathfrak{u}_{l-1} := \mathfrak{r}$, and the prime ideal $\mathfrak{r}$

On the other hand, in any maximal chain $\mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_n = \mathfrak{m}$, $\mathfrak{p}_0$ is a minimal prime ideal. By assumption, x is not a zero divisor. Theorem II.4.28, iii), states that x is not contained in any minimal prime ideal of R. For this reason

$$\dim(R/\langle x\rangle) \leq \dim(R) - 1,$$

and we infer $\dim(R/\langle x\rangle) = \dim(R) - 1$ as asserted. □

IV.8.3 Proposition. *Let R be a **regular** noetherian local ring. Then, R is an integral domain.*

We will need a slight generalization of prime avoidance (Proposition II.4.17, i):

IV.8.4 Lemma. *Let R be a ring, $I, J \subset R$ ideals, and $\mathfrak{p}_1, ..., \mathfrak{p}_r \subset R$ prime ideals, such that*

$$J \not\subset I, \quad J \not\subset \mathfrak{p}_i, \quad i = 1, ..., r.$$

Then,

$$J \not\subset I \cup \mathfrak{p}_1 \cup \cdots \cup \mathfrak{p}_r.$$

Proof. We abbreviate

$$P := \mathfrak{p}_1 \cup \cdots \cup \mathfrak{p}_r.$$

If $I \subset P$, then Proposition II.4.17, i), applies directly. So, we may exclude this case. Note also that, by Proposition II.4.17, i), $J \not\subset P$. Let $x \in J \setminus I$. If $x \notin P$, we are done. Otherwise, we pick $y \in J \setminus P$ and $z \in I \setminus P$. Then, it is readily verified that $x + y \cdot z \in J \setminus (I \cup P)$. □

Proof of Proposition IV.8.3. Denote the maximal ideal of R by $\mathfrak{m}$. We proceed by induction on $n := \dim(R)$.

***n* = 0.** In this case, the regularity of R implies $\mathfrak{m} = \langle 0\rangle$ (compare Proposition IV.6.2).

***n* ⟶ *n*+1.** By Theorem II.4.28, ii), a noetherian ring has only finitely many minimal prime ideals, call them $\mathfrak{p}_1, ..., \mathfrak{p}_r$. We assume $\dim(R) = n + 1 \geq 1$, so $\mathfrak{m}$ is not a mimimal prime ideal. The Nakayama lemma III.1.31 shows that $\mathfrak{m} \neq \mathfrak{m}^2$. By Lemma IV.8.4, we may pick

$$x \in \mathfrak{m} \setminus (\mathfrak{m}^2 \cup \mathfrak{p}_1 \cup \cdots \cup \mathfrak{p}_r).$$

Note that this implies that x is not a zero divisor. Let $x_1, ..., x_n \in \mathfrak{m}$ be such that the classes $[x_1], ..., [x_n], [x]$ in $\mathfrak{m}/\mathfrak{m}^2$ form a basis for that $(R/\mathfrak{m})$-vector space. Recall from Proposition IV.6.2 that

$$\mathfrak{m} = \langle\, x_1, ..., x_n, x\,\rangle.$$

Now, we pass to the ring $\overline{R} := R/\langle x\rangle$. It is clear that

$$\operatorname{edim}(\overline{R}) = n.$$

By Lemma IV.8.2,

$$\dim(\overline{R}) = n.$$

Thus, $\overline{R}$ is also a regular ring. By induction hypothesis, it is an integral domain. This means that $\langle x\rangle$ is a prime ideal.

Let $\mathfrak{q} \subset R_{\langle x\rangle}$ be a minimal prime ideal (Exercise I.4.14 or Theorem II.4.28). Then, by Corollary II.3.7, i),

$$\langle 0\rangle \subset \mathfrak{p} := \mathfrak{q}^c \subset \langle x\rangle$$

is a minimal prime ideal of R. We will show that it has to be zero, using the Nakayama lemma III.1.31. In fact, let $z \in \mathfrak{p}$. Then, there exists an element $y \in R$ with $z = y \cdot x$. Since $x \notin \mathfrak{p}$ and $\mathfrak{p}$ is a prime ideal, it follows that $y \in \mathfrak{p}$. We have shown

$$\mathfrak{p} \subset \mathfrak{m} \cdot \mathfrak{p} \subset \mathfrak{p}.$$

As announced, the Nakayama lemma III.1.31 finishes the argument. □

IV.8.5 Exercise. Let R be a noetherian local ring. Show that

$$\dim(R) \leq \operatorname{edim}(R).$$

IV.8.6 Theorem. *Let R be a **regular** noetherian local ring. Then, R is a normal ring.*

Proof. We set up an induction on the dimension n of R as in the proof of Proposition IV.8.3. In the induction step $\boldsymbol{n \longrightarrow n+1}$, we find an element $x \in \mathfrak{m} \setminus \{0\}$, such that $R/\langle x\rangle$ is a regular noetherian local ring of dimension n. By induction hypothesis, it is normal. It remains to prove[15]

Claim. *Let R be a noetherian local integral domain with maximal ideal $\mathfrak{m}$ and $x \in \mathfrak{m}\setminus\{0\}$. If the ring $R/\langle x\rangle$ is normal, then so is the ring R.*

We form the ideal

$$I := \bigcap_{l\in\mathbb{N}} \langle x^l\rangle.$$

This ideal clearly has the property $x \cdot I = I$ and, thus, $\mathfrak{m} \cdot I = I$. The Nakayama lemma III.1.31 gives $I = \langle 0\rangle$. We conclude that, for every $r \in R \setminus \{0\}$, the number

$$l(r) := \max\{\, l \in \mathbb{N} \mid r \in \langle x^l\rangle \,\}$$

exists and that

$$r = u \cdot x^{l(r)}$$

for some element $u \in R \setminus \langle x\rangle$. Since the ring $R/\langle x\rangle$ is normal, it is an integral domain, by Proposition IV.8.3. This means that $\langle x\rangle$ is a prime ideal. Using this, we infer

$$\forall r, s \in R \setminus \{0\}: \quad l(r \cdot s) = l(r) + l(s). \tag{IV.14}$$

Let $K := Q(R)$ be the quotient field of R, $\alpha \in R$, and $\beta \in R\setminus\{0\}$, such that $s := \alpha/\beta \in K$ is integral over R. We have to show that $R = S := R[s] \subset K$. By the lying-over theorem IV.2.4, there is a prime ideal $\mathfrak{q} \subset S$ with $\mathfrak{q} \cap R = \langle x\rangle$. This implies

$$\langle x\rangle = R \cap (S \cdot x). \tag{IV.15}$$

We observe that $l(\alpha) \geq l(\beta)$. To see this, let $\gamma, \delta \in R \setminus \langle x\rangle$ be elements with $\alpha = \gamma \cdot x^{l(\alpha)}$ and $\beta = \delta \cdot x^{l(\beta)}$. We have

$$\gamma = x^{l(\beta)-l(\alpha)} \cdot \delta \cdot s.$$

So, $l(\beta) > l(\alpha)$ implies $\gamma \in R \cap (S \cdot x) = \langle x\rangle$ and contradicts the fact $\gamma \in R \setminus \langle x\rangle$. We write

$$s = \frac{\alpha'}{\delta} \quad \text{with} \quad \alpha' = x^{l(\alpha)-l(\beta)} \cdot \gamma.$$

[15] The proof of this claim was kindly supplied by Professor Markus Brodmann.

We see that

$$R_\delta = S_\delta.$$

Thus, the extension $\langle x\rangle^{\mathrm{e}}$ of the prime ideal $\langle x\rangle$ via the localization $R \longrightarrow R_\delta = S_\delta$ is a prime ideal of S_δ, and

$$\mathfrak{r} := \langle x\rangle^{\mathrm{e}} \cap S$$

is a prime ideal of S with $\mathfrak{r} \cap R = \langle x\rangle$. (We need this more specific prime ideal lying over $\langle x\rangle$ for later purposes, namely (IV.16).)

We get the induced finite ring extension

$$\overline{R} := R/\langle x\rangle \longrightarrow \overline{S} := S/\mathfrak{r}.$$

It induces a field extension

$$Q(\overline{R}) \longrightarrow Q(\overline{S}).$$

The foregoing discussion shows

$$\overline{S} \subset \overline{R}_{[\delta]} \subset Q(\overline{R}),$$

so that

$$Q(\overline{R}) = Q(\overline{S}),$$

and the induction hypothesis gives $\overline{R} = \overline{S}$.

We deduce

$$S = R + \mathfrak{r} \subset R + \langle x\rangle^{\mathrm{e}} \tag{IV.16}$$

s as R-module. Since $s \in S$ and $\alpha = s \cdot \delta$, we see

$$\alpha' = s \cdot \delta \in R \cap \left(\langle\delta\rangle + \langle x\rangle^{\mathrm{e}}\right) \overset{\text{(IV.15)\&}\langle\delta\rangle\subset R}{=} \langle\delta\rangle + \langle x\rangle.$$

This means that we may pick $a, b \in R$ with

$$\alpha' = a \cdot \delta + b \cdot x, \quad \text{so that} \quad s = a + \frac{b \cdot x}{\delta}.$$

We infer that S is generated as an R-algebra by $s_1 := b \cdot x/\delta$. Pick $N \in \mathbb{N}$, such that S is generated as R-module by 1,..., s_1^N. Then, inside $Q(R)$, we have

$$R \subset S \subset \frac{1}{\delta^N} \cdot R.$$

Let us abbreviate

$$t_n := \delta^N \cdot s_1^n = \frac{\delta^N \cdot b^n \cdot x^n}{\delta^n} \in R, \quad n \in \mathbb{N}.$$

Next, we introduce

$$s_2 := \frac{s_1}{x} = \frac{b}{\delta}.$$

We set $S_1 := R[s_1] = R[s] = S$ and $S_2 := R[s_2]$. We claim that

$$R[s_2] \subset \frac{1}{\delta^N} \cdot R.$$

For $n \in \mathbb{N}$, we find

$$\delta^N \cdot s_2^n = \frac{a_n}{x^n}.$$

By definition,

$$\delta^n \cdot a_n = (\delta^N \cdot b^n) \cdot x^n \in \langle x^n \rangle, \quad n \in \mathbb{N}.$$

Since $\delta \in R \setminus \langle x \rangle$, we have $l(\delta) = 0$. By (IV.14), it follows that $l(a_n) \geq n$, $n \in \mathbb{N}$. So, there is an element $u_n \in R$ with $a_n = u_n \cdot x^n$, $n \in \mathbb{N}$. We conclude

$$\delta^N \cdot s_2^n = u_n \in R, \quad n \in \mathbb{N},$$

as asserted.

Obviously, the R-module $(1/\delta^N) \cdot R$ is finitely generated. According to Proposition III.2.4, "iv)$\Longrightarrow$i)", s_2 is integral over R. We may replace s by s_2. If we apply the procedure which led from s to s_1 to s_2, we find an element s_2'. We next set $s_3 := s_2'/x$ and $S_3 := R[s_3]$. This process can clearly be iterated and leads to a chain

$$R =: S_0 \subset S_1 \subset S_2 \subset \cdots \subset S_l \subset S_{l+1} \subset \cdots \subset \frac{1}{\delta^N} \cdot R$$

of R-modules. Since R is a noetherian ring, this chain must become stationary. Let $m \in \mathbb{N}$ be the first index for which $S_m = S_{m+1}$ holds true. Then,

$$s_{m+1} = \frac{s_m}{x} \in S_{m+1} = S_m.$$

This shows

$$s_m \in x \cdot S_m \subset \mathfrak{m} \cdot S_m. \tag{IV.17}$$

Let $t \in S_m$. Then, there exist a natural number M and elements $r_0, ..., r_M \in R$, such that

$$t = r_0 \cdot 1 + r_1 \cdot s_m + \cdots + r_M \cdot s_m^M.$$

By (IV.17), $t \in R + \mathfrak{m} \cdot S_m$. This proves

$$S_m = R + \mathfrak{m} \cdot S_m.$$

By the Nakayama lemma III.1.31, applied to $M = S_m/R$, we have $S_m = R$. We see that $s \in S_1 \subset S_m \subset R$. This finishes the argument. □

IV.8.7 Remark. In fact, a stronger[16] statement holds true, called the **Auslander[17]–Buchsbaum[18] theorem**: *A regular noetherian local ring R is factorial.*

The proof requires some tools from homological algebra which we haven't developed, so far. References are the original paper [2], [5], Satz 10.10, or [20], Theorem 20.3.

IV.8.8 Proposition. *Let R be a noetherian local ring with* $\dim(R) = 1$. *Then, R is regular if and only if it is normal.*

[16] see Lemma III.5.1

[17] Maurice Auslander (1926 - 1994), American mathematician.

[18] David Alvin Buchsbaum, born 1929, American mathematician.

Proof. We have to prove that R is regular, if R is normal. According to Proposition IV.6.2, we have to verify that the maximal ideal $\mathfrak{m}$ of R is a principal ideal. Fix $x \in \mathfrak{m} \setminus \mathfrak{m}^2$,[19] and assume

$$\langle x \rangle \subsetneq \mathfrak{m}.$$

Since R is an integral domain (Proposition III.5.2) and $\dim(R) = 1$, $\mathfrak{m}$ is the only prime ideal of R. Thus, by Corollary I.8.18,

$$\mathfrak{m} = \sqrt{\langle x \rangle}.$$

The ideal $\mathfrak{m}$ is finitely generated, so that there is some natural number s with

$$\mathfrak{m}^s \subset \langle x \rangle,$$

and we set

$$s_0 := \min\{\, s \in \mathbb{N} \mid \mathfrak{m}^s \subset \langle x \rangle \,\}.$$

Note that $s_0 > 1$. Pick

$$y \in \mathfrak{m}^{s_0 - 1} \setminus \langle x \rangle.$$

This gives

$$y \cdot \mathfrak{m} \subset \langle x \rangle,$$

and we assert

$$y \cdot \mathfrak{m} \subset x \cdot \mathfrak{m}.$$

Otherwise, there would be an element $r \in R \setminus \mathfrak{m}$, i.e., a unit of R, with $r \cdot x \in y \cdot \mathfrak{m}$. This would give

$$x = r^{-1} \cdot (r \cdot x) \in y \cdot \mathfrak{m} \subset \mathfrak{m}^2.$$

So, in the quotient field $Q(R)$, we have

$$\forall r \in \mathbb{N}: \quad \left(\frac{y}{x}\right)^r \cdot \mathfrak{m} \subset \mathfrak{m}, \quad x \cdot R\left[\frac{y}{x}\right] \subset R, \quad \text{and} \quad R\left[\frac{y}{x}\right] \subset \frac{1}{x} \cdot R.$$

This shows that y/x is contained in a finitely generated R-submodule of $Q(R)$. According to Proposition III.2.4, iii), y/x is integral over R. Since R is normal, we have $y/x \in R$, so that $y \in \langle x \rangle$, a contradiction. □

In geometric language, the above proposition says that a normal affine algebraic curve is smooth. More generally, the normalization of a possibly singular irreducible algebraic curve is non-singular. So, in the realm of curves, normalization provides a canonical way to attach to a singular irreducible curve a non-singular one.

IV.8.9 Proposition. *Let k be an algebraically closed field, $n \geq 1$, and $Z \subset \mathbb{A}^n_k$ an algebraic variety. If Z is normal, then*

$$\dim(\mathrm{Sing}(Z)) \leq \dim(Z) - 2.$$

In the proof, we will use the following result.

[19] This set is non-empty by the Nakayama lemma III.1.31 and the assumption $\dim(R) = 1$.

IV.8.10 Lemma. *Let R be a noetherian local integral domain, $\mathfrak{m} \subset R$ its maximal ideal, and $x \in \mathfrak{m} \setminus \{0\}$. If the ring $R/\langle x\rangle$ is regular, then R is regular, too.*

Proof. By Lemma IV.8.2, $\dim(R/\langle x\rangle) = \dim(R) - 1 =: d$. By assumption, there are elements $r_1, ..., r_d$, such that their images $\overline{r}_1, ..., \overline{r}_d$ generate the image $\overline{\mathfrak{m}}$ of $\mathfrak{m}$ in $R/\langle x\rangle$. Then, $\mathfrak{m} = \langle\, x, r_1, ..., r_d \,\rangle$. Remark IV.6.1 and Proposition IV.6.2 show that R is a regular local ring. □

Proof of Proposition IV.8.9. Let $\mathrm{Reg}(Z) := Z \setminus \mathrm{Sing}(Z)$ be the open subset of nonsingular points of Z. It suffices to show that

$$H \cap \mathrm{Reg}(Z) \neq \emptyset$$

holds true for every irreducible algebraic set $H \subset Z$ with

$$\dim(H) = \dim(Z) - 1.$$

Let us fix such a subset $H \subset Z$. Then,

$$\mathfrak{p} := I(H) := \{\, f \in k[Z] \mid \forall a \in H : f(a) = 0 \,\}$$

is a prime ideal in the coordinate algebra $k[Z]$ of Z. We look at the localization $k[Z]_{\mathfrak{p}}$ of the coordinate algebra at that prime ideal. Then:

- ⋆ $k[Z]_{\mathfrak{p}}$ is a normal local ring. (This is left as an exercise (compare Exercise III.2.12). Note that $k[Z]_{\mathfrak{p}}$ has the same the quotient field as $k[Z]$.)
- ⋆ $\dim(k[Z]_{\mathfrak{p}}) = 1$ (Corollary IV.4.8).

By Proposition IV.8.8, the ring $k[Z]_{\mathfrak{p}}$ is regular. So, its maximal ideal $\mathfrak{p}^{\mathrm{e}}$ is a principal ideal. This means that there is an element $r \in k[Z]$, such that

$$\mathfrak{p}^{\mathrm{e}} = r \cdot k[Z]_{\mathfrak{p}}.$$

Next, let $r_1, ..., r_s \in \mathfrak{p}$ be elements with $\mathfrak{p} := \langle\, r_1, ..., r_s \,\rangle$, and $a_1, ..., a_s \in k[Z]$, $h_1, ..., h_s \in k[Z] \setminus \mathfrak{p}$ elements with $r_i = a_i/h_i$, $i = 1, ..., s$. Then, with

$$h := h_1 \cdot \cdots \cdot h_s,$$

we find the equality

$$\mathfrak{p} \cdot k[Z]_h = r \cdot k[Z]_h. \tag{IV.18}$$

Note that $k[Z]_h$ is the coordinate algebra of the principal open subset $D(h) \subset Z$ (see Page 143f). Since $h \notin \mathfrak{p}$, we have

$$D(h) \cap H \neq \emptyset.$$

Let $\mathrm{Reg}(H) := H \setminus \mathrm{Sing}(H)$ be the open subset of non-singular points of H. Since H is irreducible, we have

$$D(h) \cap \mathrm{Reg}(H) \neq \emptyset.$$

We will show that

$$D(h) \cap \mathrm{Reg}(H) \subset \mathrm{Reg}(Z).$$

Let $a \in D(h) \cap \mathrm{Reg}(H)$ and $\mathfrak{m}_a \subset k[Z]$ the maximal ideal of a. Then, $h \notin \mathfrak{m}_a$. So, (IV.18) gives

$$\mathfrak{p} \cdot k[Z]_{\mathfrak{m}_a} = r \cdot k[Z]_{\mathfrak{m}_a}. \tag{IV.19}$$

Let $\overline{\mathfrak{m}}_a$ be the image of $\mathfrak{m}_a$ in $k[H] = k[Z]/\mathfrak{p}$. One checks

$$k[H]_{\overline{\mathfrak{m}}_a} \cong k[Z]_{\mathfrak{m}_a}/(\mathfrak{p} \cdot k[Z]_{\mathfrak{m}_a}).$$

By (IV.19),

$$k[H]_{\overline{\mathfrak{m}}_a} = k[Z]_{\mathfrak{m}_a}/(r \cdot k[Z]_{\mathfrak{m}_a}).$$

Our choice of a implies that $k[H]_{\overline{\mathfrak{m}}_a}$ is a regular local ring. Therefore, Lemma IV.8.10 shows that $k[Z]_{\mathfrak{m}_a}$ is a regular local ring, too. □

IV.8.11 Remark. The attentive reader will have noticed that, in the above proof, we used only the fact that $k[Z]_{\mathfrak{p}}$ is normal for every prime ideal $\mathfrak{p} \subset k[Z]$ of height one. In fact, for any noetherian integral domain R, it is true that R is normal if and only if $R_{\mathfrak{p}}$ is normal for every prime ideal $\mathfrak{p} \subset R$ of height one **and**

$$R = \bigcap_{\substack{\mathfrak{p} \subset R \text{ prime} \\ \mathrm{ht}(\mathfrak{p})=1}} R_{\mathfrak{p}}.$$

We refer the reader to [4], Satz (13.25).

For more information on normal rings related to the above discussion, we refer the reader to [4], p. 199ff, or [5], Section 11.

References

[1] M.F. Atiyah, I.G. Macdonald, *Introduction to commutative algebra*, Addison–Wesley Publishing Co., Reading, Mass.–London–Don Mills, Ont. 1969, ix+128 pp.

[2] M. Auslander, D.A. Buchsbaum, *Unique factorization in regular local rings*, Proc. Natl. Acad. Sci. USA **45** (1959), 733-734.

[3] B. Banaschewski, *A new proof that "Krull implies Zorn"*, Math. Log. Q. **40** (1994), 478-80.

[4] M. Brodmann, *Algebraische Geometrie — Eine Einführung*, Basler Lehrbücher, Basel etc.: Birkhäuser Verlag, 1989, xv+470 S.

[5] M. Brodmann, *Kommutative Algebra*, lecture notes by R. Boldini and F. Rohrer, `http://www.math.uzh.ch/index.php?id=publikationen&key1=115`.

[6] D. Eisenbud, J. Harris, *The geometry of schemes*, Graduate Texts in Mathematics, 197, Springer-Verlag, New York, 2000, x+294 pp.

[7] G. Fischer, *Lineare Algebra. Eine Einführung für Studienanfänger*, 17. akt. Aufl., Grundkurs Mathematik, Wiesbaden: Vieweg+Teubner, 2010, xxii+384 S.

[8] G. Fischer, R. Sacher, *Einführung in die Algebra*, 3., überarb. Aufl., Teubner Studienbücher, Mathematik, Stuttgart: B.G. Teubner, 1983, 240 S.

[9] R.W. Gilmer, *Rings in which the unique primary decomposition theorem holds*, Proc. Amer. Math. Soc. **14** (1963), 777-781.

[10] Ph. Griffiths, J. Harris, *Principles of algebraic geometry*, 2. Aufl., Wiley Classics Library, New York, NY: John Wiley & Sons Ltd., 1994, xii+813 S.

[11] R. Hartshorne, *Algebraic Geometry*, Graduate Texts in Mathematics, 52, Springer-Verlag, New York-Heidelberg, 1977, xvi+496 pp.

[12] H. Herrlich, *Axiom of choice*, Lecture Notes in Mathematics, 1876, Springer-Verlag, Berlin, 2006, xiv+194 pp.

[13] D. Huybrechts, *Complex geometry. An introduction*, Universitext, Berlin: Springer, 2005, xii+309 S.

[14] Th. de Jong, G. Pfister, *Local analytic geometry. Basic theory and applications*, Advanced Lectures in Mathematics, Braunschweig: Friedr. Vieweg & Sohn, 2000, xii+382 pp.

[15] I. Kaplansky, *Commutative rings*, 2nd revised ed., Chicago–London: The University of Chicago Press, 1974, viii+182 pp.

[16] S. Katok, *p-adic analysis compared with real*, Student Mathematical Library, 37, American Mathematical Society, Providence, RI, 2007, xiv+152 S.

[17] S. Lang, *Algebra*, 3rd revised ed., Graduate Texts in Mathematics, vol. 211, New York, NY: Springer, 2002, xv+914 pp.

[18] G. Laures, M. Szymik, *Grundkurs Topologie*, Spektrum Akademischer Verlag GmbH, Heidelberg, 2009, x+242 pp.

[19] F. Lorenz, *Lineare Algebra* I, 3., überarb. Aufl., Mannheim: B.I. Wissenschaftsverlag, 1992, x+226 pp.

[20] H. Matsumura, *Commutative ring theory*, transl. from the Japanese by M. Reid, Cambridge Studies in Advanced Mathematics, vol. 8, Cambridge etc.: Cambridge University Press, 1989, 336 pp.

[21] D. Mumford, *The red book of varieties and schemes*, second, expanded edition, includes the Michigan lectures (1974) on curves and their Jacobians, with contributions by Enrico Arbarello, Lecture Notes in Mathematics, 1358, Springer-Verlag, Berlin, 1999, x+306 pp.

[22] R. Munshi, *Hilberts Nullstellensatz*, Bull. Bombay Math. Colloq. **15** (1999), 20-24.

[23] J. Neukirch, *Algebraische Zahlentheorie*, reprint of the 1992 original, Berlin: Springer, 2007, xiv+595 pp.

[24] B. Olberding, *Noetherian rings without finite normalization*, in *Progress in commutative algebra 2. Closures, finiteness and factorization*, edited by Ch. Francisco, L. Klingler, S. Sather-Wagstaff, and J.C. Vassilev, Walter de Gruyter GmbH & Co. KG, Berlin, 2012, x+315 pp, 171-203.

[25] Y. Rav, *Variants of Rado's selection lemma and their applications*, Math. Nachr. **79** (1977), 145-65.

[26] R. Remmert, G. Schumacher, *Funktionentheorie* 1, 5., neu bearb. Aufl., Berlin: Springer, 2002, xx+402 S.

[27] A. Schmitt, *Analysis* I, lecture notes, `http://userpage.fu-berlin.de/~aschmitt`.

[28] A. Schmitt, *Analysis* II, lecture notes, `http://userpage.fu-berlin.de/~aschmitt`.

[29] A. Schmitt, *Analysis* III, lecture notes,
http://userpage.fu-berlin.de/~aschmitt.

[30] A. Schmitt, *Algebra und Zahlentheorie*, lecture notes,
http://userpage.fu-berlin.de/~aschmitt.

[31] A. Schmitt, *Funktionentheorie*, lecture notes,
http://userpage.fu-berlin.de/~aschmitt.

[32] R.-H. Schulz, *Elementargeometrie*, lecture notes,
http://page.mi.fu-berlin.de/rhschulz/Elgeo-Skript/elgeo.html

[33] V. Schulze, *Lineare Algebra*, lecture notes,
http://page.mi.fu-berlin.de/klarner/lina_skript.pdf

[34] R.G. Swan, *On Munshi's proof of the Nullstellensatz*,
www.math.uchicago.edu/~swan/nss.pdf

[35] H.-P. Tuschik, H. Wolter, *Mathematische Logik — kurzgefaßt. Grundlagen, Modelltheorie, Entscheidbarkeit, Mengenlehre*, 2nd ed., Spektrum Hochschultaschenbuch, Heidelberg: Spektrum Akademischer Verlag, 2002, viii+214 pp.

Index