Commutative Algebra

Winter Term 2020/2021
Master in Mathematics
Master in Secondary Education

Université du Luxembourg

Gabor Wiese
gabor.wiese@uni.lu

Version of 11th January 2021

Preface

The integers and basic notions of geometry are taught in and known from school. If one wants a deeper understanding, in number theory one is naturally led to study more general numbers than just the classical integers and, thus, to introduce the concept of integral elements in number fields. The rings of integers in number fields have certain very beautiful properties (such as the unique factorisation of ideals, generalising the unique factorisation of a positive integer into products of primes) which characterise them as Dedekind rings. Parallely, in geometry one studies affine varieties through their coordinate rings. It turns out that the coordinate ring of a curve is a Dedekind ring if and only if the curve is non-singular (e.g. has no self intersection).
With this in mind, we shall work towards the concept and the characterisation of Dedekind rings. Along the way, we shall introduce and demonstrate through examples basic concepts of algebraic geometry and algebraic number theory. Moreover, we shall be naturally led to treat many concepts from commutative algebra.
We will point out that and in which ways these concepts are generalisations of notions that are taught in secondary schools.

Good books are the following. But, there are many more!

- M. Reid, Undergraduate Commutative Algebra, Cambridge University Press.
- E. Kunz, Introduction to Commutative Algebra and Algebraic Geometry.
- Dino Lorenzini. An Invitation to Arithmetic Geometry, Graduate Studies in Mathematics, Volume 9, American Mathematical Society.
- M. F. Atiyah, I. G. Macdonald. Introduction to Commutative Algebra, Addison-Wesley Publishing Company.

These notes are a reworked version of my lecture notes of previous terms. In preparing them, I used several sources. The most important one is the lecture *Algebra 2*, which I taught at the Universität Duisburg-Essen in the summer term 2009, which, in turn, heavily relies on a lecture for second year students by B. H. Matzat at the Universität Heidelberg from summer term 1998.

Contents

Chapter I

Basic ring theory

In this lecture all rings are assumed to be commutative (unless otherwise stated). That's why the course is called *Commutative Algebra*; another common name for this course is *Commutative Ring Theory.*

We see the lecture Commutative Algebra as a preparation for deeper study of **Algebraic Number Theory** and **Algebraic Geometry**. Both subjects relate number theoretic or respectively geometric properties with properties of rings. These properties are then analysed via the methods provided by commutative algebra.
Motivated and inspired by this, we shall let us be guided by examples from number theory and geometry. Accordingly, we will devote some time to introduce the ring of integers in a number field and the coordinate ring of a curve.
We always point out how the notions studied arise from and are related to mathematics encountered and taught at school.
We start the lecture by an overview of some general ring theory, particularly praising properties of especially 'nice' rings: Euclidean rings, principal ideal domains (PID), unique factorisation domains (UFD). They are all generalisations of the integer ring $\mathbb{Z}$ and share many properties of it, like the unique factorisation into prime elements. Unfortunately, many of the rings one encounters naturally (like the rings of integers of number fields, or coordinate rings of affine plane curves) are not that 'nice'. We shall in later sections be concerned with finding substitutes for the 'nice' properties of unique factorisation and prinicipal ideal domains.

We assume familiarity with ring and field theory to the extent to which it is for example taught in the first three terms of the Bachelor Programme at the University of Luxembourg. For the convenience of the audience a summary is provided in two appendices.

1 Rings

Aims:

- Recall and summarise basic ring theory, as taught in most Bachelor programmes in Mathematics.

- Emphasize special properties of 'nice' rings like PIDs, UFDs (which won't hold for the rings to be considered later).

This section is merely meant as a short summary of basic ring theory. If one is not familiar (enough) with this topic, other sources must be consulted. A summary is provided in the appendix to this section.

The definition of a ring

Rings are abstractions motivated by the integers $\mathbb{Z}$. One enounters them (mostly implicitly) at school, e.g. the integers, the rationals, the reals, and square matrices of a given size.

Definition 1.1. *A set R, containing two elements 0 and 1 (not necessarily distinct), together with maps*

$$+ : R \times R \to R, (x, y) \mapsto x + y \text{ and } \cdot : R \times R \to R, (x, y) \mapsto x \cdot y$$

is called a unitary ring *if the following properties are satisfied:*

(a) $(R, +, 0)$ *is an abelian group with respect to* $+$ *and neutral element* 0*,*

(b) $R = \{0\}$ *or* $(R \setminus \{0\}, \cdot, 1)$ *is a semi-group with respect to* $\cdot$ *and neutral element* 1 *and*

(c) $a \cdot (b + c) = a \cdot b + a \cdot c$ *and* $(b + c) \cdot a = b \cdot a + c \cdot a$ *for all* $a, b, c \in R$ *(distributivity).*

The attribute unitary *refers to the existence of the element* 1 *in the ring. We only consider such rings, and will thus usually not mention the word unitary.*
If $(R \setminus \{0\}, \cdot)$ *is an abelian semi-group, then* R *is called a* commutative ring. *Most (but not all) of the lecture will only treat commutative rings; hence, the name* Commutative Algebra. *By a ring I shall usually mean a commutative ring (should be clear from the context – if not, ask!).*
If R *is a commutative ring and if in addition* $(R \setminus \{0\}, \cdot, 1)$ *is an abelian group (not only a semi-group; i.e. we ask all* $R \ni r \neq 0$ *to possess an inverse for multiplication, usually denoted* $\frac{1}{r}$ *or* r^{-1}*) and* $1 \neq 0$*, then* R *is called a* field.
A subset $S \subseteq R$ *is called a* (commutative) subring *if* $0, 1 \in S$ *and* $+$ *and* $\cdot$ *restrict to* S *making it into a ring.*
[We recall the definition of a semi-group and a group: A set S*, containing an element denoted* 1*, together with a map* $\cdot : S \times S \to S$*,* $(s, t) \mapsto s \cdot t$ *is called a* semi-group *if the following hold:*

(a) $s \cdot (t \cdot u) = (s \cdot t) \cdot u$ *for all* $s, t, u \in S$ *(*associativity*),*

(b) $1 \cdot s = s = s \cdot 1$ *for all* $s \in S$ *(*neutral element*).*

If, in addition, it holds that

(c) for all $s \in S$ *there are* $t, u \in S$ *such that* $s \cdot t = 1 = u \cdot s$ *(notation* s^{-1} *for both) (*existence of inverses*),*

then S *is called a group. If* $s \cdot t = t \cdot s$ *for all* $s, t \in S$*, then the (semi-)group is called* abelian *or* commutative.*]*

Example 1.2. *(a)* $\mathbb{Z}$*: basic example of a commutative ring.*

(b) $\mathbb{Q}$*: basic example of a field.*

(c) $M_N(\mathbb{Q})$ *($N \times N$-matrices): if $N > 1$, example of a non-commutative ring.*

(d) $\mathbb{Z}[X]$, $\mathbb{Q}[X]$*: both polynomial rings are commutative; they are not fields.*

(e) $\{0\}$ *is called the* zero-ring *(with $1 = 0$ and the only possible definitions of $+$ and $\cdot$, namely $0 + 0 = 0$ and $0 \cdot 0 = 0$).*

(f) $\mathbb{Z}/n\mathbb{Z}$ *for $n \in \mathbb{N}$, the ring of residues mod n.*

(g) $\mathbb{F}_p$, $\mathbb{F}_{p^r}$ *for a prime number p and $r \in \mathbb{N}$: finite fields of cardinality p, p^r, respectively (see below).*

(h) $\mathbb{Z} \times \mathbb{Z}$ *is also a commutative ring for $(a_1, b_1)+(a_2, b_2) = (a_1+a_2, b_1+b_2)$ and $(a_1, b_1)\cdot(a_2, b_2) = (a_1 \cdot a_2, b_1 \cdot b_2)$.*

Homomorphisms and special elements

A map $\varphi : R \to S$ is called *ring homomorphism* if

- $\varphi(1) = 1$,
- $\varphi(r + s) = \varphi(r) + \varphi(s)$ for all $r, s \in R$, and
- $\varphi(r \cdot s) = \varphi(r) \cdot \varphi(s)$ for all $r, s \in R$.

Example 1.3. *(a)* $\mathbb{Z} \to \mathbb{F}_p, a \mapsto \overline{a}$.

(b) Let R be a ring and S a subring of R. The inclusion $\iota : S \to R$ defines a ring homomorphism.

Divisibility of integers is one of the classical and fundamental objects of study in number theory and, of course, known from school. We now see its abstraction to rings.

Definition 1.4. *Let R be a ring.*

- *An element $r \in R$* divides *an element $s \in R$ (in symbols: $r \mid s$) if there is $t \in R$ such that $s = rt$.*

  Example: $3 \mid 6$ *in* $\mathbb{Z}$.

- *An element $r \in R$ is called a* unit *if there is $s \in R$ such that $rs = 1$ (equivalently, r is a unit if and only if r divides 1). The set of units forms a group w.r.t. $\cdot$, denoted as $R^\times$.*

  Examples:

  - $\mathbb{Z}^\times = \{-1, 1\}$.
  - $K^\times = K \setminus \{0\}$ *for any field K.*
  - $(\mathbb{Z}/n\mathbb{Z})^\times = \{a \mod n \mid \gcd(a, n) = 1\}$.
  - $(\mathbb{Z} \times \mathbb{Z})^\times = \{(1, 1), (1, -1), (-1, 1), (-1, -1)\}$.

- *Two elements $r, s \in R$ are* associate *if there is a unit $t \in R^\times$ such that $r = ts$ (note that being associate is an equivalence relation).*

  Example: 3 and -3 are associate in $\mathbb{Z}$ (except 3 and -3, there's no other element in $\mathbb{Z}$ that is associate with 3).

- *An element $r \in R$ is called a* zero-divisor *if there is $s \in R$, $s \neq 0$ such that $rs = 0$.*

  Examples:

  - *0 is a zero-divisor in any ring.*
  - *The class of 2 is a zero-divisor in $\mathbb{Z}/6\mathbb{Z}$ because $2 \cdot 3 \equiv 0 \mod 6$.*
  - *$(1, 0)$ is a zero-divisor in $\mathbb{Z} \times \mathbb{Z}$ because $(1, 0) \cdot (0, 1) = (0, 0)$.*

- *A ring is called an* integral domain *(or domain, for short) if 0 is its only zero-divisor. Examples:*

  - *$\mathbb{Z}$ is an integral domain.*
  - *Any field is an integral domain (because any non-zero element is invertible, hence not a zero-divisor).*
  - *The polynomial ring over any integral domain is an integral domain.*
  - *$\mathbb{Z}/n\mathbb{Z}$ with $n \in \mathbb{N}_{\geq 1}$ is an integral domain if and only if it is a field if and only if n is a prime number.*
  - *$\mathbb{Z} \times \mathbb{Z}$ is not an integral domain.*

Definition 1.5. *Let R be an integral domain.*

(a) An element $r \in R \setminus (R^\times \cup \{0\})$ is called irreducible *if, whenever $r = st$ with $s, t \in R$, then $s \in R^\times$ or $t \in R^\times$.*

Example: $n \in \mathbb{Z} \setminus \{-1, 0, 1\}$ is irreducible if and only if its only divisors are $1, -1, n, -n$; i.e., the n is irreducible if it is ± 1 a prime number (according to the 'school definition': it is ≥ 2, and its only positive divisors are $1, n$).

(b) An element $r \in R \setminus (R^\times \cup \{0\})$ is called a prime element *if, whenever $r \mid st$ with $s, t \in R$, then $r \mid s$ or $r \mid t$.*

Let R be an integral domain and $r \in R \setminus (R^\times \cup \{0\})$. One always has (see Proposition 1.20):

$$r \text{ is prime } \Rightarrow r \text{ is irreducible.}$$

The following definition is an abstraction of one of the most important properties of integers studied at school: the unique factorisation of a positive integer into a product of prime numbers.

Definition 1.6. *An integral domain R is called a* unique factorisation domain (UFD) *or* factorial ring *if any $r \in R \setminus (R^\times \cup \{0\})$ can be written as a finite product of prime elements.*

Example 1.7. *(a) $\mathbb{Z}$ is the most basic example.*

(b) Any field is a UFD (that's trivial because $R \setminus (R^\times \cup \{0\} = \emptyset$).

(c) The polynomial ring over any UFD is a UFD (that is not so easy; it has been proved by Gauß).

Lemma 1.8. *Let R be a UFD and $r \in R \setminus (R^\times \cup \{0\})$. Then one has:*

$$r \text{ is prime } \Leftrightarrow r \text{ is irreducible.}$$

Proof. For $\Rightarrow$, see above; we only have to show $\Leftarrow$. Assume r irreducible and apply the definition of UFD to write r as a finite product of prime elements: $r = p_1 \cdot p_2 \cdot \ldots \cdot p_n$. The irreducibility of r implies $n = 1$, so $r = p_1$ is prime. □

We have thus found, in particular, that over $\mathbb{Z}$ the 'school definition' of a prime number coincides with the definition given here (which is the conceptual one, in view of prime ideals, see below).
One could hope that any ring has equally nice properties as $\mathbb{Z}$. Also for appreciating the fundamental and special character of the integers (in particular, when teaching them at school), it is important to know that not all rings share the same properties as $\mathbb{Z}$. We now give an example of a ring that does not admit unique factorisation into prime elements.

Example 1.9. *The ring $R := \mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$ is a subring of $\mathbb{C}$. We have*

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

Since all four elements $2, 3, 1 + \sqrt{-5}, 1 - \sqrt{-5}$ are irreducible elements of R, we conclude that R is not a UFD (but, it is an integral domain in which all chains of strict divisors have finite length; see below).
For details see an exercise.

We remark that it makes sense to define greatest common divisors and lowest common multiples in all rings. But, they need not exist, in general. In UFDs they always do!
We shall see later that being a UFD is a property that is too strong in many cases. They will be replaced by Dedekind rings (which are *locally* PIDs – definitions come later; examples are the rings of integers in number fields).

Ideals

At school, one enounters the set of all integer multiples of a given integer $\mathbb{Z} \cdot a = \{n \cdot a \mid n \in \mathbb{Z}\}$. This is also denoted (a), and is an example of a principal ideal. Also because of the general absence of unique factorisation (but not only), one introduces a more general notion, extending the set of multiples, namely the notion of ideals.
A subset $I \subseteq R$ is called an *ideal* if

- $\forall\, i, j \in I : i + j \in I$ and
- $\forall\, i \in I \, \forall r \in R : r \cdot i \in I$.

Notation: $I \lhd R$ (or $I \trianglelefteq R$).
Let $a_1, \ldots, a_n$ be elements of R. Define the *ideal generated by* $a_1, \ldots, a_n$ as

$$(a_1, \ldots, a_n) = \{\sum_{i=1}^{n} r_i a_i \mid r_1, \ldots, r_n \in R\}.$$

Any such ideal is called *finitely generated*.
In particular, for $a \in R$, one has

$$(a) = R \cdot a = \{r \cdot a \mid r \in R\},$$

called the *principal ideal generated by* a.
Any ideal $I \trianglelefteq R$ is called *principal* if there is $a \in R$ such that $I = (a)$.
For $a, b \in R$ we have

$$(a) \subseteq (b) \Leftrightarrow b \mid a.$$

More generally, let S be an 'indexing' set and $\{a_s\}_{s \in S}$ be elements of R. The ideal generated by it is defined as the intersection of all ideals of R containing all a_s for $s \in S$; it is denoted $(a_s \mid s \in S)$. It can also be seen as the set of sums with finite subsets $T \subseteq S$ of the form $\sum_{s \in T} r_s a_s$, where $r_s \in R$ for all $s \in T$.

Example 1.10. *(a)* $(2) \lhd \mathbb{Z}$ *is the ideal of even integers.*

(b) $(2, 3) = (1) = \mathbb{Z}$.

(c) $(X) \lhd \mathbb{Q}[X]$ *is the set of polynomials divisible by* X.

(d) $(X_i \mid i \in \mathbb{N}) \lhd \mathbb{Q}[X_1, X_2, X_3, \dots]$ *is the ideal of polynomials in countably many variables with constant term* 0.

(e) The kernel of any ring homomorphism is an ideal.

(f) The definition of ideals ensures exactly that one can take quotients. More precisely, let R *be a ring and* $I \subseteq R$ *an ideal. Then the set of cosets* R/I*, consisting of the cosets* $r + I$ *for* $r \in R$*, is a ring, called* quotient of R modulo/by I*, if one defines addition as* $(r_1 + I) + (r_2 + I) = (r_1 + r_2) + I$ *and multiplication as* $(r_1 + I) \cdot (r_2 + I) = (r_1 \cdot r_2) + I$*. The point here is that this definition is independent of the choice of coset representatives. For details, see the appendix.*

(g) A major tool in many of our arguments is the isomorphism theorem. Let $f : R \to S$ *be a ring homomorphism and let* $I = \ker(f)$ *be its kernel. Then the map*

$$\overline{f} : R/I \to \mathrm{im}(f) \subseteq S, \quad \overline{f}(r + I) := f(r)$$

is well-defined and is a ring isomorphism (see also Proposition 1.26).

Definition 1.11. *An integral domain having the property that any ideal is principal is called a* principal ideal domain (PID).

Example 1.12. *(a)* $\mathbb{Z}$ *is the most basic example of a PID.*

(b) $K[X]$ *is a PID if* K *is a field.*

(c) $\mathbb{Z}[X]$ *is not a PID because* $(2, X)$ *is not a principal ideal.*

(d) More generally, any Euclidean integral domain is a PID (see Proposition 1.29).

Proposition 1.13. *Every principal ideal domain (PID) is a unique factorisation domain (UFD).*

The proof is given in the appendix to this section.

Prime ideals and maximal ideals

In $\mathbb{Z}$ and – by definition – in any other unique factorisation domain, any nonzero element can be factored uniquely into a finite product of prime elements (up to association). As we have seen, this fails to hold true for more general rings. However, in some classes of rings (e.g. Dedekind rings, see later), prime ideals are the 'building blocks' of all nonzero ideals in same way as prime numbers are the 'building blocks' of the integers. Thus prime ideals are natural generalisations of the prime numbers known from school.

Definition 1.14. *Let R be a ring and $I \lhd R$, $I \neq R$ an ideal.*
The ideal I is called maximal *if there is no ideal $J \lhd R$ such that $I \subsetneq J \subsetneq R$.*
The ideal I is called prime *if, whenever $ab \in I$, then $a \in I$ or $b \in I$.*

In any integral domain R, one has for $r \in R \setminus (\{0\} \cup R^\times)$:

$$r \text{ is a prime element } \Leftrightarrow (r) \text{ is a prime ideal.}$$

If R is a PID, then one also has (see Proposition 1.30):

$$r \text{ is an irreducible element } \Leftrightarrow (r) \text{ is a maximal ideal.}$$

Example 1.15. *(a) The prime ideals of $\mathbb{Z}$ are precisely (0) and the principal ideals (p) for p a prime number. The only prime ideal that is not also a maximal ideal is (0).*

(b) Let K be a field. The prime ideals of the polynomial ring $K[X]$ are (0) and the principal ideals $(f(X))$, where $f(X)$ is a (without loss of generality) monic (highest coefficient equal to 1) and irreducible polynomial in $K[X]$.

Proposition 1.16. *Let R be a ring and $I \lhd R$, $I \neq R$ an ideal.*

(a) Then I is a prime ideal if and only if R/I is an integral domain.

(b) Then I is a maximal ideal if and only if R/I is a field.

Proof. (a) Let I be a prime ideal and let $a + I, b + I \in R/I$ such that $(a + I)(b + I) = ab + I = 0 + I = 0$, i.e. $ab \in I$. By the property of I being a prime ideal, $a \in I$ or $b \in I$, which immediately translates to $a + I = 0$ or $b + I = 0$.
Conversely, assume that R/I is an integral domain and let $a, b \in R$ such that $ab \in I$. This means $(a + I)(b + I) = 0$, whence $a + I = 0$ or $b + I = 0$ so that $a \in I$ or $b \in I$, proving that I is a prime ideal.
(b) Suppose that I is a maximal ideal and let $x + I \neq 0$ be an element in R/I. We must show it is invertible. The condition $x + I \neq 0$ means $x \notin I$, whence the ideal $J = (I, x)$ is an ideal strictly bigger than I, whence $J = R$ by the maximality of I. Consequently, there are $i \in I$ and $r \in R$ such that $1 = i + xr$. This means that $r + I$ is the inverse of $x + I$.
Now let us assume that R/I is a field and let $J \supsetneq I$ be an ideal of R strictly bigger than I. Let x be an arbitrary element in J but not in I. As R/I is a field, the element $x + I$ is invertible, whence there is $y \in R$ such that $(x + I)(y + I) = xy + I = 1 + I \subseteq J$. So, $1 \in J$, whence $R \subseteq J$, showing that $J = R$, whence I is maximal. □

Here are some important consequences.

Corollary 1.17. *Let R be a ring.*

(a) Every maximal ideal is a prime ideal.

(b) R is an integral domain $\Leftrightarrow$ (0) is a prime ideal of R.

(c) R is a field $\Leftrightarrow$ (0) is a maximal ideal of R.

(d) If p is a prime number (in $\mathbb{Z}$), then $\mathbb{Z}/(p) =: \mathbb{F}_p$ is a field, the finite field with p elements.

(e) Let K be a field and $f \in K[X]$ a non-constant irreducible polynomial. Then (f) is a maximal ideal of the principal ideal domain $K[X]$ and the quotient $K[X]/(f)$ is a field. (In French this field has the name corps de rupture de f.*)*

(f) Let $f \in \mathbb{F}_p[X]$ be any irreducible polynomial of degree $r \geq 1$. Then $\mathbb{F}_p[X]/(f)$ is a field of cardinality p^r. It is denoted $\mathbb{F}_{p^r}$ (and if $r > 1$ it is different from $\mathbb{Z}/p^r\mathbb{Z}$, which is not even an integral domain!).

In fact, one can show (see any class on Galois theory) that all fields of cardinality p^r are isomorphic, explaining the notation.

Proof. (a) Every field is an integral domain.
(b,c) $R/(0) = R$.
(d-f) trivial. □

We later need the existence of maximal ideals.

Proposition 1.18. *Let R be a ring different from the zero-ring. Then R has a maximal ideal.*

The proof, which uses Zorn's lemma, can be found in the appendix to this section.

Corollary 1.19. *(a) Every ideal $\mathfrak{a} \subsetneq R$ is contained in some maximal ideal $\mathfrak{m}$ of R.*

(b) Every non-unit $x \in R \setminus R^\times$ is contained in a maximal ideal $\mathfrak{m}$ of R.

Proof. (a) Consider the natural projection $\pi : R \mapsto R/\mathfrak{a}$. Let $\overline{\mathfrak{m}}$ be a maximal ideal of $R/\mathfrak{a}$, which exists by Proposition 1.18. Then $\mathfrak{m} := \pi^{-1}(\overline{\mathfrak{m}})$ (preimage) is a maximal ideal of R, because $R/\mathfrak{m} \cong (R/\mathfrak{a})/\overline{\mathfrak{m}}$ is a field.
(b) If x is a non-unit, then (x) is a proper ideal of R, so we can apply (a). □

Appendix: Background on Rings

Integral domains

Proposition 1.20. *Let R be an integral domain.*

(a) Let $r \in R$. Then

$$r \in R^\times \Leftrightarrow (r) = R.$$

(b) Let $r, s \in R$. Then

$$r \mid s \Leftrightarrow (r) \supseteq (s).$$

(c) Let $r, s \in R$. Then r and s are associate if and only if $(r) = (s)$.

(d) Let $r \in R \setminus (R^\times \cup \{0\})$. Then r is a prime element if and only if (r) is a prime ideal of R.

(e) Let $r \in R$ be a prime element. Then r is irreducible.

Proof. (a), (b), (c) and (d) are an exercise.
(e) Let $r \in R$ be a prime element. In order to check that r is irreducible, let $r = st$ with $s, t \in R$. This means in particular that $r \mid st$. By the primality of r, it follows $r \mid s$ or $r \mid t$. Without loss of generality assume $r \mid s$, i.e. $s = ru$ for some $u \in R$. Then we have $r = st = rut$, whence $r(1 - ut) = 0$, which implies $1 - ut = 0$ by the property that R is an integral domain and $r \neq 0$. Thus $t \in R^\times$, as was to be shown. □

Algebras

Definition 1.21. *Let R and S be (not necessarily commutative) rings. We say that S is an R-*algebra *if there is a ring homomorphism $\varphi : R \to S$ such that $\varphi(R) \subseteq \mathcal{Z}(S)$, where $\mathcal{Z}(S) = \{s \in S \mid ts = st \ \forall\, t \in S\}$ is the* centre *of S (note that the condition $\varphi(R) \subseteq \mathcal{Z}(S)$ is empty if S is commutative). Many people use the terminology* associative R-algebra *for R-algebra; but, we will stick to the shorter one since we are not going to encounter any non-associative algebras (like Lie algebras).*

Example 1.22. *Let K be a field. Then the polynomial ring $K[X]$ is a K-algebra.*
Consider $\mathrm{End}_K(V)$ for a K-vector space V. Then $\mathrm{End}_K(V)$ is a K-algebra (K embeds into the scalar matrices, which are equal to the centre of $\mathrm{End}_K(V)$).

Ideals

Example 1.23. *(a) Let R be a ring. Then $\{0\}$, $(1) = R$ are both trivially ideals.*

(b) Let $\varphi : R \to S$ be a ring homomorphism. Then $\ker(\varphi)$ is an ideal of R.

(c) $\{nm | m \in \mathbb{Z}\} \lhd \mathbb{Z}$.

(d) $(n, m) = (g)$ with g the greatest common divisor of $n, m \in \mathbb{Z}$.

(e) $(n) \cap (m) = (\mathrm{lcm}(n, m))$.

The sum and the product of two ideals $\mathfrak{a}, \mathfrak{b}$ of some ring R are defined as

$$\mathfrak{a} + \mathfrak{b} = \{a + b \mid a \in \mathfrak{a}, b \in \mathfrak{b}\} \text{ and } \mathfrak{a} \cdot \mathfrak{b} = \{\sum_{i=1}^{m} a_i \cdot b_i \mid m \in \mathbb{N}, a_i \in \mathfrak{a}, b_i \in \mathfrak{b} \text{ for } i = 1, \ldots, m\}.$$

It is clear that both are ideals.

Quotient rings

Proposition 1.24. *Let R be a ring and $I \trianglelefteq R$ be an ideal. The relation $x \sim y :\Leftrightarrow x - y \in I$ defines an equivalence relation on R. The equivalence classes $\overline{x} = x + I$ form the ring denoted R/I with*

- $+ : R/I \times R/I \to R/I, \;\; (x + I, y + I) \mapsto x + y + I$,
- $0 = \overline{0} = 0 + I = I$ *as neutral element w.r.t. addition* $+$,
- $\cdot : R/I \times R/I \to R/I, \;\; (r + I, s + I) \mapsto rs + I$,
- $1 = \overline{1} = 1 + I$ *as neutral element w.r.t. multiplication* $\cdot$.

The ring R/I is called the quotient ring or R by I *(also called* factor ring*).*

Proof. Exercise. □

Example 1.25. *(a)* $\mathbb{Q}(i) \cong \mathbb{Q}[X]/(X^2 + 1)$.

(b) $\mathbb{F}_p = \mathbb{Z}/(p)$ *for p a prime.*

(c) $\mathbb{F}_4 = \mathbb{F}_2[X]/(X^2 + X + 1)$. *This is a field with 4 elements and will be studied explicitly in an exercise.*

Homomorphism theorem

The homomorphism theorem is also called isomorphism theorem. There are versions for groups, vector spaces, modules, etc. Here is the one for rings:

Proposition 1.26. *Let R, S be rings and $\varphi : R \to S$ be a ring homomorphism. Then the map*

$$R/\ker(\varphi) \to \operatorname{im}(\varphi), \;\; r + \ker(\varphi) \mapsto \varphi(r)$$

is well-defined and an isomorphism of rings.

Proof. Exercise. □

On maximal ideals

Proof of Proposition 1.18. This proof uses Zorn's Lemma (which one also needs for the existence of bases in general (i.e. not finite dimensional) vector spaces).
Let $\mathcal{M} := \{\mathfrak{a} \subsetneq R \text{ ideal } \}$ be the set of all proper ideals of R. Of course, $(0) \in \mathcal{M}$ (here we use that R is not the zero ring), so $\mathcal{M} \neq \emptyset$.
Inclusion $\subseteq$ gives a partial ordering on $\mathcal{M}$: by definition this means:

- $\mathfrak{a} \subseteq \mathfrak{a}$ for all $\mathfrak{a} \in \mathcal{M}$,
- If $\mathfrak{a} \subseteq \mathfrak{b}$ and $\mathfrak{b} \subseteq \mathfrak{a}$, then $\mathfrak{a} = \mathfrak{b}$.

But, for general $\mathfrak{a}, \mathfrak{b} \in \mathcal{M}$, we do not necessarily have $\mathfrak{a} \subseteq \mathfrak{b}$ or $\mathfrak{b} \subseteq \mathfrak{a}$. A subset $(\mathfrak{a}_i)_{i\in I} \subseteq \mathcal{M}$ (where I is any set) is called totally ordered if for any $i, j \in I$ one has $\mathfrak{a}_i \subseteq \mathfrak{a}_j$ or $\mathfrak{a}_j \subseteq \mathfrak{a}_i$.
Claim: Any totally ordered subset $(\mathfrak{a}_i)_{i\in I} \subseteq \mathcal{M}$ has an upper bound, namely $\mathfrak{a} := \bigcup_{i\in I} \mathfrak{a}_i$, meaning $\mathfrak{a} \subseteq \mathcal{M}$ and $\mathfrak{a}_i \subseteq \mathfrak{a}$ for all $i \in I$.
The claim is very easy to see. The last statement $\mathfrak{a}_i \subseteq \mathfrak{a}$ for $i \in I$ is trivial. In order to see that $\mathfrak{a}$ is an ideal, let $x, y \in \mathfrak{a}$. Then there are $i, j \in I$ such that $x \in \mathfrak{a}_i$ and $y \in \mathfrak{a}_j$. Because of $\mathfrak{a}_i \subseteq \mathfrak{a}_j$ or $\mathfrak{a}_j \subseteq \mathfrak{a}_i$, we have that $x + y \in \mathfrak{a}_j$ or $x + y \in \mathfrak{a}_i$, so that $x + y \in \mathfrak{a}$ in both cases. Given $r \in R$ and $x \in \mathfrak{a}$, there is $i \in I$ such that $x \in \mathfrak{a}_i$, whence $rx \in \mathfrak{a}_i$, thus $rx \in \mathfrak{a}$, showing that $\mathfrak{a}$ is an ideal of R. If $\mathfrak{a}$ were equal to the whole ring R, then there would be $i \in I$ such that $1 \in \mathfrak{a}_i$. This, however, would contradict $\mathfrak{a}_i \neq R$. Consequently, $\mathfrak{a} \in \mathcal{M}$, as claimed.
Zorn's Lemma is the statement that a partially ordered set has a maximal element if every totally ordered set of subsets has an upper bound.
So, $\mathcal{M}$ has a maximal element, i.e. an $\mathfrak{m} \in \mathcal{M}$ such that if $\mathfrak{m} \subseteq \mathfrak{a}$ for any $\mathfrak{a} \in \mathcal{M}$, then $\mathfrak{m} = \mathfrak{a}$. This is precisely the definition of a maximal ideal. □

On Euclidean rings

Definition 1.27. *An integral domain R is called a* Euclidean ring *if there is a map $\delta : R \setminus \{0\} \to \mathbb{N}_0$ such that R* has a division with remainder w.r.t. δ*, i.e. if for all $a, b \in R$, $b \neq 0$, there are $q, r \in R$ satisfying*

$$a = qb + r \text{ and } (r = 0 \text{ or } \delta(r) < \delta(b)).$$

Example 1.28. *(a) $\mathbb{Z}$ w.r.t. $\delta = |\cdot|$ (absolute value).*

(b) The Gaussian integers $\mathbb{Z}[i] := \{a + bi \in \mathbb{C} \mid a, b \in \mathbb{Z}\}$ with $+$ and $\cdot$ coming from $\mathbb{C}$, w.r.t. $\delta(a + ib) = a^2 + b^2$ (see exercise).

(c) $K[X]$ with K a field (but not $\mathbb{Z}[X]$) w.r.t. $\delta = \deg$.

(d) There are principal ideal domains which are not Euclidean. Example: $\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$, the proof that the ring is not Euclidean is quite hard.

Proposition 1.29. *Every Euclidean ring is a principal ideal domain.*

Proof. Let R be a Euclidean ring w.r.t. δ and let $I \lhd R$ be an ideal. We want to show that it is principal. If $I = \{0\}$, then it is already principal, so that we may suppose $I \neq (0)$. Consider the set $M := \{\delta(i) \in \mathbb{N} \mid i \in I \setminus \{0\}\}$. As a non-empty subset of $\mathbb{N}$ it has a smallest element (induction principal, well-ordering principle, ...). Let n be this smallest element. It is of the form $n = \delta(x)$ with $0 \neq x \in I$. Note $(x) \subseteq I$.
Let now $i \in I$ be any element. By the Euclidean property there are $q, r \in R$ such that $i = qx + r$ with $r = 0$ or $\delta(r) < \delta(n)$. Since $i \in I$ and $x \in I$, it follows that $r = i - qx \in I$. Due to the minimality of $n = \delta(x)$, we must have $r = 0$. Thus $i = qx \in (x)$. We have shown: $I \subseteq (x) \subseteq I$, hence, $I = (x)$ is a principal ideal. □

On principal ideal domains (PID)

Proposition 1.30. *Let R be a principal ideal domain and let $x \in R \setminus (R^\times \cup \{0\})$. Then the following are equivalent:*

(i) *x is irreducible.*

(ii) *(x) is a maximal ideal.*

(iii) *(x) is a prime ideal.*

(iv) *x is a prime element.*

In particular, the non-zero prime ideals are the maximal ideals.

Proof. '(i)⇒(ii):' If (x) were not a maximal ideal, then $(x) \subsetneq (y) \subsetneq R$ for some $y \in R \setminus (R^\times \cup \{0\})$, whence $y \mid x$ and y and x are not associate, so that x would not be irreducible.
'(ii)⇒(iii):' Proved in general in Corollary 1.17.
'(iii)⇒(iv):' and '(iv)⇒(i):' are proved in the context of integral domains in Proposition 1.20. □

Here is one important property of principal ideal domains (that also implies that they are Noetherian rings, but, this piece of terminology will only be introduced later and is only put here so that you recognise it when re-reading this section later).

Definition 1.31. *Let R be a ring. We say that in R* any chain of strict divisors has finite length *if the following property holds:*

> *For all elements $\{a_n\}_{n\in\mathbb{N}} \subseteq R$ such that $a_{n+1} \mid a_n$ for all $n \in \mathbb{N}$, there is $N \in \mathbb{N}$ such that for all $m \geq N$ one has $(a_m) = (a_N)$.*

An equivalent formulation of the property is:

> *Any ascending chain*
>
> $$\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \mathfrak{a}_3 \subseteq \dots$$
>
> *of principal ideals becomes stationary, i.e. there is $N \in \mathbb{N}$ such that for all $m \geq N$ one has $\mathfrak{a}_N = \mathfrak{a}_m$.*

(If one removes the word 'principal', then this is precisely the definition of being Noetherian*, which will be introduced later in this lecture.)*

Proposition 1.32. *Let R be a principal ideal domain. Then in R any chain of strict divisors has finite length. (In later terminology, this proposition states that any principal ideal domain is a* Noetherian ring.*)*

Proof. Let $\mathfrak{a}_n = (a_n)$. These ideals form an ascending ideal chain:

$$\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \mathfrak{a}_3 \subseteq \mathfrak{a}_4 \subseteq \dots$$

Form the ideal $\mathfrak{a} = \bigcup_{n\in\mathbb{N}} \mathfrak{a}_n$. It is a principal ideal, i.e. $\mathfrak{a} = (a)$ for some $a \in R$. Of course, $a \in (a)$, i.e. $a \in \bigcup_{n\in\mathbb{N}} \mathfrak{a}_n$, whence there is $N \in \mathbb{N}$ such that $a \in (a_N)$. This means $(a) \subseteq (a_m) \subseteq (a)$ for all $m \geq N$, whence $(a) = (a_N) = (a_m)$ for all $m \geq n$. □

On unique factorisation domains (UFD)

Lemma 1.33. *Let R be an integral domain in which any chain of strict divisors has finite length. Let $r \in R \setminus (R^\times \cup \{0\})$. Then there are irreducible $x_1, \dots, x_n \in R \setminus (R^\times \cup \{0\})$ such that $r = x_1 \cdot x_2 \cdot \dots \cdot x_n$.*

Proof. We first show that every $r \in R \setminus (R^\times \cup \{0\})$ has an irreducible divisor. Suppose this is not the case and pick any non-unit divisor $r_1 \mid r$ s.t. $(r) \subsetneq (r_1)$. If no such r_1 existed, then r would be irreducible itself. Of course, r_1 is not irreducible. So we can pick a non-unit divisor $r_2 \mid r_1$ s.t. $(r_1) \subsetneq (r_2)$. Like this we can continue and obtain an infinite chain of strict divisors, contrary to our hypothesis.
Now, we have an irreducible non-unit divisor $x_1 \mid r$ s.t. $(r) \subseteq (x_1)$. If r/x_1 is a unit, then we are done. Otherwise r/x_1 has an irreducible non-unit divisor $x_2 \mid r/x_1$. If $r/(x_1x_2)$ is a unit, then we are done. Otherwise $r/(x_1x_2)$ has an irreducible non-unit divisor.
Like this we continue. This process must stop as otherwise we would have an infinite chain of strict divisors $\cdots \mid \frac{r}{x_1x_2x_3} \mid \frac{r}{x_1x_2} \mid \frac{r}{x_1} \mid r$, contrary to our hypothesis. □

Proposition 1.34. *Let R be an integral domain. The following are equivalent:*

(i) *R is a UFD.*

(ii)
- *Every irreducible element $r \in R \setminus (\{0\} \cup R^\times)$ is a prime element and*
- *in R any chain of strict divisors has finite lenghts.*

(iii) *Every $r \in R \setminus (R^\times \cup \{0\})$ can be written uniquely (up to permutation and up to associate elements) as a product of irreducible elements, i.e. if $r = x_1 \cdot x_2 \cdot \dots \cdot x_n = y_1 \cdot y_2 \cdot \dots \cdot y_m$ with irreducible elements $x_i, y_j \in R \setminus (R^\times \cup \{0\})$, then $n = m$ and there is a permutation σ in the symmetric group on $\{1, \dots, n\}$ such that x_i is associate with $y_{\sigma(i)}$ for all $i = 1, \dots, n$.*

Proof. (ii) ⇒ (i): Since irreducible elements are prime, Lemma 1.33 takes care of this implication.
(i) ⇒ (iii): Recall that the prime elements are precisely the irreducible ones. So, we already have the existence. We now show the uniqueness. Let

$$r = x_1 \cdot x_2 \cdot \dots \cdot x_n = y_1 \cdot y_2 \cdot \dots \cdot y_m.$$

It follows that x_n divides $y_1 \cdot y_2 \cdot \dots \cdot y_m$. By the primality of x_1 it must divide one of the y's, say after renumbering $x_n \mid y_m$. But, since y_m is irreducible, we must have $x_n \sim y_m$ (associate!). Dividing by x_n on both sides, we obtain a shorter relation:

$$x_1 \cdot x_2 \cdot \dots \cdot x_{n-1} = \epsilon y_1 \cdot y_2 \cdot \dots \cdot y_{m-1},$$

where $\epsilon \in R^\times$ is a unit. Now it follows that x_{n-1} divides the right hand side, and, after renumbering, we have again $x_{n-1} \sim y_{m-1}$. Dividing by x_{n-1} (and possibly replacing the unit ϵ by a different one) we obtain an even shorter relation:

$$x_1 \cdot x_2 \cdot \dots \cdot x_{n-2} = \epsilon y_1 \cdot y_2 \cdot \dots \cdot y_{m-2}.$$

Like this we continue, and conclude $n = m$ and that, after the above renumbering, $x_i \sim y_i$ are associate for all $i = 1, \dots, n$.
(iii) $\Rightarrow$ (ii): We first show that every irreducible element is prime. Let $r \in R \setminus (R^\times \cup \{0\})$ be irreducible and suppose that $r \mid st$ with $s, t \in R$, i.e. $ru = st$ for some $u \in R$. We may write s, t and u uniquely (up to ordering and associates) as $s = s_1 \cdot s_2 \cdot \dots \cdot s_n$, $t = t_1 \cdot t_2 \cdot \dots \cdot t_m$ and $u = u_1 \cdot u_2 \cdot \dots \cdot u_\ell$ with irreducible elements s_i, t_j, u_k ($i = 1, \dots, n$; $j = 1, \dots, m$; $k = 1, \dots, \ell$). The uniqueness of irreducible elements occurring in the equation

$$s_1 \cdot s_2 \cdot \dots \cdot s_n \cdot t_1 \cdot t_2 \cdot \dots \cdot t_m = r \cdot u_1 \cdot u_2 \cdot \dots \cdot u_\ell$$

implies that r must be equal to one of the s's or one of the t's. This means that r divides s or it divides t, as was to be shown.
That any chain of strict divisors has finite length, simply follows from the fact that, up to associates, all divisors of a given $0 \neq r \in R$ are given by the possible products of the irreducible elements $x_1, \dots, x_n$ (using each x_i at most once) occuring in $r = x_1 \cdot x_2 \cdot \dots \cdot x_n$. □

Proof of Proposition 1.13. We have seen both properties or Proposition 1.34 (ii), namely in Propositions 1.30 and 1.32. □

Hence we have the implications: Euclidean $\Rightarrow$ PID $\Rightarrow$ UFD.

2 Modules

Aims:

- Learn and master the concept of a module;
- know examples and standard theorems;
- be able to prove simple properties.

In secondary schools, one studies 'linear algebra', that is, ways to solve systems of linear equations. While doing so, one encounters $\mathbb{R}^2$ (or even $\mathbb{R}^n$), the first example of a vector space. In linear algebra classes for first year students at the university, this theory gets a more abstract and more powerful framework. Here we are going to extend it further, by considering 'vector spaces' over a general ring, instead of a field. The notion of 'module' is obtained by dropping the requirement that the coefficients lie in a field from the definition of a vector space. It then reads as:

Definition 2.1. *Let R be a (not necessaritly commutative) ring. An abelian group $(M, +, 0)$ together with a map*

$$. : R \times M \to M, (r, x) \mapsto r.x$$

is called a (left) R-module *if the following properties are satisfied:*

(a) $1.x = x$ *for all* $x \in M$.

(b) $r.(x + y) = r.x + r.y$ *for all* $r \in R$ *and all* $x, y \in M$.

(c) $(r+s).x = r.x + s.x$ *for all* $r, s \in R$ *and all* $x \in M$.

(d) $(r \cdot s).x = r.(s.x)$ *for all* $r, s \in R$ *and all* $x \in M$.

In a similar way one defines right modules and two-sided modules (also called bi-modules*).*
A subset $N \subseteq M$ *is called an* R-submodule *of* M *if* $0 \in M$ *and* $+$ *and* $.$ *restrict to* N *making it into an* R*-module.*

Example 2.2. *(a) Let* K *be a field. Any* K*-vector space is a* K*-module, and vice versa.*

(b) Let R *be a ring. Then* R *is an* R*-module (natural* $+$ *and* $. = \cdot$*). The (left/right/two-sided) submodules of* R *as* R*-modules are precisely the (left/right/two-sided) ideals of* R*.*

(c) Let R *be a ring. Then* $M := R^n := \underbrace{R \times R \times \cdots \times R}_{n \text{ copies}}$ *is an* R*-module (natural* $+$*, diagonal* $.$*).*

From now on our rings are again commutative. We can then re-express the definition as follows.

Lemma 2.3. *Let* R *be a ring and let* M *be an abelian group* M *(with group operation* $+$ *and neutral element* 0*). Denote by* $\mathrm{End}(M)$ *the endomorphism ring of* M *as an abelian group. Suppose there is a map*

$$. : R \times M \to M, \quad (r, m) \mapsto r.m.$$

Then M *is a left* R*-module if and only if the map*

$$R \to \mathrm{End}(M), \quad r \mapsto (x \mapsto r.x)$$

is a ring homomorphism.

Proof. Exercise. □

Definition 2.4. *Let* R *be a ring and* M, N *be* R*-modules. A map* $\varphi : M \to N$ *is called an* R-module homomorphism *(or short:* R-homomorphism*, or:* R-linear (map)*) if*

- $\varphi(m_1 + m_2) = \varphi(m_1) + \varphi(m_2)$ *for all* $m_1, m_2 \in M$ *and*
- $\varphi(r.m) = r.\varphi(m)$ *for all* $m \in M$ *and all* $r \in R$*.*

Lemma 2.5. *The* kernel $\ker(\varphi) := \{m \in M \mid \varphi(m) = 0\}$ *is an* R*-submodule of* M*.*
The image $\mathrm{im}(\varphi) := \{\varphi(m) \mid m \in M\}$ *is an* R*-submodule of* N*.*
By the way, the quotient (see below) $N/\mathrm{im}(\varphi)$ *is called the* cokernel of φ*.*

Proof. This works precisely as for vector spaces. □

Definition 2.6. *Let* R *be a ring and* N, M *be* R*-modules. Let* $\varphi : M \to N$ *be an* R*-homomorphism. We say that* φ *is a* monomorphism *if* φ *is injective. It is called an* epimorphism *if* φ *is surjective. Finally, it is called an* isomorphism *if it is bijective.*
If $N = M$*, then an* R*-homomorphism* $\varphi : M \to M$ *is also called an* R-endomorphism*.*
We let $\mathrm{Hom}_R(M, N)$ *(or* $\mathrm{Hom}(M, N)$ *if* R *is understood) be the set of all* R*-homomorphisms* $\varphi : M \to N$*. If* $M = N$*, then one lets* $\mathrm{End}_R(M) := \mathrm{Hom}_R(M, M)$*.*

Lemma 2.7. *Let R be a ring and N, M be R-modules. Then $\mathrm{Hom}_R(M,N)$ is itself an R-module with respect to pointwise defined $+$ and ., i.e. $(f+g)(m) := f(m)+g(m)$ and $(r.f)(m) := r.(f(m))$ for all $f, g \in \mathrm{Hom}_R(M,N)$, all $m \in M$ and all $r \in R$.*

Proof. Exercise. □

Note that the intersection of submodules of a given module is again a submodule (however, the similar statement with the union is false).

Definition 2.8. *Let M be an R-module and let $m_i \in M$ for $i \in I$ (some 'indexing' set). Denote by*

$$\langle m_i | i \in I \rangle := \{ \sum_{j \in J} r_j.m_j \mid J \subseteq I \text{ finite subset}, r_j \in R \text{ for } j \in J \}.$$

It is thus the set of all finite R-linear combinations of the m_i for $i \in I$. It is an R-submodule of M and it is called the submodule generated by the m_i, $i \in I$.
In the special case $I = \{1, 2, 3, \ldots, n\}$ we have

$$\langle m_i | i \in I \rangle = \langle m_1, m_2, \ldots, m_n \rangle = \{ \sum_{i=1}^{n} r_i.m_i \mid r_1, \ldots, r_n \in R \}.$$

An R-module M is called finitely generated *if there are $n \in \mathbb{N}$ and elements $m_1, \ldots, m_n \in M$ such that $\langle m_1, \ldots, m_n \rangle = M$.*
Let M_i for $i \in I$ be submodules. We write

$$\sum_{i \in I} M_i := \{ \sum_{j \in J} m_j \mid J \subseteq I \text{ finite subset}, m_j \in M_j \text{ for } j \in J \}.$$

It is an R-submodule of M and it is called the sum of the submodules M_i, $i \in I$. *If the set I is finite, one also writes $+$, for example $M_1 + M_2 + \cdots + M_n$. One then has*

$$M_1 + M_2 + \cdots + M_n = \{ \sum_{i=1}^{n} m_i \mid m_1 \in M_1, m_2 \in M_2, \ldots, m_n \in M_n \}.$$

The reason why in the above definition we always have to take finite subsets $J \subseteq I$ is that in algebra only finite sums are allowed unless one has 'completed' the module. The mathematical theory of Analysis is based on completion (the reals are the completion of the rationals with respect to the standard absolute value); also in algebra one can do completions (generalising those from Analysis), but in this lecture we are probably not having the time to treat them.
The R-submodule $\langle m_i | i \in I \rangle$ can also be seen as the intersection of all submodules of M containing all m_i for $i \in I$; alternatively, it can be characterised as the smallest submodule of M containing all the m_i for $i \in I$. Furthermore, the R-submodule $\sum_{i \in I} M_i$ can be seen as the R-submodule of M generated by all elements from all M_i.

Proposition 2.9. *Let R be a ring and $N \leq M$ be R-modules. The relation $x \sim y :\Leftrightarrow x - y \in N$ defines an equivalence relation on M. The equivalence classes $\overline{x} = x+N$ form the R-module denoted M/N with*

- $+ : M/N \times M/N \to M/N, \ \ (x+N, y+N) \mapsto x+y+N$,
- $0 = \overline{0} = 0 + N = N$ *as neutral element w.r.t.* $+$,
- $. : R \times M/N \to M/N, \ \ (r, x+N) \mapsto rx + N$.

The R-module M/N is called the quotient of M by (or modulo) N *(also called* factor module*).*

Proof. This works precisely as for quotient rings, which are treated in an exercise. □

Proposition 2.10 (Homomorphism and isomorphism theorems for modules)**.** *Let R be a ring.*

(a) Let M, N be R-modules and $\varphi : M \to N$ be an R-homomorphism. Then the map

$$M/\ker(\varphi) \to \operatorname{im}(\varphi), \ \ m + \ker(\varphi) \mapsto \varphi(m)$$

is well-defined and an R-isomorphism.

(b) Let M be an R-module and let $N_1 \subseteq N_2$ be R-submodules of M. Then there is an R-isomorphism

$$(M/N_1)/(N_2/N_1) \cong M/N_2.$$

(c) Let M be an R-module and let N_1 and N_2 be R-submodules of M. Then there is an R-isomorphism

$$(N_1 + N_2)/N_1 \cong N_2/(N_1 \cap N_2).$$

Proof. Exercise. □

3 Integrality

Aims:

- Learn and master the concept of algebraic elements and algebraic field extensions;
- learn and master the concept of integral elements and integral ring extensions;
- know examples and standard theorems;
- be able to prove simple properties.

In this section, we introduce a generalisation of the integers $\mathbb{Z}$. As known from and studied at school, the integers can be characterised as those rational numbers that can be written with denominator 1. We will define integers in any finite extension of the rationals, and even beyond, called 'algebraic integers'. This new notion will not only be useful in number theory, but also allow us to study the geometry of curves. An example of an algebraic integer is $\sqrt{2}$, whereas $\frac{\sqrt{2}}{2} = \frac{1}{\sqrt{2}}$ is not an algebraic integer.
We assume some basic familiarity with fields and field extensions (see the appendix to this section for some details). In this section we shall introduce *algebraic field extensions* and their natural generalisation *integral ring extensions* in parallel.

Our guiding example is the following one. Consider the set

$$A := \{a + b\sqrt{2} \in \mathbb{C} \mid a, b \in \mathbb{Z}\}.$$

We claim that it is a subring of $\mathbb{C}$, that is, $A \subset \mathbb{C}$ is a ring extension. The only thing that one really needs to check is that A is stable under multiplication:

$$(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + (\sqrt{2}\sqrt{2})bd) + \sqrt{2}(ad + bc) = (ac + 2bd) + \sqrt{2}(ad + bc) \in A.$$

The only thing we used is $\sqrt{2}\sqrt{2} = 2 \in \mathbb{Z}$. Formulated in a fancy way this is: $\sqrt{2}$ is a zero of the polynomial $X^2 - 2 \in \mathbb{Z}[X]$. This property will be expressed below as '$\sqrt{2}$ is integral over $\mathbb{Z}$'.
Let us just point out that the set $\{a + b\sqrt[3]{2} \in \mathbb{C} \mid a, b \in \mathbb{Z}\}$ is not a subring of $\mathbb{C}$ because $\sqrt[3]{2}\sqrt[3]{2} \notin \mathbb{Z}$. However, the ring $\{a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2 \in \mathbb{C} \mid a, b, c \in \mathbb{Z}\}$ is a subring of $\mathbb{C}$ (easy check! One will notice that the fact that $\sqrt[3]{2}$ is a zero of $X^3 - 2 \in \mathbb{Z}[X]$ is the property one needs.).
As a negative example let us state (at this point without proof) that for no $n \in \mathbb{N}$ the set $\{\sum_{i=0}^{n} a_i\pi^i \in \mathbb{C} \mid a_0, \ldots, a_n \in \mathbb{Z}\}$ is a subring of $\mathbb{C}$.

Generation of subrings and subfields

We first explain generation of subrings.

Lemma 3.1. *Let $R \subseteq S$ be rings.*

(a) Let $a \in S$. Then the evaluation map

$$\mathrm{ev}_a : R[X] \to S, \quad \sum_{i=0}^{d} c_i X^i \mapsto \sum_{i=0}^{d} c_i a^i$$

is a ring homomorphism. The map is expressed more concisely as $R[X] \ni f(X) \mapsto f(a) \in S$.

(b) (The same as (a) for more than one element.) Let $a_i \in S$ for $i \in I$ (some 'indexing' set). Then the evaluation map

$$\mathrm{ev}_{(a_i)_{i\in I}} : R[X_i \mid i \in I] \to S, \quad f((X_i)_{i\in I}) \mapsto f((a_i)_{i\in I})$$

is a ring homomorphism.

Proof. Exercise. □

Definition 3.2. *Assume the set-up of Lemma 3.1.*

(a) The image of ev_a is called the subring of S generated by a over R *and denoted as $R[a]$.*

(b) The image of $\mathrm{ev}_{(a_i)_{i\in I}}$ is called the subring of S generated by the $(a_i)_{i\in I}$ over R *and denoted as $R[(a_i)_{i\in I}]$. If $I = \{1, 2, 3, \ldots, n\}$ is a finite set, we also write $R[a_1, \ldots, a_n]$.*

Note that $R[a]$ and $R[(a_i)_{i\in I}]$ are indeed subrings, since images of ring homomorphisms are always subrings. Very explicitly, the elements of $R[a]$ are all of the form $\sum_{i=0}^{d} r_i a^i$ with $d \in \mathbb{N}$ and $r_0, \ldots, r_n \in R$. Of course, sums, differences and products of such elements are again of the same form (providing a direct proof that $R[a]$ is a subring of S).

Example 3.3. *(a) The subring $\mathbb{Z}[2]$ of $\mathbb{C}$ is equal to $\mathbb{Z}$.*

(b) The subring $\mathbb{Z}[\sqrt{2}]$ of $\mathbb{C}$ is the ring A discussed in the beginning of this section. Reason:

$$\sum_{i=0}^{n} r_i \sqrt{2}^i = \sum_{i=0 \text{ even}}^{n} r_i 2^{i/2} + (\sum_{i=1 \text{ odd}}^{n} r_i 2^{(i-1)/2}) \sqrt{2}.$$

Note that $\mathbb{Z}[\sqrt{2}]$ is finitely generated as a $\mathbb{Z}$-module (i.e. as an abelian group).

We will be able to express this property by saying that $\sqrt{2}$ is integral *over $\mathbb{Z}$.*

(c) The subring $\mathbb{Z}[\frac{1}{2}]$ of $\mathbb{C}$ is contained in $\mathbb{Q}$. It is NOT finitely generated as a $\mathbb{Z}$-module.

Reason: Consider a finite set of elements $\frac{a_1}{2^{e_1}}, \ldots, \frac{a_n}{2^{e_n}}$ and let f be bigger than all $e_1, \ldots, e_n$. One can never express $\frac{1}{2^f}$ as a $\mathbb{Z}$-linear combination of the elements of the chosen set. Hence, there cannot exist a finite generating set.

This (negative) property will be expressed below as $\frac{1}{2}$ is not integral over $\mathbb{Z}$.

Let us also define the notion of the subfield generated by a set of elements. It need not coincide with the subring generated by the same set of elements because of the possible existence of non-invertible elements.
Note that the intersection of any set of subfields of a field L is again a field. Hence, it makes sense to speak of the smallest subfield of L containing a given set of elements; namely, one can define it as the intersection of all subfields of L containing that set of elements.

Definition 3.4. *Let L/K be a field extension and $a \in L$. Define $K(a)$ to be the smallest subfield of L containing a. We say that $K(a)$ is* the subfield of L generated by a over K *or* K adjoined a.
If $a_i \in L$ for $i \in I$ (some 'indexing' set), we define $K(a_i \mid i \in I)$ to be the smallest subfield of L containing a_i for all $i \in I$. It is also called the subfield of L generated by a over K *or* K adjoined the a_i for $i \in I$.

Lemma 3.5. *Let L/K be a field extension and $a \in L$. Then* $\mathrm{Frac}(K[a]) = K(a)$.

Proof. The inclusion $K[a] \subseteq K(a)$ implies $\mathrm{Frac}(K[a]) \subseteq K(a)$. As $K(a)$ is the intersection of all fields containing K and a, one also has $K(a) \subseteq \mathrm{Frac}(K[a])$. □

We now give examples analogous to the previous ones.

Example 3.6. *(a) The subring $\mathbb{Q}(2)$ of $\mathbb{C}$ is equal to $\mathbb{Q}$.*

(b) The subring $\mathbb{Q}(\sqrt{2})$ of $\mathbb{C}$ is equal to $\mathbb{Q}[\sqrt{2}]$ because the latter ring is already a field: The inverse of $a + b\sqrt{2} \neq 0$ is $\frac{a}{a^2-2b^2} - \frac{b}{a^2-2b^2}\sqrt{2}$. Note that the denominator is never 0. For, if it were, then $\sqrt{2} = \frac{a}{b} \in \mathbb{Q}$.

Below we will give a general argument that also implies this fact because $\sqrt{2}$ will turn out to be algebraic over $\mathbb{Q}$, in the definition to come.

(c) The subring $\mathbb{Q}[\frac{1}{2}]$ of $\mathbb{Q}$ is equal to $\mathbb{Q}$.

Algebraic elements

Let us specialise to fields and let $R = K \subseteq S = L$ be a field extension and $a \in L$. The question we are now going to address is when $K[a]$ is a finite or an infinite dimensional K-vector space.
The simple but very important idea is to consider the two alternatives:

(1) The elements $1 = a^0, a, a^2, a^3, a^4, \ldots$ are K-linearly independent.

(2) The elements $1 = a^0, a, a^2, a^3, a^4, \ldots$ are K-linearly dependent.

In case (1) $K[a]$ is an infinite dimensional K-vector space.
In case (2) there exists a linear combination

$$0 = \sum_{i=0}^{n} r_i a^i$$

for some $n \in \mathbb{N}$, $r_i \in K$ for $0 \leq i \leq n$ and $r_n \neq 0$. By dividing by r_n, we can assume that the linear combination takes the form

$$0 = a^n + \sum_{i=0}^{n-1} r_i a^i.$$

We can interpret this equality as follows: The monic polynomial $f(X) := X^n + r_{n-1}X^{n-1} + \cdots + r_1 X + r_0 \in K[X]$ has a as a zero: $f(a) = 0$. In the next proposition we see that $K[a]$ is a finite dimensional K-vector space, and in fact even a field itself, hence, $K[a]$ is a finite field extension of K.

Definition 3.7. *Let K be a field and L/K a field extension.*
An element $a \in L$ is called algebraic over K *if there is a non-zero polynomial $f \in K[X]$ such that $f(a) = 0$ (i.e. a is a zero (also called root) of f). By dividing by the leading coefficient of f, we can without loss of generality assume that f is monic (cf. Definition 3.11 below).*
An element $a \in L$ that is not algebraic over K is also called transcendental over K.

Note that algebraic is a *relative* notion. An element is algebraic *over* some field.

Proposition 3.8. *Let K be a field and L/K a field extension and $a \in L$.*

(a) The evaluation map $\mathrm{ev}_a : K[X] \to L$ *given by $f \mapsto f(a)$ (see Lemma 3.1) is injective if and only if a is transcendental over K.*

(b) If a is algebraic over K, then there is a unique monic polynomial $m_a \in K[X]$ such that $(m_a) = \ker(\mathrm{ev}_a)$ (i.e. the principal ideal (m_a) is equal to the kernel of the evaluation map).

The polynomial m_a is called the minimal polynomial of a over K.

(c) Let a be algebraic over K. Then the minimal polynomial $m_a \in K[X]$ of a over K is irreducible (as element of $K[X]$). It can also be characterised as the monic polynomial in $K[X]$ of smallest degree having a as a zero.

(d) Let a be algebraic over K. Then the induced map

$$\mathrm{ev}_a : K[X]/(m_a) \to L, \quad f + (m_a) \mapsto f(a)$$

is an injective field homomorphism and identifies $K[X]/(m_a)$ with $K[a]$ and $K(a)$.

(e) Let a be algebraic over K. Then $K(a)$ is a finite extension of K and its degree $[K(a) : K]$ is equal to the degree of the minimal polynomial m_a of a over K. A K-basis of $K(a)$ is given by $1, a, a^2, \ldots, a^{d-1}$, where $d = [K(a) : K]$.

Proof. (a) If a is algebraic over K, then there is a non-zero polynomial $f \in K[X]$ such that $f(a) = 0$. This just means that f is in the kernel of the evaluation map, so ev_a is not injective. Conversely, if ev_a is not injective, then there is some non-zero polynomial f in the kernel of the evaluation map. That, however, just means $f(a) = 0$, whence a is algebraic.
(b) We know that $K[X]$ is a principal ideal domain. Hence, the kernel of ev_a is a principal ideal, so, it is generated by one element f. As ev_a is not injective (a is assumed to be algebraic), f is non-zero. A generator of a principal ideal is unique up to units in the ring. So, f is unique up to multiplication by a unit of K, i.e. up to multiplication by an element from $K \setminus \{0\}$. If f is of the form $r_d X^d + r_{d-1} X^{d-1} + \cdots + r_0 \in K[X]$ with $r_d \neq 0$, then $m_a := \frac{1}{r_d} f = X^d + \frac{r_{d-1}}{r_d} X^{d-1} + \cdots + \frac{r_0}{r_d}$ is the desired unique polynomial.
(c) Let $f \in K[X]$ be a nonzero polynomial such that $f(a) = 0$. Then $f \in \ker(\mathrm{ev}_a) = (m_a)$, so that $m_a \mid f$, implying that the degree of m_a is less than or equal to the degree of f.
If m_a were reducible, then we would have $m_a = fg$ with $f, g \in K[X]$ both of smaller degree than the degree of m_a. But $0 = m_a(a) = f(a)g(a)$ would imply that $f(a) = 0$ or $g(a) = 0$. Both would contradict the minimality of the degree of m_a.
(d) Since m_a is irreducible, $K[X]/(m_a)$ is a field. The injectivity follows from the isomorphism theorem for rings Proposition 1.26. Since $K[a]$ is a field, $K[a] = \mathrm{Frac}(K[a]) = K(a)$ by Lemma 3.5.
(e) is clear. □

Example 3.9. *(a) Let K be a field. Every $a \in K$ is algebraic over K. Indeed, a is a zero of the polynomial $X - a \in K[X]$.*

(b) $\sqrt{2}$ is algebraic over $\mathbb{Q}$. Indeed, $\sqrt{2}$ is a zero of the polynomial $X^2 - 2 \in \mathbb{Q}[X]$. Note that the polynomial $X - \sqrt{2}$ may not be used here, since its coefficients are not in $\mathbb{Q}$!

(c) π is transcendental over $\mathbb{Q}$. This is the theorem of Lindemann (from analysis). It implies by Galois theory that the circle cannot be squared using compass and ruler. By this we refer to the ancient problem of constructing a square whose area is equal to that of a given circle, just using a (non-marked) ruler and a compass.

(d) π is algebraic over $\mathbb{R}$ (special case of (a)).

(e) $i = \sqrt{-1}$ is algebraic over $\mathbb{Q}$.

Let us be more explicit about the field $K(a)$ and show how to write sums and products in terms of the basis. Write the minimal polynomial of a over K as $m_a = X^d + c_{d-1} X^{d-1} + \cdots + c_0$. We know that then $K(a)$ can be represented as a K-vector space with basis $1, a, a^2, a^3, \ldots, a^{d-1}$. Suppose we have two such elements $\alpha = \sum_{i=0}^{d-1} r_i a^i$ and $\beta = \sum_{i=0}^{d-1} s_i a^i$ (with $r_i, s_i \in K$). Of course, the addition in $K(a)$ is the addition in L and comes down to:

$$\alpha + \beta = \sum_{i=0}^{d-1} (r_i + s_i) a^i.$$

But, how to multiply them and express the result in terms of the basis? Of course, we have to multiply out, yielding

$$\alpha \cdot \beta = \sum_{n=0}^{2(d-1)} \big(\sum_{i,j \text{ s.t. } i+j=n} r_i s_j \big) a^n.$$

But, what to do with a^n for $n \geq d$? Apply the minimal polynomial!

$$a^d = -\big(c_{d-1}a^{d-1} + \cdots + c_0\big).$$

We can use this to eleminate all a^n for $n \geq d$. Suppose the highest occuring power of a is a^m with $m \geq d$. Then, we multiply the above equation through with a^{m-d} and obtain:

$$a^m = -\big(c_{d-1}a^{m-1} + \cdots + c_0 a^{m-d}\big).$$

Using this, we are left with powers a^{m-1} at worst, and can apply this process again and again until only powers a^n with $n \leq d-1$ occur.

Example 3.10. *Consider the example $\mathbb{Q}(\sqrt{5})$. The minimal polynomial of $\sqrt{5}$ over $\mathbb{Q}$ (say, as an element of $\mathbb{R}$) is $X^2 - 5$, so $\mathbb{Q}(\sqrt{5})$ is the image of $\mathbb{Q}[X]/(X^2-5)$ in $\mathbb{R}$. The above $\mathbb{Q}$-basis is $1, \sqrt{5}$. So, we express any element of $\mathbb{Q}(\sqrt{5})$ as $a + b\sqrt{5}$ with $a, b \in \mathbb{Q}$.*
Now let two such elements be given $\alpha = a_0 + a_1\sqrt{5}$ and $\beta = b_0 + b_1\sqrt{5}$. Then

$$\alpha + \beta = (a_0 + b_0) + (a_1 + b_1)\sqrt{5}$$

and

$$\begin{aligned}\alpha \cdot \beta &= (a_0 + a_1\sqrt{5})(b_0 + b_1\sqrt{5}) = a_0b_0 + \sqrt{5}(a_0b_1 + a_1b_0) + a_1b_1(\sqrt{5})^2 \\ &= (a_0b_0 + 5a_1b_1) + \sqrt{5}(a_0b_1 + a_1b_0).\end{aligned}$$

Integral elements

Integral elements are generalisations of algebraic elements in the context of a ring R instead of the field K. For algebraic elements the minimal polynomial is the unique *monic* polynomial of minimal degree annihilating the element; but, in fact, we do not really care whether the polynomial is monic, since we can always divide by the leading coefficient. So, the choice of defining the minimal polynomial of an algebraic element as a monic polynomial is actually quite arbitrary, one might do it differently without changing anything in the theory. Over rings the situation is different, since we cannot divide by the leading coefficient in general.
Why are monic minimal polynomials useful? We want to construct extensions: Let L/K be a field extension and $a \in L$ be algebraic over $\mathbb{Q}$ with minimal polynomial $m_a = X^n + c_{n-1}X^{n-1} + \cdots + c_0$. This just means

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

so that we can express a^n in terms of linear combinations with coefficients in K of powers of a of lower exponents. This is precisely what we need in order for

$$\{r_{n-1}a^{n-1} + \cdots + r_0 \mid r_i \in K, i \in \{1, \ldots, n-1\}\}$$

to be a ring (as calculated in the discussion of algebraic elements).
Suppose now we work over a ring R instead of a field K. Let S be a ring containing R. Assume for a moment that $a \in S$ satisfies

$$c_n a^n = -(c_{n-1}a^{n-1} + \cdots + c_0),$$

i.e. a non-monic linear combination with coefficients in R. Note that we now cannot express a^n as a linear combination of lower powers of a with coefficients in R, unless $c_n \in R^\times$. Hence, the set

$$\{r_{n-1}a^{n-1} + \cdots + r_0 \mid r_i \in R, i \in \{1, \ldots, n-1\}\}$$

is not stable under multiplication!
The morale is that we must use monic minimal polynomials (at least polynomials whose leading coefficient is a unit), when we work over rings and want to construct extensions similar to those over fields.
This motivates the following fundamental definition.

Definition 3.11. *Let $R \subseteq S$ be rings. An element $a \in S$ is called* integral over R *if there exists a monic polynomial $f \in R[X]$ such that $f(a) = 0$.*

Note that integrality is also a relative notion; an element is integral *over* some ring. Also note the similarity with algebraic elements; we just added the requirement that the polynomial be monic, for the reasons explained above.

Example 3.12. *(a) The elements of $\mathbb{Q}$ that are integral over $\mathbb{Z}$ are precisely the integers of $\mathbb{Z}$.*

(b) $\sqrt{2} \in \mathbb{R}$ is integral over $\mathbb{Z}$ because $X^2 - 2$ annihilates it.

(c) $\frac{1+\sqrt{5}}{2} \in \mathbb{R}$ is integral over $\mathbb{Z}$ because $X^2 - X - 1$ annihilates it.

(d) $a := \frac{1+\sqrt{-5}}{2} \in \mathbb{C}$ is not integral over $\mathbb{Z}$ because $f = X^2 - X + \frac{5}{2}$ annihilates it. If there were a monic polynomial $h \in \mathbb{Z}[X]$ annihilating a, then we would have $h = fg$ with some monic polynomial $g \in \mathbb{Q}[X]$. Since $h \in \mathbb{Z}[X]$, a lemma of Gauß that is proved in most basic algebra classes implies that both f and g are in $\mathbb{Z}[X]$, which is a contradiction.

(e) Let K be a field and S a ring containing K (e.g. $L = S$ a field as above) and $a \in S$. Then a is integral over K if and only if a is algebraic over K.

Indeed, as K is a field any polynomial with coefficients in K can be made monic by dividing by the leading coefficient. So, if we work over a field, then the new notion of integrality is just the notion of algebraicity from above.

Algebraic field extensions and integral ring extensions

We treat fields and rings in parallel in order to make it obvious that (and how) integrality is a generalisation of algebraicity.

Definition 3.13. *Let K be a field and L/K a field extension.*
The field extension L/K is called algebraic *(alternatively, L is called an* algebraic field extension of K*) if every $a \in L$ is algebraic over K.*
If L/K is not algebraic, it is called transcendental.

We now generalise the notion of 'algebraic field extension' to rings.

Definition 3.14. *A ring extension $R \subseteq S$ is called* integral *if all $s \in S$ are integral over R.*

Characterisation by finiteness properties

We first characterise algebraic elements by a finiteness property.

Proposition 3.15. *Every finite field extension L/K is algebraic. It can be generated by finitely many elements of L (that are automatically algebraic over K).*

Proof. Let $a \in L$ be any element. Since $K[a]$ is a subfield of L, it must also be a finite extension of K. Hence, a is algebraic over K.
We now show that L/K can be generated by finitely many elements of L (which are automatically algebraic, since we have already seen that L/K is algebraic). Take any $a_1 \in L \setminus K$. One has $K \subsetneq K(a_1)$, hence $[L : K] > [L : K(a_1)]$. If $K(a_1) \neq L$, then take $a_2 \in L \setminus K(a_1)$. We get $K(a_1) \subsetneq K(a_1, a_2) \subseteq L$, hence $[L : K(a_1)] > [L : K(a_1, a_2)]$. Like this we continue. As the degree is a positive integer greater than or equal to 1, this process will end at some point and then $K(a_1, a_2, \ldots, a_n) = L$. □

Proposition 3.16. *Let L/K be a field extension and $a_1, \ldots, a_n \in L$. Then the following two statements are equivalent:*

(i) All the a_i for $i = 1, \ldots, n$ are algebraic over K.

(ii) The field extension $K(a_1, \ldots, a_n)/K$ is finite.

Proof. (i) ⇒ (ii): Proposition 3.8 and induction.
(ii) ⇒ (i): Every finite field extension is algebraic by Proposition 3.15, hence, by definition the a_i for $i = 1, \ldots, n$ are algebraic over K. □

This characterisation allows us to show a very important source of algebraic field extensions (for this course), namely the number fields, whose defininition we give/recall now.

Definition 3.17. *A finite field extension K of $\mathbb{Q}$ is called a* number field.

Example 3.18. *(a) $\mathbb{Q}$ is a number field (but: $\mathbb{R}$ is not a number field).*

(b) $\mathbb{Q}[X]/(f(X))$ is a number field with an irreducible non-constant polynomial $f \in \mathbb{Q}[X]$.

(c) $\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$ for $0, 1 \neq d \in \mathbb{Z}$ square-free, is a number field of degree 2 (a quadratic field).

Our next goal is to achieve a characterisation of integral elements, generalising the one for algebraic elements given above. For this, we need to apply some more general tools from linear algebra: vector spaces (if L/K is a field extension, we saw L as a K-vector space and that was a very important tool) will have to be replaced by modules. The important thing to remark is that one does not have the notion of dimension over rings, so the proofs will have to change a bit.
Recall from Linear Algebra:

Proposition 3.19 (Cramer's rule)**.** *Let R be a ring and $M = (m_{i,j})_{1\leq i,j\leq n}$ be an $n \times n$-matrix with entries in R. The* adjoined matrix *is defined as $M^* = (m^*_{i,j})_{1\leq i,j\leq n}$ with entries*

$$m^*_{i,j} := (-1)^{i+j} \det(M_{i,j}),$$

where $M_{i,j}$ is the matrix obtained from M by deleting the i-th column and the j-th row.
Then the following equation holds:

$$M \cdot M^* = M^* \cdot M = \det(M) \cdot \mathrm{id}_{n\times n}.$$

We can now state and prove the following equivalent descriptions of integrality.

Proposition 3.20. *Let S be a ring, $R \subseteq S$ a subring and $a \in S$. Then the following statements are equivalent:*

(i) *a is integral over R.*

(ii) *$R[a] \subseteq S$ is a finitely generated R-module.*

(iii) *$R[a]$ is contained in a subring $T \subseteq S$ such that T is a finitely generated R-module.*

(iv) *There is a finitely generated R-module $T \subseteq S$ which contains 1 and such that multiplication by a sends T into itself.*

Proof. (i) $\Rightarrow$ (ii): As a is integral over R, a relation of the form

$$a^n = -(c_{n-1}a^{n-1} + c_{n-2}a^{n-2} + \cdots + c_0)$$

holds. Hence, $R[a]$ can be generated as an R-module by $\{1, a, a^2, \ldots, a^{n-1}\}$.
(ii) $\Rightarrow$ (iii): Just take $T := R[a]$.
(iii) $\Rightarrow$ (iv): Take the same T.
(iv) $\Rightarrow$ (i): We must make a monic polynomial with coefficients in R annihilating a. For this we use Cramer's rule. As T is finitely generated as an R-module, we may pick a finite generating set $\{t_1, \ldots, t_n\}$, i.e. any element of $t \in T$ can be represented as $t = \sum_{j=1}^n r_j t_j$ with some $r_j \in R$ for $j \in \{1, \ldots, n\}$.
In particular, as multiplication by a sends T to itself, at_i can be written as

$$at_i = \sum_{j=1}^{n} d_{i,j} t_j.$$

Form the matrix $D = (d_{i,j})_{1\leq i,j\leq n}$. It has coefficients in R. Let $M := a\mathrm{id}_{n\times n} - D$. It is a matrix with coefficients in S. Note that we have

$$M \begin{pmatrix} t_1 \\ t_2 \\ \vdots \\ t_n \end{pmatrix} = \left(\begin{pmatrix} a & 0 & \cdots & 0 \\ 0 & a & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & a \end{pmatrix} - \begin{pmatrix} d_{1,1} & d_{1,2} & \cdots & d_{1,n} \\ d_{2,1} & d_{2,2} & \cdots & d_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ d_{n,1} & d_{n,2} & \cdots & d_{n,n} \end{pmatrix} \right) \begin{pmatrix} t_1 \\ t_2 \\ \vdots \\ t_n \end{pmatrix} = 0$$

By Cramer's rule, it follows

$$M^*M \begin{pmatrix} t_1 \\ t_2 \\ \vdots \\ t_n \end{pmatrix} = \det(M)\mathrm{id}_{n\times n} \begin{pmatrix} t_1 \\ t_2 \\ \vdots \\ t_n \end{pmatrix} = \det(M) \begin{pmatrix} t_1 \\ t_2 \\ \vdots \\ t_n \end{pmatrix} = 0,$$

so that $\det(M)t_j = 0$ for all $j \in \{1, \ldots, n\}$. But, as $1 = \sum_{j=1}^n e_j t_j$ for some $e_j \in R$, it follows

$$\det(M) = \det(M) \cdot 1 = \sum_{j=1}^{n} e_j \det(M) t_j = 0.$$

Hence, the characteristic polynomial of D:

$$f(X) := \det(X \cdot \mathrm{id}_{n\times n} - D)$$

is a monic polynomial with entries in R such that $f(a) = 0$, whence a is integral over R. □

Let us summarise this important proof in other words. The finite generation '(i) ⇒ (ii)' follows from the explicit way in which one can represent 'high' powers of a by lower ones using the relation $a^n = -(c_{n-1}a^{n-1} + c_{n-2}a^{n-2} + \cdots + c_0)$ coming from the definition of integrality. Note the importance of not having a non-unit coefficient in front of a^n! Otherwise the argument breaks down. The core of the argument is the implication '(iv) ⇒ (i)'. The finite generation and the stability of T under multiplication by a enables us to express this multiplication as a square matrix D with entries in R. Of course, a is an eigenvalue of D. As such, it should be a zero of the characteristic polynomial of D, which is a monic polynomial with coefficients in R. That is exactly what we show in the proof. The only complication is that we work over a ring, and hence the linear algebra becomes a bit more complicated (than in standard linear algebra courses, which work over fields or even $\mathbb{R}$); this forces us to apply Cramer's rule instead of a more direct argument.

Corollary 3.21. *Let S be a ring and R a subring. Furthermore, let $a_1, \ldots, a_n \in S$ be elements that are integral over R.*
Then $R[a_1, \ldots, a_n] \subseteq S$ is integral over R and it is finitely generated as an R-module.

Proof. Note that due to the implication (iii) ⇒ (i) of the Proposition it suffices to prove finite generation. We do this by induction. The case $n = 1$ is the implication (i) ⇒ (ii) of the Proposition.
Assume the corollary is proved for $n - 1$. Then we know that $R[a_1, \ldots, a_{n-1}]$ is finitely generated as an R-module, say, generated by $b_1, \ldots, b_m$. As a_n is integral over R, we have that $R[a_n]$ is generated by $1, a_n, a_n^2, \ldots, a_n^r$ for some $r \in \mathbb{N}$. Now, $R[a_1, \ldots, a_{n-1}, a_n]$ is generated by $b_i a_n^j$ with $i \in \{1, \ldots, m\}$ and $j \in \{0, \ldots, r\}$. □

The following consequence is clear.

Corollary 3.22. *Let S be a ring and R a subring. If S is finitely generated as an R-module, then S/R is an integral ring extension.*

Example 3.23. *The ring extensions $\mathbb{Z}[\sqrt{2}]/\mathbb{Z}$ and $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]/\mathbb{Z}$ are integral, whereas $\mathbb{Z}[\frac{1+\sqrt{3}}{2}]/\mathbb{Z}$ is not.*

Transitivity

Proposition 3.24. *Let $M/L/K$ be field extensions.*

(a) Assume L/K is algebraic and $a \in M$ is algebraic over L. Then a is algebraic over K.

(b) (Transitivity of algebraicity) M/K is algebraic if and only if M/L and L/K are algebraic.

Proof. (a) Let $a \in M$ and let $m_a = \sum_{i=0}^{d} c_i X^i \in L[X]$ be the minimal polynomial of a over L. The coefficients $c_i \in L$ are algebraic over K. Hence, the field extension $\widetilde{L} := K(c_0, c_1, \ldots, c_{d-1})$ of K is finite. Of course, a is algebraic over $\widetilde{L}$, hence $\widetilde{L}(a)$ is a finite field extension of $\widetilde{L}$. By multiplicativity of degrees, $\widetilde{L}(a)$ is a finite field extension of K, hence algebraic. In particular, a is algebraic over K.
(b) One direction is trivial, the other follows from (a). □

Corollary 3.25. *Let $R \subseteq S \subseteq T$ be rings. Then 'transitivity of integrality' holds:*

$$T/R \text{ is integral} \;\Leftrightarrow\; T/S \text{ is integral and } S/R \text{ is integral.}$$

Proof. This works precisely as for algebraic field extensions!
The direction '$\Rightarrow$' is trivial. Conversely, let $t \in T$. By assumption it is integral over S, i.e. t is annihilated by a monic polynomial $X^n + s_{n-1}X^{n-1} + \cdots + s_0 \in S[X]$. Since S is integral over R, all the coefficients lie in the finitely generated R-module $U := R[s_0, s_1, \ldots, s_{n-1}]$. As the coefficients of the minimal polynomial of t all lie in U, it follows that t is integral over U, whence $U[t]$ is finitely generated over U. But, as U is finitely generated over R, it follows that $U[t]$ is finitely generated over R (a generating system is found precisely as in proof of Corollary 3.21). In particular, t is integral over R. □

Algebraic closure and integral closure

We now introduce an important notion in field theory.

Definition 3.26. *Let L/K be a field extension.*

(a) The set

$$K_L := \{a \in L \mid a \text{ is algebraic over } K\}$$

is called the algebraic closure of K in L.

Note that L/K is algebraic if and only if $K_L = L$.

(b) We say that K is algebraically closed in L *if $K_L = K$.*

(c) A field K is called algebraically closed *if for any field extension L/K one has $K_L = K$.*

Note that this means that there is no proper algebraic field extension of K.

We immediately give the definition for ring extensions corresponding to (a). There is no exact analog of (b) for rings, in particular (b) and (c) of the following definition are NOT direct generalisations of (b) in the preceding definition.

Definition 3.27. *Let S be a ring and $R \subseteq S$ a subring.*

(a) *The set* $R_S = \{a \in S \mid a \text{ is integral over } R\}$ *is called the* integral closure of R in S *(compare with the algebraic closure of* R *in* S *– the two notions coincide if* R *is a field).*

An alternative name is: normalisation of R in S.

Note that S *is an* integral ring extension of R *if* $R_S = S$.

(b) R *is called* integrally closed in S *if* $R_S = R$.

We will see in a moment that the integral closure of R *in* S *is integrally closed in* S*, justifying the names.*

(c) *An integral domain* R *is called* integrally closed *(i.e. without mentioning the ring in which the closure is taken) if* R *is integrally closed in its fraction field.*

We need to understand these definitions better. We again start our discussion by the field situation.

Proposition 3.28. *Let* L/K *be a field extension.*

(a) *The algebraic closure* K_L *of* K *in* L *is an algebraic field extension of* K.

(b) *Any* $t \in L$ *that is algebraic over* K_L *lies in* K_L*. In other words,* K_L *is algebraically closed in* L *(justifying the name).*

Proof. (a) Firstly, $0, 1 \in K_L$ is clear. Let $a, b \in K_L$. We know that $K(a, b)$ is an algebraic field extension of K. Thus, $K(a, b) \subseteq K_L$. Consequently, $-a$, $1/a$ (if $a \neq 0$), $a + b$ and $a \cdot b$ are in $K(a, b)$, hence, also in K_L. This shows that K_L is indeed a field.
(b) This follows from the transitivity of algebraicity. □

We move on to rings and our next aim is to show in an elegant way that R_S is a ring. The idea is the same as for algebraic elements; we showed that $K(a)$ is a finite extension of K if and only if a is algebraic over K. Then it is clear that sums and products of algebraic elements are algebraic because the finitess property is clear.

Proposition 3.29. *Let* $R \subseteq S$ *be rings.*

(a) R_S *is a subring of* S.

(b) *Any* $t \in S$ *that is integral over* R_S *lies in* R_S*. In other words,* R_S *is integrally closed in* S *(justifying the name).*

Proof. (a) Just as for algebraic extensions! Let $a, b \in R_S$. As both of them are integral over R, the extension $R[a, b]$ is finitely generated as an R-module, hence integral. Thus, $a + b$, $a \cdot b$ are integral, whence $a + b$ and $a \cdot b$ are in R_S, showing that it is a ring (since 0 and 1 are trivially in R_S).
(b) Any $s \in S$ that is integral over R_S is also integral over R (by the transitivity of integrality), whence $s \in R_S$. □

Definition 3.30. *Recall that a* number field K *is a finite field extension of* $\mathbb{Q}$*. The* ring of integers of K *is the integral closure of* $\mathbb{Z}$ *in* K*, i.e.* $\mathbb{Z}_K$*. An alternative notation is* $\mathcal{O}_K$.

Example 3.31. *Let* $d \neq 0, 1$ *be a squarefree integer. The ring of integers of* $\mathbb{Q}(\sqrt{d})$ *is*

(1) $\mathbb{Z}[\sqrt{d}]$, *if* $d \equiv 2, 3 \pmod 4$,

(2) $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$, *if* $d \equiv 1 \pmod 4$.

(Proof as an exercise.)

Proposition 3.32. *Every UFD is integrally closed.*

Proof. Let R be a UFD with fraction field K. Let $x = \frac{b}{c} \in K$ be integral over R. We assume that b and c are coprime (i.e. do not have a common prime divisor). We want to show that $x \in R$.
Start with the equation annihilating x:

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

Multiply through with c^n and move b^n to the other side:

$$b^n = -c\big(a_{n-1}b^{n-1} + ca_{n-2}b^{n-2} + \cdots + c^{n-1}a_0\big),$$

implying $c \in R^\times$ (otherwise, this would contradict the coprimeness of b and c), so that $x = bc^{-1} \in R$. □

The following proposition shows, in particular, how one can write elements as fractions. In the situation of that proposition, any element of L can be written as a fraction $\frac{s}{r}$, where s is an integral element over R, and the denominator can be chosen in R. For instance, in $\mathbb{Q}(\sqrt{2})$, any element can be written as $\frac{a+b\sqrt{2}}{d}$ with $a, b, d \in \mathbb{Z}$ and, of course $d \neq 0$. One finds here that the integral elements are those that can be written with denominator 1. Attention! There's a little trap. The analog in $\mathbb{Q}(\sqrt{5})$ looks slightly different: any element can be written as $\frac{a+b\frac{1+\sqrt{5}}{2}}{d}$ again with $a, b, d \in \mathbb{Z}$ and $d \neq 0$; in that writing, an element is integral if and only if the denominator can be taken to be 1. Of course, one could simplify the writing to $\frac{r+s\sqrt{5}}{t}$ with $r, s, t \in \mathbb{Z}$, $t \neq 0$, but then there is an integral (over $\mathbb{Z}$) element which needs a 2 in the denominator, namely $\frac{1+\sqrt{5}}{2}$.

Proposition 3.33. *Let R be an integral domain, $K = \mathrm{Frac}(R)$, L/K a finite field extension and $S := R_L$ the integral closure of R in L. Then the following statements hold:*

(a) Every $a \in L$ can be written as $a = \frac{s}{r}$ with $s \in S$ and $0 \neq r \in R$, i.e. all denominators can be chosen in R.

(b) $L = \mathrm{Frac}(S)$ and S is integrally closed.

(c) If R is integrally closed, then $S \cap K = R$.

Proof. (a) Let $a \in L$ have the minimal polynomial over K

$$m_a(X) = X^n + \frac{c_{n-1}}{d_{n-1}}X^{n-1} + \frac{c_{n-2}}{d_{n-2}}X^{n-2} + \cdots + \frac{c_0}{d_0} \in K[X]$$

with $c_i, d_i \in R$ and $d_i \neq 0$ (for $i = 0, \ldots, n-1$). We form a common denominator $d := d_0 \cdot d_1 \cdot \cdots \cdot d_{n-1} \in R$, plug in a and multiply through with d^n:

$$0 = d^n m_a(a) = (da)^n + \frac{c_{n-1}d}{d_{n-1}}(da)^{n-1} + \frac{c_{n-2}d^2}{d_{n-2}}(da)^{n-2} + \cdots + \frac{c_0 d^n}{d_0} \in R[X],$$

showing that da is integral over R, i.e. $da \in S$, or in other words, $a = \frac{s}{d}$ for some $s \in S$.
(b) By (a) we know that L is contained in the fraction field of S. As S is contained in L, it is clear that also the fraction field of S is contained in L, showing the claimed equality. That S is integrally closed means that it is integrally closed in L. We have already seen that the integral closure of R in L is integrally closed in L.
(c) This is just by definition: If $s \in S$, then it is integral over R; if s is also in K, then as R is integrally closed (in K), it follows that $s \in R$. The other inclusion $S \cap K \supseteq R$ is trivial. □

We end this section with some short notes on algebraically closed fields.

Proposition 3.34. *A field K is algebraically closed if and only if any non-constant polynomial $f \in K[X]$ has a zero in K.*

Proposition 3.35. *Let K be a field. Then there exists an algebraic field extension $\overline{K}/K$ such that $\overline{K}$ is algebraically closed.*
The field $\overline{K}$ is called an algebraic closure of K *(it is not unique, in general).*

The proof is not so difficult, but, a bit long, so I am skipping it.

Example 3.36. *(a) $\mathbb{C}$ is algebraically closed; $\mathbb{R}$ is not. $\mathbb{R}_{\mathbb{C}} = \mathbb{C}$.*

(b) $\mathbb{Q}_{\mathbb{C}} = \{x \in \mathbb{C} \mid x$ is algebraic over $\mathbb{Q}\} =: \overline{\mathbb{Q}}$. We have $\overline{\mathbb{Q}}$ is an algebraic closure of $\mathbb{Q}$.

(c) Both $\overline{\mathbb{Q}}$ and $\mathbb{C}$ are algebraically closed, but $\mathbb{C}$ is not an algebraic closure of $\mathbb{Q}$ because the extension $\mathbb{C}/\mathbb{Q}$ is not algebraic.

(d) Note that $\overline{\mathbb{Q}}$ is countable (Exercise), since we can count the set of polynomials with coefficients in $\mathbb{Q}$ and each polynomial only has finitely many zeros; but, as we know, $\mathbb{C}$ is not countable.

Appendix: Background on fields

In this section we recall some background on field extension.

Definition 3.37. *A commutative ring R is called a* field *if $R^\times = R \setminus \{0\}$, that is, if all non-zero elements are (multiplicatively) invertible.*

Definition 3.38. *Let L be a field.*
A subring $K \subseteq L$ is called a subfield *if K is also a field. In that case, one also speaks of L as a* field extension *of K, denoted as L/K or $K \hookrightarrow L$.*
If L/K is a field extension, then L is a K-vector space with respect to the natural $+$ and $\cdot$, i.e. $+ : L \times L \to L$, $(x, y) \mapsto x + y$ (the $+$ is the $+$ of the field L) and scalar multiplication $+ : K \times L \to L$, $(x, y) \mapsto x \cdot y$ (the $\cdot$ is the $\cdot$ of the field L).
The degree *of L/K is defined as $[L : K] := \dim_K(L)$, the dimension of L as K-vector space.*
One says that L/K is a finite *field extension if $[L : K] < \infty$.*

Lemma 3.39 (Multiplicativity of field degrees)**.** *Let $K \subseteq L \subseteq M$ be finite field extensions. Then*

$$[M : K] = [M : L][L : K]$$

(in other words: $\dim_K M = (\dim_K L)(\dim_L M)$*.).*

Proof. Exercise. □

Proposition 3.40. *Let R be an integral domain. Then the following statements hold:*

(a) The relation

$$(r_1, s_1) \sim (r_2, s_2) \Leftrightarrow r_1 s_2 = r_2 s_1$$

defines an equivalence relation on $R \times (R \setminus \{0\})$. Denote the equivalence class of an element (r, s) by $\frac{r}{s}$. Let $\mathrm{Frac}(R)$ denote the set of equivalence classes.

(b) Define $+$ and $\cdot$ on $\mathrm{Frac}(R)$ by

$$\frac{r_1}{s_1} + \frac{r_2}{s_2} := \frac{r_1 s_2 + r_2 s_1}{s_1 s_2} \quad \text{and} \quad \frac{r_1}{s_1} \cdot \frac{r_2}{s_2} := \frac{r_1 r_2}{s_1 s_2}.$$

Then $\mathrm{Frac}(R)$ is a field with respect to $+$ and $\cdot$ with $0 = \frac{0}{1}$ and $1 = \frac{1}{1}$.

One calls $\mathrm{Frac}(R)$ the fraction field *(or* field of fractions*) of R.*

Proof. It suffices to make some easy checks. □

Note that it is essential that R is an integral domain. We will later in the lecture identify the fraction field with the localisation of R at the prime ideal (0).

Proof of Proposition 3.34. (a) Firstly, $0, 1 \in K_L$ is clear. Let $a, b \in K_L$. We know that $K(a, b)$ is an algebraic field extension of K. Thus, $K(a, b) \subseteq K_L$. Consequently, $-a$, $1/a$ (if $a \neq 0$), $a + b$ and $a \cdot b$ are in $K(a, b)$, hence, also in K_L. This shows that K_L is indeed a field.
(b) Assume K is algebraically closed and let $f \in K[X]$ be a non-constant polynomial. Let $g = \sum_{i=0}^{d} c_i X^i$ be a non-constant irreducible divisor of f. The natural injection $K \to K[X]/(g) =: M$ is a finite field extension of K (remember that (g) is a maximal ideal of the principal ideal domain $K[X]$). Now, the class $a := X + (g) \in M$ is a zero of g, since

$$g(a) = g(X + (g)) = \sum_{i=0}^{d} c_i (X + (g))^i = \sum_{i=0}^{d} c_i X^i + (g) = 0 + (g).$$

As K is algebraically closed, $M = K$, whence $a \in K$.
Conversely, suppose that K is such that any non-constant polynomial $f \in K[X]$ has a zero in K. This means that there are no irreducible polynomials in $K[X]$ of degree strictly bigger than 1. Let L/K be a field extension and $a \in L$ algebraic over K. The minimal polynomial $m_a \in K[X]$ is an irreducible polynomial admitting a as a zero. Hence, the degree of m_a is 1, whence $m_a = X - a$, so that $a \in K$, showing $K_L = K$. □

For constructing field extensions one needs irreducible polynomials. There are two very useful criteria for deciding that a given polynomial with rational coefficients is irreducible: the reduction criterion and the Eisenstein criterion.
Let A be a UFD. A polynomial $f(X) = \sum_{i=0}^{d} a_i X^i \in A[X]$ is called *primitive* if the greatest common divisors of its coefficients is 1. In particular, monic polynomials are primitive.
In order to understand the proofs we must recall some theory about the polynomial ring $A[X]$ for a UFD A.

Theorem 3.41 (Gauß)**.** *Let A be a UFD with field of fractions K.*

(a) $A[X]$ is a UFD.

(b) Let $f, g \in K[X]$ be monic polynomials. If $fg \in A[X]$, then $f, g \in A[X]$.

(c) Let $f \in A[X]$ be a non-constant primitive polynomial. Then the following statements are equivalent:

(i) f is irreducible in $A[X]$.

(ii) f is a prime element of $A[X]$.

(iii) f is a prime element of $K[X]$.

(iv) f is irreducible in $K[X]$.

Proof. Any book on Basic Algebra. □

Proposition 3.42 (Reduction criterion)**.** *Let A be a UFD and $f(X) = \sum_{i=0}^{d} a_i X^i \in A[X]$ a non-constant primitive polynomial. For a prime element $p \in A$ we consider the* reduction mod p*:*

$$\pi : A[X] \to A/(p)[X], \quad \sum_{i=0}^{r} a_i X^i \mapsto \sum_{i=0}^{r} \overline{a_i} X^i,$$

which is a ring homomorphism (here $\overline{a_i}$ denotes the class of a_i in $A/(p)$).
If p does not divide a_d and $\pi(f)$ is irreducible in $A/(p)[X]$, then f is irreducible in $K[X]$.

Proof. Suppose the contrary: $f = gh$ with $g, h \in A[X]$ non-constant. Hence, we have $\pi(f) = \pi(gh) = \pi(g)\pi(h)$. As $\pi(f)$ is irreducible, it follows that $\pi(g)$ or $\pi(h)$ is constant.
We now use $p \nmid a_d$. We write $g(X) = \sum_{i=1}^{r} b_i X^i$ and $h(X) = \sum_{i=1}^{s} c_i X^i$ with $b_r \neq 0 \neq c_s$. Since $a_d = b_r c_s$, we obtain that $p \nmid b_r$ and $p \nmid c_s$. Thus, the degree of $\pi(g)$ is equal to the degree of g, and the degree of $\pi(h)$ is equal to the degree of h. One thus sees that either g is constant or h is constant. This contradiction finishes the proof. □

Example 3.43. • *Consider $f_1(X) = X^2 + X + 1 \in \mathbb{Z}[X]$, $f_2(X) = X^2 + 15X - 53 \in \mathbb{Z}[X]$, $f_3(X) = X^2 + 14X - 55 \in \mathbb{Z}[X]$ and $f_4(X) = X^2 + 15X - 54 \in \mathbb{Z}[X]$.*

These polynomials are monic, hence primitive. Note that the polynomial $X^2 + X + 1 \in \mathbb{F}_2[X]$ is irreducible (for the polynomials of degree at most 3 it suffices to verify that they do not have a zero).

The reduction criterion modulo 2 thus shows that f_1 and f_2 are irreducible as elements of $\mathbb{Q}[X]$. This argumentation does not apply to f_3. The reduction of f_3 modulo 3 is $X^2+2X+2 \in \mathbb{F}_3[X]$ which is irreducible; hence, we obtain the same conclusion. For f_4 one cannot use reduction modulo 2 nor modulo 3. In fact, no criterion can work because $X^2 + 15X - 54 = (X + 18)(X - 3)$.

- *Let $A = \mathbb{Q}[T]$ and consider a polynomial of the form $f(T, X) = \sum_{i=0}^{d} a_i(T)X^i \in A[X]$. Note that T is a prime element of $\mathbb{Q}[T]$: if $T \mid g(T)h(T)$ with $g, h \in \mathbb{Q}[T]$, then either $T \mid h(T)$ or $T \mid g(T)$.*

  The reduction of a polynomial $a(T) \in A[T]$ modulo T is just the evaluation at zero, $a(0)$: if $a(T) = b_0 + b_1T + \cdots + b_eT^e$, then the class of $a(T)$ and the class of $b_0 = a(0)$ modulo T are the same because $a(T) - b_0 = T \cdot (b_1 + b_2T + \ldots b_eT^{e-1}) \in (T)$.

  Hence, if $f(T, X)$ is monic in the variable X and $f(0, X)$ is irreducible, then $f(T, X)$ is irreducible in $A[X] = \mathbb{Q}[T, X]$.

- *The polynomial $X^2+X+2TX+5T^2X+T^3+1 \in \mathbb{Q}[T, X]$ is irreducible because it is monic (in the variable X) and $f(0, X) = X^2 + X + 1$ is irreducible.*

Proposition 3.44 (Eisenstein criterion)**.** *Let A be a UFD and $f(X) = \sum_{i=0}^{d} a_iX^i \in A[X]$ a non-constant primitive polynomial. Let $p \in A$ be a prime element such that*

$$p \nmid a_d, \quad p \mid a_i \text{ for all } 0 \leq i \leq d-1 \quad \text{and } p^2 \nmid a_0.$$

Then f is irreducible $K[X]$.

Proof. Suppose the contrary and write $f = gh$ with $g(X) = \sum_{i=0}^{r} b_iX^i \in A[X]$ and $h(X) = \sum_{i=0}^{s} c_iX^i \in A[X]$ non-constant and $b_r \neq 0 \neq c_s$. Because of $a_d = b_rc_s$, the condition $p \nmid a_d$ implies $p \nmid b_r$ and $p \nmid c_s$. Because of $a_0 = b_0c_0$, the conditions $p \mid a_0$ and $p^2 \nmid a_0$ imply without loss of generality that $p \mid b_0$ and $p \nmid c_0$.
Let t be the smallest integer between 1 and r such that $p \nmid b_t$. Hence, $1 \leq t \leq r < d$ because $p \mid b_0$ and $p \nmid b_r$. Writing $c_i = 0$ for $i > s$ we find

$$\underbrace{a_t}_{\text{divisible by } p} = \underbrace{b_0c_t + b_1c_{t-1} + \cdots + b_{t-1}c_1}_{\text{divisible by } p} + \underbrace{b_tc_0}_{\text{not divisible by } p}.$$

This contradiction finishes the proof. □

Example 3.45.

- *Consider $f_1(X) = X^2 + 2X + 2 \in \mathbb{Z}[X]$ and $f_2(X) = X^7 + 72X^2 + 111X - 30 \in \mathbb{Z}[X]$. These polynomials are monic, hence primitive. The Eisenstein criterion with $p = 2$ shows that f_1 is irreducible in $\mathbb{Q}[X]$. The irreducibility of f_2 follows from the Eisenstein criterion with $p = 3$.*

- *Let p be a prime number and $A = \mathbb{F}_p[T]$. Let $f(T, X) = X^p - T \in A[X] = \mathbb{F}_p[T, X]$. As in Example 3.43 on sees that T is a prime element of A. The polynomial $f(T, X)$ satisfies the assumptions of the Eisenstein criterion as a polynomial in the variable X for the prime element T. Hence $f(T, X)$ is irreducible.*

  This polynomial is actually an example of an irreducible, but inseparable *polynomial.*

- *Let p be a prime number. Consider the polynomial $X^p-1 \in \mathbb{Q}[X]$. It is not irreducible because*

$$X^p - 1 = (X-1)\underbrace{(X^{p-1} + X^{p-2} + \cdots + X + 1)}_{=:\Phi_p(X)} \in \mathbb{Z}[X].$$

One calls $\Phi_p(X)$ the p-th cyclotomic polynomial (in German: Kreisteilungspolynom). *We now show that Φ_p is irreducible in $\mathbb{Q}[X]$.*

It suffices to show that $\Phi_p(X+1)$ is irreducible (because if $\Phi_p(X+1) = f(X)g(X)$, then $\Phi_p(X) = f(X-1)g(X-1)$). We have

$$\Phi_p(X+1) = \frac{(X+1)^p - 1}{(X+1)-1} = \frac{(X+1)^p - 1}{X} = \frac{\sum_{i=1}^{p} \binom{p}{i} X^i}{X} = X^p + \sum_{i=1}^{p-1} \binom{p}{i} X^{i-1},$$

which is an Eisenstein polynomial for the prime p because $p \mid \binom{p}{i}$ for all $1 \leq i \leq p-1$ and $p^2 \nmid \binom{p}{1} = p$. Hence, $\Phi_p(X)$ is irreducible in $\mathbb{Q}[X]$.

4 Affine plane curves

Aims:

- Learn and master the concept of affine algebraic sets;
- learn and master the concept of the Zariski topology;
- know first examples of the translation of geometric into algebraic properties;
- know examples and standard theorems;
- be able to prove simple properties.

Curves are known from and studied at school. Here we take an algebraic point of view on them. This point of view will enable us to express geometric properties in an algebraic way.

Definition 4.1. *Let K be a field and L/K a field extension. Let $n \in \mathbb{N}$. The set of L-*points of affine n-space *is defined as $\mathbb{A}^n(L) := L^n$ (i.e. n-dimensional L-vector space).*
Let $S \subseteq K[X_1, \ldots, X_n]$ be a subset. Then

$$\mathcal{V}_S(L) := \{(x_1, \ldots, x_n) \in \mathbb{A}^n(L) \mid f(x_1, \ldots, x_n) = 0 \text{ for all } f \in S\}$$

*is called the set of L-*points of the affine (algebraic) set belonging to S.
If $L = \overline{K}$ is an algebraic closure of K, then we also call $\mathcal{V}_S(\overline{K})$ the affine set belonging to S.
If the set S consists of a single non-constant polynomial, then $\mathcal{V}_S(\overline{K})$ is also called a hyperplane in $\mathbb{A}(\overline{K})$.
If $n = 2$ and $S = \{f\}$ with non-constant f, then $\mathcal{V}_S(\overline{K})$ is called a plane curve *(because it is a curve in the plane $\mathbb{A}^2(\overline{K})$. Its L-points are defined as $\mathcal{V}_S(L)$ for L/K a field extension.*

Convention: When the number of variables is clear, we write $K[\underline{X}]$ for $K[X_1, \ldots, X_n]$. In the same way a tuple $(x_1, \ldots, x_n) \in \mathbb{A}^n(K)$ is also abbreviated as $\underline{x}$ if no confusion can arise.
The letter 'V' is chosen because of the word 'variety'. But, we will define affine varieties below as 'irreducible' affine sets.

Example 4.2. *(a) $K = \mathbb{R}$, $n = 2$, $K[X, Y] \ni f(X, Y) = aX + bY + c$ non-constant. Then $V_{\{f\}}(\mathbb{R})$ is a line ($y = -\frac{a}{b}x - \frac{c}{b}$ if $b \neq 0$; if $b = 0$, then it is the line with x-coordinate $-\frac{c}{a}$ and any y-coordinate).*

(b) $K = \mathbb{R}$, $n = 2$, $K[X, Y] \ni f(X, Y) = X^2 + Y^2 - 1$. Then $V_{\{f\}}(\mathbb{R})$ is the circle in $\mathbb{R}^2$ around the origin with radius 1.

(c) $K = \mathbb{Q}$, $f(X, Y) := X^2 + Y^2 + 1$. Note $\mathcal{V}_{\{f\}}(\mathbb{R}) = \emptyset$, but $(0, i) \in \mathcal{V}_{\{f\}}(\mathbb{C})$.

(d) $K = \mathbb{F}_2$, $f(X, Y) := X^2 + Y^2 + 1 = (X + Y + 1)^2 \in \mathbb{F}_2[X]$. Because of $f(a, b) = 0 \Leftrightarrow a + b + 1 = 0$ for any $a, b \in L$, $L/\mathbb{F}_2$, we have

$$\mathcal{V}_{\{f\}}(L) = \mathcal{V}_{\{X+Y+1\}}(L),$$

which is a line.

Lemma 4.3. *A plane curve has infinitely many points over any algebraically closed field. More precisely, let K be a field, $\overline{K}$ an algebraic closure of K and $f(X, Y) \in K[X, Y]$ a non-constant polynomial.*
Then $\mathcal{V}_{\{f\}}(\overline{K})$ is an infinite set.

Proof. Any algebraically closed field has infinitely many elements. This can be proved using Euclid's argument for the infinity of primes, as follows. Suppose $\overline{K}$ only has finitely many elements $a_1, \ldots, a_n$. Form the polynomial $g(X) := 1 + \prod_{i=1}^{n}(X - a_i)$. Note that $g(a_i) = 1 \neq 0$ for all $i = 1, \ldots, n$. Hence, we have made a polynomial of positive degree without a zero, contradiction.
Back to the proof. We consider f as a polynomial in the variable Y with coefficients in $K[X]$, i.e.

$$f(X, Y) = \sum_{i=0}^{d} a_i(X)Y^i \quad \text{with } a_i(X) \in K[X].$$

First case: $d = 0$, i.e. $f(X, Y) = a_0(X)$. Let $x \in \overline{K}$ be any zero of $a_0(x)$, which exists as $\overline{K}$ is algebraically closed. Now (x, y) satisfies f for any $y \in \overline{K}$, showing the infinity of solutions.
Second case: $d > 0$. Then $a_d(x) \neq 0$ for all but finitely many $x \in \overline{K}$, hence, for infinitely many x. Note that the polynomial $f(x, Y) = \sum_{i=0}^{d} a_i(x)Y^i$ has at least one zero y, so that (x, y) satisfies f, again showing the infinity of solutions. □

Example 4.4. *(a) Let $K = \mathbb{Q}$ and consider $f(X, Y) = X^2 + Y^2 - 1$ and the $\mathbb{Q}$-points of the associated curve $C = S^1 = \mathcal{V}_{\{f\}}(\mathbb{Q})$. They correspond in a precise way to primitive pythagorean triples (a, b, c) for $a, b, c \in \mathbb{Z}$ and $a^2 + b^2 = c^2$. For details see an exercise.*

Note that this is a nice and first illustration of the deep relations between geometry and number theory (algebra). We will encounter several in this course.

(b) Let K be a field and consider $f(X,Y) = X^2 + Y^2$.

The only solution of the form $(x,0)$ is $(0,0)$ in any field K. Suppose now (x,y) is a solution with $y \neq 0$. Then $x^2 = -y^2$, or $z^2 = -1$ with $z = \frac{x}{y}$.

Hence, $\mathcal{V}_{\{f\}}(K) = \{(0,0)\}$ if and only if $X^2 = -1$ has no solution in K.

In particular, $\mathcal{V}_{\{f\}}(\mathbb{R}) = \{(0,0)\}$ (but: $\mathcal{V}_{\{f\}}(\mathbb{C}) = \mathcal{V}_{\{X-iY\}}(\mathbb{C}) \cup \mathcal{V}_{\{X+iY\}}(\mathbb{C})$, union of two lines) and $\mathcal{V}_{\{f\}}(\mathbb{F}_p) = \{(0,0)\}$ if and only if $p \equiv 3 \pmod 4$.

Example 4.5. *Let K be a field and $f(X) = X^3 + aX^2 + bX + c$ be a separable polynomial (meaning that it has no multiple zeros over $\overline{K}$).*
Any plane curve of the form $\mathcal{V}_{\{Y^2 - f(X)\}}$ is called an elliptic curve*. It has many special properties (see e.g. lectures on cryptography).*

Definition 4.6. *Let $\mathcal{X}$ be a set and $\mathcal{O}$ a set of subsets of $\mathcal{X}$ (i.e. the elements of $\mathcal{O}$ are sets; they are called the* open sets*).*
Then $\mathcal{O}$ is called a topology on $\mathcal{X}$ *(alternatively: $(\mathcal{X}, \mathcal{O})$ is called a* topological space*) if*

(1) $\emptyset, \mathcal{X} \in \mathcal{O}$ (in words: the empty set and the whole space are open sets);

(2) if $A_i \in \mathcal{O}$ for $i \in I$, then $\bigcup_{i \in I} A_i \in \mathcal{O}$ (in words: the union of arbitrarily many open sets is an open set);

(3) if $A, B \in \mathcal{O}$, then $A \cap B \in \mathcal{O}$ (in words: the intersection of two (and, consequently, finitely many) open sets is an open set).

A set $C \subseteq \mathcal{X}$ is called closed *if $\mathcal{X} \setminus C \in \mathcal{O}$ (in words: the closed sets are the complements of the open sets).*

The basic example known from any first course on Analysis is the topology on $\mathbb{R}$ or, more generally, on $\mathbb{R}^n$. In the latter case one defines $\mathcal{O}$ to consist of those sets $U \subseteq \mathbb{R}^n$ such that for every $x \in U$ there is $\epsilon > 0$ such that all $y \in \mathbb{R}^n$ with $|y - x| < \epsilon$ belong to U. These are by definition the open subsets of $\mathbb{R}^n$. It is a well-known exercise to show that $\mathcal{O}$ is indeed a topology on $\mathbb{R}^n$. One be aware that this standard topology behaves very differently from the topology on $\mathbb{A}^n(K)$ that we are going to define now.

Proposition 4.7. *Let K be a field and $n \in \mathbb{N}$. Define*

$$\mathcal{O} := \{\mathbb{A}^n(K) \setminus \mathcal{V}_S(K) \mid S \subseteq K[X_1, \ldots, X_n]\}.$$

Then $(\mathbb{A}^n(K), \mathcal{O})$ is a topological space. The thus defined topology is called the Zariski topology on $\mathbb{A}^n(K)$.
Note that, in particular, the closed subsets of $\mathbb{A}^n(K)$ for the Zariski topology are precisely the affine sets.

Lemma 4.8. *Let K be a field, L/K a field extension and $n \in \mathbb{N}$.*

(a) $\mathcal{V}_{\{(0)\}}(L) = \mathbb{A}^n(L)$ and $\mathcal{V}_{\{(1)\}}(L) = \emptyset$.

(b) Let $S \subseteq T \subseteq K[X_1, \ldots, X_n]$ be subsets. Then $\mathcal{V}_T(L) \subseteq \mathcal{V}_S(L)$.

(c) Let $S_i \subseteq K[X_1, \ldots, X_n]$ for $i \in I$ (some indexing set) be subsets. Then $\mathcal{V}_{\bigcup_{i\in I} S_i}(L) = \bigcap_{i\in I} \mathcal{V}_{S_i}(L)$.

(d) Let $S \subseteq K[X_1, \ldots, X_n]$ and let $\mathfrak{a} := (s \mid s \in S) \lhd K[X_1, \ldots, X_n]$ be the ideal generated by S. Then $\mathcal{V}_S(L) = \mathcal{V}_{\mathfrak{a}}(L)$.

(e) Let $\mathfrak{a}, \mathfrak{b} \lhd K[X_1, \ldots, X_n]$ be ideals. Then $\mathcal{V}_{\mathfrak{a}\cdot\mathfrak{b}}(L) = \mathcal{V}_{\mathfrak{a}}(L) \cup \mathcal{V}_{\mathfrak{b}}(L)$.

Proof. (a) and (b) are clear.
(c) Let $\underline{x} \in \mathbb{A}^n(L)$. Then

$$\underline{x} \in \mathcal{V}_{\bigcup_{i\in I} S_i}(L) \Leftrightarrow \forall f \in \bigcup_{i\in I} S_i : f(\underline{x}) = 0 \Leftrightarrow \forall i \in I : \forall f \in S_i : f(\underline{x}) = 0$$
$$\Leftrightarrow \forall i \in I : \underline{x} \in \mathcal{V}_{S_i}(L) \Leftrightarrow \underline{x} \in \bigcap_{i\in I} \mathcal{V}_{S_i}(L).$$

(d) The inclusion $\mathcal{V}_{\mathfrak{a}}(L) \subseteq \mathcal{V}_S(L)$ follows from (b). Let now $\underline{x} \in \mathcal{V}_S(L)$, meaning that $f(\underline{x}) = 0$ for all $f \in S$. Since any $g \in \mathfrak{a}$ can be written as a sum of products of elements from S, it follows that $g(\underline{x}) = 0$, proving the reverse inclusion.
(e) Since $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{a}$ and $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{b}$, (b) gives the inclusions $\mathcal{V}_{\mathfrak{a}}(L), \mathcal{V}_{\mathfrak{b}}(L) \subseteq \mathcal{V}_{\mathfrak{a}\mathfrak{b}}(L)$, hence $\mathcal{V}_{\mathfrak{a}}(L) \cup \mathcal{V}_{\mathfrak{b}}(L) \subseteq \mathcal{V}_{\mathfrak{a}\mathfrak{b}}(L)$. For the reverse inclusion, let $\underline{x} \notin \mathcal{V}_{\mathfrak{a}}(L) \cup \mathcal{V}_{\mathfrak{b}}(L)$, meaning that there exists $f \in \mathfrak{a}$ and $g \in \mathfrak{b}$ such that $f(\underline{x}) \neq 0 \neq g(\underline{x})$. Thus, $f(\underline{x}) \cdot g(\underline{x}) \neq 0$, whence $\underline{x} \notin \mathcal{V}_{\mathfrak{a}\mathfrak{b}}(L)$. □

Proof of Proposition 4.7. We need to check the axioms (1), (2) and (3). Note that (1) is Lemma 4.8 (a).
(2) For open sets $\mathbb{A}^n(K) \setminus \mathcal{V}_{S_i}(K)$ with $S_i \subseteq K[\underline{X}]$ for $i \in I$, we have: $\bigcup_{i\in I} \mathbb{A}^n(K) \setminus \mathcal{V}_{S_i}(K) = \mathbb{A}^n(K) \setminus \bigcap_{i\in I} \mathcal{V}_{S_i}(K) \overset{\text{Lemma 4.8(c)}}{=} \mathbb{A}^n(K) \setminus \mathcal{V}_{\bigcup_{i\in I} S_i}(K)$.
(3) By Lemma 4.8 (d), any two open sets are of the form $\mathbb{A}^n(K) \setminus \mathcal{V}_{\mathfrak{a}}(K)$ and $\mathbb{A}^n(K) \setminus \mathcal{V}_{\mathfrak{b}}(K)$ with ideals $\mathfrak{a}, \mathfrak{b} \lhd K[\underline{X}]$. It follows: $(\mathbb{A}^n(K) \setminus \mathcal{V}_{\mathfrak{a}}(K)) \cap (\mathbb{A}^n(K) \setminus \mathcal{V}_{\mathfrak{b}}(K)) = \mathbb{A}^n(K) \setminus (\mathcal{V}_{\mathfrak{a}}(K) \cup \mathcal{V}_{\mathfrak{b}}(K)) \overset{\text{Lemma 4.8(e)}}{=} \mathbb{A}^n(K) \setminus \mathcal{V}_{\mathfrak{a}\cdot\mathfrak{b}}(K)$. □

Definition 4.9. *Let $\mathcal{X}$ be a subset of $\mathbb{A}^n(K)$. We define the* vanishing ideal of $\mathcal{X}$ *as*

$$\mathcal{I}_{\mathcal{X}} := \{f \in K[\underline{X}] \mid f(\underline{x}) = 0 \text{ for all } \underline{x} \in \mathcal{X}\}.$$

The quotient ring $K[\mathcal{X}] := K[X]/\mathcal{I}_{\mathcal{X}}$ is called the coordinate ring of $\mathcal{X}$.

Lemma 4.10. *(a) The vanishing ideal is indeed an ideal of $K[\underline{X}]$ because it is the kernel of a ring homomorphism.*

(b) The ring homomorphism

$$\varphi : K[\underline{X}] \to \mathrm{Maps}(\mathcal{X}, K), \quad f \mapsto \big((x_1, \ldots, x_n) \mapsto f(x_1, \ldots, x_n)\big)$$

(with $+$ and $\cdot$ on $\mathrm{Maps}(\mathcal{X}, K)$ defined pointwise: $(f+g)(\underline{x}) := f(\underline{x}) + g(\underline{x})$ and $(f \cdot g)(\underline{x}) := f(\underline{x}) \cdot g(\underline{x})$) induces an injection of the coordinate ring $K[\mathcal{X}]$ into $\mathrm{Maps}(\mathcal{X}, K)$.

Proof. (a) is trivial. (b) is the isomorphism theorem. □

We may even replace $\mathrm{Maps}(\mathcal{X}, K)$ by $\mathcal{C}(\mathcal{X}, \mathbb{A}^1(K))$, the continuous maps for the Zariski topology (see exercise).
The coordinate ring consists hence of the polynomial functions from $\mathcal{X}$ to K. There are some special ones, namely, the projection to the i-th coordinate, i.e. $(x_1, \ldots, x_n) \mapsto x_i$; this clearly deserves the name *i-th coordinate function*; let us denote it by $\mathfrak{x}_i$. The name *coordinate ring* is hence explained! Note that any function $f(X_1, \ldots, X_n) + \mathcal{I}_\mathcal{X} = \sum a_{i_1,\ldots,i_n} X_1^{i_1} \ldots X_n^{i_n} + \mathcal{I}_\mathcal{X}$ is a combination of the coordinate functions, namely, $\sum a_{i_1,\ldots,i_n} \mathfrak{x}_1^{i_1} \ldots \mathfrak{x}_n^{i_n}$.

Lemma 4.11. *Let L/K be a field extension and $\mathcal{X} \subseteq \mathbb{A}^n(L)$ be a subset.*

(a) Every L-point $(a_1, \ldots, a_n) \in \mathcal{X}$ gives rise to the K-algebra homomorphism

$$\mathrm{ev}_{(a_1,\ldots,a_n)} : K[\mathcal{X}] = K[X_1, \ldots, X_n]/\mathcal{I}_\mathcal{X} \to L, \quad g(X_1, \ldots, X_n) + \mathcal{I}_\mathcal{X} \mapsto g(a_1, \ldots, a_n).$$

(b) If $L = K$, then the kernel of $\mathrm{ev}_{(a_1,\ldots,a_n)}$ is equal to $(X_1 - a_1, \ldots, X_n - a_n) + \mathcal{I}_\mathcal{X}$.

Proof. (a) is clear.
(b) The ideal $(X_1 - a_1, X_2 - a_2, \ldots, X_n - a_n)$ is clearly maximal because the quotient by it is K. As $(X_1 - a_1, X_2 - a_2, \ldots, X_n - a_n) \subseteq \ker(\mathrm{ev}_{(a_1,\ldots,a_n)})$ it follows that the two are equal (as $\mathrm{ev}_{(a_1,\ldots,a_n)}$ is not the zero-map – look at constants). □

Example 4.12.

- *Line $f(X, Y) := X - Y + 2 \in \mathbb{R}[X, Y]$, $\mathcal{L} := \mathcal{V}_f(\mathbb{R})$:*

  We have $\mathcal{I}_\mathcal{L} = (X - Y + 2)$, i.e. that the vanishing ideal of L is the principal ideal generated by f. This is a consequence of Proposition 4.14, which will be proved below.

  We compute the structure of the coordinate ring in this case. Consider the ring homomorphism:

  $$\varphi : \mathbb{R}[X, Y] \to \mathbb{R}[T], \quad g(X, Y) \mapsto g(T, T + 2).$$

  Note that this homomorphism is chosen such that $X - Y + 2$ gets mapped to $T - (T + 2) + 2 = 0$ and so lies in the kernel. We now prove that the kernel is equal to $\mathcal{I}_\mathcal{L}$ (and hence to $(X - Y + 2)$). Let $g \in \ker(\varphi)$. This means $g(T, T + 2)$ is the zero polynomial. If we now take a point $(x, y) \in \mathcal{L}$, then it satisfies $y = x + 2$, whence $g(x, y) = g(x, x + 2) = 0$ because it is equal to $g(T, T + 2)$ evaluated at $T = x$. This means $g \in \mathcal{I}_\mathcal{L}$, as claimed.

  From the isomorphism theorem, we now obtain that the coordinate ring is just the polynomial ring in one variable:

  $$\mathbb{R}[\mathcal{L}] = \mathbb{R}[X, Y]/\mathcal{I}_\mathcal{L} = \mathbb{R}[X, Y]/(X - Y + 2) \cong \mathbb{R}[T].$$

  In other words, the coordinate functions satisfy the equality $\mathfrak{x}_2 = \mathfrak{x}_1 + 2$.

- *Parabola $f(X, Y) := X^2 - Y + 2 \in \mathbb{R}[X, Y]$, $\mathcal{P} := \mathcal{V}_f(\mathbb{R})$:*

  Again by Proposition 4.14 we have $\mathcal{I}_\mathcal{P} = (X^2 - Y + 2)$.

With arguments similar to those used before, we conclude that the coordinate ring is

$$\mathbb{R}[\mathcal{P}] = \mathbb{R}[X,Y]/\mathcal{I}_{\mathcal{P}} = \mathbb{R}[X,Y]/(X^2 - Y + 2) \cong \mathbb{R}[T],$$

where the last isomorphism is given by sending the class of $g(X,Y)$ to $g(T, T^2+2)$. So, it is again isomorphic to the polynomial ring in one variable.

- *Hyperbola $f(X,Y) := XY - 1 \in \mathbb{R}[X,Y]$, $\mathcal{H} := \mathcal{V}_f(\mathbb{R})$:*
  We again have $\mathcal{I}_{\mathcal{H}} = (XY-1)$ by Proposition 4.14. This time we obtain

$$\begin{aligned}\mathbb{R}[\mathcal{H}] = \mathbb{R}[X,Y]/(XY-1) &\cong \mathbb{R}[X, \frac{1}{X}] \\ &= \{\sum_{i=e}^{f} a_i X^i \mid e, f \in \mathbb{Z}, a_i \in \mathbb{R}\} \subset \mathbb{R}(X) := \mathrm{Frac}(\mathbb{R}[X]).\end{aligned}$$

  Note that this ring is not isomorphic to the polynomial ring in one variable. For, suppose to the contrary that there is a ring isomorphism $\varphi : \mathbb{R}[X, \frac{1}{X}] \to \mathbb{R}[T]$. As X is a unit, so is $\varphi(X)$. Thus, $\varphi(X) \in \mathbb{R}[T]^\times = \mathbb{R}^\times$ is a constant polynomial. Consequently, the image of φ lands in $\mathbb{R}$, contradicting the surjectivity.

Here are basic properties of the vanishing ideal.

Lemma 4.13. *Let K be a field and $n \in \mathbb{N}$. Then the following statements hold:*

(a) Let $\mathcal{X} \subseteq \mathcal{Y} \subseteq \mathbb{A}^n(K)$ be subsets. Then $\mathcal{I}_{\mathfrak{X}} \supseteq \mathcal{I}_{\mathfrak{Y}}$.

(b) $\mathcal{I}_{\emptyset} = K[\underline{X}]$.

(c) If K has infinitely many elements, then $\mathcal{I}_{\mathbb{A}^n(K)} = (0)$.

(d) Let $S \subseteq K[\underline{X}]$ be a subset. Then $\mathcal{I}_{\mathcal{V}_S(K)} \supseteq S$.

(e) Let $\mathcal{X} \subseteq \mathbb{A}^n(K)$ be a subset. Then $\mathcal{V}_{\mathcal{I}_{\mathcal{X}}}(K) \supseteq \mathcal{X}$.

(f) Let $S \subseteq K[\underline{X}]$ be a subset. Then $\mathcal{V}_{\mathcal{I}_{\mathcal{V}_S(K)}}(K) = \mathcal{V}_S(K)$.

(g) Let $\mathcal{X} \subseteq \mathbb{A}^n(K)$ be a subset. Then $\mathcal{I}_{\mathcal{V}_{(\mathcal{I}_{\mathcal{X}})}(K)} = \mathcal{I}_{\mathcal{X}}$.

Proof. Exercise. □

Proposition 4.14. *Let K be a field. Let $f \in K[X,Y]$ a nonconstant irreducible polynomial. Assume that $\mathcal{V}_f(K)$ is infinite (which is automatic if $K = \overline{K}$ is algebraically closed by Lemma 4.3). Let $C = \mathcal{V}_f(K)$ be the associated plane curve.*
Then the vanishing ideal $\mathcal{I}_C$ is (f) and the coordinate ring $K[C]$ is isomorphic to $K[X,Y]/(f)$.

The most conceptual proof uses Hilbert's Nullstellensatz; we include that proof on page 86. We now give a direct proof, which relies on the following Lemma 4.15. In fact, once we have the notion of Krull dimension, we can give yet another very short proof. All proofs are essentially the same, except that in the more direct ones we specialise to curves, which makes the arguments shorter.

We include an easy counter example to show that some assumption on the field or the curve C is needed. Consider the irreducible polynomial $f(X,Y) = X^2 + 1 \in \mathbb{R}[X,Y]$. The associated curve $C = \mathcal{V}_f(\mathbb{R})$ is the empty set and hence the vanishing ideal $\mathcal{I}_C$ is the entire polynomial ring.
The next lemma uses the same idea as Nagata's normalisation lemma 8.10 specialised to the case of two variables. It shows that the coordinate ring is not 'too far off' a polynomial ring in one variable, in the following sense: there is a transcendental element $\overline{T}$ in the coordinate ring (the transcendence assumption means that the subring $K[\overline{T}]$ of the coordinate ring is isomorphic to a polynomial ring) such that the coordinate ring is an integral ring extension of $K[\overline{T}]$. This will be essential in the proof of Proposition 4.14.

Lemma 4.15. *Let K be a field and $\mathcal{I} \trianglelefteq K[X,Y]$ be an ideal containing $f \in \mathcal{I}$, a nonconstant polynomial of total degree $d > 0$. Let $\overline{T} := X - Y^{d+1} + \mathcal{I} \in K[X,Y]/\mathcal{I}$.*

(a) The ring extension $K[\overline{T}] \subseteq K[X,Y]/\mathcal{I}$ is integral.

(b) Assume that $\mathcal{V}_f(K)$ is infinite (automatic if $K = \overline{K}$ is algebraically closed by Lemma 4.3). If $\mathcal{I} = \mathcal{I}_C$ with $C = V_f(K)$ a curve, then $\overline{T}$ is transcendental over K.

Proof. (a) We explicitely write down the polynomial $f(X,Y) = \sum_{0\leq i,j \text{ s.t. } i+j\leq d} a_{i,j}X^iY^j$. Consider the polynomial $g(T,Z) = f(T+Z^{d+1}, Z) \in K[T][Z]$, i.e. we see it as a polynomial in the variable Z with coefficients in $K[T]$. We find

$$g(T,Z) = \sum_{0\leq i,j \text{ s.t. } i+j\leq d} a_{i,j}(T+Z^{d+1})^iZ^j = \sum_{0\leq i,j \text{ s.t. } i+j\leq d} a_{i,j}Z^{(d+1)i+j} + \text{lower degree terms in } Z.$$

Note that all the $(d+1)i + j$ are distinct for i, j in the considered range. This description makes it clear that the coefficient in front of the highest power of Z does not involve any T; it is one of the $a_{i,j}$, say $a := a_{r,s}$. This means we can divide by it. Call the resulting monic polynomial $h(T,Z) = \frac{1}{a}g(T,Z) \in K[T][Z]$.
Now let us use the $\overline{T}$ from the assertion, i.e. $\overline{T} = X - Y^{d+1} + \mathcal{I}$. Write $h(Z)$ for the image of $h(\overline{T}, Z) \in (K[\overline{T}])[Z] \subseteq (K[X,Y]/\mathcal{I})[Z]$. It is a monic polynomial. Then we get

$$h(Y) = \frac{1}{a}g(\overline{T}, Y) = \frac{1}{a}f(X - Y^{d+1} + Y^{d+1}, Y) = \frac{1}{a}f(X,Y) \in \mathcal{I}.$$

This means that the class $Y + \mathcal{I}$ is annihilated by the monic polynomial $h(Z)$. Thus, $Y + \mathcal{I}$ is integral over $K[\overline{T}]$.
As $K[X,Y]/\mathcal{I}$ is generated over $K[\overline{T}]$ by $Y + \mathcal{I}$, the integrality of $K[\overline{T}] \subseteq K[X,Y]/\mathcal{I}$ follows.
(b) Suppose that $\overline{T}$ is not transcendental over K, then it is algebraic over K, hence the ring extension $K \subseteq K[\overline{T}]$ is integral. Furthermore, by (a), the ring extension $K[\overline{T}] \subseteq K[X,Y]/\mathcal{I}$ is also integral, whence by the transitivity of integrality (Corollary 3.25) the ring extension $K \subseteq K[X,Y]/\mathcal{I}$ is integral as well. In particular, the classes of X and Y are integral, hence algebraic, over K. So there are polynomials $m_X, m_Y \in K[Z]$ such that $m_X(X + \mathcal{I}) = 0 = m_Y(Y + \mathcal{I})$, in other words $m_X(X), m_Y(Y) \in \mathcal{I}$. This means that for any point $(x,y) \in C = \mathcal{V}_{\mathcal{I}}(K)$ (the equality follows from Lemma 4.13 (f)), we have $m_X(x) = 0 = m_Y(y)$. Consequently, there are only finitely many possibilities for the x-coordinate and only finitely many possibilities for the y-coordinate of any point of the curve. Thus, the curve C only has finitely many points, contradicting our assumption. □

First proof of Proposition 4.14. The inclusion $(f) \subseteq \mathcal{I}_C$ is clear. We need to show the reverse inclusion. In order to do this, we consider the natural projection (coming from the inclusion $(f) \subseteq \mathcal{I}_C$)

$$\pi : K[X,Y]/(f) \twoheadrightarrow K[X,Y]/\mathcal{I}_C.$$

It suffices to show that it is an isomorphism. In order to do so, let $g \in \mathcal{I}_C$ and consider its class $\overline{g} = g + (f) \in K[X,Y]/(f)$; we aim to show that it is the zero class, i.e. $g \in (f)$.
Next, we want to use Lemma 4.15; we therefore consider elements $T := X - Y^{d+1} \in K[X,Y]$ with d being the total degree of f and its images $\overline{T} \in K[X,Y]/(f)$ and $\tilde{T} := \pi(\overline{T}) \in K[X,Y]/\mathcal{I}_C$. Part (b) of the lemma tells us that $\tilde{T}$ (and hence also $\overline{T}$) is transcendental over K, and by part (a), the ring extension $K[\overline{T}] \subseteq K[X,Y]/(f)$ is integral.
We apply the latter statement to the element $\overline{g}$ in order to get an equality of the form

$$\overline{g}^n + \sum_{i=1}^{n-1} r_i(\overline{T})\overline{g}^i + r_0(\overline{T}) = 0$$

in the ring $K[X,Y]/(f)$, where the $r_i \in K[\overline{T}]$ are polynomials (we can see them as usual polynomials because $\overline{T}$ is transcendental over K). Let us suppose that n is minimal with this property.
As $\overline{g}$ vanishes on all points of C, so do $r_0(\overline{T})$ and $r_0(T) = r_0(X - Y^{d+1})$. This implies that $r_0(T) = r_0(X - Y^{d+1})$ belongs to $\mathcal{I}_C$, so that $r_0(\tilde{T})$ is zero in $K[X,Y]/\mathcal{I}_C$.
As $\tilde{T}$ in $K[X,Y]/\mathcal{I}_C$ is transcendental over K, this implies that $r_0 = 0$, i.e. r_0 is the zero polynomial (all coefficients are zero). Thus, in the ring $K[X,Y]/(f)$ we have the equality

$$\overline{g}(\overline{g}^{n-1} + \sum_{i=1}^{n-1} r_i(\overline{T})\overline{g}^{i-1}) = 0.$$

In other words

$$g(g^{n-1} + \sum_{i=1}^{n-1} r_i(X - Y^{d+1})g^{i-1}) \in (f).$$

As f is irreducible, the ideal (f) is prime. Consequently, $g \in (f)$, as desired; for, if g were not in (f), we would have $\overline{g}^{n-1} + \sum_{i=1}^{n-1} r_i(\overline{T})\overline{g}^{i-1} = 0$, contradicting the minimality of n. □

Lemma 4.16. *Let $(\mathcal{X}, \mathcal{O}_\mathcal{X})$ be a topological space and $\mathcal{Y} \subseteq \mathcal{X}$ be a subset. Define $\mathcal{O}_\mathcal{Y} := \{U \cap \mathcal{Y} \mid U \in \mathcal{O}_\mathcal{X}\}$.*
Then $\mathcal{O}_\mathcal{Y}$ is a topology on $\mathcal{Y}$, called the relative topology *or the* subset topology.

Proof. Exercise. □

Definition 4.17. *Let $\mathcal{X}$ be a topological space (we do not always mention $\mathcal{O}$ explicitly).*
A subset $\mathcal{Y} \subseteq \mathcal{X}$ is called reducible *if there are two closed subsets $\mathcal{Y}_1, \mathcal{Y}_2 \subsetneq \mathcal{Y}$ for the relative topology on $\mathcal{Y}$ such that $\mathcal{Y} = \mathcal{Y}_1 \cup \mathcal{Y}_2$. By the definition of the relative topology, $\mathcal{Y} \subseteq \mathcal{X}$ is reducible if and only if there are closed subsets $\mathcal{X}_1, \mathcal{X}_2 \subseteq \mathcal{X}$ such that $\mathcal{Y} \subseteq \mathcal{X}_1 \cup \mathcal{X}_2$, $\mathcal{Y} \not\subseteq \mathcal{X}_1$ and $\mathcal{Y} \not\subseteq \mathcal{X}_2$.*
If $\mathcal{Y}$ is not reducible, it is called irreducible.
An affine set $\mathcal{X} \subseteq \mathbb{A}^n(K)$ is called an affine variety *if $\mathcal{X}$ is irreducible.*

Example 4.18.
- *Let $f(X,Y) = XY \in \mathbb{R}[X,Y]$. Then $\mathcal{V}_f(\mathbb{R})$ is the union of the x-axis and the y-axis, so clearly $\mathcal{V}_f(\mathbb{R})$ is reducible for the Zariski topology (and also the usual real topology). More precisely,*
$$\mathcal{V}_f(\mathbb{R}) = \mathcal{V}_X(\mathbb{R}) \cup \mathcal{V}_Y(\mathbb{R}).$$
- *The line $X - Y + 2$ is irreducible for the Zariski topology, but not for the usual real topology (take two closed 'half lines' overlapping).*
- *The hyperbola $\mathcal{H}$ is also irreducible for the Zariski topology. This is a consequence of the next proposition, since the coordinate ring $\mathbb{R}[\mathcal{H}]$ is an integral domain. This might contradict our intuition, since the the hyperbola consists of two branches and is reducible for the usual real topology.*

At the end of this section we are able to formulate a topological statement on an affine algebraic set as a purely algebraic statement on the coordinate ring! This kind of phenomenon will be encountered all the time in the sequel of the lecture.

Proposition 4.19. *Let $\emptyset \neq \mathcal{X} \subseteq \mathbb{A}^n(K)$ be an affine set. Then the following statements are equivalent:*

(i) $\mathcal{X}$ is irreducible for the Zariski topology (i.e. $\mathcal{X}$ is a variety).

(ii) $\mathcal{I}_\mathcal{X}$ is a prime ideal of $K[X_1, \ldots, X_n]$.

(iii) The coordinate ring $K[\mathcal{X}]$ is an integral domain.

Proof. The equivalence of (ii) and (iii) is Proposition 1.16 (recall $K[\mathcal{X}] = K[\underline{X}]/\mathcal{I}_\mathcal{X}$).
¬(ii) ⇒ ¬(i): Suppose $\mathcal{I}_\mathcal{X}$ is not a prime ideal. Then there are two elements $f_1, f_2 \in K[\underline{X}] \setminus \mathcal{I}_\mathcal{X}$ such that $f_1 \cdot f_2 \in \mathcal{I}_\mathcal{X}$. This, however, implies:
$$\mathcal{X} = \big(\mathcal{V}_{(f_1)}(K) \cup \mathcal{V}_{(f_2)}(K)\big) \cap \mathcal{X} = \big(\mathcal{V}_{(f_1)}(K) \cap \mathcal{X}\big) \cup \big(\mathcal{V}_{(f_2)}(K) \cap \mathcal{X}\big),$$
since $\mathcal{V}_{(f_1)}(K) \cup \mathcal{V}_{(f_2)}(K) = \mathcal{V}_{(f_1 \cdot f_2)}(K) \supseteq \mathcal{X}$. Note that $f_1 \notin \mathcal{I}_\mathcal{X}$ precisely means that there is $\underline{x} \in \mathcal{X}$ such that $f_1(\underline{x}) \neq 0$. Hence, $\mathcal{X} \neq \mathcal{V}_{(f_1)}(K) \cap \mathcal{X}$. Of course, the same argument applies with f_1 replaced by f_2, proving that $\mathcal{X}$ is reducible.
¬(i) ⇒ ¬(ii): Suppose $\mathcal{X}$ is reducible, i.e. $\mathcal{X} = \mathcal{X}_1 \cup \mathcal{X}_2$ with $\mathcal{X}_1 \subsetneq \mathcal{X}$ and $\mathcal{X}_2 \subsetneq \mathcal{X}$ closed subsets of $\mathcal{X}$ (and hence closed subsets of $\mathbb{A}^n(K)$, since they are the intersection of some closed set of $\mathbb{A}^n(K)$ with the closed set $\mathcal{X}$). This means $\mathcal{I}_{\mathcal{X}_i} \supsetneq \mathcal{I}_\mathcal{X}$ for $i = 1, 2$ as otherwise $\mathcal{X} = \mathcal{X}_i$ by Lemma 4.13. Hence, there are $f_1 \in \mathcal{I}_{\mathcal{X}_1}$ and $f_2 \in \mathcal{I}_{\mathcal{X}_2}$ such that $f_1, f_2 \notin \mathcal{I}_\mathcal{X}$. Note that $f_1(\underline{x})f_2(\underline{x}) = 0$ for all $\underline{x} \in \mathcal{X}$, as at least one of the two factors is 0. Thus, $f_1 \cdot f_2 \in \mathcal{I}_\mathcal{X}$. This shows that $\mathcal{I}_\mathcal{X}$ is not a prime ideal. □

We add an example that becomes important later, when we will discuss the relationship between non-singularity and normality.

Example 4.20. *Let $f(X,Y) = Y^2 - X^3 \in \mathbb{C}[X,Y]$ and consider the curve $C_f := \mathcal{V}_f(\mathbb{C})$ defined by f. Consider its coordinate ring $R = \mathbb{C}[C_f] = \mathbb{C}[X,Y]/(Y^2 - X^3)$.*

(a) We have that R is an integral domain because $Y^2 - X^3$ is an irreducible polynomial.

(b) Write x, y for the classes of X, Y in R. Let K be the field of fractions of R. Put $t = y/x$.

As $y = tx$, we find $0 = t^2x^2 - x^3 = x^2(t^2 - x)$, from which we derive $t^2 = x$ and $y = tx = t^3$ because the calculations are done in the field K.

Moreover, we have $K = \mathbb{C}(t) := \mathrm{Frac}(\mathbb{C}[t])$. Indeed, the inclusion $\subseteq$ follows from the fact that K is generated over $\mathbb{C}$ by $x = t^2$ and $y = t^3$. The other inclusion is obvious because $t = y/x \in K$.

(c) The ring R is not normal, i.e. not integrally closed in $K = \mathbb{C}(t)$. The reason is that t is integral over R (e.g. because $t^2 = x$) but $t \notin R$.

(d) We have that $\mathbb{C}[t]$ is the normalisation of R, i.e. the integral closure of R in K. The reason is simply that $\mathbb{C}[t]$ is normal, as it is integrally closed and that $R \subset \mathbb{C}[t]$ is integral and both rings have the same field of fractions.

Chapter II

Modules

5 Direct sums, products, free modules and exact sequences

Aims:

- Learn and master the concepts of direct products and direct sums of modules, and know the differences between the two;
- learn and master the concept of free modules;
- learn and master the concept of exact sequences;
- get to know the Hom-functor and its exactness properties;
- know examples and standard theorems;
- be able to prove simple properties.

Direct products and direct sums

We first define direct products and direct sums of modules.

Definition 5.1. *Let R be a ring and M_i for $i \in I$ (some set) R-modules.*

(a) The direct product of the M_i for $i \in I$ *is defined as the cartesian product $\prod_{i\in I} M_i$ with component-wise operation. More precisely, let $(x_i)_{i\in I}, (y_i)_{i\in I} \in \prod_{i\in I} M_i$ and $r \in R$, then one puts*

$$(x_i)_{i\in I} + (y_i)_{i\in I} := (x_i + y_i)_{i\in I} \text{ and } r.(x_i)_{i\in I} := (r.x_i)_{i\in I}.$$

One checks easily that $\prod_{i\in I} M_i$ is an R-module.

If $I = \{1, \ldots, n\}$ is a finite set, one also writes $\prod_{i=1}^{n} M_i = M_1 \times M_2 \times \cdots \times M_n$ and its elements are denoted as $(x_1, x_2, \ldots, x_n)$.

(b) The natural map $\pi_j : \prod_{i\in I} M_i \to M_j$ given by $(x_i)_{i\in I} \mapsto x_j$ is called the j-th projection. *One checks easily that π_j is a surjective R-module homomorphism.*

(c) *The* direct sum of the M_i for $i \in I$ *is defined as the subset of the cartesian product* $\prod_{i\in I} M_i$ *with component-wise operation consisting of those* $(x_i)_{i\in I} \in \prod_{i\in I} M_i$ *such that* $x_i \neq 0$ *only for finitely many* $i \in I$*. The notation is* $\bigoplus_{i\in I} M_i$*.*

One checks easily that $\bigoplus_{i\in I} M_i$ *is an* R*-module.*

If $I = \{1, \ldots, n\}$ *is a finite set, one also writes* $\bigoplus_{i=1}^n M_i = M_1 \oplus M_2 \oplus \cdots \oplus M_n$ *and its elements are denoted as* $(x_1, x_2, \ldots, x_n)$ *or* $x_1 \oplus x_2 \oplus \cdots \oplus x_n$*.*

(d) *The natural map* $\epsilon_j : M_j \to \bigoplus_{i\in I} M_i$ *given by* $\epsilon(x) = (x_i)_{i\in I}$ *with* $x_j = x$ *and* $x_i = 0$ *for* $i \neq j$ *is called the* j-th injection*.*

One checks easily that ϵ_j *is an injective* R*-module homomorphism.*

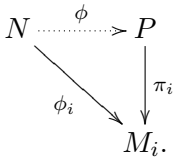
Corollary 5.2. *Let* R *be a ring and* $M_1, \ldots, M_n$ *be* R*-modules. Then the identity induces an* R*-isomorphism* $\bigoplus_{i=1}^n M_i \cong \prod_{i=1}^n M_i$*.*

Proof. This is obvious. □

Proposition 5.3. *Let* R *be a ring and* M_i *for* $i \in I$ *(some set)* R*-modules.*

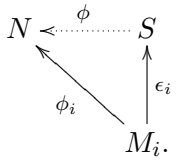
(a) *The direct product* $P := \prod_{i\in I} M_i$ *together with the projections* π_i *satisfies the following universal property:*

> *For all* R*-modules* N *together with* R*-homomorphisms* $\phi_i : N \to M_i$ *for* $i \in I$ *there is one and only one* R*-homomorphism* $\phi : N \to P$ *such that* $\pi_i \circ \phi = \phi_i$ *for all* $i \in I$*, as in the diagram*



(b) *The direct sum* $S := \bigoplus_{i\in I} M_i$ *together with the injections* ϵ_i *satisfies the following universal property:*

> *For all* R*-modules* N *together with* R*-homomorphisms* $\phi_i : M_i \to N$ *for* $i \in I$ *there is one and only one* R*-homomorphism* $\phi : S \to N$ *such that* $\phi \circ \epsilon_i = \phi_i$ *for all* $i \in I$*, as in the diagram*



Proof. Exercise. □

Free modules

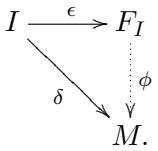
Definition 5.4. *Let R be a ring and M an R-module.*
Recall the definition of a generating set: A subset $B \subseteq M$ is called a generating set of M as R-module *if for every $m \in M$ there are $n \in \mathbb{N}$, $b_1, \dots, b_n \in B$ and $r_1, \dots, r_n \in R$ such that $m = \sum_{i=1}^n r_i b_i$.*
*A subset $B \subseteq M$ is called R-*free (or: R-linearly independent) *if for any $n \in \mathbb{N}$ and any $b_1, \dots, b_n \in B$ the equation $0 = \sum_{i=1}^n r_i b_i$ implies $0 = r_1 = r_2 = \cdots = r_n$.*
*A subset $B \subseteq M$ is called an R-*basis of M *if B is an R-free generating set.*
A module M having a basis B is called a free R-module.

Proposition 5.5. *Let R be a ring, let I be a set and $F_I := \bigoplus_{i \in I} R$. Define $\epsilon : I \to F_I$ by $\epsilon(j) = (x_i)_{i \in I}$, where $x_j = 1$ and $x_i = 0$ if $i \neq j$.*

(a) Then F_I is R-free with basis $B = \{\epsilon(i) \mid i \in I\}$.

(b) F_I together with ϵ satisfies the following universal property:

> *For all R-modules M and all maps $\delta : I \to M$ there is one and only one R-homomorphism $\phi : F_I \to M$ such that $\phi \circ \epsilon = \delta$, as in the diagram*



Proof. (a) is clear.
(b) For $(x_i)_{i \in I} \in F_I$ define $\phi((x_i)_{i \in I}) := \sum_{i \in I} x_i \delta(i)$; note that this is a finite sum (because of the definition of the direct sum) and hence makes sense; clearly $\phi \circ \epsilon = \delta$ holds. It is trivial to check that ϕ is an R-homomorphism.
For the uniqueness note that $\phi(\epsilon(i)) := \delta(i)$ forces $\phi((x_i)_{i \in I}) := \sum_{i \in I} x_i \delta(i)$ by the properties of an R-homomorphism. This shows the uniqueness. □

Example 5.6. *(a) Let $R = K$ be a field. Then R-modules are K-vector spaces. Hence, all R-modules are free. Their rank is the dimension as a K-vector space.*

(b) Let $R = \mathbb{Z}$. Then $\mathbb{Z}^n$ is a free $\mathbb{Z}$-module of rank n.

(c) Let $R = \mathbb{Z}$ and $M = \mathbb{Z}/2\mathbb{Z}$. Then M is not $\mathbb{Z}$-free.

Proposition 5.7. *Let R be a ring.*

(a) Let M be an R-module and $B \subseteq M$ a generating set. Then there is a surjective R-homomorphism $F_B \to M$, where F_B is the free R-module from Proposition 5.5. In other words, M is a quotient of F_B.

(b) Let M be a free R-module with basis B. Then M is isomorphic to F_B.

Proof. (a) Consider $\delta : B \to M$ given by the identity, i.e. the inclusion of B into M. The universal property of F_B gives an R-homomorphism $\phi : F_B \to M$. As $\phi \circ \epsilon = \delta$, B is in the image of ϕ. As the image contains a set of generators for the whole module M, the image is equal to M, i.e. ϕ is surjective.
(b) Then ϕ (from (a)) is given by $(r_b)_{b\in B} \mapsto \sum_{b\in B} r_b b$. If $(r_b)_{b\in B}$ is in the kernel of ϕ, then $\sum_{b\in B} r_b b = 0$. The freeness of the basis B now implies $r_b = 0$ for all $b \in B$, showing $(r_b)_{b\in B} = 0$, i.e. the injectivity. □

Lemma 5.8. *Let R be a ring and M a finitely generated free R-module. Then all R-bases of M have the same length.*
This length is called the R-rank *or the* R-dimension *of* M.

Proof. We prove this using linear algebra. Let $B = \{b_1, \dots, b_n\}$ and $C = \{c_1, \dots, c_m\}$ with $n \geq m$ be two R-bases of M. Of course, we can express one basis in terms of the other one:

$$b_i = \sum_{j=1}^{m} t_{i,j} c_j \text{ and } c_j = \sum_{k=1}^{n} s_{j,k} b_k, \text{ hence } b_i = \sum_{k=1}^{n} (\sum_{j=1}^{m} t_{i,j} s_{j,k}) b_k.$$

As B is a basis, we conclude

$$\sum_{j=1}^{m} t_{i,j} s_{j,k} = \delta_{i,k}.$$

Writing this in matrix form with $T = (t_{i,j})_{1\leq i\leq n, 1\leq j\leq m}$ and $S = (s_{j,k})_{1\leq j\leq m, 1\leq k\leq n}$ yields

$$T \cdot S = \begin{pmatrix} t_{1,1} & \dots & t_{1,m} \\ \vdots & \ddots & \vdots \\ t_{m,1} & \dots & t_{m,m} \\ t_{m+1,1} & \dots & t_{m+1,m} \\ \vdots & \ddots & \vdots \\ t_{n,1} & \dots & t_{n,m} \end{pmatrix} \circ \begin{pmatrix} s_{1,1} & \dots & s_{1,m} & s_{1,m+1} & \dots & s_{1,n} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ s_{m,1} & \dots & s_{m,m} & s_{m,m+1} & \dots & s_{m,n} \end{pmatrix} = \mathrm{id}_{n\times n}.$$

Assume $n > m$. Then we can add $n - m$ rows with entries 0 to S at the bottom and $n - m$ columns with entries 0 to T on the right without changing the product. However, the determinant of these enlarged matrices is 0, whence also the determinant of their product is zero, which contradicts the fact that their product is the identity, which has determinant 1. □

Exact sequences

Definition 5.9. *Let R be a ring and let $a < b \in \mathbb{Z} \cup \{-\infty, \infty\}$. For each $n \in \mathbb{Z}$ such that $a \leq n \leq b$, let M_n be an R-module. Also let $\phi_n : M_{n-1} \to M_n$ be an R-homomorphism. In other words, for all $a', b' \in \mathbb{Z}$ such that $a \leq a' < b' \leq b$ we have the sequence*

$$M_{a'} \xrightarrow{\phi_{a'+1}} M_{a'+1} \xrightarrow{\phi_{a'+2}} M_{a'+2} \xrightarrow{\phi_{a'+3}} \dots \xrightarrow{\phi_{b'-2}} M_{b'-2} \xrightarrow{\phi_{b'-1}} M_{b'-1} \xrightarrow{\phi_{b'}} M_{b'}.$$

Such a sequence is called a complex *if* $\mathrm{im}(\phi_{n-1}) \subseteq \ker(\phi_n)$ *for all n in the range. That is the case if and only if $\phi_n \circ \phi_{n-1} = 0$ for all n in the range.*

The sequence is called exact *if* $\mathrm{im}(\phi_{n-1}) = \ker(\phi_n)$ *for all* n *in the range (of course, this implies that it is also a complex).*

We will often consider finite sequences, mostly of the form

$$(*) \quad 0 \to M_1 \to M_2 \to M_3 \to 0,$$

where 0 denotes the zero module $\{0\} \subseteq R$. If a sequence of the form $(*)$ is exact, then it is called a *short exact sequence*.

Lemma 5.10. *Let R be a ring.*

(a) Let $A \xrightarrow{\alpha} B$ be an R-homomorphism. Then α is injective if and only if the sequence $0 \to A \to B$ is exact.

(b) Let $B \xrightarrow{\beta} C$ be an R-homomorphism. Then β is surjective if and only if the sequence $B \xrightarrow{\beta} C \to 0$ is exact.

(c) Let $0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0$ be a complex. It is an exact sequence if and only if $C = \mathrm{im}(\beta)$ and α is an isomorphism from A to $\ker(\beta)$.

Proof. (a) Just note: $\ker(\alpha) = \mathrm{im}(0 \to A) = \{0\}$.
(b) Just note: $C = \ker(C \to 0) = \mathrm{im}(\alpha)$.
(c) Combine (a) and (b) with the exactness at B. □

Proposition 5.11. *Let R be a ring and M_i, N_i for $i = 1, 2, 3$ be R-modules.*

(a) Let

$$0 \to N_1 \xrightarrow{\phi_2} N_2 \xrightarrow{\phi_3} N_3$$

be a sequence. This sequence is exact if and only if

$$0 \to \mathrm{Hom}_R(M, N_1) \xrightarrow{\tilde{\phi}_2} \mathrm{Hom}_R(M, N_2) \xrightarrow{\tilde{\phi}_3} \mathrm{Hom}_R(M, N_3)$$

is exact for all R-modules M. The R-homomorphism $\tilde{\phi}_i$ sends $\alpha \in \mathrm{Hom}_R(M, N_{i-1})$ to $\phi_i \circ \alpha \in \mathrm{Hom}_R(M, N_i)$ for $i = 2, 3$.

(b) Let

$$M_1 \xrightarrow{\psi_2} M_2 \xrightarrow{\psi_3} M_3 \to 0$$

be a sequence. This sequence is exact if and only if

$$0 \to \mathrm{Hom}_R(M_3, N) \xrightarrow{\tilde{\psi}_3} \mathrm{Hom}_R(M_2, N) \xrightarrow{\tilde{\psi}_2} \mathrm{Hom}_R(M_1, N)$$

is exact for all R-modules N. The R-homomorphism $\tilde{\psi}_i$ sends $\alpha \in \mathrm{Hom}_R(M_i, N)$ to $\alpha \circ \psi_i \in \mathrm{Hom}_R(M_{i-1}, N)$ for $i = 2, 3$.

For the directions '⇒' one also says that in case (a) that the functor $\mathrm{Hom}_R(M, \cdot)$ is covariant (preserves directions of arrows) and left-exact and in case (b) that the functor $\mathrm{Hom}_R(\cdot, N)$ is contravariant (reverses directions of arrows) and left-exact.

Proof. (a) '⇒':

- We know that ϕ_2 is injective. If $\alpha \in \ker(\tilde{\phi}_2)$, then by definition $\phi_2 \circ \alpha$ is the zero map. This implies that α is zero, showing that $\tilde{\phi}_2$ is injective.
- We know that $\phi_3 \circ \phi_2$ is the zero map. This implies that $\tilde{\phi}_3\big(\tilde{\phi}_2(\alpha)\big) = \phi_3 \circ \phi_2 \circ \alpha$ is the zero map for all $\alpha \in \mathrm{Hom}_R(M, N_1)$. Hence, $\mathrm{im}(\tilde{\phi}_2) \subseteq \ker(\tilde{\phi}_3)$.
- Let $\beta \in \ker(\tilde{\phi}_3)$, i.e. $\phi_3 \circ \beta$ is the zero map. This means $\mathrm{im}(\beta) \subseteq \ker(\phi_3)$, hence, we obtain that
$$\phi_2^{-1} \circ \beta : M \xrightarrow{\beta} \mathrm{im}(\beta) \subseteq \ker(\phi_3) = \mathrm{im}(\phi_2) \xrightarrow{\phi_2^{-1}} N_1$$
is an element in $\mathrm{Hom}_R(M, N_1)$. It satisfies $\tilde{\phi}_2(\phi_2^{-1} \circ \beta) = \phi_2 \circ \phi_2^{-1} \circ \beta = \beta$, whence $\beta \in \mathrm{im}(\tilde{\phi}_2)$, showing $\mathrm{im}(\tilde{\phi}_2) \supseteq \ker(\tilde{\phi}_3)$.

'⇐':

- We know that $\tilde{\phi}_2$ is injective for all R-modules M. Choose $M := \ker(\phi_2)$, and consider the inclusion $\iota : \ker(\phi_2) \to N_1$. Note that
$$\tilde{\phi}_2(\iota) = \phi_2 \circ \iota : \ker(\phi_2) \xrightarrow{\iota} N_1 \xrightarrow{\phi_2} N_2$$
is the zero-map. But, as $\tilde{\phi}_2$ is injective, it follows that already ι is the zero map, meaning that $\ker(\phi_2)$ is the zero module, so that ϕ_2 is injective.
- We want to show $\phi_3 \circ \phi_2 = 0$. For this take $M := N_1$, and consider id_{N_1} the identity on N_1. We know that $\tilde{\phi}_3 \circ \tilde{\phi}_2$ is the zero map. In particular,
$$0 = \tilde{\phi}_3 \circ \tilde{\phi}_2(\mathrm{id}_{N_1}) = \phi_3 \circ \phi_2 \circ \mathrm{id}_{N_1} = \phi_3 \circ \phi_2.$$
- We want to show that $\ker(\phi_3) \subseteq \mathrm{im}(\phi_2)$. For this take $M := \ker(\phi_3)$ and consider the inclusion $\iota : \ker(\phi_3) \to N_2$. Note that
$$0 = \tilde{\phi}_3(\iota) = \phi_3 \circ \iota : \ker(\phi_3) \xrightarrow{\iota} N_2 \xrightarrow{\phi_3} N_3$$
is the zero map. We know that $\ker(\tilde{\phi}_3) \subseteq \mathrm{im}(\tilde{\phi}_2)$. Hence, there is some $\beta : \ker(\phi_3) \to N_1$ such that $\iota = \tilde{\phi}_2(\beta) = \phi_2 \circ \beta$. In particular, the image of ι, which is equal to $\ker(\phi_3)$, equals the image of $\phi_2 \circ \beta$, which is certainly contained in the image of ϕ_2, as was to be shown.

(b) Exercise. □

Proposition 5.12. *Let R be a ring, M, N, M_i and N_i for $i \in I$ (some set) be R-modules. Then there are natural R-isomorphisms:*

(a) $\Phi : \mathrm{Hom}_R(M, \prod_{i\in I} N_i) \to \prod_{i\in I} \mathrm{Hom}_R(M, N_i)$ *and*

(b) $\Psi : \mathrm{Hom}_R(\bigoplus_{i\in I} M_i, N) \to \prod_{i\in I} \mathrm{Hom}_R(M_i, N)$.

Proof. (a) Let $\pi_j : \prod_{i\in I} N_i \to N_j$ be the j-th projection. Define Φ as follows:

$$\Phi(\varphi : M \to \prod_{i\in I} N_i) := (\pi_i \circ \varphi : M \to N_i)_{i\in I}.$$

It is clear that Φ is an R-homomorphism. The rest of the statement is exactly the universal property of the product from Proposition 5.3. Indeed, suppose that we are given $\varphi_i : M \to N_i$ for each $i \in I$. Then the universal property of $\prod_{i\in I} N_i$ tells us that there is a unique $\varphi : M \to \prod_{i\in I} N_i$ such that $\varphi_i = \pi_i \circ \varphi$ for all $i \in I$. This is precisely the required preimage, showing the surjectivity. The uniqueness of φ gives us a unique preimage, which also implies injectivity.
(b) Exercise. □

Lemma 5.13. *Let R be a ring and M an R-module. Then the map*

$$\Phi : \mathrm{Hom}_R(R, M) \to M, \quad \Phi(\alpha : R \to M) := \alpha(1)$$

is an R-isomorphism.

Proof. Clear. □

Proposition 5.14. *Let R be a ring and*

$$0 \longrightarrow A \underset{\alpha}{\overset{t}{\rightleftarrows}} B \underset{\beta}{\overset{s}{\rightleftarrows}} C \longrightarrow 0$$

be a short exact sequence. Then the following statements are equivalent:

(i) There is an R-homomorphism $s : C \to B$ such that $\beta \circ s = \mathrm{id}_C$. Then s is called a split *and one says that the short exact sequence* is split/splits.

(ii) There is an R-homomorphism $t : B \to A$ such that $t \circ \alpha = \mathrm{id}_A$. Then t is also called a split *and one also says that the short exact sequence* is split/splits.

(iii) There is an R-isomorphism $\varphi : A \oplus C \to B$ such that $\varphi \circ (A \xrightarrow{a\mapsto a} A \oplus C) = \alpha$ and $\beta \circ \varphi \circ (C \xrightarrow{c\mapsto c} A \oplus C) = \mathrm{id}_C$.

Proof. Exercise. □

Proposition 5.15. *Let R be a ring and F a free R-module.*

(a) Then F satisfies the following universal property:

> *For all surjective R-homomorphisms $\phi : M \twoheadrightarrow N$ and all R-homomorphisms $\psi : F \to N$, there exists an R-homomorphism $\alpha : F \to M$ such that $\phi \circ \alpha = \psi$, as in the diagram*

$$\begin{array}{ccc} & & F \\ & \overset{\alpha}{\swarrow} & \downarrow \psi \\ M & \xrightarrow[\phi]{} & N. \end{array}$$

A module that satisfies this universal property is called projective. *Thus, F is projective.*

(b) If $0 \to A \to B \to F \to 0$ is a short exact sequence of R-modules, then $B \cong A \oplus F$.

Proof. (a) Let B be an R-basis of F, so that we can identify F with F_B; we have the inclusion $\epsilon : B \to F_B$. Let hence $\phi : M \twoheadrightarrow N$ be a surjective R-homomorphism and $\psi : F \to N$ an R-homomorphism. For each $b \in B$ choose an $m_b \in M$ such that $\phi(m_b) = \psi(b)$, using the surjectivity of ϕ.
Consider the map $\delta : B \to M$ sending $b \in B$ to m_b. By the universal property of F_B there exists the required α.
(b) The universal property of (a) (applied with $\psi = \mathrm{id}_F$) shows that there is $\alpha : F \to B$ such that $\phi \circ \alpha = \mathrm{id}_F$. Hence, the exact sequence is split and Proposition 5.14 shows $B \cong A \oplus F$. □

Appendix: Tensor products

This section will not be treated in the lecture and the sequel of the lecture does not depend on it.
Tensor products of modules are very important tools in algebra. Without any effort we could state (almost) the whole section for non-commutative rings. However, then we would have to make distinctions between left and right modules. For the sake of simplicity we stick to commutative rings and all modules are considered as left modules.

Definition 5.16. *Let R be a ring, M, N be R-modules.*
Let P be a $\mathbb{Z}$-module (note that this just means abelian group). A $\mathbb{Z}$-bilinear map

$$f : M \times N \to P$$

is called balanced *if for all $r \in R$, all $m \in M$ and all $n \in N$ one has*

$$f(rm, n) = f(m, rn).$$

In this case, we call (P, f) a balanced product of M and N.
A balanced product $(M \otimes_R N, \otimes)$ is called a tensor product of M and N over R *if the following universal property holds:*

> *For all balanced products (P, f) there is a unique group homomorphism $\phi : M \otimes_R N \to P$ such that $f = \phi \circ \otimes$ (draw diagram).*

Of course, we have to show that tensor products exists. This is what we start with.

Proposition 5.17. *Let R be a ring and let M, N be R-modules.*
Then a tensor product $(M \otimes_R N, \otimes)$ of M and N over R exists. If (P, f) is any other tensor product, then there is a unique group isomorphism $\phi : M \otimes_R N \to P$ such that $f = \phi \circ \otimes$.

Proof. The uniqueness statement is a consequence of the uniqueness in the universal property. This works similarly as the uniqueness of the direct product, the direct sum, etc. (that are proved in the exercises).

Let $F := \mathbb{Z}[M \times N]$, i.e. the free $\mathbb{Z}$-module with basis $M \times N$, that is the finite $\mathbb{Z}$-linear combinations of pairs (m, n) for $m \in M$ and $n \in N$.
Define G as the $\mathbb{Z}$-submodule of F generated by the following elements:

$$\begin{aligned} (m_1 + m_2, n) - (m_1, n) - (m_2, n) \qquad & \forall m_1, m_2 \in M,\ \forall n \in N, \\ (m, n_1 + n_2) - (m, n_1) - (m, n_2) \qquad & \forall m \in M,\ \forall n_1, n_2 \in N, \\ (rm, n) - (m, rn) \qquad & \forall r \in R,\ \forall m \in M,\ \forall n \in N. \end{aligned}$$

Define $M \otimes_R N := F/G$, as $\mathbb{Z}$-module. We shall use the notation $m \otimes n$ for the residue class $(m, n) + G$. Define the map $\otimes$ as

$$\otimes : M \times N \to M \otimes_R N, \quad (m, n) \mapsto m \otimes n.$$

It is $\mathbb{Z}$-bilinear and balanced by construction.
We now need to check the universal property. Let hence (P, f) be a balanced product of M and N. First we use the universal property of the free module $F = \mathbb{Z}[M \times N]$. For that let $\epsilon : M \times N \to F$ denote the inclusion. We obtain a unique group homomorphism $\phi : F \to P$ such that $\phi \circ \epsilon = f$ (draw diagram).
Claim: $G \subseteq \ker(\phi)$. Note first that $f(m, n) = \phi \circ \epsilon(m, n) = \phi((m, n))$ for all $m \in M$ and all $n \in N$. In particular, we have due to the bilinearity of f for all $m_1, m_2 \in M$ and all $n \in N$:

$$\phi((m_1 + m_2, n)) = f(m_1 + m_2, n) = f(m_1, n) + f(m_2, n) = \phi((m_1, n)) + \phi((m_2, n)),$$

whence $(m_1 + m_2, n) - (m_1, n) - (m_2, n) \in \ker(\phi)$. In the same way one shows that the other two kinds of elements also lie in $\ker(\phi)$, implying the claim.
Due to the claim, ϕ induces a homomorphism $\phi : F/G \to P$ such that $\phi \circ \otimes = f$ (note that $\otimes$ is just ϵ composed with the natural projection $F \to F/G$).
As for the uniqueness of ϕ. Note that the image of $\otimes$ is a generating system of F/G. Its elements are of the form $m \otimes n$. As we have $\phi \circ \otimes(m, n) = \phi(m \otimes n) = f(m, n)$, the values of ϕ at the generating set are prescribed and ϕ is hence unique. □

Example 5.18. *(a) Let $R = \mathbb{Z}$, $M = \mathbb{Z}/(m)$ and $N = \mathbb{Z}/(n)$ with $\gcd(m, n) = 1$. Then $M \otimes N = \mathbb{Z}/(m) \otimes_{\mathbb{Z}} \mathbb{Z}/(n) = 0$.*

Reason: As the gcd is 1, there are $a, b \in \mathbb{Z}$ such that $1 = am + bn$. Then for all $r \in \mathbb{Z}/(m)$ and all $s \in \mathbb{Z}/(n)$ we have:

$$\begin{aligned} r \otimes s = r \cdot 1 \otimes s = r(am + bn) \otimes s = ram \otimes s + (rbn \otimes s) \\ = 0 \otimes s + rb \otimes ns = 0 \otimes 0 + rb \otimes 0 = 0 \otimes 0 + 0 \otimes 0 = 0. \end{aligned}$$

(b) Let $R = \mathbb{Z}$, $M = \mathbb{Z}/(m)$ and $N = \mathbb{Q}$. Then $M \otimes N = \mathbb{Z}/(m) \otimes_{\mathbb{Z}} \mathbb{Q} = 0$.

Reason: Let $r \in \mathbb{Z}/(m)$ and $\frac{a}{b} \in \mathbb{Q}$. Then we have

$$r \otimes \frac{a}{b} = r \otimes m\frac{a}{mb} = rm \otimes \frac{a}{mb} = 0 \otimes \frac{a}{mb} = 0 \otimes 0 = 0.$$

(c) Let $R = \mathbb{Z}$, $M = \mathbb{Q}$ and N any $\mathbb{Z}$-module. Then $\mathbb{Q} \otimes_{\mathbb{Z}} N$ is a $\mathbb{Q}$-vector space.

Reason: It is an abelian group. The $\mathbb{Q}$-scalar multiplication is defined by $q.(r \otimes n) := qr \otimes n$.

(d) Let M be any R-module. Then $R \otimes_R M \xrightarrow{r\otimes m \mapsto rm} M$ is an isomorphism.

Reason: It suffices to show that M together with the map $R \times M \xrightarrow{(r,m)\mapsto rm} M$ is a tensor product. That is a very easy checking of the universal property.

Next we need to consider tensor products of maps.

Proposition 5.19. *Let R be a ring and let $f : M_1 \to M_2$ and $g : N_1 \to N_2$ be R-homomorphisms. Then there is a unique group homomorphism*

$$f \otimes g : M_1 \otimes_R N_1 \to M_2 \otimes_R N_2$$

such that $f \otimes g(m \otimes n) = f(m) \otimes g(n)$.
The map $f \otimes g$ is called the tensor product of f and g.

Proof. The map $\otimes \circ (f, g) : M_1 \times N_1 \xrightarrow{f,g} M_2 \times N_2 \xrightarrow{\otimes} M_2 \otimes_R N_2$ makes $M_2 \otimes_R N_2$ into a balanced product of M_1 and N_1 (draw diagram). By the universal property there is thus a unique homomorphism $M_1 \otimes_R N_1 \to M_2 \otimes_R N_2$ with the desired property. □

Lemma 5.20. *Let $M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} M_3$ and $N_1 \xrightarrow{g_1} N_2 \xrightarrow{g_2} N_3$ be R-homomorphisms.*
Then $(f_2 \otimes g_2) \circ (f_1 \otimes g_1) = (f_2 \circ f_1) \otimes (g_2 \circ g_1)$.

Proof. $(f_2 \circ f_1) \otimes (g_2 \circ g_1)(m \otimes n) = (f_2 \circ f_1(m)) \otimes (g_2 \circ g_1(n)) = f_2 \otimes g_2(f_1(m) \otimes g_1(n)) = (f_2 \otimes g_2) \circ (f_1 \otimes g_1)(m \otimes n)$. □

Corollary 5.21. *Let $f : M_1 \to M_2$ and $g : N_1 \to N_2$ be R-homomorphisms.*
Then $f \otimes g = (\mathrm{id}_{M_2} \otimes g) \circ (f \otimes \mathrm{id}_{N_1}) = (f \otimes \mathrm{id}_{N_2}) \circ (\mathrm{id}_{M_1} \otimes g)$.

Proof. This follows immediately from the previous lemma. □

Proposition 5.22. *Let R be a ring.*

(a) Let M_i for $i \in I$ and N be R-modules. Then there is a unique group isomorphism

$$\Phi : (\bigoplus_{i\in I} M_i) \otimes_R N \to \bigoplus_{i\in I} (M_i \otimes_R N)$$

such that $(m_i)_{i\in I} \otimes n \mapsto (m_i \otimes n)_{i\in I}$.

(b) Let N_i for $i \in I$ and M be R-modules. Then there is a unique group isomorphism

$$\Phi : M \otimes_R (\bigoplus_{i\in I} N_i) \to \bigoplus_{i\in I} (M \otimes_R N_i)$$

such that $m \otimes (n_i)_{i\in I} \mapsto (m \otimes n_i)_{i\in I}$.

Proof. We only prove (a), as (b) works in precisely the same way.
First we show the existence of the claimed homomorphism Φ by using the universal property of the tensor product. Define the map

$$f : (\bigoplus_{i\in I} M_i) \times N \to \bigoplus_{i\in I}(M_i \otimes_R N), \quad ((m_i)_{i\in I}, n) \mapsto (m_i, n)_{i\in I}.$$

This map makes $\bigoplus_{i\in I}(M_i\otimes_R N)$ into a balanced product of $\bigoplus_{i\in I} M_i$ and N, whence by the universal property of the tensor product the claimed homomorphism exists (and is unique).
Next we use the universal property of the direct sum to construct a homomorphism Ψ in the opposite direction, which will turn out to be the inverse of Φ. Let $j \in I$. By ϵ_j denote the embedding of M_j into the j-th component of $\bigoplus_{i\in I} M_i$. From these we further obtain maps $M_j \otimes_R N \xrightarrow{\epsilon_j\otimes \mathrm{id}_N} (\bigoplus_{i\in I} M_i) \otimes_R N$. Further consider the embeddings ι_j of $M_j \otimes_R N$ into the j-th component of $\bigoplus_{i\in I}(M_i \otimes_R N)$ from the definition of a direct sum. The universal property of direct sums now yields a homomorphism $\Psi : \bigoplus_{i\in I}(M_i \otimes_R N) \to (\bigoplus_{i\in I} M_i) \otimes_R N$ such that $\Psi \circ \iota_j = \epsilon_j \otimes \mathrm{id}_N$ for all $j \in J$.
Now it is easy to compute on generators that $\Phi \circ \Psi = \mathrm{id}$ and $\Psi \circ \Phi = \mathrm{id}$. □

Lemma 5.23. *Let R be a ring and let M, N be R-modules. Then $M \otimes_R N \cong N \otimes_R M$.*

Proof. This is not difficult and can be done as an exercise. □

Example 5.24. *Let L/K be a field extension. Then $L \otimes_K K[X]$ is isomorphic to $L[X]$ as an L-algebra.*

Lemma 5.25. *Let R and S be rings. Let M be an R-module, P an S-module, N an S-module and an R-module such that $s(rn) = r(sn)$ for all $r \in R$, all $s \in S$ and all $n \in N$.*

(a) $M \otimes_R N$ is an S-module via $s.(m \otimes n) = m \otimes (sn)$.

(b) $N \otimes_S P$ is an R-module via $r.(n \otimes p) = (rn) \otimes p$.

(c) There is an isomorphism

$$(M \otimes_R N) \otimes_S P \cong M \otimes_R (N \otimes_S P).$$

Proof. This is not difficult and can be done as an exercise. □

Lemma 5.26. *Let R be a ring, let M, N be R-modules, and let P be a $\mathbb{Z}$-module.*

(a) $\mathrm{Hom}_{\mathbb{Z}}(N, P)$ is an R-module via $(r.\varphi)(n) := \varphi(rn)$ for $r \in R$, $n \in N$, $\varphi \in \mathrm{Hom}_{\mathbb{Z}}(N, P)$.

(b) There is an isomorphism of abelian groups:

$$\mathrm{Hom}_R(M, \mathrm{Hom}_{\mathbb{Z}}(N, P)) \cong \mathrm{Hom}_{\mathbb{Z}}(M \otimes_R N, P).$$

(c) $\mathrm{Hom}_{\mathbb{Z}}(P, M)$ is an R-module via $(r.\varphi)(m) := \varphi(rm)$ for $r \in R$, $m \in M$, $\varphi \in \mathrm{Hom}_{\mathbb{Z}}(P, M)$.

(d) There is an isomorphism of abelian groups:

$$\mathrm{Hom}_R(\mathrm{Hom}_{\mathbb{Z}}(P, M), N) \cong \mathrm{Hom}_{\mathbb{Z}}(P, M \otimes_R N).$$

Proof. (a) and (c): Simple checking.
(b) The key point is the following bijection:

$$\{\text{Balanced maps } f : M \times N \to P\} \longrightarrow \mathrm{Hom}_R(M, \mathrm{Hom}_{\mathbb{Z}}(N, P)),$$

which is given by

$$f \mapsto \big(m \mapsto (n \mapsto f(m, n))\big).$$

To see that it is a bijection, we give its inverse:

$$\varphi \mapsto \big((m, n) \mapsto (\varphi(m))(n)\big).$$

Now it suffices to use the universal property of the tensor product.
(d) is similar to (b). □

Proposition 5.27. *Let R be a ring.*

(a) Let N, M_1, M_2, M_3 be R-modules. If the sequence

$$M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3 \to 0$$

is exact, then so is the sequence

$$M_1 \otimes_R N \xrightarrow{f\otimes \mathrm{id}} M_2 \otimes_R N \xrightarrow{g\otimes \mathrm{id}} M_3 \otimes_R N \to 0.$$

One says that the functor $\cdot \otimes_R N$ is right-exact.

(b) Let M, N_1, N_2, N_3 be R-modules. If the sequence

$$N_1 \xrightarrow{f} N_2 \xrightarrow{g} N_3 \to 0$$

is exact, then so is the sequence

$$M \otimes_R N_1 \xrightarrow{\mathrm{id}\otimes f} M \otimes_R N_2 \xrightarrow{\mathrm{id}\otimes g} M \otimes_R N_3 \to 0.$$

One says that the functor $M \otimes_R \cdot$ is right-exact.

Proof. We only prove (a), since (b) works precisely in the same way. We use Proposition 5.11 and obtain the exact sequence:

$$0 \to \mathrm{Hom}_R(M_3, \mathrm{Hom}_{\mathbb{Z}}(N, P)) \to \mathrm{Hom}_R(M_2, \mathrm{Hom}_{\mathbb{Z}}(N, P)) \to \mathrm{Hom}_R(M_1, \mathrm{Hom}_{\mathbb{Z}}(N, P))$$

for any $\mathbb{Z}$-module P. By Lemma 5.26 this exact sequence is nothing else but:

$$0 \to \mathrm{Hom}_{\mathbb{Z}}(M_3 \otimes_R N, P) \to \mathrm{Hom}_{\mathbb{Z}}(M_2 \otimes_R N, P) \to \mathrm{Hom}_{\mathbb{Z}}(M_1 \otimes_R N, P).$$

As P was arbitrary, again from Proposition 5.11 we obtain the exact sequence

$$M_1 \otimes_R N \to M_2 \otimes_R N \to M_3 \otimes_R N \to 0,$$

as claimed. □

Definition 5.28. *Let R be a ring.*

(a) An R-module M is called flat over R *if for all injective R-homomorphisms*

$$\varphi : N_1 \to N_2$$

also the group homomorphism

$$\mathrm{id}_M \otimes \varphi : M \otimes_R N_1 \to M \otimes_R N_2$$

is injective.

(b) An R-module M is called faithfully flat over R *if M is flat over R and for all R-homomorphisms $\varphi : N_1 \to N_2$, the injectivity of $\mathrm{id}_M \otimes \varphi$ implies the injectivity of φ.*

(c) A ring homomorphism $\phi : R \to S$ is called (faithfully) flat *if S is (faithfully) flat as R-module via ϕ.*

Lemma 5.29. *Let R be a ring and let M, N be R-modules.*

(a) M is flat over $R \Leftrightarrow M \otimes_R \bullet$ preserves exactness of sequences.

(b) N is flat over $R \Leftrightarrow \bullet \otimes_R N$ preserves exactness of sequences.

Proof. Combine Definition 5.28 and Proposition 5.27. □

Example 5.30. *(a) $\mathbb{Q}$ is flat as $\mathbb{Z}$-module.*

Reason: We don't give a complete proof here (since we haven't discussed the module theory over $\mathbb{Z}$). The reason is that any finitely generated abelian group is the direct sum of its torsion elements (that are the elements of finite order) and a free module. Tensoring with $\mathbb{Q}$ kills the torsion part and is injective on the free part (we will see that below).

(b) $\mathbb{Q}$ is not faithfully flat as $\mathbb{Z}$-module.

Reason: Consider $\mathbb{Z}/(p^2) \to \mathbb{Z}/(p)$, the natural projection (for p a prime), which is not injective. Tensoring with $\mathbb{Q}$ kills both sides (see Example 5.18), so we get $0 \cong \mathbb{Z}/(p^2) \otimes_{\mathbb{Z}} \mathbb{Q} \to \mathbb{Z}/(p) \otimes_{\mathbb{Z}} \mathbb{Q} \cong 0$, which is trivially injective.

(c) $\mathbb{F}_p$ is not flat as $\mathbb{Z}$-module (for p a prime).

Reason: The homomorphism $\mathbb{Z} \xrightarrow{n \mapsto pn} \mathbb{Z}$ (multiplication by p) is clearly injective. But, after tensoring it with $\mathbb{F}_p$ over $\mathbb{Z}$, we obtain the zero map, which is not injective.

6 Localisation

Aims:

- Learn and master the concepts of local rings and the localisation of modules;

- learn and master Nakayama's lemma and some of its consequences;
- learn and master exactness properties of localisation;
- know examples and standard theorems;
- be able to prove simple properties.

Definition 6.1. *A ring R is called* local *if it has a single maximal ideal.*

Example 6.2. *(a) Every field K is a local ring, its unique maximal ideal being the zero ideal.*

(b) Let p be a prime number. The ring $\mathbb{Z}/(p^n)$ is a local ring with unique maximal ideal generated by p.

Reason: (p) is a maximal ideal, the quotient being $\mathbb{F}_p$, a field. If $\mathfrak{a} \subsetneq \mathbb{Z}/(p^n)$ is a proper ideal and $x \in \mathfrak{a}$, then $x = py + (p^n)$, as otherwise x would be a unit. This shows that $x \in (p)$, whence $\mathfrak{a} \subseteq (p)$.

(c) $\{\frac{a}{b} \in \mathbb{Q} \mid a, b \in \mathbb{Z}, \gcd(a, b) = 1, 2 \nmid b\}$ is a local ring (see Example 6.7, where one also finds a geometric example).

Lemma 6.3. *Let R be a local ring with unique maximal ideal $\mathfrak{m}$. Then we have*

$$R = \mathfrak{m} \sqcup R^\times \quad \text{(disjoint union).}$$

Hence, the set of units is the complement of the maximal ideal $R^\times = R \setminus \mathfrak{m}$, and, equivalently, the maximal ideal is the set on non-units $\mathfrak{m} = R \setminus R^\times$.
Moreover, any ring R is local if and only if $R \setminus R^\times$ is an ideal of R.

Proof. We already know from Corollary 1.19 (b) that every non-unit lies in some maximal ideal, whence it lies in $\mathfrak{m}$. On the other hand, every element of $\mathfrak{m}$ is a non-unit, as otherwise $\mathfrak{m} = R$. To see the last statement, just note that if $I := R \setminus R^\times$ is an ideal, then it is necessarily maximal and also the only maximal ideal, as any ideal containing an element outside I contains a unit. □

We will now introduce/recall the process of localisation of rings and modules, which makes modules/rings local.

Proposition 6.4. *Let R be a ring, $D \subset R$ a multiplicatively closed subset (i.e. for $d_1, d_2 \in D$ we have $d_1 d_2 \in D$) containing 1.*

(a) An equivalence relation on $D \times R$ is defined by

$$(d_1, r_1) \sim (d_2, r_2) \;\Leftrightarrow\; \exists s \in D : \; s(r_1 d_2 - r_2 d_1) = 0.$$

The equivalence class of (d_1, r_1) is denoted by $\frac{r_1}{d_1}$. So, D is the set of denominators.

(b) The set of equivalence classes $D^{-1}R$ is a ring with respect to

$$+ : D^{-1}R \times D^{-1}R \to D^{-1}R, \ \ \frac{r_1}{d_1} + \frac{r_2}{d_2} = \frac{r_1 d_2 + r_2 d_1}{d_1 d_2}$$

and

$$\cdot : D^{-1}R \times D^{-1}R \to D^{-1}R, \ \ \frac{r_1}{d_1} \cdot \frac{r_2}{d_2} = \frac{r_1 r_2}{d_1 d_2}.$$

Neutral elements are $0 := \frac{0}{1}$ and $1 := \frac{1}{1}$.

(c) The map $\mu : R \to D^{-1}R$, $r \mapsto \frac{r}{1}$, is a ring homomorphism with kernel $\{r \in R \mid \exists d \in D : rd = 0\}$. In particular, if R is an integral domain, then this ring homomorphism is injective.

Proof. Easy checking. □

Note that for an integral domain R, the equivalence relation takes the easier form

$$(d_1, r_1) \sim (d_2, r_2) \ \Leftrightarrow \ r_1 d_2 - r_2 d_1 = 0,$$

provided $0 \notin D$ (if $0 \in D$, then $D^{-1}R$ is always the zero ring, as any element is equivalent to $\frac{0}{1}$).
If R is an integral domain and $1 \in D' \subset D$ is a multiplicatively closed subset, then $D'^{-1}R$ is the subring of $D^{-1}R$ the elements of which can be written as fractions $\frac{r}{d'}$ with denominator $d' \in D'$.

Example 6.5. *Let R be an integral domain. Then $D = R \setminus \{0\}$ is a multiplicatively closed subset. Then $\mathrm{Frac}(R) := D^{-1}R$ is the field of fractions of R.*
Subexamples:

(a) For $R = \mathbb{Z}$, we have $\mathrm{Frac}\,\mathbb{Z} = \mathbb{Q}$.

(b) Let K be a field and $R := K[X_1, \ldots, X_n]$. Then $\mathrm{Frac}\,K[X_1, \ldots, X_n] =: K(X_1, \ldots, X_n)$ is the field of rational functions over K (in n variables)*. To be explicit, the elements of $K(X_1, \ldots, X_n)$ are equivalence classes written as $\frac{f(X_1,\ldots,X_n)}{g(X_1,\ldots,X_n)}$ with $f, g \in K[X_1, \ldots, X_n]$, $g(X_1, \ldots, X_n)$ not the zero-polynomial. The equivalence relation is, of course, the one from the definition; as $K[X_1, \ldots, X_n]$ is a UFD, we may represent the class $\frac{f(X_1,\ldots,X_n)}{g(X_1,\ldots,X_n)}$ as a 'lowest fraction', by dividing numerator and denominator by their greatest common divisor.*

Definition 6.6. *Let R be a ring and $\mathfrak{p} \lhd R$ be a prime ideal. Then $D := R \setminus \mathfrak{p}$ is multiplicatively closed and $1 \in D$ and $0 \notin D$.*
Then $R_\mathfrak{p} := D^{-1}R$ is called the localisation of R at $\mathfrak{p}$.

Example 6.7. *(a) Let R be an integral domain. Then (0) is a prime ideal and $\mathrm{Frac}(R) = R_{(0)}$ (hence the examples above can also be seen as localisations).*

In that case, we also have $D = R \setminus \mathfrak{p} \subseteq R \setminus \{0\}$ and so the localisation $R_\mathfrak{p}$ at any prime ideal $\mathfrak{p}$ is the subring of $R_{(0)} = \mathrm{Frac}(R)$ consisting of fractions $\frac{r}{d}$ that can be written with denominator $d \in D$, i.e. $d \notin \mathfrak{p}$.

(b) Let $R = \mathbb{Z}$ and p a prime number, so that (p) is a prime ideal. Then the localisation of $\mathbb{Z}$ at (p) is $\mathbb{Z}_{(p)}$ and its elements are $\{\frac{r}{d} \in \mathbb{Q} \mid p \nmid d, \gcd(r, d) = 1\}$. Here we used that $\mathbb{Z}$ is an integral domain and so $\mathbb{Z}_{(p)} \subset \mathrm{Frac}(\mathbb{Z}) = \mathbb{Q}$.

(c) *Let R be a local ring with maximal ideal $\mathfrak{m}$. As all maximal ideals are prime, we can consider $R_{\mathfrak{m}}$, the localisation of R at $\mathfrak{m}$. Because of Lemma 6.3, $D = R \setminus \mathfrak{m} = R^\times$, the map $\mu : R \to R_{\mathfrak{m}}$ is an isomorphism.*

(d) *Let K be a field and consider $\mathbb{A}^n(K)$. Let $\underline{a} = (a_1, \ldots, a_n) \in \mathbb{A}^n(K)$.*

Let $\mathfrak{p}$ be the kernel of the ring homomorphism

$$K[X_1, \ldots, X_n] \to K, \quad f \mapsto f(a_1, \ldots, a_n).$$

Explicitly, $\mathfrak{p} = \{f \in K[X_1, \ldots, X_n] \mid f(\underline{a}) = 0\}$. As this homomorphism is clearly surjective (take constant polynomials as preimages), we have that $K[X_1, \ldots, X_n]/\mathfrak{p}$ is isomorphic to K, showing that $\mathfrak{p}$ is a maximal (and, hence, a prime) ideal.

The localisation $K[X_1, \ldots, X_n]_{\mathfrak{p}}$ is the subring of $K(X_1, \ldots, X_n)$ consisting of elements that can be written as $\frac{f(X_1,\ldots,X_n)}{g(X_1,\ldots,X_n)}$ with $g(a_1, \ldots, a_n) \neq 0$.

This is the same as the set of rational functions $K(X_1, \ldots, X_n)$ that are defined in a Zariski-open neighbourhood of a. Namely, let $\frac{f}{g} \in K[X_1, \ldots, X_n]_{\mathfrak{p}}$ so that $g(\underline{a}) \neq 0$. Then the function $\underline{x} \mapsto \frac{f(\underline{x})}{g(\underline{x})}$ is well-defined (i.e. we do not divide by 0) on the Zariski-open set $\mathbb{A}^n(K) \setminus \mathcal{V}_{(g)}(K)$, which contains $\underline{a}$. On the other hand, if for $\frac{f}{g} \in K(X_1, \ldots, X_n)$ the function $\underline{x} \mapsto \frac{f(\underline{x})}{g(\underline{x})}$ is well-defined in some Zariski-open neighbourhood of $\underline{a}$, then, in particular, it is well-defined at $\underline{a}$, implying $\frac{f}{g} \in K[X_1, \ldots, X_n]_{\mathfrak{p}}$.

In conclusion, $K[X_1, \ldots, X_n]_{\mathfrak{p}}$ is the ring of rational functions that are well-defined in a Zariski-open neighbourhood of $\underline{a}$.

Example 6.8. *Let R be a ring and let $f \in R$ be an element which is not nilpotent (i.e. $f^n \neq 0$ for all $n \in \mathbb{N}$). Then $D := \{f^n \mid n \in \mathbb{N}\}$ (use $0 \in \mathbb{N}$) is multiplicatively closed and we can form $D^{-1}R$. This ring is sometimes denoted R_f (Attention: easy confusion is possible).*
Subexample: Let $R = \mathbb{Z}$ and $0 \neq a \in \mathbb{N}$. Let $D = \{a^n \mid n \in \mathbb{N}\}$. Then $D^{-1}\mathbb{Z} = \{\frac{r}{a^n} \in \mathbb{Q} \mid r \in R, n \in \mathbb{N}, \gcd(r, a^n) = 1\}$.

Proposition 6.9. *Let R be a ring and $D \subseteq R$ a multiplicatively closed subset with $1 \in D$. Let $\mu : R \to D^{-1}R$, given by $r \mapsto \frac{r}{1}$. Note that $\mu^{-1}(\mathfrak{b})$ can be identified with the subset of elements in an ideal $\mathfrak{b} \in D^{-1}R$ that can be written with denominator 1.*

(a) *The map*

$$\{\mathfrak{b} \lhd D^{-1}R \text{ ideal } \} \longrightarrow \{\mathfrak{a} \lhd R \text{ ideal } \}, \quad \mathfrak{b} \mapsto \mu^{-1}(\mathfrak{b}) \lhd R$$

is an injection, which preserves inclusions and intersections. Moreover, if $\mathfrak{b} \lhd D^{-1}R$ is a prime ideal, then so is $\mu^{-1}(\mathfrak{b}) \lhd R$.

(b) *Let $\mathfrak{a} \lhd R$ be an ideal. Then the following statements are equivalent:*

(i) $\mathfrak{a} = \mu^{-1}(\mathfrak{b})$ for some $\mathfrak{b} \lhd D^{-1}R$ (i.e. $\mathfrak{a}$ is in the image of the map in (a)).

(ii) $\mathfrak{a} = \mu^{-1}(\mathfrak{a}D^{-1}R)$ (here $\mathfrak{a}D^{-1}R$ is short for the ideal of $D^{-1}R$ generated by $\mu(\mathfrak{a})$, i.e. by all elements of the form $\frac{a}{1}$ for $a \in \mathfrak{a}$).

(iii) Every $d \in D$ is a non-zero divisor modulo $\mathfrak{a}$, meaning that if $r \in R$ and $rd \in \mathfrak{a}$, then $r \in \mathfrak{a}$.

Note that in these cases $D \cap \mathfrak{a} = \emptyset$.

(c) The map in (a) defines a bijection between the prime ideals of $D^{-1}R$ and the prime ideals $\mathfrak{p}$ of R such that $D \cap \mathfrak{p} = \emptyset$. In particular, if $\mathfrak{p}$ is a prime ideal of R with $D \cap \mathfrak{p} = \emptyset$, then $\mathfrak{p}D^{-1}R$ is a prime ideal.

Proof. Exercise. □

Corollary 6.10. *Let R be a ring and $\mathfrak{p} \lhd R$ be a prime ideal. Then the localisation $R_{\mathfrak{p}}$ of R at $\mathfrak{p}$ is a local ring (in fact, its maximal ideal is $D^{-1}\mathfrak{p}$, in the notation of Proposition 6.17).*

Proof. Let $D = R \setminus \mathfrak{p}$. Note that $\emptyset = \mathfrak{a} \cap D = \mathfrak{a} \cap (R \setminus \mathfrak{p})$ is equivalent to $\mathfrak{a} \subseteq \mathfrak{p}$.
Hence, Proposition 6.9 (c) gives an inclusion preserving bijection between the prime ideals of $D^{-1}R$ and the prime ideals of R which are contained in $\mathfrak{p}$. The corollary immediately follows. □

Definition 6.11. *Let R be a ring. The* Jacobson radical *is defined as the intersection of all maximal ideals of R:*

$$J(R) := \bigcap_{\mathfrak{m} \lhd R \text{ maximal ideal}} \mathfrak{m}$$

For instance, $J(\mathbb{Z}) = 0$ because it consists of those integers that are divisible by all prime numbers. If R is a local ring, then $J(R) = \mathfrak{m}_R$, its maximal ideal.

Lemma 6.12. *Let R a ring and let $\mathfrak{a} \lhd R$ be an ideal which is contained in $J(R)$. Then for any $a \in \mathfrak{a}$, one has $1 - a \in R^\times$.*

Proof. If $1 - a$ were not a unit, then there would be a maximal ideal $\mathfrak{m}$ containing $1 - a$. Since $a \in J(R)$, it follows that $a \in \mathfrak{m}$, whence $1 \in \mathfrak{m}$, contradiction. □

Lemma 6.13. *Let R be a ring, M an R-module and $\mathfrak{a} \lhd R$ an ideal. Then $\mathfrak{a}M = \{\sum_{i=1}^n a_i m_i \mid n \in \mathbb{N}, a_i \in \mathfrak{a},\ m_i \in M \text{ for } i = 1, \ldots, n\} \subseteq M$ is an R-submodule of M.*

Proof. Easy checking. □

Proposition 6.14 (Nakayama's Lemma)**.** *Let R be a ring and M a finitely generated R-module. Let $\mathfrak{a} \lhd R$ be an ideal such that $\mathfrak{a} \subseteq J(R)$. Suppose $\mathfrak{a}M = M$. Then $M = 0$.*

Proof. We use that M is finitely generated by choosing finitely many generators $m_1, \ldots, m_n$ for M as an R-module. Now we use $\mathfrak{a}M = M$ in order to express each generator as an $\mathfrak{a}$-linear combination of these generators. More precisely, for each $i \in \{1, \ldots, n\}$ there are $a_{i,j} \in \mathfrak{a}$ (for $1 \leq j \leq n$) such that

$$m_i = \sum_{j=1}^n a_{i,j} m_j.$$

We write the coefficients into a matrix $A = (a_{i,j})_{1 \leq i,j \leq n}$. It satisfies:

$$A := \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n,1} & a_{n,2} & \cdots & a_{n,n} \end{pmatrix} \cdot \begin{pmatrix} m_1 \\ m_2 \\ \vdots \\ m_n \end{pmatrix} = \begin{pmatrix} m_1 \\ m_2 \\ \vdots \\ m_n \end{pmatrix}.$$

We now form the matrix $B := \mathrm{id}_{n \times n} - A$. By the previous calculation we obtain

$$B \cdot \begin{pmatrix} m_1 \\ m_2 \\ \vdots \\ m_n \end{pmatrix} = 0.$$

Let B^* be the adjoint matrix, which satisfies $B^* \cdot B = \det(B) \cdot \mathrm{id}_{n \times n}$. Hence:

$$0 = B^* \cdot B \cdot \begin{pmatrix} m_1 \\ m_2 \\ \vdots \\ m_n \end{pmatrix} = \det(B) \cdot \begin{pmatrix} m_1 \\ m_2 \\ \vdots \\ m_n \end{pmatrix}.$$

Hence, for all $i \in \{1, \ldots, n\}$ we find $\det(B) \cdot m_i = 0$, thus $\det(B) \cdot M = 0$. The usual rules for computing the determinant immediately show $\det(B) = 1 - a$ for some $a \in A$. Hence, we have $(1-a)M = 0$.
By Lemma 6.12 we get $(1-a) \in R^\times$, let $b \in R^\times$ be such that $b(1-a) = 1$. Hence $0 = b \cdot (1-a) \cdot M = M$. □

The following corollary turns out to be very useful in many applications.

Corollary 6.15. *Let R be a local ring with maximal ideal $\mathfrak{a}$ and let M be a finitely generated R-module. Let $x_1, \ldots, x_n \in M$ be elements such that their images $\overline{x}_i := x_i + \mathfrak{a}M$ are generators of the quotient module $M/\mathfrak{a}M$.*
Then $x_1, \ldots, x_n$ generate M as an R-module.

Proof. Let N be the submodule of M generated by $x_1, \ldots, x_n$. We want to show $M = N$, or in other terms $M/N = 0$. Let $m \in M$ be any element. By assumption there exists $y \in N$ such that

$$m + \mathfrak{a}M = y + \mathfrak{a}M.$$

This means that there are elements $a_1, \ldots, a_r \in \mathfrak{a}$ and $m_1, \ldots, m_r \in M$ such that

$$m = y + \sum_{i=1}^{r} a_i m_i.$$

Passing to classes in M/N we get

$$m + N = \sum_{i=1}^{r} a_i (m_i + N)$$

thus $m + N \in \mathfrak{a}(M/N)$. This shows $\mathfrak{a}(M/N) = M/N$. By Proposition 6.14 we obtain $M/N = 0$, hence $M = N$, as required. □

Example 6.16. *Let p be a prime number and consider $\mathbb{Z}_{(p)}$, the localisation of $\mathbb{Z}$ at (p). We can represent its elements as fractions $\frac{a}{b} \in \mathbb{Q}$ with $\gcd(a,b) = 1$ and $p \nmid b$. Note that the map*

$$\pi : \mathbb{Z}_{(p)} \to \mathbb{F}_p, \quad \frac{a}{b} \mapsto ab^{-1} \mod p$$

is a well-defined surjective ring homomorphism. Its kernel is $\mathfrak{p} := p\mathbb{Z}_{(p)}$, the elements of which are of the form $\frac{pa}{b} \in \mathbb{Q}$ with $\gcd(pa,b) = 1$. This shows that $\mathfrak{p}$ is a maximal (and hence a prime) ideal of $\mathbb{Z}_{(p)}$.
Consider $V = \mathbb{Z}_{(p)}^n$. Then by Corollary 6.15, a list of vectors $v_1, \ldots, v_m \in V$ generates V if and only if $\pi(v_1), \ldots, \pi(v_m)$ generates $\mathbb{F}_p^n$.
For this conclusion, we use that $V/\mathfrak{p}V \cong \mathbb{F}_p^n$.

Proposition 6.17. *Let R be a ring, $D \subset R$ a multiplicatively closed subset containing 1. Let M be an R-module.*

(a) An equivalence relation on $D \times M$ is defined by

$$(d_1, m_1) \sim (d_2, m_2) \;\Leftrightarrow\; \exists s \in D : \; s(d_1 m_2 - d_2 m_1) = 0.$$

(b) The set of equivalence classes $D^{-1}M$ is an $D^{-1}R$-module with respect to

$$+ : D^{-1}M \times D^{-1}M \to D^{-1}M, \quad \frac{m_1}{d_1} + \frac{m_2}{d_2} = \frac{d_2 m_1 + d_1 m_2}{d_1 d_2}$$

and scalar-multiplication

$$\cdot : D^{-1}R \times D^{-1}M \to D^{-1}M, \quad \frac{r}{d_1} \cdot \frac{m}{d_2} = \frac{rm}{d_1 d_2}.$$

The neutral element is $0 := \frac{0}{1}$.

(c) The map $\mu : M \to D^{-1}M$, $m \mapsto \frac{m}{1}$, is an R-homomorphism with kernel $\{m \in M \mid \exists d \in D : dm = 0\}$.

Proof. Easy checking. □

Lemma 6.18. *Let R be a ring, $D \subset R$ multiplicatively closed containing 1. Let M, N be R-modules and $\phi : M \to N$ an R-homomorphism.*

(a) The map

$$\phi_D : D^{-1}M \to D^{-1}N, \quad \frac{m}{d} \mapsto \frac{\phi(m)}{d}$$

is an $D^{-1}R$-homomorphism.

(b) Let

$$A \xrightarrow{\alpha} B \xrightarrow{\beta} C$$

be an exact sequence of R-modules. Then the sequence

$$D^{-1}A \xrightarrow{\alpha_D} D^{-1}B \xrightarrow{\beta_D} D^{-1}C$$

is also exact. One says that localisation is an exact functor.

In particular ϕ_D is injective (surjective, bijective) if ϕ is injective (surjective, bijective).

Proof. (a) Easy checking.
(b) First of all $\beta \circ \alpha = 0$ immediatly implies $\beta_D \circ \alpha_D = 0$ because $\beta_D \circ \alpha_D(\frac{a}{d}) = \frac{\beta \circ \alpha(a)}{d} = \frac{0}{d} = 0$. Let now $\frac{b}{d}$ be in the kernel of β_D, that is $0 = \beta_D(\frac{b}{d}) = \frac{\beta(b)}{d}$. Hence, there is $s \in D$ such that $0 = s\beta(b) = \beta(sb)$. Using the exactness of the original sequence, we find an $a \in A$ such that $\alpha(a) = sb$. Thus, $\frac{b}{d} = \frac{\alpha(a)}{sd} = \alpha_D(\frac{a}{sd})$. □

Lemma 6.19. *Let R be a ring and $\mathfrak{m}$ a maximal ideal.*

(a) The natural map $\mu : R \to R_{\mathfrak{m}}$, $r \mapsto \frac{r}{1}$ induces a ring isomorphism

$$R/\mathfrak{m} \cong R_{\mathfrak{m}}/\mathfrak{m}R_{\mathfrak{m}}.$$

(b) Let M be an R-module and denote by $M_{\mathfrak{m}}$ its localisation at $\mathfrak{m}$. Then:

$$M/\mathfrak{m}M \cong M_{\mathfrak{m}}/\mathfrak{m}R_{\mathfrak{m}}M_{\mathfrak{m}}.$$

Proof. Exercise. □

The next proposition gives local characterisations, i.e. it gives criteria saying that a certain property (injectivity, surjectivity) holds if and only if it holds in all localisations. We first start with a lemma that gives a local characterisation of a module to be zero.

Lemma 6.20. *Let R be a ring and M an R-module. Then the following statements are equivalent:*

(i) M is the zero module.

(ii) For all prime ideals $\mathfrak{p} \lhd R$, the localisation $M_{\mathfrak{p}}$ is the zero module.

(iii) For all maximal ideals $\mathfrak{m} \lhd R$, the localisation $M_{\mathfrak{m}}$ is the zero module.

Proof. '(i) $\Rightarrow$ (ii)': Clear.
'(ii) $\Rightarrow$ (iii)' is trivial because all maximal ideals are prime.
'(iii) $\Rightarrow$ (i)': Assume $M \neq 0$ and let $0 \neq m \in M$, put $N := R.m \subseteq M$ and let $\mathfrak{a}$ be the kernel of the surjective ring homomorphism $R \xrightarrow{r \mapsto r.m} N$. As $m \neq 0$, the unit 1 is not in its kernel, and hence $\mathfrak{a}$ is a proper ideal of R. As such it is contained in some maximal ideal $\mathfrak{m}$. The injectivitiy $N \hookrightarrow M$ leads to the injectivity of $N_{\mathfrak{m}} \hookrightarrow M_{\mathfrak{m}}$ by Lemmata 6.18 and 5.10. Hence, $N_{\mathfrak{m}} = 0$. So, $\frac{m}{1} = \frac{0}{1} \in N_{\mathfrak{m}}$. So, there is $s \in R \setminus \mathfrak{m}$ such that $sm = 0$. This, however, means $s \in \mathfrak{a} \subseteq \mathfrak{m}$, contradiction. □

Proposition 6.21. *Let R be a ring and $\varphi : M \to N$ an R-homomorphism. For a prime ideal $\mathfrak{p} \lhd R$, denote by $\varphi_{\mathfrak{p}} : M_{\mathfrak{p}} \to N_{\mathfrak{p}}$ the localisation at $\mathfrak{p}$. Then the following statements are equivalent:*

(i) φ is injective (surjective).

(ii) For all prime ideals $\mathfrak{p} \lhd R$, the localisation $\varphi_{\mathfrak{p}}$ is injective (surjective).

(iii) For all maximal ideals $\mathfrak{m} \lhd R$, the localisation $\varphi_{\mathfrak{m}}$ is injective (surjective).

Proof. '(i) $\Rightarrow$ (ii)': Lemma 6.18.
'(ii) $\Rightarrow$ (iii)' is trivial because all maximal ideals are prime.
'(iii) $\Rightarrow$ (i)': We only show this statement for the injectivity. The surjectivity is very similar. Let K be the kernel of φ, so that we have the exact sequence

$$0 \to K \to M \xrightarrow{\varphi} N.$$

By Lemma 6.18, also the sequence

$$0 \to K_{\mathfrak{m}} \to M_{\mathfrak{m}} \xrightarrow{\varphi_{\mathfrak{m}}} N_{\mathfrak{m}}$$

is exact for any maximal ideal $\mathfrak{m}$. As $\varphi_{\mathfrak{m}}$ is injective, it follows that $K_{\mathfrak{m}} = 0$. By Lemma 6.20, $K = 0$, showing that φ is injective. □

Appendix: Localisation as a tensor product

Lemma 6.22. *Let R be a ring, $D \subset R$ multiplicatively closed containing 1 and M an R-module. The map*

$$\psi : D^{-1}M \to D^{-1}R \otimes_R M, \quad \frac{m}{d} \mapsto \frac{1}{d} \otimes m$$

is an $D^{-1}R$-isomorphism, where $D^{-1}R \otimes_R M$ is an $D^{-1}R$-module via $\frac{x}{d}.(\frac{y}{s} \otimes m) := (\frac{x}{d}\frac{y}{s}) \otimes m$.

Proof. First we check that ψ is well-defined: Let $\frac{m_1}{d} = \frac{m_2}{s}$, i.e. there is $u \in S$ such that $u(sm_1 - dm_2) = 0$. Now $\frac{1}{d} \otimes m_1 = \frac{su}{sdu} \otimes m_1 = \frac{1}{sdu} \otimes sum_1 = \frac{1}{sdu} \otimes dum_2 = \frac{du}{sdu} \otimes m_2 = \frac{1}{s} \otimes m_2$. That ψ is an $D^{-1}R$-homomorphism is easily checked.
We now construct an inverse to ψ using the universal property of the tensor product. Define

$$f : D^{-1}R \times M \to D^{-1}M, \quad (\frac{x}{d}, m) \mapsto \frac{xm}{d}.$$

This is a balanced map over R. Hence, there is a unique $\mathbb{Z}$-homomorphism $\phi : D^{-1}R \otimes M \to D^{-1}M$ such that $\phi(\frac{x}{d} \otimes m) = \frac{xm}{d}$.
It is clear that ϕ is an $D^{-1}R$-homomorphism and that $\phi \circ \psi$ and $\psi \circ \phi$ are the identity. □

Chapter III

Advanced ring theory

7 Noetherian rings and Hilbert's Basissatz

Aims:

- Learn and master the concepts of Noetherian and Artinian modules and rings;
- know Hilbert's Basissatz;
- be able to prove simple properties.

In this short section, we treat Noetherian and Artinian rings and prove Hilbert's basis theorem.

Definition 7.1. *Let R be a ring and M an R-module. The module M is called* Noetherian *(resp.* Artinian*) if every ascending (resp. descending) chain of R-submodules of M*

$$M_1 \subseteq M_2 \subseteq M_3 \subseteq \dots$$

(resp. $M_1 \supseteq M_2 \supseteq M_3 \supseteq \dots$) becomes stationary, i.e. there is $N \in \mathbb{N}$ such that for all $n \geq N$ we have $M_n = M_N$.
The ring R is called Noetherian *(resp.* Artinian*) if it has this property as an R-module, i.e. if every ascending (descending) chain of ideals becomes stationary.*

Lemma 7.2. *Let R be a ring and M an R-module.*
Then M is Noetherian (resp. Artinian) if and only if every non-empty set S of submodules of M has a maximal (resp. minimal) element.
By a maximal (resp. minimal) element of S we mean an R-module $N \in S$ such that $N \subseteq N_1$ (resp. $N \supseteq N_1$) implies $N = N_1$ for any $N_1 \in S$.

Proof. We only prove the Lemma for the Noetherian case. The Artinian case is similar.
Let S be a non-empty set of R-submodules of M that does not have a maximal element. Then construct an infinite ascending chain with strict inclusions as follows. Choose any $M_1 \in S$. As M_1 is not maximal, it is strictly contained in some $M_2 \in S$. As M_2 is not maximal, it is strictly contained in some $M_3 \in S$, etc. leading to the claimed chain. Hence, M is not Noetherian.

Conversely, let $M_1 \subseteq M_2 \subseteq M_3 \subseteq \ldots$ be an ascending chain. Let $S = \{M_i \mid i \in \mathbb{N}\}$. This set contains a maximal element M_N by assumption. This means that the chain becomes stationary at N. □

Proposition 7.3. *Let R be a ring and M an R-module. The following statements are equivalent:*

(i) M is Noetherian.

(ii) Every submodule $N \leq M$ is finitely generated as R-module.

Proof. '(i) ⇒ (ii)': Assume that N is not finitely generated. In particular, there are then elements $n_i \in N$ for $i \in \mathbb{N}$ such that $\langle n_1 \rangle \subsetneq \langle n_1, n_2 \rangle \subsetneq \langle n_1, n_2, n_3 \rangle \subsetneq \ldots$, contradicting the Noetherian-ness of M.
'(ii) ⇒ (i)': Let $M_1 \subseteq M_2 \subseteq M_3 \subseteq \ldots$ be an ascending chain of R-submodules. Form $U := \bigcup_{i \in \mathbb{N}} M_i$. It is an R-submodule of M, which is finitely generated by assumption. Let $x_1, \ldots, x_d \in U$ be generators of U. As all x_i already lie in some M_{j_i}, there is an N such that $x_i \in M_N$ for all $i = 1, \ldots, d$. Hence, the chain becomes stationary at N. □

The proposition shows that in particular every principal ideal domain is a Noetherian ring, since all ideals (recall that the ideals of a ring R are precisely the R-submodules of R) are generated by a single element, hence, finitely generated. Hence, we obtain that $\mathbb{Z}$ and $K[X]$ (for K a field) are Noetherian; however, we do not yet know about the polynomial ring in more than one variable; its Noetherian property is the content of Hilbert's Basissatz.

Lemma 7.4. *Let R be a ring and $0 \to N \to M \to M/N \to 0$ be an exact sequence of R-modules. The following statements are equivalent:*

(i) M is Noetherian (resp. Artinian).

(ii) N and M/N are Noetherian (resp. Artinian).

Proof. We only prove this in the Noetherian case. The Artinian one is similar.
'(i) ⇒ (ii)': N is Noetherian because every ascending chain of submodules of N is also an ascending chain of submodules of M, and hence becomes stationary.
To see that M/N is Noetherian consider an ascending chain of R-submodules $\overline{M}_1 \subseteq \overline{M}_2 \subseteq \overline{M}_3 \subseteq \ldots$ of M/N. Taking preimages for the natural projection $\pi : M \to M/N$ gives an ascending chain in M, which by assumption becomes stationary. Because of $\pi(\pi^{-1}(\overline{M}_i)) = \overline{M}_i$, also the original chain becomes stationary.
'(ii) ⇒ (i)': Let

$$M_1 \subseteq M_2 \subseteq M_3 \subseteq \ldots$$

be an ascending chain of R-submodules. The chain

$$M_1 \cap N \subseteq M_2 \cap N \subseteq M_3 \cap N \subseteq \ldots$$

becomes stationary (say, at the integer n) because its members are submodules of the Noetherian R-module N. Moreover, the chain

$$(M_1 + N)/N \subseteq (M_2 + N)/N \subseteq (M_3 + N)/N \subseteq \ldots$$

also becomes stationary (say, at the integer m) because its members are submodules of the Noetherian R-module M/N. By one of the isomorphism theorems, we have $(M_i + N)/N \cong M_i/(M_i \cap N)$. Let now i be greater than n and m. We hence have for all $j \geq 0$:

$$M_i/(M_i \cap N) = M_{i+j}/(M_i \cap N).$$

The other isomorphism theorem then yields:

$$0 \cong (M_{i+j}/(M_i \cap N))/(M_i/(M_i \cap N)) \cong M_{i+j}/M_i,$$

showing $M_i = M_{i+j}$. □

Proposition 7.5. *Let R be a Noetherian (resp. Artinian) ring. Then every finitely generated R-module is Noetherian (resp. Artinian).*

Proof. Exercise. □

Proposition 7.6 (Hilbert's Basissatz)**.** *Let R be a Noetherian ring and $n \in \mathbb{N}$. Then $R[X_1, \ldots, X_n]$ is a Noetherian ring. In particular, every ideal $\mathfrak{a} \lhd R[X_1, \ldots, X_n]$ is finitely generated.*

Proof. By induction it clearly suffices to prove the case $n = 1$. So, let $\mathfrak{a} \lhd R[X]$ be any ideal. We show that $\mathfrak{a}$ is finitely generated, which implies the assertion by Proposition 7.3.
The very nice trick is the following:

$$\begin{aligned}
&\mathfrak{a}_0 := \{a_0 \in R \mid a_0 \in \mathfrak{a}\} \lhd R \\
&\mid\cap \\
&\mathfrak{a}_1 := \{a_1 \in R \mid \exists b_0 \in R : a_1 X + b_0 \in \mathfrak{a}\} \lhd R \\
&\mid\cap \\
&\mathfrak{a}_2 := \{a_2 \in R \mid \exists b_0, b_1 \in R : a_2 X^2 + b_1 X + b_0 \in \mathfrak{a}\} \lhd R \\
&\mid\cap \\
&\ \ \vdots
\end{aligned}$$

So, $\mathfrak{a}_n$ is the set of highest coefficients of polynomials of degree n lying in $\mathfrak{a}$. The inclusion $\mathfrak{a}_{n-1} \subseteq \mathfrak{a}_n$ is true because if we multiply a polynomial of degree $n-1$ by X, we obtain a polynomial of degree n with the same highest coefficient.
The ascending ideal chain $\mathfrak{a}_0 \subseteq \mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \ldots$ becomes stationary because R is Noetherian, say $\mathfrak{a}_d = \mathfrak{a}_{d+i}$ for all $i \in \mathbb{N}$. Moreover, since R is Noetherian, all the $\mathfrak{a}_i$ are finitely generated (as ideals of R) by Proposition 7.3, say, $\mathfrak{a}_i = (a_{i,1}, \ldots, a_{i,m_i})$.
By construction, for each $a_{i,j}$ there is a polynomial $f_{i,j} \in \mathfrak{a}$ of degree i with highest coefficient $a_{i,j}$. Let $\mathfrak{b}$ be the ideal of $R[X]$ generated by the finitely many $f_{i,j} \in \mathfrak{a}$ for $0 \leq i \leq d$ and $1 \leq j \leq m_i$.
Claim: $\mathfrak{b} = \mathfrak{a}$.
Of course, $\mathfrak{b} \subseteq \mathfrak{a}$. We show by induction on e that any $f \in \mathfrak{a}$ of degree e lies in $\mathfrak{b}$. If $e = 0$, then $f \in \mathfrak{a}_0$, whence $f \in \mathfrak{b}$.
Next we treat $0 < e \leq d$. Suppose we already know that any polynomial in $\mathfrak{a}$ of degree at most $e-1$ lies in $\mathfrak{b}$. Let now $f \in \mathfrak{a}$ be of degree e. The highest coefficient a_e of f lies in $\mathfrak{a}_e$. This means

that $a_e = \sum_{j=1}^{m_e} r_j a_{e,j}$ for some $r_j \in R$. Now, the polynomial $g(X) = \sum_{j=1}^{m_e} r_j f_{e,j}$ has highest coefficient a_e and is of degree e. But, now $f - g$ is in $\mathfrak{a}$ and of degree at most $e-1$, whence it lies in $\mathfrak{b}$. We can thus conclude that f lies in $\mathfrak{b}$, as well.
Finally we deal with $d < e$. Just as before, suppose we already know that any polynomial in $\mathfrak{a}$ of degree at most $e-1$ lies in $\mathfrak{b}$ and let again $f \in \mathfrak{a}$ be of degree e. The highest coefficient a_e of f lies in $\mathfrak{a}_e = \mathfrak{a}_d$ and, hence, there are r_j for $j = 1, \ldots, m_d$ such that $a_e = \sum_{j=1}^{m_d} r_j a_{d,j}$. Consequently, the polynomial $g(X) = \sum_{j=1}^{m_d} r_j f_{d,j}$ has highest coefficient a_e and is of degree d. But, now $f(X) - g(X)X^{e-d}$ is in $\mathfrak{a}$ and of degree at most $e-1$, whence it lies in $\mathfrak{b}$. We can thus conclude that f lies in $\mathfrak{b}$, as well, finishing the proof of the claim and the Proposition. □

Proposition 7.7. *Let R be a Noetherian ring and $D \subseteq R$ be a multiplicatively closed subset with $1 \in D$. Then $D^{-1}R$ is also a Noetherian ring.*

Proof. Exercise. □

8 Krull dimension in integral ring extensions

Aims:

- Learn and master the concept of Krull dimension;
- know the going up theorem for prime ideals in integral extensions;
- know that the Krull dimension is invariant under integral ring extensions;
- know examples (in particular, that of rings of integers in number fields and coordinate rings of curves) and standard theorems;
- be able to prove simple properties.

This section has two main corollaries:

- The ring of integers of a number field has Krull dimension 1.
- The coordinate ring of a plane curve has Krull dimension 1 (fitting well with the intuitive concept that a curve is a 'geometric object of dimension 1').

Definition 8.1. *Let R be a ring. A* chain of prime ideals of length n in R *is*

$$\mathfrak{p}_n \subsetneq \mathfrak{p}_{n-1} \subsetneq \mathfrak{p}_{n-2} \subsetneq \cdots \subsetneq \mathfrak{p}_1 \subsetneq \mathfrak{p}_0,$$

where $\mathfrak{p}_i \lhd R$ is a prime ideal for all $i = 0, \ldots, n$.
The height $h(\mathfrak{p})$ of a prime ideal $\mathfrak{p} \lhd R$ *is the supremum of the lengths of all prime ideal chains with $\mathfrak{p}_0 = \mathfrak{p}$.*
The Krull dimension $\dim(R)$ of the ring R *is the supremum of the heights of all prime ideals of R.*

Example 8.2. *(a) The Krull dimension of $\mathbb{Z}$ is* 1.

Reason: Recall that the prime ideals of $\mathbb{Z}$ are (0) (height 0) and (p) for a prime p, which is also maximal. So, the longest prime ideal chain is $(0) \subsetneq (p)$.

(b) The Krull dimension of any field is 0.

Reason: (0) *is the only ideal, hence, also the only prime ideal.*

(c) Let K *be a field. The polynomial ring* $K[X_1, \ldots, X_n]$ *has Krull dimension* n*. This needs a non-trivial proof! See below.*

Primes in integral extensions

In the sequel, we are going to consider ring extensions $R \subseteq S$. If we denote $\iota : R \to S$ the inclusion and $\mathfrak{b} \lhd S$ an ideal, then $\iota^{-1}(\mathfrak{b}) = \mathfrak{b} \cap R$ (in the obvious sense). In particular, if $\mathfrak{b}$ is a prime ideal, then so is $\iota^{-1}(\mathfrak{b}) = \mathfrak{b} \cap R$ (see Exercise).

Lemma 8.3. *Let* $R \subseteq S$ *be a ring extension such that* S *is integral over* R*. Let* $\mathfrak{b} \lhd S$ *be an ideal and* $\mathfrak{a} := \mathfrak{b} \cap R \lhd R$*.*

(a) Then $R/\mathfrak{a} \hookrightarrow S/\mathfrak{b}$ *is an integral ring extension (note that this is injective because of the isomorphism theorem).*

(b) Assume that $\mathfrak{b}$ *is a prime ideal. Then* $\mathfrak{a}$ *is maximal* $\Leftrightarrow$ $\mathfrak{b}$ *is maximal.*

(c) Assume in addition that S *is an integral domain. Then:* R *is a field* $\Leftrightarrow$ S *is a field.*

Proof. Exercise. □

Lemma 8.4. *Let* $R \subseteq S$ *be an integral ring extension.*

(a) Let $\mathfrak{b} \lhd S$ *be an ideal containing* $x \in \mathfrak{b}$ *which is not a zero-divisor. Then* $\mathfrak{b} \cap R =: \mathfrak{a} \lhd R$ *is not the zero ideal.*

(b) Let $\mathfrak{P}_1 \subsetneq \mathfrak{P}_2$ *be a chain of prime ideals of* S*. Then* $\mathfrak{p}_1 := \mathfrak{P}_1 \cap R \subsetneq \mathfrak{P}_2 \cap R =: \mathfrak{p}_2$ *is a chain of prime ideals of* R*.*

Proof. (a) Since S is integral over R, there are $n \in \mathbb{N}$ and $r_0, \ldots, r_{n-1} \in R$ such that

$$0 = x^n + \sum_{i=0}^{n-1} r_i x^i.$$

We assume that n is minimal with this property. This implies $r_0 \neq 0$ as otherwise we could write

$$0 = x \cdot \big(x^{n-1} + \sum_{i=1}^{n-1} r_i x^{i-1}\big)$$

and, from the fact that x is not a zero-divisor, conclude $x^{n-1} + \sum_{i=1}^{n-1} r_i x^{i-1} = 0$, leading to a contradiction. Thus, rewriting gives

$$0 \neq r_0 = -x \cdot \big(x^{n-1} + \sum_{i=1}^{n-1} r_i x^{i-1}\big) \in R \cap \mathfrak{b} = \mathfrak{a}.$$

(b) Consider the integral (see Lemma 8.3) ring extension $R/\mathfrak{p}_1 \hookrightarrow S/\mathfrak{P}_1$. The ideal $\mathfrak{P}_2/\mathfrak{P}_1$ in $S/\mathfrak{P}_1$ is prime because $(S/\mathfrak{P}_1)/(\mathfrak{P}_2/\mathfrak{P}_1) \cong S/\mathfrak{P}_2$ (isomorphism theorem) is an integral domain. This also means that $\mathfrak{P}_2/\mathfrak{P}_1$ consists of non-zero divisors only (except for 0). Consequently, by (a), we have $(0) \neq \big(\mathfrak{P}_2/\mathfrak{P}_1\big) \cap \big(R/\mathfrak{p}_1\big) \cong \mathfrak{p}_2/\mathfrak{p}_1$. □

Lemma 8.5. *Let $R \subseteq S$ be an integral ring extension and let $T \subseteq R$ be a multiplicatively closed subset containing 1. Then $T^{-1}R \subseteq T^{-1}S$ is an integral ring extension.*

Proof. Exercise. □

Lemma 8.6. *Let $R \subseteq S$ be an integral ring extension and let $\mathfrak{p} \lhd R$ be a prime ideal. Then there is a prime ideal $\mathfrak{P} \lhd S$ lying over $\mathfrak{p}$, by which we mean $\mathfrak{p} = \mathfrak{P} \cap R$.*

Proof. Let $T := R \setminus \mathfrak{p}$ so that $R_\mathfrak{p} = T^{-1}R$ is the localisation of R at $\mathfrak{p}$. By Lemma 8.5, $R_\mathfrak{p} \hookrightarrow T^{-1}S$ is an integral ring extension. Let $\mathfrak{m}$ be a maximal ideal of $T^{-1}S$.
Consider the commutative diagram:

$$\begin{array}{ccc} R & \xhookrightarrow{\text{integral}} & S \\ \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} \\ R_\mathfrak{p} & \xhookrightarrow{\text{integral}} & T^{-1}S. \end{array}$$

Put $\mathfrak{P} := \beta^{-1}(\mathfrak{m})$. It is a prime ideal. Note that $\mathfrak{m} \cap R_\mathfrak{p}$ is maximal by Lemma 8.3, hence, $\mathfrak{m} \cap R_\mathfrak{p} = \mathfrak{p}R_\mathfrak{p}$ is the unique maximal ideal of the local ring $R_\mathfrak{p}$. Consequently, we have due to the commutativity of the diagram:

$$\mathfrak{p} = \alpha^{-1}(\mathfrak{p}R_\mathfrak{p}) = \alpha^{-1}(\mathfrak{m} \cap R_\mathfrak{p}) = R \cap \beta^{-1}(\mathfrak{m}) = R \cap \mathfrak{P},$$

showing that $\mathfrak{P}$ satisfies the requirements. □

Proposition 8.7 (Going up)**.** *Let $R \subseteq S$ be an integral ring extension. For prime ideals $\mathfrak{p}_1 \subsetneq \mathfrak{p}_2$ in R and a prime ideal $\mathfrak{P}_1 \lhd S$ lying over $\mathfrak{p}_1$ (i.e. $\mathfrak{P}_1 \cap R = \mathfrak{p}_1$), there is a prime ideal $\mathfrak{P}_2$ in S lying over $\mathfrak{p}_2$ (i.e. $\mathfrak{P}_2 \cap R = \mathfrak{p}_2$) such that $\mathfrak{P}_1 \subsetneq \mathfrak{P}_2$.*

Proof. By Lemma 8.3, $R/\mathfrak{p}_1 \hookrightarrow S/\mathfrak{P}_1$ is an integral ring extension. By Lemma 8.6, there is $\overline{\mathfrak{P}}_2 \lhd S/\mathfrak{P}_1$ lying over $\overline{\mathfrak{p}}_2 := \mathfrak{p}_2/\mathfrak{p}_1$ such that $\overline{\mathfrak{P}}_2 \cap R/\mathfrak{p}_1 = \mathfrak{p}_2/\mathfrak{p}_1$. Define $\mathfrak{P}_2$ as $\pi_S^{-1}(\overline{\mathfrak{P}_2})$ for $\pi_S : S \to S/\mathfrak{P}_1$ the natural projection. Clearly, $\mathfrak{P}_2 \supseteq \mathfrak{P}_1$ (as $\mathfrak{P}_1$ is in the preimage, being the preimage of the 0 class). By the commutativity of the diagram

$$\begin{array}{ccc} R & \xhookrightarrow{\text{integral}} & S \\ \downarrow{\scriptstyle \pi_R} & & \downarrow{\scriptstyle \pi_S} \\ R/\mathfrak{p}_1 & \xhookrightarrow{\text{integral}} & S/\mathfrak{P}_1, \end{array}$$

we have

$$\mathfrak{P}_2 \cap R = \pi_S^{-1}(\overline{\mathfrak{P}_2}) \cap R = \pi_R^{-1}(\overline{\mathfrak{P}_2} \cap R/\mathfrak{p}_1) = \pi_R^{-1}(\mathfrak{p}_2/\mathfrak{p}_1) = \mathfrak{p}_2.$$

This also implies $\mathfrak{P}_2 \neq \mathfrak{P}_1$. □

Corollary 8.8. *Let $R \subseteq S$ be an integral ring extension. Then the Krull dimension of R equals the Krull dimension of S.*

Proof. We first note that the Krull dimension of R is at least the Krull dimension of S. Reason: If $\mathfrak{P}_n \subsetneq \mathfrak{P}_{n-1} \subsetneq \cdots \subsetneq \mathfrak{P}_0$ is an ideal chain in S, then $\mathfrak{P}_n \cap R \subsetneq \mathfrak{P}_{n-1} \cap R \subsetneq \cdots \subsetneq \mathfrak{P}_0 \cap R$ is an ideal chain in R by Lemma 8.4.
Now we show that the Krull dimension of S is at least that of R. Let $\mathfrak{p}_n \subsetneq \mathfrak{p}_{n-1} \subsetneq \cdots \subsetneq \mathfrak{p}_0$ be an ideal chain in R and let $\mathfrak{P}_n$ be any prime ideal of S lying over $\mathfrak{p}_n$, which exists by Lemma 8.6. Then Proposition 8.7 allows us to obtain an ideal chain $\mathfrak{P}_n \subsetneq \mathfrak{P}_{n-1} \subsetneq \cdots \subsetneq \mathfrak{P}_0$ such that $\mathfrak{P}_i \cap R = \mathfrak{p}_i$ for $i = 0, \ldots, n$, implying the desired inequality. □

Corollary 8.9. *Let R be an integral domain of Krull dimension 1 and let L be a finite extension of $K := \operatorname{Frac} R$. Then the integral closure of R in L has Krull dimension 1.*
In particular, rings of integers of number fields have Krull dimension 1.

Proof. The integral closure of R in L is an integral ring extension of R. By Corollary 8.8, the Krull dimension of S is the same as that of R, whence it is 1. □

Krull dimension of the coordinate ring of a curve

Our next aim is to compute the Krull dimension of $K[X_1, \ldots, X_n]$ for some field K. First we need Nagata's Normalisation Lemma, which will be an essential step in the proof of Noether's Normalisation Theorem and of the computation of the Krull dimension of $K[X_1, \ldots, X_n]$.

Proposition 8.10 (Nagata)**.** *Let K be a field and $f \in K[X_1, \ldots, X_n]$ be a non-constant polynomial. Then there are $m_2, m_3, \ldots, m_n \in \mathbb{N}$ such that the ring extension $R := K[f, z_2, z_3, \ldots, z_n] \subseteq K[X_1, \ldots, X_n] =: S$ with $z_i := X_i - X_1^{m_i} \in K[X_1, \ldots, X_n]$ is integral.*

Proof. The proof works like the proof of Lemma 4.15 (a), except that now the number of variables is abitrary but finite.
First note: $S = R[X_1]$. Reason: The inclusion $\supseteq$ is trivial. For $n \geq i > 1$, we have $X_i = z_i + X_1^{m_i} \in R[X_1]$, proving the inclusion $\subseteq$.
It suffices to show that X_1 is integral over R. The main step is to construct a monic polynomial $h \in R[T]$ such that $h(X_1) = 0$. We take the following general approach: For any $m_i \in \mathbb{N}$ for $i = 2, 3, \ldots, n$ the polynomial

$$h(T) := f(T, z_2 + T^{m_2}, z_3 + T^{m_3}, \ldots, z_n + T^{m_n}) - f(X_1, \ldots, X_n) \in R[T]$$

obviously has X_1 as a zero. But, in order to prove the integrality of X_1 we need the highest coefficient of h to be in $R^\times = K[X_1, \ldots, X_n]^\times = K^\times$, so that we can divide by it, making h monic. We will achieve this by making a 'good' choice of the m_i, as follows.
Let d be the total degree of f in the following sense:

$$f(X_1, \ldots, X_n) = \sum_{(i_1, \ldots, i_n) \text{ s.t. } |i| \leq d} a_{(i_1, \ldots, i_n)} X_1^{i_1} \cdots X_n^{i_n}$$

with one of the $a_{(i_1,\dots,i_n)} \neq 0$ for $|i| := \sum_{j=1}^n i_j = d$. Now we compute (letting $m_1 = 1$)

$$\begin{aligned} &h(T) \\ &= \Big(\sum_{(i_1,\dots,i_n) \text{ s.t. } |i| \leq d} a_{(i_1,\dots,i_n)} T^{i_1} (z_2 + T^{m_2})^{i_2} (z_3 + T^{m_3})^{i_3} \dots (z_n + T^{m_n})^{i_n} \Big) - f(X_1, \dots, X_n) \\ &\qquad = \sum_{(i_1,\dots,i_n) \text{ s.t. } |i| \leq d} a_{(i_1,\dots,i_n)} T^{\sum_{j=1}^n i_j m_j} + \text{ terms of lower degree in } T. \end{aligned}$$

Now choose $m_j = (d+1)^{j-1}$. Then the $\sum_{j=1}^n i_j m_j = \sum_{j=1}^n i_j (d+1)^{j-1}$ are distinct for all choices of $0 \leq i_j \leq d$ (consider it as the $(d+1)$-adic expansion of an integer). In particular, among these numbers there is a maximal one with $0 \neq a_{(i_1,\dots,i_n)}$. Then this is the highest coefficient of h and it lies in $K^\times$, as needed. □

Definition 8.11. *Let K be a field. A finitely generated K-algebra is also called an* affine K-algebra. *Any such is of the form $K[X_1, \dots, X_n]/I$ with $n \in \mathbb{N}$ and $I \trianglelefteq K[X_1, \dots, X_n]$ and ideal.*

Proposition 8.12 (Noether's Normalisation Theorem)**.** *Let K be a field and R an affine K-algebra which is an integral domain and which can be generated by n elements (as K-algebra). Then there is $r \in \mathbb{N}$, $r \leq n$ and there are elements $y_1, \dots, y_r \in R$ such that*

(1) $R/K[y_1, \dots, y_r]$ is an integral ring extension and

(2) $y_1, \dots, y_r$ are K-algebraically independent (by definition, this means that $K[y_1, \dots, y_r]$ is isomorphic to the polynomial ring in r variables).

The subring $K[y_1, \dots, y_r]$ of R is called a Noether normalisation of R.

Proof. By induction on $n \in \mathbb{N}$ we shall prove: Every affine K-algebra that can be generated by n elements satisfies the conclusion of the proposition.
Start with $n = 0$. Then $R = K$ and the result is trivially true. Assume now that the result is proved up to $n - 1$. We show it for n. Let $x_1, \dots, x_n \in R$ be a set of generators of R as K-algebra. So, we have the surjection of K-algebras:

$$\varphi : K[X_1, \dots, X_n] \twoheadrightarrow R, \quad X_i \mapsto x_i.$$

Its kernel is a prime ideal $\mathfrak{p} := \ker(\varphi)$ since R is an integral domain.
We distinguish two cases. Assume first $\mathfrak{p} = (0)$. Then R is isomorphic to $K[X_1, \dots, X_n]$ and the result is trivially true. Now we put ourselves in the second case $\mathfrak{p} \neq (0)$. Let $f \in \mathfrak{p}$ be a non-constant polynomial. We apply Nagata's Normalisation Lemma 8.10 and obtain elements $z_2, \dots, z_n \in K[X_1, \dots, X_n]$ such that $K[X_1, \dots, X_n]/K[f, z_2, \dots, z_n]$ is an integral ring extension. Now, apply φ to this extension and obtain the integral ring extension $R/\varphi(K[f, z_2, \dots, z_n])$, i.e. the integral ring extension R/R' with $R' := K[\varphi(z_2), \dots, \varphi(z_n)]$. Now, R' is generated by $n - 1$ elements, hence, it is an integral extension of $K[y_1, \dots, y_r]$ with $r \leq n - 1$ algebraically independent elements $y_1, \dots, y_r \in R' \subseteq R$. As integrality is transitive, R is integral over $K[y_1, \dots, y_r]$, proving the proposition. □

Note that by Corollary 8.8 one obtains that the Krull dimension of R is equal to r in view of the following proposition.

Proposition 8.13. *Let K be a field. The Krull dimension of $K[X_1, \ldots, X_n]$ is equal to n.*

Proof. We apply induction on n to prove the Proposition. If $n = 0$, then the Krull dimension is 0 being the Krull dimension of a field. Let us assume that we have already proved that the Krull dimension of $K[X_1, \ldots, X_{n-1}]$ is $n - 1$.
Let now m be the Krull dimension of $K[X_1, \ldots, X_n]$. We first prove $m \geq n$. The reason simply is that we can write down a chain of prime ideals of length n, namely:

$$(0) \subsetneq (X_1) \subsetneq (X_1, X_2) \subsetneq (X_1, X_2, X_3) \subsetneq \cdots \subsetneq (X_1, X_2, \ldots, X_n).$$

Now let

$$(0) \subsetneq \mathfrak{P}_1 \subsetneq \mathfrak{P}_2 \subsetneq \mathfrak{P}_3 \subsetneq \cdots \subsetneq \mathfrak{P}_m$$

be a chain of prime ideals of $K[X_1, \ldots, X_n]$. We pick any non-constant $f \in \mathfrak{P}_1$ and apply Nagata's Normalisation Lemma 8.10, which yields elements $z_2, \ldots, z_n \in K[X_1, \ldots, X_n]$ such that $R \subseteq K[X_1, \ldots, X_n]$ with $R := K[f, z_2, \ldots, z_n]$ is an integral ring extension. Setting $\mathfrak{p}_i := R \cap \mathfrak{P}_i$ we obtain by Lemma 8.4 the chain of prime ideals of R of length m:

$$(0) \subsetneq \mathfrak{p}_1 \subsetneq \mathfrak{p}_2 \subsetneq \mathfrak{p}_3 \subsetneq \cdots \subsetneq \mathfrak{p}_m.$$

Let $\overline{R} := K[f, z_2, \ldots, z_n]/\mathfrak{p}_1$. Note that this is an integral domain, which can be generated (as a K-algebra) by $n - 1$ elements, namely, the classes of $z_2, \ldots, z_n$. Let $\pi : R = K[f, z_2, \ldots, z_n] \to K[f, z_2, \ldots, z_n]/\mathfrak{p}_1 = \overline{R}$ be the natural projection. We apply it to the prime ideal chain of the $\mathfrak{p}_i$ and get:

$$(0) = \mathfrak{p}_1/\mathfrak{p}_1 \subsetneq \mathfrak{p}_2/\mathfrak{p}_1 \subsetneq \mathfrak{p}_3/\mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_m/\mathfrak{p}_1,$$

which is a prime ideal chain of $\overline{R}$ of length $m - 1$. By Noether's Normalisation Theorem 8.12 it follows that the Krull dimension of $\overline{R}$ is at most $n - 1$, yielding the other inequality $m \leq n$ and finishing the proof. □

Corollary 8.14. *Let K be a field and $f(X, Y) \in K[X, Y]$ be a non-constant polynomial. Let $C = \mathcal{V}_{(f)}(K)$ be the resulting plane curve.*
Then the Krull dimension of the coordinate ring $K[C] = K[X, Y]/\mathcal{I}_C$ is equal to 1.

Proof. This is now immediate by Lemma 4.15. □

We include an easy lemma on Krull dimensions, which enables us to give another proof of Proposition 4.14.

Lemma 8.15. *Let $\varphi : R \twoheadrightarrow S$ be a surjective ring homomorphism.*

(a) The Krull dimension of S is less than or equal to the Krull dimension of R.

(b) If R is an integral domain and the Krull dimensions of R and S are equal and finite, then φ is an isomorphism.

Proof. (a) φ^{-1} of a prime ideal is a prime ideal. Moreover, if $\varphi^{-1}(\mathfrak{a}) = \varphi^{-1}(\mathfrak{b})$, then $\varphi(\varphi^{-1}(\mathfrak{a})) = \varphi(\varphi^{-1}(\mathfrak{b}))$, hence, $\mathfrak{a} = \mathfrak{b}$ using here the surjectivity of φ. This shows that the inverse image of any prime ideal chain is a prime ideal chain of the same length.
(b) Since R is an integral domain, any prime ideal chain of maximal length starts with the prime ideal (0). Let $\mathfrak{a}$ be the kernel of φ. It is contained in any $\varphi^{-1}(\mathfrak{p})$. Hence, if φ is non-zero, the pull-back of any chain of prime ideals of S can be prolonged by starting it with (0), showing that the Krull dimension of R is strictly larger than that of S. □

Second proof of Proposition 4.14. (This proof is shorter, but depends on Krull dimensions.) The Krull dimensions of $K[X,Y]/(f)$ and $K[C] = K[X,Y]/\mathcal{I}_C$ are both equal to 1 due to Lemma 4.15. As f is irreducible, (f) is prime and $K[X,Y]/(f)$ is an integral domain. Consequently, the natural projection $K[X,Y]/(f) \twoheadrightarrow K[X,Y]/\mathcal{I}_C$ is an isomorphism by Lemma 8.15 (b). Thus $(f) = \mathcal{I}_C$. □

9 Dedekind rings

Aims:

- Learn and master the concept of regular local rings;
- learn and master the concept of Dedekind rings;
- learn and master the local characterisation of Dedekind rings;
- learn and master the characterisation of smoothness of a curve in terms of Dedekind rings;
- know examples and standard theorems;
- be able to prove simple properties.

Lemma 9.1. *Let R be an integral domain with field of fractions K and $D \subseteq R$ a multiplicatively closed subset containing* 1.

(a) If R is integrally closed, then $D^{-1}R$ is integrally closed.

(b) Let $\widetilde{R}$ be the integral closure of R in K and let $\widetilde{D^{-1}R}$ be the integral closure of $D^{-1}R$ in K. Then $D^{-1}\widetilde{R} = \widetilde{D^{-1}R}$.

Proof. (a) Note that K is also the field of fractions of $D^{-1}R$. Let $\frac{a}{b} \in K$ be integral over $D^{-1}R$. Then (after choosing a common demoninator of the coefficients) there is an equation of the form:

$$0 = \big(\frac{a}{b}\big)^n + \frac{c_{n-1}}{d}\big(\frac{a}{b}\big)^{n-1} + \frac{c_{n-2}}{d}\big(\frac{a}{b}\big)^{n-2} + \cdots + \frac{c_1}{d}\frac{a}{b} + \frac{c_0}{d}$$

with $c_0, c_1, \ldots, c_{n-1} \in R$ and $d \in D$. Multiplying by d^n we obtain:

$$0 = \big(\frac{ad}{b}\big)^n + c_{n-1}\big(\frac{ad}{b}\big)^{n-1} + c_{n-2}d\big(\frac{ad}{b}\big)^{n-2} + \cdots + c_1 d^{n-2}\frac{ad}{b} + c_0 d^{n-1},$$

showing that $\frac{da}{b}$ is integral over R. As R is integrally closed, it follows that $\frac{da}{b}$ is in R, whence $\frac{a}{b} \in D^{-1}R$.
(b) By (a), $D^{-1}\widetilde{R}$ is integrally closed. As $\widetilde{R}/R$ is an integral ring extension, by Lemma 8.5 it follows that $D^{-1}\widetilde{R}/D^{-1}R$ is an integral ring extension. This shows that $D^{-1}\widetilde{R}$ is the integral closure of $D^{-1}R$. □

Now we can prove the local characterisation of integrally closed integral domains.

Proposition 9.2. *Let R be an integral domain. Then the following statements are equivalent:*

(i) R is integrally closed.

(ii) $R_\mathfrak{p}$ is integrally closed for all prime ideals $\mathfrak{p} \lhd R$.

(iii) $R_\mathfrak{m}$ is integrally closed for all maximal ideals $\mathfrak{m} \lhd R$.

Proof. '(i) ⇒ (ii)': Lemma 9.1.
'(ii) ⇒ (iii)': Trivial because every maximal ideal is prime.
'(iii) ⇒ (i)': Let us denote by $\widetilde{R}$ the integral closure of R. By Lemma 9.1, we know that the localisation $\widetilde{R}_\mathfrak{m}$ of $\widetilde{R}$ at $\mathfrak{m}$ is the integral closure of $R_\mathfrak{m}$.
Let $\iota : R \hookrightarrow \tilde{R}$ be the natural embedding. Of course, R is integrally closed if and only if ι is an isomorphism. By Proposition 6.21 this is the case if and only if the localisation $\iota_\mathfrak{m} : R_\mathfrak{m} \hookrightarrow \tilde{R}_\mathfrak{m}$ is an isomorphism for all maximal ideals $\mathfrak{m}$. That is, however, the case by assumption and the previous discussion. □

Lemma 9.3. *Let R be a Noetherian local ring and $\mathfrak{m} \lhd R$ its maximal ideal.*

(a) $\mathfrak{m}^n/\mathfrak{m}^{n+1}$ is an $R/\mathfrak{m}$-vector space for the natural operation.

(b) $\dim_{R/\mathfrak{m}}(\mathfrak{m}/\mathfrak{m}^2)$ is the minimal number of generators of the ideal $\mathfrak{m}$.

(c) If $\dim_{R/\mathfrak{m}}(\mathfrak{m}/\mathfrak{m}^2) = 1$, then $\mathfrak{m}$ is a principal ideal and there are no ideals $\mathfrak{a} \lhd R$ such that $\mathfrak{m}^{n+1} \subsetneq \mathfrak{a} \subsetneq \mathfrak{m}^n$ for any $n \in \mathbb{N}$.

Proof. Exercise. □

Definition 9.4. *A Noetherian local ring with maximal ideal $\mathfrak{m}$ is called* regular *if $\dim_{R/\mathfrak{m}}(\mathfrak{m}/\mathfrak{m}^2)$ equals the Krull dimension of R.*

Proposition 9.5. *Let R be a regular local ring of Krull dimension 1.*

(a) There is $x \in R$ such that all non-zero ideals are of the form (x^n) for some $n \in \mathbb{N}$.

(b) Every non-zero $r \in R$ can be uniquely written as ux^n with $u \in R^\times$ and $n \in \mathbb{N}$.

(c) R is a principal ideal domain (in particular, it is an integral domain).

Proof. By Lemma 9.3 we know that $\mathfrak{m}$ is a principal ideal. Let x be a generator, i.e. $(x) = \mathfrak{m}$. As a preparation, we first consider $M := \bigcap_{n\in\mathbb{N}} \mathfrak{m}^n = \bigcap_{n\in\mathbb{N}}(x^n)$. As an ideal in a Noetherian ring, it is finitely generated. We obviously have $\mathfrak{m}M = M$, whence by Nakayama's Lemma (Proposition 6.14) $M = 0$.
Now we show (b) and let $0 \neq r \in R$. As $R = (x^0) \supset (x) \supset (x^2) \supset (x^3) \supset \cdots$ and because of the preparation, there is a maximal n such that $r \in (x^n)$. So, we can write $r = vx^n$ for some $v \in R$. As R is a local ring, we have $R = R^\times \cup \mathfrak{m} = R^\times \cup (x)$. Consequently, $v \in R^\times$ because otherwise $r \in (x^{n+1})$, contradicting the maximality of n.
Let $0 \neq \mathfrak{a} \lhd R$ be any non-zero ideal. Let $u_i x^{n_i}$ (with $u_i \in R^\times$ and $i = 1, \ldots, s$) be generators of the ideal. Put $n := \min_i n_i$. Then $\mathfrak{a} = (x^n)$ because all other generators are multiples of $u_j x^{n_j}$, where j is such that $n_j = n$.
None of the ideals $\mathfrak{m}^n$ for $n \geq 2$ is a prime ideal (consider $x \cdot x^{n-1}$). As the Krull dimension is 1, it follows that (0) is a (hence, the) minimal prime ideal, showing that R is an integral domain. □

Our next aim is to prove that regular local rings of Krull dimension 1 are precisely the local principal ideal domains and also the local integrally closed integral domains.
The following lemma is proved very similarly to Nakayama's Lemma. It is essentially a ring version of the characteristic polynomial known from linear algebra.

Lemma 9.6. *Let R be a ring, $\mathfrak{a} \lhd R$ an ideal and M a finitely generated R-module. Let $\varphi : M \to M$ be an R-homomorphism such that the image $\varphi(M)$ is contained in $\mathfrak{a}M$.*
Then there are $n \in \mathbb{N}$ and $a_0, a_1, \ldots, a_{n-1} \in \mathfrak{a}$ such that

$$\varphi^n + a_{n-1}\varphi^{n-1} + a_{n-2}\varphi^{n-2} + \cdots + a_2\varphi^2 + a_1\varphi + a_0\mathrm{id}$$

is the zero-endomorphism on M.

Proof. Let $x_1, \ldots, x_n$ be generators of M as R-module. By assumption there are $a_{i,j} \in \mathfrak{a}$ for $1 \leq i, j \leq n$ such that

$$\varphi(x_i) = \sum_{j=1}^{n} a_{i,j} x_j.$$

Consider the matrix

$$D(T) := T \cdot \mathrm{id}_{n\times n} - (a_{i,j})_{1\leq i,j\leq n} \in \mathrm{Mat}_n(R[T]).$$

Note that $D(T)$ is made precisely in such a way that

$$D(\varphi)\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \left(\begin{pmatrix} \varphi & 0 & \cdots & 0 \\ 0 & \varphi & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \varphi \end{pmatrix} - \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n,1} & a_{n,2} & \cdots & a_{n,n} \end{pmatrix}\right)\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} \varphi(x_1) \\ \varphi(x_2) \\ \vdots \\ \varphi(x_n) \end{pmatrix} - \begin{pmatrix} \varphi(x_1) \\ \varphi(x_2) \\ \vdots \\ \varphi(x_n) \end{pmatrix} = 0.$$

If we multiply with the adjoint matrix $D(T)^*$, we obtain $D(T)^*D(T) = \det(D(T))\mathrm{id}_{n\times n}$. This yields

$$0 = \det(D(\varphi))\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = D(\varphi)^*D(\varphi)\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}.$$

Consequently, $\det(D(\varphi))$ is zero on all generators. We are done because the determinant $\det(D(\varphi))$ is of the desired form. □

Lemma 9.7. *Let R be a local Noetherian integral domain of Krull dimension 1 with maximal ideal $\mathfrak{m}$. Let $(0) \subsetneq I \lhd R$ be an ideal. Then there is $n \in \mathbb{N}$ such that $\mathfrak{m}^n \subseteq I$.*

Proof. Let Σ be the set of all ideals $I \lhd R$ such that $\mathfrak{m}^n \not\subseteq I$ for all $n \in \mathbb{N}$. This set is non-empty as $(0) \in \Sigma$. So, it contains a maximal element J as R is Noetherian. Assume $J \neq (0)$. Note that J is not prime since it is neither (0) nor equal to $\mathfrak{m}$. Hence, J contains a product xy with $x, y \in R$ without containing x and y individually. Due to the maximality of J among the elements of Σ, the ideals (J, x) and (J, y) do not lie in Σ. Consequently, there are $m, n \in \mathbb{Z}_{\geq 0}$ such that $\mathfrak{m}^n \subseteq (J, x)$ and $\mathfrak{m}^m \subseteq (J, y)$. We conclude

$$\mathfrak{m}^{m+n} \subseteq (J, x)(J, y) \subseteq J,$$

a contradiction. □

Proposition 9.8. *Let R be a local Noetherian ring of Krull dimension 1. Then the following statements are equivalent:*

(i) R is an integrally closed integral domain.

(ii) R is regular.

(iii) R is a principal ideal domain.

Proof. '(ii) ⇒ (iii)': This was proved in Proposition 9.5.
'(iii) ⇒ (i)': Principal ideal domains are UFDs (Proposition 1.13) and UFDs are integrally closed (Proposition 3.32).
'(i) ⇒ (ii)': It suffices to show that $\mathfrak{m}$ is a principal ideal because this means that $\dim_{R/\mathfrak{m}}(\mathfrak{m}/\mathfrak{m}^2) = 1$, which is the Krull dimension of R, so that R is regular by definition.
We now construct an element x such that $\mathfrak{m} = (x)$. To that aim, we start with any $0 \neq a \in \mathfrak{m}$. By Lemma 9.7 there is $n \in \mathbb{N}$ such that $\mathfrak{m}^n \subseteq (a)$ and $\mathfrak{m}^{n-1} \not\subseteq (a)$. Take any $b \in \mathfrak{m}^{n-1} \setminus (a)$. Put $x = \frac{a}{b} \in K$, where K is the field of fractions of R.
We show that $\mathfrak{m} = (x)$, as follows:

- $x^{-1}\mathfrak{m} \subseteq R$ ideal, i.e. $\frac{m}{x} \in R$ for all $m \in \mathfrak{m}$ because $\frac{m}{x} = \frac{mb}{a}$ and $mb \in \mathfrak{m}\mathfrak{m}^{n-1} = \mathfrak{m}^n \subseteq (a)$.
- $x^{-1} \notin R$ because otherwise $r = x^{-1} = \frac{b}{a} \in R$ would imply $b = ra \in (a)$.
- $x^{-1}\mathfrak{m} \not\subseteq \mathfrak{m}$ because of the following: Assume the contrary, i.e. $x^{-1}\mathfrak{m} \subseteq \mathfrak{m}$. Then we have the R-homomorphism $\varphi : \mathfrak{m} \xrightarrow{m \mapsto mx^{-1}} \mathfrak{m}$. As $\mathfrak{m}$ is finitely generated (because R is Noetherian), there are $a_0, a_1, \ldots, a_{n-1} \in R$ such that

  $$\varphi^n + a_{n-1}\varphi^{n-1} + a_{n-2}\varphi^{n-2} + \ldots a_1\varphi + a_0\mathrm{id}$$

  is the zero-endomorphism on $\mathfrak{m}$ by Lemma 9.6 (with $\mathfrak{a} = R$). This means that

  $$0 = \big(x^{-n} + a_{n-1}x^{-(n-1)} + a_{n-2}x^{-(n-2)} + \ldots a_1x^{-1} + a_0\big)\mathfrak{m}.$$

  As R is an integral domain and $\mathfrak{m} \neq 0$ because the Krull dimension is not 0, we obtain

  $$0 = x^{-n} + a_{n-1}x^{-(n-1)} + a_{n-2}x^{-(n-2)} + \ldots a_1x^{-1} + a_0,$$

  showing that x^{-1} is integral over R. As R is integrally closed, we obtain further $x^{-1} \in R$, which we excluded before.

So, $x^{-1}\mathfrak{m}$ is an ideal of R which is not contained in $\mathfrak{m}$. Thus, $x^{-1}\mathfrak{m} = R$, whence $\mathfrak{m} = Rx = (x)$, as was to be shown. □

Definition 9.9. *A Noetherian integrally closed integral domain of Krull dimension* 1 *is called a* Dedekind ring.

Example 9.10. *Let $K/\mathbb{Q}$ be a number field and $\mathbb{Z}_K$ its ring of integers. We have proved that $\mathbb{Z}_K$ is an integrally closed integral domain and that its Krull dimension is* 1. *So, $\mathbb{Z}_K$ is a Dedekind ring because it is also Noetherian (this is not so difficult, but needs some terminology that we have not introduced; we will show this in the beginning of the lecture on Algebraic Number Theory).*
In a lecture on Algebraic Number Theory (e.g. next term) one sees that Dedekind rings have the property that every non-zero ideal is a product of prime ideals in a unique way. This replaces the unique factorisation in prime elements, which holds in a factorial ring, but, fails to hold more generally, as we have seen.
Below we shall provide further examples of Dedekind rings coming from geometry.

We can now conclude from our previous work the following local characterisation of Dedekind rings.

Proposition 9.11. *Let R be a Noetherian integral domain of Krull dimension* 1. *Then the following assertions are equivalent:*

(i) *R is a Dedekind ring.*

(ii) *R is integrally closed.*

(iii) *$R_\mathfrak{m}$ is integrally closed for all maximal ideals $\mathfrak{m} \lhd R$.*

(iv) *$R_\mathfrak{m}$ is regular for all maximal ideals $\mathfrak{m} \lhd R$.*

(v) *$R_\mathfrak{m}$ is a principal ideal domain for all maximal ideals $\mathfrak{m} \lhd R$.*

Proof. All statements have been proved earlier! But, note that the Krull dimension of $R_\mathfrak{m}$ is 1 for all maximal ideals $\mathfrak{m}$. That is due to the fact that any non-zero prime ideal in an integral domain of Krull dimension 1 is maximal and that $\mathfrak{m}R_\mathfrak{m}$ is also maximal and non-zero. □

Let us now see what this means for plane curves. Let $f(X,Y) \in K[X,Y]$ and $a, b \in K$ such that $f(a,b) = 0$. Recall the Taylor expansion:

$$T_{C,(a,b)}(X,Y) = \\ \frac{\partial f}{\partial X}|_{(a,b)}(X-a) + \frac{\partial f}{\partial Y}|_{(a,b)}(Y-b) + \text{ terms of higher degree in } (X-a) \text{ and } (Y-b).$$

Definition 9.12. *Let K be a field, $f \in K[X,Y]$ a non-constant irreducible polynomial and $C = \mathcal{V}_{(f)}(K)$ the associated plane curve.*
Let $(a,b) \in C$ be a point. The tangent equation to C at (a,b) *is defined as*

$$T_{C,(a,b)}(X,Y) = \frac{\partial f}{\partial X}|_{(a,b)}(X-a) + \frac{\partial f}{\partial Y}|_{(a,b)}(Y-b) \in K[X,Y].$$

If $T_{C,(a,b)}(X,Y)$ is the zero polynomial, then we call (a,b) a singular point of C.
If (a,b) is non-singular (also called: smooth*), then $\mathcal{V}_{T_{C,(a,b)}}(K)$ is a line (instead of $\mathbb{A}^2(K)$), called the* tangent line to C at (a,b).
A curve all of whose points are non-singular is called non-singular (or smooth).

Example 9.13. *(a) Let $f(X,Y) = Y^2 - X^3 \in K[X,Y]$ with K a field (say, of characteristic 0).*

We have $\frac{\partial f}{\partial X} = -3X^2$ and $\frac{\partial f}{\partial X} = 2Y$. Hence, $(0,0)$ is a singularity and it is the only one. (Draw a sketch.)

This kind of singularity is called a cusp *(Spitze/pointe) for obvious reasons. The tangents to the two branches coincide at the cusp.*

(b) Let $f(X,Y) = Y^2 - X^3 - X^2 \in K[X,Y]$ with K a field (say, of characteristic 0).

We have $\frac{\partial f}{\partial X} = -3X^2 - 2X$ and $\frac{\partial f}{\partial X} = 2Y$. Hence, $(0,0)$ is a singularity and it is the only one. (Draw a sketch.)

This kind of singularity is called an ordinary double point. *The tangents to the two branches are distinct at the ordinary double point.*

We now state our main theorem about coordinate rings of plane curves. It again relates a geometric statement (smoothness of a curve) and an algebraic statement (coordinate ring is Dedekind).

Theorem 9.14. *Let K be an algebraically closed field, $f \in K[X,Y]$ a non-constant irreducible polynomial, $C = \mathcal{V}_{(f)}(K)$ the associated plane curve and $K[C] = K[X,Y]/(f(X,Y))$ the coordinate ring.*
Then the following two statements are equivalent:

(i) The curve C is smooth.

(ii) $K[C]$ is a Dedekind ring.

In order to prove the theorem, we first prove the following lemma, which also relates a geometric property (a point on a curve is nonsingular) and an algebraic property (the localisation of the coordinate ring is regular).

Lemma 9.15. *Let K be an algebraically closed field, $f \in K[X,Y]$ a non-constant irreducible polynomial, $C = \mathcal{V}_{(f)}(K)$ the associated plane curve and $K[C] = K[X,Y]/(f(X,Y))$ the coordinate ring. Let $(a,b) \in C$ be a point and $\mathfrak{m} = (X - a + (f), Y - b + (f)) \lhd K[C]$ be the corresponding maximal ideal (see Lemma 4.11).*
Then the following two statements are equivalent:

(i) The point (a,b) is non-singular.

(ii) $K[C]_{\mathfrak{m}}$ is a regular local ring of Krull dimension 1, i.e. $\mathfrak{m}/\mathfrak{m}^2$ can be generated by one element.

In order to derive Theorem 9.14 it suffices to prove that all maximal ideals are of the form used in the lemma. This will be proved from a field theoretic version of Hilbert's Nullstellensatz after the proof of the lemma.

Proof. After a linear variable transformation we may assume $(a, b) = (0, 0)$. Then

$$f(X, Y) = \alpha X + \beta Y + \text{ higher terms.}$$

Note that $\mathfrak{m}^2$ is generated by $X^2 + (f), Y^2 + (f), XY + (f)$, so that the $K = K[C]/\mathfrak{m}$-vector space $\mathfrak{m}/\mathfrak{m}^2$ is generated by $X + (f)$ and $Y + (f)$. Hence, the minimal number of generators is at most 2, but could be 1. Note that we are using the isomorphisms $K[C]_\mathfrak{m}/(\mathfrak{m}K[C]_\mathfrak{m}) \cong K[C]/\mathfrak{m}$ and $(\mathfrak{m}K[C]_\mathfrak{m}/(\mathfrak{m}K[C]_\mathfrak{m})^2 \cong \mathfrak{m}/\mathfrak{m}^2$ from Lemma 6.19 (b).
Note also that $K[C]$ has Krull dimension 1 and is an integral domain because f is irreducible (see Corollary 8.14). As $\mathfrak{m}$ is not the zero ideal, also the localisation $K[C]_\mathfrak{m}$ has Krull dimension 1.
'(i) $\Rightarrow$ (ii)': We assume that $(0, 0)$ is not a singular point. Then $\alpha \neq 0$ or $\beta \neq 0$. After possibly exchanging X and Y we may, without loss of generality, assume $\alpha \neq 0$. It follows:

$$X + (f) = \frac{1}{\alpha}\big(- \beta Y - \text{ higher terms} + (f)\big) \equiv -\frac{\beta}{\alpha} Y + (f) \pmod{\mathfrak{m}^2}.$$

So, $Y + (f)$ generates $\mathfrak{m}/\mathfrak{m}^2$ as K-vector space, whence the dimension of this space is 1, which is equal to the Krull dimension. This shows that $K[C]_\mathfrak{m}$ is regular.
'(ii) $\Rightarrow$ (i)': We now assume that $(0, 0)$ is a singular point. Then $\alpha = \beta = 0$. So, $X + (f)$ and $Y + (f)$ are K-linearly independent in $\mathfrak{m}/\mathfrak{m}^2$, whence the K-dimension of $\mathfrak{m}/\mathfrak{m}^2$ is bigger than the Krull dimension, showing that $K[C]_\mathfrak{m}$ is not regular. □

Proposition 9.16 (Field theoretic weak Nullstellensatz)**.** *Let K be a field, L/K a field extension and $a_1, \ldots, a_n \in L$ elements such that $L = K[a_1, \ldots, a_n]$ (that is, the K-algebra homomorphism $K[X_1, \ldots, X_n] \xrightarrow{X_i \mapsto a_i} L$ is surjective).*
Then L/K is finite and algebraic.

Proof. Let $L = K[a_1, \ldots, a_n]$. It is an affine K-algebra which is a field (and hence an integral domain). So, we may apply Noether normalisation Proposition 8.12. We obtain elements $y_1, \ldots, y_r \in L$ such that $L/K[y_1, \ldots, y_r]$ is an integral extension and $K[y_1, \ldots, y_r]$ is isomorphic to a polynomial ring in r variables. This means, in particular, that there are no relations between the y_i.
Assume $r \geq 1$. Then $y_1^{-1} \in L$ and hence integral over $K[y_1, \ldots, y_r]$, so that it satisfies a monic equation of the form

$$y_1^{-n} + f_{n-1}(y_1, \ldots, y_r) y_1^{-n+1} + \cdots + f_0(y_1, \ldots, y_r) = 0,$$

where $f_i(y_1, \ldots, y_r) \in K[y_1, \ldots, y_r]$. Multiplying through with y^n we get

$$1 + f_{n-1}(y_1, \ldots, y_r) y_1 + \cdots + f_0(y_1, \ldots, y_r) y_1^n = 0,$$

i.e. a non-trivial relation between the y_i. Conclusion: $r = 0$.
Hence, L/K is integral and hence algebraic. It is a finite field extension because it is generated by finitely many algebraic elements. □

We can now determine the maximal ideals of the coordinate ring of any affine algebraic set over an algebraically closed field.

Corollary 9.17. *Let K be an algebraically closed field and $\mathfrak{a} \lhd K[X_1, \ldots, X_n]$ a proper ideal.*

(a) The maximal ideals $\mathfrak{m} \lhd K[X_1, \ldots, X_n]$ *are precisely* $(X_1 - a_1, \ldots, X_n - a_n)$ *for* $(a_1, \ldots, a_n) \in K^n$.

(b) The maximal ideals $\mathfrak{m} \lhd K[X_1, \ldots, X_n]$ *which contain* $\mathfrak{a}$ *are* $(X_1 - a_1, \ldots, X_n - a_n)$ *for* $(a_1, \ldots, a_n) \in \mathcal{V}_{\mathfrak{a}}(K)$.

(c) The maximal ideals of $K[X_1, \ldots, X_n]/\mathfrak{a}$ *are* $(X_1 - a_1 + \mathfrak{a}, \ldots, X_n - a_n + \mathfrak{a})$ *for* $(a_1, \ldots, a_n) \in \mathcal{V}_{\mathfrak{a}}(K)$.

Proof. (a) We first determine what maximal ideals look like in general. Any ideal of the form $(X_1 - a_1, \ldots, X_n - a_n)$ is clearly maximal (factoring it out gives K). Conversely, if $\mathfrak{m} \lhd K[X_1, \ldots, X_n]$ is maximal then the quotient $K[X_1, \ldots, X_n]/\mathfrak{m}$ is a finite algebraic field extension of K by Proposition 9.16, hence, equal to K because K is algebraically closed. Consequently, denoting $a_i := \pi(X_i)$ for $i = 1, \ldots, n$ with $\pi : K[X_1, \ldots, X_n] \xrightarrow{\text{natural projection}} K[X_1, \ldots, X_n]/\mathfrak{m} \cong K$, we find (special case of Lemma 4.11) that $\mathfrak{m} = (X_1 - a_1, \ldots, X_n - a_n)$.
(b) Let $\mathfrak{m} = (X_1 - a_1, \ldots, X_n - a_n)$, so that $\{(a_1, \ldots, a_n)\} = \mathcal{V}_{\mathfrak{m}}(K)$. We have:

$$\mathfrak{a} \subseteq \mathfrak{m} \Leftrightarrow \{(a_1, \ldots, a_n)\} = \mathcal{V}_{\mathfrak{m}}(K) \subseteq \mathcal{V}_{\mathfrak{a}}(K) \Leftrightarrow (a_1, \ldots, a_n) \in \mathcal{V}_{\mathfrak{a}}(K).$$

The direction $\Rightarrow$ is trivial. To see the other one, note that $f(a_1, \ldots, a_n) = 0$ for $f \in \mathfrak{a}$ implies $f \in \mathfrak{m}$, as $\mathfrak{m}$ is the kernel of $K[X_1, \ldots, X_n] \xrightarrow{X_i \mapsto a_i} K$.
(c) The maximal ideals of $K[X, Y]/\mathfrak{a}$ are precisely the maximal ideals of $K[X, Y]$ containing $\mathfrak{a}$. Thus, (b) implies the assertion. □

Proof of Theorem 9.14. By Corollary 9.17 the maximal ideals $\mathfrak{m}$ of $K[C]$ are precisely the $(X - a + (f), Y - b + (f))$ for $(a, b) \in C(K)$.
By Proposition 9.11 we have $K[C]$ is a Dedekind ring if and only if $K[C]_{\mathfrak{m}}$ is a regular ring for all maximal ideals $\mathfrak{m} \lhd K[C]$; that is the case if and only if all points (a, b) of C are smooth (by Lemma 9.15). □

10 Hilbert's Nullstellensatz

Aims:

- Learn and master the various forms of Hilbert's Nullstellensatz;
- learn and master the resulting correspondence between affine algebraic sets and radical ideals;
- know examples and standard theorems;
- be able to prove simple properties.

Proposition 10.1 (Hilbert's Nullstellensatz – weak form)**.** *Let* K *be an algebraically closed field and* $\mathfrak{a} \lhd K[X_1, \ldots, X_n]$ *be a proper ideal. Then* $\mathcal{V}_{\mathfrak{a}}(K) \neq \emptyset$.

Proof. Let $\mathfrak{m} \lhd K[X_1, \ldots, X_n]$ be a maximal ideal containing $\mathfrak{a}$. By Corollary 9.17 (b), $\mathfrak{m}$ corresponds to a point $(a_1, \ldots, a_n) \in \mathcal{V}_{\mathfrak{a}}(K)$, showing the non-emptyness of this set. □

Remark 10.2. *In fact the assertion of Proposition 10.1 is equivalent to that of Proposition 9.16, in the sense that the latter can also be deduced from the former, as follows:*
Consider a K-algebra surjection $\phi : K[X_1, \dots, X_n] \xrightarrow{X_i \mapsto a_i} L$. Its kernel $\mathfrak{m} := \ker(\phi)$ is a maximal ideal, since L is a field. By Proposition 10.1, we have $\mathcal{V}_{\mathfrak{m}}(\overline{K}) \neq \emptyset$. Let $(b_1, \dots, b_n)$ be an element of $\mathcal{V}_{\mathfrak{m}}(\overline{K})$, which gives rise to the K-algebra homomorphism $\psi : K[X_1, \dots, X_n] \xrightarrow{X_i \mapsto b_i} \overline{K}$. Note that $\mathfrak{m}$ is contained in the kernel of ψ (we have $f(b_1, \dots, b_n) = 0$ for all $f \in \mathfrak{m}$), whence they are equal. Consequently, $K \subseteq L \subseteq \overline{K}$, and we conclude that L/K is algebraic. It is finite because it is generated by finitely many algebraic elements.

Definition 10.3. *Let R be a ring and $\mathfrak{a} \lhd R$ and ideal. The* radical (ideal) of $\mathfrak{a}$ *is defined as*

$$\sqrt{\mathfrak{a}} := \{r \in R \mid \exists n \in \mathbb{N} : r^n \in \mathfrak{a}\}.$$

An ideal $\mathfrak{a}$ is called a radical ideal *if $\mathfrak{a} = \sqrt{\mathfrak{a}}$.*
The Jacobson radical of $\mathfrak{a}$ *is defined as*

$$J(\mathfrak{a}) = \bigcap_{\mathfrak{a} \subseteq \mathfrak{m} \lhd R \text{ maximal}} \mathfrak{m},$$

i.e. the intersection of all maximal ideals of R containing $\mathfrak{a}$ (recall the definition of the Jacobson radical of a ring: intersection of all maximal ideals; it is equal to $J(0)$).

Lemma 10.4. *Let K be a field and $\mathfrak{a} \lhd K[X_1, \dots, X_n]$ an ideal.*
Then $\mathcal{V}_{\mathfrak{a}}(L) = \mathcal{V}_{\sqrt{\mathfrak{a}}}(L)$ for all field extensions L/K.

Proof. The inclusion $\supseteq$ is trivial because of $\mathfrak{a} \subseteq \sqrt{\mathfrak{a}}$. Let now $(a_1, \dots, a_n) \in \mathcal{V}_{\mathfrak{a}}(L)$, that is, $f(a_1, \dots, a_n) = 0$ for all $f \in \mathfrak{a}$. Let now $g \in \sqrt{\mathfrak{a}}$. Then there is $m \in \mathbb{N}$ such that $g^m \in \mathfrak{a}$, so that $g(a_1, \dots, a_n)^m = 0$. Since we are in an integral domain, this implies $g(a_1, \dots, a_n) = 0$, showing the inclusion $\subseteq$. □

Proposition 10.5 (General Hilbert's Nullstellensatz)**.** *Let K be a field, R an affine K-algebra, $\mathfrak{a} \lhd R$ an ideal. Then $\sqrt{\mathfrak{a}} = J(\mathfrak{a})$.*

Proof. '$\subseteq$': Let $\mathfrak{m} \lhd R$ be any maximal ideal containing $\mathfrak{a}$. Let $f \in \sqrt{\mathfrak{a}}$. Then there is $m \in \mathbb{N}$ such that $f^m \in \mathfrak{a} \subseteq \mathfrak{m}$. The prime ideal property of $\mathfrak{m}$ now gives that $f \in \mathfrak{m}$. This implies $\sqrt{\mathfrak{a}} \subseteq \mathfrak{m}$.
'$\supseteq$': Let $f \in R \setminus \sqrt{\mathfrak{a}}$. We want to show $f \notin J(\mathfrak{a})$.
From $f \notin \sqrt{\mathfrak{a}}$ it follows that $f^n \notin \mathfrak{a}$ for all $n \in \mathbb{N}$. So, the set $T = \{\overline{f}^n \mid n \in \mathbb{N}\} \subseteq R/\mathfrak{a} =: \overline{R}$ is multiplicatively closed and does not contain 0 (the zero of $\overline{R} = R/\mathfrak{a}$, of course). We write $\overline{f}$ for the class $f + \mathfrak{a} \in \overline{R}$. It is a unit in $T^{-1}\overline{R}$ because we are allowing $\overline{f}$ in the denominator.
Let $\overline{\mathfrak{q}}$ be a maximal ideal of $T^{-1}\overline{R}$. As $\overline{f}$ is a unit, $\overline{f} \notin \overline{\mathfrak{q}}$. As R is an affine K-algebra, so is the field $T^{-1}\overline{R}/\overline{\mathfrak{q}} =: L$ (we modded out by a maximal ideal). Proposition 9.16 yields that L/K is a finite field extension.
Note that the ring $\overline{R}/(\overline{R} \cap \overline{\mathfrak{q}})$ contains K and lies in L. Due to the finiteness of L/K, this ring is itself a field, so that $\overline{R} \cap \overline{\mathfrak{q}}$ is a maximal ideal of $\overline{R}$.
Recall that $\overline{f} \notin \overline{\mathfrak{q}}$, so f does not lie in the maximal ideal $\overline{R} \cap \overline{\mathfrak{q}}$.
Set $\mathfrak{q} := \pi^{-1}(\overline{\mathfrak{q}})$ with the natural projection $\pi : R \twoheadrightarrow \overline{R} = R/\mathfrak{a}$. It is a maximal ideal containing $\mathfrak{a}$, but $f \notin \mathfrak{q}$. Consequently, $f \notin J(\mathfrak{a})$. □

Theorem 10.6 (Hilbert's Nullstellensatz)**.** *Let K be an algebraically closed field and consider an ideal $\mathfrak{a} \trianglelefteq K[X_1, \ldots, X_n]$.*
Then $\mathcal{I}_{\mathcal{V}_\mathfrak{a}(K)} = \sqrt{\mathfrak{a}}$.
In particular, the radical ideals of $K[X_1, \ldots, X_n]$ are in bijection with the affine algebraic sets in $\mathbb{A}^n(K)$. More precisely, the maps

$$\begin{aligned} \{\mathfrak{a} \trianglelefteq K[X_1, \ldots, X_n] \mid \mathfrak{a} = \sqrt{\mathfrak{a}}\} &\leftrightarrows \{\mathcal{V} \subseteq \mathbb{A}^n(K) \mid \mathcal{V} \text{ affine algebraic set}\} \\ \mathfrak{a} &\overset{\Phi}{\mapsto} \mathcal{V}_\mathfrak{a}(K) \\ \mathcal{I}_\mathcal{V} &\underset{\Psi}{\leftarrow\!\shortmid} \mathcal{V} \end{aligned}$$

are inverses to each other and thus bijections.

Proof. '$\supseteq$': By Lemmata 4.13 and 10.4 we have $\sqrt{\mathfrak{a}} \subseteq \mathcal{I}_{\mathcal{V}_{\sqrt{\mathfrak{a}}}(K)} = \mathcal{I}_{\mathcal{V}_\mathfrak{a}(K)}$.
'$\subseteq$': Let $\mathfrak{m}$ be a maximal ideal of $K[X_1, \ldots, X_n]$ containing $\mathfrak{a}$. By Corollary 9.17 we know $\mathfrak{m} = (X_1 - a_1, \ldots, X_n - a_n)$ for some $(a_1, \ldots, a_n) \in \mathcal{V}_\mathfrak{a}(K)$. We have

$$\mathcal{I}_{\mathcal{V}_\mathfrak{a}(K)} \subseteq \mathcal{I}_{\mathcal{V}_\mathfrak{m}(K)} = \{f \in K[X_1, \ldots, X_n] \mid f(\underline{a}) = 0\} = \mathfrak{m}.$$

Consequently, $\mathcal{I}_{\mathcal{V}_\mathfrak{a}(K)} \subseteq J(\mathfrak{a}) = \sqrt{\mathfrak{a}}$, using Proposition 10.5.
The final statement follows like this:

$$\mathcal{X} = \mathcal{V}_\mathfrak{a}(K) \mapsto \mathcal{I}_{\mathcal{V}_\mathfrak{a}(K)} = \sqrt{\mathfrak{a}} \mapsto \mathcal{V}_{\sqrt{\mathfrak{a}}}(K) = \mathcal{V}_\mathfrak{a}(K) = \mathcal{X}$$

and

$$\mathfrak{a} = \sqrt{\mathfrak{a}} \mapsto \mathcal{V}_\mathfrak{a}(K) \mapsto \mathcal{I}_{\mathcal{V}_\mathfrak{a}(K)} = \sqrt{\mathfrak{a}}.$$

This shows the correspondence. □

Finally let us prove that the vanishing ideal $\mathcal{I}_C$ of the curve defined by a non-constant irreducible $f \in K[X, Y]$ (over an algebraically closed field K) is (f) and hence the coordinate ring $K[C]$ is isomorphic to $K[X, Y]/(f)$.

Third proof of Proposition 4.14 for K algebraically closed. Recall that $K[X, Y]$ is a unique factorisation domain. Hence any irreducible element is a prime element. Thus, f is a prime element, and consequently (f) is a prime ideal, implying $\sqrt{(f)} = (f)$. Thus Hilbert's Nullstellensatz 10.6 yields $\mathcal{I}_C = \sqrt{(f)} = (f)$. □