# Commutative Algebra 

Gabor Wiese

gabor.wiese@uni.lu

University of Luxembourg
Version of 25th August 2022

## 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.
| Basic ring theory
14
1 Modules and ideals ..... 5
2 Integrality ..... 13
3 Affine plane curves ..... 24
|| Modules ..... 33
4 Direct sums, products, free modules and exact sequences ..... 33
5 Tensor products ..... 40
6 Localisation ..... 45
III Advanced ring theory ..... 53
7 Noetherian rings and Hilbert's Basissatz ..... 53
8 Krull dimension of rings ..... 56
9 Dedekind rings ..... 62
10 Hilbert's Nullstellensatz ..... 69
Appendix ..... 71
IV
Appendix ..... 73
11 Appendix: Background on rings ..... 73
12 Appendix: Background on fields ..... 80

## 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 kind of course is Commutative Ring Theory.

We see the lecture Commutative Algebra as a preparation for deeper study of Algebraic Number Theory and Algebraic Geometry or their combination Arithmetic Geometry. Those 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.

## 1 Modules and ideals

## Aims:

- Learn and master the concept of a module;
- know examples and standard theorems;
- be able to prove simple properties;
- recognise that ideals are special cases of submodules;
- understand the special roles of prime and maximal ideals and their relation to irreducible and prime elements in integral domains.


## Modules as generalisations of vector spaces

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 1.1 Let $R$ be a ring. An abelian group $(M,+, 0)$ together with a map

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

is called a (left) $R$-module if the following properties are satisfied:
(a) $1 \cdot x=x$ for all $x \in M$.
(b) $r .(x+y)=r \cdot x+r . y$ for all $r \in R$ and all $x, y \in M$.
(c) $(r+s) \cdot x=r \cdot x+s \cdot x$ 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 $x \in M$.

Example 1.2 (a) Let $K$ be a field. Any $K$-vector space is a $K$-module, and vice versa.
(b) Any ring $R$ is an $R$-module by multiplication. This rather trivial statement will allow us to see ideals as submodules below.
(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 .). We can think of the elements of $R^{n}$ also as column vectors, as one usually does in (basic) linear algebra. Later on, we shall sometimes adopt this convention when doing computations with matrices.

## Submodules and 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.

Definition 1.3 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: $I \triangleleft R$ (or $I \unlhd R$ ).
An ideal of the form $(a):=R . a:=\{r a \mid r \in R\}$ for some $a \in R$, i.e. the set of multiples of $a$, is called a principal ideal.

The notion of principal ideal captures the notion of divisibility, already treated early in school. 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 $s=r t$.

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

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

Examples:
$-\mathbb{Z}^{\times}=\{-1,1\}$.

- $K^{\times}=K \backslash\{0\}$ for any field $K$.
$-(\mathbb{Z} / n \mathbb{Z})^{\times}=\{a \bmod n \mid \operatorname{gcd}(a, n)=1\}$.
- $(\mathbb{Z} \times \mathbb{Z})^{\times}=\{(1,1),(1,-1),(-1,1),(-1,-1)\}$.
- Two elements $r, s \in R$ are associate if there is a unit $t \in R^{\times}$such that $r=t s$ (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 $r s=0$.

Examples:

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

Here is now the translation of divisibility to (principal) ideals: For $a, b \in R$ we have

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

and

$$
(a)=(b) \Leftrightarrow a \mid b \text { and } b \mid a .
$$

Next we generalise the notion of ideal, by introducing submodules, which are nothing else but vector subspaces for a ring.

Definition 1.5 Let $M$ be an $R$-module. A subset $N \subseteq M$ is called an $R$-submodule of $M$ if $0 \in N$ and + and . restrict to $N$ making it into an $R$-module, i.e. for all $n_{1}, n_{2} \in N$ and all $r \in R$ we have

$$
r . n_{1}+n_{2} \in N .
$$

Note that taking the $R$-module $M=R$ via multiplication, the $R$-submodules of $R$ are exactly the ideals of $R$.

## Generating and describing submodules and ideals

Definition 1.6 Let $M$ be an $R$-module and let $m_{i} \in M$ for $i \in I$ (some 'indexing' set). Denote by

$$
\left\langle m_{i} \mid i \in I\right\rangle:=\left\{\sum_{j \in J} r_{j} . m_{j} \mid J \subseteq I \underline{\text { finite }} \text { subset }, r_{j} \in R \text { for } j \in J\right\} .
$$

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

$$
\left\langle m_{i} \mid i \in I\right\rangle=\left\langle m_{1}, m_{2}, \ldots, m_{n}\right\rangle=\left\{\sum_{i=1}^{n} r_{i} . m_{i} \mid r_{1}, \ldots, r_{n} \in R\right\} .
$$

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 $\left\langle m_{1}, \ldots, m_{n}\right\rangle=M$.
Let $M_{i}$ for $i \in I$ be submodules. We write

$$
\sum_{i \in I} M_{i}:=\left\{\sum_{j \in J} m_{j} \mid J \subseteq I \text { finite subset }, m_{j} \in M_{j} \text { for } j \in J\right\} .
$$

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

$$
M_{1}+M_{2}+\cdots+M_{n}=\left\{\sum_{i=1}^{n} m_{i} \mid m_{1} \in M_{1}, m_{2} \in M_{2}, \ldots, m_{n} \in M_{n}\right\} .
$$

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 do not have the time to treat them.

Note that the intersection of submodules of a given module is again a submodule (however, the similar statement with the union is false). The $R$-submodule $\left\langle m_{i} \mid i \in I\right\rangle$ 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 $M_{i}$.

We now explicitly describe the special case of ideals; for that one, we also use bracket (.) instead of $\langle\cdot\rangle$. Let $a_{1}, \ldots, a_{n}$ be elements of $R$. The ideal generated by $a_{1}, \ldots, a_{n}$ (i.e. the $R$-submodule
of $R$ generated by $a_{1}, \ldots, a_{n}$ ) is

$$
\left(a_{1}, \ldots, a_{n}\right)=\left\langle a_{1}, \ldots, a_{n}\right\rangle=\left\{\sum_{i=1}^{n} r_{i} a_{i} \mid r_{1}, \ldots, r_{n} \in R\right\}
$$

Any such ideal is called finitely generated. As a particular instance, for $a \in R$ we find the principal ideal generated by a

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

More generally, if $S$ is an 'indexing' set and $\left\{a_{s}\right\}_{s \in S}$ are elements of $R$, then we also write $\left(a_{s} \mid s \in S\right)$ for $\left\langle a_{s} \mid s \in S\right\rangle$.

## Homomorphisms

We first recall the definition of a ring homomorphism.
Definition 1.7 Let $R, S$ be rings. A map $\varphi: R \rightarrow S$ 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 $r, s \in R$.

The notion of linear maps between modules is exactly the same as the notion of linear maps between vector spaces:

Definition 1.8 Let $R$ be a ring and $M, N$ be $R$-modules. A map $\varphi: M \rightarrow N$ is called an $R$-module homomorphism (or short: $R$-homomorphism, or: $R$-linear (map)) if

- $\varphi\left(m_{1}+m_{2}\right)=\varphi\left(m_{1}\right)+\varphi\left(m_{2}\right)$ 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 1.9 The kernel $\operatorname{ker}(\varphi):=\{m \in M \mid \varphi(m)=0\}$ is an $R$-submodule of $M$.
The image $\operatorname{im}(\varphi):=\{\varphi(m) \mid m \in M\}$ is an $R$-submodule of $N$.
By the way, the quotient (see below) $N / \operatorname{im}(\varphi)$ is called the cokernel of $\varphi$.
Proof. This works precisely as for vector spaces.
Since ideals are submodules, we conclude that the kernel of any ring homomorphism is an ideal. But, attention, the image of a ring homomorphism is not always an ideal: it is an $R$-submodule of the target ring, say $S$, and that is not the same as an ideal of $S$, in general; it is the same if the ring homomorphism is surjective.

Definition 1.10 Let $R$ be a ring and $N, M$ be $R$-modules. Let $\varphi: M \rightarrow N$ be an $R$-homomorphism. We say that $\varphi$ is a monomorphism if $\varphi$ is injective. It is called an epimorphism if $\varphi$ is surjective. Finally, it is called an isomorphism if it is bijective.
If $N=M$, then an $R$-homomorphism $\varphi: M \rightarrow M$ is also called an $R$-endomorphism.
We let $\operatorname{Hom}_{R}(M, N)($ or $\operatorname{Hom}(M, N)$ if $R$ is understood) be the set of all $R$-homomorphisms
$\varphi: M \rightarrow N$. If $M=N$, then one lets $\operatorname{End}_{R}(M):=\operatorname{Hom}_{R}(M, M)$.

Lemma 1.11 Let $R$ be a ring and $N, M$ be $R$-modules. Then $\operatorname{Hom}_{R}(M, N)$ 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 $f, g \in \operatorname{Hom}_{R}(M, N)$, all $m \in M$ and all $r \in R$.

Proof. Exercise.
(R)

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

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

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

$$
R \rightarrow \operatorname{End}(M), r \mapsto(x \mapsto r \cdot x)
$$

is a ring homomorphism. This can be checked as an exercise.

## Quotient modules and quotient rings

In a sense, the dual notion of a submodule is that of a quotient. We give the construction of quotient modules in a formal way. It is very useful to see it alongside the construction of the residue rings $\mathbb{Z} / n \mathbb{Z}$ for $n \in \mathbb{Z}$, i.e. to see it as a generalisation of modular arithmetic.

Proposition 1.12 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 $\bar{x}=x+N=\{x+n \mid n \in N\}$ form the $R$-module denoted $M / N$ with
$\cdot+: M / N \times M / N \rightarrow M / N,(x+N, y+N) \mapsto(x+N)+(y+N):=x+y+N$,

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

The $R$-module $M / N$ is called the quotient of $M$ by (or modulo) $N$ (also called factor module).
Proof. Exercise.
We now apply this proposition to the situation of an ideal $I$ of a ring $R$. This gives us an $R$-module structure on the quotient module $R / I$, and, in particular, a scalar multiplication

$$
.: R \times R / I \rightarrow R / I, \quad(r, s+I) \mapsto r s+I
$$

In this setting we can actually do better and observe that this formula only depends on the coset $r+I$, leading to a 'proper' product map

$$
\cdot: R / I \times R / I \rightarrow R / I, \quad(r+I, s+I) \mapsto(r+I) \cdot(s+I):=r s+I
$$

This makes $R / I$ into a ring with neutral element for multiplication $1+I$.
Example 1.13 (a) $\mathbb{C} \cong \mathbb{R}[X] /\left(X^{2}+1\right)$.
(b) $\mathbb{F}_{p}=\mathbb{Z} /(p)$ for $p$ a prime.
(c) $\mathbb{F}_{4}=\mathbb{F}_{2}[X] /\left(X^{2}+X+1\right)$. This is a field with 4 elements and will be studied explicitly in an exercise.

A major tool in many of our arguments in these lectures are the isomorphism theorems.
Proposition 1.14 - Isomorphism theorems for modules. Let $R$ be a ring.
(a) Let $M, N$ be $R$-modules and $\varphi: M \rightarrow N$ be an $R$-homomorphism. Then the map

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

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

$$
\left(M / N_{1}\right) /\left(N_{2} / N_{1}\right) \cong M / N_{2} .
$$

(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

$$
\left(N_{1}+N_{2}\right) / N_{1} \cong N_{2} /\left(N_{1} \cap N_{2}\right)
$$

Proof. Exercise.
The corresponding statement of (a) for rings also holds in the stronger form that the resulting map is actually a ring homomorphism, which means a little more than just saying that it is a linear map, namely, that products are preserved; that is checked very simply.

Proposition 1.15 Let $R, S$ be rings and $\varphi: R \rightarrow S$ be a ring homomorphism. Then the map

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

is well-defined and an isomorphism of rings.

## 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). 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. We first recall the general definition of irreducible and prime elements in integral domains, which both generalise the familiar notion of prime number in $\mathbb{Z}$.

Definition 1.16 Let $R$ be an integral domain.
(a) An element $r \in R \backslash\left(R^{\times} \cup\{0\}\right)$ is called irreducible if, whenever $r=s t$ with $s, t \in R$, then $s \in R^{\times}$or $t \in R^{\times}$.

Example: $n \in \mathbb{Z} \backslash\{-1,0,1\}$ is irreducible if and only if its only divisors are $1,-1, n,-n$; i.e., the integer $n$ is irreducible if it is $\pm 1$ a prime number (according to the 'school definition': it is $\geq 2$, and its only positive divisors are $1, n$ ).
(b) An element $r \in R \backslash\left(R^{\times} \cup\{0\}\right)$ is called a prime element if, whenever $r \mid$ st with $s, t \in R$,

```
then r|s or r|t.
```

Let $R$ be an integral domain and $r \in R \backslash\left(R^{\times} \cup\{0\}\right)$. One always has (see Proposition 11.3):

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

Definition 1.17 Let $R$ be a ring and $I \triangleleft R, I \neq R$ an ideal.
The ideal $I$ is called maximal if there is no ideal $J \triangleleft R$ such that $I \subsetneq J \subsetneq R$.
The ideal $I$ is called prime if, whenever $a b \in I$, then $a \in I$ or $b \in I$.
In any integral domain $R$, one has for $r \in R \backslash\left(\{0\} \cup R^{\times}\right)$:

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

If $R$ is a PID, then one also has (see Proposition 11.12):

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

Example 1.18 (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 1.19 Let $R$ be a ring and $I \triangleleft R, I \neq R$ 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 $(a+I)(b+I)=a b+I=$ $0+I=0$, i.e. $a b \in I$. 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 $a b \in I$. 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 $1=i+x r$. 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 $(x+I)(y+I)=x y+I=1+I \subseteq J$. So, $1 \in J$, whence $R \subseteq J$, showing that $J=R$, whence $I$ is maximal.

Here are some important consequences.

Corollary 1.20 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.
$(\mathrm{b}, \mathrm{c}) R /(0)=R$.
(d-f) trivial.
We later need the existence of maximal ideals.
Proposition 1.21 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 on page 75 .

Corollary 1.22 (a) Every ideal $\mathfrak{a} \subsetneq R$ is contained in some maximal ideal $\mathfrak{m}$ of $R$.
(b) Every non-unit $x \in R \backslash R^{\times}$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 1.21. 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).

## 2 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.

## Generation of subrings and subfields

## Definition 2.1

If $R$ is a subring of a ring $S$, then we say that $R \subseteq S$ is a ring extension.

If $K$ is a subfield of a field $L$, then we say that $K \subseteq L$ is a field extension. For the latter, the piece of notation $L / K$ is also commonly used.

As every field is a ring, a field extension is a special case of a ring extension, i.e. every field extension is also a ring extension. However, in the case of a field extension we have the tools of (usual) linear algebra at our disposal and we can prove stronger statements and/or give simpler proofs for field extensions than for ring extensions.
We now aim at constructing ring extensions, starting from a 'base ring' $R$ and adding elements to it.

Lemma 2.2 Let $R \subseteq S$ be a ring extension.
(a) Let $a \in S$. Then the evaluation map

$$
\mathrm{ev}_{a}: R[X] \rightarrow S, \quad \sum_{i=0}^{d} c_{i} X^{i} \mapsto \sum_{i=0}^{d} c_{i} a^{i}
$$

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

$$
\mathrm{ev}_{\left(a_{i}\right)_{i \in I}}: R\left[X_{i} \mid i \in I\right] \rightarrow S, \quad f\left(\left(X_{i}\right)_{i \in I}\right) \mapsto f\left(\left(a_{i}\right)_{i \in I}\right)
$$

is a ring homomorphism.

## Proof. Exercise.

Definition 2.3 Assume the set-up of Lemma 2.2.
(a) The image of $\mathrm{ev}_{a}$ is called the subring of $S$ generated by a over $R$ and denoted as $R[a]$. We thus have the ring extensions $R \subseteq R[a] \subseteq S$.
(b) The image of $\mathrm{ev}_{\left(a_{i}\right)_{i \in I}}$ is called the subring of $S$ generated by the $\left(a_{i}\right)_{i \in I}$ over $R$ and denoted as $R\left[\left(a_{i}\right)_{i \in I}\right]$. If $I=\{1,2,3, \ldots, n\}$ is a finite set, we also write $R\left[a_{1}, \ldots, a_{n}\right]$.

Note that $R[a]$ and $R\left[\left(a_{i}\right)_{i \in I}\right]$ 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 2.4 (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:

$$
\sum_{i=0}^{n} r_{i} \sqrt{2}^{i}=\sum_{i=0 \text { even }}^{n} r_{2} i^{i / 2}+\left(\sum_{i=1 \mathrm{odd}}^{n} r_{i} 2^{(i-1) / 2}\right) \sqrt{2}
$$

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 $\mathbb{Z}\left[\frac{1}{2}\right]$ 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 $\frac{a_{1}}{2^{2_{1}}}, \ldots, \frac{a_{n}}{2^{n}}$ and let $f$ be bigger than all $e_{1}, \ldots, e_{n}$. One can never express $\frac{1}{2^{\dagger}}$ 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 2.5 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 $K\left(a_{i} \mid i \in I\right)$ 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 2.6 Let $L / K$ be a field extension and $a \in L$. Then $\operatorname{Frac}(K[a])=K(a)$.
Proof. The inclusion $K[a] \subseteq K(a)$ implies $\operatorname{Frac}(K[a]) \subseteq K(a)$. As $K(a)$ is the intersection of all fields containing $K$ and $a$, one also has $K(a) \subseteq \operatorname{Frac}(K[a])$.

We now give examples analogous to the previous ones.
Example 2.7 (a) The subfield $\mathbb{Q}(2)$ of $\mathbb{C}$ is equal to $\mathbb{Q}$.
(b) The subfield $\mathbb{Q}(\sqrt{2})$ 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 $\frac{a}{a^{2}-2 b^{2}}-\frac{b}{a^{2}-2 b^{2}} \sqrt{2}$. 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 $\mathbb{Q}\left[\frac{1}{2}\right]$ of $\mathbb{Q}$ is equal to $\mathbb{Q}$.

## Algebraic and integral elements

Let $R \subseteq S$ be a ring extension and let $a \in S$. We are now going to study $R[a]$. We know that it is generated, as $R$-module, by the elements

$$
1=a^{0}, a, a^{2}, a^{3}, a^{4}, \ldots
$$

When is $R[a]$ generated, as $R$-module, by $1=a^{0}, a, a^{2}, \ldots, a^{n-1}$ for some $n \in \mathbb{Z}_{\geq 1}$ ?
Suppose this is the case. Then we can express $a^{n}$ as an $R$-linear combination of lower powers of $a$ :

$$
a^{n}=r_{0}+r_{1} a+r_{2} a^{2}+\cdots+r_{n-1} a^{n-1} \text { with } r_{0}, \ldots, r_{n-1} \in R .
$$

Setting $c_{i}=-r_{i}$ for $i=0, \ldots, n-1$, this can be rewritten as

$$
0=c_{0}+c_{1} a+c_{2} a^{2}+\cdots+c_{n-1} a^{n-1}+a^{n}=f(a)
$$

for the monic polynomial $f(X)=c_{0}+c_{1} X+c_{2} X^{2}+\cdots+c_{n-1} X^{n-1}+X^{n} \in R[X]$. We have thus produced a monic polynomial with coefficients in $R$ that annihilates $a$.
Conversely, suppose we have such a monic polynomial satisfying $f(a)=0$. Then $a^{n}$ can be written as an $R$-linear combination of $1=a^{0}, a, a^{2}, \ldots, a^{n-1}$. Even better: we can iterate this inductively and conclude that $a^{m}$ can be written as an $R$-linear combination of $1=a^{0}, a, a^{2}, \ldots, a^{n-1}$ for any integer $m \geq n$.
Our conclusion of this short discussion is the following proposition.

Proposition 2.8 The ring $R[a]$ can be generated by $1=a^{0}, a, a^{2}, \ldots, a^{n-1}$ as an $R$-module if and only if there exists a monic polynomial $f \in R[X]$ of degree $n$ such that $f(a)=0$.

We turn this important property into a definition.

## Definition 2.9

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

Let $L / K$ be a field extension.
An element $a \in L$ is called algebraic over $K$ if there exists a monic polynomial $f \in K[X]$ such that $f(a)=0$. If $a \in L$ is not algebraic over $K$, we say that it is transcendental over $K$.

Note that algebraic and integral are relative notions: an element is algebraic or integral over some field/ring. Note also that 'algebraic' is just another word for 'integral' in the case of a field extension $L / K$ because any field extension can be viewed as a ring extension.
Example 2.10 (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) $\pi$ is algebraic over $\mathbb{R}$ (special case of (a)).
(d) $i=\sqrt{-1}$ is algebraic over $\mathbb{Q}$.
(e) $\pi$ 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.
(f) Let $L / K$ be a field extension and $a \in L$. Then the evaluation map $\mathrm{ev}_{a}: K[X] \rightarrow L$ given by $f \mapsto f(a)$ (see Lemma 2.2) is injective if and only if $a$ is transcendental over $K$.

Indeed, if $a$ is algebraic over $K$, then there is a monic polynomial $f \in K[X]$ such that $f(a)=0$. This just means that $f$ is in the kernel of the evaluation map, so $\mathrm{ev}_{a}$ is not injective. Conversely, if $\mathrm{ev}_{a}$ is not injective, then there is some non-zero polynomial $f$ in the kernel of the evaluation map, which we may assume to be monic after division by the leading coefficient. That, however, just means $f(a)=0$, whence $a$ is algebraic over $K$.

Example 2.11 (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.

In the case of a field extension $L / K$, the tools of (usual) linear algebra and the fact that the polynomial ring $K[X]$ is a principal ideal domain (Attention: in general, $R[X]$ does not have this nice property! Even $\mathbb{Z}[X]$ does not.) allow us establish the existence of a unique minimal polynomial annihilating a given $a \in L$ that is algebraic over $K$; this further shows that $K[a]$ equals $K(a)$ and we obtain that the degree of the field extension $K(a) / K$ equals the degree of the minimal polynomial. The situation is a lot more complicated for general ring extensions, which are not field extensions.

Proposition 2.12 Let $L / K$ be a field extension and let $a \in L$ be algebraic over $K$.
(a) If $a$ is algebraic over $K$, then there is a unique monic polynomial $m_{a} \in K[X]$ such that $\operatorname{ker}\left(\mathrm{ev}_{a}\right)=\left(m_{a}\right)$, where $\left(m_{a}\right)$ is the principal ideal of $K[X]$ consisting of all the multiples of $m_{a}$. In particular, any $f \in K[X]$ such that $f(a)=0$ is a multiple of $m_{a}$.

The polynomial $m_{a}$ is called the minimal polynomial of a over $K$.
(b) 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.
(c) Let $a$ be algebraic over $K$. Then the induced map

$$
\mathrm{ev}_{a}: K[X] /\left(m_{a}\right) \rightarrow L, f+\left(m_{a}\right) \mapsto f(a)
$$

is an injective field homomorphism and identifies $K[X] /\left(m_{a}\right)$ with $K[a]$ and $K(a)$.
(d) 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) We know that $K[X]$ is a principal ideal domain. Hence, the kernel of $\mathrm{ev}_{a}$ is a principal ideal, so, it is generated by one element $f$. As $\mathrm{ev}_{a}$ 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 $K \backslash\{0\}$. 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.
(b) Let $f \in K[X]$ be a nonzero polynomial such that $f(a)=0$. Then $f \in \operatorname{ker}\left(\mathrm{ev}_{a}\right)=\left(m_{a}\right)$, 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 $m_{a}=f g$ 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 $m_{a}$.
(c) Since $m_{a}$ is irreducible, $K[X] /\left(m_{a}\right)$ is a field. The injectivity follows from the isomorphism theorem for rings Proposition 1.15. Since $K[a]$ is a field, $K[a]=\operatorname{Frac}(K[a])=K(a)$ by Lemma 2.6.
(d) We first notice that $1, a, a^{2}, \ldots, a^{d-1}$ are $K$-linearly independent because any non-zero $K$-linear combination of these elements would lead to an annihilating polynomial of $a$ with coefficients in $K$ of degree at most $d-1$, which does not exist. We already know from Proposition 2.8 that $1, a, \ldots, a^{d-1}$ generate $K[a]$ as a $K$-vector space. Consequently, these elements form a $K$-basis of $K[a]$.
Example 2.13 We make a minor change with respect to Example 2.11(c) and take $a:=\frac{1+\sqrt{-5}}{2} \in$ $\mathbb{C}$. This element is not integral over $\mathbb{Z}$ because the minimal polynomial of $a$ over $\mathbb{Q}$ equals $f=X^{2}-X+\frac{5}{2}$. If there were a monic polynomial $h \in \mathbb{Z}[X]$ annihilating $a$, then we would have $h=f g$ 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.

## Algebraic field extensions and integral ring extensions

## Definition 2.14

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

A field extension $L / K$ is called algebraic if every $a \in L$ is algebraic over $K$.
If the extension $L / K$ is not algebraic, it is called transcendental.

Again, as every field is a ring, any algebraic field extension can be viewed as an integral ring extension. We now characterise these notions by finiteness properties. For this, we need to apply some more general tools from linear algebra working over rings: 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 2.15 - Cramer's rule. Let $R$ be a ring and $M=\left(m_{i, j}\right)_{1 \leq i, j \leq n}$ be an $n \times n$-matrix with entries in $R$. The adjoined matrix is defined as $M^{*}=\left(m_{i, j}^{*}\right)_{1 \leq i, j \leq n}$ with entries

$$
m_{i, j}^{*}:=(-1)^{i+j} \operatorname{det}\left(M_{i, j}\right)
$$

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:

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

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

Proposition 2.16 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): This follows from Proposition 2.8.
(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 $\left\{t_{1}, \ldots, t_{n}\right\}$, 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, $a t_{i}$ can be written as

$$
a t_{i}=\sum_{j=1}^{n} d_{i, j} t_{j} \text { with } d_{i, j} \in R
$$

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

$$
M\left(\begin{array}{c}
t_{1} \\
t_{2} \\
\vdots \\
t_{n}
\end{array}\right)=\left(\left(\begin{array}{cccc}
a & 0 & \cdots & 0 \\
0 & a & \cdots & 0 \\
\vdots & \vdots & \ddots & \vdots \\
0 & 0 & \cdots & a
\end{array}\right)-\left(\begin{array}{cccc}
d_{1,1} & d_{1,2} & \cdots & d_{1, n} \\
d_{2,1} & d_{2,2} & \cdots & d_{2, n} \\
\vdots & \vdots & \ddots & \vdots \\
d_{n, 1} & d_{n, 2} & \cdots & d_{n, n}
\end{array}\right)\right)\left(\begin{array}{c}
t_{1} \\
t_{2} \\
\vdots \\
t_{n}
\end{array}\right)=0
$$

By Cramer's rule, it follows

$$
M^{*} M\left(\begin{array}{c}
t_{1} \\
t_{2} \\
\vdots \\
t_{n}
\end{array}\right)=\operatorname{det}(M) \operatorname{id}_{n \times n}\left(\begin{array}{c}
t_{1} \\
t_{2} \\
\vdots \\
t_{n}
\end{array}\right)=\operatorname{det}(M)\left(\begin{array}{c}
t_{1} \\
t_{2} \\
\vdots \\
t_{n}
\end{array}\right)=0
$$

so that $\operatorname{det}(M) t_{j}=0$ 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

$$
\operatorname{det}(M)=\operatorname{det}(M) \cdot 1=\sum_{j=1}^{n} e_{j} \operatorname{det}(M) t_{j}=0
$$

Hence, the characteristic polynomial of $D$ :

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

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) $\Rightarrow$ (ii)' follows from the explicit way in which one can represent 'high' powers of $a$ by lower ones using the relation $a^{n}=-\left(c_{n-1} a^{n-1}+c_{n-2} a^{n-2}+\cdots+c_{0}\right)$ coming from the definition of integrality. The core of the argument is the implication '(iv) $\Rightarrow$ (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.

Proposition 2.17 Let $R \subseteq S \subseteq T$ be ring extensions. Then the following statements are equivalent:
(i) $T$ is finitely generated as an $R$-module.
(ii) $T$ is finitely generated as an $S$-module and $S$ is finitely generated as an $R$-module.

Proof. (i) $\Rightarrow$ (ii): This is trivial.
(ii) $\Rightarrow$ (i): Let $t_{1}, \ldots, t_{n} \in T$ be generators of $T$ as an $S$-module. This means that any $t \in T$ can be written in the form $t=\sum i=1^{n} c_{i} t_{i}$ for $c_{1}, \ldots, c_{n} \in S$. Furthermore, let $s_{1}, \ldots, s_{m} \in S$ be generators of $S$ as an $R$-module. This implies that every $c_{i}$, for $i=1, \ldots, n$ can be written in the form $c_{i}=\sum_{j=1}^{m} r_{i, j} s_{j}$. This leads to the expression

$$
t=\sum_{i=1}^{n} \sum_{j=1}^{m} r_{i, j} s_{j} t_{i}
$$

proving that the elements $s_{j} t_{i}$ for $1 \leq j \leq m$ and $1 \leq i \leq n$ generate $T$ as an $R$-module.

Corollary 2.18 Let $R \subseteq S$ be a ring extension and let $a_{1}, \ldots, a_{n} \in S$. Then the following statements are equivalent:
(i) The elements $a_{1}, \ldots, a_{n}$ are integral over $R$.
(ii) $R\left[a_{1}, \ldots, a_{n}\right]$ is finitely generated as an $R$-module.
(iii) The ring extension $R \subseteq R\left[a_{1}, \ldots, a_{n}\right]$ is integral.

Proof. (i) $\Rightarrow$ (ii): We proceed by induction. The case $n=1$ is the implication (i) $\Rightarrow$ (ii) of Proposition 2.16. Assume the statement is proved for $n-1$. Then we know that $T=R\left[a_{1}, \ldots, a_{n-1}\right]$ is finitely generated as an $R$-module. Furthermore $T\left[a_{n}\right]$ is finitely generated as $T$-module as $a_{n}$ is integral over $R$ (and hence over $T$ ). By Proposition 2.17, $T\left[a_{n}\right]=R\left[a_{1}, \ldots, a_{n-1}, a_{n}\right]$ is finitely generated as an $R$-module.
(ii) $\Rightarrow$ (iii): Let $a \in R\left[a_{1}, \ldots, a_{n}\right]$. The implication (iii) $\Rightarrow$ (i) of Proposition 2.16 with $T=$ $R\left[a_{1}, \ldots, a_{n}\right]$ shows that $a$ is integral over $R$.
(iii) $\Rightarrow$ (i): By definition, elements in an integral ring extension are integral over the base ring.

Corollary 2.19 Let $R \subseteq S$ be a ring extension. If $S$ is finitely generated as an $R$-module, then $R \subseteq S$ is an integral ring extension.

Proof. Take generators $a_{1}, \ldots, a_{n}$ of $S$ as an $R$-module. Then $S=R\left[a_{1}, \ldots, a_{n}\right]$ and we can apply Corollary 2.18.

Example 2.20 The ring extensions $\mathbb{Z}[\sqrt{2}] / \mathbb{Z}$ and $\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right] / \mathbb{Z}$ are integral, whereas $\mathbb{Z}\left[\frac{1+\sqrt{-5}}{2}\right] / \mathbb{Z}$ is not.

Corollary 2.21 Let $R \subseteq S \subseteq T$ be ring extensions. Then 'transitivity of integrality' holds:

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

Proof. 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 $X^{n}+s_{n-1} X^{n-1}+\cdots+s_{0} \in S[X]$. All the coefficients lie in the subring $U:=R\left[s_{0}, s_{1}, \ldots, s_{n-1}\right]$. As the coefficients of the minimal polynomial of $t$ all lie in the subring $U:=R\left[s_{0}, s_{1}, \ldots, s_{n-1}\right]$, it follows that $t$ is integral over $U$, whence $U[t]$ is finitely generated as a $U$-module. However, the integrality of $R \subseteq S$ implies by Corollary 2.18 that $U$ is finitely generated as an $R$-module. Consequently, Proposition 2.17 implies that $U[t]$ is finitely generated as an $R$-module. Consequently, $t$ is integral over $R$.

## Algebraic closure and integral closure

## Definition 2.22

Let $R \subseteq S$ be a ring extension.
(a) The set

$$
R_{S}=\{a \in S \mid a \text { is integral over } R\}
$$

is called the integral closure of $R$ in $S$. An alternative name is: normalisation of $R$ in $S$. We will see in a moment that the integral closure of $R$ in $S$ is integrally closed in $S$, justifying the names.
Note that $R \subseteq S$ is an integral ring extension if and only if $R_{S}=S$.
(b) We say that $R$ is integrally closed in $S$ if $R_{S}=R$.
(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.
Note that this means that there is no proper integral extension of $R$ inside the fraction field of $R$.

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 $L$.

Also the algebraic closure of $K$ in $L$ is algebraically closed in $L$.

Note that $L / K$ is an algebraic field extension 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 (without mentioning any extension field) 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 $K$.

Note that (a) and (b) are exactly the same for both sides, in the sense that considering fields as rings, the right hand side column is a special case of the left hand side one. Attention! This is not the case for point (c).
Our next aim is to show in an elegant way that $R_{S}$ is a ring.

Proposition 2.23 Let $R \subseteq S$ be a ring extension.
(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) Let $a, b \in R_{S}$. As both of them are integral over $R$, the extension $R[a, b]$ is integral. As it contains $a+b, a \cdot b$ as well as 0 and 1 , these elements are integral over $R$ and hence lie in $R_{S}$, showing that $R_{S}$ is a ring.
(b) Any $s \in S$ that is integral over $R_{S}$ is also integral over $R$ (by the transitivity of integrality), whence $s \in R_{S}$.

We have the same for the algebraic closure of $K$ in $L$.

Proposition 2.24 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. The only point that is not covered by the ring situation Proposition 2.23 is that $K_{L}$ is a field. We know that it is a ring and so we only need to show that any $0 \neq b \in K_{L}$ has an inverse. As $b$ is algebraic over $K$, we have $K[b]=K(b)$. Consequently, $1 / b$ lies in $K(b) \subseteq K_{L}$.

## Number fields and rings of integers

Definition 2.25 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 $\mathscr{O}_{K}$.

Example 2.26 (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).

Example 2.27 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 $d \equiv 2,3(\bmod 4)$,
(2) $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$, if $d \equiv 1(\bmod 4)$.
(Proof as an exercise.)
The next couple of results are inspired by rings of integers, but we formulate the statements in more generality.

Proposition 2.28 Every unique factorisation domain (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:

$$
b^{n}=-c\left(a_{n-1} b^{n-1}+c a_{n-2} b^{n-2}+\cdots+c^{n-1} a_{0}\right)
$$

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

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 2.29 Let $R$ be an integral domain, $K=\operatorname{Frac}(R), L / K$ 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) $L=\operatorname{Frac}(S)$ 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 $d:=d_{0} \cdot d_{1}$. $\cdots d_{n-1} \in R$, plug in $a$ and multiply through with $d^{n}$ :

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

showing that $d a$ is integral over $R$, i.e. $d a \in S$, 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.

## Some notes on algebraically closed fields

Proposition 2.30 A field $K$ is algebraically closed if and only if any non-constant polynomial $f \in K[X]$ has a zero in $K$.

Proposition 2.31 Let $K$ be a field. Then there exists an algebraic field extension $\bar{K} / K$ such that $\bar{K}$ is algebraically closed.
The field $\bar{K}$ 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 2.32 (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.

## 3 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 3.1 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 $S \subseteq K\left[X_{1}, \ldots, X_{n}\right]$ be a subset. Then

$$
\mathscr{V}_{S}(L):=\left\{\left(x_{1}, \ldots, x_{n}\right) \in \mathbb{A}^{n}(L) \mid f\left(x_{1}, \ldots, x_{n}\right)=0 \text { for all } f \in S\right\}
$$

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

Convention: When the number of variables is clear, we write $K[\underline{X}]$ for $K\left[X_{1}, \ldots, X_{n}\right]$. In the same way a tuple $\left(x_{1}, \ldots, x_{n}\right) \in \mathbb{A}^{n}(K)$ is also abbreviated as $\underline{x}$ if no confusion can arise.
The letter ' V ' is chosen because of the word 'vanishing set' (German: 'Verschwindungsmenge').
Example 3.2 (a) $K=\mathbb{R}, n=2, K[X, Y] \ni f(X, Y)=a X+b Y+c$ non-constant. Then $V_{\{f\}}(\mathbb{R})$ is a line $\left(y=-\frac{a}{b} x-\frac{c}{b}\right.$ 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 $\mathscr{V}_{\{f\}}(\mathbb{R})=\emptyset$, but $(0, i) \in \mathscr{V}_{\{f\}}(\mathbb{C})$.
(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

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

which is a line.

Lemma 3.3 A plane curve has infinitely many points over any algebraically closed field. More precisely, let $K$ be a field, $\bar{K}$ an algebraic closure of $K$ and $f(X, Y) \in K[X, Y]$ a nonconstant polynomial.
Then $\mathscr{V}_{\{f\}}(\bar{K})$ 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 $\bar{K}$ only has finitely many elements $a_{1}, \ldots, a_{n}$. Form the polynomial $g(X):=1+\prod_{i=1}^{n}\left(X-a_{i}\right)$. Note that $g\left(a_{i}\right)=1 \neq 0$ 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 $x \in \bar{K}$ be any zero of $a_{0}(x)$, which exists as $\bar{K}$ is algebraically closed. Now $(x, y)$ satisfies $f$ for any $y \in \bar{K}$, showing the infinity of solutions.
Second case: $d>0$. Then $a_{d}(x) \neq 0$ for all but finitely many $x \in \bar{K}$, 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 3.4 (a) Let $K=\mathbb{Q}$ and consider $f(X, Y)=X^{2}+Y^{2}-1$ and the $\mathbb{Q}$-points of the associated curve $C=S^{1}=\mathscr{V}_{\{f\}}(\mathbb{Q})$. 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, $\mathscr{V}_{\{f\}}(K)=\{(0,0)\}$ if and only if $X^{2}=-1$ has no solution in $K$.
In particular, $\mathscr{V}_{\{f\}}(\mathbb{R})=\{(0,0)\}$ (but: $\mathscr{V}_{\{f\}}(\mathbb{C})=\mathscr{V}_{\{X-i Y\}}(\mathbb{C}) \cup \mathscr{V}_{\{X+i Y\}}(\mathbb{C})$, union of two lines) and $\mathscr{V}_{\{f\}}\left(\mathbb{F}_{p}\right)=\{(0,0)\}$ if and only if $p \equiv 3(\bmod 4)$.

Example 3.5 Let $K$ be a field and $f(X)=X^{3}+a X^{2}+b X+c$ be a separable polynomial (meaning that it has no multiple zeros over $\bar{K}$ ).
Any plane curve of the form $\mathscr{V}_{\left\{Y^{2}-f(X)\right\}}$ is called an elliptic curve. It has many special properties (see e.g. lectures on cryptography).

Definition 3.6 Let $\mathscr{X}$ be a set and $\mathscr{O}$ a set of subsets of $\mathscr{X}$ (i.e. the elements of $\mathscr{O}$ are sets; they are called the open sets).
Then $\mathscr{O}$ is called a topology on $\mathscr{X}$ (alternatively: $(\mathscr{X}, \mathscr{O})$ is called a topological space) if
(1) $\emptyset, \mathscr{X} \in \mathscr{O}$ (in words: the empty set and the whole space are open sets);
(2) if $A_{i} \in \mathscr{O}$ for $i \in I$, then $\bigcup_{i \in I} A_{i} \in \mathscr{O}$ (in words: the union of arbitrarily many open sets is an open set);
(3) if $A, B \in \mathscr{O}$, then $A \cap B \in \mathscr{O}$ (in words: the intersection of two (and, consequently, finitely many) open sets is an open set).

A set $C \subseteq \mathscr{X}$ is called closed if $\mathscr{X} \backslash C \in \mathscr{O}$ (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 $\mathscr{O}$ to consist of those sets $U \subseteq \mathbb{R}^{n}$ such that for every $x \in U$ there is $\varepsilon>0$ such that all $y \in \mathbb{R}^{n}$ with $|y-x|<\varepsilon$ belong to $U$. These are by definition the open subsets of $\mathbb{R}^{n}$. It is a well-known exercise to show that $\mathscr{O}$ 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 3.7 Let $K$ be a field and $n \in \mathbb{N}$. Define

$$
\mathscr{O}:=\left\{\mathbb{A}^{n}(K) \backslash \mathscr{V}_{S}(K) \mid S \subseteq K\left[X_{1}, \ldots, X_{n}\right]\right\} .
$$

Then $\left(\mathbb{A}^{n}(K), \mathscr{O}\right)$ 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 3.8 Let $K$ be a field, $L / K$ a field extension and $n \in \mathbb{N}$.
(a) Let $S \subseteq T \subseteq K\left[X_{1}, \ldots, X_{n}\right]$ be subsets. Then $\mathscr{V}_{T}(L) \subseteq \mathscr{V}_{S}(L)$.
(b) Let $S \subseteq K\left[X_{1}, \ldots, X_{n}\right]$ and let $\mathfrak{a}:=(s \mid s \in S) \triangleleft K\left[X_{1}, \ldots, X_{n}\right]$ be the ideal generated by $S$. Then $\mathscr{V}_{S}(L)=\mathscr{V}_{\mathrm{a}}(L)$.
(c) $\mathscr{V}_{\{(0)\}}(L)=\mathbb{A}^{n}(L)$ and $\mathscr{V}_{\{(1)\}}(L)=\emptyset$.
(d) Let $S_{i} \subseteq K\left[X_{1}, \ldots, X_{n}\right]$ for $i \in I$ (some indexing set) be subsets. Then $\mathscr{U}_{i \in I} S_{i}(L)=$ $\bigcap_{i \in I} \mathscr{V}_{S_{i}}(L)$.
(e) Let $\mathfrak{a}, \mathfrak{b} \triangleleft K\left[X_{1}, \ldots, X_{n}\right]$ be ideals. Then $\mathscr{V}_{\mathfrak{a} \cdot \mathfrak{b}}(L)=\mathscr{V}_{\mathfrak{a}}(L) \cup \mathscr{V}_{\mathfrak{b}}(L)$.

Proof. (a) and (c) are clear.
(b) The inclusion $\mathscr{V}_{\mathfrak{a}}(L) \subseteq \mathscr{V}_{S}(L)$ follows from (a). Let now $\underline{x} \in \mathscr{V}_{S}(L)$, 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.
(d) Let $\underline{x} \in \mathbb{A}^{n}(L)$. Then

$$
\begin{aligned}
\underline{x} \in \mathscr{V}_{i \in I} S_{i}(L) & \Leftrightarrow \forall f \in \bigcup_{i \in I} S_{i}: f(\underline{x})=0 \Leftrightarrow \forall i \in I: \forall f \in S_{i}: f(\underline{x})=0 \\
& \Leftrightarrow \forall i \in I: \underline{x} \in \mathscr{V}_{S_{i}}(L) \Leftrightarrow \underline{x} \in \bigcap_{i \in I} \mathscr{V}_{S_{i}}(L) .
\end{aligned}
$$

(e) Since $\mathfrak{a b} \subseteq \mathfrak{a}$ and $\mathfrak{a b} \subseteq \mathfrak{b}$, (b) gives the inclusions $\mathscr{V}_{\mathfrak{a}}(L), \mathscr{V}_{\mathfrak{b}}(L) \subseteq \mathscr{V}_{\mathfrak{b} \mathfrak{b}}(L)$, hence $\mathscr{V}_{\mathfrak{a}}(L) \cup$ $\mathscr{V}_{\mathfrak{b}}(L) \subseteq \mathscr{V}_{\mathfrak{a} \mathfrak{b}}(L)$. For the reverse inclusion, let $\underline{x} \notin \mathscr{V}_{\mathfrak{a}}(L) \cup \mathscr{V}_{\mathfrak{b}}(L)$, 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 $\underline{x} \notin \mathscr{V}_{\mathfrak{a b}}(L)$.

Proof of Proposition 3.7. We need to check the axioms (1), (2) and (3). Note that (1) is Lemma 3.8 (c).
(2) For open sets $\mathbb{A}^{n}(K) \backslash \mathscr{V}_{S_{i}}(K)$ with $S_{i} \subseteq K[\underline{X}]$ for $i \in I$, we have: $\bigcup_{i \in I} \mathbb{A}^{n}(K) \backslash \mathscr{V}_{S_{i}}(K)=$ $\mathbb{A}^{n}(K) \backslash \bigcap_{i \in I} \mathscr{V}_{S_{i}}(K) \stackrel{\text { Lemma } 3.8(\mathrm{~d})}{ } \mathbb{A}^{n}(K) \backslash \mathscr{U}_{i \in I} S_{i}(K)$.
(3) By Lemma 3.8 (b), any two open sets are of the form $\mathbb{A}^{n}(K) \backslash \mathscr{V}_{\mathfrak{a}}(K)$ and $\mathbb{A}^{n}(K) \backslash \mathscr{V}_{\mathfrak{b}}(K)$ with ideals $\mathfrak{a}, \mathfrak{b} \triangleleft K[\underline{X}]$. It follows: $\left(\mathbb{A}^{n}(K) \backslash \mathscr{V}_{\mathfrak{a}}(K)\right) \cap\left(\mathbb{A}^{n}(K) \backslash \mathscr{V}_{\mathfrak{b}}(K)\right)=\mathbb{A}^{n}(K) \backslash\left(\mathscr{V}_{\mathfrak{a}}(K) \cup\right.$ $\left.\mathscr{V}_{\mathfrak{b}}(K)\right) \stackrel{\text { Lemma } 3.8(\mathrm{e})}{=} \mathbb{A}^{n}(K) \backslash \mathscr{V}_{\mathfrak{a} \cdot \mathfrak{b}}(K)$.

We next want to consider polynomial functions from a subset $\mathscr{X} \subseteq \mathbb{A}^{n}(K)$ to $K$. Formally, we see them as the image of the ring homomorphism

$$
\varphi_{\mathscr{X}}: K[\underline{X}] \rightarrow \operatorname{Maps}(\mathscr{X}, K), \quad f \mapsto\left(\left(x_{1}, \ldots, x_{n}\right) \mapsto f\left(x_{1}, \ldots, x_{n}\right)\right)
$$

with + and $\cdot$ on $\operatorname{Maps}(\mathscr{X}, K)$ defined pointwise: $(f+g)(\underline{x}):=f(\underline{x})+g(\underline{x})$ and $(f \cdot g)(\underline{x}):=$ $f(\underline{x}) \cdot g(\underline{x})$.

Definition 3.9 Let $\mathscr{X}$ be a subset of $\mathbb{A}^{n}(K)$. We define the vanishing ideal of $\mathscr{X}$ as

$$
\mathscr{I}_{\mathscr{X}}:=\operatorname{ker}\left(\varphi_{\mathscr{X}}\right)=\{f \in K[\underline{X}] \mid f(\underline{x})=0 \text { for all } \underline{x} \in \mathscr{X}\} .
$$

The quotient ring $K[\mathscr{X}]:=K[X] / \mathscr{I}_{\mathscr{X}}$ is called the coordinate ring of $\mathscr{X}$.
Note that $\mathscr{I}_{\mathscr{X}}$ is indeed an ideal because it is the kernel of a ring homomorphism. Moreover, by the isomorphism theorem, we obtain an injection

$$
\overline{\varphi_{\mathscr{X}}}: K[\mathscr{X}] \rightarrow \operatorname{Maps}(\mathscr{X}, K)
$$

We may even replace $\operatorname{Maps}(\mathscr{X}, K)$ by $\mathscr{C}\left(\mathscr{X}, \mathbb{A}^{1}(K)\right)$, the continuous maps for the Zariski topology (see exercise).
The coordinate ring consists hence of the polynomial functions from $\mathscr{X}$ to $K$. There are some special ones, namely, the projection to the $i$-th coordinate, i.e. $\left(x_{1}, \ldots, x_{n}\right) \mapsto x_{i}$; 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 $f\left(X_{1}, \ldots, X_{n}\right)+\mathscr{I}_{\mathscr{X}}=\sum a_{i_{1}, \ldots, i_{n}} X_{1}^{i_{1}} \ldots X_{n}^{i_{n}}+\mathscr{I}_{\mathscr{X}}$ is a combination of the coordinate functions, namely, $\sum a_{i_{1}, \ldots, i_{n}} \mathfrak{r}_{1}^{i_{1}} \ldots \mathfrak{x}_{n}^{i_{n}}$.
Example $3.10 \quad$ Line $f(X, Y):=X-Y+2 \in \mathbb{R}[X, Y], \mathscr{L}:=\mathscr{V}_{f}(\mathbb{R})$ :
We have $\mathscr{I}_{\mathscr{L}}=(X-Y+2)$, i.e. that the vanishing ideal of $L$ is the principal ideal generated by $f$. This is a consequence of Proposition 3.13, which will be proved below.
We compute the structure of the coordinate ring in this case. Consider the ring homomorphism:

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

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 $\mathscr{I}_{\mathscr{L}}$ (and hence to $(X-Y+2)$ ). Let $g \in \operatorname{ker}(\varphi)$. This means $g(T, T+2)$ is the zero polynomial. If we now take a point $(x, y) \in \mathscr{L}$, 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 $g \in \mathscr{I}_{\mathscr{L}}$, as claimed.
From the isomorphism theorem, we now obtain that the coordinate ring is just the polynomial ring in one variable:

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

In other words, the coordinate functions satisfy the equality $\mathfrak{x}_{2}=\mathfrak{x}_{1}+2$.

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

Again by Proposition 3.13 we have $\mathscr{I}_{\mathscr{P}}=\left(X^{2}-Y+2\right)$.

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

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

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

- Hyperbola $f(X, Y):=X Y-1 \in \mathbb{R}[X, Y], \mathscr{H}:=\mathscr{V}_{f}(\mathbb{R})$ :

We again have $\mathscr{I}_{\mathscr{H}}=(X Y-1)$ by Proposition 3.13. This time we obtain

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

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 $\varphi: \mathbb{R}\left[X, \frac{1}{X}\right] \rightarrow \mathbb{R}[T]$. 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 $\varphi$ lands in $\mathbb{R}$, contradicting the surjectivity.

Here are basic properties of the vanishing ideal.

Lemma 3.11 Let $K$ be a field and $n \in \mathbb{N}$. Then the following statements hold:
(a) Let $\mathscr{X} \subseteq \mathscr{Y} \subseteq \mathbb{A}^{n}(K)$ be subsets. Then $\mathscr{I}_{\mathfrak{X}} \supseteq \mathscr{I}_{\mathfrak{Y}}$.
(b) $\mathscr{I}_{\emptyset}=K[\underline{X}]$.
(c) If $K$ has infinitely many elements, then $\mathscr{I}_{\mathbb{A}^{n}(K)}=(0)$.
(d) Let $S \subseteq K[\underline{X}]$ be a subset. Then $\mathscr{I}_{\mathscr{V}_{S}(K)} \supseteq S$.
(e) Let $\mathscr{X} \subseteq \mathbb{A}^{n}(K)$ be a subset. Then $\mathscr{V}_{\mathscr{I}}(K) \supseteq \mathscr{X}$.
(f) Let $S \subseteq K[\underline{X}]$ be a subset. Then $\mathscr{V}_{\mathscr{I}_{V_{S}(K)}}(K)=\mathscr{V}_{S}(K)$.
(g) Let $\mathscr{X} \subseteq \mathbb{A}^{n}(K)$ be a subset. Then $\mathscr{I}_{V_{\left(\mathscr{I}_{\mathscr{X}}\right)}(K)}=\mathscr{I}_{\mathscr{X}}$.

## Proof. Exercise.

Lemma 3.12 Let $K$ be a field and let $\mathscr{X} \subseteq \mathbb{A}^{n}(K)$ be an affine algebraic subset.
For any field extension $L / K$, consider

$$
\mathscr{X}(L):=\mathscr{V}_{\mathscr{I}_{\mathscr{X}}}(L),
$$

the set of L-points of $\mathscr{X}$.
(a) $\mathscr{X}=\mathscr{X}(K)$.
(b) Every $L$-point $\left(a_{1}, \ldots, a_{n}\right) \in \mathscr{X}(L)$ gives rise to the $K$-algebra homomorphism

$$
\operatorname{ev}_{\left(a_{1}, \ldots, a_{n}\right)}: K[\mathscr{X}]=K\left[X_{1}, \ldots, X_{n}\right] / \mathscr{I}_{\mathscr{X}} \rightarrow L, \quad g\left(X_{1}, \ldots, X_{n}\right)+\mathscr{I}_{\mathscr{X}} \mapsto g\left(a_{1}, \ldots, a_{n}\right) .
$$

(c) If $L=K$, then the kernel of $\mathrm{ev}_{\left(a_{1}, \ldots, a_{n}\right)}$ is equal to $\left(X_{1}-a_{1}+\mathscr{I}_{\mathscr{X}}, \ldots, X_{n}-a_{n}+\mathscr{I}_{\mathscr{X}}\right)$.

Proof. (a) This is Lemma 3.11(f).
(b) The point is that the map is well-defined, which is ensured because the image does not depend on the choice of representative in $K\left[X_{1}, \ldots, X_{n}\right]$ in any class in $K[\mathscr{X}]=K\left[X_{1}, \ldots, X_{n}\right] / \mathscr{I}_{\mathscr{X}}$.
(c) The ideal $\left(X_{1}-a_{1}+\mathscr{I}_{\mathscr{X}}, X_{2}-a_{2}+\mathscr{I}_{\mathscr{X}}, \ldots, X_{n}-a_{n}+\mathscr{I}_{\mathscr{X}}\right)$ is clearly maximal in $K[\mathscr{X}]$ because the quotient by it is $K$. As it is contained in $\operatorname{ker}\left(\operatorname{ev}_{\left(a_{1}, \ldots, a_{n}\right)}\right)$ it follows that the two ideals are equal (as $\operatorname{ev}_{\left(a_{1}, \ldots, a_{n}\right)}$ is not the zero-map - look at constants).

Proposition 3.13 Let $K$ be a field. Let $f \in K[X, Y]$ a nonconstant irreducible polynomial. Assume that $\mathscr{V}_{f}(K)$ is infinite (which is automatic if $K=\bar{K}$ is algebraically closed by Lemma 3.3). Let $C=\mathscr{V}_{f}(K)$ be the associated plane curve.
Then the vanishing ideal $\mathscr{I}_{C}$ 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 71. We now give a direct proof, which relies on the following Lemma 3.14. 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 $C=\mathscr{V}_{f}(\mathbb{R})$ is the empty set and hence the vanishing ideal $\mathscr{I}_{C}$ 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 $\bar{T}$ in the coordinate ring (the transcendence assumption means that the subring $K[\bar{T}]$ of the coordinate ring is isomorphic to a polynomial ring) such that the coordinate ring is an integral ring extension of $K[\bar{T}]$. This will be essential in the proof of Proposition 3.13.

Lemma 3.14 Let $K$ be a field and $\mathscr{I} \unlhd K[X, Y]$ be an ideal containing $f \in \mathscr{I}$, a nonconstant polynomial of total degree $d>0$. Let $\bar{T}:=X-Y^{d+1}+\mathscr{I} \in K[X, Y] / \mathscr{I}$.
(a) The ring extension $K[T] \subseteq K[X, Y] / \mathscr{I}$ is integral.
(b) Assume that $\mathscr{V}_{f}(K)$ is infinite ( automatic if $K=\bar{K}$ is algebraically closed by Lemma 3.3). If $\mathscr{I}=\mathscr{I}_{C}$ with $C=V_{f}(K)$ a curve, then $\bar{T}$ is transcendental over $K$.

Proof. (a) We explicitely write down the polynomial $f(X, Y)=\sum_{0 \leq i, j \text { s.t. } i+j \leq d} a_{i, j} X^{i} Y^{j}$. Consider the polynomial $g(T, Z)=f\left(T+Z^{d+1}, Z\right) \in K[T][Z]$, i.e. we see it as a polynomial in the variable $Z$ with coefficients in $K[T]$. We find
$g(T, Z)=\sum_{0 \leq i, j \text { s.t. } i+j \leq d} a_{i, j}\left(T+Z^{d+1}\right)^{i} Z^{j}=\sum_{0 \leq i, j \text { s.t. } i+j \leq d} a_{i, j} Z^{(d+1) i+j}+$ 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 $\bar{T}$ from the assertion, i.e. $\bar{T}=X-Y^{d+1}+\mathscr{I}$. Write $h(Z)$ for the image of $h(\bar{T}, Z) \in(K[\bar{T}])[Z] \subseteq(K[X, Y] / \mathscr{I})[Z]$. It is a monic polynomial. Then we get

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

This means that the class $Y+\mathscr{I}$ is annihilated by the monic polynomial $h(Z)$. Thus, $Y+\mathscr{I}$ is integral over $K[\bar{T}]$.
As $K[X, Y] / \mathscr{I}$ is generated over $K[\bar{T}]$ by $Y+\mathscr{I}$, the integrality of $K[\bar{T}] \subseteq K[X, Y] / \mathscr{I}$ follows.
(b) Suppose that $\bar{T}$ is not transcendental over $K$, then it is algebraic over $K$, hence the ring extension $K \subseteq K[T]$ is integral. Furthermore, by (a), the ring extension $K[\bar{T}] \subseteq K[X, Y] / \mathscr{I}$ is also integral, whence by the transitivity of integrality (Corollary 2.21) the ring extension $K \subseteq$ $K[X, Y] / \mathscr{I}$ 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 $m_{X}(X+\mathscr{I})=0=m_{Y}(Y+\mathscr{I})$, in other words $m_{X}(X), m_{Y}(Y) \in \mathscr{I}$. This means that for any point $(x, y) \in C=\mathscr{V}_{\mathscr{I}}(K)$ (the equality follows from Lemma 3.11 (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 3.13. The inclusion $(f) \subseteq \mathscr{I}_{C}$ is clear. We need to show the reverse inclusion. In order to do this, we consider the natural projection (coming from the inclusion $\left.(f) \subseteq \mathscr{I}_{C}\right)$

$$
\pi: K[X, Y] /(f) \rightarrow K[X, Y] / \mathscr{I}_{C} .
$$

It suffices to show that it is an isomorphism. In order to do so, let $g \in \mathscr{I}_{C}$ and consider its class $\bar{g}=g+(f) \in K[X, Y] /(f)$; we aim to show that it is the zero class, i.e. $g \in(f)$.
Next, we want to use Lemma 3.14; we therefore consider elements $T:=X-Y^{d+1} \in K[X, Y]$ with $d$ being the total degree of $f$ and its images $\bar{T} \in K[X, Y] /(f)$ and $\tilde{T}:=\pi(\bar{T}) \in K[X, Y] / \mathscr{I}_{C}$. Part (b) of the lemma tells us that $\tilde{T}$ (and hence also $\bar{T}$ ) is transcendental over $K$, and by part (a), the ring extension $K[\bar{T}] \subseteq K[X, Y] /(f)$ is integral.
We apply the latter statement to the element $\bar{g}$ in order to get an equality of the form

$$
\bar{g}^{n}+\sum_{i=1}^{n-1} r_{i}(\bar{T}) \bar{g}^{i}+r_{0}(\bar{T})=0
$$

in the ring $K[X, Y] /(f)$, where the $r_{i} \in K[\bar{T}]$ are polynomials (we can see them as usual polynomials because $\bar{T}$ is transcendental over $K$ ). Let us suppose that $n$ is minimal with this property. As $\bar{g}$ vanishes on all points of $C$, so do $r_{0}(\bar{T})$ and $r_{0}(T)=r_{0}\left(X-Y^{d+1}\right)$. This implies that $r_{0}(T)=r_{0}\left(X-Y^{d+1}\right)$ belongs to $\mathscr{I}_{C}$, so that $r_{0}(\tilde{T})$ is zero in $K[X, Y] / \mathscr{I}_{C}$.
As $\tilde{T}$ in $K[X, Y] / \mathscr{I}_{C}$ 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

$$
\bar{g}\left(\bar{g}^{n-1}+\sum_{i=1}^{n-1} r_{i}(\bar{T}) \bar{g}^{i-1}\right)=0
$$

In other words

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

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 $\bar{g}^{n-1}+\sum_{i=1}^{n-1} r_{i}(\bar{T}) \bar{g}^{i-1}=0$, contradicting the minimality of $n$.

Lemma 3.15 Let $\left(\mathscr{X}, \mathscr{O}_{\mathscr{X}}\right)$ be a topological space and $\mathscr{Y} \subseteq \mathscr{X}$ be a subset. Define $\mathscr{O}_{\mathscr{Y}}:=$ $\left\{U \cap \mathscr{Y} \mid U \in \mathscr{O}_{\mathscr{X}}\right\}$.
Then $\mathscr{O}_{\mathscr{Y}}$ is a topology on $\mathscr{Y}$, called the relative topology or the subset topology.

## Proof. Exercise.

Definition 3.16 Let $\mathscr{X}$ be a topological space (we do not always mention $\mathscr{O}$ explicitly). A subset $\mathscr{Y} \subseteq \mathscr{X}$ is called reducible if there are two closed subsets $\mathscr{Y}_{1}, \mathscr{Y}_{2} \subsetneq \mathscr{Y}$ for the relative topology on $\mathscr{Y}$ such that $\mathscr{Y}=\mathscr{Y}_{1} \cup \mathscr{Y}_{2}$. By the definition of the relative topology, $\mathscr{Y} \subseteq \mathscr{X}$ is reducible if and only if there are closed subsets $\mathscr{X}_{1}, \mathscr{X}_{2} \subseteq \mathscr{X}$ such that $\mathscr{Y} \subseteq \mathscr{X}_{1} \cup \mathscr{X}_{2}$, $\mathscr{Y} \nsubseteq \mathscr{X}_{1}$ and $\mathscr{Y} \nsubseteq \mathscr{X}_{2}$.
If $\mathscr{Y}$ is not reducible, it is called irreducible.
An affine set $\mathscr{X} \subseteq \mathbb{A}^{n}(K)$ is called an affine variety if $\mathscr{X}$ is irreducible.
Example $3.17 \quad$ Let $f(X, Y)=X Y \in \mathbb{R}[X, Y]$. Then $\mathscr{V}_{f}(\mathbb{R})$ is the union of the $x$-axis and the $y$-axis, so clearly $\mathscr{V}_{f}(\mathbb{R})$ is reducible for the Zariski topology (and also the usual real topology). More precisely,

$$
\mathscr{V}_{f}(\mathbb{R})=\mathscr{V}_{X}(\mathbb{R}) \cup \mathscr{V}_{Y}(\mathbb{R})
$$

- 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 $\mathscr{H}$ is also irreducible for the Zariski topology. This is a consequence of the next proposition, since the coordinate ring $\mathbb{R}[\mathscr{H}]$ 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 3.18 Let $\emptyset \neq \mathscr{X} \subseteq \mathbb{A}^{n}(K)$ be an affine set. Then the following statements are equivalent:
(i) $\mathscr{X}$ is irreducible for the Zariski topology (i.e. $\mathscr{X}$ is a variety).
(ii) $\mathscr{I}_{\mathscr{X}}$ is a prime ideal of $K\left[X_{1}, \ldots, X_{n}\right]$.
(iii) The coordinate ring $K[\mathscr{X}]$ is an integral domain.

Proof. The equivalence of (ii) and (iii) is Proposition 1.19 (recall $K[\mathscr{X}]=K[\underline{X}] / \mathscr{I}_{\mathscr{X}}$ ).
$\neg($ ii $) \Rightarrow \neg$ (i): Suppose $\mathscr{I}_{\mathscr{X}}$ is not a prime ideal. Then there are two elements $f_{1}, f_{2} \in K[\underline{X}] \backslash \mathscr{I}_{\mathscr{X}}$ such that $f_{1} \cdot f_{2} \in \mathscr{I}_{\mathscr{X}}$. This, however, implies:

$$
\mathscr{X}=\left(\mathscr{V}_{\left(f_{1}\right)}(K) \cup \mathscr{V}_{\left(f_{2}\right)}(K)\right) \cap \mathscr{X}=\left(\mathscr{V}_{\left(f_{1}\right)}(K) \cap \mathscr{X}\right) \cup\left(\mathscr{V}_{\left(f_{2}\right)}(K) \cap \mathscr{X}\right)
$$

since $\mathscr{V}_{\left(f_{1}\right)}(K) \cup \mathscr{V}_{\left(f_{2}\right)}(K)=\mathscr{V}_{\left(f_{1} \cdot f_{2}\right)}(K) \supseteq \mathscr{X}$. Note that $f_{1} \notin \mathscr{I}_{\mathscr{X}}$ precisely means that there is $\underline{x} \in \mathscr{X}$ such that $f_{1}(\underline{x}) \neq 0$. Hence, $\mathscr{X} \neq \mathscr{V}_{\left(f_{1}\right)}(K) \cap \mathscr{X}$. Of course, the same argument applies with $f_{1}$ replaced by $f_{2}$, proving that $\mathscr{X}$ is reducible.
$\neg\left(\right.$ i) $\Rightarrow \neg$ (ii): Suppose $\mathscr{X}$ is reducible, i.e. $\mathscr{X}=\mathscr{X}_{1} \cup \mathscr{X}_{2}$ with $\mathscr{X}_{1} \subsetneq \mathscr{X}$ and $\mathscr{X}_{2} \subsetneq \mathscr{X}$ closed subsets of $\mathscr{X}$ (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 $\mathscr{X}$ ). This means $\mathscr{I}_{\mathscr{X}_{i}} \supsetneq \mathscr{I}_{\mathscr{X}}$ for $i=1,2$ as otherwise $\mathscr{X}=\mathscr{X}_{i}$ by Lemma 3.11. Hence, there are $f_{1} \in \mathscr{I}_{\mathscr{X}_{1}}$ and $f_{2} \in \mathscr{I}_{\mathscr{X}_{2}}$ such that $f_{1}, f_{2} \notin \mathscr{I}_{\mathscr{X}}$. Note that $f_{1}(\underline{x}) f_{2}(\underline{x})=0$ for all $\underline{x} \in \mathscr{X}$, as at least one of the two factors is 0 . Thus, $f_{1} \cdot f_{2} \in \mathscr{I}_{\mathscr{X}}$. This shows that $\mathscr{I}_{\mathscr{X}}$ 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 3.19 Let $f(X, Y)=Y^{2}-X^{3} \in \mathbb{C}[X, Y]$ and consider the curve $C_{f}:=\mathscr{V}_{f}(\mathbb{C})$ defined by $f$. Consider its coordinate ring $R=\mathbb{C}\left[C_{f}\right]=\mathbb{C}[X, Y] /\left(Y^{2}-X^{3}\right)$.
(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 $y=t x$, we find $0=t^{2} x^{2}-x^{3}=x^{2}\left(t^{2}-x\right)$, from which we derive $t^{2}=x$ and $y=t x=t^{3}$ because the calculations are done in the field $K$.
Moreover, we have $K=\mathbb{C}(t):=\operatorname{Frac}(\mathbb{C}[t])$. 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.

## Tensor products

## Localisation

## II. Modules

## 4 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 4.1 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 $\left(x_{i}\right)_{i \in I},\left(y_{i}\right)_{i \in I} \in \prod_{i \in I} M_{i}$ and $r \in R$, then one puts

$$
\left(x_{i}\right)_{i \in I}+\left(y_{i}\right)_{i \in I}:=\left(x_{i}+y_{i}\right)_{i \in I} \text { and } r .\left(x_{i}\right)_{i \in I}:=\left(r . x_{i}\right)_{i \in I} .
$$

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 $\left(x_{1}, x_{2}, \ldots, x_{n}\right)$.
(b) The natural map $\pi_{j}: \prod_{i \in I} M_{i} \rightarrow M_{j}$ given by $\left(x_{i}\right)_{i \in I} \mapsto x_{j}$ is called the $j$-th projection. One checks easily that $\pi_{j}$ 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 $\left(x_{i}\right)_{i \in I} \in \prod_{i \in I} M_{i}$ 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 $\left(x_{1}, x_{2}, \ldots, x_{n}\right)$ or $x_{1} \oplus x_{2} \oplus \cdots \oplus x_{n}$.
(d) The natural map $\varepsilon_{j}: M_{j} \rightarrow \bigoplus_{i \in I} M_{i}$ given by $\varepsilon(x)=\left(x_{i}\right)_{i \in I}$ with $x_{j}=x$ and $x_{i}=0$ for $i \neq j$ is called the $j$-th injection.
One checks easily that $\varepsilon_{j}$ is an injective $R$-module homomorphism.

Corollary 4.2 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 4.3 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 $\pi_{i}$ satisfies the following universal property:

For all $R$-modules $N$ together with $R$-homomorphisms $\phi_{i}: N \rightarrow M_{i}$ for $i \in I$ there is one and only one $R$-homomorphism $\phi: N \rightarrow P$ 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 $\varepsilon_{i}$ satisfies the following universal property:

For all $R$-modules $N$ together with $R$-homomorphisms $\phi_{i}: M_{i} \rightarrow N$ for $i \in I$ there is one and only one $R$-homomorphism $\phi: S \rightarrow N$ such that $\phi \circ \varepsilon_{i}=\phi_{i}$ for all $i \in I$, as in the diagram


Proof. Exercise.

## Free modules

Definition 4.4 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 $n \in \mathbb{N}, b_{1}, \ldots, b_{n} \in B$ and $r_{1}, \ldots, r_{n} \in R$ 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 $b_{1}, \ldots, b_{n} \in B$ 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 4.5 Let $R$ be a ring, let $I$ be a set and $F_{I}:=\bigoplus_{i \in I} R$. Define $\varepsilon: I \rightarrow F_{I}$ by $\varepsilon(j)=\left(x_{i}\right)_{i \in I}$, where $x_{j}=1$ and $x_{i}=0$ if $i \neq j$.
(a) Then $F_{I}$ is $R$-free with basis $B=\{\varepsilon(i) \mid i \in I\}$.
(b) $F_{I}$ together with $\varepsilon$ satisfies the following universal property:

For all $R$-modules $M$ and all maps $\delta: I \rightarrow M$ there is one and only one $R$-homomorphism $\phi: F_{I} \rightarrow M$ such that $\phi \circ \varepsilon=\delta$, as in the diagram


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

Example 4.6 (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 4.7 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 $F_{B} \rightarrow M$, where $F_{B}$ is the free $R$-module from Proposition 4.5. 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 $\delta: B \rightarrow M$ given by the identity, i.e. the inclusion of $B$ into $M$. The universal property of $F_{B}$ gives an $R$-homomorphism $\phi: F_{B} \rightarrow M$. As $\phi \circ \varepsilon=\delta, B$ is in the image of $\phi$. As the image contains a set of generators for the whole module $M$, the image is equal to $M$, i.e. $\phi$ is surjective.
(b) Then $\phi$ (from (a)) is given by $\left(r_{b}\right)_{b \in B} \mapsto \sum_{b \in B} r_{b} b$. If $\left(r_{b}\right)_{b \in B}$ is in the kernel of $\phi$, 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 $\left(r_{b}\right)_{b \in B}=0$, i.e. the injectivity.

Lemma 4.8 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 $B=\left\{b_{1}, \ldots, b_{n}\right\}$ and $C=\left\{c_{1}, \ldots, c_{m}\right\}$ with $n \geq m$ be two $R$-bases of $M$. Of course, we can express one basis in terms of the other one:

$$
b_{i}=\sum_{j=1}^{m} t_{i, j} c_{j} \text { and } c_{j}=\sum_{k=1}^{n} s_{j, k} b_{k}, \text { hence } b_{i}=\sum_{k=1}^{n}\left(\sum_{j=1}^{m} t_{i, j} s_{j, k}\right) b_{k} .
$$

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 $T=\left(t_{i, j}\right)_{1 \leq i \leq n, 1 \leq j \leq m}$ and $S=\left(s_{j, k}\right)_{1 \leq j \leq m, 1 \leq k \leq n}$ yields

$$
T \cdot S=\left(\begin{array}{ccc}
t_{1,1} & \ldots & t_{1, m} \\
\vdots & \ddots & \vdots \\
t_{m, 1} & \ldots & t_{m, m} \\
t_{m+1,1} & \ldots & t_{m+1, m} \\
\vdots & \ddots & \vdots \\
t_{n, 1} & \ldots & t_{n, m}
\end{array}\right) \circ\left(\begin{array}{cccccc}
s_{1,1} & \ldots & s_{1, m} & s_{1, m+1} & \ldots & s_{1, n} \\
\vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\
s_{m, 1} & \ldots & s_{m, m} & s_{m, m+1} & \ldots & s_{m, n}
\end{array}\right)=\mathrm{id}_{n \times n}
$$

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 4.9 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 $\phi_{n}: M_{n-1} \rightarrow M_{n}$ be an $R$-homomorphism. In other words, for all $a^{\prime}, b^{\prime} \in \mathbb{Z}$ such that $a \leq a^{\prime}<b^{\prime} \leq b$ we have the sequence

$$
M_{a^{\prime}} \xrightarrow{\phi_{a^{\prime}+1}} M_{a^{\prime}+1} \xrightarrow{\phi_{a^{\prime}+2}} M_{a^{\prime}+2} \xrightarrow{\phi_{a^{\prime}+3}} \ldots \xrightarrow{\phi_{b^{\prime}-2}} M_{b^{\prime}-2} \xrightarrow{\phi_{b^{\prime}-1}} M_{b^{\prime}-1} \xrightarrow{\phi_{b^{\prime}}} M_{b^{\prime}}
$$

Such a sequence is called a complex if $\operatorname{im}\left(\phi_{n-1}\right) \subseteq \operatorname{ker}\left(\phi_{n}\right)$ 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 $\operatorname{im}\left(\phi_{n-1}\right)=\operatorname{ker}\left(\phi_{n}\right)$ 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

$$
(*) \quad 0 \rightarrow M_{1} \rightarrow M_{2} \rightarrow M_{3} \rightarrow 0
$$

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 4.10 Let $R$ be a ring.
(a) Let $A \xrightarrow{\alpha} B$ be an $R$-homomorphism. Then $\alpha$ is injective if and only if the sequence $0 \rightarrow A \rightarrow B$ is exact.
(b) Let $B \xrightarrow{\beta} C$ be an $R$-homomorphism. Then $\beta$ is surjective if and only if the sequence $B \xrightarrow{\beta} C \rightarrow 0$ is exact.
(c) Let $0 \rightarrow A \xrightarrow{\alpha} B \xrightarrow{\beta} C \rightarrow 0$ be a complex. It is an exact sequence if and only if $C=\operatorname{im}(\beta)$ and $\alpha$ is an isomorphism from $A$ to $\operatorname{ker}(\beta)$.

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

Proposition 4.11 Let $R$ be a ring and $M_{i}, N_{i}$ for $i=1,2,3$ be $R$-modules.
(a) Let

$$
0 \rightarrow N_{1} \xrightarrow{\phi_{2}} N_{2} \xrightarrow{\phi_{3}} N_{3}
$$

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

$$
0 \rightarrow \operatorname{Hom}_{R}\left(M, N_{1}\right) \xrightarrow{\tilde{\phi}_{2}} \operatorname{Hom}_{R}\left(M, N_{2}\right) \xrightarrow{\tilde{\phi}_{3}} \operatorname{Hom}_{R}\left(M, N_{3}\right)
$$

is exact for all $R$-modules $M$. The $R$-homomorphism $\tilde{\phi}_{i}$ sends $\alpha \in \operatorname{Hom}_{R}\left(M, N_{i-1}\right)$ to $\phi_{i} \circ \alpha \in \operatorname{Hom}_{R}\left(M, N_{i}\right)$ for $i=2,3$.
(b) Let

$$
M_{1} \xrightarrow{\psi_{2}} M_{2} \xrightarrow{\psi_{3}} M_{3} \rightarrow 0
$$

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

$$
0 \rightarrow \operatorname{Hom}_{R}\left(M_{3}, N\right) \xrightarrow{\tilde{\psi}_{3}} \operatorname{Hom}_{R}\left(M_{2}, N\right) \xrightarrow{\tilde{\psi}_{2}} \operatorname{Hom}_{R}\left(M_{1}, N\right)
$$

is exact for all $R$-modules $N$. The $R$-homomorphism $\tilde{\psi}_{i}$ sends $\alpha \in \operatorname{Hom}_{R}\left(M_{i}, N\right)$ to $\alpha \circ \psi_{i} \in \operatorname{Hom}_{R}\left(M_{i-1}, N\right)$ for $i=2,3$.

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

Proof. (a) ' $\Rightarrow$ ':

- We know that $\phi_{2}$ is injective. If $\alpha \in \operatorname{ker}\left(\tilde{\phi}_{2}\right)$, then by definition $\phi_{2} \circ \alpha$ is the zero map. This implies that $\alpha$ is zero, showing that $\tilde{\phi}_{2}$ is injective.
- We know that $\phi_{3} \circ \phi_{2}$ is the zero map. This implies that $\tilde{\phi}_{3}\left(\tilde{\phi}_{2}(\alpha)\right)=\phi_{3} \circ \phi_{2} \circ \alpha$ is the zero map for all $\alpha \in \operatorname{Hom}_{R}\left(M, N_{1}\right)$. Hence, $\operatorname{im}\left(\tilde{\phi}_{2}\right) \subseteq \operatorname{ker}\left(\tilde{\phi}_{3}\right)$.
- Let $\beta \in \operatorname{ker}\left(\tilde{\phi}_{3}\right)$, i.e. $\phi_{3} \circ \beta$ is the zero map. This means $\operatorname{im}(\beta) \subseteq \operatorname{ker}\left(\phi_{3}\right)$, hence, we obtain that

$$
\phi_{2}^{-1} \circ \beta: M \xrightarrow{\beta} \operatorname{im}(\beta) \subseteq \operatorname{ker}\left(\phi_{3}\right)=\operatorname{im}\left(\phi_{2}\right) \xrightarrow{\phi_{2}^{-1}} N_{1}
$$

is an element in $\operatorname{Hom}_{R}\left(M, N_{1}\right)$. It satisfies $\tilde{\phi}_{2}\left(\phi_{2}^{-1} \circ \beta\right)=\phi_{2} \circ \phi_{2}^{-1} \circ \beta=\beta$, whence $\beta \in \operatorname{im}\left(\tilde{\phi}_{2}\right)$, showing $\operatorname{im}\left(\tilde{\phi}_{2}\right) \supseteq \operatorname{ker}\left(\tilde{\phi}_{3}\right)$.
' $\Leftarrow$ ':

- We know that $\tilde{\phi}_{2}$ is injective for all $R$-modules $M$. Choose $M:=\operatorname{ker}\left(\phi_{2}\right)$, and consider the inclusion $t: \operatorname{ker}\left(\phi_{2}\right) \rightarrow N_{1}$. Note that

$$
\tilde{\phi}_{2}(\imath)=\phi_{2} \circ \imath: \operatorname{ker}\left(\phi_{2}\right) \xrightarrow{l} N_{1} \xrightarrow{\phi_{2}} N_{2}
$$

is the zero-map. But, as $\tilde{\phi}_{2}$ is injective, it follows that already $t$ is the zero map, meaning that $\operatorname{ker}\left(\phi_{2}\right)$ is the zero module, so that $\phi_{2}$ is injective.

- We want to show $\phi_{3} \circ \phi_{2}=0$. For this take $M:=N_{1}$, and consider id $N_{N_{1}}$ the identity on $N_{1}$. We know that $\tilde{\phi}_{3} \circ \tilde{\phi}_{2}$ is the zero map. In particular,

$$
0=\tilde{\phi}_{3} \circ \tilde{\phi}_{2}\left(\mathrm{id}_{N_{1}}\right)=\phi_{3} \circ \phi_{2} \circ \mathrm{id}_{N_{1}}=\phi_{3} \circ \phi_{2} .
$$

- We want to show that $\operatorname{ker}\left(\phi_{3}\right) \subseteq \operatorname{im}\left(\phi_{2}\right)$. For this take $M:=\operatorname{ker}\left(\phi_{3}\right)$ and consider the inclusion $t: \operatorname{ker}\left(\phi_{3}\right) \rightarrow N_{2}$. Note that

$$
0=\tilde{\phi}_{3}(\imath)=\phi_{3} \circ \imath: \operatorname{ker}\left(\phi_{3}\right) \xrightarrow{\imath} N_{2} \xrightarrow{\phi_{3}} N_{3}
$$

is the zero map. We know that $\operatorname{ker}\left(\tilde{\phi}_{3}\right) \subseteq \operatorname{im}\left(\tilde{\phi}_{2}\right)$. Hence, there is some $\beta: \operatorname{ker}\left(\phi_{3}\right) \rightarrow N_{1}$ such that $t=\tilde{\phi}_{2}(\beta)=\phi_{2} \circ \beta$. In particular, the image of $t$, which is equal to $\operatorname{ker}\left(\phi_{3}\right)$, equals the image of $\phi_{2} \circ \beta$, which is certainly contained in the image of $\phi_{2}$, as was to be shown.
(b) Exercise.

Proposition 4.12 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) $\Phi: \operatorname{Hom}_{R}\left(M, \Pi_{i \in I} N_{i}\right) \rightarrow \prod_{i \in I} \operatorname{Hom}_{R}\left(M, N_{i}\right)$ and
(b) $\Psi: \operatorname{Hom}_{R}\left(\oplus_{i \in I} M_{i}, N\right) \rightarrow \prod_{i \in I} \operatorname{Hom}_{R}\left(M_{i}, N\right)$.

Proof. (a) Let $\pi_{j}: \prod_{i \in I} N_{i} \rightarrow N_{j}$ be the $j$-th projection. Define $\Phi$ as follows:

$$
\Phi\left(\varphi: M \rightarrow \prod_{i \in I} N_{i}\right):=\left(\pi_{i} \circ \varphi: M \rightarrow N_{i}\right)_{i \in I} .
$$

It is clear that $\Phi$ is an $R$-homomorphism. The rest of the statement is exactly the universal property of the product from Proposition 4.3. Indeed, suppose that we are given $\varphi_{i}: M \rightarrow N_{i}$ for each $i \in I$. Then the universal property of $\prod_{i \in I} N_{i}$ tells us that there is a unique $\varphi: M \rightarrow \prod_{i \in I} N_{i}$ 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 $\varphi$ gives us a unique preimage, which also implies injectivity.
(b) Exercise.

Lemma 4.13 Let $R$ be a ring and $M$ an $R$-module. Then the map

$$
\Phi: \operatorname{Hom}_{R}(R, M) \rightarrow M, \quad \Phi(\alpha: R \rightarrow M):=\alpha(1)
$$

is an $R$-isomorphism.

## Proof. Clear.

Proposition 4.14 Let $R$ be a ring and

be a short exact sequence. Then the following statements are equivalent:
(i) There is an $R$-homomorphism $s: C \rightarrow B$ 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 $t: B \rightarrow A$ 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 $\varphi: A \oplus C \rightarrow B$ 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 4.15 Let $R$ be a ring and $F$ a free $R$-module.
(a) Then $F$ satisfies the following universal property:

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


A module that satisfies this universal property is called projective. Thus, $F$ is projective.
(b) If $0 \rightarrow A \rightarrow B \rightarrow F \rightarrow 0$ 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 $\varepsilon: B \rightarrow F_{B}$. Let hence $\phi: M \rightarrow N$ be a surjective $R$-homomorphism and $\psi: F \rightarrow N$ an $R$ homomorphism. For each $b \in B$ choose an $m_{b} \in M$ such that $\phi\left(m_{b}\right)=\psi(b)$, using the surjectivity of $\phi$.
Consider the map $\delta: B \rightarrow M$ sending $b \in B$ to $m_{b}$. By the universal property of $F_{B}$ there exists the required $\alpha$.
(b) The universal property of (a) (applied with $\psi=\mathrm{id}_{F}$ ) shows that there is $\alpha: F \rightarrow B$ such that $\phi \circ \alpha=\mathrm{id}_{F}$. Hence, the exact sequence is split and Proposition 4.14 shows $B \cong A \oplus F$.

## 5 Tensor products

This section is only treated briefly in the lecture and the exercises. 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 5.1 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

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

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

$$
f(r m, n)=f(m, r n)
$$

In this case, we call $(P, f)$ a balanced product of $M$ and $N$.
A balanced product $\left(M \otimes_{R} N, \otimes\right)$ 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 $\phi$ : $M \otimes_{R} N \rightarrow P$ 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 5.2 Let $R$ be a ring and let $M, N$ be $R$-modules.
Then a tensor product $\left(M \otimes_{R} N, \otimes\right)$ of $M$ and $N$ over $R$ exists. If $(P, f)$ is any other tensor product, then there is a unique group isomorphism $\phi: M \otimes_{R} N \rightarrow P$ 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:

$$
\begin{array}{rr}
\left(m_{1}+m_{2}, n\right)-\left(m_{1}, n\right)-\left(m_{2}, n\right) & \forall m_{1}, m_{2} \in M, \forall n \in N \\
\left(m, n_{1}+n_{2}\right)-\left(m, n_{1}\right)-\left(m, n_{2}\right) & \forall m \in M, \forall n_{1}, n_{2} \in N \\
(r m, n)-(m, r n) & \forall r \in R, \forall m \in M, \forall n \in N .
\end{array}
$$

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

$$
\otimes: M \times N \rightarrow M \otimes_{R} N, \quad(m, n) \mapsto m \otimes n
$$

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 $\varepsilon: M \times N \rightarrow F$
denote the inclusion. We obtain a unique group homomorphism $\phi: F \rightarrow P$ such that $\phi \circ \varepsilon=f$ (draw diagram).
Claim: $G \subseteq \operatorname{ker}(\phi)$. Note first that $f(m, n)=\phi \circ \varepsilon(m, n)=\phi((m, n))$ 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 $n \in N$ :

$$
\phi\left(\left(m_{1}+m_{2}, n\right)\right)=f\left(m_{1}+m_{2}, n\right)=f\left(m_{1}, n\right)+f\left(m_{2}, n\right)=\phi\left(\left(m_{1}, n\right)\right)+\phi\left(\left(m_{2}, n\right)\right),
$$

whence $\left(m_{1}+m_{2}, n\right)-\left(m_{1}, n\right)-\left(m_{2}, n\right) \in \operatorname{ker}(\phi)$. In the same way one shows that the other two kinds of elements also lie in $\operatorname{ker}(\phi)$, implying the claim.
Due to the claim, $\phi$ induces a homomorphism $\phi: F / G \rightarrow P$ such that $\phi \circ \otimes=f$ (note that $\otimes$ is just $\varepsilon$ composed with the natural projection $F \rightarrow F / G)$.
As for the uniqueness of $\phi$. 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 $\phi$ at the generating set are prescribed and $\phi$ is hence unique.

Example 5.3 (a) Let $R=\mathbb{Z}, M=\mathbb{Z} /(m)$ and $N=\mathbb{Z} /(n)$ with $\operatorname{gcd}(m, n)=1$. 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 $1=a m+b n$. Then for all $r \in \mathbb{Z} /(m)$ and all $s \in \mathbb{Z} /(n)$ we have:

$$
\begin{aligned}
& r \otimes s=r \cdot 1 \otimes s=r(a m+b n) \otimes s=r a m \otimes s+(r b n \otimes s) \\
& \quad=0 \otimes s+r b \otimes n s=0 \otimes 0+r b \otimes 0=0 \otimes 0+0 \otimes 0=0 .
\end{aligned}
$$

(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

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

(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 $q \cdot(r \otimes n):=q r \otimes n$.
(d) Let $M$ be any $R$-module. Then $R \otimes_{R} M \xrightarrow{r \otimes m \mapsto r m} M$ is an isomorphism.

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

Next we need to consider tensor products of maps.
Proposition 5.4 Let $R$ be a ring and let $f: M_{1} \rightarrow M_{2}$ and $g: N_{1} \rightarrow N_{2}$ be $R$-homomorphisms. Then there is a unique group homomorphism

$$
f \otimes g: M_{1} \otimes_{R} N_{1} \rightarrow M_{2} \otimes_{R} N_{2}
$$

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 $M_{1} \otimes_{R} N_{1} \rightarrow M_{2} \otimes_{R} N_{2}$ with the desired property.

Lemma 5.5 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 $\left(f_{2} \otimes g_{2}\right) \circ\left(f_{1} \otimes g_{1}\right)=\left(f_{2} \circ f_{1}\right) \otimes\left(g_{2} \circ g_{1}\right)$.
Proof. $\left(f_{2} \circ f_{1}\right) \otimes\left(g_{2} \circ g_{1}\right)(m \otimes n)=\left(f_{2} \circ f_{1}(m)\right) \otimes\left(g_{2} \circ g_{1}(n)\right)=f_{2} \otimes g_{2}\left(f_{1}(m) \otimes g_{1}(n)\right)=$ $\left(f_{2} \otimes g_{2}\right) \circ\left(f_{1} \otimes g_{1}\right)(m \otimes n)$.

Corollary 5.6 Let $f: M_{1} \rightarrow M_{2}$ and $g: N_{1} \rightarrow N_{2}$ be $R$-homomorphisms.
Then $f \otimes g=\left(\mathrm{id}_{M_{2}} \otimes g\right) \circ\left(f \otimes \mathrm{id}_{N_{1}}\right)=\left(f \otimes \mathrm{id}_{N_{2}}\right) \circ\left(\mathrm{id}_{M_{1}} \otimes g\right)$.
Proof. This follows immediately from the previous lemma.

Proposition 5.7 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

$$
\Phi:\left(\bigoplus_{i \in I} M_{i}\right) \otimes_{R} N \rightarrow \bigoplus_{i \in I}\left(M_{i} \otimes_{R} N\right)
$$

such that $\left(m_{i}\right)_{i \in I} \otimes n \mapsto\left(m_{i} \otimes n\right)_{i \in I}$.
(b) Let $N_{i}$ for $i \in I$ and $M$ be $R$-modules. Then there is a unique group isomorphism

$$
\Phi: M \otimes_{R}\left(\bigoplus_{i \in I} N_{i}\right) \rightarrow \bigoplus_{i \in I}\left(M \otimes_{R} N_{i}\right)
$$

such that $m \otimes\left(n_{i}\right)_{i \in I} \mapsto\left(m \otimes n_{i}\right)_{i \in I}$.
Proof. We only prove (a), as (b) works in precisely the same way.
First we show the existence of the claimed homomorphism $\Phi$ by using the universal property of the tensor product. Define the map

$$
f:\left(\bigoplus_{i \in I} M_{i}\right) \times N \rightarrow \bigoplus_{i \in I}\left(M_{i} \otimes_{R} N\right), \quad\left(\left(m_{i}\right)_{i \in I}, n\right) \mapsto\left(m_{i}, n\right)_{i \in I}
$$

This map makes $\bigoplus_{i \in I}\left(M_{i} \otimes_{R} N\right)$ 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 $\Psi$ in the opposite direction, which will turn out to be the inverse of $\Phi$. Let $j \in I$. By $\varepsilon_{j}$ denote the embedding of $M_{j}$ into the $j$-th component of $\bigoplus_{i \in I} M_{i}$. From these we further obtain group homomorphisms $M_{j} \otimes_{R} N \xrightarrow{\varepsilon_{j} \otimes \mathrm{id}_{N}}\left(\bigoplus_{i \in I} M_{i}\right) \otimes_{R} N$. Further consider the embeddings $l_{j}$ of $M_{j} \otimes_{R}$ $N$ into the $j$-th component of $\bigoplus_{i \in I}\left(M_{i} \otimes_{R} N\right)$ from the definition of a direct sum. The universal property of direct sums now yields a homomorphism $\Psi: \bigoplus_{i \in I}\left(M_{i} \otimes_{R} N\right) \rightarrow\left(\bigoplus_{i \in I} M_{i}\right) \otimes_{R} N$ such that $\Psi \circ \imath_{j}=\varepsilon_{j} \otimes \mathrm{id}_{N}$ 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 5.8 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 5.9 Let $L / K$ be a field extension. Then $L \otimes_{K} K[X]$ is isomorphic to $L[X]$ as an L-algebra.

Lemma 5.10 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 $s(r n)=r(s n)$ for all $r \in R$, all $s \in S$ and all $n \in N$.
(a) $M \otimes_{R} N$ is an $S$-module via $s .(m \otimes n)=m \otimes(s n)$.
(b) $N \otimes_{S} P$ is an $R$-module via $r \cdot(n \otimes p)=(r n) \otimes p$.
(c) There is an isomorphism

$$
\left(M \otimes_{R} N\right) \otimes_{S} P \cong M \otimes_{R}\left(N \otimes_{S} P\right)
$$

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

Lemma 5.11 Let $R$ be a ring, let $M, N$ be $R$-modules, and let $P$ be a $\mathbb{Z}$-module.
(a) $\operatorname{Hom}_{\mathbb{Z}}(N, P)$ is an $R$-module via $(r . \varphi)(n):=\varphi(r n)$ for $r \in R, n \in N, \varphi \in \operatorname{Hom}_{\mathbb{Z}}(N, P)$.
(b) There is an isomorphism of abelian groups:

$$
\operatorname{Hom}_{R}\left(M, \operatorname{Hom}_{\mathbb{Z}}(N, P)\right) \cong \operatorname{Hom}_{\mathbb{Z}}\left(M \otimes_{R} N, P\right)
$$

(c) $\operatorname{Hom}_{\mathbb{Z}}(P, M)$ is an $R$-module via $(r . \varphi)(m):=\varphi(r m)$ for $r \in R, m \in M, \varphi \in \operatorname{Hom}_{\mathbb{Z}}(P, M)$.
(d) There is an isomorphism of abelian groups:

$$
\operatorname{Hom}_{R}\left(\operatorname{Hom}_{\mathbb{Z}}(P, M), N\right) \cong \operatorname{Hom}_{\mathbb{Z}}\left(P, M \otimes_{R} N\right)
$$

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

$$
\{\text { Balanced maps } f: M \times N \rightarrow P\} \longrightarrow \operatorname{Hom}_{R}\left(M, \operatorname{Hom}_{\mathbb{Z}}(N, P)\right)
$$

which is given by

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

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

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

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

Proposition 5.12 Let $R$ be a ring.
(a) Let $N, M_{1}, M_{2}, M_{3}$ be $R$-modules. If the sequence

$$
M_{1} \xrightarrow{f} M_{2} \xrightarrow{g} M_{3} \rightarrow 0
$$

is exact, then so is the sequence

$$
M_{1} \otimes_{R} N \xrightarrow{f \otimes \mathrm{id}} M_{2} \otimes_{R} N \xrightarrow{g \otimes \mathrm{id}} M_{3} \otimes_{R} N \rightarrow 0 .
$$

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

$$
N_{1} \xrightarrow{f} N_{2} \xrightarrow{g} N_{3} \rightarrow 0
$$

is exact, then so is the sequence

$$
M \otimes_{R} N_{1} \xrightarrow{\mathrm{id} \otimes f} M \otimes_{R} N_{2} \xrightarrow{\mathrm{id} \otimes g} M \otimes_{R} N_{3} \rightarrow 0 .
$$

One says that the functor $M \otimes_{R}$. is right-exact.
Proof. We only prove (a), since (b) works precisely in the same way. We use Proposition 4.11 and obtain the exact sequence:

$$
0 \rightarrow \operatorname{Hom}_{R}\left(M_{3}, \operatorname{Hom}_{\mathbb{Z}}(N, P)\right) \rightarrow \operatorname{Hom}_{R}\left(M_{2}, \operatorname{Hom}_{\mathbb{Z}}(N, P)\right) \rightarrow \operatorname{Hom}_{R}\left(M_{1}, \operatorname{Hom}_{\mathbb{Z}}(N, P)\right)
$$

for any $\mathbb{Z}$-module $P$. By Lemma 5.11 this exact sequence is nothing else but:

$$
0 \rightarrow \operatorname{Hom}_{\mathbb{Z}}\left(M_{3} \otimes_{R} N, P\right) \rightarrow \operatorname{Hom}_{\mathbb{Z}}\left(M_{2} \otimes_{R} N, P\right) \rightarrow \operatorname{Hom}_{\mathbb{Z}}\left(M_{1} \otimes_{R} N, P\right) .
$$

As $P$ was arbitrary, again from Proposition 4.11 we obtain the exact sequence

$$
M_{1} \otimes_{R} N \rightarrow M_{2} \otimes_{R} N \rightarrow M_{3} \otimes_{R} N \rightarrow 0,
$$

as claimed.

Definition 5.13 Let $R$ be a ring.
(a) An $R$-module $M$ is called flat over $R$ if for all injective $R$-homomorphisms

$$
\varphi: N_{1} \rightarrow N_{2}
$$

also the group homomorphism

$$
\mathrm{id}_{M} \otimes \varphi: M \otimes_{R} N_{1} \rightarrow M \otimes_{R} N_{2}
$$

is injective.
(b) An $R$-module $M$ is called faithfully flat over $R$ if $M$ is flat over $R$ and for all $R$-homomorphisms $\varphi: N_{1} \rightarrow N_{2}$, the injectivity of $\operatorname{id}_{M} \otimes \varphi$ implies the injectivity of $\varphi$.
(c) A ring homomorphism $\phi: R \rightarrow S$ is called (faithfully) flat if $S$ is (faithfully) flat as $R$-module via $\phi$.

Lemma 5.14 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 5.13 and Proposition 5.12.

Example 5.15 (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 $\mathbb{Z} /\left(p^{2}\right) \rightarrow \mathbb{Z} /(p)$, the natural projection (for $p$ a prime), which is not injective. Tensoring with $\mathbb{Q}$ kills both sides (see Example 5.3), so we get $0 \cong \mathbb{Z} /\left(p^{2}\right) \otimes_{\mathbb{Z}} \mathbb{Q} \rightarrow$ $\mathbb{Z} /(p) \otimes_{\mathbb{Z}} \mathbb{Q} \cong 0$, which is trivially injective.
(c) $\mathbb{F}_{p}$ is not flat as $\mathbb{Z}$-module (for $p$ a prime).

Reason: The homomorphism $\mathbb{Z} \xrightarrow{n \mapsto p n} \mathbb{Z}$ (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 $\mathbb{Z} /\left(p^{n}\right)$ 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 $\mathfrak{a} \subsetneq \mathbb{Z} /\left(p^{n}\right)$ is a proper ideal and $x \in \mathfrak{a}$, then $x=p y+\left(p^{n}\right)$, as otherwise $x$ would be a unit. This shows that $x \in(p)$, whence $\mathfrak{a} \subseteq(p)$.
(c) $\left\{\left.\frac{a}{b} \in \mathbb{Q} \right\rvert\, a, b \in \mathbb{Z}, \operatorname{gcd}(a, b)=1,2 \nmid b\right\}$ 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 $R^{\times}=R \backslash \mathfrak{m}$, and, equivalently, the maximal ideal is the set of non-units $\mathfrak{m}=R \backslash R^{\times}$.
Moreover, any ring $R$ is local if and only if $R \backslash R^{\times}$is an ideal of $R$.

Proof. We already know from Corollary 1.22 (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 $I:=R \backslash R^{\times}$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 $\left.d_{1} d_{2} \in D\right)$ containing 1 .
(a) An equivalence relation on $D \times R$ is defined by

$$
\left(d_{1}, r_{1}\right) \sim\left(d_{2}, r_{2}\right) \Leftrightarrow \exists s \in D: s\left(r_{1} d_{2}-r_{2} d_{1}\right)=0 .
$$

The equivalence class of $\left(d_{1}, r_{1}\right)$ 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

$$
+: D^{-1} R \times D^{-1} R \rightarrow D^{-1} R, \frac{r_{1}}{d_{1}}+\frac{r_{2}}{d_{2}}=\frac{r_{1} d_{2}+r_{2} d_{1}}{d_{1} d_{2}}
$$

and

$$
\cdot: D^{-1} R \times D^{-1} R \rightarrow D^{-1} R, \frac{r_{1}}{d_{1}} \cdot \frac{r_{2}}{d_{2}}=\frac{r_{1} r_{2}}{d_{1} d_{2}}
$$

Neutral elements are $0:=\frac{0}{1}$ and $1:=\frac{1}{1}$.
(c) The map $\mu: R \rightarrow D^{-1} R, r \mapsto \frac{r}{1}$, is a ring homomorphism with kernel $\{r \in R \mid \exists d \in$ $D: r d=0\}$. 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

$$
\left(d_{1}, r_{1}\right) \sim\left(d_{2}, r_{2}\right) \Leftrightarrow r_{1} d_{2}-r_{2} d_{1}=0
$$

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 $1 \in D^{\prime} \subset D$ is a multiplicatively closed subset, then $D^{\prime-1} R$ is the subring of $D^{-1} R$ the elements of which can be written as fractions $\frac{r}{d^{\prime}}$ with denominator $d^{\prime} \in D^{\prime}$ (exercise).
Example 6.5 Let $R$ be an integral domain. Then $D=R \backslash\{0\}$ is a multiplicatively closed subset. Then $\operatorname{Frac}(R):=D^{-1} R$ is the field of fractions of $R$.
Subexamples:
(a) For $R=\mathbb{Z}$, we have $\operatorname{Frac} \mathbb{Z}=\mathbb{Q}$.
(b) Let $K$ be a field and $R:=K\left[X_{1}, \ldots, X_{n}\right]$. Then $\operatorname{Frac} K\left[X_{1}, \ldots, X_{n}\right]=: K\left(X_{1}, \ldots, X_{n}\right)$ is the field of rational functions over $K$ (in $n$ variables). To be explicit, the elements of $K\left(X_{1}, \ldots, X_{n}\right)$ are equivalence classes written as $\frac{f\left(X_{1}, \ldots, X_{n}\right)}{g\left(X_{1}, \ldots, X_{n}\right)}$ with $f, g \in K\left[X_{1}, \ldots, X_{n}\right], g\left(X_{1}, \ldots, X_{n}\right)$ not the zero-polynomial. The equivalence relation is, of course, the one from the definition; as $K\left[X_{1}, \ldots, X_{n}\right]$ is a UFD, we may represent the class $\frac{f\left(X_{1}, \ldots, X_{n}\right)}{g\left(X_{1}, \ldots, X_{n}\right)}$ as a 'lowest fraction', by dividing numerator and denominator by their greatest common divisor.

Definition 6.6 Let $R$ be a ring and $\mathfrak{p} \triangleleft R$ be a prime ideal. Then $D:=R \backslash \mathfrak{p}$ 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 $\operatorname{Frac}(R)=R_{(0)}$ (hence the examples above can also be seen as localisations).
In that case, we also have $D=R \backslash \mathfrak{p} \subseteq R \backslash\{0\}$ and so the localisation $R_{\mathfrak{p}}$ at any prime ideal $\mathfrak{p}$ is the subring of $R_{(0)}=\operatorname{Frac}(R)$ 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 $\left\{\left.\frac{r}{d} \in \mathbb{Q} \right\rvert\, p \nmid d, \operatorname{gcd}(r, d)=1\right\}$. Here we used that $\mathbb{Z}$ is an integral domain and so $\mathbb{Z}_{(p)} \subset \operatorname{Frac}(\mathbb{Z})=\mathbb{Q}$.
(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, $D=R \backslash \mathfrak{m}=R^{\times}$, the map $\mu: R \rightarrow R_{\mathfrak{m}}$ is an isomorphism.
(d) Let $K$ be a field and consider $\mathbb{A}^{n}(K)$. Let $\underline{a}=\left(a_{1}, \ldots, a_{n}\right) \in \mathbb{A}^{n}(K)$.

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

$$
K\left[X_{1}, \ldots, X_{n}\right] \rightarrow K, \quad f \mapsto f\left(a_{1}, \ldots, a_{n}\right)
$$

Explicitly, $\mathfrak{p}=\left\{f \in K\left[X_{1}, \ldots, X_{n}\right] \mid f(\underline{a})=0\right\}$. As this homomorphism is clearly surjective (take constant polynomials as preimages), we have that $K\left[X_{1}, \ldots, X_{n}\right] / \mathfrak{p}$ is isomorphic to $K$, showing that $\mathfrak{p}$ is a maximal (and, hence, a prime) ideal.
The localisation $K\left[X_{1}, \ldots, X_{n}\right]_{\mathfrak{p}}$ is the subring of $K\left(X_{1}, \ldots, X_{n}\right)$ consisting of elements that can be written as $\frac{f\left(X_{1}, \ldots, X_{n}\right)}{g\left(X_{1}, \ldots, X_{n}\right)}$ with $g\left(a_{1}, \ldots, a_{n}\right) \neq 0$. This is the same as the set of rational functions $K\left(X_{1}, \ldots, X_{n}\right)$ that are defined in a Zariski-open neighbourhood of $a$ :

$$
\left\{\varphi \in K\left(X_{1}, \ldots, X_{n}\right) \mid \exists \underline{a} \in U \subseteq \mathbb{A}^{n}(K) \text { Zariski-open neighbourhood },\left.\varphi\right|_{U} \text { well-defined }\right\}
$$

Namely, let $\frac{f}{g} \in K\left[X_{1}, \ldots, X_{n}\right]_{\mathfrak{p}}$ 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 $\mathbb{A}^{n}(K) \backslash \mathscr{V}_{(g)}(K)$, which contains $\underline{a}$. On the other hand, if for $\frac{f}{g} \in K\left(X_{1}, \ldots, X_{n}\right)$ 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 $\frac{f}{g} \in K\left[X_{1}, \ldots, X_{n}\right]_{\mathfrak{p}}$.

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 $D:=\left\{f^{n} \mid n \in \mathbb{N}\right\}$ (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 $D=\left\{a^{n} \mid n \in \mathbb{N}\right\}$. Then

$$
D^{-1} \mathbb{Z}=\left\{q \in \mathbb{Q} \mid \exists r \in \mathbb{Z}, \exists n \in \mathbb{Z}_{\geq 0}: q=\frac{r}{a^{n}}\right\}
$$

Proposition 6.9 Let $R$ be a ring and $D \subseteq R$ a multiplicatively closed subset with $1 \in D$. Let $\mu: R \rightarrow D^{-1} R$, given by $r \mapsto \frac{r}{1}$.
(a) The map

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

is an injection, which preserves inclusions and intersections. Moreover, if $\mathfrak{b} \triangleleft D^{-1} R$ is a prime ideal, then so is $\mu^{-1}(\mathfrak{b}) \triangleleft R$.
(b) Let $\mathfrak{a} \subsetneq R$ be an ideal. Then the following statements are equivalent:
(i) $\mathfrak{a}=\mu^{-1}\left(\mathfrak{a} D^{-1} R\right)$ (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 $a \in \mathfrak{a}$ ).
(ii) $\mathfrak{a}=\mu^{-1}(\mathfrak{b})$ for some ideal $\mathfrak{b} \triangleleft D^{-1} R$ (i.e. $\mathfrak{a}$ is in the image of the map in (a)).
(iii) Every $d \in D$ is a non-zero divisor modulo $\mathfrak{a}$, meaning that if $r \in R$ and $r d \in \mathfrak{a}$, 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 $\mathfrak{p} \triangleleft R$ 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 $D=R \backslash \mathfrak{p}$. Note that $\emptyset=\mathfrak{a} \cap D=\mathfrak{a} \cap(R \backslash \mathfrak{p})$ is equivalent to $\mathfrak{a} \subseteq \mathfrak{p}$.
Let $I \subsetneq R_{\mathfrak{p}}$ be a prime ideal. Then by Proposition $6.9, \mu^{-1}(I)$ is a prime ideal of $R$ contained in $\mathfrak{p}$. As the map in (a) is a bijection and inclusion preserving, we find $I=\left(\mu^{-1}(I)\right) R_{\mathfrak{p}} \subseteq \mathfrak{p} R_{\mathfrak{p}}$. Hence, $\mathfrak{p} R_{\mathfrak{p}}$ is the only maximal ideal of $R_{\mathfrak{p}}$ (as it contains all maximal ideals).

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

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

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 $\mathfrak{a} \triangleleft R$ 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 $\mathfrak{a} \triangleleft R$ an ideal. Then $\mathfrak{a} M=\left\{\sum_{i=1}^{n} a_{i} m_{i} \mid n \in\right.$ $\mathbb{N}, a_{i} \in \mathfrak{a}, m_{i} \in M$ for $\left.i=1, \ldots, n\right\} \subseteq M$ 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 $\mathfrak{a} \triangleleft R$ 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 $A=\left(a_{i, j}\right)_{1 \leq i, j \leq n}$. It satisfies:

$$
A:=\left(\begin{array}{cccc}
a_{1,1} & a_{1,2} & \cdots & a_{1, n} \\
a_{2,1} & a_{2,2} & \cdots & a_{2, n} \\
\vdots & \vdots & \ddots & \vdots \\
a_{n, 1} & a_{n, 2} & \cdots & a_{n, n}
\end{array}\right) \cdot\left(\begin{array}{c}
m_{1} \\
m_{2} \\
\vdots \\
m_{n}
\end{array}\right)=\left(\begin{array}{c}
m_{1} \\
m_{2} \\
\vdots \\
m_{n}
\end{array}\right) .
$$

We now form the matrix $B:=\operatorname{id}_{n \times n}-A$. By the previous calculation we obtain

$$
B \cdot\left(\begin{array}{c}
m_{1} \\
m_{2} \\
\vdots \\
m_{n}
\end{array}\right)=0 .
$$

Let $B^{*}$ be the adjoint matrix, which satisfies $B^{*} \cdot B=\operatorname{det}(B) \cdot \mathrm{id}_{n \times n}$. Hence:

$$
0=B^{*} \cdot B \cdot\left(\begin{array}{c}
m_{1} \\
m_{2} \\
\vdots \\
m_{n}
\end{array}\right)=\operatorname{det}(B) \cdot\left(\begin{array}{c}
m_{1} \\
m_{2} \\
\vdots \\
m_{n}
\end{array}\right) .
$$

Hence, for all $i \in\{1, \ldots, n\}$ we find $\operatorname{det}(B) \cdot m_{i}=0$, thus $\operatorname{det}(B) \cdot M=0$. The usual rules for computing the determinant immediately show $\operatorname{det}(B)=1-a$ 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 $\bar{x}_{i}:=x_{i}+\mathfrak{a} M$ 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

$$
m+N=\sum_{i=1}^{r} a_{i}\left(m_{i}+N\right)
$$

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 $\operatorname{gcd}(a, b)=1$ and $p \nmid b$. Note that the map

$$
\pi: \mathbb{Z}_{(p)} \rightarrow \mathbb{F}_{p}, \frac{a}{b} \mapsto a b^{-1} \quad \bmod p
$$

is a well-defined surjective ring homomorphism. Its kernel is $\mathfrak{p}:=p \mathbb{Z}_{(p)}$, the elements of which are of the form $\frac{p a}{b} \in \mathbb{Q}$ with $\operatorname{gcd}(p a, b)=1$. 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 $\pi\left(v_{1}\right), \ldots, \pi\left(v_{m}\right)$ generates $\mathbb{F}_{p}^{n}$.
For this conclusion, we use that $V / \mathfrak{p} V \cong \mathbb{F}_{p}^{n}$.
A concrete example is the following one: Let $p=2$ and $R=\mathbb{Z}_{(2)}$. Then the vectors $\binom{\frac{7}{5}}{\frac{1}{11}},\binom{\frac{10}{3}}{\frac{13}{7}}$ generate $R^{2}$ because the vectors modulo 2 are $\binom{1}{0},\binom{0}{1}$, which generate $R / 2 R=\mathbb{F}_{2}^{2}$.

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

$$
\left(d_{1}, m_{1}\right) \sim\left(d_{2}, m_{2}\right) \Leftrightarrow \exists s \in D: s\left(d_{1} m_{2}-d_{2} m_{1}\right)=0 .
$$

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

$$
+: D^{-1} M \times D^{-1} M \rightarrow D^{-1} M, \frac{m_{1}}{d_{1}}+\frac{m_{2}}{d_{2}}=\frac{d_{2} m_{1}+d_{1} m_{2}}{d_{1} d_{2}}
$$

and scalar-multiplication

$$
: D^{-1} R \times D^{-1} M \rightarrow D^{-1} M, \frac{r}{d_{1}} \cdot \frac{m}{d_{2}}=\frac{r m}{d_{1} d_{2}} .
$$

The neutral element is $0:=\frac{0}{1}$.
(c) The map $\mu: M \rightarrow D^{-1} M, m \mapsto \frac{m}{1}$, is an $R$-homomorphism with kernel $\{m \in M \mid \exists d \in$ $D: d m=0\}$.

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 $\phi: M \rightarrow N$ an $R$-homomorphism.
(a) The map

$$
\phi_{D}: D^{-1} M \rightarrow D^{-1} N, \quad \frac{m}{d} \mapsto \frac{\phi(m)}{d}
$$

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 $\phi_{D}$ is injective (surjective, bijective) if $\phi$ 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 $\beta_{D} \circ \alpha_{D}\left(\frac{a}{d}\right)=\frac{\beta \circ \alpha(a)}{d}=\frac{0}{d}=0$. Let now $\frac{b}{d}$ be in the kernel of $\beta_{D}$, that is $0=\beta_{D}\left(\frac{b}{d}\right)=\frac{\beta(b)}{d}$. Hence, there is $s \in D$ such that $0=s \beta(b)=\beta(s b)$. Using the exactness of the original sequence, we find an $a \in A$ such that $\alpha(a)=s b$. Thus, $\frac{b}{d}=\frac{\alpha(a)}{s d}=\alpha_{D}\left(\frac{a}{s d}\right)$.

Lemma 6.19 Let $R$ be a ring and $\mathfrak{m}$ a maximal ideal.
(a) The natural map $\mu: R \rightarrow R_{\mathfrak{m}}, r \mapsto \frac{r}{1}$ 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 $\mathfrak{p} \triangleleft R$, the localisation $M_{\mathfrak{p}}$ is the zero module.
(iii) For all maximal ideals $\mathfrak{m} \triangleleft R$, 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 $R \xrightarrow{r \rightarrow r . m} N$. 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 4.10. Hence, $N_{\mathfrak{m}}=0$. So, $\frac{m}{1}=\frac{0}{1} \in N_{\mathfrak{m}}$. So, there is $s \in R \backslash \mathfrak{m}$ such that $s m=0$. This, however, means $s \in \mathfrak{a} \subseteq \mathfrak{m}$, contradiction.

Proposition 6.21 Let $R$ be a ring and $\varphi: M \rightarrow N$ an $R$-homomorphism. For a prime ideal $\mathfrak{p} \triangleleft R$, denote by $\varphi_{\mathfrak{p}}: M_{\mathfrak{p}} \rightarrow N_{\mathfrak{p}}$ the localisation at $\mathfrak{p}$. Then the following statements are equivalent:
(i) $\varphi$ is injective (surjective).
(ii) For all prime ideals $\mathfrak{p} \triangleleft R$, the localisation $\varphi_{\mathfrak{p}}$ is injective (surjective).
(iii) For all maximal ideals $\mathfrak{m} \triangleleft R$, 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 $\varphi$, so that we have the exact sequence

$$
0 \rightarrow K \rightarrow M \xrightarrow{\varphi} N .
$$

By Lemma 6.18, also the sequence

$$
0 \rightarrow K_{\mathfrak{m}} \rightarrow M_{\mathfrak{m}} \xrightarrow{\varphi_{\mathfrak{m}}} N_{\mathfrak{m}}
$$

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 $\varphi$ 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

$$
\psi: D^{-1} M \rightarrow D^{-1} R \otimes_{R} M, \quad \frac{m}{d} \mapsto \frac{1}{d} \otimes m
$$

is an $D^{-1} R$-isomorphism, where $D^{-1} R \otimes_{R} M$ is an $D^{-1} R$-module via $\frac{x}{d} \cdot\left(\frac{y}{s} \otimes m\right):=\left(\frac{x}{d} \frac{y}{s}\right) \otimes m$.
Proof. First we check that $\psi$ is well-defined: Let $\frac{m_{1}}{d}=\frac{m_{2}}{s}$, i.e. there is $u \in S$ such that $u\left(s m_{1}-\right.$ $\left.d m_{2}\right)=0$. Now $\frac{1}{d} \otimes m_{1}=\frac{s u}{s d u} \otimes m_{1}=\frac{1}{s d u} \otimes s u m_{1}=\frac{1}{s d u} \otimes d u m_{2}=\frac{d u}{s d u} \otimes m_{2}=\frac{1}{s} \otimes m_{2}$. That $\psi$ is an $D^{-1} R$-homomorphism is easily checked.
We now construct an inverse to $\psi$ using the universal property of the tensor product. Define

$$
f: D^{-1} R \times M \rightarrow D^{-1} M, \quad\left(\frac{x}{d}, m\right) \mapsto \frac{x m}{d} .
$$

This is a balanced map over $R$. Hence, there is a unique $\mathbb{Z}$-homomorphism $\phi: D^{-1} R \otimes M \rightarrow$ $D^{-1} M$ such that $\phi\left(\frac{x}{d} \otimes m\right)=\frac{x m}{d}$.
It is clear that $\phi$ is an $D^{-1} R$-homomorphism and that $\phi \circ \psi$ and $\psi \circ \phi$ are the identity.

## Noetherian rings and Hilbert's Basissatz

Krull dimension of rings

## Dedekind rings

Hilbert's Nullstellensatz

## 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 $M$

$$
M_{1} \subseteq M_{2} \subseteq M_{3} \subseteq \ldots
$$

(resp. $M_{1} \supseteq M_{2} \supseteq M_{3} \supseteq \ldots$ ) 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.

Example 7.2 (a) $\mathbb{Z}$ is Noetherian.
(b) More generally, every principal ideal domain (PID) is Noetherian (see Proposition 11.14).
(c) Any field $K$ is Noetherian and Artinian (since its only ideals are the trivial ones (0) and $K$, one cannot build any infinite (ascending or descending) chain).
(d) The polynomial ring in infinitely many variables $X_{1}, X_{2}, \ldots$ over any field $K$ is not Noetherian: The ideal chain

$$
\left(X_{1}\right) \subsetneq\left(X_{1}, X_{2}\right) \subsetneq\left(X_{1}, X_{2}, X_{3}\right) \subsetneq \ldots
$$

never becomes stationary.
(e) $\mathbb{Z}$ is not Artinian: The ideal chain

$$
(2) \supsetneq\left(2^{2}\right) \supsetneq\left(2^{3}\right) \supsetneq\left(2^{4}\right) \supsetneq \ldots
$$

never becomes stationary.

Lemma 7.3 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 $N \subseteq N_{1}$ $\left(\right.$ resp. $\left.N \supseteq N_{1}\right)$ 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 $S=\left\{M_{i} \mid i \in \mathbb{N}\right\}$. This set contains a maximal element $M_{N}$ by assumption. This means that the chain becomes stationary at $N$.

Proposition 7.4 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 an $R$-module.

Proof. '(i) $\Rightarrow$ (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 $\left\langle n_{1}\right\rangle \subsetneq\left\langle n_{1}, n_{2}\right\rangle \subsetneq\left\langle n_{1}, n_{2}, n_{3}\right\rangle \subsetneq \ldots$, contradicting the Noetherian-ness of $M$.
'(ii) $\Rightarrow$ (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 7.5 Let $R$ be a ring and $0 \rightarrow N \rightarrow M \rightarrow M / N \rightarrow 0$ 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) $\Rightarrow$ (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 $\bar{M}_{1} \subseteq \bar{M}_{2} \subseteq \bar{M}_{3} \subseteq$ $\ldots$ of $M / N$. Taking preimages for the natural projection $\pi: M \rightarrow M / N$ gives an ascending chain
in $M$, which by assumption becomes stationary. Because of $\pi\left(\pi^{-1}\left(\bar{M}_{i}\right)\right)=\bar{M}_{i}$, also the original chain becomes stationary.
'(ii) $\Rightarrow$ (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

$$
\left(M_{1}+N\right) / N \subseteq\left(M_{2}+N\right) / N \subseteq\left(M_{3}+N\right) / N \subseteq \ldots
$$

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 $\left(M_{i}+N\right) / N \cong$ $M_{i} /\left(M_{i} \cap N\right)$. Let now $i$ be greater than $n$ and $m$. We hence have for all $j \geq 0$ :

$$
M_{i} /\left(M_{i} \cap N\right)=M_{i+j} /\left(M_{i} \cap N\right)
$$

The other isomorphism theorem then yields:

$$
0 \cong\left(M_{i+j} /\left(M_{i} \cap N\right)\right) /\left(M_{i} /\left(M_{i} \cap N\right)\right) \cong M_{i+j} / M_{i}
$$

showing $M_{i}=M_{i+j}$.

Proposition 7.6 Let $R$ be a Noetherian (resp. Artinian) ring. Then every finitely generated $R$-module is Noetherian (resp. Artinian).

Proof. Exercise.

Proposition 7.7 - Hilbert's Basissatz. Let $R$ be a Noetherian ring and $n \in \mathbb{N}$. Then $R\left[X_{1}, \ldots, X_{n}\right]$ is a Noetherian ring. In particular, every ideal $\mathfrak{a} \triangleleft R\left[X_{1}, \ldots, X_{n}\right]$ is finitely generated.

Proof. By induction it clearly suffices to prove the case $n=1$. So, let $\mathfrak{a} \triangleleft R[X]$ be any ideal. We show that $\mathfrak{a}$ is finitely generated, which implies the assertion by Proposition 7.4.
The very nice trick is the following:

$$
\begin{aligned}
& \mathfrak{a}_{0}:=\left\{a_{0} \in R \mid a_{0} \in \mathfrak{a}\right\} \triangleleft R \\
& \text { I } \cap \\
& \mathfrak{a}_{1}:=\left\{a_{1} \in R \mid \exists b_{0} \in R: a_{1} X+b_{0} \in \mathfrak{a}\right\} \triangleleft R \\
& \text { I } \cap \\
& \mathfrak{a}_{2}:=\left\{a_{2} \in R \mid \exists b_{0}, b_{1} \in R: a_{2} X^{2}+b_{1} X+b_{0} \in \mathfrak{a}\right\} \triangleleft R \\
& \text { I } \cap
\end{aligned}
$$

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 7.4, say, $\mathfrak{a}_{i}=\left(a_{i, 1}, \ldots, a_{i, m_{i}}\right)$.
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 7.8 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 of rings

## 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 $\mathfrak{p}_{i} \triangleleft R$ is a prime ideal for all $i=0, \ldots, n$.
The height $h(\mathfrak{p})$ of a prime ideal $\mathfrak{p} \triangleleft R$ is the supremum of the lengths of all prime ideal
chains with $\mathfrak{p}_{0}=\mathfrak{p}$.
The Krull dimension $\operatorname{dim}(R)$ 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 $K\left[X_{1}, \ldots, X_{n}\right]$ 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 $l: R \rightarrow S$ the inclusion and $\mathfrak{b} \triangleleft S$ an ideal, then $\boldsymbol{l}^{-1}(\mathfrak{b})=\mathfrak{b} \cap R$ (in the obvious sense). In particular, if $\mathfrak{b}$ is a prime ideal, then so is $\boldsymbol{t}^{-1}(\mathfrak{b})=\mathfrak{b} \cap R$ (see Exercise).

Lemma 8.3 Let $R \subseteq S$ be a ring extension such that $S$ is integral over $R$. Let $\mathfrak{b} \triangleleft S$ be an ideal and $\mathfrak{a}:=\mathfrak{b} \cap R \triangleleft R$.
(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 $\mathfrak{b} \triangleleft S$ be an ideal containing $x \in \mathfrak{b}$ which is not a zero-divisor. Then $\mathfrak{b} \cap R=: \mathfrak{a} \triangleleft R$ 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

$$
0=x \cdot\left(x^{n-1}+\sum_{i=1}^{n-1} r_{i} x^{i-1}\right)
$$

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

$$
0 \neq r_{0}=-x \cdot\left(x^{n-1}+\sum_{i=1}^{n-1} r_{i} x^{i-1}\right) \in R \cap \mathfrak{b}=\mathfrak{a}
$$

(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 $\left(S / \mathfrak{P}_{1}\right) /\left(\mathfrak{P}_{2} / \mathfrak{P}_{1}\right) \cong S / \mathfrak{P}_{2}$ (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 $(0) \neq\left(\mathfrak{P}_{2} / \mathfrak{P}_{1}\right) \cap\left(R / \mathfrak{p}_{1}\right) \cong \mathfrak{p}_{2} / \mathfrak{p}_{1}$.

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 $\mathfrak{p} \triangleleft R$ be a prime ideal. Then there is a prime ideal $\mathfrak{P} \triangleleft S$ lying over $\mathfrak{p}$, by which we mean $\mathfrak{p}=\mathfrak{P} \cap R$.

Proof. Let $T:=R \backslash \mathfrak{p}$ 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:


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:

$$
\mathfrak{p}=\alpha^{-1}\left(\mathfrak{p} R_{\mathfrak{p}}\right)=\alpha^{-1}\left(\mathfrak{m} \cap R_{\mathfrak{p}}\right)=R \cap \beta^{-1}(\mathfrak{m})=R \cap \mathfrak{P}
$$

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 $\mathfrak{P}_{1} \triangleleft S$ 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 $\overline{\mathfrak{P}}_{2} \triangleleft S / \mathfrak{P}_{1}$ 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 $\pi_{S}^{-1}\left(\overline{\mathfrak{P}_{2}}\right)$ for $\pi_{S}: S \rightarrow S / \mathfrak{P}_{1}$ 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

we have

$$
\mathfrak{P}_{2} \cap R=\pi_{S}^{-1}\left(\overline{\mathfrak{P}_{2}}\right) \cap R=\pi_{R}^{-1}\left(\overline{\mathfrak{P}_{2}} \cap R / \mathfrak{p}_{1}\right)=\pi_{R}^{-1}\left(\mathfrak{p}_{2} / \mathfrak{p}_{1}\right)=\mathfrak{p}_{2}
$$

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 $K\left[X_{1}, \ldots, X_{n}\right]$ 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 $K\left[X_{1}, \ldots, X_{n}\right]$.

Proposition 8.10 - Nagata. Let $K$ be a field and $f \in K\left[X_{1}, \ldots, X_{n}\right]$ be a non-constant polynomial. Then there are $m_{2}, m_{3}, \ldots, m_{n} \in \mathbb{N}$ such that the ring extension $R:=K\left[f, z_{2}, z_{3}, \ldots, z_{n}\right] \subseteq$ $K\left[X_{1}, \ldots, X_{n}\right]=: S$ with $z_{i}:=X_{i}-X_{1}^{m_{i}} \in K\left[X_{1}, \ldots, X_{n}\right]$ is integral.

Proof. The proof works like the proof of Lemma 3.14 (a), except that now the number of variables is abitrary but finite.
First note: $S=R\left[X_{1}\right]$. Reason: The inclusion $\supseteq$ is trivial. For $n \geq i>1$, we have $X_{i}=z_{i}+X_{1}^{m_{i}} \in$ $R\left[X_{1}\right]$, 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 $h\left(X_{1}\right)=0$. We take the following general approach: For any $m_{i} \in \mathbb{N}$ for $i=2,3, \ldots, n$ the polynomial

$$
h(T):=f\left(T, z_{2}+T^{m_{2}}, z_{3}+T^{m_{3}}, \ldots, z_{n}+T^{m_{n}}\right)-f\left(X_{1}, \ldots, X_{n}\right) \in R[T]
$$

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 $R^{\times}=K\left[X_{1}, \ldots, X_{n}\right]^{\times}=K^{\times}$, 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:

$$
f\left(X_{1}, \ldots, X_{n}\right)=\sum_{\left(i_{1}, \ldots, i_{n}\right) \text { s.t. }|i| \leq d} a_{\left(i_{1}, \ldots, i_{n}\right)} X_{1}^{i_{1}} \cdots X_{n}^{i_{n}}
$$

with one of the $a_{\left(i_{1}, \ldots, i_{n}\right)} \neq 0$ for which $|i|:=\sum_{j=1}^{n} i_{j}=d$. Now we compute (letting $m_{1}=1$ )

$$
\begin{array}{r}
h(T) \\
=\left(\sum_{\left(i_{1}, \ldots, i_{n}\right) \text { s.t. } \mid i \leq d} a_{\left(i_{1}, \ldots, i_{n}\right)} T^{i_{1}}\left(z_{2}+T^{m_{2}}\right)^{i_{2}}\left(z_{3}+T^{m_{3}}\right)^{i_{3}} \ldots\left(z_{n}+T^{m_{n}}\right)^{i_{n}}\right)-f\left(X_{1}, \ldots, X_{n}\right) \\
=\sum_{\left(i_{1}, \ldots, i_{n}\right) \text { s.t. }|i| \leq d} a_{\left(i_{1}, \ldots, i_{n}\right)^{2}} T^{\sum_{j=1}^{n} i_{j} m_{j}}+\text { terms of lower degree in } T .
\end{array}
$$

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 $0 \neq a_{\left(i_{1}, \ldots, i_{n}\right)}$. 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 $K\left[X_{1}, \ldots, X_{n}\right] / I$ with $n \in \mathbb{N}$ and $I \unlhd K\left[X_{1}, \ldots, X_{n}\right]$ and ideal.

Proposition 8.12 - Noether's Normalisation Theorem. Let $K$ be a field and $R$ a non-zero affine $K$-algebra of the form $R=K\left[X_{1}, \ldots, X_{n}\right] / I$ for some $n \in \mathbb{Z}_{\geq 0}$.
Then there is $r \in \mathbb{Z}_{\geq 0}, r \leq n$ and there are elements $y_{1}, \ldots, y_{r} \in R$ such that
(1) $K\left[y_{1}, \ldots, y_{r}\right] \subseteq R$ is an integral ring extension and
(2) $y_{1}, \ldots, y_{r}$ are $K$-algebraically independent (by definition, this means that $K\left[y_{1}, \ldots, y_{r}\right]$ is isomorphic to the polynomial ring in $r$ variables).

The subring $K\left[y_{1}, \ldots, y_{r}\right]$ of $R$ is called a Noether normalisation of $R$.

Proof. We use induction on $n \in \mathbb{Z}_{\geq 0}$. If $n=0$, then $R=K$ and the result is trivially true. Assume now that the result is proved up to $n-1$. We show it for $n$ and concretely write $R=K\left[X_{1}, \ldots, X_{n}\right] / I$. Denote by $\varphi: K\left[X_{1}, \ldots, X_{n}\right] \rightarrow R$ the natural quotient morphism.
If $I=(0)$, then $R$ is isomorphic to $K\left[X_{1}, \ldots, X_{n}\right]$ and the result is trivially true. Now assume $I \neq(0)$ and let $f \in I$ be a non-constant polynomial. We apply Nagata's Normalisation Lemma 8.10 and obtain elements $z_{2}, \ldots, z_{n} \in K\left[X_{1}, \ldots, X_{n}\right]$ such that $K\left[f, z_{2}, \ldots, z_{n}\right] \subseteq K\left[X_{1}, \ldots, X_{n}\right]$ is an integral ring extension. Now, apply $\varphi$ to this extension and obtain the integral ring extension $\varphi\left(K\left[f, z_{2}, \ldots, z_{n}\right]\right) \subseteq R$, i.e. the integral ring extension $R^{\prime} \subseteq R$ with $R^{\prime}:=K\left[\varphi\left(z_{2}\right), \ldots, \varphi\left(z_{n}\right)\right]$. Now, $R^{\prime}$ is generated by $n-1$ elements, hence, by the induction hypothesis, it is an integral extension of $K\left[y_{1}, \ldots, y_{r}\right]$ with $r \leq n-1$ algebraically independent elements $y_{1}, \ldots, y_{r} \in R^{\prime} \subseteq R$. As integrality is transitive, $R$ is integral over $K\left[y_{1}, \ldots, y_{r}\right]$, 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 $K\left[X_{1}, \ldots, X_{n}\right]$ 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 $K\left[X_{1}, \ldots, X_{n-1}\right]$ is $n-1$.

Let now $m$ be the Krull dimension of $K\left[X_{1}, \ldots, X_{n}\right]$. We first prove $m \geq n$. The reason simply is that we can write down a chain of prime ideals of length $n$, namely:

$$
(0) \subsetneq\left(X_{1}\right) \subsetneq\left(X_{1}, X_{2}\right) \subsetneq\left(X_{1}, X_{2}, X_{3}\right) \subsetneq \cdots \subsetneq\left(X_{1}, X_{2}, \ldots, X_{n}\right) .
$$

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 $K\left[X_{1}, \ldots, X_{n}\right]$. We pick any non-constant $f \in \mathfrak{P}_{1}$ and apply Nagata's Normalisation Lemma 8.10, which yields elements $z_{2}, \ldots, z_{n} \in K\left[X_{1}, \ldots, X_{n}\right]$ such that $R \subseteq K\left[X_{1}, \ldots, X_{n}\right]$ with $R:=K\left[f, z_{2}, \ldots, z_{n}\right]$ 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 $\bar{R}:=K\left[f, z_{2}, \ldots, z_{n}\right] / \mathfrak{p}_{1}$. 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 $\pi: R=K\left[f, z_{2}, \ldots, z_{n}\right] \rightarrow$ $K\left[f, z_{2}, \ldots, z_{n}\right] / \mathfrak{p}_{1}=\bar{R}$ 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 $\bar{R}$ of length $m-1$. By Noether's Normalisation Theorem 8.12 it follows that the Krull dimension of $\bar{R}$ 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 $C=\mathscr{V}_{(f)}(K)$ be the resulting plane curve.
Then the Krull dimension of the coordinate ring $K[C]=K[X, Y] / \mathscr{I}_{C}$ is equal to 1 .
Proof. This is now immediate by Lemma 3.14.
We include an easy lemma on Krull dimensions, which enables us to give another proof of Proposition 3.13.

Lemma 8.15 Let $\varphi: R \rightarrow S$ 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 $\varphi$ is an isomorphism.

Proof. (a) $\varphi^{-1}$ of a prime ideal is a prime ideal. Moreover, if $\varphi^{-1}(\mathfrak{a})=\varphi^{-1}(\mathfrak{b})$, then we have $\varphi\left(\varphi^{-1}(\mathfrak{a})\right)=\varphi\left(\varphi^{-1}(\mathfrak{b})\right)$, hence, $\mathfrak{a}=\mathfrak{b}$ using here the surjectivity of $\varphi$. 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 $\varphi$. It is contained in any $\varphi^{-1}(\mathfrak{p})$. Hence, if $\varphi$ 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 3.13. (This proof is shorter, but depends on Krull dimensions.) The Krull dimensions of $K[X, Y] /(f)$ and $K[C]=K[X, Y] / \mathscr{I}_{C}$ are both equal to 1 due to Lemma 3.14. As $f$ is irreducible, $(f)$ is prime and $K[X, Y] /(f)$ is an integral domain. Consequently, the natural projection $K[X, Y] /(f) \rightarrow K[X, Y] / \mathscr{I}_{C}$ is an isomorphism by Lemma 8.15 (b). Thus $(f)=\mathscr{I}_{C}$.

## 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:

$$
0=\left(\frac{a}{b}\right)^{n}+\frac{c_{n-1}}{d}\left(\frac{a}{b}\right)^{n-1}+\frac{c_{n-2}}{d}\left(\frac{a}{b}\right)^{n-2}+\cdots+\frac{c_{1}}{d} \frac{a}{b}+\frac{c_{0}}{d}
$$

with $c_{0}, c_{1}, \ldots, c_{n-1} \in R$ and $d \in D$. Multiplying by $d^{n}$ we obtain:

$$
0=\left(\frac{a d}{b}\right)^{n}+c_{n-1}\left(\frac{a d}{b}\right)^{n-1}+c_{n-2} d\left(\frac{a d}{b}\right)^{n-2}+\cdots+c_{1} d^{n-2} \frac{a d}{b}+c_{0} d^{n-1}
$$

showing that $\frac{d a}{b}$ is integral over $R$. As $R$ is integrally closed, it follows that $\frac{d a}{b}$ 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 $\mathfrak{p} \triangleleft R$.
(iii) $R_{\mathfrak{m}}$ is integrally closed for all maximal ideals $\mathfrak{m} \triangleleft R$.

Proof. '(i) $\Rightarrow$ (ii)': Lemma 9.1.
'(ii) $\Rightarrow$ (iii)': Trivial because every maximal ideal is prime.
'(iii) $\Rightarrow$ (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 $l: R \hookrightarrow \tilde{R}$ be the natural embedding. Of course, $R$ is integrally closed if and only if $t$ is an isomorphism. By Proposition 6.21 this is the case if and only if the localisation $\imath_{\mathrm{m}}: R_{\mathrm{m}} \hookrightarrow \tilde{R}_{\mathrm{m}}$ 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 $\mathfrak{m} \triangleleft R$ its maximal ideal.
(a) $\mathfrak{m}^{n} / \mathfrak{m}^{n+1}$ is an $R / \mathfrak{m}$-vector space for the natural operation.
(b) $\operatorname{dim}_{R / \mathfrak{m}}\left(\mathfrak{m} / \mathfrak{m}^{2}\right)$ is the minimal number of generators of the ideal $\mathfrak{m}$.
(c) If $\operatorname{dim}_{R / \mathfrak{m}}\left(\mathfrak{m} / \mathfrak{m}^{2}\right)=1$, then $\mathfrak{m}$ is a principal ideal and there are no ideals $\mathfrak{a} \triangleleft R$ 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 the Krull dimension of $R$ equals $\operatorname{dim}_{R / \mathfrak{m}}\left(\mathfrak{m} / \mathfrak{m}^{2}\right)$.

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 $\left(x^{n}\right)$ for some $n \in \mathbb{N}$.
(b) Every non-zero $r \in R$ can be uniquely written as $u x^{n}$ 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 $M:=\bigcap_{n \in \mathbb{N}} \mathfrak{m}^{n}=\bigcap_{n \in \mathbb{N}}\left(x^{n}\right)$.
We show $M=0$. This is trivial if there is an integer $n \geq 1$ such that $x^{n}=0$. We now assume that no power of $x$ equals 0 . Let $y \in M$. We can write it as $y=x r$ with some $r \in R$ because $y \in \mathfrak{m}$. We show $r \in M$. For that, we assume the opposite $r \notin M$. Then there is a minimal integer $n \geq 1$ such that $r \notin \mathfrak{m}^{n}=\left(x^{n}\right)$. Consequently, $r=u x^{n-1}$ with a unit $u \in R^{\times}=R \backslash \mathfrak{m}$. Then on the one hand $y=x r=u x^{n}$ and on the other hand $y=v x^{n+1} \in \mathfrak{m}^{n+1} \subseteq M$ with some $v \in R$. This leads to $0=x^{n}(u-v x)$. As $x^{n} \neq 0$, we conclude $u-v x \in \mathfrak{m}$, leading to $u \in \mathfrak{m}$, the desired contradiction, showing $r \in M$ and, hence $y=x r \in \mathfrak{m} M$. This shows $\mathfrak{m} M=M$. Since $M$ is an ideal in a Noetherian ring, it is finitely generated, so Nakayama's Lemma (Proposition 6.14) implies that $M=0$.
Now we show (b) and let $0 \neq r \in R$. As $R=\left(x^{0}\right) \supset(x) \supset\left(x^{2}\right) \supset\left(x^{3}\right) \supset \cdots$ and because of the preparation, there is a maximal $n$ such that $r \in\left(x^{n}\right)$. So, we can write $r=v x^{n}$ 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 $r \in\left(x^{n+1}\right)$, contradicting the maximality of $n$.
Let $0 \neq \mathfrak{a} \triangleleft R$ 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 $\mathfrak{a}=\left(x^{n}\right)$ 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, $\mathfrak{a} \triangleleft R$ an ideal and $M$ a finitely generated $R$-module. Let $\varphi: M \rightarrow M$ 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

$$
\varphi\left(x_{i}\right)=\sum_{j=1}^{n} a_{i, j} x_{j}
$$

Consider the matrix

$$
D(T):=T \cdot \operatorname{id}_{n \times n}-\left(a_{i, j}\right)_{1 \leq i, j \leq n} \in \operatorname{Mat}_{n}(R[T])
$$

Note that $D(T)$ is made precisely in such a way that

$$
D(\varphi)\left(\begin{array}{c}
x_{1} \\
x_{2} \\
\vdots \\
\vdots \\
x_{n}
\end{array}\right)=\left(\left(\left(\begin{array}{cccc}
\varphi & 0 & \cdots & 0 \\
0 & \varphi & \cdots & 0 \\
\vdots & \vdots & \ddots & \vdots \\
0 & 0 & \cdots & \varphi
\end{array}\right)-\left(\begin{array}{cccc}
a_{1,1} & a_{1,2} & \cdots & a_{1, n} \\
a_{2,1} & 1 & c_{2,2} & \cdots \\
2_{2, n} \\
\vdots & \vdots & \ddots & \vdots \\
a_{n, 1} & a_{n, 2} & \cdots & a_{n, n}
\end{array}\right)\right)\left(\begin{array}{c}
x_{1} \\
x_{2} \\
\vdots \\
x_{n}
\end{array}\right)=\left(\begin{array}{c}
\varphi\left(x_{1}\right) \\
\varphi\left(x_{2}\right) \\
\vdots \\
\varphi\left(x_{n}\right)
\end{array}\right)-\left(\begin{array}{c}
\varphi\left(x_{1}\right) \\
\varphi\left(x_{2}\right) \\
\vdots \\
\varphi\left(x_{n}\right)
\end{array}\right)=0 .\right.
$$

If we multiply with the adjoint matrix $D(T)^{*}$, we obtain $D(T)^{*} D(T)=\operatorname{det}(D(T))$ id $_{n \times n}$. This yields

$$
0=\operatorname{det}(D(\varphi))\left(\begin{array}{c}
x_{1} \\
x_{2} \\
\vdots \\
x_{n}
\end{array}\right)=D(\varphi)^{*} D(\varphi)\left(\begin{array}{c}
x_{1} \\
x_{2} \\
\vdots \\
x_{n}
\end{array}\right) .
$$

Consequently, $\operatorname{det}(D(\varphi))$ is zero on all generators. We are done because the determinant $\operatorname{det}(D(\varphi))$ 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 $(0) \subsetneq I \triangleleft R$ be an ideal. Then there is $n \in \mathbb{N}$ such that $\mathfrak{m}^{n} \subseteq I$.

Proof. Let $\Sigma$ be the set of all ideals $I \triangleleft R$ such that $\mathfrak{m}^{n} \nsubseteq I$ for all $n \in \mathbb{N}$. This set is nonempty as $(0) \in \Sigma$ because $\mathfrak{m}^{n} \neq(0)$ since $R$ is an integral domain of non-zero Krull dimension. Consequently, $\Sigma$ 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 $\mathfrak{m}$, which are the only prime ideals in $R$. Hence, $J$ contains a product $x y$ with $x, y \in R$ without containing $x$ and $y$ individually. Due to the maximality of $J$ among the elements of $\Sigma$, the ideals $(J, x)$ and $(J, y)$ do not lie in $\Sigma$. 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) $\Rightarrow$ (iii)': This was proved in Proposition 9.5.
'(iii) $\Rightarrow$ (i)': Principal ideal domains are UFDs (Proposition 11.21) and UFDs are integrally closed (Proposition 2.28).
'(i) $\Rightarrow$ (ii)': It suffices to show that $\mathfrak{m}$ is a principal ideal because this means that $\operatorname{dim}_{R / \mathfrak{m}}\left(\mathfrak{m} / \mathfrak{m}^{2}\right)=$ 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 $\mathfrak{m}^{n-1} \nsubseteq(a)$. Take any $b \in \mathfrak{m}^{n-1} \backslash(a)$. 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 $\frac{m}{x}=\frac{m b}{a}$ and $m b \in \mathfrak{m m}^{n-1}=\mathfrak{m}^{n} \subseteq(a)$.
- $x^{-1} \notin R$ because otherwise $r=x^{-1}=\frac{b}{a} \in R$ would imply $b=r a \in(a)$.
- $x^{-1} \mathfrak{m} \nsubseteq \mathfrak{m}$ because of the following: Assume the contrary, i.e. $x^{-1} \mathfrak{m} \subseteq \mathfrak{m}$. Then we have the $R$-homomorphism $\varphi: \mathfrak{m} \xrightarrow{m \mapsto m x^{-1}} \mathfrak{m}$. 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

$$
0=\left(x^{-n}+a_{n-1} x^{-(n-1)}+a_{n-2} x^{-(n-2)}+\ldots a_{1} x^{-1}+a_{0}\right) \mathfrak{m}
$$

As $R$ is an integral domain and $\mathfrak{m} \neq 0$ because the Krull dimension is not 0 , we obtain

$$
0=x^{-n}+a_{n-1} x^{-(n-1)}+a_{n-2} x^{-(n-2)}+\ldots a_{1} x^{-1}+a_{0}
$$

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 $\mathfrak{m}=R x=(x)$, 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 $\mathfrak{m} \triangleleft R$.
(iv) $R_{\mathfrak{m}}$ is regular for all maximal ideals $\mathfrak{m} \triangleleft R$.
(v) $R_{\mathfrak{m}}$ is a principal ideal domain for all maximal ideals $\mathfrak{m} \triangleleft R$.

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:

$$
\begin{aligned}
& T_{C,(a, b)}(X, Y)= \\
& \left.\quad \frac{\partial f}{\partial X}\right|_{(a, b)}(X-a)+\left.\frac{\partial f}{\partial Y}\right|_{(a, b)}(Y-b)+\text { terms of higher degree in }(X-a) \text { and }(Y-b)
\end{aligned}
$$

Definition 9.12 Let $K$ be a field, $f \in K[X, Y]$ a non-constant irreducible polynomial and $C=\mathscr{V}_{(f)}(K)$ the associated plane curve.
Let $(a, b) \in C$ be a point. The tangent equation to $C$ at $(a, b)$ is defined as

$$
T_{C,(a, b)}(X, Y)=\left.\frac{\partial f}{\partial X}\right|_{(a, b)}(X-a)+\left.\frac{\partial f}{\partial Y}\right|_{(a, b)}(Y-b) \in K[X, Y]
$$

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 $\mathscr{V}_{C,(a, b)}(K)$ 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 $\frac{\partial f}{\partial X}=-3 X^{2}$ and $\frac{\partial f}{\partial X}=2 Y$. 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 $\frac{\partial f}{\partial X}=-3 X^{2}-2 X$ and $\frac{\partial f}{\partial X}=2 Y$. 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, $C=\mathscr{V}_{(f)}(K)$ 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 a field, $f \in K[X, Y]$ a non-constant irreducible polynomial and $C=\mathscr{V}_{(f)}(K)$ the associated plane curve. Assume that $C$ is infinite (this is automatic if $K$ is algebraically closed) and let $K[C]=K[X, Y] /(f(X, Y))$ be the coordinate ring of $C$ (see Proposition 3.13).
Let $(a, b) \in C$ be a point and $\mathfrak{m}=(X-a+(f), Y-b+(f)) \triangleleft K[C]$ be the corresponding maximal ideal (see Lemma 3.12).
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 as $K[C] / \mathfrak{m}$-vector space.

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 $X^{2}+(f), Y^{2}+(f), X Y+(f)$, 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 $K[C]_{\mathfrak{m}} /\left(\mathfrak{m} K[C]_{\mathfrak{m}}\right) \cong K[C] / \mathfrak{m}$ and $\left(\mathfrak{m} K[C]_{\mathfrak{m}} /\left(\mathfrak{m} K[C]_{\mathfrak{m}}\right)^{2} \cong \mathfrak{m} / \mathfrak{m}^{2}\right.$ 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:

$$
X+(f)=\frac{1}{\alpha}(-\beta Y-\text { higher terms }+(f)) \equiv-\frac{\beta}{\alpha} Y+(f) \quad\left(\bmod \mathfrak{m}^{2}\right)
$$

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 $K[C]_{\mathrm{m}}$ 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 $L=K\left[a_{1}, \ldots, a_{n}\right]$ (that is, the $K$-algebra homomorphism $K\left[X_{1}, \ldots, X_{n}\right] \xrightarrow{X_{i} \mapsto a_{i}} L$ is surjective).
Then $L / K$ is finite and algebraic.
Proof. Let $L=K\left[a_{1}, \ldots, a_{n}\right]$. 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 $L / K\left[y_{1}, \ldots, y_{r}\right]$ is an integral extension and $K\left[y_{1}, \ldots, y_{r}\right]$ 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 $K\left[y_{1}, \ldots, y_{r}\right]$, so that it satisfies a monic equation of the form

$$
y_{1}^{-n}+f_{n-1}\left(y_{1}, \ldots, y_{r}\right) y_{1}^{-n+1}+\cdots+f_{0}\left(y_{1}, \ldots, y_{r}\right)=0
$$

where $f_{i}\left(y_{1}, \ldots, y_{r}\right) \in K\left[y_{1}, \ldots, y_{r}\right]$. Multiplying through with $y^{n}$ we get

$$
1+f_{n-1}\left(y_{1}, \ldots, y_{r}\right) y_{1}+\cdots+f_{0}\left(y_{1}, \ldots, y_{r}\right) y_{1}^{n}=0
$$

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 $\mathfrak{a} \triangleleft K\left[X_{1}, \ldots, X_{n}\right]$ a proper ideal.
(a) The maximal ideals $\mathfrak{m} \triangleleft K\left[X_{1}, \ldots, X_{n}\right]$ are precisely $\left(X_{1}-a_{1}, \ldots, X_{n}-a_{n}\right)$ for a point $\left(a_{1}, \ldots, a_{n}\right) \in K^{n}$.
(b) The maximal ideals $\mathfrak{m} \triangleleft K\left[X_{1}, \ldots, X_{n}\right]$ which contain $\mathfrak{a}$ are $\left(X_{1}-a_{1}, \ldots, X_{n}-a_{n}\right)$ for a point $\left(a_{1}, \ldots, a_{n}\right) \in \mathscr{V}_{\mathfrak{a}}(K)$.
(c) The maximal ideals of $K\left[X_{1}, \ldots, X_{n}\right] / \mathfrak{a}$ are precisely $\left(X_{1}-a_{1}+\mathfrak{a}, \ldots, X_{n}-a_{n}+\mathfrak{a}\right)$ for a point $\left(a_{1}, \ldots, a_{n}\right) \in \mathscr{V}_{\mathfrak{a}}(K)$.

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 $\mathfrak{m} \triangleleft$ $K\left[X_{1}, \ldots, X_{n}\right]$ is maximal then the quotient $K\left[X_{1}, \ldots, X_{n}\right] / \mathfrak{m}$ is a finite algebraic field extension of $K$ by Proposition 9.16, hence, equal to $K$ because $K$ is algebraically closed. Consequently, denoting $a_{i}:=\pi\left(X_{i}\right)$ for $i=1, \ldots, n$ with $\pi: K\left[X_{1}, \ldots, X_{n}\right] \xrightarrow{\text { natural projection }} K\left[X_{1}, \ldots, X_{n}\right] / \mathfrak{m} \cong K$, we find (special case of Lemma 3.12) that $\mathfrak{m}=\left(X_{1}-a_{1}, \ldots, X_{n}-a_{n}\right)$.
(b) Let $\mathfrak{m}=\left(X_{1}-a_{1}, \ldots, X_{n}-a_{n}\right)$, so that $\left\{\left(a_{1}, \ldots, a_{n}\right)\right\}=\mathscr{V}_{\mathfrak{m}}(K)$. We have:

$$
\mathfrak{a} \subseteq \mathfrak{m} \Leftrightarrow\left\{\left(a_{1}, \ldots, a_{n}\right)\right\}=\mathscr{V}_{\mathfrak{m}}(K) \subseteq \mathscr{V}_{\mathfrak{a}}(K) \Leftrightarrow\left(a_{1}, \ldots, a_{n}\right) \in \mathscr{V}_{\mathfrak{a}}(K) .
$$

(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 $\mathfrak{m} \triangleleft K[C]$; 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 $\mathfrak{a} \triangleleft K\left[X_{1}, \ldots, X_{n}\right]$ be a proper ideal. Then $\mathscr{V}_{\mathfrak{a}}(K) \neq \emptyset$.

Proof. Let $\mathfrak{m} \triangleleft K\left[X_{1}, \ldots, X_{n}\right]$ be a maximal ideal containing $\mathfrak{a}$. By Corollary 9.17 (b), $\mathfrak{m}$ corresponds to a point $\left(a_{1}, \ldots, a_{n}\right) \in \mathscr{V}_{\mathfrak{a}}(K)$, showing the non-emptyness of this set.
(R) 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 $\phi: K\left[X_{1}, \ldots, X_{n}\right] \xrightarrow{X_{i} \mapsto a_{i}} L$. Its kernel $\mathfrak{m}:=\operatorname{ker}(\phi)$ is a maximal ideal, since $L$ is a field. By Proposition 10.1, we have $\mathscr{V}_{\mathfrak{m}}(\bar{K}) \neq \emptyset$. Let $\left(b_{1}, \ldots, b_{n}\right)$ be an element of $\mathscr{V}_{\mathfrak{m}}(\bar{K})$, which gives rise to the $K$-algebra homomorphism $\psi: K\left[X_{1}, \ldots, X_{n}\right] \xrightarrow{X_{i} \mapsto b_{i}} \bar{K}$. Note that $\mathfrak{m}$ is contained in the kernel of $\psi$ (we have $f\left(b_{1}, \ldots, b_{n}\right)=0$ for all $f \in \mathfrak{m}$ ), whence they are equal. Consequently, $K \subseteq L \subseteq \bar{K}$, and we conclude that $L / K$ is algebraic. It is finite because it is generated by finitely many algebraic elements.

Definition 10.2 Let $R$ be a ring and $\mathfrak{a} \triangleleft R$ and ideal. The radical (ideal) of $\mathfrak{a}$ is defined as

$$
\sqrt{\mathfrak{a}}:=\left\{r \in R \mid \exists n \in \mathbb{N}: r^{n} \in \mathfrak{a}\right\} .
$$

An ideal $\mathfrak{a}$ is called a radical ideal if $\mathfrak{a}=\sqrt{\mathfrak{a}}$.
The Jacobson radical of $\mathfrak{a}$ is defined as

$$
J(\mathfrak{a})=\bigcap_{\mathfrak{a} \subseteq \mathfrak{m} \triangleleft R \text { maximal }} \mathfrak{m}
$$

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 10.3 Let $K$ be a field and $\mathfrak{a} \triangleleft K\left[X_{1}, \ldots, X_{n}\right]$ an ideal.
Then $\mathscr{V}_{\mathfrak{a}}(L)=\mathscr{V}_{\sqrt{\mathfrak{a}}}(L)$ for all field extensions $L / K$.
Proof. The inclusion $\supseteq$ is trivial because of $\mathfrak{a} \subseteq \sqrt{\mathfrak{a}}$. Let now $\left(a_{1}, \ldots, a_{n}\right) \in \mathscr{V}_{\mathfrak{a}}(L)$, that is, $f\left(a_{1}, \ldots, a_{n}\right)=0$ 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 $g\left(a_{1}, \ldots, a_{n}\right)^{m}=0$. Since we are in an integral domain, this implies $g\left(a_{1}, \ldots, a_{n}\right)=0$, showing the inclusion $\subseteq$.

Proposition 10.4 - General Hilbert's Nullstellensatz. Let $K$ be a field, $R$ an affine $K$ algebra, $\mathfrak{a} \triangleleft R$ an ideal. Then $\sqrt{\mathfrak{a}}=J(\mathfrak{a})$.

Proof. ' $\subseteq$ ': Let $\mathfrak{m} \triangleleft R$ 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 $f \in R \backslash \sqrt{\mathfrak{a}}$. 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 $D=\left\{\bar{f}^{n} \mid n \in \mathbb{N}\right\} \subseteq R / \mathfrak{a}=: \bar{R}$ is multiplicatively closed and does not contain 0 (the zero of $\bar{R}=R / \mathfrak{a}$, of course). We write $\bar{f}$ for the class $f+\mathfrak{a} \in \bar{R}$. It is a unit in $D^{-1} \bar{R}$ because we are allowing $\bar{f}$ in the denominator.
Let $\overline{\mathfrak{q}}$ be a maximal ideal of $D^{-1} \bar{R}$. As $\bar{f}$ is a unit, $\bar{f} \notin \overline{\mathfrak{q}}$. As $R$ is an affine $K$-algebra, so is the field $D^{-1} \bar{R} / \overline{\mathfrak{q}}=: L$ (we modded out by a maximal ideal). Proposition 9.16 yields that $L / K$ is a finite field extension.
Note that the ring $\bar{R} /(\bar{R} \cap \overline{\mathfrak{q}})$ contains $K$ and lies in $L$. Due to the finiteness of $L / K$, this ring is itself a field, so that $\bar{R} \cap \overline{\mathfrak{q}}$ is a maximal ideal of $\bar{R}$.
Recall that $\bar{f} \notin \overline{\mathfrak{q}}$, so $f$ does not lie in the maximal ideal $\bar{R} \cap \overline{\mathfrak{q}}$.
Set $\mathfrak{q}:=\pi^{-1}(\overline{\mathfrak{q}})$ with the natural projection $\pi: R \rightarrow \bar{R}=R / \mathfrak{a}$. It is a maximal ideal containing $\mathfrak{a}$, but $f \notin \mathfrak{q}$. Consequently, $f \notin J(\mathfrak{a})$.

Theorem 10.5 - Hilbert's Nullstellensatz. Let $K$ be an algebraically closed field and consider an ideal $\mathfrak{a} \unlhd K\left[X_{1}, \ldots, X_{n}\right]$.
Then $\mathscr{I}_{V_{\mathfrak{a}}(K)}=\sqrt{\mathfrak{a}}$.
In particular, the radical ideals of $K\left[X_{1}, \ldots, X_{n}\right]$ are in bijection with the affine algebraic sets in $\mathbb{A}^{n}(K)$. More precisely, the maps

$$
\begin{aligned}
\left\{\mathfrak{a} \unlhd K\left[X_{1}, \ldots, X_{n}\right] \mid \mathfrak{a}=\sqrt{\mathfrak{a}}\right\} & \leftrightarrows\left\{\mathscr{V} \subseteq \mathbb{A}^{n}(K) \mid \mathscr{V} \text { affine algebraic set }\right\} \\
\mathfrak{a} & \stackrel{\Phi}{\mapsto} \mathscr{V}_{\mathfrak{a}}(K) \\
\mathscr{I}_{\mathscr{V}} & \underset{\Psi}{\mathscr{V}}
\end{aligned}
$$

are inverses to each other and thus bijections.
Proof. ' $\supseteq$ ': By Lemmata 3.11 and 10.3 we have $\sqrt{\mathfrak{a}} \subseteq \mathscr{I}_{V_{\sqrt{\mathfrak{a}}}(K)}=\mathscr{I}_{V_{\mathfrak{a}}(K)}$.
' $\subseteq$ ': Let $\mathfrak{m}$ be a maximal ideal of $K\left[X_{1}, \ldots, X_{n}\right]$ containing $\mathfrak{a}$. By Corollary 9.17 we know $\mathfrak{m}=\left(X_{1}-a_{1}, \ldots, X_{n}-a_{n}\right)$ for some $\left(a_{1}, \ldots, a_{n}\right) \in \mathscr{V}_{\mathfrak{a}}(K)$. We have

$$
\mathscr{I}_{\mathscr{V}_{\mathfrak{a}}(K)} \subseteq \mathscr{I}_{\mathscr{V}_{\mathfrak{m}}(K)}=\left\{f \in K\left[X_{1}, \ldots, X_{n}\right] \mid f(\underline{a})=0\right\}=\mathfrak{m}
$$

Consequently, $\mathscr{I}_{V_{\mathfrak{a}}(K)} \subseteq J(\mathfrak{a})=\sqrt{\mathfrak{a}}$, using Proposition 10.4.
The final statement follows like this:

$$
\mathscr{X}=\mathscr{V}_{\mathfrak{a}}(K) \mapsto \mathscr{I}_{V_{\mathfrak{a}}(K)}=\sqrt{\mathfrak{a}} \mapsto \mathscr{V}_{\sqrt{\mathfrak{a}}}(K)=\mathscr{V}_{\mathfrak{a}}(K)=\mathscr{X}
$$

and

$$
\mathfrak{a}=\sqrt{\mathfrak{a}} \mapsto \mathscr{V}_{\mathfrak{a}}(K) \mapsto \mathscr{I}_{V_{\mathfrak{a}}(K)}=\sqrt{\mathfrak{a}} .
$$

This shows the correspondence.
Finally let us prove that the vanishing ideal $\mathscr{I}_{C}$ 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 3.13 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 10.5 yields $\mathscr{I}_{C}=\sqrt{(f)}=(f)$.

## IV. Appendix

## 11 Appendix: Background on rings

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.

## 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 11.1 A set $R$, containing two elements 0 and 1 (not necessarily distinct), together with maps

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

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 $(R \backslash\{0\}, \cdot, 1)$ 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 $(R \backslash\{0\}, \cdot)$ is an abelian semi-group, then $R$ is called a commutative ring. Most (but not all) of the lecture only treats commutative rings; hence, the name Commutative Algebra. By a ring, we usually mean a commutative ring.
If $R$ is a commutative ring and if in addition $(R \backslash\{0\}, \cdot, 1)$ 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 $: S \times S \rightarrow S,(s, t) \mapsto s \cdot t$ 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 11.2 (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 $\bmod n$.
(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 $\left(a_{1}, b_{1}\right)+\left(a_{2}, b_{2}\right)=\left(a_{1}+a_{2}, b_{1}+b_{2}\right)$ and $\left(a_{1}, b_{1}\right)$. $\left(a_{2}, b_{2}\right)=\left(a_{1} \cdot a_{2}, b_{1} \cdot b_{2}\right)$.

## Integral domains

Proposition 11.3 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 $r \in R \backslash\left(R^{\times} \cup\{0\}\right)$. 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 $r=s t$ 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. $s=r u$ for some $u \in R$. Then we have $r=s t=r u t$, whence $r(1-u t)=0$, which implies $1-u t=0$ 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 11.4 Let $R$ and $S$ be (not necessarily commutative) rings. We say that $S$ is an $R$-algebra if there is a ring homomorphism $\varphi: R \rightarrow S$ such that $\varphi(R) \subseteq \mathscr{Z}(S)$, where $\mathscr{Z}(S)=\{s \in S \mid t s=s t \forall t \in S\}$ is the centre of $S$ (note that the condition $\varphi(R) \subseteq \mathscr{Z}(S)$ 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 11.5 Let $K$ be a field. Then the polynomial ring $K[X]$ is a $K$-algebra.
Consider $\operatorname{End}_{K}(V)$ for a $K$-vector space $V$. Then $\operatorname{End}_{K}(V)$ is a $K$-algebra ( $K$ embeds into the scalar matrices, which are equal to the centre of $\left.\operatorname{End}_{K}(V)\right)$.

## Ideals

Example 11.6 (a) Let $R$ be a ring. Then $\{0\},(1)=R$ are both trivially ideals.
(b) Let $\varphi: R \rightarrow S$ be a ring homomorphism. Then $\operatorname{ker}(\varphi)$ is an ideal of $R$.
(c) $\{n m \mid m \in \mathbb{Z}\} \triangleleft \mathbb{Z}$.
(d) $(n, m)=(g)$ with $g$ the greatest common divisor of $n, m \in \mathbb{Z}$.
(e) $(n) \cap(m)=(\operatorname{lcm}(n, m))$.

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

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

It is clear that both are ideals.

## On maximal ideals

Proof of Proposition 1.21. 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 $\mathscr{M}:=\{\mathfrak{a} \subsetneq R$ ideal $\}$ be the set of all proper ideals of $R$. Of course, $(0) \in \mathscr{M}$ (here we use that $R$ is not the zero ring), so $\mathscr{M} \neq \emptyset$.
Inclusion $\subseteq$ gives a partial ordering on $\mathscr{M}:$ by definition this means:

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

But, for general $\mathfrak{a}, \mathfrak{b} \in \mathscr{M}$, we do not necessarily have $\mathfrak{a} \subseteq \mathfrak{b}$ or $\mathfrak{b} \subseteq \mathfrak{a}$. A subset $\left(\mathfrak{a}_{i}\right)_{i \in I} \subseteq \mathscr{M}$ (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 $\mathfrak{a}_{j} \subseteq \mathfrak{a}_{i}$.
 $\mathfrak{a} \subseteq \mathscr{M}$ 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 $r x \in \mathfrak{a}_{i}$, thus $r x \in \mathfrak{a}$, 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, $\mathfrak{a} \in \mathscr{M}$, 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, $\mathscr{M}$ has a maximal element, i.e. an $\mathfrak{m} \in \mathscr{M}$ such that if $\mathfrak{m} \subseteq \mathfrak{a}$ for any $\mathfrak{a} \in \mathscr{M}$, then $\mathfrak{m}=\mathfrak{a}$. This is precisely the definition of a maximal ideal.

## On Euclidean rings

Definition 11.7 An integral domain $R$ is called a Euclidean ring if there is a map $\delta: R \backslash\{0\} \rightarrow$ $\mathbb{N}_{0}$ such that $R$ has a division with remainder w.r.t. $\delta$, i.e. if for all $a, b \in R, b \neq 0$, there are $q, r \in R$ satisfying

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

Example 11.8 (a) $\mathbb{Z}$ w.r.t. $\delta=|\cdot|$ (absolute value).
(b) The Gaussian integers $\mathbb{Z}[i]:=\{a+b i \in \mathbb{C} \mid a, b \in \mathbb{Z}\}$ with + and $\cdot$ coming from $\mathbb{C}$, w.r.t. $\delta(a+i b)=a^{2}+b^{2}$ (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: $\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$, the proof that the ring is not Euclidean is quite hard.

Proposition 11.9 Every Euclidean ring is a principal ideal domain.
Proof. Let $R$ be a Euclidean ring w.r.t. $\delta$ and let $I \triangleleft R$ 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 $M:=\{\delta(i) \in \mathbb{N} \mid i \in I \backslash\{0\}\}$. 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 $i=q x+r$ with $r=0$ or $\delta(r)<\delta(n)$. Since $i \in I$ and $x \in I$, it follows that $r=i-q x \in I$. Due to the minimality of $n=\delta(x)$, we must have $r=0$. Thus $i=q x \in(x)$. We have shown: $I \subseteq(x) \subseteq I$, hence, $I=(x)$ is a principal ideal.

## On principal ideal domains (PID)

Recall that any ideal $I \unlhd R$ is called principal if there is $a \in R$ such that $I=(a)$.
Definition 11.10 An integral domain having the property that any ideal is principal is called a principal ideal domain (PID).

Example 11.11 (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 11.9).

Proposition 11.12 Let $R$ be a principal ideal domain and let $x \in R \backslash\left(R^{\times} \cup\{0\}\right)$. 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) $\Rightarrow$ (ii):' If $(x)$ were not a maximal ideal, then $(x) \subsetneq(y) \subsetneq R$ for some $y \in R \backslash\left(R^{\times} \cup\{0\}\right)$, whence $y \mid x$ and $y$ and $x$ are not associate, so that $x$ would not be irreducible.
'(ii) $\Rightarrow$ (iii):' Proved in general in Corollary 1.20.
'(iii) $\Rightarrow$ (iv):' and '(iv) $\Rightarrow$ (i):' are proved in the context of integral domains in Proposition 11.3.
Here is one important property of principal ideal domains, which means that they are Noetherian rings (see Definition 7.1). Since this appendix is independent of (more precisely, it precedes) the lecture, we formulate the property in a different way, which is equivalent for principal ideal domains.

Definition 11.13 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 $\left\{a_{n}\right\}_{n \in \mathbb{N}} \subseteq R$ 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 $\left(a_{m}\right)=\left(a_{N}\right)$.

An equivalent formulation of the property is:
Any ascending chain

$$
\mathfrak{a}_{1} \subseteq \mathfrak{a}_{2} \subseteq \mathfrak{a}_{3} \subseteq \ldots
$$

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.)

Proposition 11.14 Let $R$ be a principal ideal domain. Then in $R$ any chain of strict divisors has finite length. Thus, any principal ideal domain is a Noetherian ring.

Proof. Let $\mathfrak{a}_{n}=\left(a_{n}\right)$. These ideals form an ascending ideal chain:

$$
\mathfrak{a}_{1} \subseteq \mathfrak{a}_{2} \subseteq \mathfrak{a}_{3} \subseteq \mathfrak{a}_{4} \subseteq \ldots
$$

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 $a \in\left(a_{N}\right)$. This means $(a) \subseteq\left(a_{m}\right) \subseteq(a)$ for all $m \geq N$, whence $(a)=\left(a_{N}\right)=\left(a_{m}\right)$ for all $m \geq n$.

## On unique factorisation domains (UFD)

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

Example 11.16 (a) $\mathbb{Z}$ is the most basic example.
(b) Any field is a UFD (that's trivial because $R \backslash\left(R^{\times} \cup\{0\}=\emptyset\right)$.
(c) The polynomial ring over any UFD is a UFD (that is not so easy; it has been proved by Gauß).

Lemma 11.17 Let $R$ be a UFD and $r \in R \backslash\left(R^{\times} \cup\{0\}\right)$. Then one has: $r$ is prime $\Leftrightarrow r$ 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 11.18 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).

Lemma 11.19 Let $R$ be an integral domain in which any chain of strict divisors has finite length. Let $r \in R \backslash\left(R^{\times} \cup\{0\}\right)$. Then there are irreducible $x_{1}, \ldots, x_{n} \in R \backslash\left(R^{\times} \cup\{0\}\right)$ such that $r=x_{1} \cdot x_{2} \cdots \cdots x_{n}$.

Proof. We first show that every $r \in R \backslash\left(R^{\times} \cup\{0\}\right)$ has an irreducible divisor. Suppose this is not the case and pick any non-unit divisor $r_{1} \mid r$ s.t. $(r) \subsetneq\left(r_{1}\right)$. 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. $\left(r_{1}\right) \subsetneq\left(r_{2}\right)$. 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. $(r) \subseteq\left(x_{1}\right)$. 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 $r /\left(x_{1} x_{2}\right)$ is a unit, then we are done. Otherwise $r /\left(x_{1} x_{2}\right)$ 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 $\cdots\left|\frac{r}{x_{1} x_{2} x_{3}}\right| \frac{r}{x_{1} x_{2}}\left|\frac{r}{x_{1}}\right| r$, contrary to our hypothesis.

Proposition 11.20 Let $R$ be an integral domain. The following are equivalent:
(i) $R$ is a UFD.
(ii) - Every irreducible element $r \in R \backslash\left(\{0\} \cup R^{\times}\right)$is a prime element and

- in $R$ any chain of strict divisors has finite lenghts.
(iii) Every $r \in R \backslash\left(R^{\times} \cup\{0\}\right)$ can be written uniquely (up to permutation and up to associate elements) as a product of irreducible elements, i.e. if $r=x_{1} \cdot x_{2} \cdots x_{n}=y_{1} \cdot y_{2} \cdots \cdots y_{m}$ with irreducible elements $x_{i}, y_{j} \in R \backslash\left(R^{\times} \cup\{0\}\right)$, then $n=m$ and there is a permutation $\sigma$ in the symmetric group on $\{1, \ldots, n\}$ such that $x_{i}$ is associate with $y_{\sigma(i)}$ for all $i=1, \ldots, n$.

Proof. (ii) $\Rightarrow$ (i): Since irreducible elements are prime, Lemma 11.19 takes care of this implication.
(i) $\Rightarrow$ (iii): Recall that the prime elements are precisely the irreducible ones. So, we already have the existence. We now show the uniqueness. Let

$$
r=x_{1} \cdot x_{2} \cdots \cdots x_{n}=y_{1} \cdot y_{2} \cdots \cdot y_{m}
$$

It follows that $x_{n}$ divides $y_{1} \cdot y_{2} \cdots \cdots y_{m}$. 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:

$$
x_{1} \cdot x_{2} \cdots \cdots x_{n-1}=\varepsilon y_{1} \cdot y_{2} \cdots \cdots y_{m-1},
$$

where $\varepsilon \in R^{\times}$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 $\varepsilon$ by a different one) we obtain an even shorter relation:

$$
x_{1} \cdot x_{2} \cdots \cdot x_{n-2}=\varepsilon y_{1} \cdot y_{2} \cdots y_{m-2}
$$

Like this we continue, and conclude $n=m$ and that, after the above renumbering, $x_{i} \sim y_{i}$ are associate for all $i=1, \ldots, n$.
(iii) $\Rightarrow$ (ii): We first show that every irreducible element is prime. Let $r \in R \backslash\left(R^{\times} \cup\{0\}\right)$ be irreducible and suppose that $r \mid s t$ with $s, t \in R$, i.e. $r u=s t$ for some $u \in R$. We may write $s, t$ and $u$ uniquely (up to ordering and associates) as $s=s_{1} \cdot s_{2} \cdots \cdot s_{n}, t=t_{1} \cdot t_{2} \cdots \cdots t_{m}$ and $u=u_{1} \cdot u_{2} \cdots \cdot u_{\ell}$ with irreducible elements $s_{i}, t_{j}, u_{k}(i=1, \ldots, n ; j=1, \ldots, m ; k=1, \ldots, \ell)$. The uniqueness of irreducible elements occurring in the equation

$$
s_{1} \cdot s_{2} \cdots \cdots s_{n} \cdot t_{1} \cdot t_{2} \cdots \cdots t_{m}=r \cdot u_{1} \cdot u_{2} \cdots \cdots u_{\ell}
$$

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 $x_{1}, \ldots, x_{n}$ (using each $x_{i}$ at most once) occuring in $r=x_{1} \cdot x_{2} \cdots \cdot x_{n}$.

Proposition 11.21 Every principal ideal domain (PID) is a unique factorisation domain (UFD).

Proof. We have seen both properties or Proposition 11.20 (ii), namely in Propositions 11.12 and 11.14.

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

## 12 Appendix: Background on fields

In this section we recall some background on field extension.
Definition 12.1 A commutative ring $R$ is called a field if $R^{\times}=R \backslash\{0\}$, that is, if all non-zero elements are (multiplicatively) invertible.

Definition 12.2 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. $+: L \times L \rightarrow L,(x, y) \mapsto x+y$ (the + is the + of the field $L$ ) and scalar multiplication $+: K \times L \rightarrow L,(x, y) \mapsto x \cdot y$ (the $\cdot$ is the $\cdot$ of the field $L$ ).
The degree of $L / K$ is defined as $[L: K]:=\operatorname{dim}_{K}(L)$, the dimension of $L$ as $K$-vector space.
One says that $L / K$ is a finite field extension if $[L: K]<\infty$.

Lemma 12.3 - Multiplicativity of field degrees. Let $K \subseteq L \subseteq M$ be finite field extensions. Then

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

(in other words: $\operatorname{dim}_{K} M=\left(\operatorname{dim}_{K} L\right)\left(\operatorname{dim}_{L} M\right)$. .

## Proof. Exercise.

Proposition 12.4 Let $R$ be an integral domain. Then the following statements hold:
(a) The relation

$$
\left(r_{1}, s_{1}\right) \sim\left(r_{2}, s_{2}\right) \Leftrightarrow r_{1} s_{2}=r_{2} s_{1}
$$

defines an equivalence relation on $R \times(R \backslash\{0\})$. Denote the equivalence class of an element $(r, s)$ by $\frac{r}{s}$. Let $\operatorname{Frac}(R)$ denote the set of equivalence classes.
(b) Define + and $\cdot$ on $\operatorname{Frac}(R)$ 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 $\operatorname{Frac}(R)$ is a field with respect to + and $\cdot$ with $0=\frac{0}{1}$ and $1=\frac{1}{1}$.
One calls $\operatorname{Frac}(R)$ 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 2.30. (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 $K \rightarrow K[X] /(g)=: M$ 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 12.5 - 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 $f g \in A[X]$, 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 12.6 - 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 $\bmod p$ :

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

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: $f=g h$ with $g, h \in A[X]$ non-constant. Hence, we have $\pi(f)=$ $\pi(g h)=\pi(g) \pi(h)$. 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 12.7 • Consider $f_{1}(X)=X^{2}+X+1 \in \mathbb{Z}[X], f_{2}(X)=X^{2}+15 X-53 \in \mathbb{Z}[X]$, $f_{3}(X)=X^{2}+14 X-55 \in \mathbb{Z}[X]$ and $f_{4}(X)=X^{2}+15 X-54 \in \mathbb{Z}[X]$.
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 $X^{2}+2 X+2 \in \mathbb{F}_{3}[X]$ 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 $X^{2}+15 X-54=(X+18)(X-3)$.

- 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 $a(T)=b_{0}+b_{1} T+\cdots+b_{e} T^{e}$, then the class of $a(T)$ and the class of $b_{0}=a(0)$ modulo $T$ are the same because $a(T)-b_{0}=T \cdot\left(b_{1}+b_{2} T+\ldots b_{e} T^{e-1}\right) \in(T)$.

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

Proposition 12.8 - Eisenstein 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. 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 $f=g h$ with $g(X)=\sum_{i=0}^{r} b_{i} X^{i} \in A[X]$ and $h(X)=$ $\sum_{i=0}^{s} c_{i} X^{i} \in A[X]$ non-constant and $b_{r} \neq 0 \neq c_{s}$. Because of $a_{d}=b_{r} c_{s}$, the condition $p \nmid a_{d}$ implies $p \nmid b_{r}$ and $p \nmid c_{s}$. Because of $a_{0}=b_{0} c_{0}$, 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

$$
\underbrace{a_{t}}_{\text {divisible by } p}=\underbrace{b_{0} c_{t}+b_{1} c_{t-1}+\cdots+b_{t-1} c_{1}}_{\text {divisible by } p}+\underbrace{b_{t} c_{0}}_{\text {not divisible by } p} .
$$

This contradiction finishes the proof.
Example $12.9 \quad$ - $\operatorname{Consider} f_{1}(X)=X^{2}+2 X+2 \in \mathbb{Z}[X]$ and $f_{2}(X)=X^{7}+72 X^{2}+111 X-$ $30 \in \mathbb{Z}[X]$. 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 12.7 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

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

One calls $\Phi_{p}(X)$ the $p$-th cyclotomic polynomial (in German: Kreisteilungspolynom). We now show that $\Phi_{p}$ 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 $\left.\Phi_{p}(X)=f(X-1) g(X-1)\right)$. 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 $p \left\lvert\,\binom{ p}{i}\right.$ for all $1 \leq i \leq p-1$ and $p^{2} \nmid\binom{p}{1}=p$. Hence, $\Phi_{p}(X)$ is irreducible in $\mathbb{Q}[X]$.

