Commutative Algebra

Winter Term 2011/2012

Université du Luxembourg

Gabor Wiese
gabor.wiese@uni.lu

Version of 13th February 2012

Preface

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) 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.

The lecture covers the following topics:

- General concepts in the theory of commutative rings
  - Rings, ideals and modules
  - Noetherian rings
  - Tensor products
  - Localisation
  - Krull Dimension
- Number rings
  - Integral extensions
  - Noether's normalisation theorem
  - Dedekind rings

- Plane Curves
  - Affine space
  - Coordinate rings and Zariski topology
  - Hilbert's Nullstellensatz
  - Singular points

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

- 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.

In preparing these lectures, I used several sources. The most important one is the lecture *Algebra 2*, which I taught at the Universität Duisburg-Essen in the summer term 2009, which, in turn, heavily relies on a lecture for second year students by B. H. Matzat at the Universität Heidelberg from summer term 1998.

Contents

1 Rings and modules

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

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

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

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

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

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

The attribute unitary *refers to the existence of the element 1 in the ring. We only consider such rings, and will thus usually not mention the word unitary.*

If $(R \setminus \{0\}, \cdot)$ is an abelian semi-group, then R is called a commutative ring*. Most (but not all) of the lecture will only treat commutative rings; hence, the name* Commutative Algebra*. By a ring I shall usually mean to a commutative ring (should be clear from the context – if not, ask!).*

If R is a commutative ring and if in addition $(R \setminus \{0\}, \cdot, 1)$ is an abelian group (not only semi-group) and $1 \neq 0$, then R is called a field*.*

A subset $S \subseteq R$ is called a (commutative) subring *if $0, 1 \in S$ and $+$ and $\cdot$ restrict to S making it into a ring.*

[We recall the definition of a semi-group and a group: A set S, containing an element denoted 1, together with a map $\cdot : S \times S \to S$, $(s, t) \mapsto s \cdot t$ is called a semi-group *if the following hold:*

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

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

If in addition, it holds that

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

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

Example 1.2. *(a)* $\mathbb{Z}$, $\mathbb{Q}$.

(b) $M_N(\mathbb{Q})$ *($N \times N$-matrices).*

(c) $\mathbb{Z}[X]$, $\mathbb{Q}[X]$.

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

(e) $\mathbb{F}_p$, $\mathbb{F}_{p^r}$ *for a prime number p and $r \in \mathbb{N}$.*

In this lecture, we shall motivate many of the properties of commutative rings that we study by examples coming from rings of integers of number fields and plane curves. Here's already the definition of a number field. Rings of integers and plane curves will be introduced later.

Definition 1.3. *A finite field extension K of $\mathbb{Q}$ is called a* number field.

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

Example 1.4. *(a) $\mathbb{Q}$ (but: $\mathbb{R}$ is not a number field).*

(b) $\mathbb{Q}[X]/(f(X))$ 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).

The latter two examples will be explained shortly.

Definition 1.5. *Let R, S be rings. A map $\varphi : R \to S$ is called a* ring homomorphism *if the following properties are satisfied:*

(a) $\varphi(1) = 1$,

(b) $\varphi(r + s) = \varphi(r) + \varphi(s)$ for all $r, s \in R$,

(c) $\varphi(r \cdot s) = \varphi(r) \cdot \varphi(s)$ for all $r, s \in R$.

Example 1.6. *(a) $\mathbb{Z} \to \mathbb{F}_p, a \mapsto \overline{a}$.*

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

Definition 1.7. *Let R be a ring. An abelian group $(M, +, 0)$ together with a map*

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

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

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

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

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

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

In a similar way one defines right modules and two-sided modules.

*A subset $N \leq M$ is called an R-*submodule *of M if $0 \in M$ and $+$ and $.$ restrict to N making it into an R-module.*

Example 1.8. *(a) Let K be a field and V a K-vector space. Then V is a K-module.*

(b) Let R be a ring. Then R is an R-module (natural $+$ and $. = \cdot$).

(c) Let R be a ring. Then $M := R \times R \times \cdots \times R$ is an R-module (natural $+$ and diagonal .).

Lemma 1.9. *An abelian group $(M, +, 0)$ is an R-module if and only if the map*

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

is a ring homomorphism. Here $\mathrm{End}(M)$ denotes the endomorphism ring of M as an abelian group.

Definition 1.10. *Let R be a ring and M, N be R-modules. A map $\varphi : M \to N$ is called an R-*module homomorphism *(or short: R-*homomorphism*, or: R-*linear (map)*) if*

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

Lemma 1.11. *The* kernel *$\ker(\varphi) := \{m \in M \mid \varphi(m) = 0\}$ is an R-submodule of M.*

The image *$\mathrm{im}(\varphi) := \{\varphi(m) \mid m \in M\}$ is an R-submodule of N.*

By the way, the quotient (see below) $N/\,\mathrm{im}(\varphi)$ is called the cokernel *of φ.*

Proof. Simple checking. □

Definition 1.12. *Let R be a ring and N, M be R-modules. Let $\varphi : M \to N$ be an R-homomorphism. We say that φ is a* monomorphism *if φ is injective. It is called an* epimorphism *if φ is surjective. Finally, it is called an* isomorphism *if it is bijective.*

*If $N = M$, then an R-homomorphism $\varphi : M \to M$ is also called an R-*endomorphism*.*

We let $\mathrm{Hom}_R(M, N)$ (or $\mathrm{Hom}(M, N)$ if R is understood) be the set of all R-homomorphisms $\varphi : M \to N$. If $M = N$, then one lets $\mathrm{End}_R(M) := \mathrm{Hom}_R(M, M)$.

Lemma 1.13. *Let R be a ring and N, M be R-modules. Then $\mathrm{Hom}_R(M, N)$ is itself an R-module with respect to pointwise defined $+$ and ., i.e. $(f+g)(m) := f(m)+g(m)$ and $(r.f)(m) := r.(f(m))$ for all $f, g \in \mathrm{Hom}_R(M, N)$, all $m \in M$ and all $r \in R$.*

Proof. Simple checking (Exercise on Sheet 2). □

Definition 1.14. *A subset $I \subseteq R$ is called a* (left/right/two-sided) ideal *if I is a (left/right/two-sided) R-module (w.r.t. $+$ from R and $. = \cdot$ from R). Notation $I \lhd R$ (or $I \unlhd R$).*

Example 1.15. *(a) $\{0\}$, R are both trivially ideals.*

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

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

Definition 1.16. *Let M a an R-module and let $m_i \in M$ for $i \in I$ (some 'indexing' set). Denote by $\langle m_i | i \in I\rangle$ the smallest submodule of M containing all m_i for $i \in I$; it is called* the submodule generated by the *m_i, $i \in I$.*

An R-module M is called finitely generated *if there are $r \in \mathbb{N}$ and elements $m_1, \ldots, m_r \in M$ such that $\langle m_1, \ldots, m_r\rangle = M$.*

Notation: if $m_i \in R$, we write $(m_i | i \in I) := \langle m_i | i \in I\rangle$ for the ideal of R generated by the m_i for $i \in I$.

An ideal of the form $(r) \lhd R$ with $r \in R$ is called a principal ideal.

Example 1.17. *(a)* $(0) = \{0\}$, $(1) = R$.

(b) $(n) = \{nm | m \in \mathbb{Z}\} \lhd \mathbb{Z}$.

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

(d) Every ideal of $\mathbb{Z}$ *is principal (*$\mathbb{Z}$ *is a principal ideal domain). To see this, we give a proof that generalises immediately to Euclidean rings (see next section). Let* I *be any non-zero ideal of* $\mathbb{Z}$*. Let* n *be the smallest positive integer in* I*.*

Claim: $I = (n)$*. Let* $x \in I$ *be any element. Using division with remainder we write* $x = an + r$ *with* $0 \leq r < n$ *and some* $a \in \mathbb{Z}$*. As* $x \in I$ *and* $n \in I$*, also* $r = x - an \in I$*. As* n *is the smallest positive element in* I*, the remainder* r *has to be zero, whence* $x = an$ *and* $x \in (n)$*. This shows* $I \subseteq (n)$*. The converse inclusion is trivial.*

Lemma 1.18. *Let* R *be a ring and* $N \leq M$ *be* R*-modules. The relation* $x \sim y :\Leftrightarrow x - y \in N$ *defines an equivalence relation on* M*. The equivalence classes* $\overline{x} = x + N$ *form the* R*-module denoted* M/N *with*

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

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

Proof. Simple checking. The main point is that $+$ and . indeed define maps , i.e. are well-defined. The other properties then follow immediately from those of R. □

Lemma 1.19. *Let* R *be a commutative ring and* $I \trianglelefteq R$ *be an ideal. Then the quotient module* R/I *is a commutative ring with multiplication*

$$\cdot : R/I \times R/I \to R/I, \ \ (r + I, s + I) \mapsto rs + I,$$

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

Proof. Simple checking, as for the previous lemma. □

Example 1.20. *(a)* $\mathbb{Q}(i) \cong \mathbb{Q}[X]/(X^2 + 1)$.

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

(c) $\mathbb{F}_4 = \mathbb{F}_2[X]/(X^2 + X + 1)$.

Definition 1.21. *Let* R *be a ring and* $I \lhd R$*,* $I \neq R$ *an ideal.*

The ideal I *is called* maximal *if there is no ideal* $J \lhd R$ *such that* $I \subsetneq J \subsetneq R$*.*

The ideal I *is called* prime *if, whenever* $ab \in I$*, then* $a \in I$ *or* $b \in I$*.*

Proposition 1.22. *The prime ideals of* $\mathbb{Z}$ *are precisely* (0) *and* (p) *for* p *a prime number (using the 'school definition': a natural number* p *is prime if its only positive divisors are* 1 *and* p*).*

Proof. First we see that (0) is a prime ideal: $ab = 0 \Rightarrow a = 0$ or $b = 0$.

Now we check that (p) is a prime ideal if p is a prime number. Let $a, b \in \mathbb{Z}$ such that $ab \in (p)$. This means that there exists $n \in \mathbb{Z}$ such that $ab = np$. Here comes the non-trivial part. Now, we assume that $a \notin (p)$, i.e. $p \nmid a$. This means that the greatest common divisor of p and a is 1 and by the (extended) Euclidean algorithm we get $1 = ra + sp$ with some $r, s \in \mathbb{Z}$. Multiplying by b gives $b = rab + bsp = rnp + bsp = (rn + bs)p$, whence $b \in (p)$, as was to be shown.

Let now (n) be a prime ideal. If n were not prime, then $n = ab$ with $a, b \neq 1, -1$, so $ab \in (n)$, but $a \notin (n)$ and $b \notin (n)$, contradicting the prime-ness of (n). □

Definition 1.23. *Let R be a ring. An element $r \in R$ is called a* zero-divisor *if there is $s \in R$, $s \neq 0$ s.t. $rs = 0$.*

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

Proposition 1.24. *Let R be a ring and $I \lhd R$ an ideal.*

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

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

Proof. (a) Let I be a prime ideal and let $a + I, b + I \in R/I$ such that $(a + I)(b + I) = ab + I = 0 + I = 0$, i.e. $ab \in I$. By the property of I being a prime ideal, $a \in I$ or $b \in I$, which immediately translates to $a + I = 0$ or $b + I = 0$.

Conversely, assume that R/I is an integral domain and let $a, b \in R$ such that $ab \in I$. This means $(a + I)(b + I) = 0$, whence $a + I = 0$ or $b + I = 0$ so that $a \in I$ or $b \in I$, proving that I is a prime ideal.

(b) Suppose that I is a maximal ideal and let $x + I \neq 0$ be an element in R/I. We must show it is invertible. The condition $x + I \neq 0$ means $x \notin I$, whence the ideal $J = (I, x)$ is an ideal strictly bigger than I, whence $J = R$ by the maximality of I. Consequently, there are $i \in I$ and $r \in R$ such that $1 = i + xr$. This means that $r + I$ is the inverse of $x + I$.

Now let us assume that R/I is a field and let $J \supsetneq I$ be an ideal of R strictly bigger than I. Let x be an arbitrary element in J but not in I. As R/I is a field, the element $x + I$ is invertible, whence there is $y \in R$ such that $(x + I)(y + I) = xy + I = 1 + I \subseteq J$. So, $1 \in J$, whence $R \subseteq J$, showing that $J = R$, whence I is maximal. □

Corollary 1.25. *Every maximal ideal is a prime ideal.*

Proof. Every field is an integral domain. □

Example 1.26. *A ring R is an integral domain if and only if (0) is a prime ideal of R.*

Definition 1.27. *Let R and S be rings. We say that S is an R-algebra if there is a ring homomorphism $\varphi : R \to S$.*

Example 1.28. *Let K be a field. Then the polynomial ring $K[X]$ is a K-algebra.*

Consider $\mathrm{End}_K(V)$ for a K-vector space V. Then $\mathrm{End}_K(V)$ is a K-algebra (K embeds into the scalar matrices).

2 Factorial rings

Principal ideal domains and factorial rings are the 'nicest' commutative rings. Unfortunately, many of the rings one encounters naturally (e.g. rings of integers in number fields, or rings of functions on affine plane curves) are not that 'nice'. We shall in later sections be concerned with finding substitutes for the 'nice' properties of factorial rings and prinicipal ideal domains. Here, we shall as a start develop these 'nice' properties, so that we can more appreciate them and the quest for similar properties in more general cases.

Euclidean rings, principal ideal domains and factorial rings are all generalisations of the integer ring $\mathbb{Z}$. It was apparently Gauß who was the first to notice that 'obvious' statements like the one that every positive integer can be uniquely (up to ordering) written as a product of prime elements needed proof. In this section we give these proves in more generality.

Euclidean rings

Definition 2.1. *An integral domain R is called a* Euclidean ring *if there is a map $\delta : R \setminus \{0\} \to \mathbb{N}_0$ such that R* has a division with remainder w.r.t. δ*, i.e. if for all $a, b \in R$, $b \neq 0$, there are $q, r \in R$ satisfying*

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

Example 2.2. *(a) $\mathbb{Z}$ w.r.t. $\delta = |\cdot|$ (absolute value).*

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

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

Principal ideal domains

Definition 2.3. *An integral domain R is called a* principal ideal domain *if every ideal of R is principal.*

Proposition 2.4. *Every Euclidean ring is a principal ideal domain.*

Proof. Let R be a Euclidean ring w.r.t. δ and let $I \lhd R$ be an ideal. We want to show that it is principal. If $I = \{0\}$, then it is already principal, so that we may suppose $I \neq (0)$. Consider the set $M := \{\delta(i) \in \mathbb{N} \mid i \in I \setminus \{0\}\}$. As a non-empty subset of $\mathbb{N}$ it has a smallest element (induction principal, well-ordering principle, ...). Let n be this smallest element. It is of the form $n = \delta(x)$ with $0 \neq x \in I$. Note $(x) \subseteq I$.

Let now $i \in I$ be any element. By the Euclidean property there are $q, r \in R$ such that $i = qx + r$ with $r = 0$ or $\delta(r) < \delta(n)$. Since $i \in I$ and $x \in I$, it follows that $r = i - qx \in I$. Due to the minimality of $n = \delta(x)$, we must have $r = 0$. Thus $i = qx \in (x)$. We have shown: $I \subseteq (x) \subseteq I$, hence, $I = (x)$ is a principal ideal. □

Example 2.5. *(a) $\mathbb{Z}$, $\mathbb{Z}[i]$*

(b) $K[X]$ with K a field, but not $\mathbb{Z}[X]$.

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

Definition 2.6. *Let R be an integral domain.*

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

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

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

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

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

Proposition 2.7. *Let R be an integral domain.*

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

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

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

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

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

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

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

Proof. (a), (b), (c) and (d) are simple checking.

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

Proposition 2.8. *Let R be a principal ideal domain and let $x \in R \setminus (R^\times \cup \{0\})$. Then the following are equivalent:*

(i) x is irreducible.

(ii) (x) is a maximal ideal.

(iii) (x) is a prime ideal.

(iv) x is a prime element.

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

Proof. '(i)⇒(ii):' If (x) were not a maximal ideal, then $(x) \subsetneq (y) \subsetneq R$ for some $y \in R \setminus (R^\times \cup \{0\})$, whence $y \mid x$, so that x would not be irreducible. We have already seen the other implications. □

We shall use two consequences all the time:

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

Definition 2.9. *A ring R is called* Noetherian *if all ideal chains*

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

become stationary. More formally, whenever $\mathfrak{a}_i \lhd R$ for $i \in \mathbb{N}$ are ideals with the property $\mathfrak{a}_i \subseteq \mathfrak{a}_{i+1}$, then there is $n \in \mathbb{N}$ such that for all $i \geq n$ one has $\mathfrak{a}_n = \mathfrak{a}_i$.

More on Noetherian rings and modules will be said in later sections.

Proposition 2.10. *Every principal ideal domain is a Noetherian ring.*

Proof. Let $\mathfrak{a}_i = (a_i)$ with $a_i \in R$ be such an ascending ideal chain ($\mathfrak{a}_i \subseteq \mathfrak{a}_{i+1}$ for all $i \in \mathbb{N}$, or, equivalently, $a_{i+1} \mid a_i$ for all $i \in \mathbb{N}$). Then form the ideal $\mathfrak{a} = \bigcup_{i\in\mathbb{N}} \mathfrak{a}_i$. It is a principal ideal, i.e. $\mathfrak{a} = (a)$ for some $a \in R$. Of course, $a \in (a)$, i.e. $a \in \bigcup_{i\in\mathbb{N}} \mathfrak{a}_i$, whence there is $n \in \mathbb{N}$ such that $a \in (a_n)$. This means $(a) \subseteq (a_i) \subseteq (a)$ for all $i \geq n$, whence $(a) = (a_i)$ for all $i \geq n$. □

Factorial rings

Definition 2.11. *A Noetherian integral domain R is called a* factorial ring *(or a* UFD – unique factorisation domain*) if every irreducible element $r \in R \setminus (R^\times \cup \{0\})$ is a prime element.*

Proposition 2.12. *Every principal ideal domain is a factorial ring.*

Proof. We have seen both Noetherian-ness and the property that every irreducible element is prime. □

Hence we have the implications:
Euclidean ⇒ PID ⇒ UFD.

We shall see later that being factorial is a property that is too strong in many cases. They will be replaced by Dedeking rings (which are *locally* PIDs – definitions come later; examples are the rings of integers in number fields).

Lemma 2.13. *Let R be a Noetherian integral domain and $r \in R \setminus (R^\times \cup \{0\})$. Then there are irreducible $x_1, \dots, x_n \in R \setminus (R^\times \cup \{0\})$ such that $r = x_1 \cdot x_2 \cdot \dots \cdot x_n$.*

Proof. We first show that every $r \in R \setminus (R^\times \cup \{0\})$ has an irreducible divisor. Suppose this is not the case and pick any non-unit divisor $r_1 \mid r$ s.t. $(r) \subsetneq (r_1)$. If not such r_1 existed, then r would be irreducible itself. Of course, r_1 is not irreducible. So we can pick a non-unit divisor $r_2 \mid r_1$ s.t. $(r_1) \subsetneq (r_2)$. Like this we can continue and obtain an infinite ascending ideal chain, contrary to the Noetherian hypothesis.

Now, we have an irreducible non-unit divisor $x_1 \mid r$ s.t. $(r) \subseteq (x_1)$. If r/x_1 is a unit, then we are done. Otherwise r/x_1 has an irreducible non-unit divisor $x_2 \mid r/x_1$. If $r/(x_1x_2)$ is a unit, then we are done. Otherwise $r/(x_1x_2)$ has an irreducible non-unit divisor.

Like this we continue. This process must stop as otherwise we would have an infinite ascending ideal chain

$$(\frac{r}{x_1}) \subsetneq (\frac{r}{x_1x_2}) \subsetneq \dots .$$

□

Proposition 2.14. *Let R be a Noetherian integral domain. The following are equivalent:*

(i) R is a factorial ring.

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

Proof. (i) ⇒ (ii): See Lemma 2.13 for the existence. We now show the uniqueness. Recall that the prime elements are precisely the irreducible ones. This is what we are going to use. Let

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

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

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

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

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

Like this we continue, and conclude $n = m$ and that, after the above renumbering, $x_i \sim y_i$ are associate for all $i = 1, \dots, n$.

(ii) ⇒ (i): We need to show that every irreducible element is prime. So, let $r \in R \setminus (R^\times \cup \{0\})$ be irreducible and suppose that $r \mid st$ with $s, t \in R$, i.e. $ru = st$ for some $u \in R$. We may write s, t and u uniquely (up to ordering and associates) as $s = s_1 \cdot s_2 \cdot \dots \cdot s_n$, $t = t_1 \cdot t_2 \cdot \dots \cdot t_m$ and

$u = u_1 \cdot u_2 \cdot \cdots \cdot u_\ell$ with irreducible elements s_i, t_j, u_k ($i = 1, \dots, n$; $j = 1, \dots, m$; $k = 1, \dots, \ell$). The uniqueness of irreducible elements occurring in the equation

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

implies that r must be equal to one of the s's or one of the t's. This means that r divides s or it divides t, as was to be shown. □

We now want to see that not every ring is factorial.

Example 2.15. *Consider the ring* $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$ *with* $+$ *and* $\cdot$ *from* $\mathbb{C}$*. We have*

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

All four elements $2, 3, 1 + \sqrt{-5}, 1 - \sqrt{-5}$ *are irreducible elements of* $\mathbb{Z}[\sqrt{-5}]$*:*

Suppose $(a + b\sqrt{-5})|2$*. It follows that* $(a + b\sqrt{-5}) \cdot \overline{(a + b\sqrt{-5})} = a^2 + 5b^2 \mid 4 = 2 \cdot \overline{2}$*. We obtain* $b = 0$ *and* $a = \pm 2$*. It works similarly with the other three numbers.*

Hence, this example shows that in $\mathbb{Z}[\sqrt{-5}]$ *not every element can be written as a product of irreducible elements in a unique way! In other words,* $\mathbb{Z}[\sqrt{-5}]$ *is not a factorial ring (but, it is a Noetherian integral domain).*

Corollary 2.16. *Let* R *be a principal ideal domain. Then it satisfies the 'unique ideal factorisation property': Every non-zero ideal* $I \lhd R$ *can be written in a unique way (up to permutation) as*

$$I = \mathfrak{p}_1 \mathfrak{p}_2 \dots \mathfrak{p}_n$$

with $\mathfrak{p}_i$ *prime ideals.*

Proof. This is obvious. □

The unique ideal factorisation property will be the most important property of Dedekind rings, which are to be studied later. This unique ideal factorisation replaces the unique factorisation into prime elements, which fails very easily (as we have seen).

We finish this section with the 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 factorial rings they always do!

3 Algebraic elements and algebraic field extensions

We now introduce (recall) important notions from field theory. They inspire us to generalise them in order to 'integral' notions in the next section, i.e. in spirit we shall later replace $\mathbb{Q}$ by $\mathbb{Z}$. That will add some extra technicalities, but many of the concepts will be very parallel.

Lemma 3.1 (Multiplicativity of field degrees)**.** *Let* $K \subseteq L \subseteq M$ *be finite field extensions. Then*

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

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

Proof. Exercise. □

Definition 3.2. *Let K be a field and L/K a field extension (see earlier definition).*

(a) *An element $a \in L$ is called* algebraic over K *if there is a non-zero polynomial $f \in K[X]$ such that $f(a) = 0$ (i.e. a is a zero (also called root) of f).*

An element $a \in L$ that is not algebraic over K is also called transcendental over K.

(b) *The field extension L/K is called* algebraic *(alternatively, L is called an* algebraic field extension of K*) if every $a \in L$ is algebraic over K.*

If L/K is not algebraic, it is called transcendental.

Example 3.3. *(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 $X^2 - \sqrt{2}$ may not be used here, since its coefficients are not in $\mathbb{Q}$!

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

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

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

Lemma 3.4. *Let K be a field and L/K a field extension and $a \in L$.*

(a) *The* evaluation map

$$\Phi_a : K[X] \to L, \quad f \mapsto f(a)$$

is a homomorphism of rings.

(b) Φ_a is injective if and only if a is transcendental over K.

(c) If a is algebraic over K, then there is a unique monic (i.e. highest coefficient is 1, i.e. $X^d + c_{d-1}X^{d-1} + \dots + c_0$) polynomial $m_a \in K[X]$ such that $(m_a) = \ker(\Phi_a)$ (i.e. the principal ideal (m_a) is equal to the kernel of the evaluation map).

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

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

$$\Phi_a : K[X]/(m_a) \to L, \quad f + (m_a) \mapsto f(a)$$

is an injective field homomorphism. Its image is denoted by $K(a)$ and is called the field generated by a over K *or* K adjoined a.

Proof. (a) Exercise. Just check the definition.

(b) If a is algebraic over K, then there is a non-zero polynomial $f \in K[X]$ such that $f(a) = 0$. This just means that f is in the kernel of the evaluation map, so f is not injective. Conversely, if f is not injective, then there is some non-zero polynomial f in the kernel of the evaluation map. That, however, just means $f(a) = 0$, whence a is algebraic.

(c) We know that $K[X]$ is a principal ideal domain. Hence, the kernel of Φ_a is a principal ideal, so, it is generated by one element f. As Φ_a is not injective (a is assumed to be algebraic, see (b)), f is non-zero. A generator of a principal ideal is unique up to units in the ring. So, f is unique up to multiplication by a unit of K, i.e. up to multiplication by an element from $K \setminus \{0\}$ (see exercise on Sheet 3). 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.

(d) We know that $K[X]/(m_a)$ is a field, since (m_a) is a maximal ideal, which is the case due to the irreducibility of m_a. For, if m_a were reducible $m_a = fg$ with $f, g \in K[X]$ both of smaller degree than the degree of m_a, then $0 = m_a(a) = f(a)g(a)$ implies that $f(a) = 0$ or $g(a) = 0$. Suppose without loss of generality that $f(a) = 0$. Then $f \in \ker(\Phi_a) = (m_a)$, so that $m_a \mid f$, which is impossible for degree reasons.

The injectivity follows because we just ‘modded out’ by the kernel (homomorphism theorem – see exercise on Sheet 3). (Alternatively, you can also recall that any ring homomorphism between fields is necessarily injective.)

□

In words, the minimal polynomial $m_a \in K[X]$ of a (algebraic over K) is the monic polynomial of smallest degree annihilating a. Compare this to the minimal polynomial of a matrix (the map from Exercise 4 on Sheet 1 is the analogue of the evaluation map Φ_a and the minimal polynomial of a matrix is the unique monic polynomial generating the kernel of the map in the exercise).

Note that (d) says non-trivial things, namely that the subset of L of the form $\{\sum_{i=0}^{d-1} r_i a^i \mid r_i \in K\}$ is a subfield of L (and not just a subring!).

If the minimal polynomial of a is of the form $m_a = X^d + c_{d-1}X^{d-1} + \cdots + c_0$, then $K(a)$ can be represented as a K-vector space with basis $1, a, a^2, a^3, \dots, a^{d-1}$. Suppose we have two such elements $\alpha = \sum_{i=0}^{d-1} r_i a^i$ and $\beta = \sum_{i=0}^{d-1} s_i a^i$ (with $r_i, s_i \in K$). Of course, the addition in $K(a)$ is the addition in L and comes down to:

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

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

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

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

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

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

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

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

Example 3.5. *Return to the example $\mathbb{Q}(\sqrt{5})$. The minimal polynomial of $\sqrt{5}$ over $\mathbb{Q}$ (say, as an element of $\mathbb{R}$) is $X^2 - 5$, so $\mathbb{Q}(\sqrt{5})$ is the image of $\mathbb{Q}[X]/(X^2-5)$ in $\mathbb{R}$. The above $\mathbb{Q}$-basis is $1, \sqrt{5}$. So, we express any element of $\mathbb{Q}(\sqrt{5})$ as $a + b\sqrt{5}$ with $a, b \in \mathbb{Q}$.*

Now let two such elements be given $\alpha = a_0 + a_1\sqrt{5}$ and $\beta = b_0 + b_1\sqrt{5}$. Then

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

and

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

The discussion above yields, in particular:

Corollary 3.6. *Let K be a field, L/K a field extension and $a \in L$ algebraic over K with minimal polynomial $m_a \in K[X]$ of degree d. The field $K(a)$ is the subfield*

$$\{\sum_{i=0}^{d-1} r_i a^i \mid r_i \in K\} \subseteq L.$$

It can also be viewed as the smallest subfield of L containing a and K. The field extension $K(a)/K$ has degree d, i.e. $[K(a) : K] = d$.

A word of explanation about ‘smallest subfield’. One should convince oneself that given two subfields $M_1 \subseteq L$ and $M_2 \subseteq L$, their intersection $M_1 \cap M_2$ is also a subfield of L. Hence, one can formally define the smallest subfield of L containing K and a is the intersection of all such.

Of course, we shouldn’t limit ourselves to considering a single element $a \in L$. Instead, let’s look at $a_i \in L$ for $i \in I$ (some indexing set; could be finite or infinite).

Definition 3.7. *Let K be a field, L/K a field extension and $a_i \in L$ for $i \in I$ elements. We define $K(a_i | i \in I)$ to be the smallest subfield of L containing K and all a_i, $i \in I$.*

If $L = K(a_1, \ldots, a_n)$ for some n, we say that the field extension L/K is finitely generated *(not to be mixed up with finite field extension!).*

Note that for a single element a, both definitions of $K(a)$ coincide, as we have already observed. One might also want to verify that $K(a, b) = (K(a))(b)$. That equality immediately comes down to the following statement: A field L contains K and a if and only if L contains $K(a)$. That statement is clear.

We shall next develop a different point of view on algebraic elements and algebraic extensions. It is this point of view that turns out very useful in the upcoming ‘integral’ analogue of the theory.

Proposition 3.8. *Let K a field and L/K a field extension.*

(a) Let $a_1, \dots, a_n \in L$ be finitely many elements.

Then the field extension $K(a_1, a_2, \dots, a_n)/K$ is finite if and only if all a_i are algebraic over K.

(b) If L/K is finite, then it is algebraic (i.e. all its elements are algebraic over K, see Definition above).

Proof. (a) Suppose first that all a_i are algebraic over K. As

$$K(a_1, a_2, \dots, a_{n-1})(a_n) = K(a_1, a_2, \dots, a_n)$$

and due to the multiplicativity of degrees, it suffices that $K(a)/K$ is finite for any element a that is algebraic over K. That we already know.

Now suppose that one of the a_i (say, a_1 possibly after renumbering) is transcendental over K. Then $K(a_1)$ contains the image of $K[X]$ under the injective evaluation map Φ_{a_1}. As already $K[X]$ is infinite dimensional as K-vector space, it follows that $K(a_1)$ is of infinite degree over K.

(b) Let $a \in L$ be any element. Consider the set $S := \{1, a, a^2, a^3, \dots\}$. Now consider the K-subspace V of L spanned by this set. As L is finite dimensional as K-vector space, also V has to be finite dimensional. Hence, S contains a K-basis B of V. Let $a^n \in S$ a power of a that is not in the basis. But, of course, it can be expressed in terms of the basis. That means we have a non-zero polynomial annihilating a, hence, a is algebraic over K. □

Corollary 3.9. *Let K be a field and L/K a field extension. Then the following statements are equivalent:*

(i) L/K is a finite field extension.

(ii) L/K is a finite and algebraic field extension.

(iii) L/K can be generated by finitely many elements that are algebraic over K.

Proof. (i) ⇒ (ii): Every finite field extension is algebraic (proved above).

(ii) ⇒ (iii): We give a constructive proof. Take any $a_1 \in L \setminus K$. It is algebraic over K and $K \subsetneq K(a_1) \subseteq L$. Note $[L : K] > [L : K(a_1)]$. If $K(a_1) \neq L$, then take $a_2 \in L \setminus K(a_1)$. It is also algebraic over K. We get $K(a_1) \subsetneq K(a_1, a_2) \subseteq L$. Note $[L : K(a_1)] > [L : K(a_1, a_2)]$. Like this we continue. As the degree is a positive integer greater than or equal to 1, this process will end at some point and then $K(a_1, a_2, \dots, a_n) = L$.

(iii) ⇒ (i): Proved above. □

Proposition 3.10. *Let $M/L/K$ be field extensions.*

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

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

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

(b) One direction is trivial, the other follows from (a). □

Definition 3.11. *(a) Let L/K be a field extension. The set*

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

is called the algebraic closure of K in L.

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

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

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

Proposition 3.12. *(a) Let L/K be a field extension. The algebraic closure of K in L is an algebraic field extension of K.*

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

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

(b) Assume K is algebraically closed and let $f \in K[X]$ be a non-constant polynomial. Let $g = \sum_{i=0}^{d} c_i X^i$ be a non-constant irreducible divisor of f. The natural injection $K \to K[X]/(g) =: M$ is a finite field extension of K (remember that (g) is a maximal ideal of the principal ideal domain $K[X]$). Now, the class $a := X + (g) \in M$ is a zero of g, since

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

As K is algebraically closed, $M = K$, whence $a \in K$.

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

Proposition 3.13. *Let K be a field. Then there exists an algebraic field extension $\overline{K}/K$ such that $\overline{K}$ is algebraically closed.*

The field $\overline{K}$ is called an algebraic closure of K *(it is not unique, in general).*

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

Example 3.14. *(a) $\mathbb{C}$ is algebraically closed; $\mathbb{R}$ is not. $\mathbb{R}_{\mathbb{C}} = \mathbb{C}$.*

(b) $\mathbb{Q}_{\mathbb{C}} = \{x \in \mathbb{C} \mid x \text{ is algebraic over } \mathbb{Q}\} =: \overline{\mathbb{Q}}$. *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.

4 Integral elements and integral ring extensions

Integral elements are generalisations of algebraic elements, when the field K is replaced by a ring R. For algebraic elements the minimal polynomial is the unique *monic* polynomial of minimal degree annihilating the element; but, in fact, we do not really care whether the polynomial is monic, since we can always divide by the leading coefficient. So, the choice of defining the minimal polynomial of an algebraic element as a monic polynomial is actually quite arbitrary, one might do it differently without changing anything in the theory. Over rings the situation is different, since we cannot divide by the leading coefficient in general.

Why are monic minimal polynomials useful? We want to construct extensions: Let L/K be a field extension and $a \in L$ be algebraic over $\mathbb{Q}$ with minimal polynomial $m_a = X^n + c_{n-1}X^{n-1} + \cdots + c_0$. This just means

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

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

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

to be a ring.

Suppose now we work over a ring R instead of a field K. Let S be a ring containing R. Assume for a moment that $a \in S$ satisfies

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

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

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

is not stable under multiplication!

The morale is that we must use monic minimal polynomials (at least polynomials whose leading coefficient is a unit), when we work over rings and want to construct extensions similar to those over fields.

Finally, consider the following examples. Let $R = \mathbb{Z}$ be the ring over which we work. We look at: $f(X) = X - 2$ and $g(X) = 3X - 2$. The zero of f is 2 and the zero of g is $\frac{2}{3}$, so that the minimal polynomial of $\frac{2}{3}$ seen as an algebraic element over $\mathbb{Q}$ is $X - \frac{2}{3}$. The latter polynomial is not in $\mathbb{Z}[X]$ anymore! That just indicates that $\frac{2}{3}$ is not an integer. We see that each element of $\mathbb{Q}$ has a linear polynomial with integer coefficients annihilating it. The integers are precisely those elements of $\mathbb{Q}$ that have a monic integer polynomial annihilating it.

This motivates the following fundamental definition.

Definition 4.1. *Let R be a ring and S an extension ring of R (i.e. a ring containing R as a subring). An element $a \in S$ is called* integral over R *if there exists a monic polynomial $f \in R[X]$ such that $f(a) = 0$.*

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

Example 4.2. *(a) The elements of $\mathbb{Q}$ that are integral over $\mathbb{Z}$ are precisely the integers of $\mathbb{Z}$.*

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

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

(d) $a := \frac{1+\sqrt{-5}}{2} \in \mathbb{R}$ is not integral over $\mathbb{Z}$ because $f = X^2 - X + \frac{5}{2}$ annihilates it. If there were a monic polynomial $h \in \mathbb{Z}[X]$ annihilating a, then we would have $h = fg$ with some monic polynomial $g \in \mathbb{Q}[X]$. But, now it would follow that both f and g are in $\mathbb{Z}[X]$ (see Sheet 4), which is a contradiction.

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

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

Definition 4.3. *Let S be a ring and $R \subseteq S$ a subring.*

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

An alternative name is: normalisation of R in S.

(b) S is called an integral ring extension of R *if $R_S = S$, i.e. if every element of S is integral over R (compare with algebraic field extension – the two notions coincide if R and S are fields).*

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

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

(d) 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.*

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

Definition 4.4. *Let S be a ring and $R \subseteq S$ a subring and $a_i \in S$ for $i \in I$ (some indexing set).*

We let $R[a_i \mid i \in I]$ (note the square brackets!) be the smallest subring of S containing R and all the a_i, $i \in I$.

Note that as before we can see $R[a]$ inside S as the image of the ring homomorphism

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

Recall from Linear Algebra:

Proposition 4.5 (Cramer's rule). *Let R be a ring and $M = (m_{i,j})_{1 \leq i,j \leq n}$ be an $n \times n$-matrix with entries in R. The* adjoined matrix *is defined as $M^* = (m^*_{i,j})_{1 \leq i,j \leq n}$ with entries*

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

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

Then the following equation holds:

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

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

Proposition 4.6. *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) ⇒ (ii): As a is integral over R, a relation of the form

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

holds. Hence, $R[a]$ can be generated as an R-module by $\{1, a, a^2, \ldots, a^{n-1}\}$.

(ii) ⇒ (iii): Just take $T := R[a]$.

(iii) ⇒ (iv): Take the same T.

(iv) ⇒ (i): We must make a monic polynomial with coefficients in R annihilating a. For this we use Cramer's rule. As T is finitely generated as an R-module, we may pick a finite generating set $\{t_1, \ldots, t_n\}$, i.e. any element of $t \in T$ can be represented as $t = \sum_{j=1}^{n} r_j t_j$ with some $r_j \in R$ for $j \in \{1, \ldots, n\}$.

In particular, as multiplication by a sends T to itself, at_i can be written as

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

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

$$M \begin{pmatrix} t_1 \\ t_2 \\ \vdots \\ t_n \end{pmatrix} = 0$$

By Cramer's rule, it follows

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

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

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

Hence,

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

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

Corollary 4.7. *Let S be a ring and R a subring. Furthermore, let $a_1,\dots,a_n \in S$ be elements that are integral over R.*

Then $R[a_1,\dots,a_n] \subseteq S$ is integral over R and it is finitely generated as an R-module.

Proof. Note that due to the implication (iii) ⇒ (i) of the Proposition it suffices to prove finite generation. We do this by induction. The case $n = 1$ is the implication (i) ⇒ (ii) of the Proposition.

Assume the corollary is proved for $n-1$. Then we know that $R[a_1,\dots,a_{n-1}]$ is finitely generated as an R-module, say, generated by $b_1,\dots,b_m$. As a_n is integral over R, we have that $R[a_n]$ is generated by $1, a_n, a_n^2, \dots, a_n^r$ for some $r \in \mathbb{N}$. Now, $R[a_1,\dots,a_{n-1},a_n]$ is generated by $b_i a_n^j$ with $i \in \{1,\dots,m\}$ and $j \in \{0,\dots,r\}$. □

Corollary 4.8. *Let $R \subseteq S \subseteq T$ be rings. Then 'transitivity of integrality' holds:*

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

Proof. This works precisely as for algebraic field extensions!

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

Corollary 4.9. *Let $R \subseteq S$ be rings.*

(a) R_S is a subring of S.

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

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

(b) Any $s \in S$ that is integral over R_S is also integral over R (by the transitivity of integrality), whence $s \in R_S$. □

Definition 4.10. *Recall that a* number field *K is a finite field extension of $\mathbb{Q}$. The* ring of integers of *K is the integral closure of $\mathbb{Z}$ in K, i.e. $\mathbb{Z}_K$. An alternative notation is $\mathcal{O}_K$.*

Example 4.11. *Let $d \neq 0, 1$ be a squarefree integer. The ring of integers of $\mathbb{Q}(\sqrt{d})$ is*

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

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

(Proof as an exercise.)

Proposition 4.12. *Every factorial ring is integrally closed.*

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

Start with the equation annihilating x:

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

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

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

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

Proposition 4.13. *Let R be an integral domain, $K = \mathrm{Frac}(R)$, L/K a finite field extension and $S := R_L$ the integral closure of R in L. Then the following statements hold:*

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

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

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

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

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

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

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

showing that da is integral over R, i.e. $da \in S$, or in other words, $a = \frac{s}{d}$ for some $s \in S$.

(b) By (a) we know that L is contained in the fraction field of S. As S is contained in L, it is clear that also the fraction field of S is contained in L, showing the claimed equality. That S is integrally closed means that it is integrally closed in L. We have already seen that the integral closure of R in L is integrally closed in L.

(c) This is just by definition: If $s \in S$, then it is integral over R; if s is also in K, then as R is integrally closed (in K), it follows that $s \in R$. The other inclusion $S \cap K \supseteq R$ is trivial. □

We now add two propositions for whose proof one needs more field theory than what we have developed in this lecture. The kind of field theory we need is taught in any lecture on Galois theory.

Proposition 4.14. *Let R be an integral domain which is integrally closed (recall: that means integrally closed in $K = \mathrm{Frac}(R)$). Let $\overline{K}$ be an algebraic closure of K and let $a \in \overline{K}$. Then the following statements are equivalent:*

(i) a is integral over R.

(ii) The minimal polynomial $m_a \in K[X]$ of a over K has coefficients in R.

Proof. '(ii) ⇒ (i)': Since by assumption $m_a \in R[X]$ is a monic polynomial annihilating a, by definition a is integral over R.

'(i) ⇒ (ii)': Let $L := K(a) \subseteq \overline{K}$. Consider the set

$$\mathcal{S} := \{a_1 = a, a_2, \dots, a_n\} := \{\sigma(a) \mid \sigma : L \to \overline{K} \text{ field homomorphism s.t. } \sigma(x) = x \; \forall x \in K\}.$$

From field theory it is known that the minimal polynomial of a has the shape

$$f_a(X) = \prod_{i=1}^{n}(X - a_i) \in K[X].$$

Let us recall how this is proved. Of course, $f_a(a) = 0$ because $a = a_1$. But, à priori, f_a only has coefficients in $\overline{K}$ (the normal closure of L in $\overline{K}$ would suffice). Let now $\sigma : \overline{K} \to \overline{K}$ be any field homomorphism which is the identity on K. Then σ permutes the elements in the set $\mathcal{S}$. Hence, letting σ act on (the coefficients of) f_a, we see that it fixes f_a, i.e. it fixes all the coefficients of f_a. This means that all the coefficients of f_a are in K. If f_a were not irreducible, then it would factor as (possibly renumbering the $a_2, \dots, a_n$)

$$f(X) = \big(\prod_{i=1}^{r}(X - a_i)\big) \cdot \big(\prod_{i=r+1}^{n}(X - a_i)\big)$$

where both factors are polynomials in $K[X]$ and we assume the first factor to be irreducible. Then $K(a, a_2, \dots, a_r)$ would be a normal field extension of K. This, however, means that the set $\mathcal{S}$ only consists of $a = a_1, a_2, \ldots, a_r$, contradiction. So, $f_a = m_a \in K[X]$ is the minimal polynomial of a over K.

We assume that a is integral over R, so there is some monic polynomial $g_a \in R[X]$ annihilating a. It follows that f_a divides g_a. Consequently, $g_a(a_i) = 0$ for all $i = 1, \ldots, n$, proving that also $a_2, a_3, \ldots, a_n$ are integral over R. Hence, f_a has integral coefficients over R (they are products and sums of the a_i). As R is integrally closed in K, the coefficients lie in R. □

Proposition 4.15. *Let R be an integral domain, $K = \mathrm{Frac}(R)$, L/K a finite Galois extension with Galois group $G = \mathrm{Gal}(L/K)$ and $S := R_L$ the integral closure of R in L.*

Then $\sigma(S) = S$ for all $\sigma \in G$. Moreover, if R is integrally closed, then

$$S^G := \{s \in S \mid \sigma(s) = s \; \forall \sigma \in G\}$$

is equal to R.

Proof. Let $a \in S$ and $g \in R[X]$ monic such that $g(a) = 0$. As $0 = \sigma(0) = \sigma(g(a)) = g(\sigma(a))$ for all $\sigma \in G$, it follows that $\sigma(a)$ is also integral over R, i.e. that $\sigma(a) \in S$, showing $\sigma(S) \subseteq S$. Equality follows from σ being invertible.

To see the final statement, just consider

$$S^G = S \cap L^G = S \cap K = R$$

because of (c) in Proposition 4.13 and $L^G = K$. Here L^G is, of course, the set of elements of L that are fixed by all $\sigma \in G$. □

5 Affine plane curves

Definition 5.1. *Let K be a field and L/K a field extension. Let $n \in \mathbb{N}$. The set of L-*points of affine n-space *is defined as $\mathbb{A}^n(L) := L^n$ (i.e. n-dimensional L-vector space).*

Let $S \subseteq K[X_1, \ldots, X_n]$ be a subset. Then

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

*is called the set of L-*points of the affine (algebraic) set belonging to S.

If $L = \overline{K}$ is an algebraic closure of K, then we also call $\mathcal{V}_S(\overline{K})$ the affine set belonging to S.

If the set S consists of a single non-constant polynomial, then $\mathcal{V}_S(\overline{K})$ is also called a hyperplane in $\mathbb{A}(\overline{K})$.

If $n = 2$ and $S = \{f\}$ with non-constant f, then $\mathcal{V}_S(\overline{K})$ is called a plane curve *(because it is a curve in the plane $\mathbb{A}^2(\overline{K})$. Its L-points are defined as $\mathcal{V}_S(L)$ for L/K a field extension.*

Convention: When the number of variables is clear, we write $K[\underline{X}]$ for $K[X_1, \ldots, X_n]$. In the same way a tuple $(x_1, \ldots, x_n) \in \mathbb{A}^n(K)$ is also abbreviated as $\underline{x}$ if no confusion can arise.

The letter ‘V’ is chosen because of the word ‘variety’. But, we will define affine varieties below as ‘irreducible’ affine sets.

Example 5.2. *(a) $K = \mathbb{R}$, $n = 2$, $K[X,Y] \ni f(X,Y) = aX + bY + c$ non-constant. Then $V_{\{f\}}(\mathbb{R})$ is a line ($y = -\frac{a}{b}x - \frac{c}{b}$ if $b \neq 0$; if $b = 0$, then it is the line with x-coordinate $-\frac{c}{a}$ and any y-coordinate).*

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

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

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

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

which is a line.

Lemma 5.3. *A plane curve has infinitely many points over any algebraically closed field. More precisely, let K be a field, $\overline{K}$ an algebraic closure of K and $f(X,Y) \in K[X,Y]$ a non-constant polynomial.*

Then $\mathcal{V}_{\{f\}}(\overline{K})$ is an infinite set.

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

Back to the proof. We consider f as a polynomial in the variable Y with coefficients in $K[X]$, i.e.

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

First case: $d = 0$, i.e. $f(X,Y) = a_0(X)$. Let $x \in \overline{K}$ be any zero of $a_0(x)$, which exists as $\overline{K}$ is algebraically closed. Now (x,y) satisfies f for any $y \in \overline{K}$, showing the infinity of solutions.

Second case: $d > 0$. Then $a_d(x) \neq 0$ for all but finitely many $x \in \overline{K}$, hence, for infinitely many x. Note that the polynomial $f(x,Y) = \sum_{i=0}^{d} a_i(x)Y^i$ has at least one zero y, so that (x,y) satisfies f, again showing the infinity of solutions. □

Example 5.4. *Let K be a field and consider $f(X,Y) = X^2 + Y^2$.*

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

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

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

Example 5.5. *Let K be a field and $f(X) = X^3 + aX^2 + bX + c$ be a separable polynomial (meaning that it has no multiple zeros over $\overline{K}$).*

Any plane curve of the form $\mathcal{V}_{\{Y^2 - f(X)\}}$ is called an elliptic curve. *It has many special properties (see e.g. lectures on cryptography).*

Definition 5.6. *Let $\mathcal{X}$ be a set and $\mathcal{O}$ a set of subsets of $\mathcal{X}$ (i.e. the elements of $\mathcal{O}$ are sets; they are called the* open sets*).*

Then $\mathcal{O}$ is called a topology on $\mathcal{X}$ *(alternatively: $(\mathcal{X}, \mathcal{O})$ is called a* topological space*) if*

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

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

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

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

Proposition 5.7. *Let K be a field and $n \in \mathbb{N}$. Define*

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

Then $(\mathbb{A}^n(K), \mathcal{O})$ is a topological space. The thus defined topology is called the Zariski topology on *$\mathbb{A}^n(K)$.*

Note that, in particular, the closed subsets of $\mathbb{A}^n(K)$ for the Zariski topology are precisely the affine sets.

Before we prove this proposition, we include the following lemma. Recall that the sum and the product of two ideals $\mathfrak{a}, \mathfrak{b}$ of some ring R are defined as

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

It is clear that both are ideals.

Lemma 5.8. *Let K be a field, L/K a field extension and $n \in \mathbb{N}$.*

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

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

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

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

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

Proof. (a) and (b) are clear.

(c) Let $\underline{x} \in \mathbb{A}^n(L)$. Then

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

(d) The inclusion $\mathcal{V}_{\mathfrak{a}}(L) \subseteq \mathcal{V}_S(L)$ follows from (b). Let now $\underline{x} \in \mathcal{V}_S(L)$, meaning that $f(\underline{x}) = 0$ for all $f \in S$. Since any $g \in \mathfrak{a}$ can be written as a sum of products of elements from S, it follows that $g(\underline{x}) = 0$, proving the reverse inclusion.

(e) Since $\mathfrak{ab} \subseteq \mathfrak{a}$ and $\mathfrak{ab} \subseteq \mathfrak{b}$, (b) gives the inclusions $\mathcal{V}_{\mathfrak{a}}(L), \mathcal{V}_{\mathfrak{b}}(L) \subseteq \mathcal{V}_{\mathfrak{ab}}(L)$, hence $\mathcal{V}_{\mathfrak{a}}(L) \cup \mathcal{V}_{\mathfrak{b}}(L) \subseteq \mathcal{V}_{\mathfrak{ab}}(L)$. For the reverse inclusion, let $\underline{x} \notin \mathcal{V}_{\mathfrak{a}}(L) \cup \mathcal{V}_{\mathfrak{b}}(L)$, meaning that there exists $f \in \mathfrak{a}$ and $g \in \mathfrak{b}$ such that $f(\underline{x}) \neq 0 \neq g(\underline{x})$. Thus, $f(\underline{x}) \cdot g(\underline{x}) \neq 0$, whence $\underline{x} \notin \mathcal{V}_{\mathfrak{ab}}(L)$. □

Proof of Proposition 5.7. We need to check the axioms (1), (2) and (3). Note that (1) is Lemma 5.8 (a).

(2) For open sets $\mathbb{A}^n(L) \setminus \mathcal{V}_{S_i}(L)$ with $S_i \subseteq K[\underline{X}]$ for $i \in I$, we have: $\bigcup_{i\in I} \mathbb{A}^n(L) \setminus \mathcal{V}_{S_i}(L) = \mathbb{A}^n(L) \setminus \bigcap_{i\in I} \mathcal{V}_{S_i}(L) \overset{\text{Lemma 5.8(c)}}{=} \mathbb{A}^n(L) \setminus \mathcal{V}_{\bigcup_{i\in I} S_i}(L)$.

(3) By Lemma 5.8 (d), any two open sets are of the form $\mathbb{A}^n(L) \setminus \mathcal{V}_{\mathfrak{a}}(L)$ and $\mathbb{A}^n(L) \setminus \mathcal{V}_{\mathfrak{b}}(L)$ with ideals $\mathfrak{a}, \mathfrak{b} \lhd K[\underline{X}]$. It follows: $(\mathbb{A}^n(L) \setminus \mathcal{V}_{\mathfrak{a}}(L)) \cap (\mathbb{A}^n(L) \setminus \mathcal{V}_{\mathfrak{b}}(L)) = \mathbb{A}^n(L) \setminus (\mathcal{V}_{\mathfrak{a}}(L) \cup \mathcal{V}_{\mathfrak{b}}(L)) \overset{\text{Lemma 5.8(e)}}{=} \mathbb{A}^n(L) \setminus \mathcal{V}_{\mathfrak{a}\cdot\mathfrak{b}}(L)$. □

Definition 5.9. *Let $\mathcal{X}$ be a subset of $\mathbb{A}^n(K)$. We define the* vanishing ideal of $\mathcal{X}$ *as*

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

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

Lemma 5.10. *(a) The vanishing ideal is indeed an ideal of $K[\underline{X}]$.*

(b) The ring homomorphism

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

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

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

We may even replace $\mathrm{Maps}(\mathcal{X}, K)$ by $\mathcal{C}(\mathcal{X}, \mathbb{A}^1(K))$, the continuous maps for the Zariski topology (see exercise on Sheet 6).

The coordinate ring consists hence of the polynomial functions from $\mathcal{X}$ to K. There are some special ones, namely, the projection to the i-th coordinate, i.e. $(x_1, \dots, x_n) \mapsto x_i$; this clearly deserves the name *i-th coordinate function*; let us denote it by $\mathfrak{x}_i$. The name *coordinate ring* is hence explained! Note that any function $f(X_1, \dots, X_n) + \mathcal{I}_{\mathcal{X}} = \sum a_{i_1,\dots,i_n} X_1^{i_1} \dots X_n^{i_n} + \mathcal{I}_{\mathcal{X}}$ is a combination of the coordinate functions, namely, $\sum a_{i_1,\dots,i_n} \mathfrak{x}_1^{i_1} \dots \mathfrak{x}_n^{i_n}$.

Lemma 5.11. *Let K be a field and $n \in \mathbb{N}$. Then the following statements hold:*

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

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

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

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

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

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

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

Proof. Exercise on Sheet 6. □

Lemma 5.12. *Let $(\mathcal{X}, \mathcal{O}_{\mathcal{X}})$ be a topological space and $\mathcal{Y} \subseteq \mathcal{X}$ be a subset. Define $\mathcal{O}_{\mathcal{Y}} := \{U \cap \mathcal{Y} \mid U \in \mathcal{O}_{\mathcal{X}}\}$.*

Then $\mathcal{O}_{\mathcal{Y}}$ is a topology on $\mathcal{Y}$, called the relative topology *or the* subset topology.

Proof. Exercise on Sheet 6. □

Definition 5.13. *Let $\mathcal{X}$ be a topological space (we do not always mention $\mathcal{O}$ explicitly).*

A subset $\mathcal{Y} \subseteq \mathcal{X}$ is called reducible *if there are two closed subsets $\mathcal{Y}_1, \mathcal{Y}_2 \subsetneq \mathcal{Y}$ for the relative topology on $\mathcal{Y}$ such that $\mathcal{Y} = \mathcal{Y}_1 \cup \mathcal{Y}_2$.*

If $\mathcal{Y}$ is not reducible, it is called irreducible.

An affine set $\mathcal{X} \subseteq \mathbb{A}^n(K)$ is called an affine variety *if $\mathcal{X}$ is irreducible.*

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

(i) $\mathcal{X}$ is irreducible (i.e. $\mathcal{X}$ is a variety).

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

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

Proof. The equivalence of (ii) and (iii) was shown directly after the definition of a prime ideal (recall $K[\mathcal{X}] = K[\underline{X}]/\mathcal{I}_{\mathcal{X}}$).

(i) ⇒ (ii): Suppose $\mathcal{I}_{\mathcal{X}}$ is not a prime ideal. Then there are two elements $f_1, f_2 \in K[\underline{X}] \setminus \mathcal{I}_{\mathcal{X}}$ such that $f_1 \cdot f_2 \in \mathcal{I}_{\mathcal{X}}$. This, however, implies:

$$\mathcal{X} = \big(\mathcal{V}_{(f_1)}(K) \cap \mathcal{X}\big) \cup \big(\mathcal{V}_{(f_2)}(K) \cap \mathcal{X}\big) = \big(\mathcal{V}_{(f_1)}(K) \cup \mathcal{V}_{(f_2)}(K)\big) \cap \mathcal{X},$$

since $\mathcal{V}_{(f_1)}(K) \cup \mathcal{V}_{(f_2)}(K) = \mathcal{V}_{(f_1 \cdot f_2)}(K) \supseteq \mathcal{X}$. Note that $f_1 \notin \mathcal{I}_{\mathcal{X}}$ precisely means that there is $\underline{x} \in \mathcal{X}$ such that $f_1(\underline{x}) \neq 0$. Hence, $\mathcal{X} \neq \mathcal{V}_{(f_1)}(K) \cap \mathcal{X}$. Of course, the same argument applies with f_1 replaced by f_2, proving that $\mathcal{X}$ is reducible, contradiction.

(ii) ⇒ (i): Suppose $\mathcal{X}$ is reducible, i.e. $\mathcal{X} = \mathcal{X}_1 \cup \mathcal{X}_2$ with $\mathcal{X}_1 \subsetneq \mathcal{X}$ and $\mathcal{X}_2 \subsetneq \mathcal{X}$ closed subsets of $\mathcal{X}$ (and hence closed subsets of $\mathbb{A}^n(K)$, since they are the intersection of some closed set of $\mathbb{A}^n(K)$ with the closed set $\mathcal{X}$). This means $\mathcal{I}_{\mathcal{X}_i} \supsetneq \mathcal{I}_{\mathcal{X}}$ for $i = 1, 2$ as otherwise $\mathcal{X} = \mathcal{X}_i$ by Lemma 5.11. Hence, there are $f_1 \in \mathcal{I}_{\mathcal{X}_1}$ and $f_2 \in \mathcal{I}_{\mathcal{X}_2}$ such that $f_1, f_2 \notin \mathcal{I}_{\mathcal{X}}$. Note that $f_1(\underline{x})f_2(\underline{x}) = 0$ for all $\underline{x} \in \mathcal{X}$, as at least one of the two factors is 0. Thus, $f_1 \cdot f_2 \in \mathcal{I}_{\mathcal{X}}$. This shows that $\mathcal{I}_{\mathcal{X}}$ is not a prime ideal, contradiction. □

6 Direct sums, products and free modules

We first define direct products, then direct sums of modules.

Definition 6.1. *Let R be a ring and M_i for $i \in I$ (some set) R-modules.*

An R-module P together with R-homomorphisms $\pi_i : P \to M_i$ (called projections*) for $i \in I$ is called a* direct product of the M_i for $i \in I$, *notation $\prod_{i \in I} M_i$, if the following universal property holds:*

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

Don't worry; although the definition is abstract, the direct product is the one you expect:

Proposition 6.2. *Let R be a ring and M_i for $i \in I$ (some set) R-modules.*

(a) $P := \prod_{i \in I} M_i$ with component-wise defined addition and R-multiplication together with $\pi_i : P \to M_i$, the projection on the i-th component, is a direct product of the M_i in the sense of the definition.

(b) If P' together with $\pi' : P' \to M_i$ is any other direct product of the M_i then there is a unique R-isomoprhism $P \to P'$.

Proof. (a) We have to check the universal property. Let N and ϕ_i be as in the definition. Define $\phi : N \to P$ by sending $n \in N$ to the element of P, whose i-th component is $\phi_i(n)$. Then clearly, $\pi_i \circ \phi = \phi_i$.

Conversely, if we have any $\phi : N \to P$ such that $\pi_i \circ \phi = \phi_i$, then the i-th component of $\phi(n)$ for $n \in N$ has to be $\phi_i(n)$, showing the uniqueness.

(b) We do not use the special form of P, just the defining properties. Considering P as a direct product and the P' as the module N from the definition, we obtain a unique R-homomorphism $\phi' : P' \to P$ such that $\pi' = \pi_i \circ \phi'$. Exchanging the roles of P and P' we get a unique R-homomorphism $\phi : P \to P'$ such that $\pi = \pi'_i \circ \phi$.

The main point to remember is that $\alpha : P \xrightarrow{\phi} P' \xrightarrow{\phi'} P$ satisfies

$$\pi \circ \alpha = \pi \circ \phi' \circ \phi = \pi' \circ \phi = \pi.$$

Now consider P as a direct product and as the module N from the definition. Then there is a unique R-homomorphism $P \to P$ satisfying the requirements. Our calculation has shown that this R-homomorphism is α. Of course, the identity on P is another one, whence α is the identity, implying that ϕ is injective and ϕ' surjective. Exchanging the roles of P and P' we get that ϕ is surjective and ϕ' injective, whence both are isomorphisms. □

Next we define direct sums. The universal property definition is the one for direct products with reversed arrows.

Definition 6.3. *Let R be a ring and M_i for $i \in I$ (some set) R-modules.*

An R-module S together with R-homomorphisms $\epsilon_i : M_i \to S$ for $i \in I$ is called a direct sum of the M_i for $i \in I$*, notation $\bigoplus_{i \in I} M_i$, if the following universal property holds:*

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

Don't worry; although the definition is abstract, also the direct sum is the one you expect:

Proposition 6.4. *Let R be a ring and M_i for $i \in I$ (some set) R-modules.*

(a) $S := \{(m_i)_{i \in I} \in \prod_{i \in I} M_i \mid m_i = 0$ for all but finitely many $i \in I\}$ with $\epsilon_j : M_j \to S$, sending $m \in M_j$ to the element $(m_i)_{i \in I}$ such that $m_i = m$ and $m_j = 0$ for all $j \in I \setminus \{i\}$, is a direct sum of the M_i in the sense of the definition.

(b) If S' together with $\epsilon'_i : M_i \to S'$ is any other direct sum of the M_i, then there is a unique R-isomoprhism $S \to S'$.

Proof. (a) We have to check the universal property. Let N and ϕ_i be as in the definition. We define $\phi : S \to N$ by sending $(m_i)_{i \in I} \in S$ to $\sum_{i \in I} m_i$. Here we use that only finitely many of the m_i are non-zero, so that we have a finite sum. Of course, $\phi \circ \epsilon_i = \phi_i$.

On the other hand, given $\phi : S \to N$ such that $\phi \circ \epsilon_j = \phi_j$ for $j \in I$ it follows with $(m_i)_{i \in I}$ with $m_j = m$ and $m_i = 0$ for $i \neq j$ that $\phi_j(m) = \phi \circ \epsilon_j(m) = \phi((m_i)_{i \in I})$. However, elements $(m_i)_{i \in I}$ of the chosen form generate S, whence ϕ is uniquely determined.

(b) This is a formal matter and works as in Proposition 6.2 with reversed arrows (see also Exercise on Sheet 7). □

Corollary 6.5. *Let R be a ring and $M_1, \dots, M_n$ be R-modules. Then there is an R-isomorphism $\bigoplus_{i=1}^n M_i \cong \prod_{i=1}^n M_i$.*

Proof. This is obvious from the explicit descriptions given in Propositions 6.2 and 6.4. □

Definition 6.6. *Let R be a ring and I be a set. An R-module F_I together with a map $\epsilon : I \to F_I$ is called* a free R-module over I *if the following universal property holds:*

> *For all R-modules M and all maps $\delta : I \to M$ there is one and only one R-homomorphism $\phi : F_I \to M$ such that $\phi \circ \epsilon = \delta$ (draw diagram).*

Also here, free modules over a set are what you expect.

Proposition 6.7. *Let R be a ring and I be a set. Define $F_I := \bigoplus_{i\in I} R$ and $\epsilon : I \to F_I$ by sending $j \in I$ to the element $(m_i)_{i\in I}$ such that $m_j = 1$ and $m_i = 0$ for all $i \in I \setminus \{j\}$.*

(a) F_I is a free R-module over I.

(b) If G is any other free R-module over I, then there is a unique R-isomorphism $F \to G$.

Proof. Exercise on Sheet 7. □

Definition 6.8. *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 a free generating set.*

A module M having a basis B is called a free R-module. *(Note that at the moment we are making a distinction between free R-modules, and free R-modules over a set I. We see in a moment that this distinction is unnecessary.)*

Lemma 6.9. *Let R be a ring.*

(a) Let I be a set and F_I be the free R-module over I. Then F_I is R-free with basis $B = \{\epsilon(i) \mid i \in I\}$.

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

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

Proof. (a) is clear.

(b) Consider $\delta : B \to M$ given by the identity, i.e. the inclusion of B into M. The universal property of F_B gives an R-homomorphism $\phi : F_B \to M$. As $\phi \circ \epsilon = \delta$, B is in the image of ϕ. As the image contains a set of generators for the whole module M, the image is equal to M, i.e. ϕ is surjective.

(c) Let us identify F_B with $\bigoplus_{b\in B} R$, as in the proposition showing the existence of F_B. Then ϕ is given by $(r_b)_{b\in B} \mapsto \sum_{b\in B} r_b b$. If $(r_b)_{b\in B}$ is in the kernel of ϕ, then $\sum_{b\in B} r_b b = 0$. The freeness of B now implies $r_b = 0$ for all $b \in B$, showing $(r_b)_{b\in B} = 0$, i.e. the injectivity. □

Lemma 6.10. *Let R be a ring and M a finitely generated free R-module. Then all R-bases of M have the same length.*

This length is called the R-rank *or the* R-dimension *of M.*

Proof. We prove this using linear algebra. Let $B = \{b_1, \dots, b_n\}$ and $C = \{C_1, \dots, C_m\}$ with $n \leq m$ be two R-bases of M. Of course, we can express one basis in terms of the other one:

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

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

$$\underline{b} = T\underline{c} \text{ and } \underline{c} = S\underline{b}.$$

Hence, we have $ST = \mathrm{id}_{m \times m}$. Assume $n < m$. Then we can add $m - n$ columns with entries 0 to S on the right and $m - n$ columns with entries 0 to T on the bottom 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. □

Example 6.11. *(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 free.

7 Exact sequences

Definition 7.1. *Let R be a ring and let $a < b \in \mathbb{Z} \cup \{-\infty, \infty\}$. For each $a \leq n \leq b$, let M_n be an R-module. Also let $\phi_n : M_{n-1} \to M_n$ be an R-homomorphism. I.e. if $a, b \in \mathbb{Z}$, then we have the sequence*

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

If $a \in \mathbb{Z}$ and $b = \infty$, then we have

$$M_a \xrightarrow{\phi_{a+1}} M_{a+1} \xrightarrow{\phi_{a+2}} M_{a+2} \xrightarrow{\phi_{a+3}} \dots,$$

with the sequence being unbounded on the right. If $a = -\infty$ and $b = \infty$, we have

$$\dots \xrightarrow{\phi_{n-1}} M_{n-1} \xrightarrow{\phi_n} M_n \xrightarrow{\phi_{n+1}} M_{n+1} \xrightarrow{\phi_{n+2}} \dots$$

with the sequence being bounded on both sides. The remaining case $a = -\infty$ and $b \in \mathbb{Z}$ is unbounded on the left and should now be obvious.

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

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

We will often consider finite sequences, mostly of the form

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

If a sequence of the form $(*)$ is exact, then it is called a *short exact sequence*.

Lemma 7.2. *Let R be a ring.*

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

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

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

Proof. (a) Just note: $\ker(\alpha) = \mathrm{im}(0 \to A) = \{0\}$.

(b) Just note: $C = \ker(C \to 0) = \mathrm{im}(\alpha)$.

(c) Combine (a) and (b) with the exactness at B. □

Proposition 7.3. *Let R be a ring and M_i, N_i for $i = 1, 2, 3$ be R-modules.*

(a) Let

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

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

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

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

(b) Let

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

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

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

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

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

Proof. (a) '⇒':

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

'$\Leftarrow$':

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

(b) Exercise. □

Definition 7.4. *Let R be a ring. An R-module P is called* projective *if the following universal property holds:*

> *For all R-modules M, N, all surjective R-homomorphisms $\phi : M \to N$ and all R-homomorphisms $\psi : P \to N$ there is an R-homomorphism $\tilde{\psi} : P \to M$ such that $\phi \circ \tilde{\psi} = \psi$ (draw diagram).*
>
> *In other words, the R-homomorphism $\mathrm{Hom}_R(P, M) \xrightarrow{\tilde{\psi} \mapsto \phi \circ \tilde{\psi}} \mathrm{Hom}_R(P, N)$ is surjective.*

An R-module I is called injective *if the following universal property holds (note: same property as for projective modules, but, with arrow directions reversed and surjective replaced by injective):*

> *For all R-modules M, N, all injective R-homomorphisms $\phi : N \to M$ and all R-homomorphisms $\psi : N \to P$ there is an R-homomorphism $\tilde{\psi} : M \to P$ such that $\tilde{\psi} \circ \phi = \psi$ (draw diagram).*
>
> *In other words, the R-homomorphism $\mathrm{Hom}_R(M, I) \xrightarrow{\tilde{\psi} \mapsto \tilde{\psi} \circ \phi} \mathrm{Hom}_R(N, I)$ is surjective.*

Corollary 7.5. *Let R be a ring and P, I R-modules.*

1. *P is projective if and only if the covariant functor $\mathrm{Hom}_R(P, \cdot)$ is exact (i.e. maps exact sequences to exact sequences).*
2. *I is injective if and only if the contravariant functor $\mathrm{Hom}_R(\cdot, I)$ is exact.*

Proof. Both follow immediately from Proposition 7.3 and the 'In other words' part of the definition. □

Corollary 7.6. *Let R be a ring.*

(a) Let P be a projective R-module. Then every short exact sequence of R-modules

$$0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} P \to 0$$

is split, i.e. there is an R-homomorphism $\gamma : P \to B$ such that $\beta \circ \gamma$ is the identity on P.

(b) Let I be an injective R-module. Then every short exact sequence of R-modules

$$0 \to I \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0$$

is split, i.e. there is an R-homomorphism $\delta : B \to I$ such that $\delta \circ \alpha$ is the identity on I.

Proof. Just apply the universal property to the identity on P, respectively on I. □

Note that by an Exercise on Sheet 7, (a) means that $B \cong A \oplus P$ and (b) means $B \cong I \oplus C$.

Proposition 7.7. *Let R be a ring, M, N, M_i and N_i for $i \in I$ (some set) be R-modules. Then there are natural R-isomorphisms:*

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

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

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

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

It is clear that Φ is an R-homomorphism.

Let $\varphi \in \mathrm{Hom}_R(M, \prod_{i\in I} N_i)$ such that $\Phi(\varphi) = 0$. This means $\pi_i \circ \varphi = 0$ for all $i \in I$. Now we use the universal property of $\prod_{i\in I} N_i$. Namely, there is a unique R-homomorphism $M \to \prod_{i\in I} N_i$ for given $M \to N_i$. As these maps are all zero, certainly the zero map $M \to \prod_{i\in I} N_i$ satisfies the universal property. Consequently, $\varphi = 0$. This shows that Φ is injective.

Now for the surjectivity. Suppose hence that we are given $\varphi_i : M \to N_i$ for each $i \in I$. Then the universal property of $\prod_{i\in I} N_i$ tells us that there is a unique $\varphi : M \to \prod_{i\in I} N_i$ such that $\varphi_i = \pi_i \circ \varphi$ for all $i \in I$. This is precisely the required preimage. Actually, we could have skipped the proof of injectivity because the uniqueness of φ gives us a unique preimage, which also implies injectivity.

(b) Exercise on Sheet 7. □

Lemma 7.8. *Let R be a ring and M an R-module. Then the map*

$$\Phi : Hom_R(R, M) \to M, \quad \Phi(\alpha : R \to M) := \alpha(1)$$

is an R-isomorphism.

Proof. Clear. □

Proposition 7.9. *Let R be a ring and F a free R-module. Then F is projective.*

Proof. Let B be an R-basis of F, so that we can identify F with F_B; we have the inclusion $\epsilon : B \to F_B$. We check that F satisfies the universal property of a projective module. Let hence $\phi : M \twoheadrightarrow N$ be a surjective R-homomorphism and $\psi : F \to N$ an R-homomorphism. For each $b \in B$ choose an $m_b \in M$ such that $\phi(m_b) = \psi(b)$, using the surjectivity of ϕ.

Consider the map $\delta : B \to M$ sending $b \in B$ to m_b. By the universal property of F_B there exists the required $\tilde{\psi}$. □

Corollary 7.10. *Let R be a ring and P an R-module. Then the following statements are equivalent:*

(i) P is projective.

(ii) P is a direct summand of a free R-module F, i.e. there is an R-module X such that $P \oplus X \cong F$.

Proof. '(i) ⇒ (ii)': Let F be a free R-module having P as a quotient. In other words, we have an exact sequence

$$0 \to X \to F \to P \to 0.$$

As this exact sequence splits, we get $F \cong X \oplus P$.

'(ii) ⇒ (i)': Let $F = X \oplus P$ be a free R-module. We check the universal property of a projective module for P. Let hence $\phi : M \twoheadrightarrow N$ be a surjective R-homomorphism and $\psi : P \to N$ an R-homomorphism. Consider now the surjection $\mathrm{id}_X \oplus \phi : X \oplus M \twoheadrightarrow X \oplus N$ and the R-homomorphism $\mathrm{id}_X \oplus \psi : F = X \oplus P \to X \oplus N$. As F is free, it is projective, giving some $\alpha : F = X \oplus P \to X \oplus M$ such that $(\mathrm{id}_X \oplus \phi) \circ \alpha = \mathrm{id}_X \oplus \psi$. Let $p \in P$ and $(x, m) := \alpha((0, p))$. Let us set $\tilde{\psi}(p) := m$; this defines an R-homomorphism. Then we have

$$(\mathrm{id}_X \oplus \phi) \circ \alpha((0, p)) = (\mathrm{id}_X \oplus \phi)((x, m)) = (x, \phi(m)) = (0, \psi(p)).$$

Hence, $\phi \circ \tilde{\psi}(p) = \psi(p)$, as was to be shown. □

8 Tensor products

In this section we shall for the sake of generality consider general unitary rings, i.e. not necessarily commutative ones.

Definition 8.1. *Let R be a ring, M a right R-module and N a left R-module.*

Let P be a $\mathbb{Z}$-module (note that this just means abelian group). A $\mathbb{Z}$-bilinear map

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

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

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

In this case, we call (P, f) a balanced product of M and N.

A balanced product $(M \otimes_R N, \otimes)$ is called a tensor product of M and N over R *if the following universal property holds:*

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

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

Proposition 8.2. *Let R be a ring, M a right R-module and N a left R-module.*

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

Proof. The uniqueness statement is a consequence of the uniqueness in the universal property (Exercise Sheet 8).

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

Define G as the $\mathbb{Z}$-submodule of F generated by the following elements:

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

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

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

It is $\mathbb{Z}$-bilinear and balanced by construction.

We now need to check the universal property. Let hence (P, f) be a balanced product of M and N. First we use the universal property of the free module $F = \mathbb{Z}[M \times N]$. For that let $\epsilon : M \times N \to F$

denote the inclusion. We obtain a unique group homomorphism $\phi : F \to P$ such that $\phi \circ \epsilon = f$ (draw diagram).

Claim: $G \subseteq \ker(\phi)$. Note first that $f(m, n) = \phi \circ \epsilon(m, n) = \phi((m, n))$ for all $m \in M$ and all $n \in N$. In particular, we have due to the bilinearity of f for all $m_1, m_2 \in M$ and all $n \in N$:

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

whence $(m_1 + m_2, n) - (m_1, n) - (m_2, n) \in \ker(\phi)$. In the same way one shows that the other two kinds of elements also lie in $\ker(\phi)$, implying the claim.

Due to the claim, ϕ induces a homomorphism $\phi : F/G \to P$ such that $\phi \circ \otimes = f$ (note that $\otimes$ is just ϵ composed with the natural projection $F \to F/G$).

As for the uniqueness of ϕ. Note that the image of $\otimes$ is a generating system of F/G. Its elements are of the form $m \otimes n$. As we have $\phi \circ \otimes(m, n) = \phi(m \otimes n) = f(m, n)$, the values of ϕ at the generating set are prescribed and ϕ is hence unique. □

Example 8.3. *(a) Let $R = \mathbb{Z}$, $M = \mathbb{Z}/(m)$ and $N = \mathbb{Z}/(n)$ with $\gcd(m, n) = 1$. Then $M \otimes N = \mathbb{Z}/(m) \otimes_{\mathbb{Z}} \mathbb{Z}/(n) = 0$.*

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

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

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

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

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

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

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

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

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

Next we need to consider tensor products of maps.

Proposition 8.4. *Let R be a ring, $f : M_1 \to M_2$ a homomorphism of right R-modules and $g : N_1 \to N_2$ a homomorphism of left R-modules. Then there is a unique group homomorphism*

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

such that $f \otimes g(m \otimes n) = f(m) \otimes g(n)$.

The map $f \otimes g$ is called the tensor product *of f* and *g.*

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

Lemma 8.5. *Let $M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} M_3$ be homomorphisms of right R-modules and $N_1 \xrightarrow{g_1} N_2 \xrightarrow{g_2} N_3$ homomorphisms of left R-modules.*

Then $(f_2 \otimes g_2) \circ (f_1 \otimes g_1) = (f_2 \circ f_1) \otimes (g_2 \circ g_1)$.

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

Corollary 8.6. *Let $f : M_1 \to M_2$ be a homomorphism of right R-modules and $g : N_1 \to N_2$ be a homomorphism of left R-modules.*

Then $f \otimes g = (\mathrm{id}_{M_2} \otimes g) \circ (f \otimes \mathrm{id}_{N_1}) = (f \otimes \mathrm{id}_{N_2}) \circ (\mathrm{id}_{M_1} \otimes g)$.

Proof. This follows immediately from the previous lemma. □

Proposition 8.7. *Let R be a ring.*

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

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

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

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

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

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

Proof. We only prove (a), as (b) works in precisely the same way.

First we show the existence of the claimed homomorphism Φ by using the universal property of the tensor product. Define the map

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

This map makes $\bigoplus_{i\in I}(M_i \otimes_R N)$ into a balanced product of $\bigoplus_{i\in I} M_i$ and N, whence by the universal property of the tensor product the claimed homomorphism exists (and is unique).

Next we use the universal property of the direct sum to construct a homomorphism Ψ in the opposite direction, which will turn out to be the inverse of Φ. Let $j \in I$. By ϵ_j denote the embedding of M_j into the j-th component of $\bigoplus_{i\in I} M_i$. From these we further obtain maps $M_j \otimes_R N \xrightarrow{\epsilon_j \otimes \mathrm{id}_N} (\bigoplus_{i\in I} M_i) \otimes_R N$. Further consider the embeddings ι_j of $M_j \otimes_R N$ into the j-th component of $\bigoplus_{i\in I}(M_i \otimes_R N)$ from the definition of a direct sum. The universal property of direct sums now yields a homomorphism $\Psi : \bigoplus_{i\in I}(M_i \otimes_R N) \to (\bigoplus_{i\in I} M_i) \otimes_R N$ such that $\Psi \circ \iota_j = \epsilon_j \otimes \mathrm{id}_N$ for all $j \in J$.

Now it is easy to compute on generators that $\Phi \circ \Psi = \mathrm{id}$ and $\Psi \circ \Phi = \mathrm{id}$. □

Lemma 8.8. *Let R be a commutative ring , and M, N R-modules. Then $M \otimes_R N \cong N \otimes_R M$.*

Proof. Exercise. □

Example 8.9. *Let L/K be a field extension. Then $L \otimes_K K[X]$ is isomorphic to $L[X]$ as an L-algebra.*

Lemma 8.10. *Let R and S be rings. Let M be a right R-module, P a left S-module, N a right S-module and a left R-module such that $(rn)s = r(ns)$ for all $r \in R$, all $s \in S$ and all $n \in N$.*

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

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

(c) There is an isomorphism

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

Proof. Exercise. □

Lemma 8.11. *Let R be a ring, M a right R-module, N a left R-module and P a $\mathbb{Z}$-module.*

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

(b) There is an isomorphism of abelian groups:

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

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

(d) There is an isomorphism of abelian groups:

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

Proof. (a) and (c): Simple checking.

(b) The key point is the following bijection:

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

which is given by

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

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

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

Now it suffices to use the universal property of the tensor product. The details are dealt with in an exercise.

(d) is similar to (b). □

Proposition 8.12. *Let R be a ring.*

(a) *Let N be a left R-module and M_1, M_2, M_3 be right R-modules. If the sequence*

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

is exact, then so is the sequence

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

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

(b) *Let M be a right R-module and N_1, N_2, N_3 be left R-modules. If the sequence*

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

is exact, then so is the sequence

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

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

Proof. We only prove (a), since (b) works precisely in the same way. We use Proposition 7.3 and obtain the exact sequence:

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

for any $\mathbb{Z}$-module P. By Lemma 8.11 this exact sequence is nothing else but:

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

As P was arbitrary, again from Proposition 7.3 we obtain the exact sequence

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

as claimed. □

9 More on modules

In this section we collect and prove important 'basic' statements on modules.

We first need the existence of maximal ideals.

Proposition 9.1. *Let R be a ring different from the zero-ring. Then R has a maximal ideal.*

Proof. This proof uses Zorn's Lemma (which one also needs for the existence of bases in general (i.e. not finite dimensional) vector spaces).

Let $\mathcal{M} := \{\mathfrak{a} \subsetneq R \text{ ideal }\}$ be the set of all proper ideals of R. Of course, $(0) \in \mathcal{M}$ (here we use that R is not the zero ring), so $\mathcal{M} \neq \emptyset$.

Inclusion $\subseteq$ gives a partial ordering on $\mathcal{M}$: by definition this means:

- $\mathfrak{a} \subseteq \mathfrak{a}$ for all $\mathfrak{a} \in \mathcal{M}$,

- If $\mathfrak{a} \subseteq \mathfrak{b}$ and $\mathfrak{b} \subseteq \mathfrak{a}$, then $\mathfrak{a} = \mathfrak{b}$.

But, for general $\mathfrak{a}, \mathfrak{b} \in \mathcal{M}$, we do not necessarily have $\mathfrak{a} \subseteq \mathfrak{b}$ or $\mathfrak{b} \subseteq \mathfrak{a}$. A subset $(\mathfrak{a}_i)_{i \in I} \subseteq \mathcal{M}$ (where I is any set) is called totally ordered if for any $i, j \in I$ one has $\mathfrak{a}_i \subseteq \mathfrak{a}_j$ or $\mathfrak{a}_j \subseteq \mathfrak{a}_i$.

Claim: Any totally ordered subset $(\mathfrak{a}_i)_{i \in I} \subseteq \mathcal{M}$ has an upper bound, namely $\mathfrak{a} := \bigcup_{i \in I} \mathfrak{a}_i$, meaning $\mathfrak{a} \subseteq \mathcal{M}$ and $\mathfrak{a}_i \subseteq \mathfrak{a}$ for all $i \in I$.

The claim is very easy to see. The last statement $\mathfrak{a}_i \subseteq \mathfrak{a}$ for $i \in I$ is trivial. In order to see that $\mathfrak{a}$ is an ideal, let $x, y \in \mathfrak{a}$. Then there are $i, j \in I$ such that $x \in \mathfrak{a}_i$ and $y \in \mathfrak{a}_j$. Because of $\mathfrak{a}_i \subseteq \mathfrak{a}_j$ or $\mathfrak{a}_j \subseteq \mathfrak{a}_i$, we have that $x + y \in \mathfrak{a}_j$ or $x + y \in \mathfrak{a}_i$, so that $x + y \in \mathfrak{a}$ in both cases. Given $r \in R$ and $x \in \mathfrak{a}$, there is $i \in I$ such that $x \in \mathfrak{a}_i$, whence $rx \in \mathfrak{a}_i$, thus $rx \in \mathfrak{a}$, showing that $\mathfrak{a}$ is an ideal of R. If $\mathfrak{a}$ were equal to the whole ring R, then there would be $i \in I$ such that $1 \in \mathfrak{a}_i$. This, however, would contradict $\mathfrak{a}_i \neq R$. Consequently, $\mathfrak{a} \in \mathcal{M}$, as claimed.

Zorn's Lemma is the statement that a partially ordered set has a maximal element if every totally ordered set of subsets has an upper bound.

So, $\mathcal{M}$ has a maximal element, i.e. an $\mathfrak{m} \in \mathcal{M}$ such that if $\mathfrak{m} \subseteq \mathfrak{a}$ for any $\mathfrak{a} \in \mathcal{M}$, then $\mathfrak{m} = \mathfrak{a}$. This is precisely the definition of a maximal ideal. □

Corollary 9.2. *(a) Every ideal $\mathfrak{a} \subsetneq R$ is contained in some maximal ideal $\mathfrak{m}$ of R.*

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

Proof. (a) Consider the natural projection $\pi : R \mapsto R/\mathfrak{a}$. Let $\overline{\mathfrak{m}}$ be a maximal ideal of $R/\mathfrak{a}$, which exists by Proposition 9.1. 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). □

Definition 9.3. *A ring R is called* local *if it has a single maximal ideal.*

Example 9.4. *(a) Every field K is a local ring, its unique maximal ideal being the zero ideal.*

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

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

Lemma 9.5. *Let R be a ring, M an R-module and $\mathfrak{a} \lhd R$ an ideal. Then $\mathfrak{a}M = \{\sum_{i=1}^n a_i m_i \mid n \in \mathbb{N}, a_i \in \mathfrak{a},\ m_i \in M \text{ for } i = 1, \ldots, n\} \subseteq M$ is an R-submodule of M.*

Proof. Easy checking. □

Lemma 9.6. *Let R be a local ring with unique maximal ideal $\mathfrak{m}$. Then the set of units $R^\times$ of R is precisely the set $R \setminus \mathfrak{m}$.*

Proof. The statement is equivalent to the following: The maximal ideal $\mathfrak{m}$ is equal to the set of non-units.

We already know from Corollary 9.2 (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 $\mathfrak{m} = R$. □

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

Proposition 9.7. *Let R be a ring, $S \subset R$ a multiplicatively closed subset (i.e. for $s_1, s_2 \in S$ we have $s_1 s_2 \in S$) containing* 1.

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

$$(s_1, r_1) \sim (s_2, r_2) \;\Leftrightarrow\; \exists t \in S :\; t(r_1 s_2 - r_2 s_1) = 0.$$

The equivalence class of (s_1, r_1) is denoted by $\frac{r_1}{s_1}$.

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

$$+ : S^{-1}R \times S^{-1}R \to S^{-1}R,\;\; \frac{r_1}{s_1} + \frac{r_2}{s_2} = \frac{r_1 s_2 + r_2 s_1}{s_1 s_2}$$

and

$$\cdot : S^{-1}R \times S^{-1}R \to S^{-1}R,\;\; \frac{r_1}{s_1} \cdot \frac{r_2}{s_2} = \frac{r_1 r_2}{s_1 s_2}.$$

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

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

Proof. Exercise. □

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

$$(s_1, r_1) \sim (s_2, r_2) \;\Leftrightarrow\; r_1 s_2 - r_2 s_1 = 0,$$

provided $0 \notin S$ (if $0 \in S$, then $S^{-1}R$ is always the zero ring, as any element is equivalent to $\frac{0}{1}$).

Example 9.8. *(a) Let R be an integral domain. Then $S = R \setminus \{0\}$ is a multiplicatively closed subset. Then $\mathrm{Frac}(R) := S^{-1}R$ is the field of fractions of R.*

Subexamples:

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

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

(b) Let R be a ring and $\mathfrak{p} \lhd R$ be a prime ideal. Then $S := R \setminus \mathfrak{p}$ is multiplicatively closed and $1 \in S$ and $0 \notin S$.

Then $R_{\mathfrak{p}} := S^{-1}R$ is called the localisation of R at $\mathfrak{p}$.

Subexamples:

(1) Let $R = \mathbb{Z}$ and p a prime number, so that (p) is a prime ideal. Then the localisation of $\mathbb{Z}$ at (p) is $\mathbb{Z}_{(p)}$ and its elements are $\{\frac{r}{s} \in \mathbb{Q} \mid p \nmid s, \gcd(r,s) = 1\}$.

(2) Let K be a field and consider $\mathbb{A}^n(K)$. Let $\underline{a} = (a_1, \ldots, a_n) \in \mathbb{A}^n(K)$.
Let $\mathfrak{p}$ be the kernel of the ring homomorphism

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

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

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

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

(c) 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 $S := \{f^n \mid n \in \mathbb{N}\}$ (use $0 \in \mathbb{N}$) is multiplicatively closed and we can form $S^{-1}R$. This ring is sometimes denoted R_f (Attention: easy confusion is possible).

Subexample:

(1) Let $R = \mathbb{Z}$ and $0 \neq a \in \mathbb{N}$. Let $S = \{a^n \mid n \in \mathbb{N}\}$. Then $S^{-1}\mathbb{Z} = \{\frac{r}{a^n} \in \mathbb{Q} \mid r \in R, n \in \mathbb{N}, \gcd(r, a^n) = 1\}$.

Proposition 9.9. *Let R be a ring and $S \subseteq R$ a multiplicatively closed subset with $1 \in S$. Let $\mu : R \to S^{-1}R$, given by $r \mapsto \frac{r}{1}$.*

(a) The map

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

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

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

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

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

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

(c) The map in (a) defines a bijection between the prime ideals of $S^{-1}R$ and the prime ideals $\mathfrak{p}$ of R such that $S \cap \mathfrak{p} = \emptyset$.

Proof. Exercise. □

Corollary 9.10. *Let R be a ring and $\mathfrak{p} \lhd R$ be a prime ideal. Then the localisation $R_\mathfrak{p}$ of R at $\mathfrak{p}$ is a local ring with maximal ideal $S^{-1}\mathfrak{p}$.*

Proof. Let $S = R \setminus \mathfrak{p}$. Note that $\emptyset = \mathfrak{a} \cap S = \mathfrak{a} \cap (R \setminus \mathfrak{p})$ is equivalent to $\mathfrak{a} \subseteq \mathfrak{p}$.

Hence, Proposition 9.9 (c) gives an inclusion preserving bijection between the prime ideals of $S^{-1}R$ and the prime ideals of R which are contained in $\mathfrak{p}$. The corollary immediately follows. □

Definition 9.11. *Let R be a ring. The* Jacobson radical *is defined as the intersection of all maximal ideals of R:*

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

Lemma 9.12. *Let R a ring and let $\mathfrak{a} \lhd R$ be an ideal which is contained in $J(R)$. Then for any $a \in \mathfrak{a}$, one has $1 - a \in R^\times$.*

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

Proposition 9.13 (Nakayama's Lemma)**.** *Let R be a ring and M a finitely generated R-module. Let $\mathfrak{a} \lhd R$ be an ideal such that $\mathfrak{a} \subseteq J(R)$. Suppose $\mathfrak{a}M = M$. Then $M = 0$.*

Proof. Exercise. □

The following corollary turns out to be very useful in many applications.

Corollary 9.14. *Let R be a local ring with maximal ideal $\mathfrak{m}$ and let M be a finitely generated R-module. Let $m_1, \dots, m_n \in M$ be elements such that their images $\overline{m_i} := m_i + \mathfrak{m}M$ are generators of the quotient module $M/\mathfrak{m}M$.*

Then $m_1, \dots, m_n$ generate M as an R-module.

Proof. Exercise. □

Proposition 9.15. *Let R be a ring, $S \subset R$ a multiplicatively closed subset containing* 1. *Let M be an R-module.*

(a) An equivalence relation on $S \times M$ is defined by

$$(s_1, m_1) \sim (s_2, m_2) \Leftrightarrow \exists t \in S : \ t(s_1m_2 - s_2m_1) = 0.$$

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

$$+ : S^{-1}M \times S^{-1}M \to S^{-1}M, \ \ \frac{m_1}{s_1} + \frac{m_2}{s_2} = \frac{s_2m_1 + s_1m_2}{s_1s_2}$$

and scalar-multiplication

$$\cdot : S^{-1}R \times S^{-1}M \to S^{-1}M, \ \ \frac{r}{s_1} \cdot \frac{m}{s_2} = \frac{rm}{s_1s_2}.$$

The neutral element is $0 := \frac{0}{1}$.

(c) The map $\mu : M \to S^{-1}M$, $m \mapsto \frac{m}{1}$, is an R-homomorphism with kernel $\{m \in M \mid \exists s \in S : sm = 0\}$.

Proof. Easy checking. □

Lemma 9.16. *Let R be a ring, $S \subset R$ multiplicatively closed containing 1. Let M, N be R-modules and $\phi : M \to N$ an R-homomorphism.*

(a) The map

$$\phi_S : S^{-1}M \to S^{-1}N, \quad \frac{m}{s} \mapsto \frac{\phi(m)}{s}$$

is an $S^{-1}R$-homomorphism.

(b) ϕ_S is injective (surjective, bijective) if ϕ is injective (surjective, bijective).

Proof. (a) Easy checking.

(b) Suppose ϕ is injective and let $\phi_S(\frac{x}{s}) = \frac{\phi(x)}{1} = 0$; then there is $s \in S$ such that $0 = s\phi(x) = \phi(sx)$, whence $sx = 0$ and, thus, $\frac{x}{1} = \frac{0}{1}$.

Suppose ϕ is surjective and let $\frac{y}{s} \in S^{-1}N$. There is $x \in M$ such that $\phi(x) = y$, thus $\phi_S(\frac{x}{s}) = \frac{\phi(x)}{s} = \frac{y}{s}$, showing that ϕ_S is surjective. □

Lemma 9.17. *Let R be a ring, $S \subset R$ multiplicatively closed containing 1 and M an R-module. The map*

$$\psi : S^{-1}M \to S^{-1}R \otimes_R M, \quad \frac{m}{s} \mapsto \frac{1}{s} \otimes m$$

is an $S^{-1}R$-isomorphism, where $S^{-1}R \otimes_R M$ is an $S^{-1}R$-module via $\frac{x}{s}.(\frac{y}{t} \otimes m) := (\frac{x}{s}\frac{y}{t}) \otimes m$.

Proof. First we check that ψ is well-defined: Let $\frac{m_1}{s} = \frac{m_2}{t}$, i.e. there is $u \in S$ such that $u(tm_1 - sm_2) = 0$. Now $\frac{1}{s} \otimes m_1 = \frac{tu}{stu} \otimes m_1 = \frac{1}{stu} \otimes tum_1 = \frac{1}{stu} \otimes sum_2 = \frac{su}{stu} \otimes m_2 = \frac{1}{t} \otimes m_2$. That ψ is an $S^{-1}R$-homomorphism is easily checked.

We now construct an inverse to ψ using the universal property of the tensor product. Define

$$f : S^{-1}R \times M \to S^{-1}M, \quad (\frac{x}{s}, m) \mapsto \frac{xm}{s}.$$

This is a balanced map over R. Hence, there is a unique $\mathbb{Z}$-homomorphism $\phi : S^{-1}R \otimes M \to S^{-1}M$ such that $\phi(\frac{x}{s} \otimes m) = \frac{xm}{s}$.

It is clear that ϕ is an $S^{-1}R$-homomorphism and that $\phi \circ \psi$ and $\psi \circ \phi$ are the identity. □

Lemma 9.18. *Let R be a ring and $\mathfrak{m}$ a maximal ideal.*

(a) The natural map $\mu : R \to R_{\mathfrak{m}}$, $r \mapsto \frac{r}{1}$ induces a ring isomorphism

$$R/\mathfrak{m} \cong R_{\mathfrak{m}}/\mathfrak{m}R_{\mathfrak{m}}.$$

(b) Let M be an R-module and denote by $M_{\mathfrak{m}}$ its localisation at $\mathfrak{m}$. Then:

$$M/\mathfrak{m}M \cong M_{\mathfrak{m}}/\mathfrak{m}R_{\mathfrak{m}}M_{\mathfrak{m}}.$$

Proof. Exercise on Sheet 10. □

10 Flat modules

Definition 10.1. *Let R be a not necessarily commutative ring.*

(a) A right R-module M is called flat over R *if for all injective homomorphisms of left R-modules*

$$\varphi : N_1 \to N_2$$

also the group homomorphism

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

is injective.

(b) A left R-module N is called flat over R *if for all injective homomorphisms of right R-modules*

$$\varphi : M_1 \to M_2$$

also the group homomorphism

$$\varphi \otimes \mathrm{id}_N : M_1 \otimes_R N \to M_2 \otimes_R N$$

is injective.

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

(d) A left R-module N is called faithfully flat over R *if N is flat over R and for all R-homomorphisms of right R-modules $\varphi : M_1 \to M_2$, the injectivity of $\varphi \otimes_R \mathrm{id}_N$ implies the injectivity of φ.*

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

Lemma 10.2. *Let R be a not necessarily commutative ring and let M be a right R-module and N be a left R-module.*

(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 10.1 and Proposition 8.12. □

Example 10.3. *(a) $\mathbb{Q}$ is flat as $\mathbb{Z}$-module.*

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

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

Reason: Consider $\mathbb{Z}/(p^2) \to \mathbb{Z}/(p)$, the natural projection (for p a prime), which is not injective. Tensoring with $\mathbb{Q}$ kills both sides (see Example 8.3), so we get $0 \cong \mathbb{Z}/(p^2) \otimes_{\mathbb{Z}} \mathbb{Q} \to \mathbb{Z}/(p) \otimes_{\mathbb{Z}} \mathbb{Q} \cong 0$, which is trivially injective.

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

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

Proposition 10.4. *Let R be a ring and M_i for $i \in I$ be R-modules. Then the following statements are equivalent:*

(i) *M_i is flat over R for all $i \in I$.*

(ii) *$\bigoplus_{i \in I} M_i$ is flat over R.*

Proof. Exercise. This follows from Proposition 8.7 and the injectivity of the direct sum of injective homomorphisms. □

Lemma 10.5. *Let R be a ring (commutative again) and N an R-module.*

(a) *Let $\mathfrak{a} \lhd R$ be an ideal. Then $R/\mathfrak{a} \otimes_R N \cong N/\mathfrak{a}N$.*

(b) *The following statements are equivalent:*

(i) *N is faithfully flat.*

(ii) *N is flat and for all R-modules $M \neq 0$ one has: $M \otimes_R N \neq 0$.*

Proof. (a) Start with the trivial exact sequence

$$0 \to \mathfrak{a} \to R \to R/\mathfrak{a} \to 0$$

of R-modules. Now tensor over R with N and get

$$\mathfrak{a} \otimes_R N \xrightarrow{\psi} R \otimes_R N \xrightarrow{\varphi} R/\mathfrak{a} \otimes_R N \to 0.$$

Use the isomorphism $R \otimes_R N \xrightarrow{r \otimes n \mapsto rn} N$, to place N into the previous exact sequence. Exactness at the centre precisely means $\ker(\varphi) = \operatorname{im}(\psi)$, but $\operatorname{im}(\psi) = \mathfrak{a}N$. Hence, the homomorphism theorem yields $N/\mathfrak{a}N \cong R/\mathfrak{a} \otimes_R N$, as claimed.

(b) '(i) ⇒ (ii)': Let N be faithfully flat. Now let M be an arbitrary R-module and consider the zero map $M \xrightarrow{\varphi} 0$. Of course, this gives rise to the zero map $M \otimes_R N \xrightarrow{\varphi \otimes \mathrm{id}_N} 0$. If $M \otimes_R N = 0$, then $\varphi \otimes \mathrm{id}_N$ is injective. By faithful flatness, it follows that φ is injective, but that is only possible if M is the zero module.

'(ii) ⇒ (i)': Let N be flat and consider any R-homomorphism $\varphi : M_1 \to M_2$. Let $K := \ker(\varphi)$, so that we have the exact sequence

$$0 \to K \to M_1 \xrightarrow{\varphi} M_2.$$

Flatness of N implies that also the sequence

$$0 \to K \otimes_R N \to M_1 \otimes_R N \xrightarrow{\varphi\otimes\mathrm{id}_N} M_2 \otimes_R N.$$

is exact. If $\varphi \otimes \mathrm{id}_N$ is injective, then $K \otimes_R N$ is the zero-module. By assumption, K is the zero module, whence φ is injective, showing the faithful flatness of N. □

Proposition 10.6. *Let R be a ring and N a flat R-module. The following statements are equivalent:*

(i) N is faithfully flat.

(ii) For all maximal ideals $\mathfrak{m} \lhd R$ we have $\mathfrak{m}N \neq N$.

Proof. '(i) ⇒ (ii)': Let $\mathfrak{m}$ be a maximal ideal of R. By the previous lemma we know that $R/\mathfrak{m}\otimes_R N \cong N/\mathfrak{m}N$. Hence, it suffices to show that $R/\mathfrak{m}\otimes_R N$ is not the zero module. But, by the faithful flatness of N, the contrary would mean that $R/\mathfrak{m}$ is the zero module (also, by the previous lemma), which it clearly is not (as $\mathfrak{m} \neq R$).

'(ii) ⇒ (i)': Let M be an arbitrary non-zero R-module. We want to show $M \otimes_R N \neq 0$; this suffices because of the previous lemma. Let $0 \neq m \in M$ be an arbitrary element and consider the homomorphism

$$\varphi : R \to M, \quad r \mapsto rm.$$

Its kernel $\mathfrak{a}$ is a proper ideal of R (since $1m = m \neq 0$); write M_1 for $\mathrm{im}(\varphi)$. By the homomorphism theorem, we thus have

$$R/\mathfrak{a} \cong M_1 \subseteq M.$$

Now we have

$$M_1 \otimes_R N \cong R/\mathfrak{a} \otimes_R N \cong N/\mathfrak{a}N,$$

by the previous lemma. Let $\mathfrak{m}$ be a maximal ideal of R containing $\mathfrak{a}$. Because $N/\mathfrak{m}N$ is non-zero by assumption, it follows that $N/\mathfrak{a}N$ is non-zero, since we have the natural surjection $N/\mathfrak{a}N \to N/\mathfrak{m}N$. So, we have shown $M_1 \otimes_R N \neq 0$. However, the flatness of N implies that $M_1 \otimes_R N$ injects into $M \otimes_R N$, which is consequently also non-zero, as was to be shown. □

Corollary 10.7. *Let R be a ring.*

(a) Projective R-modules are flat over R.

(b) Non-zero free R-modules are faithfully flat over R.

Proof. (a) First note that R is a flat R-module because of the isomorphism $R \otimes_R N \xrightarrow{r\otimes n \mapsto rn} N$. Hence, free R-modules are flat by Proposition 10.4.

Let P be projective. We know that there is an R-module X such that $P \oplus X$ is R-free, and hence flat. Proposition 10.4 '(ii) ⇒ (i)' now gives that P is flat.

(b) Let $F = F_I = \bigoplus_{i\in I} R$ be R-free (with basis I). Let N be an R-module. We compute:

$$F \otimes_R N = (\bigoplus_{i\in I} R) \otimes_R N \cong \bigoplus_{i\in I}(R \otimes_R N) \cong \bigoplus_{i\in I} N.$$

Hence, if $F \otimes_R N = 0$, then $N = 0$. By Lemma 10.5 we conclude that F is faithfully flat over R. □

Corollary 10.8. *Let R be a local ring with maximal ideal $\mathfrak{m}$ and M a finitely generated R-module. Then the following statements are equivalent:*

(i) M is free over R.

(ii) M is a projective R-module.

(iii) M is flat over R.

Proof. The implications '(i) $\Rightarrow$ (ii)' and '(ii) $\Rightarrow$ (iii)' have already been shown. So, we now prove '(iii) $\Rightarrow$ (i)'. Let M be flat over R and let $n = \dim_{R/\mathfrak{m}} M/\mathfrak{m}M$. Using the corollary of Nakayama's Lemma, any $R/\mathfrak{m}$-basis of the $R/\mathfrak{m}$-vector space $M/\mathfrak{m}M$ can be lifted to a set of generators of M as an R-module. Consequently, there is a surjection from the free R-module F of rank n to M, let G be its kernel. Hence, we have the exact sequence

$$0 \to G \to F \to M \to 0.$$

Claim: $\mathfrak{m}F \cap G = \mathfrak{m}G$. Tensor the above sequence with $\mathfrak{m}$ over R and obtain the exact sequence:

$$\mathfrak{m} \otimes_R G \to \mathfrak{m} \otimes_R F \to \mathfrak{m} \otimes_R M \to 0.$$

Using the flatness of F and M and the resulting identifications of $\mathfrak{m} \otimes_R F$ with $\mathfrak{m}F$ and of $\mathfrak{m} \otimes_R M$ with $\mathfrak{m}M$, we obtain that $\mathfrak{m}F \cap G$ is the image of $m \otimes G \to F$, which is $\mathfrak{m}G$, as claimed.

Claim: The following sequence is exact:

$$0 \to G/\mathfrak{m}G \to F/\mathfrak{m}F \to M/\mathfrak{m}M \to 0.$$

We apply the isomorphism theorems:

$$M/\mathfrak{m}M \cong (F/G)/\mathfrak{m}(F/G) \cong (F/G)/((\mathfrak{m}F + G)/G) \cong F/(\mathfrak{m}F + G).$$

Hence, the kernel of the natural surjection $F/\mathfrak{m}F \to M/\mathfrak{m}M$ is isomorphic to $\mathfrak{m}F + G/\mathfrak{m}F$, which is isomorphic to $G/(\mathfrak{m}F \cap G)$. The previous claim now gives this claim.

But, both $F/\mathfrak{m}F$ and $M/\mathfrak{m}M$ are $R/\mathfrak{m}$-vector spaces of the same dimension, so the surjectivity of the natural map $F/\mathfrak{m}F \to M/\mathfrak{m}M$ implies that it is in fact an isomorphism, whence $G/\mathfrak{m}G$ is zero by the exactness. Now, again the corollary to Nakayama's Lemma gives that G can be generated by 0 elements, whence $G = 0$. Consequently, the surjection $F \to M$ is an isomorphism and M is free. □

Lemma 10.9. *Let R be a ring and $S \subseteq R$ be a multiplicatively closed subset containing 1. Let M be a (faithfully) flat R-module.*

Then $S^{-1}M$ is a (faithfully) flat $S^{-1}R$-module and a flat R-module.

Proof. Let N be an $S^{-1}R$-module. Then we have by the transitivity of tensoring (Lemma 8.10 and Lemma 9.17)

$$N \otimes_{S^{-1}R} S^{-1}M \cong N \otimes_{S^{-1}R} (S^{-1}R \otimes_R M) \cong (N \otimes_{S^{-1}R} S^{-1}R) \otimes_R M \cong N \otimes_R M.$$

Thus, the (faithful) flatness of $S^{-1}M$ is obvious.

Next we show that $S^{-1}R$ is flat over R. Let $M \hookrightarrow M'$ be an injection of R-modules. Because of Lemma 9.16 the $S^{-1}R$-module homomorphism $S^{-1}M \to S^{-1}M'$ is also injective. Using again Lemma 9.17), we rewrite this injection as $S^{-1}R \otimes_R M \hookrightarrow S^{-1}R \otimes_R M'$, proving the flatness of $S^{-1}R$ over R.

Finally, invoking Exercise 4(c) from Sheet 10, gives that $S^{-1}M$ is a flat R-module. □

The next two propositions give local characterisations, i.e. they give criteria saying that a certain property (injectivity, surjectivity, flatness, faithful flatness) 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 10.10. *Let R be a ring and M an R-module. Then the following statements are equivalent:*

(i) M is the zero module.

(ii) For all prime ideals $\mathfrak{p} \lhd R$, the localisation $M_{\mathfrak{p}}$ is the zero module.

(iii) For all maximal ideals $\mathfrak{m} \lhd R$, the localisation $M_{\mathfrak{m}}$ is the zero module.

Proof. ‘(i) $\Rightarrow$ (ii)’: Clear.

‘(ii) $\Rightarrow$ (iii)’ is trivial because all maximal ideals are prime.

‘(iii) $\Rightarrow$ (i)’: Let $T := \bigoplus_{\mathfrak{m}} R_{\mathfrak{m}}$, where the sum runs over all maximal ideals $\mathfrak{m}$. As $\mathfrak{m}R_{\mathfrak{m}} \neq R_{\mathfrak{m}}$ for any maximal ideal $\mathfrak{m}$, it follows that $\mathfrak{m}T \neq \mathfrak{m}$. By Proposition 10.6 and the fact that all $R_{\mathfrak{m}}$ are flat over R, it follows that T is faithfully flat over R.

The assumption implies that $0 = \bigoplus_{\mathfrak{m}} M_{\mathfrak{m}}$. We rewrite this as follows:

$$0 = \bigoplus_{\mathfrak{m}} M_{\mathfrak{m}} \cong \bigoplus_{\mathfrak{m}} (R_{\mathfrak{m}} \otimes_R M) \cong (\bigoplus_{\mathfrak{m}} R_{\mathfrak{m}}) \otimes_R M \cong T \otimes_R M.$$

By Lemma 10.5 it follows that $M = 0$. □

Proposition 10.11. *Let R be a ring and $\varphi : M \to N$ an R-homomorphism. For a prime ideal $\mathfrak{p} \lhd R$, denote by $\varphi_{\mathfrak{p}} : M_{\mathfrak{p}} \to N_{\mathfrak{p}}$ the localisation at $\mathfrak{p}$. Then the following statements are equivalent:*

(i) φ is injective (surjective).

(ii) For all prime ideals $\mathfrak{p} \lhd R$, the localisation $\varphi_{\mathfrak{p}}$ is injective (surjective).

(iii) For all maximal ideals $\mathfrak{m} \lhd R$, the localisation $\varphi_{\mathfrak{m}}$ is injective (surjective).

Proof. ‘(i) $\Rightarrow$ (ii)’: Lemma 9.16.

‘(ii) $\Rightarrow$ (iii)’ is trivial because all maximal ideals are prime.

‘(iii) $\Rightarrow$ (i)’: We only show this statement for the injectivity. The surjectivity is very similar. Let K be the kernel of φ, so that we have the exact sequence

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

As $R_{\mathfrak{m}}$ is flat over R, also the sequence

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

is exact. As $\varphi_{\mathfrak{m}}$ is injective, it follows that $K_{\mathfrak{m}} = 0$. By Lemma 10.10, $K = 0$, showing that φ is injective. □

Proposition 10.12. *Let R be a ring and M an R-module. Then the following statements are equivalent:*

(i) M is (faithfully) flat over R.

(ii) For all prime ideals $\mathfrak{p} \lhd R$, the localisation $M_\mathfrak{p}$ is (faithfully) flat over R.

(iii) For all maximal ideals $\mathfrak{m} \lhd R$, the localisation $M_\mathfrak{m}$ is (faithfully) flat over R.

Proof. '(i) ⇒ (ii)': Lemma 10.9.

'(ii) ⇒ (iii)' is trivial because all maximal ideals are prime.

'(iii) ⇒ (i)': We start with a preliminary calculation. Let N be an R-module. Then:

$$N \otimes_R M_\mathfrak{m} \cong N \otimes_R (M \otimes_R R_\mathfrak{m}) \cong (N \otimes_R M) \otimes_R R_\mathfrak{m} \cong (N \otimes_R M)_\mathfrak{m}.$$

Now let $N \hookrightarrow N'$ be an injection of R-modules. By the flatness of $M_\mathfrak{m}$ and the preliminary calculation, we obtain the injection:

$$(N \otimes_R M)_\mathfrak{m} \hookrightarrow (N' \otimes_R M)_\mathfrak{m}.$$

The previous proposition yields that $N \otimes_R M \to N' \otimes_R M$ is injective. Consequently, M is flat over R.

Now suppose in addition that $M_\mathfrak{m}$ is faithfully flat over $R_\mathfrak{m}$. By Lemma 9.18 we have

$$0 \neq M_\mathfrak{m}/\mathfrak{m}R_\mathfrak{m}M_\mathfrak{m} \cong M/\mathfrak{m}M,$$

which is equivalent to $\mathfrak{m}M \neq M$. As this holds for all maximal ideals, Proposition 10.6 yields that M is faithfully flat over R. □

11 Noetherian rings and Hilbert's Basissatz

In this short section, we treat Noetherian and Artinian rings and prove Hilbert's basis theorem.

Recall that in Definition 2.9 we have already defined Noetherian rings. Here we repeat this definition and extend it to modules

Definition 11.1. *Let R be a ring and M an R-module. The module M is called* Noetherian *(resp.* Artinian*) if every ascending (resp. descending) chain of R-submodules of M*

$$M_1 \subseteq M_2 \subseteq M_3 \subseteq \dots$$

(resp. $M_1 \supseteq M_2 \supseteq M_3 \supseteq \dots$) becomes stationary, i.e. there is $N \in \mathbb{N}$ such that for all $n \geq N$ we have $M_n = M_N$.

The ring R is called Noetherian *(resp.* Artinian*) if it has this property as an R-module.*

Lemma 11.2. *Let R be a ring and M an R-module.*

Then M is Noetherian (resp. Artinian) if and only if every non-empty set S of submodules of M has a maximal (resp. minimal) element.

By a maximal (resp. minimal) element of S we mean an R-module $N \in S$ such that $N \subseteq N_1$ (resp. $N \supseteq N_1$) implies $N = N_1$ for any $N_1 \in S$.

Proof. We only prove the Lemma for the Noetherian case. The Artinian case is similar.

Let S be a non-empty set of R-submodules of M that does not have a maximal element. Then construct an infinite ascending chain with strict inclusions as follows. Choose any $M_1 \in S$. As M_1 is not maximal, it is strictly contained in some $M_2 \in S$. As M_2 is not maximal, it is strictly contained in some $M_3 \in S$, etc. leading to the claimed chain. Hence, M is not Noetherian.

Conversely, let $M_1 \subseteq M_2 \subseteq M_3 \subseteq \dots$ be an ascending chain. Let $S = \{M_i \mid i \in \mathbb{N}\}$. This set contains a maximal element M_N by assumption. This means that the chain becomes stationary at N. □

Proposition 11.3. *Let R be a ring and M an R-module. The following statements are equivalent:*

(i) M is Noetherian.

(ii) Every submodule $N \leq M$ is finitely generated as R-module.

Proof. '(i) ⇒ (ii)': Assume that N is not finitely generated. In particular, there are then elements $n_i \in N$ for $i \in \mathbb{N}$ such that $\langle n_1 \rangle \subsetneq \langle n_1, n_2 \rangle \subsetneq \langle n_1, n_2, n_3 \rangle \subsetneq \dots$, contradicting the Noetherian-ness of M.

'(ii) ⇒ (i)': Let $M_1 \subseteq M_2 \subseteq M_3 \subseteq \dots$ 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 $x_1, \dots, x_d \in U$ 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 $i = 1, \dots, d$. Hence, the chain becomes stationary at N. □

Lemma 11.4. *Let R be a ring and $0 \to N \to M \to M/N \to 0$ be an exact sequence of R-modules. The following statements are equivalent:*

(i) M is Noetherian (resp. Artinian).

(ii) N and M/N are Noetherian (resp. Artinian).

Proof. We only prove this in the Noetherian case. The Artinian one is similar.

'(i) ⇒ (ii)': N is Noetherian because every ascending chain of submodules of N is also an ascending chain of submodules of M, and hence becomes stationary.

To see that M/N is Noetherian consider an ascending chain of R-submodules $\overline{M}_1 \subseteq \overline{M}_2 \subseteq \overline{M}_3 \subseteq \dots$ of M/N. Taking preimages for the natural projection $\pi : M \to M/N$ gives an ascending chain in M, which by assumption becomes stationary. Because of $\pi(\pi^{-1}(\overline{M}_i)) = \overline{M}_i$, also the original chain becomes stationary.

'(ii) ⇒ (i)': Let

$$M_1 \subseteq M_2 \subseteq M_3 \subseteq \dots$$

be an ascending chain of R-submodules. The chain

$$M_1 \cap N \subseteq M_2 \cap N \subseteq M_3 \cap N \subseteq \dots$$

becomes stationary (say, at the integer n) because its members are submodules of the Noetherian R-module N. Morepver, the chain

$$(M_1 + N)/N \subseteq (M_2 + N)/N \subseteq (M_3 + N)/N \cap N \subseteq \dots$$

also becomes stationary (say, at the integer m) because its members are submodules of the Noetherian R-module M/N. By one of the isomorphism theorems, we have $(M_i + N)/N \cong M_i/(M_i \cap N)$. Let now i be greater than n and m. We hence have for all $j \geq 0$:

$$M_i/(M_i \cap N) = M_{i+j}/(M_i \cap N).$$

The other isomorphism theorem then yields:

$$0 \cong (M_{i+j}/(M_i \cap N))/(M_i/(M_i \cap N)) \cong M_{i+j}/M_i,$$

showing $M_i = M_{i+j}$. □

Proposition 11.5. *Let R be a Noetherian (resp. Artinian) ring. Then every finitely generated R-module is Noetherian (resp. Artinian).*

Proof. Exercise. □

Proposition 11.6 (Hilbert's Basissatz)**.** *Let R be a Noetherian ring and $n \in \mathbb{N}$. Then $R[X_1, \dots, X_n]$ is a Noetherian ring. In particular, every ideal $\mathfrak{a} \lhd R[X_1, \dots, X_n]$ is finitely generated.*

Proof. By induction it clearly suffices to prove the case $n = 1$. So, let $\mathfrak{a} \lhd R[X]$ be any ideal. We show that $\mathfrak{a}$ is finitely generated, which implies the assertion by Proposition 11.3.

The very nice trick is the following:

$$\begin{aligned}
&\mathfrak{a}_0 := \{a_0 \in R \mid a_0 \in \mathfrak{a}\} \lhd R \\
&\cap \\
&\mathfrak{a}_1 := \{a_1 \in R \mid \exists b_0 \in R : a_1 X + b_0 \in \mathfrak{a}\} \lhd R \\
&\cap \\
&\mathfrak{a}_2 := \{a_2 \in R \mid \exists b_0, b_1 \in R : a_2 X^2 + b_1 X + b_0 \in \mathfrak{a}\} \lhd R \\
&\cap \\
&\ \vdots
\end{aligned}$$

So, $\mathfrak{a}_n$ is the set of highest coefficients of polynomials of degree n lying in $\mathfrak{a}$. The inclusion $\mathfrak{a}_{n-1} \subseteq \mathfrak{a}_n$ is true because if we multiply a polynomial of degree $n-1$ by X, we obtain a polynomial of degree n with the same highest coefficient.

The ascending ideal chain $\mathfrak{a}_0 \subseteq \mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \dots$ 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 11.3, say, $\mathfrak{a}_i = (a_{i,1}, \dots, a_{i,m_i})$.

By construction, for each $a_{i,j}$ there is a polynomial $f_{i,j} \in \mathfrak{a}$ of degree i with highest coefficient $a_{i,j}$. Let $\mathfrak{b}$ be the ideal of $R[X]$ generated by the finitely many $f_{i,j} \in \mathfrak{a}$ for $1 \leq i \leq d$ 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 $j = 1, \dots, m_d$ 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. □

12 Dimension theory

This section has two main parts. The principal corollary of the first part is that the ring of integers of a number field has dimension 1, whereas we will conclude from the second part that the coordinate ring of a plane curve has dimension 1 (that shouldn't be too astonishing, but because of the abstract nature of the definition needs a non-trivial proof).

Definition 12.1. *Let R be a ring. A* chain of prime ideals of length n in R *is*

$$\mathfrak{p}_n \subsetneq \mathfrak{p}_{n-1} \subsetneq \mathfrak{p}_{n-2} \subsetneq \cdots \subsetneq \mathfrak{p}_1 \subsetneq \mathfrak{p}_0,$$

where $\mathfrak{p}_i \lhd R$ is a prime ideal for all $i = 0, \dots, n$.

The height $h(\mathfrak{p})$ of a prime ideal $\mathfrak{p} \lhd R$ *is the supremum of the lengths of all prime ideal chains with $\mathfrak{p}_0 = \mathfrak{p}$.*

The Krull dimension $\dim(R)$ of the ring R *is the supremum of the heights of all prime ideals of R.*

Example 12.2. *(a) The Krull dimension of $\mathbb{Z}$ is 1.*

Reason: Recall that the prime ideals of $\mathbb{Z}$ are (0) (height 0) and (p) for a prime p, which is also maximal. So, the longest prime ideal chain is $(0) \subsetneq (p)$.

(b) The Krull dimension of any field is 0.

Reason: (0) is the only ideal, hence, also the only prime ideal.

(c) Let K be a field. The polynomial ring $K[X_1, \dots, X_n]$ has Krull dimension n. This needs a non-trivial proof and is shown below.

In the sequel, we are going to consider ring extensions $R \subseteq S$. If we denote $\iota : R \to S$ the inclusion and $\mathfrak{b} \lhd S$ an ideal, then $\iota^{-1}(\mathfrak{b}) = \mathfrak{b} \cap R$ (in the obvious sense). In particular, if $\mathfrak{b}$ is a prime ideal, then so is $\iota^{-1}(\mathfrak{b}) = \mathfrak{b} \cap R$ (see Exercise).

Lemma 12.3. *Let $R \subseteq S$ be a ring extension such that S is integral over R. Let $\mathfrak{b} \lhd S$ be an ideal and $\mathfrak{a} := \mathfrak{b} \cap R \lhd R$.*

(a) Then $R/\mathfrak{a} \hookrightarrow S/\mathfrak{b}$ is an integral ring extension (note that this is injective because of the homomorphism 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 12.4. *Let $R \subseteq S$ be an integral ring extension.*

(a) Let $\mathfrak{b} \lhd S$ be an ideal containing $x \in \mathfrak{b}$ which is not a zero-divisor. Then $\mathfrak{b} \cap R =: \mathfrak{a} \lhd R$ is not the zero ideal.

(b) Let $\mathfrak{P}_1 \subsetneq \mathfrak{P}_2$ be a chain of prime ideals of S. Then $\mathfrak{p}_1 := \mathfrak{P}_1 \cap R \subsetneq \mathfrak{P}_2 \cap R =: \mathfrak{p}_2$ is a chain of prime ideals of R.

Proof. (a) Since S is integral over R, there are $n \in \mathbb{N}$ and $r_0, \dots, r_{n-1} \in R$ such that

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

As x is not a zero-divisor, it is in particular not nilpotent, i.e. there is some coefficient $r_i \neq 0$ (for some $i = 0, \dots, n-1$). Let j be the smallest index ($\leq n-1$) such that $r_j \neq 0$. Now we have

$$0 = x^j \big(x^{n-j} + \sum_{i=j}^{n-1} r_i x^{i-j}\big),$$

implying (as x is not a zero-divisor):

$$0 = x^{n-j} - \sum_{i=j}^{n-1} r_i x^{i-j}.$$

Rewriting yields:

$$r_j = x(-x^{n-j-1} - \sum_{i=j+1}^{n-1} r_i x^{i-j-1}) \in R \cap \mathfrak{b} = \mathfrak{a},$$

showing that $\mathfrak{a}$ is non-zero.

(b) Consider the integral (see Lemma 12.3) ring extension $R/\mathfrak{p}_1 \hookrightarrow S/\mathfrak{P}_1$. The ideal $\mathfrak{P}_2/\mathfrak{P}_1$ in $S/\mathfrak{P}_1$ is prime because $(S/\mathfrak{P}_1)/(\mathfrak{P}_2/\mathfrak{P}_1) \cong S/\mathfrak{P}_1$ (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 $(0) \neq \mathfrak{P}_2/\mathfrak{P}_1 \cap R/\mathfrak{p}_1 \cong \mathfrak{p}_2/\mathfrak{p}_1$. □

Lemma 12.5. *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 12.6. *Let $R \subseteq S$ be an integral ring extension and let $\mathfrak{p} \lhd R$ be a prime ideal. Then there is a prime ideal $\mathfrak{P} \lhd S$ lying over $\mathfrak{p}$, by which we mean $\mathfrak{p} = \mathfrak{P} \cap R$.*

Proof. Let $T := R \backslash \mathfrak{p}$ so that $R_\mathfrak{p} = T^{-1}R$ is the localisation of R at $\mathfrak{p}$. By Lemma 12.5, $R_\mathfrak{p} \hookrightarrow T^{-1}S$ is an integral ring extension. Let $\mathfrak{m}$ be a maximal ideal of $T^{-1}S$.

Consider the commutative diagram:

$$\begin{tikzcd}
R \arrow[r, "\text{integral}"] \arrow[d, "\alpha"] & S \arrow[d, "\beta"] \\
R_\mathfrak{p} \arrow[r, "\text{integral}"] & T^{-1}S.
\end{tikzcd}$$

Put $\mathfrak{P} := \beta^{-1}(\mathfrak{m})$. It is a prime ideal. Note that $\mathfrak{m} \cap R_\mathfrak{p}$ is maximal by Lemma 12.3, hence, $\mathfrak{m} \cap R_\mathfrak{p} = \mathfrak{p}R_\mathfrak{p}$ is the unique maximal ideal of the local ring $R_\mathfrak{p}$. Consequently, we have due to the commutativity of the diagram:

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

showing that $\mathfrak{P}$ satisfies the requirements. □

Proposition 12.7 (Going up). *Let $R \subseteq S$ be an integral ring extension. For prime ideals $\mathfrak{p}_1 \subseteq \mathfrak{p}_2$ in R and a prime ideal $\mathfrak{P}_1 \lhd S$ lying over $\mathfrak{p}_1$ (i.e. $\mathfrak{P}_1 \cap R = \mathfrak{p}_1$), there is a prime ideal $\mathfrak{P}_2$ in S lying over $\mathfrak{p}_2$ (i.e. $\mathfrak{P}_2 \cap R = \mathfrak{p}_2$) such that $\mathfrak{P}_1 \subseteq \mathfrak{P}_2$.*

Proof. By Lemma 12.3, $R/\mathfrak{p}_1 \hookrightarrow S/\mathfrak{P}_1$ is an integral ring extension. By Lemma 12.6, there is $\overline{\mathfrak{P}}_2 \lhd S/\mathfrak{P}_1$ lying over $\overline{\mathfrak{p}}_2 := \mathfrak{p}_2/\mathfrak{p}_1$ such that $\overline{\mathfrak{P}}_2 \cap R/\mathfrak{p}_1 = \mathfrak{p}_2/\mathfrak{p}_1$. Define $\mathfrak{P}_2$ as $\pi^{-1}(\overline{\mathfrak{P}_2})$ for $\pi : S \to S/\mathfrak{P}_1$ the natural projection. Clearly, $\mathfrak{P}_2 \supseteq \mathfrak{P}_1$ (as $\mathfrak{P}_1$ is in the preimage, being the preimage of the 0 class) and $\mathfrak{P}_2 \cap R = \mathfrak{p}_2$ also follows. □

Corollary 12.8. *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 12.4.

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 12.6. Then Proposition 12.7 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 12.9. *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 12.8, the Krull dimension of S is the same as that of R, whence it is 1. □

Our next aim is to compute the Krull dimension of $K[X_1, \ldots, X_n]$ for some field K. First we need Nagata's Normalisation Lemma, which will be an essential step in the proof of Noether's Normalisation Theorem and of the computation of the Krull dimension of $K[X_1, \ldots, X_n]$.

Proposition 12.10 (Nagata). *Let K be a field and $f \in K[X_1, \ldots, X_n]$ be a non-constant polynomial. Then there are $m_2, m_3, \ldots, m_n \in \mathbb{N}$ such that the ring extension $R := K[f, z_2, z_3, \ldots, z_n] \subseteq K[X_1, \ldots, X_n] =: S$ with $z_i := X_i - X_1^{m_i} \in K[X_1, \ldots, X_n]$ is integral.*

Proof. First note: $S = R[X_1]$. Reason: The inclusion $\supseteq$ is trivial. For $n \geq i > 1$, we have $X_i = z_i + X_1^{m_i} \in R[X_1]$, proving the inclusion $\subseteq$.

It suffices to show that X_1 is integral over R. The main step is to construct a monic polynomial $h \in R[T]$ such that $h(X_1) = 0$. We take the following general approach: For any $m_i \in \mathbb{N}$ for $i = 2, 3, \ldots, n$ the polynomial

$$h(T) := f(T, z_2 + T^{m_2}, z_3 + T^{m_3}, \ldots, z_n + T^{m_n}) - f(X_1, \ldots, X_n) \in R[T]$$

obviously has X_1 as a zero. But, in order to prove the integrality of X_1 we need the highest coefficient of h to be in $R^\times = K[X_1, \ldots, X_n]^\times = K^\times$, so that we can divide by it, making h monic. We will achieve this by making a 'good' choice of the m_i, as follows.

Let d be the total degree of f in the following sense:

$$f(X_1, \ldots, X_n) = \sum_{(i_1, \ldots, i_n) \text{ s.t. } |i| \leq d} a_{(i_1, \ldots, i_n)} X_1^{i_1} \cdots X_n^{i_n}$$

with one of the $a_{(i_1, \ldots, i_n)} \neq 0$ for $|i| := \sum_{j=1}^n i_j = d$. Now we compute (letting $m_1 = 1$)

$$\begin{aligned} & h(T) \\ & = \Big(\sum_{(i_1, \ldots, i_n) \text{ s.t. } |i| \leq d} a_{(i_1, \ldots, i_n)} T^{i_1} (z_2 + T^{m_2})^{i_2} (z_3 + T^{m_3})^{i_3} \ldots (z_n + T^{m_n})^{i_n} \Big) - f(X_1, \ldots, X_n) \\ & \qquad = \sum_{(i_1, \ldots, i_n) \text{ s.t. } |i| \leq d} a_{(i_1, \ldots, i_n)} T^{\sum_{j=1}^n i_j m_j} + \text{ terms of lower degree in } T. \end{aligned}$$

Now choose $m_j = (d+1)^{j-1}$. Then the $\sum_{j=1}^n i_j m_j = \sum_{j=1}^n i_j (d+1)^{j-1}$ are distinct for all choices of $0 \leq i_j \leq d$ (consider it as the $(d+1)$-adic expansion of an integer). In particular, among these numbers there is a maximal one with $0 \neq a_{(i_1, \ldots, i_n)}$. Then this is the highest coefficient of h and it lies in $K^\times$, as needed. □

Definition 12.11. *Let K be a field. A finitely generated K-algebra is also called an* affine K-algebra.

Proposition 12.12 (Noether's Normalisation Theorem). *Let K be a field and R an affine K-algebra, which is an integral domain. Then there is $r \in \mathbb{N}$, $r \leq n$ and there are elements $y_1, \ldots, y_r \in R$ such that*

(1) $R/K[y_1, \ldots, y_r]$ is an integral ring extension and

(2) $y_1, \ldots, y_r$ are K-algebraically independent (by definition, this means that $K[y_1, \ldots, y_r]$ is isomorphic to the polynomial ring in r variables).

The subring $K[y_1,\dots,y_r]$ of R is called a Noether normalisation of R.

Proof. By induction on $n \in \mathbb{N}$ we shall prove: Every affine K-algebra that can be generated by n elements satisfies the conclusion of the proposition.

Start with $n = 0$. Then $R = K$ and the result is trivially true. Assume now that the result is proved for $n - 1$. We show it for n. Let $x_1,\dots,x_n \in R$ be a set of generators of R as K-algebra. So, we have the surjection of K-algebras:

$$\varphi : K[X_1,\dots,X_n] \twoheadrightarrow R, \quad X_i \mapsto x_i.$$

Its kernel is a prime ideal $\mathfrak{p} := \ker(\varphi)$ since R is an integral domain.

We distinguish two cases. Assume first $\mathfrak{p} = (0)$. Then R is isomorphic to $K[X_1,\dots,X_n]$ and the result is trivially true. Now we put ourselves in the second case $\mathfrak{p} \neq (0)$. Let $f \in \mathfrak{p}$ be a non-constant polynomial. We apply Nagata's Normalisation Lemma Proposition 12.10 and obtain elements $z_2,\dots,z_n \in K[X_1,\dots,X_n]$ such that $K[X_1,\dots,X_n]/K[f,z_2,\dots,z_n]$ is an integral ring extension. Now, apply φ to this extension and obtain the integral ring extension $R/\varphi(K[f,z_2,\dots,z_n])$, i.e. the integral ring extension R/R' with $R' := K[\varphi(z_2),\dots,\varphi(z_n)]$. Now, R' is generated by $n-1$ elements, hence, it is an integral extension of $K[y_1,\dots,y_r]$ with $r \le n-1$ algebraically independent elements $y_1,\dots,y_r \in R' \subseteq R$. As integrality is transitive, R is integral over $K[y_1,\dots,y_r]$, proving the proposition. □

Note that by Corollary 12.8 one obtains that the Krull dimension of R is equal to r.

Proposition 12.13. *Let K be a field. The Krull dimension of $K[X_1,\dots,X_n]$ is equal to n.*

Proof. We apply induction on n to prove the Proposition. If $n = 0$, then the Krull dimension is 0 being the Krull dimension of a field. Let us assume that we have already proved that the Krull dimension of $K[X_1,\dots,X_{n-1}]$ is $n-1$.

Let now m be the Krull dimension of $K[X_1,\dots,X_n]$. We first prove $m \ge n$. The reason simply is that we can write down a chain of prime ideals of length n, namely:

$$(0) \subsetneq (X_1) \subsetneq (X_1,X_2) \subsetneq (X_1,X_2,X_3) \subsetneq \cdots \subsetneq (X_1,X_2,\dots,X_n).$$

Now let

$$(0) \subsetneq \mathfrak{P}_1 \subsetneq \mathfrak{P}_2 \subsetneq \mathfrak{P}_3 \subsetneq \cdots \subsetneq \mathfrak{P}_m$$

be a chain of prime ideals of $K[X_1,\dots,X_n]$ of maximal length. We pick any non-constant $f \in \mathfrak{P}_1$ and apply Nagata's Normalisation Lemma Proposition 12.10 yielding elements $z_2,\dots,z_n \in K[X_1,\dots,X_n]$ such that $K[X_1,\dots,X_n]/R$ with $R := K[f,z_2,\dots,z_n]$ is an integral ring extension. Setting $\mathfrak{p}_i := R \cap \mathfrak{P}_i$ we obtain by Lemma 12.4 the chain of prime ideal of R of length m:

$$(0) \subsetneq \mathfrak{p}_1 \subsetneq \mathfrak{p}_2 \subsetneq \mathfrak{p}_3 \subsetneq \cdots \subsetneq \mathfrak{p}_m.$$

Since the Krull dimension of R equals that of $K[X_1,\dots,X_n]$ by Corollary 12.8, this prime ideal chain is of maximal length.

Let $\overline{R} := K[f,z_2,\dots,z_n]/\mathfrak{p}_1$. Note that this is an integral domain, which can be generated (as a K-algebra) by $n-1$ elements, namely, the classes of $z_2,\dots,z_n$. Let $\pi : R = K[f,z_2,\dots,z_n] \to$

$K[f, z_2, \dots, z_n]/\mathfrak{p}_1 = \overline{R}$ be the natural projection. We apply it to the prime ideal chain of the $\mathfrak{p}_i$ and get:

$$(0) = \mathfrak{p}_1/\mathfrak{p}_1 \subsetneq \mathfrak{p}_2/\mathfrak{p}_1 \subsetneq \mathfrak{p}_3/\mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_m/\mathfrak{p}_1,$$

which is a prime ideal chain of $\overline{R}$ of length $m-1$. By Noether's Normalisation Theorem Proposition 12.12 it follows that the Krull dimension of $\overline{R}$ is at most $n-1$, yielding the other inequality $m \le n$ and finishing the proof. □

Corollary 12.14. *Let K be a field and $f(X,Y) \in K[X,Y]$ be a non-constant irreducible polynomial. Let $C = \mathcal{V}_{(f)}(K)$ be the resulting irreducible plane curve.*

The Krull dimension of the coordinate ring $K[C] = K[X,Y]/(f(X,Y))$ is equal to 1.

Proof. Nagata's Normalisation Lemma Proposition 12.10 yields an element $z \in K[X,Y]$ such that $K[f,z] \subseteq K[X,Y]$ is an integral ring extension. Modding out (f), we see that $K[f,z]/(f) \subseteq K[C]$ is an integral ring extension, whence the Krull dimensions of the two rings coincide and is at most 1 by Noether's Normalisation Theorem Proposition 12.12 and Proposition 12.13 because $K[f,z]/(f)$ is an integral domain that can be generated by one element as a K-algebra, namely, by the class of z.

If the Krull dimension of $K[C]$ were 0, then $K[C]$ would be a finite field extension of K (being a finitely generated integral extension of a field). Hence, there would only be finitely many embeddings of $K[C]$ into an algebraic closure $\overline{K}$ of K. However, we know that each of the infinitely many points (x,y) of C (we proved this earlier!) gives a different embedding, namely, $K[C] \xrightarrow{g(X,Y)+(f)\mapsto g(x,y)} \overline{K}$. This contradiction shows that the Krull dimension of $K[C]$ cannot be 0. □

13 Dedekind rings

Lemma 13.1. *Let R be an integrally closed integral domain and $T \subseteq R$ a multiplicatively closed subset containing* 1. *Then $T^{-1}R$ is integrally closed.*

Proof. Let K be the field of fractions of R, it is also the field of fractions of $T^{-1}R$. Let $\frac{a}{b} \in K$ be integral over $T^{-1}R$. Then (after choosing a common demoninator of the coefficients) there is an equation of the form:

$$0 = \big(\frac{a}{b}\big)^n + \frac{c_{n-1}}{t}\big(\frac{a}{b}\big)^{n-1} + \frac{c_{n-2}}{t}\big(\frac{a}{b}\big)^{n-2} + \cdots + \frac{c_1}{t}\frac{a}{b} + \frac{c_0}{t}$$

with $c_0, c_1, \dots, c_{n-1} \in R$ and $t \in T$. Multiplying through with t^n we obtain:

$$0 = \big(\frac{at}{b}\big)^n + c_{n-1}\big(\frac{at}{b}\big)^{n-1} + c_{n-2}t\big(\frac{at}{b}\big)^{n-2} + \cdots + c_1 t^{n-2}\frac{at}{b} + c_0 t^{n-1},$$

showing that $\frac{ta}{b}$ is integral over R. As R is integrally closed, it follows that $\frac{ta}{b}$ is in R, whence $\frac{a}{b} \in T^{-1}R$. □

Corollary 13.2. *Let R be an integral domain with field of fractions K and $T \subseteq R$ a multiplicatively closed subset containing* 1. *Let $\widetilde{R}$ be the integral closure of R in K and let $\widetilde{T^{-1}R}$ be the integral closure of $T^{-1}R$ in K.*

Then $T^{-1}\widetilde{R} = \widetilde{T^{-1}R}$.

Proof. By Lemma 13.1, $T^{-1}\widetilde{R}$ is integrally closed. As $\widetilde{R}/R$ is an integral ring extension, by Lemma 12.5 it follows that $T^{-1}\widetilde{R}/T^{-1}R$ is an integral ring extension. This shows that $T^{-1}\widetilde{R}$ is the integral closure of $T^{-1}R$. □

Now we can prove the local characterisation of integrally closed integral domains.

Proposition 13.3. *Let R be an integral domain. Then the following statements are equivalent:*

(i) R is integrally closed.

(ii) $R_\mathfrak{p}$ is integrally closed for all prime ideals $\mathfrak{p} \lhd R$.

(iii) $R_\mathfrak{m}$ is integrally closed for all maximal ideals $\mathfrak{m} \lhd R$.

Proof. '(i) ⇒ (ii)': Lemma 13.1.

'(ii) ⇒ (iii)': Trivial because every maximal ideal is prime.

'(iii) ⇒ (i)': Let us denote by $\widetilde{R}$ the integral closure of R. By Corollary 13.2, we know that the localisation $\widetilde{R}_\mathfrak{m}$ of $\widetilde{R}$ at $\mathfrak{m}$ is the integral closure of $R_\mathfrak{m}$.

Let $\iota : R \hookrightarrow \tilde{R}$ the natural embedding. Of course, R is integrally closed if and only if ι is an isomorphism. By Proposition 10.11 this is the case if and only if the localisation $\iota_\mathfrak{m} : R_\mathfrak{m} \hookrightarrow \tilde{R}_\mathfrak{m}$ is an isomorphism for all maximal ideals $\mathfrak{m}$. That is, however, the case by assumption and the previous discussion. □

Lemma 13.4. *Let R be a Noetherian local ring and $\mathfrak{m} \lhd R$ its maximal ideal.*

(a) $\mathfrak{m}^n/\mathfrak{m}^{n+1}$ is an $R/\mathfrak{m}$-vector space for the natural operation.

(b) $\dim_{R/\mathfrak{m}}(\mathfrak{m}/\mathfrak{m}^2)$ is the minimal number of generators of the ideal $\mathfrak{m}$.

(c) If $\dim_{R/\mathfrak{m}}(\mathfrak{m}/\mathfrak{m}^2) = 1$, then $\mathfrak{m}$ is a principal ideal and there are no ideals $\mathfrak{a} \lhd R$ such that $\mathfrak{m}^{n+1} \subsetneq \mathfrak{a} \subsetneq \mathfrak{m}^n$ for any $n \in \mathbb{N}$.

Proof. Exercise on Sheet 12. □

Definition 13.5. *A Noetherian local ring with maximal ideal $\mathfrak{m}$ is called* regular *if $\dim_{R/\mathfrak{m}}(\mathfrak{m}/\mathfrak{m}^2)$ equals the Krull dimension of R.*

Proposition 13.6. *Let R be a regular local ring of Krull dimension 1.*

(a) There is $x \in R$ such that all non-zero ideals are of the form (x^n) for some $n \in \mathbb{N}$.

(b) Every non-zero $r \in R$ can be uniquely written as ux^n with $u \in R^\times$ and $n \in \mathbb{N}$.

(c) R is a principal ideal domain (in particular, it is an integral domain).

Proof. By Lemma 13.4 we know that $\mathfrak{m}$ is a principal ideal. Let x be a generator, i.e. $(x) = \mathfrak{m}$. We also know that there are no ideals $\mathfrak{a} \lhd R$ such that $\mathfrak{m}^{n+1} \subsetneq \mathfrak{a} \subsetneq \mathfrak{m}^n$ for any $n \in \mathbb{N}$.

Let $0 \neq r \in R$. We show that $r = ux^n$ with unique $u \in R^\times$ and $n \in \mathbb{N}$. In order to do so, we first consider $M := \bigcap_{n\in\mathbb{N}} \mathfrak{m}^n$. We obviously have $\mathfrak{m}M = M$, whence by Nakayama's Lemmma (Proposition 9.13) $M = 0$.

As $r \neq 0$, there is a maximal n such that $r \in (x^n)$. So, we can write $r = vx^n$ for some $v \in R$. As R is a local ring, we have $R = R^\times \cup \mathfrak{m} = R^\times \cup (x)$. Consequently, $v \in R^\times$ because otherwise $r \in (x^{n+1})$, contradicting the maximality of n.

Let $0 \neq \mathfrak{a} \lhd R$ be any non-zero ideal. Let $u_i x^{n_i}$ (with $u_i \in R^\times$) be generators of the ideal. Put $n := \min_i n_i$. Then $\mathfrak{a} = (x^n)$ because all other generators are multiples of $u_j x^{n_j}$, where j is such that $n_j = n$.

None of the ideals $\mathfrak{m}^n$ for $n \geq 2$ is a prime ideal (consider $x \cdot x^{n-1}$). As the Krull dimension is 1, it follows that (0) is a (hence, the) minimal prime ideal, showing that R is an integral domain. □

Our next aim is to prove that regular local rings of Krull dimension 1 are precisely the local principal ideal domains and also the local integrally closed integral domains.

The following lemma is proved very similarly to Nakayama's Lemma (which was an exercise).

Lemma 13.7. *Let R be a ring, $\mathfrak{a} \lhd R$ an ideal and M a finitely generated R-module. Let $\varphi : M \to M$ be an R-homomorphism such that the image $\varphi(M)$ is contained in $\mathfrak{a}M$.*

Then there are $n \in \mathbb{N}$ and $a_0, a_1, \dots, a_{n-1} \in \mathfrak{a}$ such that

$$\varphi^n + a_{n-1}\varphi^{n-1} + a_{n-2}\varphi^{n-2} + \dots a_1\varphi + a_0\mathrm{id}$$

is the zero-endomorphism on M.

Proof. Let $x_1, \dots, x_n$ be generators of M as R-module. By assumption there are $a_{i,j} \in \mathfrak{a}$ for $1 \leq i, j \leq n$ such that

$$\varphi(x_i) = \sum_{j=1}^{n} a_{i,j} x_j.$$

Consider the matrix

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

Note that $D(T)$ is made precisely in such a way that $D(\varphi)(x_i) = 0$ for all $1 \leq i \leq n$. This means that $D(\varphi)$ is the zero-endomorphism on M (as it is zero on all generators). We multiply with the adjoint matrix $D(T)^*$ and obtain $D(T)^* D(T) = \det(D(T))\mathrm{id}_{n \times n}$. Consequently, $\det(D(\varphi))$ is the zero-endomorphism on M. We are done because the determinant $\det(D(\varphi))$ is of the desired form. □

Lemma 13.8. *Let R be a local Noetherian integral domain of Krull dimension 1 with maximal ideal $\mathfrak{m}$. Let $(0) \subsetneq I \lhd R$ be an ideal. Then there is $n \in \mathbb{N}$ such that $\mathfrak{m}^n \subseteq I$.*

Proof. Exercise on Sheet 12. □

Proposition 13.9. *Let R be a local Noetherian ring of Krull dimension 1. Then the following statements are equivalent:*

(i) R is an integrally closed integral domain.

(ii) R is regular.

(iii) R is a principal ideal domain.

Proof. '(ii) ⇒ (iii)': This was proved in Proposition 13.6.

'(iii) ⇒ (i)': Principal ideal domains are factorial (Proposition 2.12) and factorial rings are integrally closed (Proposition 4.12).

'(i) ⇒ (i)': It suffices to show that $\mathfrak{m}$ is a principal ideal because this means that $\dim_{R/\mathfrak{m}}(\mathfrak{m}/\mathfrak{m}^2) = 1$, which is the Krull dimension of R, so that R is regular by definition.

We now construct an element x such that $\mathfrak{m} = (x)$. To that aim, we start with any $0 \neq a \in \mathfrak{m}$. By Lemma 13.8 there is $n \in \mathbb{N}$ such that $\mathfrak{m}^n \subseteq (a)$ and $\mathfrak{m}^{n-1} \not\subseteq (a)$. Take any $b \in \mathfrak{m}^{n-1} \setminus (a)$. Put $x = \frac{a}{b} \in K$, where K is the field of fractions of R.

We show that $\mathfrak{m} = (x)$, as follows:

- $\frac{m}{x} \in R$ for all $m \in \mathfrak{m}$ because $\frac{m}{x} = \frac{mb}{a}$ and $mb \in \mathfrak{m}\mathfrak{m}^{n-1} = \mathfrak{m}^n \subseteq (a)$.
- $x^{-1} \notin R$ because otherwise $r = x^{-1} = \frac{b}{a} \in R$ would imply $b = ra \in (a)$.
- $x^{-1}\mathfrak{m} \not\subseteq \mathfrak{m}$ because of the following: Assume the contrary, i.e. $x^{-1}\mathfrak{m} = \mathfrak{m}$. Then we have the R-homomorphism $\varphi : \mathfrak{m} \xrightarrow{m \mapsto mx^{-1}} \mathfrak{m}$. As $\mathfrak{m}$ is finitely generated (because R is Noetherian), there are $a_0, a_1, \dots, a_{n-1} \in R$ such that
$$\varphi^n + a_{n-1}\varphi^{n-1} + a_{n-2}\varphi^{n-2} + \dots a_1\varphi + a_0\mathrm{id}$$
is the zero-endomorphism on $\mathfrak{m}$ by Lemma 13.7 (with $\mathfrak{a} = R$). This means that
$$0 = \big(x^{-n} + a_{n-1}x^{-(n-1)} + a_{n-2}x^{-(n-2)} + \dots a_1x^{-1} + a_0\big)\mathfrak{m}.$$
As R is an integral domain, we obtain
$$0 = x^{-n} + a_{n-1}x^{-(n-1)} + a_{n-2}x^{-(n-2)} + \dots a_1x^{-1} + a_0,$$
showing that x^{-1} is integral over R. As R is integrally closed, we obtain further $x^{-1} \in R$, which we excluded before.

So, $x^{-1}\mathfrak{m}$ is an ideal of R which is not contained in $\mathfrak{m}$. Thus, $x^{-1}\mathfrak{m} = R$, whence $\mathfrak{m} = Rx = (x)$, as was to be shown. □

Definition 13.10. *A Noetherian integrally closed integral domain of Krull dimension 1 is called a* Dedekind ring.

Example 13.11. *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 13.12. *Let R be a Noetherian integral domain of Krull dimension 1. Then the following assertions are equivalent:*

(i) *R is a Dedekind ring.*

(ii) *R is integrally closed.*

(iii) *$R_\mathfrak{m}$ is integrally closed for all maximal ideals $\mathfrak{m} \lhd R$.*

(iv) *$R_\mathfrak{m}$ is regular for all maximal ideals $\mathfrak{m} \lhd R$.*

(v) *$R_\mathfrak{m}$ is a principal ideal domain for all maximal ideals $\mathfrak{m} \lhd R$.*

Proof. All statements have been proved earlier! But, note that the Krull dimension of $R_\mathfrak{m}$ is 1 for all maximal ideals $\mathfrak{m}$. That is due to the fact that any non-zero prime ideal in an integral domain of Krull dimension 1 is maximal and that $\mathfrak{m}R_\mathfrak{m}$ is also maximal and non-zero. □

Let us now see what this means for plane curves. Let $f(X, Y) \in K[X, Y]$. Recall the Taylor expansion:

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

Definition 13.13. *Let K be a field, $f \in K[X, Y]$ a non-constant irreducible polynomial and $C = \mathcal{V}_{(f)}(K)$ the associated plane curve.*

Let $(a, b) \in C$ be a point. The tangent equation to C at (a, b) *is defined as*

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

If $T_{C,(a,b)}(X, Y)$ is the zero polynomial, then we call (a, b) a singular point of C.

If (a, b) is non-singular (also called: smooth*), then $\mathcal{V}_{T_{C,(a,b)}}(K)$ is a line (instead of $\mathbb{A}^2(K)$), called the* tangent line to C at (a, b).

A curve all of whose points are non-singular is called non-singular (or smooth).

Example 13.14. *(a) Let $f(X, Y) = Y^2 - X^3 \in K[X, Y]$ with K a field (say, of characteristic 0).*

We have $\frac{\partial f}{\partial X} = -3X^2$ and $\frac{\partial f}{\partial X} = 2Y$. Hence, $(0, 0)$ is a singularity and it is the only one. (Draw a sketch.)

This kind of singularity is called a cusp *(Spitze/pointe) for obvious reasons. The tangents to the two branches coincide at the cusp.*

(b) Let $f(X, Y) = Y^2 - X^3 - X^2 \in K[X, Y]$ with K a field (say, of characteristic 0).

We have $\frac{\partial f}{\partial X} = -3X^2 - 2X$ and $\frac{\partial f}{\partial X} = 2Y$. Hence, $(0, 0)$ is a singularity and it is the only one. (Draw a sketch.)

This kind of singularity is called an ordinary double point *. The tangents to the two branches are distinct at the ordinary double point.*

Lemma 13.15. *Let K be a field, $S \subseteq K[X_1, \dots, X_n]$ be a subset, $\mathcal{X} = \mathcal{V}_S(K)$ the K-points of the associated affine algebraic set. Let $(a_1, \dots, a_n) \in \mathcal{X}$ be a K-point.*

The kernel of the K-algebra homomorphism

$$\Phi_{(a_1,\dots,a_n)} : K[\mathcal{X}] = K[X_1, \dots, X_n]/\mathcal{I}_{\mathcal{X}} \to K, \quad g(X_1, \dots, X_n) + (f) \mapsto g(a_1, \dots, a_n)$$

is equal to $(X_1 - a_1, \dots, X_n - a_n)$.

Proof. By a variable transformation $Y_i := X_i - a_i$ (formally, we take the K-algebra isomorphism $K[Y_1, \dots, Y_n] \xrightarrow{Y_i \mapsto X_i + a_i} K[X_1, \dots, X_n]$), we may assume that $0 = a_1 = a_2 = \dots = a_n$. The ideal $(X_1, X_2, \dots, X_n)$ is clearly maximal because the quotient by it is K. As $(X_1, X_2, \dots, X_n) \subseteq \ker(\Phi_{(0,\dots,0)})$ it follows that the two are equal (as $\Phi_{(0,\dots,0)}$ is not the zero-map – look at constants). □

Lemma 13.16. *Let K be an algebraically closed field, $f \in K[X, Y]$ a non-constant irreducible polynomial, $C = \mathcal{V}_{(f)}(K)$ the associated plane curve and $K[C] = K[X, Y]/(f(X, Y))$ the coordinate ring. Let $(a, b) \in C$ be a point and $\mathfrak{m} = (X - a + (f), Y - b + (f)) \lhd K[C]$ be the corresponding maximal ideal (see Lemma 13.15).*

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.

Proof. After a variable transformation (as in the previous lemma) we may assume $(a, b) = (0, 0)$. Then

$$f(X, Y) = \alpha X + \beta Y + \text{ higher terms.}$$

Note that $\mathfrak{m}^2$ is generated by $X^2 + (f), Y^2 + (f), XY + (f)$, so that the $K = K[C]/\mathfrak{m}$-vector space $\mathfrak{m}/\mathfrak{m}^2$ is generated by $X + (f)$ and $Y + (f)$. Hence, the minimal number of generators is at most 2, but could be 1.

Note also that $K[C]$ has Krull dimension 1 and is an integral domain because f is irreducible (see Corollary 12.14). As $\mathfrak{m}$ is not the zero ideal, also the localisation $K[C]_{\mathfrak{m}}$ has Krull dimension 1.

'(i) ⇒ (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:

$$X = \frac{1}{\alpha}\big(f(X, Y) - \beta Y - \text{ higher terms}\big) \equiv \frac{\beta}{\alpha} Y \pmod{\mathfrak{m}^2}.$$

So, $X + (f)$ generates $\mathfrak{m}/\mathfrak{m}^2$ as K-vector space, whence the dimension of this space is 1, which is equal to the Krull dimension. This shows that $K[C]_{\mathfrak{m}}$ is regular.

'(ii) ⇒ (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. □

We now get another important occurence of Dedekind rings: As coordinate rings of non-singular plane curves.

Proposition 13.17. *Let K be an algebraically closed field, $f \in K[X,Y]$ a non-constant irreducible polynomial, $C = \mathcal{V}_{(f)}(K)$ the associated plane curve and $K[C] = K[X,Y]/(f(X,Y))$ the coordinate ring.*

Then the following two statements are equivalent:

(i) The curve C is smooth.

(ii) $K[C]$ is a Dedekind ring.

14 Hilbert's Nullstellensatz

Proposition 14.1 (Hilbert's Nullstellensatz – weak form)**.** *Let K be a field and $\mathfrak{a} \lhd K[X_1, \dots, X_n]$ a proper ideal. Then $\mathcal{V}_{\mathfrak{a}}(\overline{K}) \neq \emptyset$, where $\overline{K}$ is an algebraic closure of K.*

This will be proved as a consequence of the Proposition.

Proposition 14.2 (Field theoretic weak Nullstellensatz)**.** *Let K be a field, L/K a field extension and $a_1, \dots, a_n \in L$ elements such that $L = K[a_1, \dots, a_n]$ (that is, the K-algebra homomorphism $K[X_1, \dots, X_n] \xrightarrow{X_i \mapsto a_i} L$ is surjective).*

Then L/K is finite and algebraic.

Lemma 14.3. *The statements of Proposition 14.1 and 14.2 are equivalent.*

Proof. '14.2 $\Rightarrow$ 14.1': Let $\mathfrak{m} \lhd \overline{K}[X_1, \dots, X_n]$ be a maximal ideal containing $\mathfrak{a}$. Then $L := \overline{K}[X_1, \dots, X_n]/\mathfrak{m}$ is a field extension (we factored out a maximal ideal) of $\overline{K}$, which is, of course, the image of a surjective K-algebra homomorphism $\pi : \overline{K}[X_1, \dots, X_n] \to L$ (the natural projection!). By the statement of 14.2 it follows that $L/\overline{K}$ is a finite algebraic extension, hence, $L = \overline{K}$ because $\overline{K}$ is algebraically closed. Writing $a_i := \pi(X_i)$, it follows that $a_i \in \overline{K}$ for $i = 1, \dots, n$. Hence, $(X_1 - a_1, \dots, X_n - a_n) \subseteq \ker(\pi) = \mathfrak{m}$. Due to the maximality of the ideal $(X_1 - a_1, \dots, X_n - a_n)$, it follows that $\mathfrak{a} \subseteq \mathfrak{m} = (X_1 - a_1, \dots, X_n - a_n)$. Consequently, $\mathcal{V}_{\mathfrak{a}}(\overline{K}) \supseteq \mathcal{V}_{\mathfrak{m}}(\overline{K}) = \{(a_1, \dots, a_n)\}$.

'14.1 $\Rightarrow$ 14.2': Consider a K-algebra surjection $\phi : K[X_1, \dots, X_n] \xrightarrow{X_i \mapsto a_i} L$. Its kernel $\mathfrak{m} := \ker(\phi)$ is a maximal ideal, since L is a field. By the statement of 14.1, we have $\mathcal{V}_{\mathfrak{m}}(\overline{K}) \neq \emptyset$. Let $(b_1, \dots, b_n)$ be an element of $\mathcal{V}_{\mathfrak{m}}(\overline{K})$, which gives rise to the K-algebra homomorphism $\psi : K[X_1, \dots, X_n] \xrightarrow{X_i \mapsto b_i} \overline{K}$. Note that $\mathfrak{m}$ is contained in the kernel of ψ (we have $f(b_1, \dots, b_n) = 0$ for all $f \in \mathfrak{m}$), whence they are equal. Consequently, $K \subseteq L \subseteq \overline{K}$, and we conclude that L/K is algebraic. It is finite because it is generated by finitely many algebraic elements. □

Next we are going to prove Proposition 14.2, which by the virtue of Lemma 14.3 automatically proves Proposition 14.1, too.

Proof of Proposition 14.2. Let $L = K[a_1, \dots, a_n]$. It is an affine K-algebra which is a field (and hence an integral domain). So, we may apply Noether normalisation Proposition 12.12. We obtain elements $y_1, \dots, y_r \in L$ such that $L/K[y_1, \dots, y_r]$ is an integral extension and $K[y_1, \dots, y_r]$ is isomorphic to a polynomial ring in r variables. This means, in particular, that there are no relations between the y_i.

Assume $r \geq 1$. Then $y_1^{-1} \in L$ and hence integral over $K[y_1, \dots, y_r]$, so that it satisfies a monic equation of the form

$$y_1^{-n} + f_{n-1}(y_1, \dots, y_r)y_1^{-n+1} + \dots + f_0(y_1, \dots, y_r) = 0,$$

where $f_i(y_1, \dots, y_r) \in K[y_1, \dots, y_r]$. Multiplying through with y^n we get

$$1 + f_{n-1}(y_1, \dots, y_r)y_1 + \dots + f_0(y_1, \dots, y_r)y_1^n = 0,$$

i.e. a non-trivial relation between the y_i. Conclusion: $r = 0$.

Hence, L/K is integral and hence algebraic. It is a finite field extension because it is generated by finitely many algebraic elements. □

Lemma 14.4. *Let K be an algebraically closed field and $\mathfrak{a} \lhd K[X_1, \dots, X_n]$ a proper ideal. Then the maximal ideals $\mathfrak{m} \lhd K[X_1, \dots, X_n]$ which contain $\mathfrak{a}$ are $(X_1 - a_1, \dots, X_n - a_n)$ for $(a_1, \dots, a_n) \in \mathcal{V}_{\mathfrak{a}}(K)$.*

Proof. We first determine what maximal ideals look like in general. Any ideal of the form $(X_1 - a_1, \dots, X_n - a_n)$ is clearly maximal (factoring it out gives K). Conversely, if $\mathfrak{m} \lhd K[X_1, \dots, X_n]$ is maximal then the quotient $K[X_1, \dots, X_n]/\mathfrak{m}$ is a finite algebraic field extension of K by Proposition 14.2, hence, equal to K because K is algebraically closed. Consequently, denoting $a_i := \pi(X_i)$ for $i = 1, \dots, n$ with $\pi : K[X_1, \dots, X_n] \xrightarrow{\text{natural projection}} K[X_1, \dots, X_n]/\mathfrak{m} \cong K$, we find (special case of Lemma 13.15) that $\mathfrak{m} = (X_1 - a_1, \dots, X_n - a_n)$.

Now we prove the assertion. Let $\mathfrak{m} = (X_1 - a_1, \dots, X_n - a_n)$, so that $\{(a_1, \dots, a_n)\} = \mathcal{V}_{\mathfrak{m}}(K)$. We have:

$$\mathfrak{a} \subseteq \mathfrak{m} \Leftrightarrow \{(a_1, \dots, a_n)\} = \mathcal{V}_{\mathfrak{m}}(K) \subseteq \mathcal{V}_{\mathfrak{a}}(K) \Leftrightarrow (a_1, \dots, a_n) \in \mathcal{V}_{\mathfrak{a}}(K).$$

The direction $\Rightarrow$ is trivial. To see the other one, note that $f(a_1, \dots, a_n) = 0$ for $f \in \mathfrak{a}$ implies $f \in \mathfrak{m}$, as $\mathfrak{m}$ is the kernel of $K[X_1, \dots, X_n] \xrightarrow{X_i \mapsto a_i} K$. □

Definition 14.5. *Let R be a ring and $\mathfrak{a} \lhd R$ and ideal. The* radical (ideal) of $\mathfrak{a}$ *is defined as*

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

An ideal $\mathfrak{a}$ is called a radical ideal *if $\mathfrak{a} = \sqrt{\mathfrak{a}}$.*

The Jacobson radical of $\mathfrak{a}$ *is defined as*

$$J(\mathfrak{a}) = \bigcup_{\mathfrak{a} \subseteq \mathfrak{m} \lhd R \text{ maximal}} \mathfrak{m},$$

i.e. the intersection of all maximal ideals of R containing $\mathfrak{a}$ (recall the definition of the Jacobson radical of a ring: intersection of all maximal ideals; it is equal to $J(0)$).

Lemma 14.6. *Let K be a field and $\mathfrak{a} \lhd K[X_1, \dots, X_n]$ an ideal.*

Then $\mathcal{V}_{\mathfrak{a}}(L) = \mathcal{V}_{\sqrt{\mathfrak{a}}}(L)$ for all field extensions L/K.

Proof. The inclusion $\supseteq$ is trivial because of $\mathfrak{a} \subseteq \sqrt{\mathfrak{a}}$. Let now $(a_1, \ldots, a_n) \in \mathcal{V}_{\mathfrak{a}}(L)$, that is, $f(a_1, \ldots, a_n) = 0$ for all $f \in \mathfrak{a}$. Let now $g \in \sqrt{\mathfrak{a}}$. Then there is $m \in \mathbb{N}$ such that $g^m \in \mathfrak{a}$, so that $g(a_1, \ldots, a_n)^m = 0$. Since we are in an integral domain, this implies $g(a_1, \ldots, a_n) = 0$, showing the inclusion $\subseteq$. □

Proposition 14.7 (General Hilbert's Nullstellensatz)**.** *Let K be a field, R an affine K-algebra, $\mathfrak{a} \lhd R$ an ideal. Then $\sqrt{\mathfrak{a}} = J(\mathfrak{a})$.*

Proof. '$\subseteq$': Let $\mathfrak{m} \lhd R$ be any maximal ideal containing $\mathfrak{a}$. Let $f \in \sqrt{\mathfrak{a}}$. Then there is $m \in \mathbb{N}$ such that $f^m \in \sqrt{\mathfrak{a}} \subseteq \mathfrak{m}$. The prime ideal property of $\mathfrak{m}$ now gives that $f \in \mathfrak{m}$. This implies $\sqrt{\mathfrak{a}} \subseteq \mathfrak{m}$.

'$\supseteq$': Let $f \in R \setminus \sqrt{\mathfrak{a}}$. We want to show $f \notin J(\mathfrak{a})$.

From $f \notin \sqrt{\mathfrak{a}}$ it follows that $f^n \notin \mathfrak{a}$ for all $n \in \mathbb{N}$. So, the set $S\{\overline{f}^n \mid n \in \mathbb{N}\} \subseteq R/\mathfrak{a} =: \overline{R}$ is multiplicatively closed and does not contain 0 (the zero of $\overline{R} = R/\mathfrak{a}$, of course). We write $\overline{f}$ for the class $f + \mathfrak{a} \in \overline{R}$. It is a unit in $S^{-1}\overline{R}$ because we are allowing $\overline{f}$ in the denominator.

Let $\overline{\mathfrak{q}}$ be a maximal ideal of $S^{-1}\overline{R}$. As $\overline{f}$ is a unit, $\overline{f} \notin \overline{\mathfrak{q}}$. As R is an affine K-algebra, so is the field $S^{-1}\overline{R}/\overline{\mathfrak{q}} =: L$ (we modded out by a maximal ideal). Proposition 14.2 yields that L/K is a finite field extension.

Note that the ring $\overline{R}/(\overline{R} \cap \overline{\mathfrak{q}})$ contains K and lies in L. Due to the finiteness of L/K, this ring is itself a field, so that $\overline{R} \cap \overline{\mathfrak{q}}$ is a maximal ideal of $\overline{R}$.

Recall that $f \notin \overline{\mathfrak{q}}$, so f does not lie in the maximal ideal $\overline{R} \cap \overline{\mathfrak{q}}$.

Set $\mathfrak{q} := \pi^{-1}(\overline{\mathfrak{q}})$ with the natural projection $\pi : R \twoheadrightarrow \overline{R} = R/\mathfrak{a}$. It is a maximal ideal containing $\mathfrak{a}$, but $f \notin \mathfrak{q}$. Consequently, $f \notin J(\mathfrak{a})$. □

Proposition 14.8 (Hilbert's Nullstellensatz)**.** *Let K be an algebraically closed field and consider an ideal $\mathfrak{a} \lhd K[X_1, \ldots, X_n]$.*

Then $\mathcal{I}_{\mathcal{V}_{\mathfrak{a}}(K)} = \sqrt{\mathfrak{a}}$.

In particular, taking $\mathcal{V}_{\mathfrak{a}}(K)$, the radical ideals of $K[X_1, \ldots, X_n]$ are in bijection with the affine algebraic sets in $\mathbb{A}^n(K)$.

Proof. '$\supseteq$': By Lemmata 5.11 and 14.6 we have $\sqrt{\mathfrak{a}} \subseteq \mathcal{I}_{\mathcal{V}_{\sqrt{\mathfrak{a}}}(K)} = \mathcal{I}_{\mathcal{V}_{\mathfrak{a}}(K)}$.

'$\subseteq$': Let $\mathfrak{m}$ be a maximal ideal of $K[X_1, \ldots, X_n]$ containing $\mathfrak{a}$. By Lemma 14.4 we know $\mathfrak{m} = (X_1 - a_1, \ldots, X_n - a_n)$ for some $(a_1, \ldots, a_n) \in \mathcal{V}_{\mathfrak{a}}(K)$. Let $f \in \mathcal{I}_{\mathcal{V}_{\mathfrak{a}}(K)}$. Then $f(a_1, \ldots, a_n) = 0$ so that $f \in \mathfrak{m}$, as $\mathfrak{m}$ is the kernel of $K[X_1, \ldots, X_n] \xrightarrow{X_i \mapsto a_i} K$. This shows $\mathcal{I}_{\mathcal{V}_{\mathfrak{a}}(K)} \subseteq \mathfrak{m}$, and, hence, $\mathcal{I}_{\mathcal{V}_{\mathfrak{a}}(K)} \subseteq J(\mathfrak{a})$. By Proposition 14.7 we thus get $\mathcal{I}_{\mathcal{V}_{\mathfrak{a}}(K)} \subseteq \sqrt{\mathfrak{a}}$, as was to be shown.

The final statement follows like this:

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

and

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

This shows the correspondence. □