ALGEBRAIC GEOMETRY I

UNIVERSITÄT STUTTGART

Ohne Gewähr auf Vollständig- oder Richtigkeit

ABSTRACT. It is well-known that a complex polynomial $f \in \mathbb{C}[x]$ – an *algebraic object* – is determined up to scalars in $\mathbb{C}^*$ by its zero locus, the n zeroes (counted with multiplicity) in $\mathbb{C}$ – a *geometric object*. This is the simplest instance of an equivalence between an algebraic and a geometric category. To make this statement rigourous will occupy us in the first half of this lecture. In the second half we use algebraic methods to deduce elementary properties of the geometric objects under investigation.

CONTENTS

Date: February 13, 2016.

0. Basic commutative algebra

To keep the prerequesites to a minimum (as covered by the basic algebra courses LAAG I & II and Algebra, see for instance also the books by S. Bosch, *Linear algebra* and *Algebra*, Springer) we will develop the necessary background of *commutative algebra* as we go along. This text is essentially taken from

(i) M. Atiyah and I. MacDonald, *Introduction to Commutative Algebra*, Addison-Wesley;
(ii) D. Eisenbud, *Commutative algebra*, Springer;
(iii) A. Gathmann, *Commutative Algebra*, available at
mathematik.uni-kl.de/agag/mitglieder/professoren/gathmann/notes/;
(iv) M. Reid, *Undergraduate Commutative Algebra*, Cambridge University Press.

No claim of any originality in the presentation of this material is made. Commutative algebra is a theory interesting in its own right with various ramifications, see for instance [Re, Chapter 0.8] or [Ei, Chapter I.1]. Here, of course, we are going to stress the geometric side of the theory.

0.1. **Rings and ideals.**

Basic ring theory. Unless mentioned otherwise, rings will be *commutative* and *with unit* 1. We denote rings generically by A. A *(ring) momorphism* $\phi : A \to B$ is assumed to satisfy $\phi(1_A) = 1_B$. A subring of a ring shares the same identity element. Note in passing that we usually only speak of a morphism and leave it to the context whether it is a morphism of rings, modules, varieties etc. A field is ring in which $1 \neq 0$ and every nonzero element is a unit. If A and B are rings, the direct product $A \times B$ is the set of pairs $\{(a, b) \mid a \in A,\ b \in B\}$ with componentwise addition and multiplication. In particular, if we consider A and B as subsets of $A \times B$ via the embedding $a \mapsto (a, 0)$ and $b \mapsto (0, b)$, then $A \cdot B = 0$ on $A \times B$. Note in passing that A and B embedded this way are *not* subrings for their respective identity elements are $e_1 = (1, 0)$ and $e_2 = (0, 1)$ and thus different from $(1, 1)$, the identity element of $A \times B$. Rather, they form a *complete set of orthogonal idempotents*, in the sense that they satisfy $e_i^2 = e_i$ (idempotency), $e_1 e_2 = 0$ (orthogonality) and $e_1 + e_2 = 1$ (completeness). In general, if $e_1, \ldots, e_r$ is a complete set of orthogonal idempotents in a ring A, then $A \cong Ae_1 \times \ldots \times Ae_r$. If A_i is an infinite family of rings we distinguish between the direct product $\times A_i$ and the direct sum $\bigoplus A_i$. For the latter, there are only a finite number of nonzero components. For a finite number of rings both notions coincide.

A *zerodivisor* $x \in A$ divides 0, i.e. there exists $y \in A \backslash 0$ such that $xy = 0$. An element $x \in A$ is *nilpotent* if $x^n = 0$ for some n. In particular, x is a zerodivisor if $A \neq 0$. A nontrivial ring A is *integral* if A has no zerodivisors, e.g. $A = \mathbb{Z}$. Recall in passing that an integral ring has a *field of fractions* $k = \operatorname{Quot} A$, for instance $\mathbb{Q} = \operatorname{Quot} \mathbb{Z}$. An element $x \in A$ is *invertible* or a *unit* if it divides 1, i.e. there exists $y \in A$ such that $xy = 1$. Units forms a multiplicative subgroup of A which we denote by A^*. For example, if $x \in A$ is nilpotent, then $1 - x$ is invertible in A, for $(1 - x) \cdot \sum_{i=0}^{n-1} x = 1$.

For an integral domain A we say that a nonzero nonunit element $x \in A$ is *irreducible* if $x = yz$ for $y, z \in A$ implies that either y or z is a unit. Further, a nonzero nonunit x is called *prime* if $x|yz$ (x divides yz) implies either $x|y$ or $x|z$. Prime obviously implies irreducible, but the converse is false in general. An integral domain A is said to be a *unique factorisation domain* (UFD for short) if every $a \in A \backslash (A^* \cup \{0\})$ admits a *prime decomposition* $a = a_1 \cdot \ldots \cdot a_r$ into primes which is unique up to order and units. Note that if A is a UFD, then $x \in A$ is irreducible if and only if it is prime [Bo, 2.4.10]. Examples are provided by Euclidean rings such as $\mathbb{Z}$,

$k[x]$. Further, by Gauß' Theorem, the polynomial ring $A[x]$ is a UFD if A is a UFD [Bo, 2.7.1]. In particular, the *polynomial rings* $k[X_1, \dots, X_n]$ are UFDs. For the following exercise, recall that a polynomial $f \in A[x]$ is **monic** if its leading coefficient is 1, i.e. $f = x^n + \sum_{i=0}^{n-1} a_i x^i$.

1. Exercise (roots of monic polynomials). *Let A be a UFD and $k = \operatorname{Quot} A$ its field of fractions. If $f \in A[x]$ is monic and has a root $\alpha \in k \Rightarrow \alpha \in A$.*

Proof. Assume $\alpha \notin A$. Write $\alpha = p/q$, where p and q have no common factors in A. This is possible since A is a UFD. If q is a unit, then $\alpha \in A$ so assume that q is not a unit. If $f = x^n + \sum a_i x^i$, then by assumption, $p^n = -\sum_{i=0}^{n-1} a_i p^i q^{n-i}$, hence $q \mid p^n$. Decompose $q = \prod q_i$ into irreducible factors. Then $q_1 \mid p^n = p^{n-1}p$. Since q_1 is prime it divides either p or p^{n-1}. In the second case we can continue until also $q_1 \mid p$. Contradiction, for q and p have no common factors. □

If a number x divides a and b, then x also divides their sum. This leads to the notion of an *ideal* $\mathfrak{a}$ of A. By definition, this is an additive subgroup such that $xa \in \mathfrak{a}$ whenever $x \in A$ and $a \in \mathfrak{a}$. If $\Sigma \subset A$ is a subset, we write

$$(\Sigma) = \{ \sum_{\text{finite}} x_i a_i \mid x_i \in A,\ a_i \in \Sigma \}$$

for the **ideal generated by** Σ. Geometrically, ideals arise as follows. If $X \subset k^n$, and f and g are two polynomials in $k[x_1, \dots, x_n]$ which considered as polynomial functions vanish on X (i.e. $f(x) = g(x) = 0$ for all $x \in X$), then so does their sum $f + g$. Further, if h is any other polynomial, $h \cdot f$ also vanishes on X. In other words,

$$\mathcal{I}(X) = \{ f \in k[x_1, \dots, x_n] \mid f(x) = 0 \text{ for all } x \in X \}$$

is an ideal. This notion gains its importance from the fact that if $\mathfrak{a}$ is an ideal, then the group quotient $A/\mathfrak{a}$ inherits a natural ring structure and becomes the so-called *quotient ring*. In this sense, an ideal is the ring analogue of a normal subgroup of a group. An important example of ideals are kernels $\ker \phi$ of ring morphisms $\phi : A \to B$. Note in passing that the image $\operatorname{im} \phi$ is merely a subring and not an ideal in general; we have a natural ring isomorphism $\operatorname{im} \phi \cong A/\ker \phi$.

2. Proposition. *For a ring $A \neq \{0\}$, the following properties are equivalent.*

(i) *A is a field;*
(ii) *the only ideals in A are $\{0\} = (0)$ and $A = (1)$;*
(iii) *every morphism of A into a nonzero ring is injective.*

Proof. For (i)⇒(ii) we note that any nonzero ideal in a field k contains a unit and is thus equal to k. For (ii)⇒(iii) we note that $1 \neq 0$ (otherwise $(0) = (1)$) so that any homomorphism $A \to B \neq \{0\}$ is nontrivial (it maps 1_A to 1_B). Hence its kernel must be (0) whence injectivity. Finally, for (iii)⇒(i) we assume that $x \in A$ is nonunit. Then $(x) \subsetneq (1) = A$ so that $B := A/(x)$ is a nontrivial ring. However, the canonical projection $A \to B$ is injective, whence $(x) = 0$. □

In a field k, all ideals are of the form $(x) = \{\sum_{finite} a_i x^i \mid a_i \in k\}$. More generally, an integral domain for which this is true is called a *principal ideal domain (PID)*. This is slightly less general than the notion of a *Euclidean ring* where the Euclidean algorithm can be used to perform divisions with remainder. We have the following implications: A Euclidean ⇒ PID ⇒ UFD ⇒ integral domain. Prime examples of

Euclidean rings are $\mathbb{Z}$ or the polynomial rings $k[x]$ where k is a field (this essentially accounts for their similarity). Note that for more than one variable, $k[x_1, \ldots, x_n]$ is factorial, but not principal.

Maximal and prime ideals. An ideal $\mathfrak{m}$ of A is *maximal* if $\mathfrak{m} \neq A$ and $\mathfrak{m} \subset \mathfrak{a} \subset A$ implies either $\mathfrak{m} = \mathfrak{a}$ or $\mathfrak{m} = A$. In particular, A is a field if and only if (0) is maximal. An ideal $\mathfrak{p} \neq A$ is *prime* if $ab \in \mathfrak{p}$ implies $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$. In particular, A is integral if and only if the ideal (0) is prime.

3. Examples.

(i) Let k be a field and $A := k[x_1, \ldots, x_n]$. If $f \in A$ is irreducible, then the ideal *generated by* f, $(f) = \{gf \mid g \in A\}$, is prime by unique factorisation.
(ii) The prime ideals of $\mathbb{Z}$ are precisely of the form (p) for $p \in \mathbb{Z}$ prime. In fact, this is true for a general ring: $p \in A$ is prime $\Leftrightarrow$ (p) is prime. The same is true for (i) if $n = 1$; , but for $n > 1$, A is no longer principal as we are going to see later.
(iii) In a PID, every nontrivial ideal is maximal. Indeed, let $(a) \neq 0$ be a prime ideal and assume $(b) \supset (a)$, that is $a \in (b)$, or equivalently, $a = xb$. Then either $b \in (a)$ and we have equality, or $x \in (a)$, that is $x = ya$. But then $a = yba$, that is, yb is a unit, so that $(b) = A$.

Existence of maximal ideals is a standard application of *Zorn's lemma* (see for instance [Re, Chapter 1.7 and 1.8]). In fact, one can show that any proper ideal of A is contained in some maximal ideal. It follows in particular that any nonunit of A is contained in some maximal ideal so that for any ring A we have a decomposition $A = A^* \cup \bigcup \mathfrak{m}$, where the union is taken over all maximal ideals. More generally, if $S \subset A$ is a multiplicative subset, any ideal disjoint from S is contained in some prime ideal in $A \backslash S$ [Re, Section 1.9]. (Recall that a subset $S \subset A$ is *multiplicative* if $1 \in S$ and $f, g \in S$ implies $fg \in S$.) The following characterisation is classical [Bo, 2.3.8]:

(i) $\mathfrak{p}$ *is prime if and only if* $A/\mathfrak{p}$ *is an integral domain;*
(ii) $\mathfrak{m}$ *is maximal if and only if* $A/\mathfrak{m}$ *is a field.*

In particular, a maximal ideal is prime, and every prime ideal is obtained as the kernel of a homomorphism $\phi : A \to k$ where $k = \mathrm{Quot}\,(A/\mathfrak{p})$ is the so-called *residue field.*

The set of prime ideals of a ring is obviously a partially ordered set with respect to inclusion, i.e. $\mathfrak{p}_1 \leqslant \mathfrak{p}_2 \Leftrightarrow \mathfrak{p}_1 \supset \mathfrak{p}_2$. Minimal elements are called *minimal primes.*

4. Exercise (Minimal primes). *Use Zorn's lemma to show that any prime ideal contains a minimal prime.*

Proof. Let $\mathfrak{q}$ be a prime ideal and let Σ be the set of prime ideals contained in $\mathfrak{p}$. If $C \subset \Sigma$ is a chain $\{\mathfrak{p}_\lambda\}_{\lambda \in \Lambda}$ for some ordered index set Λ, i.e. $\mathfrak{p}_\lambda \subset \mathfrak{p}_\mu$ if $\lambda \geqslant \mu$, then $\mathfrak{p} = \bigcap \mathfrak{p}_\lambda$ is a prime ideal. Indeed, let $ab \in \mathfrak{p}$ so that $ab \in \mathfrak{p}_\lambda$ for any $\lambda \in \Lambda$. If $a \notin \mathfrak{p}$, then there exists λ_0 such that $a \notin \mathfrak{p}_{\lambda_0}$, whence $a \notin \mathfrak{p}_\lambda$ any $\lambda \geqslant \lambda_0$. In particular, $b \in \mathfrak{p}_\lambda$ for p_λ is prime. Since $\mathfrak{p}_{\lambda_0} \subset \mathfrak{p}_\mu$ for all $\mu \leqslant \lambda_0$, $b \in \mathfrak{p}$ so that $\mathfrak{p} \in \Sigma$. By design, $\mathfrak{p}$ is a lower bound for C. Therefore, Zorn's lemma implies that there exists a minimal element $\mathfrak{p}_0 \in \Sigma$. □

5. Example. Associate with $a \in k^n$ the *evaluation morphism*

$$ev_a : k[x_1, \ldots, x_n] \to k, \quad f \mapsto f(a).$$

Since $A/\ker ev_a \cong k$ is a field, $\mathfrak{m}_a = \ker ev_a$ is a maximal ideal. We show that $\mathfrak{m}_a = (x_1 - a_1, \ldots, x_n - a_n)$. The inclusion $\supset$ is obvious. For the other inclusion, let us first assume $a_i = 0$ and write $f = \sum c_{i_1 \ldots i_n} x_1^{i_1} \ldots x_n^{i_n} \in \mathfrak{m}_a$ as

$$f(x_1, \ldots, x_n) = x_1 g_1(x_1, \ldots, x_n) + f_2(x_2, \ldots, x_n),$$

where $f_2(0, \ldots, 0) = f(0, \ldots, 0) = 0$. We can repeat this proces to obtain

$$f_i(x_i, \ldots, x_n) = x_i g_i(x_i, \ldots, x_n) + f_{i+1}(x_{i+1}, \ldots, x_n)$$

with $f_{i+1}(0, \ldots, 0) = 0$, whence $f = x_1 g_1 + \ldots + x_n g_n \in (x_1, \ldots, x_n)$. The general case now follows from the coordinate change $y_i = x_i - a_i$.

In fact, any maximal ideal is precisely of this form if k is algebraically closed. This will be an easy consequence of the

6. Theorem (weak Nullstellensatz). *If $\mathfrak{m}$ is a maximal ideal in $k[x_1, \ldots, x_n]$, then $k \subset k[x_1, \ldots, x_n]/\mathfrak{m}$ is a finite field extension (see also Appendix for a recap on field extensions).*

Proof. This is a standard fact from algebra which we will assume for the moment as its proof (given in 2.29) requires some additional machinery. □

7. Corollary (points and maximal ideals). *If k is algebraically closed (as we always assume unless mentioned otherwise) every maximal ideal $\mathfrak{m} \subset k[x_1, \ldots, x_m]$ is of the form $\mathfrak{m} = (x_1 - a_1, \ldots, x_n - a_n)$ for $a = (a_1, \ldots, a_n) \in k^n$. Geometrically, this means that maximal ideals in $k[x_1, \ldots, x_n]$ correspond to* points $a = (a_1, \ldots, a_n)$ *in k^n.*

Proof. Indeed, $k \subset K = k[x_1, \ldots, x_n]/\mathfrak{m}$ is a finite, hence algebraic field extension of k. Since k is algebraically closed, $k \cong k[x_1, \ldots, x_n]/\mathfrak{m}$. Compose this isomorphism with the evaluation map $k[x_1, \ldots, x_n] \to K$, $f(x_1, \ldots, x_n) \mapsto f(\alpha_1, \ldots, \alpha_n)$ for α_i = the image of x_i in K. Since this restricts to the identity on k we have $x_i - a_i \in \mathfrak{m}$, the kernel of this map. Hence $(x_1 - a_1, \ldots, x_n - a_n) \subset \mathfrak{m}$. The conclusion follows since $(x_1 - a_1, \ldots, x_n - a_n)$ is maximal by Example 0.5. □

8. Remark. The weak Nullstellensatz has various generalisations (see for instance [Ei, Theorem 4.19]). In particular, we can drop the requirement of algebraically closedness of k, where the weak Nullstellsatz reads as follows. *The maximal ideals of $k[x_1, \ldots, x_n]$ are of the form $\mathfrak{m} = (x_1 - a_1, \ldots, x_n - a_n) \cap k[x_1, \ldots, x_n]$ for $a = (a_1, \ldots, a_n) \in K^n$ where $k \subset K$ is an algebraic field extension*, cf. also Exercise 0.9). The point a is in general not uniquely determined. Indeed, if the field extension $k \subset K$ is Galois with Galois group G, then two points a and $b \in K^n$ give rise to the same maximal ideal if and only if there is an element $\sigma \in G$ such that $\sigma(a) = b$ (cf. [Re, Exercise 5.7]).

9. Exercise (Evaluation maps in nonalgebraically closed fields). *Let $k \subset K$ be an algebraic field extension. For $a = (a_1, \ldots, a_n) \in K^n$, consider the evaluation map* $\mathrm{ev}_a : k[x_1, \ldots, x_n] \to K$.

(i) *Determine the image of* ev_a.
(ii) *Show that* $\ker \mathrm{ev}_a$ *is a maximal ideal.*

(iii) *Show that* $\ker \mathrm{ev}_a = (x_1 - a_1, \ldots, x_n - a_n) \cap k[x_1, \ldots, x_n]$ *(the intersection taking place in* $K[x_1, \ldots, x_n]$*, that is, we consider* $k[x_1, \ldots, x_n]$ *as a subring in* $K[x_1, \ldots, x_n]$ *and* $(x_1 - a_1, \ldots, x_n - a_n)$ *as an ideal in* $K[x_1, \ldots, x_n]$*).*

Proof. (i) $\mathrm{Im}\,\mathrm{ev}_a = k[a_1, \ldots, a_n] = \{\sum_{i_1,\ldots,i_n=0}^{d_1,\ldots,d_n} c_{i_1\ldots i_n} a_1^{i_1} \cdot \ldots \cdot a^{i_n} \mid c_{i_1\ldots i_n} \in k\}$, where $a_i^{d_i+1} = 0$ (recall that $k \subset K$ is algebraic).

(ii) As a subring of an integral domain, $k[a_1, \ldots, a_n]$ has a quotient field which we denote by $k(a_1, \ldots, a_n)$ and which lies inside K. By induction on n we see that $k[a_1, \ldots, a_n] = k(a_1, \ldots, a_n)$ ($n = 1$ was just discussed above). By (i), $k[a_1, \ldots, a_n] \cong k[x_1, \ldots, x_n]/\ker \mathrm{ev}_a$ which shows that $\ker \mathrm{ev}_a$ is maximal.

(iii) The inclusion $\supset$ is clear. For the converse, consider ev_a as a map $K[x_1, \ldots, x_n] \to K$ and let $f \in \ker \mathrm{ev}_a \cap k[x_1, \ldots, x_n]$. By Corollary 0.7, f regarded as an element in $K[x_1, \ldots, x_n]$ lies in $(x_1 - a_1, \ldots, x_n - a_n)$, whence $f \in (x_1 - a_1, \ldots, x_n - a_n) \cap k[x_1, \ldots, x_n]$. □

Local rings. We now come to a key notion in commutative algebra and algebraic geometry. Despite the definition which looks rather special local rings exist in abundance, cf. Section 1.1.3.

10. Definition (local ring and residue field). A ring A is local if it has a unique maximal ideal $\mathfrak{m}$. The field $k = A/\mathfrak{m}$ is called the **residue field** of A.

Trivial examples of local rings are fields. To get more interesting ones we use the following

11. Proposition. *The following properties on a ring* A *are equivalent.*

(i) *A ring* A *is local with maximal ideal* $\mathfrak{m}$*;*
(ii) *all the nonunits of* A *form an ideal* $\mathfrak{m}$*;*
(iii) *there exists an ideal* $\mathfrak{m} \neq (1)$ *such that every* $x \in A\backslash\mathfrak{m}$ *is a unit in* A*;*
(iv) *there exists a maximal ideal* $\mathfrak{m}$ *of* A *such that* $1 + \mathfrak{m} = \{1 + x \mid x \in \mathfrak{m}\} \subset A^*$.

Proof. (i)⇔(ii) If A is local with maximal ideal $\mathfrak{m}$, then we have a disjoint union $A = A^* \cup \mathfrak{m}$, that is, $\mathfrak{m}$ is the set of nonunits which therefore form an ideal. Conversely, any maximal ideal consists of nonunits and must be contained in $\mathfrak{m}$ by assumption. Therefore, $\mathfrak{m}$ is maximal and is the unique ideal with this property.

(ii)⇔(iii) This is a trivial reformulation.

(i)⇔(iv) If $A = A^* \cup \mathfrak{m}$ is local with maximal ideal $\mathfrak{m}$, then $1 + \mathfrak{m} \subset A^*$ for $1 + \mathfrak{m} \cap \mathfrak{m}$ is the empty set. Conversely, let $x \in A\backslash\mathfrak{m}$. By (iii) we must show that x is a unit. Since $\mathfrak{m}$ is maximal, the ideal generated by x and $\mathfrak{m}$ must be A so that there exists $y \in A$ and $m \in \mathfrak{m}$ with $xy + m = 1$. By assumption, $xy = 1 - m \in A^* \subset A\backslash\mathfrak{m}$, thus $x \in A^*$. □

12. Examples. The following examples of local rings are obtained by *localisation* which we will explain in fuller detail in Section 1.1.3. This is the typical way how local rings arise in geometry.

(i) Suppose that one is interested in divisibility in $\mathbb{Z}$ by a particular prime, say 5. Then n is divisible by 5 in $\mathbb{Z} \Leftrightarrow$ it is divisible by 5 in $\mathbb{Z}[1/2, 1/3, 1/7]$. Actually, there is no reason to stop here, so we put

$$\mathbb{Z}_{(5)} = \{\frac{p}{q} \in \mathbb{Q} \mid 5 \nmid q\} \subset \mathbb{Q}.$$

It follows that $5 \nmid n$ in $\mathbb{Z} \Leftrightarrow n/m \in \mathbb{Z}_{(5)}$ is a unit. The nonunits are thus given by $\{p/q \in \mathbb{Z}_{(5)} \mid 5 \mid p\} = 5\mathbb{Z}_{(5)}$ which is an ideal. Therefore, $\mathbb{Z}_{(5)}$ and more generally, $\mathbb{Z}_{(p)}$ for any prime number $p \in \mathbb{Z}$, is a local ring.

(ii) Similarly, we can replace $\mathbb{Z}$ by $k[x]$ to get a more geometrically flavoured example. For instance,

$$\begin{aligned} k[x]_{(x)} &= \{\frac{f}{g} \in k(x) \mid X \nmid g\} \subset k(x) \\ &= \{\frac{f}{g} \mid g(0) \neq 0\} \end{aligned}$$

which is a local ring with maximal ideal $\{\frac{f}{g} \mid f(0) = 0\}$. This example explains the word 'localisation'. Indeed, thinking of $k[x]$ as functions on the x-axis, $k[x]_{(x)}$ can be thought of as the ring of rational functions which are defined near $x = 0$. The maximal ideal is then given by functions which vanish at $x = 0$.

(iii) More generally, let $\mathfrak{p}$ in A a prime ideal of an integral domain, and let

$$A_{\mathfrak{p}} := \{\frac{f}{g} \in \operatorname{Quot} A \mid g \notin \mathfrak{p}\}.$$

One easily checks that this is a ring whose set of nonunits $\{f/g \mid f \in \mathfrak{p},\, g \notin \mathfrak{p}\}$ is an ideal. In particular, $A_{(0)} = \operatorname{Quot} A$.

Radical ideals. In k consider the zero locus $\mathcal{Z}(f) = \{0\}$ of $f(x) = x^2$. Any polynomial $g \in (f)$ also vanishes on $\mathcal{Z}(f)$. Further, so does $p(x) = x$, but $p \notin (f)$. Intuitively, the equation $f = 0$ which defines $\mathcal{Z}(f)$ is not of minimal degree. However, $p^2 \in (f)$. This phenomen leads to a key notion in algebraic geometry:

13. Definition (radical ideal, nilradical, reduced ring). Let $\mathfrak{a} \subset A$ be an ideal. Its **radical** is

$$\sqrt{\mathfrak{a}} := \{a \in A \mid a^n \in \mathfrak{a} \text{ for some } n\}.$$

We obviously have $\mathfrak{a} \subset \sqrt{\mathfrak{a}}$. If equality holds we call $\mathfrak{a}$ a **radical ideal**. Further, we call

$$\operatorname{nil} A := \sqrt{(0)} = \{x \in A \mid x^n = 0 \text{ for some } n \in \mathbb{N}\}$$

the **nilradical** of A. By definition, this is the set of nilpotent elements of A. If $\operatorname{nil} A = 0$, then A is called **reduced**.

14. Remark. In general, consider an ideal $\mathfrak{a} \subset k[x_1, \ldots, x_n]$. Subsets of the form $\mathcal{Z}(\mathfrak{a}) = \{a \in k^n \mid f(a) = 0 \text{ for all } f \in \mathfrak{a}\}$ are called *algebraic sets*. As the example before the definition shows, $\mathfrak{a} \subset \mathcal{I} \circ \mathcal{Z}(\mathfrak{a})$, but the inclusion might be strict. In fact, Hilbert's Nullstellensatz 1.16 states that $\mathcal{I} \circ \mathcal{Z}(\mathfrak{a}) = \sqrt{\mathfrak{a}}$.

15. Lemma (quotient ring characterisation of radical ideals). *The radical of an ideal is itself an ideal. Furthermore, $\mathfrak{a}$ is radical $\Leftrightarrow$ $A/\mathfrak{a}$ is reduced.*

Proof. To show that $\sqrt{\mathfrak{a}}$ is an ideal we first note that it is closed under multiplication. if $a \in \sqrt{\mathfrak{a}}$ so that $a^n \in \mathfrak{a}$, and $x \in A$, then $(xa)^n = x^n a^n \in \mathfrak{a}$ for $\mathfrak{a}$ is an ideal. Further, $0 \in \sqrt{\mathfrak{a}}$, and if a, $b \in \mathfrak{a}$, then $(a+b)^{2k} = \sum_{i=1}^{k} c_i^{2k} a^i b^{2k-i} \in \mathfrak{a}$ for k such that a^k and $b^k \in \mathfrak{a}$. Here, c_i^{2k} are the standard binomial coefficients. Again, since $\mathfrak{a}$ is an ideal, this sum is in $\mathfrak{a}$. Next, let $\bar{x}$ denote the equivalence class of $x \in A$ in $A/\mathfrak{a}$.

$\Rightarrow$) If $\bar{x} \in A/\mathfrak{a}$ is nilpotent, then there exists $n \in \mathbb{N}$ such that $\bar{x}^n = 0$, i.e. $x^n \in \mathfrak{a}$. Hence $x \in \sqrt{\mathfrak{a}}$ which is $\mathfrak{a}$ by assumption, so $\bar{x} = 0$.

$\Leftarrow$) If $x \in \sqrt{\mathfrak{a}}$, i.e. $x^n \in \mathfrak{a}$, then also $\bar{x}^n = 0$ in $A/\mathfrak{a}$. Since the quotient ring is assumed to be reduced, $\bar{x} = 0$, whence $x \in \mathfrak{a}$. □

16. Proposition (Nilradical and prime ideals).

$$\operatorname{nil} A = \bigcap_{\mathfrak{p} \subset A \text{ prime}} \mathfrak{p}$$

Put differently, $f \in A$ is not nilpotent $\Leftrightarrow$ there is a prime ideal $\mathfrak{p} \subset A$ such that $f \notin \mathfrak{p}$.

Proof. $\Leftarrow$) If f is nilpotent it belongs to every prime ideal for $0 = f^n = f^{n-1} f \in \mathfrak{p}$ etc.

$\Rightarrow$) Let $f \in A$ be not nilpotent. Consider the multiplicative subset $S = \{1, f, f^2, \ldots\}$ of A generated by f. Since f is not nilpotent, $0 \notin S$ so that $S \cap (0) = \varnothing$. By 0.0.1 we know that there is a prime ideal which does not intersect S. □

17. Corollary (radical ideals and prime ideals). *If $\mathfrak{a} \subset A$ is radical $\Rightarrow$*

$$\mathfrak{a} = \bigcap_{\mathfrak{a} \subset \mathfrak{p} \text{ prime}} \mathfrak{p}.$$

Proof. Just apply the previous proposition to $A/\mathfrak{a}$ and recall that for any surjective morphism $p : A \to B \cong p(A)$ (and in particular, for $B = A/\mathfrak{a}$), there is a $1-1$ order preserving correspondence between ideals $\mathfrak{a}$ containing $\ker p$, and ideals $\mathfrak{b}$ in $p(A)$ provided by $p^{-1}(\mathfrak{b})$. □

18. Corollary (rings with zerodivisors). *If A is a ring with zerodivisors, then either A is not reduced, or it has more than one minimal prime ideal.*

Proof. Indeed, assume that $\operatorname{nil} A = \bigcap \mathfrak{p} = (0)$, where the intersection is taken over all prime ideals, cf. Proposition 0.16. Now any prime ideal contains a minimal one (a consequence of Zorn's lemma, since the intersection of prime ideals in a prime ideal is again prime), so we can restrict the intersection to minimal primes in A. If there is only one minimal prime $\mathfrak{p}_0$, then $(0) = \bigcap \mathfrak{p} = \mathfrak{p}_0$ and A is an integral domain, a contradiction. □

More generally, we can define $\sqrt{E}$ in the same way for any subset $E \subset A$. Of course, $\sqrt{E}$ is no longer an ideal in general. For later use we note the following

19. Proposition.

(i) $\sqrt{\bigcup_i E_i} = \bigcup_i \sqrt{E_i}$ for any family of subsets E_i.

(ii) *Let* $\operatorname{ann}(x) = \{a \in A \mid a \cdot x = 0\}$ *denote the* **annihilator of** x **in** A. *then* $D =$ *the set of zero-divisors of* $A = \bigcup_{x \neq 0} \sqrt{\operatorname{ann}(x)}$.

Proof. (i) Straightforward.

(ii) We need to show $D = \sqrt{D}$. Indeed, if $a^n \in D$, then there exists $0 \neq x \in A$ such that $x \cdot a^n = x \cdot a \cdot a^{n-1} = 0$. Hence, either $x \cdot a = 0$ and thus $a \in D$, or $a^{n-1} \in D$. After a finite number of steps, $a \in D$. □

In the same way, we can also consider the intersection of all maximal ideals.

20. Definition (Jacobson radical). The Jacobson radical $\mathcal{J}(A)$ of a ring A is the intersection of all maximal ideals. of A.

By Remark 0.23 below this is indeed a radical ideal. It can be characterised as follows:

21. Proposition. $x \in \mathcal{J}(A) \Leftrightarrow 1 - xy$ *is a unit in* A *for all* $y \in A$.

Proof. $\Rightarrow$) Suppose that $1 - xy$ is not a unit. Then it is contained in some maximal ideal $\mathfrak{m}$. Since $x \in \mathcal{J}(A) \subset \mathfrak{m}$, $xy \in \mathfrak{m}$ and thus $1 \in \mathfrak{m}$, a contradiction.

$\Leftarrow$) By contraposition. Suppose $x \notin \mathfrak{m}$ for some maximal ideal. Then $(\mathfrak{m}, x) = A$ by maximality of $\mathfrak{m}$, hence $m + yx = 1$ for some $m \in \mathfrak{m}$ and $y \in A$. Hence $m = 1 - xy$ is not a unit. □

Operations on ideals. If $\mathfrak{a}$ and $\mathfrak{b}$ are two ideals of A, the following operations give new ideals.

(i) The **sum** is the ideal defined by

$$\mathfrak{a} + \mathfrak{b} := \{a + b \mid a \in \mathfrak{a} \text{ and } b \in \mathfrak{b}\} = (\mathfrak{a} \cup \mathfrak{b})$$

(check the latter identity!). It is the smallest ideal containing $\mathfrak{a}$ and $\mathfrak{b}$. Similarly, $\sum_i \mathfrak{a}_i$ consists of elements of the form $\sum a_i$ with $a_i \in \mathfrak{a}_i$ all of which are zero but a finite number.

(ii) The **intersection** $\mathfrak{a} \cap \mathfrak{b}$ is again an ideal, while the union is not, in general.

(iii) The **product** is the ideal defined by

$$\mathfrak{a} \cdot \mathfrak{b} := (\{a \cdot b \mid a \in \mathfrak{a},\ b \in \mathfrak{b}\}).$$

Similarly, we can define the product of a finite number of ideals. In particular, we have the *powers* $\mathfrak{a}^n$ of an ideal (with the convention $\mathfrak{a}^0 = (1)$. Thus $\mathfrak{a}^n$ is the ideal generated by all products $x_1 \cdot \ldots \cdot x_n$ with $x_i \in \mathfrak{a}$.

(iv) The **quotient** is the ideal defined by

$$\mathfrak{b} : \mathfrak{a} := \{x \in A \mid x\mathfrak{a} \subset \mathfrak{b}\}.$$

As usual, we often write simply x for the principal ideal (x) generated by x. In particular, if $\mathfrak{a} = (a)$ and $\mathfrak{b} = (ab)$, then $\mathfrak{b} : \mathfrak{a} = ab : b = (b)$ if a is not a zerodivisor. In particular, $0 : \mathfrak{b} = \{x \in A \mid x\mathfrak{b} = 0\}$ is called the **annihilator of** $\mathfrak{b}$ **in** A and is also written $\operatorname{ann}(\mathfrak{b})$. Note that $\operatorname{ann}(x) = \operatorname{ann}((x))$ so that the notation is consistent with the one introduced in Proposition 0.19.

22. Examples.

(i) If $A = \mathbb{Z}$, $\mathfrak{a} = (m)$ and $\mathfrak{b} = (n)$, then $\mathfrak{a} + \mathfrak{b} = (g.c.d.(n, m))$; $\mathfrak{a} \cap \mathfrak{b} = (l.c.m.(n, m))$; and $\mathfrak{ab} = (nm)$. Thus $\mathfrak{a} \cdot \mathfrak{b} = \mathfrak{a} \cap \mathfrak{b} \Leftrightarrow m$, n are coprime. Similar statements are true in any principal ideal domain.
(ii) Let $\mathfrak{a} = (x_1, \ldots, x_n) \subset A = k[x_1, \ldots, x_n]$. Then $\mathfrak{a}^k$ is the set of polynomials with no terms of degree $< k$.

23. Remark. We have the following properties which can be checked by direct computation.

(i) Sum, intersection, and product are all commutative and associative.
(ii) $\mathfrak{a}(\mathfrak{b} + \mathfrak{c}) = \mathfrak{ab} + \mathfrak{ac}$.
(iii) $\mathfrak{a} \cap (\mathfrak{b} + \mathfrak{c}) = \mathfrak{a} \cap \mathfrak{b} + \mathfrak{a} \cap \mathfrak{c}$ if $\mathfrak{a} \supset \mathfrak{b}$ or $\mathfrak{a} \supset \mathfrak{c}$.
(iv) $\mathfrak{ab} \subset \mathfrak{a} \cap \mathfrak{b}$ with equality provided $\mathfrak{a} + \mathfrak{b} = (1)$, that is, $\mathfrak{a}$ and $\mathfrak{b}$ are *coprime*.
(v) $\mathfrak{a} \subset (\mathfrak{a} : \mathfrak{b})$.
(vi) $(\mathfrak{a} : \mathfrak{b})\mathfrak{b} \subset \mathfrak{a}$.
(vii) $((\mathfrak{a} : \mathfrak{b}) : \mathfrak{c}) = (\mathfrak{a} : \mathfrak{bc}) = ((\mathfrak{a} : \mathfrak{c}) : \mathfrak{b})$.
(viii) $(\bigcap_i \mathfrak{a}_i : \mathfrak{b}) = \bigcap_i (\mathfrak{a}_i : \mathfrak{b})$.
(ix) $(\mathfrak{a} : \sum_i \mathfrak{b}_i) = \bigcap_i (\mathfrak{a} : \mathfrak{b}_i)$.
(x) $\sqrt{\sqrt{\mathfrak{a}}} = \sqrt{\mathfrak{a}}$, i.e. any radical is a radical ideal.
(xi) $\sqrt{\mathfrak{ab}} = \sqrt{\mathfrak{a} \cap \mathfrak{b}} = \sqrt{\mathfrak{a}} \cap \sqrt{\mathfrak{b}}$.
(xii) $\sqrt{\mathfrak{a}} = (1) \Leftrightarrow \mathfrak{a} = (1)$.
(xiii) $\sqrt{\mathfrak{a} + \mathfrak{b}} = \sqrt{\sqrt{\mathfrak{a}} + \sqrt{\mathfrak{b}}}$.
(xiv) If $\mathfrak{p}$ is prime, $\sqrt{\mathfrak{p}^n} = \mathfrak{p}$ for all $n > 0$.

24. Proposition (union of primes and primes as intersection).

(i) *Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ be prime ideals and let $\mathfrak{a}$ be an ideal contained in $\bigcup \mathfrak{p}_i \Rightarrow \mathfrak{a} \subset \mathfrak{p}_i$ for some i.*
(ii) *Let $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ be ideals, and let $\mathfrak{p}$ be a prime ideal containing $\bigcap \mathfrak{a}_i \Rightarrow \mathfrak{a}_i \subset \mathfrak{p}$ for some i. If $\mathfrak{p} = \bigcap \mathfrak{a}_i$, then $\mathfrak{a}_i = \mathfrak{p}$.*

Proof. (i) Proof by induction on n in the form

$$\mathfrak{a} \not\subset \mathfrak{p}_i \text{ for } 1 \leqslant i \leqslant n \Rightarrow \mathfrak{a} \not\subset \bigcup \mathfrak{p}_i.$$

For $n = 1$ there is nothing to prove, so let $n > 1$. By induction, the result is true for $n - 1$ so that for all i there is $x_i \in \mathfrak{a}$ such that $x_i \notin \bigcup_{j \neq i} \mathfrak{p}_j$. Then, if for some $i = 1, \ldots, n$, $x_i \notin \mathfrak{p}_i$, we are done. Otherwise, $x_i \in \mathfrak{p}_i$ for all $i = 1, \ldots, n$. Consider the element

$$y = \sum_{j=1}^{n} x_1 \cdot \ldots \cdot \hat{x}_j \cdot \ldots \cdot x_n,$$

where $\hat{x}_j$ denotes ommission. Then $y \in \mathfrak{a}$ and $y \notin \mathfrak{p}_i$, $i = 1 \ldots, n$, hence $a \not\subset \bigcup_i \mathfrak{p}_i$. Indeed, if $y \in \mathfrak{p}_i$ for some i, then $x_1 \cdot \ldots \cdot \hat{x}_i \cdot \ldots \cdot x_n = y - \sum_{j \neq i} x_1 \cdot \ldots \cdot \hat{x}_j \cdot \ldots \cdot x_n \in \mathfrak{p}_i$. However, this implies that at least one $x_j \in \bigcup_{l \neq j} \mathfrak{p}_l$, a contradiction to defining property of x_j.

(ii) Proof by contraposition. Suppose $a_i \not\subset \mathfrak{p}$ for all i. Then there exists $x_i \in \mathfrak{a}_i$ with $x_i \notin \mathfrak{p}$, and thus $x_1 \cdot \ldots \cdot x_n \in \mathfrak{a}_1 \cdot \ldots \cdot \mathfrak{a}_n \subset \bigcap \mathfrak{a}_i$. However, $x_1 \cdot \ldots \cdot x_n \notin \mathfrak{p}$ for $\mathfrak{p}$ is prime so that $\bigcap \mathfrak{a}_i \not\subset \mathfrak{p}$. Finally, if $\mathfrak{p} = \bigcap \mathfrak{a}_i$, then $\mathfrak{p} \subset \mathfrak{a}_i$, whence $\mathfrak{p} = \mathfrak{a}_i$ for some i. □

25. Exercise (Reduced rings with finitely many primes). *Let A be a reduced ring with finitely many distinct minimal primes $\mathfrak{p}_i$, $i = 1, \dots, n \Rightarrow$*

$$A \to \oplus_i A/\mathfrak{p}_i, \quad a \mapsto (a \bmod \mathfrak{p}_1, \dots, a \bmod \mathfrak{p}_n)$$

is an injection. Furthermore, the image has nontrivial intersection with every summand.

Proof. Assume that $(a \bmod \mathfrak{p}_1, \dots, a \bmod \mathfrak{p}_n) = 0$. Then $a \in \bigcap_i \mathfrak{p} = \bigcap \mathfrak{p}$, where the intersection is taken over all primes (here we use the minimality). Since $\bigcap \mathfrak{p} = \operatorname{nil} A = \{0\}$ (here we use that A is reduced), $a = 0$. Hence the map is injective. Now let $i \in \{1, \dots, n\}$. We must show that there exists $a \in A$ such that $a \bmod \mathfrak{p}_i \neq 0$, but $a \bmod \mathfrak{p}_j = 0$ for $j \neq i$. Assume that this is not the case. Then for all $a \in \bigcap_{j \neq i} \mathfrak{p}_j$, $a \bmod \mathfrak{p}_i = 0$, i.e. $a \in \mathfrak{p}_i$ so that $\bigcap_{j \neq i} \mathfrak{p}_j \subset \mathfrak{p}_i$. By Proposition 0.24, there exists $j \neq i$ with $\mathfrak{p}_j \subset \mathfrak{p}_i$, and thus $\mathfrak{p}_j = \mathfrak{p}_i$ by minimality. Contradiction! □

Ideals under morphisms. Next we investigate the behaviour of ideals under ring morphisms $\varphi : A \to B$. Such a morphism can be factorised as

$$A \overset{\pi}{\twoheadrightarrow} f(A) \overset{\iota}{\hookrightarrow} B,$$

so it is enough to understand what is happening for surjective and injective maps.

First we consider the surjective case, i.e. morphisms of the form $\pi : A \to \pi(A) \cong A/\mathfrak{a}$ for an ideal $\mathfrak{a} \subset A$. We have already used in Corollary 0.17 the $1-1$ order preserving correspondence between ideals $\mathfrak{a}$ containing $\ker p$, and ideals $\mathfrak{b}$ in $\pi(A)$ provided by $\pi^{-1}(\mathfrak{b})$. Moreover, if $\mathfrak{a}$ is a radical/prime/maximal ideal, and if $\mathfrak{b} \subset \mathfrak{a}$ is an ideal, then $\mathfrak{a}/\mathfrak{b}$ is radical/prime/maximal in $A/\mathfrak{b}$ as follows from the isomorphism $(A/\mathfrak{b})/(\mathfrak{a}/\mathfrak{b}) \cong A/\mathfrak{a}$.

Now some general observations. The inverse image under φ of an ideal $\mathfrak{b}$ in B is always an ideal. However, the image under φ of an ideal $\mathfrak{a}$ is usually no longer an ideal as the example of the inclusion $\mathbb{Z} \to \mathbb{Q}$ shows (take any nonzero ideal $(m) \subset \mathbb{Z}$).

26. Definition (extension and contraction of an ideal). If $\mathfrak{a}$ is an ideal in A, then the ideal $\mathfrak{a}^e := (\varphi(\mathfrak{a}))$ in B generated by the image of $\mathfrak{a}$ is called the **extension of $\mathfrak{a}$ (under φ)**. Explicitly, $\mathfrak{a}^e = \{\sum_{\text{finite}} b_i \varphi(a_i) \mid a_i \in \mathfrak{a},\, b_i \in B\}$. Further, we call the ideal $\mathfrak{b}^c = \varphi^{-1}(\mathfrak{b})$ the **contraction of $\mathfrak{b}$ (under φ)**.

27. Remark. The contraction of a maximal ideal need not be maximal again. However, the contraction of a prime ideal is prime again, while the extension of a prime ideal is not prime in general

28. Example. For an integral domain A, consider the inclusion $A \to k = \operatorname{Quot} A$. As a field, k has only two ideals, (0) and k. Their respective contractions in A are (0) and A respectively. Note that $(0)^c$ is no longer maximal, but still prime. Conversely, let $\mathfrak{a} \subset A$ be an ideal in $\mathbb{Z}$. Then unless $\mathfrak{p} = (0)$, $\mathfrak{p}^e = \operatorname{Quot} A$.

A more interesting case is the following classical

29. Example from algebraic number theory. Consider $\mathbb{Z} \hookrightarrow \mathbb{Z}[i]$, where $\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}$ is the ring of *Gaussian integers* (this is a Euclidean ring). The extension of a prime ideal (p) of $\mathbb{Z}$ may or may not stay prime. Indeed, there are three cases to consider:

(i) $(2)^e = ((1+i)^2)$, which is the square of the prime ideal $(1+i)$ in $\mathbb{Z}[i]$;

(ii) if $p \equiv 1 \bmod 4$, then $(p)^e$ is the product of two distinct prime ideals (for example, $(5)^e = (2+i)(2-i)$;
(iii) if $p \equiv 3 \bmod 4$, then $(p)^e$ is prime in $\mathbb{Z}[i]$.

This yields all prime ideals of $\mathbb{Z}[i]$.

30. Exercice (Extensions and Contraction of ideals). *Let $\varphi : A \to B$ a ring morphism. Then*

(i) $\mathfrak{a} \subset \mathfrak{a}^{ec}$ *and* $\mathfrak{b} \supset \mathfrak{b}^{ce}$*;*
(ii) $\mathfrak{b}^c = \mathfrak{b}^{cec}$ *and* $\mathfrak{a}^e = \mathfrak{a}^{ece}$*;*
(iii) *if $\mathcal{C}$ is the set of contracted ideals in A and if $\mathcal{E}$ is the set of extended ideals in B, then $\mathcal{C} = \{\mathfrak{a} \mid \mathfrak{a}^{ec} = \mathfrak{a}\}$, $\mathcal{E} = \{\mathfrak{b} \mid \mathfrak{b}^{ce} = \mathfrak{b}\}$;*
(iv) $\mathfrak{a} \mapsto \mathfrak{a}^e$ *is a bijective map of $\mathcal{C}$ onto $\mathcal{E}$, whose inverse is $\mathfrak{b} \mapsto \mathfrak{b}^c$.*

Proof. Direct computation. □

Spectra.

31. Definition (spectrum of a ring). The **(prime) spetrum** of a ring A is defined by

$$\operatorname{Spec} A = \{\mathfrak{p} \subset A \mid \mathfrak{p} \text{ is prime in } A\}.$$

One sometimes also considers the **maximal spectrum** $\operatorname{mSpec} A$ consisting of maximal ideals only.

32. Examples.

(i) A ring k is a field $\Leftrightarrow$ (0) is maximal. Hence $\operatorname{mSpec} k = \operatorname{Spec} k = \{0\}$. More generally, $\operatorname{mSpec} k[x_1, \ldots, x_n] \cong k^n$ for a field k by Corollary 0.7.
(ii) $\operatorname{Spec} \mathbb{Z} = \{(0), (2), (3), (5), \ldots\}$ while $\operatorname{Spec} \mathbb{Z}[i]$ consists of the following types of prime ideals (cf. Example 0.29) (0), $(1+i) = (1-i)$, p^e if $p \equiv 3 \bmod 4$ (the extension being taken with respect to the inclusion $\mathbb{Z} \to \mathbb{Z}[i]$), and prime ideals $\mathfrak{q}$ such that $\mathfrak{q}\bar{\mathfrak{q}} = (p)^e$ for $p \equiv 1 \bmod 4$.
(iii) If k is a (not necessarily algebraically closed) field, then $k[x]$ is Euclidean. In particular, a nontrivial ideal $\mathfrak{p} = (f)$ in $k[x]$ is prime $\Leftrightarrow$ f is irreducible, that is,

$$\operatorname{Spec} k[x] = \{(0)\} \cup \{(f) \mid f \text{ irreducible}\}.$$

For instance, we find for $k = \mathbb{R}$ that f is irreducible if and only if up to units, $f = x - a$ or $f = (x-z)(x-\bar{z}) = \mathbb{R}[x] \cap (x-z)$ for $z \in \mathbb{C}\backslash\mathbb{R}$. Hence $\operatorname{Spec} \mathbb{R}[x] = \{(0)\} \cup \mathbb{R} \cup \{z \in \mathbb{C} \mid \operatorname{im} z > 0\}$. If, in addition, k is algebraically closed, then irreducible polynomials are up to units of the form $x - a$ for $a \in k$ so that in this case, $\operatorname{Spec} k[x] = \{(0)\} \cup k$. Note that $\operatorname{mSpec} k[x] = k$ can be thought of as the set of points of k. For the geometric interpretation of the trivial ideal (0), see Exercise 0.38.
(iv) Let $\mathfrak{a} \subset A$ be an ideal. By what we said before Definition 0.103, $\operatorname{Spec} A/\mathfrak{a} = \{\mathfrak{p} \in \operatorname{Spec} A \mid \mathfrak{a} \subset \mathfrak{p}\}$.
(v) Let k be a not necessarily algebraically closed field. We think of $k[x,y]$ as $(k[x])[y]$. Then the prime ideals of $k[x,y]$ are as follows: (0), (f) for $f \in k[x,y]$ irreducible, and maximals ideals of the form $\mathfrak{m} = (p, g)$ where $p \in k[x]$ is an irreducible polynomial, and $g \in k[x,y]$ a polynomial such $\bar{g} \in (k[x]/(p))[y]$ is irreducible. In particular, $k[x,y]/\mathfrak{m} = (k[x]/(p))[y]/(\bar{g})$ is a finite extension field of k (see Proposition 0.33 below).

(vi) The prime ideals of $\mathbb{Z}[y]$ are as follows: (0), (f) for $f \in \mathbb{Z}[x]$ irreducible, and maximal ideals of the form $\mathfrak{m} = (p, g)$ where $p \in \mathbb{Z}$ is a prime number, and $g \in \mathbb{Z}[y]$ a polynomial such $\bar{g} \in \mathbb{F}_p[y]$ where $\mathbb{F}_p = \mathbb{Z}/(p)$ is irreducible. In particular, $\mathbb{Z}[y]/\mathfrak{m} = (\mathbb{Z}/(p))[y]/(\bar{g}) = \mathbb{F}_p[y]/(\bar{g})$ is a finite extension field of $\mathbb{F}_p$. Note the similarity between the previous example (think of $k[x, y]$ as $(k[x])[y]$) which highlights again the analogy between the Euclidean rings $k[x]$ and $\mathbb{Z}$ (see Proposition 0.33 below).

The cases (iv) and (v) follow from the following proposition if we put $B = k[x]$ with $K = k(x) = \operatorname{Quot} B$, and $B = \mathbb{Z}$ with $K = \mathbb{Q}$ respectively.

33. Proposition. *Let B be a principal ideal domain and K its field of fractions $\Rightarrow$ the prime ideals of the UFD $A = B[y]$ are as follows:*

(i) (0);
(ii) (p) *for $p \in A$ with p prime*;
(iii) *maximal ideals of the form $\mathfrak{m} = (p, g)$ where $p \in B$ is irreducible, and $g \in A$ such that $\bar{g} \in B/(p)[y]$ is irreducible.*

Proof. Recall that a polynomial $f \in K[y]$ for $K = \operatorname{Quot} B$, B a UFD, has a *reduced expression* $f = af_0$ where $a \in K$ and $f_0 \in B[y]$ is *primitive*, that is, its coefficients have no common factor in B other than units. *Gauß' lemma* asserts that the product of two primitive polynomials is again primitive.

If the prime ideal $\mathfrak{p}$ in A is principal, then there is nothing to prove. Otherwise we can assume that $\mathfrak{p}$ contains two elements f_1 and $f_2 \in A = B[y]$ with no common factor in A (since A is a UFD it is enough to pick an irreducible element $f_1 \neq 0$ in $\mathfrak{p}$, and to take $f_2 \in \mathfrak{p} \backslash (f_1)$).

Step 1. *f_1 and f_2 have no common factors in $K[y] \supset B[y] = A$.* Assume not. Write $f_i = hg_i$ with h, g_1 and g_2 in $K[y]$, and $\deg h > 0$. Consider their reduced expressions $h = ah_0$, $g_i = b_i\gamma_i$ with a, b_1 and $b_2 \in K$ and h_0, γ_1 and γ_2 in $B[y]$ primitive. By Gauß' lemma, $h_0\gamma_i$ is again primitive, so that $A = B[y] \ni f_i = hg_i = (ab_i)(h_0\gamma_i)$ implies $ab_1 \in B$, and similarly, $ab_2 \in B$. Hence h_0 divides f_1 and f_2 in A, a contradiction.

Step 2. *The ideal $\mathfrak{a}$ generated by f_1 and f_2 has nonzero intersection with B, that is, $(f_1, f_2) \cap B \neq 0$.* Indeed, $K[y]$ is a PID, and $\gcd(f_1, f_2) = 1$ by the previous step. Hence there exist g_1, $g_2 \in K[y]$ such that $g_1f_1 + g_2f_2 = 1$. If $b \in B$ is a common denominator of the coefficients of g_1 and g_2, then bg_1 and $bg_2 \in A = B[y]$, whence $\mathfrak{a} \ni bg_1f_1 + bg_2f_2 = b$ is also in B.

Step 3. *Conclusion.* If $\mathfrak{p}$ is a prime of $A = B[y]$, then $B \cap \mathfrak{p}$ is a prime of B. By the previous step, $B \cap \mathfrak{p} = (p)$ for p a prime in B (B is a PID!). Now any nontrivial prime in a PID is maximal so that $k_p := B/(p)$ is in fact a field. Moreover, the natural map $A = B[y] \to k_p[y]$ obtained by reducing the coefficients mod p is surjective with kernel given by $(p)^e \subset \mathfrak{p}$ (the extension being taken with respect to the inclusion $B \subset A$). Consequently, $\mathfrak{p}$ corresponds to a prime (and thus maximal) ideal in $k_p[y]$ which must be of the form $(\bar{g})$ for a reduced element $g \in A$. Hence $\mathfrak{p} = (p, g)$, and $\mathfrak{p}$ is maximal.

□

34. Remark. Note that $A/\mathfrak{p} \cong (A/(p)^e)/(\mathfrak{p}/(p)^e) \cong k_p[y]/(\bar{g})$ is a finite field extension of $k_p = B/(p)$. Hence, if $B = k[x]$ where k is algebraically closed, any

finite extension of k is just k so that p and g are irreducible polynomials in $k[x]$ resp. $k[y]$, and therefore linear. In particular, $\mathfrak{m} = (x-a, y-b)$ for $a, b \in k$.

35. Exercise (Zariski topology of $\operatorname{Spec} A$**).** *For each $T \subset A$, let $\mathcal{Z}(T) \subset \operatorname{Spec} A$ denote the set of all prime ideals of A which contain T. Show that*

(i) *if $\mathfrak{a}$ is the ideal generated by T, then $\mathcal{Z}(T) = \mathcal{Z}(\mathfrak{a}) = \mathcal{Z}(\sqrt{\mathfrak{a}})$ and $\mathcal{Z}(\mathfrak{a}) = \operatorname{Spec} A/\mathfrak{a}$;*

(ii) *$\mathcal{Z}(0) = \operatorname{Spec} A$ and $\mathcal{Z}(1) = \varnothing$;*

(iii) *if $(T_i)_{i\in I}$ is any family of subsets of A, then*

$$\mathcal{Z}\Big(\bigcup_{i\in I} T_i\Big) = \bigcap_{i\in I} \mathcal{Z}(T_i);$$

(iv) *$\mathcal{Z}(\mathfrak{a}\cap\mathfrak{b}) = \mathcal{Z}(\mathfrak{a}\mathfrak{b}) = \mathcal{Z}(\mathfrak{a}) \cup \mathcal{Z}(\mathfrak{b})$ for any two ideals $\mathfrak{a}$, $\mathfrak{b}$ of A.*

It follows that the sets $\mathcal{Z}(T)$ satisfy the axioms for closed sets in a topological space. The resulting topology is called the **Zariski topology** *of* $\operatorname{Spec} A$.

Proof. (i) The only nontrivial inclusion requires to show that for any prime ideal $\mathfrak{p}$, $\mathfrak{a} \subset \mathfrak{p}$ implies $\sqrt{\mathfrak{a}} \subset \mathfrak{p}$. Now if $a \in \sqrt{\mathfrak{a}}$, then $a^n \in \mathfrak{a} \subset \mathfrak{p}$ for some n. Hence either $a \in \mathfrak{p}$ or $a^{n-1} \in \mathfrak{p}$. Continuing this way if necessary, we see that $a \in \mathfrak{p}$ after a finite number of steps. Next we know that the prime ideals in $A/\mathfrak{a}$ correspond precisely to the prime ideals of A containing $\mathfrak{a}$.

(ii) Clear.

(iii) $\mathfrak{p} \in \mathcal{Z}(\bigcup T_i) \Leftrightarrow T_i \subset \mathfrak{p}$ for all i, whence the assertion.

(iv) Since $\sqrt{\mathfrak{a}\mathfrak{b}} = \sqrt{\mathfrak{a}\cap\mathfrak{b}} = \sqrt{\mathfrak{a}\mathfrak{b}}$ by Remark 0.23, the only nontrivial inclusion is $\mathcal{Z}(\mathfrak{a}\cap\mathfrak{b}) \subset \mathcal{Z}(\mathfrak{a}) \cup \mathcal{Z}(\mathfrak{b})$. Now by Proposition 0.24 (ii), $\mathfrak{a}\cap\mathfrak{b} \subset \mathfrak{p}$ implies $\mathfrak{a} \subset \mathfrak{p}$ or $\mathfrak{b} \subset \mathfrak{p}$, whence $\mathfrak{p} \in \mathcal{Z}(\mathfrak{a}) \cup \mathcal{Z}(\mathfrak{b})$. □

36. Exercise (Basic open sets for the Zariski topology). *For each $a \in A$ let D_a denote the complement of $\mathcal{Z}(a)$ in $\operatorname{Spec} A$. In particular, D_a is open, the so-called* **basic open set**. *Show that*

(i) *$\{D_a\}_{a\in A}$ forms a basis of open sets for the Zariski topology (i.e. any open set is a union of open sets of the form D_a);*

(ii) *$D_a \cap D_b = D_{ab}$;*

(iii) *$D_a = \varnothing \Leftrightarrow a$ is nilpotent;*

(iv) *$D_a = \operatorname{Spec} A \Leftrightarrow a$ is a unit;*

(v) *$D_a = D_b \Leftrightarrow \sqrt{(a)} = \sqrt{(b)}$;*

(vi) $\operatorname{Spec} A$ *is* quasi-compact *(i.e. every open covering of $\operatorname{Spec} A$ has a finite subcovering).*

Proof. (i) This follows from $\mathcal{Z}(T) = \bigcap_{a\in T} \mathcal{Z}(a)$ by taking complements.

(ii) $(D_a \cap D_b)^c = \mathcal{Z}(a) \cup \mathcal{Z}(b) = \mathcal{Z}(ab)$ by (iv) of the previous exercise.

(iii) $D_a = \varnothing \Leftrightarrow \mathcal{Z}(a) = \operatorname{Spec} A \Leftrightarrow a \subset \bigcap_{\mathfrak{p}\in\operatorname{Spec} A} \mathfrak{p} = \operatorname{nil} A$ by Proposition 0.16.

(iv) $D_a = \operatorname{Spec} A \Leftrightarrow \mathcal{Z}(a) = \varnothing \Leftrightarrow a$ is a unit. (otherwise a would be contained in some maximal ideal).

(v) $D_a = D_b \Leftrightarrow \mathcal{Z}(\sqrt{(a)}) = \mathcal{Z}(a) = \mathcal{Z}(b) = \mathcal{Z}(\sqrt{(b)})$. This implies that a prime ideal $\mathfrak{p}$ contains $\sqrt{(a)} \Leftrightarrow \mathfrak{p}$ contains $\sqrt{(b)}$. By Corollary 0.17, $\sqrt{(a)} = \bigcap_{\sqrt{(a)}\subset\mathfrak{p}} \mathfrak{p} = \bigcap_{\sqrt{(b)}\subset\mathfrak{p}} \mathfrak{p} = \sqrt{(b)}$.

(vi) By (i) of this exercise it is enough to consider coverings by basic open subsets, i.e. $\operatorname{Spec} A = \bigcup D_{a_i}$. By (ii) of the previous exercise, $\operatorname{Spec} A = D_1$, so $\bigcap \mathcal{Z}(a_i) = \mathcal{Z}(\bigcup a_i) = D_1 = \varnothing$. Hence $1 \in (a_i \mid i \in I)$, the ideal generated by the a_i.

In particular, $1 = \sum_{j\in J} x_j a_j$ for a *finite* subset $J \subset I$ which implies $\operatorname{Spec} A = \bigcup_{j\in J} D_{a_j}$. □

37. Remark. We can regard $\mathcal{Z}$ as a map which takes subsets of a ring A to subsets of its spectrum $\operatorname{Spec} A$. Conversely, we can assign to a given subset $X \subset \operatorname{Spec} A$ the ideal

$$\mathcal{I}(X) = \bigcap_{\mathfrak{p}\in X} \mathfrak{p} \subset A.$$

These operations are inverse in the following sense, namely

$$\mathcal{Z} \circ \mathcal{I}(X) = \bar{X} \quad \text{and} \quad \mathcal{I} \circ \mathcal{Z}(\mathfrak{a}) = \sqrt{\mathfrak{a}},$$

where $\bar{X} = \bigcap_{X\subset\mathcal{Z}(T)} \mathcal{Z}(T) = \mathcal{Z}(\bigcup_{X\subset\mathcal{Z}(T)} T)$ denotes the **closure** of X, the smallest closed subset which contains X (cf. also Section 1.1.1, in particular Proposition 1.18). Indeed, let us show that $\mathcal{Z} \circ \mathcal{I}(X) = \bar{X}$. First, if $\mathfrak{p} \in X$, then $\mathcal{I}(X) \subset \mathfrak{p}$ so that $\mathfrak{p} \in \mathcal{Z}(\mathcal{I}(X))$. Hence $X \subset \mathcal{Z}(\mathcal{I}(X))$, and since X is closed, we have also $\bar{X} \subset \mathcal{Z}(\mathcal{I}(X))$. Conversely, let $Y \subset \operatorname{Spec} A$ be any closed set containing X. Then $Y = \mathcal{Z}(\mathfrak{a})$ for an ideal $\mathfrak{a} \subset A$. If $\mathfrak{p} \in X \subset Y$, then $\mathfrak{a} \subset \mathfrak{p}$ so that $\mathfrak{a} \subset \bigcup_{\mathfrak{p}\in X} \mathfrak{p} = \mathcal{I}(X)$. Then $\mathcal{Z} \circ \mathcal{I}(X) \subset Y$; in particular, this is true for $Y = \bar{X}$.

For the second identity we note that

$$\mathcal{I} \circ \mathcal{Z}(\mathfrak{a}) = \mathcal{I}(\{\mathfrak{p} \in \operatorname{Spec} A \mid \mathfrak{a} \subset \mathfrak{p}\}) = \bigcap_{\mathfrak{a}\subset\mathfrak{p}} \mathfrak{p} = \sqrt{\mathfrak{a}}$$

by Corollary 0.17 and Exercise 0.35 (i) which implies that $\mathfrak{a} \subset \mathfrak{p}$ implies $\sqrt{\mathfrak{a}} \subset \mathfrak{p}$ (the converse being clear).

38. Exercise (Closure of a point). *Show that the closure of the point* $\mathfrak{p} \in \operatorname{Spec} A$, $\overline{\{\mathfrak{p}\}} = \bigcap_{T\subset\mathfrak{p}} \mathcal{Z}(T)$, *is given by* $\mathcal{Z}(\mathfrak{p})$. *Conclude that*

(i) $\mathfrak{p}$ *is a* closed point *(i.e.* $\overline{\{\mathfrak{p}\}} = \{\mathfrak{p}\}$*)* $\Leftrightarrow$ $\mathfrak{p}$ *is maximal*;
(ii) $\mathfrak{q} \in \overline{\{\mathfrak{p}\}} \Leftrightarrow \mathfrak{p} \subset \mathfrak{q}$.

For later use we say that $\mathfrak{q}$ *is a* **specialisation** *of* $\mathfrak{p}$. *An everywhere dense point (e.g.* (0)*), i.e.* $\overline{\{\mathfrak{p}\}} = \operatorname{Spec} A$ *is called* **generic**.

Proof. (i) and (ii) are easy consequences of the equality $\overline{\{\mathfrak{p}\}} = \mathcal{Z}(\mathfrak{p})$. The latter immediately follows from the preceeding remark. □

39. Exercise (Morphisms of rings and spectra). *Let* $\varphi : A \to B$ *be a ring morphism.*

(i) *Show that the associated map* $\varphi^a : \operatorname{Spec} B \to \operatorname{Spec} A$ *which sends* $\mathfrak{p} \in \operatorname{Spec} B$ *to* $\mathfrak{p}^c = \varphi^{-1}(\mathfrak{p}) \in \operatorname{Spec} A$ *is well-defined and* continuous *with respect to the Zariski topology, i.e. the preimage of a closed set is again closed in* $\operatorname{Spec} B$.
(ii) *Compute explicitely the map* φ^a *for the three types of prime ideals in* $\mathbb{Z}[i]$ *for the inclusion* $\varphi : \mathbb{Z} \to \mathbb{Z}[i]$.

Proof. (i) By Remark 0.27 the map φ^a is well-defined. We show that for $T \subset A$, $(\varphi^a)^{-1}(\mathcal{Z}(T)) = \mathcal{Z}(\varphi(T))$. For the inclusion $\subset$, let $\mathfrak{p} \in (\varphi^a)^{-1}(\mathcal{Z}(T))$, i.e. $T \subset \varphi^a(\mathfrak{p}) = \varphi^{-1}(\mathfrak{p})$, whence $\varphi(T) \subset \varphi(\varphi^{-1}(\mathfrak{p})) \subset \mathfrak{p}$. Therefore $\mathfrak{p} \in \mathcal{Z}(\varphi(T))$. Conversely, for the inclusion $\mathcal{Z}(\varphi(T)) \subset (\varphi^a)^{-1}(\mathcal{Z}(T))$, let $\mathfrak{p} \in \mathcal{Z}(\varphi(T))$, i.e. $\varphi(T) \subset \mathfrak{p}$. Then $T \subset \varphi^{-1}\varphi(T) \subset \varphi^{-1}(\mathfrak{p}) = \varphi^a(\mathfrak{p})$ so that $\varphi^a(\mathfrak{p}) \in \mathcal{Z}(T)$, i.e. $\mathfrak{p} \in (\varphi^a)^{-1}(\mathcal{Z}(T))$.

(ii) Obviously, $\iota^a((0)) = (0)$ and $\iota^a((1+i)) = (2)$. If $\mathfrak{p} \in \operatorname{Spec} \mathbb{Z}[i]$ is of type $(p)^e$ for $p \equiv 3 \bmod 4$, then $\iota^a(\mathfrak{p}) = (p)$. Similarly, if we are given $\mathfrak{q}$ and $\bar{\mathfrak{q}}$ induced by $p \equiv 1 \bmod 4$, then $\iota^a(\mathfrak{q}) = \iota^a(\bar{\mathfrak{q}}) = (p)$, see also Figure 0.1 below. □

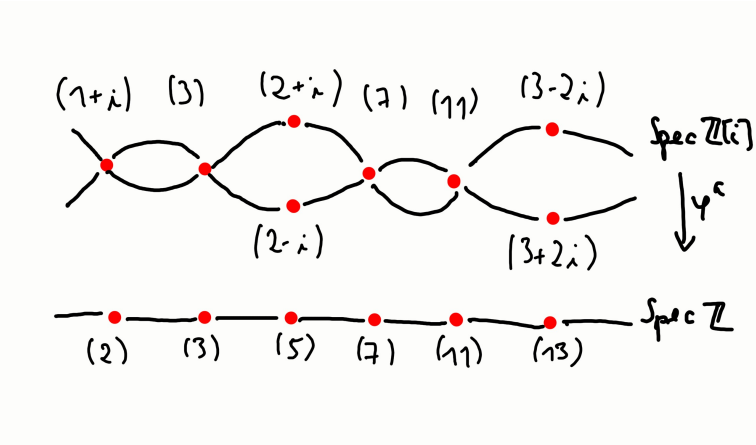

FIGURE 1. The associated morphism $\varphi^a : \operatorname{Spec} \mathbb{Z}[i] \to \operatorname{Spec} \mathbb{Z}$

0.2. **Modules.** Modules are a natural generalisation of ideals and will play an important rôle in the second half of the course.

Basic examples and properties.

40. Definition (module). An **A-module** is an Abelian group M with a multiplication map

$$A \times M \to M, \quad (a, m) \mapsto a \cdot m$$

satisfying

(i) $a \cdot (m \pm n) = a \cdot m \pm a \cdot n$;
(ii) $(a + b) \cdot m = a \cdot m + g \cdot m$;
(iii) $(ab) \cdot m = a \cdot (b \cdot m)$;
(iv) $1_A \cdot m = m$

for all a, $b \in A$ and m, $n \in M$. If no confusion arises, we simply write am for $a \cdot m$. A subset N of M is called a **submodule** if $am + bn \in N$ for all a, $b \in A$, m, $n \in N$. A **morphism between A-modules** or simply an **A-linear map** is a map satisfying $f(am + bn) = af(m) + bf(n)$ for all a, $b \in A$, m, $n \in N$. We write $\operatorname{End}(M)$ for the set of **endomorphisms**, i.e. morphisms $M \to M$. More generally, we can consider the set of linear morphisms $\operatorname{Hom}(M, N) = \{\varphi : M \to N\}$.

41. Examples.

(i) Any k-vector space is a k-module.
(ii) Any ring A is an A-module over itself, and its submodules are precisely the *ideals* of A.
(iii) Any Abelian group is a $\mathbb{Z}$-module.
(iv) If $A = k[x]$, then an A-module is a k-vector space V together with a linear map $x : V \to V$.

(v) Similar to vector spaces, $\mathrm{Hom}(M,N)$ is again an A-module if M and N are A-modules. In particular, $\mathrm{Hom}(A,M) \cong M$, for $f \in \mathrm{Hom}(A,M)$ is determined by $f(1)$. Morphisms $\psi : M' \to M$ and $\varphi : N \to N'$ induce morphisms $\Psi : \mathrm{Hom}(M,N) \to \mathrm{Hom}(M',N)$ and $\Phi : \mathrm{Hom}(M,N) \to \mathrm{Hom}(M,N')$ by $\Psi(f) = f \circ \psi$ and $\Phi(f) = \varphi \circ f$.

(vi) If A is a subring of B, then multiplication in B makes B into an A-module. A B-module gives an A-module by restricting multiplication to A.

(vii) As for vector spaces there is a natural notion of sub- and quotient module, direct sum of modules etc. For example, if $f : M \to N$ is a morphism, then $\ker f$ and $\operatorname{im} f$ are submodules of M and N respectively, while the *cokernel of* f, $\operatorname{coker} f = N/\operatorname{im} f$ is a quotient module.

42. Proposition (isomorphism theorems). We have the following natural isomorphisms.

(i) For any A-module morphism $\varphi : M \to N$, $\operatorname{im}\varphi \cong M/\ker\varphi$ as A-modules.

(ii) If $L \subset N \subset M$ are submodules, then

$$M/N \cong (M/L)/(N/L).$$

(iii) If M is a module, and L, $N \subset M$ are submodules of M, then

$$(N+L)/L \cong N/(N \cap L).$$

Proof. As in the case of vector spaces, see for instance [AtMa, Proposition 2.1]. □

43. Remark. (ii) can be interpreted as saying that if L is not contained in N, there are two ways of making sense of N/L. Either we increase N by L by taking the sum, or we decrease L until it is contained in N. Both ways give the same result.

Exact sequences. A sequence of modules $L \xrightarrow{\alpha} M \xrightarrow{\beta} N$ is called **exact** if $\operatorname{im}\alpha = \ker\beta$. A sequence of the form $0 \to L \xrightarrow{\alpha} M \xrightarrow{\beta} N \to 0$ is called a **short exact sequence** (s.e.s. for short).

44. Proposition (split exact sequences). *Let* $0 \to L \xrightarrow{\alpha} M \xrightarrow{\beta} N \to 0$ *be a s.e.s. Are equivalent*

(i) *There exists an isomorphism* $M \cong L \oplus N$ *under which* $\alpha(l) = (l,0)$ *and* $\beta(l,n) = n$*;*

(ii) *there exists a* section *of* β*, that is, a map* $\sigma : N \to M$ *such that* $\beta \circ \sigma = \mathrm{Id}_N$*;*

(iii) *there exists a* retraction *of* α*, that is, a map* $\rho : M \to L$ *such that* $\rho \circ \alpha = \mathrm{Id}_L$*.*

A sequence which admits a section is called a split sequence*.*

Proof. (i)⇒(ii) or (iii) Obvious.

(ii)⇒(i) σ is injective, for if $\sigma(n_1) = \sigma(n_2)$, then $n_1 = \beta\circ\sigma(n_1) = \beta\circ\sigma(n_2) = n_2$. Claim: $M = \alpha(L) \oplus \sigma(N)$. Indeed, let $m \in M$ and write

$$m = (m - \sigma(\beta(m))) + \sigma(\beta(m)).$$

The second term is in $\sigma(N)$ by design. Further, the first term is in $\ker\beta = \operatorname{im}\alpha$ which shows that $M = \alpha(L) + s(N)$. To show that the sum is direct, assume that $\sigma(n) \in \operatorname{im}\alpha = \ker\beta$. Then $n = \beta(\sigma(n)) = 0$, whence $\alpha(L) \cap \sigma(N) = \{0\}$.

(iii)⇒(i) Similar to the previous step. □

45. Remark.

(i) Note that for k-vector spaces, any s.e.s. is split. Put differently, knowing a subspace L of M and the corresponding quotient M/L determines M completely. This is false for modules. In fact, the so-called *extension problem for modules* asks precisely which A-modules M can occur in an exact sequence $0 \to L \to M \to N \to 0$ given L and N. Of course, the direct sum $L \oplus N$ is a trivial extension, but is usually not unique.

(ii) A s.e.s. is in general not split. In fact, a module P is called **projective** if for any exact sequence $M \to P \to 0$ there exists a section $\sigma : P \to M$.

Still, given a submodule M_1 of M such that $\alpha(L) \cap M_1 = \alpha(L) \cap M$ and $\beta(M_1) = \beta(M)$ we can conclude $M_1 = M$. More generally, we have the

46. Lemma. *If $0 \to L \xrightarrow{\alpha} M \xrightarrow{\beta} N \to 0$ is a short exact sequence, and $M_1 \subset M_2$ two submodules of M, then*

$$\alpha(L) \cap M_1 = \alpha(L) \cap M_2 \text{ and } \beta(M_1) = \beta(M_2) \Rightarrow M_1 = M_2.$$

Proof. Indeed, if $m \in M_2$, then $\beta(m) \in \beta(M_2) = \beta(M_1)$. Hence there is $n \in M_1 \subset M_2$ such that $\beta(n) = \beta(m)$, i.e. $m - n \in M_2 \cap \ker \beta = M_2 \cap \alpha(L) = M_1 \cap \alpha(L)$. It follows that $m \in M_1$. □

S.e.s. often arise from long exact sequences:

47. Exercise (splitting and glueing of exact sequences).

(i) *(Splitting) If*

$$M_1 \xrightarrow{\alpha_1} M_2 \xrightarrow{\alpha_2} M_3 \xrightarrow{\alpha_3} M_4$$

is an exact sequence of A-modules, then the sequences

$$M_1 \xrightarrow{\alpha_1} M_2 \longrightarrow \operatorname{im}\alpha_2 = \ker\alpha_3 \longrightarrow 0$$

and

$$0 \longrightarrow \ker\alpha_3 = \operatorname{im}\alpha_2 \longrightarrow M_3 \xrightarrow{\alpha_3} M_4\ ,$$

where $\ker\alpha \to M_3$ is the inclusion map, are also exact.

(ii) *(Glueing) Conversely, if we have exact sequences*

$$M_1 \xrightarrow{\alpha_1} M_2 \xrightarrow{\alpha_2} N \longrightarrow 0$$

and

$$0 \longrightarrow N \longrightarrow M_3 \xrightarrow{\alpha_3} M_4\ ,$$

where $N \to M_3$ is the inclusion map, then the induced sequence

$$M_1 \xrightarrow{\alpha_1} M_2 \xrightarrow{\alpha_2} M_3 \xrightarrow{\alpha_3} M_4$$

is also exact.

(iii) *Conclude that any exact sequence*

$$0 \longrightarrow M_1 \xrightarrow{\alpha_1} M_2 \xrightarrow{\alpha_2} \dots \qquad M_n \xrightarrow{\alpha_{n-1}} 0$$

can be split up into s.e.s.

$$0 \longrightarrow \ker\alpha_i \longrightarrow M_i \xrightarrow{\alpha_i} \operatorname{im}\alpha_i \longrightarrow 0\ .$$

Proof. By direct verification, see also [Ga, Lemma 4.4 and Remark 4.5] for a proof. □

There are several natural exact sequences which can be built from morphisms $\alpha : M \to N$ of A-modules. The subsequent lemma is immediate.

48. Corollary (exact sequence of a morphism). *Let $\alpha : M \to N$ be a morphism of A-modules. Then there are s.e.s.*

$$0 \longrightarrow \ker\alpha \longrightarrow M \xrightarrow{\alpha} \operatorname{im}\alpha \longrightarrow 0$$

and

$$0 \longrightarrow \operatorname{im}\alpha \longrightarrow N \longrightarrow \operatorname{coker}\alpha \longrightarrow 0\ .$$

In particular, glueing yields

$$0 \longrightarrow \ker\alpha \longrightarrow M \xrightarrow{\alpha} N \longrightarrow \operatorname{coker}\alpha \longrightarrow 0\ .$$

49. Lemma (snake lemma). *Let*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & L & \xrightarrow{\alpha} & M & \xrightarrow{\beta} & N & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle h} & & \\ 0 & \longrightarrow & L' & \xrightarrow{\alpha'} & M' & \xrightarrow{\beta'} & N' & \longrightarrow & 0 \end{array}$$

be a commutative diagramm of A-modules. Then there exists a sequence

$$0 \longrightarrow \ker f \xrightarrow{\bar\alpha} \ker g \xrightarrow{\bar\beta} \ker h \xrightarrow{d}$$

$$\operatorname{coker} f \xrightarrow{\bar\alpha'} \operatorname{coker} g \xrightarrow{\bar\beta'} \operatorname{coker} h \longrightarrow 0,$$

where $\bar\alpha$ and $\bar\beta$ are restrictions of α and β and $\bar\alpha'$ and $\bar\beta'$ are induced by α' and β'. For instance, $\bar\alpha'([l']) = [\alpha'(l')]$ etc.

Proof. The proof is a routine exercise in diagram-chasing. We just give the definition of the boundary morphism $d : \ker h \to \operatorname{coker} f$. For a complete proof as well as an explanation of the name "snake lemma", see [Ga, Lemma 4.7].

If $n \in \ker h \subset N$, then for $m \in M$ with $\beta(m) = n$ (β is onto), $\beta' \circ g(m) = h \circ \beta(m) = 0$, hence $g(m) \in \ker\beta' = \operatorname{im}\alpha'$. Hence there exists $l' \in L'$ with $\alpha'(l') = g(m)$, and we let $d(n) = [l']$, where $[\cdot]$ denotes the equivalence class in $\operatorname{coker} f$. □

Generating families. Given $m_1, \dots, m_r \in M$ we can consider the submodule **generated** by these elements, namely

$$(m_1, \dots, m_r) = \sum Am_i = \{\sum a_i m_i \in M \mid a_i \in A\} \subset M$$

More generally, let $\{m_\lambda\}_{\lambda\in\Lambda}$ be any set of elements in M. We can define an A-module morphism

$$\varphi : \bigoplus_{\lambda\in\Lambda} A \to M, \quad \oplus_{\lambda\in\Lambda} a_\lambda \mapsto \sum_{\lambda\in\Lambda} a_\lambda m_\lambda.$$

Note that the sum is finite since only a finite number of the $a_\lambda \neq 0$ by definition of the direct sum of modules.

50. Definition (family of generators and free modules). $\{m_\lambda\}$ is a **family of generators** if φ is surjective, i.e. we have $\bigoplus_\lambda A \xrightarrow{\varphi} M \to 0$. If the indexing set Λ is finite, then M is **finitely generated** or simply **finite**. Finally, if φ is an isomorphism, $\{m_\lambda\}_{\lambda\in\Lambda}$ is a **basis** and M is **free**.

51. Examples (free modules and their submodules and quotients).

(i) $A[x]$ is a free A-module with infinite set of generators $(x^k)_{k\geqslant 0}$. As an $A[x]$-module, it is of course free and finitely generated.

(ii) If $\mathfrak{a}$ is a nontrivial ideal of A, then $A/\mathfrak{a}$ is never a free A-module, for any map $\varphi : \bigoplus_\lambda A \to A/\mathfrak{a}$, $(a_\lambda) \mapsto \sum a_\lambda m_\lambda$ has nontrivial kernel since $\varphi(a, 0, \ldots) = 0$ if $a \in \mathfrak{a}$. However, A is obviously free as an A-module. It follows that in general, the *quotient of a free module is not free again.*

(iii) If A is an integral domain, then a nontrivial ideal $\mathfrak{a}$ is free $\Leftrightarrow$ $\mathfrak{a}$ is principal. In particular, *the submodule of a free module is usually not free again.* Indeed, if $\mathfrak{a} = (a)$, then $\varphi : A \to \mathfrak{a}$, $x \mapsto xa$ is the desired isomorphism. Conversely, assume that $\mathfrak{a}$ is free so that we have an isomorphism $\varphi : \bigoplus_\lambda A \to \mathfrak{a}$ defined by a set of generators. If there were more than one generator, say m_1 and m_2, then $\varphi(-m_2, m_1, \ldots) = -m_2m_1 + m_1m_2 = 0$. Hence there can be only one generator, that is, the ideal is principal.

Summarising, if we have a s.e.s. $0 \to L \to \bigoplus_\lambda A \to N \to 0$, L nor N need to be free in general.

52. Remark. In the case of a vector space, a basis always exists, either by taking a generating set of linearly independent vectors or an irredundant generating set. This, however, fails in the case of modules. Indeed, $\mathfrak{m} = (x, y)$ in $A = k[x, y]$ is generated by two linearly independent x and y, but it is not free (cf. (iii) of the previous example). On the other hand, for $M = A = k[x]$, we have $M = (x, 1-x)$. Here, the generators form an irredundant set of the free module M, but obviously not a basis.

53. Examples (finitely generated modules and their submodules and quotients).

(i) Almost by definition, a finitely generated A-module is of the form $A^n/\ker\phi$. Every ideal of the form $\mathfrak{a} = (m_1, \ldots, m_n)$ in A is finitely generated as an A-module.

(ii) If $m_1, \ldots, m_n$ is a generating set for M, then so is $\bar{m}_1, \ldots, \bar{m}_n$ for M/N, where N is some submodule of M. In particular, *quotients of finitely generated modules* are again finitely generated.

(iii) By definition, a ring A which is not *Noetherian* admits an ideal which is not finitely generated as an A-module (see Section 0.0.3). Since non-Noetherian rings exist (for instance $k[x_1, x_2, \ldots]$), *the submodule of a finitely generated module is in general not finitely generated again.*

Summarising, if we have a s.e.s. $0 \to L \to \bigoplus_{i=1}^n A/\ker\phi \to N \to 0$, N is finitely generated, but not L in general.

54. Exercise (finitely generated submodules). *Let M be a finitely generated A-module and $\phi : M \to A^n$ a surjective morphism of A-modules $\Rightarrow$ $\ker\phi$ is finitely generated.*

Hint: Let $e_1, \ldots, e_n$ be a basis of A^n and choose $u_i \in M$ such that $\phi(u_i) = e_i$ for $i = 1, \ldots, n$. Show that $M = \ker\phi \oplus \langle u_1, \ldots, u_n\rangle$ and conclude.

Proof. The map $e_i \mapsto u_i$ defines a section $s : A^n \to M$ of the s.e.s. $0 \to \ker\phi \to M \xrightarrow{\phi} A^n \to 0$. By Proposition 0.44, $M = \ker\phi \oplus s(A^n)$. Next let $m_1, \ldots, m_r$ be

a generating system of M. Since the sum is direct, $m_i = k_i \oplus u_i$ with $k_i \in \ker \phi$. Now if $k \in \ker \phi$, then $k = \sum a_i m_i = \sum a_i k_i + \sum a_i u_i$. Again, by directness of the sum, $\sum a_i u_i = 0$ so that k_i, $i = 1, \ldots, r$, generate $\ker \phi$. □

55. Exercise (Koszul complex of a pair). *Let A be a UFD, and x, $y \in A$ be two elements without common factor except for units. Write $\mathfrak{a} = (x, y) \subset A$ for the ideal generated by x and y.*

(i) *Show that the sequence*

$$0 \longrightarrow A \xrightarrow{\alpha} A^2 \xrightarrow{\beta} \mathfrak{a} \longrightarrow 0,$$

with $\alpha(a) = (-ay, ax)$ and $\beta(a, b) = ax + by$ is exact.

(ii) *Find an example where $\mathfrak{a} \neq A$. Show that in this case, $\mathfrak{a}$ needs at least two generators, and is not a free module.*

Proof. (i) Surjectivity of β is clear by definition of $\mathfrak{a} = (x, y)$, and so is injectivity of α. It remains to show that $\operatorname{im} \alpha = \ker \beta$. The inclusion $\subset$ is obvious. For the inclusion $\supset$, let $(r, s) \in \ker \beta$, that is $rx = -sy$. Since x has no common factor with y, $x \mid s$. Similarly, $y \mid r$. It follows that $r = cy$, $s = dx$ and $c = -d$. hence $(r, s) = (cy, -cx) = \alpha(-c)$.

(ii) An example is provided by $A = k[x, y]$. Now assume that $\mathfrak{a} = (c)$ for some $c \in A$. Then $c \mid \beta(1, 0) = x$ and $\beta(0, 1) = y$. Since x and y have no common factor except units, c must be a unit, whence $\mathfrak{a} = A$. If $\mathfrak{a}$ were free, one could find two linearly independent generators m_i without common factors. However, the map $\phi(a, b) = am_1 + bm_2$ necessarily has a kernel as (i) shows. □

Cayley-Hamilton theorem and corollaries. If M is an A-module we can view $a \in A$ as a morphism $M \to M$ sending m to am. In this way we get a map $A \to \operatorname{End}(M)$, a *representation of the ring A*; if this map is injective, the module M is said to be a *faithful A-module*. If $\varphi \in \operatorname{End}(M)$ we write $A[\varphi]$ for the subring of $\operatorname{End}(M)$ which is generated by φ and the image of A in $\operatorname{End}(M)$. In the sequel, we let for an ideal $\mathfrak{a} \subset A$

$$\mathfrak{a}M = \{ \sum_{\text{finite}} a_i m_i \mid a_i \in \mathfrak{a},\ m_i \in M \}.$$

56. Proposition (Cayley-Hamilton). *Let M be a finite A-module, generated by n elements, and $\varphi : M \to M$ a homomorphism. Suppose that $\mathfrak{a}$ is an ideal of A such that $\varphi(M) \subset \mathfrak{a}M$. Then φ satisfies a relation of the form*

$$\varphi^n + a_1 \varphi^{n-1} + \ldots + a_{n-1}\varphi + a_n = 0$$

in $\operatorname{End}(M)$, where $a_i \in \mathfrak{a}^i$ for $i = 1, \ldots, n$.

Proof. Let $m_1, \ldots, m_n$ be a set of generators of M. Since $\varphi(m_i) \in \mathfrak{a}M$ we can write

$$\varphi(m_i) = \sum_j a_{ij} m_j \quad \text{with } a_{ij} \in \mathfrak{a}.$$

In terms of the subring $A[\varphi]$ of $\operatorname{End}(M)$, we can rewrite this as follows. First,

$$\sum_j (\delta_{ij}\varphi - a_{ij}) m_j = 0$$

(with δ_{ij} the Kronecker symbol). Let $\Delta := (\delta_{ij}\varphi - a_{ij})_{ij}$ and consider Δ as an $n \times n$-matrix with entries in $A[\varphi]$. The above equation then reads $\sum_j \Delta_{ij} m_j = 0$, and multiplying by $(\operatorname{adj}\Delta)_{ki}$ and summing over i (where adj denotes the adjugate matrix) yields $(\det\Delta)m_k = 0$ for all k (recall that $\det\Delta \in A[\varphi]$!). Hence $\det\Delta = 0$ in $A[\varphi]$, and expanding out the determinant yields the result (see also [Re, Section 2.6] for an extended version of this proof). □

57. Corollary. *If M is a finite module and $M = \mathfrak{a}M$, then there exists an element $x \in A$ such that $x \equiv 1 \bmod \mathfrak{a}$ and $xM = 0$.*

Proof. Apply the previous theorem to $\varphi = \mathrm{Id}_M$. Since $\mathrm{Id}_M^k = \mathrm{Id}_M$ the identity reads $(1+b)\,\mathrm{Id}_M = 0$ for $b = \sum a_i \in \mathfrak{a}$. Hence $x = 1 + b$ is the desired element. □

58. Remark. The submodule

$$M_{\mathrm{tor}} = \{m \in M \mid \text{there exists } 0 \neq a \in A \text{ such that } am = 0\}$$

is called the **torsion module** of M. If $M_{\mathrm{tor}} = 0$, then M is called **torsionfree**. The previous corollary then asserts that if $\mathfrak{a}M = M$ for some proper ideal $\mathfrak{a}$ of A, then M is **pure torsion**, i.e. $M = M_{\mathrm{tor}}$.

59. Corollary. *If M is a finitely generated A-module, and $\varphi : M \to M$ is an A-linear map which is onto, then φ is injective, i.e. φ is an automorphism of M.*

Proof. Let $m \in M$ be such that $\varphi(m) = 0$. We need to show that $m = 0$. Let us view M as an $A[x]$-module via $x \cdot m = \varphi(m)$ (cf. 0.41 (iv)). By assumption, $\mathfrak{a}M = M$ for $\mathfrak{a} = (x) \subset A[x]$. Hence there exists $a = 1 + bx \in A[x]$ such that $aM = 0$. In particular, $0 = am = m + b\varphi(m) = m$. □

60. Corollary (Nakayama's lemma). *Let $(A, \mathfrak{m})$ be a local ring, and M a finite A-module. Then $M = \mathfrak{m}M$ implies that $M = 0$. (For instance, if A is a field, then $\mathfrak{m} = (0)$ and the implication holds trivially.) In particular, if $M \neq 0$, then $M/\mathfrak{m}M$ is a non-trivial vector space over $k = A/\mathfrak{m}$.*

Proof. By the previous corollary there exists $x \equiv 1 \bmod \mathfrak{m}$ such that $xM = 0$. By 0.11, x must be a unit, whence $x^{-1}xM = M = 0$. □

This can be generalised as follows ($N = 0$ in the following lemma gives Nakayama's version).

61. Corollary. *Let $(A, \mathfrak{m})$ be a local ring, M an A-module, and $N \subset M$ a submodule such that M/N is finite. If $M = N + \mathfrak{m}M$, then $N = M$. In particular, if M is finite over A, and if $m_1, \ldots, m_n$ are elements whose images in $M/\mathfrak{m}M$ span the vector space, then $m_1, \ldots, m_n$ generate M.*

Proof. By assumption, $\mathfrak{m}(M/N) = \mathfrak{m}M/(\mathfrak{m}M \cap N) = (\mathfrak{m}M + N)/N = M/N$, so that by Nakayama's lemma, $M/N = 0$, hence $M = N$. For the second assertion, let $N = (m_1, \ldots, m_n)$. The composition $N \hookrightarrow M \twoheadrightarrow M/\mathfrak{m}M$ maps N onto $M/\mathfrak{m}M$ by design, so that $N + \mathfrak{m}M = M$. Now apply the previous corollary. □

62. Proposition and Definition (rank of a module). *Let M be a finitely generated A-module and let $\varphi : M \to M$ be a surjective morphism. Then φ is an isomorphism. In partcular, if M is a free module with isomorphim $M \cong A^n$, then n does not depend on the isomorphism. It is called the* **rank** *of M.*

Proof. By setting $x \cdot m := \varphi(m)$ we can see the pair (M, φ) in a natural way as an $A[x]$-module, cf. also Example 0.41 (iv). Since φ is surjective, $(x)M = M$ so that by Corollary 0.57, there exists $f = \sum_{i=1}^{n} a_i x^i \in (x)$ with $f \cdot m = \sum a_i \varphi^i(m) = m$. It follows that $\varphi(m) = 0$ implies $m = 0$, whence injectivity. □

63. Remark. Unlike for vector space, injectivity is not enough to conclude surjectivity as the map $m \in \mathbb{Z} \mapsto 2m \in \mathbb{Z}$ shows.

Tensor products. As for vector spaces we can form the tensor product of two A-modules. More precisely, we have the following.

64. Proposition and Definition (tensor product). *Let N and M be A-modules. Then there exists a pair (T, τ) consisting of an A-module T and an A-module T and an A-bilinear mapping $\tau : M \times N \to T$, with the following universal property: Given any A-module L and any morphism $\alpha : M \times N \to L$, there exists a unique morphism $\tilde{\alpha} : T \to L$ such that $\alpha = \tilde{\alpha} \circ \tau$. Moreover, if (T, τ) and (T', τ') are two such pairs then there exists a unique isomorphism $j : T \to T'$ such that $j \circ \tau = \tau'$. T is called the* **tensor product** *and is denoted by $M \otimes_A N$ or simply $M \otimes N$.*

Proof.

Step 1. *Uniqueness.* Note that for $(L, \alpha) = (T, \tau)$, uniqueness of the induced morphism $T \to L = T$ implies that $\tilde{\tau} = \mathrm{Id}_T$. Replacing (L, α) by (T', τ') we get a unique map $\tilde{\tau}' : T \to T'$. Interchanging the rôles of (T, τ) and (T', τ') gives a map $\tilde{\tau} : T' \to T$ inverse to $\tilde{\tau}'$.

Step 2. *Existence.* Let $\hat{T}$ denote the free A-module generated by $M \times N$, i.e. T consists of formal linear combinations $\sum_{i=1}^{n} a_i(m_i, n_i)$. Let R be the submodule generated by all elements of $\hat{T}$ of the form

$$\begin{gathered}(m + m', n) - (m, n) - (m', n)\\ (m, n + n') - (m, n) - (m, n')\\ (am, n) - a(m, n)\\ (m, an) - a(m, n).\end{gathered}$$

Define $T := \hat{T}/R$. Denote the equivalence class of (m, n) by $m \otimes n$. Then $\tau : M \times N \to T$, $(m, n) \mapsto m \otimes n$ yields the desired map.

□

65. Remark.

(i) $M \otimes N$ is *generated* by $\{m \otimes n \mid m \in M,\, n \in N\}$. In particular, any element in $M \otimes N$ is of the form $\sum_{i=1}^{n} m_i \otimes n_i$. If M and N are finitely generated by $\{m_i\}_{i \in I}$ and $\{n_j\}_{j \in J}$ respectively, then so is $M \otimes N$ by $\{m_i \otimes n_j\}_{(i,j) \in I \times J}$.

(ii) Note that the expression $m \otimes n$ is ambigous as long as we do not specify the tensor product to which it belongs. For instance, let $A = M = \mathbb{Z}$, $N = \mathbb{Z}/2\mathbb{Z}$ and $M' = 2\mathbb{Z}$. If 1 denotes the nonzero element in N, $2 \otimes 1 = 1 \otimes 2 = 0$ in $M \otimes N$, but $\neq 0$ in $M' \otimes N$.

(iii) We can form the tensor product of several factors, that is, we have a multilinear map $M_1 \times \ldots \times M_r \to M_1 \otimes \ldots \otimes M_r$ etc.

(iv) If $\alpha : M \to N$, $\beta : M' \to N'$ are morphisms we can from the **tensor product of morphisms** $\alpha \otimes \beta : M \otimes M' \to N \otimes N'$ by taking the induced map from $M \times M' \to N \otimes N'$, $(m, m') \mapsto \alpha(m) \otimes \beta(m')$. In particular, $\alpha \otimes \beta(m \otimes m') = \alpha(m) \otimes \beta(m')$.

66. Lemma. *Let $x_i \in M$, $y_i \in N$ be such that $\sum x_i \otimes y_i = 0$ in $M \otimes N$. Then there exists finitely generated submodules M_0 and N_0 of M and N respectively such that $\sum x_i \otimes y_i = 0$ in $M_0 \otimes N_0$. (For an application of this result, see Proposition 0.74 below.)*

Proof. If we write $M \otimes N = \langle M \times N \rangle / R$ as in Proposition 0.64, then $\sum x_i \otimes y_i = 0$ in $M \otimes N$ implies $\sum (x_i, y_i) \in R$. Let M_0 resp. N_0 be the submodule of M resp. N generated by the x_i resp. y_i occuring in the sum. Then $\sum (x_i, y_i) \in R \cap \langle M_0 \times N_0 \rangle$, i.e. $\sum x_i \otimes y_i = 0$ in $M_0 \otimes N_0$. □

67. Proposition. *Let L, M and N be A-modules. Then there exists unique isomorphisms such that*

(i) $M \otimes N \to N \otimes M$, $x \otimes y \mapsto y \otimes x$;

(ii) $(M \otimes N) \otimes L \to M \otimes (N \otimes L) \to M \otimes N \otimes L$, $(x \otimes y) \otimes z \mapsto x \otimes (y \otimes z)$ and $x \otimes (y \otimes z) \mapsto x \otimes y \otimes z$;

(iii) $(M \oplus N) \otimes L \to (M \otimes L) \oplus (N \otimes L)$, $(x, y) \otimes z \mapsto (x \otimes z, y \otimes z)$;

(iv) $A \otimes M \to M$, $a \otimes x \mapsto ax$.

*Furthermore, let B be a ring, $\tilde{N}$ a B-module, and $\tilde{L}$ an (A, B)-**bimodule**, i.e. $\tilde{L}$ is a simultaneous A- and a B-module such that $a(xb) = (ax)b$ for all $a \in A$, $b \in B$ and $x \in L$. Then $M \otimes_A \tilde{L}$ and $L \otimes_B \tilde{N}$ are natural (A, B)-bimodules, and we have*

$$(M \otimes_A \tilde{L}) \otimes_B \tilde{N} \cong M \otimes_A (\tilde{L} \otimes_B \tilde{N})$$

as an (A, B)-bimodule.

Proof. This is a routine application of the universal property of tensor products. For instance, consider the map $\alpha : M \times N \to N \otimes M$ defined by $\alpha(x, y) = y \otimes x$ which gives rise to a map $\tilde{\alpha} : M \otimes N \to N \otimes M$ satisfying $\tilde{\alpha}(x \otimes y) = \tilde{\alpha}(\tau(x, y)) = \alpha(x, y) = y \otimes x$. Similarly, the map $\beta : N \times M \to M \otimes N$, $\beta(y, x) = x \otimes y$ gives rise to a linear map $\tilde{\beta} : N \otimes M \to M \otimes N$. Clearly, $\tilde{\beta} \circ \tilde{\alpha} = \mathrm{Id}_{M \otimes N}$ and $\tilde{\alpha} \circ \tilde{\beta} = \mathrm{Id}_{N \otimes M}$. As another example, consider the associative law (ii). Fix $l \in L$ and consider the map $\varphi_l : M \times N \to M \otimes N \otimes L$ given by $\varphi(m, n) = m \otimes n \otimes l$. This is bilinear in m and n and therefore factorise via $\hat{\varphi}_l : M \otimes N \to M \otimes N \otimes L$. Next we define a map $\Phi : (M \otimes N) \times L \to M \otimes N \otimes L$ via $\Phi(v, l) = \hat{\varphi}_l(v)$. Here, $M \otimes N \otimes L$ is defined as in Remark 0.65 (iii). This is bilinear in v and l and thus factorises via $\hat{\Phi} : (M \otimes N) \otimes L \to M \otimes N \otimes L$. This is the desired isomorphism for $\hat{\Phi}(m \otimes n \otimes l) = \Phi(m \otimes n, l) = \hat{\varphi}_l(m \otimes n) = m \otimes n \otimes l$ etc. For the (A, B)-bimodule isomorphism, see http://math.stackexchange.com/questions/878660/atiyah-macdonald-exercise-2-15. □

68. Remark. If we tried to define the map $f : M \otimes N \to N \otimes M$ directly via $f(m \otimes n) = n \otimes m$ we would face the problem to show that this is well-defined – $\{m \otimes n \mid m \in M,\, n \in N\}$ is merely a generating system. This is the reason why we invoke the universal property.

Another way of looking at the tensor product is to fix an A-module M and to put $T_M(L) = M \otimes_A L$ for any other A-module L. Further, if $\alpha : L \to N$ is an A-linear map we let $T_M(\alpha) = \alpha \otimes \mathrm{Id}_M : L \otimes_A M = T_M(L) \to N \otimes_A M = T_M(N)$. In particular, we have $T_M(\alpha \circ \beta) = T_M(\alpha) \circ T_M(\beta)$. In the language of abstract nonsense (that is, category theory), this means that T_M is a *covariant functor* (see Appendix A for the basic notions of category theory). In algebraic geometry, and more generally, in *homological algebra*, it is a natural question to ask whether such a functor is *exact*, i.e. whether or not it preserves exact sequences.

69. Proposition (T_M is right-exact). *Let M be an A-module. If*

$$N' \xrightarrow{\alpha} N \xrightarrow{\beta} N'' \longrightarrow 0\ .$$

is an exact sequence of A-modules, then so is

$$T_M(N') \xrightarrow{T_M(\alpha)} T_M(N) \xrightarrow{T_M(\beta)} N'' \longrightarrow 0\ .$$

One also says that T_M is **right-exact**.

Proof. This follows from a straightforward, if tedious computation, see [Ga, Proposition 5.22]. □

Recall that $\mathfrak{a}M$ denotes the submodule $\{\sum_{\text{finite}} a_i m_i \mid a_i \in \mathfrak{a}\}$ of M (cf. also the second assertion in Nakayama's lemma 0.60).

70. Exercise (quotient modules as tensor products). *Let $\mathfrak{a} \subset A$ be an ideal, and M an A-module* $\Rightarrow$

$$(A/\mathfrak{a}) \otimes_A M \cong M/\mathfrak{a}M.$$

Proof. The map $A/\mathfrak{a} \times M \to M/\mathfrak{a}$ given by $(\bar{a}, m) \mapsto \overline{am}$ (where the bars denote the respective equivalence classes in $A/\mathfrak{a}$ and $M/\mathfrak{a}M$ respectively) is bilinear, whence induces a map $\varphi : A/\mathfrak{a} \otimes_A M \to M/\mathfrak{a}M$. On the other hand, the kernel of the A-linear map $M \to A/\mathfrak{a} \otimes M$, $m \mapsto \bar{1} \otimes m$ clearly contains $\mathfrak{a}M$. Therefore it descends to a map $\psi : M/\mathfrak{a}M \to A/\mathfrak{a} \otimes_A M$ sending $\bar{m}$ to $\bar{1} \otimes \bar{m}$. Since ψ and φ are inverse to each other, we have the desired isomorphism. □

71. Remark. If M is *flat* (see Definition 0.74 below), we can argue as follows. By 0.69 we have an exact sequence $\mathfrak{a} \otimes_A M \to A \otimes_A M \to (A/\mathfrak{a}) \otimes_A M \to 0$. By (iv) of 0.67, $A \otimes_A M \cong M$, and under this isomorphism, $\mathfrak{a} \otimes_A M$ is identified with $\mathfrak{a}M$, Indeed, since the inclusion $\mathfrak{a} \subset A$ is injective, then so is the induced map $\mathfrak{a} \otimes_A M \to A \otimes_A M$. Hence $M/\mathfrak{a}M \cong (A/\mathfrak{a}) \otimes_A M$.

72. Exercise (trivial tensor product). *Let $(A, \mathfrak{m})$ be a local ring with residue field $k = A/\mathfrak{m}$, and let M and N be finitely generated A-modules. Prove that*

(i) *$M_k := M \otimes_A k$ has a natural k vector space structure which makes M_k isomorphic with $M/\mathfrak{m}M$ (cf. also Exercise 0.70);*
(ii) *$(M \otimes_A N)_k \cong M_k \otimes_k N_k$ as k-vector spaces;*

(iii) *if* $M \otimes_A N = 0$*, then* $M = 0$ *or* $N = 0$*.*

Hint for (ii): Apply Nakayama's lemma.

Proof. (i) We only define the scalar multiplication: For $x \in k$ and $m \otimes y \in M \otimes_A k$, define $x \cdot m \otimes y := m \otimes xy$. To construct an isomorphism with $M/\mathfrak{m}$, consider the A-bilinear map $M \times k \to M/\mathfrak{m}$ defined by $(m, \bar{a}) \mapsto \overline{am}$, where $\bar{a} \in k = A/\mathfrak{m}$ denotes the euqivalence class in k and $\overline{am}$ the equivalence class in $M/\mathfrak{m}$. This induces a map $\varphi : M \otimes_A k \to M/\mathfrak{m}$ which is in fact k-linear for the k-vector space structure defined above. Indeed, $\varphi(\bar{b} \cdot m \otimes \bar{a}) = \varphi(m \otimes \overline{y \cdot x}) = \overline{bam} = \bar{b} \cdot \overline{am}$. On the other hand, we define a map $\psi : M/\mathfrak{m} \to M \otimes_A k$ by $\psi(\bar{m}) = m \otimes \bar{1}$. This is well-defined for if $am \in \mathfrak{m}M$, then $am \otimes \bar{1} = m \otimes a\bar{1} = m \otimes \bar{a} = 0$, for $a \in \mathfrak{m}$.

(ii) By Exercise 0.70 we have to show that $M \otimes_A N/\mathfrak{m}(M \otimes_A N) \cong M/\mathfrak{m}M \otimes_k N/\mathfrak{m}N$. As in (i) we can construct a k-linear map $\psi : M/\mathfrak{m}M \otimes_k N/\mathfrak{m}N \to M \otimes_A N/\mathfrak{m}(M \otimes_A N)$ sending $\bar{m} \otimes \bar{n}$ to $\overline{m \otimes n}$, as well as *an A-linear* map $\varphi : M \otimes_A N/\mathfrak{m}(M \otimes_A N) \to M/\mathfrak{m}M \otimes_k N/\mathfrak{m}N$ sending $\overline{m \otimes n}$ to $\bar{m} \otimes \bar{n}$. It remains to see that φ is k-linear. So let $\bar{a} \in k$. Then $\bar{a} \cdot \overline{m \otimes n} = \overline{a \cdot m \otimes n}$ is sent to $\overline{am} \otimes \bar{n} = \bar{m} \otimes \overline{an} = \bar{a} \cdot \bar{m} \otimes \bar{n}$.

(iii) By assumption, $0 = (M \otimes_A N)_k = M_k \otimes_k N_k$ which implies either $M_k = 0$ or $N_k = 0$ for M_k and N_k are vector spaces, and the dimension of the product is the product of the dimensions. Since $M_k \cong M/\mathfrak{m}M$ and $N_k \cong N/\mathfrak{m}N$, Nakayama's lemma implies $M = 0$ or $N = 0$. □

73. Example. Take $A = \mathbb{Z}$ and consider the exact sequence $0 \to \mathbb{Z} \xrightarrow{2\cdot} \mathbb{Z}$. If we tensor with $M = \mathbb{Z}/2\mathbb{Z}$, then $0 \to \mathbb{Z} \otimes_{\mathbb{Z}} M \to \mathbb{Z} \otimes_{\mathbb{Z}} M$ is *not* exact, since for any $x \otimes m \in \mathbb{Z} \otimes_{\mathbb{Z}} M$, $2 \otimes \mathrm{Id}(x \otimes m) = 2x \otimes m = x \otimes 2m = 0$. Hence $2 \otimes \mathrm{Id}$ is the zero map, while $\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \neq 0$.

74. Proposition and Definition (flat modules). Are equivalent for an A-module M:

(i) M *is* **flat***, that is, T_M takes exact sequences to exact sequences: If*

$$0 \longrightarrow N' \xrightarrow{\alpha} N \xrightarrow{\beta} N'' \longrightarrow 0$$

is an exact sequence of A-modules, then so is

$$0 \longrightarrow T_M(N') \xrightarrow{T_M(\alpha)} T_M(N) \xrightarrow{T_M(\beta)} T_M(N'') \longrightarrow 0\ ;$$

(ii) *If*

$$N' \xrightarrow{\alpha} N \xrightarrow{\beta} N''$$

is an exact sequence of A-modules, then so is

$$T_M(N') \xrightarrow{T_M(\alpha)} T_M(N) \xrightarrow{T_M(\beta)} T_M(N'')\ ;$$

(iii) *if $N' \to N \to N''$ is exact, then so is $T_M(N') \to T_M(N) \to T_M(N'')$;*
(iv) *if $\alpha : N' \to N$ is injective, then so is $T_M(\alpha) = \alpha \otimes \mathrm{Id}$.*
(v) *if N and N' are finitely generated, and $\alpha : N' \to N$ is injective, then $T_M(\alpha) = \alpha \otimes \mathrm{Id}$ is injective.*

Proof. (i)⇔(ii) This follows directly from splitting and glueing of the exact sequence

$$0 \longrightarrow \ker \alpha \xrightarrow{\iota} N' \xrightarrow{\alpha} N \xrightarrow{\beta} N'' \xrightarrow{\pi} \operatorname{coker} \beta \longrightarrow 0\ ,$$

cf. Exercise 0.47.

(iii)⇔(iv) Follows directly from Proposition 0.69.

(iv)⇒(iii) Obvious.

(iv)⇒(iii) Let $\alpha : N' \to N$ be injective. Let $u = \sum x_i \otimes y_i \in \ker(\alpha \otimes 1)$, that is, $\sum \alpha(x_i) \otimes y_i = 0$ in $N \otimes M$. Let N_0' be module generated by the (finitely many) x_i. By Lemma 0.66 there exists a finitely generated submodule N_0 of N which contains $\alpha(N_0')$ and such that $\sum \alpha(x_i) \otimes y_i = 0$ in $N_0 \otimes M$. It follows that T_M of the restriction $\alpha_0 : N_0' \to N_0$ maps $\sum x_i \otimes y_i \in N_0' \otimes M$ to $0 \in N_0 \otimes M$. Since $T_M(\alpha_0)$ is injective by assumption, $\sum x_i \otimes y_i = 0$ in $N_0' \otimes M$, hence in $N \otimes M$. Therefore, $T_M\alpha$ is injective. □

75. Examples. Vector spaces, or more generally, free modules are flat.

Algebras. Let $f : A \to B$ be a ring morphism. The operation $a \cdot b := f(a)b$ turns B into an A-module. The module structure is compatible with the ring structure in the obvious sense, i.e. $(a_1 + a_2) \cdot b = a_1 \cdot b + a_2 \cdot b$, $a \cdot (b_1 + b_2) = a \cdot b_1 + a \cdot b_2$ and $a \cdot (b_1 b_2) = (a \cdot b_1)b_2 = b_1(a \cdot b_2)$.

76. Definition (A-algebra). An **A-algebra** is by definition an A-module structure on a ring B provided by a morphism $f : A \to B$ as above. An **A-algebra morphism** $f : B \to C$ is a ring morphism which is also an A-module morphism.

77. Example. The ring $A[x_1, \ldots, x_n]$ is an A-algebra with respect to the natural inclusion $A \hookrightarrow A[x_1, \ldots, x_n]$. More generally, $A[x_1, \ldots, x_n]/\mathfrak{a}$ for any ideal $\mathfrak{a} \subset A[x_1, \ldots, x_n]$ is an A-algebra.

78. Remarks.

(i) If $A = k$ is a field, then any nontrivial morphism $k \to B$ is injective (cf. Proposition 0.2). In particular, any k-algebra is a ring containing k.

(ii) Let A be any ring. Then there is a natural map $\mathbb{Z} \to A$, $n \mapsto 1 + \ldots + 1$ (n times 1). In particular, every ring is automatically a $\mathbb{Z}$-algebra in the sense of Definiton 0.76.

79. Definition. A ring morphism $f : A \to B$ is called **finite**, and B is a **finite A-algebra**, if B is a finite A-module. Further, f is of **finite type**, and B is a **finitely generated A-algebra** if there exists a surjective A-algebra morphism $F : A[x_1, \ldots, x_n] \to B$ with $F(A) = f(A)$, i.e. B is isomorphic (as an A-algebra!) to $A[x_1, \ldots, x_n]/\mathfrak{a}$ for some ideal $\mathfrak{a} \subset A[x_1, \ldots, x_n]$ and $n \in \mathbb{N}$. Equivalently, any element in B can be written as a polynomial in $F(x_i)$ with coefficients in $f(A)$.

We usually drop the reference to the underyling morphism $f : A \to B$ and simply speak of an A-algebra B.

80. Exercise (finitely generated algebra vs. finitely generated module). *Let A be an integral domain with field of fractions k, and let $f \in A\backslash\{0\}$ be not a unit. Then $A[1/f]$, the algebra generated by A and $1/f$ inside k, is not a finite A-module.*

Proof. Indeed, assume the contrary. Then there exists $k \in \mathbb{N}$ such that $f^{-(k+1)} = \sum_{i=0}^{k} a_i f^{-i}$. Hence $1 = \sum_{i=0}^{k} a_i f^{k-i+1} = f \sum_{i=0}^{k} a_i f^{k-i}$. In particular, f is a unit. Contradiction! □

81. Proposition (tensor product of algebras). *Let B and C be two A-algebras. Then $B \otimes_A C$ is also an A-algebra.*

Proof. Let T be the A-module $B \otimes_A C$. We define a ring structure via the multiplication $\mu : T \times T \to T$ induced by $\mu(b \otimes c, \tilde{b} \otimes \tilde{c}) = b\tilde{b} \otimes c\tilde{c}$. Again, the point to show is that μ is well-defined. First, define a map $B \times C \times B \times C \to T$ by $(b, c, \tilde{b}, \tilde{c}) \mapsto b\tilde{b} \otimes c\tilde{c}$. Since this is linear in each factor, the universal property yields an A-linear map $B \otimes C \otimes B \otimes \tilde{C} = T \otimes T \to T$ which corresponds to a bilinear map $\mu : T \times T \to T$. It is straightforward to check that this turns T into an A-module. □

82. Exercise (flat A-modules). *Let $A \to B$ be a ring morphism, and M a flat A-module $\Rightarrow M_B := B \otimes_A M$ is a flat B-module.*

Proof. Let $\varphi : N_1 \to N_2$ be an injective B-linear map between two B-modules $N_{1,2}$. We regard B as an (A, B)-bimodule so that by Proposition 0.67 we have

$$N_i \otimes_B M_B = N_i \otimes_B (B \otimes_A M) \cong (N_i \otimes_B B) \otimes_A M \cong N_i \otimes_A M. \tag{1}$$

Under these isomorphisms $\varphi \otimes 1 : N_1 \otimes_B M_B \to N_2 \otimes_B M_B$ becomes an A-linear morphism $N_1 \otimes_A M \to N_2 \otimes_A M$ which sends $(bn) \otimes_A m$ to $(b\varphi(n)) \otimes_A m = \varphi(bn) \otimes_A m$ induces a B-linear map $N_1 \otimes_A M \to N_2 \otimes_A M$. Since M is a flat A-module, this map, and a fortiori $\varphi \otimes 1$ is injective, whence M_B is a flat B-module according to Proposition 0.74. □

0.3. **Noetherian rings and modules.** Next we discuss one of the most important classes of rings, namely those rings whose ideals are finitely generated modules. In particular, the rings of the form $k[x_1, \ldots, x_n]/\mathfrak{a}$, which play a key rôle in algebraic geometry, belong to this class.

83. Definition (ascending and descending chain condition). A partially ordered set Σ[1] has the **ascending chain condition** (a.c.c. for short) if every chain $s_1 \leqslant s_2 \leqslant s_3 \leqslant \ldots \leqslant s_n \leqslant \ldots$ becomes eventually stationary, that is, there exists $k \in \mathbb{N}$ such that $s_k = s_{k+1} = \ldots$. Similarly, one defines the **descending chain condition** (d.c.c.) for chains $s_1 \geqslant s_2 \geqslant s_3 \geqslant \ldots \geqslant s_n \geqslant \ldots$.

84. Example. The set of vector subspaces of a finite dimensional vector space ordered with respect to inclusion satisfies the a.c.c..

85. Remark. For every partially ordered set $(\Sigma, \leqslant)$ a.c.c. is equivalent with every nonempty subset S having a maximal element m (i.e. if $s \in S$ with $s \geqslant m$, then $s = m$): Indeed, a stationary sequence has a maximal element. Conversely, if we had no maximal element, we could inductively construct a sequence which does not become stationary.

86. Proposition and Definition (Noetherian rings). *For a ring A are equivalent:*

(i) *The set of ideals of A has the a.c.c.;*

[1] Recall that this means that there exists a binary relation "$\leqslant$" on Σ which is reflexive, antisymmetric, and transitive.

(ii) *every nonempty set of ideals has a maximal element with respect to inclusion;*
(iii) *every ideal is finitely generated.*

If any of these conditions is satisfied we call A **Noetherian**.

Proof. (i)⇔(ii) This is just the previous remark.

(i)⇒(iii) Let $\mathfrak{a}$ be an ideal of A and pick $x_1 \in \mathfrak{a}$. Choose inductively a sequence $x_{i+1} \in \mathfrak{a}\backslash(x_1, \ldots, x_i)$. Since the sequence $(x_1) \subset (x_1, x_2) \subset \ldots \subset (x_1, \ldots, x_n) \subset \ldots$ eventually becomes stationary, we must have $(x_1, \ldots, x_m) = \mathfrak{a}$ for some m.

(ii)⇒(iii) Let $\mathfrak{a}$ be an ideal and S be the set of finitely generated ideals in A which are contained in $\mathfrak{a}$. Since $(0) \in S$ this is nonempty, hence has a maximal element $\mathfrak{b}$ by assumption. However, if there exists $x \in \mathfrak{a}\backslash\mathfrak{b}$ then the ideal generated by x and $\mathfrak{m}$ would be finitely generated, be contained in $\mathfrak{a}$ and strictly contain $\mathfrak{b}$, a contradiction. Hence $\mathfrak{a} = \mathfrak{b}$.

(iii)⇒(i) Let $\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \ldots \subset a_n \subset \ldots$ be a sequence of ideals. Since $\mathfrak{b} = \bigcup \mathfrak{a}_i$ is again an ideal which by assumption is finitely generated, we have $\mathfrak{b} = (x_1, \ldots, x_n)$. Since the are finitely many ideals $\mathfrak{a}_i$ which contain the generators, the sequence eventually stops. □

87. Remark. Similarly, the d.c.c. is equivalent to the existence of *minimal elements*. A ring satisfying the d.c.c. is called **Artinian** (cf. for instance [AtMa, Chapter 8]). An Artinian ring is always Noetherian, that is, d.c.c. on ideals implies always a.c.c.. More precisely, a ring A is Artinian if and only if A is Noetherian and every prime ideal is maximal (see for instance [Ga, Proposition 7.17]). However, the d.c.c. is not equivalent with ideals being finitely generated which is why Noetherian rings are more important than Artinian ones.

88. Examples.

(i) $\mathbb{Z}$ satisfies a.c.c. but not d.c.c. Indeed, consider the infinite chain $(a) \supset (a^2) \supset (a^3) \supset \ldots$ for $a \neq 0$.
(ii) Similarly, $k[x]$ satisfies a.c.c., but not d.c.c. Indeed, consider $(x_1) \supset (x_1^2) \supset \ldots$. In fact, Hilbert's base theorem 0.102 asserts A Noetherian (for instance $A = k$) $\Rightarrow A[x]$ is Noetherian. The proof can be extended to show that A Noetherian $\Rightarrow A[\![x]\!]$ (ring of formal power series) is Noetherian, see Theorem 0.102 and Exercise 0.104.
(iii) $k[x_1, x_2, \ldots]$ in an infinite number of indeterminates x_i satiesfies neither chain condition. Indeed, consider $(x_1) \subset (x_1, x_2) \subset (x_1, x_2, x_3) \subset \ldots$.
(iv) Consider the germ of continuous functions at $0 \in \mathbb{R}$, i.e. the set of equivalence classes $[U, f]$ where $U \subset \mathbb{R}$ is an open subset containing 0 and $f : U \to R$ a continuous function. We have $[U, f] = [V, g] \Leftrightarrow$ there exists an open neighbourhood W of 0 in $U \cap V$ with $f|_W \equiv g|_W$. Multiplication and addition of germs turn this into a commutative ring A. Further, $[U, f]$ is a unit in $A \Leftrightarrow f(0) \neq 0$. Hence, the nonunits form an ideal $\mathfrak{m}$ which by Proposition 0.11 is maximal. In particular, $(A, \mathfrak{m})$ is a local ring. However, it is not Noetherian. Namely, assume that $\mathfrak{m}$ has a finite number of generators $f_1, \ldots, f_n$. Then for any $g \in \mathfrak{m}$ we have $g = \sum a_i f_i$ for continuous functions a_i defined near 0. In particular, there exists a constant c (depending on g of course) such that $|g(x)| < c \max |f_i(x)|$ as $x \to 0$. In particular, $|g(x)| / \max |f_i(x)|$ is bounded for any g as $x \to 0$ which of course cannot be true for there exist functions which vanish at 0 yet decrease much faster than $\max |f_i(x)|$. For instance, put $g(x) = \sqrt{\max |x|, |f_i(x)|}$, then $g / \max |f_i(x)| \geqslant g / \max |x|, |f_i(x)| \to \infty$ as $x \to 0$. Similarly, the ring of C^∞ germs is not Noetherian, while the

Noetherian property holds for holomorphic functions (this follows essentially from the power series property of holomorphic functions and (ii) above).

(v) In a similar vein, consider an infinite compact Hausdorff space X together with the ring of continuous functions $A = C(X)$. Take a strictly decreasing sequence of closed sets $F_1 \supset F_2 \supset \ldots$, and let $\mathfrak{a}_i = \{f \in A \mid f(F_i) = 0\}$. Then $\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \ldots$ is a strictly increasing sequence of ideals, hence A is not Noetherian.

Proposition 0.86 generalises easily to modules:

89. Definition (Noetherian module). A module M is called **Noetherian** if its set of submodules satisfies the a.c.c. with respect to inclusion.

90. Remark.

(i) In particular, A is a Noetherian ring if and only if it is a Noetherian A-module.
(ii) In the same way, we can define **Artinian** modules which satisfy the d.c.c.

91. Proposition (Noetherian modules and finitely generated submodules). *M is a Noetherian A-module if and only if every submodule of M is finitely generated. In particular, M is itself finite over A.*

Proof. $\Rightarrow$) Let N be a submodule of M, and let Σ be the set of all finitely generated submodules of N. Since $0 \in \Sigma$, Σ is nonempty. By the a.c.c. it must have a maximal element, say L. If $N = L$, then N is finitely generated. If not, there exists $x \in N \backslash L$, and L and x generate a submodule which both is finitely generated and properly contains L, a contradiction to its maximality.

$\Leftarrow$) Let $N_1 \subset N_2 \subset \ldots$ be an ascending chain of submodules. Then the union $\bigcup N_i$ is also a submodule which by assumption is finitely generated, say by $m_1, \ldots, m_r \in M$. But then there must be an n such that $m_i \in N_l$ for $l \geqslant r$. It follows that $N_l = N_r$ for all $l \geqslant r$ so that the chain is stationary. □

92. Proposition (quotients and submodules of Noetherian and Artinian modules). *Let $0 \to L \xrightarrow{\alpha} M \xrightarrow{\beta} N \to 0$ be a short exact sequence of A-modules. Then*

$$M \text{ is Noetherian (Artinian)} \Leftrightarrow L \text{ and } N \text{ are.}$$

In particular, quotients and submodules of Noetherian (Artinian) modules are again Noetherian (Artinian).

Proof. We prove the statement for Noetherian modules, the Artinian case being similar.

$\Rightarrow$) Any ascending chain in L or N corresponds to an ascending chain in M so that L and N inherit the a.c.c. from M.

$\Leftarrow$) Suppose $M_1 \subset M_2 \subset \ldots$ is an ascending chain of submodules. Thinking of L as a submodule of M we have the chain $L \cap M_1 \subset L \cap M_2 \subset$, and applying β we also get $\beta(M_1) \subset \beta(M_2) \subset \ldots$ of submodules in N. Each of these chains eventually stops by assumption and the result follows from Lemma 0.46. □

93. Corollary (direct sum of Noetherian (Artinian) modules). *If M_i are a finite number n of Noetherian (Artinian) modules $\Rightarrow \bigoplus_i M_i$ is Noetherian (Artinian).*

Proof. $0 \to M_1 \to M_1 \oplus M_2 \to M_2 \to 0$ is a split exact sequence which implies the assertion for $n = 2$. Then proceed by induction. □

94. Exercise (subrings of Noetherian rings). *Are subrings of Noetherian rings again Noetherian?*

Proof. No. Take an integral ring which is not Noetherian, for instance $A = k[x_1, x_2, \ldots]$, and consider the inclusion $A \subset k = \operatorname{Quot} A$. As a field, k is Noetherian. However, A is not. □

95. Corollary (modules over Noetherian rings). *Let A be a Noetherian ring.*

(i) *If M a finite A-module $\Leftrightarrow$ M is Noetherian. In particular, any submodule of a finite module over A is itself finite.*
(ii) *If $\mathfrak{a} \subset A$ is an ideal $\Rightarrow$ $A/\mathfrak{a}$ is Noetherian ring.*
(iii) *If $\varphi : A \to B$ is a ring morphism such that B is a finite A-module $\Rightarrow$ B is Noetherian ring.*

Proof. (i) If M is Noetherian it is finite as we have seen above. If M is finite over A, then $M \cong A^n/N$ so that M is Noetherian A-module as the quotient of a Noetherian A-module A^n.

(ii) $A/\mathfrak{a}$ is a Noetherian A-module. Since the scalar multiplication of A and $A/\mathfrak{a}$ coincide, it is also a Noetherian A-module, that is, $A/\mathfrak{a}$ is a Noetherian ring.

(iii) B is obviously Noetherian as an A-module. Its ideals are A-submodules, hence finite as A-modules and a fortori as B-modules. □

96. Exercise (finite presentation of finitely generated modules over Noetherian rings). *If A is Noetherian and M finitely generated, then it is* **finitely presented***, that is, there exists an exact sequence*

$$A^q \xrightarrow{\varphi_2} A^p \xrightarrow{\varphi_1} M \to 0.$$

Remark: Any finitely presented module (over an arbitrary ring) is obviously finitely generated. The exercise shows that the converse holds if A is Noetherian.

Proof. Since M is finitely generated, by definition there is an epimorphism $\varphi_2 : A^p \to M$, This gives the exact sequence $0 \to \ker \varphi_1 \to A^p \to M \to 0$. Since A is Noetherian as a module over itself, so is A^p by (i) of the previous corollary. Hence $\ker \varphi$ is a finitely generated A-module so that there exists an epimorphism $\varphi_2 : A^q \to \ker \varphi_1$. □

97. Remark. If A is Artinian, and

(i) M a finite A-module $\Rightarrow$ M is Artinian;
(ii) $\mathfrak{a} \subset A$ an ideal $\Rightarrow$ $A/\mathfrak{a}$ is an Artinian ring.

98. Exercise (Cohen's theorem). *If all prime ideals of A are finitely generated $\Rightarrow$ A is Noetherian.*

Hint: Consider the set Σ of ideals which are not finitely generated.

Proof. Assume $\Sigma \neq \varnothing$. By Zorn's lemma, there exists a maximal element $\mathfrak{a}$ which by assumption is not prime ideal. Indeed, take a chain $\mathfrak{a}_0 \subset \mathfrak{a}_1 \subset \ldots$. Then the union $\bigcup \mathfrak{a}_i$ is again an ideal because the union is taken over a chain. If it was finitely generated, then the generators must be contained in some ideal $\mathfrak{a}_N$ for N large enough, so $\mathfrak{a} \in \Sigma$ is an upper bound. It follows that there are a, $b \in A$ with $ab \in \mathfrak{a}$, but a, $b \notin \mathfrak{a}$. Since $\mathfrak{a} + (a)$ contains $\mathfrak{a}$ it must be finitely generated, say $\mathfrak{a} + (a) = (x_1, \ldots, x_r, a)$ with $x_i \in \mathfrak{a}$ (otherwise, write $x_i = \alpha_i + c_i a$ with $\alpha_i \in \mathfrak{a}$ and $c_i \in A$ and replace x_i by α_i. Moreover, $\mathfrak{a} : (a) = \{x \in A \mid xa \in \mathfrak{a}\}$ contains b. Hence $\mathfrak{a}$ is strictly contained in $\mathfrak{a} : (a)$ which therefore has a finite set of generators $\{y_1, \ldots, y_s\}$. But then $\mathfrak{a} = (x_1, \ldots, x_n, y_1 a, \ldots, y_s a)$ for if $\alpha = \sum a_i x_i + ca \in \mathfrak{a}$, then $ca \in \mathfrak{a}$ so that c must be a linear combination of the $y_i \in \mathfrak{a} : (a)$. Thus $\mathfrak{a}$ is finitely generated, a contradiction. Hence $\Sigma = \varnothing$ so that A is Noetherian. □

99. Exercise (prime ideals in Artinian rings). *Let A be an Artinian integral domain. Prove that A is a field. Deduce that every prime ideal of a general Artinian ring is maximal.*

Hint: For $a \in A$, the d.c.c. applied to $(a) \supset (a^2) \supset \ldots \supset (a^k)$ gives a relation $a^k = xa^{k+1}$, $x \in A$.

Proof. Let $0 \neq a \in A$. By the d.c.c. there exsist $k \in \mathbb{N}$ und $x \in A$ so that $a^k = xa^{k+1}$. If $k = 0$, then $xa = 1$, so that a is a unit. Otherwise, $a(xa^k - a^{k-1}) = 0$. Since A is integral, $xa^k - a^{k-1} = 0$. Continuing in this way, we arrive again at $xa = 1$, whence A is a field.

If A is a general Artinian ring and $\mathfrak{p} \subset A$ a prime ideal, then $A/\mathfrak{p}$ is an integral Artinian ring. Let $\mathfrak{m} \supset \mathfrak{p}$ be an ideal of A containing $\mathfrak{p}$. Then there exists $\bar{\mathfrak{m}}$ in $A/\mathfrak{p}$ whose inverse image is $\mathfrak{m}$. However, $\bar{\mathfrak{m}}$ is either trivial or $A/\mathfrak{p}$ by the previous step. Hence either $\mathfrak{m} = \mathfrak{p}$ or $\mathfrak{m} = A$ so that $\mathfrak{p}$ is maximal. □

100. Exercise. *Let $(A, \mathfrak{m})$ be an Artinian local ring. Prove that $\mathfrak{m}$ is nilpotent, i.e. there exists $k \in \mathbb{N}$ with $\mathfrak{m}^k = 0$.*

Hint: The d.c.c. yields $k \in \mathbb{N}$ such that $\mathfrak{m}^k = \mathfrak{m}^{k+1}$. Assume that $\mathfrak{m} \neq 0$, otherwise there is nothing to prove. Let $\mathfrak{a}_0$ be minimal among the ideals of A with $\mathfrak{a} \cdot \mathfrak{m}^k \neq 0$ (why does it exist?). Prove that $\mathfrak{a}_0 = (x)$ is prinicpal before applying Nakayama's lemma 0.60 to it.

Proof. Since A is Artinian, $\mathfrak{a}_0$ exists by Zorn's Lemma. By design, there exists $x \in \mathfrak{a}_0$ such that $x\mathfrak{m}^k \neq 0$, whence $(x) = \mathfrak{a}_0$ by minimality. Further, since $(x)\mathfrak{m} \subset (x)$ and $(x)\mathfrak{m} \cdot \mathfrak{m}^k = (x)\mathfrak{m}^{k+1} = (x)\mathfrak{m}^k \neq 0$ we conclude by minimality again that $(x)\mathfrak{m} = \mathfrak{m}$. But $M = (x)$ is a finite A-module, hence $M = 0 = x$ by Nakayama's lemma. Contradiction! □

101. Remark. The structure theorem for Artinian rings asserts that *an Artinian ring is uniquely (up to isomorphism) a finite direct product of Artianian local rings*, see for instance [AtMa, Theorem 8.7].

102. Theorem (Hilbert basis theorem). *If A is Noetherian, then so is the polynomial ring $A[x]$.*

Proof. We prove that any ideal $\mathfrak{A} \subset A[x]$ is finitely generated by "reducing" it to A.

Step 1. *Construction of the generators.* For $n \geqslant 0$ we consider the sets

$$\mathfrak{a}_n := \{a \in A \mid \text{there exists } f \in \mathfrak{A} \text{ such that } f = ax^n + b_{n-1}x^{n-1} + \ldots + b_0\},$$

that is, $\mathfrak{a}_n$ is the set of elements in A which arise as leading coefficient of a polynomial of degree n in $\mathfrak{A}$. Since $\mathfrak{A}$ is an ideal, so are the $\mathfrak{a}_n$. Further, since $f \in \mathfrak{A}$ implies $xf \in \mathfrak{A}$, $\mathfrak{a}_n \subset \mathfrak{a}_{n+1}$ is an increasing chain of ideals. By the Noether property of A, (i) the sequence eventually becomes sationary for $n \geqslant m$; (ii) there exist $\{a_{n1}, \ldots, a_{nr_n}\}$ which generate $\mathfrak{a}_n$. From the definition of these ideals, there exist polynomials $f_{ni} \in \mathfrak{A}$ of degree n having a_{ni} as the leading coefficient.

Step 2. *We show that the set $\mathfrak{B}$ generated by $\{f_{li}\}_{l \leqslant m,\, i \leqslant r_l}$ contains $\mathfrak{A}$.* This follows from an induction on the degree of polynomials in $\mathfrak{A}$. If $f \in \mathfrak{A}$ is a polynomial of degree 0, then $f \in \mathfrak{B}$ since $\mathfrak{a}_0 \subset \mathfrak{B}$. For $\deg f = n > 0$ with leading coefficient a we consider two cases. If $n \geqslant m$, then $\mathfrak{a}_n = \mathfrak{a}_m$ so that $a = \sum_{i=1}^{r_m} b_i a_{mi}$ with $b_i \in A$. But then $g = f - \sum b_i x^{n-m} f_{mi} \in \mathfrak{A}$ has degree $< n$ for we have killed the leading coefficient of f. By induction, $g \in \mathfrak{B}$, and therefore $f \in \mathfrak{B}$. On the other hand, if $n \leqslant m$, then $f - \sum b_i f_{ni}$ has degree $< n$ if $a = \sum b_i a_{ni}$ (check the indeces in both cases!). Again $f \in \mathfrak{B}$.

□

103. Corollary (Noetherness of polynomial rings). *Let A be Noetherian $\Rightarrow A[x_1, \ldots, x_n]$ is Noetherian. More generally, any finitely generated A-algebra is Noetherian.*

Proof. By induction on n using Hilbert's basis theorem. □

104. Exercise (Noetherness of the ring of formal power series). *Adapt the proof of Hilbert's basis theorem to show: If A is Noetherian $\Rightarrow A[\![x]\!]$ is Noetherian.*

Proof. The proof is similar to Hilbert's basis theorem, the essential difference being the definition of the ideals $\mathfrak{a}_n$. If $\mathfrak{A}$ is an ideal of $A[\![x]\!]$, let

$$\mathfrak{a}_n := \{a \in A \mid \text{there exists } f \in \mathfrak{A} \cap x^n A[\![x]\!] \text{ such that } f = ax^n + b_{n+1}x^{n+1} + \ldots\}.$$

This yields an increasing chain of ideal $\mathfrak{a}_0 \subset \mathfrak{a}_1 \subset \ldots$ in A, and one can proceed as in Theorem 0.102, see also [Ma, Theorem 3.3]. Namely, since A is Noetherian,

(i) the chain becomes stationary, i.e. there exists $N \in \mathbb{N}$ such that $\mathfrak{a}_N = \mathfrak{a}_{N+1} = \ldots$;
(ii) the ideals $\mathfrak{a}_s$ are generated by a finite number of elements a_{si}, $i = 1, \ldots, r_s$. We take $a_{N+j,i} = a_{Ni}$ for $i = 1, \ldots, r_{N+j} = r_N$.

For each a_{si} choose $g_{si} \in \mathfrak{A} \cap x^s A[\![x]\!]$ of the form $g_{si} = a_{si}x^s + \sum_{j \geqslant n+1} b_j x^j$. For $s = N + j$ we take $g_{N+j,i} = x^j g_{Ni}$. We wish to show that these g_{si} generate $\mathfrak{A}$ over $k[\![x]\!]$. So, if $f = \sum_{i \geqslant 0} a_i x^i \in \mathfrak{A} = \mathfrak{A} \cap x^0 A[\![x]\!]$, $a_0 = \sum_{i=0}^{r_0} \alpha_0^i a_{0i}$ so that $f - g_0 \in \mathfrak{A} \cap XA[\![x]\!]$ for $g_0 = \sum \alpha_0^i g_{0i}$. Similarly, we can construct $g_1, g_2, \ldots, g_N$ such that $f_{N+1} := f - g_0 - g_1 - \ldots - g_N = ax^{N+1} + \sum_{j \geqslant N+2} b_j x^j \in \mathfrak{A} \cap X^{N+1} A[\![x]\!]$. In particular, $a \in \mathfrak{a}_{N+1} = \mathfrak{a}_N$ so that $a = \sum_{i=1}^{r_N} \alpha_{N+1}^i a_{Ni}$ so that $f_{N+1} - g_{N+1} \in \mathfrak{A} \cap X^{N+2} A[\![x]\!]$ with $g_{N+1} = X \sum \alpha_{N+1}^i g_{Ni}$. In the same way we can construct

$g_{N+j} = x^j \sum_{i=1}^{r_N} \alpha^i_{N+j} g_{Ni}$ for $j \geqslant 2$. For each $i \geqslant 1$ we set $h_i = \sum_{j\geqslant 0} \alpha^i_{N+j} x^j \in A[\![x]\!]$ so that

$$\begin{aligned} f =& g_0 + \ldots + g_N + \sum_{j\geqslant 1} g_{N+j} \\ &= g_0 + \ldots + g_N + \sum_{i=1}^{r_N} \big(\sum_{j\geqslant 1} \alpha^i_{N+j} x^j \big) g_{Ni} \\ &= g_0 + \ldots + g_N + \sum_{i=1}^{r_N} h_i g_{Ni}. \end{aligned}$$

Then $g_0, \ldots, g_N$ are in the finite A-module generated by g_{si}, $s \leqslant N$, while g_{N+j}, $j \geqslant 0$ are in the finite $A[\![x]\!]$-module also generated by g_{si}. □

105. Exercise (finite modules over Noetherian local rings). *Let $(A, \mathfrak{m})$ be a local Noetherian ring, and M be a finite A-module. If any exact sequence of A-modules $0 \to N \to A^n \to M \to 0$ is preserved under tensoring with $k = A/\mathfrak{m} \Rightarrow M$ is free.*

Hint: Let $\bar{m}_1, \ldots, \bar{m}_n$ be a basis of the k vector space $M/\mathfrak{m}M$. By Nakayama's lemma, $m_1, \ldots, m_n$ generate M. Let $F = A^n$ be the free module of rank n and define the map $\phi(e_i) = m_i$, where $e_1, \ldots, e_n$ denotes the standard basis of F.

Proof. From the exact sequence $0 \to \ker\phi \to F \to M \to 0$ we get the exact sequence $0 \to k \otimes_A \ker\phi \to k \otimes_A F \to k \otimes_A M \to 0$. Since $k \otimes_A F$ and $k \otimes_A M$ are vector spaces of the same dimension, the induced map $1 \otimes \phi$ is an isomorphism, hence $k \otimes_A \ker\phi \cong \ker\phi/\mathfrak{m}\ker\phi = 0$ (the isomorphism is provided by Exercise 0.70). In particular, $\ker\phi = \mathfrak{m}\ker\phi$. But $\ker\phi$ is finite as the submodule of a Noetherian module (F is finite over A), whence $\ker\phi = 0$ by Nakayama. Thus $F \cong M$, so M is free. □

1. Varieties and morphisms

We saw already several examples of algebraic categories, for instance the category of rings whose morphisms where ring morphisms, or the catgeory of A-modules whose morphisms where A-linear maps. In this section we introduce the geometric category we will mainly be concerned with in the first part of this course, namely the *category of varieties*. We first define the objects, namely the *varieties*, and second the morphisms. Finally, we will construct a contravariant functor to the algebraic categories of finitely generated algebras and field extensions which will be the bridge from geometry to algebra.

What is then a "geometric category" one may ask? Roughly speaking, this is a category whose objects are topological spaces defined (at least locally) by functional equations (piecewise linear, differentiable, polynomial etc.). These give rise to a *ring of functions* which determines the morphisms and thus the geometric category (piecewise linear, smooth, algebraic etc.). The link between geometry and algebra will be thus given by polynomial rings $k[x_1, \ldots, x_n]$ (or rings derived from them such as quotients). For instance, consider $X = \mathbb{C}$. We declare a subset U of X to be *open* if it is the complement in $\mathbb{C}$ of a finite set of points. As ring of functions we take $A = \mathbb{C}[x]$ which are continuous with respect to this topology. More abstractly, consider $\operatorname{Spec} A$ of a general ring A. We have already seen in the exercises at the end of Section 0.0.1 that $X := \operatorname{Spec} A$ is a topological space in a natural way. Now

for any $x = \mathfrak{p} \in X$ we have a natural map $A \to \mathrm{Quot}\,(A/\mathfrak{p})$ (since $\mathfrak{p}$ is prime, $A/\mathfrak{p}$ is integral!). For $f \in A$ we define a "function" on X which associates with $x \in X$ the image of a under the map $A \to \mathrm{Quot}\,(A/\mathfrak{p})$, which we denote by $f(x)$. In particular, unlike ordinary functions, $f(x)$ takes values in different fields. In this sense, A becomes a "ring of functions" for the "geometric object" $\operatorname{Spec} A$. For instance, if $A = \mathbb{Z}$, we can view $f(p)$, where p is a prime, as the $\bmod p$ reduction of f in the field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. If $A = \mathbb{C}[x]$, then for $\mathfrak{p} = (x - z)$ we have $f(\mathfrak{p}) \in \mathbb{C}[x]/\mathfrak{p} \cong \mathbb{C}$, where the latter isomorphism is induced by evaluation at z. Hence, in this case, we can identify $f(\mathfrak{p})$ with $f(z)$ so that we recover $\mathbb{C}$ (actually as a topological space, as we will see later) and its ring of functions $\mathbb{C}[x]$.

Literature. This course follows mostly the standard textbook in algebraic geometry, namely

- R. Hartshorne, *Algebraic Geometry*, Springer, 1977.

For a more leisurely paced introduction we recommend

- K. Hulek, *Elementare algebraische Geometrie*, Springer, 2000.

Further references we occasionally use are

- A. Gathmann, *Algebraic Geometry*, lecture notes available at mathematik.uni-kl.de/agag/mitglieder/professoren/gathmann/notes/.
- M. Reid, *Undergraduate algebraic geometry*, LMS, 1988.

General remark on fields. Unless mentioned otherwise, k will always denote an algebraically closed field. This has two consequences: First, k has infinitely many elements which allows us to identify the *polynomial algebra* $k[x_1, \ldots, x_n]$ with the set of *polynomial functions* $k^n \to k$ obtained by evaluation. This is false for instance over $\mathbb{Z}_2$, since $x(x+1)$ is identically zero as polynomial function, but nonzero as a polynomial in $\mathbb{Z}_2[x]$. Secondly, we can directly apply Hilbert's Nullstellensatz 2.16 instead of appealing to results from Galois theory (cf. [Re, Chapter 5.4]).

1.1. Affine and projective varieties.

Affine varieties. Let k be a(n algebraically closed) field. The most basic algebraic geometric object associated with k is the **affine space** $\mathbb{A}^n_k$. If the underlying field is clear from the context we simply write $\mathbb{A}^n$. As a set, $\mathbb{A}^n_k$ is just k^n but we reserve the latter notation for the n-dimensional *vector space* over k. In particular, k^n has a distinguished element, namely the origin or zero element. If we forget about the algebraic structure we obtain $\mathbb{A}^n$. An element $a = (a_1, \ldots, a_n) \in \mathbb{A}^n$ will be called a **point**, and the $a_i \in k$ are its **coordinates**. Moreover, $\mathbb{A}^n$ comes with a natural topology to be defined below. Affine spaces arise as solutions of (inhomogeneous) linear systems $Aa - b = 0$ where $A \in k^{m \times m}$ and $b \in k^m$. More generally, we can replace linear equations by polynomial equations. Consider a subset $T \subset k[x_1, \ldots, x_n]$. Since k is algebraically closed, it is infinite, and we can freely identify polynomials with polynomial functions on $\mathbb{A}^n$. Define

$$\mathcal{Z}(T) = \{a \in \mathbb{A}^n \mid f(a) = 0 \text{ for all } f \in T\}.$$

If (T) is the ideal generated by T, then clearly $\mathcal{Z}(T) = \mathcal{Z}((T))$. If $T = \{f\}$ for a polynomial $f \in k[x_1, \ldots, x_n]$ we simply write $\mathcal{Z}(f)$.

1. Definition (algebraic set). A subset Y of $\mathbb{A}^n$ is **algebraic** if there exists $T \subset k[x_1, \ldots, x_n]$ such that $Y = \mathcal{Z}(T)$.

2. Example. Consider $\mathbb{A}^1$. Since $k[x]$ is principal (in fact Euclidean), we have for any $T \subset k[x]$ that $\mathcal{Z}(T) = Z(f)$ for some $f \in k[x]$. Since k is algebraically

closed, $f = c(x - a_1) \cdot \ldots \cdot (x - a_n)$ for $a_i \in k$ unless f is a constant, whence $\mathcal{Z}(T) = \{a_1, \ldots, a_n\}$. Since $\mathcal{Z}(0) = \mathbb{A}^1$ and $\mathcal{Z}(1) = \varnothing$, the algebraic sets of $\mathbb{A}^1$ are as follows: $\varnothing$, finite subsets of k, and k.

We thus get a map

$$\text{subsets in } k[x_1, \ldots, x_n] \to \text{algebraic sets in } \mathbb{A}^n, \quad T \mapsto \mathcal{Z}(T).$$

In general, it is not obvious that $\mathcal{Z}(\mathfrak{a}) \neq \varnothing$ for ideals strictly contained in $k[x_1, \ldots, x_n]$. As a consequence of the weak Nullstellensatz of Theorem 0.6 and Corollary 0.7 rules out this gloomy possibility. That is also the reason why it is called "Nullstellensatz" – it ensures the existence of a rich theory of algebraic sets:

3. Proposition (algebraic sets exist in abundance). *If $\mathfrak{a} \subsetneq k[x_1, \ldots, x_n]$ is a proper ideal, then $\mathcal{Z}(\mathfrak{a}) \neq \varnothing$.*

Proof. Since $\mathfrak{a}$ is a proper ideal it is contained in some maximal ideal which by Corollary 0.7 is of the form $(x_1 - a_1, \ldots, x_n - a_n)$. Hence $(a_1, \ldots, a_n) \in \mathcal{Z}(\mathfrak{a})$. □

4. Examples.

(i) *Conics* are algebraic sets given by polynomial equations of order 2: $f = \sum a_{ij} x_i x_j + b_i x_i + c = 0$. In $\mathbb{A}^2$, these comprise the circle $x^2 + y^2 - 1 = 0$, the parabola $y - x^2 = 0$ and the hyperbola $xy - 1 = 0$ (see Figure 1.2 for a picture over $k = \mathbb{R}$).

(ii) *Cubics* are given by polynomial equations of order 3. Two important examples in $\mathbb{A}^2$ which we will use for illustration later are the *nodal cubic* $y^2 - x^3 - x^2 = 0$ and the *cuspidal cubic* $y^2 - x^3 = 0$ (see Figure 1.3).

(iii) Interesting examples come often in families. For instance, *elliptic curves* are given by the family $y^2 - x(x-1)(x-\lambda) = 0$, $\lambda \in k$ (see Figure 1.4 with $k = \mathbb{R}$). For finite fields these curves play an important rôle in cryptography (so-called "eec" – elliptic curve cryptography).

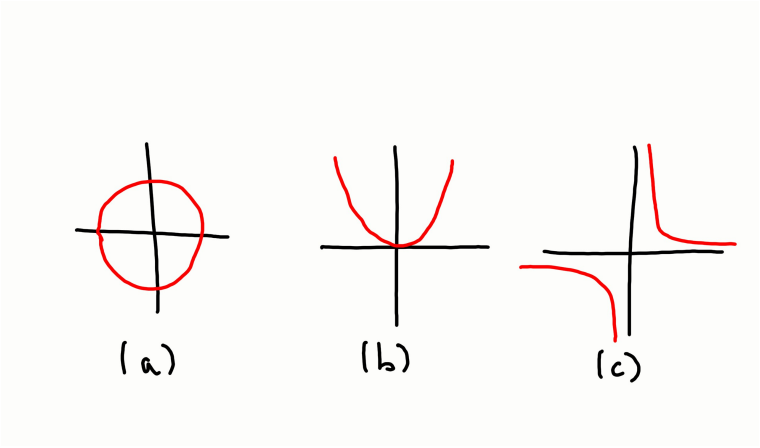

FIGURE 2. The standard conics in $\mathbb{A}^2_{\mathbb{R}}$. the circle (a) the parabola (b) the hyperbola (c).

We summarise the properties of the assignement $T \mapsto \mathcal{Z}(T)$ in the following

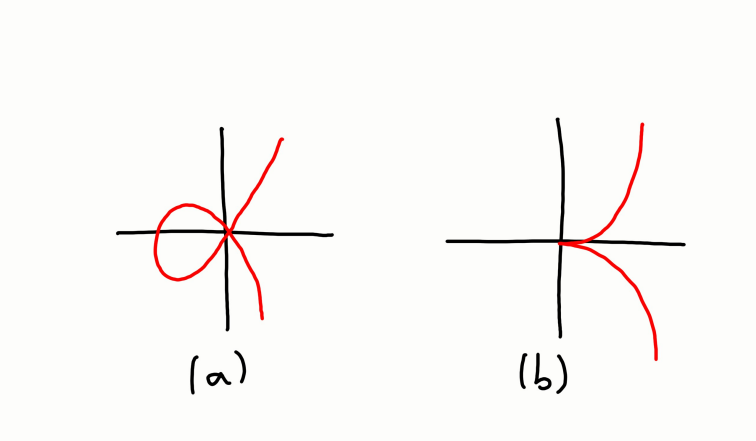

FIGURE 3. The nodal (a) and cuspidal (b) cubic in $\mathbb{A}^2_{\mathbb{R}}$.

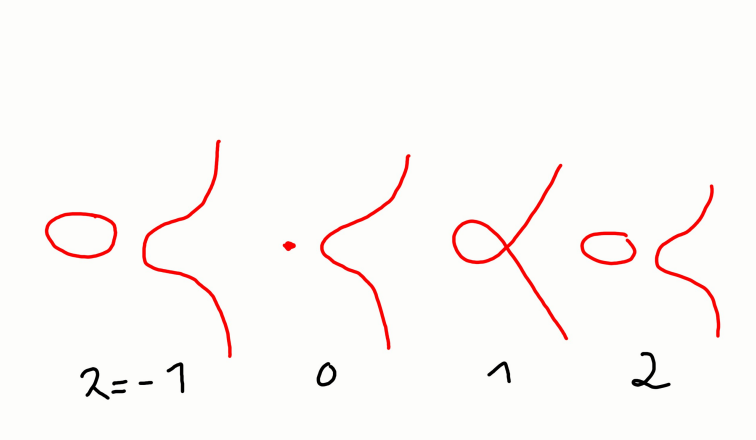

FIGURE 4. Elliptic curves for various $\lambda \in \mathbb{R}$.

5. Proposition.

(i) $T_1 \subset T_2 \subset k[x_1, \ldots, x_n] \Rightarrow \mathcal{Z}(T_1) \supset \mathcal{Z}(T_2)$.
(ii) $\mathcal{Z}(1) = \varnothing$ *and* $\mathcal{Z}(0) = \mathbb{A}^n$. *Hence the empty set and* $\mathbb{A}^n$ *are algebraic.*
(iii) $\mathcal{Z}(T_1) \cup \mathcal{Z}(T_2) = \mathcal{Z}(T_1 T_2)$, *where* $T_1 T_2 = \{f_1 \cdot f_2 \mid f_i \in T_i\}$. *Hence the finite union of algebraic sets is again algebraic.*
(iv) $\bigcap_i \mathcal{Z}(T_i) = \mathcal{Z}(\bigcup_i T_i)$. *Hence the intersection of any family of algebraic sets is again algebraic.*

Proof. Only (iii) requires proof. Let $a \in \mathcal{Z}(T_1) \cup \mathcal{Z}(T_2)$. Then either $a \in \mathcal{Z}(T_1)$ so that $f_1(a) = 0$ for $f_1 \in T_1$, or $a \in \mathcal{Z}(T_2)$ so that $f_2(a) = 0$ for $f_2 \in T_1$. Hence $a \in \mathcal{Z}(T_1 T_2)$. Conversely, let $a \in \mathcal{Z}(T_1 T_2)$. Assume that $a \notin \mathcal{Z}(T_1)$. Then there exists $f_1 \in T_1$ such that $f_1(a) \neq 0$. By definition, $f_1 \cdot f_2(a) = f_1(a) f_2(a) = 0$ so that $f_2(a) = 0$ for all $f_2 \in T_2$. □

6. Remark. If $\mathfrak{a} = (T)$ is the ideal generated by $T \subset k[x_1, \ldots, x_n]$, then $\mathcal{Z}(\mathfrak{a}) = \mathcal{Z}(T)$. In particular, we have

(i) $\mathcal{Z}(T_1T_2) = \mathcal{Z}(\mathfrak{a}_1\mathfrak{a}_2) = \mathcal{Z}(\mathfrak{a}_1 \cap \mathfrak{a}_2)$, for $\mathfrak{a}_1\mathfrak{a}_2 \subset \mathfrak{a}_1 \cap \mathfrak{a}_2$ by 0.23. More concretely, if $\mathfrak{a}_1 = (f_1, \ldots, f_s)$ and $\mathfrak{a}_2 = (g_1, \ldots, g_r)$, then

$$\mathcal{Z}(\mathfrak{a}_1 \cdot \mathfrak{a}_2) = \mathcal{Z}((f_i g_j \mid i = 1, \ldots, s \text{ and } j = 1, \ldots, r)) = \mathcal{Z}(\mathfrak{a}_1) \cup \mathcal{Z}(\mathfrak{a}_2).$$

(ii) Similarly, we have

$$\mathcal{Z}(\mathfrak{a}_1 + \mathfrak{a}_2) = \mathcal{Z}((f_1, \ldots, f_s, g_1, \ldots, g_r)) = \mathcal{Z}(\mathfrak{a}_1) \cap \mathcal{Z}(\mathfrak{a}_2).$$

(iii) $\mathcal{Z}(T) = \varnothing \Leftrightarrow (T) = k[x_1, \ldots, x_n]$. Indeed, if $\mathfrak{a}$ were a proper ideal of $k[x_1, \ldots, x_n]$, then it is contained in some maximal ideal $\mathfrak{m}$.

7. Definition (Zariski topology). We declare a set to be **open** if it is the complement of an algebraic set. The topology thus defined is called the **Zariski topology** of $\mathbb{A}^n$. We always think of $\mathbb{A}^n$ as being equipped with the Zariski topology; the closed sets are then the algebraic sets of $\mathbb{A}^n$.

8. Example.

(i) In the example of $\mathbb{A}^1$ considered above we see that a proper nonempty subset of $\mathbb{A}^1$ is Zariski open in $\mathbb{A}^1$ if and only if it is the complement of a finite subset. In particular, open sets are dense and the Zariski topology is not Hausdorff.

(ii) For any $f \in k[x_1, \ldots, x_n]$ define the so-called **basic open set** by $D_f := \mathbb{A}^n \backslash \mathcal{Z}(f)$. It is easy to see that the basic open sets form a base for the Zariski topology, i.e. every open set is a union of basic open sets.

9. Remark.

(i) To explain the link with the Zariski topology on spectra of rings, consider $\operatorname{mSpec} k[x]$ endowed with the subspace topology coming from $\operatorname{Spec} k[x]$. Its closed subsets are of the form $\mathcal{Z}(\mathfrak{a}) = \{\mathfrak{m} \in \operatorname{mSpec} k[x] \mid \mathfrak{a} \subset \mathfrak{m}\}$ for any ideal $\mathfrak{a} \subset k[x]$. Since $k[x]$ is a principal ideal ring, $\mathfrak{a} = (f)$. Moreover, $f = c(x - a_1) \cdot \ldots \cdot (x - a_n)$ so that the maximal ideals containing $\mathfrak{a}$ are precisely $(x - a_i)$, $i = 1, \ldots, n$. Under the map which sends the maximal ideal $(x - a)$ to the point $a \in k$ it represents (cf. Example 0.33), $\mathcal{Z}(\mathfrak{a})$ gets map to $\{a_1, \ldots, a_n\} = \mathcal{Z}(f)$, the corresponding closed subset of k. Hence the identification of $\mathbb{A}^1$ with $\operatorname{mSpec} k[x]$ is actually a homeomorphism.

(ii) Under the natural identification $\mathbb{R}^2 \cong \mathbb{C}$ we have $\mathbb{A}^2_{\mathbb{R}}$ is $\mathbb{A}^1_{\mathbb{C}}$ as sets, but not as topological spaces. For instance, $x^2 + y^2 - 1 \in \mathbb{R}[x, y]$ defines an algebraic set (the unit circle) which is obviously not finite in $\mathbb{C}$ (note that the discussion of the Zariski topology did not require k to be algebraically closed so that $\mathbb{A}^2_{\mathbb{R}}$ is actually defined).

10. Exercise (Products of Zariski topologies). *Identify $\mathbb{A}^2$ with $\mathbb{A}^1 \times \mathbb{A}^1$ as sets in the natural way. Show that the Zariski topology on $\mathbb{A}^2$ is not the product of the Zariski topologies on the two copies of $\mathbb{A}^1$.*

Proof. Think of $\mathbb{A}^2 = \{(x, y) \mid x, y \in \mathbb{A}^1\} = \mathbb{A}^1 \times \mathbb{A}^1$. Open sets in $\mathbb{A}^1$ are $\varnothing$, complements of finite sets, or $\mathbb{A}^1$. It follows that a base of open sets in $\mathbb{A}^1 \times \mathbb{A}^1$ is given by $\varnothing$, complements of finite families of lines parallel to the x- or y-axis, or $\mathbb{A}^2$ (i.e. any open sets with respect to the product topology can be written as a union of these sets). But $\mathbb{A}^2$ contains for instance the open subset $D_{(x-y)}$ ($\mathbb{A}^2$ without the diagonal) which is not of this type. □

11. Definition (irreducible sets). A nonempty subset X of a topological space is called **irreducible** if it cannot be written as the union $X = X_1 \cup X_2$ of two proper subsets, each of which is closed in X.

12. Example. The affine space $\mathbb{A}^1$ is irreducible for its proper closed subsets are finite, while $\mathbb{A}^1 \cong k$ is infinite, k being algebraically closed.

The following remarks are general in nature and apply to any *irreducible topological space* X.

13. Proposition (irreducible topological spaces). *Let X be an irreducible topological space. Then*

(i) $X \neq \varnothing$.
(ii) *Any two nonempty open subsets U_1, U_2 of an irreducible space X must intersect. In particular, X is not Hausdorff.*
(iii) *Any nonempty open subset U of an irreducible set X is irreducible and dense.*
(iv) *If X is irreducible, then so is its closure $\bar{X}$.*

Proof. (i) This is true by definition.

(ii) If $U_1 \cap U_2 = \varnothing$ for two open subsets, then $U_1^c \cup U_2^c = X$, where ^{c} denotes taking the complement in X.

(iii) Indeed, $X = U \cup X \backslash U$, where $X \backslash U$ is closed. A decomposition of U into closed subsets therefore yields a decomposition of X. Furthermore, $X = \bar{U} \cup X \backslash U$ so that $\bar{U} = X$ if X is irreducible.

(iv) Assume that $\bar{X} = Z_1 \cup Z_2$ with Z_i closed and properly contained in $\bar{X}$. Since $\bar{X}$ is closed, $X \cap Z_i$ is closed in X and thus gives a decomposition of X. □

14. Definition (affine and quasi-affine varieties). An **affine (algebraic) variety** is an irreducible closed subset of $\mathbb{A}^n$ together with the subspace topology induced from the Zariski topology. A **quasi-affine variety** is an open subset of an affine variety.

15. Remark. It follows from Proposition 1.13 that *any two nonempty open subsets of an affine variety intersect*, and *any nonempty open subset is dense.*

To establish a dictionary between geometry and algebra we associate with a subset $X \subset \mathbb{A}^n$ the *ideal*

$$\mathcal{I}(X) = \{f \in k[x_1, \ldots, x_n] \mid f(a) = 0 \text{ for all } a \in X\}.$$

The main theorem for the assignement $\mathcal{I}$ is the

16. Theorem (Nullstellensatz). *Let k be an algebraically closed field. Then*

$$\mathcal{I}(\mathcal{Z}(\mathfrak{a})) = \sqrt{\mathfrak{a}}.$$

Put differently, $f(x) = 0$ for all $x \in \mathcal{Z}(\mathfrak{a}) \subset \mathbb{A}^n$ if and only if $f^k \in \mathfrak{a}$ for some k.

Proof. Suppose $f \in A := k[x_1, \dots, x_n]$ is such that $f(p) = 0$ for all $p \in \mathcal{Z}(\mathfrak{a})$. We introduce the auxiliary variable Y and consider the ideal

$$\hat{\mathfrak{a}} = (\mathfrak{a}, fY - 1) \subset A[Y].$$

Now $p = (a_1, \dots, a_n, b)$ of $\mathcal{Z}(\hat{\mathfrak{a}})$ satisfies $(a_1, \dots, a_n) \in \mathcal{Z}(\mathfrak{a})$ and $f(a_1, \dots, a_n)b = 1$, whence $f(a_1, \dots, a_n) \neq 0$, a contradiction. Thus $\mathcal{Z}(\hat{\mathfrak{a}}) = \varnothing$ so that by (i), $1 \in \hat{\mathfrak{a}}$. Hence there exists $g_i \in A[Y]$ and $h_i \in \mathfrak{a}$ such that

$$\sum g_i h_i + g_0(fY - 1) = 1.$$

By multiplying a polynomial $g(x_1, \dots, x_n, y)$ by f^k for a sufficiently big power k we obtain a polynomial $G(x_1, \dots, x_n, fY)$ (note that f is itself an expression in $x_1, \dots, x_n$). Therefore we can write the identity between polynomials as

$$\sum G_i(x_1, \dots, x_n, fY)h_i + G_0(fY - 1) = f^k(x_1, \dots, x_n).$$

In particular, substituting $fY = 1$ gives

$$f^k = \sum G_i(x_1, \dots, x_n, 1)h_i \in \mathfrak{a},$$

whence the assertion. □

17. Corollary. *Let $\mathfrak{p} \subset k[x_1, \dots, x_n]$ be a prime ideal. Then $\mathcal{I}(\mathcal{Z}(\mathfrak{p})) = \mathfrak{p}$.*

We summarise the properties of $\mathcal{I}$ in the next

18. Proposition ($\mathcal{Z} \circ \mathcal{I}$). *Let X and Y be two subsets in $\mathbb{A}^n$.*

(i) *If $Y \subset X \subset \mathbb{A}^n$, then $\mathcal{I}(Y) \supset \mathcal{I}(X)$.*
(ii) *For any subset $X \subset \mathbb{A}^n$, $\mathcal{Z}(\mathcal{I}(X)) = \bar{X}$, the closure of X. In particular, $\mathcal{Z}(\mathcal{I}(X)) = X$ for any algebraic set.*
(iii) *For any ideal $\mathfrak{a} \subset k[x_1, \dots, x_n]$, $\mathcal{I}(\mathcal{Z}(\mathfrak{a})) = \sqrt{\mathfrak{a}}$.*
(iv) *We have $\mathcal{I}(X \cup Y) = \mathcal{I}(X) \cap \mathcal{I}(Y)$. Further, if Y is closed, then $\mathcal{I}(X \backslash Y) = \mathcal{I}(X) : \mathcal{I}(Y)$.*
(v) *$\mathcal{I}(X)$ is a radical ideal.*

Proof. (i) Clear from the definition.

(ii) Obviously, X is contained in the closed set $\mathcal{Z}(\mathcal{I}(X))$, whence $\bar{X} \subset \mathcal{Z}(\mathcal{I}(X))$. On the other hand, let Y be any closed set containing X, then $Y = \mathcal{Z}(\mathfrak{a})$ for some ideal $\mathfrak{a} \subset k[x_1, \dots, x_n]$. Consequently, $\mathfrak{a} \subset \mathcal{I}(X)$ and thus $\mathcal{Z}(\mathcal{I}(X)) \subset \mathcal{Z}(\mathfrak{a}) = Y$. This is in particular true for $Y = \bar{X}$.

(iii) This is the Nullstellensatz 1.16

(iv) We have

$$\begin{aligned}\mathcal{I}(X \cup Y) &= \{f \in k[x_1, \dots, x_n] \mid f(x) = 0 \text{ for all } x \in X \cup Y\} \\ &= \{f \in k[x_1, \dots, x_n] \mid f(x) = 0 \text{ for all } x \in X\} \cap \{f \in k[x_1, \dots, x_n] \mid f(x) = 0 \text{ for all } x \in Y\} \\ &= \mathcal{I}(X) \cap \mathcal{I}(Y)\end{aligned}$$

and

$$\begin{aligned}\mathcal{I}(X \backslash Y) &= \{f \in k[x_1, \dots, x_n] \mid f(x) = 0 \text{ for all } x \in X \backslash Y\} \\ &= \{f \in k[x_1, \dots, x_n] \mid f(x) \cdot g(x) = 0 \text{ for all } x \in X \text{ and } g \in \mathcal{I}(Y)\} \\ &= \{f \in k[x_1, \dots, x_n] \mid f \cdot \mathcal{I}(Y) \subset \mathcal{I}(X)\} \\ &= \mathcal{I}(X) : \mathcal{I}(Y).\end{aligned}$$

For the second step we used (ii) and that Y is closed.

(v) Let $f \in A(X)$ and suppose that $f^k = 0$. Evaluating f at $a \in X$ gives $f^k(a) = (f(a))^k = 0$, whence $f(a) = 0$ since k is a field. In particular, $f \equiv 0$ in $A(X)$, that is, $A(X)$ has no nontrivial nilpotent elements and is thus reduced. □

Furthermore, with $\mathcal{I}(X)$ we can associate a k-algebra giving the *functions* on an affine variety.

19. Definition (Coordinate rings). If $X \subset \mathbb{A}^n$ is an algebraic set, we define its **coordinate ring** $A(X)$ of X to be

$$A(X) := k[x_1, \ldots, x_n]/\mathcal{I}(X).$$

20. Remark. In particular, a coordinate ring is a finitely generated k-algebra. Furthermore, $\mathcal{I}(X)$ is radical by Proposition 1.18 (v), so that a coordinate ring must be reduced. Conversely, *any finitely generated reduced k-algebra A arises as the coordinate ring of an affine variety.* Indeed, Let A be a finitely generated algebra which is necessarily of the form $A \cong k[x_1, \ldots, x_n]/\mathfrak{a}$. Put $X = \mathcal{Z}(\mathfrak{a}) \subset \mathbb{A}^n$. If A is reduced, then $\mathfrak{a}$ is radical so that $\mathcal{I}(X) = \sqrt{\alpha} = \alpha$. Hence $A(X) = k[x_1, \ldots, x_n]/\mathfrak{a} = A$. Note that two different affine varieties (e.g. $\mathcal{Z}(x)$ and $\mathcal{Z}(y)$ in $\mathbb{A}^2$) can have isomorphic coordinate rings (e.g. $k[t]$). We will see later (Proposition 1.135) that the coordinate ring determines the affine variety up to isomorphism.

21. Examples.

(i) If $\mathfrak{m}_a = (x_1 - a_1, \ldots, x_n - a_n)$ is a maximal ideal of $k[x_1, \ldots, x_n]$ corresponding to the point $\{a\} = \mathcal{Z}(\mathfrak{m}_a)$, then its coordinate ring is $k[x_1, \ldots, x_n]/\mathfrak{m}_a = k$ (cf. 0.6 – any "function" on $\{a\}$ must be a constant.

(ii) Since $\mathcal{Z}(\mathbb{A}^n) = 0$, $A(\mathbb{A}^n) \cong k[x_1, \ldots, x_n]$. We define

$$A[n] := A(\mathbb{A}^n) = k[x_1, \ldots, x_n]$$

and often use $A[n]$ as a shorthand notation for $k[x_1, \ldots, x_n]$.

22. Exercise.

(i) *Let $X = \mathcal{Z}(x^2 - y) \subset \mathbb{A}^2_k$. Show that $A(X)$ is isomorphic to a polynomial ring in one variable of the form $k[t]$.*

(ii) *Let $Y = \mathcal{Z}(xy - 1) \subset \mathbb{A}^2$. Show that $A(Y)$ is* not *isomorphic to some $k[t]$.*

Proof. (i) By definition, $A(X) = k[x, y]/(x^2 - y)$. Since $\bar{y} = \bar{x}^2$, $A(X) = k[\bar{x}, \bar{x}^2] = k[\bar{x}]$. Formally, an isomorphism is provided by $k[t] \to A(X)$ is induced by the assignement $t \mapsto \bar{x}$.

(ii) Here, $A(Y) = k[x, y]/(xy - 1)$ so that $\bar{x} = 1/\bar{y}$. Hence $A(X) = k[\bar{x}, 1/\bar{x}]$ which contains a unit which is not in k. Thus $A(X)$ cannot be of the form $k[t]$. □

23. Remark.

(i) We can think of $A(X)$ as the ring of *polynomial functions* on X viewing an equivalence class $\bar{f} \in A(X)$ as a map $\mathbf{f} : a \in X \mapsto f(a) \in k$. Since f is determined up to elements in $\mathcal{I}(X)$ this is indeed well-defined. Further, $A[n] = k[x_1, \ldots, x_n]$ and $A(X)$ are Noetherian rings by Section 0.0.3. Choosing generators $\bar{x}_1, \ldots, \bar{x}_n$ of $A(X)$ is the same thing as choosing coordinates $x_1, \ldots, x_n$ on $\mathbb{A}^n$ which give rise to "coordinates" $\bar{x}_i$ on X. Of course, the $\bar{x}_i$ are not, in general, linearly independent (they could be zero for instance).

(ii) If for $a \in X$, we let $\mathfrak{m}_a \subset A(X)$ be the ideal of functions vanishing at a, then the assignement $a \mapsto \mathfrak{m}_a$ gives a $1-1$ correspondence between the points of X and the maximal ideals of $A(X)$. Indeed, we have a correspondence between points $a \in X$ and maximal ideals $\mathfrak{m}_a \subset A[n]$ which contain $\mathcal{I}(X)$ by Corollary 0.7. The latter correspond to maximal ideals in $A(X) = A[n]/\mathcal{I}(X)$.

A necessary algebraic condition for irreducibility is this.

24. Proposition (irreducibility and prime ideals). *Let $X \subset \mathbb{A}^n$ be algebraic. If X is irreducible (and thus an affine variety) $\Leftrightarrow$ $\mathcal{I}(X)$ is a prime ideal in $A[n]$, that is, the coordinate ring of X is an integral domain.*

Proof. $\Rightarrow$) Let $f \cdot g \in \mathcal{I}(X)$. Hence $(f \cdot g) \subset \mathcal{I}(X)$ so that by Proposition 1.18 we have $\mathcal{Z}(fg) = \mathcal{Z}(f) \cup \mathcal{Z}(g) \supset \mathcal{Z}(\mathcal{I}(X)) = X$. In particular, we have a decomposition into closed subsets $X = (X \cap \mathcal{Z}(f)) \cup (X \cap \mathcal{Z}(g))$ so that either $X \subset \mathcal{Z}(f)$ or $X \subset \mathcal{Z}(g)$, whence $f \in \mathcal{I}(X)$ or $g \in \mathcal{I}(X)$.
$\Leftarrow$) Let $\mathfrak{p} = \mathcal{I}(X)$ be prime, and assume that $X = X_1 \cup X_2$, where X_i are two closed subsets of X. Then $\mathfrak{p} = \mathcal{I}(X) = \mathcal{I}(X_1) \cap \mathcal{I}(X_2)$ by Proposition 1.18, hence $\mathcal{I}(X) = \mathcal{I}(X_1)$ or $\mathcal{I}(X) = \mathcal{I}(X_2)$ by Proposition 0.24. Applying Z and Proposition 1.18 again implies $X = X_1$ or $X = X_2$. Hence X is irreducible. □

25. Example.

(i) Consider a point $a = (a_1, \ldots, a_n) \in \mathbb{A}^n$. Geometrically it is obvious that it is irreducible. Hence $\mathcal{I}(\{a\})$ is prime. Indeed, as we have seen in Example 0.5, its associated ideal $(x_1 - a_1, \ldots, x_n - a_n)$ is maximal in $A[n]$.

(ii) $\mathbb{A}^n = \mathcal{Z}(0)$. It follows immediately (!) that $\mathbb{A}^n$ is irreducible (try to prove it starting from the definition).

26. Exercise. *Let $X = \mathcal{Z}(x^2 - yz, x(z-1)) \subset \mathbb{A}^3_k$. Show that X is a union of three irreducible components. Describe their prime ideals.*

Proof. We have

$$\begin{aligned} X &= \mathcal{Z}(x^2 - yz, x(z-1)) = \mathcal{Z}(x^2 - yz) \cap \mathcal{Z}(x(z-1)) \\ &= \mathcal{Z}(x^2 - yz) \cap (\mathcal{Z}(x) \cup \mathcal{Z}(z-1)) \\ &= (\mathcal{Z}(x^2 - yz) \cap \mathcal{Z}(x)) \cup (\mathcal{Z}(x^2 - yz) \cap \mathcal{Z}(z-1)) \\ &= \mathcal{Z}(x, y) \cup \mathcal{Z}(x, z) \cup \mathcal{Z}(x^2 - y, z - 1). \end{aligned}$$

Hence X is the union of the irreducible components $\mathcal{Z}(x, y)$, $\mathcal{Z}(x, z)$ and $\mathcal{Z}(x^2 - y, z - 1)$ whose coordinate rings are isomorphic to $k[t]$. □

We have natural notions of subvarieties and product of varieties.

27. Definition (locally closed subspaces and affine subvarieties). A subset of a topological space is called **locally closed** if it an open subset of its closure, or equivalently, if it is the interseciton of an open set with a closed set. If $X \subset \mathbb{A}^1$ is a quasi-affine variety, and Y is an irreducible locally closed subset, then Y is open in its closure $\bar{Y}$, a closed irreducible subset of X. In particular, $\bar{Y} = X \cap \mathcal{Z}(\mathfrak{a}) = \mathcal{Z}(\mathcal{I}(X) + \mathfrak{a}) \subset \mathbb{A}^n$ is again an affine variety, and Y inherits a natural structure of a quasi-affine variety being an open subset of $\bar{Y}$. We call Y a **subvariety of** X.

28. Exercise (subvarieties of X and prime ideals of $A(X)$). *Let $X \subset \mathbb{A}^n$ be an affine variety. Show that there is a $1-1$ correspondence between closed subvarieties of X and prime ideals in $A(X)$.*

Proof. If $Y \subset X$ is a closed subvariety of X, then $Y = \bar{Y} = \mathcal{Z}(\mathcal{I}(X) + \mathfrak{a})$, where $\mathfrak{p} = \mathcal{I}(X) + \mathfrak{a} \subset A[n]$ is a prime ideal (Y is irreducible!) containing $\mathcal{I}(X)$. Hence $\mathfrak{p}$ corresponds to a prime ideal in the quotient $A(X) = A[n]/\mathcal{I}(X)$. Conversely, if $\mathfrak{q} \subset A(X)$ is a prime ideal, then $\mathfrak{q}$ is the image of a prime ideal $\mathfrak{p} \subset A[n]$ containing $\mathfrak{p}$. Then $Y = \mathcal{Z}(\mathfrak{p}) \cap X = \mathcal{Z}(\mathfrak{p} + \mathcal{I}(X)) = \mathcal{Z}(\mathfrak{p})$ is closed in X (being the intersection of X with an algebraic set of $\mathbb{A}^n$) and irreducible (being defined by a prime ideal). □

29. Proposition (product of affine varieties). *The product $X \times Y$ of two affine varieties $X \subset \mathbb{A}^n$ and $Y \subset \mathbb{A}^m$ with coordinate rings $A(X)$ and $A(Y)$ is also an affine variety with coordinate ring $A(X \times Y) = A(X) \otimes_k A(Y)$.*

Proof. Indeed, it is clear that if $X = \mathcal{Z}(\mathfrak{a})$ and $Y = \mathcal{Z}(\mathfrak{b})$ for $\mathfrak{a} \subset k[x_1, \dots, x_n]$ and $\mathfrak{b} \subset k[x_1, \dots, x_m]$, then $X \times Y$ can be identified (as a set) with $\mathcal{Z}(\mathfrak{a} + \mathfrak{b})$, the zero locus of the ideal in $k[x_1, \dots, x_{n+m}]$ generated by $\mathfrak{a} + \mathfrak{b}$. The only point to check is irreducibility. So assume that we had a decomposition $X \times Y = Z_1 \cup Z_2$. Projection on the first resp. second factor induces *isomorphisms* $X \times \{b\} \cong X$ for all $b \in Y$ and $\{a\} \times Y \cong Y$ for all $a \in X$. In particular, the fibres of the projections are irreducible. Further, we obtain a decomposition

$$X \times \{b\} = (X \times \{b\} \cap Z_1) \cup (X \times \{b\} \cap Z_2).$$

Hence either $X \times \{b\} \cap Z_1 = X \times \{b\}$ or $X \times \{b\} \cap Z_2 = Z_2$. Let $Y_i := \{b \in Y \mid X \times \{b\} \subset Z_i\}$. But this yields a decomposition of Y into the closed sets $Y_1 \cup Y_2$ so that by irreducibility of Y we have either $X \times Y = Z_1$ or $X \times Y = Z_2$ (note that $Y_i = \bigcap_{a \in X} \{a \in X \mid (a, b) \in Z_i\}$ is indeed closed as an intersection of closed sets). □

30. Remark. Note that the topology on $X \times Y$ induced from $\mathbb{A}^{n+m}$ is *not* the product topology (which we can define independently from any affine structure). For instance, the construction above yields $\mathbb{A}^1 \times \mathbb{A}^1 = \mathbb{A}^2$, but this is not homoemorphic to $\mathbb{A}^1 \times \mathbb{A}^1$ (cf. Exercise 1..10).

Let us summarise the correspondence between alegebra and geometry.

algebraic sets in $\mathbb{A}^n$	$\longleftrightarrow$	radical ideals of $A[n]$
affine varieties in $\mathbb{A}^n$	$\longleftrightarrow$	prime ideals of $A[n]$
points in $\mathbb{A}^n$	$\longleftrightarrow$	maximal ideals of $A[n]$
$\mathbb{A}^n$	$\longleftrightarrow$	$(0) \subset A[n]$
$\varnothing$	$\longleftrightarrow$	$(1) \subset A[n]$
product $X \times Y$	$\longleftrightarrow$	tensor product $A(X) \otimes_k A(Y)$
closed subvarities of X	$\longleftrightarrow$	prime ideals in $A(X)$
points of X	$\longleftrightarrow$	maximal ideals in $A(X)$

Next we investigate further topological consequences coming from the fact that the coordinate rings are finitely generated.

31. Definition (Noetherian topological spaces). A topological space is called **Noetherian** if it satisfies the d.c.c. for closed subsets.

32. Example.

(i) The affine space $\mathbb{A}^n$ is Noetherian for $A[n] = k[x_1, \ldots, x_n]$ is a Noetherian ring. Indeed, a sequence of closed sets $X_1 \supset X_2 \supset \ldots$ corresponds to an ascending sequence of ideals $\mathcal{I}(X_1) \subset \mathcal{I}_(X_2) \subset \ldots$ which eventually becomes stationary. This also explains why we call this topology Noetherian instead of Artinian.

(ii) If A is Noetherian, then so is $\operatorname{Spec} A$ as a topological space for its closed sets are of the form $\mathcal{Z}(\mathfrak{a})$ for ideals $\mathfrak{a}$ of A (cf. Exercise 0.35).

The following property holds in any Noetherian topological space.

33. Proposition and Definition (irreducible components). *In a Noetherian topological space, every nonempty closed subset X can be expressed as a finite union $X = X_1 \cup \ldots \cup X_r$ of irreducible closed subsets X_i. If we require that $X_i \subsetneq X_j$ for $i \neq j$, then the set $\{X_i\}$ is uniquely determined. Its elements are called the* **irreducible components of X.**

Proof.

Step 1. *Existence.* Let Σ be the set of nonempty closed subsets with no decomposition as required. In particular, no element of Σ can be irreducible. We claim that $\Sigma = \varnothing$. Assume to the contrary that $\Sigma \neq \varnothing$. Then by the d.c.c., Σ has a minimal element, say X. Since X is not irreducible, it must have a decomposition $X = X_1 \cup X_2$ into closed proper subsets $X_{1,2} \subsetneq X$. However, $X_{1,2}$ must have a decomposition into irreducible components by minimality of X which would give one for X, contradiction. Hence $\Sigma = \varnothing$.

Step 2. *Uniqueness.* This is easy, see also [Ha, Proposition I.1.5].

□

34. Corollary (Noetherian rings have only finitely many minimal primes). *If $\mathfrak{a}$ is an ideal of a Noetherian ring A, then there are only finitely many primes of A containing $\mathfrak{a}$ and which are minimal with this property. In particular, any Noetherian reduced ring admits an injection $A \hookrightarrow \bigoplus A/\mathfrak{p}$, where the sum is taken over all minimal primes of A, and whose image intersects any summand nontrivially.*

Proof. We apply Proposition 1.33 to the topological space Spec A. We can then decompose $\mathcal{Z}(\mathfrak{a})$ into a finite number of components which correspond to the minimal primes containing $\mathfrak{a}$. Now apply Exercise 0.25. □

35. Remark. In particular, we see that by Corollary 0.17 *any radical ideal* $\mathfrak{a}$ *of a Noetherian ring* is the intersection of a finite number of minimal primes,

$$\mathfrak{a} = \bigcap_{\mathfrak{a}\subset\mathfrak{p} \text{ minimal}} \mathfrak{p} = \bigcap_{i=1}^{r} \mathfrak{p}_i,$$

which in the case of $A = k[x_1, \dots, x_n]$ gives precisely the decomposition into irreducibles: $\mathcal{Z}(\mathfrak{a}) = \mathcal{Z}(\bigcap_i \mathfrak{p}_i) = \bigcup_i \mathcal{Z}(\mathfrak{p}_i)$.

36. Corollary (decomposition into irreducible subsets). *Every algebraic set $X \subset \mathbb{A}^n$ can be (up to ordering) uniquely expressed as a union of affine varieties, no one containing another. These correspond to the* minimal *prime ideals containing $\mathcal{I}(X)$.*

Proof. Instead of appealing to the general topological theory we can give a direct algebraic argument here. Namely, let Σ be the set of ideals $\mathcal{I}(X) \subset k[x_1, \dots, x_n]$ of algebraic sets X which do not have a composition as in Proposition 1.33. The assertion is that $\Sigma = \varnothing$, so oppose to the contrary that $\Sigma \neq \varnothing$. By the Noetherian property of $A[n]$ there is a minimal element of Σ, say $\mathcal{I}(Y)$. Now Y is itself not irreducible (for then it cannot be an element of Σ). Hence $Y = Y_1 \cup Y_2$ for two strictly contained closed subsets of Y. In particular, $Y_i \notin \Sigma$ so they do have a decomposition as in Proposition 1.33. □

37. The rôle of zerodivisors. Let $X \subset \mathbb{A}^n$ be an algebraic set whose coordinate ring $A(X)$ is not an integral domain. In particular, (0) is not a prime ideal. Then we have zerodivisors $f, g \neq 0$ in $A(X)$ such that $fg = 0$. Recall that by Corollary 0.18, $A(X)$ is either reduced, or has more than one minimal prime. To see what these two cases mean geometrically, consider the coordinate rings

(i) $A(\mathcal{Z}(x_1^2)) = k[x_1, x_2]/(x_1^2)$, where $f = g = x_1$;
(ii) $A(\mathcal{Z}(x_1x_2)) = k[x_1, x_2]/(x_1x_2)$, where $f = x_1$ and $g = x_2$.

The first case is the coordinate ring of $\mathcal{Z}(x_1^2)$ = the x_2-axis in k^2. We can think of $k[x_1, x_2]/(x_1^2)$ as the set of polynomials $\{f(x_2) + x_1 f(x_2) \mid f \in k[x]\}$. Put differently, $A(\mathcal{Z}(x_1^2))$ remembers the x_1-derivative $\partial f/\partial x_1(0, x_2)$ of a general $f(x_1, x_2) \in k[x_1, x_2]$ at each point $(0, x_2)$. This is sometimes pictured as a thickened $x_1 = 0$ line (see Figure 1.8). Although this seems to rely on a rather unalgebraic intuition it is really at the heart of scheme theory as we will see below. In the second case, $\bar{x}_1$ and $\bar{x}_2$ generate two prime ideals in $A = A(\mathcal{Z}(x_1x_2)) = k[x_1, x_2]/(x_1x_2)$ for $\big(k[x_1, x_2]/(x_1x_2)\big)/\big((x_1)/(x_1x_2)\big) \cong k[x_1, x_2]/(x_1) = k[x_2]$ which is integral etc. Since $\mathcal{Z}(x_i)$ are just the irreducible components of $\mathcal{Z}(x_1x_2)$ these prime ideals are minimal. In this way, we can see $k[x_1, x_2]/(x_1x_2)$ as a subring of $A/(\bar{x}_1) \oplus A/(\bar{x}_2) \cong k[x_1] \oplus k[x_2]$ with $\bar{x}_1$ and $\bar{x}_2$ mapping to different factors so that their product is zero, cf. Corollary 1.34.

Projective varieties. There a various reasons to study not only affine, but also *projective varieties*. Historically, projective spaces were introduced in order to have a properly working *intersection theory*. For instance, two lines in a plane intersect precisely in one point if they are not parallel. To get a uniform theory where any

two lines intersect one adds to every line the point at infinity (identifying the two ends of the line), then two parallel lines also intersect, namely at "infinity" (think of two rails!) (for a very good explanation of this viewpoint, see also [CLS, Chapter 8.1]).

To define the projective space, consider the natural action of the multiplicative group k^* on $\mathbb{A}_k^{n+1}\backslash\{0\}$ by scalar multiplication. As a set, the **n-dimensional projective space** is

$$\mathbb{P}_k^n := \mathbb{A}^{n+1}\backslash\{0\}/k^*.$$

Equivalently, we can think of $\mathbb{P}^n$ as the set of lines in k^{n+1} passing through the origin.

38. Examples. It is easy to see that

(i) $\mathbb{P}^1_{\mathbb{R}} = S^1$ (see Figure 1.5);
(ii) $\mathbb{P}^2_{\mathbb{R}} = \mathbb{R}^2 \cup \mathbb{P}^1_{\mathbb{R}}$ (see Figure) 1.6).

More generally, $\mathbb{P}^n_k = k^n \cup \mathbb{P}^{n-1}_k$ for any field, see Example 1.39 below.

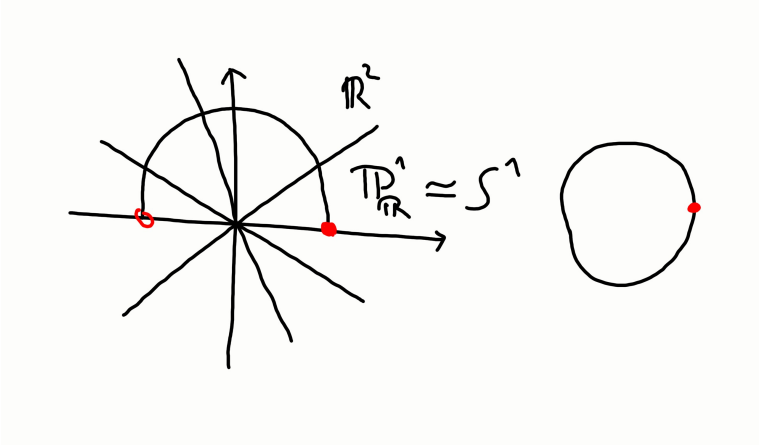

FIGURE 5. The bijection $\mathbb{P}^1_{\mathbb{R}} \cong S^1$

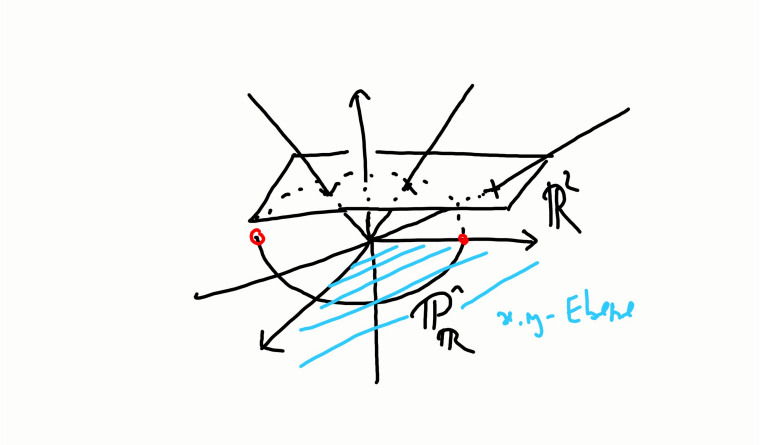

FIGURE 6. The bijection $\mathbb{P}^2_{\mathbb{R}} \cong \mathbb{R}^2 \cup \mathbb{P}^1_{\mathbb{R}}$

For concrete computations it is useful to have a coordinate description. Fix coordinates $x_0, \ldots, x_n$ on $\mathbb{A}^{n+1}$. A line through the origin is then specified by any point $a = (a_0, \ldots, a_n) \in \mathbb{A}^{n+1}\backslash\{0\}$. We denote its equivalence class by $\pi(a_0, \ldots, a_n) = [a_0 : \ldots : a_n]$, that is, $[a_0 : \ldots : a_n] = [\lambda a_0 : \ldots : \lambda a_n]$ for $\lambda \in k^*$, and we think of $\pi : \mathbb{A}^{n+1}\backslash\{0\} \to \mathbb{P}^n$ as a projection map. In particular, $\mathbb{P}^n = \{[a_0 : \ldots : a_n] \mid (a_0, \ldots, a_n) \in \mathbb{A}^{n+1}\backslash\{0\}\}$. If $a = [a_0 : \ldots : a_n] \in \mathbb{P}^n$, then the $n+1$ numbers a_i are called the **homogeneous coordinates** of a.

The geometric objects we consider in $\mathbb{P}^n$ are given by *homogeneous equations*. A polynomial function $f(x_0, \ldots, x_n) = \sum c_{i_0 \ldots i_n} x_0^{i_0} \cdot \cdots \cdot \ldots \cdot \cdots \cdot x_n^{i_n}$ is called **homogeneous of degree** d if all the monomials have the same degree $d = i_0 + \ldots + i_n$. In particular, $f(\lambda x_0, \ldots, \lambda x_n) = \lambda^d f(x_0, \ldots, x_n)$ so that the zero locus

$$\mathcal{Z}_p(f) := \{[a_0 : \ldots : a_n] \in \mathbb{P}^n \mid f(a_0, \ldots, a_n) = 0\}$$

is well-defined.

39. Example. We call the set $H_i = \mathcal{Z}_p(x_i) = \{[a_0 : \ldots : a_n] \in \mathbb{P}^n \mid a_i = 0\}$ the **i-th hyperplane at infinity**. As a set, it is bijective with $\mathbb{P}^{n-1}$. Note that its complement $U_i := H_i^c$ can be identified with k^n via the map

$$\varphi_i : U_i \to k^n, \quad \varphi_i([a_0 : \ldots : a_n]) = (a_0/a_i, \ldots, a_n/a_i)$$

where we omit $a_i/a_i = 1$ (see also Exercise 1.49).

It is ultimately the action of k^* on $k[x_0, \ldots, x_n]$ which singles out the homogeneous elements in $k[x_0, \ldots, x_n]$, or more invariantly, gives rise to a *grading*.

40. Graded rings and modules. A **graded ring** is a ring S together with a direct sum decomposition $S = \bigoplus_{d \geqslant 0} S_d$ as Abelian groups such that

$$S_d S_e \subset S_{d+e} \quad \text{for } d,\, e \geqslant 0.$$

The prime example is the polynomial ring

$$S[n] := k[x_0, \ldots, x_n] = \bigoplus_{d \geqslant 0} k[x_0, \ldots, x_n]_d,$$

where $k[x_0, \ldots, x_n]_d$ is the vector space of homogeneous polynomials of degree d. Of course, $S[n] = A[n+1]$ as a polynomial ring. We write $S[n]$ if we want to emphasise this precise grading into homogeneous polynomials.

41. Remark. If we extend the k^*-action on $\mathbb{A}^{n+1}$ to $A[n+1]$ by regarding $f \in A[n+1]$ as a polynomial function, and set $\lambda(f(x_0, \ldots, x_n)) = f(\lambda x_0, \ldots, \lambda x_n)$, then S_d = vector subspace of S on which k^* acts with weight d, i.e. $f \in S_d \Leftrightarrow \lambda(f) = \lambda^d \cdot f$.

In general, a **homogeneous** element of S is simply an element of one of the groups S_d. We refer to d as the **degree** of the element. In the decomposition $f = f_0 + f_1 + \ldots$, $f_d \in S_d$, f_d is refered to as a **homogeneous component** of f. For future reference, we let

$$S_h = \{f \in S \mid f \text{ homogeneous}\},$$

i.e. S_h is the set of homogeneous elements of S. An ideal $\mathfrak{a}$ is **homogeneous** if and only if it is generated by homogeneous elements. Equivalently, $\mathfrak{a}$ is homogeneous if and only if the homogeneous of any $f \in \mathfrak{a}$ are again in $\mathfrak{a}$, i.e.

$$\mathfrak{a} = \bigoplus_{d \geqslant 0} (\mathfrak{a} \cap S_d).$$

Note that any homogeneous element f of a homogeneous ideal $\mathfrak{a}$ can be uniquely written as $\sum g_i f_i$ where f_i are the homogeneous generators of $\mathfrak{a}$ and g_i are homogeneous elements of S. Further, the sum, the product, the intersection and the radical of homogeneous ideals are again homogeneous. Finally, to test whether a homogeneous ideal is prime it is sufficient to show that for any homogeneous elements f and $g \in \mathfrak{a}$ with $fg \in \mathfrak{a}$ we have $f \in \mathfrak{a}$ or $g \in \mathfrak{a}$. If S is a graded ring, we let

$$S_+ = \bigoplus_{d>0} S_d$$

be the (maximal) ideal consisting of all homogeneous elements of degree greater than zero. For instance if $S = S[n]$, then $S_+ = (x_0, \ldots, x_n)$.

If S is a graded ring, then a **graded S-module** is an S-module M together with a family $(M_d)_{d\geqslant 0}$ of subgroups of M such that

$$M = \bigoplus M_d \quad \text{and} \quad S_e M_d \subset M_{d+e}$$

for all d, $e \geqslant 0$. In particular, and M_d is an S_0-module. An element $x \in M_d$ is called **homogeneous of degree** d; any element $x \in M$ has a decomposition into a finite sum of its **homogeneous components** $\sum x_d$. If M and N are graded S-modules, then a **morphism of graded A-modules** $\varphi : M \to N$ is a degree preserving module morphism, i.e. $\varphi(M_d) \subset N_d$ for all $d \geqslant 0$.

42. Exercise (Noetherian graded rings). *Let S be a graded ring. Are equivalent:*

(i) *S is a Noetherian ring.*
(ii) *S_0 is Noetherian and S is finitely generated as an S_0-algebra.*

Proof. (ii)⇒(i) Since $S \cong S_0[x_1, \ldots, x_n]/\mathfrak{a}$ this follows from Hilbert's basis theorem 0.102 and 0.92.

(i)⇒(ii) Since $S_0 \cong S/S_+$, S_0 is Noetherian. Further, S_+ is an ideal of S, hence finitely generated as an S-module, say by the (homogeneous) elements $x_1, \ldots, x_n$ of S. Let d_i denote their respective degree > 0. Let S' be the subring of S generated by $x_1, \ldots, x_n$ over S_0 (this is the smallest subring containing S_0 and the x_i). In particular, S' is a finitely generated S_0 algebra. We need to show that $S_d \subset S'$ for all d. By induction on d. By design this is true for $d = 0$. Next let $d > 0$ and $x \in S_d \subset S_+$. Then $x = \sum a_i x_i$ with $a_i \in S$. Since $d_i > 0$, the degree of the homogenous components of the a_i must be smaller than $d = \deg(a_i) + d_i > 0$, thus $a_i \in S'$. Therefore, the $a_i = \sum x_i b_i$ with $b_i \in S_0$ so that finally $x \in S'$. □

As noted above, a homogeneous polynomial $f \in k[x_0, \ldots, x_n]_d$ yields a well-defined function $\mathbb{P}^n \to \{0, 1\}$ also denoted by f and which is given by $f([a_0 : \ldots : a_n]) = 0$ if $f(a_0, \ldots, a_n) = 0$ and 1 if not. For any $T \subset S[n]_h$, we set

$$\mathcal{Z}_p(T) := \{a \in \mathbb{P}^n \mid f(a) = 0 \text{ for all } f \in T\}.$$

Of course, T defines also an affine algebraic set $\mathcal{Z}(T) \subset \mathbb{A}^{n+1}$ which is why we write $\mathcal{Z}_p(T)$. The relation between $\mathcal{Z}_p(T)$ and $\mathcal{Z}(T)$ will be discussed in Proposition 1.56. If the context makes it clear that we are working in projective space we sometimes simply write $\mathcal{Z}(T)$. If $\mathfrak{a}$ is a homogeneous ideal, then we set

$$\begin{aligned}\mathcal{Z}_p(\mathfrak{a}) &:= \mathcal{Z}_p(\{f \in \mathfrak{a} \cap k[x_0, \ldots, x_n]_d \mid d \geqslant 0\}) \\ &= \mathcal{Z}_p(\{\text{homogeneous polynomials of } \mathfrak{a}\}).\end{aligned}$$

On the other hand, if $X \subset \mathbb{P}^n$ we define the **homogeneous ideal generated by** X to be

$$\begin{aligned}\mathcal{I}(X) &= (\{f \in k[x_0, \ldots, x_n]_d \mid d \geqslant 0,\ f(a) = 0 \text{ for all } a \in \mathbb{P}^n\}) \\ &= \{\text{ideal generated by homogeneous polynomials } f \text{ with } f|_X = 0\}.\end{aligned}$$

43. Definition (algebraic sets of $\mathbb{P}^n$ and their coordinate ring). A subset X of $\mathbb{P}^n$ is **algebraic** if there exists a set $T \subset S[n]_h$ of homogeneous polynomials such that $X = \mathcal{Z}_p(T)$. The **homogeneous coordinate ring** of X is

$$S(X) = S[n]/\mathcal{I}(X).$$

44. Remark.

(i) The coordinate ring of $\mathbb{P}^n$ is $S[n]$, that is, $k[x_0, \ldots, x_n]$ together with the grading defined by homogneous polynomials. If we forget the grading, then $k[x_0, \ldots, x_n]$ is just the coordinate ring of $\mathbb{A}^{n+1}$ which we continue to write $A[n+1]$.

(ii) Any projective algebraic set can be written as the zero locus of finitely many homogeneous polynomials of *same degree* since $\mathcal{Z}(f) = \mathcal{Z}(x_0^d f, \ldots, x_n^d f)$.

45. Example.

(i) Let $L \subset \mathbb{A}^{n+1}$ be a linear subspace of dimension $k+1$ which is given by the linear equations, say, $x_{k+2} = \ldots = x_{n+1} = 0$. Since these are homogeneous they define a projective variety in $\mathbb{P}^n$, which is the image of L under the projection $\mathbb{A}^{n+1}\backslash\{0\} \to \mathbb{P}^n$. This is a so-called **linear subspace** of $\mathbb{P}^n$. Once we have a notion of morphisms (which we do not have yet for varieties!) it easily follows that L is isomorphic as a *projective variety* to $\mathbb{P}^k$.

(ii) Consider

$$X = \{[a_0 : \ldots : a_3] \mid \operatorname{rank} \begin{pmatrix} a_0 & a_1 & a_2 \\ a_1 & a_2 & a_3 \end{pmatrix} \leqslant 1\}.$$

This is an example of a so-called *determinantal variety*. Namely, $X = \mathcal{Z}_p(x_0x_2 - x_1^2,\ x_0x_3 - x_1x_2,\ x_1x_3 - x_2^2)$ is given by the common zero locus of the three 2×2-minors of the matrix given in the definition of X.

46. Proposition.

(i) *If $\{\mathfrak{a}_i\}$ is a family of homogeneous ideals, then*

$$\bigcap_i \mathcal{Z}_p(\mathfrak{a}_i) = \mathcal{Z}_p(\bigcup_i \mathfrak{a}_i.)$$

(ii) *If $\mathfrak{a}_{1,2}$ are two homogeneous ideals, then*

$$\mathcal{Z}_p(\mathfrak{a}_1) \cup \mathcal{Z}_p(\mathfrak{a}_2) = \mathcal{Z}_p(\mathfrak{a}_1\mathfrak{a}_2).$$

(iii) *The empty space and $\mathbb{P}^n$ are algebraic sets.*

Proof. Similar to Proposition 1.5. □

47. Definition (Zariski topology on $\mathbb{P}^n$). The open sets of the **Zariski topology** are the complements of algebraic sets.

48. Remark. As for affine varieties, we have

(i) $T_1 \subset T_2 \subset S[n]_h \Rightarrow \mathcal{Z}_p(T_1) \supset \mathcal{Z}_p(T_2)$;
(ii) $X_1 \subset X_2 \subset \mathbb{P}^n \Rightarrow \mathcal{I}(X_1) \supset \mathcal{I}(X_2)$;
(iii) for any two subsets $X_1, X_2 \subset \mathbb{P}^n$, $\mathcal{I}(X_1 \cup X_2) = \mathcal{I}(X_1) \cap \mathcal{I}(X_2)$;
(iv) for any subset $X \subset \mathbb{P}^n$, $\mathcal{Z}_p(\mathcal{I}(X)) = \bar{X}$.

The statement corresponding to the Nullstellensatz (i.e. $\mathcal{I} \circ \mathcal{Z}(\mathfrak{a}) = \sqrt{\mathfrak{a}}$) will be discussed in Exercise 1.58

49. Proposition (standard open cover of $\mathbb{P}^n$). *Fix homogeneous coordinates $x_0, \ldots, x_n$ on $\mathbb{P}^n$. For $i = 0, \ldots, n$ we consider the sets $U_i = \{x_i \neq 0\}$ from Example 1.39. Show that*

(i) *the U_i provide an open cover for $\mathbb{P}^n$.*
(ii) *$\varphi_i : U_i \to \mathbb{A}^n$, $\varphi_i([x_0 : \ldots : x_n]) = (x_0/x_i, \ldots, \hat{x}_i, \ldots, x_n/x_i)$ (where $\hat{}$ denotes omission) defines a homeomorphism between U_i and $\mathbb{A}^n$.*

For $T \subset S[n]_h$ try to write $\varphi(\mathcal{Z}_p(T) \cap U_0)$ as $\mathcal{Z}(T')$, $T' \subset A[n]$.

Proof. (i) Since $U_i = \mathcal{Z}_p(x_i)^c$, the sets U_i are open. Further, if $a = [a_0 : \ldots : a_n] \in \mathbb{P}^n$, then there exists at least one $a_j \neq 0$. Hence $a \in U_j$ so that the open sets U_i cover $\mathbb{P}^n$.

(ii) Without loss of generality we assume $i = 0$ and consider the maps $\alpha : S[n]_h \to A[n] = k[y_1, \ldots, y_n]$ defined by $\alpha(f) = f(1, y_1, \ldots, y_n)$ and $\beta : A[n] \to S[n]_h$ defined on polynomials g of degree d by $\beta(g) = x_0^d g(x_1/x_0, \ldots, x_n/x_0)$. The map $\varphi = \varphi_0$ is clearly bijective. We show that it identifies the closed subsets of $X \subset U = U_0$ with those of $\mathbb{A}^n$. Let $\bar{X}$ be the closure of X in $\mathbb{P}^n$. Let $T \subset S[n]_h$ be such that $\bar{X} = \mathcal{Z}_p(T)$ and put $T' = \alpha(T)$. We claim that $\varphi(X) = \varphi_0(\mathcal{Z}_p(T) \cap U) = \mathcal{Z}(T') \subset \mathbb{A}^n$. Indeed, if $[a_0 : \ldots : a_n] \in X$ and $f \in T$ of degree d, then

$$\alpha(f)(\varphi([a_0 : \ldots : a_n])) = f(1, a_1/a_0, \ldots, a_n/a_0) = a_0^d f(a_0, a_1, \ldots, a_n) = 0,$$

hence $\varphi([a_0 : \ldots : a_n]) \in \mathcal{Z}(T')$. On the other hand, if $y = (y_1, \ldots, y_n) \in \mathcal{Z}(T')$, put $a = [1 : y_1 : \ldots : y_n]$. Then $a \in U$ and if $f \in T$, then $f(1, y_1, \ldots, y_n) = \alpha(f)(y_1, \ldots, y_n) = 0$ so that also $a \in \bar{X}$, i.e. $a \in U \cap \bar{X} = X$. Hence φ maps closed sets in U to closed sets to $\mathbb{A}^n$. Conversely, let $Y \subset \mathbb{A}^n$ be closed. Then $Y = \mathcal{Z}(T')$ for some subset T' of $k[y_1, \ldots, y_n]$. We claim that $\varphi^{-1}(Y) = \mathcal{Z}_p(\beta(T')) \cap U_0$ which is closed in U_0. Indeed, let $a = [a_0 : \ldots : a_n] \in \varphi^{-1}(Y)$. Then $a \in U$ and $f(a_1/a_0, \ldots, a_n/a_0) = 0$ for all $f \in T'$. Hence $\beta(f)(a_0, \ldots, a_n) = a_0^d f(a_1/a_0, \ldots, a_n/a_0) = 0$, that is, $\varphi(a) \in \mathcal{Z}(T')$. On the other hand, let $b = [1 : b_1 : \ldots : b_n] \in \mathcal{Z}_p(\beta(T')) \cap U_0$. Then $\varphi(b)$ is defined, and if $f \in T'$, then $f(\varphi(b)) = \beta(f)(1, b_1, \ldots, b_n) = 0$, whence $b \in \varphi^{-1}(Y)$. □

50. Remark. In fact, the maps φ_i from Exercise 1.49 actually identify U_i with $\mathbb{A}^n$ as varieties, see Lemma 1.141.

51. Definition (projective variety). An irreducible algebraic set in $\mathbb{P}^n$ together with the induced subset topology is called a **projective variety**. A **quasi-projective variety** is an open subset of a projective variety.

The following exercise gives an easy way to construct projective varieties from affine ones.

52. Exercise (projective closure of an affine variety). *If $X \subset \mathbb{A}^n$ is an affine variety, and we identify $\mathbb{A}^n$ with U_0 via the map φ_0 of Exercise 1.49, then we call $\bar{X} \subset \mathbb{P}^n$ the* **projective closure** *of X. Using the notation of the previous exercise, show that $\mathcal{I}(\bar{X})$ is the ideal generated by $\beta(\mathcal{I}(X))$.*

Proof. If $g \in \mathcal{I}(X)$, then $\beta(g) = x_0^d g(x_1/x_0, \ldots, x_n/x_0)$ is homogeneous of degree d = degree of g and vanishes on X, hence the closure of X in $\mathbb{P}^n$, i.e. $\bar{X}$, is contained in the closed set $\mathcal{Z}(\beta(g))$. It follows that $\beta(g) \in \mathcal{I}(\bar{X}) \cap S[n]_h$. Conversely, any homogeneous $f \in \mathcal{I}(\bar{X})$ is in the image of β (indeed, taking $g(a_1, \ldots, a_n) = f(1, a_1, \ldots, a_n)$ gives $\beta(g) = f$), whence the result. □

53. Example. Consider the conics $X_1 = \mathcal{Z}(x_2 - x_1^2)$ and $X_2 = \mathcal{Z}(x_1 x_2 - 1)$ in $\mathbb{A}^2$ of which we think as subsets of U_0 in $\mathbb{P}^2$. Under this identification the projective closures of X_1 and X_2 are $\bar{X}_1 = \mathcal{Z}_p(x_0 x_2 - x_1^2)$ and $\bar{X}_2 = \mathcal{Z}_p(x_1 x_2 - x_0^2)$ respectively. Geometrically, we obtain $\bar{X}_1$ and $\bar{X}_2$ by adding the points "at infinity" $[0:0:1]$ respectively $\{[0:1:0], [0:0:1]\}$. Note that the lines defined by $(0,1)$ and $(1,0)$ and $(0,1)$ in $\mathbb{A}^2$ are just the asysmptotics of the curves X_1 and X_2 in $\mathbb{A}^2$. In this way, we can think of $\bar{X}_i \subset \mathbb{P}^2$ as the projective *complexification* of $X_i \subset \mathbb{A}^2$; the projective closure of a parabola or a hyperbola in $\mathbb{A}^2$ gives rise to the same conic (i.e. hypersurface defined by a homogeneous polynomial of degree 2) in $\mathbb{P}^2$.

54. Proposition (irreducible projective algebraic sets). *For $X \subset \mathbb{P}^n$ algebraic are equivalent:*

(i) *X is irreducible;*
(ii) *$\mathcal{I}(X)$ is prime;*
(iii) *$S(X)$ is an integral domain.*

Proof. This follows as in the affine case: If $X = X_1 \cup X_2$, then $\mathcal{I}(X) = \mathcal{I}(X_1) \cap \mathcal{I}(X_2)$. Hence, if $\mathcal{I}(X)$ is prime, then either $\mathcal{I}(X) = \mathcal{I}(X_1)$ or $\mathcal{I}(X_2)$, whence $X = X_1$ or X_2. Conversely, if $\mathcal{I}(X)$ is not prime, then there exists a product $f \cdot g \in \mathcal{I}(X)$ with $f, g \notin \mathcal{I}(X)$. Then $X = (X \cap \mathcal{Z}_p(f)) \cup (X \cap \mathcal{Z}_p(g))$ gives a decomposition so that X is reducible. □

Another way to make contact with affine varieties is the *cone construction*.

55. Definition.

(i) A nonempty set $X \subset \mathbb{A}^{n+1}$ is called a **cone** if it is invariant under the k^*-action on $\mathbb{A}^{n+1}$, that is,

$$(a_0, \ldots, a_n) \in X \Rightarrow (\lambda a_0, \ldots, \lambda a_n) \in X$$

for all $\lambda \in k^*$.

(ii) For a nonempty set $X \subset \mathbb{P}^n$ the cone

$$C(X) := \{(x_0, \ldots, x_n) | [x_0 : \ldots : x_n] \in X\} \cup \{0\} \subset \mathbb{A}^{n+1}$$

is called the **cone over** X (see Figure 1.7).

56. Proposition (ideals of projective algebraic sets and their cones).

(i) *$X \subset \mathbb{A}^{n+1}$ is a cone $\Leftrightarrow$ $\mathcal{I}(X) \subset A[n+1] = k[x_0, \ldots, x_n]$ is homogeneous.*
(ii) *Let $\mathfrak{a} \subset S[n]$ be a homogeneous ideal. If $X = \mathcal{Z}_p(\mathfrak{a}) \subset \mathbb{P}^n$, then its cone is given by $C(X) = \mathcal{Z}(\mathfrak{a}) \subset \mathbb{A}^{n+1}$. In particular, $C(X)$ is indeed a cone in the sense of Definition 1.55 (i).*
(iii) *Let $X \subset \mathbb{P}^n$ be a projective algebraic set with homogeneous ideal $\mathcal{I}(X) \subset S[n]$, then $\mathcal{I}(C(X)) = \mathcal{I}(X)$ as an ideal of $A[n+1]$. In particular, X is irreducible $\Leftrightarrow$ $C(X)$ is irreducible.*

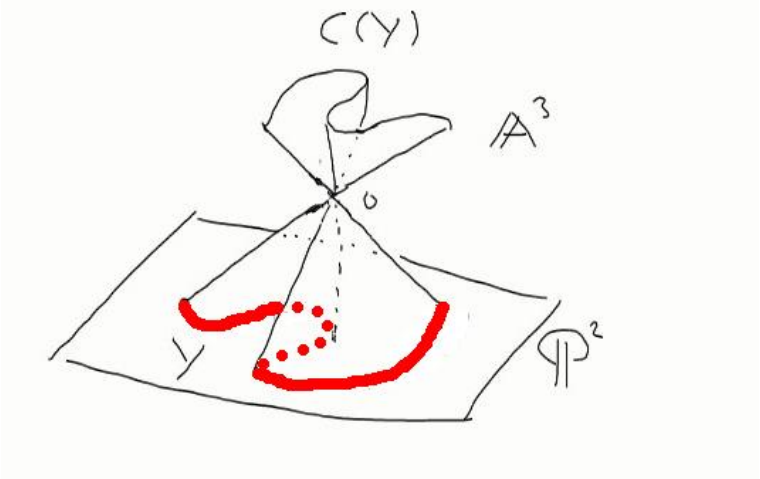

FIGURE 7. The cone over Y

Hence, there is a $1-1$ *correspondence between projective algebraic sets in* $\mathbb{P}^n$ *and affine cones in* $\mathbb{A}^{n+1}$.

Proof. (i) If X is a cone, $f \in \mathcal{I}(X)$, and $a \in X$, then $f(\lambda a) = \sum f_d(\lambda a) = \sum \lambda^d f(a) = 0$. Hence $f_d(a) = 0$ since k is infinite, so $f_d \in \mathcal{I}(X)$. The converse is obvious.

(ii) The inclusion $\mathcal{Z}(\mathfrak{a}) \subset C(X)$ is clear. So let $a = (a_0, \ldots, a_n) \in C(X)$. Then $\pi(a) = [a_0 : \ldots : a_n] \in X$ so that $f(a_0, \ldots, a_n) = 0$ for all $f \in \mathfrak{a}$. Hence $C(X) \subset \mathcal{Z}(\mathfrak{a})$. In particular, $\mathcal{I}(X) = \sqrt{\mathfrak{a}}$ is homogeneous since $\mathfrak{a}$ is homegenous. Hence $C(X)$ is a cone by (i).

(iii) Since $C(X)$ is a cone, $\mathcal{I}(C(X))$ is homogeneous, and a homogeneous polynomial $f \in \mathcal{I}(C(X))$ if and only if $f \in \mathcal{I}(X)$. □

57. Example. We have $C(\mathbb{P}^n) = \mathbb{A}^{n+1}$. In particular, $\mathcal{I}(\mathbb{P}^n) = \mathcal{I}(\mathbb{A}^{n+1}) = (0)$ so that $\mathbb{P}^n$ is irreducible.

58. Exercise (projective Nullstellensatz). *For any homogeneous ideal* $\mathfrak{a} \subset S[n]$ *such that* $\mathcal{Z}_p(\mathfrak{a}) \neq \varnothing$ *we have* $\mathcal{I}(\mathcal{Z}(\mathfrak{a})) = \sqrt{\mathfrak{a}}$. *In particular, there is a* $1-1$ *inclusion reversing correspondence between algebraic sets in* $\mathbb{P}^n$ *and homogeneous radical ideals of* S *not equal to* S_+.

Proof. Let $X = \mathcal{Z}_p(\mathfrak{a}) \subset \mathbb{P}^n$. By Proposition 1.56 and the usual Nullstellensatz,

$$\sqrt{\mathfrak{a}} = \mathcal{I}(\mathcal{Z}(\mathfrak{a})) = \mathcal{I}(C(X)) = \mathcal{I}(X) = \mathcal{I}(\mathcal{Z}_p(\mathfrak{a})).$$

□

59. Exercise. *For a homogeneous ideal* $\mathfrak{a} \subset S[n]$ *are equivalent:*

(i) $\mathcal{Z}_p(\mathfrak{a}) = \varnothing$ *in* $\mathbb{P}^n$;
(ii) $\sqrt{\mathfrak{a}} =$ *either* $S[n]$ *or* $S_+ = \bigoplus_{d>0} S_d$;
(iii) $S_d \subset \mathfrak{a}$ *for some* $d > 0$.

Hint: For (i)⇒(ii): Consider the cone of $\mathcal{Z}_p(\mathfrak{a})$.

Proof. (i)⇒(ii) If $\mathcal{Z}_p(\mathfrak{a}) = \varnothing$ in $\mathbb{P}^n$, then its cone in $\mathbb{A}^{n+1}$ is either $\mathcal{Z}(\mathfrak{a}) = \varnothing$, i.e. $\mathfrak{a} = (1)$, or $\mathcal{Z}(\mathfrak{a}) = \{0\}$, i.e. $\mathfrak{a} = (x_0, \ldots, x_n)$. Otherwise, there would be a point $0 \neq a \in \mathcal{Z}(\mathfrak{a})$ and by homogeneity, $\mathcal{Z}(\mathfrak{a})$ would contain the entire line $\langle a \rangle$ spanned by a. In the first case, $\mathcal{I}(\mathcal{Z}(\mathfrak{a})) = \sqrt{(1)} = S[n]$ while $\mathcal{I}(\mathcal{Z}(\mathfrak{a})) = \sqrt{(x_0, \ldots, x_n)} = S_+$ in the second.

(ii)⇒(iii) In both cases $\sqrt{\mathfrak{a}}$ contains the monomials x_i so that $x_i^m \in \mathfrak{a}$ for some m. In particular, $S_{m(n+1)} \subset \mathfrak{a}$ as any monomial of degree $m(n+1)$ must have at least one factor of the form x_i^m.

(iii)⇒(i) Since $x_i^d \in S_d \subset \mathfrak{a}$, $\mathcal{Z}_p(\mathfrak{a}) \subset \bigcap_{i=0}^n \mathcal{Z}_p(x_i^d) = \varnothing$. □

60. Remark. Because of (ii) in the previous exercises, the maximal ideal S_+ corresponds to the empty set and is therefore sometimes called the **irrelevant ideal**.

61. Definition (variety). A **variety (over k)** is any affine, quasi-affine, projective or quasi-projective variety. A **subvariety** of a variety X is an irreducible locally closed subset which inherits from X the structure of a quasi-affine or -projective variety.

Varieties will be the *objects* of our category. Next we need the *morphisms*; before we can define these, we need to discuss functions on varieties.

62. Remark. Some authors consider a more general notion of variety obtained by glueing affine varieties (cf. for instance [Ga]) via isomorphisms, similar to the notion of a differentiable manifold obtained by glueing open sets of $\mathbb{R}^n$ via diffeomorphisms (the isomorphisms in the catgeory of differentiable manifolds). We call this more general object an *abstract variety* which will arise as the special case of a still more general object, namely a *scheme*, to be discussed in Section 5.

63. Exercise (varieties covered by Noetherian spaces). *If X is a variety which is covered by finitely many Noetherian subsets, then X is itself Noetherian. Conclude that $\mathbb{P}^n$ is a Noetherian topological space, and that any algebraic subset of $\mathbb{P}^n$ can be written uniquely as a finite union of irreducible components, i.e. closed irreducible sets, no one containing another.*

Proof. Assume that $X_1 \supset X_2 \supset \ldots$ is an infinite chain of closed subsets of X. Since the U_i are Noetherian, the sequence $X_j \cap U_i$ must become stationary for all i, that is, there exists an integer N such that $X_j \cap U_i = X_l \cap U_i$ for all j, $l \geqslant N$ and all i. Hence $X_j = \bigcup_i (X_j \cap U_i) = X_l$ for all j, $l \geqslant N$, i.e. the sequence becomes stationary. For instance, the open cover of $\mathbb{P}^n$ provided by Proposition 1.49 immediately implies that $\mathbb{P}^n$ is Noetherian (of course, we could also argue by the associated chain of ideals $\mathcal{I}(X_i)$ in the Noetherian ring $S[n]$). The decomposability of algebraic sets follows from Proposition 1.33. □

1.2. **Regular functions and sheaves.** A **function** f **on** X is a map $X \to \mathbb{A}^1$. We usually abuse notation and simply write $X \to k$ though we will think of k as affine space endowed with its Zariski topology (in the case of $k = \mathbb{R}$ or $\mathbb{C}$, another natural choice would be the Euclidean topology, for instance if we considered C^∞ or holomorphic functions) We recall that k is algebraically closed, hence infinite, so we can freely identify polynomials in n variables with polynomial functions $\mathbb{A}^n \to k$ and thus with functions on X by restriction.

64. Definition (regular functions).

(i) Let X be a quasi-affine variety. A function $f : X \to k$ is **regular at** $a \in X$ if there is an open neighbourhood V of a in X, and polynomials g, $h \in k[x_1, \ldots, x_n]$ such that h is nowhere zero on V, and $f = g/h$ on V. If f is regular at any point $a \in U$ of an open set of X, then we call f **regular on** U.

(ii) Let X be a quasi-projective variety. A function $f : X \to k$ is **regular at** $p \in X$ if there is an open neighbourhood V of a in X, and polynomials g, $h \in S(n) = k[x_0, \ldots, x_n]$ of the *same* degree, such that h is nowhere zero on V, and $f = g/h$ on V. If f is regular at any point $a \in U$ of an open set of X, then we call f **regular on** U.

(iii) If X is a variety, we denote by $\mathcal{O}_X(U)$ or simply $\mathcal{O}(U)$ the regular functions on the open subset U of X. Note that because regularity of a function was defined for quasi-affine resp. quasi-projective varieties, $\mathcal{O}_X(U)$ makes actually sense.

65. Remark.

(i) The degree assumption in the quasi-projective case ensures that the quotient f/g is indeed a well-defined function (while f and g are not unless they vanish).

(ii) From the definition it follows that $\mathcal{O}_X(U)$ forms a ring.

(iii) We actually have $\mathcal{O}_X(X) = A(X)$ as we will prove in Proposition 1.93 below. Of course, the inclusion $\supset$ is obvious.

66. Proposition (continuity of regular functions). *A regular function is continuous.*

Proof. We consider the case of a quasi-affine variety; the projective case works similarly. We show that the preimage of a closed set under a regular function f is again closed. Since closed sets in $\mathbb{A}^1$ are finite collections of points it is enough to show that $f^{-1}(a)$ is closed for any $a \in \mathbb{A}^1$. Note that a subset Z of a topological space X is closed $\Leftrightarrow$ Z can be covered by open sets U such that $Z \cap U$ is closed in U for each U. By definition of regularity, we can cover X by open sets U such that $f = g/h$ with h nowhere vanishing on U. Then $f^{-1}(a) \cap U = \{p \in U \mid g(p)/h(p) = a\}$. Since $g(p)/h(p) = a \Leftrightarrow (g - ah)(p) = 0$ we have $f^{-1}(a) \cap U = \mathcal{Z}(g - ap) \cap U$ which is closed with respect to the subspace topology of U. Hence $f^{-1}(a)$ is closed in X. □

Since nonempty open subsets of irreducible spaces are dense, cf. Proposition 1.13, we immediately obtain the following

67. Corollary. *A regular function on a variety is determined by its restriction to any nonempty open subset.*

Proof. It is enough to show that $f|_U \equiv 0$ on a nonempty open subset U of X implies $f \equiv 0$ on X. Indeed, $U \subset f^{-1}(0)$. Since f is regular, thus continuous, the latter set is closed and thus contains the closure $\bar{U}$ of U. But since U is dense, $\bar{U} = X$. □

68. Definition (ring of regular functions at a point and function fields). Let X be a variety.

(i) For $a \in X$ we define the **local ring of a on X**, $\mathcal{O}_{X,a}$ or simply $\mathcal{O}_a$, to be the *ring of germs* of regular functions on X near a. Put differently, elements of $\mathcal{O}_{X,a}$ are equivalence classes $[U, \varphi]$ where $\varnothing \neq U \subset X$ is open and contains a, and $f \in \mathcal{O}_X(U)$. We have $[U, \varphi] = [V, \psi]$ if $\varphi \equiv \psi$ on $U \cap V$.

(ii) The **function field** $K(X)$ consists of elements $[U, \varphi]$ of $\varnothing \neq U \subset X$ open and $\varphi \in \mathcal{O}_X(U)$, where we identify $[U, \varphi]$ with $[V, \psi]$ if $\varphi \equiv \psi$ on $U \cap V$. Its elements are called **rational functions**.

69. Remark.

(i) Since X is irreducible, any two nonempty open sets have a nonempty intersection, so that we can define addition and multiplication in a natural way: $[U, f] + [V, g] = [U \cap V, f + g]$ etc., so that $\mathcal{O}_{X,a}$ is indeed a ring. By Proposition 0.11, $\mathcal{O}_a$ is a local ring, for the set of non-units $\mathfrak{m}_a = \{[U, f] \mid f(a) = 0\}$ is an ideal (note that $f \cdot g(a) = 1$ entails that both f and g do not vanish in a and thus not in a neighbourhood of a). The residue field is $\mathcal{O}_a/\mathfrak{m}_a \cong k$, where the isomorphism is given by evaluation of an equivalence class $[U, f]$ at a.

(ii) $K(X)$ is indeed a field. If $[U, f] \neq [X, 0]$, then we can restrict f to the nonempty open set $U^* = U \backslash (f^{-1}(0))^c$ where it never vanishes, and $[U, f] = [U^*, f]$ is invertible with inverse $[U^*, 1/f]$.

(iii) For $a \in U$ we have a natural sequence of injective maps

$$\mathcal{O}_X(U) \hookrightarrow \mathcal{O}_{X,a} \hookrightarrow K(X).$$

The first inclusion assigns to f the equivalence class $[U, f]$. In fact, we can think of a regular function $f : U \to k$ as a function whose germ at any point $x \in X$ can be represented by a rational function, i.e. as a fraction pf polynomial functions. The second inclusion assigns to a germ $[U, f]$ the corresponding equivalence class in $K(X)$. We therefore usually think of $\mathcal{O}_X(U)$ and $\mathcal{O}_{X,a}$ as subrings of $K(X)$.

70. Exercise (local ring only depends on a neighbourhood). *Let X be a variety and $V \subset X$ be an open subset. Show that $\mathcal{O}_V(U)$ (considering V as a quasi-affine or -projective variety) equals $\mathcal{O}_X(U)$. Conclude that $\mathcal{O}_{X,a} = \mathcal{O}_{V,a}$ for any open subset $V \subset X$ containing a.*

Proof. We assume that $X \subset \mathbb{A}^n$ is affine, the projective case being following along the same lines. Since $V \subset \mathbb{A}^n$ is a quasi-affine variety, $f \in \mathcal{O}_V(U)$ if and only if f is locally of the form h_1/h_2 with $h_i \in A[n]$. Since U is open in V if and only if U is open in X, we clearly have $\mathcal{O}_V(U) = \mathcal{O}_X(U)$. Next consider the map $\mathcal{O}_{X,a} \to \mathcal{O}_{U,a}$ given by $[U, f] \mapsto [U \cap V, f|_{U \cap V}]$. This map is clearly injective and well-defined, for the restriction of F to any open set is again regular. Furthermore, it is surjective for any $[W, f] \in \mathcal{O}_{V,a}$ is clearly also in $\mathcal{O}_{X,a}$, W being open in X as well. □

Sheaves. To understand the topological nature of regular functions we give a basic introduction to sheaf theory which we will develop more completely in subsequent chapters.

71. Definition (presheaves). Let X be a topological space. A **presheaf $\mathcal{F}$ of Abelian groups on** X consists of the following data:

(i) For every open subset $U \subset X$, an Abelian group $\mathcal{F}(U)$;
(ii) for every inclusion $V \subset U$ of open subsets of X, a morphism of Abelian groups $\rho_{UV} : \mathcal{F}(U) \to \mathcal{F}(V)$ subject to the conditions
- $\mathcal{F}(\emptyset) =$ the trivial group $\{0\}$;
- $\rho_{UU} : \mathcal{F}(U) \to \mathcal{F}(U)$ is the identity map, and
- if $W \subset V \subset U$ are three open subsets, then $\rho_{UW} = \rho_{VW} \circ \rho_{UV}$.

72. Remark. More generally, we can consider sheaves of rings, modules or any other object in some fixed category $\mathcal{C}$. In fact, if we let $\mathbf{TOP}_X$ be the category consisting of open subsets of X as objects and inclusions as morphisms (cf. Example A.3, then a presheaf defines a contravariant functor $\mathbf{TOP}_X \to \mathcal{C}$. For instance, we can consider a differentiable manifold/complex manifold/variety X together with the sheaf $\mathcal{O}_X$ of rings which assigns to an open $U \subset X$ the ring of C^∞/holomorphic/regular functions on U. In this way, $(X, \mathcal{O}_X)$ becomes a *ringed space*, i.e. a topological space X together with a sheaf of rings $\mathcal{O}_X$ of (continuous) functions which is the starting point for any geometric theory in contrast to topology.

73. Examples.

(i) Let X be a variety. For each open set $U \subset X$, let $\mathcal{O}(U)$ be the ring of regular functions $U \to k$, and ρ_{UV} restriction of V in the usual sense.
(ii) Similarly, we can define the presheaf of continuous/differentiable/holomorphic functions on any topological/differentiable/complex manifold.
(iii) Let M be a topological/differentiable/complex manifold and $E \to M$ a topologcial/differentiable/holomorphic vector bundle. Then $\mathcal{E}(U) := \Gamma(U, E)$ is the associated presheaf of sections.

In order to stress the analogy with functions and sections of vector bundles, the group $\mathcal{F}(U)$ is also refered to as the **sections over** U. Consequently, we sometimes use the notation $\Gamma(U, \mathcal{F})$ nadwrite $s|_V$ instead of $\rho_{UV}(s)$.

Next we define sheaves which are roughly speaking presheaves determined by local data.

74. Definition (sheaves). A presheaf $\mathcal{F}$ on X is called a **sheaf** if for any open covering $\{V_i\}$ of an open subset U of X, the following conditions hold:

(i) If $s \in \mathcal{F}(U)$ is such that $s|_{V_i} = 0 \in \mathcal{F}(V_i)$ for all i, then $s = 0$ in $\mathcal{F}(U)$ ("s is determined by restriction to open subsets", "local injectivity").
(ii) If there exists $s_i \in \mathcal{F}(V_i)$ for each i such that $s_i|_{V_i \cap V_j} = s_j|_{V_i \cap V_j}$, then there exists $s \in \mathcal{F}(U)$ such that $s|_{V_i} = s_i$ ("local compatible sections can be glued together", "local surjectivity").

75. Examples.

(i) All the presheaves considered in the previous example are in fact sheaves. For instance, consider $\mathcal{O}$ the **sheaf of regular functions** on a variety X. A regular function on U which is locally 0 must be 0 on all of U. Further, a function $U \to k$ which is locally regular is by definition regular. The same applies to the the presheaf of continuous/differentiable/holomorphic functions.

(ii) Let X be a topological space and G an Abelian group. We define the **constant sheaf $\mathcal{G}$ on** X as follows. Endow G with the discrete topology, and let $\mathcal{G}(U)$ be the continuous functions $U \to G$. Then for any connected set, $\mathcal{G}(U) = G$, whence the name. If U is an open set whose connected components are open, then $\mathcal{G}(U)$ is a direct product of copies of G. Note that if we defined a presheaf by $\mathbf{G}(U) = G$ for *any* nonempty open subset of X, then $\mathbf{G}$ is *not* a sheaf. Indeed, take two disjoint nonempty open subsets U and V. Then if $s \in \mathbf{G}(U) = G$ and $t \in \mathbf{G}(V) = G$ are not equal, they do not glue to an element in $\mathbf{G}(U \cup V)$, yet they are compatible for the condition on the intersection is vacuous.

(iii) If $\varphi : \mathcal{F} \to \mathcal{G}$ is a morphism of sheaves, then the presheaf given by the Abelian groups $\ker \phi(U) = \ker \varphi_U \subset \mathcal{F}(U)$ with restriction maps induced by restricting the restriction maps from $\mathcal{F}$ to $\ker \phi$, is actually a sheaf, the so-called *kernel sheaf of* φ. If $\ker \varphi = 0$, we say that φ is **injective**.

76. Remark. The naive definition $\operatorname{im} \phi(U) := \operatorname{im} \phi_U$ of the "image sheaf" of φ only yields a presheaf. We will give a proper definition of the image sheaf further below when we consider the "sheafification" of presheaves. For the definition of a surjective morphism, see Exercise 1.85 below.

77. Definition (morphism of sheaves). If $\mathcal{F}$ and $\mathcal{G}$ are (pre)sheaves on X, then a **morphism $\varphi : \mathcal{F} \to \mathcal{G}$ of (pre)sheaves** is a group morphism $\varphi_U : \mathcal{F}(U) \to \mathcal{G}(U)$ which commutes with the restriction maps of $\mathcal{F}$ and $\mathcal{G}$, i.e. $\varphi_V \circ \rho^{\mathcal{F}}_{UV} = \rho^{\mathcal{G}}_{UV} \circ \varphi_U$. An **isomorphism** is a morphism with two-sided inverse.

78. Example. Let $\mathcal{O}$ denote the sheaf of holomorphic functions on $\mathbb{C}$ with the usual group structure by addition of functions, and $\mathcal{O}$ the sheaf of invertible holomorphic functions with its multiplicative group structure. Then $f \in \mathcal{O}(U) \mapsto e^f := \exp(2\pi i f) \in \mathcal{O}^*(U)$ is a sheaf morphism, for $e^{(f+g)} = e^f \cdot e^g$.

79. Definition (stalk of a sheaf). If $\mathcal{F}$ is a presheaf on X, and $x \in X$, we define the **stalk $\mathcal{F}_x$ of $\mathcal{F}$ at** x to be the direct limit

$$\varinjlim_{U \ni x} \mathcal{F}(U) = \bigsqcup_{U \ni x} \mathcal{F}(U) / \sim$$

where $s \in \mathcal{F}(U)$ and $t \in \mathcal{F}(V)$ are equivalent if there exists an open subset $W \subset U \cap V$ such that $\rho_{UW}(s) = \rho_{VW}(t)$. Put differently, an element in $\mathcal{F}_x$ is given by an equivalence $[U, s]$ where $s \in \mathcal{F}(U)$ and where $[U, s] = [V, t]$ if there exists an open set W of $U \cap V$ containing x such that $s|_W = t|_W$. In this way we may think of the stalk as the group of germs of sections at x. If $\varphi : \mathcal{F} \to \mathcal{G}$ is a morphism of sheaves, then for $x \in X$ we obtain the induced group morphism $\varphi_x : \mathcal{F}_x \to \mathcal{G}_x$ defined by $\varphi_x[U, f] = [U, \varphi_U(f)]$.

80. Example. The local ring $\mathcal{O}_x$ is just the stalk of the sheaf of regular functions.

81. Exercise. *Let $\varphi : \mathcal{F} \to \mathcal{G}$ a morphism between sheaves on X. Show that*

(i) *for each $x \in X$, $(\ker \varphi)_x = \ker(\varphi_x)$;*

(ii) $\ker\varphi$ *is indeed a sheaf.*

Proof. (i) We have $(\ker\varphi)_x = \{[U,f] \mid x \in U,\ f \in \ker\varphi_U\}$ and $\ker(\varphi_x) = \{[U,f] \mid x \in U,\ \varphi_x[U,f] := [U,\varphi_U(f)] = 0 \in \mathcal{G}_x\}$. The map which assigns $[U,f] \in (\ker\varphi)_x$ to $[U,f] \in \ker(\varphi_x)$ is therefore a well-defined injection. Conversely, if $[U,f] \in \ker(\varphi_x)$, then there exists an open neighbourhood W of x in U such that $\varphi_U(f)|_W = \varphi_W(f|_W) = 0$, that is, $[W, f|_W] \in (\ker\varphi)_x$. Since $[W,f|_W] = [U,f]$ this assignement is surjective.

(ii) Since $\ker\varphi_U \subset \mathcal{F}(U)$, and $\mathcal{F}$ is a sheaf by assumption, the injectivity property of sheaves holds trivially. For surjectivity, let $s_i \in \ker\varphi_{U_i}$ such that $s_i|_{U_i\cap U_j} = s_j|_{U_i\cap U_j}$, where U_i is an open covering of some open set U. Since $\mathcal{F}$ is a sheaf, there exists $s \in \mathcal{F}(U)$ such that $s|_{U_i} = s_i$. Since φ is a morphism it commutes with restriction, whence $\varphi_U(s)|_{U_i} = \varphi_{U_i}(s|_{U_i}) = 0$. By the injectivity property, $\varphi_U(s) = 0$ in $\mathcal{G}(U)$, whence $s \in \ker\varphi_U$. □

82. Proposition. *Let $\varphi : \mathcal{F} \to \mathcal{G}$ be a morphism of sheaves. Then φ is an isomorphism $\Leftrightarrow$ φ_x is an isomorphism for every $x \in X$.*

Proof. $\Rightarrow$) Clear.

$\Leftarrow$) We show that $\varphi_U : \mathcal{F}(U) \to \mathcal{G}(U)$ is a (group) isomorphism for any open subset U of X. Then $\psi : \mathcal{G} \to \mathcal{F}$ defined by $\psi_U = \varphi_U^{-1}$ is an inverse to φ.

Step 1. *φ_U is injective.* Let $s \in \mathcal{F}(U)$ and assume that $\varphi_U(s) = 0$. This means that $\varphi_x[U,s] = [U,\varphi(s)] = 0$ for all $x \in U$. But φ_x is injective, whence $0 = [U,s] \in \mathcal{F}_x$ for all $x \in U$. By definition, this means that for any $x \in U$ there exists an open neighbourhood of x such that $s|_U = 0$, whence $s = 0$ by the injectivity property.

Step 2. *φ_U is surjective.* Suppose we have a section $t \in \mathcal{G}(U)$. For each $x \in U$, surjectivity at stalk level implies that there exists $s_x \in \mathcal{F}_x$ such that $\varphi(s_x) = t_x$. Let s_x be represented by a local section $s(x)$ defined near x, say on $V(x)$. Restricting $V(x)$ if necessary we may assume that $\varphi(s(x)) = t|_{V(x)}$. If $y \in V(x) \cap V(\tilde{x})$ then $\varphi(s(x)) = \varphi(s(\tilde{x}))$ near y. By injectivity proved in the first step, $s(x)|_{V(x)\cap V(\tilde{x})} = s(\tilde{x})|_{V(x)\cap V(\tilde{x})}$. The glueing property of sheaves entails the existence of $s \in \mathcal{F}(U)$ such that $s|_{V(x)} = s(x)$, whence $\varphi(s)|_{V(x)} = t|_{V(x)}$. The injectivity property of sheaves finally implies $\varphi(s) = t$.

□

83. Remark. We say that a morphism of sheaves $\varphi : \mathcal{F} \to \mathcal{G}$ is **injective** if $\ker\varphi = 0$. Then the previous proof shows the equivalence between

(i) *φ is injective, i.e.* $\ker\varphi = 0$*;*
(ii) *$\varphi_U : \mathcal{F}(U) \to \mathcal{G}(U)$ is injective for all open subsets U of X.*
(iii) *$\varphi_x : \mathcal{F}_x \to \mathcal{G}_x$ is injective for all $x \in X$.*

The case of surjectivity is more subtle (we use injectivity in Step 2, see also Exercise 1.85). This is at the origin of the cohomology of sheaves which we consider later.

The previous proposition is false for presheaves and highlights the local nature of sheaves in contrast to presheaves.

84. Example. For $U \subset \mathbb{C}$ open let $\mathcal{O}(U)$ resp. $\mathcal{O}^*(U)$ denote the sheaf of holomorphic resp. invertible holomorphic functions on U. Further, let $\mathbb{Z}(U) = \mathbb{Z}$

denote the constant *presheaf* (U is an abritrary open set, cf. Example (iii) in 1.75). Define the presheaf $\mathcal{F}(U) := \mathcal{O}(U)/\mathbb{Z}(U)$ and consider the morphism $\varphi : \mathcal{F} \to \mathcal{O}^*$ induced by the exponential map $\exp(2\pi i)$. For U non simply connected φ_U is not necessarily surjective. However, at the level of stalks, $\varphi_x : \mathcal{F}_x \to \mathcal{O}_x^*$ will be an isomorphism for we can always choose a representative defined on a simply connected open neighbourhood.

85. Exercise (Surjective sheaf morphisms). *Let $\varphi : \mathcal{F} \to \mathcal{G}$ be a morphism of sheaves. We say that φ is* **surjective** *if and only if for every open set $U \subset X$ and $t \in \mathcal{G}(U)$ there exists a covering $\{U_i\}$ of U and elements $s_i \in \mathcal{F}(U_i)$ such that $\varphi_{U_i}(s_i) = t|_{U_i}$ for all i. (You might want to think of this as a "local" surjectivity.) Show that*

(i) *φ is surjective $\Leftrightarrow$ φ_x is surjective for all $x \in X$.*
(ii) *φ is an isomorphism $\Leftrightarrow$ φ is injective and surjective.*
(iii) *Give an example of a surjective morphism and an open set U such that $\varphi_U : \mathcal{F}(U) \to \mathcal{G}(U)$ is not surjective.*

Proof. (i) Consider the map $\varphi_x : \mathcal{F}_x \to \mathcal{G}_x$ and $[U, t] \in \mathcal{G}_x$. Then φ_x is a surjective group morphism $\Leftrightarrow$ there exists an open neighbourhood W of x in U such that $[W, t|_W] = [W, \varphi_W(s)]$ for some $s \in \mathcal{F}(W)$.

$\Rightarrow$) If $[U, t] \in \mathcal{G}_x$ is given, choose a covering of U as in the definition of surjectivity. Let $W = U_i$ with $x \in U_i$. By assumption, there exists $s = s_i$ such that $[W, \varphi_W(s)] = [W, t|_W]$. Hence, φ_x is surjective.

$\Leftarrow$) Given $t \in \mathcal{G}(U)$ we can find for any $x \in U$ open neighbourhoods U_x of x in U, as well as sections $s_x \in \mathcal{F}(U_x)$ such that $[U_x, t|_{U_x}] = [U_x, \varphi_{U_x}(s_x)]$.

(ii) By Proposition 1.82 it follows that φ is an isomorphism if and only if φ_x is an isomorphism, i.e. injective and surjective, for all $x \in X$. But by the Remark 1.83 and (i) this is equivalent to φ being injective and surjective.

(iii) As discussed in the previous example, the map $\exp : \mathcal{O} \to \mathcal{O}^*$ for $\mathcal{O} =$ the sheaf of holomorphic functions on $\mathbb{C}$, is stalkwise surjective, for $\exp : \mathcal{O}(U) \to \mathcal{O}^*(U)$ is surjective if U is simply-connected, and every $x \in \mathbb{C}$ admits a basis of simply-connected neighbourhoods, i.e. any open neighbourhood of x admits an open simply-connected subset containing x. However, exp is not surjective for general U. □

1.3. **Localisation.** We now come to an important technique in commutative algebra, namely *localisation*. Algebraically, this reduces many problems to the case of local rings. Geometrically, it corresponds to considering functions on an open subset or close to a given point. In a way this is an algebraic counterpart to the topological side of regular functions via sheaves. As a motivating example we prove that the local ring at $a \in X$, the germ $\mathcal{O}_{X,a}$, can be realised geometrically as follows.

86. Proposition (algebraic description of $\mathcal{O}_{X,a}$). *Let X be an affine variety. Then*

$$\mathcal{O}_{X,a} = A(X)_{\mathfrak{m}_a} := \{\frac{f}{g} \mid f, g \in A(X) \text{ and } g \notin \mathfrak{m}_a\},$$

where $\mathfrak{m}_a$ denotes the maximal ideal of $A(X)$ given by $\{g \in A(X) \mid g(a) = 0\}$.

Proof. If f/g such that $g(a) \neq 0$ we can associate the germ $[X\backslash g^{-1}(0), f/g] \in \mathcal{O}_{X.a}$ as $f/g \in \mathcal{O}_X(X\backslash g^{-1}(0))$. Since X is a variety, a regular function is determined by any of its germes. Therefore, this map is injective. On the other hand, this map is surjective by the definition of a regular function. □

The ring $A(X)_{\mathfrak{m}_a}$ is called the **localisation of** $A(X)$ **at** $\mathfrak{m}_a$. We now study this concept in detail.

87. Definition (ring of fractions). Let A be a ring and $S \subset A$ be a multiplicative subset (recall that this means that $1 \in S$ and $a, b \in S$ implies $ab \in S$). On $A \times S$ we say that two elements are equivalent,

$$(a, s) \sim (b, t) \Leftrightarrow \text{there exists } u \in S \text{ such that } u(at - bs) = 0. \tag{2}$$

The **ring of fractions** is

$$S^{-1}A = (A \times S)/\sim .$$

If a/s denotes the equivalence class of (a, s), then the ring operations are given by

$$\frac{a}{s} \pm \frac{b}{t} = \frac{(at \pm bs)}{st} \quad \text{and} \quad \frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st}.$$

88. Example. Let $A = k[x, y]/(y^2)$ together with the multiplicative set $S = \{a(\bar{x}) + b(\bar{x})\bar{y} \mid a(\bar{x}) \neq 0\}$. We claim that $S^{-1}A = k(\bar{x})[y]/(y^2)$. Indeed, $k(\bar{x})[y]/(y^2) = \{r(\bar{x}) + s(\bar{x})\bar{y} \mid r, s \in k(\bar{x})\}$. Now if $r/(a + b\bar{y}) \in S^{-1}A$, then $r/(a + by) = r(a - by)/a^2$. Since $a \neq 0$ this is indeed an element in $k(x)[y]/(y^2)$. Conversely, any element in $k(x)[y]/(y^2)$ can be written as an element in $S^{-1}A$.

89. Exercise (ring structure on localisations).

(i) *The equivalence relation of Definition 1.87 is well-defined;*
(ii) *the operations of Definition 1.87 are well-defined and turn* $S^{-1}A$ *into a ring;*
(iii) $S^{-1}A = 0 \Leftrightarrow 0 \in S \Leftrightarrow S$ *contains a nilpotent element;*
(iv) *the natural map* $\varphi : A \to S^{-1}A$ *which maps* a *to* $a/1$ *is a ring morphism. If* $\varphi(a) = 0$*, then* $as = 0$ *for some* $s \in S$*. Moreover, any element in* $S^{-1}A$ *is of the form* $\varphi(a)\varphi(s)^{-1}$*.*

Proof. (i) and (ii) are easy, if tedious, verifications, see for instance [Re, Proposition in 6.1]. The additive neutral element is represented by $0/s$ for any $s \in S$ (we may take $s = 1$), and the multiplicative neutral element is $1/1$.

(iii) $S^{-1}A = 0 \Leftrightarrow 0 \in S$: If $1/1 = 0/1$, then there exists $u \in S$ such that $u(1{\cdot}1 - 0{\cdot}1) = u = 0$, hence $0 \in S$. Conversely, if $0 \in S$, then $a/s = 0/1$ for all $a \in A$, $s \in S$ (take $u = 0$ in the equivalence relation (2).

$0 \in S \Leftrightarrow S$ contains a nilpotent element: $0 \in S$ is obviously nilpotent. Conversely, if $s \in S$ is nilpotent, then $s^n = 0 \in S$, for S is multiplicative.

(iv) It is clear that φ is a ring morphism with $\ker \phi = \{a \in A \mid \text{there exists } u \in S \text{ such that } ua = 0\}$. Finally, for $s \in S$, $\varphi(s)$ is invertible with inverse $1/s$ so that $a/s = (a/1) \cdot (1/s) = \varphi(a) \cdot \varphi(s)^{-1}$. □

90. Remark.

(i) From the view point of solving equations we can divide any equation $a = b$ with $a, b \in A$ by an element in s, hence $a/s = b/s$. Conversely, when we lift the identity $a/s = b/t$ in $S^{-1}A$ to A we can merely say that there exists $u \in S$ such that $u(at - bs) = 0$.

(ii) In general, $\varphi : A \to S^{-1}A$ is not injective unless S has no zerodivisors. In this case,

$$S^{-1}A = A[S^{-1}] = \{\frac{a}{s} \mid s \in S\} \subset \operatorname{Quot} A$$

and the map $\varphi : A \to S^{-1}A$ is injective. The condition on the right hand side of (2) is designed to define an equivalence relation even if zerodivisors are present. Furthermore, if A is integral, then so is $S^{-1}A$.

(iii) Geometrically, the idea of localising consists in identifying functions which coincide near a point or a subvariety. We come back to this point later on. For the moment, we motivate this idea by the following example. Consider the variety $X = \mathcal{Z}(xy)$ in $\mathbb{A}^2$; we want to localise around the point $a = (1, 0)$. We put $S = \{f \in A(X) \mid f(a) \neq 0\}$. On X, the functions 0 and y agree near the point $(1, 0)$, and $y/1$ and $0/1$ get indeed identified in $S^{-1}A$, for $x(1 \cdot y - 0 \cdot 1) = 0$ and $x \in S$. Of course, this would be wrong without the Definition from (2).

There two popular choices for S.

91. Localising with respect to $f \in A$. Here, we consider for $f \in A$ the multiplicative set $S_f = \{1, f, f^, \ldots\}$. We write

$$A_f := S_f^{-1}A$$

for the localised ring. We claim that

$$A_f \cong A[x]/(xf - 1).$$

In particular, $A_f = A[f^{-1}]$ if f is not nilpotent (otherwise $0 \in S$). Indeed, let $\alpha : A[x] \to A_f$ the (surjective) ring morphism determined by $\alpha(a) = a/1$ for $a \in A$ and $\alpha(x) = 1/f$. We need to show that $\ker \alpha \subset (xf - 1)$, the reverse inclusion being obvious. Let $h(x) \in \ker \alpha$ so that $h(1/f) = 0 \in A_f$. We first prove that $f^n h \in (xf - 1)$ for some n. Clearly, $0 = f^n h(1/f) \in A$ for $n \geqslant \deg f$. Hence $f^n h(x) = G(fx)$ where $G = G(y) \in A[y]$ satisfies $G(1) = 0$. But then $G = (y - 1)G_1(y)$ which implies $f^n h(x) = (fx - 1)G_1(fx)$. Now $1 = xf - (xf - 1)$ so that by the binomial theorem we get

$$1 = 1^n = \big(xf - (xf - 1)\big)^n = x^n f^n + p(xf - 1)$$

for $p \in A[x]$. Hence $h(x) = x^n f^n h(x) + p(xf - 1)h(x) = \big(x^n G_1(fx) + ph(x)\big)(xf - 1) \in (xf - 1)$.

92. Example. Consider $X = \mathcal{Z}(xy)$ with $A(X) = k[x, y]/(xy)$. Then $A(X)_{\bar{x}} = k[\bar{x}, \bar{x}^{-1}]$. This follows from the discussion above and the relation $\bar{x}\bar{y} = 0$ in $A(X)$, so that $\bar{y} = 0$ if $\bar{x}$ is invertible. Geometrically, this corresponds to considering the functions of $\mathcal{Z}(xy)$ on the complement of the closed set $x = 0$ which makes the polynomial function x invertible.

93. Proposition. *Let $X \subset \mathbb{A}^n$ be an affine variety, and let $f \in A(X)$. Recall that $D_f = \{x \in X \mid f(x) \neq 0\}$. Then*

$$\mathcal{O}(D_f) = A(X)_f.$$

In particular, taking $f = 1$, we get $\mathcal{O}_X(X) = A(X)$.

Proof. The inclusion $A(X)_f \subset \mathcal{O}(D_f)$ is clear, so let $g \in \mathcal{O}(D_f) \subset K(X)$. We define an ideal $\mathfrak{a} = \{h \in A(X) \mid gh \in A(X)\}$ in $A(X)$ and want to show that $f^r \in \mathfrak{a}$ for some $r \geqslant 0$. Now for $a \in D_f$ we have $g \in \mathcal{O}_{X,a}$, so $g = h_1/h_2$ with $h_i \in A(X)$ and $h_2(a) \neq 0$. It follows that $h_2 \in \mathfrak{a}$, that is, there exists an element in $\mathfrak{a}$ which does not vanish in a. In particular, if $\hat{\mathfrak{a}}$ denotes the contraction of $\mathfrak{a}$ with respect to the projection $A[n] \to A(X)$, then $\mathcal{Z}(\hat{\mathfrak{a}}) \subset \mathcal{Z}(F)$, where $F \in A[n]$ is a representative of $f \in A(X)$. Indeed, $a \in D_f$, i.e. $f(a) \neq 0$ implies $F(a) \neq 0$. Since there is $H \in \hat{\mathfrak{a}}$ such that $h = \bar{H}(a) \neq 0$, $H(x) = 0$ for all $H \in \hat{\mathfrak{a}}$ implies $F(x) = 0$. It follows that $F \in \sqrt{(F)} \subset \mathcal{I}(\mathcal{Z}(\hat{\mathfrak{a}})) = \sqrt{\mathfrak{a}}$ by the Nullstellensatz. Hence, there exists $r \geqslant 0$ such that $F^r \in \hat{\mathfrak{a}}$ so that passing to $A(X)$ we get $f^r \in \mathfrak{a}$. □

94. Proposition. *Let X be an affine variety. Then*

(i) $\mathcal{O}_X(U) = \bigcap_{a \in U} \mathcal{O}_{X,a}$;
(ii) $K(X) \cong \operatorname{Quot} A(X)$.

Proof. (i) Indeed, by Proposition 1.93 we have $A(X) = \mathcal{O}(X) \subset \bigcap_{a \in X} \mathcal{O}_a = \bigcap_{\mathfrak{m}_a} A(X)_{\mathfrak{m}_a}$. Now in general, if A is an integral domain, then in its quotient field, $A = \bigcap_{\mathfrak{m}} A_{\mathfrak{m}}$, whence the assertion. (To see this, let $x \in \bigcap_{\mathfrak{m}} A_{\mathfrak{m}}$. Then $x = f/g$ and we need to show that g is a unit. If not, then g lies in at least one maximal ideal $\mathfrak{m}_0$. In particular, $f/g \notin A_{\mathfrak{m}_0}$, contradiction. The inclusion $\supset$ is trivial.)

(ii) We have $\operatorname{Quot} \mathcal{O}_{X,a} \cong \operatorname{Quot} A(X)_{\mathfrak{m}_a} \cong \operatorname{Quot} A(X)$ for all $a \in X$. Since every rational function lies in at least one $\mathcal{O}_{X,a}$, $K(X) \subset \bigcup \operatorname{Quot} \mathcal{O}_{X,a} = \operatorname{Quot} A(X)$. As the quotient field of a finitely generated k-algebra, $K(X)$ is a finite field extension of k. □

95. Example. Consider $X = \mathcal{Z}(x_1x_4 - x_2x_3) \subset \mathbb{A}^4$, and let $U = (D_{x_2} \cup D_{x_4}) \cap X$. The function x_1/x_2 is defined on D_{x_2} while the function x_3/x_4 is defined on D_{x_4}. We have $\bar{x}_1/\bar{x}_2, \bar{x}_3/\bar{x}_4 \in \operatorname{Quot} A(X) \cong K(X)$, and by definition of X, $\bar{x}_1/\bar{x}_2 = \bar{x}_3/\bar{x}_4$ whenever defined. In particular, this induces a regular function on U by the sheaf property.

The second natural choice is this.

96. Localisation of A at $\mathfrak{p}$. Let $S = A \backslash \mathfrak{p}$, where $\mathfrak{p} \subset A$ is a prime ideal. Here, the resulting ring of fractions will be written as $A_{\mathfrak{p}}$; in particular, $A_{(0)} = \operatorname{Quot} A$ if A is integral. $A_{\mathfrak{p}}$ is called the **localisation of A at $\mathfrak{p}$** (cf. also Example 1.97).

97. Examples.

(i) The localisation of $\mathbb{Z}$ at $\mathfrak{p} = (p)$ is

$$\mathbb{Z}_{(p)} = \{a/b \in \mathbb{Q} \mid p \nmid b\}.$$

(ii) The localisation of $k[x]$ at $\mathfrak{p} = (x - a)$ is

$$k[x]_{(x-a)} = \{f/g \in k(x) \mid (x - a) \nmid g\} \cong \mathcal{O}_{\mathbb{A}^1,a},$$

the local ring of $a \in \mathbb{A}^1_k$. As we have seen above, these are precisely the regular functions defined near $a \in \mathbb{A}^1$: The zeroes of g are isolated so if $(x - a) \nmid g$, then $g(a) \neq 0$, and this remains true sufficiently close to a.

(iii) If $\mathfrak{p} \in \operatorname{Spec} A[n]$ with corresponding affine variety $X = \mathcal{Z}(\mathfrak{p}) \subset \mathbb{A}^n$, the localisation of $A[n]$ at $\mathfrak{p}$ consists of rational functions f/g where $g \not\equiv 0$ on X. Since for generic $a \in X$, $g(a) \neq 0$, the localisation $A[n]_{\mathfrak{p}}$ can be interpreted as the ring of rational functions defined locally near a generic point of X. We will elaborate further on this idea in Section 5

(iv) If $\mathfrak{q} \subset \mathfrak{p}$, then $\mathfrak{q} \cap (A \backslash \mathfrak{p}) = \varnothing$, so that $\mathfrak{q}^e = \mathfrak{q}A_{\mathfrak{P}}$ is a prime ideal of $A_{\mathfrak{p}}$ by Proposition 1.103. Then $A_{\mathfrak{q}} = (A_{\mathfrak{p}})_{\mathfrak{q}^e}$ by 1.101. To see what this means geometrically, consider the maximal ideal $\mathfrak{m} := (x, y)$ in $\mathbb{A}^2$. Then $A_{\mathfrak{m}}$ consists of all rational functions f/g with $g(0,0) \neq 0$. Now let $\mathfrak{p} \in \operatorname{Spec} A_{\mathfrak{m}}$. Then $\mathcal{Z}(\mathfrak{p})$ is an irreducible curve C through the origin, and since $\mathfrak{p} \subset \mathfrak{m}$, the localisation of $A_{\mathfrak{m}}$ at $\mathfrak{p}^e$ is $A_{\mathfrak{p}} = \{f/g \mid g \notin \mathfrak{p}\} \subset k(x, y)$ – these are the rational functions which are defined on sufficiently general points of C.

98. Remark. In our notation, $\mathbb{Z}_p = \{a/p^n \mid a \in \mathbb{Z}, n \in \mathbb{N}\}$. Be careful to distinguish it from the quotient ring $\mathbb{Z}/p\mathbb{Z}$ which is sometimes also denoted by $\mathbb{Z}_p$.

99. Proposition ($A_{\mathfrak{p}}$ is local). *Let $\mathfrak{p}$ be a prime ideal of A. Then $a/s \in A_{\mathfrak{p}}$ is a unit of $A_{\mathfrak{p}} \Leftrightarrow a \notin \mathfrak{p} \Leftrightarrow a \in S_{\mathfrak{p}}$. Thus the nonunits of $A_{\mathfrak{p}}$ form the ideal $\mathfrak{m} = \mathfrak{p}^e = \mathfrak{p}S_{\mathfrak{p}}^{-1}A$, the extension of $\mathfrak{p}$ with respect to $\varphi : A \to S^{-1}A$. In particular, $(A_{\mathfrak{p}}, \mathfrak{m})$ is a local ring.*

Proof. If $(a/s)(b/t) = 1$ there exists $u \in S$ such that $u(st - ab) = 0$. Since $ust \in S$ it follows that $abu = stu \notin \mathfrak{p}$, hence $a \notin \mathfrak{p}$ for $\mathfrak{p}$ is an ideal. The converse is obvious for $a \notin \mathfrak{p}$ implies $a \in S$. □

100. Universal property of the ring of fractions. *If $S^{-1}A \neq 0$ then $\varphi(S)$ consists of units, and $\varphi : A \to S^{-1}A$ is the universal ring with this property. More precisely, if $\psi : A \to B$ is a ring morphism such that $\psi(S)$ consists of units then there is a unique ring morphism $\hat{\psi} : S^{-1}A \to B$ such that $\psi = \hat{\psi} \circ \varphi$.*

Proof.

Step 1. *Uniqueness.* If $\hat{\psi} : S^{-1}A \to B$ satisfies the condition, then $\hat{\psi}(a/1) = \hat{\psi} \circ \varphi(a) = \psi(a)$. For $a = s \in S$ it follows in particular that $\hat{\psi}(1/s) = \psi(s)^{-1}$. Therefore, $\hat{\psi}(a/s) = \hat{\psi}(a)\hat{\psi}(1/s) = \psi(a)\psi(s)^{-1}$ is uniquely determined by ψ.

Step 2. *Existence.* Define $\hat{\psi}(a/s) := \hat{\psi}(a) \cdot \hat{\psi}(s)^{-1}$. This is indeed well-defined. If $a/s = b/t$, then $u(at - bs) = 0$ for $u \in S$. Hence $\psi(u(at - bs) = \psi(u)\psi(at - bs) = 0$. Since $\psi(u)$ is invertible, $\psi(at - bs) = \psi(a)\psi(t) - \psi(b)\psi(s) = 0$. But then $\hat{\psi}(a/s) = \psi(a)\psi(s)^{-1} = \psi(b)\psi(t)^{-1} = \psi(b/t)$.

□

101. Corollary (localising again). *If $T \subset S$ are two multiplicative sets, let $\varphi_T : A \to T^{-1}A$ and $S_T = \varphi_T(S)$. Then $S_T^{-1}T^{-1}A = S^{-1}A$. In particular, the localisation of a localisation is again a localisation.*

Proof. Since $T \subset S$ there is a well-defined morphism $\psi : T^{-1}A \to S^{-1}A$, $\psi(a/t) = a/t$. Here, the fractions are taken in the respective rings, that is, $\psi \circ \varphi_T = \varphi_S$. By the universal property of $\varphi_{S_T} : T^{-1}A \to S_T^{-1}T^{-1}A$, there is a uniquely determined $\hat{\psi} : S_T^{-1}T^{-1}A \to S^{-1}A$ with $\hat{\psi} \circ \varphi_{S_T} = \psi$. On the other hand, the morphism

$\eta := \varphi_{S_T} \circ \varphi_T : A \to S_T^{-1}T^{-1}A$ gives rise to a uniquely determined morphism $\hat{\eta} : S^{-1}A \to S_T^{-1}T^{-1}A$. Now $\hat{\psi} \circ \eta : A \to S^{-1}A$ satisfies

$$\hat{\psi} \circ \eta = \hat{\psi} \circ \varphi_{S_T} \circ \varphi_T = \psi \circ \varphi_T = \varphi_S.$$

By the universal property, this implies $\hat{\psi} \circ \hat{\eta} = \mathrm{Id}_{S^{-1}A}$. Conversely, we have

$$\hat{\eta} \circ \psi(\frac{a}{t}) = \hat{\eta}(\frac{a}{t}) = \hat{\eta}(a) \cdot \hat{\eta}(t)^{-1} = \frac{a}{t} = \varphi_{S_T}(\frac{a}{t})$$

(check that multiplication/fractions are taking place in the right rings!), whence $\hat{\eta} \circ \hat{\psi} = \mathrm{Id}_{S_T^{-1}S^{-1}A}$ by the universal property. □

102. Example (localising again). Let $A(\mathbb{A}^2) = k[x, y]$ the coordinate ring of $\mathbb{A}^2$ of which we think as its ring of polynomial functions. Let $\mathfrak{m} = (x, y)$, the maximal ideal which corresponds to the origin. The localisation $A_\mathfrak{m}$ is the stalk of regular functions at the origin; it has one maximal ideal, namely $\mathfrak{m}^e$. On the other hand, every irreducible curve in $\mathbb{A}^2$ going through the origin with prime ideal $\mathfrak{p}$ gives a prime ideal $\mathfrak{p}^e$ in $A_\mathfrak{m}$. Indeed, $\mathfrak{p} \subset \mathfrak{m}$ so that $\mathfrak{p} \cap S_\mathfrak{m} = \varnothing$. Hence $(A_\mathfrak{m})_{\mathfrak{p}^e} = \{f/g \mid g \notin \mathfrak{p}\} \subset k(x, y)$ consists of functions which are well-defined in a neighbourhood of the origin and generically defined on the curve $\mathcal{Z}(\mathfrak{p})$.

Next we investigate ideals in $S^{-1}A$. Intuitively, this should be simpler than in A, for taking fractions creates more units.

103. Proposition (Extension and contraction of ideals for $\varphi : A \to S^{-1}A$).

(i) *For any ideal $\mathfrak{b}$ of $S^{-1}A$ we have $\mathfrak{b}^{ce} = \mathfrak{b}$.*
(ii) *For any ideal $\mathfrak{a}$ of A we have*

$$\mathfrak{a}^{ec} = \{a \in A \mid as \in \mathfrak{a} \text{ for some } s \in S\}.$$

(iii) *For any prime ideal $\mathfrak{p}$ contained in $A \backslash S$, $\mathfrak{p}^e$ is a prime ideal of $S^{-1}A$.*

Proof. (i) If $b/s \in \mathfrak{b}$ then $b \in \mathfrak{b}^c$, and so $b/s \in \mathfrak{b}^{ce}$. The other inclusion is trivial.
(ii) If $a \in \mathfrak{a}^{ec}$, then $a/1 = b/t \in S^{-1}A$ for some $b \in \mathfrak{a}$, $t \in S$ (note that $a \notin \mathfrak{a}$!). Hence there exists $u \in S$ such that $u(at - b) = 0$, whence $uta = ub \in \mathfrak{a}$, and so $as \in \mathfrak{a}$ for $s = ut \in S$. The other inclusion is again trivial.
(iii) Let $(a/s) \cdot (b/t) \in \mathfrak{p}^e$, that is, $a \cdot b/s \cdot t = p/q$ with $p \in \mathfrak{p}$ and $q \in S$. Then there exists $u \in S$ such that $u(abq - pst) = 0$. Hence $ab(uq) = stup \in \mathfrak{p}$ so that $ab \in \mathfrak{p}$, for $uq \in S$ which has empty intersection with $\mathfrak{p}$ by assumption. Since $\mathfrak{p}$ is prime, we have either $a \in \mathfrak{p}$, and then $a/s \in \mathfrak{p}^e$, or $b \in \mathfrak{p}$ which implies $b/t \in \mathfrak{p}^e$. □

104. Example. For instance, consider the inclusion $\varphi : \mathbb{Z} \hookrightarrow \mathbb{Q} = (\mathbb{Z}\backslash\{0\})^{-1}\mathbb{Z}$. The only ideals in $\mathbb{Q}$ are (0) and $\mathbb{Q}$. Obviously, $\mathbb{Q}^{ce} = \mathbb{Q}$ and $(0)^{ce} = (0)$. On the other hand, if $\mathfrak{a} = (m)$ is a nontrivial ideal in $\mathbb{Z}$, then $\mathfrak{a}^{ec} = \mathbb{Z}$ and $(0)^{ec}$ as asserted in (ii). Finally, if $\mathfrak{p} = (p)$ is prime such that $\mathfrak{p} \cap \mathbb{Z}\backslash\{0\} = \varnothing$, then $p = 0$ so that $\mathfrak{p}^e = (0)$ is indeed prime in $\mathbb{Q}$.

105. Corollary.

(i) *For an ideal $\mathfrak{a}$ in A we have $\mathfrak{a}^{ec} = \mathfrak{a} \Leftrightarrow$*

$$as \in \mathfrak{a} \Rightarrow a \in \mathfrak{a} \text{ for all } s \in S. \qquad (*)$$

(ii) *Contraction and extension define a* $1-1$*-correpondence*

$$\{\text{ideals of } A \text{ satsifying } (*)\} \leftrightarrow \{\text{ideals in } S^{-1}A\}.$$

(iii) $\mathfrak{a}^{ec} = A \Leftrightarrow \mathfrak{a}^e = S^{-1}A \Leftrightarrow \mathfrak{a} \cap S \neq \varnothing$.

(iv) *If* A *is Noetherian, then so is* $S^{-1}A$*. In particular, any localisation* $A_\mathfrak{p}$ *of a Noetherian ring* A *is again Noetherian.*

(v) *The map* $\varphi^a : \operatorname{Spec} S^{-1}A \hookrightarrow \operatorname{Spec} A$ *coming from the natural map* $\varphi : A \to S^{-1}A$ *identifies* $\operatorname{Spec} S^{-1}A$ *with* $\{\mathfrak{p} \in \operatorname{Spec} A \mid \mathfrak{p} \cap S = \varnothing\}$.

Proof. This follows directly from the previous proposition. For instance (iv): Take an ideal $\mathfrak{b} \subset S^{-1}A$. Then $\mathfrak{b}^c \subset A$ is finitely generated by $\{a_1, \ldots, a_r\}$ say. It follows that $\{\varphi(a_1), \ldots, \varphi(a_r)\}$ generates the extension $\mathfrak{b}^{ce}$ in $S^{-1}A$. Since the latter ideal is $\mathfrak{b}$, any ideal in $S^{-1}A$ is finitely generated. □

106. Exercise (Spectrum of $A_\mathfrak{p}$). *Show that* $\operatorname{Spec} A_\mathfrak{p}$ *is homeomorphic to* $U_\mathfrak{p} = \{\mathfrak{q} \in \operatorname{Spec} A \mid \mathfrak{q} \subset \mathfrak{p}\}$*. Give a geometric interpretation for* $A = A[n]$.

Proof. By Corollary 1.105, $U_\mathfrak{p}$ is the image of the associated map $\varphi^a : \operatorname{Spec} A_\mathfrak{p} \hookrightarrow \operatorname{Spec} A$ so that $\operatorname{Spec} A_\mathfrak{p} \cong U_\mathfrak{p}$ as a set. Now $U_\mathfrak{p}$ has the subspace topology, that is, $F \subset U_\mathfrak{p}$ is closed $\Leftrightarrow F = U_\mathfrak{p} \cap V(\mathfrak{a})$ for some ideal $\mathfrak{a} \subset A$. We know already by Exercise 0.39 that $\varphi^a : \operatorname{Spec} A_\mathfrak{p} \to \operatorname{Spec} A$ is continuous. Further, φ^a has an inverse $\psi : U_\mathfrak{p} \to \operatorname{Spec} A_\mathfrak{p}$ given by $\psi(\mathfrak{q}) = \mathfrak{q}^e = \mathfrak{q}A_\mathfrak{p}$. Then $\psi^{-1}(\mathcal{Z}(\mathfrak{a}) \cap U_\mathfrak{p}) = \mathcal{Z}(\mathfrak{a}A_\mathfrak{p})$ which is closed. Hence ψ is also continuous so that ϕ defines a homeomorphism onto its image $U_\mathfrak{p}$.

If $A = A[n]$, then $\operatorname{Spec} A$ is the set of irreducible subvarieties of $\mathbb{A}^n$. Hence $\operatorname{Spec} A_\mathfrak{p}$ is the set of irreducible subvarieties which contain $\mathcal{Z}(\mathfrak{p})$. For instance, if $\mathfrak{p} = \mathfrak{m} = (x_1 - a_1, \ldots, x_n - a_n)$, then $\operatorname{Spec} A_\mathfrak{m}$ is the set of all irreducible subvarieties of $\mathbb{A}^n$ passing through $(a_1, \ldots, a_n)$. □

Modules of fractions. Localisation can be generalised to modules.

107. Definition (modules of fractions and localisation). Let M be an A-module and $S \subset A$ a multiplicative subset. Then $S^{-1}M$ is the $S^{-1}A$-module defined as follows. Let

$$(m, s) \sim (n, t) \Leftrightarrow \text{there exists } u \in S \text{ such that } u(tm - sn) = 0.$$

Then we call

$$S^{-1}M = (M \times S)/\sim$$

the **module of fractions**. The operations

$$(a/s)(m/t) = am/st, \quad m/s + n/t = (mt + ns)/st$$

turn $S^{-1}M$ into an $S^{-1}A$-module. The **localisation of** M at $\mathfrak{p} \in \operatorname{Spec} A$ is $M_\mathfrak{p} := (A \backslash \mathfrak{p})^{-1}M$. We also let $M_f = S_f^{-1}M$ where $S = \{1, f, f^2, \ldots\}$. Finally, if $\varphi : M \to N$ is an A-morphism, we define an $S^{-1}A$-morphism by

$$S^{-1}\varphi : S^{-1}M \to S^{-1}N, \quad S^{-1}\varphi(m/s) = \varphi(m)/s.$$

This turns S^{-1} into a covariant functor.

In fact, the functor S^{-1} is *exact*:

108. Proposition (Exactness of S^{-1}). *If $L \xrightarrow{\alpha} M \xrightarrow{\beta} N$ is an exact sequence, then so is $S^{-1}L \xrightarrow{S^{-1}\alpha} S^{-1}M \xrightarrow{S^{-1}\beta} S^{-1}N$. In particular, localisation of modules is an exact functor.*

Proof. Let $m/s \in S^{-1}M$. Then

$$S^{-1}\beta(m/s) = \beta(m)/s = 0 \Leftrightarrow \text{ there exists } u \in S \text{ such that } u\beta(m) = \beta(um) = 0.$$

However, $\ker \beta = \operatorname{im} \alpha$ by exactness of the original sequence, hence $S^{-1}\beta(m/s) = 0$ if and only there exists $u \in S$ and $l \in L$ such that $um = \alpha(l)$. Dividing by us yields $m/s = S^{-1}\alpha(l/us)$. □

In particular, considering the exact sequences $0 \to L \to M \to M/L \to 0$ and $0 \to L \cap L' \to L \to M/L'$ for submodules L, $L' \subset M$ immediately implies (i) and (ii) of the

109. Proposition. *If L, $L' \subset M$ are submodules, then*

(i) $S^{-1}L \subset S^{-1}M \quad$ *and* $\quad S^{-1}(M/L) \cong S^{-1}M/S^{-1}L$.
(ii) $S^{-1}(L \cap L') = S^{-1}L \cap S^{-1}L' \subset S^{-1}M$.
(iii) $S^{-1}(L + L') = S^{-1}L + S^{-1}L'$.
(iv) *Let T be the image of S in $A/\mathfrak{a}$. Then $T^{-1}(A/\mathfrak{a}) \cong (S^{-1}A)/\mathfrak{a}^e$. In particular, $A_\mathfrak{p}/\mathfrak{p}^e \cong \big((A\backslash\mathfrak{p})/\mathfrak{p}\big)^{-1}A/\mathfrak{p} = \operatorname{Quot}(A/\mathfrak{p})$. In other words, the residue field of the local ring $A_\mathfrak{p}$ equals the quotient field of $A/\mathfrak{p}$.*

Proof. (iii) Follows directly from the definition of $+$.

(iv) Viewing A and $\mathfrak{a}$ as A-modules, the ring of fractions $T^{-1}(A/\mathfrak{a})$ is isomorphic with $S^{-1}(A/\mathfrak{a})$ as modules, hence with $S^{-1}A/S^{-1}\mathfrak{a}$ by (i). This is in fact a ring morphism. Further, $S^{-1}\mathfrak{a} = \mathfrak{a}S^{-1}A = \mathfrak{a}^e$. Note also that $(A\backslash\mathfrak{p})/\mathfrak{p}$ is just $(A/\mathfrak{p})\backslash\{\bar{0}\}$. □

110. Proposition. *Let M be an A-module $\Rightarrow$*

$$S^{-1}M \cong S^{-1}A \otimes_A M$$

as $S^{-1}A$-modules. In fact, there is a uniqe isomorphism $\varphi : S^{-1}A \otimes_A M \to S^{-1}M$ for which $\varphi(a/s \otimes m) = am/s$ for all $a \in A$, $s \in S$ and $m \in M$.

Proof. We define a map $S^{-1}A \times M \to S^{-1}M$ by sending $(a/s, m) \to am/s$. Clearly, this is bilinear and induces a uniquely determined surjective map φ as stated. It remains to show injectivity. So let $\varphi(\sum a_i/s_i \otimes m_i) = \sum a_i m_i/s_i = 0$. By passing to a common denominator s we may write $\sum a_i/s_i \otimes m_i = 1/s \otimes \sum b_i m_i = 1/s \otimes m$ with $s \in S$ and $m \in M$. Hence we only need to show that if $m/s = 0$, then $1/s \otimes m = 0$. But $m/s = 0 \Leftrightarrow$ there exists $u \in S$ such that $um = 0$, hence $1/s \otimes m = u/us \otimes m = 1/us \otimes um = 0$. □

111. Corollary. *If M and N are A-modules, there exists a unique $S^{-1}A$-module morphism $f : S^{-1}M \otimes_{S^{-1}A} S^{-1}N \to S^{-1}(M \otimes_A N)$ such that $f(m/s \otimes n/t) = (m \otimes n)/st$. In particular, we have*

$$M_\mathfrak{p} \otimes_{A_\mathfrak{p}} N_\mathfrak{p} \cong (M \otimes_A N)_\mathfrak{p}$$

as $A_\mathfrak{p}$-modules.

Proof. This follows directly from the previous proposition and the standard tensor product isomorphisms. □

Local properties. A property P of an A-module M is called **local** if

$$M \text{ has P} \Leftrightarrow M_{\mathfrak{p}} \text{ has P for all prime ideals } \mathfrak{p} \text{ in } A.$$

Here, we will consider two examples.

112. Proposition (triviality is local). *Let M be an A-module. Are equivalent:*

(i) $M = 0$;
(ii) $M_{\mathfrak{p}} = 0$ *for all prime ideals* $\mathfrak{p}$ *in* A;
(iii) $M_{\mathfrak{m}} = 0$ *for all maximal ideals* $\mathfrak{m}$ *in* A;

In particular, triviality of an A-module is a local property.

Proof. We only need to prove (iii)⇒(i). Assume $M \neq 0$ and let $0 \neq x \in M$, $\mathfrak{a} = \operatorname{ann}(x) = \{a \in A \mid ax = 0\}$. Then $\mathfrak{a}$ is an ideal strictly contained in A (otherwise $1 \cdot x = x = 0$), and therefore contained in some maximal ideal $\mathfrak{m}$. However, $x/1 \in M_{\mathfrak{m}} = 0$ by assumption, that is, there exists $u \in A \backslash \mathfrak{m}$ such that $ux = 0$. But this implies $u \in \operatorname{ann}(x) \subset \mathfrak{m}$, a contradiction. □

113. Proposition (injectivity and surjectivity are local). *Let $\phi : M \to N$ be a morphism. Are equivalent:*

(i) ϕ *is injective;*
(ii) $\phi_{\mathfrak{p}} : M_{\mathfrak{p}} \to N_{\mathfrak{p}}$ *is injective for all prime ideals* $\mathfrak{p}$ *in* A;
(iii) $\phi_{\mathfrak{m}} : M_{\mathfrak{m}} \to N_{\mathfrak{m}}$ *is injective for all prime ideals* $\mathfrak{m}$ *in* A;

The same holds true for "surjective" instead of "injective". Hence injectivity (surjectivity) of a linear map is a local property.

Proof. (i)⇒(ii) $0 \to M \to N$ is exact, hence $0 \to M_{\mathfrak{p}} \to N_{\mathfrak{p}}$ is exact, i.e. $\phi_{\mathfrak{p}}$ is injective.

(ii)⇒(iii) Obvious.

(iii)⇒(i) Let $L = \ker \phi$ so that $0 \to L \to M \xrightarrow{\phi} N$ is exact, whence $0 \to L_{\mathfrak{m}} \to M_{\mathfrak{m}} \xrightarrow{\phi_{\mathfrak{m}}} N_{\mathfrak{m}}$ is exact. But $\phi_{\mathfrak{m}}$ is injective, hence $L_{\mathfrak{m}} = 0$ for all $\mathfrak{m}$. Consequently, $L = 0$ from the previous proposition, and ϕ is injective. □

Flatness is also a local property (cf. the notion of flatness in differential geometry!).

114. Exercise (flatness is local). *Let M be an A-module. Are equivalent:*

(i) M *is a flat A-module;*
(ii) $M_{\mathfrak{p}}$ *is a flat $A_{\mathfrak{p}}$-module for all prime ideals* $\mathfrak{p}$ *in* A;
(iii) $M_{\mathfrak{m}}$ *is a flat $A_{\mathfrak{m}}$-module for all maximal ideals* $\mathfrak{m}$ *in* A;

In particular, flatness of an A-module is a local property.

Proof. (i)⇒(ii): If M is a flat A-module and $A \to B$ a ring morphism turning B into an A-module, then $M_B = M \otimes_A B$ is a flat B-module, see Exercise 0.82. Taking $B = A_\mathfrak{p}$, we have $M \otimes_A A_\mathfrak{p} \cong M_\mathfrak{p}$ by Proposition 1.110, whence $M_\mathfrak{p}$ is flat.
(ii)⇒(iii): Trivial.
(iii)⇒(i): Let $\varphi : N \to N'$ be an injective A-linear map. We have to show that $T_M(\varphi) : T_M N \to T_M N'$ is injective, cf. Proposition 0.74. Since injectivity is a local property, $\varphi_\mathfrak{m} : N_\mathfrak{m} \to N'_\mathfrak{m}$ is injective. By assumption, $M_\mathfrak{m}$ is flat, hence $T_{M_\mathfrak{m}}\varphi_\mathfrak{m} : N_\mathfrak{m} \otimes_{A_\mathfrak{m}} M_\mathfrak{m} \to N'_\mathfrak{m} \otimes_{A_\mathfrak{m}} M_\mathfrak{m}$ is injective. But $(N_\mathfrak{m} \otimes_{A_\mathfrak{m}} M_\mathfrak{m}) \cong (N \otimes_A M)_\mathfrak{m}$ by Corollary 1.111. Consequently, for every maximal ideal $\mathfrak{m}$ of A the localisation of $T_M\varphi : N \otimes_A M \to N' \otimes_A M$ is injective, hence $T_M\varphi$ is itself injective. □

1.4. **Primary decomposition*.** We have now introduced the basic players of commutative algebra. Next we want to discuss further aspects in connection with geometry in the spirit of the first section. The first topic we address is the so-called primary decomposition which generalises the decomposition into primes in a UFD. Polynomial rings such as $k[x_1, \ldots, x_n]$ are UFD (Gauß theorem), but already simple rings such as $\mathbb{Z}[\sqrt{5}]$ are not UFD. Indeed, $2 \cdot 3 = 6 = (1 + \sqrt{5})(1 - \sqrt{5})$ so that there is no unique decomposition. However, there is a generalised version involving ideals rather than elements of the ring, and which holds for a large class of rings. A we will see that corresponds to decomposing an affine variety into irreducible components together with further geometric information such as multiplicities or tangency conditions (i.e. conditions on the formal derivatives of the defining polynomials).

We first need some definitions. A prime ideal can be thought of as a generalisation of a prime number p (think of $\mathbb{Z}$ for instance). A *primary ideal* is the analogue of the power p^n.

115. Definition (primary ideal). An ideal $\mathfrak{q}$ is **primary** if $x \cdot y \Rightarrow x \in \mathfrak{q}$ or $y^n \in \mathfrak{q}$ for some $n > 0$, that is, either $x \in \mathfrak{q}$ or $y \in \sqrt{\mathfrak{q}}$.

116. Remark. In terms of quotient rings this can be expressed as follows. $\mathfrak{q}$ is primary ⇔ if every zero-divisor in $A/\mathfrak{q}$ is nilpotent.

117. Examples.

(i) Any prime ideal is primary.
(ii) If $\mathfrak{a}$ is primary and $\mathfrak{b} \subset \mathfrak{a}$ is a further ideal, then $\mathfrak{a}/\mathfrak{b}$ is primary in $A/\mathfrak{b}$ as follows from the isomorphism $(A/\mathfrak{b})/(a/\mathfrak{b}) \cong A/\mathfrak{a}$.
(iii) The contraction of a primary ideal is primary, for if $f : A \to B$ is a ring morphism and $\mathfrak{q} \subset B$ is primary, then $A/\mathfrak{q}^c$ can be identified with a subring of B/q, hence any zero-divisor is nilpotent.

118. Proposition and Definition ($\mathfrak{p}$-primary).

(i) *Let $\mathfrak{q}$ be primary. Then $\mathfrak{p} = \sqrt{\mathfrak{q}}$ is the smallest prime ideal containing $\mathfrak{q}$. We say that $\mathfrak{q}$ is* **$\mathfrak{p}$-primary.**
(ii) (Partial converse) *If $\sqrt{\mathfrak{q}} = \mathfrak{m}$ is maximal, then $\mathfrak{q}$ is ($\mathfrak{m}$-)primary. In particular, all the powers of a maximal ideal $\mathfrak{m}$ are $\mathfrak{m}$-primary.*

119. Examples.

(i) The primary ideals in $\mathbb{Z}$ are (0) and (p^n) where $p \in \mathbb{Z}$ is prime. It is clear that they are primary. Further, $\sqrt{\mathfrak{a}} = (p)$ prime implies $\mathfrak{a} = (p^n)$ for some $n \in \mathbb{N}$. More generally, this is true in any principal ideal ring using also the fact that it is UFD.

(ii) Let $A = k[x, y]$, $\mathfrak{q} = (x, y^2)$. Then $A/\mathfrak{q} \cong k[y]/(y^2)$, hence the zerodivisors such as the equivalence class of y, are nilpotent. In particular, it follows that a *primary ideal is not necessarily a prime power* $\mathfrak{p}^n$.

(iii) Conversely, *a prime power is not necessarily primary*, although its radical is prime 1..23 (xiv). For instance, let $A = k[x, y, z]/(xy - z^2)$ and let $\bar{x}$, $\bar{y}$ and $\bar{z}$ denote the images of x, y and z of $k[x, y, z]$ in A. Then $\mathfrak{p} = (\bar{x}, \bar{z})$ is prime for $A/\mathfrak{p} \cong k[y]$ which is integral. Further, $\bar{x}\bar{y} = \bar{z}^2 \in \mathfrak{p}^2$, but $\bar{x} \notin \mathfrak{p}^2$. Also, $\bar{y} \notin \mathfrak{p} = \sqrt{\mathfrak{p}^2}$ so that $y^n \notin \mathfrak{p}^2$ for any $n \in \mathbb{N}$. Hence $\mathfrak{p}^2$ is not primary.

(iv) If $\mathfrak{q}_i$ is a finite number of $\mathfrak{p}$-primary ideals, then so is the intersection $\mathfrak{q} = \bigcap \mathfrak{q}_i$. Indeed, $\sqrt{\mathfrak{q}} = \sqrt{\bigcap_i \mathfrak{q}_i} = \bigcap \sqrt{\mathfrak{q}_i} = \mathfrak{p}$.

(v) If $\mathfrak{q}$ is $\mathfrak{p}$-primary with $\mathfrak{p} = (f_1, \dots, f_n)$ finitely generated, then $\mathfrak{p}^m \subset \mathfrak{q} \subset \mathfrak{p}$ for some $m \in N$. Indeed, $f_i^{n_i} \in \mathfrak{q}$ for suitable $n_i \in N$ since $\mathfrak{p} = \sqrt{\mathfrak{q}}$. Let $m > 2 \max n_i$, then every monomial of degree m in $f_1, \dots, f_k$ is a multiple of $f_i^{n_i}$ for some i, hence in Q. (Our choice of m is of course not optimal.) This condition is not sufficient. Consider the ideal $\mathfrak{a} = (x^2, xy) \subset k[x, y]$. Then $\sqrt{\mathfrak{a}} = (x)$. (A geometric way of seeing this is to apply the Nullstellensatz: $\sqrt{\mathfrak{a}} = \mathcal{I} \circ \mathcal{Z}(\mathfrak{a}) = \mathcal{I}(\mathcal{Z}(x^2) \cap \mathcal{Z}(xy)) = \mathcal{I} \circ \mathcal{Z}(x)$.) In particular, $(x^2) \subset \mathfrak{a} \subset \sqrt{\mathfrak{a}} = (x)$. However, $\mathfrak{a}$ is not primary, for the zero divisor $\bar{y}$ is not nilpotent. However, if $\mathfrak{p}$ is maximal, then $\mathfrak{p}^n \subset \mathfrak{q} \subset \mathfrak{p}$ is sufficient, for taking radicals gives $\sqrt{\mathfrak{p}^m} \subset \sqrt{\mathfrak{q}} \subset \sqrt{\mathfrak{m}} = \mathfrak{m}$, whence equality by the previous proposition.

120. Lemma. *Let $\mathfrak{q}$ be $\mathfrak{p}$-primary, and $x \in A$. Then*

(i) *if $x \notin \mathfrak{q}$, $\mathfrak{q} : x$ is $\mathfrak{p}$-primary;*
(ii) *if $x \notin \mathfrak{p}$, $\mathfrak{q} : x = \mathfrak{q}$.*

Proof. (i) $\mathfrak{q} : x$ is primary: Let $yz \in \mathfrak{q} : x$ with $y \notin \sqrt{(\mathfrak{q} : x)}$. Then $xyz \in \mathfrak{q}$, hence $xz \in \mathfrak{q}$, and finally $z \in \mathfrak{q} : x$. Next we compute the radical: If $y \in \mathfrak{q} : x$, then $yx \in \mathfrak{q} \subset \sqrt{\mathfrak{q}} = \mathfrak{p}$, hence (as $x \notin \mathfrak{q}$) we have $y \in \mathfrak{p}$. Therefore $\mathfrak{q} \subset \mathfrak{q} : x \subset \mathfrak{p}$; taking radicals we obtain $\mathfrak{p} \subset \sqrt{(\mathfrak{q} : x)} \subset \mathfrak{p}$.

(ii) follows directly from the definition. □

121. Definition (primary decomposition). Let A be a ring, and $\mathfrak{a} \subset A$ be an ideal. An ideal $\mathfrak{a}$ is **decomposable** if it admits a **primary decomposition**, i.e. an expression

$$\mathfrak{a} = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_k$$

with each $\mathfrak{q}_i$ primary. This decomposition is called **minimal** if no term is redundant (i.e. $\mathfrak{a} \subsetneq \bigcap_{i \neq j} Q_i$) and if $i \neq j \Rightarrow \sqrt{\mathfrak{q}_i} \neq \sqrt{\mathfrak{q}_j}$. Note that by ignoring the redundant terms and replacing two $\mathfrak{p}$-primary ideals by their intersection we may always assume that the primary decomposition of a decomposable ideal is minimal.

122. Geometric examples.

(i) Assume that $\mathfrak{a} \subset A[n]$ is radical, i.e. $\mathfrak{a} = \sqrt{\mathfrak{a}}$. Then by Hilbert's Nullstellensatz, Corollary 1.36 (decomposition into irreducibles), and Remark 1.18

$$\mathfrak{a} = \mathcal{I}(\mathcal{Z}(\mathfrak{a})) = \mathcal{I}(\bigcup_{i=1}^{k} \mathcal{Z}(\mathfrak{p}_i)) = \bigcap_{i=1}^{k} \mathcal{I}(\mathcal{Z}(\mathfrak{p}_i) = \bigcap_{i=1}^{k} \mathfrak{p}_i$$

the primary decomposition is just the decomposition into irreducible subvarieties.

(ii) To get a feeling for the general case, consider an ideal $\mathfrak{a}$ which is primary to the maximal ideal $\mathfrak{m} = (x, y)$ in $k[x, y]$. In particular, $\mathcal{Z}(\mathfrak{a}) = \mathcal{Z}(\sqrt{\mathfrak{a}}) = \mathcal{Z}(\mathfrak{m}) = (0, 0) \in k^2$. What kind of geometric object X is encapsulated in $\mathfrak{a}$? The idea is that X should contain $\mathcal{Z}(\mathfrak{m})$ *and* characterise the coordinate ring $k[2]/\mathfrak{a}$. If, for instance, $\mathfrak{a} = (x^2, y)$, then the residue class of a polynomial $f = \sum a_{ij} x^i y^j \in k[x, y]$ is $[a_{00} + a_{10}x]$. Hence, if we "restrict" f to X we see $a_{00} = f(0, 0)$ and $a_{10} = \partial_x f(0, 0)$ the first derivative. So we think of X as the point $(0, 0)$ plus the horizontal tangent vector at the origin which encodes an infinitesimal first order neighbourhood of the origin in the x-direction. If we add an actual neighbourhood of the origin in the x-direction, for instance by adding the horizontal line $y = 0$, that is, we consider $\mathfrak{a} \cap (y)$ the first-order information becomes redundant which is reflected in the idnetity $\mathfrak{a} \cap (y) = (y)$. Similarly, if we let $\mathfrak{a} = (x^2, xy, y^2)$, then we get in addition $a_{01} = \partial_y f(0, 0)$, that is, X is the origin plus its whole first-order neighbourhood. If we replace $\mathfrak{m}$ by $\mathfrak{m}^{n+1}$ we see the origin plus the derivative up to order n, that is, X is the origin plus the whole infinitesimal nth-order neighbourhood. On the other hand, if we take $\mathfrak{p} = (x) \subset k[x, y]$ which describes the y-axis $\{x = 0\}$, then $\mathfrak{a} = (x^2)$ describes the first-order neighbourhood in the x-direction of the y-axis, that is, we get the first-order neighbourhood of the y-axis, see Figure 1.8 (a)-(c).

More complicated ideals can be treated similarly. For instance, let $\mathfrak{a} = (x) \cdot \mathfrak{m} = (x^2, xy)$. Every $f \in \mathfrak{a}$ gives a polynomial function that vanishes along $\{x = 0\}$ and has multiplicity (i.e. order of vanishing) $\geqslant 2$ at the origin. Conversely, any polynomial with these properties must be of the form xg where $g \in \mathfrak{m}$. Hence we have a primary decomposition $\mathfrak{a} = (x) \cap (x, y)^2$ whose components belong to the ideals (x) and $\mathfrak{m}$, and the resulting geometric object is the vertical line plus the thickened origin which indicates its first-order neighbourhood, see Figure 1.8 (d). Note that we could decompose $\mathfrak{a}$ equally well as $(x) \cap (x^2, y)$. This corresponds to the fact that the only information about a function which is avalaible on the first-order neighbourhood of the origin, but not on the vertical line, is the first-order information in the x-direction.

We first address *uniqueness* of the decomposition which holds for a general ring.

123. Theorem (first uniqueness theorem). *Let $\mathfrak{a}$ be a decomposable ideal with $\mathfrak{a} = \bigcap \mathfrak{q}_i$ a minimal primary decomposition into $\mathfrak{p}_i$-primaries. Then the $\mathfrak{p}_i$ which occur are precisely the prime ideals of the set $\{\sqrt{(\mathfrak{q} : x)} \mid x \in A\}$. In particular, they are independent of the underlying minimal primary decomposition.*

Proof. For any $x \in A$ we have $\mathfrak{a} : x = \bigcap \mathfrak{q}_i : x = \bigcap (\mathfrak{q}_i : x)$, hence $\sqrt{(\mathfrak{a} : x)} = \bigcap \mathfrak{p}_i$ by Lemma 1.120. If $\sqrt{(\mathfrak{a} : x)}$ is prime, then by 0.24, $\sqrt{(\mathfrak{a} : x)} = \mathfrak{p}_i$ for some $i.$, so every prime ideal associated with the primary decomposition of $\mathfrak{a}$ is of this form. Conversely, by minimality there exists for each i an element $x_i \notin \mathfrak{q}_i$ and such that $x_i \bigcap_{j \neq i} \mathfrak{q}_j$ (i.e. $\bigcap_{j \neq i} \mathfrak{q}_j \subsetneq \mathfrak{q}_i$. But then $\sqrt{(\mathfrak{a} : x_i)} = \mathfrak{p}_i$. □

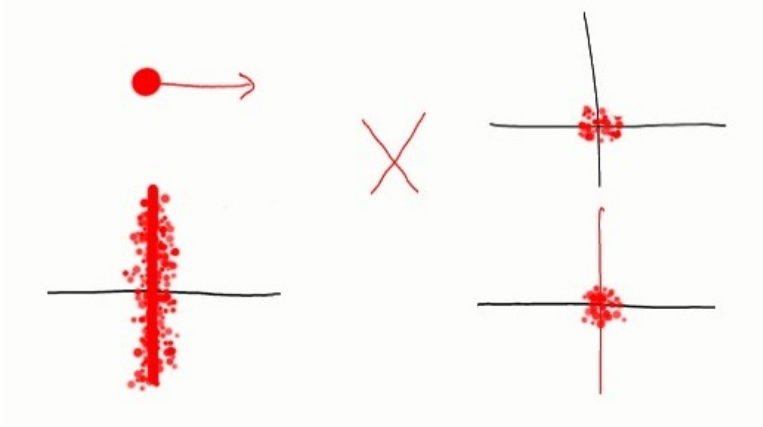

FIGURE 8. The varieties X (a)-(d)

124. Remark. Viewing $A/\mathfrak{a}$ as an A-module, the theorem is equivalent to saying that the $\mathfrak{p}_i$ are precisely the prime ideals which occur as radicals of annihilators of elements of $A/\mathfrak{a}$.

The prime ideals $\mathfrak{p}_i$ are said to be **associated with** $\mathfrak{a}$. In particular, $\mathfrak{a}$ is primary $\Leftrightarrow$ $\mathfrak{a}$ has only one associated prime ideal. The minimal elements of the set $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$ are called the **isolated** primes while the remaining ones are called **embedded**.

125. Example. If $\mathfrak{a} \subset A[n]$, then the minimal primes correspond to the irreducible components of $\mathcal{Z}(\mathfrak{a})$. The embedded primes are subvarities of these components. For instance, in the decomposition $(x^2, xy) = (x) \cap (x, y)^2$, $\mathfrak{p} = (x)$ is minimal, while $\mathfrak{m} = (x, y)$ is embedded.

126. Proposition (isolated primes of a decomposable $\mathfrak{a}$). *Let $\mathfrak{a}$ be decomposable. Then any prime $\mathfrak{p} \supset \mathfrak{a}$ contains a minimal prime belonging to $\mathfrak{a}$. Hence, the isolated prime ideals of $\mathfrak{a}$ are precisely the minimal elements of the set of all primes containing $\mathfrak{a}$.*

Proof. If $\mathfrak{p} \supset \mathfrak{a} = \bigcap \mathfrak{q}_i$, then $\mathfrak{p} = \sqrt{\mathfrak{p}} \supset \bigcap \sqrt{\mathfrak{q}_i} = \bigcap \mathfrak{p}_i$. Therefore $\mathfrak{p} \supset \mathfrak{p}_i$ for some i by Proposition 0.24. Now either $\mathfrak{p}_i$ is minimal or contains a minimal prime. □

Note that it is *not* true that the primary components are independent of the decomposition as we have seen above in Example 1.122. Still, we have some kind of uniqueness, namely the decomposition into irreducible components.

127. Theorem (second uniqueness theorem). *Let $\mathfrak{a}$ be a decomposable ideal with minimal primary decomposition $\bigcap_{i=1}^{n} \mathfrak{q}_i$ and let $\{\mathfrak{p}_{i_1}, \ldots, \mathfrak{p}_{i_m}\}$ be a set of isolated primes. Then $\mathfrak{q}_{i_1} \cap \ldots \cap \mathfrak{q}_{i_m}$ is independent of the decomposition. In particular, the primary ideals corresponding to isolated primes are uniquely determined by $\mathfrak{a}$.*

128. Proposition (union of the associated ideals). *Let $\mathfrak{a}$ be decomposable, and let $\mathfrak{a} = \bigcap \mathfrak{q}_i$ be a minimal primary decomposition with $\sqrt{\mathfrak{q}_i} = \mathfrak{p}_i$. Then*

$$\bigcup \mathfrak{p}_i = \{x \in A \mid \mathfrak{a} : x \neq \mathfrak{a}\}.$$

In particular, if the zero ideal is decomposable, the sets D of zerodivisors is the union of all prime ideals belonging to (0).

Proof. If $\mathfrak{a}$ is decomposable, then $0 = \bigcap \bar{\mathfrak{q}}_i$, where $\bar{\mathfrak{q}}_i$ are the (primary) images of $\mathfrak{q}_i$ in $A/\mathfrak{a}$. Hence we only need to prove the last statement. By Proposition 0.19 we have $D = \bigcup_{x \neq 0} \sqrt{(0:x)}$; on the other hand, from the proof of the First Uniqueness Theorem 1.123 we have $\sqrt{(0:x)} = \bigcap_{x \notin \mathfrak{q}_i} \mathfrak{p}_i \subset \mathfrak{p}_i$ for some i, hence $D \subset \bigcup \mathfrak{p}_i$. But each $\mathfrak{p}_i$ is of the form $\sqrt{(0:x)}$ for some $x \in A$, hence $\bigcup \mathfrak{p}_i \subset D$. □

129. Remark. If (0) is decomposable, the set of nilpotent elements is the *intersection* of all minimal primes belonging to (0).

We now turn to the existence of primary decompositions in Noetherian rings which was the initial motivation for their study.

130. Theorem (existence of primary decompositions in Noetherian rings). *In a Noetherian ring A, every ideal $\mathfrak{a}$ has a primary decomposition.*

Proof. Say that an ideal $\mathfrak{a}$ is *irreducible* if

$$\mathfrak{a} = \mathfrak{b} \cap \mathfrak{c} \Rightarrow \mathfrak{a} = \mathfrak{b} \text{ or } \mathfrak{a} = \mathfrak{c}.$$

For example, any prime ideal is indecomposable by 0.24. The result follows from the next two statements.

Step 1. *In a Noetherian ring A every ideal is a finite intersection of irreducible ideals.* Suppose not. Then the set of ideals $\Sigma \subset A$ for which the assertion is false is not empty. In particular, there exists a maximal element $\mathfrak{a}$ with respect to inclusion. By definition, we can write this ideal $\mathfrak{a} = \mathfrak{b} \cap \mathfrak{c}$ for two ideals strictly containing $\mathfrak{a}$. These are therefore irreducible so that $\mathfrak{a} \notin \Sigma$, a contradiction.

Step 2. *In a Noetherian ring every irreducible ideal is primary.* Let $\mathfrak{a}$ be irreducible. By passing to the quotient ring we only need to show that $(\bar{0})$ is primary in $A/\mathfrak{a}$. So let $xy = 0$ in $A/\mathfrak{a}$ with $y \neq 0$. The chain of ideals $\operatorname{ann}(x) \subset \operatorname{ann}(x^2) \subset \dots$ becomes eventually stationary at some n, i.e. $\operatorname{ann}(x^n) = \operatorname{ann}(x^{n+1}) = \dots$. Then $(x^n) \cap (y) = (0)$. For if $a \in (y)$, then $ax = 0$, and if $a \in (x^n)$, then $a = bx^n$, hence $bx^{n+1} = 0$. Thus $b \in \operatorname{ann}(x^{n+1}) = \operatorname{ann}(x^n)$ and therefore $bx^n = 0$, that is, $a = 0$. Since (0) is irreducible by assumption and $(y) \neq (0)$ we must have $(x^n) = (0)$, i.e. $x \in \sqrt{(0)}$.

□

1.5. **Regular and rational maps.** We now come to the definition of *maps between varieties* – the morphisms of our category.

Regular maps. The first notion of morphism is this.

131. Definition (morphism between varieties). A **morphism** or **regular map** $\varphi : X \to Y$ between varieties X and Y is a continuous map such that for every open set $V \subset Y$, and every regular function $f : V \to k \in \mathcal{O}_Y(V)$, the function

$$\varphi^*(f) := f \circ \varphi : \varphi^{-1}(V) \to k$$

is regular, i.e. in $\mathcal{O}_X(\varphi^{-1}(V))$. Put differently, $\varphi : X \to Y$ is a morphism of varieties $\Leftrightarrow \varphi^* : \mathcal{O}_Y(V) \to \mathcal{O}_X(\varphi^{-1}(V))$ is a k-algebra morphism (and in particular

a morphism of sheaves of k-algebras). It is easy to see that the composition of two morphisms $f : X \to Y$ and $g : Y \to Z$ is again a morphism $g \circ f : X \to Z$ so that we get the category **VAR** (or $\mathbf{VAR}_k$ if we want to emphasise the field), the **category of varieties (over k)**.

132. Remark.

(i) Regularity is a *local* property, i.e. $\varphi : X \to Y$ is regular if and only if $\varphi|_U$ is regular for any open set. In particular, it is enough to verify regularity for an open cover $\bigcup_i U_i$ of X.

(ii) An **isomorphism** $\varphi : X \to Y$ is a morphism such that there exists a morphism $\psi : Y \to X$ with $\varphi \circ \psi = \mathrm{Id}_Y$ and $\psi \circ \varphi = \mathrm{Id}_X$. If such an isomorphism exists, then we say that X and Y are **isomorphic**. In particular, any isomorphism is a *homeomorphism* (i.e. bijective and bicontinuous). Note in passing that there are homeomorphisms which are not isomorphisms between varieties, see Examples 1.134 and 1.137. This allows us to consider *abstract varieties* obtained by glueing together affine varieties. These abstract varieties are the algebraic counterpart to smooth or complex manifolds. We pursue this aspect further in Section 5 when we will glue *affine schemes*.

The following lemma is useful to get explicit examples of regular maps.

133. Lemma (morphisms and coordinate functions). *Let X be any variety, $Y \subset \mathbb{A}^n$ an affine variety, and chose coordinate functions $x_1, \ldots, x_n$ on $\mathbb{A}^n$ which generate $A[n]$. A map of sets $\psi : X \to Y$ is morphism $\Leftrightarrow \psi^* x_i = x_i \circ \psi$ is a regular function on X for each i.*

Proof. If ψ is a morphism, then $x_i \circ \psi$ is a regular function by definition, so only the converse needs proof. Suppose that $x_i \circ \psi$ is regular. Then for any polynomial $f \in A[n] \cong k[x_1, \ldots, x_n]$, $f \circ \psi$ is also a regular function. Since the closed sets of Y are defined by polynomials f_j, their preimages under ψ are given by $\psi^* f_j(x_i) = f(\psi^* x_i) = 0$. By assumption, these functions are regular and in particular continuous. Hence the preimage is also closed and ψ is therefore continuous. Finally, since regular functions are locally quotients of polynomials, $\psi^* g = g \circ \psi$ is regular for any regular function $g \in \mathcal{O}_Y(U)$. Hence ψ is a morphism. □

134. Example (the cuspidal curve). Consider the map $\varphi : \mathbb{A}^1 \to \mathbb{A}^2$, $\varphi(t) = (t^2, t^3)$ onto the *cuspidal curve* $Y = \mathcal{Z}(x^3 - y^2) \subset \mathbb{A}^2$. By Lemma 1.133, φ is regular. We can check this directly, since $\varphi^* f(t) = f(t^2, t^3)$ is a polynomial if f is a polynomial. More precisely, let $f \in \mathcal{O}_Y(V)$. Locally, $f(\bar{x}, \bar{y}) = g(\bar{x}, \bar{y})/h(\bar{x}, \bar{y})$ for g, $h \in A[2]$, where $\bar{x}$ and $\bar{y}$ are the "coordinate functions" in $A(Y) = k[x, y]/(y^2 - x^3)$. Therefore, $\varphi^* f(t) = g(t^2, t^3)/h(t^2, t^3)$ for $t \in U$ open with $\varphi(U) \subset V$. Further, φ is bijective and bicontinuous. Indeed, its inverse is given by $\psi : Y \to \mathbb{A}^1$, $\psi(x, y) = y/x$ if $x \neq 0$, and $\psi(0, 0) = 0$. Since φ takes finite sets of $\mathbb{A}^1$ (these are the closed sets of $\mathbb{A}^1$ modulo $\mathbb{A}^1$ and $\varnothing$) to finite sets of Y, whence ψ is continuous. However, we will see in Example 1.137 that its inverse cannot be regular, so that $\mathbb{A}^1$ and Y are homeomorphic, but not isomorphic as varieties.

The next proposition characterises morphisms of affine varieties.

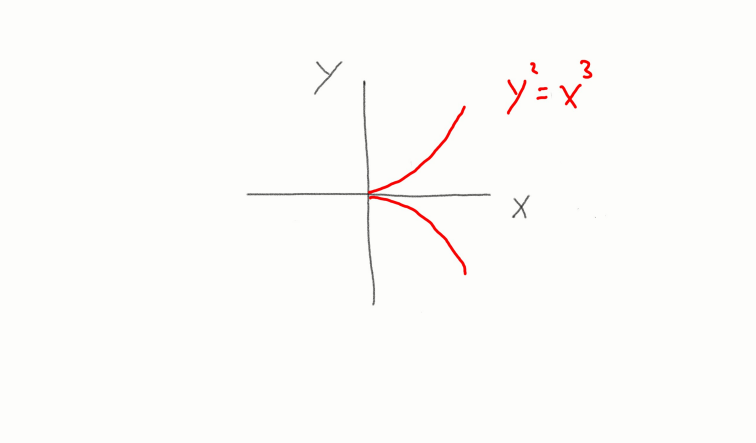

FIGURE 9. The curve $y^2 = x^3$

135. Proposition. *Let X be any variety and $Y \subset \mathbb{A}^m$ be an affine variety. Then there is a natural bijective mapping of sets*

$$\mathrm{Mor}(X, Y) \cong \mathrm{Mor}(\mathcal{A}(Y), \mathcal{O}(X)),$$

where the right hand side means morphism of k-algebras. In particular, if $X \subset \mathbb{A}^n$ is also affine, then $\mathcal{O}(X) \cong A(X)$ and any k-algebra homomorphism $\Phi : A(Y) \to A(X)$ is of the form $\varphi^* = \Phi$ for a uniquely determined regular map $\varphi : X \to Y$. Hence in this case, the bijection is provided by

Proof. Given a morphism $\varphi : X \to Y$ we get by definition a map $\varphi^* : \mathcal{O}(Y) \to \mathcal{O}(X)$. Since Y is affine, $\mathcal{O}(Y) \cong A(Y)$ by Proposition 1.93 we get the desired k-algebra morphism $A(Y) \to \mathcal{O}(X)$.

Conversely, let $\Phi : A(Y) \to \mathcal{O}(X)$ be a k-algebra morphism. Choose coordinate functions $y_1, \ldots, y_m$ on $\mathbb{A}^m$ so that $A(Y) = k[y_1, \ldots, y_m]/\mathcal{I}(Y)$. We define $\varphi_i = \Phi(\bar{y}_i) \in A(X)$ and $\varphi : X \to \mathbb{A}^m$ by $\varphi(a) = (\varphi_1(a), \ldots, \varphi_m(a))$. This is a regular map by Lemma 1.133. We show that its image is contained in Y. Indeed, let $g \in \mathcal{I}(Y)$, that is, $g(\bar{y}_1, \ldots, \bar{y}_m) = 0$ in $A(Y)$. Here, we look at g as a relation between the coordinate functions $\bar{y}_i$ of Y. Since Φ is a k-algebra morphism, we have

$$\Phi(g(\bar{y}_1, \ldots, \bar{y}_m)) = g(\Phi(\bar{y}_1), \ldots, \Phi(\bar{y}_m)) = g(\varphi_1, \ldots, \varphi_m) = 0,$$

hence $g(\varphi_1(a), \ldots, \varphi_m(a)) = 0$ for all $a \in X$, i.e. $\varphi(X) \subset Y$. In order to show that $\varphi^* = \Phi$ it is enough to see that they agree on the generators $\bar{y}_i$ of $A(Y)$. But $\varphi^*(\bar{y}_i) = \varphi_i = \Phi(\bar{y}_i)$. Moreover, φ is uniquely determined by this condition. □

In terms of category theory, the previous proposition just says that in the case of affine varieties X and Y, the assignement $X \mapsto A(X)$ is full and faithful (cf. Definition A.6), whence the

136. Corollary. *Two affine varieties X and Y are isomorphic if and only if $A(X)$ and $A(Y)$ are isomorphic as k-algebras. Put differently, X and Y are isomorphic if and only if X and Y carry the "same" global functions. In particular, this establishes an equivalence between the category of affine varieties and the category of finitely generated k-algebras which are integral domains.*

137. Example (the cuspidal curve again). Consider again Example 1.134 where $\varphi : X = \mathbb{A}^1 \to Y \subset \mathbb{A}^2$, $\varphi(t) = (t^2, t^3)$. Then $A(\mathbb{A}^1) = A[1] = k[t]$, while $A(Y) = k[x,y]/(x^2 - y^3)$. Then $\varphi^*(\bar{x}) = t^2$ and $\varphi^*(\bar{y}) = t^3$ so that the image of φ^* is the k-subalgebra of $k[t]$ generated by t^2 and t^3 which is proper (it does not contain t for instance). Intuitively, the reason is that $X = \mathbb{A}^1$ has a polynomial function with non-zero derivative, while Y has a "singularity" at $(0,0)$ (see Figure 1.9) which squahes up the derivative of any polynomial function at 0. In this sense, Y has fewer regular functions than X. We will discuss the issues further in Chapter 3.

138. Proposition. *Let $f \in A[n]$. Then the basic open set $D_f = \mathbb{A}^n \backslash \mathcal{Z}(f)$ is isomorphic to the hypersurface $H \subset \mathbb{A}^{n+1}$ given by $x_{n+1} f = 1$ (see Figure 1.10 and cf. also 1.91).*

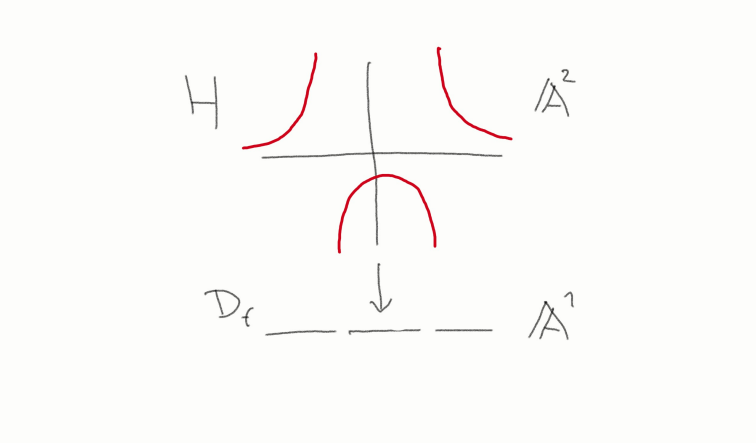

FIGURE 10. The coordinate ring of D_f, $f = x^2 - 1$

Proof. If $a = (a_1, \ldots, a_{n+1}) \in H$, then $f(a_1, \ldots, a_n) \neq 0$ and $a_{n+1} = 1/f(a_1, \ldots, a_n)$. Let $\varphi : H \to D_f$ be defined by $\varphi(a) = (a_1, \ldots, a_n)$. As a set-theoretic map, this has an inverse $\psi : D_f \to H$ defined by $\psi(a_1, \ldots, a_n) = (a_1, \ldots, a_n, 1/f(a_1, \ldots, a_n))$. By Lemma 1.133, φ and ψ are morphisms. □

139. Remark. By Proposition 1.135 we see that

$$A(H) = \mathcal{O}(D_f) \cong k[x_1, \ldots, x_n]_f = \{g/f^n \mid g \in k[x_1, \ldots, x_n],\ n \in \mathbb{N}\}.$$

140. Exercise (Quasi-affine varieties which are not affine). *Show that the quasi-affine variety $X = \mathbb{A}^2 \backslash \{(0,0)\}$ is not affine.*

Hint: Consider the inclusion $i : X \hookrightarrow \mathbb{A}^2$ and use Proposition 1.135.

Proof. The k-algebra morphism $i^* : A[2] = k[x,y] \to \mathcal{O}(X)$ induced by the inclusion is just restriction of polynomial functions. Since by Corollary 1.67, polynomial functions are determined by their restriction to any open set, and thus in particular to $X \subset \mathbb{A}^2$, i^* is injective, and we can regard $k[x,y]$ as a subring of $\mathcal{O}(X)$. Now take $a \in X \subset \mathbb{A}^2$. By Exercise 1.70, $\mathcal{O}_{X,a} = \mathcal{O}_{\mathbb{A}^2,a} = k[x,y]_{\mathfrak{m}_a} \subset k(x,y)$, where $\mathfrak{m}_a$ is the maximal ideal corresponding to $a \in X$. It follows that $\mathcal{O}(X) \subset \bigcap_{a \in X} \mathcal{O}_{X,a} \subset k(x,y)$. If $f/g \in \mathcal{O}(X)$ with $f,\ g \in k[x,y]$, then for any $a \in X$, $g(a) \neq 0$ for $f/g \in k[x,y]_{\mathfrak{m}_a} = \{h_1/h_2 \mid h_i \in k[x,y],\ h_2(a) \neq 0\}$. Hence $\mathcal{Z}(g) \subset \mathbb{A}^2$ is either

empty (in which case g is a unit) or contains only the origin $(0,0)$. But then the ideal (g) must be maximal in $k[x,y]$ which is absurd. Hence g is a unit so that $f/g \in k[x,y]$. Hence i^* provides an isomorphism $k[x,y] \cong \mathcal{O}(X)$, which implies that i is a biregular map by Proposition 1.135. This is absurd, for i is not even surjective. □

Next we dicuss regular maps for (quasi-)projective varieties. First we note that the standard cover $U_i = \mathcal{Z}_p(x_i)$ of $\mathbb{P}^n$ is not only open, but also *affine*.

141. Lemma (the open cover of $\mathbb{P}^n$ by affine varieties). *Let $U_i \subset \mathbb{P}^n$ be the open subset defined by the equation $x_i \neq 0$. Then the mapping $\varphi_i : U_i \to \mathbb{A}^n$ is an isomorphism of varieties (cf. Exercise 1.49).*

Proof. Without loss of generality we assume that $i = 0$ and put $\varphi = \varphi_0$ and $U = U_0$. We need to show that φ and $\psi = \varphi^{-1}$ are regular. Now locally, a regular function f on $V \subset \mathbb{A}^n$ is the quotient of two polynomials g and h in $y_1, \ldots, y_n$ which under φ^* gets mapped to

$$\varphi^* f = \varphi^*(g/f) = g(x_1/x_0, \ldots, x_n/x_0)/h(x_1/x_0, \ldots, x_n/x_0) = x_0^{\deg h - \deg g}\beta(g)/\beta(h)$$

which is the quotient of two homogeneous polynomials of degree $\deg h$. Conversely, the action of ψ^* corresponds to the action of α on the denominator and numerator. □

142. Example. For $\mathbb{P}^1$ we have the two maps $\varphi : U_0 \to \mathbb{A}^1$, $\varphi[x_0 : x_1] = x_1/x_0$ and $\varphi : U_1 \to \mathbb{A}^1$, $\varphi[x_0 : x_1] = x_0/x_1$. Note that if we define a biregular map $f : k^* \to k^*$ by $f(x) = 1/x$, then $f \circ \varphi_0 = \varphi_1$. Put differently, we have glued the two affine open sets U_0 and U_1 by the biregular map f.

Lemma 1.141 is a special case of the following general fact.

143. Corollary (base for the Zariski topology). *On any variety there exists a base for the topology consisting of open affine subsets. In particular, any point admits an affine neighbourhood.*

Proof. We must show that for any $a \in X$, and any open set U containing a, there exsists an affine set V in U which contains a. Since U is a variety, we may as well assume that $X = U$. Further, any variety is covered by quasi-affine varieties, we may assume that $X \subset \mathbb{A}^n$ is quasi-affine. Consider then $Y = \bar{X}\backslash X$ which is closed in $\mathbb{A}^n$, and let $\mathfrak{a} = \mathcal{I}(Y)$. Then $\mathcal{Z}(\mathfrak{a}) = Y$ by Proposition 1.18 so that we can find $f \in \mathfrak{a}$ with $f(a) \neq 0$. Let $H = \mathcal{Z}(f) \subset \mathbb{A}^n$. Since $a \notin H$, $a \in V := X\backslash(X \cap H) = X \cap H^c$, which is an open subset of X. On the other hand, $X\backslash(X \cap H) = X \cap D_f$ is a closed subset of $D_f = \mathbb{A}^n\backslash H$, hence equal to it. By the previous proposition, D_f is affine, hence V is the desired open affine subset. □

As an application, we prove the following

144. Lemma. *If $X \subset \mathbb{P}^n$ is a quasi-projective variety, and $f_0, \ldots, f_m \in S[n]$ are homogeneous polynomials of same degree in the homogeneous coordinates on $\mathbb{P}^n$ without any common zero, then*

$$f : X \to \mathbb{P}^m, \quad p \in X \mapsto [f_0(p) : \ldots : f_m(p)]$$

defines a morphism.

Proof. The assumptions on the f_i imply that f is well-defined set-theoretically as well as continuous. To verify that f defines a morphism we can work locally on the open set $V_i = f^{-1}(U_i) = \{p \in X \mid f_i(p) \neq 0\}$, where U_i is the standard affine cover of $\mathbb{P}^m$. In the coordinates provided by U_i, $f|_{V_i} = (f_j/f_i)_{j \neq i}$, so f is a morphism since its components are regular being locally quotients of polynomials. □

145. Corollary (Segre embedding). *Let $\mathbb{P}^N = \mathbb{P}^{(n+1)(m+1)-1}$ be projective space with homogeneous coordinates z_{ij}, $0 \leqslant i \leqslant n$, $0 \leqslant j \leqslant m$. if $x_0, \ldots, x_n$, $y_0, \ldots, y_m$ are homogeneous coordinates on $\mathbb{P}^n$ resp. $\mathbb{P}^m$, consider the map $\varphi : \mathbb{P}^n \times \mathbb{P}^m \to \mathbb{P}^N$ given by $\varphi([x_i], [y_j]) = [z_{ij}] = [x_i y_j]$. Then φ defines a bijection onto the image $\Sigma_{n,m} = \varphi(\mathbb{P}^n \times \mathbb{P}^m)$ which is a projective variety in $\mathbb{P}^N$ with ideal generated by $z_{ij}z_{kl} - z_{il}z_{kj}$ for all $0 \leqslant i, k \leqslant n$ and $0 \leqslant j, l \leqslant m$. The map φ is called the* **Segre embedding**. *It gives $\mathbb{P}^n \times \mathbb{P}^m$ the structure of a projective variety by identifying the product with $\Sigma_{n,m} \subset \mathbb{P}^N$.*

Proof. The inclusion $\varphi(\mathbb{P}^n \times \mathbb{P}^m) \subset \Sigma_{n,m}$ is obvious. Conversely, let $a = [a_{ij}] \in \Sigma_{n,m} \subset \mathbb{P}^N$ so that $a_{ij}a_{kl} - a_{ik}a_{jl} = 0$. At least one $a_{ij} \neq 0$; without loss of generality, $a_{00} \neq 0$ so that $a \in U_0$. We pass to affine coordinates by setting $a_{00} = 1$, hence a corresponds to the point $(a_{ij})_{(i,j) \neq (0,0)} \in \mathbb{A}^N$. But $a_{ij} = a_{ij}a_{00} = a_{i0}a_{0j}$ for $a \in X$, hence $a_{ij} = x_i y_j$ and $a = \varphi([x_0 : \ldots : x_n], [y_0 : \ldots : y_m])$. To show injectivity let $a = f(x, y) \in X$ be a point with $a_{00} = 1$. Hence $x_0, y_0 \neq 0$. We can scale the homogeneous coordinates of x and y such that $x_0 = y_0 = 1$. Then $x_i = z_{i0}$ and $y_j = z_{0j}$, hence φ is injective. It is clear that φ is regular by Lemma 1.144. Computing the inverse in affine coordinates shows that φ^{-1} is locally a polynomial map, hence also regular. To show that X is irreducible, let $q_n : \Sigma_{n,m} \to \mathbb{P}^n$ and $q_m : \Sigma_{n,m} \to \mathbb{P}^m$ be defined on U_{ij}, the set of points where $z_{ij} \neq 0$, by $q_n([z_{ij}]) = [z_{ij}]_{i=0}^n$ and $q_m([z_{ij}]_{j=0}^n$. We obtain a commutative diagramm

$$\begin{array}{ccc} & & \mathbb{P}^n \\ & \overset{\pi_n}{\nearrow} & \uparrow{\scriptstyle q_n} \\ \mathbb{P}^n \times \mathbb{P}^m & \xrightarrow{\varphi} & \Sigma_{n,m} \\ & \underset{\pi_m}{\searrow} & \downarrow{\scriptstyle q_m} \\ & & \mathbb{P}^m \end{array} \tag{3}$$

where π_i denotes the natural projection. Restricting the Segre embedding to $\mathbb{P}^n \times \{[y]\}$ and $\{[x]\} \times \mathbb{P}^m$ induces isomorphisms between $\mathbb{P}^n$ and $\mathbb{P}^m$ and subspaces of $\mathbb{P}^N$ whose fibres are irreducible. We can now imitate the proof of irreducibility for the product of two affine varieties from Example 1.29. □

146. Remark. As for affine varieties, the topology on $\mathbb{P}^n \times \mathbb{P}^m$ is *not* the product topology. In fact, the closed sets of $\mathbb{P}^n \times \mathbb{P}^m$ with its induced structure as projective variety via the Segre embedding are given by the zero loci of bihomogeneous polynomials in $k[x_1, \ldots, x_n, y_1, \ldots, y_m]$, that is, polynomials which are separately homogeneous in the x_i and y_j. Indeed, the zero locus of bihomogenous polynomials can be written as the zero locus of bihomogeneous polynomials of the same degree in the x_i and y_j (cf. Remark 1.44 (ii)) and are thus polynomials in the z_{ij}, that is, the zero locus defines a closed subset for the topology induced by $\mathbb{P}^N$. Conversely, if a subset of $\Sigma_{n,m} \cong \mathbb{P}^n \times \mathbb{P}^m$ is given as the zero locus of polynomials in the z_{ij},

substituting $z_{ij} = x_i y_j$ yields a bihomogeneous polynomial. In particular, if X and Y are projective varieties sitting inside $\mathbb{P}^n$ and $\mathbb{P}^m$ respectively then $X \times Y \subset \Sigma_{n,m}$ is again projective for it is closed while irreducibility follows as in the affine case, cf. Proposition 1.29.

147. Example. Consider the case $n = m = 1$. Then $\Sigma_{1,1} = \varphi(\mathbb{P}^1 \times \mathbb{P}^1) \subset \mathbb{P}^3$ is the quadric surface given by $\mathcal{Z}(z_{00}z_{11} - z_{10}z_{01})$. Explicitly, we have the isomorphism

$$\mathbb{P}^1 \times \mathbb{P}^1 \to \Sigma_{1,1}, \quad \big([x_0 : x_1], [y_0 : y_1]\big) \mapsto [x_0y_0 : x_0y_1 : x_1y_0 : x_1y_1] \in X.$$

In particular, the families of projective lines $\mathbb{P}^1 \times \{a\}$ and $\{b\} \times \mathbb{P}^1$ get mapped to the families of lines L_a and M_b in $\mathbb{P}^3$, see Figure 1.11 below.

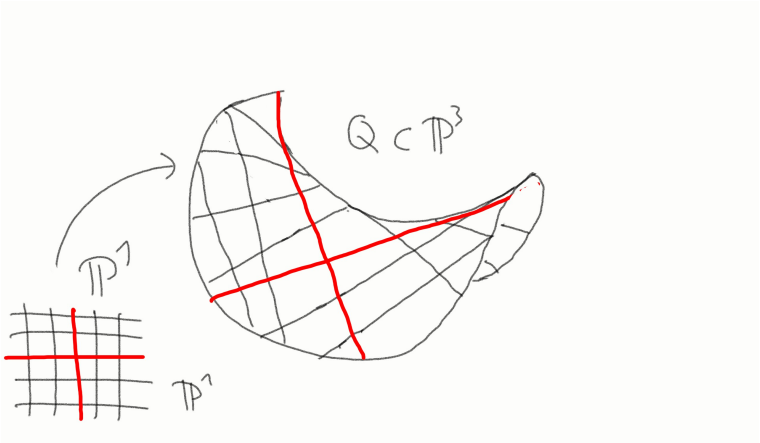

FIGURE 11. The Segre embedding of $\mathbb{P}^1 \times \mathbb{P}^1$ and the two families of lines

148. Exercise (products of quasi-projective varieties). *We consider $\mathbb{P}^n \times \mathbb{P}^m$ as a projective variety via the Segre embedding. If $X \subset \mathbb{P}^n$ and $Y \subset \mathbb{P}^m$ are two quasi-projective varieties, consider the (set theoretic) product $X \times Y \subset \mathbb{P}^n \times \mathbb{P}^m$. Show that $X \times Y$ is a quasi-projective variety.*

Proof. If X and Y are quasi-projective, then $X = U \cap W$ and $Y = V \cap Z$ for U and V open and W and Z closed in $\mathbb{P}^n$ and $\mathbb{P}^m$ respectively. But $\varphi(X \times Y) = q_n^{-1}(X) \cap q_m^{-1}(Y)$ (cf.(3)) so that the image is an open set of a closed subset. That the image is irreducible follows as in the affine case, cf. Proposition 1.29. □

Lemma 1.141 can be also used to describe the stalk of regular functions of $\mathbb{P}^n$. As in the case of affine varieties, the stalk can be described in terms of localisation. First, however, we need to discuss how to put a grading on these localised rings.

149. Localisation of graded rings. Let $S = \bigoplus_{d \geqslant 0} S_d$ be a graded ring, and let $T \subset S$ be a multiplicatively closed system of *homogeneous* elements. To give the ring of fractions $T^{-1}S$ the structure, we say that f/g is **homogeneous** if $f \in S$ is homogeneous and put $\deg(f/g) := \deg f - \deg g$. If this is well-defined, then we have a decomposition $T^{-1}S = \bigoplus_{d \geqslant 0} (T^{-1}S)_d$ which gives indeed a grading. Now if $f/g = f'/g'$, then there exists $h \in T$ such that $h(fg' - f'g) = 0$, hence

$\deg h + \deg f + \deg g' = \deg h + \deg f' - \deg g$ so that deg is well-defined on $T^{-1}S$. We then put

$$S_{(T)} := \{f/g \in T^{-1}S \mid f/g \text{ is homogeneous of degree } 0\}.$$

The notation is slightly ambigous but standard in the literature. The most important examples are these:

(i) If $\mathfrak{p} \subset S$ is a homogeneous prime ideal we let $T_{\mathfrak{p}} = \bigcup_{d \geqslant 0}\{f \in S_d \mid f \notin \mathfrak{p}\}$ and write $S_{(\mathfrak{p})}$ for $S_{(T_{\mathfrak{p}})}$. This is a local ring with maximal ideal $(\mathfrak{p}T_{\mathfrak{p}}^{-1}S) \cap S_{(\mathfrak{p})}$. In particular, if S is an integral domain, then for $\mathfrak{p} = (0)$ we obtain the field $S_{((0))}$.

(ii) If $f \in S_h$, then $T_f = \{f^k \mid k \geqslant 0\}$ is a multiplicative subset of homogeneous elements. We let $S_{(f)} := S_{(T_f)}$ be the subring of elements of degree 0 in the localised ring S_f.

150. Proposition (regular functions on $\mathbb{P}^n$). *Let $X \subset \mathbb{P}^n$ be a projective variety with homogeneous coordinate ring $S(X)$. Then*

(i) *for any $a \in X$, let $\mathfrak{m}_a \subset S(X)$ be the ideal generated by the set of homogeneous $f \in S(X)$ such that $f(a) = 0$. Then $\mathcal{O}_{X,a} = S(X)_{(\mathfrak{m}_a)}$;*

(ii) $K(X) \cong S(X)_{((0))}$;

Proof. We start with the following general remark. If $X \subset \mathbb{P}^n$ is a projective variety, and $\varphi : U_i \to \mathbb{A}^n$ a standard chart, then $A(X_i) = S(X)_{(x_i)}$ where $X_i = X \cap U_i$ (in particular, $\bar{X}_i = X$ so that by Exercise 1.52, $\mathcal{I}(X)$ is the ideal generated by $\beta(\mathcal{I}(X_i))$). Put differently, the regular functions on the (affine) variety X_i are the degree 0 functions in the localised ring $S(X)_{x_i}$. Indeed, let $i = 0$, $\varphi_i = \varphi$ and $U_i = U$ for convenience. Then $\varphi^* f = f(x_1/x_0, \ldots, x_n/x_0) \in k[x_0, \ldots, x_n]_{(x_i)}$. Clearly, φ^* is an isomorphism between $A[n]$ and $k[x_0, \ldots, x_n]_{(x_i)}$. A polynomial $f \in A[n]$ of degree d gets mapped to $\beta(f)/x_0^d$. It follows that under this isomorphism, $\mathcal{I}(X_0)$ is mapped to the ideal generated by $F/x_0^{\deg F}$ for $F \in \mathcal{I}(X)$ homogeneous. Hence $A(X)/\mathcal{I}(X) \cong k[x_0, \ldots, x_n]_{(x_0)}/\langle F/x_0^d \mid F \in \mathcal{I}(X)_d\}\rangle$. It is easy to see that the latter ring is isomorphic to $S(X)_{(\bar{x}_0)}$ by sending $[f/x_0^{\deg f}] \in k[x_0, \ldots, x_n]_{(x_0)}/\langle F/x_0^d \mid F \in \mathcal{I}(X)_d\}\rangle$ to $\bar{f}/\bar{x}_0^{\deg f}$ where $\bar{\cdot}$ denotes the equivalence class in $S(X)$.

(i) If $a \in X$ choose i such that $a \in X_i$. In particular, $x_i(a) \neq 0$. Without loss of generality we assume again $i = 0$. The associated maximal ideal $\mathfrak{m}'_a \subset A(X_0)$ consists of functions $f \in A(X_0)$ such that $f(a) = 0$. Under the isomorphism $A(X_0) \cong S(X)_{(\bar{x}_0)}$ this gets mapped to the maximal ideal $\mathfrak{m}_a$. Therefore, $\mathcal{O}_{X,a} \cong A(X_0)_{\mathfrak{m}_a} \cong (S(X)_{(\bar{x}_0)})_{\mathfrak{m}_a}$. Since x_0 is a unit, Corollary 1.101 gives the result.

(ii) $K(X)$ is isomorphic to $K(X_i) = \operatorname{Quot} A(X_i)$. Via φ_i^*, the latter is isomorphic to $S(X)_{((0))}$. □

Rational maps and blow-ups. As we have seen in Section 1.3, $A[n]_{\mathfrak{p}}$ has the interpretation of functions which are generically defined on $X = \mathcal{Z}(\mathfrak{p})$. We also introduced the function field $K(X)$ of rational functions in Section 1.2. Next we generalise this notion to rational maps and define a further category of varieties.

151. Lemma (Identity property of morphisms). *Let φ and ψ be two morphisms between varieties $X \to Y$, and suppose there is a nonempty open subset $U \subset X$ such that $\varphi|_U = \psi|_U$. Then $\varphi = \psi$.*

Proof. We may assume that $Y \subset \mathbb{P}^n$ for some n. By composing with this inclusion we may assume that $Y = \mathbb{P}^n$. The morphisms φ and $\psi : X \to \mathbb{P}^n$ determine a morphism $\varphi \times \psi : X \to \mathbb{P}^n \times \mathbb{P}^n$ with projective target by 1.145. Let $\Delta = \{(p,p) \mid p \in \mathbb{P}^n\} \subset \mathbb{P}^n \times \mathbb{P}^n$ be the *diagonal* of $\mathbb{P}^n \times \mathbb{P}^n$. If $[x_0 : \ldots : x_n]$ and $[y_0 : \ldots : y_n]$ denote the homogeneous coordinates on the left resp. right hand side factor, $\Delta = \mathcal{Z}(\{x_i y_j - x_j y_i \mid i, j = 0, 1, \ldots, n\})$, so Δ is a closed subset. By assumption, $\varphi \times \psi(U) \subset \Delta$. But U is dense in X, i.e. $\bar{U} = X$, and Δ is closed in $\mathbb{P}^n \times \mathbb{P}^n$, whence $\varphi \times \psi(X) \subset \overline{\varphi \times \psi(U)} \subset \Delta$. Hence $\varphi = \psi$. □

We are now prepared for the

152. Definition (rational map). Let X, Y be varieties. A **rational map** $\Phi : X \dashrightarrow Y$ is an equivalence class of pairs $[U, \phi]$, where U is a nonempty open subset of X and $\phi : U \to Y$ a morphism, and where $[U, \phi] = [V, \psi]$ if ϕ and ψ agree on $U \cap V$. By Corollary 1.151 this actually defines an equivalence relation. The rational map Φ is called **dominant**, if for some, hence for every pair $[U, \phi]$ representing Φ, the image $\phi(U)$ is dense in Y (use again that $f(\bar{U}) \subset \overline{f(U)}$ for f continuous).

153. Remark. Despite appearance, a rational map is not a map from $X \to Y$ which is what we indicate by an dotted arrow; it is only densely defined on X. The identity property 1.151 shows that the underlying equivalence relation is well-defined. Indeed, if $[U, \phi] = [V, \psi]$ so that $\phi|_{U \cap V} = \psi|_{U \cap V}$, and $[V, \psi] = [W, \eta]$, whence $\psi|_{W \cap V} = \eta|_{W \cap V}$, it follows that $\phi|_{U \cap V \cap W} = \eta|_{U \cap V \cap W}$, hence $\phi|_{U \cap W} = \eta|_{U \cap W}$ for $U \cap V \cap W$ is dense in $U \cap W$. However, we cannot compose rational maps in general which is why we also consider dominant maps: The composition of two dominant maps is indeed well-defined and again dominant: If $\Phi : X \dashrightarrow Y$ and $\Psi : Y \dashrightarrow Z$ are rational maps represented by $[U, \phi]$ and $[V, \psi]$ respectively, we define $\Psi \circ \Phi : X \dashrightarrow Z$ by $[U \cap \phi^{-1}(V), \psi \circ \phi]$ provided $\phi^{-1}(V)$ is not empty. If it were empty, then $\phi(X) \subset Y \backslash V$, hence $\overline{\phi(X)} = V^c = Y$, whence $V = \varnothing$, a contradiction. To understand this condition from a more algebraic point of view, we note that a rational map $\Phi : X \dashrightarrow Y = [U, \phi]$ induces a map

$$\Phi^* : A(Y) \to K(X), \quad f \mapsto \Phi^* f = [U, f \circ \phi].$$

Then we have $\Phi^*(f) = 0 \Leftrightarrow \phi(U) \subset \mathcal{Z}(f)$, whence Φ^* is injective $\Leftrightarrow$ Φ is dominant. We can then extend Φ^* to a morphism

$$\Phi^* : K(Y) \to K(X), \quad \Phi^*[V, f] = [U \cap \phi^{-1}(V), f \circ \phi]$$

which is well-defined in view of the dominance of Φ. In particular, if $\Psi : Y \dashrightarrow Z$, then $(\Psi \circ \Phi) : A(Z) \to K(X)$ can be computed via

$$(\Psi \circ \Phi)^* f = [U, f \circ \psi\phi] = [U \cap \phi^{-1}(V), f \circ \psi \circ \phi] = \Phi^*[V, f \circ \psi] = \Phi^* \Psi^* [V, f]$$

which shows that $\Psi \circ \Phi$ is dominant if Ψ and Φ are dominant and that $(\Psi \circ \Phi)^* = \Phi^* \circ \Psi^* : K(Z) \to K(X)$. We therefore can define the **category of varieties and dominant rational maps RAT**.

In analogy with Proposition 1.135 which asserted that k-algebra morphism $A(Y) \to A(X)$ are of the form φ^* for a regular map $\varphi : X \to Y$ we can prove the

154. Proposition. *If X and Y are affine varieties, any k-algebra morphism $f : K(Y) \to K(X)$ is of the form $f = \Phi^*$ for a unique dominant rational map $\Phi : X \dashrightarrow Y$.*

Proof. Construction and uniqueness are precisely as in 1.135. Furthermore, Φ^* is necessarily injective since it it nontrivial, hence Φ is injective by Remark 1.153. Hence Φ is dominant. □

Recall that a field extension $k \subset K$ is **finitely generated** if K is a finite extension of $k(x_1, \dots, x_r)$ for algebraically independent elements $\alpha_i \in K$ (cf. also Appendix B). Equivalently, $K = k(\alpha_1, \dots, \alpha_s)$ for $\alpha_i = K$, that is, K coincides with the smallest subfield of K which contains k and the α_i.

155. Corollary (equivalence of RAT with the category of finitely generated field extensions). *For any two varieties X and Y we have a bijection between*

(i) *the set of dominant rational maps $X \dashrightarrow Y$;*
(ii) *the set of k-algebra homomorphisms $K(Y) \to K(X)$.*

This correspondence gives a contravariant equivalence of the categories **RAT** *and finitely generated field extensions $k \subset K$.*

Proof.

Step 1. *Construction of the bijection.* Let $[U, \varphi] = \varphi : X \dashrightarrow Y$ be a dominant rational map, and let $[V, f] \in K(Y)$ be a rational function. Since $\varphi(U)$ is dense in Y, $\varphi^{-1}(V)$ is a nonempty open subset of X, whence $\varphi^* f := f \circ \varphi$ is a regular function on $\varphi^{-1}(U)$, and thus defines a rational function $[\varphi^{-1}(U), f] \in K(X)$. One easily checks that $\varphi^* : K(Y) \to K(X)$ is a k-algebra homomorphism.

Step 2. *Construction of the inverse.* Let $\theta : K(Y) \to K(X)$ be a homomorphism of k-algebras. We define a rational map $\varphi : X \dashrightarrow Y$ as follows. By Proposition 1.143 Y is covered by affine varieties. Since rational maps are only densely defined anyway, we may assume that Y is affine. Let $y_1, \dots, y_n$ be generators of the k-algebra $A(Y)$. Then $\theta(y_1), \dots, \theta(y_n)$ are rational functions on X. Taking the intersection of the domains of the representatives we can find an open set U in X such that $\theta(y_i)$ are regular on U. In particular, we get an injective morphism $A(Y) \to \mathcal{O}_X(U)$. By Proposition 1.135 this corresponds to a morphism $U \to Y$ giving a dominant rational map $X \dashrightarrow Y$ which is an inverse to the map constructed in the first step.

Step 3. Finally, we need to show that for any variety X, $K(X)$ is finitely generated over k, and conversely, if $k \subset K$ is a finitely generated field extension, then $K = K(X)$ for some variety X. Since $K(U) = K(X)$ for any open subset U of X, we may assume that X is affine. But then Proposition 1.94 implies that $K(X) = \operatorname{Quot} A(X)$. Since $A(X) = k[\alpha_1, \dots, \alpha_r]$ we have $K(X) = k(\alpha_1, \dots, \alpha_r)$, that is, $K(X)$ is finitely generated. On the other hand, if $k \subset K$ is any finitely generated field extension, let $K = k(\alpha_1, \dots, \alpha_r)$. Then $A = k[\alpha_1, \dots, \alpha_r]$ is a finitely generated k-algebra without any zerodivisors, hence $A = A(X)$ for some affine variety X. It follows that $K = K(X)$.

□

156. Corollary and Definition (birational maps). An isomorphism in this category is called a **birational map**. This is a rational map $\Phi : X \dashrightarrow Y$ which admits an inverse $\Psi : Y \dashrightarrow X$ such that $\Psi \circ \Phi = \mathrm{Id}_X$ and $\Phi \circ \Psi = \mathrm{Id}_Y$ as rational maps. If there is a birational map between X and Y we call X and Y **birationally equivalent** or simply **birational**.

157. Corollary. *For any two varieties X and Y, the following are equivalent:*

(i) *X and Y are birationally equivalent;*
(ii) *there are open subsets $U \subset X$ and $U \subset Y$ with U isomorphic to V;*
(iii) *$K(X) \cong K(Y)$ as k-algebras.*

Proof. (i) $\Rightarrow$ (ii) Let $\Phi : X \dashrightarrow Y$ and $\Psi : Y \dashrightarrow X$ be rational maps which are inverse to each other and which are represented by $[U, \varphi]$ and $[V, \psi]$ respectively. Then $\Psi \circ \Phi$ is represented by $[\varphi^{-1}(V), \psi \circ \varphi]$ and since $\Psi \circ \Phi = \mathrm{Id}_X$ as rational maps, $\psi \circ \varphi$ is the identity on $\phi^{-1}(V)$. Similarly, $\varphi \circ \psi$ is the identity on $\psi^{-1}(U)$ so that $\varphi^{-1}(\psi^{-1}(U))$ and $\psi^{-1}(\varphi^{-1}(V))$ are isomorphic open sets of X and Y.

(ii) $\Rightarrow$ (iii) follows from the definition of function fields.

(iii) $\Rightarrow$ (i) follows from the previous theorem. □

158. Exercise. *Let X and Y be two varieties. Suppose there are points $p \in X$ and $q \in Y$ such that the local rings $\mathcal{O}_{X,p}$ and $\mathcal{O}_{Y,q}$ are isomorphic as k-algebras. Then there exist open neighbourhoods U and V of p and q respectively as well as a biregular map which identifies U and V and takes p to q.*

Proof. Since any point of a variety admits an affine neighbourhood, and the stalks of regular functions are determined by restriction to any open neighbourhood, we may assume that X and Y are affine. Furthermore, by embedding $\mathbb{A}^m \hookrightarrow \mathbb{A}^n$ we may assume that X, $Y \subset \mathbb{A}^n$ are affine. Let $x_1, \ldots, x_n$ be coordinate functions on $\mathbb{A}^n$ which define regular functions on X by restriction and thus elements in $\mathcal{O}_{X,p}$ which we still denote by x_i. If we have a k-algebra isomorphism $\theta : \mathcal{O}_{X,p} \cong \mathcal{O}_{Y,q}$, then $\theta(x_i)$ define rational functions on Y which are regular on $V_i \subset Y$. Let $\tilde{U} = \bigcap V_i \cap X$. This is an open subset of X on which we can define the map

$$\tilde{\varphi} : \tilde{U} \to Y, \quad \tilde{\varphi}(a) := (\theta(x_1)(a), \ldots, \theta(x_n)(a)).$$

By Lemma... this is a regular map. Similarly, we can define a regular map

$$\tilde{\psi} : \tilde{V} \to X, \quad \tilde{\psi}(a) := (\theta^{-1}(x_1), \ldots, \theta^{-1}(x_n)),$$

where $\theta^{-1}(x_i)$ is regular on U_i and $\tilde{V} = \bigcap U_i \cap Y$. Whenever defined, $\tilde{\varphi}$ and $\tilde{\psi}$ are inverse to each other. Finally, let $U = \tilde{U} \cap \tilde{\varphi}^{-1}(\tilde{V})$ and $V = \tilde{V} \cap \tilde{\varphi}^{-1}(\tilde{U})$ and $\varphi = \tilde{\varphi}|_U$ and $\psi = \tilde{\psi}|_V$. Then $\varphi \circ \psi$ and $\psi \circ \varphi$ are clearly defined and give the identity on U and Y. For instance, let $a \in U$. Then $y = \varphi(a) = \tilde{\varphi}(a) \in \tilde{V} \cap \tilde{\varphi}(\tilde{U})$. It remains to show that $y \in \tilde{\psi}^{-1}(\tilde{U})$ which entails $\varphi(a) = y \in V$. But $\tilde{\psi}(y) = \tilde{\psi}(\tilde{\varphi}(a)) \in \tilde{U}$ by design. Note that $\tilde{\psi}(\tilde{\varphi}(a))$ is defined since $\tilde{\varphi}(a) \in \tilde{V}$. Finally, if $\tau : \mathbb{A}^n \to \mathbb{A}^n$ is the translation $\tau(a) = a - \varphi(p) + q$, the maps $\hat{\varphi} := \tau \circ \varphi : \hat{U} := U \cap \hat{\varphi}^{-1}(U) \to \hat{V} := V \cap \hat{\psi}^{-1}(V)$ and $\hat{\psi} := \psi \circ \tau^{-1} : \hat{V} \to \hat{U}$ are inverse to each other with $\varphi(p) = q$. □

Therefore, despite being "local rings", the stalk of regular functions determines the birational type of the variety. From this point of view, a local ring still contains a lot of global information though birationality is a much weaker concept than biregularity, as the following result shows.

159. Proposition. *Any variety X is birational to a hypersurface $Y \subset \mathbb{P}^n$.*

Proof. (The proof requires some material from Appendix .) The function field $K(X)$ is a finitely generated extension field of k. By Proposition B.14, K is separably generated over k, that is, there exists a transcendence base $x_1, \ldots, x_n$ such that $k(x_1, \ldots, x_n) \subset K$ is a finite separable extension of k. Hence, by the Theorem of the

Primitive Element B.9, $K = k(x_1, \ldots, x_n, \alpha)$. Since α is algebraic over $k(x_1, \ldots, x_n)$ it satisfies a polynomial relation with coefficents given by rational functions in the x_i. Clearing denominators gives an irreducible polynomial $f(x_1, \ldots, x_n, \alpha) = 0$ which defines a hypersurface in $\mathbb{A}^{n+1}$. Its coordinate ring is $A[n+1]/(f)$ so that its quotient ring is $K(X)$. The result follows from Corollary 1.157. □

160. Remark. Once we have a properly defined notion of dimension, we will see that the proof implies that $n-1$ equals the dimension of X.

As a concrete example of a birational map we discuss the notion of *blow up of a variety at a point*. This is a fundamental construction and a main tool in the resolution of singularities of an algebraic variety (cf. Hironaka's theorem which unfortunately – despite its importance – is far beyond the scope of this course).

First we construct the blow up of $\mathbb{A}^n$ at the origin 0. Consider the product $\mathbb{A}^n \times \mathbb{P}^{n-1}$ which is a quasi-projective variety (thinking of $\mathbb{A}^n$ as being embedded into $\mathbb{P}^n$), cf. Exercise 1.148. If $x_1, \ldots, x_n$ are affine coordinates on $\mathbb{A}^n$ and $y_1, \ldots, y_n$ homogeneous coordinates of $\mathbb{P}^{n-1}$ (observe the index shift: we start with 1 instead of 0), then the closed sets of $\mathbb{A}^n \times \mathbb{P}^{n-1}$ are given by polynomials in the x_i, y_i which are homogeneous in the y_i.

161. Definition. We define the **blow up of $\mathbb{A}^n$ at the origin** 0 to be the closed subset X of $\mathbb{A}^n \times \mathbb{P}^{n-1}$ defined by the equations $\{x_i y_j = x_j y_i \mid i, j = 1, \ldots, n\}$.

We have a natural morphism $\varphi : X \to \mathbb{A}^n$ by restriction of the projection onto the first factor. Regularity follows directly from Lemma 1.133. Here are some properties of this map.

162. Proposition (fibres of $\varphi : X \to \mathbb{A}^n$).

(i) *If $a \in \mathbb{A}^n$, $a \neq 0$, then $\varphi^{-1}(a)$ consists of a single point. In fact, φ induces an isomorphism of $X \backslash \varphi^{-1}(0)$ and $\mathbb{A}^n \backslash \{0\}$. In particular, we get a birational isomorphism $X \dashrightarrow \mathbb{A}^n$ (φ is of course defined on X, but its inverse is only densely defined and therefore gives only rise to an inverse in the category* **RAT***).*

(ii) *$E := \varphi^{-1}(0) \cong \mathbb{P}^{n-1}$, the so-called* **exceptional divisor***. In fact, we can think of the points of $\varphi^{-1}(0)$ as the set of lines through 0 in $\mathbb{A}^n$.*

Proof. (i) Let $a = (a_1, \ldots, a_n) \in \mathbb{A}^n$ with some $a_i \neq 0$. Now if $(a, [y_1 : \ldots : y_n]) \in \varphi^{-1}(a))$, then for each j, $y_j = (a_j/a_i)y_i$, so $[y_1 : \ldots : y_n] = [a_1 : \ldots : a_n]$ is uniquely determined as a point in $\mathbb{P}^{n-1}$. Moreover, the map $\psi : \mathbb{A}^n \backslash \{0\} \to X$, $\psi(a) = ((a_1, \ldots, a_n), (a_1, \ldots, a_n))$ defines the inverse morphism.

(ii) Clearly, $(0, [y_1 : \ldots : y_n]) \in X$ for any $[y_1 : \ldots : y_n] \in \mathbb{P}^{n-1}$. Geometrically, we can identify the points in $\varphi^{-1}(0)$ with lines l in $\mathbb{A}^n$ through the origin as follows. If $a = (a_1, \ldots, a_n) \in l \backslash \{0\}$ (whose choice obviously determines l), a parametrisation of l is given by $x_i(t) = a_i t$, $t \in \mathbb{A}^1$. Its preimage $\tilde{l}$ under φ has then the parametrisation $x_i = a_i t$, $y_i = a_i t$, $t \in \mathbb{A}^1 \backslash \{0\}$. Since $[a_1 t : \ldots : a_n t] = [a_1 : \ldots : a_n]$ we can parametrise $\tilde{l}$ by $x_i = a_i t$ and $y_i = a_i$ which also makes sense in $t = 0$ and gives the closure of $\tilde{l}$ in X. But $\tilde{l}$ meets $\mathbb{P}^{n-1} \cong \varphi^{-1}(0)$ precisely in $[a_1 : \ldots : a_n]$. Hence sending the point $[a_1 : \ldots : a_n] \in \varphi^{-1}(0)$ to the line determined by 0 and $a = (a_1, \ldots, a_n)$ sets up a $1-1$-correspondence. □

163. Corollary (irreducibility of the blow up). *X is irreducible.*

Proof. Indeed, X is the union of $X\backslash\varphi^{-1}(0)$ and $\varphi^{-1}(0)$. The first set is isomorphic to $\mathbb{A}^{n-1}\backslash\{0\}$ which is irreducible as an open subset of an affine variety. On the other hand, we have seen that every point $\varphi^{-1}(0)$ is in the closure of some line in $X\backslash\varphi^{-1}(0)$. Hence $X\backslash\varphi^{-1}(0)$ is dense in X so that X is irreducible itself (alternatively, argue by Exercise 1.63). □

164. Definition (blow up a subvariety). If Y is a closed subvariety of $\mathbb{A}^n$ passing through the origin, we define the **blow up of Y at** 0 to be

$$\tilde{Y} = \overline{\varphi^{-1}(Y\backslash\{0\})},$$

where $\varphi : X \to \mathbb{A}^n$ is the blow up of $\mathbb{A}^n$ at the point 0 described above. We keep on denoting by φ the restriction of this map to $\tilde{Y}$. To blow up at any other point $a \in Y$ we make a linear change of coordinates sending a to 0.

165. Remark.

(i) φ induces a birational morphism of $\tilde{Y}$ to Y.

(ii) Although the definition seems to depend on the embedding of Y into $\mathbb{A}^n$ (that is, two isomorphic subvarieties might not have the same blow up), we will see below that the blow up is actually intrinsic and therefore independent of the actual representative of the isomorphism class of subvarieties.

166. Example.

(i) Consider the line $L = \mathcal{Z}(\lambda x - \mu y)$ in $\mathbb{A}^2$. We assume that $\lambda,\ \mu \neq 0$ so that λ/μ is the slope of L. What is the blow up of L at the origin? If we choose the parametrisation $(\mu t, \lambda t)$, then for $\varphi^{-1}(L\backslash\{0\}) = \{(\mu t, \lambda t), [\mu : \lambda] \mid t \neq 0\}$. Therefore, the total inverse image of L under φ consists of two irreducible curves: The exceptional divisor (here: the "exceptional curve") $E = \{(0,0), [u : v]\}$ and the irreducible curve $\tilde{L} = \{(\mu t, \lambda t), [\mu : \lambda] \mid t \in k\}$, the blow up of L, which meets the exceptional curve in $[\mu : \lambda]$, the point corresponding to the line L itself.

(ii) Let Y be the plane cubic curve given by the equation $y^2 = x^2(x+1)$ in $\mathbb{A}^2$. We compute the blow up of Y at 0. The blow up $X = \tilde{\mathbb{A}}^2$ of $\mathbb{A}^2$ at the origin is defined by the equation $xu = yt$ in $\mathbb{A}^2 \times \mathbb{P}^1$ where $[t : u]$ are homogeneous coordinates on $\mathbb{P}^1$. The inverse image of Y under φ is given by the equations $y^2 = x^2(x+1)$ and $xu = ty$ in $\mathbb{A}^2 \times \mathbb{P}^1$. Now $\mathbb{P}^1$ is covered by the two open sets $t \neq 0$ and $s \neq 0$. If $t \neq 0$ we can set $t = 1$ and get the equations

$$y^2 = x^2(x+1), \quad y = xu$$

in $\mathbb{A}^3$ with coordinates x, y and u. Substituting yields $x^2u^2 - x^2(x+1) = 0$. Hence we get two irreducible components given by $x = y = 0$, u arbitrary, which belongs to the exceptional divisor E, and $u^2 = x + 1$, $y = xu$, which belongs to $\tilde{Y}$. Further, $\tilde{Y}$ intersects E in $[1 : \pm 1]$, see Figure 1.12. The solutions $u = \pm 1$ correspond to the different slopes of the two branches of Y in $\mathbb{A}^2$ at the origin; the blow up has thus the property of pulling apart lines of different slope.

167. Exercise. *Let Y be the cuspidal curve $\mathcal{Z}(y^2 - x^3) \subset \mathbb{A}^2$ which we blow up at the origin. Show that the exceptional curve E and the blow up $\tilde{Y}$ meet in one point, and that $\tilde{Y} \cong \mathbb{A}^1$.*

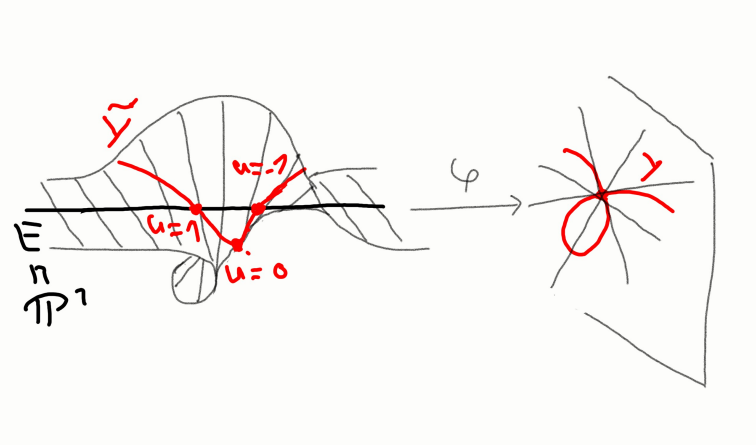

FIGURE 12. The blow up of the plane and the strict transform of a curve.

Remark: In particular, the morphism $\varphi : \tilde{Y} \to Y$ is a homeomorphism, but not biregular.

Proof. We parametrise the cuspidal curve by (t^2, t^3) so that the equation for $\tilde{Y}$ are $t^2 v = t^3 u$. It follows that $\varphi^{-1}(Y \backslash \{0\}) = \{(t^2, t^3), [1 : t]\}$ so that $\tilde{Y}$ intersects E in the point $[1 : 0]$. The rational function $\{(x, y), [u : v]\} \mapsto v/u$ yields a well-defined regular function when restricted to $\tilde{Y}$ which gives the desired isomorphism. □

2. Integral ring extensions and the Nullstellensatz

We now come to the proof of the Nullstellensatz. In its so-called *weak form* it asserts that

if $k \subset K$ is a field extension such that K is of finite type, i.e. finitely generated as a k-algebra, then $k \subset K$ is a finite field extension.

2.1. **Integral ring extensions.**

If we have a field extension $k \subset K$, and $a \in K$ is algebraic over k, then the extension field $k(a)$ is a finite dimensional vector space over k. Indeed, there exists a polynomial $f \in k[x]$ such that $f(a) = \sum c_i a^i = 0$ since a is algebraic. By dividing by the leading coefficient of f we get the relation $a^n = \sum_{i=0}^{n-1} c_i a^i / c_n$. Similarly, if $A \subset B$ are rings we call B an **extension ring** of A and say that $A \subset B$ is a **ring extension**. However, if $f(b) = 0$ for $b \in B$ and $f \in A[x]$, $A[a]$ is in general not a finite-dimensional module as the easy example $\mathbb{Z}[1/2]$ shows. Still, for rings there is a useful analogue of algebraic field extensions which will occupy us next.

1. Definition (integral and finite ring extensions). Let $A \subset B$ be a ring extension.

(i) We call $b \in B$ **integral** over A if there is a monic polynomial $f \in A[x]$ such that $f(b) = 0$. If every $b \in B$ is integral over A, then $A \subset B$ is an **integral extension**.
(ii) The ring extension is **finite** if this turns B into a finitely generated A-module.

2. Remark. If A and B are fields, then integral and finite ring extensions coincide with algebraic and finite field extensions.

3. Algebraic examples.

(i) If A is an integral domain we have the natural ring extension $A \subset k = \operatorname{Quot} A$. In particular, if A is a UFD, then $x \in k$ is integral over $A \Leftrightarrow x \in A$ (see Exercise 0.1).

(ii) $\mathbb{Z} \subset \mathbb{Z}[1/2]$, the subring of $\mathbb{Q}$ generated by $\mathbb{Z}$ and $1/2$, is not integral. Indeed, assume that $x = p/q \in \mathbb{Z}[1/2]$ with $p \in \mathbb{Z}$ and $0 \neq q \in 2\mathbb{Z}$ coprime. If we had a polynomial relation

$$\big(\frac{p}{q}\big)^n + c_{n-1}\big(\frac{p}{q}\big)^{n-1} + \ldots + c_0 = 0,$$

then multiplying with q^n shows that $p^n = -q(c_{n-1}p^{n-1} + \ldots + c_0 q^{n-1})$, hence q divides p, a contradiction.

(iii) $\tau = (1+\sqrt{5})/2$ (the "golden ratio") is integral for $\mathbb{Z} \subset \mathbb{Z}[\tau]$, where $\mathbb{Z}[\tau]$ is the subring in $\mathbb{Q}$ generated by $\mathbb{Z}$ and τ. Indeed, $\tau^2 - \tau - 1 = 0$. On the other hand, $\sigma = (1+\sqrt{3})/2$ is not integral for $\mathbb{Z} \hookrightarrow \mathbb{Z}[\sigma]$ for $\mathbb{Z}[1/2] \subset \mathbb{Z}[\sigma]$. Indeed, $2(\sigma^2-1) = \sqrt{3} \in \mathbb{Z}[\sigma]$ so that $(\sigma^2-1)\sqrt{3} - 1 = 1/2 \in \mathbb{Z}[1/2]$. But $1/2$ is not integral over $\mathbb{Z}$.

4. Geometric examples. As we will see at the end of this Section 2, a ring extension between finitely generated, reduced k-algebras can be thought of as a morphism of varieties. To get a geometrical feeling, let $A = k[x]$ and $B = A[y]/(f)$, where $f \in A[y]$ is a nonconstant polynomial which we think of as a nontrivial relation on y. Geometrically, A corresponds to $X = \mathbb{A}^1$ while B is the coordinate ring of $Y = \mathcal{Z}(f) \subset \mathbb{A}^2$ the curve defined by f. We assume that we get an injection $\iota : A \to B$, $x \mapsto \bar{x}$ giving a ring extension. This corresponds to a morphism $\pi : Y \to X$ given by $(x, y) \mapsto x$.

(i) Consider first the case $f(y) = y^2 - x^2$ so that $y \in B$ (strictly speaking $\bar{y} \in B$) is integral over A. We will see in the next proposition that this implies that $A \subset B$ is integral. Since any nonzero value for x yields a quadratic relation on y, the fibre $\pi^{-1}(x)$ consists of two points unless $x = 0$ where the fibre consists of one point.

(ii) Next consider $f(y) = xy - 1$. Lifting the monic relation to $k[2]$ we see that there exists a monic polynomial $\bar{g} \in A/(f)[z]$, the image of $g \in k[x][z]$ such that $\bar{g}(\bar{y}) = 0$ if and only if there exists $h \in k[x][z]$ such that $g(y) = h(y)(xy-1)$. Considering the leading term in y shows that this cannot happen, hence $\bar{y}$ is not integral. Here, the fibre over x consists of one point if $x \neq 0$ and is empty, if $x = 0$.

(iii) Finally, consider $f(y) = xy$. The same argument as in (ii) shows that y is not integral. The fibre over $x \neq 0$ consists again of one element, while in $x = 0$ it is infinite.

Therefore, as a first approximation, we think an integral ring extension as a surjective variety morphism with finite fibres ("ramified coverings"), see also Figure 2.13.

5. Proposition (finite versus integral extensions). *Let $A \subset B$ be a ring extension, and let $b \in B$. Then are equivalent:*

(i) *b is integral over A;*

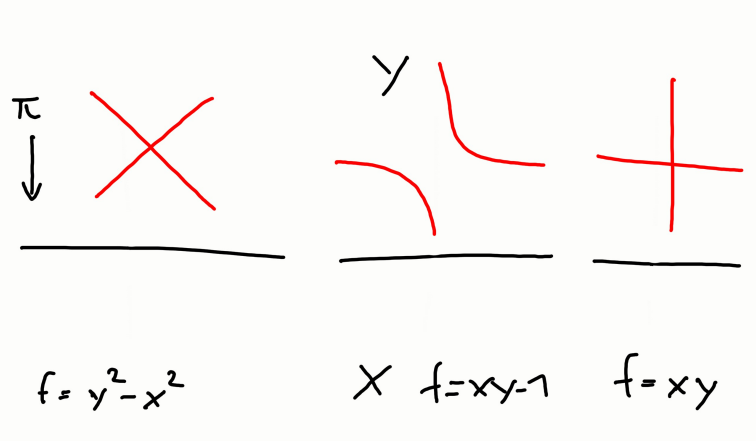

FIGURE 13. The covering maps from ring extensions.

(ii) *the subring $A[b]$ generated by A and b is finite over A;*
(iii) *there exists a subring $C \subset B$ such that $A[b] \subset C$ and C is finite over A.*

In particular, a finite ring extension is integral. In fact, any finite ring extension $A \subset B$ is of the form $B = A[b_1, \ldots, b_n]$ with b_i integral over A, i.e.

$$\text{finite type} \ + \text{integral} \ \Leftrightarrow \ \text{finite}$$

Proof. (i) $\Rightarrow$ (ii) If b satisfies a monic relation of the form $b^n = -\sum_{i=0}^{n-1} a_i b^i$ with $a_i \in A$, then $A[b]$ is generated by $1, b, \ldots, b^{n-1}$.

(ii) $\Rightarrow$ (iii) Take $C = A$.

(iii) $\Rightarrow$ (i) Consider b as a map $\mu_b : C \to C$, $c \mapsto b \cdot c$. Since C is a finite A-module the Cayley-Hamilton theorem 0.56 applies, and μ_b satisfies a monic relation $\mu_b^n + a_{n-1}\mu_b^{n-1} + \ldots + a_0 = 0$ in $\mathrm{End}(M)$ with $a_i \in A$. Evaluating at 1 gives (i). □

6. Corollary. *Let $X \subset \mathbb{P}_k^n$ be a projective variety. Then $\mathcal{O}(X) \cong k$.*

Proof. Let $f \in \mathcal{O}_X(X)$ be a global regular function. Restriction induces an injection $\mathcal{O}_X(X) \hookrightarrow A(X_i) \cong S(X)_{(x_i)}$. In particular, $f = g_i/x_i^{d_i}$ for $g_i \in S(X)$ homogeneous of degree d_i. We have the inclusions $\mathcal{O}(X) \subset \mathcal{O}_a \subset K(X) \subset \bigcup_{a \in X} \mathcal{O}_a$ so that by (i), $\mathcal{O}(X)$, $K(X)$ and $S(X)$ can be considered as subrings of $L = \mathrm{Quot}\, S(X)$. In particular, $x_i^{d_i} f \in S(X)_{d_i}$, the degree d_i polynomials of $S(X)$. Next choose $d \geqslant \sum d_i$. As a k-vector space, $S(X)_d$ is spanned by monomials of degree d in $\bar{x}_0, \ldots, \bar{x}_n$. In any such monomial, at least one x_i occurs to a power $\geqslant d_i$ by the choice of d. Since for such an i, $x_0^{e_0} \ldots x_i^{e_i} \ldots x_n^{e_n} f = x_0^{e_0} \ldots x_i^{e_i - d_i} \ldots x_n^{e_n} g_i \in S(X)_d$ we have $S(X)_d \cdot f \subset S(X)_d$. Iterating we get $S(X)_d \cdot f^q \subset S(X)_d$ for all $q > 0$. In particular, $x_0^d f^q \in S(X)$ for all $q > 0$ which shows that the subring $S(X)[f]$ of L is contained in $x_0^{-d} S(X)$, a finitely generated $S(X)$-module. Since $S(X)$ is Noetherian, $S(X)[f]$ is also a finitely generated $S(X)$-module by Corollary 0.95. Therefore, f must be integral over $S(X)$, i.e. satisfy a relation of the form $f^n + \sum c_i f^i = 0$ for $c_i \in S(X)$. But f is of degree 0, so the equation $f^n + \sum (c_i)_0 f^i = 0$, where $(c_i)_0 \in S(X)_0 = k$ denotes the degree 0 part of c_i, is also valid. In particular, $f \in L$ is algebraic over k, so that $f \in k$ for k is algebraically closed. □

7. Remark. The last property is familiar from complex geometry: As a trivial consequence of the maximal modulus theorem, any holomorphic function globally defined on a complex compact manifold must be constant.

8. Proposition (tower laws).

(i) *If $A \subset B \subset C$ are extension rings such that C is a finite B-algebra, and B is a finite A-algebra, then C is a finite A-algebra.*

(ii) *If $A \subset B \subset C$ with C is integral over B and B is integral over A, then C is integral over A.*

Proof. (i) By Proposition 2.5, $A[b_1]$ is finite over A. Then proceed by induction using (i).

(ii) Let $c \in C$ satisfy the relation $c^n + b_{n-1}c^{n-1} + \ldots + b_0 = 0$, with $b_0, \ldots, b_{n-1} \in B$. Since each b_i is integral over A, each extension $A \subset A[b_0, \ldots, b_{n-1}] \subset A[b_0, \ldots, b_{n-1}, c]$ is finite by (i). Hence c belongs to an intermediate algebra $A \subset A[b_0, \ldots, b_{n-1}, c] \subset C$ which is finite over A. By 2.5 (iii), c is integral over A. □

9. Proposition and definition (integral closure). *The set*

$$\bar{A} = \{b \in B \mid b \text{ integral over } A\} \subset B$$

is a subring of B. In particular, the sum and the product of two integral rings is again integral. Moreover, if $b \in B$ is integral over $\bar{A}$, then $b \in \bar{A}$, so that $\bar{\bar{A}} = A$. We call $\bar{A}$ the **integral closure** *of A in B. If $A = \bar{A}$, then A is called* **integrally closed in** *B.*

Proof. If $x, y \in \bar{A}$, then $A[x, y]$ is finite over A, whence $x + y$ and $x \cdot y$ are integral over A and thus in $\bar{A}$. $\bar{\bar{A}} = A$ follows from Proposition 2.8. □

10. Exercise. *Let $A \subset B$ be a ring extension of integral rings, and let $\bar{A}$ be the integral closure of A in $B \Rightarrow$ for any two monic polynomials f, $g \in B[x]$ with $fg \in \bar{A}[x]$ we have f, $g \in \bar{A}[x]$.*

Hint: Consider a field extension $B \subset \operatorname{Quot} B \subset K$ where $f = \Pi(x - \xi_i)$ and $g = \Pi(x - \eta_i)$ split.

Proof. Using the hint and the fact that $fg = \Pi(x - \xi_i)(x - \eta_j) \in \bar{A}[x]$ is monic, the roots ξ and η_i in K are integral over $\bar{A}$. This does not immediately imply that they are in $\bar{A}$, for $\bar{A}$ is the integral closure in B, not in K. However, it implies that the coefficients of f and g which are sums and products of the ξ_i and η_j respectively, are integral over $\bar{A}$ by Proposition 2.9. But f and $g \in B[x]$, that is, the coefficients of f and g are in B. Since they are integral, they are in $\bar{A}$, whence f and $g \in \bar{A}[x]$. □

11. Definition (normal ring). An integral domain A is called **normal** or **integrally closed** if A is integrally closed in its quotient field.

12. Algebraic examples of normal rings.

(i) As we have seen in Example 2.3 (i), any UFD is normal.

(ii) A **number field** is a finite field extension $\mathbb{Q} \subset K$. By definition, its **ring of integers** $\mathcal{O}_K$ is the integral closure of $\mathbb{Z}$ in K. In particular, $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$ by (i). It is an example of a *Dedekind ring* (see below) and as such it is normal. For instance, consider the quadratic number field $\mathbb{Q}(\sqrt{n})$, where n is a squarefree integer. Then $\mathcal{O}_{\mathbb{Q}(\sqrt{n})} = \mathbb{Z}[\alpha]$ with $\alpha = (1+\sqrt{n})/2$ if $n \equiv 1 \bmod 4$ and $\alpha = \sqrt{n}$ if $n \equiv 2$ or $\bmod 4$. For instance, consider the second case. $\mathbb{Z} \subset \mathbb{Z}[\sqrt{n}]$ is an integral extension for $x^2 - n \in \mathbb{Z}[x]$ is monic. Moreover, it is well-known that $Z[\sqrt{n}]$ is a UFD (see for instance [Bo, Section 2.4]). This is integrally closed in its quotient field which is obviously $\mathbb{Q}(\sqrt{n})$.

13. Geometric examples of normal rings. Let $A = A(X)$ be the coordinate ring of an affine variety X so that Quot A is the ring of rational functions on X. Hence if A is normal, then any rational function φ satisfying a monic relation $\varphi^n + c_{n-1}\varphi^{n-1} + \ldots + c_0 = 0$ for $c_i \in A$ is in fact already contained in A. In particular, it has a well-defined value at any point, that is, an integral rational function has an extension to all of X. Such extension theorems are familiar in complex analysis, where under certain conditions, meromorphic functions (corresponding to rational functions) can be extended to holomorphic functions (corresponding to regular functions), cf. Riemann's extension theorem (in complex dimension ome) or Hartog's theorem (in higher dimensions).

(i) Let $A = \mathbb{C}[x]$ so that $X = \mathbb{A}^1$ and $K = \mathbb{C}(x)$. Then A is normal as a UFD. Geometrically, if φ is a rational function which is ill-defined at a point p, it must be of the form $f(x)/(x-p)^k g(x)$ for $f(p)$, $g(p) \neq 0$, that is, φ has a pôle of order k. In particular, it cannot satisfy a monic equation, for φ^n has a pôle of order kn which cannot be cancelled by pôles of lower order.

(ii) Consider the ring $A = k[x,y]/(y^2 - x^3)$, the coordinate ring of the cusp curve $Y = \mathcal{Z}(y^2 - x^3) \subset \mathbb{A}^2$. It is integral with ring of fractions isomorphic to $k(t)$. Indeed, the map $k(t) \to$ Quot A sending $f/g(t)$ to $f/g(\bar{y}/\bar{x})$ is an isomorphism (check!). In particular, $\tau = \bar{y}/\bar{x}$ is integral over A (for instance, $\tau^2 - \bar{x} = 0$), but $\tau \notin A$: We cannot extend the rational function τ over $(0,0) \in Y$. On the other hand, $k[t]$ is normal in $k(t)$ for it is a UFD. This shows that normality can detect singularities such as the cusp. Indeed, we will see in Section 3 that a "smooth" curve (more generally, a smooth variety) has always a normal coordinate ring.

(iii) Consider $X = \mathcal{Z}(y^2 - x^2 - x^3) \subset \mathbb{A}^2_{\mathbb{R}}$ with $A = A(X) = \mathbb{R}[x,y]/(y^2 - x^2 - x^3)$ (the real numbers are chosen for sake of the geometric argument). In this case, A is not normal. Indeed, consider the rational function $\varphi = \bar{y}/\bar{x} \in$ Quot (A) for which $\varphi^2 - \bar{x} - 1 = 0$. Hence φ is integral. However, it is ill-defined in the origin. For x and y small we can neglect the x^3 term so that the curve near the origin is approximatively given by $y^2 - x^2 = 0$. Hence it has two branches near the origin given by $y = \pm x$. It follows that φ approaches two different values at the origin depending on the branch which one goes along in order to reach the origin. This makes φ^2 well-defined and thus a regular function, but $\varphi \notin A$, that is, we cannot extend φ over the origin into a regular function. To see this, assume that F is a regular function which extends τ over $(0,0)$ to all of X. Since $\tau^2 = \bar{x}$ we necessarily have $F(0,0) = 0$. Further, $F \in A(X)_{\mathfrak{m}}$, where $\mathfrak{m}$ is the maximal ideal corresponding to $(0,0)$. Hence, there exists a (dense) open neighbourhood U of $(0,0)$ and f, $g \in A(X)$ with $\bar{f}/\bar{g} = F$ and $\bar{g}(0,0) \neq 0$, where f, $g \in k[x,y]$ are representatives of $\bar{f}$ and $\bar{g}$. If U^* is the open set $U \backslash \{(0,0)\}$, then we get the identity $\bar{x}\bar{f} - \bar{y}\bar{g} = 0$ on U^*. Since the left and the right hand side are well-defined on all of X, the identity property of

Corollary 2.67 gives $\bar{x}\bar{f} - \bar{y}\bar{g} = 0$ in $A(X)$. Lifting this to $k[x,y]$, it follows that $xf - yg = h(x,y)(y^2 - x^3)$ for a polynomial (function) $h \in k[x,y]$. In particular, we obtaian for $x = y = t$ the identity $f - g = h(t,t)(t - t^2)$ in $k[t]$. Setting $t = 0$ implies $g(0,0) = 0$, a contradiction.

14. Exercise (normal rings in number theory). *Let $N \subset B$ be an integral extension of integral rings, and assume that N is normal $\Rightarrow$ For any $b \in B$ its minimal polynomial f over $k = \operatorname{Quot} N$ has actually coefficients in N.*

Let $d \neq 0, 1$ be a squarefree integer, that is, no square divides d in $\mathbb{Z}$. Use the first part of the exercise to show that the integral closure of $\mathbb{Z}$ in $\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\} \subset \mathbb{C}$ is given by

$$\bar{\mathbb{Z}} = \{a + b\sqrt{d} \mid a, b \in \mathbb{Q},\ -2a \in \mathbb{Z},\ a^2 - db^2 \in \mathbb{Z}\}.$$

These rings play an important rôle in number theory.

Proof. Since $b \in B$ is integral over N, $g(b) = 0$ for some monic polynomial $g \in N[x]$. Hence, $f|g$ in $k[x]$ by the properties of the minimal polynomial, that is, $g = f \cdot h \in N[x]$ for some monic polynomial $h \in k[x]$. Applying Exercise 2.?? with $\bar{A} = N$ and $B = k$ shows that f (and h) in $N[x]$.

We apply this for the computation of N the integral closure of $A = \mathbb{Z}$ (which is normal as a UFD) in $B = \mathbb{Q}(\sqrt{d})$. The ring $\mathbb{Z}$ is certainly normal for it is integrally closed in $\mathbb{Q} = \operatorname{Quot}\mathbb{Z}$. The minimal polynomial of $a + b\sqrt{d}$ over $\mathbb{Q}$ is $f(x) = (x - a - b\sqrt{d})(x - a + b\sqrt{d})$, and this is integral over $\mathbb{Z}$ if and only if $f(x) = x^2 - 2ax + b^2d - a^2$ has integer coefficients. This gives $\{a + b\sqrt{d} \mid a, b \in \mathbb{Q},\ -2a \in \mathbb{Z},\ a^2 - db^2 \in \mathbb{Z}\} \subset \bar{\mathbb{Z}}$. The converse inclusion is obvious. □

Next we want to show that normality is a local property in accordance with our idea that normality links into the geometric idea of regularity. First we prove:

15. Lemma (Integrality is preserved under taking quotients and localising). *Let $A \subset B$ be an integral ring extension.*

(i) *If $\mathfrak{b}$ is an ideal of B and $\mathfrak{a} = \mathfrak{b}^e = A \cap \mathfrak{b}$, then $B/\mathfrak{b}$ is integral over $A/\mathfrak{a}$.*
(ii) *If S is a multiplicative set of A, then $S^{-1}B$ is integral over $S^{-1}A$.*

Proof. If $b \in B$ we have $b^n + a_1b^{n-1} + \ldots + a_n = 0$ with $a_i \in A$.

(i) Reducing this equation modulo $\mathfrak{b}$ gives the desired polynomial relation.

(ii) Let $b/s \in S^{-1}B$. Then $(b/s)^n + (a_1/s)(b/s)^{n-1} + \ldots + a_n/s^n = 0$. □

16. Lemma (integral closure and localisation). *Let $A \subset B$ be a ring extension, and let S be a multiplicative subset of A. Then $S^{-1}\bar{A}$ is the integral closure of $S^{-1}A$ in $S^{-1}B$.*

Proof. By Lemma 2.15, $S^{-1}\bar{A}$ is integral over $S^{-1}A$. It remains to show that if $b/s \in S^{-1}B$ is integral over $S^{-1}A$, then $b/s \in S^{-1}\bar{A}$. First, we have

$$(b/s)^n + (a_1/s_1)(b/s)^{n-1} + \ldots + a_n/s_n = 0,$$

where $a_i \in A$, $s_i \in S$. Let $t = s_1 \cdot \ldots \cdot s_n$ and multiply the latter equation with $(st)^n$. Then it becomes a monic relation on bt with coefficients in A, that is $bt \in \bar{A}$. Hence $b/s = bt/st \in S^{-1}\bar{A}$. □

17. Proposition (normality is a local property). *Let A be an integral domain. Are equivalent:*

(i) *A is normal;*
(ii) *$A_\mathfrak{p}$ is normal, for each prime ideal $\mathfrak{p}$;*
(iii) *$A_\mathfrak{m}$ is normal, for each maximal ideal $\mathfrak{m}$.*

Proof. Let $k = \operatorname{Quot} A$ and $f : A \subset k \to \bar{A} \subset k$ be the restriction of the identity mapping Id_k. Then A is normal $\Leftrightarrow$ f is surjective. By Lemma 2.16, $A_\mathfrak{p}$ and $A_\mathfrak{m}$ are normal if and only if $S_\mathfrak{p}^{-1}f$ and $S_\mathfrak{m}^{-1}f$ are surjective, whence the assertion by Proposition 1.113. □

As we have seen we can think geometrically of an integral ring extension $A(X) \to A(Y)$ as a finite (ramified) cover $Y \to X$. In particular, one should be able to lift subvarieties of X to subvarieties Y, or more algebraically, prime ideals to prime ideals. This "lying over" property will occupy us next.

18. Lemma (Integral ring extensions and fields). *Let $A \subset B$ be an integral ring extension of integral domains. Then A is a field $\Leftrightarrow$ B is a field.*

Proof. $\Rightarrow$) Let $0 \neq b \in B$. Since $A \subset B$ is an integral ring extension, $b^n + a_{n-1}b^{n-1} + \ldots + a_0 = 0$ for some $a_i \in A$ and minimal $n \in \mathbb{N}$. In particular, $a_0 \neq 0$ (otherwise, n would not be minimal). Since A is a field, a_0 is invertible whence b is invertible with inverse

$$b^{-1} = -a_0^{-1}(b^{n-1} + a_{n-1}b^{n-2} + \ldots a_2 b + a_1) \in B.$$

$\Leftarrow$) Conversely, assume that $0 \neq a \in A$. Then a^{-1} exists as an element of B whence

$$(a^{-1})^n + a_{n-1}(a^{-1})^{n-1} + \ldots + a_0 = 0$$

with coefficients $a_i \in A$ and $a_0 \neq 0$. Multiplying by a^{n-1} shows that $a^{-1} = -a_{n-1} - a_{n-2}a - \ldots - a^{n-1}a_0 \in A$. □

19. Corollary. *Let $A \subset B$ be an integral ring extension.*

(i) *Let $\mathfrak{q}$ be a prime ideal of B. Then $\mathfrak{q}^c = \mathfrak{a} \cap A$ is maximal $\Leftrightarrow$ $\mathfrak{q}$ is maximal.*
(ii) *Let $\mathfrak{q} \subset \mathfrak{q}'$ be prime ideals of B such that $\mathfrak{p} = \mathfrak{q}^c = \mathfrak{q}'^c$. Then $\mathfrak{q} = \mathfrak{q}'$.*

Proof. (i) $B/\mathfrak{q}$ is integral over $A/\mathfrak{q}^c$ by Lemma 2.15. Now apply Lemma 2.18.

(ii) By Lemma 2.15, $A_\mathfrak{p} \subset (A\backslash\mathfrak{p})^{-1}B =: B(\mathfrak{p})$ is integral. Let $\mathfrak{m}$ be the extension of $\mathfrak{p}$ in $A_\mathfrak{p}$, and let $\mathfrak{n} \subset \mathfrak{n}'$ be the extensions in $B(\mathfrak{p})$ of $\mathfrak{q} \subset \mathfrak{q}'$ respectively. Then $\mathfrak{m}$ is the maximal ideal of $A_\mathfrak{p}$ (cf. 1.99), and $\mathfrak{n}^c = \mathfrak{n}'^c = \mathfrak{m}$ (indeed, if $\mathfrak{a} = \mathfrak{b}^c = A \cap \mathfrak{b}$ for an ideal $\mathfrak{b} \subset B$ in a ring extension $A \subset B$, then $S^{-1}\mathfrak{a} = S^{-1}A \cap S^{-1}\mathfrak{b} = (S^{-1}\mathfrak{b})^c$, where the contraction is now being taken with respect to the ring extension $S^1{-}1A \subset S^{-1}B$, cf. Proposition 1.109 (ii)). So $\mathfrak{n}$ and $\mathfrak{n}'$ are maximal by (i), and $\mathfrak{n} \subset \mathfrak{n}'$, whence $\mathfrak{n} = \mathfrak{n}'$. But then $\mathfrak{q} = \mathfrak{q}'$ by Corollary 1.105 (v), since $\mathfrak{q}$ and $\mathfrak{q}'$ do not intersect $A\backslash\mathfrak{p}$. □

20. Theorem ("lying over"). *Let $A \subset B$ be an integral ring extension, and let $\mathfrak{p} \subset A$ be prime $\Rightarrow$ there exists a prime ideal $\mathfrak{q} \subset B$ such that $\mathfrak{q}^c = A \cap \mathfrak{q} = \mathfrak{p}$.*

Proof. Let again $B(\mathfrak{p})$ denote the localisation $(A\backslash\mathfrak{p})^{-1}B$. The natural diagramm

$$\begin{array}{ccc} A & \longrightarrow & B \\ \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} \\ A_{\mathfrak{p}} & \longrightarrow & B(\mathfrak{p}) \end{array}$$

in which the horizontal arrows are inclusions, is commutative. Let $\mathfrak{n}$ be a maximal ideal of $B(\mathfrak{p})$. Then $\mathfrak{n}^c \subset A_{\mathfrak{p}}$ is maximal by the previous corollary, and thus $\mathfrak{n}^c = \mathfrak{p}^e$, the unique maximal ideal of the local ring $A_{\mathfrak{p}}$. If $\mathfrak{q} = \beta^{-1}(\mathfrak{n})$, then $\mathfrak{q}$ is prime and $\mathfrak{q}^c = \mathfrak{q} \cap A = \mathfrak{p}$. □

The previous theorem can be refined to the following relative versions:

21. Theorem ("going-up"). *Let $A \subset B$ be an integral ring extension. Moreover, let $\mathfrak{p}$, $\mathfrak{p}'$ be prime ideals of A with $\mathfrak{p} \subset \mathfrak{p}'$, and let $\mathfrak{q}$ be a prime ideal of B such that $\mathfrak{q}^c = \mathfrak{p}$. Then there exists a prime ideal $\mathfrak{q}' \supset \mathfrak{q}$ of B such that $\mathfrak{q}'^c = \mathfrak{p}'$.*

Proof. Let $\hat{A} = A/\mathfrak{p}$ and $\hat{B} = B/\mathfrak{q}$. Then $\hat{A} \subset \hat{B}$ is an integral ring extension. Hence, there exists a prime ideal $\hat{\mathfrak{q}}$ in $\hat{B}$ such that $\hat{\mathfrak{q}} \cap \hat{A} =$ the image of $\mathfrak{p}'$ in $A/\mathfrak{p}$. Contracting $\hat{\mathfrak{q}}$ via the projection map $B \to \hat{B}$ yields the desired prime ideal. □

22. Exercise. *Let $\iota : A \hookrightarrow B$ be an integral ring extension (considering ι as an inclusion). Show that the associated map $\iota^a : \operatorname{Spec}(B) \to \operatorname{Spec}(A)$ defined by $\iota^a(\mathfrak{q}) = \mathfrak{q} \cap A$ is a closed mapping, that is, it maps closed sets to closed sets.*

Proof. The closed sets of $\operatorname{Spec}(B)$ are $V(\mathfrak{b}) = \{\mathfrak{q} \in \operatorname{Spec}(B) \mid \mathfrak{b} \subset \mathfrak{q}\}$ for $\mathfrak{b} \subset B$ an ideal of B. We show that $\iota^a(V(\mathfrak{b})) = V(\mathfrak{b}^c)$. The inclusion $\subset$ is trivial, so let $\mathfrak{p}$ be a prime ideal of A containing $\mathfrak{a} := \mathfrak{b}^c$. We need to find $\mathfrak{q} \in \operatorname{Spec}(B)$ with $\mathfrak{q}^c = \mathfrak{p}$. Lemma 2.15 (i), $\hat{A} := A/\mathfrak{a} \subset \hat{B} := B/\mathfrak{b}$ is an integral extension. Now $\hat{\mathfrak{p}}$, the image of $\mathfrak{p}$ in $\hat{A}$ is prime, so that by the lying-over property of integral ring extensions, there exists a prime ideal $\hat{\mathfrak{q}}$ of $\hat{B}$ whose contraction gives $\hat{\mathfrak{p}}$. Contracting with respect to the projection map $B \to \hat{B}$ yields the desired $\mathfrak{q} \in \operatorname{Spec}(B)$. □

In a similar vein, one can prove the

23. Theorem ("going-down"). *Let $A \subset B$ be an integral ring extension. Assume that A is normal and B an integral domain. Assume that $\mathfrak{p} \subset \mathfrak{p}'$ are prime ideals of A, and that there exists a prime ideal $\mathfrak{q}' \subset B$ such that $\mathfrak{q}'^c = \mathfrak{q}' \cap A = \mathfrak{p}'$ ⇒ There exists a prime ideal $\mathfrak{q} \subset \mathfrak{q}' \subset B$ such that $\mathfrak{q}^c = \mathfrak{p}$.*

Proof. The proof is slightly more technical, see for instance [AtMa, Theorem 5.16]. The normality is used to apply Exercises 2.14. □

We summarise our discussion in Figure 2.14

24. Geometric interpretation. To get some geometric feeling for integral ring extensions we interpret the previous theorems in terms of ramified covering maps. In general, a continuous surjective map $\pi : X \to Y$ between connected topological spaces which restricted to X minus a finite set of points is a local

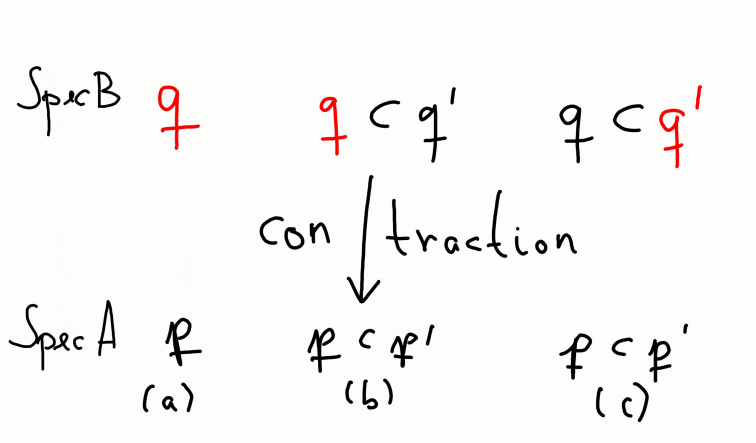

FIGURE 14. Extension and contraction for integral extensions: (a) lying-over (b) going-up (c) going-down. The red colour indicates existence.

homemomorphism and such that the fibres are finite is called a *(ramified) covering map*. The cardinality of the fibre is the *degree* of the map. Generically, where π is a local homeomorphism, the fibre has precisely $\deg \pi$ points; multiple points (where the covering map "branches" or "ramifies") occur where π fails to be a local homeomorphism.

In our geometric situation, connected topological spaces correspond to varieties, say affine ones. The surjective map $\pi : X \to Y$ can be thought of as an injective k-algebra morphism $\pi^* : A(Y) \hookrightarrow A(X)$. If this ring extension is integral, then any maximal ideal of $A(Y)$ (corresponding to a point of Y) is the contraction of a maximal ideal of $A(X)$ (corresponding to a point of X). This is essentially the surjectivity property of the covering map π. The finiteness of the fibre was partially discussed in 2.4, cf. also Example 2.25. Finally, the previous Exercise shows that π^* is a closed map which corresponds to the local homeomorphism property of π. In this way we should think of an integral extension of coordinate rings in terms of ramified coverings of the corresponding affine varieties.

2.2. **Noether normalisation and Hilbert's Nullstellensatz.** Hilbert's Nullstellensatz is an easy consequence of Noether normalisation. To motivate the latter we consider the following

25. Example (geometric motivation of Noether normalisation). Consider the ring extension $A = k[x_1] \subset B = k[x_1, x_2]/(x_1x_2 - 1)$ (where we identify $f \in A$ with the residue class $\bar{f} \in B$ so that A becomes a subring of B). Of course, B is not integral over A for the "lying-over" property fails for the origin, i.e. the prime (in fact maximal) ideal $\mathfrak{m}_0 \subset A$ (cf. Example 2.4). However, performing the coordinate change $x_1 = y_1 + y_2$, $x_2 = -y_1 + y_2$ gives a finite ring extension $k[y_1] \subset k[y_1, y_2]/(y_1^2 - y_2^2 - 1) \cong B$ for $\bar{y}_2^2 - \bar{y}_1^2 + 1 = 0$ is a monic relation on y_2, cf. Proposition 2.5 and Figure 2.26.

Let B be a k-algebra. Recall that B is **finitely generated** if $B = k[\alpha_1, \ldots, \alpha_n]$ for some $\alpha_1, \ldots, \alpha_n$, or equivalently, if we have a surjection $k[x_1, \ldots, x_n] \to B \to 0$

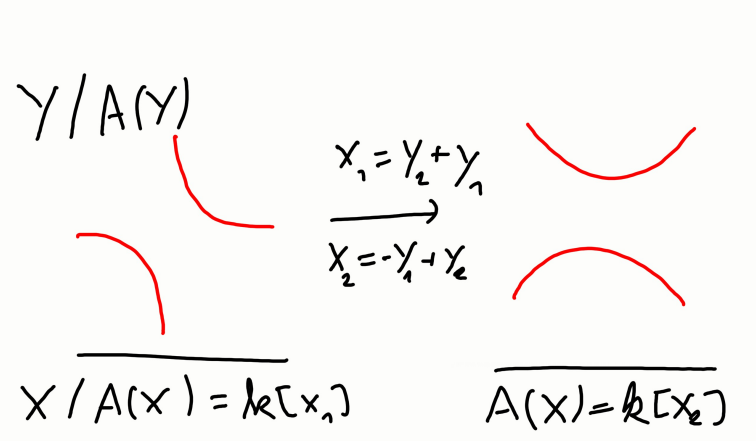

FIGURE 15. A geometric example of Noether normalisation.

so that $B = k[x_1, \ldots, x_n]/\mathfrak{a}$. Recall that elements $a_1, \ldots a_n \in A$ are **algebraically independent** if the natural surjection

$$k[x_1, \ldots, x_n] \to k[a_1, \ldots, a_n] \to 0$$

sending x_i to a_i is actually an isomorphism of k-algebras, that is, we have an injection $k[x_1, \ldots, x_n] \hookrightarrow A$ by sending x_i to a_i. Put differently, there is no nonzero polynomial relation of the form $f(a_1, \ldots, a_n) = 0$ for $f \in A[n]$, and A is just a polynomial algebra in the unknowns a_i. In the previous Example 2.25 where $B \cong k[x_1, x_2]/(x_1 x_2 - 1)$ is a finitely generated k-algebra, we saw that we could find an injection $k[y_1] \to B$ such that B became a finite ring extension of $k[y_1]$. More generally we have the

26. Theorem (Noether normalisation lemma). *Let B be a finitely generated k-algebra. Then there exists algebraically independent elements $y_1, \ldots, y_k \in B$ such that B is finite over $A = k[y_1, \ldots, y_k]$. In other words, a ring extension $k \subset B$ given by a finitely generated k-algebra B can be written as a composite*

$$k \subset A = k[y_1, \ldots, y_l] \subset B,$$

where A is a polynomial algebra over k and B a finite module over A.

27. Remark. Though we have not a rigorous definition of dimension yet we can interpret the number l as the dimension of the variety with coordinate ring B, cf. also Figure 2.26 where this variety is clearly one dimensional. The induced map $\operatorname{Spec} B \to \operatorname{Spec} A = \mathbb{A}^k$ can be regarded as a ramified covering.

28. Proof of Theorem 2.26. We will proceed in three steps, assuming that k is infinite (though the theorem holds for general k).

Step 1. *Let $0 \neq f \in k[x_1, \ldots, x_n]$ be a homogeneous polynomial of degree d. Then there exist $a_1, \ldots, a_{n-1} \in k$ such that $f(a_1, \ldots, a_{n-1}, 1) \neq 0$.* By induction on n. The case $n = 1$ is trivial for $f = x^d$. So assume $n > 1$ and write $f = \sum_{i=0}^{d} f_i x_1^i$, where f_i is a homogeneous polynomial of degree $d - i$ in $x_2, \ldots, x_n$. Since $f \neq 0$ we have $f_i \neq 0$ for at least one i. The induction hypothesis applies so that $f_i(a_2, \ldots, a_{n-1}, 1) \neq 0$ for certain $a_2, \ldots, a_{n-1}$. In particular, $f(\cdot, a_2, \ldots, a_{n-1}, 1) \in k[x_1]$ is a non-zero polynomial which has only finitely many roots. It follows that $f(a_1, \ldots, a_{n_1}, 1) \neq 0$ for almost any choices of $a_1 \in k$ (here we use that k is infinite!).

Step 2. *Let $B = k[b_1, \dots, b_n]$ be a finitely generated k-algebra and suppose that there is $0 \neq f \in k[x_1, \dots, x_n]$ a polynomial of degree d. Then there exist $a_1, \dots, a_{n-1} \in k$ such that $f(b_1 + a_1 b_n, \dots, b_{n-1} + a_{n-1} b_n, b_n) = 0$ is monic in b_n over the ring $k[b_1, \dots, b_{n-1}]$.* Indeed, write $f = \sum_{m_1,\dots,m_n} c_{m_1 \dots m_n} x_1^{m_1} \cdot \ldots \cdot x_n^{m_n}$. Then the leading term of

$$\begin{aligned} & f(b_1 + a_1 b_n, \dots, b_{n-1} + a_{n-1} b_n, b_n) \\ &= \sum_{m_1,\dots,m_n, \sum m_i = d} c_{m_1 \dots m_n} (b_1 + a_1 b_n)^{m_1} \cdot \ldots \cdot (b_{n-1} + a_{n_1} b_n)^{m_{n-1}} b_n^{m_n} \end{aligned}$$

in b_n is equal to

$$\sum_{m_1,\dots,m_n, \sum m_i = d} c_{m_1 \dots m_n} a_1^{m_1} \dots a_{n-1}^{m_{n-1}} b_n^d = f_d(a_1, \dots, a_{n-1}, 1) b_n^d,$$

where $f_d(x_1, \dots, x_n) = \sum_{m_1 + \dots + m_n = d} c_{m_1 \dots m_n} x_1^{m_1} \cdot \ldots \cdot x_n^{m_n}$ denotes the (homogeneous) degree d part of f which is not zero for f has degree d. By the first step we can choose $a_1, \dots, a_{n-1} \in k$ such that $f_d(a_1, \dots, a_{n-1}, 1) \neq 0$ which is therefore a unit in $k[b_1, \dots, b_{n-1}]$.

Step 3. We now prove the theorem by an induction on the number n of generators b_i of B. For $n = 0$ there is nothing to prove since $B = A = k$. If $n > 0$ and the generators $b_1, \dots, b_n \in B$ are algebraically independent over k, then again we can take $B = A = k[y_1, \dots, y_n]$ with $y_i = b_i$. So assume that we are given n generators $b_1, \dots, b_n \in B$ such that $B = k[b_1, \dots, b_n]$ and that there exists $0 \neq f \in k[x_1, \dots, x_n]$ such that $f(b_1, \dots, b_n) = 0$. For $a_i \in k$, $i = 1, \dots, n-1$ we put $b_i' = b_i - a_i b_n$, $i = 1, \dots, n-1$, $b_n' = b_n$ so that $k[b_1', \dots, b_{n-1}', b_n'] = k[b_1, \dots, b_n] = B$. Hence $f(b_1, \dots, b_n) = f(b_1' + a_1 b_n', \dots, b_1' + a_1 b_n', b_n') = 0$ so that if we choose the a_i as in the previous step, $b_n' = b_n$ is integral over $A' := k[b_1', \dots, b_{n-1}'] \subset B$. In particular, $B = A'[b_n]$ is finite over A'. By induction hypothesis, A' is finite over $A = k[y_1, \dots, y_l]$ for $y_i \in A'$ algebraically independent, so that B is finite over A.■

29. Theorem (weak Nullstellensatz). *Let k be a field, and $k \subset K$ be a field extension such that K is finitely generated as a k-algebra. Then K is a finite field extension over k, i.e. $[K : k] < \infty$.*

Proof. By Noether normalisation 2.26 K is finite, hence integral extension of some polynomial ring $A = k[y_1, \dots, y_n]$. Since K is a field, so is A by Lemma 2.18. But the polynomial ring A can be a field only if $n = 0$, i.e. $A = k$. Hence $[K : k] < \infty$. □

3. Local properties

Next we want to study geometric properties of varieties which are *local*, that is, they can by studied by restricting attention to an affine neighbourhood. The example of the cuspidal curve showed that geometric properties (the existence of a cusp) is reflected in the algebraic properties of the coordinate ring (its nonnormality). Our line of attack is therefore to reformulate these properties in terms of algebraic properties of the underlying function rings.

3.1. **Completions.** One way of studying local properties is localisation of rings. The local rings we obtain this way still carry a lot of information. We saw in Exercise 2.158 that the local ring $\mathcal{O}_{X,a}$ of a point $a \in X$ determines X up to birational isomorphism. Another idea to study local properties is the *completion* of rings. To get an intuitive idea, we consider a polynomial ring $k[x_1, \ldots, x_n]$ whose completion is the ring of formal power series $k[\![x_1, \ldots, x_n]\!]$. In a way, this imitates transcendental techniques from complex algebraic geometry where we can use holomorphic functions – power series converging uniformly near a point. Geometrically, this means to focus on "small" neighbourhoods unlike big open dense sets. Still, completion keeps two essential properties of localisation: it is an exact operation and preserves the Noether property. To give a concrete idea, consider the integral ring extension $k[x] \subset k[x,y]/(y^2 - x - 1)$. This corresponds to a ramified finite cover which generically is $2 - -1$. In the neighbourhood with no branching points one should be able to invert this map and to find local sections of this covering – this is certainly true if $k = \mathbb{R}$ or $\mathbb{C}$ when we have the inverse function at our disposal. However, the map $x \mapsto \sqrt{x+1}$ is not polynomial so that if we are working with polynomial rather than smooth or holomorphic functions, local section do not exist. However, $\sqrt{x+1}$ possesses a formal development so that at the level of power series there is indeed an inverse $k[\![x,y]\!]/(y^2 - x - 1) \to k[\![x]\!]$, $x \mapsto x$, $y \mapsto 1 + x/2 - x^2/8 + \ldots$. In general we will consider a ring A with ideal $\mathfrak{a}$ whose powers induce a topology on A, the so-called $\mathfrak{a}$-*adic topology*. Completing this topology gives the *completion* $\hat{A}$. Similarly, one can complete A-modules. The most important instance of this are completions of local Noetherian rings $(A, \mathfrak{m})$ (such as the stalks $\mathcal{O}_{X,a}$) with respect to $\mathfrak{m}$. In particular, we want to prove the

1. Theorem. Let $(A, \mathfrak{m})$ be a Noetherian local ring with completion $\hat{A}$.

(i) $(\hat{A}, \mathfrak{m}\hat{A})$ *is a Noetherian local ring with natural injective homomorphism* $A \to \hat{A}$*;*

(ii) *if* M *is a finitely generated* A*-module, its completion* $\hat{M}$ *with respect to* $\mathfrak{m}$ *is isomorphic as* $\hat{A}$*-module to* $M \otimes_A \hat{A}$*.*

A second important statement which we will state more precisely below, is *Cohen's structure theorem*. In a simplified version it reads as follows.

2. Theorem (Cohen, special case). *The completion of the localisation* $k[x_1, \ldots, x_n]_{\mathfrak{m}}$*, the stalk of regular functions at* $a \in \mathbb{A}^n$ *corresponding to the maximal ideal* $\mathfrak{m}$*, is isomorphic to* $k[\![x_1, \ldots, x_n]\!]$*.*

In a way, we can think of the completion of the stalk of regular functions of a (smooth) variety (yet to be defined) as ring of power series in the coordinates.

3. Definition. We say that two points $a \in X$ and $b \in Y$ of two varieties X and Y are **analytically isomorphic** if $\hat{\mathcal{O}}_{X,a} = \hat{\mathcal{O}}_{Y,b}$.

In particular, any two points of $\mathbb{A}^n$ (or more generally, of a smooth variety) are analytically isomorphic in accordance with the intution coming from classical manifolds. A less trivial example is this.

4. Example. Let X be the plane nodal curve given by $y^2 - x^3 - x^2 = 0$ in $\mathbb{A}^2$ and Y the reducible algebraic set $xy = 0$. Let us show that X and Y are analytically isomorphic at the point $(0,0)$. By Corollary proven below we have $\hat{\mathcal{O}}_{X,0} \cong k[\![x,y]\!]/(y^2 - x^2 - x^3)$ (where we view the ideal $(y^2 - x^2 - x^3)$ as an ideal in $k[\![x,y]\!]$). Similarly, $\hat{\mathcal{O}}_{Y,0} \cong k[\![x,y]\!]/(xy)$. The key point is that we can factor

$y^2-x^2-x^3$ into formal power series $g = y+x+g_2+g_3+\ldots$ and $h = y-x+h_2+h_3+\ldots$ in $k[\![x,y]\!]$ with g_i and h_i homogeneous of degree i, that is, $y^2 - x^2 - x^3 = gh$. We can construct g and h step by step. Namely, $(y-x)g_2 + (y+h)h_2 = -x^3$ since x^3 lies in the ideal generated by $y-x$ and $y+x$, and so on. Therefore, $\hat{\mathcal{O}}_{X,0} = k[\![x,y]\!]/(gh)$. Since g and h begin with linearly independent terms, we can define an automorphism of $k[\![x,y]\!]$ which sends g and h to x and y, respectively. Hence $\hat{\mathcal{O}}_{X,0} \cong k[\![x,y]\!]/(xy) \cong \hat{\mathcal{O}}_{Y.0}$. Geometrically, this corresponds to the fact that near the origin (in a Euclidean sense!), X looks like Y, see Figure 3.16.

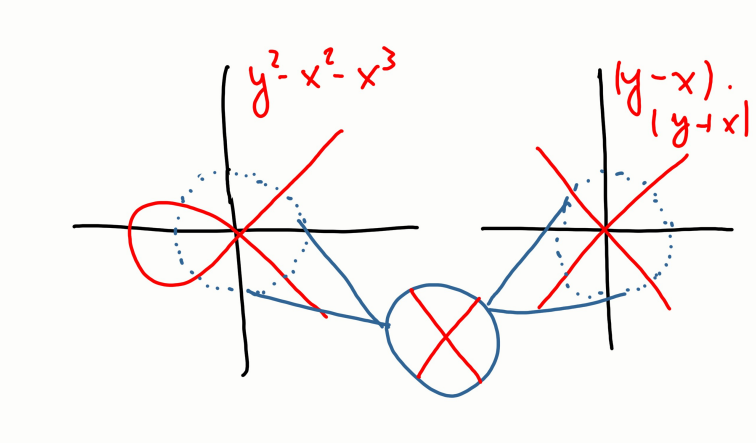

FIGURE 16. The local equivalence between $\mathcal{Z}(y^2 - x^2 - x^3)$ and $\mathcal{Z}(xy)$..

Topology. Let G be a topological Abelian group, not necessarily Hausdorff. This implies in particular that the *translations* $T_a : G \to G$, $T_a(g) = a + g$ are continuous maps and in fact homeomorphisms (with inverse T_{-a}). The topology of G is therefore determined by the neighbourhoods of $0 \in G$.

5. Exercise. Let H be the intersection of all neighbourhoods of 0 in G. Then

(i) H is a subgroup;
(ii) H is the closure of $\{0\}$;
(iii) G/H is Hausdorff;
(iv) G is Hausdorff $\Leftrightarrow H = 0$.

Proof. (i) Let $x_i \in H$, and let V be a neighbourhood of 0. We have to show that $x_1 + x_2 \in V$. By continuity of $+$ there exist U_i neighbourhood of 0 such that $U_1 + U_2 \subset V$. Since $x_i \in H$, $x_i \in U_i$, hence $x_1 + x_2 \in V$.

(ii) $x \in H \overset{(i)}{\Leftrightarrow} -x \in H \Leftrightarrow 0 \in T_x(U)$ for any neighbourhood U of $0 \Leftrightarrow 0 \in V$ for any neighbourhood V of $x \Leftrightarrow 0 \in \overline{\{0\}}$.

(iii) By (ii), cosets $a + H$ are closed. Hence the points of G/H are closed which means that G/H is Hausdorff.

(iv) Trivial. □

Next assume that $0 \in G$ has a countable fundamental system of neighbourhoods (this avoids using *nets* instead of sequences). Then we can define the **completion of** G to be the space $\hat{G}$ of all Cauchy sequences (x_n) modulo the equivalence relation

$(x_n) \cong (y_n) \Leftrightarrow x_n - y_n \to 0$. Addition of Cauchy sequences gives $\hat{G}$ a natural group structure. To define a topology on $\hat{G}$ we specify the open neighbourhoods of $\hat{0} = (0)$ of $\hat{G}$: For any open neighbourhood U of 0 in G, we let $\hat{U}$ be the set of equivalence classes of sequences which eventually ly in U. This turns $\hat{G}$ into a topological group. For instance, if $G = \mathbb{Q}$ then $\hat{G} = \mathbb{R}$. Note that we have a natural map $\phi : G \to \hat{G}$, $\phi(x) = (x)$ the constant Cauchy sequence $x_n = x$ for all n. Then $\ker \phi = \bigcap U = H$ where U is an open neighbourhood of 0. In particular, ϕ is injective $\Leftrightarrow$ G is Hausdorff. If ϕ is an isomorphism, we say that G is **complete**. In particular, G must be Hausdorff. Next, if $f : G \to H$ is a group morphism between Abelian topological groups with countable fundamental systems of neighbourhoods for 0, then f maps Cauchy sequences to Cauchy sequences (check!) and induces thus a (continuous) group morphism $\hat{f} : \hat{G} \to \hat{H}$. Since $\widehat{g \circ f} = \hat{g} \circ \hat{f}$ we obtain a covariant functor.

In the following we restrict to the situation where we have a fundamental system of neighbourhoods of 0 of *subgroups* G_n of G

$$G = G_0 \supset G_1 \supset G_2 \supset \ldots \supset G_n \supset \ldots .$$

The most important class of examples arises as follows.

6. Definition ($\mathfrak{a}$-adic topology). Take $G = A$ a ring, and let $G_n = \mathfrak{a}^n$ for an ideal $\mathfrak{a} \subset G$. The topology induced on A is called the **$\mathfrak{a}$-adic topology**. For this topology, a sequence $(g_i) \subset G$ is Cauchy if and only if for all n there exists $N(n)$ such that $g_i - g_j \in \mathfrak{a}^n$ for all $i, j \geqslant N(n)$.

Since $\mathfrak{a}$ is an ideal, the resulting completion $\hat{A}$ is in fact a topological ring, and $\phi : A \to \hat{A}$ is a ring morphism with kernel $\bigcap \mathfrak{a}^n$. More generally, we can consider A-modules M, i.e. $G = M$ and $G_n = \mathfrak{a}^n M$. Its completion $\hat{M}$ is a (topological) $\hat{A}$-module, and any A-module morphism $f : M \to N$ determines an $\hat{A}$-linear map $f : \hat{M} \to \hat{N}$ between the respective completions.

7. Example. Let $A = k[x]$ and $\mathfrak{a} = (x)$. Then $\hat{A} = k[\![x]\!]$, the *ring of formal power series*. Indeed, let (a_n) be a Cauchy sequence in A. Then $a_n = \sum_{i=0}^{k_n} c_i(n) x^i$. Since $a_n - a_m \in (x^M)$ for $n, m \geqslant N$, the first M terms must be fixed for any a_n with $r \geqslant n$. Hence the "Taylor development" of the a_n stabilises for $N \to \infty$, and the higher gets M, the closer $\sum_{i \geqslant M} c_i x^i$ gets to 0, i.e. $\sum_{i \geqslant M} c_i x^i \to 0$ as $M \to \infty$.

Of course, different filtrations, i.e. infinite chains of the form $M = M_0 \supset M_1 \supset \ldots$ of submodules of M can give rise to the same topology as $\mathfrak{a}^n M$.

8. Definition (stable $\mathfrak{a}$-filtrations). A filtration (M_n) is called an **$\mathfrak{a}$-filtration** if $\mathfrak{a} M_n \subset M_{n+1}$ for all n. If we have equality for all sufficiently large n, then the filtration is called **$\mathfrak{a}$-stable**.

Of course, the prototype of a stable $\mathfrak{a}$-filtration is $M_n = \mathfrak{a}^n M$.

9. Lemma (stable $\mathfrak{a}$-filtrations induce the same topology). *If (M_n) and (M'_n) are stable $\mathfrak{a}$-filtrations, then there exists an integer k such that $M_{n+k} \subset M'_n \subset M_{n-k}$ for all $n \geqslant k$, i.e. both filtrations have* **bounded difference**. *In particular, all stable $\mathfrak{a}$-filtrations induce the same topology.*

Proof. Without loss of generality, $M'_n = \mathfrak{a}^n M$. Since $\mathfrak{a} M_n \subset M_{n+1}$ we have $M'_{n+k} \subset M'_n = \mathfrak{a}^n M \subset M_n$ for all k and n. The last inclusion becomes equality if $n \geqslant k$ for k sufficiently big, whence $M_{n+k} = \mathfrak{a}^n M_k \subset \mathfrak{a}^n M_0 = M'_n$. □

To understand the previous examples from an algebraic point of view, the following alternative contruction of completions is useful. Open sets always contain open sets of the form $x + G_m$ which defines an element in G/G_m. On the other hand, if (x_n) is a Cauchy sequence, then for any $m \in \mathbb{N}$ there exists m_0 with $x_i - x_j \in G_m$ for all $i,\ j \geqslant m_0$. Hence, the image $\bar{x}_i = x_i + G_m$ in G/G_m of the Cauchy sequence is ultimately constant, equal say to ξ_m. Under the projection $\pi_{m+1} : G/G_{m+1} \to G/G_m$, ξ_m maps to ξ_{m+1} (if all but a finite number of the x_i are contained in G_{m+1} then they are also contained in $G_m \supset G_{m+1}$). We also say that (ξ_n) is a **coherent sequence** in the sense that $\pi_{m+1}(\xi_{m+1}) = \xi_m$ for all m. Further, equivalent sequences obviously define the same sequence (ξ_n). Therefore, we can view $\hat{G}$ as the set of coherent sequences with its obvious group structure. Now in general, a sequence of groups $\{H_n\}$ with morphisms $\theta_{n+1} : H_{n+1} \to H_n$ is called an **inverse system**, and the group of coherent sequences is called the **inverse limit** for which one writes $\varprojlim H_n$: Coming back to our case we can identify $\varprojlim G/G_n$ with $\hat{G}$ as defined in the sense above.

10. Example.

(i) Let $A = \mathbb{Z}$, $\mathfrak{a} = (p)$ for p prime. Then $\hat{A} = \varprojlim \mathbb{Z}/p^n\mathbb{Z}$ is the *ring of p-adic integers* given by infinite series $(a_n)_{n=0}^{\infty}$ with $0 \leqslant a_n \leqslant p^n - 1$ and $a_n = a_{n+1} \bmod p^n$.

(ii) Let $A = k[x_1, \ldots, x_n]$, $\mathfrak{m} = (x_1, \ldots, x_n)$ the maximal ideal corresponding to the origin. Then $k[\![x_1, \ldots, x_n]\!] = \hat{A}$.

The main advantage of this algebraic description comes when dealing with exact sequences. An **exact sequence of inverse systems** $0 \to \{A_n\} \to \{B_n\} \to \{C_n\} \to 0$ consists of a commutative diagramm

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A_{n+1} & \longrightarrow & B_{n+1} & \longrightarrow & C_{n+1} & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & A_n & \longrightarrow & B_n & \longrightarrow & C_n & \longrightarrow & 0 \end{array}$$

of exact sequences.

11. Proposition. *If $0 \to \{A_n\} \to \{B_n\} \to \{C_n\} \to 0$ is an exact sequence of inverse systems, then*

$$0 \to \varprojlim A_n \to \varprojlim B_n \to \varprojlim C_n$$

is exact. Furthermore, if $\{A_n\}$ is **surjective***, that is, the projections maps π_n of the inverse systems are always surjective, then*

$$0 \to \varprojlim A_n \to \varprojlim B_n \to \varprojlim C_n \to 0$$

is exact.

Proof. This is essentially an application of the Snake lemma 0.49, see [AtMa, Proposition 10.2]. □

Note that inverse systems of the form $\{G/G_n\}$ are always surjective.

12. Corollary (completion is an exact functor). *Let $0 \to G' \to G \to G'' \xrightarrow{p} 0$ be an exact sequence of groups. Let G have the topology defined by a sequence $\{G_n\}$*

of subgroups, and endow G' and G'' with the induced topologies defined by $G' \cap G_n$ and $p(G_n)$. Then

$$0 \to \hat{G}' \to \hat{G} \to \hat{G}'' \to 0$$

is an exact sequence of groups.

Proof. Apply Proposition 3.11 to the exact sequence

$$0 \to G'/(G' \cap G_n) \to G/G_n \to G''/p(G_n) \to 0.$$

□

13. Corollary. *$\hat{G}_n$ is a subgroup of $\hat{G}$ and*

$$\hat{G}/\hat{G}_n \cong G/G_n. \tag{4}$$

In particular, $\hat{\hat{G}} \cong \hat{G}$, that is, the completion is actually complete.

Proof. Apply the previous corollary with $G' = G_n$ and $G'' = G/G_n$ yields $\hat{G}_n \cong \hat{G}/\hat{G}_n = \hat{G}''$. Since the induced topology on G'' is discrete, $\hat{G}'' = G'' = G/G_n$. Finally, taking the inverse limit of (4) shows that $\hat{G} = \varprojlim G/G_n = \varprojlim \hat{G}/\hat{G}_n = \hat{\hat{G}}$. □

If (M_n) is a filtration for an A-module $M_0 = M$, a submodule $N \subset M$ inherits a natural subfiltration $N \cap M_n$. Our next goal is to establish the following

14. Theorem. *Let A be a Noetherian ring, $\mathfrak{a}$ an ideal of A, M a finitely generated A-module, and N a submodule of M. Then the filtrations $\mathfrak{a}^n N$ and $(\mathfrak{a}^n M) \cap N$ have bounded difference. In particular, the $\mathfrak{a}$-topology of N coincides with the topology induced by the $\mathfrak{a}$-topology of M.*

Proof. The proof will be based on a series of lemmatas. We introduce some notation first. Let A be a ring and $\mathfrak{a}$ be an ideal of A. Then we define the graded ring $A^* = \bigoplus_{n \geqslant 0} \mathfrak{a}^n$. More generally, if M is an A-module with $\mathfrak{a}$-filtration (M_n), then we put $M^* = \bigoplus_{n \geqslant 0} M_n$. This is a graded A^*-module, since $A_m M_n = \mathfrak{a}^m M_n \subset M_{n+m}$.

15. Lemma. *Let A be a Noetherian ring, M a finitely generated A-module, and (M_n) an $\mathfrak{a}$-filtration of M. Are equivalent:*

(i) *M^* is a finitely generated A^*-module;*
(ii) *The filtration is stable.*

In particular, any $\mathfrak{a}$-filtration of a finitely generated A^*-module M for A Noetherian induces the same topology on M.

Proof. Since M must be Noetherian by Corollary 0.95, each M_n must be finitely generated, and hence so is $Q_n = \bigoplus_{i=0}^{n} M_i \subset M^* = \langle m_1, \ldots, m_r \rangle$. To turn Q_n into an A^*-submodule, we put

$$M_n^* := Q_n \oplus \bigoplus_{i \geqslant 1} \mathfrak{a}^i M_n.$$

This is generated by $m_1, \dots, m_r$ over A^*. Now $\{M_n^*\}$ forms an anascending chain whose union is all of M^*. Now

$$\begin{aligned} M^* \text{ is finitely generated as an } A-\text{module} &\Leftrightarrow \\ \text{the chain stops} &\Leftrightarrow \\ M^* = M_{n_0}^* \text{ for some } n_0 &\Leftrightarrow \\ M_{n_0+r} = \mathfrak{a}^r M_{n_0} \text{ for all } r \geqslant 0 &\Leftrightarrow \\ \text{the filtration is stable,} & \end{aligned}$$

whence the result. □

16. Proposition (Artin-Rees). *Let A be a Noetherian ring, $\mathfrak{a}$ an ideal in A, M a finitely generated A-module, (M_n) a stable $\mathfrak{a}$-filtration of M. If M' is a submodule of $M \Rightarrow (M' \cap M_n)$ is a stable $\mathfrak{a}$-filtration of M'. In particular, taking $M_n = \mathfrak{a}^n M$, then there exists an integer k such that*

$$(\mathfrak{a}^n M) \cap M' = \mathfrak{a}^{n-k}((\mathfrak{a}^k M) \cap M')$$

for all $n \geqslant k$.

Proof. We have $\mathfrak{a}(M' \cap M_n) \subset \mathfrak{a}M' \cap \mathfrak{a}M_n \subset M' \cap M_{n+1}$, hence $(M' \cap M_n)$ is an $\mathfrak{a}$-filtration. This defines a graded A^*-module which is a submodule of M^* and thus finitely generated (for M^* is by the previous lemma, and A is Noetherian). Again, Lemma 3.15 implies that $(M' \cap M_n)$ is stable. □

Lemma 3.9 immediately implies Theorem 3.14 □

In particular, exactness of the completion (Corollary 3.12) gives

17. Proposition (completion is exact on finitely-generated modules over Noetherian rings. *Let*

$$0 \to M' \to M \to M'' \to 0$$

be an exact sequence of finitely generated modules over a Noetherian ring A. Let $\mathfrak{a}$ be an ideal of $A \Rightarrow$ The sequence of $\mathfrak{a}$-adic completions

$$0 \to \hat{M}' \to \hat{M} \to \hat{M}'' \to 0$$

is exact.

The completion $\hat{A}$ is a natural A-module via the completion map $A \to \hat{A}$. In particular, given an A-module M we can form the $\hat{A}$-module $\hat{A} \otimes_A M$. Moreover, there is the completion map $M \to \hat{M}$ which is also an A-module morphism. Hence we get an induced sequence of $\hat{A}$-module morphisms

$$\hat{A} \otimes_A M \to \hat{A} \otimes_A \hat{M} \to \hat{A} \otimes_{\hat{A}} \hat{M} = \hat{M}.$$

This induced map behaves particularly well for A Noetherian and finitely generated M.

18. Proposition. *If M is finitely generated $\Rightarrow \hat{A} \otimes_A M \to \hat{M}$ is surjective. If, moreover, A is Noetherian $\Rightarrow \hat{A} \otimes_A M \to \hat{M}$ is an isomorphism.*

Proof. If M is finitely generated, we get an exact sequence $0 \to N \to F \to M$ for a free A-module $F \cong A^n$. It follows from Corollary 3.12 that $\mathfrak{a}$-adic completion commutes with taking direct sums so that for $F \cong A^n$, $\hat{A} \otimes_A F \cong (\hat{A} \otimes_A A)^n \cong \hat{A}^n$. This gives rise to a diagramm

$$\begin{array}{ccccccccc} & & \hat{A} \otimes_A N & \longrightarrow & \hat{A} \otimes_A F & \longrightarrow & \hat{A} \otimes_A M & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \gamma} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \alpha} & & \\ 0 & \longrightarrow & \hat{N} & \longrightarrow & \hat{F} & \xrightarrow{\delta} & \hat{M} & \longrightarrow & 0 \end{array}$$

in which the top line is exact since ($\hat{A} \otimes_A$ is right exact). Moreover (again by Corollary 3.12) δ is exact which implies that α is surjective for β is an isomorphism. Moreover, if A is Noetherian then N is finitely generated as an A-submodule of a finitely generated A-module which implies that γ is surjective, and thus that the bottom line is exact. This in turn implies that α is injective, hence an isomorphism. □

19. Corollary. *If A is Noetherian ⇒ The functor $T_{\hat{A}}$ is exact on the category of finitely generated A-modules. In particular, it follows from Proposition 0.74 that the $\mathfrak{a}$-adic completion $\hat{A}$ of A is a flat A-algebra.*

For the next proposition, recall that the Jacobson radical $\mathcal{J}(A)$ of a ring A is the intersection of all maximal ideals (see Section 0.0.1).

20. Proposition (further properties of $\hat{A}$). *Let A be Noetherian with $\mathfrak{a}$-adic completion $\hat{A}$ ⇒*

(i) $\hat{\mathfrak{a}} \cong \hat{A} \otimes_A \mathfrak{a} = \hat{A}\mathfrak{a} = \mathfrak{a}^e$;
(ii) $\widehat{\mathfrak{a}^n} = (\hat{\mathfrak{a}})^n$;
(iii) $\mathfrak{a}^n/\mathfrak{a}^{n+1} \cong \hat{\mathfrak{a}}^n/\hat{\mathfrak{a}}^{n+1}$;
(iv) $\hat{\mathfrak{a}}$ *is contained in the Jacobson radical of* $\hat{A}$.

Proof. (i) Since A is Noetherian, $\mathfrak{a}$ is finitely generated. In particular, the map $\hat{A} \otimes_A \mathfrak{a} \to \hat{\mathfrak{a}}$ is an isomorphism. Since $\hat{A}$ is flat, the injection $0 \to \mathfrak{a} \to A$ induces an isomorphism $\mathfrak{a} \otimes_A \hat{A} \to A \otimes_A \hat{A} \cong M$, which sends $x \otimes \hat{a}$ to $x \cdot \hat{a}$. Hence the image of this isomorphism is just $\hat{A}\mathfrak{a} = \mathfrak{a}^e$, where the extension is taken with respect to the natural completion map $A \to \hat{A}$.

(ii) Applying (i) to $\mathfrak{a}^n$ we see that $\widehat{\mathfrak{a}^n} = \hat{A}\mathfrak{a}^n = (\hat{A}\mathfrak{a})^n$ since extension commutes with taking powers (see for instance [AtMa, Exercise 1.18]). But the latter is equal to $(\hat{\mathfrak{a}})^n$.

(iii) From (4) we immediately deduce that $A/\mathfrak{a}^n \cong \hat{A}/\hat{\mathfrak{a}}^n$ from which (iii) follows by taking quotients.

(iv) For any $x \in \hat{\mathfrak{a}}$, the sequence $a_n = \sum_{i=0}^{n} x^i$ is Cauchy in A for its $\mathfrak{a}$-adic topology. Further, as a completion, $\hat{A}$ is itself complete. Therefore, a_n converges to $\sum x^i = (1-x)^{-1}$, that is, $1-x$ is a unit. From Proposition 0.21 it follows that $\mathfrak{a} \subset \mathcal{J}(A)$. □

21. Corollary ($\hat{A}$ is local if A is local). *Let $(A, \mathfrak{m})$ be a Noetherian local ring ⇒ the $\mathfrak{m}$-adic completion $\hat{A}$ of A is a local ring with maximal ideal $\hat{\mathfrak{m}}$.*

Proof. By the previous proposition we have $\hat{A}/\hat{\mathfrak{m}} \cong A/\mathfrak{m}$, hence $\hat{A}/\hat{\mathfrak{m}}$ is a field, so $\hat{\mathfrak{m}}$ is a maximal ideal. Further, $\hat{\mathfrak{m}}$ is contained in $\mathcal{J}(\hat{A})$, hence is equal to it by maximality. Hence $\hat{\mathfrak{m}}$ is the unique maximal ideal, and $(\hat{A}, \hat{\mathfrak{m}})$ is a local ring. □

22. Corollary.

(i) *Let A be a Noetherian ring, and $\mathfrak{a}$ be an ideal. Then the $\mathfrak{a}$-adic completion is*

$$\hat{A} \cong A[\![x_1, \ldots, x_n]\!]/(x_1 - a_1, \ldots, x_n - a_n)$$

for elements $a_i \in A$.

(ii) *The completion of the coordinate ring $A = k[x_1, \ldots, x_n]/\mathfrak{a}$ with respect to the maximal ideal $\mathfrak{m} = (\bar{x}_1, \ldots, \bar{x}_n)$ is*

$$\hat{A} \cong k[\![x_1, \ldots, x_n]\!]/\mathfrak{a}k[\![x_1, \ldots, x_n]\!].$$

Proof. (i) Since A is Noetherian, $\mathfrak{a}$ is finitely generated, say by $a_1, \ldots, a_n$. We consider the exact sequence of finitely generated $A[x_1, \ldots, x_n]$-modules

$$0 \longrightarrow (x_1 - a_1, \ldots, x_n - a_n) \longrightarrow A[x_1, \ldots, x_n] \longrightarrow A \longrightarrow 0$$

induced by the evaluation morphism $A[x_1, \ldots, x_n] \to A$ sending x_i to a_i. Completion by the ideal $\mathfrak{b} = (x_1, \ldots, x_n)$ of $A[x_1, \ldots, x_n]$ is exact by Proposition 3.17. Further, the completion of A with respect to $\mathfrak{b}$ coincides with the completion by $\mathfrak{a}$.

(ii) Consider the exact sequence of finitely generated $k[x_1, \ldots, x_n]$-modules $0 \to \mathfrak{a} \to k[x_1, \ldots, x_n] \to A \to 0$ and apply Proposition 3.17 as well as (i) from Proposition 3.20. □

23. Example. Let us compute the completion of the ring $k[x, y]/(y^2 - x^2 - x^3)$ localised at the maximal ideal (x, y), i.e. the ring $\mathcal{O}_{Y,0}$, cf. Example 3.4. By the exactness of localisation, $(k[x, y]/(y^2 - x^2 - x^3))_{(x,y)}$ is isomorphic to $k[x, y]_{(x,y)}/(y^2 - x^2 - x^3)$ (considering $(y^2 - x^2 - x^3)$ as an ideal in $k[x, y]_{(x,y)}$). By the previous corollary as well as Cohen's structure theorem 3.2, the completion of $k[x, y]_{(xy)}$ is $k[\![x, y]\!]$ whence $\hat{\mathcal{O}}_{Y,a} \cong k[\![x, y]\!]/(y^2 - x^2 - x^3)$ (considering now the extended ideal $(y^2 - x^2 - x^3)$ as an ideal in $k[\![x, y]\!]$).

24. Theorem (Krull). *Let A be a Noetherian ring, $\mathfrak{a}$ an ideal of A, M a finitely generated A-module and $\hat{M}$ the $\mathfrak{a}$-completion of $M \Rightarrow$ The kernel $N = \bigcap_{n \geqslant 0} \mathfrak{a}^n M$ of the completion $M \to \hat{M}$ consists of those $x \in M$ annihilated by some element of $1 + \mathfrak{a}$.*

Proof. If $(1 - a)x = 0$ for some $a \in \mathfrak{a}$, then $x = ax = a^2x = \ldots \in \bigcap_{n=1}^{\infty} \mathfrak{a}^n M = N$. Conversely, we note that the induced topology on N is trivial, i.e. N is the only neighbourhood of $0 \in N$ since N is the intersection of all neighbourhoods of $0 \in M$. But it follows from Artin-Rees that this trivial topology coincides with the $\mathfrak{a}$-adic topology of N. In particular, since $\mathfrak{a}N$ is an open neighbourhood of 0, $\mathfrak{a}N = N$. Since A is Noetherian and M is finitely generated, so is N. By Cayley-Hamilton (cf. Corollary 0.57), there exists $a \in \mathfrak{a}$ such that $(1 - a)N = 0$. □

25. Remark.

(i) If S is the multiplicatively closed set $1+\mathfrak{a}$, then the kernel of $A \to \hat{A}$ is precisely the kernel of the natural map $S^{-1}A \to A$, cf. Exercise 1.89. Furthermore, for any $a \in \hat{\mathfrak{a}}$, the Cauchy sequence $\sum_{i=0}^{n} a^i$ converges, namely to $(1-a)^{-1}$, so that every element of S in becomes a unit in $\hat{A}$. By the universal property of localisations 1.100, there exists a natural morphism $S^{-1}A \to \hat{A}$ which is injective, and $S^{-1}A$ can be identified with a subring of $\hat{A}$.

(ii) Krull's theorem may fail whenever A is not Noetherian. Consider, for instance, $C^\infty(\mathbb{R})$ (cf. Example 0.88 (iv)). Let $\mathfrak{m}$ be the maximal ideal of functions which vanish at the origin. By Taylor's theorem, $\mathfrak{m} = (x)$ and $N = \bigcap \mathfrak{m}^k$ consists of functions whose derivative up to any order vanishes at the origin. Further, $f \in C^\infty(\mathbb{R})$ is annihilated by some element in $1 + \mathfrak{a}$ if and only if f vanishes identically near 0. However, the well-known function e^{-1/x^2} lies in N, but does not vanish for $x > 0$.

There are two immediate corollaries.

26. Corollary. *Let A be a Noetherian integral domain, and $\mathfrak{a} \neq (1)$ an ideal of $A \Rightarrow \bigcap \mathfrak{a}^n = 0$. In particular, the $\mathfrak{a}$-adic topology on A is Hausdorff.*

Proof. Otherwise, there would be zerodivisors. □

27. Corollary. *Let A be a Noetherian ring, $\mathfrak{a}$ an ideal of A contained in $\mathcal{J}(A)$, and M be a finitely generated A-module. Then the $\mathfrak{a}$-topology of M is Hausdorff, i.e. $\bigcap \mathfrak{a}^n M = 0$. This applies in particular to the situation of a Noetherian local ring $(A, \mathfrak{m})$ and the $\mathfrak{m}$-adic topology on M.*

Proof. By Proposition 0.21 we know that any $1+a$, $a \in \mathfrak{a}$, must be a unit. Therefore $x \mapsto (1+a) \cdot x$ has trivial kernel. □

The associated graded ring. Our final goal is to show that the $\mathfrak{a}$-adic completion of a Noetherian ring is again Noetherian.

Let A be a ring and $\mathfrak{a}$ an ideal of A. We define the **associated graded ring** by

$$Gr_{\mathfrak{a}}(A) = \bigoplus_{n \geqslant 0} \mathfrak{a}^n/\mathfrak{a}^{n+1}$$

(with the convention $\mathfrak{a}^0 = A$). If the underlying ideal $\mathfrak{a}$ is clear from the context we also write simply $Gr(A)$. This is indeed a graded ring with multiplication defined as follows. If $x_n \in \mathfrak{a}^n$ whose induced equivalence class in $\mathfrak{a}^n/\mathfrak{a}^{n+1}$ is denoted by $\bar{x}_n$, then $\bar{x}_m \bar{x}_n := \overline{x_m x_n}$. For example, if A is Noetherian, we have $\mathfrak{a} = (x_1, \ldots, x_r)$. Let $\bar{x}_i$ be the image of x_i in $\mathfrak{a}/\mathfrak{a}^2$, then $Gr(A) = (A/\mathfrak{a})[\bar{x}_1, \ldots, \bar{x}_r]$. Similarly, if M is an A-module with $\mathfrak{a}$-filtration (M_n), then we define

$$Gr(M) := \bigoplus_{n \geqslant 0} M_n/M_{n+1}.$$

This is a graded $Gr_{\mathfrak{a}}(A)$-module. We let $Gr_n(M) = M_n/M_{n+1}$.

28. Proposition. *Let A be a Noetherian ring, and let $\mathfrak{a}$ be an ideal of $A \Rightarrow$*

(i) *$Gr_{\mathfrak{a}}(A)$ is Noetherian;*

(ii) *$Gr_{\mathfrak{a}}(A)$ and $Gr_{\hat{\mathfrak{a}}}(\hat{A})$ are isomorphic as graded rings;*

(iii) *if M is a finitely generated A-module and (M_n) is a stable $\mathfrak{a}$-filtration of M, then $Gr(M)$ is a finitely generated graded $Gr_{\mathfrak{a}}(A)$-module.*

Proof. (i) We have $Gr(A) = (A/\mathfrak{a})[\bar{x}_1, \ldots, \bar{x}_r]$ for A is Noetherian. Since $A/\mathfrak{a}$ is Noetherian, $Gr(A)$ is Noetherian by the Hilbert basis theorem.

(ii) $\mathfrak{a}^n/\mathfrak{a}^{n+1} \cong \hat{\mathfrak{a}}^n/\hat{\mathfrak{a}}^{n+1}$ by Proposition 3.20.

(iii) There exists n_0 such that $M_{n_0+i} = \mathfrak{a}^i M_{n_0}$ for all $i \geqslant 0$, so that as an $Gr(A)$-module, $Gr(M)$ is generated by $\bigoplus_{n \leqslant n_0} Gr_n(M)$. Furthermore, each $Gr_n(M)$ is Noetherian and annihilated by $\mathfrak{a}$, therefore it is a finitely generated $A/\mathfrak{a}$-module. Consequently, $\bigoplus_{n \leqslant n_0} Gr_n(M)$ is a finitely generated $A/\mathfrak{a}$-module. These generators generate $Gr(M)$ as a $Gr(A)$-module. □

29. Lemma. *Let $\phi : M' \to M$ be a module morphism between filtered modules with $\phi(M'_n) \subset M_n$, and let $G(\phi) : Gr(M') \to Gr(M)$ and $\hat{\phi} : \hat{M}' \to \hat{M}$ be the induced morphisms of the associated graded and completed groups ⇒*

(i) *$G(\phi)$ is injective ⇒ $\hat{\phi}$ is injective;*
(ii) *$G(\phi)$ is surjective ⇒ $\hat{\phi}$ is surjective.*

Proof. This is again a consequence of the Snake Lemma 0.49 and Proposition 3.11, see [AtMa, Lemma 10.23]. □

This enables us to prove a kind of converse to item (iii) of the previous Proposition.

30. Proposition. *Let A be a ring, $\mathfrak{a}$ an ideal of A, M an A-module, and (M_n) an $\mathfrak{a}$-filtration of M. Suppose that A is complete in the $\mathfrak{a}$-topology and that M is Hausdorff in its filtration topology (i.e. $\bigcap M_n = 0$). Suppose also that $G(M)$ is a finitely generated $G(A)$-module ⇒ M is a finitely generated A-module.*

Proof. Let $\bar{x}_i$, $0 \leqslant i \leqslant \nu$, $x_i \in M_{n_i}$ be the homogeneous components of degree n_i of the finite set of generators of $G(M)$. Let $F^i = A$ be the module with stable $\mathfrak{a}$-filtration given by $F^i_n = \mathfrak{a}^{n-n_i}$ and put $F = \bigoplus_{i=1}^{\nu} F^i \cong A^\nu$. Mapping the generator $1 \in F^i$ to x_i defines a morphism $\phi : F \to M$ of filtered groups (with $F_n = \bigoplus_{i=0}^{\nu} \mathfrak{a}^{n-n_i}$), for $\phi(\mathfrak{a}^{n-n_i}) \subset \mathfrak{a}^{n-n_i} M_{n_i} \subset M_n$. By design, the induced morphism of $G(A)$-modules $G(\phi) : G(F) \to G(M)$ is surjective. Hence $\hat{\phi}$ is surjective by the lemma. Consider now the diagramm:

$$\begin{array}{ccc} F & \xrightarrow{\phi} & M \\ \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} \\ \hat{F} & \xrightarrow{\hat{\phi}} & \hat{M} \end{array}$$

Since $F \cong A^\nu$ is free and $A = \hat{A}$ for A is complete it follows that α is an isomorphism. Further, β is injective for M is Hausdorff. Now the surjectivity of $\hat{\phi}$ implies the surjectivity of ϕ, and in particular that M is finitely generated. □

31. Corollary. *Under the assumptions of the previous proposition, if $G(M)$ is a Noetherian $G(A)$-module ⇒ M is a Noetherian A-module.*

Proof. We show that every submodule M' of M is finitely generated. Indeed, let $M'_n = M' \cap M_n$. Then (M'_n) is an $\mathfrak{a}$-filtration of M', and the inclusion $M'_n \hookrightarrow M_n$ induces an injection $M'_n/M'_{n+1} \to M_n/M_{n+1}$ and thus an embedding $G(M') \to G(M)$. Since $G(M)$ is Noetherian by assumption, $G(M')$ is finitely generated. Further, $\bigcap M'_n \subset \bigcap M_n = 0$ so that M' is Hausdorff. It follows from the previous proposition that M' is finitely generated. □

This finally induces the desired result:

32. Theorem (the $\mathfrak{a}$-adic completion of a Noetherian ring is again Noetherian). *Let A be a Noetherian ring, $\mathfrak{a}$ an ideal, and $\hat{A}$ the $\mathfrak{a}$-adic completion $\Rightarrow$ $\hat{A}$ is Noetherian.*

Proof. In general, a ring is Noetherian if and only if it is Noetherian regarded as a module over itself. We have already seen that $Gr_{\mathfrak{a}}(A) = Gr_{\hat{\mathfrak{a}}}(\hat{A})$ is Noetherian, that is, setting $M = \hat{A}$ and $M_n = \mathfrak{a}^n$, $Gr(M)$ is a Noetherian $Gr_{\hat{\mathfrak{a}}}(\hat{A})$-module. Now $\hat{A}$ is Hausdorff being a complete space so that $\bigcap \mathfrak{a}^n = \bigcap M_n = \{0\}$. Applying the previous corollary gives the result. □

From this and Example 3.7 we get another proof for Exercise 0.104.

33. Corollary. *If A is Noetherian, then so is the ring of formal power series $A[\![x_1, \ldots, x_n]\!]$.*

3.2. **Dimension.** We are now prepared to investigate two local notions: dimension and non-singularity.

Dimension of varieties. Geometrically, we think of the dimension of a variety as the number of "coordinates" or degrees of freedom. However, one can define dimension in a purely topological context.

34. Definition. If X is a topological space, then we define its **dimension** $\dim X$ to be the supremum of all integers n such that there exists a chain $Z_0 \subset Z_1 \subset \ldots Z_n$ of distinct irreducible closed subsets of X. We define the **dimension of a variety** to be its dimension as a topological space.

Note that the dimension is *finite* for a Noetherian topological space. Of course, this notion of dimension is not very interesting on general topological spaces. For instance, $\mathbb{C}$ with its standard Euclidean topology has dimension 0 (the only irreducible sets are points) while seen as affine space $\mathbb{A}^1_{\mathbb{C}}$ it has dimension 1 (take the chain $\{0\} \subset \mathbb{A}^1_{\mathbb{C}}$). This notion is therefore well adapted to our algebraic context and as such, one expects this notion to have a ring theoretic description.

35. Definition (height of a prime ideal and dimension of a ring). The **codimension** or **height** of a prime ideal $\mathfrak{p}$ in A is the supremum of lengths of strict chains of prime ideals $\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \ldots \subset \mathfrak{p}_r = \mathfrak{p}$ which end at $\mathfrak{p}$. The **(Krull) dimension** $\dim A$ of A is the supremum of heights of all prime ideals, i.e. lengths of strict chains of prime ideals $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \ldots \subsetneq \mathfrak{p}_n$.

36. Example.

(i) $\dim k[x] = 1$. Indeed, (0) is a prime ideal, and since $k[x]$ is a principal ideal domain, any non-trivial prime ideal is maximal.
(ii) The dimension of a point $a \in \mathbb{A}^1$ is obviously 0 so that its codimension is 1. On the other hand, the height of its associated maximal ideal $(x - a)$ in $k[x]$ also equals 1.
(iii) By Exercise 1.106, $\operatorname{height} \mathfrak{p} = \dim A_{\mathfrak{p}}$. Geometrically, this corresponds to the *codimension* of the affine variety $\mathcal{Z}(\mathfrak{p}) \subset \operatorname{Spec} A$ as we will see below.

The first item of the previous example shows that the Krull dimension of the coordinate ring of $\mathbb{A}^1_k$ equals its topological dimension. This holds in general.

37. Proposition. *If $X \subset \mathbb{A}^n$ is an affine algebraic set, then the (topological) dimension of X equals the (Krull) dimension of its affine coordinate ring $A(X)$.*

Proof. The prime ideals in $A(X) = A[n]/\mathcal{I}(X)$ correspond to prime ideals in $A[n]$ which contain $\mathcal{I}(X)$, that is, to closed irreducible subsets of X. Hence the longest strict chain of closed irreducible subsets of X corresponds to the longest strict chain of prime ideals in $A(X)$. □

While this definition of the dimension of a ring easily relates to its toplogical counterpart t makes the actual computation of dimension difficult. One goal of this section is to show the following

38. Theorem. *Let k be a field, and B a finitely generated k-algebra which is an integral domain. Then*

(i) *the dimension of B is equal to the transcendence degree of the field extension $k \subset \operatorname{Quot} B$;*
(ii) *for any prime ideal $\mathfrak{p} \subset B$, we have*

$$\operatorname{height} \mathfrak{p} + \dim B/\mathfrak{p} = \dim B.$$

39. Corollary. *The dimension of $\mathbb{A}^n$ is n. Further, if $X \subset \mathbb{A}^n$ is any affine variety defined by the prime ideal $\mathfrak{p}$, then* $\operatorname{codim} X := n - \dim X = \operatorname{height} \mathfrak{p}$.

Proof. The transcendence degree of $\operatorname{Quot} A(\mathbb{A}^n) = k(x_1, \ldots, x_n)$ is just n which by the previous theorem equals the dimension of $A(\mathbb{A}^n) = k[x_1, \ldots, x_n]$. By Proposition 3.37, this is the dimension of $\mathbb{A}^n$. Moreover, $\operatorname{height} \mathfrak{p} = \dim \mathbb{A}^n - \dim X = \operatorname{codim} X$. □

40. Proposition. *If X is a quasiaffine variety, then* $\dim X = \dim \bar{X}$.

Proof. If $Z_0 \subset Z_1 \subset \ldots \subset Z_n$ is a sequence of distinct closed irreducible subsets of Y, then $\bar{Z}_0 \subset \bar{Z}_1 \subset \ldots \subset \bar{Z}_n$ is asequence of distinct closed irreducible subsets of $\bar{Y}$. Hence $\dim Y \leqslant \dim \bar{Y}$ and $\dim Y$ is finite. So choose a maximal sequence $Z_0 \subset Z_1 \subset \ldots \subset Z_n$, i.e. $n = \dim Y$. Then $Z_0 = \{a\}$ must be a point, and we have an induced sequence $\bar{Z}_0 \subset \bar{Z}_1 \subset \ldots \subset \bar{Z}_n$ in $\bar{Y}$. But a corresponds to a maximal ideal $\mathfrak{m}$ of $A(\bar{Y})$, the coordinate ring of $A(\bar{Y})$. Then the $\bar{Z}_i$ correspond to prime ideals in $\mathfrak{m}$ so that $n = \operatorname{height} \mathfrak{m}$. Now $A(\bar{Y})/\mathfrak{m} \cong k$ whence $n = \dim A(\bar{Y}) - 0 = \dim \bar{Y}$. Hence $\dim Y = \dim \bar{Y}$. □

Composition series and length. In linear algebra, the dimension of a vector space is just the cardinality of a minimal generating set. To define an analogue notion for modules is rather subtle. Of course, for free modules we could use just the rank. However, we saw that submodules of free modules need not be free again. On the other hand, geometric intuition makes desirable a notion of dimension for which the implication $N \subset M \Rightarrow$ "dimension" of N is smaller than "dimension" of M. The notion of *length* provides a substitute. As one might suspect, the theory is particularly pleasant for Noetherian rings and modules. Further, dimension is also one of the most basic geometric notions and we will briefly explore the link between geometric dimension and algebraic length.

41. Definition (Composition series and their length). Consider a *strict chain* of submodules $M = M_0 \supset M_1 \supset \ldots \supset M_n = 0$ where the inclusions are *strict*. The number n is called the **length** of the chain. A **composition series** of M is a *maximal strict chain*, that is, no extra submodules can be inserted. Equivalently, each quotient M_i/M_{i+1} is *simple*, i.e. it has no subquotient except 0 and itself.

42. Proposition and Definition (Length of a module). *Suppose that M has a composition series of length n. Then every composition series of M has length n, and every strict chain can be extended to a composition series. The common length will be denoted by $l(M)$ and called the* **length of** *M. We put $l(M) = \infty$ if M has no composition series.*

Proof. For the moment, let $l(M)$ be the least length of a composition series of M.

Step 1. *We first show $N \subset M \Rightarrow l(N) \leqslant l(M)$ with equality $\Leftrightarrow N = M$.* Let M_i be a composition series of length $l(M)$. By definition, this exists. Consider then the strict series $N_i = N \cap M_i$ of N. Since N_{i-1}/N_i injects into the simple module M_{i-1}/M_i we have either $N_{i-1}/N_i = M_{i-1}/M_i$ or $N_{i-1}/N_i = 0$, that is $N_{i-1} = N_i$. By removing the repeated terms we thus obtain a composition series of N; obviously, $l(N) \leqslant l(M)$. Equality can only occur if $N_{i-1}/N_i = M_{i-1}/M_i$ for all i which implies $N_{n-1} = M_{i-1}$ and by induction $N_i = M_i$, whence $N = M$.

Step 2. *Any strict chain M_i, $i = 0, \ldots, k$ of M has length $\leqslant l(M)$.* Indeed, we have $l(M) = l(M_0) > l(M_1) > \ldots > l(M_k) = 0$, whence $l(M_0) \geqslant k$.

Step 3. If M_i, $i = 0, \ldots, k$ is a composition series of M, then $k \geqslant l(M)$ by the provisional definition of $l(M)$, and $k \leqslant l(M)$ by the second step. Hence any composition series must have length $n = l(M)$. It follows that if M_i is a strict chain which is not a composition series then we can insert further modules until the length is n in which case it is a composition series.

□

Note that it is a nontrivial fact for a module to have a composition series. In fact, we have the

43. Proposition (Existence of composition series). *A module M has a composition series $\Leftrightarrow$ M is satisfies both the a.c.c. and d.c.c..*

Proof. $\Rightarrow$) All chains are of bounded length by the previous proposition, hence both the a.c.c. and the d.c.c. hold.

$\Leftarrow$) Construct a composition series of M as follows. Since M satisfies the a.c.c. the set of strictly contained submodules has a maximal element M_1 by Proposition 3.**??**. M_1 satisfies again the a.c.c. so that we can continue with this proces. We eventually get a sequence $M = M_0 \supset M_1 \supset \ldots$ which stops after a finite number of submodules by the d.c.c. □

44. Definition (modules of finite length). A module M which satisfies both the a.c.c. and the d.c.c. is called a module of **finite length**. The common length of any composition series is denoted $l(M)$ and called the **length of** M.

45. Remark.

(i) It follows from the first step in Proposition 3.42 that if N is a submodule of a finite module M, then N is itself finite and $l(N) \leqslant l(M)$.

(ii) Call two composition series M_i and N_i **equivalent** if they have the same length and if up to a permutation $M_{i-1}/M_i \cong N_{i-1}/N_i$. Then one can prove a *Jordan-Hölder type theorem* for modules: Any two composition are equivalent. In the case of $\mathbb{Z}$-modules (i.e. Abelian groups) this is just the classical Jordan-Hölder theorem.

The first remark is reminiscent of the dimension of a vector space. A further common property is this. Recall first that a function λ defined on the class of modules is called **additive**, if for every s.e.s. $0 \to L \to M \to N \to 0$, the identity $\lambda(M) = \lambda(L) + \lambda(N)$ holds.

46. Proposition ($l(M)$ is additive). *On the class of all A-modules of finite length, $l(M)$ is an additive function.*

Proof. Let $0 \to L \xrightarrow{\alpha} M \xrightarrow{\beta} N \to 0$ be an exact sequence. For a composition series in M' take its image in M under α. In particular, the resulting composition series in M is in the kernel of β. For a composition series in N take the inverse image under β, and this fits together to a composition series in M, whence the assertion. □

Finally, we see that the length coincides with the dimension if M is in fact a finite vector space. More precisely, we have

47. Proposition. *For a k-vector space, the following conditions are equivalent:*

(i) *finite dimension;*
(ii) *finite length;*
(iii) *a.c.c.;*
(iv) *d.c.c.*

Moreover, if any of these conditions is satisfied, then length = dimension.

Proof. The implications (i) $\Rightarrow$ (ii) is easy, (ii) $\Rightarrow$ (iii) and (ii) $\Rightarrow$ (iv) follow directly from Proposition 3.43. It remains to show (iii) $\Rightarrow$ (i) and (iv) $\Rightarrow$ (i). Suppose (i) is false so that there exists an infinite sequence (x_n) of linearly independent elements in the vector space V. Let U_n resp. V_n be the vector space spanned by $x_1, \ldots, x_n$ resp. by $x_{n+1}, x_{n+2}, \ldots$. Then the chain U_n resp. V_n are infinite ascending resp. descending. □

Hilbert functions. Let $S = \bigoplus S_d$ be a Noetherian graded ring. By Exercise 1.42, S_0 is Noetherian, and S is a finitely generated S_0-algebra with generators $x_1, \dots, x_n$ which we take to be homogeneous of degrees $d_i > 0$. More generally, we can consider a finitely generated graded S-module with generators $y_1, \dots, y_m$ of degrees e_j. Every element in $y \in M_e$ can be written as $y = \sum a_j y_j$ with $a_j \in S_{e-e_j}$. Since S_d is a finite S_0-module, it follows that M_d is a finite S_0-module.

Let λ be an additive $\mathbb{Z}$-valued function on the class of finitely generated S_0-modules. The **Poincaré series** of a graded S-module M is the power series

$$P(M,t) = \sum \lambda(M_e) t^e \in \mathbb{Z}[\![t]\!].$$

48. Theorem (Hilbert-Serre). *$P(M,t)$ is a rational function in t of the form $f(t)/\prod_{i=1}^{n}(1-t^{d_i})$ where $f(t) \in \mathbb{Z}[t]$.*

Proof. By induction on n the number of generators of S over S_0. If $n = 0$ then $S_d = 0$ for $d > 0$, that is $S_0 = S$. Hence M is a finite S_0-module which means that $M_e = 0$ for e large enough. Hence $P(M,t) \in \mathbb{Z}[t]$. For $n > 0$ consider x_n as a module morphism $S_e \to S_{e+n}$. Consider the exact sequence

$$0 \to K_e \to M_e \xrightarrow{x_n} M_{e+n} \to L_{e+n} = \operatorname{coker} x_n \to 0. \tag{5}$$

Let $K = \bigoplus K_i$ and $L = \bigoplus L_i$. As a quotient module of a finitely S-generated module, L is finitely generated (cf. Example 0.53); as a submodule of a finitely generated module over a Noetherian ring, K is finite over S, cf. Proposition 0.91. Further, both are annihilated by the induced action of x_n. Hence K and L are (finite) $S_0[x_1, \dots, x_{n-1}]$-modules. Applying the additive function to the exact sequence, we get $\lambda(K_e) - \lambda(M_e) + \lambda(M_{n+e}) - \lambda(L_{n+e}) = 0$. Multiplying with t^{e+n} and summing with respect to e yields

$$(1-t^n)P(M,t) = P(L,t) - t^n P(L,t) + g(t) \tag{6}$$

where $g(t) \in \mathbb{Z}[t]$ (the polynomial g comes from the index shift $+n$). By the induction hypothesis the result follows. □

Next we define the number

$$d(M) := \text{order of the pole of } P(M,t) \text{ at } 1.$$

Then we have the

49. Corollary. *If in the notation of the previous theorem, each $k_i = 1$, then for all sufficiently lagre n, $\lambda(M_n)$ is a polynomial in n with rational coefficents and of degree $d-1$ (with the convention that the degree of the zero polynomial is -1).*

Proof. □

50. Remark.

(i) Note that a polynomial $f(x)$ such that $f(n)$ is an integer for all n sufficiently high does not imply that f has itself integer coefficents; consider, for instance, $x(x+1)/2$.

(ii) The polynomial in the proof of the previous corollary is usually called the **Hilbert function** or **polynomial** of M with respect to λ.

In the exact sequence 3.5 replace x_s by any element $x \in A_k$ which is not a zerodivisor in M, i.e. $xm = 0$ implies $m = 0$. Then $K = 0$ and Equation 3.6 shows that $d(L) = d(M) - 1$, whence the

51. Proposition. *If $x \in A_k$ is not a zerodivisor in M, then $d(M/xM) = d(M)-1$.*

We shall mostly use Theorem 3.48 when $\lambda(M)$ is the length $l(M)$ of a finitely-generated A-module.

52. Example. Let $M = k[x_1, \ldots, x_n]$ be the polynomial ring in n variables over the field k. Then $M_d =$ the $M_0 = k$-module (in fact, vector space) of homogeneous polynomials has dimension $\binom{n+d-1}{d-1}$, hence $P(M,t) = (1-t)^{-d}$.

Next we consider the Hilbert functions obtained from a local ring by passing to its associated graded ring as in the previous section on completions. This will be also important when dealing with projective varieties later on.

53. Proposition. *Let $(A, \mathfrak{m})$ be a Noetherian local ring, and $\mathfrak{q}$ an $\mathfrak{m}$-primary ideal, i.e. $\sqrt{\mathfrak{q}} = \mathfrak{m}$. Further, let M be a finitely generated A-module, and (M_n) a stable $\mathfrak{q}$-filtration. Then*

(i) *M/M_n is of finite length, for each $n \geqslant 0$;*
(ii) *for all sufficiently large n this length is a polynomial $g(n)$ of degree $\leqslant s$ in n, where s is the least number of generators of $\mathfrak{q}$;*
(iii) *the degree and leading coefficient of $g(n)$ depend only on M and $\mathfrak{q}$, not on the filtration chosen.*

The polynomial $g(n)$ corresponding to the filtration $(\mathfrak{q}^n M)$ is denoted by $\chi_{\mathfrak{q}}^M(n)$, i.e.

$$\chi_{\mathfrak{q}}^M(n) = l(M/\mathfrak{q}^n M) \qquad \text{for all large } n.$$

If $M = A$ we simply write $\chi_{\mathfrak{q}}$ and call it the **characteristic polynomial** of the $\mathfrak{m}$-primary ideal $\mathfrak{q}$.

54. Corollary. *For all large n, the length $l(A/\mathfrak{q}^n)$ is a polynomial $\chi_{\mathfrak{q}}(n)$ of degree $\leqslant s$, where s is the least number of generators of $\mathfrak{q}$.*

55. Proposition. *If A, $\mathfrak{m}$ and $\mathfrak{q}$ are as above, then*

$$\deg \chi_{\mathfrak{q}}(n) = \deg \chi_{\mathfrak{m}}(n).$$

In particular, the common degree equals $d(A) = d(G_{\mathfrak{m}}(A))$ as defined above.

Dimension theory of Noetherian local rings. 56. Definition (Dimension). The **(Krull) dimension** $\dim A$ of A is the supremum of lengths of strict chains of prime ideals $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \ldots \supsetneq \mathfrak{p}_n$.

57. Examples.

(i) A field has dimension 0, $\mathfrak{p} = (0)$ being the only prime ideal.
(ii) By Remark 0.87, A is Artinian $\Leftrightarrow$ A is Noetherian and $\dim A = 0$. Geometrically this corresponds to the fact that A is the coordinate ring of a finite union of points – a zero-dimensional variety.

(iii) $\mathbb{Z}$ has dimension 1, any chain being of the form $(0) \subsetneq (p)$. More generally, this is true for any principal ideal domain which is not a field, for any prime ideal is maximal. In particular, $k[x]$ has dimension 1 in accordance with the geometric dimension of $\mathbb{A}^1$. More generally, we will see below REF that $\dim k[x_1, \ldots, x_n] = n$

58. Remark. Note that in general, strict chains of prime ideals do not have the same length. Geometrically, this can be roughly interpreted in terms of different dimensional components of an algebraic set. For instance, consider $X = \mathcal{Z}(x_1x_3, x_2x_3)$ in $\mathbb{A}^3$, the union of the x_1x_2-plane (of dimension 2) and the x_3-axis (of dimension 1). Then we have the maximal chains $(x_1, x_2, x_3 - 1) \supset\neq (x_1, x_2)$ coming from the inclusions of $(0, 0, 1) \subset x_3$-axis, and $(x_1, x_2, x_3) \supset\neq (x_2, x_3) \supsetneq (x_3)$ corresponding to the inclusions of $(0, 0, 0) \subset x_1$-axis $\subset x_1$, x_2-plane.

From now on, let $(A, \mathfrak{m})$ be a local Noetherian ring. Let $\delta(A)$ be the least number of generators of an $\mathfrak{m}$-primary ideal. Our goal is to prove

$$\delta(A) = d(A) = \dim A.$$

We will establish this by showing $\delta(A) \geqslant d(A) \geqslant \dim(A) \geqslant \delta(A)$. The first inequality is a direct consequence of Corollary 3.54 and Proposition 3.55:

59. Proposition. *$\delta(A) \geqslant d(A)$.*

60. Proposition. *Let A, $\mathfrak{m}$ and $\mathfrak{q}$ as before. Let M be a finitely generated A-module, $x \in A$ a non zerodivisor in M and $M' = M/xM$. Then*

$$\deg \chi_{\mathfrak{q}}^{M'} \leqslant \deg \chi_{\mathfrak{q}}^{M} - 1.$$

61. Corollary. *If $(A, \mathfrak{m})$ is a Noetherian local ring, x a nonzero divisor in A, then $d(A/(x)) \leqslant d(A) - 1$.*

We are now in a position to prove the crucial inequality:

62. Proposition. *$d(A) \geqslant \dim A$.*

63. Corollary. *If A is a Noetherian local ring, $\dim A$ is finite.*

64. Definition (height of a prime ideal). The **codimension** or **height** of a prime ideal $\mathfrak{p}$ in A is the supremum of lengths of strict chains of prime ideals $\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \ldots \subset \mathfrak{p}_r = \mathfrak{p}$ which end at $\mathfrak{p}$.

65. Example. By Exercise 1.106, $\operatorname{height} \mathfrak{p} = \dim A_{\mathfrak{p}}$. Geometrically, this corresponds to the *codimension* of the affine variety $\mathcal{Z}(\mathfrak{p}) \subset \operatorname{Spec} A$.

66. Corollary. *In a Noetherian ring every prime ideal has a finite height, and therefore the set of prime ideals in a Noetherian ring satisfies the descending chain condition.*

3.3. **Smoothness.** The notion of smoothness which is modelled on the corresponding notion of differentiable manifolds.

67. Definition (nonsingular affine varieties). Let $X \subset \mathbb{A}^n$ be an affine variety, and let $\mathcal{I}(X) = \langle f_1, \dots, f_r \rangle$. We say that X is **smooth** or **nonsingular at** $a \in X$ if the rank of the matric $(\partial_i f_j(a))$ is $n - r$

68. Definition (local regular ring).

69. Theorem (algebraic characterisation of nonsingularity).

70. Definition (nonsingular varieties).

4. First applications to geometry

4.1. **Smooth curves.**

4.2. **Intersection theory.**

5. Schemes

6. Cohomology

7. Curves

Appendix A. Rudiments of category theory

We discuss the basic notions of category theory. For a further development see for instance [GeMa].

1. Definition (category). A **category** $\mathcal{C}$ consists of the following data:

(i) A class of **objects** $\operatorname{Ob}\mathcal{C}$;
(ii) for any two objects A, $B \in \operatorname{Ob}\mathcal{C}$ a *set* $\operatorname{Mor}_{\mathcal{C}}(A, B)$ of *morphisms*. We denote an element of $\operatorname{Mor}_{\mathcal{C}}(A, B)$ usually by $A \to B$.

Furthermore, for any three objects A, B and $C \in \mathcal{C}$ there exists a map

$$\circ : \operatorname{Mor}_{\mathcal{C}}(A, B) \times \operatorname{Mor}_{\mathcal{C}}(B, C) \to \operatorname{Mor}_{\mathcal{C}}(A, C), \quad (f, g) \mapsto g \circ f$$

such that $\operatorname{Mor}_{\mathcal{C}}(A, B)$ is a monoid, i.e.

(i) $\circ$ is *associative*, i.e. $(g \circ f) \circ h = g \circ (f \circ h)$;
(ii) for all $A \in \operatorname{Ob}\mathcal{C}$ there exists a morphism $\operatorname{Id}_A \in \operatorname{Mor}_{\mathcal{C}}(A, A)$, the so-called **identity** of A such that for all $B \in \operatorname{Ob}\mathcal{C}$ and for all $f \in \operatorname{Mor}_{\mathcal{C}}(A; B)$ and $g \in \operatorname{Mor}_{\mathcal{C}}(B, A)$ we have

$$f \circ \operatorname{Id}_A = f \quad \text{and} \quad \operatorname{Id}_A \circ g = g.$$

To simplify the notation we often write Mor instead of $\operatorname{Mor}_{\mathcal{C}}$. A category $\mathcal{C}$ is **small** if $\operatorname{Ob}\mathcal{C}$ is a set.

2. Definition (isomorphism). Let $\mathcal{C}$ be a category. A morphism $f \in \operatorname{Mor}_{\mathcal{C}}(A, B)$ is called a **(categorical) isomorphism** if there exists $g \in \operatorname{Mor}_{\mathcal{C}}(B, A)$ such that $g \circ f = \operatorname{Id}_A$ and $f \circ g = \operatorname{Id}_B$, that is, f has a two sided inverse. In this case we also write $g = f^{-1}$. If $\mathcal{C}$ is small, then being isomorphic defines an equivalence relation on $\operatorname{Ob}\mathcal{C}$ and we denote by $\operatorname{Iso}(\mathcal{C})$ the set of equivalence classes.

3. Examples. (see also [GeMa, Section II.§1.5] for examples.)

(i) The basic example is the category **SET** of sets with maps as morphisms. Note that there is no set of sets (cf. Russell's paradoxon) which is why the objects form a class, not a set. On the other hand, $\mathrm{Mor}_{\mathbf{SET}}(A,B) \subset A \times B$ is of course a set. Isomorphisms are just bijective maps. Further examples in this vein are given by algebraic categories such as the category of abelian groups **ABG** or A-modules $\mathbf{MOD}_A$ with the corresponding notion of (iso)morphisms (group morphisms, A-linear (bijective) maps, etc.) or geometric categories (e.g. category of varieties with (bi)regular maps as (iso)morphisms). This also explains the general notation $A \to B$ for morphisms.

(ii) More exotic examples include the catgeory $\mathcal{C}(I)$ of a partially ordered set I, where $\mathrm{Ob}\,\mathcal{C}(I) = I$, and $\mathrm{Mor}_{\mathcal{C}(I)}(i,j)$ consists of one element if $i \leqslant j$ and is empty otherwise. In particular, $\mathrm{Mor}_{\mathcal{C}(I)}(i,i) = \{\mathrm{Id}_i\}$ and an element $f \in \mathrm{Mor}_{\mathcal{C}}(i,j)$ is an isomorphism if and only if $i = j$ and $f = \mathrm{Id}_i$. If X is a topological space we can consider the category $\mathbf{TOP}_X$. Here, the objects are the open subsets of X (a subset of the power set of X), and $\mathrm{Mor}(U,V)$ is the inclusion if $U \subset V$ and the empty set otherwise. Again, $\mathrm{Mor}(U,U) = \mathrm{Id}_U$ and $f \in \mathrm{Mor}(U,V)$ is an isomorphism if and only if $U = V$ and $f = \mathrm{Id}_U$. Finally, we can consider the category $\mathbf{SHEAF}_X$ whose objetcs are sheaves on X, and $\mathrm{Mor}(\mathcal{F},\mathcal{G})$ are sheaf morphisms. Here, the notion of isomorphism is the catgeorical one, i.e. $\varphi : \mathcal{F} \to \mathcal{G}$ is an isomorphism of sheaves if and only if it has a two sided inverse (cf. Definition 1.77). The definition of injective and surjective sheaf morphism was designed in such a way that an isomorphism is precisely a morphism which is injective and surjective, cf. Exercise 1.85.

We can also consider "maps" between categories.

4. Definition (functor). For two categories $\mathcal{C}$ and $\mathcal{D}$ we call $F : \mathcal{C} \to \mathcal{D}$ a **functor** an assignement which associates with any object A in $\mathcal{C}$ an object $F(A)$ in $\mathcal{D}$, and for any two objects A and B a map $\mathrm{Mor}_{\mathcal{C}}(A,B) \to \mathrm{Mor}_{\mathcal{D}}(F(A),F(B))$ (F is **covariant**) or $\mathrm{Mor}_{\mathcal{C}}(A,B) \to \mathrm{Mor}_{\mathcal{D}}(F(B),F(A))$ (F is **contravariant**) taking f to $F(f)$, and having the following properties:

(i) $F(\mathrm{Id}_A) = \mathrm{Id}_{F(A)}$;

(ii) $F(f \circ g) = F(f) \circ F(g)$ (F covariant) or $F(f \circ g) = F(g) \circ F(f)$ (F contravariant);

(iii) A presheaf onb X can be regarded as a contravariant functor $\mathbf{Top}_X \to \mathbf{AbG}$.

5. Examples.

(i) The basic example of a covariant functor is the so-called **forgetful functor** from a category $\mathcal{C}$ to **Set** which associates with say an A-module its underlying set,and with an A-linear map its underlying set theoretic map.

(ii) The assignement which takes an A-module M to its dual module $M^\vee$, and an A-linear map $f : M \to N$ to the dual map $f^\vee : N^\vee \to M^\vee$ defined by $f(\lambda)(m) = \lambda(f(m))$ for all $m \in M$ is a contravariant functor.

(iii)

A useful notion of "isomorphic" catgeories is this.

6. Definition (equivalence of categories). Two small categories $\mathcal{C}$ and $\mathcal{D}$ are **(covariantly) equivalent** if there exists a covariant functor $F : \mathcal{C} \to \mathcal{D}$ such that F

(i) induces a surjective map on isomorphism classes $\mathrm{Iso}(\mathcal{C}) \to \mathrm{Iso}(\mathcal{D})$. Put differently, for any object y in $\mathcal{D}$ there exists an object x in $\mathcal{C}$ with $F(x)$ is isomorphic with y.
(ii) *full and faithful*, that is, for any two objects x_1, x_2 in $\mathcal{C}$ the induced map $F(x_1, x_2) : \mathrm{Mor}(x_1, x_2) \to \mathrm{Mor}(F(x_1), F(x_2))$ is surjective and injective.

An analogous definition applies for **contravariant equivalent** categories.

7. Example. The category of affine varieties over k is equivalent with the category of finitely generated k-algebras without zero divisors (cf. Corollary 1.136).

Appendix B. Recap on field extensions

A **field extension** is an embedding $k \hookrightarrow K$ of the ground field k into some bigger field K (note in passing that any nontrivial k-linear map between fields is ncessarily injective). In particular, we may view K as a k vector space; it is customary to write K/k for the field extension and $[K : k]$ for $\dim_k K$, the **degree** of the field extension, but we will not do that. There are several types of field extensions which are important for us. A good reference is [Bo].

1. Definition (finite and algebraic field extensions). A field extension $k \subset K$ is **finite** if the dimension $\dim_k K < +\infty$. Moreover, $k \subset K$ is *algebraic* if for any $\alpha \in K$ there exists $f \in k[x]$ such that $f(\alpha) = 0$.

2. Proposition. *A finite field extension is algebraic.*

Proof. Indeed, if $\alpha \in K$, then there must be an n so that $\{1, \alpha, \alpha^2, \ldots, \alpha^n\}$ becomes linearly dependent over k, that is $\alpha^n = \sum_{i=0}^{n-1} a_i \alpha^i$. We let $k[\alpha]$ denote the subring of K generated by k and α, that is, $k[\alpha] = \{\sum_{i=0}^{n-1} a_i x^i \mid a_i \in k\}$. Since this is an integral domain and $k[x]$ Euclidean, so in particular a PID, the kernel of $k[x] \to k[\alpha]$, $X \mapsto \alpha$, must be a principal ideal, so $\ker = (f)$ for an irreducible element f. In particular, (f) is maximal so that $k[\alpha] = k(\alpha) := \mathrm{Quot}\, k[\alpha]$ is actually a field. Moreover, $\dim_k k(\alpha) = \deg f$. Indeed, $k[x]$ is Euclidean so that $g = qf + r$ with uniquely determined polynomials $\deg r < \deg f$. It follows that equivalence classes $1, \bar{x}, \bar{x}^2, \ldots, \bar{x}^{n-1}$ form a k-basis of $k[x]/(f) \cong k(\alpha)$. □

3. Remark. If in the proof of the previous proposition we normalise the polynomial f so that it is *monic*, i.e. $f = x^n + a_{n-1}x^{n-1} + \ldots + a_0$, then f is called the **minimal polynomial** of α and is uniquely determined. In general, if $f \in k[x]$ is irreducible, then $k \subset k[x]/(f)$ is a finite extension in which f has a root.

4. Examples.
(i) Let $k = \mathbb{R}$ and $f = x^2 + 1$, then $\mathbb{C} = \mathbb{R}[x]/(x^2 + 1)$.
(ii) $\bar{\mathbb{Q}} = \{\alpha \in \mathbb{C} \mid \alpha \text{ algebraic over } \mathbb{C}\}$ be the *algebraic closure of* $\mathbb{Q}$. Then $\mathbb{Q}(\sqrt[n]{3}) \subset \bar{\mathbb{Q}}$ has minimal polynomial $X^n - 3$ since it is irreducible by Eisenstein's criterion. It follows that $\dim_{\mathbb{Q}} \mathbb{Q}(\sqrt[n]{3}) = n$. In particular, $\dim_{\mathbb{Q}} \bar{\mathbb{Q}} = \infty$ which shows that algebraic extensions need not be finite in general.

As the first example shows, a field k need not be algebraically closed, i.e. there are polynomials $f \in k[x]$ which do not admit a root in k. However, we have the following

5. Theorem (existence of the algebraic closure). *For any field k there exists an algebraic field extension $k \subset K$ such that K is algebraically closed field.*

Proof. See [Bo, Theorem 3.4.4]. □

Item (ii) in the previous example can be generalised as follows:

6. Definition. If k is a field and K an algebraically closed field so that $k \subset K$ is algebraic, we call

$$\bar{k} = \{\alpha \in K \mid \alpha \text{ is algebraic over } k\}$$

the **algebraic closure of** k. The field $\bar{k}$ is determined up to isomorphism which restricts to the identity on k (cf. [Bo, Corollaries 3.4.7 and 10]).

7. Definition (Galois extensions). A field extension $k \subset K$ is **normal** if any irreducible polynomial $f \in k[x]$ which has a root in K splits into linear factors in $K[x]$. Further, $k \subset K$ is called **separable** if it is algebraic and every $a \in K$ is the root of a separable polynomial in $k[x]$, i.e. a polynomial whose roots are simple. A field extension is **Galois** if it is normal and separable. In this case, the group of automorphisms of K which leave k fixed is called the **Galois group**of the field extension $k \subset K$.

In characterstic 0 every algebraic field extension is separable [Bo, Remark 3.6.4]. We will not make much use of Galois extensions; its main importance for us stems from Remark 0.8. For a field extension $k \subset K$ with K algebraically complete and Galois, the Galois group allows in principle to identify those points in K^n which correspond to maximal ideals in $k[x_1, \ldots, x_n]$, see Remark 0.8.

8. Definition. A field k is called **perfect** if any algebraic field extension of k is separable.

Since any irreducible polynomial over a field of characteristic 0 is separable [Bo, Proposition 3.6.2], any such field is perfect. Further examples are finite fields or algebraically closed fields are also perfect. One of the main features of finite separable extensions is the

9. Theorem of the Primitive element. *If $k \subset K$ is a finite separable field extension, then there exists a so-called* **primitive element** *$\alpha \in K$ such that $K = k(\alpha)$.*

Proof. See [Bo, Proposition 3.6.12] □

Next we consider non-algebraic field extensions.

10. Definition (transcendence base). Consider a field extension $k \subset K$. Elements $\alpha_1, \ldots \alpha_n \in K$ are **algebraically independent** if the natural surjection

$$k[x_1, \ldots, x_n] \to k[\alpha_1, \ldots, \alpha_n] \subset K \to 0$$

sending x_i to α_i is actually an isomorphism of k-algebras, that is, we have an injection $k[x_1, \ldots, x_n] \hookrightarrow K$ sending x_i to α_i. Put differently, if there is a polynomial relation of the form $f(\alpha_1, \ldots, \alpha_n) = 0$ for $f \in k[x_1, \ldots, x_n]$, then $f = 0$. A family $\mathfrak{B} = \{\alpha_i\}_{i \in I}$ is algebraically independent if the previous definition applies for any finite subset of $\mathfrak{B}$. If in this case the field extension $k(\mathfrak{B}) \subset K$ is algebraic, then

A is called a **transcendence base**. If $K = k(\mathfrak{B})$ for some transcendence base, we call the field extension $k \subset K$ purely transcendental.

Any field extension $k \subset K$ can be factorised into a purely transcendental field extension $k \subset k(\mathfrak{B}) \subset K$, where the latter field extension is algebraic:

11. Proposition and Definition (transcendence degree). *Any field extension $k \subset K$ admits a transcendence base. Any two transcendence bases have the same cardinality which we call the* **transcendence degree**.

Proof. See [Bo, Proposition 7.1.3 and Theorem 7.1.5]. □

12. Proposition (Zariski's lemma). *Let $k \subset K$ be a field extension, where K is a finitely generated k-algebra. Then $k \subset K$ is a finite field extension.*

Proof. Let $K = k[\alpha_1, \ldots, \alpha_n]$. If K is algebraic over k, we are done. So assume otherwise and relabel the α_i in such a way that $x_1, \ldots, x_r$ are algebraically independent over k, and x_i are algebraic over the field $L = k(\alpha_1, \ldots, \alpha_r)$. Hence K is a finite algebraic extension of L and therefore a finite L-module. From Proposition 2.8 (i) applied to $k \subset L \subset K$, we infer that $L = k[\beta_1, \ldots, \beta_s]$ is a finitely generated k-algebra (we can, of course, also directly appeal to Noether normalisation). But this can only happen if $L = k$. To see this rigourosly, we note that each $\beta_i \in L$ so that $\beta_i = f_i/g_i$ for polynomials f_i and g_i in $x_1, \ldots, x_r$. Now there are infinitely many irreducibles in the factoriel ring $k[x_1, \ldots, x_r]$ (there are infinitely many primes just by the same argument as for $\mathbb{Z}$). Hence there is an irreducible polynomials which is prime to any of the finitely many g_i (for instance, take $h = g_1 \cdot \ldots \cdot g_s + 1$ would do). Therefore, $h^{-1} \in L$ cannot be a polynomial in the y_i (clear the common denominator and multiply by h). Contradiction. □

Do not confuse the notion of a finitely generated k-algebra K with a finitely generated field extension $k \subset K$. If K is a finitely generated k-algebra, then there exist $\alpha_i \in K$ such that $K = k[\alpha_1, \ldots, \alpha_n]$. The previous proposition then says that no subset of these generators is algebraically independent. If $k \subset K$ is a finitely generated field extension, then $K = k(\alpha_1, \ldots, \alpha_r)$ where we can label the α_i in such a way that $\alpha_1, \ldots, \alpha_n$ form a transcendence base so that $k(\alpha_1, \ldots, \alpha_n) \subset K$ is an algebraic, in fact finite extension of the *purely transcendental field extension* $k \subset k(\alpha_1, \ldots, \alpha_n)$.

13. Proposition and definition (separably generated field extensions). *A field extension $k \subset K$ is* **separably generated** *if there is a transcendence base $\mathfrak{B}$ such that $k(\mathfrak{B}) \subset K$ is a separable algebraic extension. In this case, $\mathfrak{B}$ is called a* **separating transcendence base**. *For a finitely and separably generated field extension $k \subset K = k(\alpha_1, \ldots, \alpha_r)$ the set of generators $\{\alpha_i\}$ contains a separating transcendence base.*

Proof. See [Bo, Proposition 7.3.7] □

14. Proposition (perfect fields and separably generated field extensions). *If k is a perfect field, any finitely generated field extension $k \subset K$ is separably generated.*

Proof. See [Bo, Corollary 3.7.8]. □

References

[AtMa] M. Atiyah and I. MacDonald, *Introduction to Commutative Algebra*, Addison-Wesley, .

[Bo] S. Bosch, *Algebra*, Springer, 2006.

[CLS] D. Cox, J. Little, and D. O'Shea, *Ideals, varieties, and algorithms*, Springer, 1996.

[Ei] D. Eisenbud, *Commutative Algebra*, Springer, 1995.

[Ga] A. Gathmann, *Commutative Algebra*, lecture notes available at mathematik.uni-kl.de/agag/mitglieder/professoren/gathmann/notes/.

[GeMa] S. Gelfand and Y. Manin, *Methods of homological algebra*, Springer, 2003.

[Ha] R. Hartshorne, *Algebraic Geometry*, Springer, 1977.

[Ma] H. Matsumura, *Commutative ring theory*, CUP 1986.

[Re] M. Reid, *Undergraduate Commutative Algebra*, LMS, 1995.