COMMUTATIVE ALGEBRA, LECTURE NOTES

P. SOSNA

Contents

1. Very brief introduction

These are notes for a lecture (14 weeks, 2×90 minutes per week) held at the University of Hamburg in the winter semester 2014/2015. The goal is to introduce and study some basic concepts from commutative algebra which are indispensable in, for instance, algebraic geometry. There are many references for the subject, some of them are in the bibliography. In Sections 2-8 I mostly closely follow [2], sometimes rearranging the order in which the results are presented, sometimes omitting results and sometimes giving statements which are missing in [2]. In Section 9 I mostly rely on [9], while most of the material in Section 10 closely follows [4]. Clearly, many topics, such as completions, are missing from these notes. Another obvious shortcoming is the lack of examples in the last two sections, which is due to lack of time.

Despite the lecturers' personal bias and the occasional subsection with "geometry" in the title, there is not much explicit algebraic geometry in these notes. For those interested in these connections, [8] is a fairly concise source, while [4] is a more elaborate treatise. Should other suitable references for these connections, and for commutative algebra in general, be missing in the bibliography, my ignorance is to blame.

2. Rings and Ideals

Definition. A *ring* is a set A with two binary operations, the addition "$+$" and multiplication "$\cdot$", such that

1) The set A is an abelian group with respect to addition. This means that the addition is associative, commutative, that there is a neutral element denoted by 0 and every element x has an inverse, denoted by $-x$;
2) The multiplication is associative and distributive over the addition.

A ring is called *commutative* if $xy = yx$ for all $x, y \in A$. A ring is said to have an identity element if there exists an element $1 \in A$ such that $1x = x1 = x$ for all $x \in A$.

Convention. In the following "ring" will mean a commutative ring with an identity element.

Example 2.1. We do not exclude the possibility that $1 = 0$ in a ring A. In this case, $x = x1 = x0 = 0$, so A has only one element 0. We call this A the *zero ring*.

Another example is given by the integers $\mathbb{Z}$ with the usual addition and multiplication.

If A is any ring, then the set

$$A[X] = \left\{ \sum_{i=0}^{n} a_i X^i \mid a_i \in A, n \in \mathbb{N} \right\}$$

consisting of all polynomials with coefficients in A is a ring with respect to the usual addition and multiplication of polynomials.

Definition. Let A and B be two rings. A *ring homomorphism* from A to B is a map $f \colon A \longrightarrow B$ such that

i) $f(x+y) = f(x) + f(y)$ for all $x, y \in A$,
ii) $f(xy) = f(x)f(y)$ for all $x, y \in A$,
iii) $f(1) = 1$.

A *subring* A' of a ring A is a subset of A admitting a ring structure such that the inclusion map $A' \longrightarrow A$ is a ring homomorphism. In other words, A' is a subset of A which is closed under addition and multiplication and contains the identity element of A.

Note that i) implies that f is a homomorphism of the abelian groups underlying the rings.

Example 2.2. The inclusion $\mathbb{Z} \longrightarrow \mathbb{Q}$ is a ring homomorphism.

The map $A[X] \longrightarrow A$ sending a polynomial p to $p(1)$ (or, more generally, $p \longmapsto p(a)$ for some $a \in A$) is a ring homomorphism.

The conjugation map of the complex numbers $\mathbb{C}$ is a ring homomorphism.

Definition. Let A be a ring. An *ideal* I of A is a subset which is an additive subgroup and has the property that $xi \in I$ for all $x \in A$ and $i \in I$. We also write $AI \subseteq I$.

If I is an ideal, then the quotient group A/I inherits a uniquely defined multiplication from A (given two cosets $x + I$ and $y + I$, set $(x + I)(y + I) = xy + I$) which makes it into a ring, called the *quotient ring*. The map $A \longrightarrow A/I$ which sends x to its coset $x + I$, is a surjective ring homomorphism.

Example 2.3. If $A = \mathbb{Z}$, then (n) (also written as $n\mathbb{Z}$), the set of all integers divisible by some fixed integer n, is an ideal. For instance, if we take $n = 2$, then the quotient ring $\mathbb{Z}/2\mathbb{Z}$ is a ring with two elements 0 and 1.

If $f\colon A \longrightarrow B$ is a ring homomorphism, then $\ker(f) = f^{-1}(0)$ is an ideal in A. As an example let $A = \mathbb{C}[X]$, $B = \mathbb{C}$ and $f\colon A \longrightarrow B$ the homomorphism sending p to $p(1)$. Then its kernel is the set of all polynomials which vanish in 1, or, to put it differently, have 1 as a root.

Note that $\mathrm{im}(f)$ is always a subring of B but usually not an ideal (take, for instance, $A = \mathbb{Z}$, $B = \mathbb{Q}$ and f to be the inclusion). Using the homomorphism theorem, we see that $A/\ker(f) \simeq \mathrm{im}(f)$.

We will now prove our first result, which is quite easy but very useful.

Proposition 2.4. *There is a one-to-one order preserving correspondence between ideals of A/I and ideals J of A containing I.*

Proof. Given an ideal J of A which contains I, the quotient J/I is easily seen to be an ideal of A/I. Conversely, if I' is an ideal in A/I, then its preimage under the projection map is an ideal containing I. It is clear that these two maps are inverse to each other. □

We can perform certain operations on ideals.

Definition. Let A be a ring. If I and J are ideals, then the ideal $I + J$ is the set of all $x + y$ with $x \in I$ and $y \in J$. Similarly one defines the sum of (possibly infinitely many) ideals as the set of all finite sums as above.

Given any family I_α of ideals, the intersection $\cap_\alpha I_\alpha$ is again an ideal.

The product IJ of two ideals is the ideal generated by all products xy with $x \in I$ and $y \in J$, that is, the set of all finite sums $\sum_k x_k y_k$ where each $x_k \in I$ and each $y_k \in J$. Similarly, we can define the product of any finite family of ideals.

Example 2.5. Let $A = \mathbb{Z}$, $I = (m)$ and $J = (n)$. Then $I \cap J$ is the ideal generated by the lowest common multiple of m and n; $I + J$ is the ideal generated by the highest common factor; and $IJ = (mn)$.

For a different example, we can consider $A = \mathbb{R}[X_1, \ldots, X_k]$ and $I = (X_1, \ldots, X_k)$. Then $I^m = I \cdots I$ is the set of all polynomials with no terms of degree $< m$.

Remark 2.6. It is clear that taking the sum, intersection and product of ideals are commutative and associative operations. There is also a distributive law for the sum and the product.

Definition. Let A be a ring. An element $x \neq 0$ in A is called a *zero divisor* if there exists an element $y \neq 0$ such that $xy = 0$. A ring without any zero divisors is called an *integral domain*, or simply *domain*.

An element $x \in A$ is called *nilpotent* if there exists an integer $n \in \mathbb{N}_{>0}$ such that $x^n = 0$. In a non-zero ring, any nilpotent element is a zero divisor but the converse does not hold in general.

A *unit* is an element $x \in A$ such $xy = 1$ for some $y \in A$. One writes x^{-1} for this so-called *inverse* y of x. Note that the set of all units is a multiplicative subgroup of A.

Given any element $x \in A$, the multiples of x form an ideal (x), called the *principal ideal generated by* x. We will frequently write 0 for the zero ideal (0).

Example 2.7. The integers $\mathbb{Z}$ are a domain and so is $\mathbb{Z}[X]$. The former being clear, let us consider the latter case. If $f = \sum_{k=0}^{n} \alpha_k X^k$ and $g \sum_{l=0}^{m} \beta_l X^l$ are in $\mathbb{Z}[X]$ such that $fg = 0$, then, in particular, $\alpha_{k_0}\beta_{l_0} = 0$, where k_0 and l_0 are the minimal indices such that $\alpha_{k_0} \neq 0$ and $\beta_{l_0} \neq 0$. Since $\mathbb{Z}$ is an integral domain, this leads to a contradiction.

For an example of zero-divisors, consider the ring $A = k[X, Y]/(XY)$ and the elements $\overline{X}$ and $\overline{Y}$. Note that A does not have any nilpotent elements, while in $B = k[X]/(X^2)$ the element $\overline{X}$ is nilpotent.

Remark 2.8. First of all, the inverse of an element is uniquely determined, since if $1 = xy = xy'$, then

$$y = y1 = y(xy') = (yx)y' = (xy)y' = y'.$$

A commutative ring with 1 is called a *field* if $1 \neq 0$ and for all $0 \neq x \in A$ there exists an element $x^{-1} \in A$ such that $xx^{-1} = x^{-1}x = 1$. In other words, every non-zero element of A is a unit. Clearly, every field is an integral domain, but not conversely (e.g. $\mathbb{Z}$).

Note that if x is a unit, then $(x) = A = (1)$.

Also note that if x is nilpotent, then $1 - x$ is a unit. Indeed, $x^n = 0$ for some integer, so $(1 - x)(1 + x + \ldots + x^{n-1}) = 1$. It follows easily from this that the sum of a unit and a nilpotent element is again a unit.

Proposition 2.9. *Let $A \neq 0$ be a ring. The following are equivalent:*

a) *A is a field,*
b) *the only ideals in A are 0 and (1);*
c) *every homomorphism $f\colon A \longrightarrow B$, where $B \neq 0$, is injective.*

Proof. a)⇒b) Let $0 \neq I \subseteq A$ be an ideal and let $0 \neq i \in I$ be any non-zero element. Since i is a unit, the ideal generated by i is A. But this ideal is contained in I, so $I = A$.

b)⇒c) Let f be a homomorphism to a non-zero ring. The kernel of f is an ideal of A. Since A has only two ideals and the map f sends 1 to 1, f cannot be constant, hence the kernel is 0.

c)⇒a) Let x be an element of A which is not a unit. Then $(x) \neq (1)$, so $B = A/(x)$ is not the zero ring. Therefore, the projection $f\colon A \longrightarrow A/(x)$ is injective. But the kernel of f is (x), so $(x) = 0$, hence $x = 0$. □

We will now turn our attention to special types of ideals.

Definition. An ideal $\mathfrak{p} \neq (1)$ in a ring A is *prime* if $xy \in \mathfrak{p}$ implies that either $x \in \mathfrak{p}$ or $y \in \mathfrak{p}$. An ideal $\mathfrak{m}$ is called *maximal* if $\mathfrak{m} \neq (1)$ and there is no ideal I such that there exists a strict inclusion of $\mathfrak{m}$ in I.

Equivalently, an ideal $\mathfrak{p}$ is prime if and only if $A/\mathfrak{p}$ is an integral domain and an ideal $\mathfrak{m}$ is maximal if and only if $A/\mathfrak{m}$ is a field. The second statement follows immediately from Propositions 2.4 and 2.9. For the first note that $A/\mathfrak{p}$ is an integral domain if and only if $x \notin \mathfrak{p}$ and $y \notin \mathfrak{p}$ implies that $xy \notin \mathfrak{p}$.

Remark 2.10. If $f\colon A \longrightarrow B$ is a ring homomorphism and $\mathfrak{p}$ is a prime ideal in B, then $f^{-1}(\mathfrak{p})$ is a prime ideal in A. Indeed, $A/f^{-1}(\mathfrak{p})$ is isomorphic to a subring of $B/\mathfrak{p}$ (the induced map $A/f^{-1}(\mathfrak{p}) \longrightarrow B/\mathfrak{p}$ is injective) and the latter is an integral domain, hence so is the former. The corresponding statement does not hold for maximal ideals, for instance, take $f\colon \mathbb{Z} \longrightarrow \mathbb{Q}$ and $\mathfrak{m} = 0$.

Our first major result below will use Zorn's lemma which states that if S is a non-empty partially ordered set, and any chain in S has an upper bound, then S has at least one maximal element. Here, a partial order $\leq$ is a relation on S which is reflexive and transitive and such that $x \leq y$ and $y \leq x$ imply that $x = y$. A subset T of S is a chain if either $x \leq y$ or $y \leq x$ for any two elements $x, y \in T$. An upper bound of a subset T is, of course, an element x such that $t \leq x$ for all $t \in T$.

Theorem 2.11. *Every ring $A \neq 0$ has at least one maximal ideal.*

Proof. Let Σ be the set of all ideals $\neq (1)$ in A. The inclusion relation makes Σ into a partially ordered set. Clearly, $0 \in \Sigma$, so Σ is non-empty. Now let T be a chain in Σ, that is, we are given a sequence of ideals I_α such that for any pair of indices α, β either $I_\alpha \subseteq I_\beta$ or vice versa. Let $I = \cup_\alpha I_\alpha$. Clearly, this is an ideal and $1 \notin I$, hence $I \in \Sigma$ and every chain in Σ has an upper bound. By Zorn's lemma, Σ has a maximal element, that is, there exists a maximal ideal in A. □

Corollary 2.12. *If $I \neq (1)$ is an ideal in A, then there exists a maximal ideal containing I.*

Proof. Apply the theorem to A/I, using Proposition 2.4. □

Corollary 2.13. *Every non-unit x of A is contained in a maximal ideal.*

Proof. The element x is contained in $(x) \neq (1)$. □

Example 2.14. Let $A = \mathbb{Z}$. Every ideal in $\mathbb{Z}$ is of the form (n) with $n \geq 0$. The ideal (n) is prime if and only if n is a prime number or $n = 0$. In fact, all the ideals with n prime are actually maximal. The corresponding quotient rings are the fields with n elements. Of course, every integer is divisible by some prime number.

If $A = k[X_1, \ldots, X_n]$ is the polynomial ring in n variables over a field k and f is an irreducible polynomial, then (f) is a prime ideal. But for $n > 1$, not every ideal in A is generated by one element. For example, the kernel of the map $A \twoheadrightarrow k$ sending a polynomial f to its value at 0 is a maximal ideal but requires at least n generators.

A *principal ideal domain* is an integral domain in which every ideal is principal. In such a ring every non-zero prime ideal is maximal. Indeed, if $(x) \neq 0$ is a prime ideal and $(y) \supset (x)$, then $x \in (y)$, so $x = yz$, so $yz \in x$. Since (x) is prime and $y \notin (x)$, $z \in (x)$, so $z = tx$. Then $x = yz = ytx$, hence $yt = 1$ and $(y) = (1)$.

Definition. A *local ring* is a ring with exactly one maximal ideal. A ring is called *semi-local* if it has only finitely many maximal ideals.

Note that any field is a local ring and its maximal ideal is 0.

Proposition 2.15. *Let A be a ring and $\mathfrak{m} \neq (1)$ be an ideal in A with the property that any element $x \in A \setminus \mathfrak{m}$ is a unit. Then A is a local ring and $\mathfrak{m}$ is its maximal ideal. Furthermore, if A is a ring and $\mathfrak{m}$ is a maximal ideal of A such that every element of the form $1 + m$ with $m \in \mathfrak{m}$ is a unit, then A is local.*

Proof. Let $I \neq (1)$ be an ideal. Since no unit is contained in I, $I \subseteq \mathfrak{m}$, hence the first claim holds. To prove the second claim, let $x \in A \setminus \mathfrak{m}$. The ideal generated by $\mathfrak{m}$ and x has to be (1), because $\mathfrak{m}$ is maximal. Therefore there exist $y \in A$ and $t \in \mathfrak{m}$ such that $xy + t = 1$, so $xy = 1 - t \in 1 + \mathfrak{m}$ is a unit by assumption and then the second claim follows from the first. □

Example 2.16. Let $A[[X]]$ be the ring of formal power series, that is, elements of $A[[X]]$ are infinite sums $\sum_{k=0}^{\infty} a_k X^k$ with $a_k \in A$ for all k. A power series $f = a_0 + a_1 X + \ldots$ is a unit in $A[[X]]$ if and only if a_0 is a unit in A. Indeed, if $f^{-1} = b_0 + b_1 X + \ldots$ exists, then $a_0 b_0 = 1$. Conversely, if a_0 is a unit, the equation

$$1 = (a_0 + a_1 X + \ldots)(b_0 + b_1 X + \ldots) = a_0 b_0 + (a_0 b_1 + a_1 b_0) X + \ldots$$

is solvable by setting $b_0 = a_0^{-1}$, then solving the equation $a_0 b_1 + a_1 b_0$ for b_1 and so on.

It follows that an element in $A[[X_1, \ldots, X_n]]$ is a unit if and only if a_0 is a unit in A. In particular, $k[[X_1, \ldots, X_n]]$ is a local ring with maximal ideal $(X_1, \ldots, X_n)$ if k is a field. This does not hold for the polynomial ring, even if $n = 1$.

Proposition 2.17. *Let A be a ring. The set of all nilpotent elements in A, denoted by* $\mathrm{rad}(0)$ *or* $\sqrt{0}$ *is an ideal, called the nilradical of A. The ring $B = A/\mathrm{rad}(0)$ has no nilpotent elements.*

Proof. Clearly, $0 \in \mathrm{rad}(0)$. If x and y are in $\mathrm{rad}(0)$, then $x^n = 0$ and $y^m = 0$ for some integers n, m. Then $(x+y)^{n+m+1} = 0$ by the binomial formula. Next, if $x \in \mathrm{rad}(0)$ and $a \in A$, then clearly $ax \in \mathrm{rad}(0)$ and so $\mathrm{rad}(0)$ is an ideal.

Now if $\overline{x} \in B$ is nilpotent, then $\overline{x}^n = 0$ in B, that is, for a representative x of the coset $\overline{x}$ we have $x^n \in \mathrm{rad}(0)$. But this just means that x is nilpotent, so $\overline{x} = 0$ in B. □

Proposition 2.18. *The nilradical* $\mathrm{rad}(0)$ *of A is equal to the intersection of all prime ideals of A.*

Proof. Let $x \in \mathrm{rad}(0)$, so $x^n = 0$ for some integer n. In particular, x^n is contained in every prime ideal, and so x is indeed contained in the intersection of all the prime ideals of A.

Conversely, let x be not nilpotent. Let Σ be the set of ideals I such that $n > 0 \Rightarrow x^n \notin I$. Then $\Sigma \neq \emptyset$ because $0 \in \Sigma$. Applying Zorn's lemma to Σ (which is a partially ordered set with respect to inclusion), we get a maximal element $\mathfrak{p}$. We will show that this is a prime ideal. To see this, let $a, b \notin \mathfrak{p}$. Then $(a) + \mathfrak{p} \supsetneq \mathfrak{p}$ and $(b) + \mathfrak{p} \supsetneq \mathfrak{p}$, so $(a) + \mathfrak{p} \notin \Sigma$ and $(b) + \mathfrak{p} \notin \Sigma$. Therefore, $x^n \in (a) + \mathfrak{p}$ and $x^m \in (b) + \mathfrak{p}$ for some $n, m > 0$. It follows that $x^{n+m} \in (ab) + \mathfrak{p}$, hence $(ab) + \mathfrak{p} \notin \Sigma$, so $ab \notin \mathfrak{p}$. Therefore, any element which is not nilpotent is not contained in some prime ideal. □

We can also consider the intersection of all the maximal ideals $\mathrm{Jac}(A)$, which is called the *Jacobson radical*.

Proposition 2.19. *Let A be a ring. An element x is in the Jacobson radical* $\mathrm{Jac}(A)$ *if and only if $1 - xy$ is a unit for all $y \in A$.*

Proof. "⇒" If $1 - xy$ is not a unit, it is contained in some maximal ideal $\mathfrak{m}$. Since $xy \in \mathfrak{m}$, it follows that $1 \in \mathfrak{m}$, a contradiction.

"⇐" Assume $x \notin \mathfrak{m}$ for some maximal ideal $\mathfrak{m}$. Then x and $\mathfrak{m}$ generate the unit ideal (1), so $u + xy = 1$ for some $u \in \mathfrak{m}$ and some $y \in A$. But then $1 - xy$ cannot be a unit. □

Now recall that we defined several operations on ideals, namely sum, intersection and product. Going back to the definition, it is clear that $IJ \subseteq I \cap J$ for any ideals I and J. A little more difficult to see (write down the conditions) is the modular law which states that if $I \supset J$ or $I \supset K$, then

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

Hence,

$$(I + J)(I \cap J) \subseteq (I \cap J)I + (I \cap J)J \subseteq IJ.$$

We conclude that if $I + J = (1)$, then $IJ = I \cap J$. We therefore say that two ideals I, J are *coprime* if $I + J = (1)$.

Definition. Let $A_1, \ldots, A_k$ be rings. Their *direct product* $A = \prod_{i=1}^k A_i$ is the set $A_1 \times \ldots \times A_k$ endowed with the componentwise addition and multiplication. The identity element of A is $(1, \ldots, 1)$. We will denote the canonical projections $A \longrightarrow A_i$ by p_i. These are ring homomorphisms.

Proposition 2.20. *Let A be a ring and let $I_1, \ldots, I_k$ be ideals of A. Let $\varphi\colon A \longrightarrow \prod_{i=1}^k A/I_i$ be the canonical map. Then*

i) *If I_i and I_j are coprime whenever $i \neq j$, then $\prod I_i = \cap I_i$.*
ii) *The map φ is surjective if and only if I_i and I_j are coprime whenever $i \neq j$.*
iii) *The map φ is injective if and only if $\cap_i I_i = (0)$.*

In particular, if I_i and I_j are coprime whenever $i \neq j$, then

$$\varphi\colon (A/\cap_i I_i) \simeq \prod_{i=1}^k A/I_i.$$

Proof. To prove i), we will use induction. The case $k = 2$ was done above. So assume $k > 2$ and set $J = \prod_{i=1}^{k-1} I_i = \cap_{i=1}^{k-1} I_i$. For $1 \leq i \leq k-1$ we have $I_i + I_k = (1)$, hence $1 = x_i + y_i$ for $x_i \in I_i$ and $y_i \in I_k$. Therefore

$$\prod_{i=1}^{k-1} x_i = \prod_{i=1}^{k-1} (1 - y_i)$$

and hence $I_k + J = (1)$. It follows that

$$\prod_{i=1}^{k} I_i = JI_k = J \cap I_k = \bigcap_{i=1}^{k} I_i.$$

Let us now prove ii). First assume that φ is surjective and note that it is sufficient to show that, for example, I_1 and I_2 are coprime. Let x be an element in A with $\varphi(x) = (1, 0, \ldots, 0)$. This means that $x \in I_2$ and $1 - x \in I_1$. Therefore $1 = (1-x) + x \in I_1 + I_2$.

Conversely, it is sufficient to show that $(1, 0 \ldots, 0)$ is in the image of φ. For every $i > 1$ we have an equation $u_i + v_i = 1$ with $u_i \in I_1$ and $v_i \in I_i$. Define $x = \prod_{i \geq 2} v_i$. Then $x = \prod_i (1 - u_i) = 1 + y$ with $y \in I_1$ and $x = 0$ in A/I_i for all $i > 1$. Therefore, $\varphi(x) = (1, 0, \ldots 0)$.

Lastly, iii) is clear, because $\cap I_i = \ker(\varphi)$. □

Proposition 2.21. *The following holds.*

i) *Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ be prime ideals and let I be an ideal contained in the union $\cup_{i=1}^k \mathfrak{p}_i$. Then there exists an index i_0 such that $I \subseteq \mathfrak{p}_{i_0}$.*
ii) *Let $I_1, \ldots, I_k$ be ideals and let $\mathfrak{p}$ be a prime ideal containing $\cap_{i=1}^k I_i$. Then $\mathfrak{p} \supset I_{i_0}$ for some i_0. If $\mathfrak{p} = \cap_{i=1}^k I_i$, then $\mathfrak{p} = I_{i_0}$ for some i_0.*

Proof. i) We use induction on k in the form

$$I \not\subseteq \mathfrak{p}_i \; \forall 1 \leq i \leq k \Rightarrow I \not\subseteq \bigcup_{i=1}^{k} \mathfrak{p}_i.$$

The case $k = 1$ is clear. If $k > 1$ and the result holds for $k-1$, then for each i there exists an element $x_i \in I$ such that $x_i \notin \mathfrak{p}_j$ for all $j \neq i$. If also $x_i \notin \mathfrak{p}_i$, then we are done. Otherwise, $x_i \in \mathfrak{p}_i$ for all i and we define

$$y = \sum_{i=1}^{k} x_1 x_2 \cdots x_{i-1} x_{i+1} \cdots x_k.$$

Then clearly $y \in I$ and $y \notin \mathfrak{p}_i$ for $1 \leq i \leq k$ (for example, consider $i = 1$ and note that all the summands in y except the first one are in $\mathfrak{p}_1$, so if y were in $\mathfrak{p}_1$ the first summand $x_2 \cdots x_k$ would also be in $\mathfrak{p}_1$, contradiction). So, $I \not\subseteq \cup_{i=1}^{k} \mathfrak{p}_i$.

ii) Suppose that $I_i \not\subseteq \mathfrak{p}$ for all i. Then there exist $x_i \in I_i$, $x_i \notin \mathfrak{p}$ and therefore $\prod x_i \in \prod I_i \subseteq \cap I_i$. Since $\mathfrak{p}$ is prime, $\prod x_i \notin \mathfrak{p}$. Hence $\cap I_i \not\subseteq \mathfrak{p}$.

Finally, if $\mathfrak{p} = \cap I_i$, then $\mathfrak{p} \subseteq I_i \; \forall i$ and hence $\mathfrak{p} = I_{i_0}$ for some i_0. □

Definition. Let I be an ideal. The *annihilator* of I, denoted by $\mathrm{Ann}(I)$ is the set of all elements $x \in A$ such that $xI = 0$. More generally, for ideals I, J we define their *ideal quotient* $(I : J)$ as

$$(I : J) = \{x \in A \mid xJ \subseteq I\}.$$

The *radical* of an ideal I is defined as

$$\mathrm{rad}(I) = \{x \in A \mid x^n \in I \text{ for some } n > 0\}.$$

In the same vein, we can define the radical $\mathrm{rad}(E)$ of any subset E of A, which will not be an ideal in general.

Proposition 2.22. *The radical of an ideal I is the intersection of all prime ideals containing I.*

Proof. Apply Proposition 2.18 to A/I. □

Proposition 2.23. *The set D of all zero divisors of A is equal to $\cup_{0 \neq x \in A} \mathrm{rad}(\mathrm{Ann}(x))$.*

Proof. First note that for any family of subsets E_α of A we have $\mathrm{rad}(\cup_\alpha E_\alpha) = \cup_\alpha \mathrm{rad}(E_\alpha)$ and that $D = \cup_{x \neq 0} \mathrm{Ann}(x)$. Using this, we compute

$$D = \mathrm{rad}(D) = \mathrm{rad}(\cup_{x \neq 0} \mathrm{Ann}(x)) = \cup_{x \neq 0} \mathrm{rad}(\mathrm{Ann}(x)).$$ □

We will now investigate the set of all prime ideals of a ring A a bit more thoroughly.

Definition. Let A be a ring. We define $X = \mathrm{Spec}(A)$, the *spectrum* of A, to be the set of all prime ideals in A. For a subset E of A, denote by $V(E)$ the set of all prime ideals containing E.

Proposition 2.24. *The following holds.*

i) *If I is the ideal generated by E, then $V(E) = V(I) = V(\mathrm{rad}(I))$.*
ii) *$V(0) = X$ and $V(1) = \emptyset$.*
iii) *If $(E_\alpha)_\alpha$ is any family of subsets of A, then $V(\cup_\alpha E_\alpha) = \cap_\alpha V(E_\alpha)$.*
iv) *If I and J are ideals in A, then $V(I \cap J) = V(I) \cup V(j)$.*

Proof. i) Clearly, $E \subseteq I$, so $V(E) \supset V(I)$. But since I is the smallest ideal containing E, any prime ideal which contains E also has to contain I. Hence, $V(E) = V(I)$.

Now, $V(I) \supset V(\mathrm{rad}(I))$. But if $I \subseteq \mathfrak{p}$ and $x \in \mathrm{rad}(I)$, that is $x^n \in I \subseteq \mathfrak{p}$, then also $x \in \mathfrak{p}$, so $V(I) \subseteq V(\mathrm{rad}(I))$.

ii) This is trivial.

iii) Let $\mathfrak{p}$ be an ideal containing $\cup_\alpha E_\alpha$. Then $\mathfrak{p}$ contains all the E_α and hence $\mathfrak{p}$ is contained in $\cap_\alpha V(E_\alpha)$. Conversely, a prime ideal containing all the E_α contains their union.

iv) If $\mathfrak{p}$ contains I or J, it also contains $I \cap J$. On the other hand, if $\mathfrak{p}$ contains $I \cap J$, it contains one of the ideals by Proposition 2.21.ii). □

Example 2.25. If A is a field, then $\mathrm{Spec}(A)$ is a point which corresponds to the unique maximal ideal (0).

If $A = \mathbb{Z}$, then $\mathrm{Spec}(\mathbb{Z})$ consists of a countable number of points, namely one for each prime number and the zero ideal. Note that the zero ideal is a point in $\mathrm{Spec}(\mathbb{Z})$ but while $V(n) = (n)$ for n prime, we have $V(0) = \mathrm{Spec}(\mathbb{Z})$.

If $A = \mathbb{C}[X]/(X^2)$, then $\mathrm{Spec}(A)$ is again just a point corresponding to the unique maximal ideal generated by the image of X under the quotient map. Hence, as a set the spectrum of A is the same as the spectrum of a field, but since the underlying rings are quite different, one might expect the spectra to reflect this difference. We might come back to this observation later.

3. Modules

Definition. Let A be a ring. An *A-module* is an abelian group M together with a *scalar multiplication* by A, that is, there is a map $\rho\colon A \times M \longrightarrow M, (a, m) \longmapsto \rho(a, m) =: am$ satisfying the following properties for $a, a' \in A$ and $m, m' \in M$: i) $a(m+m') = am+am'$, ii) $(a + a')m = am + a'm$, iii) $a(a'm) = (aa')m$ and iv) $1m = m$.

Example 3.1. If $A = k$ is a field, then an A-module is simply a k-vector space.

Any ideal in a ring A is a module over A. In particular, A itself is an A-module.

If $A = \mathbb{Z}$, then an A-module M is an abelian group and vice versa (if $x \in M$, then define $nx = x + \ldots + x$).

If $A = k[X]$, then an A-module is a k-vector space endowed with a linear transformation which corresponds to the scalar multiplication by X. In a similar vein, a module over $k[X, Y]$ is a k-vector space endowed with two commuting endomorphisms.

Definition. Let M and N be two A-modules. A map $f\colon M \longrightarrow N$ is an *A-module homomorphism* or *A-linear* if $f(m + m') = f(m) + f(m')$ and $f(am) = af(m)$ for all $a \in A$, $m, m' \in M$.

Equivalently, f is a homomorphism of abelian groups and commutes with the action of A on M and N, respectively. Of course, if A is a field, then an A-linear map is simply a linear map between vector spaces. Clearly, the composition of two A-linear maps is again A-linear.

Example 3.2. Any homomorphism of abelian groups is a $\mathbb{Z}$-linear map.

Remark 3.3. Let M and N be A-modules. The abelian group $\mathrm{Hom}(M,N)$ is an A-module as follows. For $f,g \in \mathrm{Hom}(M,N)$ and $a \in A$ we define $f+g, af\colon M \longrightarrow N$ by $m \longmapsto f(m)+g(m)$ and $m \longmapsto af(m)$. An easy computation shows that this definition indeed endows $\mathrm{Hom}(M,N)$ with an A-module structure. One then writes $\mathrm{Hom}_A(M,N)$. We will frequently omit the subscript when the ring will be clear from the context.

More specifically, we can consider the module $\mathrm{Hom}(M,M) =: \mathrm{End}(M)$ for an A-module M. This A-module is in fact a *non-commutative* ring, with multiplication given by composition. Using this, an A-module M is an abelian group together with a ring homomorphism $A \longrightarrow \mathrm{End}(M)$.

Remark 3.4. Let $\alpha\colon M \longrightarrow M'$ and $\beta\colon N \longrightarrow N'$ be A-linear maps between A-modules. Then we get induced A-linear maps

$$\overline{\alpha}\colon \mathrm{Hom}(M',N) \longrightarrow \mathrm{Hom}(M,N), \quad f \longmapsto f\circ\alpha$$

and

$$\overline{\beta}\colon \mathrm{Hom}(M,N) \longrightarrow \mathrm{Hom}(M,N'), \quad g \longmapsto \beta\circ g.$$

Also note that for any A-module M there is an isomorphism

$$\mathrm{Hom}_A(A,M) \simeq M$$

of A-modules given by sending a map $f\colon A \longrightarrow M$ to $f(1)$. Conversely, any A-linear map from A to M is uniquely determined by its value at 1.

Definition. A *submodule* M' of M is a subgroup of M which is closed under multiplication by elements of A, that is $am' \in M'$ for all $a \in A$ and all $m' \in M'$.

If M' is a submodule of M, the *quotient module* is the abelian group M/M' with the A-module structure given by $a(m+M') = am + M'$.

If $f\colon M \longrightarrow N$ is A-linear, then the *kernel* of f is the following submodule of M: $\ker(f) = \{m \in M \mid f(m) = 0\}$. The *image* of f is the set $\mathrm{im}(f) = f(M)$ and is a submodule of N. The *cokernel* of f is the module $N/\mathrm{im}(f)$.

If M' is a submodule of M with the property that $M' \subseteq \ker(f)$, then f induces a homomorphism $\overline{f}\colon M/M' \longrightarrow N$ whose kernel is $\ker(\overline{f}) = \ker(f)/M'$. In particular, $M/\ker(f) \simeq \mathrm{im}(f)$.

Note that there is a one-to-one order-preserving correspondence between submodules of M which contain M' and submodules of M/M'.

Example 3.5. Any subgroup of an abelian group is a submodule.

If A is a ring, then it is a subring of the A-module $A[X]$ and, in particular, a submodule.

In the first section we have defined several operations on ideals. Some of them have counterparts for modules.

Definition. If M is an A-module and $(M_i)_{i\in I}$ is a family of submodules, then their *sum* $\sum_i M_i$ is the set of all sums $\sum_i m_i$ where $m_i \in M_i$ for all $i \in I$ and all but finitely many m_i are zero. The sum is the smallest submodule of M containing all the M_i.

Given a family as above, the set-theoretic intersection $\cap_i M_i$ is again a submodule of M.

Proposition 3.6. *If $N \subseteq M \subseteq L$ are A-modules, then*

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

If M_1 and M_2 are submodules of M, then

$$(M_1 + M_2)/M_1 \simeq M_2/(M_1 \cap M_2).$$

Proof. To prove the first claim, we define a map $f\colon L/N \longrightarrow\!\!\!\!\!\rightarrow L/M$ by sending $l + N$ to $l + M$, that is, by sending a class of an element modulo N to its class modulo M. The kernel of f is M/N and f is surjective and well-defined, hence the claim.

To prove the second claim, note that the map

$$M_2 \longrightarrow\!\!\!\!\!\rightarrow M_1 + M_2 \longrightarrow\!\!\!\!\!\rightarrow (M_1 + M_2)/M_1$$

is surjective and its kernel is precisely $M_1 \cap M_2$. □

Definition. If I is an ideal of A and M is an A-module, we define the module IM as the set of all finite sums $\sum_i a_i m_i$ where $a_i \in I$ and $m_i \in M$. This is a submodule of M.

If N, P are submodules of a module M, define $(N : P)$ to be the set of all $a \in A$ such that $aP \subseteq N$. This is an ideal of A. Setting $N = 0$, gives the *annihilator* $\mathrm{Ann}(P)$ of a module P, namely the set of all $a \in A$ such that $aP = 0$.

Note that if $I \subset \mathrm{Ann}(M)$ for a module M, then M is an A/I-module as follows: $\overline{a}m = am$, where a is any representative of the class $\overline{a} \in A/I$. This is well-defined by our assumption.

Example 3.7. Let $A = \mathbb{Z}$, $M = \mathbb{Z}[X]$ and $I = (2)$. Then IM is the submodule consisting of all polynomials whose coefficients are even.

If $M = A = P$, then $\mathrm{Ann}(P) = 0$. For a more interesting example, let $A = k[X]$, $M = P = k[X]/(X^2)$. Then $\mathrm{Ann}(M) = (X^2)$.

Definition. If $m \in M$, then the set $\{am \mid a \in A\}$, denoted by Am, is a submodule of M. If $M = \sum_{i\in I} Am_i$, then the elements m_i are said to be *generators* of M. An A-module M is said to be *finitely generated* if it has a finite set of generators.

If M, N are A-modules, their *direct sum* is the abelian group $M \times N$ endowed with componentwise scalar multiplication. We will write $M \oplus N$ for the direct sum. Similarly, given any family of modules M_i, $i \in I$, their direct sum $\oplus_{i\in I} M_i$ is the set of all families $(m_i)_{i\in I}$ with $m_i \in M_i$ for all $I \in I$ and all but a finite number of the m_i are zero. If we take all families, then we get the *direct product* $\prod_{i\in I} M_i$.

Example 3.8. Assume that a ring A is a product of finitely many rings $A_1, \ldots, A_n$. Then A is, as an A-module, isomorphic to $\oplus_{j=1}^n I_j$, where I_j is the set of all elements $(0, \ldots, 0, a_j, 0, \ldots, 0)$ with $a_j \in A_j$. Conversely, if $A = I_1 \oplus \ldots \oplus I_n$ is a direct sum of ideals, define $J_k = \oplus_{j \neq k} I_j$ and note that then $A \simeq \prod_{k=1}^n (A/J_k)$.

Definition. An A-module M is *free* if it is isomorphic to $\oplus_i M_i$ with $M_i \simeq A$ for all $i \in I$. Consequently a finitely generated free module is isomorphic to A^n for some $n \in \mathbb{N}$.

Proposition 3.9. *An A-module M is finitely generated if and only if it is isomorphic to a quotient of the free module A^n for some $n > 0$.*

Proof. "$\Rightarrow$" Let $m_1, \ldots, m_n$ be a finite set of generators for M. Define a map $f\colon A^n \longrightarrow\!\!\!\!\rightarrow M$ by sending the i-th basis vector e_i of A^n to m_i. This is clearly an A-linear surjective map, hence $M \simeq A^n/\ker(f)$.

"$\Leftarrow$" Let $f\colon A^n \longrightarrow\!\!\!\!\rightarrow M$ be a surjection. Set $m_i = f(e_i)$. Then the m_i are a finite set of generators for M. □

Proposition 3.10 (Nakayama's lemma)**.** *Let M be a finitely generated A-module and let I be an ideal which is contained in the Jacobson radical* $\mathrm{Jac}(A)$ *of A. If $IM = M$, then $M = 0$.*

Proof. Suppose $M \neq 0$ and let $m_1, \ldots, m_n$ be a minimal set of generators of M. Since $IM = M$, there exists an equation of the form $m_n = a_1 m_1 + \ldots + a_n m_n$ with $a_j \in I$ for all j. Rewriting gives

$$(1 - a_n) m_n = a_1 m_1 + \ldots + a_{n-1} m_{n-1}.$$

Since $I \subseteq \mathrm{Jac}(A)$, $1 - a_n$ is a unit by Proposition 2.19, hence m_n can be generated by the first $n - 1$ elements, a contradiction. □

Corollary 3.11. *Let M be a finitely generated A-module, N a submodule of M and $I \subseteq \mathrm{Jac}(A)$ an ideal. Then $M = IM + N$ implies that $M = N$.*

Proof. Follows by applying Nakayama's lemma to M/N and using that $I(M/N) = (IM + N)/N$. □

Corollary 3.12. *Let A be a local ring, $\mathfrak{m}$ its maximal ideal, $k = A/\mathfrak{m}$ the residue field and M be a finitely generated A-module. Since $M/\mathfrak{m}M$ is naturally a $A/\mathfrak{m} = k$-module, let m_i, $1 \leq i \leq n$, be elements of M whose images in $M/\mathfrak{m}M$ form a basis of this vector space. Then the m_i generate M.*

Proof. Let N be the submodule of M generated by the m_i. Consider the composition $N \longrightarrow\!\!\!\!\rightarrow M \longrightarrow\!\!\!\!\rightarrow M/\mathfrak{m}M$ which is clearly surjective, so $N + \mathfrak{m}M = M$. Since A is assumed to be local, $\mathrm{Jac}(A) = \mathfrak{m}$ and it follows that $M = N$. □

Definition. A sequence of A-modules and A-linear maps

$$\ldots \longrightarrow M_{i-1} \xrightarrow{f_{i-1}} M_i \xrightarrow{f_i} M_{i+1} \longrightarrow \ldots$$

is *exact at* M_i if $\ker(f_i) = \mathrm{im}(f_{i-1})$. It is *exact* if it is exact at M_i for all $i \in \mathbb{Z}$.

A *short exact sequence* is an exact sequence of the form

$$0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0,$$

hence f is injective, g is surjective and $\ker(g) = \mathrm{im}(f)$.

Example 3.13. The sequence

$$0 \longrightarrow \mathbb{Z} \xrightarrow{\cdot 2} \mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow 0$$

is short exact, while the sequence

$$\mathbb{Z} \xrightarrow{i_1} \mathbb{Z}^3 \xrightarrow{p_3} \mathbb{Z}\,,$$

where $i_1(x) = (x, 0, 0)$ and $p_3 = (x, y, z) = z$, is not. Note that $\mathrm{im}(i_1) \subsetneq \ker(p_3)$.

Proposition 3.14. *A sequence* $M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$ *is exact if and only if for all modules* N *the sequence*

$$0 \longrightarrow \mathrm{Hom}(M'', N) \xrightarrow{\overline{g}} \mathrm{Hom}(M, N) \xrightarrow{\overline{f}} \mathrm{Hom}(M', N)$$

is exact.

Similarly, a sequence $0 \longrightarrow N' \xrightarrow{f} N \xrightarrow{g} N''$ *is exact if and only if for all modules* M *the sequence*

$$0 \longrightarrow \mathrm{Hom}(M, N') \xrightarrow{\overline{f}} \mathrm{Hom}(M, N) \xrightarrow{\overline{g}} \mathrm{Hom}(M, N'')$$

is exact.

Proof. We only prove the second claim since the first is similar. Assume first that f is injective and that $\ker(g) = \mathrm{im}(f)$. Let $\varphi\colon M \longrightarrow N'$ be a map. Then $\overline{f}(\varphi) = f \circ \varphi$. If $\varphi \neq 0$, there is an element $m \in M$ such that $\varphi(m) \neq 0$. Then also $f \circ \varphi(m) \neq 0$, since f is injective, so $\overline{f}$ is injective.

Now note that $\overline{g}\overline{f}(\varphi) = g \circ f \circ \varphi = 0$, since $g \circ f = 0$. Therefore, $\mathrm{im}(\overline{f}) \subseteq \ker(\overline{g})$. But if $\psi \in \ker(\overline{g})$, then $g \circ \psi = 0$, so ψ maps to the kernel of g which is the image of f. Hence, $\psi = f \circ \varphi$ for some $\varphi \in \mathrm{Hom}(M, N')$.

Now assume the second sequence to be exact. To show that f is injective, let $n' \in \ker(f)$ and consider the submodule An' and its embedding α into N'. Then $\overline{f}(\alpha) = 0$, hence $\alpha = 0$, so $n' = 0$. Next, since $\overline{g} \circ \overline{f} = 0$, we have, for any $\varphi\colon M \longrightarrow N'$, $g \circ f \circ \varphi = 0$. Taking $M = N'$ and $\varphi = \mathrm{id}$, we get $g \circ f = 0$, so $\mathrm{im}(f) \subseteq \ker(g)$. Lastly, if $n \in \ker(g)$, take $M = An$ and $\alpha \in \mathrm{Hom}(M, N)$ the embedding. Then $\overline{g}(\alpha) = 0$, so $\alpha = f \circ \beta$ for some $\beta \in \mathrm{Hom}(An, N')$, hence $n \in \mathrm{im}(f)$. □

Proposition 3.15. *Let*

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

be a commutative diagram of A-modules and A-linear maps. Assume that both rows are exact. Then there exists an exact sequence

$$0 \longrightarrow \ker(\alpha') \xrightarrow{\overline{f}} \ker(\alpha) \xrightarrow{\overline{g}} \ker(\alpha'') \xrightarrow{d}$$

$$\longrightarrow \operatorname{coker}(\alpha') \xrightarrow{\overline{f'}} \operatorname{coker}(\alpha) \xrightarrow{\overline{g'}} \operatorname{coker}(\alpha'') \longrightarrow 0$$

in which $\overline{f}$ and $\overline{g}$ are the restrictions of f and g, while $\overline{f'}$ and $\overline{g'}$ are induced by f' and g'.

Proof. We will only give an outline of the proof since it is a good exercise. Since $\alpha \circ f = f' \circ \alpha'$, any element in $\ker(\alpha')$ gets mapped by f to an element of $\ker(\alpha)$. Now f is injective, so its restriction to $\ker(\alpha')$ is of course still injective. The commutativity of the diagram also implies, in particular, that $\operatorname{im}(\alpha')$ is mapped to $\operatorname{im}(\alpha)$ by f'. Therefore $\operatorname{im}(\alpha')$ is contained in the kernel of the map $N' \longrightarrow N \longrightarrow \operatorname{coker}(\alpha)$, hence there is an induced map $\operatorname{coker}(\alpha') \longrightarrow \operatorname{coker}(\alpha)$ as claimed.

The most interesting part of the proof is the construction of the boundary map d. Let $x \in \ker(\alpha'')$. Since g is surjective, there exists an $m \in M$ mapping to x under g. Using the equation $\alpha'' \circ g = g' \circ \alpha$, we see that $\alpha(m) \in \ker(g')$. By the exactness of the lower row, there is an element $n' \in N'$ such that $f'(n') = \alpha(m)$. The map d is now defined by sending x to the class of $n' \in \operatorname{coker}(\alpha')$. Checking that this is a well-defined map and the exactness of the sequence is left to the reader. □

3.1. **Tensor product of modules.**

Definition. Let M, N and P be A-modules. A map $f\colon M \times N \longrightarrow P$ is called *A-bilinear* if for every $m \in M$ the map $f(m, -)\colon N \longrightarrow P$ is A-linear and for every $n \in N$ the map $f(-, n)\colon M \longrightarrow P$ is A-linear.

Proposition 3.16. *Let M and N be A-modules. There exists a pair (T, g) consisting of an A-module T and a bilinear map $g\colon M \times N \longrightarrow T$ such that the following universal property holds: Given any A-module P and any bilinear map $f\colon M \times N \longrightarrow P$ there exists a unique linear map $f'\colon T \longrightarrow P$ such that $f = f' \circ g$. Moreover, if (T', g') is a second pair satisfying the universal property, then there is a unique isomorphism $j\colon T \longrightarrow T'$ such that $j \circ g = g'$. The module T is called the* tensor product *of M and N and frequently written as $M \otimes N$.*

Proof. We will first prove that if such a pair exists, it has to be unique. So, let (T, g) and (T', g') be two pairs satisfying the universal property. Choosing $P = T$ and $f = g'$ we get a unique linear map $j\colon T \longrightarrow T'$ such that $g' = j \circ g$. Now setting $P = T'$ and $f = g$ and using the universal property of the pair (T', g'), we get a unique map $j'\colon T' \longrightarrow T$ such that $g = j' \circ g'$. Since the map j and j' are unique, their compositions have to be the respective identity, hence j is an isomorphism.

Now we will show that the tensor product indeed exists. Let $C = A^{(M\times N)}$. Note that the elements of C are formal linear combinations of $M \times N$ with coefficients in A. Consider the submodule D of C generated by all elements of the following types

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

Define $T = C/D$. For each basis element $(m, n) \in C$ we will write $m \otimes n$ for its image in T. Clearly, T is generated by the elements of the form $m \otimes n$ and we have

$$\begin{aligned}(m + m') \otimes n = m \otimes n + m' \otimes n, \quad m \otimes (n + n') = m \otimes n + m \otimes n'\\ (am) \otimes n = a(m \otimes n) = m \otimes (an).\end{aligned}$$

To put it differently, the map $g\colon M \times N \longrightarrow T$, $(m, n) \longmapsto m \otimes n$ is bilinear.

Given any map $f\colon M \times N \longrightarrow P$, we get an induced map $\overline{f}\colon C \longrightarrow P$. If f is bilinear, then $\overline{f}$ vanishes on the generators of D, hence on D, so we get a linear map $f'\colon T \longrightarrow P$ such that $f'(m \otimes n) = f(m, n)$. The latter condition uniquely determines f', hence the pair (T, g) satisfies the universal property. □

Example 3.17. If $M \simeq A^k$ and $N \simeq A^l$, then $M \otimes_A N \simeq A^{kl}$. The proof is the same as for vector spaces.

Remark 3.18. We already noted above that the elements of the form $m \otimes n$ generate the tensor product $M \otimes N$. It follows that if M and N are finitely generated, then the same holds for $M \otimes N$ (take the tensor products of the generators).

One has to be a bit careful when working with the tensor product. For example, let $A = \mathbb{Z}$, $M = \mathbb{Z}$, $N = \mathbb{Z}/2\mathbb{Z}$, $M' = 2\mathbb{Z} \subseteq M$ and $N' = N$. Let $x \neq 0 \in N$ and consider $2 \otimes x$. Then $2 \otimes x = 1 \otimes 2x = 1 \otimes 0 = 0 \in M \otimes N$, but $2 \otimes x \neq 0 \in M' \otimes N'$.

Instead of working with bilinear maps, one can also start with a multilinear map $f\colon M_1 \times \ldots \times M_k \longrightarrow P$ and appropriately changing the above construction then gives

Proposition 3.19. *Let $M_1, \ldots, M_k$ be A-modules. Then there exists a pair (T, g) consisting of an A-module T and an A-multilinear map $g\colon M_1 \times \ldots \times M_k \longrightarrow T$ with the following property: Given any A-module P and any A-multilinear map $f\colon M_1 \times \ldots \times M_k \longrightarrow P$, there exists a unique A-linear map $f'\colon T \longrightarrow P$ such that $f' \circ g = f$. Moreover, any two modules satisfying this property are isomorphic.* □

The tensor product has several nice properties.

Proposition 3.20. *Let M, N and P be A-modules. Then there exist unique isomorphisms*

(1) $M \otimes N \longrightarrow N \otimes N$, $m \otimes n \longmapsto n \otimes n$;
(2) $(M \otimes N) \otimes P \longrightarrow M \otimes (N \otimes P) \longrightarrow M \otimes N \otimes P$, $(m \otimes n) \otimes p \longmapsto m \otimes (n \otimes p) \longmapsto m \otimes n \otimes p$;
(3) $(M \oplus N) \otimes P \longrightarrow M \otimes P \oplus N \otimes P$, $(m, n) \otimes p \longmapsto (m \otimes p, n \otimes p)$;
(4) $A \otimes M \longrightarrow M$, $a \otimes m \longmapsto am$.

Proof. The idea in all cases is to construct a suitable bilinear or multilinear mapping and use the universal property to show the existence of the homomorphisms given in the proposition. We will do this in the third case and leave the rest to the reader. Consider the map $f\colon (M \oplus N) \times P \longrightarrow M \otimes P \oplus N \otimes P$ defined by $(m, n) \times p \longmapsto (m \otimes p, n \otimes p)$. This map is clearly bilinear and hence induces the map described in the proposition. On the other hand, the maps $M \times P \longrightarrow (M \oplus N) \otimes P$ and $N \times P \longrightarrow (M \oplus N) \otimes P$ given by $(m, p) \longmapsto (m, 0) \otimes p$ and $(n, p) \longmapsto (0, n) \otimes p$ are both bilinear and hence induce maps $M \otimes P \longrightarrow (M \oplus N) \otimes P$ and $N \otimes P \longrightarrow (M \oplus N) \otimes P$. The direct sum of these maps is the map g which sends $(m \otimes p, n \otimes p)$ to $(m, n) \otimes p$ and hence is the required inverse to f. □

Definition. Let $f\colon M \longrightarrow M'$ and $g\colon N \longrightarrow N'$ be homomorphisms of A-modules. Define the map $h\colon M \times N \longrightarrow M' \otimes N'$, $h(m, n) = f(m) \otimes g(n)$. Since h is bilinear, it induces an A-linear map $f \otimes g\colon M \otimes M' \longrightarrow N \otimes N'$, $(f \otimes g)(m \otimes n) = f(m) \otimes g(n)$.

Note that if $f'\colon M' \longrightarrow M''$ and $g'\colon N' \longrightarrow N''$ are A-linear, then $(f' \circ f) \otimes (g' \circ g) = (f' \otimes g') \circ (f \otimes g)$.

Definition. Let $f\colon A \longrightarrow B$ be a ring homomorphism and let N be a B-module. The multiplication $A \times N \longrightarrow N$ defined by $(a, n) \longmapsto f(a)n$ makes N into an A-module, sometimes denoted by N_A. We say that N_A is obained by *restriction of scalars*. Since, in particular, B becomes an A-module through this procedure, we can, for any A-module M consider the tensor product $M_B = B \otimes_A M$. This A-module has the structure of a B-module via $b'(b \otimes m) = b'b \otimes m$. The B-module M_B is said to be obtained from M by *extension of scalars*.

Proposition 3.21. *If N is a finitely generated B-module and B is finitely generated as an A-module, then N_A is finitely generated as an A-module.*

Proof. If $n_1, \ldots, n_k$ generate N over B and $b_1, \ldots, b_l$ generate B over A, then $n_i b_j$ generate N_A over A. □

Proposition 3.22. *If M is a finitely generated A-module, then M_B is a finitely generated B-module.*

Proof. If $m_1, \ldots, m_k$ generate M over A, then the elements $1 \otimes m_1, \ldots, 1 \otimes m_k$ generate M_B over B. □

Proposition 3.23. *Let M, N and P be A-modules. Then there exists a canonical isomorphism $\mathrm{Hom}(M \otimes N, P) \simeq \mathrm{Hom}(M, \mathrm{Hom}(N, P))$ of A-modules.*

Proof. If $f\colon M \times N \longrightarrow P$ is bilinear, then for any $m \in M$ the map $n \longrightarrow f(m, n)$ is linear. Therefore, we get a map $M \longrightarrow \mathrm{Hom}(N, P)$ which is linear because f is linear in m. On the other hand, if

$$\varphi\colon M \longrightarrow \mathrm{Hom}(N, P)$$

is a linear map, it induces a bilinear map

$$M \times N \longrightarrow P, \quad (m, n) \longmapsto \varphi(m)(n).$$

In conclusion, there is a one-to-one correspondence between bilinear maps from $M \times N$ to P and the linear maps $\mathrm{Hom}(M, \mathrm{Hom}(N, P))$. Since the first set is in one-to-one correspondence with $\mathrm{Hom}(M \otimes N, P)$, the claim follows. □

Proposition 3.24. *Let*

$$M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$$

be an exact sequence of A-modules and A-linear maps and let N be an arbitrary A-module. Then the sequence

$$M' \otimes N \xrightarrow{f \otimes \mathrm{id}} M \otimes N \xrightarrow{g \otimes \mathrm{id}} M'' \otimes N \longrightarrow 0$$

is exact.

Proof. Denote the first sequence by Δ, the second by $\Delta \otimes N$ and let P be any A-module. Since Δ is exact, by Proposition 3.14 the sequence $\mathrm{Hom}(\Delta, \mathrm{Hom}(N, P))$ is exact. By the previous proposition the sequence $\mathrm{Hom}(\Delta \otimes N, P)$ is exact. By Proposition 3.14 again, the sequence $\Delta \otimes N$ is exact. □

Example 3.25. Let $A = \mathbb{Z}$ and consider the exact sequence $0 \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Z}$ where the second map is multiplication by 2. Tensoring this sequence with $N = \mathbb{Z}/2\mathbb{Z}$ over $\mathbb{Z}$, gives the sequence $0 \longrightarrow N \longrightarrow N$ which is not exact because the second map is identically zero. Here we used that $N \otimes_{\mathbb{Z}} \mathbb{Z} \simeq N$, so the second map is $x = x \otimes 1 \longmapsto x \otimes 2 = 0$. In particular, the tensor product in general does not respect exactness "on the left".

3.2. **Flatness.**

Definition. An A-module N is called *flat* if for any exact sequence Δ the sequence $\Delta \otimes N$ is exact.

Proposition 3.26. *If N is an A-module, then the following statements are equivalent:*

1. *N is flat.*
2. *If Δ is a short exact sequence, then Δ is a short exact sequence.*
3. *If $f\colon M' \longrightarrow M$ is injective, then $f \otimes \mathrm{id}\colon M' \otimes N \longrightarrow M \otimes N$ is injective.*
4. *If $f\colon M' \longrightarrow M$ is injective and M, M' are finitely generated, then $f \otimes \mathrm{id}\colon M' \otimes N \longrightarrow M \otimes N$ is injective.*

Proof. "(1)⇒(2)" Clear.

"(2)⇒(1)" Any long exact sequence can be split up into short exact sequences. Indeed, if a long exact sequence

$$\ldots \longrightarrow M_{i-1} \xrightarrow{f_{i-1}} M_i \xrightarrow{f_i} M_{i+1} \longrightarrow \ldots$$

is given, we get short exact sequences of the form

$$0 \longrightarrow \operatorname{im}(f_{i-1}) = \ker(f_i) \longrightarrow M_i \longrightarrow \operatorname{im}(f_i) \longrightarrow 0.$$

"(2)⇔(3)" By Proposition 3.24.

"(3)⇒(4)" Clear.

"(4)⇒(3)" Let $f\colon M' \longrightarrow M$ be injective and let $\sum m_i' \otimes n_i \in \ker(f \otimes \mathrm{id})$. Let M_0' be the submodule of M' generated by the m_i'. Since the sum is finite, this module is finitely generated. Denote by x the element $\sum m_i' \otimes n_i \in M_0' \otimes N$. The image $f(M_0')$ is also finitely generated, so there exists a submodule M_0 of M containing $f(M_0')$ and such that $\sum f(m_i') \otimes n_i = 0$ in $M_0 \otimes N$. If we denote by $f_0\colon M_0' \longrightarrow M_0$ the restriction of f, then $(f \otimes \mathrm{id})(x) = 0$. Our assumption gives that $x = 0$, so $\sum m_i' \otimes n_i$ is 0 in $M \otimes N$. □

Example 3.27. It is easy to see that any free module A^k of finite rank is flat. However, there are flat modules which are not free. For example, let $A = \mathbb{Z}$ and $M = \mathbb{Q}$. Then M is a flat $\mathbb{Z}$-module (this follows for example from Proposition 4.7 below but can also be shown directly) but is not free. Indeed, any two elements $\frac{p}{q}$ and $\frac{p'}{q'}$ are linearly dependent, since $0 = p'q\frac{p}{q} - pq'\frac{p'}{q'}$.

We can also give the following characterisation of flatness which, in particular, shows that $\mathbb{Q}$ is indeed a flat $\mathbb{Z}$-module.

Proposition 3.28. *An A-module M is flat if and only if for every ideal I of A the canonical homomorphism $I \otimes_A M \longrightarrow IM$ is an isomorphism.*

Proof. Assume that M is flat. Tensoring the canonical injection $I \longrightarrow A$ with M gives an injection $I \otimes_A M \longrightarrow A \otimes_A M \simeq M$. The image of this map is clearly IM.

Conversely, assume that $I \otimes_A M \longrightarrow IM$ is an isomorphism for every ideal I. We need to show that for any injective map $N' \longrightarrow N$ the induced map $N' \otimes_A M \longrightarrow N \otimes_A M$ is still injective.

We will first assume that N is free of finite rank n and prove the claim by induction on n. The case $n = 1$ is precisely our assumption. Let now N be of rank $n \geq 2$. We can write N as a direct sum of two non-trivial free submodules N_1 and N_2 for which the claim holds since their rank is smaller than n. Setting $N_1' = N' \cap N_1$ and $N_2' = \operatorname{im}(N' \longrightarrow N/N_1 = N_2)$, we get a diagram

$$\begin{array}{ccccccc} & & N_1' \otimes M & \longrightarrow & N' \otimes M & \longrightarrow & N_2' \otimes M \longrightarrow 0 \\ & & \downarrow f & & \downarrow & & \downarrow g \\ 0 \longrightarrow & N_1 \otimes M & \longrightarrow & N \otimes M & \longrightarrow & N_2 \otimes M & \longrightarrow 0 \end{array}$$

Since f and g are injective by the induction hypothesis, it follows from a diagram chase that $N' \otimes M \longrightarrow N \otimes M$ is injective.

Next, we can show the claim for a free module N of arbitrary rank by using that any element of $N' \otimes M$ is in the image of $(N' \cap N_0) \otimes M \longrightarrow N' \otimes M$ for some direct factor N_0 of N of finite rank.

Lastly, let N be arbitrary. There exists a surjection $p\colon L \longrightarrow N$ from a free module L (for instance, we can take $L = A^N$). Set $L' = p^{-1}N'$. We then get a commutative diagram

$$\begin{array}{ccccccc} \ker(p) \otimes M & \longrightarrow & L' \otimes M & \longrightarrow & N' \otimes M & \longrightarrow & 0 \\ \downarrow{=} & & \downarrow & & \downarrow & & \\ \ker(p) \otimes M & \longrightarrow & L \otimes M & \longrightarrow & N \otimes M & \longrightarrow & 0 \end{array}$$

and a diagram chase shows that the map $N' \otimes M \longrightarrow N \otimes M$ is injective. □

The next result shows that over a principal ideal domain flatness is very easy to characterise. Recall that if M is a module over an integral domain A, an element $m \in M$ is *torsion* if there exists an $a \neq 0$ such that $am = 0$. A module M is *torsion free* if there are no non-zero torsion elements in M.

Corollary 3.29. *Let A be a principal ideal domain. An A-module M is flat if and only if it is torsion free.*

Proof. Let I be a non-zero ideal of A. Since A is a principal ideal domain, $I = Aa$ for some $a \neq 0$. The multiplication by a map $t_a\colon A \longrightarrow I$, $b \longmapsto ab$, is an isomorphism. Denote by u_a the map $M \longrightarrow M$, $m \longmapsto am$. The diagram

$$\begin{array}{ccc} A \otimes_A M = M & \xrightarrow{t_a \otimes \mathrm{id}} & I \otimes_A M \\ {\scriptstyle u_a}\downarrow & \swarrow_{f} & \\ IM & & \end{array}$$

is commutative.

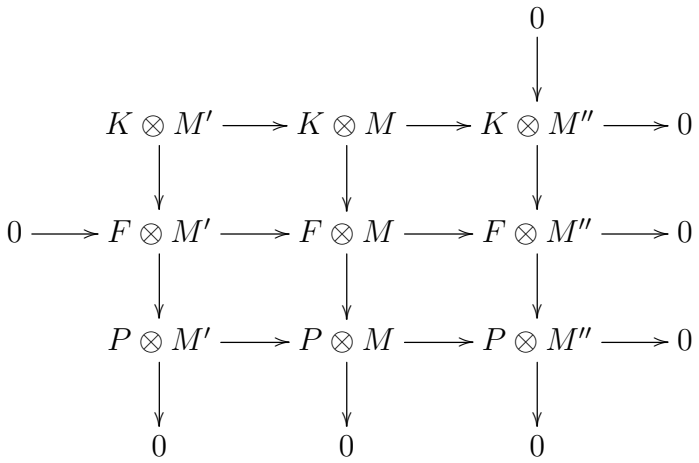
If M is flat, then $t_a \otimes \mathrm{id}$ and f are isomorphisms, hence the same holds for u_a which is equivalent to saying that M is torsion free.

Conversely, if M is torsion free, then u_a is an isomorphism. Therefore, $t_a \otimes \mathrm{id}$ is injective, and hence an isomorphism, since it is surjective anyway. Therefore, f is an isomorphism and we are done by the previous proposition. □

Another somewhat peculiar property of flat modules is the following.

Proposition 3.30. *Let $0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$ be an exact sequence of A-modules and assume that M'' is flat. Then for any module P the sequence $0 \longrightarrow M' \otimes P \longrightarrow M \otimes P \longrightarrow M'' \otimes P \longrightarrow 0$ is exact.*

Proof. Take a projection $F \twoheadrightarrow P$ from a free module and denote by K the kernel of this map. We therefore get a commutative diagram



A diagram chase shows that the map $P \otimes M' \to P \otimes M$ is injective. □

3.3. **Algebras.**

Definition. Let A be a ring. An *A-algebra* is a ring B together with a ring homomorphism $f\colon A \to B$.

Example 3.31. If A is a field and $B \neq 0$, then f is injective, so any algebra over a field contains the field as a subring. For a specific example consider the polynomial ring.

Also note that any ring A is a $\mathbb{Z}$-algebra, since any ring homomorphism $\mathbb{Z} \to A$ is already determined by the requirement $1 \mapsto 1$.

Definition. If $f\colon A \to B$ and $g\colon A \to C$ are two A-algebras, an *A-algebra homomorphism* is a ring homomorphism $h\colon B \to C$ such that $h \circ f = g$.

A ring homomorphism $f\colon A \to B$ is *finite* and B is then called a *finite A-algebra* if B is finitely generated as an A-module. The homomorphism f is said to be *of finite type* and B a *finitely generated A-algebra* if there exists an A-algebra homomorphism from $A[X_1, \ldots, X_k] \to B$ for some $k > 0$.

Note that B is a finitely generated A-algebra if and only if there exists a finite set of elements $b_1, \ldots, b_k$ such that any element of B can be written as a polynomial in the b_i with coefficients from $f(A)$.

Now we want to define the tensor product of two algebras $f\colon A \to B$ and $g\colon A \to C$. Since B and C are in particular A-modules, the tensor product $D = B \otimes_A C = B \otimes C$ exists. Hence we only need to define a multiplication on it. For this, consider the map $B \times C \times B \times C \to D$ defined by $(b, c, b', c') \mapsto bb' \otimes cc'$, note that it is linear in every factor and hence we get an A-linear map $B \otimes C \otimes B \otimes C = D \otimes D \to D$. The reader

can easily check that the multiplication defined in this manner is given by

$$(\sum_i b_i \otimes c_i)(\sum_j b'_j \otimes c'_j) = \sum_{i,j}(b_i b'_j \otimes c_i c'_j).$$

The identity element is $1 \otimes 1$. The required map from A into D is given by $a \longmapsto f(a) \otimes 1 = 1 \otimes g(a)$.

4. Localisation

The purpose of this section is to explain the procedure of localisation in which one formally adds inverses for some subset of a ring. As an example consider $A = \mathbb{Z}$. The passage to the rational numbers $\mathbb{Q}$ is a special instance of localisation since we basically add an inverse for every non-zero integer.

Definition. Let A be a ring. A *multiplicatively closed subset* of A is a set S in A such that $1 \in S$ and for any two elements $s, s' \in S$, their product ss' is also in S.

If S is a multiplicatively closed subset of A, define a relation $\equiv$ on $A \times S$ by $(a, s) \equiv (b, t) \iff (at - bs)u = 0$ for some $u \in S$. One sees immediately that this relation is reflexive (take $u = 1$) and symmetric (if $(at-bs)u = 0$, then also $(bs-at)u = 0$). To show that it is transitive, assume that $(a, s) \equiv (b, t)$ and $(b, t) \equiv (c, u)$, so there exist $v, w \in S$ such that $(at - bs)v = 0 = (bu - ct)w$. Hence, $atv = bsv$ so $au(tvw) = bsuvw = cs(tvw)$. Since $v, w, t \in S$ are in S, so is their product, hence $(a, s) \equiv (c, u)$ and the relation is transitive.

Definition. Let A be a ring, S a multiplicatively closed subset of A and $\equiv$ the equivalence relation defined above. Denote the set of equivalences classes $A/\equiv$ by $S^{-1}A$ and write its elements as $\frac{a}{s}$ with $a \in A$ and $s \in S$. This set becomes a ring, the *ring of fractions of A with respect to S* or *the localisation of A with respect to S* as follows:

$$\frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st}$$
$$\frac{a}{s}\frac{b}{t} = \frac{ab}{st}.$$

Of course, we need to check that the above is well-defined and makes $S^{-1}A$ into a ring. The latter is quite clear from the definition, compare with the rational numbers. Let us give an example how to check that the addition is well-defined. Assume that $\frac{a}{s} = \frac{a'}{s'}$, so there exists a $u \in S$ with $(as' - a's)u = 0$. We need to show that $\frac{at+bs}{st} = \frac{a't+bs'}{s't}$ which amounts to showing the existense of an element $v \in S$ such that $((at + bs)s't - (a't + bs')st)v = 0$. Setting $v = u$ our equation becomes $(as' - a's)ttv = 0$, and $ttv \in S$.

Remark 4.1. It is easy to check that the map $f\colon A \longrightarrow S^{-1}A$ which sends a to $\frac{a}{1}$ is a ring homomorphism. However, it is not injective in general. It is injective when A is an integral domain and$0 \notin S$.

If A is an integral domain and $S = A \setminus 0$, then $S^{-1}A$ is called the *field of fractions* of A.

The localisation satisfies a universal property described in the following

Proposition 4.2. *Let A be a ring, S a multiplicatively closed subset of A and $S^{-1}A$ the localisation of A with respect to S. If $g\colon A \longrightarrow B$ is a ring homomorphism such that $g(s)$ is a unit for all $s \in S$, then there exists a unique ring homomorphism $h\colon S^{-1}A \longrightarrow B$ such that $h \circ f = g$, where $f\colon A \longrightarrow S^{-1}A$ is the canonical map.*

Proof. First we will show that there is at most one map h satisfying the conditions. Note that $h(\frac{a}{1}) = h(f(a)) = g(a)$ and if $s \in S$, then $h(\frac{1}{s}) = h((\frac{s}{1})^{-1}) = h(\frac{s}{1})^{-1} = g(s)^{-1}$. Therefore, $h(\frac{a}{s}) = g(a)g(s)^{-1}$, so h is uniquely determined by g.

To show existence, set $h(\frac{a}{s}) = g(a)g(s)^{-1}$. Let us show that this is well-defined, so let $\frac{a}{s} = \frac{a'}{s'}$. Thus there exists an element $u \in S$ such that $(as' - a's)u = 0$, hence $(g(a)g(s') - g(a')g(s))g(u) = 0$. Since $g(u)$ is a unit in B, it follows that $g(a)g(s') = g(a')g(s)$ or, equivalently, $g(a)g(s)^{-1} = g(a')g(s')^{-1}$. Therefore, h is well-defined. On the other hand, it is clearly a ring homomorphism so we are done. □

Corollary 4.3. *If $g\colon A \longrightarrow B$ is a ring homomorphism such that the following conditions are satisfied:*

1. *If $s \in S$, then $g(s)$ is a unit in B;*
2. *If $g(a) = 0$, then $as = 0$ for some $s \in S$;*
3. *Every element of B is of the form $g(a)g(s)^{-1}$.*

Then there exists a unique isomorphism $h\colon S^{-1}A \longrightarrow B$ such that $g = h \circ f$.

Proof. Using (1) we only need to check that $h\colon S^{-1}A \longrightarrow B$ defined by $h(\frac{a}{s}) = g(a)g(s)^{-1}$ is an isomorphism. By (3), h is surjective. Now let $h(\frac{a}{s}) = 0$, then $g(a) = 0$, so by (2) $at = 0$ for some $t \in S$. It follows that $\frac{a}{s} = \frac{0}{1} = 0 \in S^{-1}A$, so h is injective. □

Example 4.4.

i) Let $\mathfrak{p}$ be a prime ideal in A. Then $S = A \setminus \mathfrak{p}$ is a multiplicatively closed subset, since if $s, s' \notin \mathfrak{p}$, then also $ss' \notin \mathfrak{p}$ (in fact, $\mathfrak{p}$ prime $\Leftrightarrow A \setminus \mathfrak{p}$ is multiplicatively closed). In this case, we write $A_{\mathfrak{p}}$ for $S^{-1}A$. Note that the elements of the form $\frac{a}{s}$ with $a \in \mathfrak{p}$ form an ideal $\mathfrak{m}$ in $A_{\mathfrak{p}}$ by definition. On the other hand, if $\frac{b}{t} \notin \mathfrak{m}$, then $b \notin \mathfrak{p}$, so $b \in S$ and $\frac{b}{t}$ is a unit in $A_{\mathfrak{p}}$. It follows that $\mathfrak{m}$ is the only maximal ideal in $A_{\mathfrak{p}}$ so $A_{\mathfrak{p}}$ is a local ring. We call $A_{\mathfrak{p}}$ the *localisation of A at $\mathfrak{p}$*.

ii) The ring $S^{-1}A$ is the zero ring if and only if $0 \in S$ (use that if $S^{-1}A = 0$, then $\frac{1}{1} = \frac{0}{1}$).

iii) Let $f \in A$ and define $S = (f^n)_{n \in \mathbb{N}}$. We will write A_f for $S^{-1}A$ in this case.

iv) If I is any ideal in A, the $S = 1 + I = \{1 + x \mid x \in I\}$ is a multiplicatively closed subset in A.

v) As special cases of i) and iii) consider $A = \mathbb{Z}$ and $\mathfrak{p} = (p)$ where p is a prime number. Then $A_{\mathfrak{p}}$ is the set of all rational numbers whose denominator is not divisible by p. If $\mathfrak{p} = (0)$, then $A_{\mathfrak{p}} = \mathbb{Q}$. If $f \in \mathbb{Z}$, then A_f is the set of all rational numbers whose denominator is a power of f.

Definition. Let M be an A-module and S be a multiplicatively closed subset of A. We define the set $S^{-1}M$ as the quotient $M \times S/\equiv$, where $(m,s) \equiv (m',s')$ if and only if there exists a $u \in S$ such that $(ms' - m's)u = 0 \in M$. This is in fact an $S^{-1}A$-module with respect to the addition defined as in the ring case and scalar multiplication given by $\frac{a}{s}\frac{m}{t} = \frac{am}{st}$.

As before we will write $M_{\mathfrak{p}}$ is $S = A \setminus \mathfrak{p}$ for a prime ideal $\mathfrak{p}$ and M_f if $S = (f^n)_{n\geq 1}$ for an element f in A.

If $f\colon M \longrightarrow N$ is A-linear, then

$$S^{-1}f\colon S^{-1}M \longrightarrow S^{-1}N, \quad \frac{m}{s} \longmapsto \frac{f(m)}{s}$$

is $S^{-1}A$-linear.

Proposition 4.5. *If the sequence $M' \xrightarrow{f} M \xrightarrow{g} M''$ is exact at M, then the sequence $S^{-1}M' \xrightarrow{S^{-1}f} S^{-1}M \xrightarrow{S^{-1}g} S^{-1}M''$ is exact at $S^{-1}M$.*

Proof. Since $g \circ f = 0$, also $S^{-1}g \circ S^{-1}f = S^{-1}(g \circ f) = 0$, so $\operatorname{im}(S^{-1}f) \subseteq \ker(S^{-1}g)$. Now take $\frac{m}{s} \in \ker(S^{-1}g)$, so $\frac{g(m)}{s} = 0$ in $S^{-1}M''$. By definition, this means that there exists an element $u \in S$ such that $0 = ug(m) = g(um)$. Therefore, $um \in \ker(g) = \operatorname{im}(f)$, so $um = f(m')$ for some $m' \in M'$. So in $S^{-1}M$ we have the equalities

$$\frac{m}{s} = \frac{um}{us} = \frac{f(m')}{us} = S^{-1}f(\frac{m'}{us}),$$

hence $\ker(S^{-1}g) \subseteq \operatorname{im}(S^{-1}f)$ and the proposition is proved. □

In particular, $S^{-1}M'$ is a submodule of $S^{-1}M$ if M' is a submodule of M.

Corollary 4.6. *If N and P are submodules of M, then*

(1) $S^{-1}(N+P) = S^{-1}N + S^{-1}P$,
(2) $S^{-1}(N \cap P) = S^{-1}N \cap S^{-1}P$,
(3) $S^{-1}(M/N) \simeq S^{-1}M/S^{-1}N$.

Proof. To see (3), apply S^{-1} to the sequence

$$0 \longrightarrow N \longrightarrow M \longrightarrow M/N \longrightarrow 0.$$

Item (1) being rather obvious, we will now prove (2). Clearly, $S^{-1}(N \cap P) \subseteq S^{-1}N$ and also $S^{-1}(N \cap P) \subseteq S^{-1}P$, so one inclusion is obvious. To see that $S^{-1}N \cap S^{-1}P \subseteq S^{-1}(N \cap P)$, take an element $\frac{n}{s} = \frac{p}{t}$ in $S^{-1}N \cap S^{-1}P$. Then $u(nt - ps) = 0$ for some $u \in S$, hence $utn = usp = w \in N \cap P$, so $\frac{n}{s} = \frac{w}{stu} \in S^{-1}(N \cap P)$. □

Proposition 4.7. *If M is an A-module, then the map*

$$f\colon S^{-1}A \otimes_A M \longrightarrow S^{-1}M, \quad \frac{a}{s} \otimes m \longmapsto \frac{am}{s}$$

is an isomorphism of $S^{-1}A$-modules. In particular, $S^{-1}A$ is a flat A-module.

Proof. The map $S^{-1}A \times M \longrightarrow S^{-1}M$ defined by $(\frac{a}{s}, m) \longmapsto \frac{am}{s}$ is bilinear, hence induces the map f described in the proposition. Clearly, f is surjective and uniquely defined. Now let $\sum_i \frac{a_i}{s_i} \otimes m_i \in S^{-1}A \otimes M$ be arbitrary. Setting $s = \prod_i s_i \in S$ and $t_i = \prod_{j \neq i} s_j$, we have

$$\sum_i \frac{a_i}{s_i} \otimes m_i = \sum_i \frac{a_i t_i}{s} \otimes m_i = \frac{1}{s} \otimes \sum_i a_i t_i m.$$

It follows that any element of $S^{-1}A \otimes M$ can be written in the form $\frac{1}{s} \otimes m$. If such an element is in the kernel of f, then $\frac{m}{s} = 0$ in $S^{-1}M$, hence $um = 0$ for some $u \in S$, so

$$\frac{1}{s} \otimes m = \frac{u}{us} \otimes m = \frac{1}{us} \otimes um = 0.$$

Therefore, f is injective.

To prove the second claim, just use that S^{-1} is exact. □

Proposition 4.8. *Let M and N be A-modules. There exists a unique isomorphism of $S^{-1}A$-modules $f\colon S^{-1}M \otimes_{S^{-1}A} S^{-1}N \longrightarrow S^{-1}(M \otimes_A N)$ defined by*

$$f(\frac{m}{s} \otimes \frac{n}{t}) = \frac{m \otimes n}{st}.$$

In particular, if $\mathfrak{p}$ is a prime ideal, then $M_\mathfrak{p} \otimes_{A_\mathfrak{p}} N_\mathfrak{p} \simeq (M \otimes_A N)_\mathfrak{p}$.

Proof. We have

$$\begin{aligned} S^{-1}M \otimes_{S^{-1}A} S^{-1}N &\simeq (M \otimes_A S^{-1}A) \otimes_{S^{-1}A} (S^{-1}A \otimes_A N) \\ &\simeq S^{-1}A \otimes_A (M \otimes_A N) \simeq S^{-1}(M \otimes_A N). \end{aligned}$$

□

4.1. **Local properties.**

Definition. Let Pr be a property of a ring A or an A-module M. Then Pr is said to be a *local property* if the following holds: A (or M) has $Pr \iff A_\mathfrak{p}$ (or $M_\mathfrak{p}$) has Pr for each prime ideal $\mathfrak{p}$ of A.

We will give some examples of local properties in the following.

Proposition 4.9. *Let M be an A-module. Then the following are equivalent.*

1. *$M = 0$.*
2. *$M_\mathfrak{p} = 0$ for all prime ideals $\mathfrak{p}$ of A.*
3. *$M_\mathfrak{m} = 0$ for all maximal ideals $\mathfrak{m}$ of A.*

Proof. Clearly, (1) implies (2) and (2) implies (3). So suppose that (3) holds and assume that $M \neq 0$. Take $0 \neq x \in M$ and let $I = \operatorname{Ann}(x) \neq (1)$ be the annihilator of x. There exists a maximal ideal $\mathfrak{m}$ such that $I \subseteq \mathfrak{m}$. Since $M_\mathfrak{m} = 0$, the element $\frac{x}{1} \in M_\mathfrak{m}$ has to be zero, hence $ux = 0$ for some $u \in A \setminus \mathfrak{m}$. But $\operatorname{Ann}(x) \subseteq \mathfrak{m}$, a contradiction. □

Proposition 4.10. *Let $f\colon M \longrightarrow N$ be A-linear. Then the following are equivalent.*

1. *The map f is injective.*
2. *The map $f_\mathfrak{p}\colon M_\mathfrak{p} \longrightarrow N_\mathfrak{p}$ is injective for all prime ideals $\mathfrak{p}$ of A.*

(3) *The map* $f_{\mathfrak{m}}\colon M_{\mathfrak{m}} \longrightarrow N_{\mathfrak{m}}$ *is injective for all maximal ideals* $\mathfrak{m}$ *of* A.

The same statements hold with "injective" replaced by "surjective".

Proof. "(1)⇒(2)" Follows from exactness of S^{-1}.

"(2)⇒(3)" Clear.

"(3)⇒(1)" If $M' = \ker(f)$, then the sequence

$$0 \longrightarrow M' \longrightarrow M \xrightarrow{f} N$$

is exact. Localising at $\mathfrak{m}$ gives the exact sequence

$$0 \longrightarrow M'_{\mathfrak{m}} \longrightarrow M_{\mathfrak{m}} \xrightarrow{f_{\mathfrak{m}}} N_{\mathfrak{m}}\ .$$

By assumption, $M'_{\mathfrak{m}} = 0$, since $f_{\mathfrak{m}}$ is injective. Hence, $M' = 0$ by the previous proposition.

To prove the statements about surjectivity, reverse all the arrows. □

Proposition 4.11. *Let* M *be an* A*-module. Then the following are equivalent.*

(1) M *is a flat* A*-module.*

(2) $M_{\mathfrak{p}}$ *is a flat* $A_{\mathfrak{p}}$*-module for all prime ideals* $\mathfrak{p}$ *of* A.

(3) $M_{\mathfrak{m}}$ *is a flat* $A_{\mathfrak{m}}$*-module for all maximal ideals* $\mathfrak{m}$ *of* A.

Proof. "(1)⇒(2)" By Proposition 3.26, the module M is flat if and only if for any injective map $f\colon N \longrightarrow N'$ the induced map $N \otimes_A M \longrightarrow N' \otimes_A M$ is still injective. Then the claim follows from the previous proposition and the exactness of S^{-1}.

"(2)⇒(3)" Obvious.

"(3)⇒(1)" Let $N \longrightarrow N'$ be an A-linear map between A-modules and let $\mathfrak{m}$ be any maximal ideal of A. If $N \longrightarrow N'$ is injective, then $N_{\mathfrak{m}} \longrightarrow N'_{\mathfrak{m}}$ is injective by the previous proposition. It follows that $N_{\mathfrak{m}} \otimes_{A_{\mathfrak{m}}} M_{\mathfrak{m}} \longrightarrow N'_{\mathfrak{m}} \otimes_{A_{\mathfrak{m}}} M_{\mathfrak{m}}$ is injective by the flatness of $M_{\mathfrak{m}}$. By Proposition 4.8, the map $(N \otimes_A M)_{\mathfrak{m}} \longrightarrow (N' \otimes_A M)_{\mathfrak{m}}$ is injective, hence $N \otimes_A M \longrightarrow N' \otimes_A M$ is injective by the previous proposition. □

Here is a description of flatness over a local ring.

Proposition 4.12. *If* M *is a finitely generated flat module over a local ring* A*, then* M *is free.*

Proof. Let $\mathfrak{m}$ be the maximal ideal of A and $k = A/\mathfrak{m}$ the residue field. Let $x_1, \dots, x_n$ be a set of elements of M whose images in the vector space $M/\mathfrak{m}M$ form a linearly independent set. We want to show that the x_i are linearly independent. Assume that $\sum_i a_i x_i = 0$ for elements $a_1, \dots, a_n \in A$. These elements, written as a row vector, define a linear map $f\colon A^n \longrightarrow A$. Tensoring the exact sequence $0 \longrightarrow \ker(f) \longrightarrow A^n \longrightarrow A \longrightarrow 0$ with M and using the flatness of M, we get an exact sequence

$$0 \longrightarrow \ker(f) \otimes M \longrightarrow M^n \xrightarrow{f_M} M \longrightarrow 0,$$

where the map f_M sends a tuple $(m_1, \dots, m_n)$ to $\sum_i a_i m_i$. By our assumption,

$$(x_1, \dots, x_n) \in \ker(f_M) \simeq \ker(f) \otimes M,$$

hence $(x_1, \ldots, x_n) = \sum_{j=1}^{r} b_j \otimes y_j$ for some $r \in \mathbb{N}$ and elements $b_j = (b_{1j}, \ldots, b_{nj}) \in \ker(f)$, $y_j \in M$. At least one of the elements b_{ij} is not in $\mathfrak{m}$ (since the x_i give a linearly independent set in the quotient) and, without loss of generality, we can assume that $b_{11} \notin \mathfrak{m}$ and hence is invertible. Denote the inverse by z. From the equation $f(b_1) = \sum_i a_i b_{i1} = 0$ we get, setting $c_i = b_{i1}z$,

$$a_1 + a_2 b_{21} z + \ldots + a_n b_{n1} z = a_1 + a_2 c_1 + \ldots + a_n c_n = 0.$$

If $n = 1$, then $a_1 = 0$. If $n \geq 2$, then rewriting the equation $\sum_i a_i x_i = 0$ gives

$$a_2(x_2 - c_2 x_1) + \ldots + a_n(x_n - c_n x_1) = 0.$$

It follows by induction that the set $\{x_1, \ldots, x_n\}$ is lineary independent over A.

Now let $\{z_1, \ldots, z_n\}$ be a set of elements of M whose images in $M/\mathfrak{m}M$ form a basis, and let N be the submodule of M generated by the z_i. Then $N \otimes k \longrightarrow M \otimes k$ is an isomorphism, hence $M/N \otimes k \simeq 0$. Since $P \otimes A/I \simeq P/IP$ for any ideal I and any module P (tensor the exact sequence $0 \longrightarrow I \longrightarrow A \longrightarrow A/I \longrightarrow 0$ with P), it follows that $(M/N) \simeq \mathfrak{m}(M/N)$, hence $M/N \simeq 0$ by Nakayama's lemma. Therefore, M is a free module. □

In a somewhat similar vein we can prove the following result.

Proposition 4.13. *Let A be an integral domain and K its field of fractions. Then*

$$A = \bigcap_{\mathfrak{m} \in Y} A_{\mathfrak{m}},$$

where Y is the set of all maximal ideals of A and we take the intersection inside K.

Proof. Since all the maps $A \longrightarrow A_{\mathfrak{m}}$ are injective, the inclusion $\subseteq$ is clear. Conversely, let $x \in K$, so $x = \frac{a}{s}$ for non-zero elements a, s in A (the case $x = 0$ is trivial). If $x \in A_{\mathfrak{m}}$, then $s \notin \mathfrak{m}$, so $x \in \cap_{\mathfrak{m}} A_{\mathfrak{m}}$ if and only if $s \notin \mathfrak{m}$ for all maximal ideals of A. This means that s is a unit in A, so $x = s^{-1}a \in A$. □

We will now study the connection between ideals in A and ideals in the ring of fractions $S^{-1}A$ for some multiplicatively closed subset S. Denote by $f \colon A \longrightarrow S^{-1}A$ the canonical map. We already noted before that for any ring homomorphism $g \colon B \longrightarrow C$ the preimage $g^{-1}I =: I^c$ of an ideal I of C is an ideal of B, called *contracted ideal*. On the contrary, the image of an ideal J of B under g is not an ideal in general, but we can take the ideal J^e generated by it, called the *extended ideal*. It is clear that for any ideal I of C, we have $(g^{-1}I)^e = I^{ce} \subseteq I$.

Note that if I is an ideal in A, then I^e in $S^{-1}A$ is $S^{-1}I$. Indeed, if $y \in I^e$, then, by definition of I^e, $y = \sum_i \frac{a_i}{s_i}$ where $a_i \in I$ and $s_i \in S$. Bringing this to a common denominator proves the claim.

Proposition 4.14. *The following holds.*

1. *Every ideal in $S^{-1}A$ is an extended ideal.*
2. *If I is an ideal in A, then $f^{-1}(I^e) = I^{ec} = \bigcup_{s \in S}(I : s)$ (here we write $(I : s)$ for $(I : (s))$).*

(3) $I = f^{-1}J = J^c \iff$ *no element of* S *is a zero-divisor in* A/I.
(4) *The prime ideals of* $S^{-1}A$ *are in one-to-one correspondence with the prime ideals of* A *which do not meet* S.

Proof. (1) Let J be an ideal in $S^{-1}A$ and $\frac{a}{s} \in J$. Then $s\frac{a}{s} = \frac{a}{1} \in J$, so $a \in f^{-1}J$ and hence $\frac{a}{s} \in (f^{-1}J)^e$. Since $(f^{-1}J)^e \subseteq J$ in any case, we have proved the claim.

(2)

$$\begin{aligned} x \in f^{-1}(I^e) = f^{-1}(S^{-1}I) &\iff \exists a \in I, t \in S : \ \frac{x}{1} = \frac{a}{t} \\ &\iff \exists u \in S : \ (xt - a)u = 0 \\ &\iff xtu \in I \\ &\iff x \in \bigcup_{s \in S} (I : s) \end{aligned}$$

(3)

$$\begin{aligned} I = f^{-1}J \iff f^{-1}(I^e) \subseteq I &\iff (\exists s \in S : \ \ sx \in I \Rightarrow x \in I) \\ &\iff \text{no element of } S \text{ is a zero-divisor in } A/I \end{aligned}$$

(4) If $\mathfrak{q}$ is a prime ideal in $S^{-1}A$, then $f^{-1}\mathfrak{q}$ is a prime ideal in A. Conversely, if $\mathfrak{p}$ is a prime ideal in A, then $A/\mathfrak{p}$ is an integral domain. Denoting by $\overline{S}$ the image of S in $A/\mathfrak{p}$, we have $S^{-1}A/S^{-1}\mathfrak{p} \simeq \overline{S}^{-1}(A/\mathfrak{p})$. The latter ring is either 0 or contained in the field of fractions of $A/\mathfrak{p}$. In the latter case, $\overline{S}^{-1}(A/\mathfrak{p})$ is an integral domain, so $S^{-1}\mathfrak{p}$ is a prime ideal. Now $\overline{S}^{-1}(A/\mathfrak{p}) = 0$ if and only if $S^{-1}\mathfrak{p}$ is the unit ideal if and only if $\mathfrak{p} \cap S \neq \emptyset$ by (1).

□

Remark 4.15. We have proved earlier that if $f \in A$ is not nilpotent, then there exists a prime ideal which does not contain f. Let us given a new proof using localisation. If f is not nilpotent, then $S = (f^n)_{n \in \mathbb{N}}$ does not contain 0, so $S^{-1}A = A_f \neq 0$. Therefore, there exists a maximal ideal $\mathfrak{m}$ of A_f and takings its inverse image under the map $A \longrightarrow A_f$ gives a prime ideal $\mathfrak{p}$ which does not intersect S, hence $f \notin \mathfrak{p}$.

Corollary 4.16. *If* $\mathrm{rad}(0)$ *is the nilradical of* A*, then* $S^{-1}(\mathrm{rad}(0))$ *is the nilradical of* $S^{-1}A$.

Proof. We use that S^{-1} commutes with intersections and that the nilradical is the intersection of all prime ideals. □

Corollary 4.17. *The prime ideals of the local ring* $A_\mathfrak{p}$ *are in one-to-one correspondence with the prime ideals of* A *contained in* $\mathfrak{p}$.

Proof. Use (4) of Proposition 4.14 with $S = A \setminus \mathfrak{p}$. □

Remark 4.18. Note that if $\mathfrak{p}$ is a prime ideal in A, then the passage to $A/\mathfrak{p}$ cuts out all the prime ideals except for those containing $\mathfrak{p}$ while the passage to $A_\mathfrak{p}$ cuts out all

the prime ideals not contained in $\mathfrak{p}$. Therefore, if we have two prime ideals $\mathfrak{p}$ and $\mathfrak{q}$, then localising with respect to $\mathfrak{p}$ and taking the quotient with respect to $\mathfrak{q}$ (these two operations commute by Corollary 4.6) leaves us with the prime ideals between $\mathfrak{p}$ and $\mathfrak{q}$. Note that taking $\mathfrak{p} = \mathfrak{q}$, we get the *residue field at* $\mathfrak{p}$, which can be obtained as the field of fractions of $A/\mathfrak{p}$ or as the residue field of the local ring $A_\mathfrak{p}$.

Proposition 4.19. *Let M be a finitely generated A-module and S be a multiplicatively closed subset of A. Then $S^{-1}(\mathrm{Ann}(M)) = \mathrm{Ann}(S^{-1}M)$.*

Proof. We will first prove that if the statement holds for two modules M and N, then it also holds for their sum $M + N$:

$$\begin{aligned} S^{-1}(\mathrm{Ann}(M+N)) &= S^{-1}(\mathrm{Ann}(M) \cap \mathrm{Ann}(N)) \\ &= S^{-1}(\mathrm{Ann}(M)) \cap S^{-1}(\mathrm{Ann}(N)) \\ &= \mathrm{Ann}(S^{-1}M) \cap \mathrm{Ann}(S^{-1}N) \\ &= \mathrm{Ann}(S^{-1}M + S^{-1}N) = \mathrm{Ann}(S^{-1}(M+N)), \end{aligned}$$

where we used the easy to prove equality $\mathrm{Ann}(P+P') = \mathrm{Ann}P \cap \mathrm{Ann}P'$ in the first step and last step, Corollary 4.6 in the second step and the assumption in the third.

So we are reduced to proving the claim in the case where M is generated by a single element, hence $M \simeq A/I$, where $I = \mathrm{Ann}(M)$. Then $S^{-1}M = S^{-1}A/S^{-1}I$ by Corollary 4.6 again, so $\mathrm{Ann}(S^{-1}M) = S^{-1}I = S^{-1}\mathrm{Ann}(M)$. □

Proposition 4.20. *Let $f\colon A \longrightarrow B$ be a ring homomorphism and let $\mathfrak{p}$ be a prime ideal of A. Then $\mathfrak{p}$ is the contraction of a prime ideal of B if and only if $\mathfrak{p}^{ec} = \mathfrak{p}$.*

Proof. If $\mathfrak{p} = \mathfrak{q}^c$, then $\mathfrak{p}^{ec} = \mathfrak{q}^{cec} = \mathfrak{q}^c$, since for any ideal $I^{cec} = I^c$. Conversely, if $\mathfrak{p}^{ec} = \mathfrak{p}$, let $S = f(A \setminus \mathfrak{p})$ and note that $\mathfrak{p}^e \cap S = \emptyset$, hence the extension of $\mathfrak{p}^e$ in $S^{-1}B$ is a proper ideal and therefore contained in a maximal ideal $\mathfrak{m}$ of $S^{-1}B$. Defining $\mathfrak{q} = \mathfrak{m}^c$ in B, we note that $\mathfrak{q}$ is prime, contains $\mathfrak{p}^e$, hence $\mathfrak{q}^c \supseteq \mathfrak{p}^{ec} \supseteq \mathfrak{p}$, and satisfies the property that $\mathfrak{q} \cap S = \emptyset$, hence $\mathfrak{q}^c \subseteq \mathfrak{p}$. The claim follows. □

5. Chain conditions, Noetherian and Artin rings

In order to get nicer results, we will usually restrict ourselves to rings and modules satisfying some finiteness conditions.

To begin our discussion, let Σ be a set partially ordered by a relation $\leq$, that is, $\leq$ is reflexive and transitive and if $x \leq y$ and $y \leq x$, then $x = y$.

Proposition 5.1. *The following conditions on a partially ordered set Σ are equivalent.*

i) *Every increasing sequence $x_1 \leq x_2 \leq \ldots$ in Σ is stationary, which means that there is an index n such that $x_n = x_{n+1} = \ldots$*
ii) *Every non-empty subset of Σ has a maximal element.*

Proof. "i)⇒ii)": If there were a non-empty subset T of Σ without a maximal element, we could inductively construct an infinite strictly increasing sequence in T and hence in Σ.

"ii)⇒i)": The set $T = \{x_i \mid i \in \mathbb{N}\}$ has a maximal element. □

Definition. If M is an A-module and Σ is the set of submodules of M ordered by the relation $\subseteq$, then i) is called the *ascending chain condition* (a.c.c.) and ii) the *maximal condition*. If Σ is ordered by $\supseteq$, then i) is called the *descending chain condition* (d.c.c.) and ii) the *minimal condition*.

A module satisfying d.c.c. is called *Artin* and a module satisfying a.c.c. is called *Noetherian*.

Example 5.2.
(1) Any finite abelian group, which is a $\mathbb{Z}$-module, satisfies both d.c.c. and a.c.c.
(2) The ring $\mathbb{Z}$ satisfies a.c.c. but not d.c.c. To see the latter statement consider the sequence $(a) \supsetneq (a^2) \supsetneq (a^3) \supsetneq \dots$ for any $0 \neq a \in \mathbb{Z}$.
(3) If k is a field and $A = k[X]$, then A satisfies a.c.c. but not d.c.c. on ideals (similar proof as for $\mathbb{Z}$, using, e.g., X).
(4) The polynomial ring $k[X_1, X_2 \dots]$ satisfies neither a.c.c. nor d.c.c. The latter statement is clear, while for the former consider the sequence $(X_1) \subsetneq (X_1, X_2) \subsetneq (X_1, X_2, X_3) \subsetneq \dots$

Proposition 5.3. *Let* $0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$ *be an exact sequence of A-modules. Then*
(1) *M is Noetherian if and only if both M' and M'' are Noetherian.*
(2) *M is Artin if and only if both M' and M'' are Artin.*

In particular, the direct sum of finitely many Noetherian resp. Artin modules is again Noetherian respectively Artin.

Proof. We will prove the second statement since the first is very similar.

"⇒" Any descending chain of submodules of M' or M'' gives a descending chain of submodules of M which has to be stationary.

"⇐" If $M_1 \supseteq M_2 \supseteq \dots$ is a descending chain of submodules of M, then $(g(M_i))_i$ is a descending chain in M'' and $(f^{-1}(M_i))_i$ is a descending chain in M'. For some large index both these chains are stationary, hence so is the original chain.

To prove the last claim, use induction to reduce to the case of two modules M and N and then use the exact sequence $0 \longrightarrow M \longrightarrow M \oplus N \longrightarrow N \longrightarrow 0$. □

Definition. A ring A is *Noetherian* respectively *Artin* if it is so as an A-module, that is, it satisfies the a.c.c. respectively the d.c.c. condition on ideals.

Example 5.4. Any field is both Noetherian and Artin and so is any finite ring of the form $\mathbb{Z}/n\mathbb{Z}$. We have already seen that the integers are Noetherian but not Artin. More generally, any principal ideal domain is Noetherian, since every ideal is generated by one element.

The polynomial ring in a countable number of variables is neither Artin nor Noetherian. But it is a subring of a Noetherian ring, namely of its field of fractions.

Proposition 5.5. *Let A be a Noetherian (resp. Artin) ring. If M is a finitely generated A-module, then M is Noetherian (resp. Artin).*

Proof. If M is finitely generated, there exists a surjection from A^n, a Noetherian module, to M, hence the claim holds. The same proof works in the Artin case. □

5.1. **Noetherian rings and modules.**

Proposition 5.6. *A module M is Noetherian if and only if every submodule of M is finitely generated.*

Proof. Assume that M is Noetherian, let N be a submodule of M and Σ be the set of all finitely generated submodules of N. Then $0 \in \Sigma$, so Σ is non-empty and therefore Σ has a maximal element N_0. If $N_0 \neq N$, then for any $x \in N \setminus N_0$ the module $N_0 + Ax$ is finitely generated and is strictly bigger than N_0, a contradiction. Therefore, $N_0 = N$.

Now assume that every submodule of M is finitely generated. Let $M_1 \subseteq M_2 \subseteq \dots$ be an ascending chain of submodules of M. Set $N = \cup_i M_i$. This is a submodule of M, hence finitely generated. Writing $x_1, \dots, x_n$ for the generators, we have $x_i \in M_{n_i}$ for some indices n_i. Taking n to be the maximum over all the n_i, we get that $N = M_n$ is finitely generated. □

The statement of Proposition 5.6 can be strengthened for a ring A.

Proposition 5.7. *If all prime ideals of a ring A are finitely generated, then A is Noetherian.*

Proof. Let Σ be the set of ideals which are not finitely generated. If $\Sigma \neq \emptyset$, then it has a maximal element I by Zorn's lemma. Since I cannot be a prime ideal, there exist elements $x, y \in A$ such that $xy \in I$ but $x \notin I$ and $y \notin I$. Note that $I + Ay$ is an ideal which strictly contains I, hence is finitely generated, say by $(u_1 \dots, u_n, y)$ with $u_i \in I$. On the other hand, the ideal $(I : y) = \{a \in A \mid ay \in I\}$ contains x and, of course, I itself, hence is also bigger than I and therefore finitely generated with generators $(v_1, \dots, v_m)$. Now note that $I = \operatorname{span}(u_1, \dots, u_n, v_1 y, \dots, v_m y)$ (for instace, "$\supseteq$" is clear, since $v_j y \in I$ for all j and $u_i \in I$ for all i), so I is finitely generated, a contradiction to the assumption. Therefore, all ideals in A are finitely generated and hence A is Noetherian. □

Proposition 5.8. *Let A be a Noetherian ring.*

1. *If I is an ideal in A, then A/I is a Noetherian ring. In particular, if $f\colon A \twoheadrightarrow B$ is a surjective ring homomorphism, then B is Noetherian.*
2. *The ring $S^{-1}A$ is Noetherian for any multiplicatively closed subset S of A.*
3. *If A is a subring of B and B is finitely generated as an A-module, then B is Noetherian as a ring.*

Proof. (1) Just note that A/I is Noetherian as an A-module, hence also as an A/I-module. For the last statement use that $B \simeq A/\ker(f)$.

(2) By Proposition 4.14 the prime ideals in $S^{-1}A$ are in one-to-one correspondence with the prime ideals of A which do not meet S. Hence, all prime ideals in $S^{-1}A$ are finitely generated and therefore $S^{-1}A$ is Noetherian by Proposition 5.7. Alternatively use that all ideals in $S^{-1}A$ are extended ideals by Proposition 4.14 and that if $a_1, \dots, a_k$ generate an ideal I in A, then their images under the canonical map $A \longrightarrow S^{-1}A$ generate $S^{-1}I$.
(3) We know that B is Noetherian as an A-module, hence it is also Noetherian as a B-module. □

Sometimes taking a quotient of non-Noetherian ring produces a Noetherian ring.

Proposition 5.9. *Let A be a ring and M be a Noetherian A-module. Then the ring $A/\mathrm{Ann}M$ is a Noetherian ring.*

Proof. Set $\mathrm{Ann}M = I$, $B = A/I$ and note that M is also Noetherian as a B-module. Therefore, we can replace A by B and can assume that $I = 0$. Since M is finitely generated by, say, $(m_1, \dots, m_k)$, we can define an A-linear map $A \longrightarrow M^k$ by sending a to $(am_1, \dots, am_k)$, and this map is clearly injective. Therefore, A is a submodule of the Noetherian module M^k, so itself Noetherian as an A-module. □

We now come to Hilbert's Basis Theorem.

Theorem 5.10. *If A is a Noetherian ring, then $A[X]$ is a Noetherian ring.*

Proof. Let I be any ideal in $A[X]$. Consider the set J of all leading coefficients of polynomials in I and note that J is an ideal in A. Indeed, since I is an ideal, for every polynomial $f \in I$ the polynomial af is in I for any $a \in A$, so J is closed under scalar multiplication. If a is the leading coefficient of $f \in I$ and b is the leading coefficient of $g \in I$, then, assuming without loss of generality that $\deg(f) \geq \deg(g)$, we see that $a + b$ is the leading coefficient of $f + gX^{\deg(f)-\deg(g)} \in I$. As an ideal in a Noetherian ring J is finitely generated, say by $a_1, \dots, a_k$. For any i consider a polynomial $f_i = a_i X^{r_i} +$(terms of lower degree) in I with leading coefficient a_i. Clearly, the f_i generate an ideal I' which is contained in I. Set $r = \max\limits_{1 \leq i \leq k} r_i$.

Now take any element $f = aX^m +$(terms of lower degree) in I. Of course, $a \in J$, so write $a = \sum_{i=1}^k u_i a_i$ with $u_i \in A$. If $m \geq r$, then $f - \sum_i u_i f_i X^{m-r_i}$ is in I and has degree $< m$. In this way we can subtract elements from I' from f to get a polynomial g of degree $< r$. In other words, $f = g + h$ with $h \in I'$ and $\deg(g) < r$.

Consider the submodule M of $A[X]$ generated by $X^0, \dots, X^{r-1}$. The above equation $f = g + h$ translates into $I = (I \cap M) + I'$. Since M is a finitely generated A-module, it is Noetherian and so is its submodule $I \cap M$. If $I \cap M$ is generated by $g_1, \dots, g_l$, then I is generated by $g_1, \dots, g_l, f_1, \dots, f_k$. Therefore, I is finitely generated. □

Corollary 5.11. *If A is Noetherian, then $A[X_1, \dots, X_n]$ is Noetherian.*

Proof. Use induction, the theorem and the isomorphism $A[X_1, X_2] \simeq A[X_2][X_1]$. □

Corollary 5.12. *If A is Noetherian, then every finitely generated A-algebra B is Noetherian. In particular, every finitely generated algebra over a field is Noetherian.*

Proof. By assumption, B is a quotient of $A[X_1, \ldots, X_n]$ for some n. The latter ring is Noetherian by the previous corollary, and then so is B by Proposition 5.8. □

We can also say something about the ring of power series.

Theorem 5.13. *If A is Noetherian, then $A[[X]]$ is Noetherian.*

Proof. The proof is somewhat similar to the one given for $A[X]$. Consider an ideal I of $B = A[[X]]$. Define $I(r)$ to be the ideal of all leading coefficients a_r of $f = a_r X^r + \ldots$ as f runs through $I \cap X^r B$. Since for every $f \in I \cap X^r B$, we have $Xf \in I \cap X^{r+1} B$, we have a sequence

$$I(0) \subseteq I(1) \subseteq I(2) \subseteq \ldots$$

Since A is Noetherian, there is an index s such that $I(s + j) = I(s)$ for all $j \geq 0$. Furthermore, every $I(i)$ is finitely generated, say by a finite set of elements $a_{i\nu}$. For every $a_{i\nu}$ there is an element $g_{i\nu} \in I \cap X^i B$ having $a_{i\nu}$ as its leading coefficient. We claim that the set of these finitely many elements $g_{i\nu}$ generates I. To see this, let $f \in I$ be arbitrary. Then there exists a linear combination g_0 of the $g_{0\nu}$ such that $f - g_0 \in I \cap XB$. Continuing this, we get

$$f - g_0 - \ldots - g_s \in I \cap X^{s+1} B.$$

Since $I(s + 1) = I(s)$, there is a linear combination g_{s+1} of the elements $Xg_{s\nu}$ such that

$$f - g_0 - \ldots - g_s - g_{s+1} \in I \cap X^{s+2} B.$$

Proceed in the same way for $s + 2$ etc. For each $i \geq s$ we can write $g_i = \sum a_{i\nu} X^{i-s} g_{s\nu}$. Setting $h_\nu = \sum_{i=s}^{\infty} a_{i\nu} X^{i-s}$, we have

$$f = g_0 + \ldots + g_{s-1} + \sum_\nu h_\nu g_{s\nu}.$$ □

Definition. A *chain* of submodules of a module M is a finite sequence of submodules of the form

$$0 = M_n \subsetneq M_{n-1} \subsetneq \ldots \subsetneq M_1 \subsetneq M_0 = M.$$

The *length* of the chain is n. A *composition series* of M is a maximal chain, that is, a chain where every quotient module M_i/M_{i+1} is *simple* in the sense that its only submodules are 0 and itself.

Remark 5.14. An A-module M is simple if and only if it is generated by any $0 \neq m \in M$. Indeed if M is simple, take any $m \neq 0$ and consider the submodule $Am \subseteq M$. Since $Am \neq 0$, we have $Am = M$. Conversely, if $0 \neq M' \subseteq M$ is a submodule, then take an element $m' \in M'$. Since this is a non-zero element of M, we have $Am' = M \subseteq M'$.

Proposition 5.15. *If a module M has a composition series of length n, then every composition series has length n and every chain can be extended to a composition series.*

Proof. Write $l(M)$ for the length of a composition series of a module M and set $l(M) = \infty$ if no composition series exists.

We will first show that for a submodule N of M we have $l(N) \leq l(M)$ with equality if and only if $N = M$. Indeed, if $(M_i)_i$ is a composition series of M, then $(M_i) \cap N = N_i$ is a submodule in N for all i. Since $N \subseteq M$, we also have $N_i \subseteq M_i$ for all i and consequently $N_i/N_{i+1} \subseteq M_i/M_{i+1}$. Since the latter module is simple, N_i/N_{i+1} is either 0 or equal to M_i/M_{i+1}. If there is an index i_0 where the former occurs, hence $N_{i_0} = N_{i_0+1}$, then removing this factor (and others where repetition occurs) gives a composition series of N such that $l(N) < l(M)$. On the other hand, if $N_i/N_{i+1} \simeq M_i/M_{i+1}$ for all i, then $M_{l(M)-1} \simeq N_{l(m)-1}$, $M_{l(M)-2} \simeq N_{l(M)-2}$ and so forth, hence $N \simeq M$.

Using what we just proved, we can easily show that any chain in M has length at most $l(M)$. Indeed, if $M = M_1 \supsetneq M_2 \ldots$ is a chain of length k, then $l(M) > \ldots > l(M_{n-1}) = 1$. Since the length of a non-zero module is at least 1, the claim is proved.

Now consider any composition series of M and note that its length k is at most $l(M)$, hence has to be equal to $l(M)$. Therefore, all composition series have the same length.

Finally, consider any chain in M. If its length is $l(M)$, it is a composition series; if its length is strictly smaller than $l(M)$, then it is not maximal, so we can insert new terms to achieve length $l(M)$. □

Proposition 5.16. *A module M has a composition series if and only if it satisfies a.c.c. and d.c.c.*

Proof. "⇒": By the previous result, all chains in M have finite length.

"⇐": Since M satisfies a.c.c. it has a maximal submodule M_1. We then take a maximal submodule M_2 of M_1 and so forth. This gives a descending sequence $M_0 \supsetneq M_1 \supsetneq M_2 \supsetneq \ldots$ which has to terminate by the d.c.c., so M has a composition series. □

Remark 5.17. The length has the following property: For any short exact sequence

$$0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$$

of A-modules of finite length, we have $l(M) = l(M') + l(M'')$. Indeed, take a composition series of M' and its image under f and combine it with the preimage of a composition series of M'' to get a composition series of M.

Definition. Let A be a ring and M be an A-module. The *support* of M is defined to be the following subset of $\mathrm{Spec}(A)$:

$$\mathrm{Supp}(M) = \{\mathfrak{p} \in \mathrm{Spec}(A) \mid M_{\mathfrak{p}} \neq 0\}.$$

See Exercise 15 (Sheet 4, Exercise 3) for some properties of the support.

Theorem 5.18. *Let A be a ring and M be a module admitting a composition series. Then*

$$\mathrm{Supp}(M) = \{\mathfrak{m} \in \mathrm{Spec}(A) \mid \mathfrak{m} = \mathrm{Ann}(M_{i-1}/M_i) \text{ for some } i\},$$

all the prime ideals in the support of M are in fact maximal and there is a canonical isomorphism

$$\varphi\colon M \xrightarrow{\simeq} \prod_{\mathfrak{m}\in\mathrm{Supp}(M)} M_{\mathfrak{m}}.$$

The length $l(M_{\mathfrak{m}})$ of $M_{\mathfrak{m}}$ is equal to the number of i with $\mathfrak{m} = \mathrm{Ann}(M_{i-1}/M_i)$.

Proof. Let $\mathfrak{p}$ be an prime in A and

$$M = M_0 \supsetneq M_1 \supsetneq \ldots \supsetneq M_l = 0$$

be a composition series of M. By exactness of localisation, we get

$$M_{\mathfrak{p}} = M_0 \supseteq (M_1)_{\mathfrak{p}} \supseteq \ldots \supseteq (M_l)_{\mathfrak{p}} = 0.$$

Take any maximal ideal $\mathfrak{m}$. If $\mathfrak{p} = \mathfrak{m}$, then $(A/\mathfrak{m})_{\mathfrak{p}} = A/\mathfrak{m}$ by Corollary 4.6. If $\mathfrak{p} \neq \mathfrak{m}$, then there exists an element $x \in \mathfrak{m} \setminus \mathfrak{p}$, so $(A/\mathfrak{m})_{\mathfrak{p}} = 0$.

Now, for all i the module M_{i-1}/M_i is simple and therefore, by Exercise 22 (Exercise 2 on Sheet 6), it is of the form $A/\mathfrak{m}_i$, where $\mathfrak{m}_i = \mathrm{Ann}(M_{i-1}/M_i)$ is a maximal ideal. By Proposition 4.5, we have

$$(M_{i-1}/M_i)_{\mathfrak{p}} = (M_{i-1})_{\mathfrak{p}}/(M_i)_{\mathfrak{p}}.$$

This term is zero if $\mathfrak{p} \neq \mathfrak{m}_i$ and isomorphic to $A/\mathfrak{m}_i$ if $\mathfrak{p} = \mathfrak{m}_i$. It follows that (note that an $\mathfrak{m}_i$ can appear multiple times)

$$\mathrm{Supp}(M) = \{\mathfrak{m}_1, \ldots, \mathfrak{m}_k\}.$$

Looking at the localised filtration and omitting repeated terms, we get a composition series for $M_{\mathfrak{p}}$. By the above arguments, its length is precisely the number of i with $M_{i-1}/M_i = A/\mathfrak{p}$.

Finally, we investigate φ which clearly exists. It suffices to check that $\varphi_{\mathfrak{p}}$ is an isomorphism for every maximal ideal $\mathfrak{p}$. Since localisation commutes with finite products, we get

$$\varphi_{\mathfrak{p}}\colon M_{\mathfrak{p}} \longrightarrow \prod_{\mathfrak{m}} (M_{\mathfrak{m}})_{\mathfrak{p}} = \prod_{\mathfrak{m}} (M_{\mathfrak{m}})_{\mathfrak{p}} = M_{\mathfrak{p}},$$

because, again by the above arguments, $(M_{\mathfrak{m}})_{\mathfrak{p}} = 0$ if $\mathfrak{p} \neq \mathfrak{m}$ and $M_{\mathfrak{p}}$ is $\mathfrak{p} = \mathfrak{m}$. □

Proposition 5.19. *If V is a vector space over a field k, then the following conditions are equivalent.*

(1) *V is finite-dimensional.*
(2) *V has finite length.*
(3) *V satisfies a.c.c.*
(4) *V satisfies d.c.c.*

Proof. "(1)⇒"(2): Use that a vector space is simple if and only if it is one-dimensional.

"(2)⇒"(3), "(2)⇒"(4): By Proposition 5.16.

"(3)⇒"(1), "(4)⇒"(1): If V is not finite-dimensional, there are at least countably many linearly independent elements $e_1, e_2, \ldots$ in V. Consider, for $n \in \mathbb{N}$, the spaces

$U_n = \operatorname{span}(e_1, \dots, e_n)$ and $V_n = \operatorname{span}(e_{n+1}, e_{n+2}, \dots)$. Then the U_i form an infinite ascending sequence and the V_i form an infinite decreasing sequence contradicting (3) and (4), respectively. □

Corollary 5.20. *Let A be a ring in which the zero ideal is the product $\mathfrak{m}_1 \cdots \mathfrak{m}_k$ of finitely many not necessarily distinct maximal ideals. Then A is Noetherian if and only if A is Artin.*

Proof. Consider the sequence $A \supsetneq \mathfrak{m}_1 \supseteq \mathfrak{m}_1\mathfrak{m}_2 \supseteq \ldots \supseteq \mathfrak{m}_1 \cdots \mathfrak{m}_k = 0$ and note that ever factor $\mathfrak{m}_1 \cdots \mathfrak{m}_i / \mathfrak{m}_1 \cdots \mathfrak{m}_{i+1}$ is a vector space over the field $A/\mathfrak{m}_{i+1}$. Therefore, a.c.c ⇔ d.c.c for each factor. Using Proposition 5.3, this implies that a.c.c ⇔ d.c.c. for A. □

Example 5.21. If M is a Noetherian A-module and $f\colon M \twoheadrightarrow M$ is a surjective A-linear map, then f is an isomorphism. Indeed, note that there is an increasing sequence $\ker(f) \subseteq \ker(f^2) \subseteq \ldots$ By a.c.c. there exists an index n such that $\ker(f^n) = \ker(f^{n+1}) = \ldots$

Let $x \in \ker(f)$. Since f is surjective, $x = f(x_1)$, $x_1 = f(x_2)$ and so forth. Hence, $x = f^n(y)$ for some y. But $0 = f(x) = f^{n+1}(y) = f(f^n(y))$ and $\ker(f^n) = \ker(f^{n+1})$, so $f^n(y) = x = 0$ and f is injective.

Similarly, if M is Artin and f is injective, then it is an isomorphism. To see this, use the quotient modules $\operatorname{coker}(f^n)$.

5.2. **Artin rings.** We will now prove some results concerning Artin rings. Despite the formally quite similar definition, Artin rings turn out to be much simpler than Noetherian rings.

Proposition 5.22. *If A is an Artin ring, then every prime ideal in A is maximal.*

Proof. Let $\mathfrak{p}$ be a prime ideal in A and recall that $B = A/\mathfrak{p}$ is Artin by Proposition 5.5. Furthermore, B is an integral domain. Let $x \in B$ be a non-zero element. The descending sequence of ideals $(x) \supseteq (x^2) \ldots$ has to become stationary by d.c.c., hence there exists an index n such that $(x^n) = (x^{n+i})$ for all $i \geq 0$. In particular, $x^n = x^{n+1}y$ for some $y \in B$. Therefore, $x^n(1 - xy) = 0$, so $1 - xy = 0$, because B is an integral domain. Hence, x is a unit, so $B/\mathfrak{p}$ is a field, thus $\mathfrak{p}$ is a maximal ideal. □

Proposition 5.23. *An Artin ring has only finitely many maximal ideals.*

Proof. Consider the set of all finite intersections $\mathfrak{m}_1 \cap \ldots \cap \mathfrak{m}_k$ of maximal ideals. This set has a minimal element by d.c.c., say $\mathfrak{m}_1 \cap \ldots \cap \mathfrak{m}_n$. Then for any maximal ideal $\mathfrak{m}$ we have $\mathfrak{m} \cap \mathfrak{m}_1 \cap \ldots \cap \mathfrak{m}_n = \mathfrak{m}_1 \cap \ldots \cap \mathfrak{m}_n$, hence $\mathfrak{m}$ contains $\mathfrak{m}_1 \cap \ldots \cap \mathfrak{m}_n$. By Proposition 2.21, $\mathfrak{m} \supseteq \mathfrak{m}_i$ for some i. But both these ideals are maximal, so $\mathfrak{m} = \mathfrak{m}_i$. □

Remark 5.24. Recall that the spectrum of a ring is the set of all prime ideals. The above propositions in particular tell us that the spectrum of an Artin ring is a finite set.

Proposition 5.25. *In an Artin ring A the nilradical $\sqrt{0}$ is nilpotent.*

Proof. By d.c.c. there exists an index $k > 0$ such that $(\sqrt{0})^k = (\sqrt{0})^{k+l} = I$ for all $l \geq 0$. Suppose that $I \neq 0$ and consider Σ, the set of all ideals J such that $IJ \neq 0$. Then Σ is not empty since $I \in \Sigma$, so ordering Σ with respect to inclusion, it has a minimal element J_0. There exists $0 \neq x \in J_0$ such that $xI \neq 0$, that is, $(x) \in \Sigma$. Since the principal ideal (x) is contained in J_0, we have $(x) = J_0$ by minimality. Then $(xI)I = xI^2 = xI$, so $xI \in \Sigma$ and therefore $xI = (x)$, because $xI \subset (x)$ and $(x) = J_0$ is minimal. We conclude that there exists an element $y \in I$ such that $xy = x$. Iterating we get $xy^n = x$ for all $n \geq 1$. But $y \in (\sqrt{0})^k \subseteq \sqrt{0}$, hence y is nilpotent and $x = 0$. Therefore, $I = 0$. □

Proposition 5.26. *Any Artin ring A is Noetherian.*

Proof. There are only finitely many maximal ideals $\mathfrak{m}_1, \ldots, \mathfrak{m}_n$ in A. Write k for an index such that $(\mathrm{rad}0)^k = 0$. Then

$$\prod_{i=1}^{n} \mathfrak{m}_i^k \subseteq (\bigcap_{i=1}^{n} \mathfrak{m}_i)^k = (\mathrm{rad}0)^k = 0.$$

We conclude by Corollary 5.20 (recall that the maximal ideals whose product is the zero ideal were not required to be distinct). □

For the following major result, we will need an easy lemma.

Lemma 5.27. *Let A be an arbitrary ring and let I and J be ideals in A. Then*

(1) $\mathrm{rad}I = (1) \iff I = (1)$.
(2) $\mathrm{rad}(I + J) = \mathrm{rad}(\mathrm{rad}I + \mathrm{rad}J)$.
(3) *If* $\mathrm{rad}I$ *and* $\mathrm{rad}J$ *are coprime, then I and J are coprime.*

Proof. (1) If $I = (1)$, then of course $\mathrm{rad}(I) = (1)$. Conversely, $1 \in \mathrm{rad}I$ implies that $1 \in I$.
(2) "$\subseteq$" is clear since $I + J \subseteq \mathrm{rad}I + \mathrm{rad}J$. To see that "$\supseteq$" also holds, take an element x in the left hand side, so $x^n = a + b$ with $a \in \mathrm{rad}I$ and $b \in \mathrm{rad}J$. By definition $a^k \in I$ and $b^l \in J$ for some $k, l > 0$, so taking a sufficient power of both sides shows that $x^m \in I + J$ for some $m > 0$.
(3) Using (1) and (2) we have $\mathrm{rad}(I + J) = \mathrm{rad}(\mathrm{rad}I + \mathrm{rad}J) = \mathrm{rad}(1) = (1)$, so $I + J = (1)$. □

Proposition 5.28. *If A is an Artin ring, then A is isomorphic to a finite direct product of Artin local rings.*

Proof. As above, we know that $\prod_{i=1}^{n} \mathfrak{m}_i^k = 0$ for some $k > 0$, where $\mathfrak{m}_1, \ldots, \mathfrak{m}_n$ are the distinct maximal ideals of A. Now note that the radical of the ideal $\mathfrak{m}_i^k$ is $\mathfrak{m}_i$, so the radicals of the ideals in the product are pairwise coprime by maximality. By the above lemma, the ideals $\mathfrak{m}_i^k$ are pairwise coprime, hence $\prod_{i=1}^{n} \mathfrak{m}_i^k = \cap_{i=1}^{n} \mathfrak{m}_i^k$ by Proposition 2.20. The same proposition shows that $A \simeq \prod_{i=1}^{n} A/\mathfrak{m}_i^k$. Every factor in the product is an Artin local ring, hence the result. □

Remark 5.29. We will see later that the converse of the statement in the proposition also holds.

For future use, we recall the following notion.

Definition. Let X be a set. A *topology* on X is a collection of subsets $\sigma = \{U_j\}_{j\in J}$ satisfying the following properties a) $X \in \sigma$, b) $\emptyset \in \sigma$, c) any union of elements in σ is an element of σ and d) every finite intersection of elements of σ is an element in σ.

The elements of σ are the *open subsets* of the topology given by σ. The pair (X, σ) is called a *topological space*.

If $Y \subset X$ is a subset, then Y becomes a topological space by declaring a subset V to be open if $V = Y \cap U$ with $U \in \Sigma$.

Note that we can equivalently define a topology using closed subsets by taking complements. That is, to define a topology we can specify a family of closed subsets such that X and $\emptyset$ are closed, arbitrary intersections of closed subsets are closed and finite unions of closed subsets are closed.

Example 5.30. The space $\mathbb{R}^n$ becomes a topological space if we define a subset U to be open if for every $x \in U$ there exists an $r > 0$ such that $B_r(0) \subseteq U$.

Recall that $X = \mathrm{Spec}(A)$ is the set of all prime ideals in a ring A. Proposition 2.24 shows that the subsets $V(E)$ satisfy the axioms of a topology, called the *Zariski topology*.

Every set X becomes a topological space by declaring only X and $\emptyset$ to be open. This topology is usually called the trivial topology. The other extreme is obtained by declaring every subset of X to be open (or closed). In this case the resulting topological space is called discrete.

6. Primary decomposition

Definition. Let A be a ring. A proper ideal I in A is called *primary* if whenever $xy \in I$, then either $x \in I$ or $y^n \in I$ for some $n > 0$.

Remark 6.1. A prime ideal is primary.

A useful reformulation of the definition is the following: I is primary if and only if $A/I \neq 0$ and every zero divisor in A/I is nilpotent.

Also note that if $f\colon A \longrightarrow B$ is a ring homomorphism, then $f^{-1}I = I^c$ is primary if I is primary.

Proposition 6.2. *If I is a primary ideal in A, then* rad$I$ *is the smallest prime ideal containing I.*

Proof. Since the radical of I is the intersection of all prime ideals containing I, it is enough to show that $\mathfrak{p} = \mathrm{rad}I$ is a prime ideal. So let $xy \in \mathfrak{p}$. By definition, $(xy)^m \in I$ for some $m > 0$, so either $x^m \in I$ or $y^{mk} \in I$ for some $k > 0$. Hence, either $x \in \mathfrak{p}$ or $y \in \mathfrak{p}$. □

Definition. If I is a primary ideal with rad$I = \mathfrak{p}$, we will call I $\mathfrak{p}$*-primary*.

Example 6.3. (1) If $A = \mathbb{Z}$, then the primary ideals in A are (0) and (p^n) for p a prime number and $n > 0$.

(2) If $A = k[X, Y]$ and $I = (X^3, Y)$. Then $A/I \simeq k[X]/(X^3)$ in which all zero divisors are nilpotent because they are multiples of X. Therefore, I is primary. Its radical is $\mathfrak{p} = (X, Y)$. Note that I is not a power of $\mathfrak{p}$.

(3) A power of a prime ideal need not be primary. Let $A = k[X, Y, Z]/(XY - Z^2)$. Denote by $\overline{X}$, $\overline{Y}$ and $\overline{Z}$ the images of X, Y and Z in A, respectively. The ideal $\mathfrak{p} = (\overline{X}, \overline{Z})$ is prime in A, since $A/\mathfrak{p} \simeq k[Y]$ and the latter is an integral domain. Note that $\overline{XY} = \overline{Z}^2 \in \mathfrak{p}^2$, but $\overline{X} \notin \mathfrak{p}^2$ and $\overline{Y} \notin \mathrm{rad}\mathfrak{p}^2 = \mathfrak{p}$. Therefore, $\mathfrak{p}^2$ is not primary.

Proposition 6.4. *If* $\mathrm{rad}I$ *is a maximal ideal, then* I *is primary. In particular, the powers of a maximal ideal are primary.*

Proof. Since $\mathrm{rad}I$ is the nilradical of A/I, every element of A/I is either a unit or nilpotent, so the latter ring has only one prime ideal. □

Our next goal is to study the question when an ideal can be written as an intersection of primary ideals. We will need the following results.

Lemma 6.5. *If the ideals* I_k *are* $\mathfrak{p}$*-primary for* $1 \leq k \leq n$*, then* $I = \cap_k I_k$ *is* $\mathfrak{p}$*-primary.*

Proof. We compute the radical: $\mathrm{rad}(I) = \mathrm{rad}(\cap_k I_k) = \cap_k \mathrm{rad}I_k = \mathfrak{p}$. If $xy \in I$, $y \notin I$, then for some index k_0 we have $xy \in I_k$ but $y \notin I_k$, hence $x \in \mathfrak{p} = \mathrm{rad}I_k = \mathrm{rad}I$. □

Lemma 6.6. *Let* I *be a* $\mathfrak{p}$*-primary ideal and let* $x \in A$*. Then the following holds.*

(1) *If* $x \in I$*, then* $(I : x) = (1)$.
(2) *If* $x \notin I$*, then* $(I : x)$ *is* $\mathfrak{p}$*-primary and therefore* $\mathrm{rad}(I : x) = \mathfrak{p}$.
(3) *If* $x \notin \mathfrak{p}$*, then* $(I : x) = I$.

Proof. (1) We recall that $(I : x) = \{a \in A \mid ax \in I\}$. Hence, $1 \in I$.

(2) Consider an element $y \in (I : x)$, so $yx \in I$. Since $x \notin I$, we have $y \in \mathfrak{p} = \mathrm{rad}I$. Therefore we have inclusions $I \subseteq (I : x) \subseteq \mathfrak{p}$. Taking radicals we see that $\mathrm{rad}(I : x) = \mathfrak{p}$. To check that $(I : x)$ is $\mathfrak{p}$-primary, assume that $yz \in (I : x)$ with $y \notin \mathfrak{p}$, so $yzx \in I$, hence $zx \in I$, thus $z \in (I : x)$.

(3) Since I is $\mathfrak{p}$-primary, $ax \in I$ and $x \notin \mathfrak{p}$ implies that $a \in I$. □

Definition. A *primary decomposition* of an ideal I in a ring A is an expression of I as a finite intersection of primary ideals J_k:

$$I = \cap_{k=1}^{n} J_k.$$

If the radicals of the J_k are distinct and $\cap_{k \neq l} J_k \nsubseteq J_l$ for $1 \leq l \leq n$, the primary decomposition is said to be *minimal*.

An ideal is said to be *decomposable* if it admits a primary decomposition.

In general, a primary decomposition need not exist. We will see below that it does exist for ideals in Noetherian rings. Also note that by Lemma 6.5 we can achieve that

all radicals are distinct and we can reduce any primary decomposition to a minimal one by omitting superfluous terms.

Theorem 6.7. *Let I be a decomposable ideal and let $I = \cap_{k=1}^{n} J_k$ be a minimal primary decomposition of I. Then the radicals $\mathfrak{p}_k = \mathrm{rad} J_k$ for $1 \leq k \leq n$ are precisely the prime ideals which occur in the set of ideals $\mathrm{rad}(I : x)$ (where x runs through all elements of A) and hence the $\mathfrak{p}_k$ are independent of the particular decomposition of I.*

Proof. Note that, for any $x \in A$, we have

$$(I : x) = (\cap_k J_k \colon x) = \{a \mid ax \in \cap_k J_k\} = \cap_k (J_k \colon x).$$

Therefore, $\mathrm{rad}(I : x) = \cap_k \mathrm{rad}(J_k : x)$. By the items (1) and (2) of the previous lemma, we then get $\mathrm{rad}(I : x) = \cap_{l \colon x \notin J_l} \mathfrak{p}_l$. If $\mathrm{rad}(I : x)$ is prime, then $\mathrm{rad}(I : x) = \mathfrak{p}_l$ for some l by Proposition 2.21.

Conversely, for each index k_0 there exists, by mimimality, an element x such that $x \notin J_{k_0}$ but $x \in \cap_{k \neq k_0} J_k$. It follows that $\mathrm{rad}(I : x) = \mathfrak{p}_{k_0}$. □

Definition. Let I be a decomposable ideal and $I = \cap_{k=1}^{n} J_k$ a minimal primary decomposition of I. The radicals $\mathfrak{p}_k = \mathrm{rad} J_k$ are called the *AM-associated prime ideals* of I.

The minimal elements of the set of the AM-associated prime ideals are called the *minimal* or *isolated* prime ideals; the others are called *embedded* prime ideals.

Clearly, an ideal I is primary if and only if it has only one AM-associated prime ideal, namely its radical.

Example 6.8. Let $A = k[X, Y]$ and $I = (X^2, XY)$. Setting $\mathfrak{p}_1 = (X)$ and $\mathfrak{p}_2 = (X, Y)$, we have $\mathfrak{p}_2^2 = (X^2, XY, Y^2)$, so $I = \mathfrak{p}_1 \cap \mathfrak{p}_2^2$. Since $\mathrm{rad}\mathfrak{p}_2^2 = \mathfrak{p}_2$ is maximal, the ideal $\mathfrak{p}_2$ is primary and so is the prime ideal $\mathfrak{p}_1$. Here, $\mathfrak{p}_1$ is minimal while $\mathfrak{p}_2$ is an embedded prime ideal. Note that I is not primary but its radical is $\mathfrak{p}_1$, hence prime.

Proposition 6.9. *If I be a decomposable ideal, then any prime ideal $I \subseteq \mathfrak{p}$ contains a minimal prime ideal AM-associated with I. Hence, the isolated prime ideals of I are the minimal elements in the set of all prime ideals containing I.*

Proof. Let $I = \cap_k J_k$, then $\mathrm{rad}(\cap_k J_k) = \cap_k \mathrm{rad}(J_k) \subseteq \mathrm{rad}\mathfrak{p} = \mathfrak{p}$. Hence $\mathfrak{p}$ contains one of the $\mathrm{rad}(J_k)$ by Proposition 2.21. □

Proposition 6.10. *If I is a decomposable ideal and $I = \cap_k J_k$ a minimal primary decomposition with $\mathrm{rad} J_k = \mathfrak{p}_k$, then*

$$\bigcup_k \mathfrak{p}_k = \{a \in A \mid (I : a) \neq I\}.$$

In particular, if the zero ideal is decomposable, then the set of all zero divisors of A is precisely the union over the prime ideals AM-associated with the zero ideal.

Proof. First note that if $f\colon A \longrightarrow A/I$ is the canonical ring homomorphism and $J_k =: J$ in A appears in the primary decomposition of I, then $f(J)$ is also primary. Indeed, let $f(a)f(a') = f(j)$ with $j \in J$, then $aa' - j \in I$, so $aa' \in J$ and hence either $f(a) \in f(J)$ or $f(a'^n) = f(a')^n \in f(J)$. Therefore, the zero ideal in A/I is decomposable and we reduce to proving the last statement of the proposition.

Writing D for the set of zero divisors, we have, by Proposition 2.23,

$$D = \cup_{0\neq x\in A}\mathrm{rad}(\mathrm{Ann}(x)) = \cup_{0\neq x\in A}\mathrm{rad}(0:x).$$

On the other hand, we have seen above that for any $x \in A$ we have $\mathrm{rad}(0:x) = \cap_{k:\, x\notin J_k}\mathfrak{p}_k \subset \mathfrak{p}_l$ for some l; hence, $D \subseteq \cup_{k=1}^n \mathfrak{p}_k$. Conversely, each $\mathfrak{p}_k$ is of the form $\mathrm{rad}(0:x)$ for some $x \in A$, hence the other inclusion also holds. □

Corollary 6.11. *If the zero ideal is decomposable, then the set of all zero divisors is the union of all prime ideals AM-associated with* 0 *and the set of nilpotent elements is the intersection of all minimal prime ideals AM-associated with* 0. □

Proposition 6.12. *Let S be a multiplicatively closed subset of A and let J be $\mathfrak{p}$-primary ideal. Then the following holds:*

1. *If $S \cap \mathfrak{p} \neq \emptyset$, then $S^{-1}J = S^{-1}A$.*
2. *If $S \cap \mathfrak{p} = \emptyset$, then $S^{-1}J$ is $S^{-1}\mathfrak{p}$-primary and its contraction in A is J.*

Proof. (1) The condition $S\cap\mathfrak{p} \neq \emptyset$ implies that $\mathfrak{p}$ contains an element which becomes a unit in $S^{-1}A$. Since $\mathfrak{p} = \mathrm{rad}J$, it follows that $S^{-1}J$ contains a unit.

(2) If $s \in S$ and $a \in (J : s)$, i.e. $as \in J$, then $a \in J$, since $S\cap\mathfrak{p} = \emptyset$. Hence, $J^{ec} = J$ by Proposition 4.14. By the same proposition, $\mathrm{rad}(J^e) = \mathrm{rad}(S^{-1}J) = S^{-1}\mathrm{rad}(J) = \mathfrak{p}$. To show that $S^{-1}J$ is primary, we need to show that $S^{-1}A/S^{-1}J \simeq S^{-1}(A/J)$ is non-zero and has the property that every zero divisor is nilpotent. But this immediately follows from the corresponding statements for A/J.

□

Remark 6.13. Using Proposition 4.14(3), we see that primary ideals correspond to primary ideals under the correspondence between ideals in $S^{-1}A$ and contracted ideals in A.

Proposition 6.14. *Let S be a multiplicatively closed subset of A and let I be a decomposable ideal with a minimal primary decomposition $I = \cap_{k=1}^n J_k$. Write $\mathfrak{p}_k = \mathrm{rad}J_k$ and suppose that S does not meet $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$, but does meet $\mathfrak{p}_{m+1}, \ldots, \mathfrak{p}_n$. Then we have the minimal primary decompositions*

$$S^{-1}I = \bigcap_{k=1}^{m} S^{-1}J_k, \quad (S^{-1}I)^c = \bigcap_{k=1}^{m} J_k.$$

Proof. Since S^{-1} commutes with intersections, we have

$$S^{-1}I = \cap_{k=1}^n S^{-1}J_k.$$

By (1) of the previous proposition, $S^{-1}J_k = S^{-1}A$ for all $k > m$. Therefore, $S^{-1}I = \cap_{k=1}^{m} S^{-1}J_k$ and the $S^{-1}J_k$ are $S^{-1}\mathfrak{p}_k$-primary by (2) of the previous proposition. The decomposition is minimal because the $\mathfrak{p}_k$ are all distinct, hence so are the $S^{-1}\mathfrak{p}_k$ for $1 \leq k \leq m$. Taking the preimage under the canonical map $A \longrightarrow S^{-1}A$ we get

$$(S^{-1}I)^c = (\bigcap_{k=1}^{m} S^{-1}J_k)^c = \bigcap_{k=1}^{m} (S^{-1}J_k)^c = \bigcap_{k=1}^{m} J_k,$$

where we one again used the previous proposition for the last equality. □

Definition. Let I be a decomposable ideal. A set Σ of prime ideals AM-associated with I is called *isolated* if the following condition is satisfied: if $\mathfrak{p}'$ is AM-associated with I and $\mathfrak{p}' \subseteq \mathfrak{p}$ for some $\mathfrak{p} \in \Sigma$, then $\mathfrak{p}' \in \Sigma$.

For example, the set consisting of the isolated prime ideals is an isolated set.

Now, if Σ is an isolated set of prime ideals, set $S = A \setminus \cup_{\mathfrak{p}\in\Sigma}\mathfrak{p}$. Then S is a multiplicatively closed subset and we have the following statements

$$\mathfrak{p}' \in \Sigma \Longrightarrow \mathfrak{p}' \cap S = \emptyset$$
$$\mathfrak{p}' \notin \Sigma \Longrightarrow \mathfrak{p}' \not\subseteq \cup_{\mathfrak{p}\in\Sigma}\mathfrak{p} \Longrightarrow \mathfrak{p}' \cap S \neq \emptyset,$$

where we used Proposition 2.21 in the second line.

Theorem 6.15. *Let I be a decomposable ideal and $I = \cap_{k=1}^{n} J_k$ a minimal primary decomposition. Furthermore, let $\{\mathfrak{p}_{i_1}, \ldots, \mathfrak{p}_{i_m}\}$ be an isolated set of prime ideals of I. Then $J_{i_1} \cap \ldots \cap J_{i_m}$ is independent of the decomposition.*

Proof. Setting $S = A \setminus \mathfrak{p}_{i_1} \cup \ldots \cup \mathfrak{p}_{i_m}$, we have $(S^{-1}I)^c = J_{i_1} \cap \ldots \cap J_{i_m}$ by the previous proposition. Since the $\mathfrak{p}_i$ depend only on I, so does this intersection. □

Corollary 6.16. *The primary components corresponding to the isolated prime ideals are uniquely determined by I.* □

To summarise the two major results of this section: If I is decomposable, then the radicals of the primary ideals appearing in a minimal primary decomposition, i.e. the primes AM-associated with I, are uniquely determined. Furthermore, the primary ideals belonging to an isolated set of AM-associated prime ideals are also uniquely determined.

Remark 6.17. Not all the primary components are uniquely determined. For example, let $A = k[X, Y]$ and let $I = (X^2, XY)$. Then $I = (X, Y)^2 \cap (X) = (X) \cap (X^2, Y)$. Of course, the radicals of both components, namely (X) and (X, Y) are uniquely determined. But, as we can see, only the primary component belonging to the isolated prime ideal (X) is determined by I.

6.1. **Primary decompositions in Noetherian rings.** In the following we will apply the above results to Noetherian rings.

Definition. An ideal I in a ring is called *irreducible* if $I = J \cap K$ implies that $I = J$ or $I = K$.

Lemma 6.18. *Every ideal in a Noetherian ring is a finite intersection of irreducible ideals.*

Proof. If the set of all ideals for which the lemma does not hold is non-empty, then it has a maximal element I. Since I cannot be irreducible, we can write it as $I = J \cap K$, where $I \subsetneq J$ and $I \subsetneq K$. By maximality, J and K can be written as a finite intersection of irreducible ideals, hence the same holds for I, contradiction. □

Lemma 6.19. *If A is a Noetherian ring, then every irreducible ideal I is primary.*

Proof. We can reduce to proving the statement for the zero ideal by passing to the quotient ring A/I. So, assume that $xy = 0$ with $x \neq 0$ and consider the chain of ideals $\mathrm{Ann}(y) \subseteq \mathrm{Ann}(y^2) \subseteq \ldots$ Since A is Noetherian, there is an index n such that $\mathrm{Ann}(y^n) = \mathrm{Ann}(y^{n+j})$ for all $j \geq 0$. Then $(y^n) \cap (x) = 0$. Indeed, any element $z \in (x)$ satisfies $zy = 0$, so if z is also in (y^n), then $z = ay^n$, so $ay^{n+1} = 0$, hence $a \in \mathrm{Ann}(y^{n+1}) = \mathrm{Ann}(y^n)$, so $ay^n = z = 0$. By the irreducibility of the zero ideal, we must have $(y^n) = 0$, hence y is nilpotent and the zero ideal is primary. □

Theorem 6.20. *If A is a Noetherian ring, then every ideal has a primary decomposition.*

Proof. Any ideal is a finite intersection of irreducible ideals which are primary. □

Proposition 6.21. *In a Noetherian ring every ideal I contains a power of its radical. In particular, the nilradical is nilpotent.*

Proof. Let $J = \mathrm{rad}I$ be generated by $x_1, \ldots, x_k$, hence there exist integers n_i such that $x_i^{n_i} \in I$ for $1 \leq i \leq k$. Setting $n = \sum_{l=1}^{k}(n_l - 1) + 1$, it follows that J^n is generated by the products $x_1^{r_1} \cdots x_k^{r_k}$ with $\sum r_i = n$ and by our choice of n there is at least one index l_0 such that $r_{l_0} \geq n_{l_0}$ (if $r_l < n_l$ for all l, then $r_l \leq n_l - 1$ for all l), hence every product is contained in I, so $(\mathrm{rad}I)^n \subseteq I$. □

Corollary 6.22. *If A is a Noetherian ring, $\mathfrak{m}$ a maximal ideal in A and I any ideal in A, then the following conditions are equivalent*

i) *I is $\mathfrak{m}$-primary.*
ii) $\mathrm{rad}I = \mathfrak{m}$.
iii) $\mathfrak{m}^n \subseteq I \subseteq \mathfrak{m}$ *for some $n > 0$.*

Proof. "i)⇒ii)": Clear.
"ii)⇒i)": Proposition 6.4.
"ii)⇒iii)": Previous proposition.
"iii)⇒ii)": Take radicals. □

6.2. **Application to Artin rings.** We can also use primary decompositions to prove a structure theorem for Artin rings.

Theorem 6.23. *An Artin ring A is, up to isomorphism, uniquely a finite direct product of Artin local rings.*

Proof. The statement that an Artin ring is a finite product of Artin local rings is precisely the statement of Proposition 5.28.

Conversely, suppose that A is a product of Artin local rings A_k for $1 \leq k \leq n$. Note that A is an Artin ring. Let $I_k = \ker(p_k)$ where $p_k \colon A \longrightarrow\!\!\!\!\rightarrow A_k$ is the canonical projection. Since $A \simeq \prod_k A_k$, the ideals I_k are coprime and $\cap_k I_k = 0$. Since A_k is Artin and local for each k, it possesses exactly one prime ideal, which we will call $\mathfrak{p}_k$. Let $\mathfrak{q}_k = p_k^{-1}(\mathfrak{p}_k)$. Since contractions of prime ideals are prime, $\mathfrak{q}_k$ is a prime ideal in A, hence maximal because A is Artin. Furthermore, since A_k is Artin, it is also Noetherian, hence the nilradical, which is $\mathfrak{p}_k$, is nilpotent for all k. This implies that I_k is $\mathfrak{q}_k$-primary for all k, so $\cap_k I_k = (0)$ is a primary decomposition of the zero ideal of A. Now the ideals I_k are coprime, hence so are the $\mathfrak{q}_k$, hence they are the isolated prime ideals of (0). It follows that all the primary components I_k are isolated, hence uniquely determined by A, see Theorem 6.15. Therefore, the rings $A_k \simeq A/I_k$ are uniquely determined by A. □

6.3. **Some geometry.** We now want to interpret the results concerning primary decompositions geometrically. We will, in particular, require the following notion.

Definition. A topological space X is called *irreducible* if every pair of non-empty open sets in X intersects.

Equivalently, X is irreducible if it cannot be written as a union of two proper closed subsets.

Proposition 6.24. *The topological space* $X = \operatorname{Spec}(A)$ *is irreducible if and only if* $\operatorname{rad}(0)$ *is a prime ideal. In particular, if* $\mathfrak{p} \in \operatorname{Spec}(A)$*, then* $V(\mathfrak{p})$ *is an irreducible closed subset of* $\operatorname{Spec}(A)$*.*

Proof. "⇒" Assume that $\operatorname{rad}(0)$ is not a prime ideal, so there exist $a, b \in A$ such that 1) $ab \in \operatorname{rad}(0)$ and 2) $a \notin \operatorname{rad}(0)$, $b \notin \operatorname{rad}(0)$. The latter condition implies that there are prime ideals $\mathfrak{p}_a$, $\mathfrak{p}_b$ such that $a \notin \mathfrak{p}_a$ and $b \notin \mathfrak{p}_b$, so $V(a) \subsetneq X$, $V(b) \subsetneq X$. Since $\operatorname{rad}(0)$ is the intersection of all prime ideals in A, the first condition implies that $X = V(a) \cup V(b)$ so X is not irreducible.

"⇐" Conversely, if X is not irreducible, then $X = V(I) \cup V(J)$ for some ideals I and J and there exist prime ideals $\mathfrak{p}_I$ and $\mathfrak{p}_J$ such that $I \nsubseteq \mathfrak{p}_I$ and $J \nsubseteq \mathfrak{p}_J$, so there are elements $i \in I$, $i \notin \mathfrak{p}_I$ and $j \in J$, $j \notin \mathfrak{p}_J$. Therefore, $i \notin \operatorname{rad}(0)$ and $j \notin \operatorname{rad}(0)$. On the other hand, the product ij is contained in $IJ \subseteq I \cap J$, hence in every prime ideal, hence in $\operatorname{rad}(0)$, which is therefore not a prime ideal. □

If V is any subset of a topological space X, we define its *closure* $\overline{V}$ as the smallest closed subset containing V. Clearly, $\overline{V}$ is the intersection of all the closed subsets containing V. Of course, $V = \overline{V}$ if and only if V is closed.

It is easily checked that a set V is irreducible if and only if its closure $\overline{V}$ is irreducible (use that taking the closure commutes with finite unions).

Furthermore, it is an application of Zorn's lemma that any irreducible subset of a topological space is contained in a maximal irreducible subset.

Combining the two facts we have: The maximal irreducible subsets of a topological space X are closed and their union is X. The maximal irreducible subsets of X are called the *irreducible components of* X.

Lemma 6.25. *Let A be a non-zero ring. Then the set of prime ideals of A has minimal elements with respect to inclusion. Furthermore, if $I \neq (1)$ is any ideal in A, then the set of primes containing I has minimal elements.*

Proof. We want to apply Zorn's lemma. Let $(\mathfrak{p}_i)_{i\in I}$ be a chain of primes ordered by "$\supseteq$". Then $\cap_i \mathfrak{p}_i$ is a prime ideal, hence an upper bound for the chain. Therefore, Zorn's lemma gives the existence of minimal prime ideals.

The second claim follows by applying the first to A/I. □

Proposition 6.26. *The irreducible components of $X = \mathrm{Spec}(A)$ are the closed subsets $V(\mathfrak{p})$, where $\mathfrak{p}$ is a minimal prime ideal of A.*

Proof. Note that any point y in a topological space Y is irreducible, hence so is its closure. Also note that the closure of a point $x \in X$ which corresponds to a prime ideal $\mathfrak{p}_x$ is precisely $V(\mathfrak{p}_x)$. Indeed, let $V(I)$ be any closed subset containing x. Then $I \subseteq \mathfrak{p}_x$, hence $V(\mathfrak{p}_x) \subseteq V(I)$, that is, $V(\mathfrak{p}_x)$ is the smallest closed subset containing x. Combining the statements we just proved, we see that $V(\mathfrak{p})$ is an irreducible closed subset for any prime ideal. If $\mathfrak{p}$ is minimal, then $V(\mathfrak{p})$ is a maximal irreducible subset, hence an irreducible component, and conversely. □

Proposition 6.27. *If an ideal I has a primary decomposition, then $V(I) = \mathrm{Spec}(A/I)$ has only finitely many irreducible components. In particular, the statement holds for any ideal in a Noetherian ring.*

Proof. There are finitely many minimal primes AM-associated with I. □

6.4. **Associated primes.**

Definition. Let M be an A-module. A prime ideal $\mathfrak{p}$ is *associated* with M if $\mathfrak{p} = \mathrm{Ann}(m) = \{a \in A \mid am = 0\}$ for some $0 \neq m \in M$. The set of all associated primes of M is denoted by $\mathrm{Ass}M$.

If I is an ideal in A, then the associated primes of I are defined to be the associated primes of the module A/I.

Remark 6.28. Note that is follows from Theorem 6.7 that an AM-associated prime ideal is one which is the *radical* of $\mathrm{Ann}(m)$ for some $0 \neq m$. Clearly, any associated prime ideal is also AM-associated, since $\mathfrak{p} = \mathrm{Ann}(m)$ implies $\mathrm{rad}\mathfrak{p} = \mathfrak{p} = \mathrm{radAnn}(m)$. We will see in Proposition 6.38 that for Noetherian rings the two notions "associated" and "AM-associated" coincide.

Proposition 6.29. *Let A be a Noetherian ring. Then an A-module M is zero if and only if $\mathrm{Ass}M = \emptyset$.*

Proof. Clearly, if $M = 0$, then $\mathrm{Ass}M = \emptyset$.

Conversely, if $M \neq 0$, then consider the set $\mathcal{F} = \{\mathrm{Ann}(m) \mid m \neq 0\}$ of all annihilators of non-zero elements of M. If $\mathcal{F}$ has a maximal element $\mathfrak{p} = \mathrm{Ann}(m)$, then $\mathfrak{p}$ is a prime ideal. Clearly, $\mathfrak{p} \neq A$, since $1 \notin \mathfrak{p}$ ($m \neq 0$). Assume that $ab \in \mathfrak{p}$, so $abm = 0$. If $a \notin \mathfrak{p}$, then $am \neq 0$. Hence, $\mathfrak{p} \subseteq \mathrm{Ann}(am)$. We have $b \in \mathrm{Ann}(am)$ and, by maximality, we have $\mathfrak{p} = \mathrm{Ann}(am)$, so $b \in \mathfrak{p}$. We are now done, because A is Noetherian and, therefore, $\mathcal{F}$ has at least one maximal element. □

Proposition 6.30. *Let M be an A-module. Then $\mathfrak{p} \in \mathrm{Ass}M \iff \exists A/\mathfrak{p} \hookrightarrow M$. In particular, if N is a submodule of M, then $\mathrm{Ass}N \subseteq \mathrm{Ass}M$.*

Proof. If $\mathfrak{p} \in \mathrm{Ass}(M)$, then $\mathfrak{p} = \mathrm{Ann}(m)$ for some $0 \neq m$. Define $f\colon A \longrightarrow M$ by $a \longmapsto am$. Then $\mathfrak{p} = \ker(f)$, hence $A/\mathfrak{p} \hookrightarrow M$. Conversely, if $f\colon A/\mathfrak{p} \hookrightarrow M$ is injective, set $m = f(\overline{1})$, then $\mathfrak{p} = \mathrm{Ann}(m)$. □

Proposition 6.31. *If $\mathfrak{p}$ is prime, then $\mathrm{Ass}A/\mathfrak{p} = \{\mathfrak{p}\}$.*

Proof. By the previous proposition, $\mathfrak{p} \in \mathrm{Ass}A/\mathfrak{p}$. If $\mathrm{Ann}(m) = \mathfrak{q} \in \mathrm{Ass}A/\mathfrak{p}$ for some $0 \neq m \in A/\mathfrak{p}$, then $m \notin \mathfrak{p}$, but for any $x \in \mathfrak{q}$ we have $xm \in \mathfrak{p}$, so $x \in \mathfrak{p}$. Since clearly $\mathfrak{p} \subseteq \mathfrak{q}$, we have equality. □

There is a connection between associated primes and the support of a module.

Proposition 6.32. *Let M be an A-module. If $\mathfrak{p} \in \mathrm{Ass}(M)$, then $\mathfrak{p} \in \mathrm{Supp}(M)$. More precisely, if $\mathfrak{p} \in \mathrm{Ass}(M)$, then $V(\mathfrak{p}) \in \mathrm{Supp}(M)$.*

Proof. By definition, $\mathfrak{p} = \mathrm{Ann}(m)$ for some $m \in M$. Consider $\frac{m}{1} \in M_{\mathfrak{p}}$. This element cannot be zero since no element in $S = A \setminus \mathfrak{p}$ annihilates m. Therefore, $M_{\mathfrak{p}} \neq 0$, so $\mathfrak{p} \in \mathrm{Supp}(M)$.

Now let $\mathfrak{q} \in V(\mathfrak{p})$, that is, $\mathfrak{q} \supseteq \mathfrak{p}$. Then $0 \neq A/\mathfrak{p} \subseteq (A/\mathfrak{p})_{\mathfrak{q}} \subseteq M_{\mathfrak{q}}$, hence $\mathfrak{q} \in \mathrm{Supp}(M)$. □

Definition. If M is an A-module, a *zero divisor* of M is an element $a \in A$ such that $am = 0$ for some $0 \neq m \in M$. The set of all zero divisors of M will be denoted by $\mathrm{ZD}(M)$.

Proposition 6.33. *For any A module M we have $\bigcup_{\mathfrak{p} \in \mathrm{Ass}M} \mathfrak{p} \subseteq \mathrm{ZD}(M)$. The reverse inclusion holds if A is Noetherian.*

Proof. The first claim is obvious. For the second, let $a \in \mathrm{ZD}(M)$, so $am = 0$ for some $m \neq 0$. If we denote by N the module generated by m, then $\mathrm{Ass}N \neq \emptyset$, so there exists a prime ideal $\mathfrak{p}$ such that $\mathfrak{p} = \mathrm{Ann}(bm)$ for some $b \in A$ (and $bm \neq 0$). It follows that $a \in \mathfrak{p}$. Since $\mathrm{Ass}N \subseteq \mathrm{Ass}M$, we have proved the second claim. □

Proposition 6.34. *If $0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$ is an exact sequence, then $\mathrm{Ass}M \subseteq \mathrm{Ass}M' \cup \mathrm{Ass}M''$. Furthermore,*

$$\mathrm{Ass}(\oplus_{j \in J} M_j) = \cup_{j \in J} \mathrm{Ass}M_j$$

for any family of modules $(M_j)_{j \in J}$.

Proof. First note that $M'' \simeq M/M'$. Let $\mathfrak{p} \in \mathrm{Ass}M$, so we have a monomorphism $f\colon A/\mathfrak{p} \hookrightarrow M$. Set $N = M' \cap \mathrm{im}(f)$. If $N \simeq 0$, then $\mathfrak{p} \in \mathrm{Ass}M''$ because the composition of f with the projection $M \twoheadrightarrow M/M'$ is injective. If $N \neq 0$, take a non-zero element $n \in N$. Then $0 \neq n \in \mathrm{im}(f) \simeq A/\mathfrak{p}$ and since $\mathrm{Ass}A/\mathfrak{p} = \{\mathfrak{p}\}$, we have $\mathrm{Ann}(n) = \mathfrak{p}$. Since N is a submodule of M', we get $\mathfrak{p} \in \mathrm{Ass}M'$.

To prove the second statement first note that the inclusion "$\supseteq$" is clear by Proposition 6.30. The inclusion "$\subseteq$" is OK for finite direct sums by induction and the first claim. For an infinite direct sum, set $M = \oplus_j M_j$ and let $\mathfrak{p} \in \mathrm{Ass}M$. Then $A/\mathfrak{p}$ is a submodule of M which is generated by the image of $\overline{1}$. Therefore, it lies in a finite direct sum. □

Proposition 6.35. *If A is a Noetherian ring and $0 \neq M$ a finitely generated A-module, then*

(1) *There exists a chain of submodules*

$$0 = M_0 \subsetneq M_1 \subsetneq \ldots \subsetneq M_n = M$$

such that for all $1 \leq i \leq n$ there is a prime ideal $\mathfrak{p}_i$ with $M_i/M_{i-1} \simeq A/\mathfrak{p}_i$.

(2) *For any such chain, $\mathrm{Ass}M \subseteq \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$, hence $\mathrm{Ass}M$ is a finite set.*

Proof. (1) By Proposition 6.29, $\mathrm{Ass}M \neq \emptyset$. So let $\mathfrak{p}_1 = \mathrm{Ann}(m_1) \in \mathrm{Ass}M$. Let M_1 be the submodule of M generated by m_1. Considering the surjective map $A \twoheadrightarrow M_1$ given by $a \mapsto am_1$, we see that its kernel is $\mathfrak{p}_1$, hence $M_1 \simeq A/\mathfrak{p}_1$. Now continue with the module $M' = M/M_1$ which has an associated prime $\mathfrak{p}_2 = \mathrm{Ann}(\overline{m}_2)$ and letting $M_2 \subseteq M$ be the submodule generated by m_1 and m_2 we see that $M_2/M_1 \simeq A/\mathfrak{p}_2$. We can continue this process which has to terminate since M is finitely generated.

(2) By Proposition 6.34, we have $\mathrm{Ass}M_i/M_{i-1} = \mathrm{Ass}A/\mathfrak{p}_i = \{\mathfrak{p}_i\}$ for all $1 \leq i \leq n$ and from the exact sequences

$$0 \twoheadrightarrow M_{i-1} \twoheadrightarrow M_i \twoheadrightarrow A/\mathfrak{p}_i \twoheadrightarrow 0$$

we get $\mathrm{Ass}M_i \subset \mathrm{Ass}M_{i-1} \cup \{\mathfrak{p}_i\}$ and hence the claim.

□

Proposition 6.36. *Let A be a ring, M be an A-module, $\mathfrak{p}$ be a prime ideal and S be a multiplicatively closed subset. If $\mathfrak{p} \cap S = \emptyset$ and $\mathfrak{p} \in \mathrm{Ass}M$, then $S^{-1}\mathfrak{p} = \mathfrak{p}S^{-1}A \in \mathrm{Ass}(S^{-1}M)$. The converse holds if $\mathfrak{p}$ is finitely generated (for example, if A is Noetherian).*

Proof. If $\mathfrak{p} \in \mathrm{Ass}M$, then $A/\mathfrak{p} \hookrightarrow M$. Localising this injection gives an injection $S^{-1}(A/\mathfrak{p}) = S^{-1}A/S^{-1}\mathfrak{p} \hookrightarrow S^{-1}M$. If $\mathfrak{p} \cap S = \emptyset$, then $S^{-1}\mathfrak{p}$ is a prime ideal in $S^{-1}A$, so the first claim holds.

To see the second, assume $S^{-1}\mathfrak{p} \in \mathrm{Ass}S^{-1}M$, so $S^{-1}\mathfrak{p} = \mathrm{Ann}(\frac{m}{t})$ for some $m \in M$ and $s \in S$. If $\mathfrak{p}$ is generated by $x_1, \ldots, x_n$, then $\frac{x_i}{1}\frac{m}{t} = 0$ for all i, hence $x_i s_i m = 0$ for some $s_i \in S$. If $s := \prod_i s_i$, then $x_i \in \mathrm{Ann}(sm)$. It follows that $\mathfrak{p} \subseteq \mathrm{Ann}(sm)$.

Now any element $b \in \mathrm{Ann}(sm)$ satisfies $\frac{bsm}{st} = \frac{b}{1}\frac{m}{t} = 0$, so $\frac{b}{1} \in S^{-1}\mathfrak{p}$. It is easily seen that $b \in \mathfrak{p}$, hence $\mathfrak{p} = \mathrm{Ann}(sm)$, so $\mathfrak{p} \in \mathrm{Ass}M$. To conclude, note that $S^{-1}\mathfrak{p}$ is prime, so in particular a proper ideal, which implies that $\mathfrak{p} \cap S = \emptyset$. □

Corollary 6.37. *If A is a Noetherian ring and M an A-module, then*

$$\mathfrak{p} \in \mathrm{Ass}_A M \iff \mathfrak{p}A_{\mathfrak{p}} \in \mathrm{Ass}_{A_{\mathfrak{p}}} M_{\mathfrak{p}}.$$

□

Proposition 6.38. *If M is an A-module and A is a Noetherian ring, then any AM-associated prime ideal is also associated.*

Proof. By the previous corollary, it is enough to show that any AM-associated prime ideal $\mathfrak{p}$ is an element of $\mathrm{Ass}_{A_{\mathfrak{p}}} M_{\mathfrak{p}}$. We can therefore assume that A is a Noetherian local ring with maximal ideal $\mathfrak{p}$. Since $\mathfrak{p}$ is AM-associated, we have $\mathfrak{p} = \mathrm{rad}\mathrm{Ann}(m)$ for some $0 \neq m \in M$. Since in a Noetherian ring every ideal contains a power of its radical, see Proposition 6.21, there exists an $n > 0$ such that $\mathfrak{p}^n \subseteq \mathrm{Ann}(m)$. Now consider the set $\mathcal{G} = \{\mathrm{Ann}(a) \mid a \in A : \mathrm{Ann}(m) \subseteq \mathrm{Ann}(a)\}$ which has to have a maximal element since A is Noetherian. Calling this maximal element $\mathfrak{q}$, we note that this is a prime ideal; compare the proof of Proposition 6.29. Hence, $\mathfrak{p}^n \subseteq \mathrm{Ann}(m) \subseteq \mathfrak{q} \subseteq \mathfrak{p}$ (the last containment holds since $\mathfrak{q}$ is prime and $\mathfrak{p}$ is maximal). By Corollary 6.22, we get that $\mathrm{rad}\mathfrak{q} = \mathfrak{q} = \mathfrak{p}$, hence $\mathfrak{p} \in \mathrm{Ass}M$. □

Using the above, we can now prove the following statement, which can be seen as a converse to Proposition 6.32.

Proposition 6.39. *Let A be a Noetherian ring and M be an A-module. Then every minimal element $\mathfrak{p} \in \mathrm{Supp}(M)$ is in $\mathrm{Ass}(M)$. In particular, if M is finitely generated, then $\mathrm{Supp}(M) = \cup_{i=1}^n V(\mathfrak{p}_i)$, where the $\mathfrak{p}_i$ are minimal primes containing $\mathrm{Ann}(M)$ and all the $\mathfrak{p}_i$ are in $\mathrm{Ass}(M)$.*

Proof. Let $\mathfrak{p} \in \mathrm{Supp}(M)$ be a minimal element. Then $M_{\mathfrak{p}} \neq 0$, but by minimality $M_{\mathfrak{q}} = 0$ for any prime ideal $\mathfrak{q} \subsetneq \mathfrak{p}$. Now, $M_{\mathfrak{p}}$ is a module over $A_{\mathfrak{p}}$. The latter ring is Noetherian, hence $\mathrm{Ass}(M_{\mathfrak{p}}) \neq \emptyset$. Let $\mathfrak{p}' \in \mathrm{Spec}(A_{\mathfrak{p}})$ be an ideal which is not the maximal ideal in $A_{\mathfrak{p}}$. Then $\mathfrak{p}'$ is the extension of a prime ideal $\mathfrak{q} \in \mathrm{Spec}(A)$ with $\mathfrak{q} \subseteq \mathfrak{p}$. Since $(M_{\mathfrak{p}})_{\mathfrak{p}'} = M_{\mathfrak{q}} = 0$, we conclude that $\mathrm{Supp}(M_{\mathfrak{p}}) = \{\mathfrak{p}A_{\mathfrak{p}}\}$ is the maximal ideal of $A_{\mathfrak{p}}$. Therefore $\mathrm{Ass}(M_{\mathfrak{p}}) = \{\mathfrak{p}A_{\mathfrak{p}}\}$ as well. Corollary 6.37 then gives $\mathfrak{p} \in \mathrm{Ass}(M)$.

To see the second claim, note that if M is finitely generated, then $\mathrm{Supp}(M) = V(\mathrm{Ann}(M))$ by Exercise 15 (Exercise 3 on Sheet 4). By Propositions 6.26 and 6.27, $V(\mathrm{Ann}(M)) = \mathrm{Spec}(A/\mathrm{Ann}(M)) = \cup_{i=1}^n V(\mathfrak{p}_i)$, where the $\mathfrak{p}_i$ are minimal primes containing $\mathrm{Ann}(M)$. By the above, they are contained in $\mathrm{Ass}(M)$. □

We conclude this section by briefly describing how primary decompositions of ideals can be generalised to arbitrary modules. Until the end of this section, A will be a *Noetherian ring*.

Definition. Let M be an A-module and Q be a submodule of M. If $\mathrm{Ass}(M/Q) = \{\mathfrak{p}\}$, we call Q $\mathfrak{p}$-*primary* in M.

A *primary decomposition* of N is a decomposition $N = Q_1 \cap \ldots \cap Q_r$ with Q_i $\mathfrak{p}_i$-primary. We call such a decomposition *minimal* if all the $\mathfrak{p}_i$ are distinct and $\cap_{j \neq i} Q_j \nsubseteq Q_i$ for all i.

Any decomposition can be made minimal. Indeed, if Q_1 and Q_2 are $\mathfrak{p}$-primary, then so is $Q = Q_1 \cap Q_2$. To see this, consider $M \longrightarrow M/Q_1 \oplus M/Q_2$, note that the kernel is Q, hence M/Q injects into the direct sum, and therefore, $\mathrm{Ass}(M/Q) \subseteq \mathrm{Ass}(M/Q_1) \cup \mathrm{Ass}(M/Q_2) = \{\mathfrak{p}\}$. On the other hand, $\mathrm{Ass}(M/Q)$ is not empty by Proposition 6.29 (recall that A is Noetherian).

Theorem 6.40. *If M is a module over a Noetherian ring A and N is a submodule having a minimal primary decomposition $N = \cap_{i=1}^{r} Q_i$ where the Q_i are $\mathfrak{p}_i$-primary, then the prime ideals $\mathfrak{p}_i$ are uniquely determined.*

Proof. First of all, $\mathrm{Ass}(M/N) \subseteq \{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$. Indeed, the kernel of the map $M \longrightarrow \oplus_i (M/Q_i)$ is precisely N, so M/N injects into $\oplus_i (M/Q_i)$, hence $\mathrm{Ass}(M/N)$ is a subset of the union of the $\mathrm{Ass}(M/Q_i)$, which is what we wanted to prove.

Now given i, let $P_i = \cap_{j \neq i} Q_j$, hence $P_i \cap Q_i = N$ and $P_i/N \neq 0$ since the decomposition is minimal. The injection $P_i/N \hookrightarrow M/Q_i$ then shows that $\mathrm{Ass}(P_i/N) = \{\mathfrak{p}_i\}$, while the injection $P_i/N \hookrightarrow M/N$ shows that $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\} \subseteq \mathrm{Ass}(M/N)$. In particular, the $\mathfrak{p}_i$ are just the distinct associated prime ideals of M/N and, therefore, uniquely determined. □

One can also show in this more general setting that the primary components corresponding to the minimal associated primes of M/N are uniquely determined.

7. Ring extensions

Definition. Let A be a subring of a ring B. An element $x \in B$ is called *integral over* A if there is an equation of the form

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

with $a_i \in A$ for $1 \leq i \leq n$.

We will give a characterisation of integral elements after the following

Lemma 7.1. *Let M be a finitely generated module over a ring A, let I be an ideal of A and let $f \colon M \longrightarrow M$ be an A-linear map such that $f(M) \subseteq IM$. Then there exists an $n > 0$ such that*

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

with $a_k \in I$ for all k.

Proof. Let $x_1, \dots, x_n$ be a set of generators of M. Since $f(x_l) \in IM$ for all l, we have $f(x_l) = \sum_{j=1}^n a_{lj} x_j$ with $a_{lj} \in I$. Hence,

$$\sum_{j=1}^{n} (\delta_{lj} f - a_{lj}) x_j = 0.$$

Using that the well-known statement $\mathrm{Adj}A \cdot A = \det(A)\mathrm{id}_n$ for an $n \times n$-matrix A over a field also holds over any commutative ring, we can multiply the equation with the adjoint matrix of $(\delta_{lj} f - a_{lj})$ to conclude that $\det(\delta_{lj} f - a_{lj})$ kills all the x_j, hence is the zero map of M. Expanding the determinant gives the claim. □

Proposition 7.2. *The following are equivalent.*

(1) $x \in B$ *is integral over* A.
(2) $A[x]$ *is a finitely generated* A*-module.*
(3) $A[x]$ *is contained in a subring* C *of* B *which is a finitely generated* A*-module.*
(4) *There exists a faithful* $A[x]$*-module* M *which is finitely generated as an* A*-module (a module* M *is faithful if* $\mathrm{Ann}(M) = 0$*).*

Proof. "(1)⇒(2)": We have $x^n = -a_1 x^{n-1} - \ldots - a_n$. By induction, every x^m with $m \geq n$ is a linear combination of $1, \dots, x^{n-1}$, hence $A[x]$ is finitely generated.

"(2)⇒(3)": Set $C = A[x]$.

"(3)⇒(4)": Set $M = C$; since C is a ring, $a1 = 0$ implies $a = 0$, so $\mathrm{Ann}(C) = 0$.

"(4)⇒(1)": Apply the above lemma to the case where f is the multiplication by x and $I = A$. Since M is an $A[x]$-module, we indeed have $f(M) \subseteq M$. Since M is faithful, the above lemma gives the wanted equation. □

Remark 7.3. We can give an alternative proof of Nakayama's lemma using the above "determinant trick" 7.1. Namely, if M is a finitely generated A-module and $IM = M$ for an ideal I, then there exists $x \equiv 1$ modulo I such that $xM = 0$ by setting $f = \mathrm{id}$. Now if I is contained in the Jacobson radical of A, then x is a unit, so $M = x^{-1}xM = 0$.

Corollary 7.4. *Let* $A \subseteq B$ *be rings. If* $x_i \in B$, $1 \leq i \leq n$ *are integral over* A*, then* $A[x_1, \dots, x_n]$ *is a finitely generated* A*-module. Furthermore, the set of elements* C *which are integral over* A *is a subring of* B*.*

Proof. To prove the first claim, we use induction on n.

The case $n = 1$ is given by the previous proposition. Now use that $A[x_1, \dots, x_n] \simeq A[x_1, \dots, x_{n-1}][x_n]$. By the induction hypothesis, the ring $A[x_1, \dots, x_{n-1}]$ is finitely generated over A and x_n is integral over this ring, hence $A[x_1, \dots, x_{n-1}][x_n]$ is a finitely generated $A[x_1, \dots, x_{n-1}]$-module. Since being finitely generated is transitive by Proposition 3.21, the claim holds.

To prove the second claim, note that if x, y are integral over A, then $D = A[x, y]$ is finitely generated over A, hence $x + y \in D$ and $xy \in D$ are integral over A. □

Definition. Let $A \subseteq B$ be rings. The set of elements C of B which are integral over A is called the *integral closure* of A in B. If $C = B$, then we say that B is *integral* over A. If $C = A$, then A is said to be *integrally closed in* B.

If A is a domain, then we say that A is *integrally closed* (or *normal*) if it is integrally closed in its field of fractions.

Example 7.5. The integers $\mathbb{Z}$ are integrally closed. Indeed, if $x = \frac{r}{s} \in \mathbb{Q}$, with r and s coprime, is integral over $\mathbb{Z}$, then multiplying the equation

$$(\frac{r}{s})^n + a_1(\frac{r}{s})^{n-1} + \ldots + a_n = 0$$

by s^n, we get $r^n + a_1 s r^{n-1} + \ldots + a_n s^n = 0$. Hence, s divides r^n, so $s = \pm 1$.

More generally, any unique factorization domain is integrally closed. Here, we call an integral domain A a *unique factorization domain* if every element $x \in A$ can be uniquely written as $x = ua_1 \ldots a_n$ where u is a unit and the a_k are *irreducible*, i.e. they cannot be written as products of non-units.

Corollary 7.6. *Let $A \subseteq B$ be rings and let C be the integral closure of A in B. Then C is integrally closed in B.*

Proof. Every element of B which is integral over C is also integral over A, hence is in C. □

Proposition 7.7. *Let $A \subseteq B$ and let B be integral over A. Then*

1. *If J is an ideal of B and $I = J \cap A$, then B/J is integral over A/I.*
2. *If S is a multiplicatively closed subset of A, then $S^{-1}B$ is integral over $S^{-1}A$.*

Proof.

1. Since for every b in B there is an equation of the form $b^n + a_1 b^{n-1} + \ldots + a_n = 0$ with $a_k \in A$ for all k, we can reduce it modulo I.
2. Let $\frac{b}{s} \in S^{-1}B$ and divide the above equation by s^n to get

$$(\frac{b}{s})^n + \frac{a_1}{s}(\frac{b}{s})^{n-1} + \ldots + \frac{a_n}{s^n} = 0.$$

Hence, $\frac{b}{s}$ is integral over $S^{-1}A$.

□

Proposition 7.8. *Let $A \subseteq B$ be integral domains and let B be integral over A. Then A is a field if and only if B is a field.*

Proof. Assume first that A is a field and let $b \in B$ be an arbitrary non-zero element. Since b is integral over A, we have an equation $b^n + a_1 b^{n-1} + \ldots + a_n = 0$. Assume that this equation is of minimal possible degree and note that $a_n \neq 0$, since otherwise we would have $b(b^{n-1} + a_1 b^{n-2} + \ldots + a_{n-1}) = 0$, so b would be a zero divisor (by minimality), a contradiction. Since A is a field and $a_n \neq 0$, its inverse exists, so $b^n + a_1 b^{n-1} + \ldots + a_{n-1} b = -a_n$, hence $b(-a_n^{-1}(b^{n-1} + a_1 b^{n-2} + \ldots + a_{n-1})) = 1$, so $b^{-1} = -a_n^{-1}(b^{n-1} + a_1 b^{n-2} + \ldots + a_{n-1}) \in B$.

Now assume that B is a field. Let $0 \neq x \in A$ be arbitrary. Then x^{-1} exists in B, hence there is an equation

$$x^{-m} + a'_1 x^{-m+1} + \ldots + a'_m = 0.$$

Multiplying this equation with x^{m-1} gives $x^{-1} = -a'_1 - \ldots - a'_m x^{m-1} \in A$, hence A is a field. □

Corollary 7.9. *Let $A \subseteq B$ be rings, B integral over A. Let $\mathfrak{q}$ be a prime ideal of B and $\mathfrak{p} = \mathfrak{q} \cap A$ (which is prime since inverse images of prime ideals are prime). Then $\mathfrak{p}$ is maximal if and only if $\mathfrak{q}$ is maximal.*

Proof. By Proposition 7.7, the domain $B/\mathfrak{q}$ is integral over the domain $A/\mathfrak{p}$. Hence the former is a field if and only if the latter is a field, which is precisely our claim. □

Corollary 7.10. *Let $A \subseteq B$ be rings, B integral over A. Let $\mathfrak{q}$ and $\mathfrak{q}'$ be prime ideals of B satisfying $\mathfrak{q} \subseteq \mathfrak{q}'$ and $\mathfrak{q} \cap A = \mathfrak{q}' \cap A = \mathfrak{p}$. Then $\mathfrak{q} = \mathfrak{q}'$.*

Proof. By Proposition 7.7, $B_\mathfrak{p}$ is integral over $A_\mathfrak{p}$. Denoting by $\mathfrak{m}$ the extension of $\mathfrak{p}$ in $A_\mathfrak{p}$ and by $\mathfrak{n}$, $\mathfrak{n}'$ the extensions of $\mathfrak{q}$, $\mathfrak{q}'$ in $B_\mathfrak{p}$, we have $\mathfrak{n} \subseteq \mathfrak{n}'$ and $\mathfrak{n}^c = \mathfrak{n}'^c = \mathfrak{m}$. Since $\mathfrak{m}$ is maximal, the previous corollary shows that $\mathfrak{n} = \mathfrak{n}'$, hence $\mathfrak{q} = \mathfrak{q}'$ by Proposition 4.14. □

Theorem 7.11 (Going-up theorem)**.** *Let $A \subseteq B$ be rings, B integral over A. Let $\mathfrak{p}_1 \subseteq \ldots \subseteq \mathfrak{p}_n$ be a chain of prime ideals of A and let $\mathfrak{q}_1 \subseteq \ldots \subseteq \mathfrak{q}_m$, $m < n$, be a chain of prime ideals of B such that $\mathfrak{q}_i \cap A = \mathfrak{p}_i$ for $1 \leq i \leq m$. Then the chain $\mathfrak{q}_1 \subseteq \ldots \subseteq \mathfrak{q}_m$ can be extended to a chain $\mathfrak{q}_1 \subseteq \ldots \subseteq \mathfrak{q}_n$ with $\mathfrak{q}_i \cap A = \mathfrak{p}_i$ for $1 \leq i \leq n$.*

Proof. Let us first show that if $\mathfrak{p}$ is a prime ideal in A, then there exists an ideal $\mathfrak{q}$ in B such that $\mathfrak{q} \cap A = \mathfrak{p}$. Indeed, $B_\mathfrak{p}$ is integral over $A_\mathfrak{p}$ and we have a commutative diagram

$$\begin{array}{ccc} A & \longrightarrow & B \\ {\scriptstyle f}\downarrow & & \downarrow \\ A_\mathfrak{p} & \longrightarrow & B_\mathfrak{p}. \end{array}$$

If $\mathfrak{n}$ is the maximal ideal of $B_\mathfrak{p}$, then $\mathfrak{m} = A_\mathfrak{p} \cap \mathfrak{n}$ is maximal by Corollary 7.9. The preimage $\mathfrak{q}$ of $\mathfrak{n}$ under the canonical map $B \longrightarrow B_\mathfrak{p}$ is a prime ideal and by commutativity $\mathfrak{q} \cap A = f^{-1}(\mathfrak{m}) = \mathfrak{p}$.

Now note that by induction we can immediately reduce to the case $m = 1$, $n = 2$. Let $\overline{A} = A/\mathfrak{p}_1$ and $\overline{B} = B/\mathfrak{q}_1$. Then $\overline{A} \subseteq \overline{B}$ and the latter is integral over the former. Denoting by $\overline{\mathfrak{p}}_2$ the image of $\mathfrak{p}_2$ in $\overline{A}$, by what we just proved there exists a prime ideal $\overline{\mathfrak{q}}_2$ in $\overline{B}$ such that $\overline{\mathfrak{q}}_2 \cap \overline{A} = \overline{\mathfrak{p}}_2$. Taking the preimage of $\overline{\mathfrak{q}}_2$ in B gives us the required prime ideal. □

It might be good to remember the short version of the theorem. Namely, if $A \subseteq B$, B is integral over A and if $\mathfrak{p}_1 \subseteq \mathfrak{p}_2$ are prime ideals of A and there exists $\mathfrak{q}_1$ such that $\mathfrak{q}_1 \cap A = \mathfrak{p}_1$, there also exists $\mathfrak{q}_2$ with $\mathfrak{q}_2 \cap A = \mathfrak{p}_2$. Perhaps in this formulation it is a little easier to recognize the origin of the name of the theorem.

Our next goal is to prove the Going-down theorem. This will require us to prove some preliminary results first.

Proposition 7.12. *Let $A \subseteq B$ be rings and let C be the integral closure of A in B. If S is a multiplicatively closed subset of A, then $S^{-1}C$ is the integral closure of $S^{-1}A$ in $S^{-1}B$.*

Proof. We already know that $S^{-1}C$ is integral over $S^{-1}A$. Let $\frac{b}{s} \in S^{-1}B$ be an element integral over $S^{-1}A$, so we have an equation

$$(\frac{b}{s})^n + \frac{a_1}{s_1}(\frac{b}{s})^{n-1} + \ldots + \frac{a_n}{s_n} = 0.$$

Multiply this equation by $(st)^n$, where $t = s_1 \cdots s_n$, to get

$$(bt)^n + a_1 s s_2 \cdots s_n (bt)^{n-1} + \ldots + s^n a_n t^{n-1} s_1 \cdots s_{n-1} = 0.$$

This is an equation of integral dependence for bt over A, hence $bt \in C$ and $\frac{bt}{st} = \frac{b}{s} \in S^{-1}C$. □

We will next show that being interally closed is a local property.

Proposition 7.13. *Let A be an integral domain. The following are equivalent.*

1. *A is integrally closed.*
2. *$A_{\mathfrak{p}}$ is integrally closed for every prime ideal $\mathfrak{p}$.*
3. *$A_{\mathfrak{m}}$ is integrally closed for every maximal ideal $\mathfrak{m}$.*

Proof. Let $K = A_{(0)}$ be the field of fractions of A, C be the integral closure of A in K and $\iota\colon A \longrightarrow C$ the canonical embedding. Then A is integrally closed if and only if ι is surjective. Similarly, $A_{\mathfrak{p}}$ resp. $A_{\mathfrak{m}}$ is integrally closed if and only if the map $\iota_{\mathfrak{p}}$ resp. $\iota_{\mathfrak{m}}$ is surjective. But these two conditions are equivalent by Proposition 4.10. □

Definition. Let $A \subseteq B$ be rings and let I be an ideal of A. An element $b \in B$ is *integral over I* if it is a root of a monic polynomial with coefficients in I. The *integral closure of I in B* is the set of all elements of B which are integral over I.

Lemma 7.14. *Let $A \subseteq B$ be rings, let C be the integral closure of A in B and I be an ideal in A. Furthermore, let I^e be the extension of I in C. Then the integral closure of I in B is* $\mathrm{rad}I^e$.

Proof. If $b \in B$ is integral over I, then $b^n + a_1 b^{n-1} + \ldots + a_n = 0$ for some $a_k \in I$. Hence, $b^n \in I^e \subseteq C$ and consequently $b \in \mathrm{rad}I^e$.

Conversely, if $b \in \mathrm{rad}I^e$, then for some $n > 0$ we have $b^n = \sum_{k=1}^m a_k x_k$, where $a_k \in I$ and $x_k \in C$. By definition of C, the module $M = A[x_1, \ldots, x_m]$ is finitely generated over A and $b^n M \subseteq IM$. Applying Lemma 7.1 with f being the multiplication by b^n gives that b^n is integral over I, hence so is b. □

Proposition 7.15. *Let $A \subseteq B$ be integral domains with A integrally closed and let $b \in B$ be integral over an ideal I of A. Then b is algebraic over the field of fractions $K = A_{(0)}$ of A. Its minimal polynomial $t^n + a_1 t^{n-1} + \ldots + a_n$ over K has the property that $a_k \in \mathrm{rad}I$ for all $1 \leq k \leq n$.*

Proof. Since b is integral over A, it is algebraic over K. Let χ be the minimal polynomial of b over K and consider the splitting field L of χ. Denoting the other roots of χ by $x_1, \ldots, x_m$, we see that each x_k is integral over I because it satisfies the same equation of integral dependence as b does. Since the coefficients of χ are polynomials in the x_k, they are all integral over A by the previous proposition (the radical is closed under addition and multiplication). Since A is integrally closed, $A = C$ in Lemma 7.14, so all the coefficients lie in $\mathrm{rad}I$. □

Theorem 7.16 (Going-down theorem)**.** *Let $A \subseteq B$ be integral domains, let A be integrally closed and B be integral over A. Let $\mathfrak{p}_1 \supseteq \ldots \supseteq \mathfrak{p}_n$ be a chain of prime ideals of A and let $\mathfrak{q}_1 \supseteq \ldots \supseteq \mathfrak{q}_m$, $m < n$, be a chain of prime ideals of B satisfying $\mathfrak{q}_k \cap A = \mathfrak{p}_k$ for $1 \leq k \leq m$. Then the chain $\mathfrak{q}_1 \supseteq \ldots \supseteq \mathfrak{q}_m$ can be extended to a chain $\mathfrak{q}_1 \supseteq \ldots \supseteq \mathfrak{q}_n$ such that $\mathfrak{q}_k \cap A = \mathfrak{p}_k$ for all $1 \leq k \leq n$.*

Proof. Similar to the proof of the going-up theorem we can reduce to the case $m = 1$ and $n = 2$. Since prime ideals in $B_{\mathfrak{q}_1}$ correspond to prime ideals contained in $\mathfrak{q}_1$, we have to show that $\mathfrak{p}_2$ is the contraction of a prime ideal in $B_{\mathfrak{q}_1}$. Since the latter is the case if and only if $\mathfrak{p}_2 B_{\mathfrak{q}_1} \cap A = \mathfrak{p}_2^{ec} = \mathfrak{p}_2$ (the second equality is Proposition 4.20, while the first is by definition), we need to show that $\mathfrak{p}_2^{ec} = \mathfrak{p}_2$. Of course, "$\supseteq$" holds. So, let $x \in \mathfrak{p}_2 B_{\mathfrak{q}_1}$. Then $x = \frac{y}{s}$ with $y \in \mathfrak{p}_2 B$ and $s \in B \setminus \mathfrak{q}_1$. By Lemma 7.14 y is integral over $\mathfrak{p}_2$, so by the previous proposition its minimal equation over K, the field of fractions of A, has the form

$$y^r + a_1 y^{r-1} + \ldots + a_r = 0$$

with $a_k \in \mathfrak{p}_2$ for all k.

If $x \in \mathfrak{p}_2 B_{\mathfrak{q}_1} \cap A$, then $s = yx^{-1} = \frac{y}{x}$ with $x^{-1} \in K$. Dividing the previous equation by x^r we get

$$s^r + a_1 y^{r-1} x^{-r} + \ldots + a_r x^{-r} = s^r + u_1 s^{r-1} + \ldots + u_r = 0$$

where $u_k = \frac{a_k}{x^k}$. It follows that

$$a_k = x^k u_k \in \mathfrak{p}_2 \quad \forall\, 1 \leq k \leq r. \tag{7.1}$$

Since s is integral over A, we have $u_k \in A$ for all $1 \leq k \leq r$ by the previous proposition. If $x \notin \mathfrak{p}_2$, then Equation (7.1) gives that $u_k \in \mathfrak{p}_2$ for all k, so $s^r \in \mathfrak{p}_2 B \subseteq \mathfrak{p}_1 B \subseteq \mathfrak{q}_1$, which is a contradiction. Hence, $x \in \mathfrak{p}_2$ and we are done. □

Below we will interpret the Going-up and Going-Down theorems geometrically. But first we want to use some of the theory we have developed to prove a form of Hilbert's Nullstellensatz. We will need several preliminary results, starting with

Proposition 7.17. *Let $A \subseteq B \subseteq C$ be rings. Suppose that A is Noetherian, that C is a finitely generated A-algebra and that C is either 1) finitely generated as a B-module or 2) integral over B. Then B is finitely generated as an A-algebra.*

Proof. Of course, 1) and 2) are equivalent, so we will prove 1). Assume that $x_1, \ldots, x_n$ generate C as an A-algebra and $y_1, \ldots, y_m$ generate C as a B-module. We therefore have expressions

$$x_i = \sum_j b_{ij} y_j$$
$$y_i y_j = \sum_k b_{ijk} y_k$$

where $b_{ij} \in B$ and $b_{ijk} \in B$.

Define B_0 to be the algebra generated by the b_{ij} and the b_{ijk} over A. Since B_0 is finitely generated over a Noetherian ring, it is itself Noetherian.

Since any element in C is a polynomial in the x_i with coefficients in A we conclude, using both equations above, that C is finitely generated as a B_0-module. Hence, B is finitely generated as a B_0-module, since it is a submodule of C. Therefore, we have the chain of inclusions $A \subseteq B_0 \subseteq B$, where B is a finitely generated B_0-module and B_0 is a finitely generated A-algebra. It follows that B is a finitely generated A-algebra. □

Proposition 7.18. *If E is a finitely generated algebra over a field k and E is itself a field, then E is a finite algebraic extension of k.*

Proof. We can assume that $E = k[x_1, \ldots, x_n]$. Suppose that E is not an algebraic extension of k. We then renumber the x_i such that $x_1, \ldots, x_r$ are algebraically independent over k, that is, $F = k(x_1, \ldots, x_r)$ is a a transcendental extension, and such that $x_{r+1}, \ldots, x_n$ are algebraic over F. Applying the previous proposition to $k \subseteq F \subseteq E$ and using that E is finitely generated as an F-module (since it is an algebraic extension of F), we conclude that F is a finitely generated k-algebra. Therefore, $F = k[y_1, \ldots, y_r]$, where the y_i are quotients of polynomials in $x_1, \ldots, x_r$. Write $y_i = \frac{f_i}{g_i}$.

Adapting the classical proof by Euclid that there exist infinitely many primes, we can show that there are infinitely many irreducible polynomials in $k[x_1, \ldots, x_r]$. In particular, taking $h = g_1 \cdots g_r + 1$, we see that h is prime to each of the g_i. Its inverse h^{-1} exists in F but it cannot be a polynomial in the y_i, contradiction. Hence, E is algebraic over k. □

Theorem 7.19 (Hilbert's Nullstellensatz, weak form)**.** *Let k be a field and let A be a finitely generated k-algebra. Let $\mathfrak{m}$ be a maximal ideal in A. Then the field $A/\mathfrak{m}$ is a finite algebraic extension of k. In particular, if k is algebraically closed, then $A/\mathfrak{m} \simeq k$.*

Proof. Apply the previous proposition to $E = A/\mathfrak{m}$. □

We can use the "weak" form to deduce the following statement.

Theorem 7.20 (Hilbert's Nullstellensatz, strong form)**.** *Let k be an algebraically closed field, $A = k[T_1, \ldots, T_n]$ be the polynomial ring in n variables over k and let $\mathfrak{a}$ be an ideal in A. Consider*

$$Z(\mathfrak{a}) = \{x \in k^n \mid g(x) = 0 \ \forall g \in \mathfrak{a}\}$$

and

$$I(Z(\mathfrak{a})) = \{f \in A \mid f(x) = 0 \ \forall x \in Z(\mathfrak{a})\}.$$

Then $I(Z(\mathfrak{a})) = \mathrm{rad}\mathfrak{a}$.

Proof. One inclusion is easy. If $g \in \mathrm{rad}\mathfrak{a}$, then $g^m \in \mathfrak{a}$ and $g^m(x) = 0$ for all $x \in Z(\mathfrak{a})$ by definition. Hence also $g(x) = 0$ for all $x \in Z(\mathfrak{a})$, so $g \in I(Z(\mathfrak{a}))$.

For the converse, let $f \notin \mathrm{rad}\mathfrak{a}$. Then there exists a prime ideal $\mathfrak{p}$ containing $\mathfrak{a}$ such that $f \notin \mathfrak{p}$. Consider $B = A/\mathfrak{p}$ and $C = B_f$. Since C is a local ring, denote by $\mathfrak{m}$ its maximal ideal. Clearly, B, and therefore also C, is a finitely generated k-algebra and it follows that $C/\mathfrak{m} \simeq k$. Denote by x_i the image of T_i under the map $A \longrightarrow B = A/\mathfrak{p} \longrightarrow C = (A/\mathfrak{p})_f \longrightarrow C/\mathfrak{m} \simeq k$ for $1 \leq i \leq n$. This defines a point $x = (x_1, \ldots, x_n) \in k^n$ and since $\mathfrak{a} \subseteq \mathfrak{p}$, we have $g(x) = 0$ for all $g \in \mathfrak{a}$, so $x \in Z(\mathfrak{a})$. On the other hand, by construction $f(x) \neq 0$, so $f \notin I(Z(\mathfrak{a}))$. □

7.1. **More geometry.** We now want to interpret some of the results of this section geometrically. First a general

Definition. Let (X, σ) and (Y, τ) be topological spaces. We say that a map $f\colon X \longrightarrow Y$ is *continuous* if $f^{-1}(U) \in \tau$ for all $U \in \sigma$. In other words, the preimage of any open/closed subset is open/closed.

A *homeomorphism* is a continuous bijection f whose set-theoretic inverse f^{-1} is also continuous.

Recall that for a ring A the spectrum $\mathrm{Spec}(A)$ of A is the set of all prime ideals of A. Let $f\colon A \longrightarrow B$ be a ring homomorphism. Since $f^{-1}(\mathfrak{q})$ is a prime ideal for any $\mathfrak{q} \in \mathrm{Spec}(B)$, the map f induces a map $f^*\colon \mathrm{Spec}(B) \longrightarrow \mathrm{Spec}(A)$ defined by $\mathfrak{q} \longmapsto f^{-1}(\mathfrak{q})$.

Also recall that $\mathrm{Spec}(A)$ is a topological space with closed subsets given by subsets of the form $V(I)$. Let us summarise some of the properties of the map f^* a ring homomorphism f induces.

Proposition 7.21. *Let* $f\colon A \longrightarrow B$ *be a ring homomorphism and*

$$f^*\colon Y = \mathrm{Spec}(B) \longrightarrow \mathrm{Spec}(A) = X$$

be the induced map on spectra. Then

1. $f^{*-1}(V(I)) = V(I^e)$ *for any ideal* I *in* A. *In particular,* f^* *is a continuous map.*
2. *If* f *is surjective, then* f^* *is a homeomorphism between* Y *and* $V(\ker(f))$.
3. *Let* $g\colon B \longrightarrow C$ *be another ring homomorphism. Then* $(g \circ f)^* = f^* \circ g^*$.

Proof. (1) We have

$$\begin{aligned} f^{*-1}(V(I)) &= \left\{\mathfrak{q} \in \mathrm{Spec}(B) \mid f^*(\mathfrak{q}) = f^{-1}(\mathfrak{q}) \in V(I)\right\} \\ &= \left\{\mathfrak{q} \in \mathrm{Spec}(B) \mid I \subseteq f^{-1}(\mathfrak{q})\right\} \\ &= \{\mathfrak{q} \in \mathrm{Spec}(B) \mid I^e \subseteq \mathfrak{q}\} = V(I^e). \end{aligned}$$

Let us give some details concerning the third equality. Clearly, if $I^e \subseteq \mathfrak{q}$, then $I \subseteq f^{-1}(I^e) \subseteq f^{-1}(\mathfrak{q})$. Conversely, if $I \subseteq f^{-1}(\mathfrak{q})$, then for all $i \in I$ we have $f(i) \in \mathfrak{q}$, so the ideal generated by I is also contained in $\mathfrak{q}$.

(2) We have $B \simeq A/\ker(f)$ by assumption. Now $V(\ker(f))$ are all the prime ideals of A which contain $\ker(f)$. On the other hand, $\operatorname{Spec}(A/\ker(f))$ are also the prime ideals containing $\ker(f)$ by Proposition 2.4 and it is clear that the correspondence given there is precisely f^* and the topologies also obviously coincide.

(3) If $\mathfrak{q} \in \operatorname{Spec}(C)$, then

$$(g \circ f)^*(\mathfrak{q}) = (g \circ f)^{-1}(\mathfrak{q}) = f^{-1} \circ g^{-1}(\mathfrak{q}) = f^* \circ g^*(\mathfrak{q}). \qquad \square$$

Proposition 7.22. *Let $f\colon A \longrightarrow B$ be a ring homomorphism and assume B is integral over $f(A)$. Then $f^*\colon \operatorname{Spec}(B) \longrightarrow \operatorname{Spec}(A)$ is a closed map, i.e., it sends closed subsets to closed subsets.*

Proof. Write f as $\alpha \circ \pi$ where $\pi\colon A \longrightarrow A/\ker(f)$ is the quotient map and $\alpha\colon A/\ker(f) \longrightarrow B$ is the induced map. Then $f^* = \pi^* \circ \alpha^*$ by item (3) of the previous proposition. Note that α is injective, that B is integral over $A/\ker(f) \simeq f(A)$ and that π^* is a closed map by item (2) of the previous proposition. Since the composition of closed maps is closed, it suffices to prove the claim for α^*, so without loss of generality we may assume that $f\colon A \subseteq B$ is an integral extension.

First of all, if I is an ideal in B, it is clear that $f^*(V(I)) \subseteq V(f^{-1}(I))$. Clearly, the claim is proved if we show the reverse inclusion.

By the first step in the proof of the Going-up theorem, for any $\mathfrak{p} \in \operatorname{Spec}(A)$ there exists an element $\mathfrak{q} \in \operatorname{Spec}(B)$ with $f^{-1}(\mathfrak{q}) = f^*(\mathfrak{q}) = \mathfrak{p}$. So if $f^{-1}I = I^c \subseteq \mathfrak{p}' = f^{-1}(\mathfrak{q}') = \mathfrak{q}'^c$ with $\mathfrak{p}' \in \operatorname{Spec}(A)$, then $I = I^{cec} \subseteq \mathfrak{q}'^{cec} = \mathfrak{q}'$. Hence, any $\mathfrak{p}' \in V(f^{-1}(I))$ is of the form $f^*(\mathfrak{q}')$ for some $\mathfrak{q}' \in V(I)$. $\square$

8. Dimension theory

The purpose of this section is to introduce and compare several notion of dimension for (local) rings. We begin with the maybe easiest one.

Definition. Let A be a ring. Its *Krull dimension* is defined as the supremum over the lenghts r taken over all strictly increasing chains of prime ideals $\mathfrak{p}_0 \subset \ldots \subset \mathfrak{p}_r$. The Krull dimension of A will be denoted by $\dim A$.

Example 8.1. Any field has dimension 0. The same holds for any Artin ring by Proposition 5.22. For a more precise statement concerning Artin rings, see the next proposition.

Any principal ideal domain, for instance $\mathbb{Z}$, has dimension 1 by Example 2.14.

Proposition 8.2. *A ring A is Artin if and only if it is Noetherian and* $\dim(A) = 0$.

Proof. Any prime ideal in an Artin ring is maximal by Proposition 5.22, hence $\dim(A) = 0$. By Proposition 5.26, A is Noetherian.

Conversely, if A is Noetherian, the zero ideal has a primary decomposition by Theorem 6.20. Therefore, A has only finitely many minimal prime ideals, which are all maximal,

since $\dim(A) = 0$. The nilradical of A is then the intersection of these finitely many maximal ideals $\mathfrak{m}_1, \ldots, \mathfrak{m}_n$. On the other hand, the nilradical is nilpotent by Proposition 6.21. It follows that

$$\prod_{i=1}^{n} \mathfrak{m}_i^k \subseteq \bigcap_{i=0}^{n} \mathfrak{m}_i^k = 0,$$

hence A is Artinian by Corollary 5.20. □

For our next notion we will need to work with graded rings and modules.

Definition. A ring A is a *graded ring* if $A = \oplus_{n=0}^{\infty} A_n$ for abelian subgroups $(A_n)_{n\in\mathbb{N}}$ such that $A_m A_n \subseteq A_{m+n}$ for all $m, n \geq 0$.

If A is a graded ring, set $A_+ = \oplus_{n\geq 1} A_n$, which is easily seen to be an ideal of A.

Clearly, A_0 is a subring of A and each A_n is a module over A_0.

Similarly, one has

Definition. If A is a graded ring, a *graded A-module* is an A-module M together with a family of subgroups M_n for $n \in \mathbb{N}$ such that $M = \oplus_{n=0}^{\infty} M_n$ and $A_m M_n \subseteq M_{m+n}$ for all $m, n \geq 0$.

An element x of M is *homogeneous* if $x \in M_n$ for some n. This n is then called the *degree* of x.

A *homomorphism* between graded A-modules M and N is an A-linear map $f\colon M \longrightarrow N$ such that $f(M_k) \subseteq N_k$ for all $k \geq 0$.

Note that any M_n is an A_0-module and that any element in M can be uniquely written as a finite sum of homogeneous elements.

Proposition 8.3. *If A is a graded ring, then the following conditions are equivalent:*

i) *A is a Noetherian ring.*
ii) *A_0 is a Noetherian ring and A is finitely generated as an A_0-algebra.*

Proof. ii)⇒ i): By Hilbert's basis theorem.

i)⇒ ii): Since $A_0 \simeq A/A_+$, it is Noetherian as a quotient of a Noetherian ring.

Now, A_+ is an ideal in A, hence is finitely generated by some elements $x_1, \ldots, x_t$ which we can assume to be homogeneous of positive degrees $k_1, \ldots, k_t$. Define A' to be the subring of A generated by the x_i over A_0. Clearly, $A_0 \subseteq A'$. We will now show by induction that $A_n \subseteq A'$ for all $n \geq 0$. Let $y \in A_n$ for some $n > 0$. We can write $y = \sum_{i=1}^{t} a_i x_i$ for $a_i \in A_{n-k_i}$ (here we set $A_m = 0$ for $m < 0$). Since $k_i > 0$, $n - k_i < n$, hence by the inductive hypothesis any a_i can be written as a polynomial in the elements x_j with coefficients in A_0, so the same holds for y. Therefore, $A = A'$. □

Let M be a finitely generated graded A-module, which, in particular, implies that M is generated by a finite number of homogeneous elements m_j, $1 \leq j \leq t$ with degrees r_j. It follows from this that any $m \in M_n$ can be written as $\sum_j f_j(x) m_j$, where $f_j(x)$ is homogeneous of degree $n - r_j$. Therefore, M_n is finitely generated as an A_0-module.

Definition. Consider the category $\mathrm{mod}(A)$ of all finitely generated A-modules. A function λ from $\mathrm{mod}(A)$ to $\mathbb{Z}$ is called *additive* if for every short exact sequence of A-modules of the form

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$$

we have $\lambda(M) = \lambda(M') + \lambda(M'')$.

Example 8.4. Let $A = k$ be a field and consider the category of all finite-dimensional vector spaces. Then $\lambda = \dim_k$ is an additive function on this category.

Definition. Let A be a Noetherian graded ring and M a finitely generated graded A-module. Let λ be an additive function on $\mathrm{Mod}(A_0)$.

The *Poincaré series* $P(M,t)$ of M with respect to λ is the following power series

$$P(M,t) = \sum_{n=0}^{\infty} \lambda(M_n) t^n \in \mathbb{Z}[[t]].$$

Remark 8.5. Below we will frequently study the situation where A is an Artin ring and $\lambda(M)$ is the length of a finitely generated A-module M.

Theorem 8.6. *The function $P(M,t)$ is a rational function in t of the form*

$$f(t)/(\prod_{i=1}^{s}(1-t^{k_i}))$$

for some $f \in \mathbb{Z}[t]$, where A is a finitely generated A_0-algebra in generators $x_1, \ldots, x_s$ with $\deg(x_i) = k_i$ for all i.

Proof. We will prove the statement by induction over s, the number of generators of A over A_0.

First, if $s = 0$, then $A_n = 0$ for all $n > 0$, so $A = A_0$ and M is a finitely generated A_0-module, hence $M_n = 0$ for all large n. It follows that $P(m,t)$ is a polynomial.

Now assume that $s > 0$. Recall that A is finitely generated as an A_0-algebra and denote the generators by $x_1, \ldots, x_s$ and their degrees by $k_1 \ldots, k_s$.

We have an exact sequence

$$0 \longrightarrow K_n \longrightarrow M_n \xrightarrow{x_s} M_{n+k_s} \longrightarrow L_{n+k_s} \longrightarrow 0,$$

where K_n is the kernel of the multiplication by x_s map and L_{n+k_s} the cokernel. Since this works for every n, we can set $K = \oplus_n K_n$ and $L = \oplus_n L_n$ and observe that both these modules are finitely generated over A, because the former is a submodule of M and the latter a quotient module of M. Furthermore, x_s annihilates K and L, hence both are modules over $A_0[x_1, \ldots, x_{s-1}]$. Since the above exast sequence can be split up into the exact sequences

$$0 \longrightarrow K_n \longrightarrow M_n \longrightarrow M_n/K_n \longrightarrow 0$$

and

$$0 \longrightarrow M_n/K_n \xrightarrow{x_s} M_{n+k_s} \longrightarrow L_{n+k_s} \longrightarrow 0,$$

we get

$$\lambda(M_n) = \lambda(K_n) + \lambda(M_n/K_n) = \lambda(K_n) + \lambda(M_{n+k_s}) - \lambda(L_{n+k_s}).$$

Multiplying by t^{n+k_s} and summing with respect to n we get

$$(1 - t^{k_s})P(M,t) = P(L,t) - t^{k_s}P(K,t) + g(t), \tag{8.1}$$

where $g(t)$ is a polynomial. Applying the inductive hypothesis to the right-hand side gives the result. □

Definition. Let A be a Noetherian graded ring and M a finitely generated graded A-module. The order of the pole of $P(M,t)$ at $t = 1$ will be denoted by $d(M)$.

Corollary 8.7. *If $k_i = 1$ for all i, then, for sufficiently large n, $\lambda(M_n)$ is a polynomial in n with rational coefficients of degree $d(M) - 1$.*

Proof. By the theorem, $\lambda(M_n)$ is the coefficient of t^n in $f(t)(1-t)^{-s}$. We may therefore assume that $s = d = d(M)$ and $f(1) \neq 0$. Write $f(t) = \sum_{k=0}^{N} a_k t^k$. Since $(1-t)^{-1} = 1 + t + t^2 + \ldots$, differentiation of both sides gives

$$(1-t)^{-d} = \sum_{k=0}^{\infty} \binom{d+k-1}{d-1} t^k.$$

Then

$$\lambda(M_n) = a_0\binom{d+n-1}{d-1} + a_1\binom{d+n-2}{d-1} + \ldots + a_N\binom{d+n-N-1}{d-1},$$

where $\binom{b}{d-1} = 0$ if $b < d-1$. The right-hand side is a polynomial in n with rational coefficients and the leading term is

$$\frac{n^{d-1}(\sum a_k)}{(d-1)!} \neq 0.$$

□

Corollary 8.8. *If a is an element of A such that $am = 0$ implies that $m = 0$, then $d(M/aM) = d(M) - 1$.*

Proof. Simply use Equation 8.1. □

Example 8.9. Let A_0 be an Artin ring and $A = A_0[X_1, \ldots, X_n]$ be the polynomial ring in n intedeterminates. Then A_k is a free A_0-module of dimension $\binom{n+k-1}{n-1}$. It follows that $P(A,t) = (1-t)^{-n}$ (note that $N = 0$ and $a_0 = 1$ in the proof of Theorem 8.7).

In order to prove our next results, we first need the following

Definition. Let M be an A-module and I an ideal. A sequence of submodules

$$M = M_0 \supseteq M_1 \supseteq M_2 \supseteq \ldots$$

is called a *filtration* of M. It is an *I-filtration* if $IM_n \subseteq M_{n+1}$ for all n and a *stable I-filtration* if $IM_n = M_{n+1}$ for all sufficiently large n.

Example 8.10. Defining $M_n = I^n M$, gives a stable I-filtration.

Lemma 8.11. *Any two stable I-filtrations (M_n) and (M'_n) of a module M have bounded difference, that is, there exists an integer n_0 such that $M_{n+n_0} \subseteq M'_n$ and $M'_{n+n_0} \subseteq M_n$ for all $n \geq 0$.*

Proof. Without loss of generality we may assume that $M'_n = I^n M$. Since $IM_n \subseteq M_{n+1}$ for all n, we have $M'_{n+n_0} \subseteq M'_n = I^n M \subseteq M_n$.

On the other hand, by stability, $IM_n = M_{n+1}$ for all $n \geq n_0$, hence $M_{n+n_0} = I^n M_{n_0} \subseteq I^n M = M'_n$. □

Definition. Let A be a ring and I an ideal of A. The graded group

$$G(A) = G_I(A) = \bigoplus_{n=0}^{\infty} I^n/I^{n+1}$$

(where $I^0 = A$) is a graded ring where the multiplication is defined in the obvious way.

If M is an A-module and (M_n) is an I-filtration of M, then

$$G(M) = G_I(M) = \bigoplus_{n=0}^{\infty} M_n/M_{n+1}$$

is a graded $G(A)$-module in a natural way.

Lemma 8.12. *If A is Noetherian, then $G_I(A)$ is Noetherian for any ideal I of A. If M is a finitely generated A-module and (M_n) is a stable I-filtration of M, then $G_I(M)$ is a finitely generated graded $G_I(A)$-module.*

Proof. The ideal I is finitely generated by elements $a_1, \ldots, a_k$. Denoting their images in I/I^2 by $\overline{a_i}$, we have

$$G(A) = A/I[\overline{a}_1, \ldots, \overline{a}_k].$$

Since A/I is Noetherian, the first claim follows by Hilbert's basis theorem.

Since the filtration of M is I-stable by assumption, $M_{n_0+r} = I^r M_{n_0}$ for all $r \geq 0$. Therefore, $G(M)$ is generated by $\oplus_{n \leq n_0} G_n(M) = N$, where we write $G_n(M)$ for M_n/M_{n+1}. Every such module is, of course Noetherian and annihilated by I, hence a finitely generated A/I-module. It follows that N is a finitely generated A/I-module, so $G(M)$ is a finitely generated $G(A)$-module. □

Proposition 8.13. *Let A be a Noetherian local ring, $\mathfrak{m}$ its maximal ideal, $\mathfrak{q}$ an $\mathfrak{m}$-primary ideal, M a finitely generated A-module and (M_n) a stable $\mathfrak{q}$-filtration of M. Then*

1. *For every $n \geq 0$, M/M_n is of finite length.*
2. *for all sufficiently large n this length is a polynomial $g(n)$ in n of degree $\leq s$, where s is the least number of generators of $\mathfrak{q}$.*
3. *the degree and leading coefficient of $g(n)$ depend only on M and $\mathfrak{q}$ and not the filtration chosen.*

In particular, if $M = A$, the length $l(A/\mathfrak{q}^n)$ is a polynomial $\chi_\mathfrak{q}(n)$ of degree at most s, where s is the smallest number of generators of $\mathfrak{q}$.

Proof. (1) First, note that $A/\mathfrak{q}$ is Noetherian, local and has dimension 0, hence is Artin. By the previous lemma, the graded ring $G_\mathfrak{q}(A) = G(A)$ is Noetherian and $G_\mathfrak{q}(M) = G(M)$ is finitely generated over $G(A)$. Every component M_n/M_{n+1} is a Noetherian A-module and annihilated by $\mathfrak{q}$. Therefore, it is a Noetherian $A/\mathfrak{q}$-module, hence of finite length. Therefore, M/M_n is of finite length and

$$l(M/M_n) = \sum_{r=1}^{n} l(M_{r-1}/M_r).$$

(2) If the ideal $\mathfrak{q}$ is generated by elements $x_1, \dots, x_s$, then their images $\overline{x}_i$ in $\mathfrak{q}/\mathfrak{q}^2$ generate $G(A)$ as an algebra over $A/\mathfrak{q}$ and each of the elements $\overline{x}_i$ has degree 1. By Corollary 8.7, for all large n, the length $l(M_n/M_{n+1}) = f(n)$ is a polynomial in n of degree at most $s-1$. Using that $l(M/M_{n+1}) - l(M/M_n) = f(n)$, it follows that $g(n)$ is a polynomial of degree at most s for all large n.

(3) Let $(\widetilde{M}_n)$ be another stable $\mathfrak{q}$-filtration of M and let $\widetilde{g}(n) = l(M/\widetilde{M}_n)$. These two filtrations have bounded differences by Lemma 8.11. Therefore, $M_{n+n_0} \subseteq \widetilde{M}_n$ and $\widetilde{M}_{n+n_0} \subseteq M_n$ for some index n_0 and all $n \geq 0$. It follows that $g(n+n_0) \geq \widetilde{g}(n)$ and $\widetilde{g}(n+n_0) \geq g(n)$. For large n, g and $\widetilde{g}$ are polynomials and the limes of $g(n)/\widetilde{g}(n)$ for $n \longrightarrow \infty$ is 1, hence g and $\widetilde{g}$ have the same degree and leading coefficient, say by L'Hospital.

□

Definition. The polynomial $g(n)$ belonging to the stable filtration $(\mathfrak{q}^n M)$ is denote by $\chi_\mathfrak{q}^M(n)$. If $M = A$, we will write $\chi_\mathfrak{q}(n)$ for $\chi_\mathfrak{q}^A(n)$.

Proposition 8.14. *For any Noetherian local ring A with maximal ideal $\mathfrak{m}$ and any $\mathfrak{m}$-primary ideal $\mathfrak{q}$, we have*

$$\deg \chi_\mathfrak{q}(n) = \deg \chi_\mathfrak{m}(n).$$

Proof. By Corollary 6.22, we have $\mathfrak{m}^r \subseteq \mathfrak{q} \subseteq \mathfrak{m}$ for some r, hence $\mathfrak{m}^{rn} \subseteq \mathfrak{q}^n \subseteq \mathfrak{m}^n$, so

$$\chi_\mathfrak{m}(n) \leq \chi_\mathfrak{q}(n) \leq \chi_\mathfrak{m}(rn)$$

for all large n. Taking the limit $n \longrightarrow \infty$ and using that the terms involved are polynomials, gives the result. □

Definition. If A is a Noetherian local ring with maximal ideal $\mathfrak{m}$ and $\mathfrak{q}$ any $\mathfrak{m}$-primary ideal, then the degree of $\chi_\mathfrak{q}(n)$ will be denoted by $d(A)$.

The least number of generators of an $\mathfrak{m}$-primary ideal will be denoted by $\delta(A)$.

The main result of this section will be the equality $d(A) = \delta(A) = \dim(A)$.

Proposition 8.15. *For any Noetherian local ring we have $\delta(A) \geq d(A)$.*

Proof. Combine Proposition 8.13 with Proposition 8.14. □

The next step will be to prove that $d(A) \geq \dim(A)$. We will need some preliminary results. To formulate them, if A is a ring and I an ideal of A, we can define a graded ring

$$A^* = \bigoplus_{i=0}^{\infty} I^n.$$

Similarly, if M is an A-module and M_n is an I-filtration of M, then

$$M^* = \bigoplus_{i=0}^{\infty} M_n$$

is a graded A^*-module, because $I^k M_n \subseteq M_{n+k}$.

Note that if A is Noetherian, then A^* is a quotient of $A[x_1, \ldots, x_r]$, where the x_i are the generators of I. In particular, A^* is Noetherian.

Lemma 8.16. *If A is a Noetherian ring, I an ideal in A, M a finitely generated A-module and (M_n) an I-filtration of M, the following statements are equivalent:*

(1) *The module M^* is finitely generated over A^*.*
(2) *The filtration (M_n) is stable.*

Proof. Since M is finitely generated, the same holds for all its submodules M_n, hence the modules $N_k = \oplus_{i \leq k} M_i$ are finitely generated. Clearly, for any k this is a subgroup of M^*, albeit not a submodule. Now consider

$$M_k^* = N_k \oplus IM_k \oplus I^2 M_k \oplus \ldots$$

Since N_k is a finitely generated A-module, M_k^* is a finitely generated A^*-module. Clearly, all the M_k^* are submodules of M^* and they form an ascending chain whose union is M^*. Using the Noetherianity of A^*, we now have the following chain of equivalent statements:

M^* is finitely generated as an A^*-module $\iff$ the chain becomes stationary, that is, $M^* = M_{k_0}^*$ for some $k_0 \iff M_{k_0+r} = I^r M_{k_0}$ for all $r \geq 0 \iff$ the filtration (M_n) is stable. □

The following result is usually called the *Artin-Rees lemma*.

Proposition 8.17. *If A is a Noetherian ring, I an ideal in A, M a finitely generated A-module and (M_n) a stable I-filtration of M, then, for any submodule $M' \subseteq M$, the chain $(M' \cap M_n)$ is a stable I-filtration of M'.*

In particular, taking $M_n = I^n M$, there exists an integer k such that

$$(I^n M) \cap M' = I^{n-k}((I^k M) \cap M') \quad \forall n \geq k.$$

Proof. Clearly,

$$I(M' \cap M_n) \subseteq IM' \cap IM_n \subseteq IM' \cap M_{n+1} \subseteq M' \cap M_{n+1},$$

so $(M' \cap M_n)$ is indeed an I-filtration of M'. This filtration defines a graded A^*-module which by construction is a submodule of M^*. Since A^* is Noetherian, this submodule is finitely generated. By the lemma, the filtration is stable. □

We can now take the first step towards proving the inequality $d(A) \geq \dim(A)$.

Proposition 8.18. *Let A be a Noetherian local ring with maximal ideal $\mathfrak{m}$, $\mathfrak{q}$ be any $\mathfrak{m}$-primary ideal, M be a finitely generated A-module and a a non zero-divisor for M, that is, $am = 0$ implies $m = 0$. Setting $M' = M/aM$, we have*

$$\deg \chi_{\mathfrak{q}}^{M'}(n) \leq \deg \chi_{\mathfrak{q}}^{M}(n) - 1.$$

In particular, if x is not a zero-divisor, then $d(A/x) \leq d(A) - 1$.

Proof. By assumption, the modules M and $N = aM$ are isomorphic. Define a filtration on N by setting $N_n = N \cap \mathfrak{q}^n M$. Dividing the exact sequence

$$0 \longrightarrow N \longrightarrow M \longrightarrow M' \longrightarrow 0$$

by $\mathfrak{q}^n$ gives

$$0 \longrightarrow N/N_n \longrightarrow M/M_n \longrightarrow M'/\mathfrak{q}^n M' \longrightarrow 0.$$

Setting $g(n) = l(N/N_n)$, we get, by the additivity of the length, for all large n

$$g(n) - \chi_{\mathfrak{q}}^{M}(n) = -\chi_{\mathfrak{q}}^{M'}(n).$$

By the Artin-Rees lemma, (N_n) is a stable $\mathfrak{q}$-filtration of N and since $N \simeq M$, the polynomials $g(n)$ and $\chi_{\mathfrak{q}}^{M}(n)$ have the same degree and leading term by item (3) of Proposition 8.13. The result follows. □

Proposition 8.19. *With $A, \mathfrak{m}, \mathfrak{q}$ as above, we have $d(A) \geq \dim(A)$. In particular, the dimension of a Noetherian local ring is finite.*

Proof. We will use induction on $d = d(A)$. If $d = 0$, then $l(A/\mathfrak{m}^n)$ is constant for all large n, hence $\mathfrak{m}^n = \mathfrak{m}^{n+1}$ for all large n, so $\mathfrak{m}^n = 0$ by Nakayama's lemma and, therefore, A is an Artin ring and $\dim(A) = 0$.

Suppose that $d > 0$ and let

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \ldots \subsetneq \mathfrak{p}_r$$

be any chain of prime ideals in A.

Take any element $x \in \mathfrak{p}_1 \setminus \mathfrak{p}_0$. Its image x' in the ring $A' = A/\mathfrak{p}_0$ is non-zero and the latter ring is an integral domain, hence

$$d(A'/x') \leq d(A') - 1$$

by Proposition 8.18.

Note that A' is still a local ring. Denoting its maximal ideal by $\mathfrak{m}'$, we have, for all $n \geq 1$, a surjection $A/\mathfrak{m}^n \twoheadrightarrow A'/\mathfrak{m}'^n$. Therefore, $l(A/\mathfrak{m}^n) \geq l(A'/\mathfrak{m}'^n)$, hence $d(A) \geq d(A')$. This implies that

$$d(A'/x') \leq d(A') - 1 \leq d(A) - 1 = d - 1.$$

By the induction hypothesis, the length of any chain of prime ideals in A'/x' is at most $d - 1$. Now note that the images of the prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ under the quotient map $A \longrightarrow A'/(x')$ form a chain of prime ideals of length $r-1$, so $r-1 \leq d-1$ or, equivalently, $r \leq d$. Therefore, $\dim(A) \leq d$. □

Definition. Let A be a ring and $\mathfrak{p}$ be a prime ideal in A. The *height* of $\mathfrak{p}$, denoted by $\text{height}(\mathfrak{p})$ is the supremum of the length of chains of prime ideals

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n = \mathfrak{p}$$

which end at $\mathfrak{p}$.

Example 8.20. The height of $\mathfrak{p}$ is equal to the dimension of $A_{\mathfrak{p}}$.

Every prime ideal in $\mathbb{Z}$ except for the zero ideal has height 1.

Corollary 8.21. *In a Noetherian ring every prime ideal has finite height, so the set of prime ideals in a Noetherian ring satisfies the descending chain condition.* □

Proposition 8.22. *If A is a Noetherian local ring of dimension d, there exists an $\mathfrak{m}$-primary ideal generated by d elements. Therefore,* $\dim(A) \geq \delta(A)$.

Proof. We will produce the generating set inductively such that every prime ideal containing $(x_1, \ldots, x_i)$ has height at least i for each i. Of course, this is possible if $i = 0$.

Assume that $i > 0$ and $x_1, \ldots, x_{i-1}$ have been constructed. Denote the minimal prime ideals of $(x_1, \ldots, x_{i-1})$ which have height exactly $i-1$ (if they exist) by $\mathfrak{p}_j$, where $1 \leq j \leq r$. Now $\dim(A)$ is the height of the maximal ideal $\mathfrak{m}$ and $i - 1 < d = \dim(A)$, hence $\mathfrak{m} \neq \mathfrak{p}_j$ for all j. Therefore, $\mathfrak{m} \neq \cup_{j=1}^{r} \mathfrak{p}_j$ by Proposition 2.21. Hence, there exists an element $x_i \in \mathfrak{m}$, $x_i \notin \cup_{j=1}^{r} \mathfrak{p}_j$ and we take any prime ideal $\mathfrak{q}$ containing the ideal $(x_1, \ldots, x_i)$. This ideal $\mathfrak{q}$ has to contain some minimal prime $\mathfrak{p}$ of $(x_1, \ldots, x_{i-1})$. If $\mathfrak{p} = \mathfrak{p}_j$ for some j, then $\mathfrak{p} \subsetneq \mathfrak{q}$, hence the height of $\mathfrak{q}$ is at least i. If $\mathfrak{p} \neq \mathfrak{p}_j$ for all j, then the height of $\mathfrak{p}$ is already at least i, hence the same holds for $\mathfrak{q}$. Therefore, every prime ideal containing $(x_1, \ldots, x_i)$ has height at least i.

Now assume that $\mathfrak{p}$ is a prime ideal containing $(x_1, \ldots, x_d)$. By construction, the height of $\mathfrak{p}$ is at least d, hence $\mathfrak{p} = \mathfrak{m}$, since if $\mathfrak{p} \subsetneq \mathfrak{m}$, then $\text{height}(\mathfrak{p}) < \text{height}(\mathfrak{m})$. Therefore, $\text{rad}(x_1, \ldots, x_d) = \mathfrak{m}$, hence the ideal $(x_1, \ldots, x_d)$ is $\mathfrak{m}$-primary. □

Theorem 8.23. *If A is a Noetherian local ring, then the following three integers are equal.*

1. $\dim(A)$*, that is, the maximum length of chains of prime ideals in A.*
2. $d(A)$*, the degree of the polynomial $\chi_{\mathfrak{m}}(n) = l(A/\mathfrak{m}^n)$.*
3. $\delta(A)$*, the least number of generators of an $\mathfrak{m}$-primary ideal of A.*

Proof. We have shown that $\delta(A) \geq d(A) \geq \dim(A) \geq \delta(A)$. □

Example 8.24. Let $A = k[X_1, \ldots, X_n]$ and $A_{\mathfrak{m}}$ be the localisation of A at the maximal ideal $\mathfrak{m} = (X_1, \ldots, X_n)$. Then $G_{\mathfrak{m}}(A)$ is a polynomial ring in n indeterminates, hence its Poincaré series is $(1-t)^{-n}$ and $\dim A_{\mathfrak{m}} = n$.

Corollary 8.25. *If A is a local Noetherian ring with maximal ideal $\mathfrak{m}$, then* $\dim(A) \leq \dim_k \mathfrak{m}/\mathfrak{m}^2$.

Proof. Pick elements $x_1, \ldots, x_k$ in $\mathfrak{m}$ such that their classes in $\mathfrak{m}/\mathfrak{m}^2$ form a basis. Then they generate $\mathfrak{m}$, which of course is an $\mathfrak{m}$-primary ideal, hence $k \geq \delta(A) = \dim(A)$. □

Corollary 8.26. *Let A be a Noetherian ring and $x_1, \dots, x_k$ be elements in A. Then every minimal prime $\mathfrak{p}$ belonging to $I = (x_1, \dots, x_k)$ has height $\leq k$.*

Proof. In the localised ring $A_\mathfrak{p}$ the ideal I is $\mathfrak{p}^e$-primary by Proposition 6.14 and the fact that $\mathfrak{p}$ is minimal. Since $\mathfrak{p}^e$ is the maximal ideal in $A_\mathfrak{p}$, we have $k \geq \dim(A_\mathfrak{p}) = \text{height}\mathfrak{p}$. □

Corollary 8.27. *If A is a Noetherian ring and x an element in A which is neither a zero-divisor nor a unit, then every minimal prime $\mathfrak{p}$ belonging to $I = (x)$ has height 1.*

Proof. By the previous corollary, $\text{height}\,\mathfrak{p} \leq 1$. On the other hand, if $\text{height}\,\mathfrak{p} = 0$ (so $\mathfrak{p}$ is a minimal prime of A), then $\mathfrak{p}$ is a minimal prime belonging to 0, hence every element of $\mathfrak{p}$ is a zero-divisor by Proposition 6.10, which contradicts the fact that $x \in \mathfrak{p}$. □

Corollary 8.28. *If A is a Noetherian local ring and x an element in $\mathfrak{m}$ which is not a zero-divisor, then* $\dim(A/(x)) = \dim(A) - 1$.

Proof. By Proposition 8.18 we have the inequality $\leq$. Now let $x_1, \dots, x_d$ be elements in $\mathfrak{m}$ whose images in $A/(x)$ generate an $\mathfrak{m}/(x)$-primary ideal. Then the ideal $(x, x_1, \dots, x_d)$ in A is $\mathfrak{m}$-primary, hence $d + 1 \geq \dim(A)$. □

8.1. **Regular rings.**

Definition. A *system of parameters* is a sequence of elements $x_1, \dots, x_d$ generating an $\mathfrak{m}$-primary ideal in a Noetherian local ring A, where $d = \dim(A)$.

Proposition 8.29. *Let $x_1, \dots, x_d$ be a system of parameters and let $\mathfrak{q} = (x_1, \dots, x_d)$ be the $\mathfrak{m}$-primary ideal generated by these elements. Let $f(T_1, \dots, T_d) \in A[T_1, \dots, T_d]$ be a homogeneous degree s polynomial with the property that $f(x_1, \dots, x_d) \in \mathfrak{q}^{s+1}$. Then all the coefficients of f lie in $\mathfrak{m}$.*

Proof. Recall that $G_\mathfrak{q}(A) = \oplus_{i \geq 0} \mathfrak{q}^i/\mathfrak{q}^{i+1}$. We have a map of graded rings

$$\varphi \colon (A/\mathfrak{q})[T_1, \dots, T_d] \twoheadrightarrow G_\mathfrak{q}(A), \quad T_i \mapsto \overline{x}_i,$$

where $\overline{x}_i$ is x_i modulo $\mathfrak{q}^2$. Clearly, this map is surjective and $\overline{f}$, the reduction of f modulo $\mathfrak{q}$ is in the kernel of φ. Assume that some coefficient of f is not in $\mathfrak{m}$, hence a unit, so f is easily seen to not be a zero-divisor. This gives

$$\begin{aligned} d(G_\mathfrak{q}(A)) &\leq d((A/q)[T_1, \dots, T_d]/(\overline{f})) = d((A/q)[T_1, \dots, T_d]) - 1 \\ &= d - 1, \end{aligned}$$

where we used Proposition 8.18 for the second equality and the last follows from Example 8.9. But $d(G_\mathfrak{q}(A)) = d$ by the main theorem of this section, which gives the wanted contradiction. □

Theorem 8.30. *Let A be a Noetherian local ring of dimension d with maximal ideal $\mathfrak{m}$ and let $k = A/\mathfrak{m}$. Then the following conditions are equivalent.*

(1) $\dim_k(\mathfrak{m}/\mathfrak{m}^2) = d$.

(2) $\mathfrak{m}$ *can be generated by* d *elements.*
(3) $G_{\mathfrak{m}}(A) \simeq k[T_1, \ldots, T_d]$.

Proof. Clearly, (3) implies (1). The implication "(1)⇒(2)" is provided by Corollary 3.12. Lastly, if (2) holds, then, setting $\mathfrak{m} = (x_1, \ldots, x_d)$, the map φ of the previous proposition is an isomorphism of graded rings, hence (2) implies (3). □

Definition. A Noetherian local ring A satisfying one of the equivalent conditions of Theorem 8.30 is called a *regular local ring.*

The first thing we can say about regular local rings is the following

Proposition 8.31. *Any regular local ring is an integral domain.*

Proof. We will show the following *claim*: If A is a ring, I an ideal such that $\cap_n I^n = 0$ and $G_I(A)$ is an integral domain, then A is an integral domain.

The claim implies the proposition by setting $I = \mathfrak{m}$ and using (3) of Theorem 8.30.

So let us prove the claim. Take $0 \neq x$, $0 \neq y$ in A. Since $\cap_n I^n = 0$, there exist indices r_x, r_y such that $x \in I^{r_x}$, $x \notin I^{r_x+1}$ and $y \in I^{r_y}$, $y \notin I^{r_y+1}$. This implies that $\overline{x}$ and $\overline{y}$ are non-zero in $G_I(A)$, hence their product is also non-zero in $G_I(A)$. Then $xy \neq 0$ in A. □

Example 8.32. Theorem 8.30 in particular tells us that the only local regular rings of dimension 0 are fields. The previous proposition can be used to conclude that an Artin ring which is not a field is not an integral domain.

In the following we want to study an example of regular rings in dimension 1. We begin with the following

Definition. Let K be a field. A surjective map $v\colon K^* \longrightarrow \mathbb{Z}$ is called a *discrete valuation* if the following conditions are satisfied: 1) $v(xy) = v(x) + v(y)$ for all $x, y \in K^*$ and 2) $v(x+y) \geq \min\{v(x), v(y)\}$ if $x \neq -y$.

As a convention, we set $v(0) = \infty$. Note that condition 1) just means that v is a group homomorphism, hence $v(1) = 0$ and $v(x^{-1}) = -x$ for all $x \in K^*$.

Definition. The *discrete valuation ring* of v is the set

$$A = \{x \in K^* \mid v(x) \geq 0\} \cup \{0\}.$$

Note that A is indeed a subring of K^*, hence in particular a domain.

Proposition 8.33. *Let A be a discrete valuation ring. Then A is a local ring with maximal ideal*

$$\mathfrak{m} = \{x \in K^* \mid v(x) > 0\}.$$

In particular, $A^* = \{x \in K^* \mid v(x) = 0\}$ and A is a local domain which is not a field.

Proof. If y is in $A \setminus \mathfrak{m}$, then $v(y) = 0$. The element y has an inverse in K^*. Since v is a valuation, we have $v(y^{-1}) = -v(y) = 0$, hence $y^{-1} \in A$. Therefore, A is a local ring by Proposition 2.15. □

Definition. A *uniformizing parameter* is an element t of a discrete valuation ring A such that $v(t) = 1$.

Note that any uniformizing parameter is an irreducible element of A. Indeed, if $t = xy$ in A, then $1 = v(x) + v(y)$, hence $v(x) = 0$ or $v(y) = 0$, since $v(x) \geq 0$ and $v(y) \geq 0$ in any case. Therefore, either x or y is a unit in A.

Let $x \in K^*$ be arbitrary. Set $n = v(x)$, then $v(xt^{-n}) = v(x) + v(t^{-n}) = v(x) - n = 0$, hence $u = xt^{-n}$ is a unit in A^* and we have a unique factorization $x = ut^n$. In particular, if t' is another uniformizing parameter, then $t' = u't$ for some $u' \in A^*$. The same argument shows that A is a unique factorization domain.

Furthermore, A is a principal ideal domain. Indeed, let I be a non-zero ideal in A and let $y \in I$. Then $y = ut^n$ for some $u \in A^*$, where $n = v(y)$. If we define $m = \min\{v(x) \mid x \in I\}$, then $n \geq m$, and setting $w = ut^{n-m} \in A$, we have $y = ut^{n-m}t^m$, hence $I \subseteq (t^m)$. On the other hand, any $x \in I$ such that $x = ut^m$, satisfies $(x) = (t^m)$, so $(t^m) \subseteq I$. Therefore, we get

Proposition 8.34. *Let A be a discrete valuation ring. Then A is a regular local ring of dimension 1. Furthermore, A is normal.*

Proof. Since A is a domain, (0) is a prime ideal and $(0) \subsetneq \mathfrak{m}$. It follows from the above discussion that $\mathfrak{m} = (t)$ and there are no prime ideals between (0) and $\mathfrak{m}$, hence $\dim(A) = 1$. The ring A is regular since it satisfies condition (2) of Theorem 8.30.

Since A is a unique factorization domain, it is normal. □

Example 8.35. Let k be a field and let $K = k((X))$ be the field of formal power series in X whose elements are of the form $f(X) = \sum_{i \geq n} a_i X^i$, $a_i \in k$, where $n \in \mathbb{Z}$ and $a_n \neq 0$. Set $v(f) = n$. Then v is a discrete valuation, $k[[X]]$ the associated DVR and $\mathfrak{m} = (X)$ the maximal ideal.

Remark 8.36. In fact, any regular local ring of dimension 1 is a discrete valuation ring.

9. Homological methods

9.1. **Recollections.** We begin by recalling some facts from homological algebra. Whenever we will consider a module in this section, we will for simplicity assume that it is non-zero and leave it to the reader to figure out which of the statements do not hold for the zero module.

Definition. Let A be a ring and M be an A-module. We call M *projective* if the functor $\mathrm{Hom}(M, -)$ is exact.

With this definition, the following statements are equivalent:

(1) M is projective.
(2) For any surjection $f\colon N \twoheadrightarrow N'$ and any map $g\colon M \to N'$ there exists a map $h\colon M \to N$ such that $f \circ h = g$.
(3) M is a direct summand of a free module.

Since $\mathrm{Hom}(M,-)$ is left exact in any case, it is clear that (1) and (2) are equivalent. To see that (2) implies (3), note that taking for N any free module surjecting onto M, $N' = M$ and for g the identity, we get a map splitting the identity, thus establishing M as a direct summand of N. Conversely, any free module is easily seen to be projective. So, if $M \oplus N \simeq F$, then $\mathrm{Hom}(M,-) \oplus \mathrm{Hom}(N,-) \simeq \mathrm{Hom}(F,-)$ and the right hand side is exact, hence the same holds for the left hand side.

Proposition 9.1. *A finitely generated projective module P over a local ring A is free.*

Proof. Choose elements $m_1, \ldots, m_n \in P$ whose classes form a basis of the $A/\mathfrak{m} = k$-vector space $P/\mathfrak{m}P$. By Nakayama's lemma, the elements $m_1, \ldots, m_n$ generate P, hence the map

$$\alpha\colon A^n \longrightarrow P, (a_1, \ldots, a_n) \longmapsto \sum_i a_i m_i$$

is surjective. Now P is projective, so $A^n \simeq P \oplus \ker(\alpha)$. Since $k^n \simeq A^n/\mathfrak{m}A^n \simeq P/\mathfrak{m}P$, we have $\ker(\alpha) \subseteq \mathfrak{m}A^n$. Considering P as a submodule of A^n, we conclude that $A^n = P + \mathfrak{m}A^n$, hence $A^n \simeq P$ by Nakayama's lemma. □

Dually, a module M is called *injective* if $\mathrm{Hom}(-,M)$ is an exact functor or, equivalently, if for any injection $f\colon N \longrightarrow N'$ and any map $g\colon N \longrightarrow M$, there exists a map $h\colon N' \longrightarrow M$ making the appropriate diagram commutative.

An important fact concerning injective modules is

Proposition 9.2 (Baer's criterion)**.** *A module E is injective if and only if for every ideal I of A any map $I \longrightarrow E$ can be extended to $A \longrightarrow E$.*

Proof. Of course, the only if direction follows immediately from the definition of being injective.

Suppose $0 \longrightarrow M \longrightarrow N$ is exact and a map $\alpha\colon M \longrightarrow E$ is given. We need to show that α can be extended to a map $N \longrightarrow E$. Consider the partially ordered set of intermediate extensions $\alpha'\colon M' \longrightarrow E$, where $M \subseteq M' \subseteq N$. Any chain in this set has of course an upper bound, namely N, so by Zorn's lemma, there exists a maximal extension $\alpha'\colon M' \longrightarrow E$ and we will show that $M' = N$. Assume that there exists an element $n \in N \setminus M'$. The set $J = \{a \in A \mid an \in M'\}$ is an ideal in A. Therefore, the map

$$J \xrightarrow{n} M' \xrightarrow{\alpha'} E$$

extends to a map $f\colon A \longrightarrow E$. Let $M'' = M' + An \subseteq N$ and define $\alpha''\colon M'' \longrightarrow E$ by

$$\alpha''(m' + an) = \alpha'(m') + f(a).$$

Since $\alpha'(an) = f(a)$ for $an \in M' \cap An$, α'' is well-defined and extends α'. Therefore, $M' = N$. □

Notation. We will write $\mathrm{Mod}A$ for the category of A-modules and $\mathrm{mod}A$ for its subcategory of finitely generated A-modules.

Remark 9.3. Since every free module is projective, the category of A-modules has *enough projectives* meaning that for every module M there exists a projective module P surjecting onto M. This implies that any module has a *projective resolution*, that is, there exists an exact sequence

$$\ldots \longrightarrow P_i \longrightarrow P_{i-1} \longrightarrow \ldots \longrightarrow P_0 \longrightarrow M \longrightarrow 0,$$

where every P_k is projective.

Indeed, take any surjection $P = P_0 \twoheadrightarrow M$ and its kernel K. Now take a projective module P_1 surjecting onto K and consider the sequence $P_1 \twoheadrightarrow P_0 \twoheadrightarrow M$, where the first map is the composition of the surjection $P_1 \twoheadrightarrow K$ and the inclusion $K \hookrightarrow P_0$. Clearly, this sequence is exact and we can continue this process inductively.

Dually, we say that $\mathrm{Mod}A$ has *enough injectives* if every module embeds into an injective module. If this holds, then every module has an *injective resolution* defined in the obvious way. It is a fact that $\mathrm{Mod}A$ does have enough injectives.

We also need to recall derived functors in a special case. Firstly, recall that a sequence of A-modules

$$\ldots \longrightarrow M^{i-1} \xrightarrow{d^{i-1}} M^i \xrightarrow{d^i} M^{i+1} \longrightarrow \ldots$$

is a *complex* if $d^i \circ d^{i-1} = 0$ for all i. The *i-th cohomology* of the above complex $M^\bullet$ is $H^i(M^\bullet) := \ker(d^i)/\operatorname{im}(d^{i-1})$.

Now let M be an A-module and let $F\colon \mathrm{Mod}A \longrightarrow \mathrm{Mod}A$ be the functor $\mathrm{Hom}(M, -)$. For any module N, take an injective resolution of N, written as $N \hookrightarrow E^\bullet$. The *$i$-th* Ext*-group* $\mathrm{Ext}^i(M, N)$ is the module $H^i(\mathrm{Hom}(M, E^\bullet))$, that is, we take the i-th cohomology of the complex with objects $\mathrm{Hom}(M, E^k)$.

It is a fact that this definition does not depend on the injective resolution chosen and that $\mathrm{Ext}^0(M, N) = \mathrm{Hom}(M, N)$. Another fact is that the Ext-groups can also be computed by taking a projective resolution $P_\bullet$ of M and taking cohomology of the complex $\mathrm{Hom}(P_\bullet, N)$.

Another fact is that if $0 \longrightarrow N' \longrightarrow N \longrightarrow N'' \longrightarrow 0$ is a short exact sequence, we get a long exact sequence

$$0 \longrightarrow \mathrm{Hom}(M, N') \longrightarrow \mathrm{Hom}(M, N) \longrightarrow \mathrm{Hom}(M, N'') \longrightarrow \mathrm{Ext}^1(M, N') \longrightarrow \ldots$$

Similarly, if $0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$ is a short exact sequence, we get a long exact sequence

$$0 \longrightarrow \mathrm{Hom}(M'', N) \longrightarrow \mathrm{Hom}(M, N) \longrightarrow \mathrm{Hom}(M', N) \longrightarrow \mathrm{Ext}^1(M'', N) \longrightarrow \ldots$$

A similar thing can be done for the tensor product functor $G(-) = M \otimes -$ which is right exact. Namely, take a projective resolution $P_\bullet$ of any module N and define the *i-th Tor-group* $\mathrm{Tor}_i(N, M)$ as the i-th cohomology of the complex with objects $M \otimes P_k$.

Once again, it can be checked that we get the same result by taking a projective resolution of M and taking cohomology after we tensor this resolution with N. In fact, one can reduce to taking flat resolutions. Note that this is indeed a reduction since every

projective module is flat (use that a projective module is a direct summand of a free module and the latter is of course flat).

In this case, we also get a long exact sequence involving the Tor-groups starting from a short exact sequence.

9.2. **Global dimension.**

Definition. Let M be an A-module.

(1) The *projective dimension* $\mathrm{pdim}(M)$ of M is the minimum integer n, if it exists, such that there exists a projective resolution of M of length n

$$0 \longrightarrow P_n \longrightarrow \ldots \longrightarrow P_0 \longrightarrow M \longrightarrow 0.$$

(2) The *injective dimension* $\mathrm{idim}(M)$ of M is the minimum integer n, if it exists, such that there exists an injective resolution of M of length n

$$0 \longrightarrow M \longrightarrow E^0 \longrightarrow \ldots \longrightarrow E^n \longrightarrow 0.$$

In both cases, we set the respective dimension to be ∞ if no n exists.

Lemma 9.4. *The following statements are equivalent for an A-module M.*

i) $\mathrm{pdim}(M) \leq d$.
ii) $\mathrm{Ext}^k(M,N) = 0$ *for* $k > d$ *and all modules* N.
iii) $\mathrm{Ext}^{d+1}(M,N) = 0$ *for all modules* N.
iv) *If*

$$0 \longrightarrow S_d \longrightarrow P_{d-1} \longrightarrow \ldots \longrightarrow P_0 \longrightarrow M \longrightarrow 0$$

is any resolution with all the P_i projective, then the so-called syzygy S_d (the kernel of the map $P_{d-1} \longrightarrow P_{d-2}$) is also projective.

Proof. We know that $\mathrm{Ext}^*(M,N)$ can be computed by using a projective resolution of M, hence iv)⇒i)⇒ii)⇒ii). By dimension shifting (Exercise 2 on Sheet 12), $\mathrm{Ext}^{d+1}(M,N) \simeq \mathrm{Ext}^1(S_d,N)$ and S_d is projective if any only if $\mathrm{Ext}^1(S_d,N) \simeq 0$, hence iii) implies iv). □

The same arguments also prove

Lemma 9.5. *The following statements are equivalent for an A-module N.*

i) $\mathrm{idim}(N) \leq d$.
ii) $\mathrm{Ext}^k(M,N) = 0$ *for* $k > d$ *and all modules* M.
iii) $\mathrm{Ext}^{d+1}(M,N) = 0$ *for all modules* M.
iv) *If*

$$0 \longrightarrow N \longrightarrow E^0 \longrightarrow \ldots \longrightarrow E^{d-1} \longrightarrow S^d \longrightarrow 0$$

is any resolution with all the E^i injective, then the so-called syzygy S^d (the cokernel of the map $E^{d-2} \longrightarrow E^{d-1}$ is also injective.

□

Lemma 9.6. *A module M is injective if and only if $\mathrm{Ext}^1(A/I, M) = 0$ for all ideals I of A.*

Proof. Applying $\mathrm{Hom}(-, M)$ to the exact sequence

$$0 \longrightarrow I \longrightarrow A \longrightarrow A/I \longrightarrow 0$$

we get

$$\mathrm{Hom}(A, M) \longrightarrow \mathrm{Hom}(I, M) \longrightarrow \mathrm{Ext}^1(A/I, M) \longrightarrow 0.$$

By Baer's criterion, M is injective if and only if the first map is surjective, that is, if and only if $\mathrm{Ext}^1(A/I, M) = 0$. □

Theorem 9.7. *Let A be a ring. The following numbers are equal:*

(1) $\sup\{\mathrm{idim}(M) \mid M \in \mathrm{Mod}(A)\}$.
(2) $\sup\{\mathrm{pdim}(M) \mid M \in \mathrm{Mod}(A)\}$.
(3) $\sup\{\mathrm{pdim}(A/I) \mid I \subseteq A \text{ ideal}\}$.
(4) $\sup\{d : \mathrm{Ext}^d(M, N) \neq 0 \text{ for some } M, N \in \mathrm{Mod}(A)\}$.

This number is called the global dimension *of A and denoted by* $\mathrm{gdim}(A)$.

Proof. Lemmas 9.4 and 9.5 show that the numbers in (1), (2) and (4) are equal. Obviously, the number in (2) is at least the number in (3). So, assume that $d = \sup\{\mathrm{pdim}(A/I) \mid I \subseteq A \text{ ideal}\} < \infty$ and that there exists a module M such that $\mathrm{idim}(M) > d$. Choose an injective resolution

$$0 \longrightarrow M \longrightarrow E^0 \longrightarrow \ldots \longrightarrow E^{d-1} \longrightarrow N \longrightarrow 0$$

with all E^i injective. By dimension shifting we have, for any ideal I of A and by definition of d,

$$\mathrm{Ext}^1(A/I, N) \simeq \mathrm{Ext}^{d+1}(A/I, M) \simeq 0.$$

By the previous lemma, N is injective, hence $\mathrm{idim}(M) = d$, a contradiction. Therefore, the numbers in (2) and (3) also coincide and the theorem is proved. □

Our next goal will be to relate the global dimension to the other notions of dimension we had before. This will take a lot of preparation.

Proposition 9.8. *Let x be a non zero-divisor in a ring A. If $M \neq 0$ is an A/x-module such that $\mathrm{pdim}_{A/x}(M) < \infty$, then*

$$\mathrm{pdim}_A(M) = 1 + \mathrm{pdim}_{A/x}(M).$$

Proof. Since M is an A/x-module, we have $xM = 0$, so M cannot be a projective A-module. Indeed, otherwise $M \oplus N \simeq F$ would be a free module; but multiplication with x is injective on F, while M is in the kernel of this map, a contradiction. Therefore, $\mathrm{pdim}_A(M) \geq 1$. Note that $\mathrm{pdim}_A(A/x) = 1$, since

$$0 \longrightarrow A \xrightarrow{\cdot x} A \longrightarrow A/x \longrightarrow 0$$

is a projective resolution. If $\mathrm{pdim}_{A/x}(M) = 0$, so M is a projective A/x-module, then M is a direct summand of a free A/x-module, hence $\mathrm{pdim}_A(M) = \mathrm{pdim}_A(A/x) = 1$.

Assume that $\mathrm{pdim}_{A/x}(M) \geq 1$ and consider an exact sequence

$$0 \longrightarrow N \longrightarrow P \longrightarrow M \longrightarrow 0$$

with P a projective A/x-module. By dimension shifting, $\mathrm{pdim}_{A/x}(M) = \mathrm{pdim}_{A/x}(N)+1$. By induction on projective dimension, the proposition holds for N, hence $\mathrm{pdim}_A(N) = 1+\mathrm{pdim}_{A/x}(N) \geq 1$. Considering the above sequence as a sequence of A-modules, we note that $\mathrm{pdim}_A(P) = 1$. There are two possibilities: either, a) $\mathrm{pdim}_A(M) = \mathrm{pdim}_A(N) + 1$ and we are done, or b) $1 = \mathrm{pdim}_A(P) = \sup\{\mathrm{pdim}_A(N), \mathrm{pdim}_A(M)\}$. We will exclude the latter possibility.

Let F be a free A-module surjecting onto M and K be the kernel of the surjection, so we have an exact sequence

$$0 \longrightarrow K \longrightarrow F \longrightarrow M \longrightarrow 0.$$

If $\mathrm{pdim}_A(M) = 1$, then K has to be projective. Tensoring this sequence with $A/xA = A/x$ yields

$$0 \longrightarrow \mathrm{Tor}_1^A(M, A/x) \longrightarrow K/xK \longrightarrow F/xF \longrightarrow M \longrightarrow 0.$$

If $\mathrm{pdim}_{A/x}(M) \geq 2$, then $\mathrm{Tor}_1^A(M, A/x)$ has to be a projective A/x-module, because the modules K/xK and F/xF are of course projective over A/x. But, as can be easily seen from the definition of Tor by resolving A/x, we have

$$\mathrm{Tor}_1^A(M, A/x) \simeq \{m \in M \mid xm = 0\} \simeq M,$$

hence $\mathrm{pdim}_{A/x}(M) = 0$, a contradiction, since we have seen above that M is not a projective A/x-module. Therefore, $\mathrm{pdim}_A(M) \neq 1$, we excluded b) above and the proof is complete. □

Example 9.9. The conclusion of the theorem fails if $\mathrm{pdim}_{A/x}(M) = \infty$, but $\mathrm{pdim}_A(M) < \infty$. For instance, $\mathrm{pdim}_{\mathbb{Z}}(\mathbb{Z}/2\mathbb{Z}) = 1$, since

$$0 \longrightarrow \mathbb{Z} \xrightarrow{\cdot 2} \mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow 0$$

is a projective resolution of length 1.

On the other hand, $\mathrm{pdim}_{\mathbb{Z}/4\mathbb{Z}}(\mathbb{Z}/2\mathbb{Z}) = \infty$, since

$$\ldots \longrightarrow \mathbb{Z}/4\mathbb{Z} \xrightarrow{\cdot 2} \mathbb{Z}/4\mathbb{Z} \xrightarrow{\cdot 2} \mathbb{Z}/4\mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow 0$$

is a projective resolution of infinite length and one can easily check that no syzygy (that is, $\mathbb{Z}/2\mathbb{Z}$) of this resolution is projective.

Proposition 9.10. *Let x be a non zero-divisor in a ring A. If M is an A-module and x is a non zero-divisor on M, then* $\mathrm{pdim}_A(M) \geq \mathrm{pdim}_{A/x}(M/xM)$.

Proof. Clearly, there is nothing to prove if $\mathrm{pdim}_A(M) = \infty$, so let us assume that $\mathrm{pdim}_A(M) = n$. We will use induction on n. If M is a projective A-module, then M/xM is a projective A/xA-module, so the result is true for $n = 0$. If $\mathrm{pdim}_A(M) \neq 0$, consider an exact sequence

$$0 \longrightarrow K \longrightarrow F \longrightarrow M \longrightarrow 0,$$

where F is a free module and K is the kernel of the surjection $F \longrightarrow M$. By dimension shifting, $\mathrm{pdim}_A(K) = n - 1$ and by induction

$$\mathrm{pdim}_{A/x}(K/xK) \leq n - 1.$$

Tensoring the above sequence with A/x yields

$$0 \longrightarrow \mathrm{Tor}_1^A(M, A/x) \longrightarrow K/xK \longrightarrow F/xF \longrightarrow M/xM \longrightarrow 0.$$

Since $\mathrm{Tor}_1^A(M, A/x) \simeq 0$, either M/xM is projective or we have

$$\mathrm{pdim}_{A/x}(M/xM) = 1 + \mathrm{pdim}_{A/x}(K/xK) \leq 1 + (n-1) = \mathrm{pdim}_A(M).$$

□

Corollary 9.11. *Let A be a ring, $A[X]$ the polynomial ring over A, M be an A-module and $M[X]$ be the $A[X]$-module $M \otimes_A A[X]$. Then*

$$\mathrm{pdim}_{A[X]}(M[X]) = \mathrm{pdim}_A(M).$$

Proof. Note that X is a non zero-divisor on $M[X]$, that $A[X]/X \simeq A$ and $M[X]/X \simeq M$, hence $\mathrm{pdim}_{A[X]}(M[X]) \geq \mathrm{pdim}_A(M)$ by the previous proposition.

On the other hand, take any projective resolution $P_\bullet \longrightarrow M$ over A and note that $A[X] \otimes P_\bullet \longrightarrow M[X]$ is a projective resolution of $M[X]$, because $\mathrm{Hom}(A[X] \otimes N, -) \simeq \mathrm{Hom}(A[X], \mathrm{Hom}(N, -))$ for any A-module N and $A[X]$ is a free A-module. Therefore,

$$\mathrm{pdim}_{A[X]}(M[X]) \leq \mathrm{pdim}_A(M)$$

as well and the corollary is proved. □

Proposition 9.12. *If A is a ring, then* $\mathrm{gdim}(A[X_1, \ldots, X_r]) = n + \mathrm{gdim}(A)$.

Proof. By induction over r, we are reduced to prove the claim for $A[X]$. Of course, if $\mathrm{gdim}(A) = \infty$, then $\mathrm{gdim}(A[X]) = \infty$ by the previous corollary, so assume that $\mathrm{gdim}(A) = n < \infty$. By Proposition 9.8, $\mathrm{gdim}(A[X]) \geq 1 + \mathrm{gdim}(A) = 1 + n$.

To prove the other inequality, consider any $A[X]$-module M. Of course, M can be considered as an A-module, which we will write as M_A. Let

$$\beta \colon A[X] \otimes_A M_A \longrightarrow A[X] \otimes_A M_A, \quad t \otimes m \longmapsto t(X \otimes m - 1 \otimes Xm),$$

where $t \in A[X]$ and $m \in M$, and let $\mu \colon A[X] \otimes_A M_A \longrightarrow M$ be the multiplication map. Note that every nonzero element $f \in A[X] \otimes M_A$ can be written as

$$f = X^k \otimes m_k + \ldots + X \otimes m_1 + 1 \otimes m_0,$$

where $m_i \in M$ and $m_k \neq 0$. This implies that β is injective, since the leading term of $\beta(f) = X^{k+1} \otimes m_k$. It is also clear that $\mu \circ \beta = 0$. Hence, to see that the sequence

$$(*)\quad 0 \longrightarrow A[X] \otimes_A M_A \xrightarrow{\beta} A[X] \otimes_A M_A \xrightarrow{\mu} M \longrightarrow 0$$

is exact, we need to show that if $f \in \ker(\mu)$, then $f \in \mathrm{im}(\beta)$. We will do this by induction on k, the degree of f. The case $k = 0$ is trivial, since $\mu(1 \otimes f) = f$. If $k > 0$, then $\mu(f) = \mu(g)$, where $g = f - \beta(X^{k-1} \otimes m_k)$. Since $\deg(g) < \deg(f)$, if $f \in \ker(\mu)$, then $g \in \ker(\mu)$, so $g = \beta(h)$ for some h and therefore, $f = \beta(h + X^{k-1} \otimes m_k)$. We thus proved that $(*)$ is exact, which yields

$$\mathrm{pdim}_{A[X]}(M) \leq 1 + \mathrm{pdim}_{A[X]}(A[X] \otimes_A M_A) = 1 + \mathrm{pdim}_A(M_A) \leq 1 + n.$$

Since M was arbitrary, we conclude that $\mathrm{gdim}(A[X]) \leq 1 + n$. □

Lemma 9.13. *If A is a commutative Noetherian local ring, M a finitely generated A-module and if $x \in \mathfrak{m}$ is a non zero-divisor on both A and M, the following holds: If M/xM is a free A/x-module, then M is a free A-module.*

Proof. Choose elements $m_1, \ldots, m_n$ mapping onto a basis of M/xM. Since $(m_1, \ldots, m_n)A + xM = M$, Nakayama's lemma shows that $M = (m_1, \ldots, m_n)A$, hence we have a generating set.

Now suppose that $\sum_i a_i m_i = 0$ for some $a_i \in A$. Since the images of the m_i give a basis of M/xM, we have $a_i \in xA$ for all i. By assumption on x, we can divide to get $a_i/x \in A$ such that $\sum_i (a_i/x)m_i = 0$. We can continue this process to get a sequence of elements $a_i, a_i/x, a_i/x^2, \ldots$ and this sequence generates a strictly ascending chain of ideals of A. Since A is Noetherian, we have $a_i = 0$ for all i. □

Proposition 9.14. *If A is a Noetherian local ring with maximal ideal $\mathfrak{m}$, M is a finitely generated A-module and $x \in \mathfrak{m}$ is a non zero-divisor on both A and M, then* $\mathrm{pdim}_A(M) = \mathrm{pdim}_{A/x}(M/xM)$.

Proof. Proposition 9.10 gives the inequality $\geq$. We will prove equality by induction on $n = \mathrm{pdim}_{A/x}(M/xM)$. If $n = 0$, then M/xM is projective, hence free by Proposition 9.1. By the previous lemma, M is also free, hence projective. Therefore, the claim holds when $n = 0$.

Assume now that $n > 0$. Consider an exact sequence

$$0 \longrightarrow K \longrightarrow F \longrightarrow M \longrightarrow 0$$

with F a free module and K the kernel of the map $F \longrightarrow M$. As before, $\mathrm{Tor}_1^A(M, A/x) \simeq 0$, so we can tensor this sequence with A/x to get

$$0 \longrightarrow K/xK \longrightarrow F/xF \longrightarrow M/xM \longrightarrow 0.$$

As F/xF is free, $\mathrm{pdim}_{A/x}(K/xK) = n-1$. Since A is Noetherian, K is finitely generated, so, by induction, $\mathrm{pdim}_A(K) = n - 1$. This implies that $\mathrm{pdim}_A(M) = n$. □

Corollary 9.15. *Let A be a commutative Noetherian local ring, M be a finitely generated A-module with $\mathrm{pdim}_A(M) < \infty$. If $x \in \mathfrak{m}$ is a non zero-divisor on both A and M, then $\mathrm{pdim}_A(M/xM) = 1 + \mathrm{pdim}_A(M)$.*

Proof. Proposition 9.8 gives $\mathrm{pdim}_A(M/xM) = 1 + \mathrm{pdim}_{A/x}(M/xM)$ and the previous proposition gives $\mathrm{pdim}_A(M) = \mathrm{pdim}_{A/x}(M/xM)$. □

Remark 9.16. One can show that Propositions 9.8, 9.10 and 9.14 hold with pdim substituted by idim.

9.3. **Regular sequences, global dimension and regular rings.**

Definition. Let A be a Noetherian local ring and M be a finitely generated A-module. A *regular sequence* on M, or an *M-sequence*, is a sequence $(x_1, \dots, x_n)$ of elements in the maximal ideal $\mathfrak{m}$ such that x_1 is a non zero-divisor on M and each x_i is a non zero-divisor on $M/(x_1, \dots, x_{i-1})M$ for $i > 1$. The *depth* $\mathrm{depth}(M)$ of M is the length of the longest regular sequence on M. In particular, the *depth* of A is defined.

Remark 9.17. For any local Noetherian ring A we have $\mathrm{depth}(A) \leq \dim(A)$. Indeed, recall that the set of zero-divisors is the union of the associated primes of A by Proposition 6.33. By Proposition 6.39, every minimal prime of A is associated, hence any non zero-divisor is not contained in the union of the minimal primes of A. Induction then gives $0 \leq \dim(A/\underline{x}A) = \dim(A) - n$, where $\underline{x} = (x_1, \dots, x_n)$ is a regular sequence.

Here is one simple result concerning regular sequences.

Proposition 9.18. *Let A be a local Noetherian ring, M be an A-module and $x_1, \dots, x_n$ be elements in $\mathfrak{m}$. For any $i < n$, the following statements are equivalent.*

1. *$x_1, \dots, x_n$ is a regular sequence on M.*
2. *$x_1, \dots, x_i$ is a regular sequence on M and $x_{i+1}, \dots, x_n$ is a regular sequence on $M/(x_1, \dots, x_i)M$.*

Proof. This follows from the easily proved fact that if I and J are ideals in any ring A and N is any A-module, then $N'/JN' \simeq N/(I+J)N$, where $N' = N/IN$. □

Another simple statement is

Proposition 9.19. *If $(x_1, \dots, x_n)$ is a regular sequence on M, then the chain of ideals (x_1), (x_1, x_2), ... is strictly ascending.*

Proof. Assume the converse, so there exists an i such that $(x_1, \dots, x_i) = (x_1, \dots, x_{i+1})$. This implies $x_{i+1} \in (x_1, \dots, x_i)$, hence x_{i+1} is a zero-divisor on $M/(x_1, \dots, x_i)M$, a contradiction. □

In view of Remark 9.17, the following definition is reasonable.

Definition. A local Noetherian ring A is called *Cohen-Macaulay* if $\mathrm{depth}(A) = \dim(A)$.

Example 9.20. Every zero-dimensional local Noetherian ring A is Cohen-Macaulay, but by Proposition 8.31 A is not regular unless it is a field.

Unless the maximal ideal consists entirely of zero-divisors, any 1-dimensional local Noetherian ring A is Cohen-Macaulay. However, A is regular only if A is a discrete valuation ring. For example, $k[[x^2, x^3]]$ is Cohen-Macaulay but not regular.

Convention. Until the end of this section we will always assume that our rings are Noetherian.

Proposition 9.21. *Any regular local ring A is Cohen-Macaulay and any set of elements $x_1, \dots, x_d \in \mathfrak{m}$ mapping to a basis of $\mathfrak{m}/\mathfrak{m}^2$ is an A-sequence.*

Proof. We already know that $\operatorname{depth}(A) \leq \dim(A)$. If $x_1 \in A$ is not a zero-divisor on A, it suffices to prove that $x_2, \dots, x_d$ form a regular sequence on A/x_1A. This follows by induction on d and Proposition 9.18. □

For the following result we recall some of the facts proved before. If every element in the maximal ideal $\mathfrak{m}$ of a local ring A is a zero-divisor on a finitely generated A-module M, then $\mathfrak{m} = \operatorname{Ann}(m)$ for some $0 \neq m \in M$. Indeed, by Proposition 6.33 the zero-divisors of M coincide with the union of all primes associated with M, hence $\mathfrak{m}$ is contained in this union and, therefore, has to be one of the associated primes by Proposition 2.21i). If this is the case, then $k = A/\mathfrak{m} \simeq Am \subseteq M$. In particular, if $\operatorname{depth}(M) = 0$ (so every element of $\mathfrak{m}$ is a zero-divisor on M), then $\operatorname{Hom}_A(k, M) \neq 0$.

If $\operatorname{depth}(M) \neq 0$ and $\operatorname{depth}(A) \neq 0$, then some element of $\mathfrak{m} \setminus \mathfrak{m}^2$ must be a non zero-divisor on both A and M. First of all, note that if $\mathfrak{p}_1, \dots, \mathfrak{p}_i$ are the associated primes of A and $\mathfrak{q}_1, \dots, \mathfrak{q}_j$ are the associated primes of M, then the assumptions give that $\mathfrak{m} \subsetneq \mathfrak{p}_1 \cup \dots \cup \mathfrak{p}_i$ and $\mathfrak{m} \subsetneq \mathfrak{q}_1 \cup \dots \cup \mathfrak{q}_j$, hence by prime avoidance $\mathfrak{m} \subsetneq \mathfrak{p}_1 \cup \dots \cup \mathfrak{p}_i \cup \mathfrak{q}_1 \cup \dots \cup \mathfrak{q}_j$. Hence, there exists an element $x \in \mathfrak{m}$ which is a non zero-divisor on both A and M. One can then argue that we can achieve that $x \in \mathfrak{m} \setminus \mathfrak{m}^2$.

Furthermore, recall that if $x \in \mathfrak{m}$ is a non zero-divisor on A, then $\dim(A/x) = \dim(A) - 1$ by Corollary 8.28.

Theorem 9.22. *If A is a local ring and M is a non-zero finitely generated A-module, then every maximal M-sequence has the same length* $\operatorname{depth}(M)$. *Moreover,* $\operatorname{depth}(M)$ *is the smallest n such that* $\operatorname{Ext}^n_A(k, M) \neq 0$, *where $k = A/\mathfrak{m}$.*

Proof. We will use induction on the length n of a maximal M-sequence.

We have already argued that if $\operatorname{depth}(M) = 0$, then $\operatorname{Hom}_A(k, M) \neq 0$. Conversely, if $\operatorname{Hom}_A(k, M) \neq 0$, then for some $0 \neq m \in M$ we have $Am \simeq k$, hence $xm = 0$ for all $x \in \mathfrak{m}$. Therefore, $\operatorname{depth}(M) = 0$ in this case.

Now assume $n \geq 1$ and $x_1, \dots, x_n$ is a maximal M-sequence. Since $x = x_1$ is a non zero-divisor on M, the sequence

$$0 \longrightarrow M \xrightarrow{\cdot x} M \longrightarrow M/xM \longrightarrow 0$$

is exact and $x_2, \dots, x_n$ is a maximal regular sequence on M/xM. Applying $\mathrm{Hom}(k, -)$ to the above exact sequence, we get

$$\dots \longrightarrow \mathrm{Ext}^{i-1}(k, M) \xrightarrow{\cdot x} \mathrm{Ext}^{i-1}(k, M) \longrightarrow \mathrm{Ext}^{i-1}(k, M/xM) \longrightarrow$$

$$\longrightarrow \mathrm{Ext}^{i}(k, M) \xrightarrow{\cdot x} \mathrm{Ext}^{i}(k, M) \longrightarrow \dots$$

Since $xk = 0$, $\mathrm{Ext}^i(k, M)$ is a module over A/xA and the first and last maps in the previous exact sequence are zero. By induction, $\mathrm{Ext}^i(k, M) = 0$ for $0 \leq i < n$ and $\mathrm{Ext}^n(k, M) \neq 0$. □

Lemma 9.23. *Let $(A, \mathfrak{m})$ be a local Noetherian ring, $\mathfrak{p} \neq \mathfrak{m}$ be a prime ideal and let M be a finitely generated A-module. If $\mathrm{Ext}^{i+1}(A/\mathfrak{q}, M) = 0$ for every prime ideal $\mathfrak{q}$ properly contaning $\mathfrak{p}$, then $\mathrm{Ext}^i(A/\mathfrak{p}, M) = 0$.*

Proof. Let $x \in \mathfrak{m} \setminus \mathfrak{p}$ and write $B = A/\mathfrak{p}$. Note that x is not a zero-divisor on B and we have an exact sequence

$$0 \longrightarrow B \xrightarrow{\cdot x} B \longrightarrow B/xB \longrightarrow 0$$

which induces

$$(*)\ \mathrm{Ext}^i(B, M) \xrightarrow{\cdot x} \mathrm{Ext}^i(B, M) \longrightarrow \mathrm{Ext}^{i+1}(B/xB, M).$$

Note that B/xB is a finitely generated A-module, so applying Proposition 6.35(1) we see that this module admits a filtration with quotients of the form $A/\mathfrak{q}$ with $\mathfrak{q}$ properly contaning $\mathfrak{p}$. It follows that the last term in $(*)$ vanishes, so the first map is surjective. Since M is finitely generated, Nakayama's lemma implies that $\mathrm{Ext}^i(B, M) = 0$. □

Proposition 9.24. *If A is a local ring and M a finitely generated A-module, then*

$$\mathrm{idim}(M) \leq d \Longleftrightarrow \mathrm{Ext}^n_A(k, M) = 0\ \forall n > d.$$

Hence, the injective dimension of a module M is the largest integer n such that $\mathrm{Ext}^n(k, M) \neq 0$.

Proof. Only one direction needs a proof. So assume that $\mathrm{Ext}^n_A(k, M) = 0\ \forall n > d$ and let $\mathfrak{p}$ be any prime ideal. If $\mathfrak{p} = \mathfrak{m}$, there is nothing to prove. Otherwise, $\mathfrak{p}$ is strictly contained in $\mathfrak{m}$. If $\mathfrak{m}$ is the only prime ideal containing $\mathfrak{p}$, then $\mathrm{Ext}^i(A/\mathfrak{p}, M) = 0$ for appropriate i by the previous lemma. If there is a prime ideal $\mathfrak{q}$ strictly containing $\mathfrak{p}$ and strictly contained in $\mathfrak{m}$, then $\mathrm{Ext}^i(A/\mathfrak{q}, M) = 0$ by the previous lemma and induction on $l = \mathrm{height}(\mathfrak{m}) - \mathrm{height}(\mathfrak{q})$. Hence, $\mathrm{Ext}^i(A/\mathfrak{p}, M) = 0$ for all prime ideals $\mathfrak{p}$ and all $i \geq d$. Using Proposition 6.35(1) again, this implies that $\mathrm{Ext}^i(N, M) = 0$ for any finitely generated A-module N, which is enough to conclude that $\mathrm{idim}(M) \leq d$. □

Definition. A local ring A is called *Gorenstein* if $\mathrm{idim}_A(A) < \infty$.

Theorem 9.25. *Any Gorenstein ring A is Cohen-Macaulay and*

$$\operatorname{depth}(A) = \operatorname{idim}_A(A) = \dim(A).$$

In particular,

$$\operatorname{Ext}^q(k, A) \neq 0 \Longleftrightarrow q = \dim(A),$$

since $\operatorname{depth}(A)$ *is the smallest q such that the Ext-group does not vanish and* $\operatorname{idim}(A)$ *the largest q.*

Proof. Theorem 9.22 shows that $\operatorname{depth}(A)$ is the smallest q such that $\operatorname{Ext}^q_A(k, A) \neq 0$. Combined with the previous proposition this shows that $\operatorname{depth}(A) \leq \operatorname{idim}(A)$.

Suppose that $\operatorname{depth}(A) = 0$ but $\operatorname{idim}(A) \neq 0$. For each $a \in A$ and $n \geq 0$ we have an exact sequence

$$\operatorname{Ext}^n(A, A) \longrightarrow \operatorname{Ext}^n(aA, A) \longrightarrow \operatorname{Ext}^{n+1}(A/aA, A)$$

Note that the left term is zero, since A is free. For $n = \operatorname{idim}(A) > 0$, the right term is also zero, so $\operatorname{Ext}^n(aA, A) = 0$ as well. But choosing a such that $aA = k$ shows that $\operatorname{Ext}^n(k, A) \neq 0$. Therefore, if $\operatorname{depth}(A) = 0$, then also $\operatorname{idim}(A) = 0$.

Now assume that $\operatorname{depth}(A) = d > 0$. Choose a non zero-divisor $x \in \mathfrak{m}$ and set $B = A/xA$. By the injective dimension version of Proposition 9.14 we have $\operatorname{idim}_B(B) = \operatorname{idim}_A(A) - 1$, hence B is still Gorenstein. By induction, B is Cohen-Macaulay and $\operatorname{depth}(B) = \operatorname{idim}_B(B) = \dim(B) = \dim(A) - 1$. Therefore, $\operatorname{idim}_A(A) = \dim(A)$. If $x_2, \ldots, x_d$ are elements of $\mathfrak{m}$ mapping onto a maximal B-sequence in $\mathfrak{m}B$, then $x_1, \ldots, x_d$ form a maximal A-sequence, hence $\operatorname{depth}(A) = \operatorname{depth}(B) + 1 = \dim(A)$. □

Remark 9.26. If M is a module over an arbitrary ring, then, substituting projective resolutions by flat resolutions leads to the notion of flat dimension of M, denoted by $\operatorname{fdim}(M)$. Since every projective module is flat, we have $\operatorname{fdim}(M) \leq \operatorname{pdim}(M)$. Furthermore, it is easy to see that $\operatorname{fdim}(M) \leq d$ if and only if $\operatorname{Tor}_{d+1}(M, N) = 0$ for all modules N. Since Tor is symmetric, the last condition is equivalent to $\operatorname{Tor}_{d+1}(N, M) = 0$.

Proposition 9.27. *If A is local with residue field k and M is a finitely generated A-module, then for every integer d we have*

$$\operatorname{pdim}(M) \leq d \Longleftrightarrow \operatorname{Tor}_{d+1}(M, k) = 0.$$

In particular, $\operatorname{pdim}(M)$ *is the largest d such that* $\operatorname{Tor}_d(A, k) \neq 0$.

Proof. Since $\operatorname{fdim}(M) \leq \operatorname{pdim}(M)$, the implication "⇒" is clear by the previous remark.

We will prove the converse by induction on d. By Nakayama's lemma, the module M can be generated by $n = \dim_k(M/\mathfrak{m}M)$ elements, so let $\{m_1, \ldots, m_n\}$ be a minimal set of generators. Consider the surjection

$$\epsilon\colon A^n \twoheadrightarrow M, \quad (a_1, \ldots, a_n) \mapsto \sum_i a_i m_i$$

and its kernel $K = \ker(\epsilon)$. If $d = 0$, then $\operatorname{Tor}_1(M, k) = 0$, so we get an exact sequence

$$0 \longrightarrow K \otimes k \longrightarrow A^m \otimes k \longrightarrow M \otimes k \longrightarrow 0.$$

Note that $K \otimes k \simeq K \otimes A/\mathfrak{m} \simeq K/\mathfrak{m}K$, $A^m \otimes k \simeq k^n$ and $M \otimes k \simeq M/\mathfrak{m}M$. By construction, the map $A^m \longrightarrow M \otimes k$ is just $\epsilon \otimes k$ and an isomorphism, hence $K/\mathfrak{m}K = 0$, so $K = 0$ by Nakayama's lemma and thus $M \simeq A^n$ is free and, in particular, $\operatorname{pdim}(M) = 0$.

The inductive step is relatively easy. Namely, if $d > 0$, then

$$\operatorname{Tor}_{d+1}(M, k) = \operatorname{Tor}_d(K, k)$$

and $\operatorname{pdim}(M) \leq 1 + \operatorname{pdim}(K)$. □

Corollary 9.28. *If A is a local ring, then* $\operatorname{gdim}(A) = \operatorname{pdim}_A(A/\mathfrak{m})$.

Proof. By the proposition, $\operatorname{pdim}(A/I) \leq \operatorname{fdim}(A/\mathfrak{m})$ for any ideal I, hence

$$\begin{aligned} \operatorname{pdim}(A/\mathfrak{m}) \leq \operatorname{gdim}(A) = \sup\{\operatorname{pdim}(A/I)\} \leq \operatorname{fdim}(A/\mathfrak{m}) \\ \leq \operatorname{pdim}(A/\mathfrak{m}). \end{aligned}$$

□

Corollary 9.29. *If A is a local ring and $x \in \mathfrak{m}$ is a non zero-divisor on A, then either* $\operatorname{gdim}(A/x) = \infty$ *or* $\operatorname{gdim}(A) = 1 + \operatorname{gdim}(A/x)$.

Proof. Set $B = A/x$, note that B is still local and assume $\operatorname{gdim}(B) = d$ is finite. Applying Proposition 9.8 with $M = k = A/\mathfrak{m}$, we get

$$\operatorname{gdim}(A) = \operatorname{pdim}_A(k) = 1 + \operatorname{pdim}_B(k) = 1 + \operatorname{gdim}(B) = 1 + d.$$

□

Lemma 9.30. *If A is local and* $\operatorname{depth}(A) = 0$*, then for any finitely generated A-module M we have either* $\operatorname{pdim}(M) = 0$ *or* $\operatorname{pdim}(M) = \infty$.

Proof. Assume for the converse that $0 < \operatorname{pdim}(M) < \infty$. In this case an appropriate syzygy N of M will be finitely generated (as a submodule of a finitely generated module) and have $\operatorname{pdim}(N) = 1$ (by dimension shifting). Using Nakayama's lemma we see that N can be generated by $n = \dim_k(N/\mathfrak{m}N)$ elements, so choose a minimal set of generators $\{u_1, \ldots, u_n\}$ of N. As before, let $\epsilon\colon A^n \longrightarrow N$ be the natural projection and consider its kernel P. By dimension shifting, $\operatorname{pdim}(P) = 0$, so P is projective. Since $A^n/\mathfrak{m}A^n \simeq k^n \simeq N/\mathfrak{m}N$ by assumption, we have $P \subseteq \mathfrak{m}A^n$. Choosing any $a \in A$ such that $\mathfrak{m} = \operatorname{Ann}(a)$ shows that $aP = 0$. But P is projective over a local ring, hence free by Proposition 9.1, so $a = 0$, a contradiction. □

Theorem 9.31 (Auslander-Buchsbaum formula)**.** *Let A be a local ring and M be a finitely generated A-module. If* $\operatorname{pdim}(M) < \infty$*, then* $\operatorname{depth}(A) = \operatorname{depth}(M) + \operatorname{pdim}(M)$.

Proof. If $\operatorname{depth}(A) = 0$ and $\operatorname{pdim}(M) < \infty$, then M is projective by the previous lemma, hence free, so $M \simeq A^n$. In particular, $\operatorname{pdim}(M) = 0$ and $\operatorname{depth}(A) = \operatorname{depth}(M)$.

Now suppose $\operatorname{depth}(A) \neq 0$ but $\operatorname{depth}(M) = 0$. The latter statement implies that every element of $\mathfrak{m}$ is a zero-divisor on M, hence $\mathfrak{m}$ is an associated prime of M. Choose

$x \in \mathfrak{m}$ and $0 \neq m \in M$ such that x is not a zero-divisor on A and $\mathfrak{m} = \mathrm{Ann}(m)$. As before, resolve M

$$0 \longrightarrow K \longrightarrow A^n \xrightarrow{\epsilon} M \longrightarrow 0$$

and choose an element $u \in A^n$ with $\epsilon(u) = m$. It follows that $u\mathfrak{m} \subseteq K$, hence $xu \in K$ and $\mathfrak{m}(xu) \subseteq xK$. However, since $u \notin K$, $xu \notin xK$, because otherwise $xu = xl$ for some $l \in K$, hence $x(u - l) = 0$, but x is not a zero-divisor on A^n. Given any $y \in \mathfrak{m}$, the multiplication by y on K/xK is not injective (so y is a zero-divisor on K), because $yxu = 0$ but $xu \neq 0 \in K/xK$. To put it differently, $\mathrm{depth}(K/xK) = 0$. Since K is a submodule of the free module A^n, x is still not a zero-divisor on K. As by assumption $0 < \mathrm{depth}(A) \neq \mathrm{depth}(M) = 0$, so M is not free, Proposition 9.14 gives

$$\mathrm{pdim}_{A/x}(K/xK) = \mathrm{pdim}_A(K) = \mathrm{pdim}_A(M) - 1.$$

Using that $\mathrm{depth}(A/x) = \mathrm{depth}(A) - 1$, induction on $\mathrm{depth}(A)$ gives

$$\begin{aligned}\mathrm{depth}(A) &= \mathrm{depth}(A/x) + 1 = 1 + \mathrm{depth}(K/xK) + \mathrm{pdim}_{A/x}(K/xK) \\ &= 1 + 0 + \mathrm{pdim}_A(M) - 1 = \mathrm{pdim}_A(M).\end{aligned}$$

From now on we assume that the statement holds for any depth of A.

Next, consider the case $\mathrm{depth}(A) \neq 0$, $\mathrm{depth}(M) \neq 0$. Pick $x \in \mathfrak{m}$ which is not a zero-divisor on both A and M. Considering a maximal M-sequence starting with x, we have $\mathrm{depth}(M/xM) = \mathrm{depth}(M) - 1$. Induction on $\mathrm{depth}(M)$ and Corollary 9.15 give

$$\begin{aligned}\mathrm{depth}(A) &= \mathrm{depth}(M/xM) + \mathrm{pdim}_A(M/xM) \\ &= (\mathrm{depth}(M) - 1) + (1 + \mathrm{pdim}_A(M)) \\ &= \mathrm{depth}(M) + \mathrm{pdim}_A(M).\end{aligned}$$

□

We now come to the main result of this section.

Theorem 9.32. *A local ring A is regular if and only if $\mathrm{gdim}(A) < \infty$. In this case*

$$\mathrm{depth}(A) = \dim(A) = \mathrm{gdim}(A) = \mathrm{pdim}_A(k) = \dim_k(\mathfrak{m}/\mathfrak{m}^2),$$

where $k = A/\mathfrak{m}$. In particular, any regular ring is Gorenstein.

Proof. First of all note that the third equality holds for any local ring by Corollary 9.28, that A is regular if and only if $\dim(A) = \dim_k(\mathfrak{m}/\mathfrak{m}^2)$ and the regularity of A also implies that $\mathrm{depth}(A) = \dim(A)$ by Proposition 9.21.

Suppose that A is regular. We will perform induction on the dimension of A. If $\dim(A) = 0$, then A is a field, hence $\mathrm{gdim}(A) = 0$ as claimed.

If $\dim(A) = d > 0$, choose an A-sequence $x_1, \ldots, x_d$ generating the maximal ideal $\mathfrak{m}$ and set $B = A/x_1$. Then $x_2, \ldots, x_d$ is a B-sequence generating the maximal ideal $\mathfrak{m}'$ of B, hence B is regular of dimension $d - 1$. We have $\mathrm{gdim}(A) = \mathrm{pdim}_A(k)$ and

$\operatorname{gdim}(B) = \operatorname{pdim}_B(B/\mathfrak{m}') = \operatorname{pdim}_B(k)$. By Proposition 9.8, $\operatorname{pdim}_B(k) + 1 = \operatorname{pdim}_A(k)$, so by induction on d, we have

$$\operatorname{gdim}(A) = 1 + \operatorname{gdim}(B) = 1 + (d-1) = d.$$

Thus, if A is regular, then $\dim(A) = \operatorname{gdim}(A) < \infty$.

In the other direction we will also use induction, this time on the global dimension of A. If $\operatorname{gdim}(A) = 0$, then every module over A is projective, hence free, so A must be a field, so it is regular of dimension 0.

If $0 < \operatorname{gdim}(A) < \infty$, then Lemma 9.30 tells us that $\operatorname{depth}(A) \neq 0$, hence $\mathfrak{m}$ contains a non zero-divisor x. We can assume that $x = x_1 \notin \mathfrak{m}^2$. Our strategy to establishing the regularity of A is to prove that $B = A/x$ is regular. Indeed, $\dim(B) = \dim(A) - 1$, so the maximal ideal $\mathfrak{m}B$ of B is generated by a B-sequence $y_2, \ldots, y_d$ and lifting the y_i to elements $x_i \in \mathfrak{m}$ gives an A-sequence $x_1, \ldots, x_d$ generating $\mathfrak{m}$, proving that A is regular.

Applying Proposition 9.14 with $A = B$ and $M = \mathfrak{m}$ (here we use that $x \notin \mathfrak{m}^2$) we get

$$\operatorname{pdim}_B(\mathfrak{m}/x\mathfrak{m}) = \operatorname{pdim}_A(\mathfrak{m}) = \operatorname{pdim}_A(k) - 1 = \operatorname{gdim}(A) - 1,$$

where the second equality stems from the exact sequence

$$0 \longrightarrow \mathfrak{m} \longrightarrow A \longrightarrow A/\mathfrak{m} = k \longrightarrow 0$$

and the third is Corollary 9.28.

Clearly, the image of $\mathfrak{m}/x\mathfrak{m}$ in B is the maximal ideal $\mathfrak{m}' = \mathfrak{m}/Ax$ of B, so we have exact sequences

$$0 \longrightarrow Ax/x\mathfrak{m} \longrightarrow \mathfrak{m}/x\mathfrak{m} \longrightarrow \mathfrak{m}' \longrightarrow 0$$

and

$$0 \longrightarrow \mathfrak{m}' \longrightarrow B \longrightarrow k \longrightarrow 0.$$

By definition and symmetry of Tor,

$$Ax/x\mathfrak{m} \simeq \operatorname{Tor}_1^A(A/x, k) \simeq \operatorname{Tor}_1^A(k, A/x) \simeq \{a \in k \mid xa = 0\} = k.$$

Furthermore, the image of x in $Ax/x\mathfrak{m}$ is not zero. We will show that $\mathfrak{m}/x\mathfrak{m} \simeq \mathfrak{m}' \oplus k$ as B-modules, which will give

$$\operatorname{gdim}(B) = \operatorname{pdim}_B(k) \leq \operatorname{pdim}_B(\mathfrak{m}/x\mathfrak{m}) = \operatorname{gdim}(A) - 1,$$

hence by induction on the global dimension we can then conclude that B is regular.

So we only need to show that $\mathfrak{m}/x\mathfrak{m} \simeq \mathfrak{m}' \oplus k$ as B-modules. Set $r = \dim_k(\mathfrak{m}/\mathfrak{m}^2)$ and choose elements $x_2, \ldots, x_r$ in $\mathfrak{m}$ such that the images of $x = x_1, \ldots, x_r$ give a basis of $\mathfrak{m}/\mathfrak{m}^2$. Set $I = (x_2, \ldots, x_r)A + x\mathfrak{m}$ and note that $I/x\mathfrak{m} \subseteq \mathfrak{m}/x\mathfrak{m}$ maps onto $\mathfrak{m}B = \mathfrak{m}'$. Since we have seen above that the kernel $Ax/x\mathfrak{m}$ of the map $\mathfrak{m}/x\mathfrak{m} \longrightarrow \mathfrak{m}' = \mathfrak{m}B$ is isomorphic to k and contains $x \notin I$, it follows that

$$(xA/x\mathfrak{m}) \cap (I/x\mathfrak{m}) = 0.$$

Thus, $I/x\mathfrak{m} \simeq \mathfrak{m}B$ and $k \oplus \mathfrak{m}B \simeq \mathfrak{m}/x\mathfrak{m}$ finishing the proof of the theorem. □

Corollary 9.33. *If A is a regular local ring, and $\mathfrak{p} \in \operatorname{Spec}(A)$, then $A_\mathfrak{p}$ is a regular local ring.*

Proof. We will show that if S is any multiplicatively closed subset of A, then $S^{-1}A$ has finite global dimension. To see this, let M be any $S^{-1}A$-module. Considering M as an A-module, we can choose a projective resolution $P_\bullet \longrightarrow M$ which is of finite length bounded by $\operatorname{gdim}(A)$. Note that if P is a projective A-module, then $S^{-1}P$ is a projective $S^{-1}A$-module (use that a projective module is the direct summand of a free module). Since $S^{-1}A$ is flat over A, and $S^{-1}M = M$, the localised sequence $S^{-1}P_\bullet \longrightarrow M$ is a projective resolution of M of finite length. □

Example 9.34. We have seen that any regular ring is Gorenstein and any Gorenstein ring is Cohen-Macaulay. These implications are strict. For example, it can be shown with Baer's criterion that $A = \mathbb{C}[X]/(X^2)$ is a Gorenstein ring, but it is clearly not regular. To show that the other inclusion is also strict, we first need to recall that for a Gorenstein ring we have

$$\operatorname{Ext}^q(k, A) = \begin{cases} 0 & q \neq \dim(A) \\ \neq 0 & q = \dim(A). \end{cases}$$

In fact, in this case $\operatorname{Ext}^{\dim(A)}(k, A) \simeq k$. Let us prove the last statement by induction on $\operatorname{idim}(A)$. If $\operatorname{idim}(A) = \operatorname{depth}(A) = 0$, then $\mathfrak{m}$ is an associated prime, hence $\mathfrak{m} = \operatorname{Ann}(x)$ for some $0 \neq x \in A$, so there exists an injection $A/\mathfrak{m} = k \longrightarrow A$. Since A is injective, any map $k \longrightarrow A$ can be lifted to a map from A to A, so there is a surjection $A = \operatorname{Hom}(A, A) \longrightarrow \operatorname{Hom}(k, A)$. Hence, the latter module can be generated by one element and since we already know that it is non-trivial, it is isomorphic to k. Now, A is injective, so all the higher Ext-groups vanish in this case. To conclude the proof, we use induction. Let y be a non zero-divisor on A and set $B = A/y$. Then $\dim(B) = \dim(A) - 1$. A part of the long exact Ext-sequence of the exact sequence

$$0 \longrightarrow A \xrightarrow{\cdot y} A \longrightarrow B \longrightarrow 0$$

then reads

$$\operatorname{Ext}^i(k, A) \longrightarrow \operatorname{Ext}^i(k, A) \longrightarrow \operatorname{Ext}^i(k, B) \longrightarrow \operatorname{Ext}^{i+1}(k, A) \longrightarrow \dots$$

and induction gives the claim.

Now, to see that there are Cohen-Macaulay rings which are not Gorenstein, one can consider, for example, $A = \mathbb{C}[X, Y]/(X^2, Y^2, XY)$. Note that this is a 0-dimensional local ring, hence Cohen-Macaulay. However, it is not Gorenstein by the above criterion, since mapping 1 to X or to Y gives a two-dimensional space of A-linear maps from $\mathbb{C}$ to A. One can also check that A does not satisfy Baer's criterion (take $I = (X, Y)$ and the map $I \longrightarrow A$ given by sending X to Y and Y to X; this map cannot be lifted), hence is not injective.

10. Differentials

10.1. **Construction and some properties.**

Definition. Let B be a ring and M be a B-module. A *derivation* is a map of abelian groups $d\colon B \longrightarrow M$ which satisfies the *Leibniz rule*

$$d(ab) = d(a)b + ad(b)$$

for all $a, b \in B$.

If B is an algebra over a ring A, then we say that the derivation d is A-*linear* if d is a map of A-modules.

The set $\mathrm{Der}_A(B, M)$ of all A-linear derivations $B \longrightarrow M$ is a B-module with scalar multiplication defined by

$$bd\colon a \longmapsto b(d(a)).$$

Example 10.1. Let $B = k[x, y]$. The partial derivative $d = \partial/\partial x$ is a derivation from B to itself. Obviously, d is k-linear, but, in fact, it is even $k[y]$-linear.

Remark 10.2. If $d\colon B \longrightarrow M$ is a derivation, then $d(1) = 0$, since $d(1 \cdot 1) = d(1)1 + 1d(1)$.

In particular, d is A-linear if and only if $da = 0$ for all $a \in A$. Indeed, if d is A-linear, then $da = d(a \cdot 1) = ad(1) = 0$. Conversely, if $da = 0$ for all $a \in A$, then $d(ab) = d(a)b + ad(b) = ad(b)$, so d is A-linear.

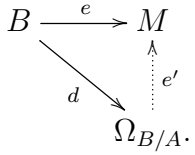
Definition. Let B be an A-algebra. The *module of Kähler differentials* of B over A, denoted by $\Omega_{B/A}$, is the B-module generated by $\{d(b) \mid b \in B\}$ subject to the following relations

$$d(bb') = d(b)b' + d(b')b$$
$$d(ab + a'b') = ad(b) + a'd(b'),$$

where $a, a' \in A$ and $b, b' \in B$. The map $d\colon B \longrightarrow \Omega_{B/A}$, $b \longmapsto db := d(b)$ is an A-linear derivation, called the *universal A-linear derivation*.

Remark 10.3. Note that the second class of relations corresponds to A-linearity, or, by Remark 10.2 to demanding that $da = 0$ for all $a \in A$.

Proposition 10.4. *The pair $(\Omega_{B/A}, d)$ defined above satisfies the following universal property: For any B-module M and any A-linear derivation $e\colon B \longrightarrow M$, there is a unique B-linear map $e'\colon \Omega_{B/A} \longrightarrow M$ such that $e = e'd$, that is, the following diagram is commutative*



Hence, $\mathrm{Der}_A(B, M) \simeq \mathrm{Hom}_A(\Omega_{B/A}, M)$.

Proof. We define $e'(db) = e(b)$. This defines a B-linear map which completes the diagram as desired. The rest of the proof proceeds along the same lines as in the case of the tensor product and is therefore omitted. □

Remark 10.5. The proposition says that $\Omega_{B/A}$ "linearises" derivations, in the same sense as the tensor product linearises bilinear maps.

Remark 10.6. If B is generated by the set $\{b_i \mid i \in I\}$ as an A-algebra, then $\Omega_{B/A}$ is generated by $\{db_i \mid i \in I\}$ as a B-module. Indeed, any element b in B is a polynomial in the b_i with coefficients in A, so applying d and using the Leibniz rule allows us to express db as a B-linear combination of the db_i ($da = 0$ for all $a \in A$). In particular, if B is a finitely generated A-algebra, then $\Omega_{B/A}$ is a finitely generated B-module.

Example 10.7. If $B = A[x_1, \ldots, x_r]$, then $\Omega_{B/A} = \oplus_{i=1}^r B d(x_i)$. The previous remark shows that B^r surjects onto $\Omega_{B/A}$. On the other hand, the partial derivative $\partial/\partial x_i$ is an A-linear derivation from B to B, hence we get a map $\partial_i \colon \Omega_{B/A} \longrightarrow B$ for all i and $\partial_i(dx_j) = \delta_{ij}$. In other words, the direct sum of the maps ∂_i is a map from $\Omega_{B/A}$ to B^r which is inverse to the above surjection.

Proposition 10.8. *Let $A \longrightarrow B \longrightarrow C$ be ring homomorphisms, then there is a right exact sequence of C-modules*

$$C \otimes_B \Omega_{B/A} \longrightarrow \Omega_{C/A} \longrightarrow \Omega_{C/B} \longrightarrow 0,$$

where the first map takes $c \otimes db$ to cdb (we are being slightly sloppy here, since cdb really means $cd\varphi(b)$, where $\varphi \colon B \longrightarrow C$ is the given map) and the second map takes dc to dc.

Proof. Clearly, the second map is surjective since the generators of both modules are the same, but in the right-hand module we factor out more relations, namely $db = 0$ for all $b \in B$ (use Remark 10.3). But these relations are precisely the images of the generators $1 \otimes db$ of the module on the left. □

Note that if $B \longrightarrow C$ is surjective, then $\Omega_{C/B} = 0$. The next result gives us more information about this case.

Proposition 10.9. *If $\pi \colon B \longrightarrow C$ is an epimorphism of A-algebras and $I = \ker(\pi)$, then there is an exact sequence, called the* conormal sequence*, of C-modules*

$$I/I^2 \xrightarrow{d} C \otimes_B \Omega_{B/A} \xrightarrow{D\pi} \Omega_{C/A} \longrightarrow 0,$$

where the left hand map takes the class of f to $1 \otimes df$ and the right hand map maps $c \otimes db$ to cdb.

Proof. We have the universal derivation $B \longrightarrow \Omega_{B/A}$ and can consider its restriction $I \longrightarrow \Omega_{B/A}$, which we will denote by d. If $b \in B$ and $x \in I$, then

$$(*)\ d(bx) = xd(b) + bd(x).$$

Note that the first summand on the right is in $I\Omega_{B/A}$. Noting that $B/I \simeq C$ and for any B-module M we have $M/IM \simeq B/I \otimes_B M$, we conclude that

$$\Omega_{B/A}/I\Omega_{B/A} \simeq \Omega_{B/A} \otimes_B C,$$

hence d induces a B-linear map $I \longrightarrow \Omega_{B/A}/I\Omega_{B/A}$. By $(*)$, I^2 gets mapped to 0 in $\Omega_{B/A} \otimes_B C$, hence we get a map of C-modules as claimed, yet again denoted by d.

To understand the cokernel of this d, note that $\Omega_{B/A} \otimes_B C$ is generated, as a C-module, by elements of the form $db \otimes 1$ for $b \in B$ subject to the Leibniz rule and the relations of A-linearity. On the other hand, the generators of $\Omega_{C/A}$ are the same, satisfy these relations as well, but in addition elements of the form df for $f \in I$ are 0 in $\Omega_{C/A}$. This shows that $\Omega_{C/A}$ is the cokernel of d as claimed. □

Differentials behave well with respect to base change.

Proposition 10.10. *Let A' and B be A-algebras. There exists a commutative diagram of the form*

$$\begin{array}{ccc} & & A' \otimes_A \Omega_{B/A} \\ & \overset{1\otimes d}{\nearrow} & \\ A' \otimes_A B & & \Big\downarrow \simeq \\ & \underset{d}{\searrow} & \\ & & \Omega_{(A'\otimes_A B)/A'}. \end{array}$$

Proof. By construction, $d\colon B \longrightarrow \Omega_{B/A}$ is an A-linear derivation, hence $1 \otimes d$ is an A'-linear derivation, so the universal property gives us a map $\Omega_{(A'\otimes_A B)/A'} \longrightarrow A' \otimes_A \Omega_{B/A}$ sending $d(a' \otimes b)$ to $a' \otimes d(b)$.

On the other hand, the map

$$B \simeq A \otimes_A B \longrightarrow A' \otimes_A B \longrightarrow \Omega_{(A'\otimes_A B)/A'}$$

is an A-linear derivation, hence we get a map $\Omega_{B/A} \longrightarrow \Omega_{(A'\otimes_A B)/A'}$ sending db to $d(1 \otimes b)$. Since the target is a module over $A' \otimes_A B$, this latter map induces an $A' \otimes_A B$-linear map

$$A' \otimes_A \Omega_{B/A} \longrightarrow \Omega_{(A'\otimes_A B)/A'}$$

sending $a' \otimes db$ to $a'd(b) = d(a' \otimes b)$, which is the inverse of the map constructed above. □

Our next goal is to study when the sequence in Proposition 10.9 is exact on the left. For this we first need a

Lemma 10.11. *Let $\varphi\colon B \longrightarrow B'$ be a morphism of A-algebras and let $\delta\colon B \longrightarrow B'$ be a map of abelian groups. If $\delta(B)^2 = 0$, then $\varphi + \delta$ is a homomorphism of A-algebras if and only if i) δ is A-linear and $(*)$ $\delta(b_1b_2) = \varphi(b_1)\delta(b_2) + \varphi(b_2)\delta(b_1)$.*

Proof. By definition,

$$(\varphi + \delta)(b_1b_2) = \varphi(b_1b_2) + \delta(b_1b_2),$$

while

$$\begin{aligned}(\varphi + \delta)(b_1) \cdot (\varphi + \delta)(b_2) = \varphi(b_1)\varphi(b_2) + \varphi(b_1)\delta(b_2) \\ + \delta(b_1)\varphi(b_2) + \delta(b_1)\delta(b_2).\end{aligned}$$

The last summand vanishes by our assumption. Therefore, the two expressions are equal if and only if $(*)$ holds. Furthermore, since φ commutes with the structure maps from A, $\varphi + \delta$ does so iff $\delta(A) = 0$ (equivalently, δ is A-linear), finishing the proof. □

Proposition 10.12. *If $\pi\colon B \longrightarrow C$ is an epimorphism of A-algebras with $I = \ker(\pi)$, then in the sequence*

$$I/I^2 \xrightarrow{d} C \otimes_B \Omega_{B/A} \xrightarrow{D\pi} \Omega_{C/A} \longrightarrow 0,$$

the left hand map is a split injection if and only if there is a map of A-algebras $\tau\colon C \longrightarrow B/I^2$ splitting the projection map $B/I^2 \longrightarrow B/I = C$.

Proof. First we will reduce to the case $I^2 = 0$. Considering the exact sequence of Proposition 10.9 for $B \longrightarrow B/I^2$, we conclude that $\Omega_{(B/I^2)/A}$ is obtained from $\Omega_{B/A}$ by factoring out $I^2\Omega_{B/A}$ and $d(I^2)$. Now, if $x, y \in I$, then $d(xy) = xd(y) + yd(x) \in I\Omega_{B/A}$, so $d(I^2) \subseteq I\Omega_{B/A}$ and, therefore, $C \otimes_B \Omega_{(B/I^2)/A} \simeq C \otimes_B \Omega_{B/A}$.

In the following we will write $d'\colon B \longrightarrow \Omega_{B/A}$ to avoid confusion.

First assume that $d\colon I \longrightarrow C \otimes_B \Omega_{B/A}$ is split by a map $\sigma\colon C \otimes_B \Omega_{B/A} \longrightarrow I$. Consider the map

$$\gamma = \pi \otimes \mathrm{id}\colon \Omega_{B/A} = B \otimes_B \Omega_{B/A} \longrightarrow C \otimes_B \Omega_{B/A}.$$

Going back to the definition of d we see that it is the restriction of $\gamma d'$ to I. Set $\delta = \sigma\gamma d'\colon B \longrightarrow I$. Since d' is an A-linear derivation and σ, γ are A-linear, δ is an A-linear derivation, hence we can apply the previous lemma with $\varphi = \mathrm{id}$ (note that $\delta(B)^2 = 0$ since $I^2 = 0$) to conclude that $1 - \delta\colon B \longrightarrow B$ is an A-algebra homomorphism. If $x \in I$, then $\sigma d(x) = x$, so $\delta(x) = \sigma\gamma d'(x) = \sigma d(x) = x$, so $(1 - \delta)(I) = 0$ and $(1 - \delta)$ induces an algebra homomorphism $\tau\colon C = B/I \longrightarrow B$. By construction, $\pi\tau = \mathrm{id}_C$.

Conversely, suppose $\tau\colon C \longrightarrow B$ is a map of A-algebras splitting the morphism $\pi\colon B \longrightarrow C$. The map $\delta = 1 - \tau\pi\colon B \longrightarrow B$ maps to the kernel of π (since $\pi\tau = \mathrm{id}$), hence $\delta(B) \subseteq I$. Since $I^2 = 0$, the previous lemma shows that δ is an A-linear derivation from B to I. By the universal property of $\Omega_{B/A}$, δ corresponds to a homomorphism $\sigma'\colon \Omega_{B/A} \longrightarrow I$. Now $I^2 = 0$, so this homomorphism factors through $\sigma\colon C \otimes \Omega_{B/A} \longrightarrow I$. If $x \in I$, then $\sigma d(x) = \sigma' d'(x) = \delta(x)$. But $\delta(x) = x - \tau\pi(x) = x$, hence σ splits d. □

To conclude this subsection, we will give a different description of differentials.

Theorem 10.13. *Let B be an A-algebra, $\mu\colon B \otimes_A B \longrightarrow B$ be the multiplication map and let $I = \ker(\mu)$. If $e\colon B \longrightarrow I/I^2$ is the map defined by $b \longmapsto 1 \otimes b - b \otimes 1$, then there is an isomorphism $\varphi\colon \Omega_{B/A} \longrightarrow I/I^2$ of B-modules such that $\varphi d = e$, that is, the pairs $(\Omega_{B/A}, d)$ and $(I/I^2, e)$ are naturally isomorphic.*

Proof. The first step is to show that e is a derivation. Consider the sequence

$$I/I^2 \longrightarrow (B \otimes_A B)/I^2 \longrightarrow B \longrightarrow 0$$

and note that the maps $B \longrightarrow (B \otimes_A B)/I^2$ defined by $b \longmapsto 1 \otimes b$ and $b \longmapsto b \otimes 1$ are algebra maps splitting this sequence. By Lemma 10.11, the difference e of these two algebra homomorphisms is a derivation.

By the universal property of $\Omega_{B/A}$ we get a unique map

$$\varphi\colon \Omega_{B/A} \longrightarrow I/I^2, \quad \varphi(db) = 1 \otimes b - b \otimes 1,$$

that is, $\varphi d = e$. In the following we will understand the inverse of φ.

Consider the ring C which, by definition, is the direct sum of B and $\Omega_{B/A}$ with multiplication given by

$$(b, u) \cdot (b', u') = (bb', bu' + b'u)$$

for $b, b' \in B$ and $u, u' \in \Omega_{B/A}$.

Define

$$\psi_1\colon B \longrightarrow C, \quad b \longmapsto (b, db) \quad \forall b \in B$$
$$\psi_2\colon B \longrightarrow C, \quad b \longmapsto (b, 0) \quad \forall b \in B.$$

Clearly, ψ_2 is a homomorphism of A-algebras. The same statement holds for ψ_1, since d is an A-linear derivation. Therefore, we get an A-algebra homomorphism

$$\psi\colon B \otimes_A B \longrightarrow C, \quad b \otimes b' \longmapsto (bb', bd(b')).$$

Note that $\psi(1 \otimes b - b \otimes 1) = (0, db)$, so the restriction of ψ to I is the desired inverse of φ. □

10.2. **Connection to regularity.** The purpose of this subsection is to establish a connection between modules of differentials and regular rings (of course, this only works in certain cases). We will have to assume some results, since their proofs need more category theory than we want to use. The proofs can be found in Section 16 of [4].

Convention. In this subsection any field will be of characteristic zero.

The following statement is a simplified version of [4, Lem. 16.15].

Proposition 10.14. *If B is an A-algebra and S a multiplicatively closed subset of B, then*

$$\Omega_{S^{-1}B/A} \simeq S^{-1}B \otimes_B \Omega_{B/A},$$

that is, taking differentials commutes with localisation. □

The following result is [4, Prop. 16.9].

Proposition 10.15. *Let $A \longrightarrow B \subseteq C$ be morphisms of rings. If B and C are fields and C is algebraic over B, then*

$$\Omega_{C/A} = C \otimes_B \Omega_{B/A}.$$

□

Proposition 10.16. *If $B \subseteq C$ are fields and $\{x_\lambda\}_{\lambda\in\Lambda} \subseteq C$ is a collection of elements, then $\{dx_\lambda\}_{\lambda\in\Lambda}$ is a basis of $\Omega_{C/B}$ as a C-vector space if and only if $\{x_\lambda\}_{\lambda\in\Lambda}$ is a transcendence basis of C over B.*

Proof. First assume that $\{x_\lambda\}_{\lambda\in\Lambda}$ is a transcendence basis of C over B. Then C is algebraic over $B' = B(\{x_\lambda\}_{\lambda\in\Lambda})$. By the previous proposition, $\Omega_{C/B} = C\otimes_{B'}\Omega_{B'/B}$. Now B' is the localisation of the polynomial ring $B[\{x_\lambda\}_{\lambda\in\Lambda}]$ at the 0-ideal, so by Proposition 10.14 and (an infinite version of) Example 10.7 the module $\Omega_{B'/B}$ has $\{dx_\lambda\}_{\lambda\in\Lambda}$ as a basis, hence the claim holds.

Conversely, suppose that $\{dx_\lambda\}_{\lambda\in\Lambda}$ is a basis of $\Omega_{C/B}$. Let $C' = B(\{x_\lambda\}_{\lambda\in\Lambda})$ be the subfield of C generated by $\{x_\lambda\}_{\lambda\in\Lambda}$. The sequence

$$C\otimes_{C'}\Omega_{C'/B}\longrightarrow\Omega_{C/B}\longrightarrow\Omega_{C/C'}\longrightarrow 0$$

is exact and $1\otimes dx_\lambda\in C\otimes_{C'}\Omega_{C'/B}$ gets mapped to $dx_\lambda\in\Omega_{C/B}$. Since these elements generate the latter vector space, wee see that $\Omega_{C/C'}=0$. If C were not algebraic over C', then it would have a transcendental basis whose differentials would be a basis of $\Omega_{C/C'}$. Hence C is algebraic over C'.

The next step is to show that the elements x_λ are algebraically independent over B. Assuming that x_1 is algebraically dependent on $\{x_\lambda\}_{\lambda\in\Lambda,\lambda\neq 1}$, we see that C is algebraic over $C' = B(\{x_\lambda\}_{\lambda\in\Lambda,\lambda\neq 1})$. By the above argument, dx_1 would be in the submodule generated by $\{dx_\lambda\}_{\lambda\in\Lambda,\lambda\neq 1}$, contradicting the assumption that the set $\{dx_\lambda\}_{\lambda\in\Lambda}$ is linearly independent. □

Corollary 10.17. *Suppose $B\subseteq C$ are fields and assume C is finitely generated over B of transcendence degree r. Then* $\dim_C\Omega_{C/B} = r$. □

We also quote the following result without a proof (see Section 13 of [4] for it). Recall that the dimension of an ideal I is $\dim(A/I)$. The codimension of a prime ideal $\mathfrak{p}$ in A is the dimension of $A_\mathfrak{p}$. If I is any ideal, then its codimension $\mathrm{codim}I$ is defined to be the minimum of the codimensions of all the primes containing I.

Proposition 10.18. *If A is a finitely generated k-algebra which is an integral domain, then* $\dim(A) = \mathrm{trdeg}_k A_{(0)}$. *If $I\subseteq A$ is an ideal, then* $\dim I + \mathrm{codim}I = \dim A$. □

In order to state the main result of this subsection, we need some preparation first. Let $B = A[x_1,\ldots,x_r]$ and $C = B/I$ for some ideal I. Since the projection $\pi\colon B\longrightarrow C$ is surjective, we have the conormal sequence $I/I^2\longrightarrow C\otimes_B\Omega_{B/A}\longrightarrow\Omega_{C/A}\longrightarrow 0$. By Example 10.7, $\Omega_{B/A}\simeq\oplus_{i=1}^r B dx_i$, so

$$C\otimes_B\Omega_{B/A}\simeq\oplus_{i=1}^r C dx_i$$

is a free C-module. Assuming $I = (f_1,\ldots,f_s)$, there is a projection $C^s\longrightarrow I/I^2$ which sends the i-th basis vector to the class of f_i. The composition

$$C^s\longrightarrow I/I^2\longrightarrow\oplus_{i=1}^r C dx_i = C\otimes_B\Omega_{B/A}$$

is represented by the *Jacobian matrix* $\mathcal{J}$, that is, $\mathcal{J} = (\partial f_i/\partial x_j)_{i,j}$. Therefore, $\Omega_{C/A}$ is the cokernel of $\mathcal{J}$. For example, if $r=1$ and $C = B/f$ for some polynomial f, then

$$\Omega_{C/A} = Cdx/df = Cdx/(Cf'dx)\simeq C/f'.$$

Theorem 10.19. *Let $B = k[x_1, \dots, x_r]$ be a polynomial ring over a field k, let $I = (f_1, \dots, f_s)$ be an ideal and set $C = B/I$. Let $\mathfrak{p} \in \operatorname{Spec}(C)$ and let c be the codimension of $I_\mathfrak{p}$ in $B_\mathfrak{p}$ (of course, here we abuse notation by writing $\mathfrak{p}$ for the preimage under the projection map). Then*

1. *The Jacobian matrix $\mathcal{J} = (\partial f_i/\partial x_j)_{i,j}$ taken modulo $\mathfrak{p}$ has rank at most c.*
2. *The ring $C_\mathfrak{p}$ is regular if and only if the rank of $\mathcal{J}$ modulo $\mathfrak{p}$ is precisely c.*

Proof. (1) Let $I \subseteq \mathfrak{q} \subseteq \mathfrak{p}$ be a prime containing I which has codimension c. If we can show that the rank of $\mathcal{J}$ modulo $\mathfrak{q}$ is at most c, then the same will hold for the rank modulo $\mathfrak{p}$, so we can assume $\mathfrak{q} = \mathfrak{p}$. By the same reasoning, we can also assume that $I = \mathfrak{q} = \mathfrak{p}$. Note that under this assumption C is a domain. Localise the conormal sequence for the epimorphism $B \twoheadrightarrow C$ at $\mathfrak{q}$ to get

$$(I/I^2)_\mathfrak{q} \twoheadrightarrow C_\mathfrak{q} \otimes (\Omega_{B/k})_\mathfrak{q} \twoheadrightarrow (\Omega_{C/k})_\mathfrak{q} \twoheadrightarrow 0.$$

By Proposition 10.14, the last term, which by the reasoning above is the cokernel of $\mathcal{J}$ regarded as a matrix over the field $C_\mathfrak{q} = C_{(0)}$, is isomorphic to $\Omega_{(C_\mathfrak{q})/k}$. By Corollary 10.17, the latter vector space has dimension $\geq r - c$ (since the transcendence degree of B is r and taking the quotient by I diminishes it by at most c), so the rank of the Jacobian matrix modulo $\mathfrak{q}$ is at most c.

(2) Set $\kappa(\mathfrak{p}) := C_\mathfrak{p}/\mathfrak{p}_\mathfrak{p}$. The map $C_\mathfrak{p} \twoheadrightarrow \kappa(\mathfrak{p})$ is surjective, hence we can consider its conormal sequence, which in this case is

$$\mathfrak{p}_\mathfrak{p}/\mathfrak{p}_\mathfrak{p}^2 \twoheadrightarrow \kappa(\mathfrak{p}) \otimes \Omega_{(C_\mathfrak{p})/k} \twoheadrightarrow \Omega_{\kappa(\mathfrak{p})/k} \twoheadrightarrow 0.$$

Applying Proposition 10.12, the first map is an injection so we have the following equality

$$\dim_{\kappa(\mathfrak{p})}(\mathfrak{p}_\mathfrak{p}/\mathfrak{p}_\mathfrak{p}^2) + \dim_{\kappa(\mathfrak{p})}(\Omega_{\kappa(\mathfrak{p})/k}) = \dim_{\kappa(\mathfrak{p})}(\kappa(\mathfrak{p}) \otimes \Omega_{(C_\mathfrak{p})/k}).$$

We already know that $\dim_{\kappa(\mathfrak{p})}(\mathfrak{p}_\mathfrak{p}/\mathfrak{p}_\mathfrak{p}^2) \geq \dim C_\mathfrak{p}$ with equality if and only if $C_\mathfrak{p}$ is a regular local ring. By Corollary 10.17, $\dim_{\kappa(\mathfrak{p})}(\Omega_{\kappa(\mathfrak{p})/k}) = \operatorname{trdeg}\kappa(\mathfrak{p})/k$ and by Proposition 10.18, $\operatorname{trdeg}\kappa(\mathfrak{p})/k = \dim(C/\mathfrak{p})$. By the same proposition applied to $\mathfrak{p} \subseteq B$ and using that $\dim(B/\mathfrak{p}) = \dim(C/\mathfrak{p}) + \dim(C_\mathfrak{p})$ (since $C_\mathfrak{p} = (B/\mathfrak{p})_\mathfrak{p}$ is a field), we have $\dim(C/\mathfrak{p}) + \dim C_\mathfrak{p} = r - c$, hence

$$\dim_{\kappa(\mathfrak{p})}(\kappa(\mathfrak{p}) \otimes \Omega_{(C_\mathfrak{p})/k}) \geq r - c$$

with equality if and only if $C_\mathfrak{p}$ is regular.

For the last statement just note that, as argued above, $\Omega_{C/k}$ is the cokernel of the Jacobian matrix, so $\kappa(\mathfrak{p}) \otimes \Omega_{C_\mathfrak{p}/k}$ is the cokernel of $\mathcal{J}$ taken modulo $\mathfrak{p}$, hence the dimension of this module is $r - c$ if and only if the rank of the Jacobian matrix is precisely c.

□

Lemma 10.20. *Let $J\colon A^m \twoheadrightarrow A^n$ be a map of free modules over a ring A, assume that $\operatorname{rk}(J) \leq c$ and set $M = \operatorname{coker}(J)$. Let $\mathfrak{p} \in \operatorname{Spec}(A)$. Then $M_\mathfrak{p}$ is free of frank $n - c$ if*

and only if the matrix J, taken modulo $\mathfrak{p}$ has rank exactly c (hence, some $c \times c$-minor of J is outside $\mathfrak{p}$).

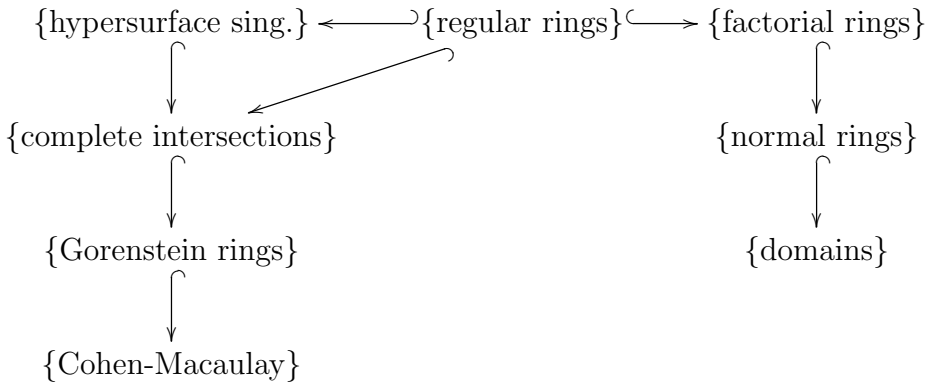
Proof. Localising the situation, we may assume that A is local and $\mathfrak{p}$ is the maximal ideal of A. Suppose that M is free. Tensoring the sequence $A^m \longrightarrow A^n \longrightarrow M$ with $A/\mathfrak{p}$ we may assume that A is a field. In this case, the rank of the vector space $M/\mathfrak{p}M$ is precisely $n - c$ because M was supposed to be free. It follows that the rank of $J \otimes A/\mathfrak{p}$ is c, which is what we wanted.

Conversely, suppose the rank of J taken modulo $\mathfrak{p}$ is c. Multiplying J by invertible matrices on the right and left, an operation which does not change the cokernel of J, we can assume that J modulo $\mathfrak{p}$ is a block matrix with a $c \times c$-identity matrix in the upper left and zero matrices in the other three blocks. It is then clear that the cokernel of J is free of rank $r - c$. □

Corollary 10.21. *Let $B = k[x_1, \ldots, x_r]$, $C = B/I$, let $\mathfrak{p} \in \operatorname{Spec}(C)$ and let c be the codimension of $I_\mathfrak{p}$ in $C_\mathfrak{p}$. The ring $C_\mathfrak{p}$ is regular local if and only if the localisation of the module $\Omega_{C/k}$ at $\mathfrak{p}$ is free of rank $r - c$.*

Proof. Apply the previous lemma to the Jacobian matrix and use Theorem 10.19. □

As a conclusion consider the following "botanics" of Noetherian (local) rings:



Here, a factorial ring is just another term for unique factorization domain, a local ring A is a *complete intersection* if there exists a regular ring B and a B-regular sequence $\underline{a} = (a_1, \ldots a_p)$ such that $A \simeq B/\underline{a}$ and A is a *hypersurface singularity* if there exists a regular local ring $(B, \mathfrak{n})$ and $f \in \mathfrak{n}$ such that $A = B/(f)$.

11. Appendix: Exercises

Sheet 1

Exercise 1. [2, Ex. I.2 b)+a)]

b) Prove that $f = \sum_{i=0}^{n} a_i X^i \in A[X]$ is nilpotent if and only if all the a_i are.

a) Show that $f = \sum_{i=0}^{n} a_i X^i \in A[X]$ is a unit if and only if a_0 is a unit in A and a_i is nilpotent for $i \geq 1$.

Exercise 2. [2, Ex. 1.4] Show that in $A[X]$ the Jacobson radical and the nilradical are equal.

Exercise 3. [2, Ex. 1.10] Show that the following conditions are equivalent: i) a ring A has only one prime ideal, ii) every element in A is either nilpotent or a unit, iii) $A/\mathrm{rad}A$ is a field.

Exercise 4. (cf. [7, Ex. 1.1.3]) Let $f\colon A \longrightarrow B$ be a ring homomorphism. Show that $f(\mathrm{rad}A) \subseteq \mathrm{rad}B$. Give an example of a *surjective* f such that the inclusion is strict.

Sheet 2

Exercise 5. [2, Ex. 1.12] Prove that if A is a local ring and e an idempotent, that is, $e^2 = e$, then $e = 0$ or $e = 1$.

Exercise 6. [2, Ex. 1.17] Let A be a ring, $f \in A$, $X = \mathrm{Spec}(A)$ and $X_f = X \setminus V(f)$. Prove the following statements.

(1) $X_f \cap X_g = X_{fg}$,
(2) $X_f = \emptyset \iff f$ is nilpotent,
(3) $X_f = X \iff f$ is a unit,
(4) $X_f = X_g \iff \mathrm{rad}(f) = \mathrm{rad}(g)$.

Exercise 7. [2, Ex. 2.9] Show that if $0 \longrightarrow M' \xrightarrow{\alpha} M \xrightarrow{\beta} M'' \longrightarrow 0$ is a short exact sequence of A-modules and M', M'' are finitely generated, then so is M.

Exercise 8. [3, Ex. 3.18] Let A be an integral domain. An element $m \in M$ is said to be torsion if $\mathrm{Ann}(m) \neq 0$. Denote by $\mathrm{tors}M$ the set of all torsion elements of M. We will say that M is torsionfree if $\mathrm{tors}M = 0$ and that M is torsion if $M = \mathrm{tors}M$.

Let

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

be a short exact sequence. Show the following statements or answer the questions, respectively.

(1) $\mathrm{tors}M$ is a submodule of M.
(2) If M is torsion, then the same holds for M' and M''.
(3) If M is torsionfree, then M' is torsionfree, but M'' need not be.
(4) If M' and M'' are torsion, is then M is also torsion?
(5) If M' and M'' are both torsionfree, does the same hold for M?

Sheet 3

Exercise 9. [2, Ex. 2.2 & 2.3] Let A be a ring, M be an A-module and I be an ideal in A. Show that $A/I \otimes_A M \simeq M/IM$. Use this to prove the following statement. If M

and N are finitely generated modules over a local ring A, then $M \otimes_A N \simeq 0$ implies that either $M \simeq 0$ or $N \simeq 0$.

Exercise 10. [2, Ex. 2.4 & 2.5] Prove that a direct sum of modules is flat if and only if every summand is flat. Use this to show that for any ring A the module $A[X]$ is flat.

Exercise 11. [2, Ex. 2.25] Let $0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$ be an exact sequence of A-modules with M'' flat. Prove that M is flat if and only if M' is flat.

Exercise 12. [2, Ex. 3.1] Let A be a ring, S a multiplicatively closed subset of A and M be a finitely generated A-module. Show that if $S^{-1}M = 0$, then there exists an element $s \in S$ such that $sM = 0$.

Sheet 4

Exercise 13. [2, Ex. 3.5] Let A be a ring. Prove that A has no nilpotent elements if $A_\mathfrak{p}$ does not have any nilpotent elements for any prime ideal $\mathfrak{p}$. Find an example of a ring A such that $A_\mathfrak{p}$ is an integral domain for any prime ideal $\mathfrak{p}$ but A is not an integral domain.

Exercise 14. (cf. [2, Ex. 3.12 & 3.13]) Let A be an integral domain and M be an A-module. Recall that $\mathrm{tors}(M)$ is the submodule of torsion elements of M, that is, elements m such that $am = 0$ for some $0 \neq a \in A$. Prove that $M/\mathrm{tors}M$ is a torsion-free module.

Now let S be a multiplicatively closed subset of A. Show that $S^{-1}(\mathrm{tors}M) = \mathrm{tors}(S^{-1}M)$. Conclude that the following statements are equivalent: i) M is torsion-free, ii) $M_\mathfrak{p}$ is torsion-free for all prime ideals $\mathfrak{p}$ and iii) $M_\mathfrak{m}$ is torsion-free for all maximal ideals $\mathfrak{m}$.

Exercise 15. (cf. [2, Ex. 3.19]) Let A be a ring and M be an A-module. We define the *support* of M to be the set of all prime ideals $\mathfrak{p}$ of A such that $M_\mathfrak{p} \neq 0$. This set is denoted by $\mathrm{Supp}(M)$. Show the following statements.

(1) $M \neq 0 \iff \mathrm{Supp}(M) \neq 0$.
(2) $V(I) = \mathrm{Supp}(A/I)$ for any ideal I of A.
(3) If $0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$ is an exact sequence, then $\mathrm{Supp}(M) = \mathrm{Supp}(M') \cup \mathrm{Supp}(M'')$.
(4) If $M = \sum_\alpha M_\alpha$, then $\mathrm{Supp}(M) = \cup_\alpha \mathrm{Supp}(M_\alpha)$.
(5) If M is finitely generated, then $\mathrm{Supp}(M) = V(\mathrm{Ann}(M))$.
(6) If M and N are finitely generated, then $\mathrm{Supp}(M \otimes N) = \mathrm{Supp}(M) \cap \mathrm{Supp}(N)$.
(7) If I is an ideal and M is finitely generated, then $\mathrm{Supp}(M/IM) = V(I + \mathrm{Ann}(M))$.

Exercise 16. (cf. [2, Ex. 3.20]) Let $f\colon A \longrightarrow B$ be a ring homomorphism, et I be an ideal of A and J be an ideal of B. Recall that I^e is the ideal generated by $f(I)$ in B and J^c is $f^{-1}(J)$. Show that $I \subseteq I^{ec}$, $J^{ce} \subseteq J$ and use this to prove that $I^e = I^{ece}$ and $J^c = J^{cec}$. Now prove the following statements concerning the map $f^*\colon \mathrm{Spec}(B) \longrightarrow \mathrm{Spec}(A)$.

(1) The map f^* is surjective if and only if every prime ideal of A is a contracted ideal.
(2) If every prime ideal of B is an extended ideal, then f^* is injective.

Sheet 5

Exercise 17. (cf. [1]) Let A be a ring, S a multiplicatively closed subset of A and I an ideal of A. The *saturation* of I is the set

$$I^S = \{a \mid \exists s \in S : as \in I\}.$$

We call I saturated if $I = I^S$.

Prove the following statements: i) $\ker(A \longrightarrow S^{-1}A) = (0)^S$, ii) $I \subseteq I^S$, iii) I^S is an ideal, iv) if $I \subseteq J$ are ideals, then $I^S \subseteq J^S$, v) $(I^S)^S = I^S$ and (vi) $(I^S J^S)^S = (IJ)^S$.

Show that if M is an A-module, then the kernel of the map $M \longrightarrow S^{-1}M$ is the set of elements $m \in M$ satisfying $\mathrm{Ann}(m) \cap S \neq \emptyset$. In particular, if $\mathrm{Ann}(M) \cap S \neq \emptyset$, then $S^{-1}M = 0$.

Exercise 18. (cf. [1]) Let M be an A-module and $M_1 \subseteq M_2$ be submodules of M. Then $M_1 = M_2$ if and only if $M_1 \cap N = M_2 \cap N$ and $(M_1 + N)/N = (M_2 + N)/N$ for all submodules N of M.

Let $0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$ be an exact sequence of modules. If M_1 and M_2 are submodules of M such that $g(M_1) = g(M_2)$ and $f^{-1}(M_1) = f^{-1}(M_2)$, is it true that $M_1 = M_2$?

Exercise 19. [2, Ex. 6.3] Let M be an A-module and N_1, N_2 be submodules of M. Assume that M/N_1 and M/N_2 are Noetherian (resp. Artinian). Prove that then $M/(N_1 \cap N_2)$ is Noetherian (resp. Artinian).

Exercise 20. [7, Ex. 3.1 & 3.2], also cf. [1] Let A be a ring and $I_1, \ldots, I_n$ be ideals such that every ring A/I_k is Noetherian. Show that $M = \oplus_k A/I_k$ is a Noetherian R-module. Prove that if $\cap_k I_k = 0$, then R is a Noetherian ring. Use this to show the following statement: If A and B are Noetherian rings and $f\colon A \longrightarrow C$ and $g\colon B \longrightarrow C$ are surjective ring homomorphisms, then the *fibre product* $A \times_C B = \{(a, b) \in A \times B \mid f(a) = g(b)\}$ is a Noetherian ring.

Let now k be a field and A be a k-algebra. Prove that if A is finite-dimensional as a k-vector space, then A is Noetherian and Artinian.

Sheet 6

Exercise 21. Recall that a nonzero module M is called simple if its only submodules are 0 and M. Prove that the following statements are equivalent.

(1) The module M is a direct sum of simple modules.
(2) Every submodule N of M is a direct summand, that is, there exists a submodule N' such that $N \oplus N' = M$.
(3) The module M is a sum of simple submodules.

Exercise 22. cf. [1, Ex. 19.2] Show that an A-module M is simple if and only if $M \simeq A/\mathfrak{m}$ for some maximal ideal $\mathfrak{m}$ and if this holds, then $\mathfrak{m} = \mathrm{Ann}(M)$. Furthermore, prove that a module of finite length is finitely generated.

Exercise 23. [2, Ex. 6.8] A topological space is called Noetherian if the open subsets satisfy the ascending chain condition (alternatively, the maximal condition) or, equivalently, the closed subsets satisfy the descending chain condition (alternatively, the minimal condition).

If A is a Noetherian ring, show that $X = \mathrm{Spec}(A)$ is a Noetherian topological space. Give an example where $\mathrm{Spec}(A)$ is Noetherian but A is not.

Exercise 24. [2, Ex. 6.5] A topological space is called quasi-compact if whenever $X = \cup_i U_i$ is a cover of X by open subsets U_i, then finitely many of the U_i already cover X.

Show that if X is a Noetherian topological space, then every subspace of X is also Noetherian and that X is quasi-compact.

Sheet 7

Exercise 25. cf. [2, Ex. 4.2 & 4.4]

a) Let A be a ring and I let be an ideal which is equal to its radical. Show that I has a (possibly infinite) primary decomposition without embedded primes.
b) If $f\colon A \longrightarrow B$ is a ring homomorphism and I is $\mathfrak{p}$-primary in B, then I^c is $\mathfrak{p}^c$-primary in A. Show that the converse holds if f is surjective.
c) Let $A = \mathbb{Z}[t]$. Show that $\mathfrak{m} = (2, t)$ is a maximal ideal, that $J = (4, t)$ is $\mathfrak{m}$-primary but J is not a power of $\mathfrak{m}$.

Exercise 26. [3, Ex. 10.5] Let $A = \mathbb{Z}[t]/(t^2 + 3)$ and $I = (2) \subseteq A$.

a) Show that there exists a unique maximal ideal $\mathfrak{m}$ such that $A/\mathfrak{m} \simeq \mathbb{Z}/2\mathbb{Z}$.
b) Prove that $\mathrm{rad}I = \mathfrak{m}$ and deduce that I is $\mathfrak{m}$-primary.
c) Show that I is not a product of prime ideals.

Exercise 27. [1, Ex. 18.7] Let k be a field, $A = k[X, Y]$ and $I = (X^2, XY)$. Show that $\mathrm{rad}I$ is prime and that I is not primary. Prove that if $fg \in I$, then either $f^2 \in I$ or $g^2 \in I$.

Exercise 28. [1, Ex. 18.16] Let k be a field, $A = k[X, Y, Z]$ and $I = (XY, X - YZ)$. Show that

$$I = (X, Z) \cap (Y^2, X - YZ)$$

and that this is a minimal primary decomposition of I.

Sheet 8

Exercise 29. [1, Ex. 17.7 & 17.10]

(1) Let $A = \mathbb{Z}$ and let $M = \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. Compute $\mathrm{Ass}M$ and find submodules L and N of M such that $L + N = M$ but $\mathrm{Ass}N \cup \mathrm{Ass}L \subsetneq \mathrm{Ass}M$.
(2) Let A be a ring with the property that $A_\mathfrak{p}$ is a domain for all $\mathfrak{p} \in \mathrm{Spec}(A)$. Show that every associated prime ideal is minimal.

Exercise 30. [2, Ex. 4.5] Let $A = k[X, Y, Z]$, $\mathfrak{p}_1 = (X, Y)$, $\mathfrak{p}_2 = (X, Z)$ and $\mathfrak{m} = (X, Y, Z)$. Let $I = \mathfrak{p}_1\mathfrak{p}_2$. Prove that $I = \mathfrak{p}_1 \cap \mathfrak{p}_2 \cap \mathfrak{m}^2$ is a minimal primary decomposition of I and determine the isolated and embedded components.

Exercise 31. [2, Ex. 4.7] Let I be an ideal in a ring A, let $B = A[X]$ and let $I[X] = \{p = \sum_{i=0}^{n} a_i X^i \in A[X] \mid a_i \in I\} \subseteq A[X]$. Show the following statements:

(1) $I[X]$ is the extension of I in B.
(2) If $\mathfrak{p} \in \mathrm{Spec}(A)$, then $\mathfrak{p}[X] \in \mathrm{Spec}(B)$.
(3) If $\mathfrak{q}$ is $\mathfrak{p}$-primary in A, then $\mathfrak{q}[X]$ is $\mathfrak{p}[X]$-primary in B.
(4) If $I = \cap_{k=1}^{n} J_k$ is a minimal primary decomposition in A, then $I[X] = \cap_{k=1}^{n} J_k[X]$ is a minimal primary decomposition in B.
(5) If $\mathfrak{p}$ is a minimal prime ideal of I, then $\mathfrak{p}[X]$ is a minimal prime ideal of $I[X]$.

Exercise 32. cf. [2, Ex. 4.20 & 4.21]

(1) Let M be an A-module and let $N \subseteq M$ be a submodule. Define
$$\mathrm{rad}_M(N) = \{a \mid \exists k > 0 : \ a^k M \subseteq N\}.$$
Prove that $\mathrm{rad}_M(N) = \mathrm{rad}(N : M) = \mathrm{rad}(\mathrm{Ann}(M/N))$.
(2) If M' is any A-module, recall that $a \in A$ is a zero-divisor on M if $am = 0$ for some $m \neq 0$; a is nilpotent on M if $a^k M = 0$ for some $k > 0$.
We say that a submodule Q of M is primary if $Q \neq M$ and every zero-divisor for M/Q is nilpotent. Show that if Q is primary, then $(Q : M)$ is a primary ideal. Conclude that $\mathrm{rad}_M(Q)$ is a prime ideal.

Sheet 9

Exercise 33. [2, Ex. 5.5 & 5.6] Let $A \subseteq B$ be rings. Prove the following statements.

(1) If B is integral over A and $x \in A$ has an inverse in B, then this inverse is already in A.
(2) If B is integral over A, the Jacobson radical of A is the contraction of the Jacobson radical of B.
(3) If $B \setminus A$ is closed under multiplication, then A is integrally closed in B.

Exercise 34. [2, Ex. 5.12] Let G be a finite group of automorphisms of a ring A and let
$$A^G = \{a \in A \mid g(a) = a \ \forall g \in G\}.$$
Prove that A^G is a ring (the so-called ring of invariants) and that A is integral over A^G.

If S is a multiplicatively closed subset of A such that $g(S) \subseteq S$ for all $g \in G$, set $S^G = S \cap A^G$. Show that the action of G extends to an action on $S^{-1}A$ and that $(S^{-1}A)^G \simeq (S^G)^{-1}A^G$.

Exercise 35. [1, Ex. 14.4] Let $A \subseteq B$ be rings, B integral over A and let $\mathfrak{p} \in \mathrm{Spec}(A)$. Assume there is only one $\mathfrak{q} \in \mathrm{Spec}(B)$ such that $A \cap \mathfrak{q} = \mathfrak{p}$. Prove that 1) $\mathfrak{q}B_{\mathfrak{p}}$ is the only maximal ideal in $B_{\mathfrak{p}}$, 2) $B_{\mathfrak{p}} = B_{\mathfrak{q}}$ and 3) $B_{\mathfrak{q}}$ is integral over $A_{\mathfrak{p}}$.

Hint. To prove 2) you might want to establish the following statement. If C is any ring, $S \subset T$ are multiplicative subsets and $T' = g_S(T)$ is the image of T under the localisation map $g_S \colon C \longrightarrow S^{-1}C$, then $T^{-1}C = T'^{-1}(S^{-1}R) = T^{-1}(S^{-1}R)$.

Exercise 36. [1, Ex. 14.5] Let $A \subseteq B$ be an integral extension of domains and let $\mathfrak{p} \in \mathrm{Spec}(A)$. Assume that there are at least two distinct prime ideals $\mathfrak{q}$ and $\mathfrak{q}'$ in B such that $\mathfrak{q} \cap A = \mathfrak{q}' \cap A$. Prove that $B_{\mathfrak{q}}$ is not integral over $A_{\mathfrak{p}}$.

Sheet 10

Exercise 37. [1, Ex. 14.6] let k be a field, X an indeterminate, $Y = X^2$, $A = k[Y]$ and $B = k[X]$. Define $\mathfrak{p} = (Y-1)A$ and $\mathfrak{p}' = (X-1)B$. Investigate whether $B_{\mathfrak{p}'}$ is always integral over $A_{\mathfrak{p}}$.

Exercise 38.

(1) (cf. [3, Ex. 14.2]) Let $A \subseteq B$ be rings and let C be the integral closure of A in B. Now assume that A and B are fields and that B is algebraically closed. Prove that C is algebraically closed.
(2) Let $A \subseteq B$ be rings and assume that B is integral over A. Show that the Krull dimensions of A and B are equal.

Exercise 39. [2, Ex. 5.28] Let A be an integral domain and K its field of fractions. We say that A is a *valuation ring* of K if for any $0 \neq x \in K$ either $x \in B$ or $x^{-1} \in B$. Show that the following conditions are equivalent.

(1) A is a valuation ring of K.
(2) For any ideals I, J of A we either have $I \subseteq J$ or $J \subseteq I$.

Deduce that if A is a valuation ring and $\mathfrak{p}$ is a prime ideal of A, then $A_{\mathfrak{p}}$ and $A/\mathfrak{p}$ are valuation rings of their fields of fractions.

Exercise 40. [2, Ex. 5.30] Let A be a valuation ring of a field K. The group U of units of A is a subgroup of the multiplicative group K^* of K. Set $\Gamma = K^*/U$ and note that Γ is a commutative group.

Given $\alpha, \beta \in \Gamma$, pick representatives $x, y \in K^*$ and define

$$\alpha \geq \beta \iff xy^{-1} \in A.$$

Show that this is a well-defined total ordering (a transitive, antisymmetric and total relation) on Γ which is compatible with the group structure, that is, $\alpha \geq \beta$ implies that $\alpha\gamma \geq \beta\gamma$ for all $\gamma \in \Gamma$. The totally ordered abelian group Γ is called the *value group* of A.

Let $v \colon K^* \longrightarrow \Gamma$ be the canonical homomorphism. Prove that $v(x+y) \geq \min\{v(x), v(y)\}$ for all $x, y \in K^*, x \neq -y$.

Sheet 11

Exercise 41. [7, Ex. 14.2] Let $(A, \mathfrak{m})$ be a Noetherian local ring and let $G = G_{\mathfrak{m}}(A)$. For $a \in A$, suppose that $a \in \mathfrak{m}^i$, but $a \notin \mathfrak{m}^{i+1}$ and write a^* for the image of a in $\mathfrak{m}^i/\mathfrak{m}^{i+1} \subseteq G$. Set $0^* = 0$. Prove the following statements.

(1) If $a^*b^* \neq 0$, then $a^*b^* = (ab)^*$.
(2) If a^* and b^* have the same degree and $a^* + b^* \neq 0$, then $a^* + b^* = (a+b)^*$.
(3) Let $I \subseteq \mathfrak{m}$ be an ideal. Write $I^* \subseteq G$ be the ideal generated by the elements i^* for $i \in I$. Setting $B = A/I$ and $\mathfrak{n} = \mathfrak{m}/I$, we have $G_{\mathfrak{n}}(B) = G/I^*$.

Exercise 42. [2, Ex. 11.1] Let k be an algebraically closed field and let $f \in k[x_1, \ldots, x_n]$ be an irreducible polynomial. We call a point $p \in Z(f)$ non-singular if not all the partial derivatives $\partial f/\partial x_i$ vanish at p.

Let $A = k[x_1, \ldots, x_n]/(f)$ and let $\mathfrak{m}$ be the maximal ideal of A corresponding to p (if $p = (a_1, \ldots, a_n)$, then $\mathfrak{m}$ is the image in A of $\mathfrak{m}_p = (x_1 - a_1, \ldots, x_n - a_n)$; here we use the Nullstellensatz). Show that p is non-singular if and only if $A_{\mathfrak{m}}$ is a regular local ring.

Exercise 43. [2, Ex. 11.6] Let A be a ring. Show that

$$\dim(A) + 1 \leq \dim(A[X]) \leq 1 + 2\dim(A).$$

Hint. Use the following fact:

If $f\colon B \longrightarrow B'$ is a ring homomorphism and $f^*\colon \operatorname{Spec}(B') \longrightarrow \operatorname{Spec}(B)$ the induced map on the spectra, then for any $\mathfrak{p} \in \operatorname{Spec}(B)$ the fibre $f^{*-1}(\mathfrak{p})$ is homeomorphic to $\operatorname{Spec}(B'_{\mathfrak{p}}/\mathfrak{p}B'_{\mathfrak{p}}) = \operatorname{Spec}(\kappa(\mathfrak{p}) \otimes_B B')$ where $\kappa(\mathfrak{p})$ is the residue field of the local ring $B_{\mathfrak{p}}$.

Exercise 44. [4, Ex. 11.10] Let A be a Noetherian ring. Show that A is reduced if and only if i) the localisation of A at any prime of height 0 is regular and ii) every prime associated with 0 is of height 0.

Sheet 12

Exercise 45. Recall that a complex of A-modules is a sequence of modules and A-linear maps $d^i\colon M^i \longrightarrow M^{i+1}$ for $i \in \mathbb{Z}$ such that $d^{i+1} \circ d^i = 0$ for all i. Write a complex as $M^\bullet$. The i-cycles of a complex is by definition $Z^i(M^\bullet) := \ker(d^i)$ and the i-boundaries are $B^i(M^\bullet) = \operatorname{im}(d^{i-1})$. Clearly, $B^i(M^\bullet) \subseteq Z^i(M^\bullet)$ and we define the i-th cohomology of $M^\bullet$ to be $H^i(M^\bullet) = Z^i(M^\bullet)/B^i(M^\bullet)$. A morphism of complexes $f^\bullet\colon M^\bullet \longrightarrow N^\bullet$ is given by maps $f^i\colon M^i \longrightarrow N^i$ for all $i \in \mathbb{Z}$ such that $d^i_{N^\bullet} \circ f^i = f^{i+1} \circ d^i_{M^\bullet}$ for all i.

Show that any morphism of complexes $f^\bullet$ induces a map

$$H^i(f^\bullet)\colon H^i(M^\bullet) \longrightarrow H^i(N^\bullet)$$

for all $i \in \mathbb{Z}$.

A morphism $f^\bullet$ is called a quasi-isomorphism if $H^i(f^\bullet)$ is an isomorphism for all i. Show that the following conditions are equivalent: (1) $M^\bullet$ is exact at every M^i, (2) $H^i(M^\bullet) = 0$ for all i, (3) the map $0 \longrightarrow M^\bullet$ is a quasi-isomosphism.

Exercise 46. cf. [9, Ex. 2.4.3] Let $F\colon \mathcal{A} \longrightarrow \mathcal{B}$ be a left exact functor between abelian categories (for instance, the categories of modules over some rings). If $\mathcal{A}$ has enough injectives, the i-th right derived functor R^iF of F is constructed as follows. For any $A \in \mathcal{A}$, take an injective resolution $A \longrightarrow E^\bullet$ and define $R^iF(A) = H^i(F(E^\bullet))$. This definition does not depend on the choice of injective resolution and if $0 \longrightarrow A' \longrightarrow A \longrightarrow A'' \longrightarrow 0$ is

exact, then there is a long exact sequence

$$0 \longrightarrow A' \longrightarrow A \longrightarrow A'' \longrightarrow R^1F(A') \longrightarrow R^1F(A) \longrightarrow R^1F(A'') \longrightarrow \dots$$
$$\dots \longrightarrow R^iF(A') \longrightarrow R^iF(A) \longrightarrow R^iF(A'') \longrightarrow R^{i+1}F(A') \longrightarrow \dots$$

If $0 \longrightarrow A \longrightarrow E \longrightarrow M \longrightarrow 0$ is exact and E is injective, show that $R^iF(A) \simeq R^{i-1}F(M)$ for $i \geq 2$ and that $R^1F(A) = \operatorname{coker}(F(E) \longrightarrow F(M))$. More generally, show that if

$$0 \longrightarrow A \longrightarrow E^0 \longrightarrow \dots \longrightarrow E^m \longrightarrow M \longrightarrow 0$$

is exact and all E^i are injective, then $R^iF(A) \simeq R^{i-m-1}F(M)$ for $i \geq m+2$ and $R^{m+1}F(A) = \operatorname{coker}(F(E^m) \longrightarrow F(M))$.

Write down the corresponding "dimension shifting" statement for left derived functors of a right exact functor F which are constructed using projective resolutions and convince yourself that a similar proof works in this case as well.

Exercise 47. cf. [9, Example 3.1.7 & Ex. 3.2.1] Let M be an A-module. Consider the endofunctor $\mathrm{Mod}A \longrightarrow \mathrm{Mod}A$ defined by $N \longmapsto N \otimes M$ and $f \longmapsto f \otimes \mathrm{id}_M$. This functor is right exact and $\mathrm{Mod}A$ has enough projectives, so there exist left derived functors defined by $\mathrm{Tor}_i(M,N) = H^i(P_\bullet \otimes M)$, where $P_\bullet$ is any projective resolution of N. It is a fact that $\mathrm{Tor}_i(M,N) = \mathrm{Tor}_i(N,M) = H^i(P'_\bullet \otimes N)$, where $P'_\bullet$ is any projective resolution of M. Furthermore, if $0 \longrightarrow N' \longrightarrow N \longrightarrow N'' \longrightarrow 0$ is exact, we get a long exact sequence

$$\dots \longrightarrow \mathrm{Tor}_1(N',M) \longrightarrow \mathrm{Tor}_1(N,M) \longrightarrow \mathrm{Tor}_1(N'',M)$$
$$\longrightarrow N' \otimes M \longrightarrow N \otimes M \longrightarrow N'' \otimes M \longrightarrow 0.$$

Suppose that $a \in A$ is not a zero-divisor. Show that $\mathrm{Tor}_0(A/a, M) \simeq M/aM$, $\mathrm{Tor}_1(A/a, M) \simeq \{m \in M \mid am = 0\}$ and $\mathrm{Tor}_n(A/a, M) = 0$ for all $n \geq 2$.

Show that the following conditions are equivalent: (1) N is flat, (2) $\mathrm{Tor}_n(M,N) = 0$ for all $n \geq 1$ and all modules M, (3) $\mathrm{Tor}_1(M,N) = 0$ for all modules M.

Exercise 48. [2, Ex. 2.25 & 2.26]

(1) Let A be any ring and let $0 \longrightarrow N' \longrightarrow N \longrightarrow N'' \longrightarrow 0$ be an exact sequence of A-modules with N'' flat. Show that N is flat if and only if N' is flat.
(2) Show that an A-module N is flat if and only $\mathrm{Tor}_1(A/I, N) = 0$ for all finitely generated ideals $I \subseteq A$.

Sheet 13

Exercise 49. [9, Ex. 4.4.1] Let A be a regular local ring and $x_1, \dots, x_d \in \mathfrak{m}$ map to a basis of $\mathfrak{m}/\mathfrak{m}^2$. Prove that every quotient ring $A/(x_1, \dots, x_i)A$ is regular local of dimension $d - i$.

Exercise 50.

(1) Let A be a local ring and $0 \longrightarrow N' \longrightarrow N \longrightarrow N'' \longrightarrow 0$ be an exact sequence of finitely generated A-modules. Show that $\operatorname{depth}(N) \geq \min\{\operatorname{depth}(N'), \operatorname{depth}(N'')\}$.

(2) Let A be as local ring and $M \neq 0$ be a finitely generated A-module. We call M maximal Cohen-Macaulay (MCM) if $\operatorname{depth}(M) = \dim(A)$. Show that if in an exact sequence
$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0,$$
the modules M' and M'' are MCM, then the same holds for M.
Hint. Use that $\operatorname{depth}(M) \leq \dim(M)$, where $\dim(M) = \dim(\operatorname{Supp}(M))$. The proof of this fact is similar to that of the statement $\operatorname{depth}(A) \leq \dim(A)$ established in the lecture.

(3) Prove that if M is MCM and admits a direct sum decomposition $M = M_1 \oplus M_2$, then M_1 and M_2 are MCM.

Exercise 51. Let A be a regular local ring and M be an MCM module. Show that M is free.

References

[1] A. Altman and S. Kleiman, *A term of commutative algebra*, http://web.mit.edu/18.705/www/12Nts-2up.pdf.
[2] M. F. Atiyah and I. G. MacDonald, *Introduction to commutative algebra*, Addison-Wesley Publishing Co., Reading Mass.-London-Don Mills, 1969.
[3] P. L. Clark, *Commutative algebra*, http://www.math.uga.edu/ pete/integral.pdf.
[4] D. Eisenbud, *Commutative algebra with a view towards algebraic geometry*, Graduate Texts in Math. 150, Springer, New York, 1995.
[5] I. Kaplansky, *Commutative Rings*, Allyn and Bacon, Boston, 1970.
[6] Q. Liu, *Algebraic geometry and arithmetic curves*, Oxford University Press, Oxford, 2002.
[7] H. Matsumura, *Commutative ring theory*, 2nd ed., Cambridge Studies in Advanced Mathematics, Cambridge University Press, Cambridge, 1989.
[8] M. Reid, *Undegraduate commutative algebra*, LMS Student Texts 29, Cambridge University Press, Cambridge, 1995.
[9] C. Weibel, *An introduction to homological algebra*, Cambridge University Press, Cambridge, 1994.

Pawel Sosna, Fachbereich Mathematik der Universität Hamburg, Bundesstrasse 55, 20146 Hamburg, Germany
E-mail address: pawel.sosna@math.uni-hamburg.de