NOTES ON COMMUTATIVE ALGEBRA

TAMÁS SZAMUELY

CONTENTS

1. DIMENSION OF RINGS, RINGS OF LOW DIMENSION

All rings are supposed to be commutative and have a unit element. We start with the following basic definition.

Definition 1.1. Let A be a ring and $P \subseteq A$ be a prime ideal. Define the *height* of P by

$$\mathrm{ht}(P) := \sup\{r \in \mathbb{N} \mid \exists P_1 \subsetneq P_2 \subsetneq \cdots \subsetneq P_r \subsetneq P \text{ chain of prime ideals in } P\}$$

The *Krull dimension* of the ring A is

$$\dim(A) := \sup\{\mathrm{ht}(P) \mid P \subseteq A \text{ prime}\}$$

We shall prove later that over a field k both the polynomial ring $k[x_1, \ldots, x_n]$ and the power series ring $k[[x_1, \ldots, x_n]]$ have Krull dimension n. In both cases $(x_1) \subset (x_1, x_2) \subset \cdots \subset (x_1, \ldots, x_n)$ is a chain of prime ideals of maximal length. Note, however, that whereas $k[x_1, \ldots, x_n]$ is a finitely generated k-algebra and n is its minimal number of generators, this is not the case for $k[[x_1, \ldots, x_n]]$.

Remarks 1.2.

1. For A the coordinate ring of an affine variety X the chain $P_1 \subsetneq P_2 \subsetneq \cdots \subsetneq P_r$ corresponds to a chain of irreducible subvarieties $Z_1 \supsetneq Z_2 \supsetneq \cdots \supsetneq Z_r$ contained in X. The dimension is thus the length of the longest such chain. This is a non-linear version of the definition of the dimension of a vector space V as the length of a maximal chain of subspaces in V.
2. Recall that the map $Q \mapsto QA_P$ induces a bijection between prime ideals $Q \subset P$ and the prime ideals of A_P. This implies $\mathrm{ht}(P) = \mathrm{ht}(PA_P) = \dim(A_P)$.

Let us look at examples of rings of low Krull dimension. Obviously, a field has Krull dimension 0. More generally, we have:

Proposition 1.3. *A Noetherian local ring A is of Krull dimension 0 if and only if it is Artinian.*

For use in the proof below we recall the following lemma.

Lemma 1.4. *The set of nilpotent elements in a ring A is an ideal, and equals the intersection of the prime ideals in A.*

The above ideal is called the *nilradical* of A.

Proof. The first statement is clear as the radical $\sqrt{I}$ of any ideal is again an ideal. For the second one, note first that a nilpotent element is contained in every prime ideal. Conversely, assume $f \in A$ is not nilpotent. We find a prime ideal not containing f. Consider the partially ordered set of ideals in A that do not contain any power of f. This set is not empty (it contains (0)) and satisfies the condition of Zorn's lemma, so it has a maximal element P. We contend that P is a prime ideal. Assume $x, y \in A \setminus P$; we have to show that $xy \notin P$. The ideals $P+(x)$, $P+(y)$ strictly contain P, hence by maximality of P both contain some power of f. But $(P+(x))(P+(y)) \subset P+(xy)$, and therefore $P+(xy)$ also contains some power of f, hence cannot equal P. This means $xy \notin P$. □

Proof of Proposition 1.3. Assume A is of Krull dimension 0. Then by Lemma 1.4 the maximal ideal P consists of nilpotent elements. Since A is Noetherian, P is finitely generated so for a generating system $y_1, \ldots, y_k$ there is a big enough exponent N such that $y_i^N = 0$ for all i. Hence all products of $k \cdot N$ elements in P are zero,i.e. $P^{kN} = 0$. Now we have a finite descending filtration $A \supseteq P \supseteq P^2 \supseteq P^3 \supseteq \cdots \supseteq P^{kN} = 0$ of A where every quotient is a finite dimensional vector space over the field A/P, hence an Artinian A-module. Since an extension of Artinian modules is again Artinian, we are done by induction.

Conversely, assume A is Artinian, and $Q \subset P$ is a prime ideal in A. We show $Q = P$; for this we may replace A by A/Q and assume moreover that A is an integral domain. Suppose there were a nonzero element $x \in P$. As A is Artinian, the chain $(x) \supset (x^2) \supset (x^3) \supset \cdots$ must stabilize, i.e we find n such that $(x^n) = (x^{n+1})$. In particular, $x^n = rx^{n+1}$ for some $r \in A$. Since A is an integral domain, this implies $rx = 1$ which is impossible for $x \in P$. □

Remark 1.5. In fact, the proposition is true without assuming A local; see e.g. the book of Atiyah–MacDonald.

Next an important class of local rings of dimension 1.

Definition 1.6. A ring A is a *discrete valuation ring* if A is a local principal ideal domain which is not a field.

Basic examples of discrete valuation rings are localizations of **Z** or $k[x]$ at a (principal) prime ideal as well as power series rings in one variable over a field.

In the proposition below we prove that discrete valuation rings are of Krull dimension 1 and much more. Observe first that if A is a local ring with maximal ideal P, then the A-module P/P^2 is in fact a vector space over the field $\kappa(P) = A/P$, simply because multiplication by P maps P into P^2.

Proposition 1.7. *For a Noetherian local domain A with maximal ideal P and fraction field K the following conditions are equivalent:*

1. *A is a discrete valuation ring.*
2. *A has Krull dimension 1 and P/P^2 is of dimension 1 over $\kappa(P)$.*
3. *The maximal ideal P is principal, and after fixing a generator t of P every element $x \neq 0$ in K can be written uniquely in the form $x = ut^n$ with u a unit in A and $n \in \mathbf{Z}$.*

For the proof we need the following well-known lemma which will be extremely useful in other situations as well:

Lemma 1.8 (Nakayama)**.** *Let A be a local ring with maximal ideal P and M a finitely generated A-module. If $PM = M$, then $M = 0$.*

Proof. Assume $M \neq 0$ and let $m_0, \ldots, m_n$ be a minimal system of generators of M over A. By assumption m_0 is contained in PM and hence we have a relation $m_0 = p_0m_0 + \ldots, p_nm_n$ with all the p_i elements of P. But here $1 - p_0$ is a unit in A (as otherwise it would generate an ideal contained in P) and hence by multiplying the equation by $(1 - p_0)^{-1}$ we may write m_0 as a linear combination of the other terms, which is in contradiction with the minimality of the system. □

Nakayama's lemma is often used through the following corollary.

Corollary 1.9. *Let A, P, M be as in the lemma and assume given elements $t_1, \ldots, t_m \in M$ whose images in the A/P-vector space M/PM form a generating system. Then they generate M over A.*

Proof. Let T be the A-submodule generated by the t_i; we have $M = T + PM$ by assumption. Hence $M/T = P(M/T)$ and the lemma gives $M/T = 0$. □

Before proving the proposition we need another easy lemma.

Lemma 1.10. *Let A be a Noetherian integral domain and $t \in A$ an element which is not a unit. Then $\cap_n (t^n) = (0)$.*

Proof. The case $t = 0$ is obvious. Otherwise suppose $a \in \cap_n (t^n)$ is a nonzero element. Then $a = a_1 t$ for some $a_1 \in A$. Since $a \in (t^2)$, there is a_2 such that $a = a_2 t^2$, so since A is a domain we have $a_1 = a_2 t$. Repeating the argument we obtain an increasing chain of ideals $(a_1) \subset (a_2) \subset (a_3) \subset \cdots$ with $a_i = a_{i+1} t$. Here the inclusions are strict because an equality $(a_i) = (a_{i+1})$ would imply that for some s we have $a_{i+1} = a_i s = a_{i+1} t s$ which is impossible as t is not a unit. This contradicts the assumption that A is Noetherian. □

Proof of Proposition 1.7. To prove $(1) \Rightarrow (2)$, assume A is a discrete valuation ring and P is generated by t. Since A is a unique factorization domain, every nonzero prime ideal is generated by some prime element p. But (p) is contained in the maximal ideal $P = (t)$, which means that t divides p. But this is only possible if $(p) = (t) = P$, so A is of Krull dimension 1. Also, the image of t is a basis of the vector space P/P^2, whence (2). Next, assume (2) and apply Corollary 1.9 with $M = P$. It follows that the maximal ideal P of A is generated by some element t. To prove (3), it will suffice to show that it holds for every nonzero element $a \in A$ with $n \geq 0$. To find n, observe that by Corollary 1.10 there is a unique $n \geq 0$ for which $a \in P^n \setminus P^{n+1}$ which means that a can be written in the required form. Moreover, if $a = ut^n = vt^n$, then $u = v$ since A is a domain. Finally, assume (3) and take an ideal I of A. As A is Noetherian, I can be generated by a finite sequence of elements $a_1, \ldots, a_k$. Write $a_i = u_i t^{n_i}$ according to the above representation and let j be an index for which $n_i \geq n_j$ for all i. Each a_i is a multiple of t^{n_j} and hence $I = (t^{n_j})$ is principal as stated in (1). □

We now explain the origin of the name "discrete valuation ring".

Definition 1.11. For any field K, a *discrete valuation* is a surjection $v : K \to \mathbf{Z} \cup \{\infty\}$ with the properties

$$v(xy) = v(x) + v(y),$$
$$v(x + y) \geq \min\{v(x), v(y)\},$$

$$v(x) = \infty \text{ if and only if } x = 0.$$

The elements $x \in K$ with $v(x) \geq 0$ form a subring $A \subset K$ called the *valuation ring* of v.

Proposition 1.12. *A domain A is a discrete valuation ring if and only if it is the valuation ring of some discrete valuation $v : K \to \mathbf{Z} \cup \{\infty\}$, where K is the fraction field of A.*

Proof. Assume first A is a discrete valuation ring. Define a function $v : K \to \mathbf{Z} \cup \{\infty\}$ by mapping 0 to ∞ and any $x \neq 0$ to the integer n given by Proposition 1.7 (3). It is immediate to check that v is a discrete valuation with valuation ring A. Conversely, given a discrete valuation v on K, the elements of A with $v(a) > 0$ form an ideal $P \subset A$ with the property that $a \in P \setminus \{0\}$ if and only if $a^{-1} \notin A$. It follows that $A \setminus P = \{a \in A : v(a) = 0\}$ is the set of units in a and hence A is local with maximal ideal P. Note that if t is an element of P with $v(t) = 1$, then for every $p \in P$ we have $v(p/t) = v(p) - 1 \geq 0$, so that $p/t \in A$ and therefore $(t) = P$. Similarly, if $a \in K$ is a nonzero element with $v(a) = n$, we have $v(a/t^n) = 0$ and condition (3) of the above proposition follows. □

There is another very useful characterization of discrete valuation rings which uses the notion of integral closure. We begin by some reminders. Recall that given an extension of rings $A \subset B$, an element $b \in B$ is said to be *integral* over A if it is a root of a *monic* polynomial $x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in A[x]$. There is the following characterization of integral elements:

Lemma 1.13. *Let $A \subset B$ an extension of rings. The following are equivalent for an element $b \in B$:*

(1) *The element b is integral over A.*
(2) *The subring $A[b]$ of B is finitely generated as an A-module.*
(3) *There is a subring C of B containing b which is finitely generated as an A-module.*
(4) *There exists a faithful $A[b]$-module C that is finitely generated as an A-module.*

Recall that an A-module C is faithful if there is no nonzero $a \in A$ with $aC = 0$.

Proof. For the implication $(1) \Rightarrow (2)$ note that if b satisfies a monic polynomial of degree n, then $1, b, \ldots, b^{n-1}$ is a basis of $A[b]$ over A. The implication $(2) \Rightarrow (3)$ is trivial, and $(3) \Rightarrow (4)$ follows because if C is a subring as in (3) and $a \in A[b]$ satisfies $aC = 0$, then $a = a \cdot 1 = 0$. Now only $(4) \Rightarrow (1)$ remains. For this let $c_1, \ldots, c_m$ be a system of A-module generators for C and consider the A-module endomorphism of C given by multiplication by b. For all i we have $bc_i = a_{i1}c_1 + \cdots + a_{im}c_m$ with some $a_{ij} \in A$. It follows that the system of homogeneous equations

$$a_{i1}c_1 + \ldots (a_{ii} - b)c_i + \cdots + a_{im}c_m = 0$$

for $i = 1, \ldots, m$ has a nontrivial solution in the c_i, hence by Cramer's rule the determinant of the coefficient matrix annihilates the c_i and therefore equals 0 by faithfulness of C. This matrix is, up to sign, a monic polynomial in $A[x]$ evaluated at $x = b$. □

Corollary 1.14. *Those elements of B which are integral over A form a subring in B.*

Proof. Indeed, given two elements $b_1, b_2 \in B$ integral over A, the elements $b_1 - b_2$ and $b_1 b_2$ are both contained in the subring $A[b_1, b_2]$ of B which is a finitely generated A-module by assumption. □

If all elements of B are integral over A, we say that the extension $A \subset B$ is *integral*.

Corollary 1.15. *Given a tower of extensions $A \subset B \subset C$ with $A \subset B$ and $B \subset C$ integral, the extension $A \subset C$ is also integral.*

Proof. Each $c \in C$ satisfies a monic polynomial equation $c^n + b_{n-1}c^{n-1} + \cdots + b_0 = 0$ with $b_i \in B$ and is therefore integral over the A-subalgebra $A[b_0, \ldots, b_{n-1}] \subset B$. This is a finitely generated A-module because the b_i are integral over A, hence so is the A-subalgebra $A[b_0, \ldots, b_{n-1}, c] \subset C$. □

For later use we note the following fact.

Lemma 1.16. *If $A \subset B$ is an integral extension of integral domains, then A is a field if and only if B is a field.*

Proof. Assume first A is a field. If $b \in B$ is a nonzero element, it satisfies a monic polynomial equation

$$b^n + a_{n-1}b^{n-1} + \cdots + a_0 = 0$$

with $a_i \in A$ and $a_0 \neq 0$ (this latter fact uses that B is an integral domain). But then $(-a_0^{-1})(b^{n-1} + b_{n-1}b^{n-2} + \cdots + a_1)$ is an inverse for b, which shows that B is a field.

For the converse, suppose B is a field and given $a \in A$, pick $b \in B$ with $ab = 1$. Since B is integral over A, we also find $a_i \in A$ with $b^n + a_{n-1}b^{n-1} + \cdots + a_1 b + a_0 = 0$ by Lemma 1.13. Multiplying by a^{n-1} we obtain $b = -a_{n-1} - \cdots - a_1 a^{n-2} - a_0 a^{n-1} \in A$ as required. □

If A is a domain with fraction field K and L is an extension of K, the *integral closure* of A in L is the subring of L formed by elements integral over A. We say that A is *integrally closed* if its integral closure in the fraction field K is just A. By Corollary 1.15 the integral closure of a domain A in some extension L of its fraction field is integrally closed.

Example 1.17. A unique factorization domain A is integrally closed. Indeed, we may write every element of the fraction field K in the form a/b with a, b coprime. If it satisfies a monic polynomial equation $(a/b)^n + a_{n-1}(a/b)^{n-1} + a_1(a/b) + a_0 = 0$ with coefficients in A, then after multiplying with b^n we see that a^n should be divisible by b, which is only possible when b is a unit.

In particular, the ring **Z** is integrally closed.

Now we can state:

Proposition 1.18. *A local domain A is a discrete valuation ring if and only if A is Noetherian, integrally closed and its Krull dimension is 1.*

Integrally closed Noetherian domains of Krull dimension 1 are usually called *Dedekind domains.* So the proposition says that a local Dedekind domain is the same thing as a discrete valuation ring.

For the proof recall the following lemma which is a starting point of the theory of associated primes.

Lemma 1.19. *Let A be a Noetherian ring, M a nonzero A-module and I a maximal element in the system of ideals of A that are annihilators of nonzero elements of M. Then I is a prime ideal.*

Recall that the annihilator of $m \in M$ is the ideal $\{a \in A : am = 0\} \subset A$. A maximal element I as in the lemma exists because A is Noetherian.

Proof. Suppose I is the annihilator of $m \in M$ and $ab \in I$ but $a \notin I$. Then $am \neq 0$ and its annihilator J contains b. But I is also contained in J, and hence $I = J$ by maximality of I. We conclude that $b \in I$. □

Proof of Proposition 1.18. Necessity of the conditions has already been checked. For sufficiency, let P be the maximal ideal of A and fix a nonzero $x \in P$. Applying the lemma to the A-module A/xA and using the fact that P is the only nonzero prime ideal of A we find $a \in A$ such that P is the annihilator of a mod xA in A/xA (note that the annihilator of 1 mod xa is nonzero). It will suffice to show that $aP \nsubseteq xP$. Indeed, suppose $y \in P$ is such that $ay \notin xP$. Since $aP \subset xA$ by definition of P, we then have $ay = xu$ with a unit $u \in A \setminus P$ and hence $x = u^{-1}ay \in aP$. Therefore $x = az$ for $z = u^{-1}y \in P$. So $aP \subset xA$ means that for every $p \in P$ we have $ap = azb$ for some $b \in A$ and hence $p \in zA$ as A is a domain. In other words, P equals the principal ideal $(z) \subset A$, and the criterion of Propostion 1.7 (2) holds.

So assume for contradiction that $aP \subseteq xP$. In the fraction field K of A we then have $(a/x)P \subset P$, so P is a faithful $A[a/x]$-module (as both $A[a/x]$ and P are subrings of K). As A is Noetherian, P is finitely generated as an A-module, so by

Lemma 1.13 the element $a/x \in K$ is integral over A. But A is integrally closed, so $a/x \in A$ and therefore $a \in xA$. But then the annihilator of a in A/xA is A and not P. □

Remark 1.20. Let K be a field of characteristic 0. It contains $\mathbf{Q}$ as its prime subfield; let A be the integral closure of $\mathbf{Z}$ in K. Then A has Krull dimension 1. Indeed, if $P \subset A$ is a nonzero prime ideal and $x \in P$ a nonzero element, then x satisfies an irreducible monic polynomial equation $x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$ over $\mathbf{Z}$. Here $a_0 \in P \cap \mathbf{Z}$ is a nonzero element by irreducibility of the polynomial, so $P \cap \mathbf{Z} \neq (0)$ and therefore $P \cap \mathbf{Z} = (p)$ for some prime number p. But then $\mathbf{Z}/p\mathbf{Z} \subset A/P$ is an integral extension of integral domains, so A/P is a field by Lemma 1.16. This shows that P is maximal.

Assume moreover K is a finite extension of $\mathbf{Q}$; in this case K is called an *algebraic number field* and A the *ring of integers* of K. Then it can be proven using arguments from field theory that A is a finitely generated $\mathbf{Z}$-module; in particular, it is Noetherian. Thus the localization A_P by a maximal P as above is a discrete valuation ring by Proposition 1.18 (one checks easily that localizations of integrally closed domains are again integrally closed). We conclude that the ring of integers in a number field is a Dedekind domain (in fact, this was the first example studied historically).

We conclude this section with a structure theorem for ideals in Dedekind domains, generalizing unique factorization in $\mathbf{Z}$.

Theorem 1.21. *In a Dedekind domain every ideal $I \neq 0$ can be written uniquely as a product $I = P_1^{n_1} \cdots P_r^{n_r}$, where the P_i are prime ideals.*

Recall the following basic property of Noetherian rings:

Lemma 1.22. *If A is a Noetherian ring and $I \subset A$ is an ideal, there are finitely many prime ideals $P \supset I$ that are minimal with this property.*

Proof. We first show that the radical $\sqrt{I}$ is the intersection of finitely many prime ideals. Indeed, assume this is not the case. Since A is Noetherian, we may assume I is maximal with this property. Plainly $\sqrt{I}$ cannot be a prime ideal, so we find $a_1, a_2 \notin \sqrt{I}$ with $a_1 a_2 \in \sqrt{I}$. For $i = 1, 2$ let I_i be the intersection of the prime ideals containing I and a_i. Then $I_1 \cap I_2 = \sqrt{I}$ by Lemma 1.4 applied to $A/\sqrt{I}$, but each I_i is the intersection of finitely many prime ideals by maximality of I, contradiction.

Now if $\sqrt{I} = P_1 \cap \cdots \cap P_r$ with some prime ideals P_i and $P \supset I$ is a prime ideal different from the P_i, then $P \supset P_1 \cdots P_r$ and therefore $P \supset P_i$ for some i, so P is not minimal above I. □

We shall need another easy lemma:

Lemma 1.23. *Let A be an arbitrary ring, I, J ideals of A. We have $I = J$ if and only if $IA_P = JA_P$ for all maximal ideals $P \subset A$.*

Proof. For the nontrivial implication assume $a \in J$ is not contained in I. Then $\{x \in A : xa \in I\} \subset A$ is an ideal different from A, hence contained in a maximal ideal P. By definition, the image of a in JA_P lies in IA_P if and only if $sa \in I$ for some $s \in A \setminus P$ but that's not possible by choice of P, so $IA_P \neq JA_P$. □

Proof of Theorem 1.21. There are only finitely many prime ideals $P_1, \ldots, P_r$ containing I by Lemma 1.22. Since A_{P_i} is a discrete valuation ring for all i, we have $IA_{P_i} = (t_i^{n_i})$ for some $n_i > 0$, where t_i generates $P_iA_{P_i}$. So $IA_{P_i} = P_i^{n_i}A_{P_i}$ for all i. Now consider $J = P_1^{n_1} \cdots P_r^{n_r}$. If P is a prime ideal different from the P_i, it does not contain I by assumption and cannot contain any of the P_i since $\dim(A) = 1$. Since it is a prime ideal, it cannot contain J either, so for $P \neq P_i$ we have $IA_P = JA_P = A_P$. A similar reasoning shows that for $i \neq j$ we have $P_i \not\supset P_j^{n_j}$, so $P_j^{n_j}A_{P_i} = A_{P_i}$ and therefore $IA_{P_i} = P_i^{n_i}A_{P_i} = JA_{P_i}$. Now the lemma above shows $I = J$. □

2. Krull's Hauptidealsatz

Our next topic is a fundamental theorem that gives a relation between the height of a prime ideal and the number of its generators.

Theorem 2.1. (Krull's Hauptidealsatz) *Let A be a Noetherian ring and $x \in A$. If P is a minimal prime ideal such that $x \in P$, then $\mathrm{ht}(P) \leq 1$.*

Note that the statement of the theorem is non-vacuous only if x is not a unit, so this is implicitly assumed. The following is Krull's original proof.

Proof. We show that if $Q \subsetneq P$ is a prime ideal, then $\mathrm{ht}(Q) = 0$. Replacing A by A_P we may assume that A is local with maximal ideal P. Define the *n-th symbolic power* of Q by

$$Q^{(n)} := \{q \in A \mid \exists s \notin Q \text{ such that } sq \in Q^n\}.$$

This is in fact the preimage of $(QA_Q)^n$ by the localization map $A \to A_Q$.

Since P is minimal over (x), the ring $A/(x)$ is local of Krull dimension 0, hence Artinian by Proposition 1.3. Therefore the chain

$$(x, Q) \supseteq (x, Q^{(2)}) \supseteq (x, Q^{(3)}) \supseteq \cdots$$

stabilizes at some level n. So if $f \in Q^{(n)} \subseteq (x, Q^{(n)}) = (x, Q^{(n+1)})$ then $f = ax + q$ for some $a \in A$ and $q \in Q^{(n+1)}$. Then $ax = f - q \in Q^{(n)}$ but $x \notin Q$ because $Q \subsetneq P$ and P is minimal over x. By definition, there exists $s \notin Q$ such that $sax \in Q^n$ but then $a \in Q^{(n)}$ since $sx \notin Q$ because Q is a prime ideal.

In summary, we got that $Q^{(n)} \subseteq (x)Q^{(n)} + Q^{(n+1)}$ and the reverse inclusion is automatic. Therefore, $Q^{(n)}/Q^{(n+1)} = P(Q^{(n)}/Q^{(n+1)})$ because $x \in P$ and we just proved that every element of $Q^{(n)}/Q^{(n+1)}$ can be expressed as an element of $(x)Q^{(n)}/Q^{(n+1)}$. So by Nakayama's lemma we get $Q^{(n)}/Q^{(n+1)} = 0$. In other words, $(QA_Q)^n = (QA_Q)^{n+1}$ as ideals in A_Q. Now we can apply Nakayama's lemma in A_Q where the maximal ideal is QA_Q, and obtain $(QA_Q)^n = 0$. Now we are left with a local ring with a nilpotent maximal ideal. By Lemma 1.4 this implies that QA_Q is the only prime ideal in A_Q, whence $\mathrm{ht}(Q) = 0$ as required. □

Remark 2.2. Equality does not always hold in the theorem. For instance, in the 0-dimensional ring $k[x]/(x^2)$ the image of x generates a prime ideal, and so does the image of 2 in the 0-dimensional ring $\mathbf{Z}/6\mathbf{Z}$.

In these examples, the generators of the principal ideal are zero-divisors. However, if x is not a zero-divisor and P is a minimal prime ideal above (x), then $\mathrm{ht}(P) = 1$. This is because the minimal prime ideals in A consist of zero-divisors. Indeed, if P is a minimal prime ideal, then A_P is local of dimension 0, so PA_P is a nilpotent ideal. But then for every $y \in P$ we have $y^n = 0$ in A_P, i.e. $sy^n = 0$ for some $s \notin P$, and therefore y is a zero-divisor.

Theorem 2.3. (Generalization of Krull's Hauptidealsatz) *Let A be a Noetherian ring and $x_1, \ldots, x_r \in A$. If P is a prime ideal which is minimal among the prime ideals with $x_i \in P$ for all i then* $\mathrm{ht}(P) \leq r$.

Proof. We proceed by induction on r. The case $r = 1$ is exactly the Hauptidealsatz. For $r > 1$ pick any prime ideal $P_1 \subsetneq P$ such that there does not exist P': $P_1 \subsetneq P' \subsetneq P$. We show that there exist $y_1, \ldots, y_{r-1} \in A$ such that P_1 is minimal over $(y_1, \ldots, y_{r-1})$, and then we can use induction.

We may assume that P is maximal by replacing A by A_P. Since $P_1 \subsetneq P$ and P is minimal above $(x_1, \ldots, x_r)$, there exists an i such that $x_i \notin P_1$, say $i = r$. Then P is a minimal prime ideal such that $(x_r, P_1) \subseteq P$, hence $A/(x_r, P_1)$ has Krull dimension 0 with nilradical the image of P. Therefore for all $i \leq r-1$ we have $x_i^m = a_i x_r + y_i$ for some $y_i \in P_1$, $a_i \in A$ and big enough m. Thus the image of $(x_1, \ldots, x_r)$ in $A/(y_1, \ldots, y_{r-1}, x_r)$ is nilpotent; on the other hand the image of P in $A/(x_1, \ldots, x_r)$ is the nilradical. We conclude that the image of P in $A/(y_1, \ldots, y_{r-1}, x_r)$ is nilpotent, hence the image of P in $A/(y_1, \ldots, y_{r-1})$ is minimal over (x_r). As such it has height ≤ 1 by the Hauptidealsatz, so the image of P_1 in $A/(y_1, \ldots, y_{r-1})$ has height 0 as required. □

Remark 2.4. The previous theorem has the following geometric interpretation. Take $I = (f_1, \ldots, f_r) \subset k[x_1, \ldots, x_n]$ and consider $X = V(I) \subset \mathbb{A}^n$. The irreducible components of X correspond to the minimal prime ideals above I. The theorem then says that *each* of these components has dimension $\geq n - r$ (it would be much easier to prove that *some* component has dimension $\geq n - r$).

More generally, we may consider an affine variety $Y \subset \mathbb{A}^n$. The ideal I induces an ideal $\bar{I} = (\bar{f}_1, \ldots, \bar{f}_r) \subset \mathcal{A}_Y$. The irreducible components of $X \cap Y$ correspond to the minimal prime ideals above $\bar{I}$. The theorem applied to $\bar{I}$ then says that each of these components has dimension $\geq \dim Y - r$.

Corollary 2.5. *In a Noetherian ring every prime ideal has finite height, hence the prime ideals satisfy the descending chain condition. Also, a Noetherian* local*ring has finite Krull dimension.*

Remark 2.6. The corollary does *not* imply that a Noetherian ring has finite Krull dimension; there are counterexamples to this statement.

The Hauptidealsatz has the following converse.

Theorem 2.7. *If A is Noetherian and $P \subset A$ is a prime ideal with $\mathrm{ht}(P) = r > 0$, there exist $x_1, \ldots, x_r \in P$ such that P is minimal above $(x_1, \ldots, x_r)$.*

For the proof we need:

Lemma 2.8. (Prime avoidance) *Let A be any ring, and $I_1, \ldots, I_n, J \subset A$ ideals such that all I_j are prime ideals except perhaps for I_{n-1} and I_n. If $J \not\subseteq I_j$ for all j, then there exists $x \in J$ such that $x \notin I_j$ for all $j \leq n$.*

Equivalently, $J \subseteq \cup I_j$ implies $J \subseteq I_j$ for some $j \leq n$.

Proof. Induction on n: the case $n = 1$ is clear. For $n > 1$, assume that $J \not\subseteq I_j$ for all j. By induction, for $i = 1, \ldots, n$ there exist $x_i \in J$ such that $x_i \notin I_j$ for all $j \neq i$. If for some i we also have $x_i \notin I_i$, we are done, so assume $x_i \in I_i$ for all i. Then for $n = 2$ we also get $x_1 + x_2 \notin I_1$ and $x_1 + x_2 \notin I_2$, so $x_1 + x_2$ works. If $n > 2$, then I_1 is necessarily a prime ideal, so $x_2 \cdots x_n \notin I_1$ and therefore $x_1 + x_2 \cdots x_n$ works. □

Proof of Proposition 2.7. We construct inductively a sequence $x_1, \ldots, x_r$ of elements of P with the property that for all $1 \leq i \leq r$ all minimal prime ideals above $(x_1, \ldots, x_i)$ will have height $\geq i$ (hence exactly i by the generalized Hauptidealsatz). For $i = r$ it will follow that P is minimal above $(x_1, \ldots, x_r)$, for otherwise its height would be $> r$.

For $1 < i \leq r$ assume we have already constructed $x_1, \ldots, x_{i-1}$. Consider the ideal

$$I_{i-1} := \begin{cases} (x_1, \ldots, x_{i-1}) & i > 1 \\ (0) & i = 1. \end{cases}$$

Choose an $x_i \in P$ not contained in the minimal primes above I_{i-1}. By Lemma 2.8 such an x_i exists; otherwise the lemma would give that one of the minimal primes above I_{i-1} contains P, but then Theorem 2.3 would give $\mathrm{ht}(P) \leq i-1 < r$ which is impossible. Now a minimal prime ideal Q_i above $(x_1, \dots, x_i)$ is not minimal above I_{i-1} by our choice of x_i, so it contains a prime ideal Q_{i-1} minimal above I_{i-1} which has height at least $i-1$ by induction. Therefore $\mathrm{ht}(Q_i) \geq i$ as required. □

Corollary 2.9. *The height of a nonzero prime ideal P is the smallest integer r such that P is minimal above an ideal generated by r elements.*

3. Dimensions of some important rings

As an application of the results of the previous section we can compute the dimensions of many concrete rings. We begin by studying the behaviour of heights of prime ideals under homomorphisms.

Proposition 3.1. *Let $\varphi : A \to B$ be a homomorphism of Noetherian rings, $Q \subseteq B$ be a prime ideal, and $P := \varphi^{-1}(Q)$. Then $\mathrm{ht}(Q) \leq \mathrm{ht}(P) + \dim B_Q/PB_Q$.*

Here, as usual, the notation PB_Q stands for $\varphi(P)B_Q$.

Proof. Without loss of generality we may replace A by A_P, P by PA_P, B by B_Q and Q by QB_Q since the heights of P and Q do not change under these localizations. (Note also that the composite $A \stackrel{\varphi}{\to} B \to B_Q$ induces a map $A_P \to B_Q$ by the universal property of localization.) So we may assume that A and B are local and then we have to prove that $\dim B \leq \dim A + \dim B/PB$. Set $r := \mathrm{ht}(P)$ and $s := \mathrm{ht}(Q \bmod PB)$. By Proposition 2.7 we find $x_1, \dots, x_r \in A$ such that P is minimal above them and similarly, we find $y_1, \dots, y_s \in B$ such that Q modulo PB is minimal above $y_1 \dots, y_s$ modulo PB. As in the proof of the Hauptidealsatz we obtain that for N and M sufficiently large $Q^N \subseteq PB + (y_1, \dots, y_s)$ and $P^M \subseteq (x_1, \dots, x_r)$. Therefore $Q^{NM} \subseteq (\varphi(x_1), \dots \varphi(x_r), y_1, \dots, y_s)$ and therefore Q is a minimal prime ideal above $(\varphi(x_1), \dots \varphi(x_r), y_1, \dots, y_s)$.

To sum up, we have $\dim(B) = \mathrm{ht}(Q) \leq r + s = \mathrm{ht}(P) + \dim(B/PB)$, where the inequality is a consequence of the Generalized Hauptidealsatz (Theorem 2.3). □

Remark 3.2. The proposition has an important geometric interpretation. We discuss an easy special case first. Suppose k is an algebraically closed field and $A = k[x]$, $B = k[x, y]$ with φ the natural inclusion. From the Nullstellensatz we know that maximal ideals of $k[x, y]$ are of the form $Q = (x-a, y-b)$ for $a, b \in K$. Here $P = \phi^{-1}(Q) = (x-a)$, so geometrically ϕ corresponds to the projection $\pi : \mathbf{A}^2_k \to \mathbf{A}^1_k$ given by $(a, b) \mapsto a$. We have $B/PB = k[x, y]/(x-a) \cong k[y]$ which is a ring of dimension 1, and so is the localization B_Q/PB_Q. The maximal ideals of B/PB

correspond to points with first coordinate a, i.e. the points in the fibre of π above the point $x = a$ of $\mathbf{A}^1_k$. The Proposition says that this fibre has dimension at least $\mathrm{ht}(Q) - \mathrm{ht}(P) = 2 - 1 = 1$ which is indeed true.

In general, a homomorphism $\phi : A \to B$ of finitely generated k-algebras corresponds to a map of affine varieties $X \to Y$ and the proposition translates as the fact that every fibre of such a morphism has dimension at least $\dim(X) - \dim(Y)$. In the above example equality holds for all fibres but not in general; for instance, there are morphisms of surfaces that contract whole curves.

As a consequences of the proposition we can determine the Krull dimension of polynomial and power series rings.

Corollary 3.3. *If A is a Noetherian ring, then $\dim A[x] = \dim A + 1$. Consequently, if k is a field, then $\dim k[x_1, \ldots, x_n] = n$.*

Proof. The inequality $\dim A[x] \geq \dim A + 1$ is easy: a chain of prime ideals $P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_n$ in A can be considered as a chain of prime ideals in $A[x]$ using the natural embedding $A \hookrightarrow A[x]$ since the quotients $A[x]/P_iA[x] \cong (A/P_i)[x]$ are again integral domains. However, a maximal ideal $P_n \subset A$ will not be maximal in $A[x]$ because the quotient $(A/P_n)[x]$ is not a field, so the Krull dimension of $A[x]$ is strictly larger.

Conversely, it is enough to show that for a maximal ideal $Q \subset A[x]$ we have $\mathrm{ht}(Q) \leq \mathrm{ht}(A \cap Q) + 1$. For this, set $P := A \cap Q$ which is a prime ideal in A. By the previous proposition we know that

$$\mathrm{ht}(Q) \leq \mathrm{ht}(P) + \dim\left(A[x]_Q/P \cdot A[x]_Q\right)$$

So we need to prove that the second term on the right is ≤ 1 (in fact it equals 1). We compute

$$A[x]_Q/PA[x]_Q \cong (A[x]/PA[x])_{\bar{Q}} \cong ((A/P)[x])_{\bar{Q}} \cong ((A/P)_P[x])_{\bar{Q}} \cong (\kappa(P)[x])_{\bar{Q}}$$

using the notation $\bar{Q} := Q \bmod PA[x]$ and $\kappa(P) := A_P/PA_P$ for the residue field at P. Since $\kappa(P)[x]$ is a one-variable polynomial ring over a field, it has dimension 1 (every irreducible polynomial generates a maximal ideal) and localizing at Q can only lower the dimension.

This proves the first statement. The second statement follows by induction from the first, noting that polynomial rings over a field are Noetherian by the Hilbert Basis Theorem. □

Remark 3.4. Without the Noetherian property the statement is not true: For a ring A, the polynomial ring $A[x]$ can have arbitrary dimension between $\dim A + 1$ and $2\dim A + 1$. The point where we rely on the Noetherian property is in Proposition 3.1 and its proof.

Similarly, we obtain:

Corollary 3.5. *If A is a Noetherian ring, then* $\dim A[[x]] = \dim A + 1$.

Proof. As in the previous proof, an increasing chain of prime ideals in A gives an increasing chain of prime ideals in $A[[x]]$ as well, whence $\dim A[[x]] \geq \dim A + 1$. Conversely, for a maximal ideal $Q \subset A$ and $P = A \cap Q$ we again have

$$\mathrm{ht}(Q) \leq \mathrm{ht}(P) + \dim\left(A[[x]]_Q / P \cdot A[[x]]_Q\right)$$

by Proposition 3.1. As before, we compute

$$A[[x]]_Q / P \cdot A[[x]]_Q \cong ((A/P)[[x]])_{\bar{Q}} \cong ((A/P)_P[[x]])_{\bar{Q}} \cong (\kappa(P)[[x]])_{\bar{Q}}$$

It remains to recall that $\kappa(P)[[x]]$ has dimension 1 because it is a discrete valuation ring. □

Corollary 3.6. *If k is a field, then* $\dim k[[x_1, \dots, x_n]] = n$.

This follows by induction from the preceding corollary, combined with the following proposition:

Proposition 3.7. *If A is a Noetherian ring, the formal power series ring $A[[x]]$ is also Noetherian.*

Proof. This is similar to the proof of the Hilbert basis theorem. Fix an ideal $I \subset A$ and write I_r for the ideal in A generated by the leading coefficients a_r of power series of the form $a_r x^r + a_{r+1}x^{r+1} + \dots$ contained in I. Then $I_0 \subset I_1 \subset I_2 \subset \dots$ is an ascending chain, so there is n for which $I_n = I_{n+1} = I_{n+2} = ...$ Choose finite sets of generators m_{ij} for the ideals I_j with $j \leq n$ and power series $s_{ij} \in I$ with leading coefficient $m_{ij} \in I_j$. Given a power series $s = a_r x + a_{r+1}x^{r+1} + \dots$ in I, we express it as an $A[[x]]$-linear combination of the s_{ij}. If $r \leq n$, we find $b_i \in A$ such that $a_r = \Sigma\, b_i m_{ir}$, so after subtracting finitely many A-linear combinations of the s_{ij} we may assume $r > n$. But then $a_r = \Sigma\, b_i^r m_{in}$ for some $b_i^r \in A$ and therefore $s - \Sigma\, b_i^r x^{r-n} s_{in}$ begins with a term $a_{r+1}x^{r+1}$. Therefore

$$s = \sum_i \left(\sum_{r=n+1}^{\infty} b_i^r x^{r-n} \right) s_{in}$$

where the coefficient in parentheses is an element of $A[[x]]$. □

Let now A be an integral domain containing a field k. Elements $a_1, \dots, a_r \in A$ are called *algebraically dependent* if there exists a nonzero polynomial $f \in k[x_1, \dots, x_r]$ such that $f(a_1, \dots, a_r) = 0$; otherwise they are *algebraically independent*. Assume moreover that A is a finitely generated k-algebra. Then the *transcendence degree* of A

over k is the maximal number of elements in A that are algebraically independent over k. It can be shown that under our assumption that A is finitely generated this is a finite number; we denote it by $\mathrm{tr.deg}_k(A)$.

Theorem 3.8. *Under the above assumptions* $\mathrm{tr.deg}_k(A) = \dim A$.

The proof is based on two ingredients. The first is:

Lemma 3.9 (Noether's normalization lemma)**.** *In the above situation assume A has transcendence degree d over k. Then there exist algebraically independent elements $x_1, \dots, x_d$ such that A is a finitely generated module over the subring $k[x_1, \dots, x_d] \subset A$.*

Here we mean the k-subalgebra of A generated by $x_1, \dots, x_d$; by algebraic independence it is isomorphic to the polynomial ring $k[x_1, \dots, x_d]$.

Proof. We only do the case where k is infinite; it is a bit easier. Let $x_1, \dots, x_n$ be a system of k-algebra generators for A; we may assume that the first d are algebraically independent. We do induction on n starting from the case $n = d$ which is obvious. Assume the case $n-1$ has been settled. Since $n > d$, there is a nonzero polynomial f in n variables over k such that $f(x_1, \dots, x_n) = 0$. Denote by m the degree of f and by f_m its homogeneous part of degree m. Since k is infinite, we find $a_1, \dots, a_{n-1} \in k$ such that $f_m(a_1, \dots, a_{n-1}, 1) \neq 0$. Setting $x'_i := x_i - a_i x_n$ for $i = 1, \dots, n-1$ we compute

$$\begin{aligned} 0 = f(x_1, \dots, x_n) &= f(x'_1 + a_1 x_n, \dots, x'_{n-1} + a_{n-1} x_n, x_n) = \\ &= f_m(a_1, \dots, a_{n-1}, 1) x_n^m + g_{m-1} x_n^{m-1} + \dots + g_0 \end{aligned}$$

with some $g_i \in k[x'_1, \dots, x'_{n-1}]$. Dividing by $f_m(a_1, \dots, a_{n-1}, 1)$ we see that x_n satisfies a monic polynomial relation with coefficients in $k[x'_1, \dots, x'_{n-1}]$, so that $A = k[x'_1, \dots, x'_{n-1}][x_n]$ is a finitely generated module over its subalgebra $k[x'_1, \dots, x'_{n-1}]$. By induction we know that $k[x'_1, \dots, x'_{n-1}]$ is a finitely generated module over the polynomial ring $k[x_1, \dots, x_d]$, and we are done. □

Now we turn to the second ingredient.

Lemma 3.10. *Suppose $A \subset B$ is an integral extension of rings. Given a prime ideal $P \subset A$, there exists a prime ideal $Q \subset B$ such that $Q \cap A = P$.*

Proof. Localizing both A and B by the multiplicatively closed subset $A \setminus P$ we obtain a ring extension $A_P \subset B_P$ where A_P is local with maximal ideal P. We contend that $PB_P \neq B_P$. Indeed, otherwise we have an equation $1 = p_1 b_1 + \dots + p_r b_r$ with $p_i \in P$ and $b_i \in B_P$. If $C \subset B_P$ is the A_P-subalgebra generated by the b_i, then C satisfies $PC = C$ and moreover is finitely generated as an A_P-module because the

b_i are integral over A_P. Thus $C = 0$ by Nakayama's lemma which is impossible since $1 \in C$. Therefore indeed $PB_P \neq B_P$ and we find a maximal ideal $Q_P \subset B_P$ containing PB_P. By construction $Q_P \cap A_P \supset P$, hence $Q_P \cap A_P = P$ by maximality of P. Thus $Q := Q_P \cap B$ will do. □

Corollary 3.11 (Going up theorem of Cohen–Seidenberg). *Under the assumptions of the lemma given a chain $P_1 \subsetneq P_2 \subsetneq \cdots \subsetneq P_r$ of prime ideals in A, there exists a chain $Q_1 \subsetneq Q_2 \subsetneq \cdots \subsetneq Q_r$ of prime ideals in B such that $Q_i \cap A = P_i$ for $i = 1, \ldots, r$.*

Proof. We use induction on r. By the lemma we find $Q_1 \subset B$ with $Q_1 \cap A = P_1$. Assume $Q_1 \subsetneq Q_2 \subsetneq \cdots \subsetneq Q_{r-1}$ have been constructed, and denote by $\bar{P}_r$ the image of P_r in A/P_{r-1}. Since B/Q_{r-1} is integral over A/P_{r-1}, the lemma gives a prime ideal $\bar{Q}_r$ in B/Q_{r-1} such that $\bar{Q}_r \cap (A/P_{r-1}) = \bar{P}_r$. Now take Q_r to be the preimage of $\bar{Q}_r$ in B. □

Proof of Theorem 3.8. By Noether's normalization lemma we find a polynomial ring $R := k[x_1, \ldots, x_d]$ contained as a k-subalgebra in A such that A is a finitely generated R-module, so in particular integral over R; we know from Corollary 3.3 that $\dim(R) = d$. By the going up theorem we may extend the maximal chain $(0) \subset (x_1) \subset (x_1, x_2) \subset \cdots \subset (x_1, \ldots x_d)$ of prime ideals in R to a chain $(0) \subsetneq Q_1 \subsetneq Q_2 \subsetneq \cdots \subsetneq Q_d$ of prime ideals in A, whence $\dim A \geq d$. On the other hand, if Q is a maximal ideal in A with $\mathrm{ht}(Q) = \dim(A)$, set $P := Q \cap R$. The algebra $A_{R \setminus P}/PA_{R \setminus P}$ is finite dimensional over the field R_P/PR_P, so it is Artinian. The local ring A_Q/PA_Q is a localization of $A_{R \setminus P}/PA_{R \setminus P}$, so its Krull dimension is 0 by Proposition 1.3. Thus Proposition 3.1 applied to the inclusion map $R_P \to A_Q$ gives $\dim A = \dim A_Q \leq \mathrm{ht}(P) \leq d$. □

Remark 3.12. The theorem contains as a special case the weak form of Hilbert's Nullstellensatz: if A as in the theorem is a field, it has Krull dimension 0, hence has transcendence degree 0 over k by the theorem, i.e. it is a finite extension. In particular, if moreover k is algebrically closed, it must be k itself. Consequently, if P is a maximal ideal in the polynomial ring $k[x_1, \ldots, x_n]$ with k algebraically closed, we have $A := k[x_1, \ldots, x_n]/P \cong k$, so denoting by a_i the image of x_i mod P we get $P \supseteq (x_1 - a_1, \ldots, x_n - a_n)$. Since $(x_1 - a_1, \ldots, x_n - a_n)$ is a maximal ideal, this inclusion is an equality. We have proven that every maximal ideal of $k[x_1, \ldots, x_n]$ is of the form $(x_1 - a_1, \ldots, x_n - a_n)$ with some $a_i \in k$.

We now prove a stronger form of Theorem 3.8.

Theorem 3.13. *Let A be an integral domain that is a finitely generated algebra of transcendence degree d over a field k. Every maximal chain of prime ideals of A has length d.*

As consequences we have:

Corollary 3.14. *Let A be as in the theorem.*

(1) *Every prime ideal $P \subset A$ satisfies the equality* $\mathrm{ht}(P) = \mathrm{tr.deg}_k(A) - \mathrm{tr.deg}_k(A/P)$.
(2) *Given two prime ideals $P \subset Q$ of A, every maximal chain of prime ideals between P and Q has length* $\mathrm{ht}(P) - \mathrm{ht}(Q)$.

Proof. For statement (1) choose a maximal chain of prime ideals $P_1 \subsetneq P_2 \cdots \subsetneq P_r \subsetneq P$ and extend it to a maximal chain $P_1 \subsetneq P_2 \cdots \subsetneq P_r \subsetneq P \subsetneq Q_1 \subsetneq \cdots \subsetneq Q_s$ of prime ideals in A. By construction $\mathrm{ht}(P) = r$ and by the theorem $\dim(A) = r + s$, $\dim(A/P) = s$. Statement (2) follows from (1). □

Rings having the property in (2) above are called *catenary* rings.
The following proof of the theorem is based on:

Proposition 3.15 (Going down theorem of Cohen–Seidenberg). *Let $A \subset B$ be an integral extension of integral domains such that A is integrally closed in its fraction field K and the fraction field L of B is a finite extension of K.*

Given prime ideals $P_1 \subsetneq P_2$ of A and a prime ideal $Q_2 \subset B$ with $Q_2 \cap A = P_2$, there exists a prime ideal $Q_1 \subsetneq Q_2$ of B with $Q_1 \cap A = P_1$.

Remarks 3.16.
1. Of course, as in Corollary 3.11 one concludes by induction that for every finite descending chain of prime ideals of A we can find a finite descending chain of prime ideals of B lying above it.
2. The proposition also holds without the assumption $L|K$ finite but we'll only use the finite case. The proof in the general case uses infinite Galois theory.

We begin the proof of the going down theorem with some preliminary observations.

Remarks 3.17.
1. If $A \subset B$ is an integral extension of rings and $Q_1 \subsetneq Q_2$ are prime ideals in B, then the intersections $P_i := Q_i \cap A$ satisfy $P_1 \subsetneq P_2$. Indeed, if $Q_1 \cap A = Q_2 \cap A = P$, then after localizing by $A \setminus P$ we obtain an integral extension $A_P \subset B_P$ with two prime ideals $Q_1 B_P \subsetneq Q_2 B_P$ whose intersection with A is the maximal ideal P. Passing to the integral extensions $A_P/PA_P \subset B_P/Q_i B_P$ we see from Lemma 1.16 that both $Q_1 B_P$ and $Q_2 B_P$ must be maximal ideals, which is impossible.

2. Let $A \subset B$ be an extension of integral domains and assume that the extension $K \subset L$ of their fraction fields is finite and purely inseparable. This means that both have characteristic $p > 0$ and $L = K(\sqrt[p^{r_1}]{a_1}, \ldots, \sqrt[p^{r_m}]{a_m})$ for some $a_i \in K$ and $r_i > 0$.

In particular, for r large enough $L^{p^r} \subset K$. Assume moreover that $B \cap K = A$ (this is the case e.g. in the situation of the proposition). Then it is straightforward to check that if $P \subset A$ is a prime ideal, then $P^B := \{b \in B : b^{p^r} \in P\}$ is a prime ideal of B. Moreover $P^B \cap A = P$ and for a prime ideal $Q \subset B$ we have $(Q \cap A)^B = Q$. Thus the assignment $P \to P^B$ gives an inclusion-preserving bijection between the prime ideals of A and B.

We also need the following lemma generalizing a well-known fact from algebraic number theory.

Lemma 3.18. *In the situation of the proposition assume moreover that B is the integral closure of A in L and the extension $L|K$ is Galois with group G. If $P \subset A$ is a prime ideal, then G acts transitively on the set of prime ideals $Q \subset B$ with $Q \cap A = P$.*

Note that if $\sigma \in G$ and $b \in B$, then $\sigma(b) \in B$ because it is integral over A (in fact it satisfies the same monic polynomial) and B is the integral closure of A in L. Furthermore, if $Q \subset B$ is a prime ideal, then $\sigma(Q) := \{\sigma(b) \in B : b \in Q\}$ is a prime ideal in B, which defines the G-action in the lemma.

Proof. Let $Q, Q' \subset B$ be prime ideals with $Q \cap A = Q' \cap A = P$ and assume that $\sigma(Q) \neq Q'$ for any $\sigma \in G$. Here $Q' \not\subseteq \sigma(Q)$ for any $\sigma \in G$ by Remark 3.17 (1), so by prime avoidance (Lemma 2.8) we find $b \in Q'$ such that $b \notin \sigma(Q)$ for any $\sigma \in G$. Then $N_{L|K}(b) := \Pi_{\sigma \in G}\sigma(b) \in B \cap K = A$ because b is fixed by G and A is integrally closed. But since G contains the identity map of L, we have $N_{L|K}(b) \in Q' \cap A = P$. But then $N_{L|K}(b) \in Q$, so since Q is a prime ideal, we have $\sigma(b) \in Q$ for some $\sigma \in G$, whence $b \in \sigma^{-1}(Q)$, a contradiction. □

Proof of Proposition 3.15. Assume first the extension $L|K$ is separable. Embed L in a finite Galois extension L' of K with group G, and let B' be the integral closure of A in L'. By the going up theorem we find prime ideals $Q'_1 \subsetneq Q'_2$ in B' such that $Q'_i \cap A = P_i$ for $i = 1, 2$. Furthermore, by Lemma 3.10 we find a prime ideal $Q' \subset B'$ with $Q' \cap B = Q_2$. Since $Q' \cap A = Q'_2 \cap A = P_2$, by Lemma 3.18 we find $\sigma \in G$ with $\sigma(Q'_2) = Q'$. It follows that $\sigma(Q'_1) \subset Q'$ is a prime ideal satisfying $\sigma(Q'_1) \cap A = P_1$, and therefore $Q_1 := \sigma(Q'_1) \cap B$ has the required properties.

In the general case let $K \subset L^s \subset L$ be the maximal separable subextension and set $B^s := B \cap L^s$. The proposition holds for the extension $A \subset B^s$ by the previous paragraph. Since $L|L^s$ is a purely inseparable extension, we conclude by applying Remark 3.17 (2) to the extension $B^s \subset B$. □

Now that the going down theorem is proven, we can turn to:

Proof of Theorem 3.13. We use induction on $d = \dim(A) = \text{tr.deg}_k(A)$. The case $d = 0$ is clear because then A is a field. Assume $d > 0$ and use the Noether normalization lemma to find a polynomial ring $R := k[x_1, \ldots, x_d]$ over which A is finitely generated as a module. Consider a maximal chain $(0) \subsetneq Q_1 \subsetneq \cdots \subsetneq Q_m$ of prime ideals of A, and set $P_i := Q_i \cap R$ for all i. Since $P_1 \neq (0)$ by Remark 3.17 (1), we find a nonzero irreducible polynomial $f \in P_1$. The principal ideal $(f) \subset P_1$ is a prime ideal as f is a prime element in the unique factorization domain $R = k[x_1, \ldots, x_d]$. If $(f) \neq P_1$, then applying the going down theorem to $(f) \subset P_1$ and Q_1 we find a prime ideal $Q_0 \subset Q_1$ in A with $Q_0 \cap R = (f)$. But then $(0) \subsetneq Q_1 \subsetneq \cdots \subsetneq Q_m$ cannot be a maximal chain, so we have $(f) = P_1$. In this case $\bar{A} := A/Q_1$ is a finitely generated $R/(f)$-module, hence of transcendence degree $d-1$. By induction every maximal chain of prime ideals in $\bar{A}$ has length $d-1$, so every maximal chain in A starting with $(0) \subset Q_1$ has length d. As Q_1 was arbitrary, the theorem is proven. □

4. Regular local rings and regular sequences

Observe that if A is a local ring with maximal ideal P, then $\kappa(P) := A/P$ is a field (the *residue field* of A) and P/P^2 inherits a $\kappa(P)$-vector space structure from the A-module structure on P.

Definition 4.1. *A Noetherian local ring A with maximal ideal P is a* regular *local ring if* $\dim_{\kappa(P)} P/P^2 = \dim A$.

If $x_1, \ldots, x_r \in P$ are such that their mod P^2 images form a basis in P/P^2, we call them a regular system of parameters.

Remarks 4.2.
1. The algebraic meaning of regularity is the following. If $x_1, \ldots, x_r \in P$ are such that their images modulo P^2 generate P/P^2, then they also generate P as an ideal by Corollary 1.9. In fact, they form a *minimal* system of generators if and only if their mod P^2 images form a $\kappa(P)$-basis of P/P^2. By the Hauptidealsatz $r \geq \dim A$, so a Noetherian local ring is regular if and only if P is generated by the smallest possible number of elements.

2. If A is the local ring of an (affine) variety X at some point P, it is a theorem of Zariski that P/P^2 is the dual space of the tangent space of X at P. Points where the dimension of the tangent space equals the dimension of the variety are called smooth (or nonsingular) points in algebraic geometry. Thus regular local rings are the local rings of smooth points. We'll come back to this fact later.

Examples 4.3.

1. Basic examples of regular local rings of dimension n are power series rings $k[[x_1, \dots, x_n]]$ over a field k. (We know that they are Noetherian and local of dimension n, and $x_1, \dots, x_n$ form a regular system of parameters.)

2. The regular local rings of dimension 1 are exactly the discrete valuation rings. This follows from Proposition 1.7 and Theorem 4.6 below.

Proposition 4.4. *If A is a regular local ring and $x_1, \dots, x_r$ a regular system of parameters in A, then $A/(x_1, \dots, x_i)$ is a regular local ring of dimension $r - i$ for all $1 \leq i \leq r$.*

In fact, we prove more:

Proposition 4.5. *If A is a Noetherian ring, P is a minimal prime ideal above $x_1, \dots, x_r$ and $\mathrm{ht}(P) = r$, then $\mathrm{ht}(P/(x_1, \dots, x_i)) = r - i$ in $A/(x_1, \dots, x_i)$ for all $1 \leq i \leq r$.*

Proof. Set $s := \mathrm{ht}(P/(x_1, \dots, x_i))$. By the generalized Hauptidealsatz we have $s \leq r - i$ since $P/(x_1, \dots, x_i)$ is minimal above the images of $x_{i+1}, \dots, x_r$ in $A/(x_1, \dots, x_i)$. On the other hand, by the converse of Hauptidealsatz (Proposition 2.7) we get elements $\bar{y}_1, \dots, \bar{y}_s$ such that $P/(x_1, \dots, x_i)$ is minimal above $\bar{y}_1, \dots, \bar{y}_s$. Lifting these elements to $y_1, \dots, y_s \in P$ we get that it is minimal above $x_1, \dots, x_i, y_1, \dots, y_s$, whence $i + s \geq r$, again by the Hauptidealsatz. This proves $s = r - i$ as required. □

Theorem 4.6. *A regular local ring is an integral domain.*

Proof. We proceed by induction on $d := \dim A$. If $d = 0$, then the maximal ideal P satisfies $P = P^2$, hence equals (0) by Nakayama's lemma and the statement is clear. Now assume the proposition holds for $d - 1$. Let $P_1, \dots, P_m$ be the minimal prime ideals of A. We apply prime avoidance (Lemma 2.8) to $P_1, \dots, P_m, P^2$ and P. We know that $P \not\subseteq P_i$ and $P \not\subseteq P^2$, so there exists an $x \in P \backslash P^2$ such that $x \notin P_i$ for all i. Since $x \notin P^2$, it is part of a regular system of parameters of A (as x mod P^2 is part of a basis of P/P^2). By Proposition 4.4 the quotient $A/(x)$ is then regular and local of dimension $d - 1$. Hence by induction we know that $A/(x)$ is an integral domain, so (x) is a prime ideal. Since $x \notin P_i$ for all i, the prime ideal (x) cannot be minimal, so it properly contains one of the minimal prime ideals P_i. In particular, $x \notin P_i$ but for all $y \in P_i$ we have $y = ax$ for some $a \in A$. So $a \in P_i$ and we conclude that $P_i = (x)P_i$. This implies $P_i = PP_i$, so by Nakayama's lemma $P_i = (0)$, i.e. (0) is a prime ideal. □

Now comes a key definition.

Definition 4.7. *Let A be a ring. Elements $x_1, \dots, x_r \in A$ form a* regular sequence *if*

(1) *x_i is not a zero-divisor modulo $(x_1, \dots, x_{i-1})$ for all $1 \leq i \leq$r.*
(2) *$(x_1, \dots, x_r) \neq A$.*

Note that when A is local, the second condition implies that all x_i are contained in the maximal ideal.

Remarks 4.8.
1. If A is Noetherian and local with maximal ideal P, every permutation of a regular sequence is again a regular sequence. (The condition that A is local is necessary: one can check that in the polynomial ring $k[x_1, x_2, x_3]$ the sequence $x_1(x_1 - 1), x_1x_2 - 1$, x_1x_3 is regular but $x_1(x_1 - 1), x_1x_3, x_1x_2 - 1$ is not.)

To see this, it is enough to show that for all i interchanging x_i and x_{i+1} in a regular sequence gives a regular sequence. Replacing A by $A/(x_1, \dots, x_{i-1})$ if necessary we reduce to $i = 1$ and then to $r = 2$. Let (x_1, x_2) be a regular sequence in A and K the kernel of the map given by multiplication by x_2. If $x \in K$, we have $x = x_1x'$ for some x' as x_2 is not a zero divisor modulo (x_1). Here $x' \in K$ because $x_2x_1x' = 0$ and x_1 is not a zero divisor. It follows that $x_1K = K$, hence $PK = K$ and $K = 0$ by Nakayama's lemma. This shows x_2 is not a zero divisor in A. To see that x_1 is not a zero divisor mod (x_2), assume $x_1y = x_2z$ for some $y, z \in A$. Since x_2 is not a zero divisor mod (x_1), we get $z = x_1z'$ for some z', whence (using that x_1 is not a zero divisor) $y = x_2z'$, as required.

2. For $A = k[x_1, \dots, x_n]$ the geometric meaning of the definition is the following: a sequence of nonconstant elements $f_1, \dots, f_r$ forms a regular sequence if and only if for all i the hypersurface $V(f_i)$ intersects each irreducible component of $V(f_1, \dots, f_{i-1})$ properly.

Theorem 4.9. *Let A be a Noetherian local ring with maximal ideal P and $x_1, \dots, x_d$ a minimal system of generators for P. Then A is a regular local ring if and only if $x_1, \dots, x_d$ is a regular sequence.*

Proof. By Remark 4.2 (1) the x_i form a minimal system of generators for P if and only if modulo P^2 their images form a basis of P/P^2. So if A is regular, then the x_i form a regular system of parameters, hence a regular sequence by Proposition 4.4 and Theorem 4.6. The converse results from the following lemma. □

Lemma 4.10. *If A is a Noetherian local ring and $x_1, \dots, x_r$ is a regular sequence in A, then* $\dim A/(x_1, \dots, x_r) = \dim A - r$.

The lemma looks similar to Proposition 4.5 but does not follow from it: there we assumed $\mathrm{ht}(P) = r$ whereas here we want to prove it using the fact that the sequence is regular.

Proof. As in the proof of Proposition 4.5, setting $s = \dim A/(x_1, \dots, x_r)$ and applying Proposition 2.7 to $A/(x_1, \dots, x_r)$ we find $y_1, \dots, y_s \in P$ such that P is a minimal prime ideal containing $x_1, \dots, x_r, y_1, \dots, y_s$. The generalized Hauptidealsatz then gives $\dim A = \mathrm{ht}P \le r + s$. For the reverse inequality, observe that x_1 is not a zero divisor in A, so for all minimal prime ideals $P' \supseteq (x_1)$ we have $\mathrm{ht}(P') = 1$ by Remark 2.2. In other words, $\dim A/(x_1) \le \dim A - 1$, so we can use induction along the regular sequence $x_1, \dots, x_r$ to obtain $s = \dim A/(x_1, \dots, x_r) \le \dim A - r$. □

Remark 4.11. If A is regular local of dimension d, it is not necessarily true that a regular sequence of length d generates the maximal ideal. One counterexample among many: $x_1, x_2, \dots, x_{d-1}, x_d^2$ in $k[[x_1, \dots, x_d]]$.

To close this section we globalize the definition of regular local rings.

Definition 4.12. A Noetherian ring A is *regular* if all localizations A_P by prime ideals $P \subseteq A$ are regular local rings.

Remark 4.13. We shall prove later that every localization of a regular local ring by a prime ideal is again regular. It will follow that a Noetherian ring is regular if and only if all localizations by *maximal* ideals are regular local rings.

Examples 4.14.

(1) By Proposition 1.18 Dedekind domains are regular.
(2) If X is a smooth affine variety over an algebraically closed field, then the coordinate ring $\mathcal{A}_X$ is regular. We'll prove this in a more general form later.

We give an algebraic proof for the latter example in the case of affine space:

Proposition 4.15. *If A is a regular ring, then $A[t]$ is regular as well. Consequently, if k is a field, then $k[t_1, \dots, t_n]$ is regular.*

Proof. Let $Q \subseteq A[t]$ be a prime ideal and take $P := Q \cap A$. Then $A[t]_Q$ is a localization of $A_P[t]$ where A_P is regular, so we can assume that A is regular local with maximal ideal P. The prime ideal Q maps to a principal ideal $(\overline{f}) \subseteq k[t]$ modulo P. If $\overline{f} = 0$, then $Q = PA[t]$ and so $\dim A[t]_Q = \dim A$ using Corollary 3.3 (and its proof), whereas a regular system of parameters for P is also one for Q. So we may assume $\overline{f} \neq 0$ and lift $\overline{f}$ to $f \in A[t]$. We obtain $Q = (P, f)$ where f is not a zero-divisor modulo P. Therefore choosing a regular system of parameters for P and adding f we get a regular sequence generating Q; by construction it is a minimal system of generators. By Theorem 4.9 this proves that $A[t]_Q$ is regular. □

5. COMPLETIONS

Completion is an algebraization of the notion of power series expansion for analytic functions. Here is the precise definition.

Definition 5.1. Let A be a ring, and $I \subset A$ an ideal. The *completion* of A with respect to I is

$$\widehat{A} := \{(a_n) \subset \prod_{n=1}^{\infty}(A/I^n) \,:\, a_n = a_{n+1} \bmod I^n \text{ for all } n\}.$$

This is again a ring with the obvious operations. There is a natural map $A \to \widehat{A}$ given by $a \mapsto (a \bmod I^n)$; if it is an isomorphism, we say that A is *complete* with respect to I.

The basic example is:

Example 5.2. Consider the polynomial ring $A = k[x_1, \dots, x_n]$, k a field, and $I = (x_1, \dots, x_n)$. Then $\widehat{A}$ is the formal power series ring $k[[x_1, \dots, x_n]]$.

Observe that we get the same power series ring if instead of A we start with the localization $A_I = k[x_1, \dots, x_n]_{(x_1,\dots,x_n)}$. We shall soon see that the completion with respect to the maximal ideal of any regular local ring containing a field is a power series ring.

Completion is a special case of the inverse limit construction in category theory. Recall that an *inverse system* of groups (rings, modules, etc.) indexed by **N** together with its natural ordering is given by a group (ring, module...) G_n for each $n \geq 0$ and a morphism $\phi_n : G_{n+1} \to G_n$ for each $n > 0$. The *inverse limit* of the system is defined by

$$\lim_{\leftarrow} G_n := \{(g_n) \subset \prod_{n=1}^{\infty} G_n \,:\, g_n = \phi_n(g_{n+1}) \text{ for all } n\}.$$

Important inverse systems of modules over a fixed ring A are given by descending chains of submodules $M = M^0 \supset M^1 \supset M^2 \supset \dots$ of a fixed A-module M; such chains are called *filtrations*. The modules in the inverse system are the quotients M/M^n and the maps the natural projections. We call the inverse limit the completion of M with respect to the chain (M^n) and denote it by $\widehat{M}$. For instance, we may take $M^n := I^n M$ for an ideal $I \subset A$; in this case we call $\widehat{M}$ the *I-adic completion of M*. The case $M = A$ gives back the completion $\widehat{A}$ defined above.

There is a natural map $M \to \widehat{M}$ given by sending $m \in M$ to the sequence $(m \bmod M^n)$. In general it is neither injective nor surjective. However, in the case when it is an isomorphism, we say that M is *complete* (with respect to the filtration (M^n)).

There are natural surjective projections $p_n : \widehat{M} \to M/M^n$ for each n; set $\bar{M}^n := \ker(p_n)$. The p_n induce isomorphisms $\widehat{M}/\bar{M}^n \cong M/M^n$, so that $\widehat{M}$ is complete with respect to the chain $(\bar{M}^n)$. Note also that by definition $\cap_n \bar{M}^n = (0)$ but $\cap_n M^n$ can be nontrivial.

The next observation shows that we have a certain freedom in choosing the inverse system defining a completion.

Proposition 5.3. *Given an A-module M, consider two filtrations $M^0 \supset M^1 \supset M^2 \supset \dots$ and $N^0 \supset N^1 \supset N^2 \supset \dots$ by submodules. If for each M^n there exists N^m with $N^m \subset M^n$ and conversely, for each N^n there exists M^m with $M^m \subset N^n$. Then there is a canonical isomorphism*

$$\lim_{\leftarrow} M/M^n \cong \lim_{\leftarrow} M/N^n.$$

Proof. In the special case when the N^n can be identified with a subsequence of the M^n there is a natural map $\lim\limits_{\leftarrow} M/M^n \to \lim\limits_{\leftarrow} M/N^n$ given by restriction to subsequences which is plainly an isomorphism.

In the general case we can find strictly increasing maps $\alpha, \beta : \mathbf{N} \to \mathbf{N}$ such that for each M^n we have $N^{\alpha(n)} \subset M^n$ and for each N^n we have $M^{\beta(n)} \subset N^n$. There are natural maps $\lim\limits_{\leftarrow} M/N^{\alpha(n)} \to \lim\limits_{\leftarrow} M/M^n$ and $\lim\limits_{\leftarrow} M/M^{\beta(n)} \to \lim\limits_{\leftarrow} M/N^n$ induced by the natural projections. Composing with the isomorphisms constructed in the special case we get maps $\lim\limits_{\leftarrow} M/N^n \to \lim\limits_{\leftarrow} M/M^n$ and $\lim\limits_{\leftarrow} M/M^n \to \lim\limits_{\leftarrow} M/N^n$ which are plainly inverse to each other. □

Remark 5.4. In the above situation we may equip M with a topology in which we declare the M^n to be a basis of open neighbourhoods of 0. In the case $M^n = I^n M$ this is called the I-adic topology. The topology is Hausdorff if and only if the intersection of the M^n is 0.

A sequence $(m_n) \subset M$ is a Cauchy sequence for this topology if $m_i - m_j \in M^n$ for i, j larger than an index N depending on n; it converges to $m \in M$ if $m - m_i \in M^n$ for i larger than an index N depending on n. In the completion $\widehat{M}$ every Cauchy sequence is convergent.

The condition of the above proposition says that the topologies generated by the submodules M^n and N^n are equivalent. Thus the completion depends only on the topology of the module.

In the remainder of this section the base ring A will always be Noetherian. The key result is:

Proposition 5.5. *Let*

$$0 \to M_1 \to M_2 \to M_3 \to 0$$

be an exact sequence of finitely generated A-modules, with A a Noetherian ring. Then for an ideal $I \subset A$ the natural sequence of I-adic completions

$$0 \to \widehat{M_1} \to \widehat{M_2} \to \widehat{M_3} \to 0$$

is exact.

Before proving the proposition we derive a series of corollaries.

Corollary 5.6. *We have canonical isomorphisms* $\widehat{A}/\widehat{I} \cong A/I$ *and* $\widehat{I}^n/\widehat{I}^{n+1} \cong I^n/I^{n+1}$ *for all* $n > 0$.

Proof. Apply the proposition with $M_1 = I^{n+1}$, $M_2 = I^n$ (also for $n = 0$, where $I^0 = A$) and observe that $\widehat{I^n/I^{n+1}} = I^n/I^{n+1}$. □

Corollary 5.7. *If* A *is Noetherian and* $J = (a_1, \ldots, a_n) \subset A$ *is any ideal, then its* I*-adic completion as an* A*-module satisfies* $\widehat{J} \cong J\widehat{A}$.

Proof. Applying the proposition to the exact sequence

$$0 \to J \to A \to A/J \to 0$$

shows $\widehat{A/J} \cong \widehat{A}/\widehat{J}$. Next, consider the exact sequence

$$A^n \xrightarrow{\phi} A \to A/J \to 0$$

where $\phi(t_1, \ldots t_n) := \Sigma\, a_i t_i$. Applying the proposition again gives the exact sequence

$$\widehat{A}^n \xrightarrow{\widehat{\phi}} \widehat{A} \to \widehat{A}/\widehat{J} \to 0$$

so we conclude $\widehat{J} = \mathrm{Im}\,(\widehat{\phi})$. But $\widehat{\phi}$ is given by $\phi(\widehat{t}_1, \ldots \widehat{t}_n) := \Sigma a_i \widehat{t}_i$ (or in other words $\widehat{\phi} = \phi \otimes \mathrm{id}_{\widehat{A}}$), so $\mathrm{Im}\,(\widehat{\phi}) = J\widehat{A}$. □

The next corollary shows that complete Noetherian rings are close to power series rings.

Corollary 5.8. *Let* A *be a Noetherian ring,* $I = (a_1, \ldots, a_n)$ *an ideal of* A*. Then the* I*-adic completion* $\widehat{A}$ *satisfies*

$$\widehat{A} \cong A[[x_1, \ldots, x_n]]/(x_1 - a_1, \ldots x_n - a_n).$$

Proof. Consider the polynomial ring $B := A[x_1, \ldots, x_n]$ and define an A-homomorphism $B \to A$ by sending x_i to a_i. It is surjective with kernel $J := (x_1 - a_1, \ldots, x_n - a_n)$, and the ideal $(x_1, \ldots, x_n) \subset B$ maps onto I in A. Applying Proposition 5.5 to the $(x_1, \ldots, x_n)$-adic completion of

$$0 \to J \to B \to A \to 0$$

shows $\widehat{A} \cong \widehat{B}/\widehat{J}$. By Corollary 5.7 we have $\widehat{J} \cong J\widehat{B}$, so it remains to observe that $\widehat{B} \cong A[[x_1, \ldots, x_n]]$. □

Combining Proposition 3.7 with Corollary 5.8 we get:

Corollary 5.9. *If* A *is a Noetherian ring, any completion* $\widehat{A}$ *of* A *by an ideal is Noetherian.*

The *proof of Proposition 5.5* will be given in two steps.

Step 1: We prove the exactness of the sequence of inverse limits

$$0 \to \varprojlim M_1/(I^n M_2 \cap M_1) \to \varprojlim M_2/I^n M_2 \to \varprojlim M_3/I^n M_3 \to 0.$$

Step 2: We establish an isomorphism $\varprojlim M_1/(I^n M_2 \cap M_1) \cong \varprojlim M_1/I^n M_1$.

Step 1 follows by applying part $a)$ of the following general lemma to the exact sequences

$$0 \to M_1/(I^n M_2 \cap M_1) \to M_2/I^n M_2 \to M_3/I^n M_3 \to 0.$$

Lemma 5.10. *Let $(A_n), (B_n)$ and (C_n) be inverse systems of abelian groups such that there are commutative diagrams with exact rows*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A_{n+1} & \longrightarrow & B_{n+1} & \longrightarrow & C_{n+1} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \phi_n^A} & & \downarrow{\scriptstyle \phi_n^B} & & \downarrow{\scriptstyle \phi_n^C} & & \\ 0 & \longrightarrow & A_n & \longrightarrow & B_n & \longrightarrow & C_n & \longrightarrow & 0 \end{array}$$

for each $n > 0$.

The induced sequence

$$1 \to \varprojlim A_n \to \varprojlim B_n \to \varprojlim C_n \to 1$$

of inverse limits is exact in each of the following cases:

$a)$ The maps ϕ_n^A are surjective for all n.

$b)$ For each n there exists $m \geq n$ such that the map $\phi_{mn}^A := \phi_n^A \circ \phi_{n+1}^A \circ \cdots \circ \phi_m^A : A_{m+1} \to A_n$ is 0.

Proof. Left exactness of the sequence (without any of the additional conditions) is immediate from the definition of the inverse limit. For surjectivity on the right we have to show that every sequence $(c_n) \in \varprojlim C_n$ is the image of a sequence $(b_n) \in \varprojlim B_n$. Choose arbitrary liftings b_n of the c_n. We modify them by adding suitable elements $a_n \in A_n$ so that $\phi_n(b_{n+1}) = b_n$ will hold for all n.

Assuming condition $a)$ we use induction on n. Assume that b_i have been constructed for $i \leq n$ such that $\phi_i(b_{i+1}) = b_i$ for $i \leq n-1$. Now consider b_{n+1}. The element $\phi_n^B(b_{n+1}) - b_n$ maps to 0 in C_n, hence it comes from some $a_n \in A_n$. As ϕ_n^A is surjective, we find $a_{n+1} \in A_{n+1}$ with $\phi_n^A(a_{n+1}) = a_n$. Then $b_{n+1} - a_{n+1}$ still maps to c_{n+1} in C_{n+1} but moreover it maps to b_n in B_n.

Assuming condition $b)$, consider $a_n = \phi_n^B(b_{n+1}) - b_n$ for all n and set

$$a_n' := a_n + \sum_{m=n}^{\infty} \phi_{mn}^A(a_{m+1}).$$

By condition $b)$ all sums here are finite. Moreover, $\phi^A_{n+1}(a'_{n+1}) = a'_n - a_n$, so replacing b_n by $b_n + a'_n$ we have $\phi^B_{n+1}(b_{n+1} + a'_{n+1}) = b_n + a'_n$ as required. □

Remarks 5.11.

1. In case $b)$ the assumption actually implies $\lim\limits_{\leftarrow} A_n = 0$, so $\lim\limits_{\leftarrow} B_n \xrightarrow{\sim} \lim\limits_{\leftarrow} C_n$.

2. A more general sufficient (but not necessary) condition for right exactness of the inverse limit is the *Mittag–Leffler condition:* the images $\phi_{mn}(A_{m+1}) \subset A_n$ for all $m \geq n$ satisfy the descending chain condition. In these notes we'll only need the easier special cases $a)$ and $b)$ above.

We shall prove **Step 2** in a stronger form. Assume given an ideal $I \subset A$ and a filtration (M^n) of an A-module M satisfying $I^m M^n \subset M^{m+n}$ for all m, n. We say that (M^n) is *stably I-adic* if $M^{n+1} = IM^n$ for all n large enough. Obviously the I-adic filtration $(I^n M)$ of M is stably I-adic.

Lemma 5.12. *If (M^n) is a stably I-adic filtration on M, there is an isomorphism*

$$\lim_{\leftarrow} M/M^n \cong \lim_{\leftarrow} M/I^n M.$$

Proof. We check the condition of Proposition 5.3. On the one hand, for all n we have $I^n M = I^n M^0 \subset M^n$ by assumption. On the other hand, if $M^{n+1} = IM^n$ for $n \geq n_0$, then $M^{n_0+m} = I^m M^{n_0} \subset I^m M$ for all $m > 0$. □

Now consider the graded ring[1]

$$I^{\oplus} := \bigoplus_{n=0}^{\infty} I^n$$

and the direct sum of A-modules

$$M^{\oplus} := \bigoplus_{n=0}^{\infty} M^n.$$

Here $M^{\oplus}$ is a graded $I^{\oplus}$-module, which means that there is an $I^{\oplus}$-module structure $I^{\oplus} \times M^{\oplus} \to M^{\oplus}$ on $M^{\oplus}$ which in all degrees m, n restricts to $I^m \times M^n \to M^{m+n}$ (this uses our condition on (M^n) above).

Lemma 5.13 (Cartier). *Assume A is Noetherian and M is finitely generated over A. The filtration (M^n) is stably I-adic if and only if $M^{\oplus}$ is a finitely generated $I^{\oplus}$-module.*

[1] Recall that a graded ring is a ring R together with a family of additive subgroups R_d for each $d \geq 0$ such that $R_d R_e \subset R_{d+e}$ and $R = \bigoplus_d R_d$.

Proof. Suppose first $M^{n+1} = IM^n$ for all $n \geq n_0$. For $n \leq n_0$ each M_n is finitely generated over A; choose a finite system S of generators for their direct sum. Since for all $m > 0$ we have $M^{n_0+m} = I^m M^{n_0}$, we conclude that S generates $M^\oplus$ over $I^\oplus$. Conversely, if $M^\oplus$ is finitely generated over $I^\oplus$, we may assume all generators lie in some homogeneous component M^n and let n_0 be the largest n involved. Now for $m > 0$ each element of M^{n_0+m} is a sum of elements of the form $i_{n_0+m-n}x_n$ with $x_n \in M^n$ a generator and $i_{n_0+m-n} \in I^{n_0+m-n}$. Since $I^{n_0+m-n} = I^m I^{n_0-n}$ and $I^{n_0-n}M^n \subset M^{n_0}$, we obtain $M^{n_0+m} = I^m M^{n_0}$. □

Corollary 5.14 (Artin–Rees lemma)**.** *Assume moreover $M_1 \subset M$ is a submodule. The filtration $(I^n M \cap M_1)$ of M_1 is stably I-adic.*

Proof. First note that the filtration $(I^n M \cap M_1)$ satisfies $I^m(I^n M \cap M_1) \subset (I^{n+m}M \cap M_1)$ for all n, m. Next, observe that a finite system of generators of I generates $I^\oplus$ as an *A-algebra*, so $I^\oplus$ is Noetherian by the Hilbert basis theorem. By the lemma $I^\oplus M = \oplus I^n M$ is a finitely generated $I^\oplus$-module, so its submodule $\oplus(I^n M \cap M_1)$ is also finitely generated. Now apply the other implication of the lemma. □

Proof of Proposition 5.5. As noted above, Lemma 5.10 $a)$ implies exactness of the sequence

$$0 \to \lim_{\leftarrow} M_1/(I^n M_2 \cap M_1) \to \lim_{\leftarrow} M_2/I^n M_2 \to \lim_{\leftarrow} M_3/I^n M_3 \to 0.$$

Now $\lim\limits_{\leftarrow} M_1/(I^n M_2 \cap M_1) \cong \lim\limits_{\leftarrow} M_1/I^n M_1$ follows from the Artin–Rees lemma (Corollary 5.14) applied with $M = M_2$ and Lemma 5.12. □

The Artin–Rees lemma has another important consequence:

Corollary 5.15. (Krull intersection theorem) *If A is a Noetherian local ring and $I \subsetneq A$ is an ideal, then*

$$\bigcap_{n=1}^{\infty} I^n = (0).$$

Proof. We may assume $I = P$, the maximal ideal of A, since $I \subset P$. Write N for the intersection of the P^n. As N is an ideal, we have $PN \subset N$. On the other hand, applying the Artin–Rees lemma to $N \subset A$ gives an n_0 for which

$$N = P^{n_0+1} \cap N = P(P^{n_0} \cap N) \subset PN.$$

Thus $PN = N$, so $N = (0)$ by Nakayama's lemma. □

Corollary 5.16. *If A is a Noetherian local ring and $\widehat{A}$ its completion with respect to some ideal $I \subsetneq A$, the natural map $A \to \widehat{A}$ is injective.*

Proof. The kernel is $\bigcap_{n=1}^{\infty} I^n$. □

While we are at local rings, let us also record the following fact.

Proposition 5.17. *If A is a Noetherian local ring with maximal ideal P, its completion $\widehat{A}$ with respect to an ideal $I \subset A$ is a local ring with maximal ideal $\widehat{P} = P\widehat{A}$.*

The proof uses a general lemma whose technique will serve many times.

Lemma 5.18. *Let A be a ring complete with respect to an ideal I. An element $a \in A$ is a unit in A if and only if a mod I is a unit in A/I.*

Proof. Assume a mod I is a unit in A/I, the other implication being trivial. We first treat the case $I^2 = 0$ (note that under this assumption A is indeed I-adically complete). There is $b \in A$ and $h \in I$ with $ab = 1 + h$. Then $ab(1 - h) = 1 - h^2 = 1$, so $b(1 - h)$ is an inverse for a.

Since $I^n/I^{n+1} \subset A/I^{n+1}$ is an ideal of square zero, we get using induction on n that the lemma holds if $I^{n+1} = 0$. In the general case we know from the above that a mod I^n has a multiplicative inverse $b_n \in A/I^n$ for each $n > 0$. Since the multiplicative inverse of a ring element is unique, we must have $b_n = b_{n+1}$ mod I^n/I^{n+1} for all n, so (b_n) defines an element of A which is an inverse of A. □

Proof of Proposition 5.17. Given $t \in \widehat{P}$, the element $1 + t$ is a unit in $\widehat{A}$. Indeed, t mod I lifts to an element $t_0 \in P$ and $1 + t_0$ is a unit in A. Now apply the lemma above.

By Corollary 5.6 the quotient $\widehat{A}/\widehat{P} \cong A/P$ is a field, so $\widehat{P}$ is a maximal ideal. Now given $t \in \widehat{P}$ and a maximal ideal $P' \subset \widehat{A}$, we have $t \in P'$. Indeed, otherwise $(t, P') = \widehat{A}$ so there exist $a \in \widehat{A}$ and $b \in P'$ with $at + b = 1$, but this contradicts the fact proven above that $1 - at$ is a unit. So $\widehat{P} \subset P'$, whence $\widehat{P} = P'$. □

Remark 5.19. The above argument also shows that if A is any ring and $\widehat{A}$ its completion with respect to an ideal $I \subset A$, then $\widehat{I}$ is contained in all maximal ideals of $\widehat{A}$, i.e. in its *Jacobson radical*.

To proceed further we need the notion of a *flat* A-module: An A-module N is flat if for every exact sequence

$$0 \to M_1 \to M_2 \to M_3 \to 0$$

of A-modules the tensored sequence

$$0 \to M_1 \otimes_A N \to M_2 \otimes_A N \to M_3 \otimes_A N \to 0$$

remains exact.

Remarks 5.20.

1. Since the sequence is always right exact by a basic property of the tensor product, flatness is equivalent to injectivity of $M_1 \otimes_A N \to M_2 \otimes_A N$ for all injective maps $M_1 \to M_2$. In fact, here we may restrict to *finitely generated* M_i. Indeed, assume $\alpha = \sum m_i \otimes a_i$ is an element of $M_1 \otimes_A N$ that maps to 0 in $M_2 \otimes_A N$. To prove that $\alpha = 0$ we may replace M_1 by the finitely generated submodule generated by the m_i. Also, by construction of the tensor product the image of α in $M_2 \otimes_A N$ is 0 if the corresponding element of the free A-module $A[M_2 \times N]$ is a sum of finitely many relations occurring in the definition of $M_2 \otimes_A N$, so we find a finitely generated submodule $M_1 \subset M^f \subset M_2$ such that α maps to 0 already in $M^f \otimes_A N$.

2. If N is flat over A and B is an A-algebra, then $N \otimes_A B$ is flat over B. Indeed, if $M_1 \to M_2$ is an injection of B-modules, it can also be viewed as an injection of A-modules via the map $A \to B$, and $M_i \otimes_B (N \otimes_A B) \cong M_i \otimes_A N$ for $i = 1, 2$.

Proposition 5.21. *If A is Noetherian and $\widehat{A}$ is the completion of A with respect to some ideal $I \subset A$, then $\widehat{A}$ is flat over A.*

Proof. First note that for all finitely generated A-modules M we have isomorphisms $\widehat{M} \cong \widehat{A} \otimes_A M$. When $M = A^n$ this is easily checked using the definition of completions. In the general case write M as a cokernel of a suitable morphism $A^m \to A^n$ and use right exactness of completion (part of Proposition 5.5) and of the tensor product. In view of Remark 5.20 (1) the flatness of $\widehat{A}$ now follows from the full statement of Proposition 5.5. □

Proposition 5.22. *If A is a Noetherian local ring and $\widehat{A}$ its completion with respect to some ideal $I \subset A$, then* $\dim A = \dim \widehat{A}$.

Proof. Applying Proposition 3.1 to the inclusion map $A \to \widehat{A}$ and the maximal ideal $P\widehat{A} \subset \widehat{A}$ we obtain $\dim \widehat{A} \leq \dim A$. To prove the reverse inequality, choose a chain $P_1 \subsetneq P_2 \subsetneq \cdots \subsetneq P_d \subsetneq P$ of maximal length in A. Applying the lemma below with $B = \widehat{A}$ and the ideals $P_d \subsetneq P$ and $P\widehat{A}$ we obtain a prime ideal $Q_d \subsetneq P\widehat{A}$ with $Q_d \cap A = P_d$. Now the process may be repeated with $P_{d-1} \subsetneq P_d$ and so on, until we obtain a chain of prime ideals $Q_1 \subsetneq Q_2 \subsetneq \cdots \subsetneq Q_d \subsetneq P\widehat{A}$. Note that the lemma applies in view of Proposition 5.21 (and Corollary 5.16). □

Lemma 5.23 (Going down theorem for flat extensions). *Let $A \subset B$ be a ring extension making B a flat A-module. If $P_1 \subsetneq P_2$ are prime ideals in A such that there exists a prime ideal $Q_2 \subset B$ with $Q_2 \cap A = P_2$, then there exists a prime ideal $Q_1 \subsetneq Q_2$ with $Q_1 \cap A = P_1$.*

Proof. By Remark 5.20 (2) the ring extension $A/P_1 \subset B/P_1B \cong B \otimes_A (A/P_1)$ is still flat, so we may replace A by A/P_1 and assume $P_1 = (0)$ (in particular, A is an integral domain). Choose a minimal prime ideal $Q_1 \subset Q_2$ in B (it exists by Zorn's lemma as the intersection of a descending chain of prime ideals is a prime ideal). If $x \in A$ is a nonzero element, the map $A \to A$ given by $a \mapsto xa$ is injective on A, hence so is the similar map $B \to B$ by flatness of B over A. So x is not a zero-divisor in B and as such cannot be contained in the minimal prime ideal Q_1 by Remark 2.2. This shows $Q_1 \cap A = (0)$ as required; in particular, $Q_1 \subsetneq Q_2$. □

Remark 5.24. In the above proof we did not really use that A was a subring of B. So the statement holds more generally for any flat A-algebra B if we understand $Q_i \cap A$ as $\varphi^{-1}(Q_i)$, where $\varphi: A \to B$ is the natural homomorphism giving the A-algebra structure on B. Of course, at the end we have to work with $\varphi(x)$ as an element of B.

The above arguments may also be used to prove that in the inequality of Proposition 3.1 equality holds when the ring B is a flat A-algebra via the map $\varphi: A \to B$.

Finally, we obtain:

Corollary 5.25. *If A is a Noetherian local ring, A is regular if and only if its completion $\widehat{A}$ with respect to the maximal ideal P is regular.*

Proof. By Corollary 5.9 and Proposition 5.17 the completion $\widehat{A}$ is again Noetherian and local. Now apply Corollary 5.6 with $I = P$ and Proposition 5.22. □

It can be shown that the statement corollary holds more generally for completions with respect to arbitrary ideals $I \subset A$.

Example 5.26. Take $A = \mathbf{Z}$, $I = (p)$. The completion $\mathbf{Z}_p := \varprojlim \mathbf{Z}/p^n\mathbf{Z}$ is the *ring of p-adic integers*. Since $\mathbf{Z}_p$ is also the completion of the localization $\mathbf{Z}_{(p)}$ by its maximal ideal, it is a discrete valuation ring by the corollary above. In particular, it is an integral domain; its fraction field $\mathbf{Q}_p$ is the *field of p-adic numbers*. Every nonzero $a \in \mathbf{Q}_p$ can be written uniquely as $a = up^{v_p(a)}$ with $u \in \mathbf{Z}_p$ a unit and $v_p(a) \in \mathbf{Z}$. The function $a \mapsto v_p(a)$ gives the discrete valuation of $\mathbf{Q}_p$.

By Corollary 5.8 we have an isomorphism $\mathbf{Z}_p \cong \mathbf{Z}[[x]]/(x - p)$. This may actually be taken as a quick, albeit unorthodox, definition of p-adic integers.

6. The Cohen structure theorem: part I

From now on, when speaking about complete local rings we always understand completion with respect to the maximal ideal. The Cohen structure theorem describes the structure of complete regular local rings. The easiest case is:

Theorem 6.1. *Let A be a complete Noetherian local ring that contains a subfield k mapping isomorphically onto its residue field. Then A is a quotient of some power series ring $k[[x_1, \ldots, x_d]]$.*

If moreover A is regular of dimension d, then $A \cong k[[x_1, \ldots, x_d]]$.

Note that all the assumptions of the theorem are satisfied by the completion of the local ring of a smooth point on an algebraic variety over an algebraically closed field.

For the proof we need the *associated graded ring* of a ring complete with respect to the I-adic filtration. It is defined by

$$\mathrm{gr}_\bullet(A) := \bigoplus_{n=0}^{\infty} I^n/I^{n+1}.$$

Lemma 6.2. *Let $\phi : A \to B$ be a homomorphism of complete local rings such that $\phi(P_A^n) \subset P_B^n$ for all $n \geq 1$, where P_A (resp. P_B) is the maximal ideal of A (resp. B).*

If the induced homomorphism $\mathrm{gr}_\bullet(A) \to \mathrm{gr}_\bullet(B)$ is injective (resp. surjective), then so is ϕ.

Proof. Consider the commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & P_A^n/P_A^{n+1} & \longrightarrow & A/P_A^{n+1} & \longrightarrow & A/P_A^n & \longrightarrow & 0 \\ & & \Big\downarrow {\scriptstyle \mathrm{gr}_n(\phi)} & & \Big\downarrow {\scriptstyle \phi_{n+1}} & & \Big\downarrow {\scriptstyle \phi_n} & & \\ 0 & \longrightarrow & P_B^n/P_B^{n+1} & \longrightarrow & B/P_B^{n+1} & \longrightarrow & B/P_B^n & \longrightarrow & 0 \end{array}$$

The injectivity of $\mathrm{gr}_n(\phi)$ shows the injectivity of ϕ_n for all n by induction on n, whence also the injectivity of ϕ. For surjectivity, given $(b_n) \subset B = \widehat{B}$ with $b_n \in B/P_B^n$, we have to find a sequence of elements $a_n \in A/P_A^n$ with $\phi_n(a_n) = b_n$ and $a_{n+1} \bmod P_A^n = a_n$. We do this by induction on n: assuming a_n has been constructed, we lift it to $a_{n+1} \in A/P_A^{n+1}$ arbitrarily. This a_{n+1} may not map to b_{n+1} in A/P_A^{n+1} but $\phi_{n+1}(a_{n+1}) - b_{n+1}$ comes from P_B^n/P_B^{n+1}. By surjectivity of $\mathrm{gr}_n(\phi)$ we may therefore modify a_{n+1} by an element of P_A^n/P_A^{n+1} so that its image becomes b_{n+1}. □

Proof of Theorem 6.1. Let $t_1, \ldots, t_d$ be a system of generators for the maximal ideal P of A. There is a unique k-algebra homomorphism $\lambda : k[[x_1, \ldots, x_d]] \to A$ sending x_i to t_i. Indeed, for all n there is a unique homomorphism $\lambda : k[[x_1, \ldots, x_d]]/(x_1, \ldots, x_d)^n \to A/P^n$ sending the image of x_i to that of t_i; as A is complete, these assemble to a homomorphism λ as required. As $A/P \cong k$ and the t_i generate P, the induced map $\mathrm{gr}_\bullet(\lambda)$ is surjective, so λ is surjective by the lemma.

If moreover A is regular, we may choose $d = \dim A$. As moreover A is then an integral domain, the kernel of λ is a prime ideal, so since A and $k[[x_1, \ldots, x_d]]$ are both of dimension d, we must have $\ker(\lambda) = 0$. □

We can use the theorem to expand elements of regular local rings in power series. To do so, we use first the fact, resulting from Corollary 5.25, that A is regular if and only if $\widehat{A}$ is. By Corollary 5.16 the natural map embeds A in $\widehat{A}$, so the theorem implies:

Corollary 6.3. *Given a regular local ring A of dimension d containing a field k mapping onto its residue field there is an injective homomorphism $A \hookrightarrow k[[x_1, \ldots, x_n]]$. It is determined by the choice of a regular system of parameters $t_1, \ldots, t_d$ in A. In other words, each element of A has a 'power series expansion' in the t_i.*

Remark 6.4. For $d = 1$ there is an easy direct proof of the corollary. In this case A is a discrete valuation ring, i.e. the maximal ideal P is principal. Fix a generator t of P and pick $a \in A$. Set $a_0 := a \bmod P$ and $b_0 = a - a_0$. Then $b_0 = b_1 t$ with a unique $b_1 \in A$ and we set $a_1 := b_1 \bmod P$. Continuing the process we get $a = a_0 + a_1 t + \ldots a_n t^n + b_n$ with $b_n \in P^n$ for each n, whence the required map $A \mapsto k[[t]]$; it is injective by the Krull intersection theorem.

For general d the obvious generalization of the above procedure still yields *some* power series expansion of a with respect to a regular system of parameters $t_1, \ldots, t_d$ but its uniqueness is not a priori clear.

We now prove that the assumption in Theorem 6.1 is always satisfied if the characteristic of A equals that of its residue field. The argument used for the proof is inspired by a classical result called Hensel's lemma, so we begin by stating it in its simplest form.

Proposition 6.5 (Hensel's lemma)**.** *Let A be a complete local ring with maximal ideal P and residue field k. Let $f \in A[T]$ be a polynomial, and write $\bar{f}$ for the image of f in $k[T]$. Assume that $\bar{a} \in k$ satisfies $\bar{f}(\bar{a}) = 0$ but $\bar{f}'(\bar{a}) \neq 0$. Then there exists a unique $a \in A$ reducing to $\bar{a}$ modulo P with $f(a) = 0$.*

As A is complete with respect to P, it suffices to construct for each $n \geq 0$ elements $a_n \in A/P^n$ satisfying $a_1 = \bar{a}$, $f(a_n) = 0$ and a_n mapping to a_{n-1} in A/P^{n-1}. We shall do this by applying

Proposition 6.6. *Let B be a ring, $I \subset B$ an ideal satisfying $I^2 = 0$, and $f \in B[T]$ a polynomial. If $b \in B$ is such that $f(b) \in I$ but $f'(b)$ is a unit in B, there exists a unique $c \in B$ with $f(c) = 0$ and $c \equiv b$ mod I.*

By the above arguments, if we apply the proposition inductively with $B = A/P^n$, $I = P^{n-1}/P^n$ and b a lift of a_{n-1} to A/P^n, Proposition 6.5 follows. Indeed, since b maps to $\bar{a}$ modulo P by construction, $f'(b)$ maps to $f'(\bar{a})$ modulo P, and so $f'(b)$ is a unit but $f(b) \in P^{n-1}/P^n$.

We prove Proposition 6.6 in an even more general form:

Proposition 6.7. *Let B be a ring, $I \subset B$ an ideal satisfying $I^2 = 0$. Assume moreover given a commutative diagram*

$$\begin{array}{ccc} S & \xrightarrow{\bar\lambda} & B/I \\ \uparrow & & \uparrow \\ R & \xrightarrow{\mu} & B \end{array} \tag{1}$$

where $S = R[T]/(f)$ with some $f \in R[T]$, and write t for the image of T in S. If $\bar\lambda(f'(t))$ is a unit in B/I, then $\bar\lambda$ lifts to a unique map $\lambda : S \to B$ making the diagram commute.

To get the previous proposition, we apply this with $R = B$, $\mu = \mathrm{id}_B$ and $\bar\lambda$ the map $B[T]/(f) \to B/I$ induced by sending $t = T \bmod (f)$ to b, and then set $c := \lambda(t)$.

Proof. Lift $\bar\lambda(t)$ to $b \in B$ arbitrarily; since $f'(b)$ maps to $\bar\lambda(f'(t)) \bmod I$, it is a unit in B by Lemma 5.18 (here we evaluate f' at b via applying μ to its coefficients). To define λ, we have to find $h \in I$ such that $f(b+h) = 0$ (with the same convention of evaluating f via μ), for then $T \mapsto b + h$ determines λ uniquely. The Taylor formula with difference h is of the shape $f(b+h) = f(b) + f'(b)h$ because $I^2 = 0$ and $h \in I$. But $f'(b)$ is a unit in B, and therefore the equation $0 = f(b) + f'(b)h$ can be solved uniquely in h. □

Remarks 6.8.

(1) Hensel's lemma (Proposition 6.5) is often stated without the uniqueness of the lifting $a \in A$. However, it can be checked directly that existence implies uniqueness.

(2) If in the above proposition $f'(t)$ is a unit in S, then the lifting property holds without any further assumption on $\bar\lambda$. This is an instance of formal smoothness (in fact, formal étaleness) that we'll study in more detail later.

We shall use Proposition 6.7 through the following consequence.

Corollary 6.9. *Let $L|K$ be a separable algebraic field extension. Assume moreover given a commutative diagram*

$$\begin{array}{ccc} L & \xrightarrow{\bar\lambda} & B/I \\ \uparrow & & \uparrow \\ K & \longrightarrow & B \end{array}$$

where B is a ring, $I \subset B$ an ideal satisfying $I^2 = 0$. Then $\bar\lambda$ lifts to a map $\lambda : L \to B$ making the diagram commute.

The same holds if instead of $I^2 = 0$ we assume that B is complete with respect to I.

Proof. Assume first that $L|K$ is a finite extension. By the theorem of the primitive element we may then write $L \cong K[T]/(f)$ with f a polynomial having only simple roots, so we may apply the proposition with $R = K$ and $S = L$ to conclude (indeed, in this case already $f'(t) \in S$ is a unit). If $L|K$ is an infinite separable algebraic extension, we may write it as a union of finite separable extensions, and then conclude from the finite case using uniqueness of the lifting in Proposition 6.7.

The second statement of the proposition reduces to the first in the same way as Proposition 6.5 reduces to Proposition 6.6. □

We now return to the assumption in Theorem 6.1.

Definition 6.10. Let A be a local ring with maximal ideal P and residue field k. A field contained in A is a *coefficient field* of A if it is mapped isomorphically onto k by the natural projection $A \to k$.

We can now state:

Theorem 6.11 (Cohen). *If A is a complete local ring containing a field, then A has a coefficient field.*

Assume moreover that A is an integral domain. We say that A is *equi-characteristic* if $\mathrm{char}(A) = \mathrm{char}(k)$. This holds if and only if A contains a field. Sufficiency is obvious, and so is necessity in positive characteristic. For necessity in characteristic 0, observe that the subring $\mathbf{Z} \subset A$ generated by 1 must meet P trivially, and therefore all of its elements are units in A, i.e. A contains $\mathbf{Q}$. Thus combining the previous theorem with Theorem 6.1 we obtain:

Corollary 6.12. *Let A be an equi-characteristic complete Noetherian local domain with residue field k. Then A is a quotient of some power series ring $k[[x_1, \dots, x_d]]$.*

If moreover A is regular of dimension d, then $A \cong k[[x_1, \dots, x_d]]$.

In the proof of Theorem 6.11 we distinguish two cases, depending on the characteristic of the subfield contained in A.

Proof of Theorem 6.11 in characteristic 0. Let $k' \subset k$ be a maximal subfield such that the identity map of k' lifts to a map $k' \to A$. By a simple application of Zorn's lemma such a k' exists and contains the prime field $\mathbf{Q}$. Assume $k' \neq k$. If k contains an element $\bar{x}$ transcendental over k', then lifting $\bar{x}$ to $x \in A$ we see that the ring $k'[x]$ meets P trivially (otherwise we would have $k'[x] \cap P = (f)$ for a polynomial $f \in k'[T]$ and $\bar{x}$ would be algebraic over k'). Therefore $k'(x) \subset A$ and the map $k'(\bar{x}) \to A$ sending $\bar{x}$ to x lifts the identity of $k'(\bar{x})$, contradicting the maximality of k'. Hence $k|k'$ is an algebraic extension, and also separable as we are in characteristic

0. Now an application of Corollary 6.9 with $L = k$, $K = k'$ and $B = A$ again contradicts the maximality of k'.

Proof of Theorem 6.11 in characteristic $p > 0$. This case follows as above from the following proposition applied to $B = A$, $L = k$ and the map $k \to A/P$:

Proposition 6.13. *Let L be a field of characteristic $p > 0$, B an $\mathbf{F}_p$-algebra, and $I \subset B$ an ideal satisfying $I^2 = 0$. Then every homomorphism $\bar{\lambda} : L \to B/I$ lifts to a homomorphism $\lambda : L \to B$.*

The same holds if instead of $I^2 = 0$ we assume that B is complete with respect to I.

Proof. Define a map $\lambda_p : L^p \to B$ as follows. Given $a \in L$, lift $\bar{\lambda}(a)$ to $b \in B$, and set $\lambda_p(a^p) := b^p$. This does not depend on the choice of b because if b' is another lifting, then $b - b' \in I$, so that $b^p - (b')^p = (b - b')^p = 0$ because B is an $\mathbf{F}_p$-algebra, $p \geq 2$ and $I^2 = 0$. The map λ_p is well defined because the map $x \mapsto x^p$ is injective on L, and it is a homomorphism. Moreover, it is the unique lifting of $\bar{\lambda}|_{L^p}$ to a map $L^p \to B$, and identifies L^p with a subfield of B.[2] By Zorn's lemma there exists a maximal subfield $L' \subset L$ containing L^p such that $\bar{\lambda}|_{L'}$ lifts to a map $L' \to B$. We know that $L^p \subset L'$ and now show that $L' = L$. Assume not, and pick $\alpha \in L \setminus L'$. Then $\alpha^p \in L^p$, and $x^p - \alpha^p$ is the minimal polynomial of α over L'. Moreover, a lifting β of $\bar{\lambda}(\alpha)$ to B satisfies $\beta^p = \lambda_p(\alpha^p)$ by uniqueness of λ_p. Therefore sending α to β defines an extension of $\bar{\lambda}|_{L'}$ to $L'(\alpha) = L'[x]/(x^p - \alpha^p)$, contradicting the maximality of L'.

To get the second statement, we apply the first part inductively to B/I^{n+1} in place of B and I^n/I^{n+1} in place of I, assuming that a lifting to B/I^n has already been constructed. □

Finally, we discuss the Cohen structure theorem for complete local domains of mixed characteristic, i.e. of characteristic 0, and with residue field of characteristic $p > 0$. There are two basic facts that go beyond the equicharacteristic case.

Fact 6.14. *Given a field k of characteristic $p > 0$, there exists a complete discrete valuation ring A_0 of characteristic 0 with residue field k and maximal ideal generated by p.*

Such an A_0 is often called a *Cohen ring*. In the case where k is perfect, the ring A_0 is unique up to unique isomorphism and depends functorially on k: it is the ring of *Witt vectors* of k. In the non-perfect case, however, uniqueness does not hold.

Fact 6.15. *Let A be a complete local domain of characteristic 0, with maximal ideal P and residue field k of characteristic $p > 0$. There exists a Cohen ring A_0 contained in A with residue field k and such that $P \cap A_0 = (p)$.*

[2] For L perfect the proof stops here.

We shall prove these facts in the case when k is perfect in the next section and in Section 10 in general. Let us take them for granted for now and prove the mixed characteristic case of the Cohen structure theorem.

Theorem 6.16. *Let A be a Noetherian complete local domain of mixed characteristic, and let $A_0 \subset A$ be a Cohen ring as in Fact 6.15.*

(1) *There is a surjective homomorphism $A_0[[x_1, \dots, x_n]] \twoheadrightarrow A$ for some $n > 0$.*
(2) *If moreover A is regular of dimension $d + 1$ and $p \in P \setminus P^2$, there is such a map with $n = d$, inducing an isomorphism $A \cong A_0[[x_1, \dots, x_d]]$.*

Here, as usual, P denotes the maximal ideal of A.

Proof. For (1) choose elements $t_1, \dots, t_n \in P$ so that $P = (p, t_1, \dots, t_n)$. For every $i > 0$ we have an isomorphism

$$A_0[[x_1, \dots, x_n]]/(p, x_1, \dots, x_n)^i \cong A_0[x_1, \dots, x_n]/(p, x_1, \dots, x_n)^i,$$

whence a unique map of A_0-algebras $A_0[[x_1, \dots, x_n]]/(p, x_1, \dots, x_n)^i \to A/P^i$ which sends x_j to t_j for all j. By passing to the inverse limit over i we obtain a map $A_0[[x_1, \dots, x_n]] \to A$ whose surjectivity follows from Lemma 6.2 as in the proof of Theorem 6.1.

Under the assumptions of (2) we may moreover take $n = d$ and find t_i so that $p, t_1, \dots, t_d$ is a regular system of parameters for P. As in the proof of Theorem 6.1, the surjection $A_0[[x_1, \dots, x_d]] \to A$ must then be an isomorphism for dimension reasons. □

If A is regular but $p \in P^2$, then p cannot be part of a regular system of parameters asin the above proof, because then A/pA cannot be an integral domain, contradicting Proposition 4.4 and Theorem 4.6. In fact, in this case there is usually no isomorphism with a power series ring as in the theorem. The best we can get is:

Proposition 6.17. *Let A be a Noetherian complete local domain of mixed characteristic and dimension $d+1$, and let $A_0 \subset A$ be a Cohen ring. There exists an injective homomorphism $A_0[[x_1, \dots, x_d]] \hookrightarrow A$ such that A is finitely generated as a module over its image.*

We shall need an easy lemma.

Lemma 6.18. *Let R be a ring complete with respect to an ideal I satisfying $\cap_j I^j = 0$, and M an R-module. If M/IM is finitely generated over R/I, then M is finitely generated over R.*

Proof. Choose elements $m_1, \dots, m_r \in M$ whose images modulo IM generate M/IM over R/I. The equality

$$M = Rm_1 \oplus \cdots \oplus Rm_r + IM \tag{2}$$

then implies

$$I^j M = I^j m_1 \oplus \cdots \oplus I^j m_r + I^{j+1} M \tag{3}$$

for all j. So if $m \in M$, we may write

$$m = \sum_i r_{i0} m_i + n_1$$

with $r_{i0} \in R$ and $n_1 \in IM$ using (2), and then construct inductively elements $r_{ij} \in I^j$ and $n_j \in I^j M$ satisfying

$$n_j = \sum_i r_{ij} m_i + n_{j+1}$$

using (3). Here the sums $r_{i0} + r_{i1} + r_{i2} + \dots$ converge to $r_i \in R$, but then the element $m - \sum_i r_i m_i$ lies in $\cap_j I^j M$, so it equals 0 by assumption. □

Proof of Proposition 6.17. The quotient ring A/pA is Noetherian local of dimension d by Lemma 4.10, so by the converse of the Hauptidealsatz we find $t_1, \dots, t_d \in P$ such that P is minimal above $J = (p, t_1, \dots, t_d)$. Since then some power of P lies in J, it follows from Proposition 5.3 that A is also J-adically complete. As in the previous proof we then obtain a map $\rho : A_0[[x_1, \dots, x_d]] \to A$ induced by sending x_i to t_i and passing to the inverse limit over the quotients A/J^i. Hence A is a module over $R := A_0[[x_1, \dots, x_d]]$ via ρ, and if we put $I = (p, x_1, \dots, x_d) \subset R$, then $J = IA$. Since A/J is Noetherian of dimension 0, it is Artinian, hence finite dimensional over $R/I \cong A_0/pA_0 \cong A/P$. So applying the lemma above with $M = A$ we see that A is a finitely generated R-module. On the other hand, applying Proposition 3.1 to the map $\rho(R) \to A$ we see that $\dim(A/IA) = 0$ implies that $\rho(R)$ has Krull dimension $\geq d + 1$, which is only possible if ρ is injective. □

7. Witt vectors

In this section we prove the statement of Fact 6.14 in the case the field k is perfect. Under this assumption, the Cohen ring with residue field k is unique up to unique isomorphism.

We prove a more general statement involving not necessarily local or Noetherian rings.

Definition 7.1. Let p be a prime number. A *strict p-ring* is a ring A complete with respect to the ideal (p) such that p is not a zero-divisor in A.

Proposition 7.2. *Assume A is a strict p-ring such that the ideal (p) is maximal. Then A is a complete discrete valuation ring with maximal ideal (p).*

Proof. Since every $x \in A \setminus (p)$ is a unit modulo the maximal ideal (p), it is a unit by Lemma 5.18. This shows that A is local with maximal ideal (p). We have $\cap_j (p^j) = (0)$ by completeness, so for every nonzero $a \in A$ we find a unique $r \geq 0$ such that $a \in (p^r) \setminus (p^{r+1})$. Then $a = up^r$ where $u \notin (p)$, hence u is a unit. It follows that $(a) = (p^r)$ and, more generally, for any nonzero ideal $I \subset (p)$ we have $I = (p^r)$ with the largest r such that $I \subseteq (p^r)$. Moreover, if $a = up^r$ were a zero-divisor, so would be p which is not the case. We conclude that A is a local principal ideal domain, i.e. a discrete valuation ring. □

Remark 7.3. In the above proof we did not use the completeness of A, only the triviality of the intersection $\cap_j (p^j) =$, so the statement remains true under this more general assumption.

Now recall that an integral domain R of characteristic $p > 0$ is *perfect* if the map $x \mapsto x^p$ is an automorphism of R.

Theorem 7.4. *Given a perfect ring R of characteristic p, there exists a strict p-ring $W(R)$ with $W(R)/pW(R) \cong R$. Such a $W(R)$ is unique up to unique isomorphism and functorial in R, i.e. any homomorphism $R \to S$ induces a homomorphism $W(R) \to W(S)$.*

When R is a perfect field, then $W(R)$ is a discrete valuation ring.

In the case when R is a perfect field the ring $W(R)$ was constructed by Ernst Witt in 1937, whence the name 'Witt vectors'. Later several other constructions have been given. Recently a particularly simple one was found by Cuntz and Deninger[3]. We explain their arguments, following the original paper closely.

Construction 7.5. View R as a monoid under multiplication and let $\mathbf{Z}[R]$ be the associated monoid algebra. Its elements are formal sums of the form $\Sigma_{r \in R} n_r [r]$ with almost all $n_r = 0$. Addition and multiplication are the obvious ones. Note that $[1] = 1$ but $[0] \neq 0$. Multiplicative maps $R \to B$ into commutative rings mapping 1 to 1 correspond to ring homomorphisms $\mathbf{Z}[R] \to B$. The identity map $R = R$ induces the surjective ring homomorphism $\pi : \mathbf{Z}[R] \to R$ which sends $\Sigma n_r [r]$ to $\Sigma n_r r$. Let I be its kernel, so that we have an exact sequence

$$0 \longrightarrow I \longrightarrow \mathbf{Z}[R] \xrightarrow{\pi} R \longrightarrow 0 \ .$$

The multiplicative isomorphism $r \mapsto r^p$ of R induces a ring isomorphism $F : \mathbf{Z}[R] \to \mathbf{Z}[R]$ mapping $\Sigma n_r [r]$ to $\Sigma n_r [r^p]$. It satisfies $F(I) = I$.

Let $W(R) := \varprojlim \mathbf{Z}[R]/I^i$ be the I-adic completion of $\mathbf{Z}[R]$. By construction $W(R)$ is complete with respect to the filtration given by the ideals

$$\widehat{I^i} := \varprojlim I^i / I^{i+n} \subset W(R)$$

[3]J.Cuntz, C. Deninger, An alternative to Witt vectors, Münster J. Math. 7 (2014), no. 1, 105-114.

where the inverse limit is taken over n. (Note that we do not know a priori that $\widehat{I^i}$ is the i-th power of $\widehat{I}$; this will follow from the proof of Proposition 7.6 below.)

Plainly, the above construction of $W(R)$ is functorial in R.

Proposition 7.6. *If R is a perfect ring of characteristic p, then $W(R)$ is a strict p-ring with $W(R)/pW(R) = R$.*

The proof will require some lemmas. Consider first the map $\delta : \mathbf{Z}[R] \to \mathbf{Z}[R]$ defined by the formula

$$\delta(x) = \frac{1}{p}(F(x) - x^p) .$$

It is well defined since $F(x) \equiv x^p \mod p\mathbf{Z}[R]$ and because $\mathbf{Z}[R]$, being a free $\mathbf{Z}$-module, has no p-torsion, and therefore for every $x \in p\mathbf{Z}[R]$ we find a unique y with $py = x$.

Lemma 7.7. *For $x, y \in \mathbf{Z}[R]$ the following equalities hold.*

(4)
$$\delta(x+y) = \delta(x) + \delta(y) - \sum_{i=1}^{p-1} \frac{1}{p}\binom{p}{i} x^i y^{p-i}$$

(5)
$$\delta(xy) = \delta(x)F(y) + x^p\delta(y) .$$

Proof. Equality (4) follows from the additivity of F and the binomial formula; equality (5) is a straightforward calculation using the multiplicativity of F. □

Corollary 7.8. *We have $\delta(I^n) \subset I^{n-1}$ for all $n \geq 1$.*

Proof. Applying (5) inductively gives the relation

$$\delta(x_1 \cdots x_n) = \sum_{i=1}^{n} x_1^p \cdots x_{i-1}^p \delta(x_i) F(x_{i+1}) \cdots F(x_n) \quad \text{for } x_i \in \mathbf{Z}[R] .$$

Equation (4) shows that we have

$$\delta(x+y) \equiv \delta(x) + \delta(y) \mod I^n \quad \text{if } x \text{ or } y \text{ is in } I^n .$$

Since elements of I^n are sums of n-fold products of elements of I, the corollary follows from the above formulas. □

Lemma 7.9. *Let R be a perfect ring of characteristic p and $n \geq 1$ an integer.*
a) If $pa \in I^n$ for some $a \in \mathbf{Z}[R]$ then $a \in I^{n-1}$.
b) $I^n = I^i + p^n\mathbf{Z}[R]$ for any $i \geq n$.

Proof. a) According to the previous corollary we have $\delta(pa) \in I^{n-1}$. On the other hand, by definition:

$$\delta(pa) = F(a) - p^{p-1}a^p \ ,$$

and therefore since $pa \in I^n$

$$\delta(pa) \equiv F(a) \mod I^n \ .$$

It follows that $F(a) \in I^{n-1}$ and hence $a \in I^{n-1}$ since F is an automorphism with $F(I) = I$.

b) We prove the inclusion $I^n \subset I^i + p^n\mathbf{Z}[R]$ for $i \geq n$ by induction with respect to $n \geq 1$. The other inclusion is clear. For $y \in \mathbf{Z}[R]$ and $i \geq 1$ we have

$$F^i(y) \equiv y^{p^i} \mod p\mathbf{Z}[R] \ .$$

Applying this to $y = F^{-i}(x)$, we get for all $x \in \mathbf{Z}[R]$

$$x \equiv F^{-i}(x)^{p^i} \mod p\mathbf{Z}[R] \ .$$

For $x \in I$ this shows that $x \in I^i + p\mathbf{Z}[R]$ settling the case $n = 1$ of the assertion. Now assume that $I^n \subset I^i + p^n\mathbf{Z}[R]$ has been shown for a given $n \geq 1$ and all $i \geq n$. Fix some $i \geq n+1$ and consider an element $x \in I^{n+1}$. By the inductive assumption $x = y + p^n z$ with $y \in I^i$ and $z \in \mathbf{Z}[R]$. Hence $p^n z = x - y \in I^{n+1}$. Using assertion a) of the lemma repeatedly shows that $z \in I$. Hence $z \in I^i + p\mathbf{Z}[R]$ by the case $n = 1$. Writing $z = a + pb$ with $a \in I^i$ and $b \in \mathbf{Z}[R]$ we find

$$x = (y + p^n a) + p^{n+1}b \in I^i + p^{n+1}\mathbf{Z}[R] \ .$$

Thus we have shown the inductive step $I^{n+1} \subset I^i + p^{n+1}\mathbf{Z}[R]$. □

Proof of Proposition 7.6. We show that there is an equality of ideals $(p^n) = \widehat{I^n}$ for all $n \geq 1$ in $W(R)$ and that p is not a zero-divisor in $W(R)$; since by construction $W(R)$ is complete with respect to the filtration given by the ideals $\widehat{I^n}$, this will show that it is a strict p-ring. We'll then also have $W(R)/pW(R) = W(R)/\widehat{I} \cong R$. Let $p^{-n}(I^i)$ be the inverse image of I^i under p^n-multiplication on $\mathbf{Z}[R]$. Then for any $i \geq n \geq 1$ we have an exact sequence

$$0 \longrightarrow p^{-n}(I^i)/I^i \longrightarrow \mathbf{Z}[R]/I^i \xrightarrow{p^n} I^n/I^i \longrightarrow 0$$

where the surjectivity on the right is due to part b) of Lemma 7.9. From this we get an exact sequence of inverse systems whose transition maps for $i \geq n$ are the reduction maps. In the limit we have an exact sequence

$$0 \longrightarrow \lim_{\leftarrow} p^{-n}(I^i)/I^i \longrightarrow W(R) \xrightarrow{p^n} \widehat{I^n} \ .$$

The transition map $p^{-n}(I^{i+n})/I^{i+n} \to p^{-n}(I^i)/I^i$ is the zero map since $a \in p^{-n}(I^{i+n})$ implies $p^n a \in I^{i+n}$ and hence $a \in I^i$ by part a) of Lemma 7.9. So condition *b*) of

Lemma 5.10 is satisfied, and therefore the map $p^n : W(R) \to \widehat{I^n}$ is surjective. By Remark 5.11 (1) it also follows that $\lim\limits_{\leftarrow} p^{-n}(I^i)/I^i = 0$, so that $p^n : W(R) \to W(R)$ is injective with image $\widehat{I^n}$, as claimed. $\square$

Remark 7.10. There is an isomorphism

$$R \xrightarrow{\sim} I^n/I^{n+1} \quad \text{given by } r \longmapsto p^n[r] \ .$$

This holds because

$$I^n/I^{n+1} = \widehat{I^n}/\widehat{I^{n+1}} = p^nW(R)/p^{n+1}W(R) \overset{p^{-n}}{=} W(R)/pW(R) = R \ .$$

It remains to show the uniqueness property of $W(R)$. We do this via a method that at the same time will yield Fact 6.15 for complete local rings of mixed characteristic with perfect residue field. We first prove:

Lemma 7.11. *Let A be a ring complete with respect to an ideal $P \subset A$ such that A/P is a perfect ring of characteristic $p > 0$. The natural map $\pi : A \to A/P$ has a unique multiplicative retraction, i.e. a map $\rho : A/P \to A$ satisfying $\pi \circ \rho = \mathrm{id}$ and $\rho(\bar{a}\bar{b}) = \rho(\bar{a})\rho(\bar{b})$ for $\bar{a}, \bar{b} \in A/P$. Moreover, $\rho(\bar{a})$ is the unique element of A with the properties*

$$\bar{a} = \rho(\bar{a}) \bmod P, \quad \rho(\bar{a}) \in \bigcap_{n=0}^{\infty} A^{p^n}. \tag{6}$$

The element $\rho(\bar{a}) \in A$ is often called the *Teichmüller representative* of $\bar{a} \in A/P$. Note that the assumption implies that $p \in P$ and therefore $p^i \in P^i$ for all $i \geq 1$.

Proof. Given $\bar{a} \in A/P$, we show that there is a unique $\rho(\bar{a}) \in A$ satisfying the properties (6). This will define the required multiplicative retraction, since for $\bar{b} \in A/P$ the product $\rho(\bar{a})\rho(\bar{b})$ lifts $\bar{a} \cdot \bar{b}$ and is contained in A^{p^n} for all $n > 0$. Note that since A/P is perfect, any multiplicative retraction ρ must satisfy the conditions in (6), so uniqueness will also follow.

First we show that for all $i \geq 0$ there is a unique element $a_i \in A/P^{i+1}$ mapping to $\bar{a}$ mod P that is in the image of A^{p^i} mod P^{i+1}. Indeed, since A/P is perfect, we find $x \in A$ with $\bar{a} = x^{p^i}$ mod P. For such an x we have $(x+y)^{p^i} = x^{p^i}$ mod P^{i+1} for $y \in P$ since $p^i \in P^i$, hence the class

$$a_i := x^{p^i} \bmod P^{i+1}$$

does not depend on x. Moreover, since obviously $x^{p^i} \in A^{p^{i-1}}$, by uniqueness we must have

$$x^{p^i} \bmod P^i = a_i \bmod P^i/P^{i+1} = a_{i-1}.$$

Therefore, since A is complete with respect to P, the sequence (a_i) defines an element of $\lim\limits_{\leftarrow} A/P^{i+1} = A$ mapping to $\bar{a}$ modulo P. Denote it by $\rho(\bar{a})$.

Now fix $n > 0$ and let $\bar{b}_n \in A/P$ be the unique element with $\bar{b}_n^{p^n} = \bar{a}$. Then $\rho(\bar{b}_n)^{p^n}$ mod P^{i+1} also comes from A^{p^i} for all i and maps to $\bar{a}$ mod P. By uniqueness of the a_i we must have $\rho(\bar{a}) = \rho(\bar{b}_n)^{p^n}$. It follows that $\rho(\bar{a}) \in A^{p^n}$ for all n, as required. □

Example 7.12. For $A = W(R)$ the composite map $R \to \mathbf{Z}[R] \to W(R)$ is multiplicative, so by uniqueness it must be the Teichmüller retraction.

Corollary 7.13. *If A is as in Lemma 7.11 and R is a perfect ring of characteristic p, every homomorphism $\bar{\varphi} : R \to A/P$ lifts to a unique homomorphism $\varphi : W(R) \to A$ such that the induced map $W(R)/pW(R) \to A/P$ coincides with $\bar{\varphi}$.*

Proof. The composite map $\rho \circ \bar{\varphi} : R \to A/P \to A$ preserves multiplication, hence extends uniquely to a ring homomorphism $\tilde{\varphi} : \mathbf{Z}[R] \to A$. By construction $\tilde{\varphi}(I) \subset P$, hence $\tilde{\varphi}(I^i) \subset P^i$. Thus there is a canonical induced map φ from the I-adic completion $W(R)$ of $\mathbf{Z}[R]$ to the P-adically complete A. For uniqueness of the lifting φ note that any lifting of $\bar{\varphi}$ must send $r \in R$ to $(\rho \circ \bar{\varphi})(r)$ by uniqueness of the Teichmüller retraction; in the remaining steps of the construction uniqueness holds. □

Proof of Theorem 7.4. Existence was proven in proposition 7.6 and uniqueness follows from the previous corollary. The last statement follows from Proposition 7.2. □

The following corollary justifies Fact 6.15.

Corollary 7.14. *Let A be a complete local integral domain of characteristic 0 with maximal ideal P and perfect residue field k of characteristic $p > 0$. The identity map of k induces an injective map $\varphi : W(k) \to A$ where $\varphi^{-1}(P) = pW(k)$.*

Proof. Apply the previous corollary with $R = k$. Since A is an integral domain of characteristic 0, the kernel of φ is a prime ideal that must be different from (p), and hence equals (0). □

Remark 7.15. Classically, elements of $W(R)$ are represented by infinite sequences ('vectors')

$$(r_0, r_1, r_2, \dots) \tag{7}$$

with $r_i \in R$. The vector (7) corresponds to the convergent sum

$$\sum_{i=0}^{\infty} r_i^{p^{-i}} p^i \in W(R).$$

Note, therefore, that the ring operations in $W(R)$ do *not* correspond to componentwise addition and multiplication on the sequences (7)!

There are two important operations on Witt vectors. The first is the *Frobenius*

$$F: (r_0, r_1, r_2, \dots) \mapsto (r_0^p, r_1^p, r_2^p, \dots).$$

It corresponds to the unique automorphism of $W(R)$ induced by F on $\mathbf{Z}[R]$; it exists because of $F(I) = I$.

The second is the *Verschiebung* ('shift') given by

$$V: (r_0, r_1, r_2, \dots) \mapsto (0, r_0, r_1, r_2, \dots).$$

On $W(R)$ it corresponds to the additive homomorphism defined by $V(x) = pF^{-1}(x)$. By definition $\operatorname{Im} V^i = p^i W(R)$ and $V \circ F = F \circ V = p$.

8. Derivations and differentials

In differential geometry, the tangent space at a point P on some variety is defined to consist of so-called *linear derivations*, i.e. linear maps that associate a scalar to each function germ at P and satisfy the Leibniz rule. Here is an algebraic version of this notion.

Definition 8.1. Let B be a ring and M a B-module. A *derivation* of B into M is a map $d: B \to M$ subject to the two conditions:

(1) (Additivity) $d(x + y) = dx + dy$;
(2) (Leibniz rule) $d(xy) = xdy + ydx$.

Here we have written dx for $d(x)$ to emphasise the analogy with the classical derivation rules. If moreover B is an A-algebra for some ring A (for example $A = \mathbf{Z}$), an A-linear derivation is called an *A-derivation*. The set of A-derivations of B to M is equipped with a natural B-module structure via the rules $(d_1 + d_2)x = d_1x + d_2x$ and $(bd)x = b(dx)$. This B-module is denoted by $\operatorname{Der}_A(B, M)$.

Note that applying the Leibniz rule to the equality $1 \cdot 1 = 1$ gives $d(1) = 0$ for all derivations; hence all A-derivations are trivial on the image of A in B.

In the example one encounters in (say) real differential geometry we have $A = M = \mathbf{R}$, and B is the ring of germs of differentiable functions at some point; $\mathbf{R}$ is a B-module via evaluation of functions. Now comes a purely algebraic example.

Example 8.2. Assume given an A-algebra B which decomposes *as an A-module* into a direct sum $B \cong A \oplus I$, where I is an ideal of B with $I^2 = 0$. Then the natural projection $d: B \to I$ is an A-derivation of B into I. Indeed, A-linearity is immediate; for the Leibniz rule we take elements $x_1, x_2 \in B$ and write $x_i = a_i + dx_i$ with $a_i \in k$ for $i = 1, 2$. Now we have

$$d(x_1x_2) = d[(a_1 + dx_1)(a_2 + dx_2)] = d(a_1a_2 + a_2dx_1 + a_1dx_2) = x_2dx_1 + x_1dx_2$$

where we used several times the facts that $I^2 = 0$ and $d(A) = 0$.

In fact, given any ring A and A-module I, we can define an A-algebra B as above by defining a product structure on the A-module $A \oplus I$ by the rule $(a_1, i_1)(a_2, i_2) = (a_1a_2, a_1i_2 + a_2i_1)$. So the above method yields plenty of examples of derivations.

Now notice that for fixed A and B the rule $M \to \mathrm{Der}_A(B, M)$ defines a functor on the category of B-modules; indeed, given a homomorphism $\phi : M_1 \to M_2$ of B-modules, we get a natural homomorphism $\mathrm{Der}_A(B, M_1) \to \mathrm{Der}_A(B, M_2)$ by composing derivations with ϕ.

Proposition 8.3. *There exists a B-module $\Omega^1_{B/A}$ together with an A-derivation $d : B \to \Omega^1_{B/A}$ such that for every B-module M and derivation $\delta \in \mathrm{Der}_A(B, M)$ we have a factorization $\delta = \phi \circ d$ with a B-homomorphism $\Omega^1_{B/A} \to M$.*

Proof. Define $\Omega^1_{B/A}$ to be the quotient of the free B-module generated by symbols dx for each $x \in B$ modulo the relations given by the additivity and Leibniz rules as in Definition 8.1 as well as the relations $d(\lambda(a)) = 0$ for all $a \in A$, where $\lambda : A \to B$ is the map defining the A-module structure on B. The map $x \to dx$ is an A-derivation of B into $\Omega^1_{B/A}$. Moreover, given any B-module M and A-derivation $\delta \in \mathrm{Der}_A(B, M)$, the map $dx \to \delta(x)$ induces a B-module homomorphism $\Omega^1_{B/A} \to M$ whose composition with d is just δ. □

We call $\Omega^1_{B/A}$ the module of *relative differentials* of B with respect to A. We shall often refer to the elements of $\Omega^1_{B/A}$ as *differential forms*.

Next we describe how to compute relative differentials of a finitely presented A-algebra.

Proposition 8.4. *Let B be the quotient of the polynomial ring $A[x_1, \dots, x_n]$ by an ideal generated by finitely many polynomials $f_1, \dots, f_m$. Then $\Omega^1_{B/A}$ is the quotient of the free B-module on generators $dx_1, \dots, dx_n$ modulo the B-submodule generated by the elements $\sum_j (\partial_j f_i) dx_j$ $(i = 1, \dots, m)$, where $\partial_j f_i$ denotes the j-th (formal) partial derivative of f_i.*

Proof. First consider the case $B = A[x_1, \dots, x_n]$. As B is the free A-algebra generated by the x_i, one sees that for any B-module M there is a bijection between $\mathrm{Der}_A(B, M)$ and maps of the set $\{x_1, \dots, x_n\}$ into B. This implies that $\Omega^1_{B/A}$ is the free A-module generated by the dx_i.

The general case follows from this in view of the easy observation that given any M, composition by the projection $A[x_1, \dots, x_n] \to B$ induces an isomorphism of $\mathrm{Der}_A(B, M)$ onto the submodule of $\mathrm{Der}_A(A[x_1, \dots, x_n], M)$ consisting of derivations mapping the f_i to 0. □

Next some basic properties of modules of differentials.

Lemma 8.5. *Let A be a ring and B an A-algebra.*

(1) *(Direct sums) For any A-algebra B'*

$$\Omega^1_{(B\oplus B')/A} \cong \Omega^1_{B/A} \oplus \Omega^1_{B'/A}.$$

(2) *(Base change) Given a ring homomorphism $A \to A'$, denote by B' the A'-algebra $B \otimes_A A'$. There is a natural isomorphism*

$$\Omega^1_{B/A} \otimes_B B' \cong \Omega^1_{B'/A'}.$$

(3) *(Localization) For any multiplicatively closed subset $S \subset B$ there is a natural isomorphism*

$$\Omega^1_{B_S/A} \cong \Omega^1_{B/A} \otimes_B B_S.$$

Proof. The first property follows from the definitions. For base change, note first that the universal derivation $d: B \to \Omega^1_{B/A}$ is an A-module homomorphism and so tensoring it by A' we get a map

$$d': B' \to \Omega^1_{B/A} \otimes_A A' \cong \Omega^1_{B/A} \otimes_B B \otimes_A A' \cong \Omega^1_{B/A} \otimes_B B'$$

which is easily seen to be an A'-derivation. Now any A'-derivation $\delta' : B' \to M'$ induces an A-derivation $\delta: B \to M'$ by composition with the natural map $B \to B'$. But δ factors as $\delta = \phi \circ d$, with a B-module homomorphism $\phi: \Omega^1_{B/A} \to M'$, whence a map $\phi' : \Omega^1_{B/A} \otimes_B B' \to M'$ constructed as above. Now one checks that $\delta' = \phi' \circ d'$ which means that $\Omega^1_{B/A} \otimes_B B'$ satisfies the universal property for $\mathrm{Der}_{A'}(B', M')$.

For the localization property, given an A-derivation $\delta: B \to M$, we may extend it uniquely to an A-derivation $\delta_S : B_S \to M \otimes_B B_S$ by setting $\delta_S(b/s) = (\delta(b)s - b\delta(s)) \otimes (1/s^2)$. (We leave it to the reader to check that for $b'/s' = b/s$ we get the same result.) This applies in particular to the universal derivation $d: B \to \Omega^1_{B/A}$, and one argues as in the previous case to show that any A-derivation $B_S \to M_S$ factors uniquely through d_S. □

There are two fundamental exact sequences that are instrumental in computing modules of differentials.

Proposition 8.6. *Let $\phi: B \to C$ be a homomorphism of A-algebras.*

(1) *There is an exact sequence of C-modules*

$$\Omega^1_{B/A} \otimes_B C \to \Omega^1_{C/A} \to \Omega^1_{C/B} \to 0. \tag{8}$$

(2) *If moreover ϕ is surjective with kernel I, we have an exact sequence of C-modules*

$$I/I^2 \to \Omega^1_{B/A} \otimes_B C \to \Omega^1_{C/A} \to 0.$$

Note that I/I^2 is indeed a module over $B/I \cong C$.

For the proof recall the following easy lemma.

Lemma 8.7. *Let M_1, M_2, M_3 be A-modules and*

$$M_1 \xrightarrow{i} M_2 \xrightarrow{p} M_3 \to 0 \tag{9}$$

a sequence of A-homomorphisms. This is an exact sequence if and only if for any A-module N the sequence induced by composition of R-homomorphisms

$$0 \to \mathrm{Hom}_A(M_3, N) \to \mathrm{Hom}_A(M_2, N) \to \mathrm{Hom}_A(M_1, N) \tag{10}$$

is an exact sequence of A-modules.

Proof. The proof that exactness of (9) implies that of (10) is easy and is left to the readers. The converse is not much harder: taking $N = M_3/M_2$ shows that injectivity of the second map in (10) implies the surjectivity on the right in (9), and taking $N = M_2/im(i)$ shows that if moreover (10) is exact in the middle, then the surjection $M_2/im(i) \to M_3$ has a section $M_3 \to M_2/im(i)$ and thus $im(i) = ker(p)$. □

Proof of Proposition 8.6. For the first statement note that for any C-module M we have a natural exact sequence

$$0 \to \mathrm{Der}_B(C, M) \to \mathrm{Der}_A(C, M) \to \mathrm{Der}_A(B, M)$$

of C-modules isomorphic to

$$0 \to \mathrm{Hom}_C(\Omega^1_{C/B}, M) \to \mathrm{Hom}_C(\Omega^1_{C/A}, M) \to \mathrm{Hom}_B(\Omega^1_{B/A}, M).$$

Now observe that there is an isomorphism $\mathrm{Hom}_B(\Omega^1_{B/A}, M) \cong \mathrm{Hom}_C(\Omega^1_{B/A} \otimes_B C, M)$ induced by mapping a homomorphism $\Omega^1_{B/A} \to M$ to the composite $\Omega^1_{B/A} \otimes_B C \to M \otimes_B C \to M$ where the second map is multiplication. An inverse is given by composition with the natural map $\Omega^1_{B/A} \to \Omega^1_{B/A} \otimes_B C$. Thus we may rewrite the previous exact sequence as

$$0 \to \mathrm{Hom}_C(\Omega^1_{C/B}, M) \to \mathrm{Hom}_C(\Omega^1_{C/A}, M) \to \mathrm{Hom}_C(\Omega^1_{B/A} \otimes_B C, M). \tag{11}$$

Set $M = \Omega^1_{C/B}$. The image of $\mathrm{id}_{\Omega^1_{C/B}} \in \mathrm{Hom}_C(\Omega^1_{C/B}, \Omega^1_{C/B})$ by the first map of the above exact sequence gives a map in $\mathrm{Hom}_C(\Omega^1_{C/A}, \Omega^1_{C/B})$ which is the second map in (8). Similarly, setting $M = \Omega^1_{C/A}$ and taking the image of $\mathrm{id}_{\Omega^1_{C/A}} \in \mathrm{Hom}_C(\Omega^1_{C/A}, \Omega^1_{C/A})$ in (11) defines the first map in (8). Finally, since the sequence (11) is exact for all C-modules M, the sequence in (8) is exact by the lemma above.

If the map $B \to C$ is surjective, then any B-derivation $C \to M$ is trivial, so $\Omega^1_{B/C} = 0$ and the first map in the first exact sequence is surjective, giving the surjectivity of the second map in the second sequence. Now define a map $\delta : I \to \Omega^1_{B/A} \otimes_B C$ by $\delta(x) := dx \otimes 1$. This is a B-module map because the Leibniz rule for d implies $\delta(bx) = bdx \otimes 1$ for $b \in B$, $x \in I$; indeed, we have $xdb \otimes 1 = db \otimes x$ which is 0 in $\Omega^1_{B/A} \otimes_B C$. If $x \in I^2$, the same argument shows that $\delta(x) = 0$, whence the C-module map $\bar{\delta} : I/I^2 \to \Omega^1_{B/A} \otimes_B C$ in the second exact sequence. To conclude, it will again suffice to verify the exactness of the dual sequence

$$0 \to \mathrm{Der}_A(C, M) \to \mathrm{Der}_A(B, M) \to \mathrm{Hom}_C(I/I^2, M)$$

for all C-modules M, where injectivity on the left is already proven. The second map is induced by composition with the inclusion map $I \to B$: indeed, if we restrict a derivation $\delta : B \to M$ to I, then the Leibniz rule for δ gives $\delta(I^2) = 0$ as well as $\delta(bx) = b\delta(x) + x\delta(b) = b\delta(x)$ for all $b \in B$, $x \in I$. This implies exactness in the middle. □

Here is a first application.

Proposition 8.8. *A finite extension $K|k$ of fields is separable if and only if $\Omega^1_{K/k} = 0$.*

Proof. If $K|k$ is separable, then $K \cong k[x]/(f)$ with a polynomial f satisfying $f' \neq 0$, so Proposition 8.4 gives $\Omega^1_{K/k} = 0$. For the converse we may assume k has characteristic $p > 0$. Recall from field theory[4] that there exists an intermediate field $k \subset K_0 \subset K$ such that $K_0|k$ is separable and $K = K_0(\sqrt[p^{r_1}]{a_1}, \dots, \sqrt[p^{r_m}]{a_m})$ for some $a_i \in K_0$ and $r_i > 0$. Applying Proposition 8.6 (1) with $A = k$, $B = K_0$, $C = K$ gives $\Omega^1_{K/k} \cong \Omega^1_{K/K_0}$ by the first part of the proof, and then Proposition 8.4 gives $\Omega^1_{K/K_0} \cong K_0^m$, which can be 0 only for $K = K_0$. □

9. Differentials, regularity and smoothness

By means of differentials we obtain a new characterization of regular local rings coming from geometry.

Proposition 9.1. *Let k be a perfect field, and let A be an integral domain of dimension d which is a finitely generated k-algebra. Given a prime ideal P, the localization A_P is a regular local ring if and only if $\Omega^1_{A_P/k}$ is a free A_P-module of rank d.*

For the proof we need a lemma from field theory:[5]

Lemma 9.2. *Let k be a perfect field and let $K|k$ be a finitely generated field extension of transcendence degree n. Then there exist algebraically independent elements $x_1, \dots, x_n \in K$ such that the finite extension $K|k(x_1, \dots, x_n)$ is separable.*

Corollary 9.3. *In the situation of the lemma, the K-vector space $\Omega^1_{K/k}$ is of dimension n, a basis being given by the dx_i.*

[4]See e.g. Lang, Algebra, Chapter V, §6.

[5]For a proof, see e.g. Lang, Algebra, Chapter VIII, Corollary 4.4.

Proof. We may write the field K as the fraction field of the quotient A of the polynomial ring $k[x_1, \dots, x_n, x]$ by a single polynomial relation f. Here f is the minimal polynomial of a generator of the extension $K|k(x_1, \dots, x_n)$ multiplied with a common denominator of its coefficients. Now according to Proposition 8.4 the A-module $\Omega^1_{A/k}$ has a presentation with generators $dx_1, \dots, dx_n, dx$ and a relation in which dx has a nontrivial coefficient because $f' \neq 0$ by the lemma. The corollary now follows using Lemma 8.5 (3). □

Proof of Proposition 9.1. We denote the maximal ideal of A_P again by P and by κ its residue field. Applying the second exact sequence of Proposition 8.6 to the surjection $A_P \twoheadrightarrow \kappa$ we obtain an exact sequence of κ-vector spaces

$$P/P^2 \to \Omega^1_{A_P/k} \otimes_{A_P} \kappa \to \Omega^1_{\kappa/k} \to 0.$$

We contend that here the first map is injective. To prove this we may replace A_P by A_P/P^2. Indeed, applying Proposition 8.6 (2) to the surjection $A_P \twoheadrightarrow A_P/P^2$ we obtain an exact sequence

$$P^2/P^4 \to \Omega^1_{A_P/k} \otimes_{A_P} (A_P/P^2) \to \Omega^1_{(A_P/P^2)/k} \to 0$$

which gives an isomorphism $\Omega^1_{A_P/k} \otimes_{A_P} \kappa \to \Omega^1_{(A_P/P^2)/k} \otimes_{A_P/P^2} \kappa$ upon tensoring with κ. Thus we may assume $P^2 = 0$, in which case A_P is *complete*. Applying Theorem 6.11 we obtain a subfield in A_P isomorphic to κ and an isomorphism of κ-vector spaces $A_P \cong \kappa \oplus P$. Now recall that for every κ-vector space M the map

$$\mathrm{Hom}_\kappa(\Omega^1_{A_P/k} \otimes_{A_P} \kappa, M) \to \mathrm{Hom}_\kappa(P, M) \tag{12}$$

identifies with the map $\mathrm{Der}_k(A_P, M) \to \mathrm{Hom}_\kappa(P, M)$ obtained by composing with the inclusion $P \to A_P$. But this map has a retraction: composing a κ-homomorphism $P \to M$ by the quotient map $A_P \to A_P/\kappa \cong P$ of k-vector spaces gives a k-derivation $A_P \to M$ as in Example 8.2. So the map (12) is surjective for all M, whence the required injectivity.

Now return to the general case. By the injectivity proven above, reading off dimensions in the above exact sequence gives

$$\dim_\kappa(\Omega^1_{A_P/k} \otimes_{A_P} \kappa) = \dim_\kappa P/P^2 + \dim_\kappa \Omega^1_{\kappa/k}.$$

Here $\dim_\kappa \Omega^1_{\kappa/k} = \mathrm{tr.deg}_k(\kappa) = d - \dim A_P$ by Corollary 9.3 and Corollary 3.14 (1). Thus A_P is regular if and only if $\dim_\kappa(\Omega^1_{A_P/k} \otimes_{A_P} \kappa) = d$. If $\Omega^1_{A_P/k}$ is free of rank d, this certainly holds. Conversely, choose elements $dt_1, \dots, dt_d \in \Omega^1_{A_P/k}$ such that their images in $\Omega^1_{A_P/k} \otimes_{A_P} \kappa = \Omega^1_{A_P/k}/P\Omega^1_{A_P/k}$ form a basis over κ. By Nakayama's lemma they then generate $\Omega^1_{A_P/k}$ as an A_P-module, so by sending the standard generators of the free module A_P^d to the dt_i we obtain an exact sequence of the form

$$0 \to N \to A_P^d \to \Omega^1_{A_P/k} \to 0.$$

The fraction field K of A_P is a flat A_P-module, so the induced sequence

$$0 \to N \otimes_{A_P} K \to K^d \to \Omega^1_{A_P/k} \otimes_{A_P} K \to 0$$

is exact. But by Lemma 8.5 (3) and Corollary 9.3 the K-vector space $\Omega^1_{A_P/k} \otimes_{A_P} K \cong \Omega^1_{K/k}$ has dimension d, so the last exact sequence gives $N \otimes_{A_P} K = 0$. Since A_P is an integral domain and N is a submodule of A_P^d, this is only possible for $N = 0$, i.e. when $\Omega^1_{A_P/k}$ is free of rank d. □

The proposition can be made explicit as follows. Consider a presentation

$$A = k[x_1, \dots, x_n]/(f_1, \dots, f_r),$$

and introduce the $n \times r$ *Jacobian matrix* $J := [\partial_i f_j]$. Given a preimage Q of P in $k[x_1, \dots, x_n]$, we consider J as a matrix with entries in $k[x_1, \dots, x_n]_Q$. In this way it makes sense to view J mod Q as a matrix with entries in κ.

Corollary 9.4 (Jacobian criterion). *With notations and assumptions as above, the ring A_P is regular if and only if the matrix $J \bmod Q$ has rank $n - d$.*

Proof. For ease of notation set $R := k[x_1, \dots, x_n]$ and write I for the ideal $(f_1, \dots, f_r)R_Q$. We then have an exact sequence $0 \to I \to R_Q \to A_P \to 0$, whence by Proposition 8.6 (2) an exact sequence of A_P-modules

$$I/I^2 \to \Omega^1_{R_Q/k} \otimes_{R_Q} A_P \to \Omega^1_{A_P/k} \to 0.$$

Tensoring by κ gives an exact sequence of κ-vector spaces

$$I/I^2 \otimes_{A_P} \kappa \xrightarrow{\bar{\delta}} \Omega^1_{R_Q/k} \otimes_{R_Q} \kappa \to \Omega^1_{A_P/k} \otimes_{A_P} \kappa \to 0.$$

Here $\Omega^1_{R_Q/k} \otimes_{R_Q} \kappa \cong \Omega^1_{R/k} \otimes_R \kappa \cong \kappa^n$ by Lemma 8.5 (3) and Proposition 8.4, and from the previous proposition we know that $\Omega^1_{A_P/k} \otimes_{A_P} \kappa \cong \kappa^d$ if and only if A_P is regular. So A_P is regular if and only if $\mathrm{Im}(\bar{\delta})$ has dimension $n - d$. Now if we identify $\Omega^1_{R_Q/k} \otimes_{R_Q} \kappa$ with κ^n via the κ-basis given by $dx_1, \dots, dx_n$, we obtain that the map $\bar{\delta}$ is induced by the map $\lambda : I \to \kappa^n$ given by $f \mapsto (\partial_1 f, \dots, \partial_n f)$ mod Q. It remains to note that $\dim \mathrm{Im}(\lambda)$ equals the rank of the matrix J mod Q. □

We now relate the above to a property encountered during the discussion of the Cohen structure theorem.

Definition 9.5 (Grothendieck)**.** An R-algebra S of rings is *formally smooth* if it satisfies the following property: given a commutative diagram

$$\begin{array}{ccc} S & \xrightarrow{\bar{\lambda}} & B/I \\ \uparrow & & \uparrow \\ R & \xrightarrow{\mu} & B \end{array} \tag{13}$$

with a ring B and an ideal $I \subset B$ satisfying $I^2 = 0$, the map $\bar{\lambda}$ lifts to a map $\lambda : S \to B$ making the diagram commute. If moreover S is finitely presented as an R-algebra, we say that S is *smooth* over R.[6]

Examples 9.6.

(1) If S is a free R-algebra (e.g. a polynomial ring $R[x_1, \dots, x_n]$), then it is formally smooth over R.
(2) We have seen in Corollary 6.9 that if $L|K$ is a separable algebraic field extension, then L is formally smooth over K. Also, Proposition 6.13 says that every field of characteristic $p > 0$ is formally smooth over $\mathbf{F}_p$.

Here are some basic properties of formal smoothness.

Lemma 9.7. *Let S be a formally smooth R-algebra.*

(1) *(Base change) If R' is any R-algebra, then $S \otimes_R R'$ is formally smooth over R'.*
(2) *(Transitivity) If S' is a formally smooth S-algebra, then it is also formally smooth over R.*
(3) *(Tensor product) If S_1 and S_2 are formally smooth R-algebras, then so is $S_1 \otimes_R S_2$.*
(4) *(Localization) If $T \subset S$ is a multiplicatively closed subset, then the localization S_T is also formally smooth over R.*

Proof. For (1), note first that any R'-algebra B' is also an R-algebra. Given an R'-algebra map $\bar{\lambda}' : S \otimes_R R' \to B'/I'$ with $I'^2 = 0$, it induces an R-algebra map $S \to B'/I'$ by composition with the map $s \mapsto s \otimes 1$, whence a lifting $S \to B'$ by formal smoothness of S. Since B' is an R'-algebra, there is an induced map $S \otimes_R R' \to B'$ lifting $\bar{\lambda}'$. For statement (2), assume given $\bar{\lambda} : S' \to B/I$ with an R-algebra B and $I^2 = 0$. By formal smoothness of S over R the composite map $S \to S' \to B/I$ lifts to an R-algebra map $S \to B$, so that B is also an S-algebra. Then by formal smoothness of S' over S $\bar{\lambda}$ lifts to a map $S' \to B$ as required. Statement (3) follows from (1) and (2): by (1) the tensor product $S_1 \otimes_R S_2$ is formally smooth over S_2, hence over R by (2).

[6]This is the definition of the Stacks Project. Grothendieck in EGA uses a weaker assumption: the algebra should be *locally* of finite presentation.

For (4) assume given $\bar{\lambda}_T : S_T \to B/I$ with an R-algebra B and $I^2 = 0$. The composite map $S \to S_T \to B/I$ lifts to a map $\lambda : S \to B$ by formal smoothness of S over R. By Lemma 5.18 the elements of $\lambda(T)$ are units in B, so λ induces a map $S_T \to B$ lifting $\bar{\lambda}_T$, as required. □

Now we come to a key example, already studied above.

Proposition 9.8. *Let k be a field, $A = k[x_1, \ldots, x_n]/(f_1, \ldots, f_r)$, and $P \subset A$ a prime ideal with preimage $Q \subset k[x_1, \ldots, x_n]$. If the Jacobian matrix $J = [\partial_i f_j]$ has rank r modulo Q, then A_P is formally smooth over k.*

Proof. We proceed like in the proof of Proposition 6.7. As before, write $R := k[x_1, \ldots, x_n]$. Assume given $\bar{\lambda} : A_P \to B/I$ with a k-algebra B and $I^2 = 0$. It will be enough to lift the composite map $\bar{\mu} : R/(f_1, \ldots, f_r) \to A_P \to B/I$ to a map $R/(f_1, \ldots, f_r) \to A_P \to B/I$, for then the lifting will factor through A_P as in the proof of Lemma 9.7 (4). Choose preimages $b_i \in B$ of $\mu(x_i) \in B/I$ for all i. In order to construct the required lifting, it suffices to find $h_i \in I$ such that $f_j(b_1 + h_1, \ldots b_n + h_n) = 0$ for all j. Now the multivariable Taylor formula of degree 2 gives a matrix equation

$$\begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix} = \begin{bmatrix} f_1(b_1 + h_1, \ldots, b_n + h_n) \\ \vdots \\ f_r(b_1 + h_1, \ldots, b_n + h_n) \end{bmatrix} = \begin{bmatrix} f_1(b_1, \ldots, b_n) \\ \vdots \\ f_r(b_1, \ldots, b_n) \end{bmatrix} + J(b_1, \ldots, b_n) \begin{bmatrix} h_1 \\ \vdots \\ h_n \end{bmatrix}$$

in view of $I^2 = 0$. Note that by assumption some $r \times r$ minor of J maps to a unit in R_Q, hence in A_P, and therefore $J(b_1, \ldots, b_n)$ mod I is a unit. Hence it is a unit in B as well, i.e. the matrix $J(b_1, \ldots, b_n)$ has rank r and the matrix equation is solvable. □

Remark 9.9. The same argument shows that if A is a ring, $B = A[x_1, \ldots, x_n]/(f_1, \ldots, f_r)$ and the Jacobian matrix $J = [\partial_i f_j]$ has an $r \times r$ minor which is a unit in B, then B is formally smooth over A.

In the presence of formal smoothness we have a strengthening of Proposition 8.6.

Proposition 9.10. *Let $\phi : B \to C$ be a formally smooth homomorphism of A-algebras.*

(1) *There is a split exact sequence of C-modules*

$$0 \to \Omega^1_{B/A} \otimes_B C \to \Omega^1_{C/A} \to \Omega^1_{C/B} \to 0.$$

(2) *If moreover ϕ is surjective with kernel I, we have a split exact sequence of C-modules*

$$0 \to I/I^2 \to \Omega^1_{B/A} \otimes_B C \to \Omega^1_{C/A} \to 0.$$

Proof. For (1), note that from the proof of Proposition 8.6 we already have an exact sequence

$$0 \to \mathrm{Der}_B(C, M) \to \mathrm{Der}_A(C, M) \to \mathrm{Der}_A(B, M).$$

for all C-modules M. It will be enough to extend it to a split exact sequence

$$0 \to \mathrm{Der}_B(C, M) \to \mathrm{Der}_A(C, M) \to \mathrm{Der}_A(B, M) \to 0.$$

Fix a derivation $D \in \mathrm{Der}_A(B, M)$ and consider the commutative diagram

$$\begin{array}{ccc} C & \xrightarrow{\mathrm{id}} & C \\ \uparrow & & \uparrow \\ B & \xrightarrow{(\phi, D)} & C \oplus M \end{array}$$

where $C \oplus M$ is given a ring structure with $M^2 = 0$ as in Example 8.2. By formal smoothness there is a map $C \to C \oplus M$ making the diagram commute which, composed with the projection $C \oplus M \to M$, gives an element in $\mathrm{Der}_A(C, M)$ whose restriction to B is D by construction. This defines the required retraction $\mathrm{Der}_A(B, M) \to \mathrm{Der}_A(C, M)$. Statement (2) is proven by the same argument as in the first half of the proof of Proposition 9.1, using formal smoothness instead of the application of Theorem 6.11. □

We may now complete Proposition 9.1 as follows.

Theorem 9.11. *Let k be a perfect field, $A = k[x_1, \ldots, x_n]/(f_1, \ldots, f_r)$ an integral domain of dimension d, and $P \subset A$ a prime ideal with preimage $Q \subset k[x_1, \ldots, x_n]$. The following are equivalent.*

(1) *The Jacobian matrix $J = [\partial_i f_j]$ has rank $n - d$ modulo Q.*
(2) *The localization A_P is formally smooth over k.*
(3) *The A_P-module $\Omega^1_{A_P/k}$ is free of rank d.*
(4) *A_P is a regular local ring.*

Proof. The equivalence of (1), (3) and (4) is Proposition 9.1 together with Corollary 9.4, and the implication $(1) \Rightarrow (2)$ will follow from Proposition 9.8 once we show that we may assume $r = n - d$. Write $R := k[x_1, \ldots, x_n]$ as before. We may number the variables x_i and the polynomials f_j so that the $(n - d) \times (n - d)$ minor $\det[(\partial_i f_j)_{1 \le i,j \le n-d}]$ is nonzero mod Q. If we set $\kappa := R_Q/QR_Q$, this means that the map $\rho : QR_Q \to \kappa^n$ given by $\rho(f) := (\partial_1 f, \ldots \partial_n f)$ mod Q maps $f_1, \ldots, f_{n-d}$ to linearly independent elements in κ^n. But ρ factors through $QR_Q/(QR_Q)^2$, so we conclude that $f_1, \ldots, f_{n-d}$ give linearly independent elements in the κ-vector space $QR_Q/(QR_Q)^2$. Here R_Q is a regular local ring, so the f_i form a regular sequence in R_Q by Theorem 4.9. On the other hand, using Lemma 4.10 we then obtain that

$\mathrm{ht}((f_1,\dots,f_{n-d})R_Q) = \mathrm{ht}(f_1,\dots,f_{n-d}) = n-d$, which is also the height of $(f_1,\dots,f_r)$ by Remark 3.14 (1). This shows $(f_1,\dots,f_{n-d}) = (f_1,\dots,f_r)$ as required.

Finally, for $(2) \Rightarrow (3)$, set $I = (f_1,\dots,f_r)R_Q$ and apply Proposition 9.10 (2) to obtain a split exact sequence

$$0 \to I/I^2 \to \Omega^1_{R_Q/k} \otimes_{R_Q} A_P \to \Omega^1_{A_P/k} \to 0.$$

Here $\Omega^1_{R_P/k}$ is free of rank n by Proposition 8.4, so the finitely generated A_P-module $\Omega^1_{A_P/k}$ is a direct summand of a free module. It is thus projective over A_P, hence free. Its rank is calculated as in the proof of Proposition 9.1: for the fraction field K of A_P we have $\Omega^1_{K/k} \cong \Omega^1_{A_P/k} \otimes_{A_P} K$ by Lemma 8.5 (3) and this K-vector space has dimension d by Corollary 9.3. □

Remark 9.12. By Lemma 9.7 (4) formal smoothness of A_P over k implies that of K. It can be shown that this implies that K is separably generated over k, whence the proof of $(2) \Rightarrow (3)$ goes through without assuming k perfect. In fact, inspection of the proof of Corollary 9.4 then shows that the equivalence of conditions $(1)-(3)$ in the above theorem holds over arbitrary k.

On the other hand, it is not hard to show using the arguments seen so far that if A is a Noetherian local ring containing a field k and A is formally smooth over k, then A is regular. The converse does not hold in general.

10. The Cohen structure theorem: part II

As an application of the theory of formal smoothness we complete the proof of the Cohen structure theorem in mixed characteristic. Recall that a local domain is of *mixed characteristic* if it is of characteristic 0 and its residue field is of characteristic $p > 0$. By the discussion in Section 6 in order to prove the Cohen structure theorem for complete local domains of mixed characteristic it suffices to give proofs for Facts 6.14 and 6.15.

Recall first that a Cohen ring is a complete discrete valuation ring of characteristic 0 with maximal ideal generated by a prime number p. The following proposition was proven for k perfect in the section on Witt vectors; we now give a general construction.

Proposition 10.1. *Given a field k of characteristic $p > 0$, there exists a Cohen ring A_0 with residue field $A_0/pA_0 \cong k$.*

Proof. First let $\langle x_\lambda : \lambda \in \Lambda \rangle \subset k$ be a maximal algebraically independent system over $\mathbf{F}_p$. Let $\mathbf{Z}_p\langle x_\lambda \rangle$ be the free $\mathbf{Z}_p$-algebra generated by the x_λ, and let R_0 be its localization by the prime ideal $p\mathbf{Z}_p\langle x_\lambda \rangle$. By construction R_0 is local with maximal ideal (p) and moreover $\cap_i(p^i) = 0$ in R_0. Thus R_0 is a discrete valuation ring by Remark 7.3.

We now construct a discrete valuation ring $R \supset R_0$ with maximal ideal pS and residue field k. This will finish the proof, as we may then take A_0 to be the p-adic completion of R. By construction k is algebraic over the residue field k_0 of R. Let $\overline{K}$ be an algebraic closure of the fraction field of R_0, and consider the system $\mathcal{S}$ of pairs (S, ρ), where $R_0 \subset S \subset \overline{K}$ is a subring that is a discrete valuation ring with maximal ideal pS, and $\rho : S \to k$ is a homomorphism with kernel pS. These pairs are naturally partially ordered by inclusion, and satisfy the condition of Zorn's lemma. Indeed, if $(S_1, \rho_1) \leq (S_2, \rho_2) \leq (S_3, \rho_3) \leq \dots$ is an ascending chain, then the union $\widetilde{S}$ of the S_i inside $\overline{K}$ has a homomorphism $\widetilde{\rho} : \widetilde{S} \to k$ with kernel $p\widetilde{S}$ induced by the ρ_i. Moreover, here $\cap_j p^j \widetilde{S} = 0$ because the S_i are discrete valuation rings. Hence $\widetilde{S}$ satisfies the assumptions of Remark 7.3, which means that $\widetilde{S}$ is a discrete valuation ring and therefore $(\widetilde{S}, \widetilde{\rho}) \in \mathcal{S}$. So let (S, ρ) be a maximal element in $\mathcal{S}$ furnished by Zorn's lemma. We contend that its residue field k_S equals k. If not, there is some $\alpha \in k \setminus k_S$ algebraic over k_S. Let $f \in S[x]$ be a monic irreducible polynomial mapping modulo pS to the minimal polynomial of α over k_S. Since S is a unique factorization domain, f is also irreducible over the fraction field of S, so since $\overline{K}$ is algebraically closed, we find an injective homomorphism $S' := S[x]/(f) \to \overline{K}$ where moreover $pS' \subset S'$ is a maximal ideal with $S'/pS' \cong k_S(\alpha)$. Now if $P' \subset S'$ is any maximal ideal, then $P' \cap S$ is maximal in S by Lemma 1.13 applied to the integral extension $S'/P' \supset S/(P' \cap S)$, so $P' = pS'$ and S' is local with maximal ideal pS'. Moreover, S' is Noetherian since it is a finitely generated S-algebra, so by Proposition 1.7 S' is a discrete valuation ring, which contradicts the maximality of S. □

Now we justify Fact 6.15 in the general case.

Theorem 10.2. *Let A be a complete local domain of mixed characteristic with maximal ideal P. There exists a subring $A_0 \subset A$ which is a Cohen ring and moreover the inclusion map $A_0 \to A$ induces an isomorphism $A_0/pA_0 \xrightarrow{\sim} A/P$.*

The key ingredient in the proof is the following proposition.

Proposition 10.3. *Let $\phi : R \to S$ be a homomorphism of rings and $I \subset R$ a nilpotent ideal. If S is projective as an R-module and S/IS is formally smooth over R/I, then S is formally smooth over R.*

Proof. Recall the following criterion from homological algebra (that uses the projectivity of S over R): S is formally smooth over R if and only if the symmetric Hochschild cohomology group $HH_s^2(S, M)$ is 0 for every S-module M. By assumption $HH^2_s(S/IS, M/IM) = 0$, so given a symmetric Hochschild 2-cocycle $f : S \times S \to M$, there is a 1-cochain $g_0 : S/IS \to M/IM$ with f mod $I = \partial^1(g_0)$. We may lift g_0 to an R-linear map $S \to M/IM$ and finally to an R-linear map $g_1 : S \to M$ by projectivity of S over R. Then $f - \partial^1(g_1)$ is a 2-cocyle with values in IM. Repeating the argument for $f - \partial^1(g_1)$ with IM in place of M we obtain a 2-cocyle with values in I^2M, so after finitely many repeats we get $g_2, \ldots, g_n : S \to M$ such that $f - \partial^1(g_1 + \cdots g_n)$ has values in I^nM which is 0 for n large enough. This proves that the class of f in $HH^2_s(S, M)$ is 0. □

In order to ensure that the projectivity assumption in the proposition holds when we shall apply it, we shall need:

Lemma 10.4. *Let A be a ring, and $I \subset A$ a nilpotent ideal. If M is a flat A-module such that M/IM is a free A/I-module, then M is a free A-module.*

Before starting the proof, recall the following simple observation: if M is a flat module over a ring A and $I \subset A$ is an ideal, then the multiplication map $I \otimes_A M \to IM$ is an isomorphism. Indeed, it is certainly surjective, and for injectivity we tensor the injection $I \to A$ by M. The resulting map $I \otimes_A M \to M$ is injective by flatness, and its image identifies with IM.

Proof. Choose a free A-module F so that F/IF (which is a free A/I-module) is isomorphic to M/IM. By projectivity of F we may lift the composite map $F \to F/IF \xrightarrow{\sim} M/IM$ to a map $\phi : F \to M$; we contend that it is an isomorphism. First note that the induced maps $\phi_n : I^nF/I^{n+1}F \to I^nM/I^{n+1}M$ are injective for all n. Indeed, since F and M are flat over A, so are F/IF and M/IM over A/I, so the ϕ_n may be identified with the maps $(I^n/I^{n+1}) \otimes_{A/I} F/IF \to (I^n/I^{n+1}) \otimes_{A/I} M/IM$ by the observation above. These are isomorphisms by assumption. Now consider the commutative diagram with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & I^nF/I^{n+1}F & \longrightarrow & F/I^{n+1}F & \longrightarrow & F/I^{n+1}F & \longrightarrow & 0 \\ & & \big\downarrow{\scriptstyle \phi_n} & & \big\downarrow & & \big\downarrow & & \\ 0 & \longrightarrow & I^nM/I^{n+1}M & \longrightarrow & M/I^{n+1}M & \longrightarrow & M/I^{n+1}M & \longrightarrow & 0 \end{array}$$

Here the left vertical arrow is an isomorphism, so it follows by induction on n (starting from the obvious case $n = 0$) that the map $F/I^{n+1}F \to M/I^{n+1}M$ is an isomorphism. We conclude by taking n large enough. □

Proof of Theorem 10.2. First note that since $p \in P$, the natural map $\mathbf{Z} \to A$ sending 1 to 1 induces homomorphisms $\mathbf{Z}/p^n\mathbf{Z} \to A/p^nA$ for all $n > 0$, whence a map $\mathbf{Z}_p \to A$ after passing to the inverse limit. We may thus consider A as a $\mathbf{Z}_p$-algebra. Now take a Cohen ring A_0 with residue field k; it is also a $\mathbf{Z}_p$-algebra by the same argument.

It will suffice to show that the identity map of k lifts to a homomorphism $A_0 \to A$; indeed, as A is a domain of characteristic 0 and the only nonzero prime ideal of A_0 is (p), the map $A_0 \to A$ must be injective.

As A_0 is an integral domain, it is torsion free over $\mathbf{Z}_p$ and hence a flat $\mathbf{Z}_p$-algebra as $\mathbf{Z}_p$ is a principal ideal domain. Since $A_0/p^n A_0$ is then flat over $\mathbf{Z}/p^n\mathbf{Z}$ as well, it follows from Proposition 10.4 that $A_0/p^n A_0$ is a free, hence projective module over $\mathbf{Z}/p^n\mathbf{Z}$ for all n. Given that k is formally smooth over $\mathbf{F}_p$ by Example 9.6 (2), Proposition 10.3 implies that $A_0/p^n A_0$ is also formally smooth over $\mathbf{Z}/p^n\mathbf{Z}$. We now prove that the identity map of k lifts to maps $\phi_n : A_0/p^n A_0 \to A/P^n$ for all n with $\phi_n = \phi_{n+1}$ mod p^n, from which the theorem will follow by passing to the inverse limit. We proceed by induction on n, the case $n = 0$ being trivial. If ϕ_n has been constructed, consider the exact sequence $0 \to P^n/P^{n+1} \to A/P^{n+1} \to A/P^n \to 0$ of $\mathbf{Z}/p^{n+1}\mathbf{Z}$-algebras. Since P^n/P^{n+1} is an ideal of square 0, the map $\phi_n : A_0/p^n A_0 \to A/P^n$ lifts to $\phi_{n+1} : A_0/p^{n+1}A_0 \to A/P^{n+1}$ by formal smoothness. □

NOTES ON HOMOLOGICAL ALGEBRA

TAMÁS SZAMUELY

CONTENTS

1. BACKGROUND FROM CATEGORY THEORY

Definition 1.1. A *category* consists of *objects* as well as *morphisms* between pairs of objects; given two objects A, B of a category $\mathcal{C}$, the morphisms from A to B form a set, denoted by $\mathrm{Hom}(A, B)$. (Notice that in contrast to this we do not impose that the objects of the category form a set.) These are subject to the following constraints.

(1) For each object A the set $\mathrm{Hom}(A, A)$ contains a distinguished element id_A, the identity morphism of A.

(2) Given two morphims $\phi \in \mathrm{Hom}(B, C)$ and $\psi \in \mathrm{Hom}(A, B)$, there exists a canonical morphism $\phi \circ \psi \in \mathrm{Hom}(A, C)$, the composition of ϕ and ψ. The composition of morphisms should satisfy two natural axioms:
   - Given $\phi \in \mathrm{Hom}(A, B)$, one has $\phi \circ \mathrm{id}_A = \mathrm{id}_B \circ \phi = \phi$.
   - (Associativity rule) For $\lambda \in \mathrm{Hom}(A, B)$, $\psi \in \mathrm{Hom}(B, C)$, $\phi \in \mathrm{Hom}(C, D)$ one has $(\phi \circ \psi) \circ \lambda = \phi \circ (\psi \circ \lambda)$.

A morphism $\phi \in \mathrm{Hom}(A, B)$ is an *isomorphism* if there exists $\psi \in \mathrm{Hom}(B, A)$ with $\psi \circ \phi = \mathrm{id}_A$, $\phi \circ \psi = \mathrm{id}_B$; we denote the set of isomorphisms between A and B by $\mathrm{Isom}(A, B)$.

Examples 1.2. In these notes, the main examples we'll consider will be algebraic. Thus we shall consider, for example, the category of groups, abelian groups, rings, or modules over a fixed ring R. In all these examples the morphisms are the homomorphisms between appropriate objects.

Remark 1.3. If the objects themselves form a set, we say that the category is *small*. In this case one can associate an oriented graph to the category by taking objects as vertices and defining an oriented edge between two objects corresponding to each morphism.

In the examples above the categories are not small but if we restrict to some set of objects we obtain small subcategories (in the sense to be defined below).

For small categories it is easy to visualize the contents of the following definition.

Definition 1.4. The *opposite category* $\mathcal{C}^{op}$ of a category $\mathcal{C}$ is "the category with the same objects and arrows reversed"; i.e. for each pair of objects (A, B) of $\mathcal{C}$, there is a canonical bijection between the sets $\mathrm{Hom}(A, B)$ of $\mathcal{C}$ and $\mathrm{Hom}(B, A)$ of $\mathcal{C}^{op}$ preserving the identity morphisms and composition.

Next we consider subcategories.

Definition 1.5. A *subcategory* of a category $\mathcal{C}$ is just a category $\mathcal{D}$ consisting of some objects and some morphisms of $\mathcal{C}$; it is a *full* subcategory if given two objects in $\mathcal{D}$, $\mathrm{Hom}_{\mathcal{D}}(A, B) = \mathrm{Hom}_{\mathcal{C}}(A, B)$, i.e. *all* $\mathcal{C}$-morphisms between A and B are morphisms in $\mathcal{D}$.

Examples 1.6. The category of abelian groups is a full subcategory of the category of groups. Given a ring $R \neq \mathbf{Z}$, the category of R-modules is a subcategory of that of abelian groups, but not a full subcategory.

Now comes the second basic definition of category theory.

Definition 1.7. A *(covariant) functor* F between two categories $\mathcal{C}_1$ and $\mathcal{C}_2$ consists of a rule $A \mapsto F(A)$ on objects and a map on sets of morphisms $\mathrm{Hom}(A, B) \to \mathrm{Hom}(F(A), F(B))$ which sends identity morphisms to identity morphisms and preserves composition. A *contravariant functor* from $\mathcal{C}_1$ to $\mathcal{C}_2$ is a functor from $\mathcal{C}_1$ to $\mathcal{C}_2^{op}$.

Examples 1.8. Here are some examples of functors.

(1) The identity functor is the functor $\mathrm{id}_{\mathcal{C}}$ on any category $\mathcal{C}$ which leaves all objects and morphisms fixed.
(2) Other basic examples of functors are obtained by fixing an object A of a category $\mathcal{C}$ and considering the covariant functor $\mathrm{Hom}(A, \_\_)$ (resp. the contravariant functor $\mathrm{Hom}(\_\_, A)$) from $\mathcal{C}$ to the category Sets which sends an object B the set $\mathrm{Hom}(A, B)$ (resp. $\mathrm{Hom}(B, A)$) and a morphism $\phi : B \to C$ to the set-theoretic map $\mathrm{Hom}(A, B) \to \mathrm{Hom}(A, C)$ (resp. $\mathrm{Hom}(C, A) \to \mathrm{Hom}(B, A)$) induced by composing with ϕ.
(3) There are *forgetful functors* defined by forgetting structure. For instance, associating to an R-module the underlying abelian group and to an R-module homomorphism the underlying group homomorphism defines the forgetful functor from the category of R-modules to that of abelian groups.
(4) On the category Mod_R of R-modules important examples of functors are given by tensor product. Fix an R-module B. The rule

$$A \mapsto A \otimes_R B, \quad (\phi : A_1 \to A_2) \mapsto (\phi \otimes \mathrm{id}_B : A_1 \otimes B \to A_2 \otimes B)$$

defines a functor $\_\_ \otimes_R B : \mathrm{Mod}_R \to \mathrm{Mod}_R$. Similarly, tensoring by a module A on the left gives a functor $A \otimes_R \_\_ : \mathrm{Mod}_R \to \mathrm{Mod}_R$.

Definition 1.9. If F and G are two functors with same domain $\mathcal{C}_1$ and target $\mathcal{C}_2$, a *morphism of functors* Φ between F and G is a collection of morphisms $\Phi_A : F(A) \to G(A)$ in $\mathcal{C}_2$ for each object $A \in \mathcal{C}_1$ such that for every morphism $\phi : A \to B$ in $\mathcal{C}_1$ the diagram

$$\begin{array}{ccc} F(A) & \xrightarrow{\Phi_A} & G(A) \\ {\scriptstyle F(\phi)}\downarrow & & \downarrow{\scriptstyle G(\phi)} \\ F(B) & \xrightarrow{\Phi_B} & G(B) \end{array}$$

commutes. The morphism Φ is an isomorphism if each Φ_A is an isomorphism; in this case we shall write $F \cong G$.

Remark 1.10. Given two categories $\mathcal{C}_1$ and $\mathcal{C}_2$ one can define (modulo some set-theoretic difficulties) a new category called the *functor category* of the pair $(\mathcal{C}_1, \mathcal{C}_2)$ whose objects are functors from $\mathcal{C}_1$ to $\mathcal{C}_2$ and whose morphisms are morphisms of functors. Here the composition rule for some Φ and Ψ is induced by the composition of the morphisms Φ_A and Ψ_A for each object A in $\mathcal{C}_1$.

We now turn to categories with additional properties, abstracting some properties of categories of modules over some ring.

Definition 1.11. A category $\mathcal{A}$ is *additive* if the following hold:

- For any two objects A, B the set $\mathrm{Hom}(A, B)$ carries the structure of an abelian group.
- The compositions of morphisms $\mathrm{Hom}(A, B) \times \mathrm{Hom}(B, C) \to \mathrm{Hom}(A, C)$ are $\mathbf{Z}$-bilinear maps.
- There is an object $0 \in \mathcal{A}$ that is both initial and final (i.e. for every object $A \in \mathcal{A}$ there is a unique morphism $0 \to A$ and a unique morphism $A \to 0$).
- For any two objects A, B the product $A \times B$ exists (defined by the usual universal property).

In an additive category the *kernel* of a morphism $\phi : A \to B$ is an object $\ker(\phi)$ together with a morphism $\kappa : \ker(\phi) \to A$ such that every morphism $\psi : C \to A$ with $\phi \circ \psi = 0$ factors uniquely as a composite $C \to \ker(\phi) \xrightarrow{\kappa} A$. Similarly, the *cokernel* of ϕ is an object $\mathrm{coker}(\phi)$ together with a morphism $\gamma : B \to \mathrm{coker}(\phi)$ such that every morphism $\psi : B \to C$ with $\psi \circ \phi = 0$ factors uniquely as a composite $B \to \mathrm{coker}(\phi) \xrightarrow{\gamma} C$.

The kernel and the cokernel may not exist for ϕ. When they do, we define the *image* of ϕ as $\mathrm{im}(\phi) := \ker(B \to \mathrm{coker}(\phi))$ and its *coimage* as $\mathrm{coim}(\phi) := \mathrm{coker}(\ker(\phi) \to A)$. Note that by definition there is a canonical morphism $\mathrm{coim}(\phi) \to \mathrm{im}(\phi)$. With these notions exact sequences are defined in the usual way.

Definition 1.12. An additive category $\mathcal{A}$ is *abelian* if every morphism ϕ has a kernel and a cokernel and the canonical morphism $\mathrm{coim}(\phi) \to \mathrm{im}(\phi)$ is an isomorphism.

Basic examples of abelian categories are categories of modules over some (not necessarily commutative) ring. The *Freyd–Mitchell embedding theorem* states that every *small* abelian category can be embedded as a full subcategory in the category modules over a suitable ring R.

Somewhat less straightforward examples are given by sheaves of abelian groups on some topological space. Later we shall encounter additive categories which are not abelian.

2. CATEGORIES OF MODULES

A functor $F : \mathcal{A} \to \mathcal{B}$ between additive categories is *additive* if for any two objects $A, B \in \mathcal{A}$ the induced map $\mathrm{Hom}(A, B) \to \mathrm{Hom}(F(A), F(B))$ is a group homomorphism. In what follows all functors between additive categories will be understood to be additive.

Definition 2.1. A functor $F : \mathcal{A} \to \mathcal{B}$ between abelian categories is *left exact* if for every short exact sequence

$$0 \to A_1 \to A_2 \to A_3 \to 0$$

in $\mathcal{A}$ the sequence

$$0 \to F(A_1) \to F(A_2) \to F(A_3)$$

is exact; it is *right exact* if

$$F(A_1) \to F(A_2) \to F(A_3) \to 0$$

is exact. We say that F is *exact* if it is both left and right exact.

There are also notions of left and right exactness for contravariant functors G: left exactness is defined by exactness of

$$0 \to G(A_3) \to G(A_2) \to G(A_1)$$

and right exactness by that of

$$G(A_3) \to G(A_2) \to G(A_1) \to 0.$$

Remark 2.2. In the Freyd–Mitchell embedding theorem cited in the previous section the functor realizing the embedding is exact.

Examples 2.3. Fix objects A and B in $\mathcal{A}$.

(1) The functor $\mathrm{Hom}(A, \_\_)$ from $\mathcal{A}$ to the category of abelian groups is left exact but not always right exact.
(2) The contravariant functor $\mathrm{Hom}(\_\_, B)$ is left exact but not always right exact.

Now we specialize to the category Mod_R of modules over a ring R. We shall assume our rings to be commutative with unit. However, everything will hold for noncommutative rings as well, one just has to choose a convention whether one considers left or right modules over a ring R.

We shall study modules satisfying exactness properties for the above two Hom-functors, and also for the tensor product functors $A \otimes_R \_\_ : \mathrm{Mod}_R \to \mathrm{Mod}_R$ and $\_\_ \otimes_R B : \mathrm{Mod}_R \to \mathrm{Mod}_R$ which do not exist in an arbitrary abelian category. They are right exact but not left exact in general. We start with the tensor product.

Definition 2.4. An R-module A is *flat* over R if the functor $A \otimes_R \_\_$ is exact.

Example 2.5. The R-module R is obviously flat. Since tensor products commute with direct sums, free R-modules are also flat. (Recall that a free R-module is by definition an R-module isomorphic to a direct sum of copies of the R-module R.)

In Proposition 5.4 below we'll see that conversely finitely generated flat modules over a Noetherian local ring are free.

We note for later use the following fact:

Proposition 2.6. *An R-module A is flat if and only if the restriction of the functor $A \otimes_R \_\_$ to the full subcategory of finitely generated R-modules is exact.*

Proof. We only have to treat left exactness. Assume $\phi : B_0 \to B$ is an injective map of R-modules, and $\alpha = \sum a_i \otimes b_i$ is an element of $A \otimes_R B_0$ that maps to 0 in $A \otimes B$. To prove that $\alpha = 0$ we may replace B_0 by the finitely generated submodule generated by the b_i. Also, by construction of the tensor product the image of α in $A \otimes_R B$ is 0 if the corresponding element of the free R-module $R[A \times B]$ is a sum of finitely many relations occurring in the definition of $A \otimes_R B$, so we find a finitely generated submodule $\phi(B_0) \subset B^f \subset B$ such that α maps to 0 already in $A \otimes_R B^f$. □

A stronger notion is that of faithful flatness:

Definition 2.7. An R-module A is *faithfully flat* over R if it is flat and for every R-module B one has $B \neq 0$ if and only if $A \otimes_R B \neq 0$.

It is easy to see that faithful flatness is equivalent to the following property: a sequence of R-modules $0 \to B_1 \to B_2 \to B_3 \to 0$ is exact *if and only if* the sequence $0 \to A \otimes_R B_1 \to A \otimes_R B_2 \to A \otimes_R B_3 \to 0$ is exact. Another important characterization is:

Lemma 2.8. *A flat R-module A is faithfully flat if and only if $A \otimes_R R/P \neq 0$ for every maximal ideal $P \subset R$.*

Proof. Necessity is obvious. For sufficiency assume $B \neq 0$ but $A \otimes_R B = 0$. For a nonzero $b \in B$ consider its annihilator $I = \mathrm{Ann}(b) := \{r \in R : rb = 0\}$. Since $b \neq 0$, we have $I \neq R$, so there is a maximal ideal $P \subset R$ with $P \supset I$. Tensoring by A the injective map $R/I \to B$ obtained by sending 1 to b we obtain an injective map $A \otimes_R R/I \hookrightarrow A \otimes_R B = 0$ by flatness of A, so $A \otimes_R R/I = 0$. But $A \otimes_R R/I$ surjects onto $A \otimes_R R/P$, so $A \otimes_R R/P = 0$ as well, contradiction. □

Now we can introduce an important class of (faithfully) flat R-modules:

Proposition 2.9. *If R is Noetherian and $\widehat{R}$ is the completion of R with respect to some ideal $I \subset R$, then $\widehat{R}$ is flat over R. If moreover R is local, then $\widehat{R}$ is faithfully flat over R.*

Proof. First note that for all finitely generated R-modules A we have isomorphisms $\widehat{A} \cong \widehat{R} \otimes_R A$. When $A = R^n$ this is easily checked using the definition of completions. In the general case write A as a cokernel of a suitable morphism $R^m \to R^n$ and use right exactness of completion and of the tensor product. In view of Proposition 2.6 flatness of $\widehat{R}$ now follows as it is known that the functor $A \mapsto \widehat{A}$ is exact on the category of finitely generated modules over Noetherian rings.

Now assume R is local with maximal ideal P. In view of the lemma above we have to check that the tensor product $\widehat{R} \otimes_R R/P \cong \widehat{R}/P\widehat{R}$ is nonzero. In fact, it is known that $\widehat{R}$ is local with maximal ideal $P\widehat{R}$. A 'cheaper' argument is as follows:

by definition of completions we have a natural surjection $\widehat{R} \to R/I$ which we may compose with the natural surjection $R/I \to R/P$ induced by the inclusion $I \subset P$. The composite $\widehat{R} \to R/P$ factors through $\widehat{R}/P\widehat{R}$ which must then be nonzero. □

Another type of important example is the following.

Example 2.10. If $S \subset R$ is a multiplicatively closed subset, the localization R_S is flat over R. In particular, when R is an integral domain, its fraction field is flat over R.

To see this, let $A' \hookrightarrow A$ be an injective morphism of R-modules. We have to show that $A' \otimes_R R_S \to A \otimes_R R_S$ is still injective. A general element of $A' \otimes_R R_S$ is a sum of elements of the form $a' \otimes (r/s')$ with $a' \in A'$, $r \in R$, $s' \in S$. Choosing a common denominator in S and using bilinearity of the tensor product we may rewrite this element in the form $a \otimes (1/s)$ with $a \in A'$, $s \in S$. An element of this form is 0 in $A' \otimes_R R_S$ if and only if $tsa = 0$ for some $t \in S$. But such an equation holds in A' if and only if it holds in A.

Note that R_S is not always faithfully flat over R. For instance, $\mathbf{Q}$ is not faithfully flat over $\mathbf{Z}$ because $A \otimes_{\mathbf{Z}} \mathbf{Q} = 0$ for every torsion abelian group A.

Now to the covariant Hom-functor. The following definition can be made in an arbitrary abelian category:

Definition 2.11. An R-module P is *projective* if the functor $\mathrm{Hom}(P, \_\_) : \mathrm{Mod}_R \to \mathrm{Mod}_R$ is exact.

By left exactness of $\mathrm{Hom}(P, \_\_)$ a module P is projective if and only if the natural map $\mathrm{Hom}(P, A) \to \mathrm{Hom}(P, B)$ given by $\lambda \to \alpha \circ \lambda$ is surjective for every *surjection* $\alpha : A \to B$.

Lemma 2.12.

(1) *The R-module R is projective.*
(2) *Arbitrary direct sums of projective modules are projective.*

Proof. For the first statement, given an R-homomorphism $\lambda : R \to B$ and a surjection $A \to B$, lift λ to an element of $\mathrm{Hom}(R, A)$ by lifting $\lambda(1)$ to an element of A. The second statement is immediate from the compatibility of Hom-groups with direct sums in the first variable. □

Corollary 2.13. *A free R-module is projective.*

Construction 2.14. Given an R-module A, define a free R-module $F(A)$ by taking direct sum of copies of R indexed by the elements of A. One has a surjection $\pi_A : F(A) \to A$ induced by mapping 1_a to a, where 1_a is the element of $F(A)$ with 1 in the component corresponding to $a \in A$ and 0 elsewhere.

When A is finitely generated by a system $a_1, \dots, a_n$ of generators, one may consider the finitely generated free module $F_{\mathrm{fg}}(A)$ defined as a finite direct sum of copies of R indexed by the elements a_i. Sending 1_{a_i} to a_i still defines a surjection $F_{\mathrm{fg}}(A) \to A$.

Thus every R-module is the quotient of a free R-module and hence of a projective module. This is expressed by saying that *the category of R-modules has enough projectives*. The full subcategory of finitely generated modules also has enough projectives by the second part of the construction.

Projective modules are in fact direct summands of free modules:

Lemma 2.15. *An R-module P is projective if and only if there exist an R-module A and a free R-module F with $P \oplus A \cong F$.*

By symmetry, A is then also projective.

Proof. For sufficiency, extend a map $\lambda : P \to B$ to F by defining it to be 0 on A and use projectivity of F. For necessity, take F to be the free R-module $F(P)$ associated with P in the above example. We claim that we have an isomorphism as required, with $A = \ker(\pi_P)$. Indeed, as P is projective, we may lift the identity map of P to a map $\pi : P \to F(P)$ with $\pi_P \circ \pi = \mathrm{id}_P$. □

Since free modules are flat, the lemma implies:

Corollary 2.16. *Projective modules are flat.*

Projective modules over local rings are in fact free:

Proposition 2.17. *Let R be a local ring with maximal ideal P and residue field k, and let A be a finitely generated R-module.*

If A is projective, then A is free over R.

Proof. Let $a_1, \dots a_n \in A$ be elements such that their mod PA images form a basis of the k-vector space A/PA. By Nakayama's lemma they generate A, so the map $\phi : R^n \to A$ sending $(r_1, \dots, r_n)$ to $r_1a_1 + \cdots + r_na_n$ is surjective and an isomorphism mod P. By projectivity of A we then have $R^n \cong A \oplus B$ where $B = \ker(\phi)$. Since $R^n/PR^n \xrightarrow{\sim} A/PA$, we get $B \subset PR^n$. But then $R^n = A + PR^n$, so $R^n \xrightarrow{\sim} A$, again by Nakayama's lemma. □

Remark 2.18. In fact, Kaplansky proved that the proposition holds without assuming A finitely generated, but the proof is much more involved.

The above proposition yields a characterization of finitely generated projective modules over arbitrary Noetherian rings.

Proposition 2.19. *Let R be a Noetherian ring. A finitely generated R-module A is projective if and only if $A \otimes_R R_P$ is free for all prime ideals $P \subseteq R$.*

In fact, one may restrict to maximal ideals in this statement.

For the proof we need some lemmas.

Lemma 2.20. *Let R be a ring.*

(1) *An R-module A is 0 if and only if $A \otimes_R R_P = 0$ for all maximal ideals P.*
(2) *A morphism $\varphi : A_1 \to A_2$ of R-modules is injective (resp. surjective) if and only if $\varphi \otimes \mathrm{id}_{R_P}$ is (resp. surjective) for all maximal ideals P.*

Proof. For the nontrivial implication of (1) assume $A \neq 0$, and pick a nonzero $a \in A$. The map $R \to A$ sending $r \in R$ to ra shows that the submodule $\langle a \rangle \subset A$ is isomorphic to R/I for some ideal $I \subsetneq R$. Pick a maximal ideal $I \subset P \subset R$. We then have $a \neq 0$ in $A \otimes_R R_P$.

Statement (2) follows by applying (1) to the kernel (resp. cokernel) of φ. □

Lemma 2.21. *Given a finitely presented R-module A, an R-module B and a prime ideal $P \subset R$, we have canonical isomorphisms*

$$\mathrm{Hom}_R(A, B) \otimes_R R_P \xrightarrow{\sim} \mathrm{Hom}_{R_P}(A \otimes_R R_P, B \otimes_R R_P).$$

Proof. We have a natural map $\mathrm{Hom}_R(A, B) \otimes_R R_P \to \mathrm{Hom}_{R_P}(A \otimes_R R_P, B \otimes_R R_P)$ induced by tensoring with R_P. If $A \cong R^n$ for some n, then this map is an isomorphism because the map $\mathrm{Hom}_R(R, B) \otimes_R R_P \xrightarrow{\sim} \mathrm{Hom}_{R_P}(R \otimes_R R_P, B \otimes_R R_P)$ identifies with the identity map of $B \otimes_R R_P$. For the general case write A as a cokernel of some map $R^m \to R^n$ (this is possible as A is finitely presented). We have a commutative diagram

$$\begin{array}{ccccccc} 0 \longrightarrow & \mathrm{Hom}_R(A, B) \otimes_R R_P & \longrightarrow & \mathrm{Hom}_R(R^n, B) \otimes_R R_P & \longrightarrow & \mathrm{Hom}_R(R^m, B) \otimes_R R_P \\ & \downarrow & & \downarrow & & \downarrow \\ 0 \longrightarrow & \mathrm{Hom}_{R_P}(A \otimes_R R_P, B \otimes_R R_P) & \longrightarrow & \mathrm{Hom}_{R_P}(R^n \otimes_R R_P, B \otimes_R R_P) & \longrightarrow & \mathrm{Hom}_{R_P}(R^m \otimes_R R_P, B \otimes_R R_P) \end{array}$$

whose rows are exact by left exactness of $\mathrm{Hom}(\_\_, B)$ and by flatness of R_P over R. The second and third vertical maps are isomorphisms by the previous case, hence so is the first. □

Proof of Proposition 2.19. The 'only if' part follows from Lemma 2.15 because if A is a direct summand of a free module over R, so is $A \otimes_R R_P$ over R_P. For the 'if' part take an exact sequence $0 \to K \to F \xrightarrow{f} A \to 0$ with F finitely generated and free. We show that this sequence splits. This is equivalent to showing that the map $\mathrm{Hom}_R(A, F) \to \mathrm{Hom}_R(A, A)$ induced by f is surjective. Indeed, if this is the case, then a splitting is given by a preimage of $\mathrm{id}_A \in \mathrm{Hom}_R(A, A)$; conversely, if id_A comes from $\mathrm{Hom}_R(A, F)$, then so does every element of $\mathrm{Hom}_R(A, A)$ by left composition.

By assumption for P maximal the induced map $\mathrm{Hom}_{R_P}(A \otimes_R R_P, F \otimes_R R_P) \to \mathrm{Hom}_{R_P}(A \otimes_R R_P, A \otimes_R R_P)$ is surjective. By the lemma above this is the same as the map $\mathrm{Hom}_R(A, F) \otimes_R R_P \to \mathrm{Hom}_R(A, A) \otimes_R R_P$ (note that A is finitely presented because R is Noetherian)), so we conclude from part (2) of Lemma 2.20. $\square$

We now consider the dual notion of injective modules.

Definition 2.22. An R-module Q is *injective* if the functor $\mathrm{Hom}(\_\_, Q) : \mathrm{Mod}_R \to \mathrm{Mod}_R$ is exact.

By right exactness of $\mathrm{Hom}(\_\_, Q)$ a module Q is injective if and only if given an injective map $\alpha : A \hookrightarrow B$, every homomorphism $\lambda_A : A \to Q$ extends to a homomorphism $\lambda_B : B \to Q$ with $\lambda_A = \lambda_B \circ \alpha$.

Remark 2.23. Arbitrary direct products of injective modules are injective. This follows from compatibility of the functor $\mathrm{Hom}(A, \_\_)$ with direct products.

Lemma 2.24 (Baer's criterion)**.** *An R-module Q is injective if and only if for every ideal $I \hookrightarrow R$ and every R-module homomorphism $\lambda_I : I \to Q$ there is an extension $\lambda_R : R \to Q$.*

Proof. Only the 'if' part requires proof. Assume given an inclusion $A \hookrightarrow B$ and a map $\lambda : A \to Q$. Consider pairs (A', λ') where $A \subset A' \subset B$ is an R-submodule and $\lambda' : A' \to Q$ extends λ. Inclusion maps $A' \hookrightarrow A''$ induce a natural partial ordering on the set of such pairs and the condition of Zorn's lemma is satisfied. Let $(\widetilde{A}, \widetilde{\lambda})$ be a maximal pair. If $\widetilde{A} = B$, we are done. Suppose $\widetilde{A} \neq B$, and pick $b \in B \setminus \widetilde{A}$. The set $I := \{r \in R : rb \in \widetilde{A}\}$ is an ideal in R equipped with a natural map $\lambda_I : I \to \widetilde{A}$ given by $r \mapsto rb$. By assumption the composite map $\widetilde{\lambda} \circ \lambda_I : I \to Q$ extends to a map $\lambda_R : R \to Q$. On the submodule $\widetilde{A} \cap \langle b \rangle \subset B$ the map $\widetilde{\lambda}$ coincides with the map $\lambda_b : \langle b \rangle \to Q, rb \mapsto \lambda_R(r)$. Hence $\widetilde{\lambda}$ and $rb \mapsto \lambda_R(r)$ patch together to a map from $\widetilde{A} + \langle b \rangle \subset B$ to Q, contradicting the maximality of $\widetilde{A}$. $\square$

Recall that an abelian group A is *divisible* if for all $n \in \mathbf{Z}$ the map $a \mapsto na$ is surjective on A. Basic examples of divisible abelian groups are $\mathbf{Q}$ and $\mathbf{Q}/\mathbf{Z}$.

Corollary 2.25. *An abelian group Q is injective if and only if it is divisible.*

Proof. For 'only if' fix $a \in Q$ and define a homomorphism $n\mathbf{Z} \to Q$ by sending n to a. By injectivity it extends to a homomorphism $\mathbf{Z} \to Q$. The image of 1 will be an element $b \in Q$ with $nb = a$. Conversely, since every ideal of $\mathbf{Z}$ is of the form $n\mathbf{Z}$, reversing the argument gives that the condition in Baer's criterion is satisfied. $\square$

This enables us to construct injective modules over an arbitrary ring R. Note first that given an abelian group T and a ring R, the set of abelian group homomorphisms $\mathrm{Hom}_{\mathbf{Z}}(R, T)$ carries a natural R-module structure by composing maps $R \to T$ by the multiplication-by r-map $R \to R$ for $r \in R$.

Lemma 2.26. *Fix an R-module A. The natural map of abelian groups*

$$\mathrm{Hom}_{\mathbf{Z}}(A, T) \to \mathrm{Hom}_R(A, \mathrm{Hom}_{\mathbf{Z}}(R, T))$$

given by $\phi \mapsto (a \mapsto (r \mapsto \phi(ra))$ for $r \in R$, $a \in A$ is an isomorphism. Moreover, this isomorphism is functorial *in A, i.e. for every R-module homomorphism $A \to B$ the diagram*

$$\begin{array}{ccc} \mathrm{Hom}_{\mathbf{Z}}(B, T) & \longrightarrow & \mathrm{Hom}_R(B, \mathrm{Hom}_{\mathbf{Z}}(R, T)) \\ \downarrow & & \downarrow \\ \mathrm{Hom}_{\mathbf{Z}}(A, T) & \longrightarrow & \mathrm{Hom}_R(A, \mathrm{Hom}_{\mathbf{Z}}(R, T)) \end{array}$$

commutes.

In other words, we have an *isomorphism of functors*

$$\mathrm{Hom}_{\mathbf{Z}}(\_\_, T) \xrightarrow{\sim} \mathrm{Hom}_R(\_\_, \mathrm{Hom}_{\mathbf{Z}}(R, T)).$$

Proof. An inverse map sends $\rho \in \mathrm{Hom}_R(A, \mathrm{Hom}_{\mathbf{Z}}(R, T))$ to $a \mapsto \rho(a)(1)$ for $a \in A$. Functoriality follows from the construction. □

Corollary 2.27. *If Q is an injective abelian group, then $\mathrm{Hom}_{\mathbf{Z}}(R, Q)$ is an injective R-module.*

Proof. Assume given an injection $\iota : A \hookrightarrow B$. We have to show surjectivity of the map $\mathrm{Hom}_R(B, \mathrm{Hom}_{\mathbf{Z}}(R, Q)) \to \mathrm{Hom}_R(A, \mathrm{Hom}_{\mathbf{Z}}(R, Q))$. By the lemma it identifies with the natural map $\mathrm{Hom}_{\mathbf{Z}}(B, Q) \to \mathrm{Hom}_{\mathbf{Z}}(A, Q)$ induced by ι which is surjective by injectivity of Q. □

Now we can prove that the *category of R-modules has enough injectives.*

Proposition 2.28. *Every R-module A can be embedded in an injective R-module.*

Proof. Set $Q := \mathrm{Hom}_{\mathbf{Z}}(R, \mathbf{Q}/\mathbf{Z})$. This is an injective R-module by the previous corollary. Define now a module $I(A)$ as the direct product of copies of Q indexed by the set $\mathrm{Hom}_R(A, Q)$. This is still an injective R-module by Remark 2.23. Define a map $A \to I(A)$ by sending $a \in A$ to $\phi(a)$ in the component indexed by $\phi \in \mathrm{Hom}_R(A, Q)$. To see that this map is injective, note first that $\mathrm{Hom}_R(A, Q) \cong \mathrm{Hom}_{\mathbf{Z}}(A, \mathbf{Q}/\mathbf{Z})$ by the previous lemma. Thus it will suffice to construct for each nonzero $a \in A$ a group homomorphism $\bar{\phi} : A \to \mathbf{Q}/\mathbf{Z}$ with $\bar{\phi}(a) \neq 0$, for then the corresponding

$\phi \in \mathrm{Hom}_R(A, Q)$ will satisfy $\phi(a) \neq 0$. Let $\langle a \rangle \subset A$ be the $\mathbf{Z}$-submodule of A generated by a. Define a group homomorphism $\langle a \rangle \to \mathbf{Q}/\mathbf{Z}$ by sending a to any nonzero element of $\mathbf{Q}/\mathbf{Z}$ if a has infinite order and to a nonzero element of order dividing n if a has finite order n. By divisibility of $\mathbf{Q}/\mathbf{Z}$ this map extends to a homomorphism $\bar{\phi} : A \to \mathbf{Q}/\mathbf{Z}$ as required. □

3. Complexes and resolutions

We begin with some constructions that work in an arbitrary abelian category.

Definition 3.1. A *(cohomological) complex* $A^\bullet$ in an abelian category $\mathcal{A}$ is a sequence of morphisms

$$\dots\dots \xrightarrow{d^{i-1}} A^i \xrightarrow{d^i} A^{i+1} \xrightarrow{d^{i+1}} A^{i+2} \xrightarrow{d^{i+2}} \dots$$

for all $i \in \mathbf{Z}$, satisfying $d^{i+1} \circ d^i = 0$ for all i.

We shall also use the convention $A_{-i} := A^i$, giving rise to the *homological indexing* of the complex.

We introduce the notations

$$Z^i(A^\bullet) := \ker(d^i), \quad B^i(A^\bullet) := \mathrm{Im}\,(d^{i-1}) \quad \text{and} \quad H^i(A^\bullet) := Z^i(A^\bullet)/B^i(A^\bullet).$$

The complex $A^\bullet$ is said to be *acyclic* or *exact* if $H^i(A^\bullet) = 0$ for all i.

A *morphism of complexes* $\phi : A^\bullet \to B^\bullet$ is a collection of homomorphisms $\phi^i : A^i \to B^i$ for all i such that the diagrams

$$\begin{array}{ccc} A^i & \longrightarrow & A^{i+1} \\ {\scriptstyle \phi^i}\downarrow & & \downarrow{\scriptstyle \phi^{i+1}} \\ B^i & \longrightarrow & B^{i+1} \end{array}$$

commute for all i. Thus complexes form a category in which morphisms are defined as above; we shall denote it by $C(\mathcal{A})$. The reader will check that this category is again abelian.

By its defining property, a morphism of complexes $\phi : A^\bullet \to B^\bullet$ induces maps $H^i(\phi) : H^i(A^\bullet) \to H^i(B^\bullet)$ for all i. We say that ϕ is a *quasi-isomorphism* if the $H^i(\phi)$ are isomorphisms for all i.

An important source for quasi-isomorphisms is the following.

Definition 3.2. Two morphisms of complexes $\phi, \psi : A^\bullet \to B^\bullet$ are *(chain) homotopic* if there exist maps $k^i : A^i \to B^{i-1}$ for all i satisfying

$$\phi^i - \psi^i = k^{i+1} \circ d_A^i + d_B^{i-1} \circ k^i \qquad (1)$$

for all i.

Two complexes $A^\bullet$ and $B^\bullet$ are *homotopy equivalent* if there exist morphisms of complexes $\phi : A^\bullet \to B^\bullet$ and $\rho : B^\bullet \to A^\bullet$ such that $\phi \circ \rho$ is homotopic to the identity map of $B^\bullet$ and $\rho \circ \phi$ is homotopic to the identity map of $A^\bullet$.

The following statement follows from the definitions:

Lemma 3.3. *If ϕ and ψ are homotopic morphisms $A^\bullet \to B^\bullet$, then $H^i(\phi) = H^i(\psi)$ for all i.*

In particular, when ϕ induces a homotopy equivalence of complexes, then ϕ is a quasi-isomorphism.

Remark 3.4. Historically one of the first examples of a (homological) complex of abelian groups was the singular complex $S_\bullet(X)$ associated with a topological space X; its homology groups are by definition the (singular) homology groups of X. The assignment $X \mapsto S_\bullet(X)$ induces a functor from the category of topological s-paces (with continuous maps as morphisms) to the category of complexes of abelian groups. It is a basic result in algebraic topology that homotopic continuous maps from a space X to a space Y induce homotopic morphisms of complexes $S_\bullet(X) \to S_\bullet(Y)$ and hence homotopy equivalent topological spaces give rise to homotopy equivalent singular complexes. This is the origin of the use of homotopical morphisms of complexes in homological algebra.

A *short exact sequence of complexes* is a short exact sequence in the category $C(\mathcal{A})$. In other words, it is a sequence of morphisms of complexes

$$0 \to A^\bullet \to B^\bullet \to C^\bullet \to 0$$

such that the sequences

$$0 \to A^i \to B^i \to C^i \to 0$$

are exact for all i. Now we have the following basic fact.

Proposition 3.5. *Given a short exact sequence*

$$0 \to A^\bullet \to B^\bullet \to C^\bullet \to 0$$

of complexes, there is a long exact sequence

$$\cdots \to H^i(A^\bullet) \to H^i(B^\bullet) \to H^i(C^\bullet) \xrightarrow{\partial} H^{i+1}(A^\bullet) \to H^{i+1}(B^\bullet) \to \dots$$

The map ∂ is usually called the *connecting homomorphism* or the *(co)boundary map*.

For the proof of the proposition we need the following equally basic lemma.

Lemma 3.6 (The Snake Lemma). *Given a commutative diagram*

$$\begin{array}{ccccccc} & & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle\alpha} & & \downarrow{\scriptstyle\beta} & & \downarrow{\scriptstyle\gamma} & & \\ 0 & \longrightarrow & A' & \longrightarrow & B' & \longrightarrow & C' & & \end{array}$$

with exact rows, there is an exact sequence

$$\ker(\alpha) \to \ker(\beta) \to \ker(\gamma) \to \operatorname{coker}(\alpha) \to \operatorname{coker}(\beta) \to \operatorname{coker}(\gamma).$$

Proof. It is easy to give a proof in a category of R-modules. The construction of all maps in the sequence is then immediate, except for the map $\partial : \ker(\gamma) \to \operatorname{coker}(\alpha)$. For this, lift $c \in \ker(\gamma)$ to $b \in B$. By commutativity of the right square, the element $\beta(b)$ maps to 0 in C', hence it comes from a unique $a' \in A'$. Define $\partial(c)$ as the image of a' in $\operatorname{coker}(\alpha)$. Two choices of b differ by an element $a \in A$ which maps to 0 in $\operatorname{coker}(\alpha)$, so ∂ is well-defined. Checking exactness is left as an exercise to the readers.

In a general abelian category take the smallest abelian subcategory containing all morphisms in the diagram. It is a small subcategory, so we may apply the Freyd–Mitchell embedding theorem to it. Since the embedding functor is exact, we deduce the required exact sequence from the case of module categories. □

Proof of Proposition 3.5. Applying the Snake Lemma to the diagram

$$\begin{array}{ccccccc} & & A^i/B^i(A^\bullet) & \longrightarrow & B^i/B^i(B^\bullet) & \longrightarrow & C^i/B^i(C^\bullet) & \longrightarrow & 0 \\ & & \downarrow \alpha & & \downarrow \beta & & \downarrow \gamma & & \\ 0 & \longrightarrow & Z^{i+1}(A^\bullet) & \longrightarrow & Z^{i+1}(B^\bullet) & \longrightarrow & Z^{i+1}(C^\bullet) & & \end{array}$$

yields a long exact sequence

$$H^i(A^\bullet) \to H^i(B^\bullet) \to H^i(C^\bullet) \to H^{i+1}(A^\bullet) \to H^{i+1}(B^\bullet) \to H^{i+1}(C^\bullet),$$

and the proposition is obtained by splicing these sequences together. □

Corollary 3.7. *Assume given a commutative diagram of morphisms of complexes*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A^\bullet & \longrightarrow & B^\bullet & \longrightarrow & C^\bullet & \longrightarrow & 0 \\ & & \phi_A \downarrow & & \phi_B \downarrow & & \phi_C \downarrow & & \\ 0 & \longrightarrow & A'^\bullet & \longrightarrow & B'^\bullet & \longrightarrow & C'^\bullet & \longrightarrow & 0 \end{array}$$

with exact rows. If any two of the vertical maps are quasi-isomorphisms, then so is the third one.

Proof. Apply the five lemma to the associated commutative diagram of long exact sequences. □

Now we assume $\mathcal{A}$ *has enough projectives* (e.g. it is a category of modules over a ring). As a consequence, every object A has a *projective resolution* $P_\bullet \to A$, i.e. there is an acyclic complex of the form

$$\cdots \to P_2 \to P_1 \to P_0 \to A \to 0$$

(note the homological indexing!) with P_i projective. Such a resolution can be obtained inductively: first take a surjection $p_0 : P_0 \to A$ with P_i projective. Once P_i and $p_i : P_i \to P_{i-1}$ have been defined (with the convention $P_{-1} = A$), one defines P_{i+1} and p_{i+1} by applying the same construction to $\ker(p_i)$ in place of A.

Remark 3.8. A projective resolution can be interpreted as a quasi-isomorphism between the complex

$$\cdots \to P_2 \to P_1 \to P_0 \to 0 \to 0 \to \cdots$$

and the complex

$$\cdots \to 0 \to 0 \to A \to 0 \to 0$$

in which A is the only nonzero term and it is placed in degree 0. Indeed, we have a morphism of complexes given by the map $P_0 \to A$ in degree 0 and the zero map elsewhere; it is a quasi-isomorphism because both complexes have trivial homology outside degree 0 and there it equals A. This almost tautological observation will be useful later.

Now the basic fact concerning projective resolutions is:

Lemma 3.9. *Assume given a diagram*

$$\begin{array}{ccccccccccc} \cdots & \longrightarrow & P_2 & \xrightarrow{p_2} & P_1 & \xrightarrow{p_1} & P_0 & \xrightarrow{p_0} & A & \longrightarrow & 0 \\ & & & & & & & & \big\downarrow{\scriptstyle \alpha} & & \\ \cdots & \longrightarrow & B_2 & \xrightarrow{b_2} & B_1 & \xrightarrow{b_1} & B_0 & \xrightarrow{b_0} & B & \longrightarrow & 0 \end{array}$$

where the upper row is a complex with the P_i projective and the lower row is an acyclic complex. Then α extends to a morphism of complexes given by the diagram:

$$\begin{array}{ccccccccccc} \cdots & \longrightarrow & P_2 & \xrightarrow{p_2} & P_1 & \xrightarrow{p_1} & P_0 & \xrightarrow{p_0} & A & \longrightarrow & 0 \\ & & \big\downarrow{\scriptstyle \alpha_2} & & \big\downarrow{\scriptstyle \alpha_1} & & \big\downarrow{\scriptstyle \alpha_0} & & \big\downarrow{\scriptstyle \alpha} & & \\ \cdots & \longrightarrow & B_2 & \xrightarrow{b_2} & B_1 & \xrightarrow{b_1} & B_0 & \xrightarrow{b_0} & B & \longrightarrow & 0 \end{array}$$

Moreover, any two such extensions are chain homotopic.

Proof. To construct α_i, assume that the α_j are already defined for $j < i$, with the convention $\alpha_{-1} = \alpha$. Observe that $\mathrm{Im}\,(\alpha_{i-1} \circ p_i) \subset \mathrm{Im}\,(b_i)$; this is immediate for $i = 0$ and follows from $b_{i-1} \circ \alpha_{i-1} \circ p_i = \alpha_{i-2} \circ p_{i-1} \circ p_i = 0$ for $i > 0$ by exactness of the lower row. Hence by the projectivity of P_i we may define α_i as a preimage in $\mathrm{Hom}(P_i, B_i)$ of the map $\alpha_{i-1} \circ p_i : P_i \to \mathrm{Im}\,(b_i)$. For the second statement, suppose $\beta_i : P_i \to B_i$ define another extension. Define $k_{-1} = 0$ and assume k_j defined for $j < i$ satisfying $\alpha_j - \beta_j = k_{j-1} \circ p_j + b_{j+1} \circ k_j$. This implies $\mathrm{Im}\,(\alpha_i - \beta_i - (k_{i-1} \circ p_i)) \subset \mathrm{Im}\,(b_{i+1})$ because

$$b_i \circ (\alpha_i - \beta_i - (k_{i-1} \circ p_i)) = (\alpha_{i-1} - \beta_{i-1}) \circ p_i - b_i \circ k_{i-1} \circ p_i = k_{i-2} \circ p_{i-1} \circ p_i = 0,$$

so, again using the projectivity of P_i, we may define k_i as a preimage of $\alpha_i - \beta_i - (k_{i-1} \circ p_i) \in \mathrm{Hom}(P_i, \mathrm{Im}\,(b_{i+1}))$ in $\mathrm{Hom}(P_i, B_{i+1})$. □

Corollary 3.10. *Any two projective resolutions of an object A are homotopy equivalent.*

Proof. Given two projective resolutions $P_\bullet \to A$ and $P'_\bullet \to A$, the identity map of A lifts to morphisms of complexes $\phi : P_\bullet \to P'_\bullet$ and $\phi' : P'_\bullet \to P_\bullet$ by the lemma above. By the second statement of the lemma $\phi \circ \phi' : P'_\bullet \to P'_\bullet$ is chain homotopic to the identity map of $P'_\bullet$ and similarly for $\phi' \circ \phi : P_\bullet \to P_\bullet$. □

For a category $\mathcal{A}$ that *has enough injectives* the preceding arguments dualize. Using the fact that every object A embeds in an injective object we construct inductively *injective resolutions* $A \to Q^\bullet$, i.e. acyclic complexes of the form

$$0 \to A \to Q^0 \to Q^1 \to Q^2 \to \cdots$$

with the Q^i injective. The analogue of the previous lemma holds, with the same proof (performed in the opposite category of $\mathcal{A}$):

Lemma 3.11. *Assume given a diagram*

$$\begin{array}{ccccccccccc} 0 & \longrightarrow & A & \xrightarrow{a^0} & A^0 & \xrightarrow{a^1} & A^1 & \xrightarrow{a^2} & A^2 & \longrightarrow & \dots \\ & & \downarrow{\scriptstyle\alpha} & & & & & & & & \\ 0 & \longrightarrow & B & \xrightarrow{q^0} & Q^0 & \xrightarrow{q^1} & Q^1 & \xrightarrow{q^2} & Q^2 & \longrightarrow & \dots \end{array}$$

where the lower row is a complex with the Q^i injective and the upper row is an acyclic complex. Then α extends to a morphism of complexes given by the diagram:

$$\begin{array}{ccccccccccc} 0 & \longrightarrow & A & \xrightarrow{a^0} & A^0 & \xrightarrow{a^1} & A^1 & \xrightarrow{a^2} & A^2 & \longrightarrow & \dots \\ & & \downarrow{\scriptstyle\alpha} & & \downarrow{\scriptstyle\alpha_0} & & \downarrow{\scriptstyle\alpha_1} & & \downarrow{\scriptstyle\alpha_2} & & \\ 0 & \longrightarrow & B & \xrightarrow{q^0} & Q^0 & \xrightarrow{q^1} & Q^1 & \xrightarrow{q^2} & Q^2 & \longrightarrow & \dots \end{array}$$

Moreover, any two such extensions are chain homotopic. In particular, any two injective resolutions of A are homotopy equivalent.

4. Derived functors

Derived functors remedy the defect of exactness of left or right exact functors.

Construction 4.1. Let $\mathcal{A}$, $\mathcal{B}$ be abelian categories and $F : \mathcal{A} \to \mathcal{B}$ an additive functor. Assume that $\mathcal{A}$ has enough projectives. Then the *left derived functors L_iF* of F are defined as follows. Given an object A in $\mathcal{A}$, choose a projective resolution $P_\bullet \to A$ and consider the complex $F(P_\bullet)$, then set $L_iF(A) := H_i(F(P_\bullet))$. Given a morphism $\alpha : A \to B$ in $\mathcal{A}$, choose projective resolutions $P^A_\bullet \to A$, $P^B_\bullet \to B$. By Lemma 3.9

the map α induces a morphism of complexes $\alpha_\bullet : P_\bullet^A \to P_\bullet^B$. Define $L_iF(\alpha) := H_i(F(\alpha_\bullet))$.

Dually, when $\mathcal{A}$ has enough injectives, the *right derived functors* R^iF of F are defined by choosing an injective resolution $A \to Q^\bullet$ for an object A, and setting $R^iF(A) := H^i(F(Q^\bullet))$. Given a morphism $\alpha : A \to B$ in $\mathcal{A}$, the morphism $R^iF(\alpha)$ is defined by lifting α to a morphism of injective resolutions using Lemma 3.11, and then taking the i-th cohomology.

Lemma 4.2. *The definition of $L_iF(A)$ does not depend on the choice of the projective resolution $P_\bullet$, and that of $L_iF(\alpha)$ on the choice of the lifting $\alpha_\bullet$ of α.*

Similar statements hold for the right derived functors R^iF.

Proof. We do the case of L_iF. If $P_\bullet \to A$, $P'_\bullet \to A$ are two projective resolutions, they are homotopy equivalent by by Corollary 3.10. Applying the functor F we get that the complexes $F(P'_\bullet)$ and $F(P'_\bullet)$ are also homotopy equivalent via $F(\phi)$ and $F(\phi')$. It follows that $F(\phi)$ induces canonical quasi-isomorphisms $F(P_\bullet) \to F(P'_\bullet)$. The well-definedness of $L_iF(\alpha)$ follows from the second statement of Lemma 3.9. $\square$

Proposition 4.3. *Assume that $\mathcal{A}$ has enough projectives and moreover F is a right exact functor. Then $L_0(F) \cong F$, and given a short exact sequence $0 \to A \to B \to C \to 0$ of R-modules, there is an associated long exact sequence of the form*

$$\cdots \to L_iF(A) \to L_iF(B) \to L_iF(C) \to L_{i-1}F(A) \to \cdots$$

ending with $F(C) \to 0$.

Similarly, when $\mathcal{A}$ has enough injectives and F is left exact, we have $R^0(F) \cong F$, and a short exact sequence $0 \to A \to B \to C \to 0$ induces a long exact sequence of the form

$$\cdots \to R^iF(A) \to R^iF(B) \to R^iF(C) \to R^{i+1}F(A) \to \cdots$$

starting with $0 \to F(A)$.

The proof uses a lemma.

Lemma 4.4 (Horseshoe Lemma). *Assume given a short exact sequence*

$$0 \to A \to B \to C \to 0$$

in $\mathcal{A}$ and projective resolutions $P_\bullet^A \to A$, $P_\bullet^C \to C$. There exists a projective resolution $P_\bullet^B \to B$ fitting in a short exact sequence of complexes

$$0 \to P_\bullet^A \to P_\bullet^B \to P_\bullet^C \to 0$$

and a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & P_\bullet^A & \longrightarrow & P_\bullet^B & \longrightarrow & P_\bullet^C & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0. \end{array}$$

A similar statement holds if we have injective resolutions $A \to Q_A^\bullet$, $C \to Q_C^\bullet$.

Proof. Notice first that any short exact sequence $0 \to P_1 \to P_2 \to P_3 \to 0$ of projective modules splits as a direct sum $P_2 \cong P_1 \oplus P_3$ (lift the identity map of P_3 to a map $P_3 \to P_2$). So if the lemma is true, we must have $P_i^B \cong P_i^A \oplus P_i^C$ for all i. We therefore set $P_i^B := P_i^A \oplus P_i^C$ and construct the maps in the required short exact sequence of resolutions by induction on i. First, by projectivity of P_0^C the map $p_C : P_0^C \to C$ lifts to a map $P_0^C \to B$. Taking the sum of this map with the composite map $P_0^A \to A \to B$ defines a map $P_0^A \oplus P_0^C \to B$, i.e. a map $p_B : P_0^B \to B$ making the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & P_0^A & \longrightarrow & P_0^B & \longrightarrow & P_0^C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle p_A} & & \downarrow{\scriptstyle p_B} & & \downarrow{\scriptstyle p_C} & & \\ 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \end{array}$$

commute. Using the Snake Lemma we see that the surjectivity of p_A and p_C implies that of p_B and moreover the sequence $0 \to \ker(p_A) \to \ker(p_B) \to \ker(p_C) \to 0$ is exact. Now we have a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & P_1^A & \longrightarrow & P_1^B & \longrightarrow & P_1^C & \longrightarrow & 0 \\ & & \downarrow & & & & \downarrow & & \\ 0 & \longrightarrow & \ker(p_A) & \longrightarrow & \ker(p_B) & \longrightarrow & \ker(p_C) & \longrightarrow & 0 \end{array}$$

with surjective vertical maps, so by repeating the above argument we get a surjective map $P_1^B \to \ker(p_B)$ making the diagram commute. Continuing the procedure we obtain the required short exact sequence of resolutions. □

Proof of Proposition 4.3. The statements $L_0(F) \cong F$ and $R^0(F) \cong F$ under the stated exactness assumptions follow from the definitions. We now derive the long exact for left derived functors, the other one being similar. Apply the construction of the Horseshoe Lemma to get an exact sequence $0 \to P_\bullet^A \to P_\bullet^B \to P_\bullet^C \to 0$ of projective resolutions. As already remarked, here in fact $P_i^B \cong P_i^A \oplus P_i^C$ for all i, so that $F(P_i^B) \cong F(P_i^A) \oplus F(P_i^C)$ by additivity of F. Thus we have a short exact sequence of complexes $0 \to F(P_\bullet^A) \to F(P_\bullet^B) \to F(P_\bullet^C) \to 0$ to which we apply Proposition 3.5. □

Remark 4.5.

(1) For a projective object P we have $L_iF(P) = 0$ for $i > 0$ as we may take $0 \to P \to P \to 0$ as a projective resolution. Similarly, $R^iF(Q) = 0$ for $i > 0$ when Q is injective. This gives rise to an important technique called *dimension shifting* which we explain for left derived functors. Given an object A we may choose an exact sequence $0 \to K \to P \to A \to 0$ with P projective. The long exact sequence then induces isomorphisms $L_iF(A) \xrightarrow{\sim} L_{i-1}F(K)$ for $i > 1$. In this way, if we have to prove a property of L_iF for all A and all $i > 0$, we may reduce to the case $i = 1$ using induction.

(2) There is an additional functoriality property of derived functors that is often useful: given a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & A' & \longrightarrow & B' & \longrightarrow & C' & \longrightarrow & 0 \end{array}$$

of short exact sequences, the diagram

$$\begin{array}{ccc} L_iF(C) & \longrightarrow & L_{i-1}F(A) \\ \downarrow & & \downarrow \\ L_iF(C') & \longrightarrow & L_{i-1}F(A') \end{array}$$

of boundary maps in the associated log exact sequences commutes for all i, and similarly for right derived functors. We omit the verification.

We now come to fundamental examples for the category of modules over a ring.

Examples 4.6. Let A be an R-module.

(1) The functor $A \otimes_R \_\_$ is right exact. Its i-th left derived functor is denoted by $\mathrm{Tor}_i^R(A, \_\_)$. Thus for every R-module B we have an isomorphism $\mathrm{Tor}_0^R(A, B) \cong A \otimes_R B$ and every short exact sequence $0 \to B_1 \to B_2 \to B_3 \to 0$ of R-modules induces a long exact sequence

$$\cdots \to \mathrm{Tor}_1^R(A, B_1) \to \mathrm{Tor}_1^R(A, B_2) \to \mathrm{Tor}_1^R(A, B_3) \to A \otimes_R B_1 \to A \otimes_R B_2 \to A \otimes_R B_3 \to 0.$$

(2) The functor $\mathrm{Hom}_R(A, \_\_)$ is left exact. Its i-th right derived functor is denoted by $\mathrm{Ext}_R^i(A, \_\_)$. Thus for every R-module B we have an isomorphism $\mathrm{Ext}_R^0(A, B) \cong \mathrm{Hom}_R(A, B)$ and every short exact sequence $0 \to B_1 \to B_2 \to B_3 \to 0$ of R-modules induces a long exact sequence

$$0 \to \mathrm{Hom}_R(A, B_1) \to \mathrm{Hom}_R(A, B_2) \to \mathrm{Hom}_R(A, B_3) \to \mathrm{Ext}_R^1(A, B_1) \to \mathrm{Ext}_R^1(A, B_2) \to \cdots$$

One can define derived functors of contravariant functors by the same method as for covariant ones; the only difference is that left derived functors are defined via injective resolutions and right derived functors via projective ones. The basic example is:

Example 4.7. Let B be an R-module. The contravariant functor $\mathrm{Hom}_R(\_\_, B)$ is left exact. Its i-th right derived functor, denoted by $\mathrm{Ext}^i_R(\_\_, B)$, is defined by taking a projective resolution $P_\bullet \to A$ of an R-module A and setting $\mathrm{Ext}^i_R(A, B) := H^i(\mathrm{Hom}_R(P_\bullet, B))$. We have an isomorphism $\mathrm{Ext}^0_R(A, B) \cong \mathrm{Hom}_R(A, B)$ and every short exact sequence $0 \to A_1 \to A_2 \to A_3 \to 0$ of R-modules induces a long exact sequence

$$0 \to \mathrm{Hom}_R(A_3, B) \to \mathrm{Hom}_R(A_2, B) \to \mathrm{Hom}_R(A_1, B) \to \mathrm{Ext}^1_R(A_3, B) \to \mathrm{Ext}^1_R(A_2, B) \to \cdots$$

Now an important question arises: we have defined the groups $\mathrm{Ext}^i_R(A, B)$ in two ways, via a projective resolution of A and an injective resolution of B. Do the two methods give the same result? Similarly, we have defined the groups $\mathrm{Tor}_i(A, B)$ via a projective resolution of B; does using a projective resolution of A yield the same groups? The answer is yes in both cases - we'll seeit in the section on total derived functors.

5. Ext and Tor

Now that we have Ext functors at our disposal, we can give another characterization of projective modules.

Proposition 5.1. *The following are equivalent for an R-module A.*

(1) *A is projective.*
(2) *$\mathrm{Ext}^i_R(A, B) = 0$ for all $i > 0$ and all R-modules B.*
(3) *$\mathrm{Ext}^1_R(A, B) = 0$ for all R-modules B.*

Proof. The implication $(1) \Rightarrow (2)$ is a special case of Remark 4.5 (1), $(2) \Rightarrow (3)$ is obvious, and $(3) \Rightarrow (1)$ follows from the long exact sequence of Ext. □

For injective modules we have a similar characterization, but it can be sharpened using Baer's criterion.

Proposition 5.2. *The following are equivalent for an R-module B.*

(1) *B is injective.*
(2) *$\mathrm{Ext}^i_R(A, B) = 0$ for all $i > 0$ and all R-modules A.*
(3) *$\mathrm{Ext}^1_R(A, B) = 0$ for all R-modules A.*
(4) *$\mathrm{Ext}^1_R(R/I, B) = 0$ for all ideals $I \subset R$.*

Proof. The equivalence of (1)–(3) is proven as above and $(3) \Rightarrow (4)$ is obvious. Now consider the exact sequence $0 \to I \to R \to R/I \to 0$ for an ideal $I \subset R$ and apply the functor $\mathrm{Hom}_R(\_\_, B)$. The associated long exact sequence together with assumption (4) shows that the map $\mathrm{Hom}_R(R, B) \to \mathrm{Hom}_R(I, B)$ is surjective, so (1) holds by Baer's criterion. □

There is a similar characterization for flat modules as well.

Proposition 5.3. *The following are equivalent for an R-module A.*

(1) *A is flat.*
(2) $\mathrm{Tor}_i^R(A, B) = 0$ *for all $i > 0$ and all R-modules B.*
(3) $\mathrm{Tor}_1^R(A, B) = 0$ *for all R-modules B.*
(4) $\mathrm{Tor}_1^R(R/I, A) = 0$ *for every ideal $I \subset R$.*

Proof. To prove $(1) \Rightarrow (2)$ we use dimension shifting. Take an exact sequence $0 \to K \to P \to B \to 0$ with P projective. The long exact sequence of Tor gives an exact sequence

$$\mathrm{Tor}_1^R(A, P) \to \mathrm{Tor}_1^R(A, B) \to A \otimes_R K \to A \otimes_R P$$

Here $\mathrm{Tor}_1^R(A, P) = 0$ because P is projective, hence $\mathrm{Tor}_1^R(A, B) = 0$ as tensoring by A is left exact by assumption. In view of $\mathrm{Tor}_i(A, P) = 0$ for $i > 0$ the continuation of the sequence gives isomorphisms

$$\mathrm{Tor}_i^R(A, B) \xrightarrow{\sim} \mathrm{Tor}_{i-1}^R(A, K)$$

for all $i > 1$, whence (2) by induction on i.

The implications $(2) \Rightarrow (3) \Rightarrow (4)$ being obvious, only $(4) \Rightarrow (1)$ remains. Assume $\phi : B_0 \to B$ is an injective map of R-modules. To prove that $\phi \otimes \mathrm{id}_R : A \otimes_R B_0 \to A \otimes_R B$ is also injective we may assume using Proposition 2.6 that B_0 and B are both finitely generated. In this case we find $t_1, \ldots, t_r \in B$ so that $B = \langle B_0, t_1, \ldots, t_r \rangle$. Setting $B_j := \langle B_0, t_1, \ldots, t_j \rangle$ for all $1 \le j \le r$ we obtain a finite filtration $B_0 \subset B_1 \subset \cdots \subset B_r = B$ such that $B_j / B_{j-1} \cong \langle t_j \rangle \cong R/I_j$ for the ideal $I_j \subset R$ annihilating t_j. But then tensoring the exact sequence $0 \to B_{j-1} \to B_j \to R/I_j \to 0$ by A gives an exact sequence

$$\mathrm{Tor}_1^R(R/I_j, A) \to A \otimes_R B_{j-1} \to A \otimes_R B_j$$

where $\mathrm{Tor}_1^R(R/I_j, A) = 0$ by assumption. Therefore $A \otimes_R B_0 \to A \otimes_R B$ is injective, being the composite of the injective maps $A \otimes_R B_{j-1} \to A \otimes_R B_j$. □

Using Proposition 5.3 it is easy to prove a structure theorem for finitely generated flat modules over Noetherian local rings.

Proposition 5.4. *Let R be a Noetherian local ring with maximal ideal P and residue field k, and let A be a finitely generated R-module. If A is flat over R, or more generally $\mathrm{Tor}_1(A,k)=0$, then A is free over R.*

Proof. Let $a_1, \dots a_n \in A$ be elements such that their mod PA images form a basis of the k-vector space A/PA. By Nakayama's lemma they generate A, so the map $\phi : R^n \to A$ sending $(r_1, \dots, r_n)$ to $r_1a_1 + \cdots + r_na_n$ is surjective, giving rise to an exact sequence $0 \to B \to R^r \to A \to 0$. Now tensor this sequence by k over R. Since $\mathrm{Tor}_1(A,k) = 0$, the long exact sequence of Tor implies the exactness of $0 \to B/PB \to R^r/PR^r \to A/PA \to 0$, whence $B = PB$. Since R is Noetherian, B is finitely generated, hence 0 by Nakayama's lemma. □

Finally we explain the origin of the names of the functors Tor and Ext. For Tor the name comes from 'torsion':

Proposition 5.5. *Let R be a ring and A an R-module. If $r \in R$ is a non-zerodivisor, then*

$$\mathrm{Tor}_1(R/(r), A) \cong \{a \in A \mid ra = 0\}.$$

The module on the right hand side is called the r-torsion in A. The module A is called torsion free if it has no r-torsion for any r. In the case $R = \mathbf{Z}$ and $n \in \mathbf{Z}$ we get back the notion of n-torsion in an abelian group. It can be shown that in this case the whole torsion subgroup is isomorphic to $\mathrm{Tor}_1(\mathbf{Q}/\mathbf{Z}, A)$.

Proof. Consider the exact sequence $0 \to R \xrightarrow{r} R \to R/(r) \to 0$. Since R is projective as an R-module, part of the associated long exact Tor-sequence gives an exact sequence

$$0 = \mathrm{Tor}_1^R(R, A) \to \mathrm{Tor}_1^R(R/(r), A) \to A \xrightarrow{r} A$$

whence the statement follows. □

Corollary 5.6. *Over a principal ideal domain a module is torsion free if and only if it is flat.*

Proof. If R is a principal ideal domain and $I \subset R$ is an ideal, then $I = (r)$ for some $r \in R$ and therefore $\mathrm{Tor}_1^R(R/I, A) = \mathrm{Tor}_1^R(R/(r), A)$. The vanishing of this group for all $r \in R$ is equivalent to A being torsion free by the proposition and to A being flat by Proposition 5.3. □

The Ext functor received its name from its relation to extensions. An *extension* of an R-module C by A is an R-module B fitting in a short exact sequence

$$0 \to A \to B \xrightarrow{p} C \to 0.$$

The extension is *split* if there is a map $i : C \to B$ with $p \circ i = \mathrm{id}_C$. In this case B is isomorphic to the direct sum $A \oplus C$.

Two extensions B and B' are *equivalent* if there is an R-module map $\phi : B \to B'$ fitting in a commutative diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \mathrm{id}} & & \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \mathrm{id}} & & \\
0 & \longrightarrow & A & \longrightarrow & B' & \longrightarrow & C & \longrightarrow & 0.
\end{array}$$

The Snake Lemma shows that in this case ϕ must be an isomorphism, whence it follows that we have indeed defined an equivalence relation. Denote by $\mathrm{Ext}(C, A)$ the set of equivalence classes of extensions of C by A.

Construction 5.7. We construct a map $\mathrm{Ext}(C, A) \to \mathrm{Ext}^1_R(C, A)$ as follows. Take a projective resolution $P_\bullet \to C$. By Lemma 3.9 the diagram

$$\begin{array}{ccccccccccc}
\dots & \longrightarrow & P_2 & \xrightarrow{p_2} & P_1 & \xrightarrow{p_1} & P_0 & \xrightarrow{p_0} & C & \longrightarrow & 0 \\
 & & & & & & & & \downarrow{\scriptstyle \mathrm{id}} & & \\
\dots & \longrightarrow & 0 & \xrightarrow{b_2} & A & \xrightarrow{b_1} & B & \xrightarrow{b_0} & C & \longrightarrow & 0
\end{array}$$

can be filled in as

$$\begin{array}{ccccccccccc}
\dots & \longrightarrow & P_2 & \xrightarrow{p_2} & P_1 & \xrightarrow{p_1} & P_0 & \xrightarrow{p_0} & C & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow{\scriptstyle \alpha_1} & & \downarrow{\scriptstyle \alpha_0} & & \downarrow{\scriptstyle \mathrm{id}} & & \\
\dots & \longrightarrow & 0 & \xrightarrow{b_2} & A & \xrightarrow{b_1} & B & \xrightarrow{b_0} & C & \longrightarrow & 0
\end{array}$$

where $\alpha_1 \circ p_2 = 0$. This shows that $\alpha_1 \in \mathrm{Hom}_R(P_1, A)$ is contained in $Z^1(\mathrm{Hom}(P_1, A))$, whence a class $e \in \mathrm{Ext}^1_R(C, A)$. Since any two projective resolutions of C are chain homotopy equivalent by Corollary 3.10, the class e does not depend on the choice of $P_\bullet$. Finally, equivalent extensions give rise to the same class $e \in \mathrm{Ext}^1_R(C, A)$ by construction.

In case of a split extension the splitting $i : C \to B$ induces a commutative diagram

$$\begin{array}{ccccccccccc}
\dots & \longrightarrow & P_2 & \xrightarrow{p_2} & P_1 & \xrightarrow{p_1} & P_0 & \xrightarrow{p_0} & C & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow{\scriptstyle 0} & & \downarrow{\scriptstyle i \circ p_0} & & \downarrow{\scriptstyle \mathrm{id}} & & \\
\dots & \longrightarrow & 0 & \xrightarrow{b_2} & A & \xrightarrow{b_1} & B & \xrightarrow{b_0} & C & \longrightarrow & 0
\end{array}$$

so that the associated class is 0.

Remark 5.8. There is another way to construct the extension class e: apply the functor $\mathrm{Hom}_R(C, \_\_)$ to the exact sequence $0 \to A \to B \to C \to 0$. The resulting long exact sequence gives rise to a coboundary map $\mathrm{Hom}_R(C, C) \to \mathrm{Ext}^1_R(C, A)$. Define e as the image of the identity map of C by this map. One can check that it depends only on the extension class of B and the resulting map $\mathrm{Ext}(C, A) \to \mathrm{Ext}^1_R(C, A)$ is the same as the one constructed above.

Proposition 5.9. *The map* $\mathrm{Ext}(C, A) \to \mathrm{Ext}^1_R(C, A)$ *constructed above is a bijection sending the class of the split extension* $A \oplus C$ *to 0.*

The proof uses the *pushout* construction: given an exact sequence of R-modules $0 \to A \to B \to C \to 0$ and an R-module map $\phi : A \to A'$, define an R-module X as the quotient of $A' \oplus B$ by the submodule of elements of the form $(\phi(a), -a)$ for $a \in A$. The natural projection $A' \oplus B \to B$ induces a map $X \to C$ sitting in a commutative diagram with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \phi} & & \downarrow & & \downarrow{\scriptstyle \mathrm{id}} & & \\ 0 & \longrightarrow & A' & \longrightarrow & X & \longrightarrow & C & \longrightarrow & 0. \end{array}$$

Moreover, X has the following universal property: for any X' sitting in a diagram of the above type there is an R-module map $X \to X'$ inducing an equivalence of extensions of C by A'. All this is straightforward to verify.

Sketch of proof of Proposition 5.9. We have already noted that the split extension class goes to 0. We construct an inverse map $\mathrm{Ext}^1_R(C, A) \to \mathrm{Ext}(C, A)$ as follows. Choose projective resolution $P_\bullet \to C$ as above. A class in $\mathrm{Ext}^1_R(C, A)$ is then represented by a homomorphism $\phi : P_1/\mathrm{Im}\,(p_2) \to A$. Now form the pushout of the extension $0 \to P_1/\mathrm{Im}\,(p_2) \to P_0 \to C \to 0$ by ϕ and take the associated class in $\mathrm{Ext}(C, A)$. As in the above construction, one verifies using Lemma 3.9 that choosing another projective resolution gives rise to the same extension class. It follows from the constructions that the two maps are inverse to each other; we leave details to the reader. $\square$

Remark 5.10. It is possible to define an abelian group structure on $\mathrm{Ext}(C, A)$ so that the above bijection becomes an isomorphism of abelian groups. Besides pushout, this also uses the analogous pullback construction: given an exact sequence of R-modules $0 \to A \to B \xrightarrow{p} C \to 0$ and an R-module map $\psi : C' \to C$, define an R-module Y as the submodule of $B \oplus C'$ given by $\{(b, c') : p(b) = \psi(c')\}$. The inclusion $A \to B$ induces an inclusion $A \to Y$ sitting in a commutative diagram with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & Y & \longrightarrow & C' & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mathrm{id}} & & \downarrow & & \downarrow{\scriptstyle \psi} & & \\ 0 & \longrightarrow & A & \longrightarrow & B & \xrightarrow{p} & C & \longrightarrow & 0. \end{array}$$

Here Y has a similar universal property as the pushout.

Now assume $0 \to A \to B \to C \to 0$ and $0 \to A \to B' \to C \to 0$ represent two classes in $\mathrm{Ext}(C, A)$. Form first the direct sum extension

$$0 \to A \oplus A \to B \oplus B' \to C \oplus C \to 0,$$

then take pushout by the map $A \oplus A \to A$, $(a_1, a_2) \mapsto a_1 + a_2$, and finally take the pullback of the resulting extension of $C \oplus C$ by A by the diagonal map $C \to C \oplus C$. The resulting extension is the *Baer sum* of the extensions given by B and B'. It can be checked that the construction respects the equivalence relation on extensions and gives $\mathrm{Ext}(C, A)$ the structure of an abelian group with zero element $A \oplus C$ so that the map $\mathrm{Ext}(C, A) \to \mathrm{Ext}^1_R(C, A)$ is an isomorphism. (Note: it is enough to check that the map $\mathrm{Ext}(C, A) \to \mathrm{Ext}^1_R(C, A)$ respects addition, then the group axioms for $\mathrm{Ext}(C, A)$ follow from those in $\mathrm{Ext}^1_R(C, A)$.)

Remark 5.11. There is a generalization of the above construction to higher Ext groups due to Yoneda. Elements of the Yoneda Ext groups $\mathrm{YExt}^n(C, A)$ are represented by n-fold extensions

$$0 \to A \to B_1 \to B_2 \to \cdots \to B_n \to C \to 0.$$

A morphism of n-fold extensions is a morphism of complexes inducing the identity map on A and C. Equivalence of extensions is then defined as the coarsest equivalence relation under which two extensions are equivalent if there is a morphism between them. Baer sum and a map $\mathrm{YExt}^n(C, A) \to \mathrm{Ext}^n_R(C, A)$ are defined by straightforward generalizations of the case $n = 1$. One then proves that the map $\mathrm{YExt}^n(C, A) \to \mathrm{Ext}^n_R(C, A)$ is a group isomorphism.

Yoneda's construction of Ext groups has several advantages. One is that it is very explicit. Moreover, it does not use the existence of enough projectives or injectives, and therefore makes sense in a general abelian category. Also, is that it is very easy to define a product structure $\mathrm{YExt}^n(C, B) \times \mathrm{YExt}^m(B, A) \to \mathrm{YExt}^{n+m}(C, A)$ by splicing an n-fold extension $0 \to B \to C_1 \to C_2 \to \cdots \to C_n \to C \to 0$ and an m-fold extension $0 \to A \to B_1 \to B_2 \to \cdots \to B_m \to B \to 0$ together in an $(n+m)$-fold extension $0 \to A \to B_1 \to B_2 \to \cdots \to B_m \to C_1 \to C_2 \to \cdots \to C_n \to C \to 0$.

6. Homological dimension

In this section and the next we employ the notation A for rings and M, N for A-modules.

Definition 6.1. Let A be a ring, M is an A-module. We say that M has a projective resolution of length i if there exists an exact sequence

$$0 \to P_i \to \cdots \to P_0 \to M \to 0$$

with all P_j projective.

The *projective dimension* $\mathrm{pd}(M)$ of M is defined as the smallest i for which M has a projective resolution of length i; it may be infinite. The *global dimension* of A is

$$\mathrm{gldim}(A) := \sup\{\mathrm{pd}(M) \mid M \text{ is an } A\text{-module}\}.$$

It can be infinite as well.

Proposition 6.2. *The following are equivalent for an A-module M:*

(1) $\mathrm{pd}(M) \leq d$,
(2) $\mathrm{Ext}^i_A(M, N) = 0$ *for all A-modules N and $i > d$,*
(3) $\mathrm{Ext}^{d+1}_A(M, N) = 0$ *for all A-modules N,*
(4) *If $0 \to M_d \to P_{d-1} \to \cdots \to P_0 \to M \to 0$ is exact and the P_i are projective, then M_d is projective.*

Proof. The implications $(4) \Rightarrow (1)$ and $(2) \Rightarrow (3)$ are obvious. $(1) \Rightarrow (2)$ follows because we may calculate the Ext functors using a projective resolution of length $\leq d$. To prove $(3) \Rightarrow (4)$, we split the exact sequence of (4) in short exact sequences of the form $0 \to M_i \to P_{i-1} \to M_{i-1} \to 0$ (here $M_0 = M$). Since the P_i are projective, the associated long exact sequences for Ext give isomorphisms $\mathrm{Ext}^{d+2-i}_A(M_{i-1}, N) \cong \mathrm{Ext}^{d+1-i}_A(M_i, N)$ for all N and all $0 \leq i \leq d$. Then (3) implies $\mathrm{Ext}^1_A(M_d, N) = 0$ for all N, so M_d is projective by Proposition 5.1. □

Corollary 6.3. *The global dimension of A is the smallest (possibly infinite) d such that $\mathrm{Ext}^{d+1}_A(M, N) = 0$ for all A-modules M, N.*

Example 6.4. The global dimension of a field is 0. The global dimension of **Z** is 1. Indeed, given an abelian group B, we may embed it in an injective abelian group Q. For abelian groups being injective is the same as being divisible, whence we get that the quotient Q/B is also injective. This means that B has an injective resolution of length 2, whence $\mathrm{Ext}^2_{\mathbf{Z}}(M, B) = 0$ for every abelian group M. (Alternatively, we could have deduced $\mathrm{gldim}(\mathbf{Z}) = 1$ from the fact that any subgroup of a free abelian group is free.) We shall see a vast generalization of this fact in Theorem 7.3 below.

Remarks 6.5.

1. One can define the injective dimension of a module as the length of the shortest possible injective resolution and prove an analogue of Proposition 6.2 for injective dimension. This shows that the global dimension of A is also the supremum of injective dimensions of modules because the previous corollary can be reproven using injective resolutions.

2. Quite generally, one can define the homological dimension of an abelian category $\mathcal{A}$ as the smallest d such that $\mathrm{Ext}^i_{\mathcal{A}}(A, B) = 0$ for all $i > d$ and all objects A, B in $\mathcal{A}$.

(Here the Ext-groups are defined, for instance, using the Yoneda method.) The above notion is the special case of module categories.

The following proposition allows us to restrict to finitely generated modules.

Lemma 6.6. *Let A be a ring and $i \geq 0$ an integer. The following are equivalent:*

(1) $\mathrm{Ext}^i_A(M, N) = 0$ *for all A-modules M, N.*
(2) $\mathrm{Ext}^i_A(M, N) = 0$ *for all A-modules N and all finitely generated A-modules M.*
(3) $\mathrm{Ext}^i_A(A/I, N) = 0$ *for all A-modules N and ideals $I \subset A$.*

Proof. The implications $(1) \Rightarrow (2) \Rightarrow (3)$ being obvious, we show $(3) \Rightarrow (1)$. Take an injective resolution $0 \to N \to Q^\bullet$ of N, and truncate it as

$$0 \to N \to Q^0 \to Q^1 \to \cdots \to Q^{i-2} \to N^{i-1} \to 0$$

By a similar dimension-shifting argument as in the previous proof we have an i-somorphism $\mathrm{Ext}^i_A(M, N) \cong \mathrm{Ext}^1_A(M, N^{i-1})$, so that $\mathrm{Ext}^i_A(M, N) = 0$ for all M if and only if $\mathrm{Ext}^1_A(M, N^{i-1}) = 0$ for all M. By Proposition 5.2 this is equivalent to N^{i-1} being injective, and also to $\mathrm{Ext}^1_A(A/I, N^{i-1}) = 0$ for all ideals $I \subset A$. This in turn is equivalent to saying that $\mathrm{Ext}^i_A(A/I, N) = 0$ for all i, again by dimension shifting. □

Corollary 6.7. $\mathrm{gldim}(A) = \sup\{\mathrm{pd}(M) \mid M$ *is a finitely generated A-module*$\}$.

In the local case projective dimension can also be calculated by Tor.

Proposition 6.8. *Let A be a Noetherian local ring with maximal ideal P and M a finitely generated A-module. Then $\mathrm{pd}(M) \leq d$ if and only if $\mathrm{Tor}^A_{d+1}(M, k) = 0$, where $k = A/P$.*

Proof. The 'only if' part follows by calculating Tor by means of a projective resolution of length $\leq d$. We prove the 'if' part by induction on d. The case $d = 0$ follows from Proposition 5.4. For the inductive step use the fact that M is finitely generated to obtain an exact sequence $0 \to N \to A^n \to M \to 0$ with some n. Here N is also finitely generated because A is Noetherian. The associated long exact Tor-sequence implies $\mathrm{Tor}^A_d(N, k) \cong \mathrm{Tor}^A_{d+1}(M, k)$ for $d > 0$, so $\mathrm{pd}(M) \leq \mathrm{pd}(N) + 1 \leq d$ by induction (for the first inequality note that a projective resolution of N can be extended by A^n to obtain a projective resolution of M). □

We can now prove a characterization of global dimension for Noetherian local rings which involves a single module.

Corollary 6.9. *If A is a Noetherian local ring with residue field k, then*

$$\mathrm{gldim}(A) = \mathrm{pd}(k) = \max\{d : \mathrm{Tor}^A_d(k, k) \neq 0\}.$$

Proof. The second equality follows from Proposition 6.8 applied with $M = k$. To prove the first one, note that by Corollary 6.7 and Proposition 6.8 we have $\mathrm{gldim}(A) \leq d$ if and only if $\mathrm{Tor}^A_{d+1}(M, k) = 0$ for all finitely generated M over A. If $\mathrm{pd}(k) \leq d$, then $\mathrm{Tor}^A_{d+1}(M, k) = 0$ follows by using a projective resolution of length $\leq d$. Conversely, if $\mathrm{Tor}^A_{d+1}(M, k) = 0$ for all finitely generated M, then in particular this holds for $M = k$, whence $\mathrm{pd}(k) \leq d$ by Proposition 6.8. □

On the other hand, computing the global dimension of a Noetherian ring can be reduced to the local case:

Proposition 6.10. *Let A be a Noetherian ring. Then*

$$\mathrm{gldim}(A) = \sup\{\mathrm{gldim}(A_Q) : Q \subset A \text{ is a maximal ideal}\}.$$

The proof uses a base change property for Ext groups (we also include the case of Tor for later use).

Lemma 6.11. *Let A be a ring, B a flat A-algebra and M, N A-modules.*

(1) *If A is Noetherian and M is finitely generated, we have isomorphisms*

$$\mathrm{Ext}^i_A(M, N) \otimes_A B \cong \mathrm{Ext}^i_B(M \otimes_A B, N \otimes_A B)$$

for all $i \geq 0$.

(2) *We also have isomorphisms*

$$\mathrm{Tor}^A_i(M, N) \otimes_A B \cong \mathrm{Tor}^B_i(M \otimes_A B, N \otimes_A B)$$

for general A and M.

Proof. (1) First we treat the case $i = 0$ and M free. Tensoring a homomorphism $M \to N$ by B gives a map $\mathrm{Hom}_A(M, N) \to \mathrm{Hom}_B(M \otimes_A B, N \otimes_A B)$ which factors through a map $\mathrm{Hom}_A(M, N) \otimes_A B \to \mathrm{Hom}_B(M \otimes_A B, N \otimes_A B)$ since the target is a B-module. For $M = A$ this map identifies with the identity map of $N \otimes_A B$ and hence is an isomorphism. Using compatibility of the Hom and tensor product functors with finite direct sums we obtain an isomorphism when M is free.

Since M is finitely generated and A is Noetherian there exists a resolution $P_\bullet \to M$ with the P_i finitely generated and free. (Indeed, there is a surjection $p : P_0 \twoheadrightarrow M$ with a finitely generated free A-module P_0; since A is Noetherian, the kernel K of p is again finitely generated and we may repeat the process starting with K.) By flatness of B we have

$$\mathrm{Ext}^i_A(M, N) \otimes_A B = H^i(\mathrm{Hom}_A(P_\bullet, N)) \otimes_A B \cong H^i(\mathrm{Hom}_A(P_\bullet, N) \otimes_A B)$$

and by the previous paragraph the latter group identifies with

$$H^i(\mathrm{Hom}_B(P_\bullet \otimes_A B, N \otimes_A B)) = \mathrm{Ext}^i_B(M \otimes_A B, N \otimes_A B).$$

(2) The case of Tor is easier: take a projective resolution $P_\bullet \to M$. Then by flatness of B over A the complex $P_\bullet \otimes_A B$ is a projective resolution of $M \otimes_A B$ over B (in particular, each $P_i \otimes_A B$ is a direct summand of a free B-module), and so

$$\mathrm{Tor}_i^B(M \otimes_A B, N \otimes_A B) \cong H_i((P_\bullet \otimes_A B) \otimes_B (N \otimes_A B)) \cong$$
$$\cong H_i((P_\bullet \otimes_A N) \otimes_A B) \cong H_i(P_\bullet \otimes_A N) \otimes_A B \cong \mathrm{Tor}_i^A(M, N) \otimes_A B,$$

again using flatness of B over A. □

Proof of Proposition 6.10. First we prove that $\mathrm{gldim}(A_Q) \leq \mathrm{gldim}(A)$ for every maximal ideal $Q \subset A$. This is obvious when $\mathrm{gldim}(A)$ is infinite, so we may assume it is a finite number d. Then for every maximal Q the A-module $k := A/Q$ has a projective resolution $P_\bullet \to k$ of length $\leq d$. But then by flatness of A_Q over A the complex $P_\bullet \otimes_A A_Q$ is a projective resolution of $k \cong k \otimes_A A_Q$ over A_Q, and we conclude by Corollary 6.9.

On the other hand, suppose $\mathrm{gldim}(A) = d$ for some d. Then there are A-modules M, N such that $\mathrm{Ext}^d_A(M, N) \neq 0$; by Lemma 6.6 we may assume M is finitely generated. By Lemma 2.20 (1) we find a maximal ideal Q such that $\mathrm{Ext}^d_A(M, N) \otimes_A A_Q \neq 0$. Since A_Q is flat over A, Lemma 6.11 (1) gives $\mathrm{Ext}^d_{A_Q}(M \otimes_A A_Q, N \otimes_A A_Q) \neq 0$, so that $\mathrm{gldim}(A_Q) \geq d$ also holds. The same argument shows that $\mathrm{gldim}(A) = \infty$ implies that for any d we can find a maximal ideal Q with $\mathrm{gldim}(A_Q) \geq d$. □

We now state one of the most important results about homological dimension.

Theorem 6.12. (Serre) *A Noetherian local ring A is regular if and only if* $\mathrm{gldim}(A) < \infty$. *In this case* $\mathrm{gldim}(A) = \dim(A)$.

We shall give several proofs of Serre's theorem in these notes. The proof given in this section will use induction along regular sequences. In Section 8 we shall give a second proof of one implication and prove a refined statement using the Koszul complex. Finally, in Section 12 we shall present a recent proof that uses derived categories.

We begin with some auxiliary statements.

Proposition 6.13. *Let A be any ring, $x \in A$ a non-zerodivisor and M an $A/(x)$-module such that* $\mathrm{pd}_{A/(x)}(M) < \infty$. *Then* $\mathrm{pd}_A(M) = \mathrm{pd}_{A/(x)}(M) + 1$.

Proof. We proceed by induction on $\mathrm{pd}_{A/(x)}(M)$. If it is 0, then M is projective over $A/(x)$. Since x is a non-zerodivisor, we have a short exact sequence

$$0 \longrightarrow A \xrightarrow{\cdot x} A \longrightarrow A/(x) \longrightarrow 0\ .$$

This is a projective resolution of $A/(x)$ over A hence $\mathrm{pd}_A(A/(x)) \leq 1$. Now $\mathrm{pd}_A(A/(x)) = 0$ would mean that $A/(x)$ is projective over A, hence a direct summand of a free A-module F. That is impossible because x is a non-zerodivisor in A, hence in F but a zero-divisor on $A/(x)$. So $\mathrm{pd}_A(A/(x)) = 1$ and therefore $\mathrm{pd}_A(F) = 1$ for any free $A/(x)$-module F. This also implies $\mathrm{pd}_A(M) = 1$ since M is a direct summand of a free $A/(x)$-module.

For the inductive step assume $\mathrm{pd}_{A/(x)}(M) > 0$ and take an exact sequence of $A/(x)$-modules

$$0 \longrightarrow K \longrightarrow P \longrightarrow M \longrightarrow 0$$

where P is projective over $A/(x)$. We have two associated long exact Ext-sequences of the form

$$\mathrm{Ext}^i(P,N) \longrightarrow \mathrm{Ext}^i(K,N) \longrightarrow \mathrm{Ext}^{i+1}(M,N) \longrightarrow \mathrm{Ext}^{i+1}(P,N)\ , \tag{2}$$

one over $A/(x)$ and one over A. Over $A/(x)$ we have $\mathrm{Ext}^i(P,N) = 0$ for all $i > 0$ hence $\mathrm{Ext}^i_{A/(x)}(K,N) \cong \mathrm{Ext}^{i+1}_{A/(x)}(M,N)$ for all $i > 0$. This implies

$$\mathrm{pd}_{A/(x)}(M) = \mathrm{pd}_{A/(x)}(K) + 1. \tag{3}$$

By induction, we then have

$$\mathrm{pd}_A(K) = \mathrm{pd}_{A/(x)}(K) + 1. \tag{4}$$

On the other hand, over A we have $\mathrm{Ext}^i(P,N) = 0$ for all $i > 1$ as we have proven $\mathrm{pd}_A(P) = 1$ above. Hence $\mathrm{Ext}^i_A(K,N) \cong \mathrm{Ext}^{i+1}_A(M,N)$ for all $i > 1$. This gives

$$\mathrm{pd}_A(M) = \mathrm{pd}_A(K) + 1$$

provided that $\mathrm{pd}_A(M) > 1$. This proves the proposition for the case $\mathrm{pd}_A(M) > 1$.

To conclude, we show that $\mathrm{pd}_{A/(x)}(M) > 0$ implies $\mathrm{pd}_A(M) > 1$. Assume this is not the case, i.e. $\mathrm{pd}_A(M) = 1$. This implies $\mathrm{Ext}^i_A(M,N) = 0$ for $i > 1$ and all N. Since P is projective over $A/(x)$, we know it has projective dimension 1 over A, so $\mathrm{Ext}^i_A(P,N) = 0$ for $i > 1$ and all N as well. From the long exact sequence (2) we get $\mathrm{Ext}^2_A(K,N) = 0$ for all N, and therefore $\mathrm{pd}_A(K) \leq 1$. Here $\mathrm{pd}_A(K) = \mathrm{pd}_{A/(x)}(M)$ by equations (3) and (4). So we have to exclude the case $\mathrm{pd}_A(M) = \mathrm{pd}_{A/(x)}(M) = 1$.

Choose an exact sequence of A-modules

$$0 \longrightarrow C \longrightarrow F \longrightarrow M \longrightarrow 0$$

with F free. Then C is projective by Proposition 6.2 since $\mathrm{pd}_A(M) = 1$. So this is, in fact, a projective resolution of M. Tensoring the sequence with $A/(x)$ yields

$$\mathrm{Tor}_1^A(F, A/(x)) \longrightarrow \mathrm{Tor}_1^A(M, A/(x)) \longrightarrow C/xC \longrightarrow F/xF \longrightarrow M/xM \longrightarrow 0$$

where the first term is 0 because F is free and $M/xM = M$ since M is an $A/(x)$-module. Since C/xC and F/xF are already projective over $A/(x)$ and $\mathrm{pd}_{A/(x)}(M) = 1$, we get that $\mathrm{Tor}_1^A(M, A/(x))$ is projective over $A/(x)$ by Proposition 6.2 (applied with $d = 2 > 1$). By Proposition 5.5 we have $\mathrm{Tor}_1^A(M, A/(x)) = \{m \in M \mid xm = 0\} = M$, and therefore M is projective over $A/(x)$, a contradiction. □

Combining the proposition with Corollary 6.9 gives

Corollary 6.14. *If A is a Noetherian local ring with maximal ideal P, $x \in P$ is a non-zerodivisor and $\mathrm{gldim}(A/(x)) < \infty$, then*

$$\mathrm{gldim}(A) = \mathrm{gldim}(A/(x)) + 1.$$

We now prove a similar transition statement for A-modules.

Proposition 6.15. *Let A be a ring, M be an A-module and x a non-zerodivisor on both A and M. Then*

$$\mathrm{pd}_A(M) \geq \mathrm{pd}_{A/(x)}(M/xM)$$

If moreover A is a Noetherian local ring with maximal ideal P, M is finitely generated and $x \in P$, then equality holds.

Proof. We may assume $d := \mathrm{pd}_A(M) < \infty$. We proceed by induction on d. If $d = 0$, then M is projective over A and then so is M/xM over $A/(x)$. For $d > 0$, choose an exact sequence of A-modules

$$0 \longrightarrow K \longrightarrow F \longrightarrow M \longrightarrow 0 \qquad (5)$$

with F free. Then as in the previous proof $\mathrm{pd}_A(K) = d-1$ and hence $\mathrm{pd}_{A/(x)}(K/xK) \leq d-1$ by induction (note that since x is a non-zerodivisor on A, the same holds for F and hence K). Tensoring the above sequence by $A/(x)$ we get an exact sequence

$$\mathrm{Tor}_1^A(M, A/(x)) \longrightarrow K/xK \longrightarrow F/xF \longrightarrow M/xM \longrightarrow 0$$

where $\mathrm{Tor}_1^A(M, A/(x)) = \{m \in M \mid xm = 0\} = 0$ by Proposition 5.5. Therefore either $\mathrm{pd}(M/xM) = 0$ and the inequality holds trivially, or the argument with the long exact sequence of Ext gives $\mathrm{pd}_{A/(x)}(M/xM) = \mathrm{pd}_{A/(x)}(K/xK) + 1 \leq d$. The first statement is proven.

We prove the second statement by induction on $n = \mathrm{pd}_{A/(x)}(M/xM)$ starting with $n = 0$. In this case M/xM is projective over $A/(x)$, hence free by Proposition 2.15. We claim that M is also free over A, which will prove the case $n = 0$. Let $m_1, \ldots, m_r$ be a free generating system of M/xM over $A/(x)$. By Nakayama's lemma, it is also a generating system over A since $x \in P$. Now, assume that $a_1 m_1 + \cdots + a_r m_r = 0$

for some $a_i \in A$. We know that $a_i \in (x)$ since modulo (x) there is no nontrivial relation. Therefore we find $a_i' \in A$ with $a_i = a_i'x$ for all i and may rewrite the relation as $(a_1'm_1 + \cdots + a_r'm_r)x = 0$. Since x is a non-zerodivisor on M, this implies $a_1'm_1 + \cdots + a_r'm_r = 0$. But then $a_i' \in (x)$ and so, after repeating the argument infinitely many times, finally obtain $a_i \in \cap_n(x^n) \subset \cap_n P^n$ for all i. This gives $a_i = 0$ by Krull's Intersection Theorem.

For the inductive step assume $n > 0$. From the proof of the first statement we already know $\mathrm{pd}_{A/(x)}(M/xM) = \mathrm{pd}_{A/(x)}(K/xK) + 1$, and from exact sequence (5) we get $\mathrm{pd}_A(M) = \mathrm{pd}_A(K) + 1$ since $\mathrm{pd}_A(M) \geq n > 0$ by the first statement. We conclude by applying the inductive hypothesis to K. □

Before starting the proof of Serre's theorem we need to recall some basic facts about associated primes.

Facts 6.16. An *associated prime* in a ring A is a prime ideal $P \subset A$ such that $P = \{x \in A : ax = 0\}$ for some $a \in A$. Not every ideal of this form is a prime ideal but every such ideal is contained in an associated prime. Consequently the union of all associated primes is the set of zero-divisors in A. When A is Noetherian, there are only finitely many associated primes in A.

Proof of Theorem 6.12. Assume first A is regular. We proceed by induction on $d := \dim(A)$. If $d = 0$ then A is a field, so every A-module is free and the global dimension is 0. If $d > 0$, then let x be a non-zerodivisor in the maximal ideal P (take an element in a regular sequence). We know that $A/(x)$ is a regular local ring of dimension $d-1$. On the other hand $\mathrm{gldim}(A/(x)) = \mathrm{gldim}(A) - 1$ by Corollary 6.14 provided that $\mathrm{gldim}(A/(x)) < \infty$, but that is true by induction. By induction we also know that $\dim(A/(x)) = \mathrm{gldim}(A/(x))$, so $\mathrm{gldim}(A) < \infty$ and $\mathrm{gldim}(A) = \dim(A)$ follow.

For the converse we use induction on $\mathrm{gldim}(A)$. If it is zero, then all A-modules are projective, hence the finitely generated ones are free by Proposition 2.15. In particular, the module $k := A/P$ is free which is only possible if $A = k$, so A is regular of dimension 0.

If $\mathrm{gldim}(A) =: d > 0$, we prove first that there exists a non-zerodivisor $x \in P \setminus P^2$. For this it will be enough to show that P is not an associated prime of A, because then the existence of x will follow from the Prime Avoidance Lemma applied to P^2 and the associated primes of A. Suppose P is the annihilator of some $x \in A$. Sending 1 to x induces a homomorphism $A \to A$ with kernel P; let C be its cokernel. We thus have an exact sequence of A-modules

$$0 \to k \to A \to C \to 0.$$

Part of the associated long exact Tor-sequence reads

$$\mathrm{Tor}^A_{d+1}(C,k) \to \mathrm{Tor}^A_d(k,k) \to \mathrm{Tor}^A_d(A,k)$$

where $\mathrm{Tor}^A_d(A,k) = 0$ because A is a free A-module and $\mathrm{Tor}^A_d(k,k) \neq 0$ by Corollary 6.9. But then $\mathrm{Tor}^A_{d+1}(C,k) \neq 0$, contradicting the assumption $\mathrm{gldim}(A) = d$.

So let $x \in P \setminus P^2$ be a non-zerodivisor. Assume for a moment that we know that $\mathrm{gldim}(A/(x)) < \infty$. Then by Corollary 6.14 we have $\mathrm{gldim}(A/(x)) = \mathrm{gldim}(A) - 1$, so by induction $A/(x)$ is regular. Lifting a regular sequence generating P mod (x) and adding x we obtain a regular sequence generating P. This proves that A is regular.

We still have to justify that $\mathrm{gldim}(A/(x)) < \infty$ if $\mathrm{gldim}(A) < \infty$. In view of Proposition 6.8 we have to prove $\mathrm{pd}_{A/(x)}(k) < \infty$. Using the exact sequence

$$0 \longrightarrow P/(x) \longrightarrow A/(x) \longrightarrow k \longrightarrow 0$$

of $A/(x)$-modules we reduce to proving $\mathrm{pd}_{A/(x)}(P/(x)) < \infty$. By the second part of Proposition 6.15,

$$\mathrm{pd}_{A/(x)}(P/xP) = \mathrm{pd}_A(P) < \infty$$

But $P/(x)$ is not the same as P/xP. So to finish the proof we shall show that the exact sequence

$$0 \longrightarrow (x)/xP \longrightarrow P/xP \longrightarrow P/(x) \longrightarrow 0$$

splits. This will suffice, since then $P/(x)$, being a direct summand of P/xP, will also have finite projective dimension (use the Ext criterion provided by Proposition 6.2).

As $x \in P \setminus P^2$ there exist $x_2, \ldots, x_r \in P$ such that $x, x_2, \ldots, x_r$ modulo P^2 is a basis of P/P^2. Then $(x) \cap ((x_2, \ldots, x_r) + P^2) \subseteq xP$. Indeed, if not, then there would exist $y \in (x_2, \ldots, x_r) + P^2$ such that $y = xu$ where $u \in A \setminus P$ is a unit. However, then $x = u^{-1}y \in (x_2, \ldots, x_r) + P^2$, contradicting the choice of $(x_2, \ldots, x_r)$. Now consider the sequence of maps

$$P/(x) \overset{=}{\to} ((x)+(x_2,\ldots,x_r)+P^2)/(x) \overset{\cong}{\to} ((x_2,\ldots,x_r)+P^2)/((x)\cap((x_2,\ldots,x_r)+P^2)) \to$$
$$\to P/xP \to P/(x).$$

The composition is the identity as one can check, and we get the required splitting. □

Remark 6.17. Notice that if we knew that the statement of Corollary 6.14 holds without the assumption $\mathrm{gldim}(A/(x)) < \infty$, the whole last section of the above proof (and hence also Proposition 6.15) would be unnecessary.

This is what we shall prove in Section 12: more precisely, we shall construct a direct sum decomposition

$$\mathrm{Tor}^A_i(k,k) \cong \mathrm{Tor}^{A/(x)}_i(k,k) \oplus \mathrm{Tor}^{A/(x)}_{i-1}(k,k)$$

assuming only that A is local with residue field k (but assuming $x \notin P^2$ which is harmless), from which the required statement follows in the Noetherian case by Corollary 6.9.

7. Applications of Serre's theorem

We now discuss structural results for regular rings whose proof is enabled, or at least greatly simplified, by homological methods. We begin with the following statement whose non-homological proof is quite cumbersome.

Corollary 7.1. *Let A be a regular local ring and $Q \subset A$ a prime ideal. Then A_Q is also regular.*

Proof. Since $\mathrm{gldim}(A) < \infty$ by Serre's theorem, we have a projective resolution

$$0 \longrightarrow P_d \longrightarrow P_{d-1} \xrightarrow{\alpha} \dots \longrightarrow P_0 \longrightarrow A/Q \longrightarrow 0.$$

Tensoring by the flat module A_Q the sequence remains exact, and the $P_i \otimes_A A_Q$ are projective over A_Q (as direct summands of free modules). Moreover, $A/Q \otimes_A A_Q \cong A_Q/QA_Q$ which is the residue field of A_Q. Hence we get a finite free resolution for the residue field of A_Q over A_Q, whence we conclude by Corollary 6.9. □

Another consequence is:

Corollary 7.2. *A Noetherian local ring A is regular if and only if its completion $\widehat{A}$ (with respect to any ideal $I \subset A$) is regular.*

Proof. Since $\widehat{A}$ is flat over A, Lemma 6.11 (2) gives isomorphisms $\mathrm{Tor}_i^{\widehat{A}}(k,k) \cong \mathrm{Tor}_i^A(k,k) \otimes_A \widehat{A}$ for all i. Since moreover $\widehat{A}$ is faithfully flat over A (Proposition 2.9), we conclude that $\mathrm{Tor}_i^{\widehat{A}}(k,k) \neq 0$ if and only if $\mathrm{Tor}_i^A(k,k) \neq 0$. The corollary now follows from Theorem 6.12 and Corollary 6.9. □

Recall now that a Noetherian ring is *regular* if all of its localizations by maximal ideals are regular local rings. By the Corollary 7.1 this is the same as requiring that all localizations by prime ideals are regular local rings. Now combining Theorem 6.12 with Proposition 6.10 we obtain:

Corollary 7.3. *If A is a Noetherian ring of finite Krull dimension d, then A is regular if and only if* $\mathrm{gldim}(A) = d$.

In particular, since polynomial rings over fields are regular, we have:

Corollary 7.4. (Hilbert's Syzygy Theorem) *If k is a field, then* $\mathrm{gldim}(k[x_1, \dots, x_d]) = d$.

Remark 7.5. In fact, over $k[x_1, \dots, x_d]$ every finitely generated projective module is free. This was a conjecture of Serre, solved independently by Quillen and Suslin. Consequently, every finitely generated module over $k[t_1, \dots, t_d]$ has a finite free resolution.

The last classical result about regular rings is:

Theorem 7.6. (Auslander – Buchsbaum) *A regular local ring is a unique factorization domain.*

For the proof we need several auxiliary statements.

Lemma 7.7. *A Noetherian integral domain A is a unique factorization domain (UFD) if and only if every height 1 prime ideal in it is principal.*

For the proof recall the following basic criterion for unique factorization: a domain A is a UFD if and only if the principal ideals satisfy the ascending chain condition (this is automatic for A Noetherian) and every irreducible element is a prime. Here $p \in A$ is called irreducible if it cannot be written as a product of two non-units and a prime if (p) is a prime ideal.

Proof. If A is a unique factorization domain, every height 1 prime ideal P contains a prime element p (take a prime divisor of some nonzero $a \in P$), so that there is an inclusion $(p) \subseteq P$ of prime ideals which must be an equality since $\mathrm{ht}(P) = 1$. Conversely, if every height 1 prime ideal is principal and $p \in A$ is an irreducible element, take a minimal prime ideal P containing p. Since A is a domain, the Hauptidealsatz gives $\mathrm{ht}(P) = 1$. By assumption we then have $P = (a)$ for some $a \in A$ which must therefore divide p. As p is irreducible, we get $P = (p)$. □

Remark 7.8. The criterion of the lemma has an interesting geometric interpretation: for a local ring of some variety at a point P it means that every codimension 1 subvariety can be defined, at least locally around a point, by a single equation, or in other words by cutting with a hypersurface. Therefore the theorem will imply that this always holds around smooth points.

The next lemma is:

Lemma 7.9. (Nagata) If A is a Noetherian integral domain such that A_x is a unique factorization domain for some prime element $x \in A$, then A is a unique factorization domain.

Here A_x denotes the localization of A by the subset $\{1, x, x^2, x^3, \dots\}$.

Proof. We use the criterion of the previous lemma. Take a height 1 prime ideal $P \subseteq A$. If $x \in P$, then $P = (x)$ since (x) is a prime ideal and $\mathrm{ht}(P) = 1$, so we are done. So assume $x \notin P$. In this case the lemma shows that there exists $p \in P$ such that $PA_x = pA_x$. We may assume that $p \notin (x) \cap P$. Indeed, if $p = ax$ for some $a \in A$, then $a \in P$ as P is a prime ideal and $x \notin P$. If $a \in (x)$ we repeat the process, obtaining an ascending chain of prime ideals $(p) \subsetneq (a) \subsetneq (a_1) \subsetneq (a_2) \subsetneq \cdots$ which must stop at some ideal (a_i) as A is Noetherian. Here a_i is not contained in (x) but $pA_x = a_iA_x$, so we may replace p by a_i.

We now show $P = (p)$. So far we know that for all $y \in P$ there exists $a \in A$ and $m, n > 0$ such that $y/x^n = p(a/x^m)$ since A is a domain. This means that $x^k y \in (p)$ for big enough k, so it is enough to show that $xy \in (p)$ implies $y \in (p)$. If $xy = ap$, then $a \in (x)$ as (x) is a prime ideal and $p \notin (x)$. Therefore $a = bx$ for some b, hence $xy = ap = bxp$ and finally $y = bp$ because A is a domain. □

Next a lemma which is basically linear algebra.

Lemma 7.10. (Kaplansky) *If A is an integral domain and $I_1, \ldots, I_n, J_1, \ldots, J_n \subseteq A$ ideals such that*

$$\bigoplus_{i=1}^{n} I_i \cong \bigoplus_{i=1}^{n} J_i$$

as A-modules, then $I_1 \cdot \cdots \cdot I_n \cong J_1 \cdot \cdots \cdot J_n$ as A-modules.

The lemma is easiest to prove using exterior products, about which we recall some basics.

Facts 7.11. Let A be a ring, M an A-module and $n \geq 0$. The n-th exterior power (or wedge power) of M is defined by

$$\Lambda^n M := M^{\otimes n} / \langle m_1 \otimes \cdots \otimes m_n \mid \exists 1 \leq i < j \leq n : \; m_i = m_j \rangle$$

where $\Lambda^0 M = A$ and $\Lambda^1 M = M$. We denote the image of $m_1 \otimes \cdots \otimes m_n$ in $\Lambda^n M$ by $m_1 \wedge \cdots \wedge m_n$. The following properties hold:

(1) The A-module $\Lambda^n M$ is characterized by the following universal property: for all A-modules N and all n-linear maps $\varphi : M \times \cdots \times M \to N$ such that $\varphi(m_1, \ldots, m_n) = 0$ if $m_i = m_j$ for some $i \neq j$ there exists a factorization $M \times \cdots \times M \to \Lambda^n M \to N$ where the first map is the natural surjection.
(2) Every A-module map $M \to N$ induces maps $\Lambda^n M \to \Lambda^n N$ for all $n \geq 0$.
(3) There are natural associative product maps $\Lambda^n M \times \Lambda^m M \to \Lambda^{n+m} M$. These two properties follow from the corresponding properties of the tensor product.

(4) If B is an A-algebra, there are canonical isomorphisms

$$\Lambda^n(M \otimes_A B) \cong (\Lambda^i M) \otimes_A B.$$

Indeed, one checks that the right hand side verifies the universal property characterizing the left hand side.

(5) In $\Lambda^n M$ we have the relations for all i:

$$m_1 \wedge \cdots \wedge m_i \wedge m_{i+1} \wedge \cdots \wedge m_n = -\, m_1 \wedge \cdots \wedge m_{i+1} \wedge m_i \wedge \cdots \wedge m_n$$

(6) If $M \cong A^r$ is free with basis $e_1, \ldots, e_r$, then $\Lambda^n M$ is free with basis

$$\{e_{i_1} \wedge \cdots \wedge e_{i_n} \mid 1 \le i_1 < i_2 < \cdots < i_n \le r\};$$

in particular, for $r = n$ it is free of rank 1. If $v_1, \ldots, v_r$ are r elements in A^r, then $v_1 \wedge \cdots \wedge v_r = \det(a_{ij}) e_1 \wedge \cdots \wedge e_r$, where $[a_{ij}]$ is the matrix of the linear map $M \to M$ given by $e_i \mapsto v_i$ for $i = 1, \ldots, r$.

(7) For all A-modules M, N we have isomorphisms

$$\Lambda^n(M \oplus N) \cong \bigoplus_{i+j=n} \Lambda^i M \otimes \Lambda^j N.$$

(The isomorphism is induced by the maps $(m_1 \wedge \cdots \wedge m_i) \otimes (n_1 \wedge \cdots \wedge n_j) \mapsto m_1 \wedge \cdots \wedge m_i \wedge n_1 \wedge \cdots \wedge n_j$ for $m_i \in M$, $n_j \in N$. That this map is indeed an isomorphism is easy to verify in the case when M and N are free modules using the previous fact, and that will be the only case we'll need. For general M and N the argument is a bit more involved.)

Proof of Lemma 7.10. Let K be the fraction field of A, and put $M := I_1 \oplus \cdots \oplus I_n$. Then $M \otimes_A K \cong K^n$ since $I \otimes_A K = K$ for all ideals I. Therefore by property (4) above $\Lambda^n M \otimes_A K \cong \Lambda^n(M \otimes_A K) \cong K$ which, composed with the map $\Lambda^n M \to \Lambda^n M \otimes_A K$ given by $m \mapsto m \otimes 1$, gives a map $\phi : \Lambda^n M \to K$. We now describe $\mathrm{Im}(\phi) \subset K$. Let $e_1, \ldots, e_n$ be the standard basis of K^n coming from the isomorphism $M \otimes_A K \cong K^n$. Use property (6) above to write a generator $m_1 \wedge \cdots \wedge m_n$ of $\Lambda^n M$ as

$$m_1 \wedge \cdots \wedge m_n = \det(a_{ij}) e_1 \wedge \cdots \wedge e_n \in \Lambda^n K^n$$

with $a_{ij} \in I_i$ for all i, so that $\phi(m_1 \wedge \cdots \wedge m_n) = \det(a_{ij}) \in K$. Since $I_1 \cdot \cdots \cdot I_n = \langle \det(a_{ij}) \mid a_{ij} \in I_i \rangle \subseteq K$, we get $\mathrm{Im}(\phi) = I_1 \cdot \cdots \cdot I_n$. The same argument gives $\mathrm{Im}(\phi) = J_1 \cdot \cdots \cdot J_n$, whence the lemma. □

Finally, a homological input.

Lemma 7.12. (Serre) *If A is a ring and P is a projective A-module such that there exists a finite free resolution of length n, then P is stably free, i.e. there exist free modules F and F' such that $P \oplus F' \cong F$. If moreover A is Noetherian and P is finitely generated, then we may find finitely generated F and F'.*

Proof. Pick a resolution

$$0 \longrightarrow F_n \xrightarrow{\varphi_n} F_{n-1} \xrightarrow{\varphi_{n-1}} \dots \longrightarrow F_1 \xrightarrow{\varphi_1} F_0 \xrightarrow{\varphi_0} P \longrightarrow 0$$

where we may choose finitely generated F_i when A is Noetherian and P is finitely generated. As P is projective, the map φ_0 has a retraction, so $F_0 \cong P \oplus \mathrm{Im}(\varphi_1)$ and $\mathrm{Im}(\varphi_1)$ is projective. We can iterate this, obtaining $F_i \cong \mathrm{Im}(\varphi_i) \oplus \mathrm{Im}(\varphi_{i+1})$ for all i, hence finally

$$P \oplus F' := P \oplus \bigoplus_{i=1}^{n} \mathrm{Im}(\varphi_i) \cong P \oplus \bigoplus_{i \text{ odd}} F_i \cong \bigoplus_{i \text{ even}} F_i =: F$$

so the statement holds. □

Proof of Theorem 7.6. : Let A be a regular local domain of dimension d. We proceed by induction on $\dim(A)$, the case $\dim(A) = 0$ being clear. Pick an $x \in P \backslash P^2$. It is known that $A/(x)$ is again regular and local,hence an integral domain. This means that (x) is a prime ideal, so by Lemmas 7.7 and 7.9 it is enough to prove that every prime ideal $Q \subseteq A_x$ of height 1 is principal.

If M is a maximal ideal of A_x, then $(A_x)_M$ is the localization of A by the prime ideal $M \cap A$, hence it is also regular by Corollary 7.1. Here $\dim(A_x)_M < \dim A$ because $x \notin M$, so $M \cap A$ is not maximal. By induction $(A_x)_M$ is then a unique factorization domain. Hence $Q(A_x)_M$ is a principal ideal, since either $Q \subset M$ and then $Q(A_x)_M$ is still of height 1, or else $Q(A_x)_M = (1)$. In other words, $Q(A_x)_M$ is a free module of rank 1 over $(A_x)_M$. This being true for all maximal ideals $M \subset A_x$, we conclude from Proposition 2.19 that Q is projective as an A_x-module.

On the other hand, we know that $Q \cap A \subset A$ is a prime ideal satisfying $Q = (Q \cap A)A_x$. From Theorem 6.12 we also know that $Q \cap A$ considered as a finitely generated A-module has a finite free resolution. But then Q has a finite free resolution as well, since we can tensor the resolution of $Q \cap A$ with A_x. Therefore by Lemma 7.12 there exist m and n such that $Q \oplus (A_x)^m \cong (A_x)^n$. Here $m = n - 1$ because tensoring with $(A_x)_M$ gives $Q(A_x)_M \oplus (A_x)_M^m \cong (A_x)_M^n$ where we have seen above that $Q(A_x)_M$ is a free module of rank 1. Hence we can conclude by Lemma 7.10 applied with $I_1 = Q$, $I_i = A_x$ for $i = 2, \dots, n$ and $J_i = A_x$ for all $i = 1, \dots, n$. □

8. The Koszul complex

We now introduce a technical tool that is very useful for the study of regular sequences.

Definition 8.1. Let A be a commutative ring, M an A-module and $f : M \to A$ an A-linear map. The *Koszul complex* $K(f)$ of f is defined as

$$\dots \longrightarrow \Lambda^n M \xrightarrow{\mathrm{d}_f^{n-1}} \Lambda^{n-1} M \xrightarrow{\mathrm{d}_f^{n-2}} \dots \longrightarrow \Lambda^2 M \xrightarrow{\mathrm{d}_f^1} M \xrightarrow{\mathrm{d}_f^0} A ,$$

where $\mathrm{d}_f^0 = f$ and

$$\mathrm{d}_f^{n-1}(m_1 \wedge \dots \wedge m_n) = \sum_{i=1}^{n} (-1)^{i+1} \cdot f(m_i) \cdot m_1 \wedge \dots \wedge m_{i-1} \wedge m_{i+1} \wedge \dots \wedge m_n$$

Note that the map d_f^{n-1} exists by the universal property of the wedge product. It is straightforward to check that $\mathrm{d}_f^{n-1} \circ \mathrm{d}_f^n = 0$.

Remark 8.2. It follows from the definition that for $x \in \Lambda^i M$ and $y \in \Lambda^j M$ we have

$$\mathrm{d}_f^{i+j-1}(x \wedge y) = \mathrm{d}_f^{i-1}(x) \wedge y + (-1)^i x \wedge \mathrm{d}_f^{j-1}(y) \tag{6}$$

If we view the direct sum of the $\Lambda^n M$ as a graded A-algebra with multiplication induced by the wedge product, the d_f^{n-1} give it the structure of a *differential graded algebra*: a graded A-algebra equipped with an A-module endomorphism d sending the degree n part to the degree $n-1$ part and satisfying the compatibility above with respect to the multiplicative structure.

Example 8.3. Consider the case $M = A$. Every A-module homomorphism $f : A \to A$ is given by multiplication by the element $x := f(1)$. The Koszul complex of $K(f)$ is of the form $A \xrightarrow{x} A$, with $H_0(K(f)) \cong A/xA$. Moreover, $H_1(K(f)) \cong \ker(A \xrightarrow{x} A)$, so that $H_1(K(f)) = 0$ if and only if x is a non-zerodivisor.

Tensoring by a general A-module M we obtain

$$H_0(M \otimes_A K(f)) \cong M/xM, \quad H_1(M \otimes_A K(f)) \cong \ker(M \xrightarrow{x} M).$$

We shall be particularly interested in the case when $M = A^r$ is a free A-module of finite rank. In this case the Koszul complex of a map $A^r \to A$ has a particularly simple form which we now proceed to determine. We first need the notion of tensor products of complexes.

Definition 8.4. Let $C_\bullet$ and $D_\bullet$ two chain complexes of A-modules concentrated in nonnegative degrees in the homological numbering. Their tensor product $C \otimes D)\bullet$ is the complex whose degree n term of $(C \otimes D)_\bullet$ is given by

$$(C \otimes D)_n = \bigoplus_{i+j=n} C_i \otimes_A D_j$$

and the differential by the formula

$$d_n^{C \otimes D}(x \otimes y) = d_i^C(x) \otimes y + (-1)^i x \otimes d_j^D(y). \tag{7}$$

Remarks 8.5.
(1) One defines the tensor product of two cohomological complexes concentrated in nonnegative degrees in the same way.
(2) We note for later use that there are natural maps

$$H_i(C_\bullet) \otimes_A H_j(D_\bullet) \to H_{i+j}((C \otimes_A D)_\bullet)$$

defined as follows. If $x \in \ker(d_i^C)$ and $y \in \ker(d_j^D)$, then $x \otimes y$ defines an element in $\ker(d_{i+j}^{C\otimes D})$. If moreover $x = d_{i+1}^C(x')$ for some $x' \in C_{i+1}$, then $d_{i+j+1}^{C\otimes D}(x' \otimes y) = x \otimes y$, so we have a map $H_i(C_\bullet) \otimes_A \ker(d_j^D) \to \ker(d_{i+j}^{C\otimes D})$. By a similar argument it factors through the image of d_{j+1}^D to give a map on homology as stated.

Example 8.6. Let $f_1, f_2 : A \to A$ be two A-module homomorphisms. Then $K(f_1) \otimes K(f_2)$ is the complex

$$A \xrightarrow{\mathrm{d}_f^1} A \oplus A \xrightarrow{\mathrm{d}_f^0} A \tag{8}$$

where the differential d_f^0 is given by $(x, y) \mapsto f_1(x) + f_2(y)$ and d_f^1 by $x \otimes y \mapsto (f_1(x)y, -f_2(y)x)$. Here we have identified $A \otimes_A A$ with A via the multiplication map $x \otimes y \mapsto xy$.

Now consider the A-module map $(f_1, f_2) : A \oplus A \to A$. Since we have canonical isomorphisms $\Lambda^2(A \oplus A) \cong A \otimes_A A \cong A$ (see below or apply Fact 7.11 (6)), the associated Koszul complex $K(f_1, f_2)$ has the shape (8). Moreover, one checks that the differentials are the same as those described above, so we obtain an isomorphism $K(f_1) \otimes K(f_2) \cong K(f_1, f_2)$.

More generally, we have:

Proposition 8.7. *Given A-modules M, N and A-module maps $f_1 : M \to A$, $f_2 : N \to A$, set $f = (f_1, f_2) : M \oplus N \to A$.*

There is a canonical isomorphism $K(f) \cong K(f_1) \otimes K(f_2)$.

Proof. The corresponding terms of $K(f)$ and $K(f_1) \otimes K(f_2)$ are canonically isomorphic by Fact 7.11 (7). To show that the differentials are the same, notice that they are the same in degree 0, and in both cases they can be built out of d_0 using the formula $d(x \wedge y) = d(x) \wedge y + (-1)^i x \wedge dy$. □

Now consider $f = (f_1, \ldots, f_r) : A^r \to A$ and set $x_i := f_i(1)$. We then have $f(a_1, \ldots, a_r) = \Sigma_i a_i x_i$. Introduce the notation

$$K(\underline{x}) = K(x_1, \ldots, x_r) := K(f).$$

By Fact 7.11 (6) it is a complex of free A-modules of length r. The previous proposition gives:

Corollary 8.8. *With notation as above we have an isomorphism of complexes*

$$K(\underline{x}) \cong K(x_1) \otimes \cdots \otimes K(x_r).$$

Now we come to the main result of this section.

Theorem 8.9. *If $x_1, \ldots, x_r$ is a regular sequence in A, then $K(\underline{x})$ is acyclic in degrees > 0 and therefore defines a finite free resolution of $A/(x_1, \ldots, x_r)$.*

For the proof of the theorem we need:

Lemma 8.10. *If $C_\bullet$ is any complex of A-modules and $x \in A$, there exists an exact sequence of complexes*

$$0 \longrightarrow C_\bullet \longrightarrow C_\bullet \otimes_A K(x) \longrightarrow C_\bullet[-1] \longrightarrow 0 \tag{9}$$

where $(C_\bullet[-1])_i = C_{i-1}$. Moreover, in the corresponding long exact sequence

$$\ldots \longrightarrow H_i(C_\bullet) \longrightarrow H_i(C_\bullet \otimes_A K(x)) \longrightarrow H_{i-1}(C_\bullet) \longrightarrow H_{i-1}(C_\bullet) \longrightarrow \ldots$$

the map $H_{i-1}(C_\bullet) \to H_{i-1}(C_\bullet)$ is multiplication by $(-1)^{i-1}x$.

Proof. We know that $K(x) = A \xrightarrow{x} A$. Thus in the complex $C_\bullet \otimes K(x)$ the degree i term is

$$(C_\bullet \otimes K(x))_i = (C_i \otimes_A A) \oplus (C_{i-1} \otimes_A A) \cong C_i \oplus C_{i-1}$$

with the differential $C_i \oplus C_{i-1} \to C_{i-1} \oplus C_{i-2}$ given by

$$\begin{bmatrix} \partial & (-1)^{i-1}x \\ 0 & \partial \end{bmatrix}$$

where ∂ is the differential of $C_\bullet$. This differential is the middle vertical map in the commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & C_i & \longrightarrow & C_i \oplus C_{i-1} & \longrightarrow & C_{i-1} & \longrightarrow & 0 \\ & & \downarrow \partial & & \downarrow & & \downarrow \partial & & \\ 0 & \longrightarrow & C_{i-1} & \longrightarrow & C_{i-1} \oplus C_{i-2} & \longrightarrow & C_{i-2} & \longrightarrow & 0 \end{array}$$

whose rows assemble to the exact sequence of complexes (9). To compute the connecting homomorphism in the long exact sequence, we applying the Snake Lemma to the above diagram: take $\alpha \in \mathrm{Ker}(C_{i-1} \to C_{i-2})$, lift it to $(0, \alpha) \in C_i \oplus C_{i-1}$, map this element to $((-1)^{i-1}x\alpha, 0) \in C_{i-1} \oplus C_{i-2}$ by applying the matrix above and finally take the component in C_{i-1}. It is $(-1)^{i-1}x\alpha$ as stated. □

The long exact sequence of the lemma gives:

Corollary 8.11. *There exists an exact sequence*

$$0 \to H_i(C_\bullet)/xH_i(C_\bullet) \to H_i(C_\bullet \otimes_A K(x)) \to \mathrm{Ker}(H_{i-1}(C_\bullet) \xrightarrow{x} H_{i-1}(C_\bullet)) \to 0.$$

Proof of Theorem 8.9. We proceed by induction on r, the case $r = 1$ being Example 8.3. Moreover, applying the results of Example 8.3 to $M = H_{i-1}(C_\bullet)$ and $M = H_i(C_\bullet)$ we may rewrite the exact sequence of Corollary 8.11 as

$$0 \to H_0(H_i(C_\bullet) \otimes_A K(x)) \to H_i(C_\bullet \otimes_A K(x)) \to H_1(H_{i-1}(C_\bullet) \otimes_A K(x)) \to 0.$$

For the inductive step, set $C_\bullet = K(x_1, \dots, x_{r-1})$, yielding $K(\underline{x}) \cong C_\bullet \otimes_A K(x_r)$ in view of Proposition 8.7. By the inductive hypothesis $H_i(C_\bullet) = H_{i-1}(C_\bullet) = 0$ for all $i > 1$, so the above short exact sequence applied with $x = x_r$ gives $H_i(K(\underline{x})) = 0$ for all $i > 1$. We still need to compute $H_1(K(\underline{x}))$. Since $H_1(C_\bullet) = 0$, the above short exact sequence reduces to an isomorphism $H_1(K(\underline{x})) \cong H_1(H_0(C_\bullet) \otimes_A K(x_r))$, where $H_0(C_\bullet) \cong A/(x_1, \dots, x_{r-1})$. But then by Example 8.3

$$H_1(K(\underline{x})) \cong \mathrm{Ker}(A/(x_1, \dots, x_{r-1}) \xrightarrow{x_r} A/(x_1, \dots, x_{r-1})) \tag{10}$$

which is 0 since $\underline{x}$ is a regular sequence. □

When A is a Noetherian local ring, the converse of Theorem 8.9 also holds. In fact, the following is true:

Proposition 8.12. *If a sequence $\underline{x} = (x_1, \dots, x_r)$ contained in the maximal ideal P of a Noetherian local ring A satisfies $H_1(K(\underline{x})) = 0$, then it is a regular sequence.*

Proof. The case $r = 1$ is again Example 8.3, and for $r > 1$ we can use induction on r. Apply Corollary 8.11 with $C_\bullet := K(x_1, \dots, x_{r-1})$. Since $C_\bullet \otimes K(x_r) \cong K(\underline{x})$, the assumption $H_1(K(\underline{x})) = 0$ gives $H_1(C_\bullet)/x_r H_1(C_\bullet) = 0$. But $x_r \in P$, hence $H_1(C_\bullet) = 0$ by Nakayama's lemma. Therefore by induction $x_1, \dots, x_{r-1}$ is a regular sequence, and moreover x_r is a non-zerodivisor modulo $(x_1, \dots, x_{r-1})$ by the vanishing of $H_1(K(\underline{x}))$ and the isomorphism (10). □

Remark 8.13. The above proposition yields another proof of the fact that in a Noetherian local ring every permutation of a regular sequence is regular.

We shall use the theorem through the corollary:

Corollary 8.14. *If $I = (x_1, \dots, x_r)$ with the x_i forming a regular sequence, then*

$$\mathrm{Tor}_i^A(A/I, M) \cong H_i(K(\underline{x}) \otimes_A M)$$

$$\mathrm{Ext}^i_A(A/I, M) \cong H^i(\mathrm{Hom}(K(\underline{x}), M))$$

for all A-modules M.

Application 8.15. The corollary makes it possible to give a quick proof of one half of Serre's theorem: *If A is a regular local ring of dimension d, then A has global dimension d.*

Indeed, applying the first statement of the corollary with I the maximal ideal of A and M its residue field k, we obtain that $\mathrm{Tor}_i^A(k,k)$ is just the degree i term of $K(\underline{x})\otimes_A k$ for all i; indeed, the differentials $K(\underline{x})\otimes_A k$ are all 0 since the x_i map to 0 in k. But by construction of the Koszul complex the degree i term of $K(\underline{x})\otimes_A k$ is a k-vector space of dimension $\binom{d}{i}$; in particular it is nonzero for $i=d$ and 0 for $i>d$. Now apply Corollary 6.9.

We can use the above proof to give a 'numerical' criterion for a Noetherian local ring to be regular.

Corollary 8.16. *Let A be a Noetherian local ring with maximal ideal P and residue field k, and set $r := \dim_k P/P^2$. The ring A is regular if and only if $\mathrm{Tor}_i^A(k,k)$ is a k-vector space of dimension $\binom{r}{i}$ for all i.*

Proof. When A is regular of Krull dimension d, we have $r=d$ and we have seen the conclusion above. Conversely, if the dimension of $\mathrm{Tor}_i^A(k,k)$ is as in the statement, it is 0 for $i>r$, and we conclude from Corollary 6.9 and Serre's theorem. □

Remark 8.17. In the situation of the corollary there is a natural way to construct an isomorphism $\mathrm{Tor}_1^A(k,k)\cong k^r$, generalizing the argument in the regular case. This is done using *minimal resolutions:* a free resolution $F_\bullet \to M$ of a finitely generated A-module M is minimal if each F_i is finitely generated and $Z_i(F_\bullet)\subset PF_i$ for all i. It follows from the defining property that the differentials of the complex $F_\bullet\otimes_A k$ are all 0. One can construct $F_\bullet$ inductively. First one takes a k-basis $x_1,\dots,x_n$ of M/PM, sets $F_0=A^n$ and defines the map $F_0\to M$ by lifting the obvious map $F_0\to M/PM$. In the inductive step the same procedure is applied to $Z_i(F_\bullet)$ in place of M. For $M=k$ one starts with $F_0=A$ and then proceeds with a map $A^r\to A$ lifting the natural map $A^r\to P/P^2\cong k^r$. Thus indeed $\mathrm{Tor}_1^A(k,k)\cong H_1(F_\bullet\otimes_A k)\cong k^r$.

To sum up: $\mathrm{Tor}_1^A(k,k)$ always has the 'correct' dimension, it is some of the higher Tor's that differ in the non-regular case.

The isomorphisms $\mathrm{Tor}_i^A(k,k)\cong\Lambda^i\mathrm{Tor}_1^A(k,k)$ of Application 8.15 are part of an even stronger statement. Quite generally, for a module M over a ring A one can equip the direct sum

$$\Lambda^\bullet(M) := \bigoplus_{i=0}^{\infty}\Lambda^i(M)$$

with a product structure induced by the product maps of Fact 7.11 (3). The resulting A-algebra is the *exterior algebra* of M.

For A regular and $M = k$ we can consider the direct sum

$$\mathrm{Tor}_\bullet^A(k,k) := \bigoplus_{i=0}^{\infty} \mathrm{Tor}_i^A(k,k)$$

which, as an A-module (or k-vector space) identifies with $\Lambda^\bullet \mathrm{Tor}_1^A(k,k)$ by the above. On the other hand, the k-vector space $\mathrm{Tor}_\bullet^A(k,k)$ already carries a product structure which is compatible with the wedge product structure on $\Lambda^\bullet \mathrm{Tor}_1^A(k,k)$. We now explain the details. We shall need the easy lemma:

Lemma 8.18. *If P_1, P_2 are projective A-modules, then so is $P_1 \otimes_A P_2$.*

Proof. We have to show that $\mathrm{Hom}_A(P_1 \otimes_A P_2, \_\_)$ is an exact functor. But

$$\mathrm{Hom}_A(P_1 \otimes_A P_2, \_\_) \cong \mathrm{Hom}_A(P_1, \mathrm{Hom}_A(P_2, \_\_))$$

where the right hand side is a composition of two exact functors by assumption. □

Construction 8.19 (Internal product for Tor)**.** Let A be a commutative ring and R an A-algebra. We construct an associative A-linear multiplication

$$\mathrm{Tor}_i^A(R,R) \times \mathrm{Tor}_j^A(R,R) \to \mathrm{Tor}_{i+j}^A(R,R)$$

for all $i, j \geq 0$ called the *internal product*.

It will be enough to construct maps

$$\mathrm{Tor}_i^A(M_1,N_1) \times \mathrm{Tor}_j^A(M_2,N_2) \to \mathrm{Tor}_{i+j}^A(M_1 \otimes_A M_2, N_1 \otimes_A N_2) \tag{11}$$

for all A-modules M_1, M_2, N_1, N_2 (the *external product*). Indeed, setting $M_1 = M_2 = N_1 = N_2 = R$ and applying the multiplication map $R \otimes_A R \to R$ in both variables we then obtain the internal product.

Choose projective resolutions $P_\bullet^1 \to M_1$, $P_\bullet^2 \to M_2$, $P_\bullet \to M_1 \otimes_A M_2$. Recall that the groups $\mathrm{Tor}_i^A(M_1,N_1)$ and $\mathrm{Tor}_j^A(M_2,N_2)$ are computed by tensoring $P_\bullet^1$ by N_1 and $P_\bullet^2$ by N_2, respectively, and then taking homology. On the other hand, the tensor product complex $(P^1 \otimes_S P^2)_\bullet$ has projective terms by Lemmas 8.18 and 2.12 (2). Moreover, the maps $P_0^1 \to M_1$, $P_0^2 \to M_2$ induce a map $(P^1 \otimes_S P^2)_\bullet \to M_1 \otimes_A M_2$, so by Lemma 3.9 the identity map of $M_1 \otimes_A M_2$ induces a morphism of complexes $(P^1 \otimes_A P^2)_\bullet \to P_\bullet$. It follows that we have a morphism of complexes

$$(P_\bullet^1 \otimes_A N_1) \otimes_A (P_\bullet^2 \otimes_A N_2) \cong (P^1 \otimes_A P^2)_\bullet \otimes_A (N_1 \otimes_A N_2) \to P_\bullet \otimes_A (N_1 \otimes_A N_2) \tag{12}$$

On the other hand, by Remark 8.5 (2) we have a natural map

$$\mathrm{Tor}_i^A(M_1,N_1) \times \mathrm{Tor}_j^A(M_2,N_2) \to H_{i+j}((P_\bullet^1 \otimes_A N_1) \otimes_A (P_\bullet^2 \otimes_A N_2))$$

whence the external product (11) arises by composition with the map induced by (12) on H_{i+j}.

The above product has the following property (called *graded-commutativity*):

Proposition 8.20. *For $a \in \mathrm{Tor}_i^A(R,R)$ and $b \in \mathrm{Tor}_j^A(R,R)$ denote by $a \cdot b \in \mathrm{Tor}_{i+j}^A(R,R)$ their internal product. Then*

$$a \cdot b = (-1)^{ij} b \cdot a.$$

For the proof we need:

Lemma 8.21. *Let $C_\bullet$ be a homological complex. Taking $a \in C_i$ and $b \in C_j$ and sending $a \otimes b$ to $(-1)^{ij} b \otimes a$ induces a morphism of complexes $\tau : (C \otimes C)_\bullet \to (C \otimes C)_\bullet$.*

Proof. We have

$$\tau(d(a \otimes b)) = \tau(da \otimes b + (-1)^i a \otimes db) = (-1)^{(i-1)j} b \otimes da + (-1)^{i+i(j-1)} db \otimes a,$$

whereas

$$d(\tau(a \otimes b)) = d((-1)^{ij} b \otimes a) = (-1)^{ij} db \otimes a + (-1)^{ij+j} b \otimes da.$$

The two are equal since $(-1)^{ij} = (-1)^{i+i(j-1)}$ and $(-1)^{ij+j} = (-1)^{(i+1)j} = (-1)^{(i-1)j}$. □

Proof of Proposition 8.20. In the construction of the internal product take $P^1_\bullet = P^2_\bullet =: C_\bullet$. Then the map $\tau : (C \otimes C)_\bullet \to (C \otimes C)_\bullet$ of the lemma gives a morphism of complexes $(P^2 \otimes_A P^1)_\bullet \to (P^1 \otimes_A P^2)_\bullet$ which, composed with a morphism $(P^1 \otimes_A P^2)_\bullet \to P_\bullet$ given by Lemma 3.9, gives a morphism of complexes $(P^2 \otimes_A P^1)_\bullet \to P_\bullet$. By construction, the first morphism computes $a \otimes b$ and the second one $(-1)^{ij} b \otimes a$. □

Proposition 8.22. *Let A be a ring, $I \subset A$ an ideal generated by a regular sequence $x_1, \ldots, x_r$ and $R := A/I$. Then we have an isomorphism of graded R-algebras*

$$\Lambda^\bullet \mathrm{Tor}_1^A(R,R) \xrightarrow{\sim} \mathrm{Tor}_\bullet^A(R,R)$$

induced by the identity in degree 1 and the internal product on $\mathrm{Tor}_\bullet^A(R,R)$.

In particular, if A is a regular local ring with residue field k, we have an isomorphism of graded k-algebras

$$\Lambda^\bullet \mathrm{Tor}_1^A(k,k) \xrightarrow{\sim} \mathrm{Tor}_\bullet^A(k,k).$$

Proof. By Corollary 8.14 and the same argument as in Application 8.15 we have isomorphisms $\mathrm{Tor}_i^A(R,R) \cong H_i(K(\underline{x}) \otimes_A R) \cong \Lambda^i(R^r)$, where $K(\underline{x})$ is the associated Koszul complex. In particular, for $i = 1$ we get $H_1(K(\underline{x}) \otimes_A R) \cong R^r$, which yields isomorphisms $\Lambda^i \mathrm{Tor}_1^A(R,R) \xrightarrow{\sim} \mathrm{Tor}_i^A(R,R)$ for all i.

It remains to check that the wedge product maps

$$\Lambda^i \mathrm{Tor}_1^A(R,R) \times \Lambda^j \mathrm{Tor}_1^A(R,R) \to \Lambda^{i+j} \mathrm{Tor}_1^A(R,R) \tag{13}$$

become identified with the internal product maps

$$\mathrm{Tor}_i^A(R,R) \times \mathrm{Tor}_j^A(R,R) \to \mathrm{Tor}_{i+j}^A(R,R)$$

via the above isomorphism. Taking $P_\bullet^1 = P_\bullet^2 = K(\underline{x})$ in the construction of the internal product above, we have to consider the map $K(\underline{x}) \otimes_A K(\underline{x}) \to K(\underline{x})$ lifting the multiplication map $R \otimes_A R \to R$ whose existence is stipulated by Lemma 3.9. Such a morphism of complexes is given in degree n by the sum of the wedge product maps

$$\bigoplus_{i+j=n} \Lambda^i(A^r) \otimes \Lambda^j(A^r) \to \Lambda^n(A^r);$$

that they induce a morphism of complexes follows from comparing formulas (6) and (7). That this morphism of complexes induces the internal product on Tor follows from the uniqueness statement of Lemma 3.9; that it induces the map (13) results from the construction. □

9. THE HOMOTOPY CATEGORY AND ITS EXACT TRIANGLES

To start our work towards the construction of derived categories, we first present some auxiliary constructions for complexes in an abelian category $\mathcal{A}$ that are important in their own right. We denote the category of complexes in $\mathcal{A}$ by $C(\mathcal{A})$.

Construction 9.1. Given a morphism of complexes $f : A^\bullet \to B^\bullet$ in $C(\mathcal{A})$, the *cone* $C(f)$ of f is the complex with terms $C(f)^i = A^{i+1} \oplus B^i$ and differentials $d_f : C(f)^i \to C(f)^{i+1}$ given by the 2×2 matrix of morphisms

$$d_f = \begin{bmatrix} -d_A & 0 \\ f & d_B \end{bmatrix}$$

where d_A and d_B are the differentials of $A^\bullet$ and $B^\bullet$, respectively. (Thus for $\mathcal{A}$ the category of abelian groups, $a \in A^{i+1}, b \in B^i$ we have $d_f((a,b)) = (-d_A(a), f(a) + d_B(b))$.) This is indeed a complex because

$$\begin{bmatrix} -d_A & 0 \\ f & d_B \end{bmatrix}^2 = \begin{bmatrix} d_A \circ d_A & 0 \\ -f \circ d_A + d_B \circ f & d_B \circ d_B \end{bmatrix}$$

which is 0 because $A^\bullet, B^\bullet$ are complexes and f is a morphism of complexes.

Given a commutative diagram

$$\begin{array}{ccc} A^\bullet & \xrightarrow{f} & B^\bullet \\ \downarrow & & \downarrow \\ A'^\bullet & \xrightarrow{g} & B'^\bullet \end{array}$$

of morphisms in $C(\mathcal{A})$, there is an obvious induced morphism $C(f) \to C(g)$; this is the *functoriality of the cone construction.*

Quite generally for a complex $A^\bullet$ and $n \in \mathbf{Z}$ the shifted complex $A^\bullet[n]$ is defined by

$$A[n]^i := A^{i+n}, \quad d_{A[n]^\bullet} = (-1)^n d_{A^\bullet}.$$

With this notation we have an exact sequence of complexes

$$0 \to B^\bullet \to C(f) \to A^\bullet[1] \to 0. \tag{14}$$

Lemma 9.2. *Let $f : A^\bullet \to B^\bullet$ be a morphism in $C(\mathcal{A})$.*

(1) *The morphisms $H^{i+1}(A^\bullet) \to H^{i+1}(B^\bullet)$ in the long exact cohomology sequence of (14) equal $H^{i+1}(f)$.*
(2) *The morphism f is a quasi-isomorphism if and only if $C(f)$ is acyclic.*

Proof. For (1), we may assume $\mathcal{A}$ is a category of modules and take $a \in Z^i(A[1]^\bullet) = Z^{i+1}(A^\bullet)$. By the proof of Proposition 3.5 the image of its class in the long exact sequence can be constructed by lifting it to $(a, 0) \in C(f)^i$ and then taking $d_f((a, 0)) = -d_A(a) + f(a) = f(a)$, which indeed represents $H^{i+1}(f)(a)$. Statement (2) follows by the long exact cohomology sequence associated with (14). □

The other standard construction is:

Construction 9.3. Given a morphism of complexes $f : A^\bullet \to B^\bullet$ in $C(\mathcal{A})$, the *cylinder* $\mathrm{Cyl}(f)$ of f is the complex with terms $\mathrm{Cyl}(f)^i = A^{i+1} \oplus B^i \oplus A^i$ and differentials $d_{\mathrm{cyl}} : \mathrm{Cyl}(f)^i \to \mathrm{Cyl}(f)^{i+1}$ given by the 3×3 matrix of morphisms

$$d_{\mathrm{cyl}} = \begin{bmatrix} -d_A & 0 & 0 \\ f & d_B & 0 \\ \mathrm{id}_A & 0 & d_A \end{bmatrix}$$

where d_A and d_B are the differentials of $A^\bullet$ and $B^\bullet$, respectively. For $\mathcal{A}$ a category of modules we have the formula

$$d_{\mathrm{cyl}}(a_{i+1}, b_i, a_i) = (-d_A(a_{i+1}), f(a_{i+1}) + d_B(b_i), a_{i+1} + d_A(a_i)). \tag{15}$$

Note that

$$\mathrm{Cyl}(f) = C(C(f)[-1] \to A) \tag{16}$$

where the morphism $C(f)[-1] \to A^\bullet$ comes from (14) after shifting by -1; it is given by $(\mathrm{id}_A, 0)$. Indeed, the terms of the two complexes are equal and equality of the differentials can be read off the matrices. From this it follows that $\mathrm{Cyl}(f)$ is a complex (which can also be checked directly) and that there is an exact sequence

$$0 \to A^\bullet \to \mathrm{Cyl}(f) \to C(f) \to 0 \tag{17}$$

in $C(\mathcal{A})$, by combining (14) and (16).

The cylinder has important chain-homotopical properties:

Proposition 9.4. *Let $f: A^\bullet \to B^\bullet$ be a morphism of complexes.*

(1) *The natural map of complexes $i: B^\bullet \to \mathrm{Cyl}(f)$ induced by the inclusion of $B^\bullet$ in the second component gives a chain homotopy equivalence between $B^\bullet$ and $\mathrm{Cyl}(f)$.*
(2) *Another morphism of complexes $g: A^\bullet \to B^\bullet$ is homotopic to f if and only if there is a morphism of complexes $\mathrm{Cyl}(-\mathrm{id}_A) \to B^\bullet$ which composed with the natural inclusions $A^\bullet \to \mathrm{Cyl}(-\mathrm{id}_A)$ in the second and third component gives back f and g, respectively.*

Proof. For (1), define a morphism of complexes $p: \mathrm{Cyl}(f) \to B^\bullet$ by sending (a_{i+1}, b_i, a_i) to $-f(a_i) + b_i$. This is a morphism of complexes because

$$(p \circ d_{\mathrm{cyl}})(a_{i+1}, b_i, a_i) = f(a_{i+1}) + d_B(b_i) - f(a_{i+1}) - f(d_A(a_i)) = d_B(-f(a_i) + b_i).$$

By construction $p \circ i = \mathrm{id}_B$, and now we check $\mathrm{id}_{\mathrm{Cyl}(f)} - i \circ p = k \circ d_{\mathrm{cyl}} + d_{\mathrm{cyl}} \circ k$, where $k: \mathrm{Cyl}(f)^i \to \mathrm{Cyl}(f)^{i-1}$ is given by $k(a_{i+1}, b_i, a_i) = (a_i, 0, 0)$. Indeed,

$$(k \circ d_{\mathrm{cyl}})(a_{i+1}, b_i, a_i) = (a_{i+1} + d_A(a_i), 0, 0),$$

$$(d_{\mathrm{cyl}} \circ k)(a_{i+1}, b_i, a_i) = d_{\mathrm{cyl}}(a_i, 0, 0) = (-d_A(a_i), f(a_i), a_i);$$

on the other hand,

$$(a_{i+1}, b_i, a_i) - (0, -f(a_i) + b_i, 0) = (a_{i+1}, f(a_i), a_i).$$

For (2) suppose k induces a chain homotopy between f and g and consider the map $\mathrm{Cyl}(-\mathrm{id}) \to B^\bullet$ induced by the triple (k, f, g); it indeed gives back f and g after composing with the natural inclusions. We compute using formula (15) for $(a_{i+1}, \bar{a}_i, a_i) \in A^{i+1} \oplus A^i \oplus A^i$

$$((k, f, g) \circ d_{\mathrm{cyl}})((a_{i+1}, \bar{a}_i, a_i) = -(k \circ d_A)(a_{i+1}) - f(a_{i+1}) + f(d_A(\bar{a}_i)) + g(a_{i+1}) + g(d_A(a_i))$$

and

$$(d_B \circ (k, f, g))((a_{i+1}, \bar{a}_i, a_i) = (d_B \circ k)(a_{i+1}) + d_B(f(\bar{a}_i)) + d_B(g(a_i))$$

Since f and g are morphisms of complexes, equality of the two is equivalent to

$$g(a_{i+1}) - f(a_{i+1}) = (d_B \circ k + k \circ d_A)(a_{i+1})$$

which holds precisely because f and g are homotopic via k. The converse follows by reversing the argument. □

As a first application, note the following. Given an exact sequence

$$0 \to A^\bullet \to B^\bullet \to C^\bullet \to 0$$

in $C(\mathcal{A})$, we have a commutative diagram with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A^\bullet & \longrightarrow & \mathrm{Cyl}(f) & \longrightarrow & C(f) & \longrightarrow & 0 \\ & & {\scriptstyle \mathrm{id}}\big\downarrow & & {\scriptstyle -p}\big\downarrow & & {\scriptstyle h}\big\downarrow & & \\ 0 & \longrightarrow & A^\bullet & \xrightarrow{f} & B^\bullet & \xrightarrow{g} & C^\bullet & \longrightarrow & 0 \end{array}$$

where the upper row is (17), $p : (a_{i+1}, b_i, a_i) \to -f(a_i) + b_i$ is the homotopy inverse of i constructed in the above proof and h is the map induced on cokernels (explicitly, $h(a_{i+1}, b_i) = -g(b_i)$).

Corollary 9.5. *The map $h : C(f) \to C^\bullet$ is a quasi-isomorphism.*

Proof. This follows from Proposition 9.4 (1) and Corollary 3.7. □

Remark 9.6. In general h is not a homotopy equivalence, even though id and i are (see Remark 9.13 below).

We now come to a crucial definition:

Definition 9.7. The *homotopy category* $K(\mathcal{A})$ is the category with the same objects as $C(\mathcal{A})$ but with morphisms

$$\mathrm{Hom}_{K(\mathcal{A})}(A, B) := \mathrm{Hom}_{C(\mathcal{A})}(A, B)/\{\phi \in \mathrm{Hom}_{C(\mathcal{A})}(A, B) : \phi \sim 0\}$$

where $\sim$ denotes homotopy equivalence of morphisms of complexes. The quotient makes sense because the ϕ homotopic to 0 form a subgroup in $\mathrm{Hom}_{C(\mathcal{A})}(A, B)$. Composition is induced from composition of morphisms in $C(\mathcal{A})$.

Remark 9.8. The category $K(\mathcal{A})$ is additive but not abelian general. Example: let $\mathcal{A}$ be the category of abelian groups, and consider the morphism $\phi : \mathbf{Z} \to \mathbf{Z}/2\mathbf{Z}$ as a morphism in $C(\mathcal{A})$ of complexes concentrated in degree 0. This morphism has a kernel in $C(\mathcal{A})$, namely $2\mathbf{Z}$ viewed again as a complex, but not in $K(\mathcal{A})$. Indeed, if ϕ had a kernel in $K(\mathcal{A})$, it would be represented by $2\mathbf{Z}$ because every morphism $\mathbf{Z} \to A$ with A an abelian group induces a morphism in $K(\mathcal{A})$. Now consider the morphism of complexes ψ given by

$$\begin{array}{ccccccccccc} \cdots & \longrightarrow & 0 & \longrightarrow & \mathbf{Z} & \longrightarrow & \mathbf{Z}/2\mathbf{Z} & \longrightarrow & 0 & \longrightarrow & \cdots \\ & & \big\downarrow & & \big\downarrow & & \big\downarrow & & \big\downarrow & & \\ \cdots & \longrightarrow & 0 & \longrightarrow & \mathbf{Z} & \longrightarrow & 0 & \longrightarrow & 0 & \longrightarrow & \cdots \end{array}$$

Then $\phi \circ \psi \sim 0$, a homotopy being given by the identity of $\mathbf{Z}/2\mathbf{Z}$ in degree 1 and by the zero map elsewhere. Now if $2\mathbf{Z}$ were a kernel for ϕ, then ψ would factor through a morphism

$$\begin{array}{ccccccccccc} \cdots & \longrightarrow & 0 & \longrightarrow & \mathbf{Z} & \longrightarrow & \mathbf{Z}/2\mathbf{Z} & \longrightarrow & 0 & \longrightarrow & \cdots \\ & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \\ \cdots & \longrightarrow & 0 & \longrightarrow & 2\mathbf{Z} & \longrightarrow & 0 & \longrightarrow & 0 & \longrightarrow & \cdots \end{array}$$

in $K(\mathcal{A})$ but that's impossible (there is no such factorization in $C(\mathcal{A})$ and no homotopy to help as the only map $\mathbf{Z}/2\mathbf{Z} \to \mathbf{Z}$ is the zero map).

Since exact sequences do not make sense in $K(\mathcal{A})$ by the above remark, we consider a substitute. A *triangle* in $K(\mathcal{A})$ is a sequence of morphisms

$$A^\bullet \to B^\bullet \to C^\bullet \to A^\bullet[1]$$

in $K(\mathcal{A})$. The basic example to have in mind is the triangle

$$A^\bullet \to B^\bullet \to C(f) \to A^\bullet[1]$$

coming from (14). An *exact (or distinguished) triangle* in $K(\mathcal{A})$ is a triangle

$$A^\bullet \to B^\bullet \to C^\bullet \to A^\bullet[1]$$

for which there is a commutative diagram

$$\begin{array}{ccccccc} A^\bullet & \longrightarrow & B^\bullet & \longrightarrow & C^\bullet & \longrightarrow & A^\bullet[1] \\ \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \downarrow{\scriptstyle \alpha[1]} \\ A'^\bullet & \longrightarrow & B'^\bullet & \longrightarrow & C(f') & \longrightarrow & A'^\bullet[1] \end{array}$$

with some $f' : A'^\bullet \to B'^\bullet$ in $K(\mathcal{A})$ such that all vertical maps are isomorphisms in $K(\mathcal{A})$. (Note that, viewed as a diagram in $C(\mathcal{A})$, the squares only commute up to homotopy!). The following statements are more or less immediate from the definition:

Lemma 9.9.

(1) *The composition of any two consecutive maps in an exact triangle is 0 in $K(\mathcal{A})$.*
(2) *If $A^\bullet \to B^\bullet \to C^\bullet \to A^\bullet[1]$ is an exact triangle, there is an associated long exact sequence*

$$\cdots \to H^i(A^\bullet) \to H^i(B^\bullet) \to H^i(C^\bullet) \to H^{i+1}(A^\bullet) \to \cdots$$

in $\mathcal{A}$.

Proof. In (1) the triviality of the composite map $B^\bullet \to C^\bullet \to A^\bullet[1]$ follows from exact sequence (14), and that of $A^\bullet \to B^\bullet \to C^\bullet$ from exact sequence (17) and Proposition 9.4 (1). The sequence in (2) identifies with the long exact sequence associated with the exact sequence of complexes (17). □

The next lemma is a bit less straightforward.

Lemma 9.10.

(1) *A triangle*

$$A^\bullet \to B^\bullet \to C^\bullet \to A^\bullet[1]$$

in $K(\mathcal{A})$ is exact if and only if the shifted triangle

$$C^\bullet[-1] \to A^\bullet \to B^\bullet \to C^\bullet$$

is exact.

(2) *Given a commutative diagram*

$$\begin{array}{ccccccc} A^\bullet & \longrightarrow & B^\bullet & \longrightarrow & C^\bullet & \longrightarrow & A^\bullet[1] \\ \downarrow{\scriptstyle\alpha} & & \downarrow{\scriptstyle\beta} & & & & \downarrow{\scriptstyle\alpha[1]} \\ A'^\bullet & \longrightarrow & B'^\bullet & \longrightarrow & C'^\bullet & \longrightarrow & A'^\bullet[1] \end{array}$$

of exact triangles in $K(\mathcal{A})$, there is a morphism $\gamma : C^\bullet \to C'^\bullet$ in $K(\mathcal{A})$ making the diagram commute.

Proof. The 'if' part of (1) follows by applying the 'only if' part twice and shifting. So suppose $A^\bullet \xrightarrow{f} B^\bullet \to C^\bullet \to A^\bullet[1]$ is exact. We may assume $C^\bullet = C(f)$ and by Proposition 9.4 (1) we may replace $B^\bullet$ by $\mathrm{Cyl}(f)$ in $K(\mathcal{A})$. But

$$C(f)[-1] \to A^\bullet \to \mathrm{Cyl}(f)^\bullet \to C(f)$$

is an exact triangle by the isomorphism (16).

For statement (2) we may again assume $C^\bullet = C(f)$ (and similarly for $C'^\bullet$), whence the statement follows by functoriality of $C(f)$. □

The two statements of the proposition are parts of the general formalism of *triangulated categories*, an axiomatic theory extracted from properties of exact triangles in $K(\mathcal{A})$. To show the power of the formalism we derive some consequences.

Corollary 9.11.

(1) *For every object $X^\bullet$ in $K(\mathcal{A})$ applying the functor $\mathrm{Hom}_{K(\mathcal{A})}(X^\bullet, \_)$ to the first row of the diagram in Lemma 9.10 (2) induces an exact sequence of abelian groups*

$$\mathrm{Hom}_{K(\mathcal{A})}(X^\bullet, A^\bullet) \to \mathrm{Hom}_{K(\mathcal{A})}(X^\bullet, B^\bullet) \to \mathrm{Hom}_{K(\mathcal{A})}(X^\bullet, C^\bullet).$$

Similarly, applying the contravariant functor $\mathrm{Hom}_{K(\mathcal{A})}(\_\_, X^\bullet)$ *to the first row of the diagram in Lemma 9.10 (2) induces an exact sequence*

$$\mathrm{Hom}_{K(\mathcal{A})}(C^\bullet, X^\bullet) \to \mathrm{Hom}_{K(\mathcal{A})}(B^\bullet, X^\bullet) \to \mathrm{Hom}_{K(\mathcal{A})}(A^\bullet, X^\bullet).$$

(2) *If any two of the maps* α, β, γ *in Lemma 9.10 (2) are isomorphisms in* $K(\mathcal{A})$*, then so is the third one.*

Proof. The sequence of statement (1) is a complex by Lemma 9.9 (1), so assume $f : X^\bullet \to B^\bullet$ becomes 0 in $K(\mathcal{A})$ after composing with the map $B^\bullet \to C^\bullet$. Noting that $C(X^\bullet \to 0) = X^\bullet[1]$, we have a diagram of exact triangles

$$\begin{array}{ccccccc} X^\bullet & \longrightarrow & 0 & \longrightarrow & X^\bullet[1] & \xrightarrow{\mathrm{id}} & X^\bullet[1] \\ \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle 0} & & & & \downarrow{\scriptstyle f[1]} \\ B^\bullet & \longrightarrow & C^\bullet & \longrightarrow & A^\bullet[1] & \longrightarrow & B^\bullet[1]. \end{array} \tag{18}$$

By Lemma 9.10 (2) there is a map $X^\bullet[1] \to A^\bullet[1]$ making the diagram commute, so after shifting we obtain a map $X^\bullet \to A^\bullet$ whose composition with $A^\bullet \to B^\bullet$ is f. The proof of the contravariant case is similar.

To prove (2) it is enough to consider the case where α, β are isomorphisms by Lemma 9.10 (1). We apply the contravariant form of statement (1) with $X^\bullet = C^\bullet$ to the triangles in Lemma 9.10 (2). Combined with Lemma 9.10 (1) we obtain a commutative diagram with exact rows

$$\begin{array}{ccccccccc} \mathrm{Hom}(A^\bullet, C^\bullet) & \longleftarrow & \mathrm{Hom}(B^\bullet, C^\bullet) & \longleftarrow & \mathrm{Hom}(C^\bullet, C^\bullet) & \longleftarrow & \mathrm{Hom}(A^\bullet[1], C^\bullet) & \longleftarrow & \mathrm{Hom}(B^\bullet[1], C^\bullet) \\ \uparrow{\scriptstyle \alpha_*} & & \uparrow{\scriptstyle \beta_*} & & \uparrow{\scriptstyle \gamma_*} & & \uparrow{\scriptstyle \alpha_*[1]} & & \uparrow{\scriptstyle \beta_*[1]} \\ \mathrm{Hom}(A'^\bullet, C^\bullet) & \longleftarrow & \mathrm{Hom}(B'^\bullet, C^\bullet) & \longleftarrow & \mathrm{Hom}(C'^\bullet, C^\bullet) & \longleftarrow & \mathrm{Hom}(A'^\bullet[1], C^\bullet) & \longleftarrow & \mathrm{Hom}(B'^\bullet[1], C^\bullet). \end{array}$$

If α, β are isomorphisms, so are all vertical maps in the diagram by the five lemma, so there is $\gamma' : C'^\bullet \to C^\bullet$ in $K(\mathcal{A})$ with $\gamma' \circ \gamma = \mathrm{id}_{C'}$. This γ' makes the diagram

$$\begin{array}{ccccccc} A'^\bullet & \longrightarrow & B'^\bullet & \longrightarrow & C'^\bullet & \longrightarrow & A'^\bullet[1] \\ \downarrow{\scriptstyle \alpha^{-1}} & & \downarrow{\scriptstyle \beta^{-1}} & & \downarrow{\scriptstyle \gamma'} & & \downarrow{\scriptstyle \alpha^{-1}[1]} \\ A^\bullet & \longrightarrow & B^\bullet & \longrightarrow & C^\bullet & \longrightarrow & A^\bullet[1] \end{array}$$

commute, so repeating the argument gives $\gamma'' : C^\bullet \to C'^\bullet$ in $K(\mathcal{A})$ with $\gamma'' \circ \gamma' = \mathrm{id}_{C^\bullet}$. But then composing with γ on the right gives $\gamma'' = \gamma$, so γ' is an inverse of γ in $K(\mathcal{A})$. □

We can now prove a stronger form of Lemma 9.2 (2).

Corollary 9.12. *A morphism* $f : A^\bullet \to B^\bullet$ *in* $C(\mathcal{A})$ *is a homotopy equivalence if and only if* $C(f)$ *is homotopically trivial (i.e. the identity map of* $C(f)$ *is homotopic to 0).*

Proof. Apply the second statement of the previous corollary to the commutative diagram of exact triangles

$$\begin{array}{ccccccc} A^\bullet & \longrightarrow & A^\bullet & \longrightarrow & 0 & \longrightarrow & A^\bullet[1] \\ \big\downarrow{\scriptstyle \mathrm{id}} & & \big\downarrow{\scriptstyle f} & & \big\downarrow{\scriptstyle 0} & & \big\downarrow{\scriptstyle \mathrm{id}} \\ A^\bullet & \longrightarrow & B^\bullet & \longrightarrow & C(f) & \longrightarrow & A^\bullet[1] \end{array}$$

where the upper triangle is obtained by applying Lemma 9.10 (1) to the upper triangle in (18). □

Remark 9.13. We can now give an example showing that an exact sequence $0 \to A^\bullet \to B^\bullet \to C^\bullet \to 0$ in $C(\mathcal{A})$ does not necessarily give rise to an exact triangle $A^\bullet \to B^\bullet \to C^\bullet \to A^\bullet[1]$ in $K(\mathcal{A})$. Consider the exact sequence of abelian groups $0 \to \mathbf{Z}/2\mathbf{Z} \xrightarrow{f} \mathbf{Z}/4\mathbf{Z} \to \mathbf{Z}/2\mathbf{Z} \to 0$ viewed as an exact sequence of complexes concentrated in degree 0. We have $C(f) = [\mathbf{Z}/2\mathbf{Z} \to \mathbf{Z}/4\mathbf{Z}]$ which is indeed quasi-isomorphic to $[0 \to \mathbf{Z}/2\mathbf{Z}]$ via the natural projection p but not homotopy equivalent. Indeed, the only possible homotopy inverse could be the natural injection $i : [0 \to \mathbf{Z}/2\mathbf{Z}] \to C(f)$ which indeed satisfies $p \circ i = \mathrm{id}$, but $i \circ p : [\mathbf{Z}/2\mathbf{Z} \to \mathbf{Z}/4\mathbf{Z}] \to [\mathbf{Z}/2\mathbf{Z} \to \mathbf{Z}/4\mathbf{Z}]$ cannot be homotopic to the identity because it is not surjective in degree 0 and no homotopy induced by a map $\mathbf{Z}/4\mathbf{Z} \to \mathbf{Z}/2\mathbf{Z}$ can remedy that.

Now were there a map $g : \mathbf{Z}/2\mathbf{Z} \to \mathbf{Z}/2\mathbf{Z}[1]$ such that the triangle $\mathbf{Z}/2\mathbf{Z} \xrightarrow{f} \mathbf{Z}/4\mathbf{Z} \to \mathbf{Z}/2\mathbf{Z} \xrightarrow{g} \mathbf{Z}/2\mathbf{Z}[1]$ is isomorphic in $K(\mathcal{A})$ to some $A'^\bullet \xrightarrow{f'} B'^\bullet \to C(f') \to A'^\bullet[1]$, the isomorphisms identifying the sources and targets of f and f' would induce a map $C(f) \to C(f')$ in $K(\mathcal{A})$ by Lemma 9.10 (2) which would be an isomorphism by Corollary 9.11 (2). But $C(f') \cong \mathbf{Z}/2\mathbf{Z}$ by assumption whereas $C(f) \ncong \mathbf{Z}/2\mathbf{Z}$ by the above.

10. The derived category

There is another way of constructing the homotopy category, via *localization*.

Proposition 10.1. *Let $\mathcal{C}$ be a category and S a collection of morphisms in $\mathcal{C}$ containing all identity maps of objects and all compositions $s \circ t$ when $t \in \mathrm{Hom}_{\mathcal{C}}(A, B)$, $s \in \mathrm{Hom}_{\mathcal{C}}(B, C)$ are both in S.*

There is a category $S^{-1}\mathcal{C}$ and a functor $Q : \mathcal{C} \to S^{-1}\mathcal{C}$ such that

1. *For every $s \in S$ the morphism $Q(s)$ is an isomorphism;*
2. *Every functor $F : \mathcal{C} \to \mathcal{D}$ that sends the elements of S to isomorphisms in $\mathcal{D}$ factors uniquely through Q.*

The category $S^{-1}\mathcal{C}$ is called the *localization* of $\mathcal{C}$ with respect to S. The pair $(S^{-1}\mathcal{C}, Q)$ is unique up to unique isomorphism.

Proof. One construction is as follows. Let $S^{-1}\mathcal{C}$ have the same objects as $\mathcal{C}$. For two objects A, B we define $\mathrm{Hom}_{S^{-1}\mathcal{C}}(A, B)$ as follows. Consider all possible chains of morphisms $A \cdots \leftarrow\leftarrow\rightarrow \cdots \leftarrow\rightarrow\rightarrow \cdots B$ where leftward morphisms are in S. We let $\mathrm{Hom}_{S^{-1}\mathcal{C}}(A, B)$ be the quotient of this set by the coarsest equivalence relation containing the following equivalences:

(1) $A \cdots \xrightarrow{f}\xrightarrow{g} \cdots B \sim A \cdots \xrightarrow{g\circ f} \cdots B$;
(2) $A \cdots \xleftarrow{s}\xleftarrow{t} \cdots B \sim A \cdots \xleftarrow{s\circ t} \cdots B$;
(3) $A \cdots \xleftarrow{s}\xrightarrow{s} \cdots B \sim A \cdots \xrightarrow{\mathrm{id}} \cdots B$ for $s \in S$;
(4) $A \cdots \xleftarrow{s}\xrightarrow{f} \cdots B \sim A \cdots \xrightarrow{g}\xleftarrow{t} \cdots B$ whenever $g \circ s = t \circ f$.

Morphisms are composed in the obvious way and there is a natural functor Q from $\mathcal{C}$ to this category that sends elements of S to isomorphisms by property (3). It satisfies the universal property (send a chain to a composition of $F(s)^{-1}$'s and $F(f)$'s for each leftward s and rightward f in the chain). □

Lemma 10.2. *If $\mathcal{A}$ is an abelian category, then $K(\mathcal{A})$ is the localization of $C(\mathcal{A})$ by the collection of homotopy equivalences.*

Proof. Suppose $F : C(\mathcal{A}) \to \mathcal{D}$ is a functor sending homotopy equivalences to isomorphisms. Recall from Proposition 9.4 (1) that for each complex $A^\bullet$ the natural map $i : a \mapsto (0, a, 0)$ induces a homotopy equivalence between $A^\bullet$ and $\mathrm{Cyl}(-id_A)$ with homotopy inverse $p : (a_{i+1}, \bar{a}_i, a_i) \mapsto \bar{a}_i + a_i$. Thus $F(p) = F(i)^{-1}$.

Now consider the map $j : A^\bullet \to \mathrm{Cyl}(-\mathrm{id}_A)$ given by $a \mapsto (0, 0, a)$. We have $p \circ j = \mathrm{id}_A$, so

$$F(i) = F(i) \circ F(p \circ j) = F(i) \circ F(p) \circ F(j) = F(j).$$

Now suppose $f, g : A^\bullet \to B^\bullet$ are homotopic via a map k. By Proposition 9.4 (2) the map (k, f, g) induces a morphism of complexes $\phi : \mathrm{Cyl}(-id_A) \to B^\bullet$ with $\phi \circ i = f$, $\phi \circ j = g$. But then

$$F(f) = F(\phi) \circ F(i) = F(\phi) \circ F(j) = F(g)$$

which means that F factors through the homotopy category $K(\mathcal{A})$. □

Definition 10.3. The *derived category* $D(\mathcal{A})$ of an abelian category $\mathcal{A}$ is the localization of $C(\mathcal{A})$ with respect to the collection of quasi-isomorphisms of complexes.

Corollary 10.4. *One can also obtain $D(\mathcal{A})$ as the localization of $K(\mathcal{A})$ with respect to the collection of morphisms represented by quasi-isomorphisms of complexes.*

Proof. The universal functor $Q : C(\mathcal{A}) \to D(\mathcal{A})$ factors through $K(\mathcal{A})$ by Lemma 10.2 and satisfies the universal property for the collection of quasi-isomorphisms in $K(\mathcal{A})$ by definition. □

The description of morphisms in the derived category furnished by the general localization construction is impractical. Here is a notion which brings it closer to the calculus of fractions for rings.

Definition 10.5. A collection S of morphisms in a category $\mathcal{C}$ is a *multiplicative system* if it satisfies the following axioms.

(1) All identity morphisms of objects of A are in S and if $t \in \mathrm{Hom}_{\mathcal{C}}(A, B), s \in \mathrm{Hom}_{\mathcal{C}}(B, C)$ are both in S, so is $s \circ t$;
(2) Given $f \in \mathrm{Hom}_{\mathcal{C}}(A, B)$ and a morphism $s : A \to A'$ in S, there are morphisms $f' \in \mathrm{Hom}_{\mathcal{C}}(A', B')$ and $t : B \to B'$ in S making the diagram

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ {\scriptstyle s}\downarrow & & \downarrow{\scriptstyle t} \\ A' & \xrightarrow{f'} & B' \end{array}$$

commute. Similarly, if f' and t are given, we may complete the diagram with f and s.

Construction 10.6. Given a multiplicative system S of morphisms in a category $\mathcal{C}$, we construct a category $S^{-1}\mathcal{C}$ as follows. The objects of $S^{-1}\mathcal{C}$ are to be the same as those of $\mathcal{C}$. Morphisms in $S^{-1}\mathcal{C}$ are to be equivalence classes of pairs

$$A \xleftarrow{s} A_1 \xrightarrow{f} B$$

with $s \in S$, $f \in \mathrm{Hom}_{\mathcal{C}}(A_1, B)$, subject to the following equivalence relation: two pairs $A \xleftarrow{s_1} A_1 \xrightarrow{f_1} B$ and $A \xleftarrow{s_2} A_2 \xrightarrow{f_2} B$ are equivalent if there is a third such pair $A \xleftarrow{s_3} A_3 \xrightarrow{f_3} B$ fitting in a commutative diagram

$$\begin{array}{ccccc} A & \xleftarrow{s_1} & A_1 & \xrightarrow{f_1} & B \\ {\scriptstyle \mathrm{id}}\uparrow & & \uparrow & & \uparrow{\scriptstyle \mathrm{id}} \\ A & \xleftarrow{s_3} & A_3 & \xrightarrow{f_3} & B \\ {\scriptstyle \mathrm{id}}\downarrow & & \downarrow & & \downarrow{\scriptstyle \mathrm{id}} \\ A & \xleftarrow{s_2} & A_2 & \xrightarrow{f_2} & B. \end{array}$$

Composition of morphisms in $S^{-1}\mathcal{C}$ is defined as follows. Given $A \stackrel{s}{\leftarrow} A_1 \stackrel{f}{\rightarrow} B$ and $B \stackrel{t}{\leftarrow} B_1 \stackrel{g}{\rightarrow} C$, we first use property (2) of multiplicative systems to find a diagram

$$\begin{array}{ccccc} & & A' & \xrightarrow{f'} & B_1 & \xrightarrow{g} & C \\ & & {\scriptstyle t'}\downarrow & & \downarrow{\scriptstyle t} & & \\ A & \xleftarrow{s} & A_1 & \xrightarrow{f} & B. & & \end{array} \tag{19}$$

We then define the composite to be the equivalence class of $A \xleftarrow{s\circ t'} A' \xrightarrow{g\circ f'} C$. One checks that this composition rule indeed preserves equivalence classes.

Finally, define a functor $Q : \mathcal{C} \to S^{-1}\mathcal{C}$ to be the identity on objects and sending each morphism $f \in \mathrm{Hom}_{\mathcal{C}}(A, B)$ to the class of $A \stackrel{\mathrm{id}}{\leftarrow} A \stackrel{f}{\rightarrow} B$. This is indeed a functor because the composition of $A \stackrel{\mathrm{id}}{\leftarrow} A \stackrel{f}{\rightarrow} B$ and $B \stackrel{\mathrm{id}}{\leftarrow} B \stackrel{g}{\rightarrow} C$ is $A \stackrel{\mathrm{id}}{\leftarrow} A \xrightarrow{g\circ f} B$, as can be seen by taking $f' = f$ and $t' = \mathrm{id}$ in the above diagram.

Proposition 10.7 (Gabriel–Zisman)**.** *Together with the functor Q the category $S^{-1}\mathcal{C}$ constructed above is the localization of $\mathcal{C}$ with respect to S.*

Proof. We check the properties in Proposition 10.1. Property (1) follows because the two-sided inverse of the class of $A \stackrel{\mathrm{id}}{\leftarrow} A \stackrel{s}{\rightarrow} B$ is represented by $B \stackrel{s}{\leftarrow} A \stackrel{\mathrm{id}}{\rightarrow} A$. Property (2) holds, because if $F : \mathcal{C} \to \mathcal{D}$ sends the morphisms in S to isomorphisms, we may factor it uniquely through $S^{-1}\mathcal{C}$ by sending the class of $A \stackrel{s}{\leftarrow} A_1 \stackrel{f}{\rightarrow} B$ to $F(f) \circ F(s)^{-1}$. That this construction respects equivalence classes follows from the definition of the equivalence relation. For it to define a functor $S^{-1}\mathcal{C} \to \mathcal{D}$ we have to check that the composition of $A \stackrel{s}{\leftarrow} A_1 \stackrel{f}{\rightarrow} B$ and $B \stackrel{t}{\leftarrow} B_1 \stackrel{g}{\rightarrow} C$ is sent to $F(g \circ f') \circ F(s \circ t')^{-1}$, with f', t' as in diagram (19). This is because applying F to the diagram implies

$$F(g) \circ F(t)^{-1} \circ F(f) \circ F(s)^{-1} = F(g) \circ F(f') \circ F(t')^{-1} \circ F(s)^{-1}$$

and F preserves composition. □

Remarks 10.8.

1. Localization by a multiplicative system can also be defined using 'right fractions' represented by pairs of morphisms $A \stackrel{f}{\rightarrow} B_1 \stackrel{t}{\leftarrow} B$; the argument is similar. One can even combine the two and consider triples $A \stackrel{s}{\leftarrow} A_1 \stackrel{f}{\rightarrow} B_1 \stackrel{t}{\leftarrow} B$.

2. In the literature one usually finds an additional axiom for multiplicative systems called the cancellation property. It was not used in the above construction; it is necessary when one wants to prove the stronger property that the Hom-sets in the category $S^{-1}\mathcal{C}$ arise as *filtered direct limits* of Hom-sets in $\mathcal{C}$.

Proposition 10.9. *If S is a multiplicative system of morphisms in an additive category $\mathcal{A}$, then $S^{-1}\mathcal{A}$ is also additive.*

Sketch of proof. Given two morphisms $A \stackrel{s}{\leftarrow} A_1 \stackrel{f}{\to} B$ and $A \stackrel{s'}{\leftarrow} A_1' \stackrel{f'}{\to} B$, we define their sum by introducing a 'common denominator'. Apply axiom (2) of multiplicative systems to find a commutative diagram

$$\begin{array}{ccc} C & \xrightarrow{r'} & A_1 \\ {\scriptstyle r}\downarrow & & \downarrow{\scriptstyle s} \\ A_1' & \xrightarrow{s'} & A \end{array}$$

with $r \in S$. By axiom (1) $t := s' \circ r = s \circ r' \in S$ and we may represent the two morphisms above by the equivalent morphisms $A \stackrel{t}{\leftarrow} C \stackrel{f\circ r'}{\to} B$ and $A \stackrel{t}{\leftarrow} C \stackrel{f'\circ r}{\to} B$. Define their sum by the equivalence class of $A \stackrel{t}{\leftarrow} C \stackrel{f\circ r' + f'\circ r}{\longrightarrow} B$. One checks that this definition is well posed and the axioms for an additive category hold (0 and $A \oplus B$ are the same objects as in A). □

Now we apply the above to the derived category.

Proposition 10.10. *Let $\mathcal{A}$ be an abelian category and let $K(\mathcal{A})$ be the associated homotopy category. The collection of quasi-isomorphisms in $K(\mathcal{A})$ is a multiplicative system.*

Consequently, every morphism in $D(\mathcal{A})$ can be represented by a pair $A \stackrel{s}{\leftarrow} A_1 \stackrel{f}{\to} B$ with s a quasi-isomorphism and f a morphism in $K(\mathcal{A})$.

Proof of Proposition 10.10. We only have to check property (2) of multiplicative systems. Assume given morphisms $f : A^\bullet \to B^\bullet$ and $s : A^\bullet \to A'^\bullet$ in $K(\mathcal{A})$, with s a quasi-isomorphism. Using Lemma 9.10 (1) we have an exact triangle

$$C(s)[-1] \stackrel{g}{\to} A^\bullet \to A'^\bullet \to C(s)$$

which, using Lemma 9.10 (2), can be inserted in a commutative diagram of exact triangles

$$\begin{array}{ccccccc} C(s)[-1] & \xrightarrow{g} & A^\bullet & \xrightarrow{s} & A'^\bullet & \longrightarrow & C(s)^\bullet \\ \downarrow{\scriptstyle \mathrm{id}} & & \downarrow{\scriptstyle f} & & \downarrow & & \downarrow{\scriptstyle \mathrm{id}} \\ C(s)[-1] & \xrightarrow{f\circ g} & B^\bullet & \longrightarrow & C(f\circ g) & \longrightarrow & C(s). \end{array}$$

We claim that the middle square of the diagram is the one we were looking for (in particular we may take $B' = C(f \circ g)$). For this we have to check that the map $B^\bullet \to C(f \circ g)$ in the lower triangle is a quasi-isomorphism. Since s is a quasi-isomorphism, the cone $C(s)$ is acyclic by Lemma 9.2, but then the long exact sequence associated with the lower triangle implies the claim. The proof for the other part of the square is similar. □

Corollary 10.11. *The derived category $D(\mathcal{A})$ is additive.*

Proof. This follows from the two previous propositions. □

For all $i \in \mathbf{Z}$ the functors $H^i : C(\mathcal{A}) \to \mathcal{A}$ given by $A^\bullet \mapsto H^i(A^\bullet), f \mapsto H^i(f)$ map quasi-isomorphisms to isomorphisms by definition, so by the universal property of localization induce functors $H^i : D(\mathcal{A}) \to \mathcal{A}$. Also, as in $K(\mathcal{A})$, define an *exact triangle in* $D(\mathcal{A})$ to be a triangle isomorphic in $D(\mathcal{A})$ to a triangle of the form $A^\bullet \to B^\bullet \to C(f) \to A^\bullet[1]$. Then the statements of Lemmas 9.9 and 9.10 and their corollaries all hold for exact triangles in $D(\mathcal{A})$. But notice a new feature:

Corollary 10.12. *An exact sequence*

$$0 \to A^\bullet \to B^\bullet \to C^\bullet \to 0$$

in $C(\mathcal{A})$ gives rise to an exact triangle

$$A^\bullet \to B^\bullet \to C^\bullet \to A^\bullet[1]$$

in $D(\mathcal{A})$.

Proof. This follows from Corollary 9.5. □

Construction 10.13. Important exact triangles in $D(\mathcal{A})$ coming from the above corollary are constructed as follows. Given a complex $A^\bullet$ in $C(\mathcal{A})$, define its *(canonical) truncations* in degree n by

$$\tau_{\leq n}(A^\bullet) := [\cdots \to A^i \to A^{i+1} \to \cdots \to A^{n-1} \to Z^n(A^\bullet) \to 0 \to 0 \to \cdots]$$

and

$$\tau_{\geq n}(A^\bullet) := [\cdots \to 0 \to 0 \to A^n/B^n(A^\bullet) \to A^{n+1} \to \cdots \to A^i \to A^{i+1} \to \cdots]$$

By definition, there are natural morphisms of complexes $\tau_{\leq n}(A^\bullet) \to A^\bullet$ and $A^\bullet \to \tau_{\geq n}(A^\bullet)$ which are quasi-isomorphisms in degrees $\leq n$ and $\geq n$, respectively, and zero maps elsewhere (notice that $H^n(\tau_{\leq n}(A^\bullet)) = H^n(\tau_{\geq n}(A^\bullet) = H^n(A^\bullet)$.) Also, given a quasi-isomorphism $A^\bullet \to B^\bullet$, the induced maps $\tau_{\leq n}(A^\bullet) \to \tau_{\leq n}(B^\bullet)$ and $\tau_{\geq n}(A^\bullet) \to \tau_{\geq n}(B^\bullet)$ are quasi-isomorphisms as well. Thus $\tau_{\leq n}$ and $\tau_{\geq n}$ induce functors $D(\mathcal{A}) \to D(\mathcal{A})$.

Now for each n we have an exact sequence of complexes

$$0 \to \tau_{\leq n-1}(A^\bullet) \to \tau_{\leq n}(A^\bullet) \to [A^{n-1}/Z^{n-1}(A^\bullet) \to Z^n(A^\bullet)] \to 0$$

where the last complex is concentrated in degrees $n-1$ and n. The natural morphism of complexes

$$[A^{n-1}/Z^{n-1}(A^\bullet) \to Z^n(A^\bullet)] \to [0 \to H^n(A^\bullet)]$$

(where the second complex is placed in the same degrees) is a quasi-isomorphism. Thus using the above corollary we have an exact triangle

$$\tau_{\leq n-1}(A^\bullet) \to \tau_{\leq n}(A^\bullet) \to H^n(A^\bullet)[-n] \to \tau_{\leq n-1}(A^\bullet)[1] \tag{20}$$

in $D(\mathcal{A})$, where $H^n(A^\bullet)$ is considered as a complex concentrated in degree 0.

Similarly, there is an exact triangle

$$H^n(A^\bullet)[-n] \to \tau_{\geq n}(A^\bullet) \to \tau_{\geq n+1}(A^\bullet) \to H^n(A^\bullet)[-n+1]. \tag{21}$$

coming from the exact sequence of complexes

$$0 \to [A^n/B^n(A^\bullet) \to B^{n+1}(A^\bullet)] \to \tau_{\geq n}(A^\bullet) \to \tau_{\geq n+1}(A^\bullet) \to 0.$$

These exact triangles are very useful in inductive arguments on complexes.

Remark 10.14. Given a morphism $A^\bullet \to B^\bullet$ in $D(\mathcal{A})$, we may insert it in an exact triangle $A^\bullet \to B^\bullet \to C^\bullet \to A^\bullet[1]$ in $D(\mathcal{A})$ as follows. First we represent the morphism by a pair $A^\bullet \stackrel{s}{\leftarrow} A_1^\bullet \stackrel{f}{\to} B^\bullet$ of morphisms in $K(\mathcal{A})$ with s a quasi-isomorphism. Setting $C^\bullet := C(f)$ we have an exact triangle $A_1^\bullet \stackrel{f}{\to} B^\bullet \stackrel{g}{\to} C^\bullet \stackrel{h}{\to} A_1^\bullet[1]$ in $K(\mathcal{A})$, hence in $D(\mathcal{A})$, and we may construct a triangle $A^\bullet \to B^\bullet \stackrel{g}{\to} C^\bullet \stackrel{h}{\to} A^\bullet[1]$ isomorphic to it in $D(\mathcal{A})$ via s and the identity maps. Note that $C^\bullet$ is unique up to isomorphism in $D(\mathcal{A})$ but not up to unique isomorphism. One sometimes calls $C^\bullet$ *a cone* of the morphism $A^\bullet \to B^\bullet$ in $D(\mathcal{A})$.

Using the above remark we can verify:

Corollary 10.15. *A morphism $\phi : A^\bullet \to B^\bullet$ in $D(\mathcal{A})$ is an isomorphism in $D(\mathcal{A})$ if and only if it induces isomorphisms $H^i(\phi) : H^i(A^\bullet) \to H^i(B^\bullet)$ for all i.*

Note that the corollary does *not* imply that ϕ comes from a quasi-isomorphism in $C(\mathcal{A})$!

Proof. The 'only if' part follows because the H^i are functors on $D(\mathcal{A})$. Assume now the $H^i(\phi)$ are all isomorphisms, and let $C^\bullet$ be a cone of ϕ as in the above remark. Then $H^i(C^\bullet) = 0$ for all i, and so the map $0 \to C^\bullet$ in $C(\mathcal{A})$ induces an isomorphism in $D(\mathcal{A})$. In the commutative diagram of exact triangles

$$\begin{array}{ccccccc}
A^\bullet & \xrightarrow{\text{id}} & A^\bullet & \longrightarrow & 0 & \longrightarrow & A^\bullet[1] \\
\Big\downarrow{\scriptstyle \text{id}} & & \Big\downarrow{\scriptstyle \phi} & & \Big\downarrow & & \Big\downarrow{\scriptstyle \text{id}} \\
A^\bullet & \xrightarrow{\phi} & B^\bullet & \longrightarrow & C^\bullet & \longrightarrow & A^\bullet[1]
\end{array}$$

three of the vertical maps are then isomorphisms, and hence so is ϕ. □

Now consider full subcategories of $C(\mathcal{A})$ defined as follows: $C^+(\mathcal{A})$ is the full subcategory spanned by objects $A^\bullet$ such that $A^i = 0$ for all $i \ll 0$. Similarly, $C^-(\mathcal{A})$

is spanned by objects $A^\bullet$ with $A^i = 0$ for all $i \gg 0$ and $C^b(\mathcal{A})$ is spanned by objects with $A^i \neq 0$ for all but finitely many i. Denote their respective essential images in $K(\mathcal{A})$ and $D(\mathcal{A})$ by $K^+(\mathcal{A})$, $K^-(\mathcal{A})$ and $K^b(\mathcal{A})$ as well as $D^+(\mathcal{A})$, $D^-(\mathcal{A})$ and $D^b(\mathcal{A})$. Here the essential image of a functor $F : \mathcal{C} \to \mathcal{D}$ is defined as the full subcategory of $\mathcal{D}$ spanned by objects D isomorphic in $\mathcal{D}$ to some $F(C)$ with C an object of $\mathcal{C}$; we apply this notion with F the natural functors $C(\mathcal{A}) \to K(\mathcal{A})$ and $C(\mathcal{A}) \to D(\mathcal{A})$.

Lemma 10.16. *The category $D^+(\mathcal{A})$ is the full subcategory of $D(\mathcal{A})$ spanned by objects $A^\bullet$ such that $H^i(A^\bullet) = 0$ for all $i \ll 0$; similar statements hold for $D^-(\mathcal{A})$ and $D^b(\mathcal{A})$.*

Proof. If $H^i(A^\bullet) = 0$ for $i < n$, then the natural morphism $A^\bullet \to \tau_{\geq n}(A^\bullet)$ is an isomorphism in $D(\mathcal{A})$, and by definition $\tau_{\geq n}(A^\bullet)$ is in the essential image of $C^+(\mathcal{A})$ in $D(\mathcal{A})$. The other proofs are similar. □

Recall now that two categories $\mathcal{C}$ and $\mathcal{D}$ are *equivalent* if there are functors $F : \mathcal{C} \to \mathcal{D}$ and $G : \mathcal{D} \to \mathcal{C}$ such that $F \circ G \cong \mathrm{id}_{\mathcal{D}}$ and $G \circ F \cong \mathrm{id}_{\mathcal{C}}$ as functors. Here F is called a *quasi-inverse* for G and vice versa.

Lemma 10.17. *The category $D^+(\mathcal{A})$ is equivalent to the localization of $K^+(\mathcal{A})$ with respect to the collection of quasi-isomorphisms in $K^+(\mathcal{A})$. Similar statements hold for $D^-(\mathcal{A})$ and $D^b(\mathcal{A})$.*

Proof. Denote by S_+ the collection of quasi-isomorphisms in $K^+(\mathcal{A})$. The natural functor $K^+(\mathcal{A}) \to D^+(\mathcal{A})$ maps the elements in S_+ to isomorphisms in $D(\mathcal{A})$, hence factors through a functor $S_+^{-1}K^+(\mathcal{A}) \to D^+(\mathcal{A})$. We construct a quasi-inverse as follows. For every object $A^\bullet$ in $D^+(A)$ the natural map $\phi_A : A^\bullet \to \tau_{\geq n}(A^\bullet)$ is an isomorphism in $D(\mathcal{A})$ for suitable n; we fix such an isomorphism ϕ_A for each $A^\bullet$. Given a morphism $\phi : A^\bullet \to B^\bullet$ in $D^+(A)$, the composite $\phi_B \circ \phi \circ \phi_A^{-1}$ can be represented by a pair $\tau_{\geq n}(A^\bullet) \xrightarrow{f} B_1^\bullet \xleftarrow{t} \tau_{\geq m}(B^\bullet)$ of morphisms in $K(\mathcal{A})$ by Remark 10.8 (1). Since t is a quasi-isomorphism here, the canonical map $t_1 : B_1^\bullet \to \tau_{\geq m}(B_1^\bullet)$ must be a quasi-isomorphism as well. So the pair $\tau_{\geq n}(A^\bullet) \xrightarrow{t_1 \circ f} \tau_{\geq m}(B_1)^\bullet \xleftarrow{t_1 \circ t} \tau_{\geq m}(B^\bullet)$ represents the same morphism in $D(\mathcal{A})$ but in fact represents a morphism in $S_+^{-1}K^+(\mathcal{A})$. Sending $A^\bullet$ to $\tau_{\geq n}(A^\bullet)$ and ϕ to the above morphism gives the required quasi-inverse. □

Assume now $\mathcal{A}$ has enough projectives and define $K^-(\mathcal{P})$ to be the full subcategory of $K^-(\mathcal{A})$ spanned by complexes with projective terms. Similarly, if $\mathcal{A}$ has enough injectives, define $K^+(\mathcal{I})$ to be the full subcategory of $K^+(\mathcal{A})$ spanned by complexes with injective terms.

Proposition 10.18. *If $\mathcal{A}$ has enough projectives, the composite functor*

$$K^-(\mathcal{P}) \to K^-(\mathcal{A}) \xrightarrow{Q} D^-(\mathcal{A})$$

induces an equivalence of categories between $K^-(\mathcal{P})$ and $D^-(\mathcal{A})$.

Similarly, if $\mathcal{A}$ has enough injectives, we have an equivalence of categories between $K^+(\mathcal{I})$ and $D^+(\mathcal{A})$.

We need a lemma.

Lemma 10.19. *Assume $\mathcal{A}$ has enough projectives (resp. injectives).*

(1) *Every complex $C^\bullet$ in $C^-(\mathcal{A})$ is quasi-isomorphic to a complex $P^\bullet$ with projective terms.*

Similarly, every complex in $C^+(\mathcal{A})$ is quasi-isomorphic to a complex $I^\bullet$ with injective terms.

(2) *An acyclic complex in $C^-(\mathcal{A})$ with projective terms is homotopically trivial, and so is an acyclic complex in $C^+(\mathcal{A})$ with injective terms.*

Proof. We postpone the proof of (1) to the end of this section. As for (2) in the projective case, notice that an acyclic complex $A^\bullet$ breaks up in short exact sequences $0 \to B^i(A^\bullet) \to A^i \to B^{i+1}(A^\bullet) \to 0$ for all i. If n is the largest index for which $A^n \neq 0$, we have $A^n = B^n(A^\bullet)$; in particular, $B^n(A^\bullet)$ is projective and the above sequence for $i = n-1$ splits as a direct sum $A^{n-1} \cong B^{n-1}(A^\bullet) \oplus B^n(A^\bullet)$. But then $B^{n-1}(A^\bullet)$ is also projective, so continuing inductively we have decompositions $A^i \cong B^i(A^\bullet) \oplus B^{i+1}(A^\bullet)$ for all i. Now $\begin{bmatrix} 0 & 0 \\ \mathrm{id}_{B^i} & 0 \end{bmatrix} : B^i(A^\bullet) \oplus B^{i+1}(A^\bullet) \to B^{i-1}(A^\bullet) \oplus B^i(A^\bullet)$ induces the required homotopy $A^i \to A^{i-1}$ between $\mathrm{id}_{A^\bullet}$ and 0. The proof in the injective case is similar. □

Corollary 10.20. *Every quasi-isomorphism in $K^-(\mathcal{P})$ (or $K^+(\mathcal{I})$) is an isomorphism.*

Proof. Let $s : P_1^\bullet \to P_2^\bullet$ be a quasi-isomorphism in $K^-(\mathcal{P})$. By Lemma 9.2 (1) the cone $C(s)$ is acyclic, hence homotopically trivial by part (2) of the above lemma. We conclude by Corollary 9.12. □

Proof of Proposition 10.18. We do the case of $K^-(\mathcal{P})$. If $S^{-1}K^-(\mathcal{P})$ denotes its localization by the collection of quasi-isomorphisms in $K^-(\mathcal{P})$, the canonical functor $K^-(\mathcal{P}) \to S^{-1}K^-(\mathcal{P})$ is an isomorphism by the previous corollary, so since the functor $K^-(\mathcal{P}) \to D^-(\mathcal{A})$ of the proposition factors through $S^{-1}K^-(\mathcal{P})$, it will be enough to construct a quasi-inverse for the induced functor $S^{-1}K^-(\mathcal{P}) \to D^-(\mathcal{A})$.

The method is the same as in the proof of Lemma 10.17. For each object $A^\bullet$ in $D^-(A)$ fix an isomorphism $\phi_A : P_A^\bullet \xrightarrow{\sim} A^\bullet$ in $D^-(\mathcal{A})$ with an object of $D^-(\mathcal{P})$; this is possible by Lemma 10.19 (1). Given a morphism $\rho : A^\bullet \to B^\bullet$ in $D^-(\mathcal{A})$, the composite $\phi_B^{-1} \circ \rho \circ \phi_A$ is a morphism $P_A^\bullet \to P_B^\bullet$ in $D^-(\mathcal{A})$. Thus we may represent $\phi_B^{-1} \circ \rho \circ \phi_A$ by a pair $P_A^\bullet \xleftarrow{s} C^\bullet \xrightarrow{f} P_B^\bullet$ in $K^-(\mathcal{A})$, with s a quasi-isomorphism. Use again Lemma 10.19 (1) to find a quasi-isomorphism $t : P_C^\bullet \to C^\bullet$ where $P_C^\bullet$ is an object in $K^-(\mathcal{P})$. Then $P_A^\bullet \overset{s\circ t}{\leftarrow} P_C^\bullet \overset{f\circ t}{\to} P_B^\bullet$ still represents $\phi_B^{-1} \circ \rho \circ \phi_A$ in $D^-(\mathcal{A})$ but $s \circ t$, $f \circ t$ are now morphisms in $K^-(\mathcal{P})$, so we have in fact a morphism in $S^{-1}K^-(\mathcal{P})$; note that it does not depend on the choice of t. Now the required quasi-inverse is defined by $A^\bullet \mapsto P_A^\bullet$, $\rho \mapsto (s \circ t, f \circ t)$. □

It remains to prove Lemma 10.19 (1). It could be done via a direct construction, but we prefer to introduce a general technique that will also serve later.

Definition 10.21. A *double complex* $A^{\bullet,\bullet}$ in an abelian category $\mathcal{A}$ is a system of objects $A^{i,j}$ indexed by $\mathbf{Z} \times \mathbf{Z}$ together with morphisms $d_h^{i,j} : A^{i,j} \to A^{i+1,j}$ (*horizontal* differentials) and $d_v^{i,j} : A^{i,j} \to A^{i,j+1}$ (*vertical* differentials) satisfying

$$d_h^{i+1,j} \circ d_h^{i,j} = 0, \quad d_v^{i,j+1} \circ d_v^{i,j} = 0, \quad d_v^{i+1,j} \circ d_h^{i,j} + d_h^{i,j+1} \circ d_v^{i,j} = 0 \tag{22}$$

for all i, j.

A *morphism* of double complexes $\varphi : A^{\bullet,\bullet} \to B^{\bullet,\bullet}$ is a family of morphisms $\varphi^{i,j} : A^{i,j} \to B^{i,j}$ for all pairs (i, j) compatible with the horizontal and vertical differentials.

A picture of a double complex looks like:

$$\begin{array}{ccccccccc}
 & & \vdots & & \vdots & & \vdots & & \\
 & & \uparrow & & \uparrow & & \uparrow & & \\
\cdots & \longrightarrow & A^{i,j+2} & \xrightarrow{d_h^{i,j+2}} & A^{i+1,j+2} & \xrightarrow{d_h^{i+1,j+2}} & A^{i+2,j+2} & \longrightarrow & \cdots \\
 & & {\scriptstyle d_v^{i,j+1}}\uparrow & & {\scriptstyle d_v^{i+1,j+1}}\uparrow & & {\scriptstyle d_v^{i+2,j+1}}\uparrow & & \\
\cdots & \longrightarrow & A^{i,j+1} & \xrightarrow{d_h^{i,j+1}} & A^{i+1,j+1} & \xrightarrow{d_h^{i+1,j+1}} & A^{i+2,j+1} & \longrightarrow & \cdots \\
 & & {\scriptstyle d_v^{i,j}}\uparrow & & {\scriptstyle d_v^{i+1,j}}\uparrow & & {\scriptstyle d_v^{i+2,j}}\uparrow & & \\
\cdots & \longrightarrow & A^{i,j} & \xrightarrow{d_h^{i,j}} & A^{i+1,j} & \xrightarrow{d_h^{i+1,j}} & A^{i+2,j} & \longrightarrow & \cdots \\
 & & \uparrow & & \uparrow & & \uparrow & & \\
 & & \vdots & & \vdots & & \vdots & &
\end{array}$$

Construction 10.22. A double complex $A^{\bullet,\bullet}$ is called *biregular* if for all $n \in \mathbf{Z}$ the set $\{(i,j) : i + j = n \text{ and } A^{i,j} \neq 0\}$ is finite. This is the case, for example, if there exists $k \in \mathbf{Z}$ such that $A^{i,j} = 0$ for $i < k, j < k$ or if $A^{i,j} = 0$ for $i > k, j > k$.

Given a biregular double complex $A^{\bullet,\bullet}$, we define the *associated simple complex* $sA^\bullet$ by setting

$$sA^n := \bigoplus_{i+j=n} A^{i,j}$$

and $d^n : sA^n \to sA^{n+1}$ given in the (i,j)-component by $d_h^{i,j} + d_v^{i,j}$. The formulas (22) ensure that this is indeed a complex.

A morphism $\varphi : A^{\bullet,\bullet} \to B^{\bullet,\bullet}$ of double complexes induces a morphism $s\varphi : sA^\bullet \to sB^\bullet$ of associated simple complexes. It is defined in degree n by the direct sum of the maps $\varphi^{i,j}$. Thus s is a functor from the category of biregular double complexes to that of simple complexes. This functor is exact because a direct sum of exact sequences is exact (exact sequences of double complexes are defined term by term, as for usual complexes).

Proposition 10.23. *Let $\varphi : A^{\bullet,\bullet} \to B^{\bullet,\bullet}$ be a morphism of biregular double complexes. If φ induces quasi-isomorphisms $A^{\bullet,j} \to B^{\bullet,j}$ for each row, then $s\varphi : sA^\bullet \to sB^\bullet$ is a quasi-isomorphism.*

Same conclusion if φ induces quasi-isomorphisms $A^{i,\bullet} \to B^{i,\bullet}$ for each column.

Proof. We do the case of columns. We have to show that the maps $H^n(s\varphi) : H^n(sA^\bullet) \to H^n(sB^\bullet)$ are isomorphisms for all n. Since the double complexes are biregular, only finitely many $A^{i,j}$ and $B^{i,j}$ contribute to $H^n(sA^\bullet)$ and $H^n(sB^\bullet)$ for fixed n. So we may assume $A^{i,j} = B^{i,j} = 0$ except for finitely many pairs i,j by setting the terms in the uninteresting range to 0. In particular, we may assume that $A^{i,\bullet} = B^{i,\bullet} = 0$ for i outside an interval $[a,b] \subset \mathbf{Z}$. Thus the morphism φ can be represented by the diagram

$$\begin{array}{ccccccccccc} 0 & \longrightarrow & A^{a,\bullet} & \longrightarrow & A^{a+1,\bullet} & \longrightarrow & \cdots & \longrightarrow & A^{b,\bullet} & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & & & \downarrow & & \\ 0 & \longrightarrow & B^{a,\bullet} & \longrightarrow & B^{a+1,\bullet} & \longrightarrow & \cdots & \longrightarrow & B^{b,\bullet} & \longrightarrow & 0 \end{array} \tag{23}$$

We proceed by induction on $b-a$. If $b-a=0$, then $A^{\bullet,\bullet}$ and $B^{\bullet,\bullet}$ are both concentrated in a single column and the assertion holds by assumption. Now assume we have proven the cases with $b-a<n$. Introduce the notation $A^{\geq a+1,\bullet}$ for the double complex obtained from $A^{\bullet,\bullet}$ by setting $A^{i,j}=0$ for $i<a+1$, and similarly for $B^{\geq a+1,\bullet}$. We have a commutative diagram of morphisms of double complexes with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A^{a,\bullet} & \longrightarrow & A^{\bullet,\bullet} & \longrightarrow & A^{\geq a+1,\bullet} & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & B^{a,\bullet} & \longrightarrow & B^{\bullet,\bullet} & \longrightarrow & B^{\geq a+1,\bullet} & \longrightarrow & 0 \end{array}$$

where on the left hand side we have the a-th columns of $A^{\bullet,\bullet}$ and $B^{\bullet,\bullet}$ considered as double complexes with 0's elsewhere. Applying the exact functor s we obtain a commutative diagram of morphisms of simple complexes with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A^{a,\bullet} & \longrightarrow & sA^{\bullet,\bullet} & \longrightarrow & sA^{\geq a+1,\bullet} & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & B^{a,\bullet} & \longrightarrow & sB^{\bullet,\bullet} & \longrightarrow & sB^{\geq a+1,\bullet} & \longrightarrow & 0 \end{array}$$

Here the first vertical map is a quasi-isomorphism by assumption and the last one by induction. Hence so is the middle one by Corollary 3.7. □

Corollary 10.24. *If $A^{\bullet,\bullet}$ is a biregular double complex whose rows (resp. columns) are acyclic, then $sA^{\bullet,\bullet}$ is acyclic.*

Proof. Apply the proposition with $B^{\bullet,\bullet} = 0$. □

Remark 10.25. There is a variant of the proposition which is often useful. Denote the cohomology groups of the j-th row of $A^{\bullet,\bullet}$ by $H_h^{i,j}(A^{\bullet,\bullet})$ for all i and the cohomology groups of the i-th column of $A^{\bullet,\bullet}$ by $H_v^{i,j}(A^{\bullet,\bullet})$ for all j. The identity $d_v^{i+1,j} \circ d_h^{i,j} + d_h^{i,j+1} \circ d_v^{i,j} = 0$ implies that the differentials 'in the other direction' induce complexes

$$\cdots \to H_h^{i,j-1}(A^{\bullet,\bullet}) \to H_h^{i,j}(A^{\bullet,\bullet}) \to H_h^{i,j+1}(A^{\bullet,\bullet}) \to \cdots$$

and

$$\cdots \to H_v^{i-1,j}(A^{\bullet,\bullet}) \to H_v^{i,j}(A^{\bullet,\bullet}) \to H_v^{i+1,j}(A^{\bullet,\bullet}) \to \cdots$$

called the i-th column and j-th row of cohomology, respectively. Now the variant states: if $\varphi : A^{\bullet,\bullet} \to B^{\bullet,\bullet}$ induces quasi-isomorphisms on each row (or column) of cohomology, then $s\varphi : sA^{\bullet} \to sB^{\bullet}$ is a quasi-isomorphism. The proof is similar to the above, using canonical truncations $\tau_{\geq a+1,\bullet}(A^{\bullet,\bullet})$ of rows, instead of the 'stupid' ones used above.

Proof of Lemma 10.19 (1). We may assume $A^i = 0$ for $i > 0$. We shall construct a double complex $P^{\bullet,\bullet}$ with $P^{i,j} = 0$ for $i > 0$ or $j > 0$ whose terms are projective and is equipped with a morphism of double complexes $P^{\bullet,\bullet} \to A^{\bullet}$, where $A^{\bullet}$ is considered as a double complex with a single nonzero row. This morphism will induce a quasi-isomorphism on columns, i.e. each column of cohomology of $P^{\bullet,\bullet}$ will give a projective resolution of A^i. Proposition 10.23, together with the fact that finite direct sums of projectives are projective, will then show that the induced morphism $sP^{\bullet,\bullet} \to A^{\bullet}$ is a quasi-isomorphism we were looking for.

To construct $P^{\bullet,\bullet}$ we revert to homological indexing. For each i consider the exact sequence

$$0 \to B_i(A_{\bullet}) \to Z_i(A_{\bullet}) \to H_i(A_{\bullet}) \to 0.$$

Choose projective resolutions $P^B_{i,\bullet} \to B_i(A_\bullet)$ and $P^H_{i,\bullet} \to H_i(A_\bullet)$, respectively. By Lemma 4.4 there is a projective resolution $P^Z_{i,\bullet} \to Z_i(A_\bullet)$ fitting in an exact sequence of complexes

$$0 \to P^B_{i,\bullet} \to P^Z_{i,\bullet} \to P^H_{i,\bullet} \to 0.$$

Now repeat the procedure with the exact sequence

$$0 \to Z_i(A_\bullet) \to A_i \to B_{i-1}(A_\bullet) \to 0.$$

and the projective resolutions $P^B_{i-1,\bullet} \to B_{i-1}(A_\bullet)$ and $P^Z_{i,\bullet} \to Z_i(A_\bullet)$. It gives a projective resolution $P^Z_{i,\bullet} \to A_i$ fitting in an exact sequence of complexes

$$0 \to P^Z_{i,\bullet} \to P_{i,\bullet} \to P^B_{i-1,\bullet} \to 0.$$

Now construct a double complex $P_{\bullet,\bullet}$ out of the $P_{i,\bullet}$ with horizontal differentials induced by the composite maps

$$P_{i,j} \to P^B_{i-1,j} \to P^Z_{i-1,j} \to P_{i-1,j}$$

coming from the above diagrams and vertical maps those of the $P_{i,\bullet}$ multiplied by $(-1)^i$. With this sign rule $P_{\bullet,\bullet}$ becomes a double complex and by construction there is a morphism $P_{\bullet,\bullet} \to A_\bullet$ with the required property. The proof in the injective case is similar. □

Remark 10.26. The proof shows that $P_{\bullet,\bullet}$ satisfies much more than stated in the beginning: it induces projective resolutions of each A_i, $Z_i(A_\bullet)$, $B_i(A_\bullet)$ and $H_i(A_\bullet)$ as well. Such double complexes are called *Cartan–Eilenberg resolutions.*

11. Total derived functors

Let $F : \mathcal{A} \to \mathcal{B}$ be an additive functor between abelian categories. It then extends uniquely to an additive functor $C(\mathcal{A}) \to C(\mathcal{B})$ and also to a functor $K(\mathcal{A}) \to K(\mathcal{B})$ on the associated homotopy categories (any homotopy between maps f and g induces a homotopy between $F(f)$ and $F(g)$). Moreover, $F : K(\mathcal{A}) \to K(\mathcal{B})$ is a *triangulated functor*, i.e. it sends exact triangles to exact triangles (this property is the natural analogue of exactness for functors between homotopy or derived categories). Now consider the following question: does there exist a triangulated functor $D(\mathcal{A}) \to D(\mathcal{B})$ making the diagram

$$\begin{array}{ccc} K(\mathcal{A}) & \xrightarrow{Q} & D(\mathcal{A}) \\ {\scriptstyle F}\downarrow & & \\ K(\mathcal{B}) & \xrightarrow{Q} & D(\mathcal{B}) \end{array}$$

commute?

When $F : \mathcal{A} \to \mathcal{B}$ is an exact functor, the answer is yes. Indeed, notice first that if $A^\bullet$ is an acyclic complex in $C(\mathcal{A})$, then $F(A^\bullet)$ is also acyclic (because F preserves exactness of the short exact sequences $0 \to Z^i(A^\bullet) \to A^i \to Z^{i+1}(A^\bullet) \to 0$), so by Lemma 9.2 (2) F preserves quasi-isomorphisms. But then the composite functor $K(\mathcal{A}) \stackrel{F}{\to} K(\mathcal{B}) \stackrel{Q}{\to} D(\mathcal{B})$ factors through $D(\mathcal{A})$ by the universal property of localization and the resulting functor is triangulated because F and Q are.

In general such an extension to $D(\mathcal{A})$ does not exist and even in good cases one has to restrict to the full subcategories $D^+(\mathcal{A})$ or $D^-(A)$. Here is the formal definition.

Definition 11.1. Let $F : K^-(\mathcal{A}) \to K^-(\mathcal{B})$ be a triangulated functor. A *left derived functor* for F is a triangulated functor $LF : D^-(\mathcal{A}) \to D^-(\mathcal{B})$ together with a morphism of functors $\varepsilon : LF \circ Q \to Q \circ F$ that is universal in the following sense: For every pair (G, η) with $G : D^-(\mathcal{A}) \to D^-(\mathcal{B})$ a triangulated functor and $\eta : G \circ Q \to Q \circ F$ there is a unique morphism of functors $\alpha : G \to LF$ with $\eta = \varepsilon \circ \alpha \circ Q$.

Similarly, if $F : K^+(\mathcal{A}) \to K^+(\mathcal{B})$ is a triangulated functor, a *right derived functor* for F is a triangulated functor $RF : D^+(\mathcal{A}) \to D^+(\mathcal{B})$ together with a morphism of functors $\varepsilon : Q \circ F \to RF \circ Q$ such that for every pair (G, η) with $G : D^+(\mathcal{A}) \to D^+(\mathcal{B})$ a triangulated functor and $\eta : Q \circ F \to G \circ Q$ there is a unique morphism of functors $\alpha : RF \to G$ with $\eta = \varepsilon \circ \alpha \circ Q$.

Of course, when LF or RF exists, it is unique up to unique isomorphism. In the case where F comes from an additive functor $\mathcal{A} \to \mathcal{B}$, one sometimes calls LF and RF *total derived functors* of F.

Proposition 11.2. *If $\mathcal{A}$ has enough projectives (resp. injectives), the left (resp. right) derived functors of F exist.*

Proof. We do the case of LF. Let $R : D^-(A) \to K^-(\mathcal{P})$ be a quasi-inverse to the functor of Proposition 10.18, and set $LF := Q \circ F|_{K^-(\mathcal{P})} \circ R$. To define ε, pick $A^\bullet \in K^-(\mathcal{A})$ and take the quasi-isomorphism $\phi_A : P^\bullet \to A^\bullet$ in $K^-(\mathcal{A})$ used in the construction of R, where $P^\bullet$ has projective terms. Now ϕ_A induces a morphism $F(\phi_A) : F(P^\bullet) \to F(A^\bullet)$; applying Q we have the required morphism $\varepsilon_A : (LF \circ Q)(A^\bullet) \to (Q \circ F)(A^\bullet)$. The definition of ε on morphisms is similar, using the induced morphisms in $K^-(\mathcal{P})$ constructed in the proof of Proposition 10.18.

To construct $\alpha : G \to LF$, consider again the above $A^\bullet$ and ϕ_A. The inverse of $(G \circ Q)(\phi_A)$ in $D^-(A)$ induces an isomorphism $(G \circ Q)(A^\bullet) \xrightarrow{\sim} (G \circ Q)(P^\bullet)$ which we may compose with $(G \circ Q)(P^\bullet) \xrightarrow{\eta} (Q \circ F)(P^\bullet) = LF(Q(A^\bullet))$. This defines α on objects; the definition on morphisms is left to the reader.

We still have to check that LF is a triangulated functor. Suppose

$$A^\bullet \to B^\bullet \to C^\bullet \to A^\bullet[1] \tag{24}$$

is an exact triangle in $D^-(\mathcal{A})$. Then

$$R(A^\bullet) \xrightarrow{g} R(B^\bullet) \to R(C^\bullet) \to R(A^\bullet)[1] \tag{25}$$

is a triangle in $K^-(\mathcal{P})$ isomorphic in $D^-(A)$ to the previous one. Moreover, it is also isomorphic in $D^-(\mathcal{A})$ to the triangle

$$R(A^\bullet) \to R(B^\bullet) \to C(g) \to R(A^\bullet)[1]$$

by the version of Lemma 9.10 (2) and Corollary 9.11 (2) for derived categories. But these last two triangles have terms in $K^-(\mathcal{P})$, so they are also isomorphic in $K^-(\mathcal{P})$ by Corollary 10.20. In particular, (25) is an exact triangle in $K^-(\mathcal{A})$, and hence applying the triangulated functor F to it we obtain an exact triangle in $K^-(\mathcal{B})$. Since Q is a triangulated functor by definition, we have proven that LF maps (24) to an exact triangle. □

In the course of the above proof we have shown:

Corollary 11.3. *When $\mathcal{A}$ has enough projectives, for each object $A^\bullet \in K(\mathcal{A})$ we have $LF(A^\bullet) \cong F(P^\bullet)$, where $P^\bullet \to A^\bullet$ is a quasi-isomorphism and $P^\bullet$ has projective terms.*

Similarly, when A has enough injectives, for each object $A^\bullet \in K(\mathcal{A})$ we have $RF(A^\bullet) \cong F(Q^\bullet)$, where $A^\bullet \to Q^\bullet$ is a quasi-isomorphism and $Q^\bullet$ has injective terms.

Note that by construction if we choose two quasi-isomorphisms $P^\bullet \to A^\bullet \leftarrow P'^\bullet$ in the corollary above, $P^\bullet$ and $P'^\bullet$ will be homotopy equivalent and hence so will be $F(P^\bullet)$ and $F(P'^\bullet)$, giving isomorphic objects in $D(\mathcal{B})$. This independence of $P^\bullet$ was built in the construction.

Definition 11.4. For $i \in \mathbf{Z}$ define the *i-th left (resp. right) derived functor* of F by $L_iF := H^{-i} \circ LF$ (resp. $R^iF := H^i \circ RF$) assuming that LF or RF exists.

Since LF and RF are triangulated functors, we have:

Corollary 11.5. *Given an exact triangle $A^\bullet \to B^\bullet \to C^\bullet \to A^\bullet[1]$ in $D^-(\mathcal{A})$, there is a long exact sequence*

$$\cdots \to L_iF(A^\bullet) \to L_iF(B^\bullet) \to L_iF(C^\bullet) \to L_{i-1}F(A^\bullet) \to \cdots$$

Similarly, for an exact triangle in $D^+(\mathcal{A})$ there is a long exact sequence

$$\cdots \to R^iF(A^\bullet) \to R^iF(B^\bullet) \to R^iF(C^\bullet) \to R^{i+1}F(A^\bullet) \to \cdots$$

Remark 11.6. There is a natural functor $E : \mathcal{A} \to D^b(\mathcal{A})$ sending an object A to the object in $D^b(\mathcal{A})$ represented by the complex with A in degree 0 and 0 elsewhere. When $\mathcal{A}$ has enough projectives or injectives and F is an additive functor $\mathcal{A} \to \mathcal{B}$, the composite functors $L_iF \circ E$ and $R^iF \circ E$ are exactly the derived functors introduced in Section 4. This follows from Corollary 11.3.

In the remainder of the section assume $\mathcal{A}$ is the category of modules over a fixed commutative ring R; in particular it has enough injectives and projectives. Recall that the tensor product of two complexes in $C^-(\mathcal{A})$ was defined in Definition 8.4. Using the language of double complexes it can be restated as follows: $(A \otimes_R B)_\bullet$ is the simple complex associated with the double complex $C^{\bullet,\bullet}$ with $C^{i,j} = A^i \otimes_R B^j$, horizontal differentials given by $d^i_A \otimes \mathrm{id}_B$ and vertical differentials by $(-1)^i \mathrm{id}_A \otimes d^j_B$.

Proposition 11.7. *For a fixed complex $B^\bullet$ in $K^-(\mathcal{A})$ the functor $K^-(\mathcal{A}) \to K^-(\mathcal{A})$ given by $A^\bullet \mapsto A^\bullet \otimes B^\bullet$ has a left derived functor $D^-(\mathcal{A}) \to D^-(\mathcal{A})$ denoted by $A^\bullet \mapsto A^\bullet \otimes^{\mathbf{L}} B^\bullet$.*

Moreover, the functor $B^\bullet \mapsto A^\bullet \otimes^{\mathbf{L}} B^\bullet$ respects quasi-isomorphisms, inducing a triangulated functor $D^-(\mathcal{A}) \to D^-(\mathcal{A})$.

All in all, $(A^\bullet, B^\bullet) \mapsto A^\bullet \otimes^{\mathbf{L}} B^\bullet$ induces a triangulated *bifunctor* $D^-(\mathcal{A}) \times D^-(\mathcal{A}) \to D^-(\mathcal{A})$ (i.e. a triangulated functor in both variables).

Proof. Only the second statement needs a proof. By Corollary 11.3 $A^\bullet \otimes^{\mathbf{L}} B^\bullet$ is computed by $P^\bullet \otimes B^\bullet$, where $P^\bullet \to A^\bullet$ is a quasi-isomorphism and $P^\bullet$ has projective terms. If $B^\bullet \to B'^\bullet$ is a quasi-isomorphism of complexes in $C^-(\mathcal{A})$, then so is $P^i \otimes_R B^\bullet \to P^i \otimes_R B'^\bullet$ for each $i \in \mathbf{Z}$ because P^i is flat over R. Now Proposition 10.23 implies that $P^\bullet \otimes B^\bullet \to P^\bullet \otimes B'^\bullet$ is a quasi-isomorphism. That the resulting functor is triangulated will follow from the remark below. □

One defines $\mathrm{Tor}_i(A^\bullet, B^\bullet) := H^{-i}(A^\bullet \otimes^{\mathbf{L}} B^\bullet)$. In the case when $A^\bullet$ and $B^\bullet$ are one-term complexes, this is the same Tor as before.

Remark 11.8. Notice that if $P^\bullet_A \to A^\bullet$ and $P^\bullet_B \to B^\bullet$ are quasi-isomorphisms with complexes having projective terms, we have isomorphisms in $D^-(\mathcal{A})$

$$A^\bullet \otimes^{\mathbf{L}} B^\bullet \cong P^\bullet_A \otimes B^\bullet \cong P^\bullet_A \otimes P^\bullet_B$$

by the proposition above. Moreover, by the same argument in the above proof, tensoring with $P^\bullet_B$ on the right also respects quasi-isomorphisms, hence we also have

$$A^\bullet \otimes^{\mathbf{L}} B^\bullet \cong P^\bullet_A \otimes P^\bullet_B \cong A^\bullet \otimes P^\bullet_B.$$

This shows that we may compute $A^\bullet \otimes^{\mathbf{L}} B^\bullet$ and hence also the groups $\mathrm{Tor}_i(A^\bullet, B^\bullet)$ indifferently by using $P^\bullet_A$ in the first variable or $P^\bullet_B$ in the second.

Now we come to the Hom-functor. For $A^\bullet$ in $C^-(\mathcal{A})$ and $B^\bullet$ in $C^+(\mathcal{A})$ define a double complex $\mathrm{Hom}(A,B)^{\bullet,\bullet}$ by

$$\mathrm{Hom}(A,B)^{i,j} := \mathrm{Hom}(A^{-i}, B^j),\ d_h^{i,j} := (-1)^{j-i+1}\mathrm{Hom}(d_A^{-i-1}, B^j),\ d_v^{i,j} := \mathrm{Hom}(A^{-i}, d_B^j).$$

One checks that in this way we obtain a biregular double complex, so we can set

$$\mathrm{Hom}(A,B)^\bullet := s\mathrm{Hom}(A,B)^{\bullet,\bullet}.$$

Thus the degree n term of $\mathrm{Hom}(A,B)^\bullet$ is

$$\mathrm{Hom}(A,B)^n = \bigoplus_{i+j=n} \mathrm{Hom}(A^{-i}, B^j) = \bigoplus_{j-i=n} \mathrm{Hom}(A^i, B^j)$$

so its elements are represented by finite collections of morphisms $f^i : A^i \to B^{i+n}$, with the differential given by $d(f^i) = d_B \circ f^i + (-1)^{n+1} f^{i+1} \circ d_A$.

Remark 11.9. For future reference let us compute the group $H^0(\mathrm{Hom}(A,B)^\bullet)$.

$$Z^0(\mathrm{Hom}(A,B)^\bullet) = \{(f^i : A^i \to B^i) : d_B \circ f^i - f^i \circ d_A = 0\} = \mathrm{Hom}_{C(\mathcal{A})}(A^\bullet, B^\bullet).$$

On the other hand,

$$B^0(\mathrm{Hom}(A,B)^\bullet) = \{(f^i : A^i \to B^i) : f^i = d_B \circ k^i + k^{i+1} \circ d_A \text{ for some } (k^i) \in \mathrm{Hom}(A,B)^{-1}\}.$$

Thus

$$H^0(\mathrm{Hom}(A,B)^\bullet) \cong \mathrm{Hom}_{K(\mathcal{A})}(A^\bullet, B^\bullet).$$

Proposition 11.10. *For a fixed complex $A^\bullet$ in $K^-(\mathcal{A})$ the functor $K^+(\mathcal{A}) \to K^+(\mathcal{A})$ given by $B^\bullet \mapsto \mathrm{Hom}(A,B)^\bullet$ has a right derived functor $D^+(\mathcal{A}) \to D^+(\mathcal{A})$ denoted by $B^\bullet \mapsto R\mathrm{Hom}(A^\bullet, B^\bullet)$.*

Moreover, the functor $A^\bullet \mapsto R\mathrm{Hom}(A^\bullet, B^\bullet)$ respects quasi-isomorphisms, inducing a triangulated functor $D^-(\mathcal{A})^{op} \to D^+(\mathcal{A})$.

Proof. Same as that of the previous proposition, using quasi-isomorphisms $B^\bullet \to Q^\bullet$ this time, where $Q^\bullet$ has injective terms. □

Remark 11.11. We now have a triangulated bifunctor $D^-(\mathcal{A})^{op} \times D^+(\mathcal{A}) \to D^+(\mathcal{A})$ given by $(A^\bullet, B^\bullet) \mapsto R\mathrm{Hom}(A^\bullet, B^\bullet)$. As in the previous remark, we can compute

$$R\mathrm{Hom}(A^\bullet, B^\bullet) \cong \mathrm{Hom}(A,Q)^\bullet \cong \mathrm{Hom}(P,B)^\bullet$$

where $P^\bullet \to A^\bullet$ is a quasi-isomorphism and $P^\bullet$ has projective terms.

We set $\mathrm{Ext}^i(A^\bullet, B^\bullet) := H^i(R\mathrm{Hom}(A^\bullet, B^\bullet))$. In the case of one-term complexes this again gives back both the covariant and the contravariant Ext functors. But there is a bonus:

Proposition 11.12. *For all $A^\bullet$ in $D^-(\mathcal{A})$, $B^\bullet$ in $D^+(\mathcal{A})$ and $i \in \mathbf{Z}$ we have functorial isomorphisms*

$$\mathrm{Ext}^i(A^\bullet, B^\bullet) \cong \mathrm{Hom}_{D(\mathcal{A})}(A^\bullet, B^\bullet[i]).$$

Proof. Replacing B by $B[-i]$ we reduce to the case $i = 0$. Choose a quasi-isomorphism $B^\bullet \to Q^\bullet$, where $Q^\bullet$ has injective terms. We compute

$$\mathrm{Ext}^0(A^\bullet, B^\bullet) = H^0(\mathrm{Hom}(A, Q)^\bullet) = \mathrm{Hom}_{K(\mathcal{A})}(A^\bullet, Q^\bullet)$$

by Remark 11.9.

On the other hand, an element of $\mathrm{Hom}_{D(\mathcal{A})}(A^\bullet, Q^\bullet)$ can be represented by a pair $A^\bullet \xrightarrow{g} C^\bullet \xleftarrow{t} Q^\bullet$ where t is a quasi-isomorphism. Choosing a quasi-isomorphism $t' : C^\bullet \to Q'^\bullet$, where $Q'^\bullet$ has injective terms, we see that $A^\bullet \xrightarrow{t'\circ g} Q'^\bullet \xleftarrow{t'\circ t} Q^\bullet$ represents the same morphism in $D(\mathcal{A})$, but $t' \circ t$ is an isomorphism in $D^+(\mathcal{A})$ by Corollary 10.20. This shows $\mathrm{Hom}_{D(\mathcal{A})}(A^\bullet, B^\bullet) \cong \mathrm{Hom}_{D(\mathcal{A})}(A^\bullet, Q^\bullet) \cong \mathrm{Hom}_{K(\mathcal{A})}(A^\bullet, Q^\bullet)$. □

Remark 11.13. The above discussion of $R\mathrm{Hom}$ works in an arbitrary abelian category having enough injectives. However, defining $\mathrm{Ext}^i(A^\bullet, B^\bullet)$ as $\mathrm{Hom}_{D(\mathcal{A})}(A^\bullet, B^\bullet[i])$ can be done in an arbitrary $\mathcal{A}$, and this is the most convenient and general definition of Ext functors. It is possible to identify the Ext functors defined in this way with the Yoneda Ext functors of Remark 5.11. The product defined there corresponds to composition of morphisms in $D(\mathcal{A})$.

12. Homological dimension revisited

As an application of derived functor techniques, we can now give a recent proof of Serre's homological characterization of regular local rings (Theorem 6.12) due to Jagadeesan, Landesman (and Gaitsgory).[1]

Proposition 12.1. *Let A be a local ring with residue field k, and let $x \in P \setminus P^2$ be a non-zerodivisor. There is an isomorphism*

$$k \otimes^{\mathbf{L}}_A A/(x) \cong k \oplus k[1]$$

in the derived category $\mathcal{D}$ of $A/(x)$-modules.

Corollary 12.2. *Assume moreover A is Noetherian. Then* $\mathrm{gl.dim}(A/(x)) = \mathrm{gl.dim}(A) - 1$.

[1]R. Jagadeesan, A. Landesman, A new proof of Serre's homological characterization of regular local rings, *Res. Number Theory* (2016) 2:18.

Proof. We have an isomorphism

$$k \otimes_A^{\mathbf{L}} A/(x) \otimes_{A/(x)}^{\mathbf{L}} k \cong k \otimes_A^{\mathbf{L}} k$$

in $\mathcal{D}$. (Indeed, we may compute the right hand side as $P_\bullet \otimes_A k$ with a projective resolution $P_\bullet \to k$ over A. But then $P_\bullet \otimes_A A/(x)$ computes $k \otimes_A^{\mathbf{L}} A/(x)$ and moreover gives a projective resolution of k as an $A/(x)$-module, so we compute the left hand side as $P_\bullet \otimes_A A/(x) \otimes_{A/(x)} k \cong P_\bullet \otimes_A k$.)

On the other hand, the proposition implies

$$(k \otimes_A^{\mathbf{L}} A/(x)) \otimes_{A/(x)}^{\mathbf{L}} k \cong k \otimes_{A/(x)}^{\mathbf{L}} k \oplus (k \otimes_{A/(x)}^{\mathbf{L}} k)[1]$$

so that

$$\mathrm{Tor}_i^A(k,k) = H^{-i}(k \otimes_A^{\mathbf{L}} k) \cong H^{-i}(k \otimes_{A/(x)}^{\mathbf{L}} k) \oplus H^{-i}((k \otimes_{A/(x)}^{\mathbf{L}} k)[1]) =$$
$$= \mathrm{Tor}_i^{A/(x)}(k,k) \oplus \mathrm{Tor}_{i-1}^{A/(x)}(k,k).$$

Therefore $\mathrm{Tor}_i^A(k,k) = 0$ if and only if $\mathrm{Tor}_i^{A/(x)}(k,k) = \mathrm{Tor}_{i-1}^{A/(x)}(k,k) = 0$, and the statement follows from Corollary 6.9. □

Remark 12.3. Let us recall that Theorem 6.12 follows quickly from the above corollary: if A is regular, then we can choose x to be part of a regular system of parameters and conclude $\mathrm{gl.dim.}(A) = \dim(A)$ by induction on $\dim(A)$; conversely, if $\mathrm{gl.dim.}(A) = d < \infty$, we show first that there is a nonzerodivisor $x \in P \setminus P^2$ as in the first proof, and then by induction on d obtain a regular sequence generating $P/(x)$ in $A/(x)$ that we may complete with x to a regular system of parameters of A.

The first step of the proof of the proposition is given by:

Lemma 12.4. *We have an isomorphism $C(f) \cong k \otimes_A^{\mathbf{L}} A/(x)$ in $\mathcal{D}$, where $f : P/xP \to A/(x)$ is the natural map.*

Proof. Consider the exact triangle coming from the exact sequence of A-modules

$$0 \to P \to A \to k \to 0.$$

Applying the functor $\otimes_A^{\mathbf{L}} A/(x)$ induces an exact triangle

$$P \otimes_A^{\mathbf{L}} A/(x) \to A \otimes_A^{\mathbf{L}} A/(x) \to k \otimes_A^{\mathbf{L}} A/(x) \to P \otimes_A^{\mathbf{L}} A/(x)[1]$$

in $\mathcal{D}$.

Here the first term can be computed by tensoring the projective resolution $[A \stackrel{x}{\to} A]$ of $A/(x)$ by P, obtaining $[P \stackrel{x}{\to} P]$. Since x is not a zero-divisor, the the only nontrivial cohomology of $P \otimes_A^{\mathbf{L}} A/(x)$ is in degree 0, where it is P/xP. Thus we have $P \otimes_A^{\mathbf{L}} A/(x) \cong \tau_{\geq 0}(P \otimes_A^{\mathbf{L}} A/(x)) \cong P/xP$. Also, $A \otimes_A^{\mathbf{L}} A/(x) \stackrel{\sim}{\to} A \otimes_A A/(x) \cong A/(x)$ as A is free over itself, so the first map in the triangle identifies with the image of f

in $\mathcal{D}$. The lemma follows by applying the derived category version of Lemma 9.10 (2) and Corollary 9.11 (2). □

Proof of Proposition 12.1. We may also compute the derived tensor product $k \otimes_A^{\mathbf{L}} A/(x)$ by tensoring the projective resolution $[A \xrightarrow{x} A]$ of $A/(x)$ by k, obtaining $[k \xrightarrow{x} k]$. Here multiplication by x is the zero map, so we get isomorphisms $H^{-1}(k \otimes_A^{\mathbf{L}} A/(x)) \cong H^0(k \otimes_A^{\mathbf{L}} A/(x)) \cong k$ and $\tau_{\geq -1}(k \otimes_A^{\mathbf{L}} A/(x)) \cong k \otimes_A^{\mathbf{L}} A/(x)$. The exact triangle

$$H^{-1}(k \otimes_A^{\mathbf{L}} A/(x))[1] \to \tau_{\geq -1}(k \otimes_A^{\mathbf{L}} A/(x)) \to H^0(k \otimes_A^{\mathbf{L}} A/(x)) \to H^{-1}(k \otimes_A^{\mathbf{L}} A/(x))[2]$$

coming from (21) thus identifies with an exact triangle

$$k[1] \to k \otimes_A^{\mathbf{L}} A/(x) \to k \to k[2].$$

Now according to the lemma we have isomorphisms

$$k \otimes_A^{\mathbf{L}} A/(x) \xrightarrow{\sim} C(f) = [P/xP \xrightarrow{f} A/(x)]$$

in $\mathcal{D}$, and in particular isomorphisms

$$k \cong H^{-1}(k \otimes_A^{\mathbf{L}} A/(x)) \cong \ker(f), \quad k \cong H^0(k \otimes_A^{\mathbf{L}} A/(x)) \cong \operatorname{coker}(f).$$

Under this identification the exact triangle above comes from the exact sequence of complexes

$$0 \to \ker(f)[1] \to [P/xP \xrightarrow{f} A/(x)] \to [(P/xP)/\ker(f) \xrightarrow{f} A/(x)] \to 0$$

noting the quasi-isomorphism $[(P/xP)/\ker(f) \xrightarrow{f} A/(x)] \xrightarrow{\sim} [0 \to \operatorname{coker}(f)]$. It suffices to show that the above exact sequence of complexes splits, for which it is enough to split the inclusion map $\ker(f) \to P/xP)$. We may compose it with the natural projection $P/xP \to P/P^2$. The composite map $k \cong \ker(f) \to P/P^2$ is nonzero since x mod xP is in $\ker(f)$ but $x \notin P^2$ by assumption. As this is a map of k-vector spaces, it must be injective with a splitting $P/P^2 \to k$. But then the composite $P/xP \to P/P^2 \to k$ is a splitting as required. □