COMMUTATIVE ALGEBRA

YURIY DROZD

Contents

We write $A \subseteq B$ if A is a subset of B and $A \subset B$ if it is a *proper subset*, that is $A \subseteq B$ and $A \neq B$.

We suppose all rings *commutative* and with unit (usually denoted 1), all homomorphisms of rings mapping unit to unit. An *algebra* over a ring A is a ring B together with a fixed homomorphism $\iota : A \to B$. Then we write ab or ba instead of $\iota(a)b$ for all $a \in A, b \in B$.

We will often use the well-known fact from the set theory called the *Zorn lemma*. Let $\mathfrak{M}$ be a (partially) ordered set with a (partial) order $\leqslant$. A subset $\mathfrak{L} \subseteq \mathfrak{M}$ is called a *chain* if it is totally ordered, that is, for any two elements $a, b \in \mathfrak{L}$, either $a \leqslant b$ or $b \leqslant a$. An *upper bound* of a subset $\mathfrak{N} \subset \mathfrak{M}$ is an element $b \in \mathfrak{M}$ such that $a \leqslant b$ for any $a \in \mathfrak{N}$.

Zorn Lemma. *Suppose that every chain $\mathfrak{L} \subseteq \mathfrak{M}$ has an upper bound. Then there are* maximal elements *in $\mathfrak{M}$, i.e. such elements $a \in \mathfrak{M}$ that $a \nleqslant b$ for any $b \neq a$.*

For references to elementary properties of groups, rings and modules we address the reader to the book of Artin [1]. For other references, exercises and additional topics we recommend the books [2, 3, 6, 7] and [4].

1. Ideals and Nullstellensatz

We start with some geometry.

Let $\Bbbk$ be a field. We usually write $\mathbb{A}^n$ (or $\mathbb{A}^n_\Bbbk$ if necessary) instead of $\Bbbk^n$ and call it the *n-dimensional affine space over the field* $\Bbbk$. Often we suppose the field $\Bbbk$ *algebraically closed* (for instance, the complex field $\mathbb{C}$).

Definition 1.1. For a subset $S \subseteq \Bbbk[\mathbf{x}] = \Bbbk[x_1, x_2, \dots, x_n]$ we denote by $\operatorname{var}(S)$ the set $\{\mathbf{a} = (a_1, a_2, \dots, a_n) \mid f(\mathbf{a}) = 0 \text{ for all } f \in S\}$ and call it the *closed subset defined by the set of equantions* $f(\mathbf{x}) = 0$, $f \in S$. The closed subsets $\operatorname{var}(g)$ are called *hypersurfaces*.

Let I be the ideal generated by S, i.e. consisting of all (finite) sums $\sum_{i=1}^k g_i f_i$, where $f_i \in S$, $g_i \in \Bbbk[\mathbf{x}]$. Obviousely, $\operatorname{var}(S) = \operatorname{var}(I)$. Moreover, we can restrict by a special class of ideals.

Definition 1.2.
(1) An ideal I of a ring R is called *radical* if $a \in I$ as soon as $a^m \in I$ for some m.
(2) The set $\sqrt{I} = \{a \in R \mid a^m \in I \text{ for some } m\}$ is called the *radical* of the ideal I.
One can check that $\sqrt{I}$ is an ideal (**prove it**).
(3) In particular, the ideal $\sqrt{0} = \{a \in R \mid a^m = 0 \text{ for some } m\}$ is called the *nilradical* of the ring R and denoted by $\operatorname{nil} R$. If $\operatorname{nil} A = \{0\}$, the ring A is called *reduced*.

Obviously, $\operatorname{var}(I) = \operatorname{var}(\sqrt{I})$ for any ideal $I \subseteq \Bbbk[x_1, x_2, \dots, x_n]$, hence a closed subset in $\mathbb{A}^n$ is defined by a radical ideal of the ring $\Bbbk[x_1, x_2, \dots, x_n]$.

Consider now some general properties of ideals of a ring. The following facts are evident.

Proposition 1.3.
(1) $\operatorname{var}(\sum_{i\in\mathfrak{I}} I_i) = \bigcap_{i\in\mathfrak{I}} \operatorname{var}(I_i)$ *for any set of ideals* $\{I_i \mid i \in \mathfrak{I}\}$.
(2) $\operatorname{var}(\prod_{i=1}^k I_i) = \bigcup_{i=1}^k \operatorname{var}(I_i)$.
(3) $\operatorname{var}(\{0\}) = \mathbb{A}^n$.
(4) $\operatorname{var}(\{1\}) = \varnothing$.

Therefore, the set of all closed subsets defines a topology on $\mathbb{A}^n$ called *Zariski topology*. Their compliments, $D(S) = \mathbb{A}^n \setminus \operatorname{var}(S)$ are called *open subsets* of $\mathbb{A}^n$. For instance, the sets $D(g) = \{\mathbf{a} \mid g(\mathbf{a}) \neq 0\}$ are called *principal open subsets*. They form a basis of the Zariski topology. Every subset $X \subseteq \mathbb{A}^n$ inherits the Zariski topology from $\mathbb{A}^n$.

Note that this topology is rather weak and not Hausdorff. For instance, if $n = 1$, the only proper closed subsets of $\mathbb{A}^1$ are finite sets. Moreover, if $\Bbbk$ is infinite, hence $D(g) \neq \varnothing$ for every nonzero $g \in \Bbbk[\mathbf{x}]$, an intersection of any two nonempty open subsets is nonempty, so every open subset in *dense* in the Zariski topology. Nevertheless, it is a T_1-topology, that is every one-point set $\{\mathbf{a}\}$ is closed (**why?**).

For any subset $X \subseteq \mathbb{A}^n$ set $I(X) = \{f \in \Bbbk[\mathbf{x}] \mid f(\mathbf{a}) = 0 \text{ for all } \mathbf{a} \in X\}$. It is a radical ideal in X and $\operatorname{var}(I(X)) = \bar{X}$, the closure of X in the Zariski

topology (**why?**). Also evident that $I(\operatorname{var} I) \supseteq \sqrt{I}$. The famous Hilbert *Nullstellensatz* ("theorem on the places of zeros") shows that, under obvious restriction, we actually have equality here.

Theorem 1.4 (Hilbert Nullstellensatz)**.** *If the field $\Bbbk$ is algebraically closed, then $I(\operatorname{var}(I)) = \sqrt{I}$ for every ideal $I \subseteq \Bbbk[\mathbf{x}]$. Therefore, the maps $I \mapsto \operatorname{var}(I)$ and $X \mapsto I(X)$ establish a one-to-one correspondence between the radical ideals of $\Bbbk[x_1, x_2, \dots, x_n]$ and the Zariski closed subsets of $\mathbb{A}^n$.*

Note that this theorem is equivalent to the following one, which is also usually cited as Nullstellensatz.

Theorem 1.5. *If the field $\Bbbk$ is algebraically closed, then $\operatorname{var}(I) = \varnothing$ if and only if $I \ni 1$.*

Indeed, if 1.4 is true and $\operatorname{var}(I) = \varnothing$, then $\sqrt{I} = I(\operatorname{var}(I)) = \Bbbk[\mathbf{x}]$, so $\sqrt{I} \ni 1$, hence also $I \ni 1$. On the other hand, let 1.5 is true and $f \in I(\operatorname{var}(I))$. Consider the ideal $J = I\Bbbk[x_1, x_2, \dots, x_{n+1}] + (x_{n+1} f(x_1, x_2, \dots, x_n) - 1)$. Obviously, $\operatorname{var}(J) = \varnothing$, hence

$$1 = \sum_{i=1}^{k} g_i(x_1, x_2, \dots, x_{n+1})\, f_i(x_1, x_2, \dots, x_n) + \\ + h(x_1, x_2, \dots, x_{n+1})\,(x_{n+1} f(x_1, x_2, \dots, x_n) - 1)$$

for some $f_i \in I$, $g_i, h \in \Bbbk[x_1, x_2, \dots, x_{n+1}]$. Substitute here $x_{n+1} = 1/f$. It gives

$$1 = \sum_{i=1}^{k} g_i(x_1, x_2, \dots, x_n, 1/f) f_i(x_1, x_2, \dots, x_n).$$

Multiplying by the common denominator, we get

$$f^m = \sum_{i=1}^{k} \sum_{i=1}^{k} \tilde{g}_i(x_1, x_2, \dots, x_n) f_i(x_1, x_2, \dots, x_n),$$

hence $f \in \sqrt{I}$.

We will prove Nullstellensatz in Section 4.9.

Definition 1.6. (1) A proper ideal $I \subset R$ is called *maximal* if there are no ideals J such that $I \subset J \subset R$.

(2) A proper ideal I is called *prime* if $a \notin I$, $b \notin I$ implies $ab \notin I$.

We denote by $\operatorname{spec} R$ the set of prime ideals of R and by $\operatorname{max.spec} R$ the set of its maximal ideals.

Exercise 1.7. (1) Let $\mathbf{a} = (a_1, a_2, \dots, a_n) \in \mathbb{A}^n$, $\mathfrak{m}_{\mathbf{a}} = I(\{\mathbf{a}\})$. Prove that $\mathfrak{m}_{\mathbf{a}} = (x_1 - a_1, x_2 - a_2, \dots, x_n - a_n)$ and is a maximal ideal in $\Bbbk[x_1, x_2, \dots, x_n]$.

(2) Using Nullstellensatz, prove that if the field $\Bbbk$ is algebraically closed, every maximal ideal in $\Bbbk[x_1, x_2, \dots, x_n]$ coincides with some $\mathfrak{m}_{\mathbf{a}}$. Therefore, the points of $\mathbb{A}^n$ are in one-to-one correspondence with $\operatorname{max.spec} \Bbbk[x_1, x_2, \dots, x_n]$.

Definition 1.8. Let R be a non-zero ring.

(1) R is called a *field* if $R^\times = R \setminus \{0\}$, i.e. all nonzero elements of R are invertible.
(2) An element $a \in R$ is called a *zero divisor* if there is a non-zero element b such that $ab = 0$.
(3) R is called a *domain* (or an *integral domain*) if all its non-zero elements are non-zero-divisors.

Exercise 1.9. Let R be a non-zero ring, $I \subset R$ be a proper ideal. Prove that

(1) I is maximal if and only if R/I is a field.
(2) I is prime if and only if R/I is a domain.
(3) Every maximal ideal is prime.
(4) The ideal $\{0\} \subset \mathbb{Z}$ is prime but not maximal.

Theorem 1.10. *Let R be a ring, $I \subset R$ be a proper ideal. There is a maximal ideal $\mathfrak{m} \supseteq I$.*

Proof. We use the Zorn lemma. Let $\mathfrak{M}$ be the set of all proper ideals $J \supseteq I$ ordered by inclusion, $\mathfrak{L} \subseteq \mathfrak{M}$ be a chain and $M = \bigcup_{J \in \mathfrak{L}} J$. If $a \in M$, evidently $ba \in M$ for any $b \in R$. If $a, b \in M$, there are $J \in \mathfrak{L}$ and $J' \in \mathfrak{L}$ such that $a \in J$, $b \in J'$. As $\mathfrak{L}$ is a chain, either $J \subseteq J'$, hence $a, b \in J'$ and $a + b \in J' \subseteq M$, or $J' \subseteq J$, hence $a, b \in J$ and $a + b \in J \subseteq M$. Therefore, M is an ideal. If $M = R$, then $1 \in M$, that is $1 \in J$ for some $J \in \mathfrak{M}$, whence $J = R$, which is impossible. Hence $M \in \mathfrak{M}$ and is an upper bound of $\mathfrak{L}$. By the Zorn's lemma, $\mathfrak{M}$ has maximal elements. Each such element is a maximal ideal containing I. □

Theorem 1.11.

$$\operatorname{nil} R = \bigcap_{\mathfrak{p} \in \operatorname{spec} R} \mathfrak{p}.$$

Proof. Let $N = \bigcap_{\mathfrak{p} \in \operatorname{spec} R} \mathfrak{p}$. Obviously, every nilpotent element belongs to N. Conversely, let $a \in N$. Suppose that it is not nilpotent. Consider the set $\mathfrak{M}$ of all ideals $I \subset R$ such that $a^n \notin I$ for all n. It is not empty, since $\{0\} \in \mathfrak{M}$. It is ordered by inclusion and if $\mathfrak{L} \subseteq \mathfrak{M}$ is a chain, $M = \bigcup_{I \in \mathfrak{M}} I$ is an ideal, obviously belonging to $\mathfrak{M}$, hence an upper bound for $\mathfrak{L}$. By Zorn lemma, $\mathfrak{M}$ has a maximal element J. Suppose that $b, c \notin J$ but $bc \in J$. Then $a^n \in J + Rb$ and $a^m \in J + Rc$ for some n, m, whence $a^{m+n} \in J + Rbc = J$ which is impossible. Therefore, J is prime and $a \notin J$, so $a \notin N$, a contradiction. □

We denote by $V(I)$ the subset $\{\mathfrak{p} \in \operatorname{spec} R \mid \mathfrak{p} \supseteq I\} \subseteq \operatorname{spec} R$. Recall that there is a bijection between the ideals of R/I and the ideals $J \subseteq R$ containing I such that $R/J \simeq (R/I)/(J/I)$. Therefore, there is a bijection between $\operatorname{spec} R/I$ and $V(I)$, as well as between $\operatorname{max.spec} R/I$ and $V_{\max}(I) = V(I) \cap \operatorname{max.spec} R$.

Corollary 1.12. $\sqrt{I} = \bigcap_{\mathfrak{p} \in V(I)} \mathfrak{p}$. *In particular, an ideal I is radical if and only if it is an intersection of prime ideals.*

2. Noetherian rings

Let $a_1, a_2, \dots, a_m$ be elements of a ring A. We denote by $(a_1, a_2, \dots, a_m)$ the ideal $\{\sum_{i=1}^m b_i a_i\}$, where b_i run through A. We call $a_1, a_2, \dots, a_m$ *generators* of the ideal $I = (a_1, a_2, \dots, a_m)$ and say that I is *finitely generated*. For instance, in the ring $\mathbb{Z}$ every ideal is finitely generated (it is of the form (a) for some $a \in \mathbb{Z}$). The same is true for the polynomial ring $\Bbbk[x]$, where $\Bbbk$ is a field.

Proposition 2.1. *The following conditions for the ring A are equivalent.*

(1) *Every ideal $I \subseteq A$ is finitely generated.*
(2) *There are no infinite ascending chains of ideals $I_1 \subset I_2 \subset \ldots \subset I_n \subset \ldots$ in A.*
Then they say that A satisfies the *ascending chain condition*, or ACC.
(3) *Every non-empty set $\mathfrak{M}$ of ideals of A has a maximal element (with respect to inclusion).*

A ring satisfying these conditions is called *Noetherian*.

Proof. (1)⇒(2) Let $I_1 \subset I_2 \subset \ldots \subset I_n \subset \ldots$ be an ascending chain if ideals, $I = \bigcup_{i=1}^\infty I_i$. Then I is an ideal, hence $I = (a_1, a_2, \dots, a_m)$ for some $a_1, a_2, \dots, a_m$. Every a_j belongs to some ideal I_{i_j}. If $i^* = \max\{i_j \mid 1 \leqslant j \leqslant m\}$, then all a_j are in I_{i^*}, so $I = I_{i^*}$ and the proper inclusion $I_{i^*} \subset I_{i^*+1}$ is imposiible, a contradiction.

(2)⇒(3) Suppose there are no maximal elements in $\mathfrak{M}$. Let $I_1 \in \mathfrak{M}$. As it is not maximal in $\mathfrak{M}$, there is an ideal $I_2 \in \mathfrak{M}$ such that $I_1 \subset I_2$. As I_2 is not maximal in $\mathfrak{M}$, there is an ideal $I_3 \in \mathfrak{M}$ such that $I_2 \subset I_3$. Iterating this procedure, we obtain an infinite ascending chain $I_1 \subset I_2 \subset \ldots \subset I_n \subset \ldots$, a contradiction.

(3)⇒(1) Let I be an ideal. Consider the set $\mathfrak{M}$ of all ideals of the form $(a_1, a_2, \dots, a_m)$, where all $a_i \in I$. It has a maximal element $J = (a_1, a_2, \dots, a_m)$ for some $a_i \in I$. If $J \neq I$, there is an element $a \in I \setminus J$. Then $J' = (a_1, a_2, \dots, a_m, a)$ belongs to $\mathfrak{M}$ and is strictly bigger than I, which is impossible. Hence $I = J = (a_1, a_2, \dots, a_m)$. □

Exercise 2.2. Prove that if A is Noetherian, so is every quotient A/I.

Every principal ideal ring, such as $\mathbb{Z}$ or $\Bbbk[x]$ ($\Bbbk$ a field) is obviously Noetherian. The following theorem gives a lot of examples of Noetherian rings, which play a crucial role in Algebraic Geometry.

Theorem 2.3 (Hilbert Basis Theorem)**.** *Let the ring A be Noetherian. Then so are also*

(1) *the polynomial rings $A[x_1, x_2, \dots, x_n]$;*
(2) *the formal power series rings $A[[x_1, x_2, \dots, x_n]]$.*

Proof. We prove (2) following [7, Thm.3.3]. As for (1), the reader can see [2, Thm.7.5] or [3, Thm.1.2] or can prove it himself modelling the nearby

method with more or less evident changes (**recommended**). Obviously, it is enough to prove the theorem for the ring $A[[x]]$, the general case is obtained by an easy induction.

Let $B = A[[x]]$ and $I \subset B$ be an ideal. Denote by $I(d)$ the set of elements $a \in A$ such that I contains a series $ax^d + \sum_{i>d} a_i x^i$. Obviously, it is an ideal in A and $I(0) \subseteq I(1) \subseteq I(2) \subseteq \dots$. As A is Noetherian, there is m such that $I(d) = I(m)$ for all $d \geqslant m$. Let $\{b_{jd}\}$ be a set of generators of $I(d)$ for $d \leqslant m$ and g_{id} be a series from I such that $g_{jd} = b_{jd}x^d + \sum_{i>d} a_i x^i$. We claim that $G = \{g_{jd} \mid 0 \leqslant d \leqslant m\}$ is a set of generators of I.

Indeed, let J be the ideal generated by the set G and $f = \sum_{i=0}^{\infty} a_i x^i \in I$. Then $a_0 = \sum_j c_{j0} b_{j0}$. Set $h_0 = \sum_j c_{j0} g_{j0}$ and $f_1 = f - h_0$. Then $f_1 = \sum_{i=1}^{\infty} a_i' x^i$. Again $a_1' = \sum_j c_{j1} b_{j1}$ and, if we set $h_1 = \sum_j c_{j1} g_{j1}$ and $f_2 = f_1 - h_1$, then $f_2 = \sum_{i=2}^{\infty} a_i'' x^i$. Note that h_0 and h_1 are in J, while f_1 and f_2 are in I. Iterating this procedure until $d = m$, we obtain a presentation $f = h + f^*$, where $h \in J$, $f^* \in I$, $f^* = \sum_{i>m} a_i^* x^i$. As $I(m+1) = I(m)$, we have $a_{m+1}^* = \sum_j c_{j,m+1} b_{jm}$. Set $q_1 = \sum_j c_{j,m+1} x g_{jm}$. Then $f_1^* = f^* - q_1$ has zero terms with x^i for $i \leqslant m+1$. In the same way, $f_1^* = f_2^* + q_2$, where $q_2 = \sum_j c_{j,m+2} x^2 g_{jm}$. Iterating, we obtain that

$$f^* = \sum_{d=1}^{\infty} c_{j,m+d} x^d g_{jm} = \sum_j g_{jm} \sum_{d=1}^{\infty} c_{j,m+d} x^d \in J.$$

Therefore, $f \in J$. □

If B is an A-algebra and $b_1, b_2, \dots, b_n$ are elements from B, there is a natural homomorphism ("*evaluation*") $\mathrm{ev} : A[x_1, x_2, \dots, x_n] \to B$ mapping $\sum_{\mathbf{i}} a_{\mathbf{i}} \mathbf{x}^{\mathbf{i}}$ to $\sum_{\mathbf{i}} a_{\mathbf{i}} \mathbf{b}^{\mathbf{i}}$. Here we write $\mathbf{i}$ instead the multiindex $i_1, i_2, \dots, i_n$ and $\mathbf{x}^{\mathbf{i}}$ means $x_1^{i_1} x_2^{i_2} \dots x_n^{i_n}$ (the same for b's). If $\mathrm{Im}(\mathrm{ev}) = B$, they say that $b_1, b_2, \dots, b_n$ is a *set of generators* of the algebra B. If such a finite set of generators exists, they say that the A-algebra B is *of finite type* (or *finitely generated algebra*). Note that then $B \simeq A[x_1, x_2, \dots, x_n]/\mathrm{Ker}(\mathrm{ev})$, so we have the following

Corollary 2.4. *If the ring A is Noetherian, any A-algebra of finite type is Noetherian as well.*

A useful tool in considering Noetherian rings is the following.

Lemma 2.5 (Noetherian induction)**.** *Let A be a Noetherian ring, $\mathscr{P}$ be a property of its ideals. Suppose that an ideal $I \in M$ has the property $\mathscr{P}$ as soon as all ideals $J \in \mathfrak{M}$ such that $J \supset I$ have this property (in particular, all maximal ideals containing I have this property). Then every ideal from $\mathfrak{M}$ has property $\mathscr{P}$.*

Proof. Otherwise, let I be maximal among the ideals that does not have the property $\mathscr{P}$. By the supposition, it has this property, a contradiction. □

Theorem 2.6. *Let A be Noetherian ring, $I \subset A$ be a proper ideal. There are prime ideals $\mathfrak{p}_1, \mathfrak{p}_2, \dots, \mathfrak{p}_m$ in $V(I)$ such that every $\mathfrak{p} \in V(I)$ contains some $\mathfrak{p}_i$ and $\mathfrak{p}_i \not\supseteq \mathfrak{p}_j$ if $i \neq j$. Moreover, $\bigcap_{i=1}^m \mathfrak{p}_i = \sqrt{I}$.*

We denote $\{\mathfrak{p}_1, \mathfrak{p}_2, \dots, \mathfrak{p}_m\}$ *by* $V_{\min}(I)$.

Proof. If I is prime (for instance, maximal), we are done with $V_{\min}(I) = \{I\}$. Suppose that I is not prime and every ideal $J \supset I$ has this property. There are bigger ideals $J, J' \supset I$ such that $I \subseteq JJ'$. By the supposition, we have $V_{\min}(J) = \{\mathfrak{p}_1, \mathfrak{p}_2, \dots, \mathfrak{p}_m\}$ and $V_{\min}(J') = \{\mathfrak{q}_1, \mathfrak{q}_2, \dots, \mathfrak{q}_k\}$. If $\mathfrak{p} \supseteq J$, it contains some of $\mathfrak{p}_i$ and if $\mathfrak{p} \supseteq J'$, it contains some of $\mathfrak{q}_j$. But if $\mathfrak{p} \supseteq I \supseteq JJ'$, it contains either J or J', hence either some $\mathfrak{p}_i$ or some $\mathfrak{q}_j$. Therefore $\{\mathfrak{p}_1, \mathfrak{p}_2, \dots, \mathfrak{p}_m, \mathfrak{q}_1, \mathfrak{q}_2, \dots, \mathfrak{q}_k\} = V_{\min}(I)$. For the last claim, use Cor. 1.12. □

Exercise 2.7. In the notations of Thm. 2.6, $\bigcup_{i=1}^m \mathfrak{p}_i$ is the set of *zero divisors modulo* $\sqrt{I}$, that is elements $a \in A$ such that $ab \in \sqrt{I}$ for some $b \notin \sqrt{I}$.

This fact has an important geometrical corollary.

Definition 2.8. A topological space X is called *irreducible* if, as soon as $X = X_1 \cup X_2$ where both X_i are closed, either $X_1 = X$ or $X_2 = X$. Equivalently, any nonempty open subset $U \subseteq X$ is dense un X (**explain it**).

For instance, if $\Bbbk$ is infinite, $\mathbb{A}^n$ is irreducible with respect to to Zariski topology (**why?**). The following results use Nullstellensatz.

Theorem 2.9. *Let the field $\Bbbk$ be algebraically closed.*

1. *A closed subset $X \subseteq \mathbb{A}^n$ is irreducible if and only if the ideal $I(X)$ is prime.*
2. *Every closed subset $X \subseteq \mathbb{A}^n$ can be presented as $\bigcup_{i=1}^m X_i$, where all X_i are closed and irreducible and $X_i \not\subseteq X_j$ if $i \neq j$.*

The subsets $X_1, X_2, \dots, X_m$ are called the irreducible components *of X.*

Proof. Let $P = I(X)$.

(1) If P is not prime, there are bigger ideals $I \supset P$, $J \supset P$ such that $IJ \subseteq P$. By Nullstellensatz, $Y = \mathrm{var}(I) \subset X$, $Z = \mathrm{var}(J) \subset X$, but $Y \cup Z = X$, so X is not irreducible.

On the contrary, it $X = Y \cup Z$, where Y, Z are proper closed subsets, then $P = I \cap J \supseteq IJ$, where $I = I(Y)$, $J = I(Z)$ are strictly bigger than $I(X)$, hence $I(X)$ is not prime.

(2) $P = \bigcap_{i=1}^m \mathfrak{p}_i$, where $\{\mathfrak{p}_1, \mathfrak{p}_2, \dots, \mathfrak{p}_m\} = V_{\min}(P)$. All $\mathrm{var}(\mathfrak{p}_i)$ are irreducible, $\mathrm{var}(\mathfrak{p}_i) \not\subseteq \mathrm{var}(\mathfrak{p}_j)$ if $i \neq j$ and $X = \mathrm{var}(P) = \bigcap_{i=1}^m \mathrm{var}(\mathfrak{p}_i)$. □

3. Noetherian modules

Recall that a *module* over a ring A is an abelian group M together with the "multiplication" $A \times M \to M,\ (a, v) \mapsto av$ such that

$$\begin{aligned} a(u+v) &= au + av, \\ (a+b)v &= av + bv, \\ (ab)v &= a(bv), \\ 1v &= v \end{aligned}$$

for all $u, v \in M,\ a, b \in A$. Again, we address the reader to the book [1] for elementary properties of modules. The set of homomorphisms of A-modules $M \to N$ is denoted by $\mathrm{Hom}_A(M, N)$. It is also an A-module according to the usual addition of homomorphisms and the action of elements $a \in A$ defined as $(af)(x) = af(x) = f(ax)$.

A set of elements $\{u_i \mid i \in \mathfrak{I}\}$ of an A-module M is called a *set of generators* if every element of M can be presented as a sum $\sum_{i\in\mathfrak{J}} a_i u_i$, where $a_i \in A$ and almost all $a_i = 0$. If, moreover, such presentation is unique, this set if called a *basis* of the A-module M. A module having a basis is called *free*. If M has a finite set of generators $\{u_1, u_2, \dots, u_m\}$, we write $M = (u_1, u_2, \dots, u_m)$ (or, if necessary, $M = (u_1, u_2, \dots, u_m)_A$) and say that M is a *finite* (or a *finitely generated*) A-module.

If B is an A-algebra, we can consider it as an A-module. If it is finite, we say that B is a *finite A-algebra*. If, moreover, the map $\iota : A \to B$ is injective, we say that B is a *finite extention* of A. Obviously, any finite algebra is of finite type.

For every set $\mathfrak{I}$ there is a free module whose basis is in a one-to-one correspondence with the set $\mathfrak{I}$. Namely, we consider new symbols e_i ($i \in \mathfrak{I}$) and the set $A^{(\mathfrak{J})}$ of formal linear combinations $\sum_{i\in\mathfrak{J}} a_i e_i$, where $a_i \in A$ and almost all $a_i = 0$. We set $\sum_{i\in\mathfrak{J}} a_i e_i + \sum_{i\in\mathfrak{J}} b_i e_i = \sum_{i\in\mathfrak{J}} (a_i + b_i) e_i$ and $a \sum_{i\in\mathfrak{J}} a_i e_i = \sum_{i\in\mathfrak{J}} (a a_i) e_i$. If the set $\mathfrak{I}$ is finite, $\mathfrak{I} = i_1, i_2, \dots, i_n$, we usually identify $\sum_{j=1}^{n} a_j e_{i_j}$ with the vector $(a_1, a_2, \dots, a_n)$ and write A^n instead of $A^{(\mathfrak{J})}$. The main property of free modules is the following.

Proposition 3.1. *Let $\{v_i \mid i \in \mathfrak{I}\}$ is a set of elements of an A-module M, F be a free A-module with a basis $\{u_i \mid i \in \mathfrak{I}\}$. There is a unique homomorphism $\mathrm{ev} : F \to M$ mapping u_i to v_i. Namely, $\mathrm{ev}(\sum_{i\in\mathfrak{J}} a_i u_i) = \sum_{i\in\mathfrak{J}} a_i v_i$.*

Obviously, the map ev is surjective if and only if $\{v_i \textit{ midi } \in \mathfrak{I}\}$ is a set of generators of M and bijective if and only if it is a basis of M. Since $\mathrm{Im}\,\mathrm{ev} \simeq F/\mathrm{Ker}\,\mathrm{ev}$, we have the corollary.

Corollary 3.2. *If $\{v_i \mid i \in \mathfrak{I}\}$ is a set of generators, $M \simeq A^{(\mathfrak{J})}/N$ for some submodule $N \subseteq A^{(\mathfrak{J})}$. In particular, every finite A-module is isomorphic to a quotient A^n/N for some n and some submodule $N \subset A^n$.*

Proposition 3.3. *Let N be a submodule of M, $L = M/N$.*

(1) *If M is finite, so is L.*
(2) *If N and L are finite, so is M.*

Proof. (1) is evident.

(2) Let $N = (u_1, u_2, \dots, u_m)$ and $L = (v_1 + N, v_2 + N, \dots, v_k + N)$. We claim that $M = (u_1, u_2, \dots, u_m, v_1, v_2, \dots, v_k)$. Indeed, let $v \in M$. Then, in the quotient M/N, $v + N = \sum_{i=1}^{k} a_i(v_i + N) = (\sum_{i=1}^{k} a_i v_i) + N$ for some $a_i \in A$. It means that $v = w + \sum_{i=1}^{k} a_i v_i$ for some $w \in N$. Then $w = \sum_{j=1}^{m} b_j u_j$ for some $b_j \in A$ and $u = \sum_{j=1}^{m} b_j u_j + \sum_{i=1}^{k} a_i v_i$. □

Exercise 3.4. In the notations of Prop. 3.3, prove that if both N and L are free, so is M.

If B is an A-algebra, M is a B-module, we can consider M as an A-module.

Exercise 3.5. If B is a finite A-algebra, $B = (b_1, b_2, \dots, b_n)_A$ and M is a finite B-module, $M = (v_1, v_2, \dots, v_m)_B$. Prove that M is a finite A-module, namely, $M = (b_i v_j \mid 1 \leqslant i \leqslant n, 1 \leqslant j \leqslant m)_A$.

Proposition 3.6. *Let M be an A-module. The following conditions are equivalent.*

(1) *Every submodule $N \subseteq M$ is finite.*
(2) *There are no infinite ascending chains $N_1 \subset N_2 \subset \dots \subset N_n \subset \dots$ of submodule of N.*
(3) *Every set of submodules of M has a maximal element (by inclusion).*

A module M satisfying these conditions is called *Noetherian.*

Proof. It is the same as of Prop. 2.1, so left to the reader. □

Certainly, Noetherian induction (Lem. 2.5) can also be used for submodules of a Noetherian module.

Proposition 3.7. *Let $N \subseteq M$ be a submodule, $L = M/N$. M is Noetherian if and only if so are both N and L.*

Proof. Let M be Noetherian. If N' is a submodule of N, it is also a submodule of M, so finite. Hence N is Noetherian. If L' is a submodule of L, $M' = \{u \in M \mid u + N \in L'\}$ is a submodule of M containing N and $L' \simeq M'/N$. As M' is finite, so is L', so L is Noetherian too.

Let now N and L be Noetherian, M' be a submodule of M, $L' = M' + N/N$ and $N' = M' \cap N$. Then L' and N' are finite and $M'/N' \simeq L'$. Therefore, M' is finite and M is Noetherian. □

Corollary 3.8. (1) *The direct sum $\bigoplus_{i=1}^{n} M_i$ is Noetherian if and only if so are all modules M_i.*
(2) *If A is Noetherian, so is every finite A-module.*

(3) *If M is Noetherian, so is $A/\operatorname{Ann}_A M$.*[1] *In pafrticular, if there is an exact Noetherian A-module, A is also Noetherian.*

Proof. (1) follows from Prop. 3.7 if $n = 2$, then use induction.

(2) By (1), A^n is Noetherian for all n. Now use Cor. 3.2 and Prop. 3.7.

(3) Let $u_1, u_2, \dots, u_m$ be a set of generators of M. Define $\varphi : A \to M^n$ such that $\varphi(a) = (au_1, au_2, \dots, au_n)$. Obviously, $\operatorname{Ker}\varphi = \operatorname{Ann}_A M$, so $\operatorname{Im}\varphi \simeq A/\operatorname{Ann}_A M$. As M^n is Noetherian by (1), so is $A/\operatorname{Ann}_A M$. □

An important property of finite modules is the *Nakayama's lemma*. For an A-module M and an element $a \in A$ we denote by a_M the homomorphism $M \to M$ sending $u \mapsto au$ (*multiplication by* a).

Lemma 3.9 (NAK lemma)**.**[2] *Let M be a finite nonzero A-module and $I \subseteq A$ be an ideal such that $IM = M$. There is an element $a \in I$ such that $(1 - a)M = 0$.*

Proof. Let $u_1, u_2, \dots, u_m$ be a set of generators of M. Then there are elements $c_{ij} \in I$ such that $u_i = \sum_{j=1}^m c_{ij}u_j$. It can be wriiten as $\mathbf{u} = C\mathbf{u}$ or $(\mathbb{1} - C)\mathbf{u} = 0$, where $\mathbf{u}$ is the column $(u_1, u_2, \dots, u_m)^\top$, $\mathbb{1}$ is the unit $m \times m$ matrix and C is the $m \times m$ matrix (c_{ij}). Multiplying by the matrix adjoint to $\mathbb{1} - C$, we obtain $\det(\mathbb{1} - C)u_i = 0$, whence $\det(\mathbb{1} - C)M = 0$. Note now that $\det(\mathbb{1} - C) = 1 - a$ for some $a \in I$. □

Most often this lemma is used when I is the *radical* of A.

Definition 3.10. The intersection of all maximal ideals of A is called the *(Jacobson) radical* and denoted by $\operatorname{rad} A$. Obviously, $\operatorname{rad} A \supseteq \operatorname{nil} A$.

Proposition 3.11. $\operatorname{rad} A = \{a \in A \mid 1 - ab \text{ is invertible for any } b \in A\}$.

Proof. If $a \in \operatorname{rad} A$, also $ab \in \operatorname{rad} A$, hence $ab \in \mathfrak{m}$ for all maximal ideals $\mathfrak{m} \subset A$. Then $1 - ab \notin \mathfrak{m}$ for all $\mathfrak{m}$, hence the ideal $(1 - ab)A$ is not proper, so $(1 - ab)A \ni 1$, so there is $c \in A$ such that $(1 - ab)c = 1$.

On the contrary, let $a \notin \operatorname{rad} A$. There is a maximal ideal $\mathfrak{m} \notin a$. Then $aA + \mathfrak{m} = A$, so there are elements $b \in A$ and $c \in \mathfrak{m}$ such that $ab + c = 1$. Therefore, $1 - ab = c \in \mathfrak{m}$, hence is not invertible. □

Corollary 3.12 (Nakayama's lemma)**.** *Let $\mathfrak{r}$ be the radical of A.*

(1) *If M is a finite A-module and $\mathfrak{r}M = M$, then $M = 0$.*
(2) *Let N be a submodule of M such that M/N is finite. (If M is finite, N can be arbitrary.) If $N + \mathfrak{r}M = M$, then $N = M$.*

Exercise 3.13. Prove that a homomorphism $\alpha : M \to N$, where the module N is finite, is surjective if and only if so is the induced homomorphism $M/\mathfrak{r}M \to N/\mathfrak{r}N$.

[1] Recall that $\operatorname{Ann}_A M = \{a \in A \mid av = 0 \text{ for all } v \in M\}$. If $\operatorname{Ann}_A M = 0$, the module M is called *exact*.

[2] Sometimes this assertion is also called "Nakayama's lemma", though Nakayama attributes it to Krull and Azumaya. Following Matsumura, we call it "NAK lemma".

4. Noether Normalization and Hilbert Nullstellensatz

We are now going to prove the Hilbert Nullstellensatz. We will prove it in the form of Thm. 1.5. The main tool in this proof is the technique of *integral extensions of rings*.

Definition 4.1. Let B be an A-algebra, that is a homomorphism of rings $\iota : A \to B$ is fixed.

(1) An element $b \in B$ is called *integral over* A if there are elements $a_1, a_2, \dots, a_n \in A$ such that

$$b^n + a_1 b^{n-1} + a_2 b^{n-2} + \dots + a_n = 0. \tag{4.1}$$

(2) We denote by $\mathrm{Int}(A, B)$ the set of all elements of B integral over A and call it the *integral closure* of A in B.
(3) If $\mathrm{Int}(A, B) = B$, we call B an *integral A-algebra*. If, moreover, ι is injective, we call B an *integral extension* of A.
(4) If the homomorphism ι is injective and $\mathrm{Int}(A, B) = A$, we call A *integrally closed* in B. In particular, if a domain A is integrally closed in its field of fractions, we call A an *integrally closed domain* or a *normal ring*.

For instance, if A is a factorial domain (see PS 1), it is integrally closed (**Prove it**).

Note that if A is a field, "integral" coincides with "algebraic." The following results (as well as their proofs) just copy the corresponding results on algebraic elements and algebraic extensions.

Lemma 4.2. *Let B be an A-algebra $b \in B$. The following conditions are equivalent:*

(1) *b is integral over A.*
(2) *The subring $A[b] = \{f(b) \mid f \in A[x]\} \subseteq B$ is finite as A-module.*
(3) *There is a finite A-submodule $M \subseteq B$ such that $bM \subseteq M$ and M contains a non-zero-divisor from B.*

In particular, any finite A-algebra is integral. On the other hand, the *ring of algebraic numbers* $\mathrm{Int}(\mathbb{Z}, \mathbb{C})$ is an integral but not finite $\mathbb{Z}$-algebra (**Explain it**).

Proof. (1)⇒(2). If b satisfies the equation (4.1), then $A[b]$ is generated by $1, b, b^2, \dots, b^{n-1}$.

(2)⇒(3) is trivial: set $M = A[b]$.

(3)⇒(1). Let M be generated by $u_1, u_2, \dots, u_n$. Then $bu_j = \sum_{i=1}^n c_{ij} u_i$ for all i, or $(bI_n - C)\,(u_1, u_2, \dots, u_n)^\top = 0$, where C is the matrix (c_{ij}) with coefficients from A. Multiplying by the matrix adjoint to $bI_n - C$, we get that $\det(bI_n - C)u_i = 0$ for all i. It implies that $\det(bI_n - C)M = 0$. As M contains a non-zero-divisor, $\det(bI_n - C) = 0$. But one easily sees that $\det(bI_n - C) = b^n + a_1 b^{n-1} + b_2 b^{n-2} \dots + a_n$ for some $a_i \in A$. □

Corollary 4.3. (1) $\mathrm{Int}(A,B)$ *is an* A*-subalgebra in* B*.*
(2) *If* $b_1, b_2, \dots, b_m$ *are integral over* A*, the* A*-algebra* $A[b_1, b_2, \dots, b_n]$ *is finite.*

Proof. (1) Let $b, c \in \mathrm{Int}(A,B)$, M, N are A-submodules such that $bM \subseteq M$, $cN \subseteq N$, $M = (u_1, u_2, \dots, u_m)$, $N = (v_1, v_2, \dots, v_n)$, $\alpha \in M$ and $\beta \in N$ are non-zero-divisor. One easily sees that $MN = (u_i v_j \mid 1 \leqslant i \leqslant m, 1 \leqslant j \leqslant n)$, $bMN \subseteq MN$ and $cMN \subseteq MN$. Then $(b+c)MN \subseteq MN$, $bcMN \subseteq MN$ and $MN \ni \alpha\beta$ which is a non-zero-divisor.
(2) is obtained by induction from Lem. 4.2(2) and Exer. 3.5. □

Corollary 4.4. *If an* A*-algebra* B *is generated by elements integral over* A*, it is integral over* A*.*

If B is an A-algebra and C is a B-algebra, C can also be considered as an A-algebra.

Corollary 4.5. $\mathrm{Int}(A,C) = \mathrm{Int}(B', C)$*, where* $B' = \mathrm{Int}(A,B)$*. In particular,* $\mathrm{Int}(A,B)$ *is integrally closed in* B*, and if* B *is integral over* A *and* C *is integral over* B*, then* C *is integral over* A*.*

Proof. Obviously, $\mathrm{Int}(A,C) \subseteq \mathrm{Int}(B', C)$. Let $t \in \mathrm{Int}(B', C)$, $t^n + b_1 t^{n-1} + b_2 t^{n-2} + \cdots + b_n = 0$, where $b_i \in B'$. Then t is integral over $B'' = A[b_1, b_2, \dots, b_n]$, i.e. $tM \subseteq M$ for some finite B''-module $M \subseteq C$ containing a non-zero-divisor. By Lem. 4.2(2) and Exer. 3.5, M is also a finite A-module. Therefore, t is integral over A and $\mathrm{Int}(B', C) \subseteq \mathrm{Int}(A,C)$. □

Lemma 4.6. *Let* $B \supseteq A$ *be an integral extension. If an element* $a \in A$ *is invertible in* B*, it is invertible in* A*. In particular, if* B *is a field, so is* A*.*

Proof. As a^{-1} is integral over A, there are $c_i \in A$ such that $a^{-n} + c_1 a^{1-n} + c_2 a^{2-n} + \cdots + c_n = 0$. Multiplying by a^{n-1}, we get that $a^{-1} \in A$. □

Exercise 4.7. Let $B \supseteq A$ be an integral extension. Prove that B is a field if and only if B has no zero divisors and A is a field.

Example 4.8. Let $K = \mathbb{Q}(\sqrt{d})$, where $d \notin \{0, 1\}$ is an interger free of squares, $A = \mathrm{Int}(\mathbb{Z}, K)$ (thathe ring of integers in K). Note that $\sigma : a + b\sqrt{d} \mapsto a - b\sqrt{d}$ is an automorphism of K and $\sigma(z) = z$ for $z \in \mathbb{Z}$. It implies that $a + b\sqrt{d}$ is integral over $\mathbb{Z}$ if and only if so is $a - b\sqrt{d}$. Therefore, if $a + b\sqrt{d} \in A$, the sum $2a$ and the product $a^2 - b^2 d$ of $a \pm b\sqrt{d}$ are integers. If $a \in \mathbb{Z}$, also $b^2 d \in \mathbb{Z}$. As d is square free, $b \in \mathbb{Z}$. Suppose that $a = m/2$, where $m \in \mathbb{Z}$ is odd. Then $m^2/4 + b^2 d \in \mathbb{Z}$, which implies that $b = n/2$, where $n \in \mathbb{Z}$ is odd. Then $m^2 - dn^2 \equiv 0 \pmod 4$. As m and n are odd, $m^2 \equiv n^2 \equiv 1 \pmod 4$, hence $d \equiv 1 \pmod 4$. So, we have proved that

$$\mathrm{Int}(\mathbb{Z}, \mathbb{Q}(\sqrt{d})) = \begin{cases} \mathbb{Z}[\sqrt{d}] & \text{if } d \equiv 2 \text{ or } 3 \pmod 4, \\ \mathbb{Z}[\frac{1+\sqrt{d}}{2}] & \text{if } d \equiv 1 \pmod 4. \end{cases}$$

The following theorem (*Noether normalization*) is the crucial step in the proof of the Hilbert's Nullstellensatz.

Theorem 4.9 (Noether normalization)**.** *Let $\Bbbk$ be a field, A be a $\Bbbk$-algebra of finite type. There is a subalgebra $A_0 \simeq \Bbbk[x_1, x_2, \dots, x_d]$ $(d \leqslant n)$ such that A is integral over A_0.*

Proof. Let $A = \Bbbk[a_1, a_2, \dots, a_n]$. We use induction by n. Let $n = 1$, $A = \Bbbk[a]$. If a is algebraic, hence integral over $\Bbbk$, set $d = 0$, $A_0 = \Bbbk$. If a is transcendent, set $d = 1$, $N = A \simeq \Bbbk[x]$. Suppose that the claim is true for algebras with $n-1$ generators. If $f(a_1, a_2, \dots, a_n) \neq 0$ for all polynomials $f \in \Bbbk[x_1, x_2, \dots, x_n]$, we can set $d = n$ and $N = A \simeq \Bbbk[x_1, x_2, \dots, x_n]$. Therefore, we suppose now that there is a nonzero polynomial $f \in \Bbbk[x_1, x_2, \dots, x_n]$ such that $f(a_1, a_2, \dots, a_n) = 0$.

Choose an integer q which is bigger than any power of every x_i that occur in f and set $b_i = a_i - a_1^{q^{i-1}}$ for $2 \leqslant i \leqslant n$. If $\mathbf{k} = (k_1, k_2, \dots, k_n)$, then

$$a_1^{k_1} a_2^{k_2} \dots a_n^{k_n} = a_1^{m(\mathbf{k})} + \sum_{i=1}^{m(\mathbf{k})-1} a_1^i g_i(b_2, \dots, b_n)$$

for some polynomials g_i, where $m(\mathbf{k}) = \sum_{j=1}^{n} k_j q^{j-1}$. Moreover, as all $k_i < q$, we have that $m(\mathbf{k}) \neq m(\mathbf{k}')$ as soon as $\mathbf{k} \neq \mathbf{k}'$.

Let $m = \max m(\mathbf{k})$ for all monomials $x_1^{k_1} \dots x_n^{k_n}$ that occur in f. Then

$$f(a_1, a_2, \dots, a_n) = \lambda x_1^m + \sum_{i=1}^{m-1} h_i(b_2, \dots, b_n) a_1^i.$$

As $f(a_1, a_2, \dots, a_n) = 0$, we see that a_1 is integral over the subalgebra $B = \Bbbk[b_2, \dots, b_n]$. Therefore, A is integral over B. Since B has $n-1$ generators, it contains a subalgebra $A_0 \simeq \Bbbk[x_1, x_2, \dots, x_d]$ $(d \leqslant n-1)$ such that B is integral over A_0. By Cor. 4.5, A is integral over A_0 □

Corollary 4.10. *If a $\Bbbk$-algebra A of finite type is a field, it is an algebraic extension of $\Bbbk$.*

Proof. By Noether Normalization, there is a subalgebra A_0 such that A is integral over A_0 and $A_0 \simeq \Bbbk[x_1, x_2, \dots, x_d]$. By Lem. 4.6, A_0 is a field, hence $d = 0$, $A_0 = \Bbbk$ and A is algebraic over $\Bbbk$. □

Corollary 4.11. *Let $\mathfrak{m}$ be a maximal ideal of a $\Bbbk$-algebra A of finite type. Then $A/\mathfrak{m}$ is an algebraic extension of $\Bbbk$. In particular, if $\Bbbk$ is algebraically closed, $A/\mathfrak{m} \simeq \Bbbk$.*

Now we are ready to prove the Hilbert's Nullstellensatz in the form 1.5.

Proof of Nullstellensatz. Recall that now the field $\Bbbk$ is algebraically closed. If $\mathfrak{m}$ is a maximal ideal of $\Bbbk[x_1, x_2, \dots, x_n]$, then $\Bbbk[a_1, a_2, \dots, a_n]/\mathfrak{m} \simeq \Bbbk$ by Cor. 4.11, so we have a homomorphism $\phi : \Bbbk[x_1, x_2, \dots, x_n] \to \Bbbk$ with the kernel $\mathfrak{m}$. Set $a_i = \phi(x_i)$. Then $f(a_1, a_2, \dots, a_n) = \phi(f) = 0$ for every $f \in \mathfrak{m}$. Thus $\operatorname{var}(\mathfrak{m}) \neq \varnothing$. If I is any proper ideal, there is a maximal ideal $\mathfrak{m} \supseteq I$. Then $\operatorname{var}(I) \supseteq \operatorname{var}(\mathfrak{m}) \neq \varnothing$. □

Corollary 4.12. *Let $\Bbbk$ be an algebraically closed field. The map $\mathbf{a} \mapsto I(\mathbf{a})$ is a bijection between $\mathbb{A}^n$ and* $\operatorname{max.spec} \Bbbk[x_1, x_2, \dots, x_n]$.

Proof. **Exercise.** □

5. Localizations

Let A be a ring, $S \subseteq A$ be a *multiplicative subset*, which means that $1 \in S$ and if $a \in S$, $b \in S$, also $ab \in S$. Consider the set P of pairs (a, s), where $a \in A$, $s \in S$. We define operations on P setting

$$(a, s) + (b, t) = (at + bs, st),$$
$$(a, s)(b, t) = (ab, st).$$

We also define an equivalence relation $\sim$ on P such that $(a, s) \sim (b, t)$ if and only if there is $r \in S$ such that $art = brs$. We denote by $A[S^{-1}]$ the quotient $P/\sim$, that is the set of equivalence classes with respect to $\sim$. The equivalence class of the pair (a, s) is denoted by $\frac{a}{s}$ or a/s.

Exercise 5.1.
(1) Prove that $\sim$ is indeed an equivalence relation, that is reflexive, symmetric and transitive.
(2) Prove that if $(a, s) \sim (a', s')$ and $(b, t) \sim (b', t')$, then $(a, s) + (b, t) \sim (a', s') + (b', t')$ and $(a, s)(b, t) \sim (a', s')(b', t')$.
Therefore, these operations induce operations on the quotient set $A[S^{-1}]$.
(3) Prove that these operations define the structure of a ring on $A[S^{-1}]$. What are the zero and the unit elements of this ring?
(4) Prove that the map $\iota_S : a \mapsto a/1$ is a homomorphism of the ring A to the ring $A[S^{-1}]$ and $\operatorname{Ker} \iota_S = \{a \in A \mid sa = 0 \text{ for some } s \in S\}$.

The ring $A[S^{-1}]$ is called the *ring of fractions of A with respect to S*. If $\mathfrak{p} \subset A$ is a prime ideal, the subset $S = A \setminus \mathfrak{p}$ is multiplicative. The ring $A[S^{-1}]$ is denoted by $A_{\mathfrak{p}}$ and called the *localization of A at the prime ideal $\mathfrak{p}$*.

Obviously, $\iota_S(s) = s/1$ is invertible in $A[S^{-1}]$. Actually, ι_S is *universal* with respect to to this property.

Exercise 5.2.
(1) Prove that if $\phi : A \to B$ is a homomorphism of rings such that $\phi(s)$ is invertible for every $s \in S$, there is a unique homomorphism $\psi : A[S^{-1}] \to B$ such that $\phi = \psi\iota_S$.
(2) Let $\gamma : A \to C$ be a homomorphism such that $\gamma(s)$ is invertible for every s and if $\phi : A \to B$ is a homomorphism of rings such that $\phi(s)$ is invertible for every $s \in S$, there is a unique homomorphism $\psi : C \to B$ such that $\phi = \psi\gamma$. Prove that there is a unique isomorphism $\theta : A[S^{-1}] \to C$ such that $\theta(a/s) = \gamma(a)\gamma(s)^{-1}$.
(3) Deduce that if $T \subseteq A$ be another multiplicative subset, $A[(ST)^{-1}] \simeq A[S^{-1}][(T/1)^{-1}]$. In particular, if $\mathfrak{p} \supseteq \mathfrak{q}$ are prime ideals, $A_{\mathfrak{q}} \simeq (A_{\mathfrak{p}})_{\mathfrak{q}A_{\mathfrak{p}}}$.

If M is an A-module, we define in the same way the $A[S^{-1}]$-module $M[S^{-1}]$), called the *module of fractions of M with respect to S* (**restore the details**). Again, the homomorphism $\iota_M : M \to M[S^{-1}]$, $u \mapsto u/1$ is defined and $\operatorname{Ker}\iota_M = \{u \in M \mid S \cap \operatorname{Ann}_A u \neq \varnothing\}$. If $S = A \setminus \mathfrak{p}$, they write $M_{\mathfrak{p}}$ instead of $M[S^{-1}]$ and call $M_{\mathfrak{p}}$ the *localization of M at the prime ideal $\mathfrak{p}$*.

Exercise 5.3. (1) Prove that the ring $A[S^{-1}]$ is zero if and only if $S \ni 0$.
(2) Let the module M is finite. Prove that the module $M[S^{-1}]$ is zero if and only if $S \cap \operatorname{Ann}_A M \neq \varnothing$.
(3) Let $M = \mathbb{Q}/\mathbb{Z}$ considered as $\mathbb{Z}$-module, $S = \mathbb{Z} \setminus \{0\}$. Prove that $\operatorname{Ann}_{\mathbb{Z}} M = \{0\}$ but $M[S^{-1}] = 0$.
(4) Prove that ι_S is injective if and only if S contains no zero divisor.

In what follows we always suppose that $0 \notin S$.

We consider the correspondence between submodules of M and $M[S^{-1}]$, in particular, between ideals of A and of $A[S^{-1}]$. For a submodule $N \subseteq M$ we identify $N[S^{-1}]$ with $\{u/s \mid u \in N, s \in S\} \subseteq M[S^{-1}]$. On the contrary, if L is a submodule of $M[S^{-1}]$, set $L \cap M = \{u \in M \mid u/1 \in L\}$.[3] Note that we can consider $A[S^{-1}]$ as an A-algebra. Then, if I is an ideal of A, $I[S^{-1}] = IA[S^{-1}]$.

Proposition 5.4. (1) *$(L \cap M)[S^{-1}] = L$ for every submodule $L \subseteq M[S^{-1}]$.*
(2) *$N[S^{-1}] \cap M = \{u \in M \mid ru \in N$ for some $r \in S\}$.*
(3) *If $\mathfrak{P}$ is a prime ideal of $A[S^{-1}]$, then $\mathfrak{P} \cap A$ is a prime ideal of A and $(\mathfrak{P} \cap A) \cap S = \varnothing$.*
(4) *If $\mathfrak{p}$ is a prime ideal of S such that $\mathfrak{p} \cap S = \varnothing$, then $\mathfrak{p}[S^{-1}]$ is a prime ideal of $A[S^{-1}]$ and $\mathfrak{p}[S^{-1}] \cap A = \mathfrak{p}$. Therefore, there is a one-to-one correspondence between prime ideals of $A[S^{-1}]$ and prime ideals $\mathfrak{p} \subset A$ such that $\mathfrak{p} \cap S = \varnothing$, in particular, between prime ideals in $A_{\mathfrak{p}}$ and prime ideals $\mathfrak{q} \subseteq \mathfrak{p}$.*
(5) *If N, N' are submodules of M, then $(N+N)[S^{-1}] = N[S^{-1}]+N'[S^{-1}]$ and $(N \cap N')[S^{-1}] = N[S^{-1}] \cap N'[S^{-1}]$.*
(6) *If $I \subseteq A$ is an ideal and $N \subseteq M$ is a submodule, then $(IM)[S^{-1}] = I[S^{-1}]N[S^{-1}]$.*

Proof. (1) If $u/s \in L$, then $u/1 = (s/1)(u/s) \in L$, hence $u \in L \cap M$ and $u/s \in (L \cap M)[S^{-1}]$.

(2) $u/1 \in N[S^{-1}]$ means that there are $v \in N$, $s \in S$ such that $u/1 = v/s$, i.e. $tsu = tv \in N$ for some $t \in S$ and $ts \in S$. On the contrary, if $ru \in N$ for some $r \in S$, then $u/1 = ru/r \in N[S^{-1}]$.

(3) $ab \in \mathfrak{P} \cap A$ means that $ab/1 = (a/1)(b/1) \in \mathfrak{P}$. As $\mathfrak{P}$ is prime, either $a/1 \in \mathfrak{P}$, hence $a \in \mathfrak{P} \cap A$, or $b/1 \in \mathfrak{P}$, hence $b \in \mathfrak{P} \cap A$. If $s \in \mathfrak{P} \cap A$ for some $s \in S$, then $1/1 = s/s \in \mathfrak{P}$, which is impossible, since $\mathfrak{P}$ is a proper ideal.

[3] If S contains no elements that are zero divisors on M, that is ι_S is an embedding of M into $M[S^{-1}]$, it is indeed the intersection.

(4) If $(a/s)(b/t) = ab/st \in \mathfrak{p}[S^{-1}]$, there is $r \in S$ such that $rab \in \mathfrak{p}$. As $r \notin \mathfrak{p}$, $ab \in \mathfrak{p}$, hence either $a \in \mathfrak{p}$, hence $a/s \in \mathfrak{p}[S^{-1}]$ or $b \in \mathfrak{p}$, hence $b/s \in \mathfrak{p}[S^{-1}]$. Moreover, if $ra \in \mathfrak{p}$ for some $r \in S$, then $a \in \mathfrak{p}$, hence $\mathfrak{p}[S^{-1}] \cap A = \mathfrak{p}$.

(5) and (6) are left to a reader as easy exercises. □

Corollary 5.5. *If a module M is Noetherian, so is $M[S^{-1}]$. In particular, if a ring A is Noetherian, so is $A[S^{-1}]$.*
Is the converse true?

Example 5.6. If $\mathfrak{p} \subset A$ is a prime ideal, the set $S = A \setminus \mathfrak{p}$ is multiplicative, so the ring of fractions $A[S^{-1}]$ is defined. It is denoted by $A_{\mathfrak{p}}$ and called the *localization of A at $\mathfrak{p}$*. In the same way, the $A_{\mathfrak{p}}$-module $M[S^{-1}]$ is denote by $M_{\mathfrak{p}}$. The set $\{\mathfrak{p} \in \operatorname{spec} A \mid M_{\mathfrak{p}} \neq 0\}$ is called the *support* of the module M and denoted by $\operatorname{supp} M$. Obviously, if $\mathfrak{p} \in \operatorname{supp} M$ and $\mathfrak{p}' \supseteq \mathfrak{p}$, also $\mathfrak{p}' \in \operatorname{supp} M$ (**why?**). Note also that if $\mathfrak{p} \supseteq \operatorname{Ann}_A v = \{a \in A \mid av = 0\}$ for a nonzero element $u \in M$, then $\mathfrak{p} \in \operatorname{supp} M$ (**why**). In particular, we have the following corollary.

Corollary 5.7. (1) *$M = 0$ if and only if $M_{\mathfrak{m}} = 0$ for every maximal ideal $\mathfrak{m}$ (**explain it**).*
(2) *If $N, N' \subseteq M$ are submodules and $N_{\mathfrak{m}} \supseteq N'_{\mathfrak{m}}$ for every maximal ideal $\mathfrak{m}$, then $N \supseteq N'$ (apply (1) to $N + N'/N$).*

Exer. 5.3 shows that, if M is finite, $\operatorname{supp} M = V(\operatorname{Ann}_A M)$. On the other hand, if $M = \mathbb{Q}/\mathbb{Z}$ considered as $\mathbb{Z}$-module, then $\operatorname{Ann}_{\mathbb{Z}} M = \{0\}$, so $\{0\} \in V(\operatorname{Ann}_{\mathbb{Z}} M)$, but $M_{\{0\}} = 0$ (Exer. 5.3(3)).

Note that, if A is a domain, the ideal $\{0\}$ is prime and $A_{\{0\}}$ is just the field of fractions of A.

The localizations $A_{\mathfrak{p}}$ are important examples of *local rings*.

Definition 5.8. A ring A is called *local* if it has a unique maximal ideal $\mathfrak{m}$. The field $A/\mathfrak{m}$ is called the *residue field* of the local ring A. Obviously, $\mathfrak{m} = \operatorname{rad} A$. Note that any field is a local ring and is its own residue field.

From Prop. 5.4 we immediately obtain the following result.

Corollary 5.9. *The ring $A_{\mathfrak{p}}$ is local and $\mathfrak{p}A_{\mathfrak{p}}$ is its unique maximal ideal. Prime ideals of $A_{\mathfrak{p}}$ are just the ideals $\mathfrak{q}A_{\mathfrak{p}}$, where $\mathfrak{q}$ runs through all prime ideals $\mathfrak{q} \subseteq \mathfrak{p}$.*

The residue field $A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}$ is called the *residue field of the ring A at prime ideal $\mathfrak{p}$*. One can verify that it is isomorphic to the field of fractions of the domain $A/\mathfrak{p}$: just map the coset $(a/s) + \mathfrak{p}A_{\mathfrak{p}}$ to the fraction of cosets $(a + \mathfrak{p})/(s + \mathfrak{p})$ (**check it!**).

If $\alpha : M \to N$ is a homomorphism of modules and S is a multiplicative set in A, we define $\alpha[S^{-1}] : M[S^{-1}] \to N[S^{-1}]$ setting $\alpha[S^{-1}](v/s) = \alpha(v)/s$ for $v \in M$, $s \in S$ (**check that it is well defined**). Obviously, $(\alpha\beta)[S^{-1}] =$

$\alpha[S^{-1}]\beta[S^{-1}]$. Therefore, the map $M \mapsto M[S^{-1}]$ defines a *functor* A-Mod $\to$ $A[S^{-1}]$-Mod.[4]

Proposition 5.10. $\operatorname{Ker}(\alpha[S^{-1}]) = (\operatorname{Ker}\alpha)[S^{-1}]$ *and* $\operatorname{Im}(\alpha[S^{-1}]) = (\operatorname{Im}\alpha)[S^{-1}]$. *If* $N \subseteq M$ *is a submodule, then* $(M/N)[S^{-1}] \simeq M[S^{-1}]/N[S^{-1}]$.

Proof. If $v \in \operatorname{Ker}\alpha$, $s \in S$, then $v/s \in \operatorname{Ker}\alpha[S^{-1}]$. On the contrary, if $v/s \in \operatorname{Ker}\alpha[S^{-1}]$, that is $\alpha(v)/s = 0$ in $N[S^{-1}]$, there exists $r \in S$ such that $r\alpha(v) = 0$. Then $v/s = rv/rx$ and $\alpha(rv) = 0$, hence $v/s \in (\operatorname{Ker}\alpha)[S^{-1}]$.

The proof for images is quite analogous and left to the reader.

The isomorphism $(M/N)[S^{-1}] \simeq M[S^{-1}]/N[S^{-1}]$ is given by the map $(u+N)/s \mapsto (u/s) + N[S^{-1}]$ (**verify it**). □

Corollary 5.11. *The functor* $M \mapsto M[S^{-1}]$ *is exact, that is if a sequence*

$$\dots \to M_{n+1} \xrightarrow{\alpha_{n+1}} M_n \xrightarrow{\alpha_n} M_{n-1} \to \dots$$

is exact, so is the sequence

$$\dots \to M_{n+1}[S^{-1}] \xrightarrow{\alpha_{n+1}[S^{-1}]} M_n[S^{-1}] \xrightarrow{\alpha_n[S^{-1}]} M_{n-1}[S^{-1}] \to \dots$$

In particular the *localization functor* $M \mapsto M_{\mathfrak{p}}$ is exact.

Localization of modules can be presented as tensor product (see App. B).

Proposition 5.12. *For every* A*-module* M *the map* $A[S^{-1}] \otimes_A M \to M[S^{-1}]$, $(a/s) \otimes u \mapsto (au)/s$ *is an isomorphism.*
(**Verify that it is well defined.**)

Proof. The inverse map is defined as $u/s \mapsto (1/s) \otimes u$ (**check it**). □

Corollary 5.13. *The* A*-algebra* $A[S^{-1}]$ *is flat* (see App. B for details about flatness).

Together with Cor. 5.7 it implies that localizations completely control exactness.

Corollary 5.14. *Let*

$$\dots \to M_{n+1} \xrightarrow{\alpha_{n+1}} M_n \xrightarrow{\alpha_n} M_{n-1} \to \dots$$

be a sequence of homomorphisms of A*-modules. It is exact if and only if the seqeunce*

$$\dots \to (M_{n+1})_{\mathfrak{m}} \xrightarrow{(\alpha_{n+1})_{\mathfrak{p}}} (M_n)_{\mathfrak{m}} \xrightarrow{(\alpha_n)_{\mathfrak{m}}} (M_{n-1}))_{\mathfrak{m}} \to \dots$$

is exact for each maximal ideal $\mathfrak{m} \subset A$.

In particular, $\alpha : M \to N$ *is injective (surjective) if and only if so is* $\alpha_{\mathfrak{m}}$ *for all* $\mathfrak{m} \in \operatorname{max.spec} A$.

The following consequences of the Nakayama Lemma are rather often used. Let $\operatorname{gen}_A(M)$ denote the minimal number of elements in sets of generators of M.

[4] See Appendix A for generalities about functors and exactness.

Corollary 5.15. *Let A be a local Noetherian ring with the maximal ideal $\mathfrak{m}$ and the residue field $\Bbbk = A/\mathfrak{m}$, M be a finite A-module. For an element $v \in M$ we denote $\bar{v} = v + \mathfrak{m}M \in M/\mathfrak{m}M$.*

(1) $\operatorname{gen}_A(M) = \dim_\Bbbk M/\mathfrak{m}M$. *Namely, if $\{\bar{v}_1, \bar{v}_2, \dots, \bar{v}_m\}$ is a basis of M, $\{v_1, v_2, \dots, v_m\}$ is a minimal set of generators of M.*
(2) *M is free if and only if it is flat.*

Proof. 1) By Cor. 3.2, if $\bar{v}_1, \bar{v}_2, \dots, \bar{v}_m$ generate $M/\mathfrak{m}M$, also $v_1, v_2, \dots, v_m$ generate M and vice versa. As a basis is a minimal set of generators of the vector space $M/\mathfrak{m}M$, it proves the assertion.

2) Every free module is obviously flat. On the contrary, let M be flat. Let $v_1, v_2, \dots, v_m$ be a minimal set of generators of M, $F = A^m$ and $\{e_1, e_2, \dots, e_m\}$ be a basis of F. There is an epimorphism $\pi : F \to M$ mapping e_i to v_i. Let $K = \operatorname{Ker}\pi$, so we have an exact sequence $0 \to K \to F \to M \to 0$. Tensoring with $A/\mathfrak{m}$ and using Prop. B.12, we obtain an exact sequence

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

As $F/\mathfrak{m}F \simeq M/\mathfrak{m}M \simeq \Bbbk^m$, the last map in this sequence is an isomorphism. Therefore $K/\mathfrak{m}K = 0$. By the Nakayama Lemma, $K = 0$ and $M \simeq F$. □

6. Associated primes

Our aim now is to obtain an analogue of the well known theorem about decomposition of integers (or polynomials in one variable, or elements of a principal ideal domain) into products of primes:

$$a = p_1^{k_1} p_2^{k_2} \dots p_m^{k_m} \quad \text{all } p_i \text{ are not associated,}$$

or, in terms of ideals,

$$(a) = (p_1)^{k_1} \cap (p_2)^{k_2} \cap \dots \cap (p_m)^{k_m},$$

decomposition into intersection of powers of different prime ideals, and uniqueness of such decomposition. Later (Thm. 11.5) we will see that it is the case if A is a *Dedekind domain* (a normal Noetherian domain of dimension 1). Actually, it is a unique class of Noetherian domains with this property.

Definition 6.1. An ideal I of a ring A is called *irreducible* if $I \neq I_1 \cap I_2$ for any $I_1 \supset I$ and $I_2 \supset I$.

One easily proves that if a ring A is Noetherian, every ideal can be presented as an intersection of irreducibles $\bigcap_{i=1}^m I_m$, where $I_i \not\subseteq I_j$ for $i \neq j$ (**why?**). In a principle ideal ring irreducible ideals are just the powers of primes and this intersection is unique. The next examples show that in general it is not the case.

Example 6.2. (1) Let $A = \Bbbk[x, y]$, where $\Bbbk$ is a field, $\mathfrak{m} = (x, y)$, $I = (x, y^2)$. Then $\mathfrak{m}$ is a maximal ideal, $\mathfrak{m} \supset I \supset \mathfrak{m}^2$ and $I \neq I_1 \cap I_2$ for

any $I_1 \supset I$ and $I_2 \supset I$ (**prove it**). Therefore, I is not an intersection of powers of prime. ideals.

(2) The same holds in $A = \Bbbk[x,y]/(x^2 - y^3)$. (It is one-dimensional but not normal: $x/y \notin A$.)

(3) Let A, $\mathfrak{m}$ and I be as in Example 1, $J = (x^2, xy)$. Then $J = (x) \cap I = (x) \cap \mathfrak{m}^2$ (**check it**).

(4) Let $A = \Bbbk[x,y,z]/(xy - z^2)$, $\mathfrak{p} = (x,z)$. Then $\mathfrak{p}$ is prime but $\mathfrak{p}^2 = (x) \cap (x^2, y, z)$ is not irreducible (**prove it**). Note that this ring is normal (it can be proved as in Exam. 4.8).

So we have to modify the framework and to investigate to what extent we can guarantee existence and uniqueness of "good" decompositions. The first step in this direction is the notion of *associated primes*.

Definition 6.3. Let M be an A-module, $\mathfrak{p} \in \operatorname{spec} A$. We say that $\mathfrak{p}$ *is associated to* M if there is an element $u \in M$ such that $\mathfrak{p} = \operatorname{Ann}_A u = \{a \in A \mid au = 0\}$. Obviously, then $\mathfrak{p} \supseteq \operatorname{Ann}_A M$. We denote by $\operatorname{Ass}_A M$ (or $\operatorname{Ass} M$ if A is fixed) the set of prime ideals of A associated to M. Hence $\operatorname{Ass}_A M \subseteq V(\operatorname{Ann}_A M)$.[5]

Note that $\operatorname{Ass}\{0\} = \varnothing$, since $\operatorname{Ann} 0 = A$. So in what follows we suppose that M is a nonzero module. First, we establish some elementary properties of $\operatorname{Ass}_A M$. Note that, if $\mathfrak{p}$ is prime, $\operatorname{Ann} u = \mathfrak{p}$ for every nonzero $u \in A/\mathfrak{p}$, so $\operatorname{Ass} A/\mathfrak{p} = \{\mathfrak{p}\}$.

Proposition 6.4. *If $\mathfrak{p}$ is maximal among the annihilators of non-zero elements of M, it is prime.*

Proof. Let $\mathfrak{p} = \operatorname{Ann} u$ and $ab \in \mathfrak{p}$, i.e. $a(bu) = 0$. If $bu = 0$, then $b \in \mathfrak{p}$. Let $bu \neq 0$. As $\operatorname{Ann} bu \subseteq \operatorname{Ann} u$ and $\mathfrak{p}$ is maximal, $\operatorname{Ann} bu = \mathfrak{p}$, so $a \in \mathfrak{p}$ and $\mathfrak{p}$ is prime. □

Certainly, maximal annihilators need not exist. But they always exist if A is noetherian. Hence, $\operatorname{Ass}_A M \neq \varnothing$ if the ring A is Noetherian and $M \neq \{0\}$.

Proposition 6.5. *Let A be Noetherian, $S \subset A$ be a multiplicative set, M be an A-module. Then*

$$\operatorname{Ass} M[S^{-1}] = \{\mathfrak{p}[S^{-1}] \mid \mathfrak{p} \in \operatorname{Ass} M,\ \mathfrak{p} \cap S = \varnothing\}.$$

Proof. Let $\mathfrak{p} = \operatorname{Ann} u$ and $\mathfrak{p} \cap S = \varnothing$. Then $\mathfrak{p}[S^{-1}] \subseteq \operatorname{Ann}(u/1)$. Moreover, if $a/s \in \operatorname{Ann}(u/1)$, there is $r \in S$ such that $rau = 0$. Therefore, $ra \in \mathfrak{p}$ and $a \in \mathfrak{p}$, since $r \notin \mathfrak{p}$.

Let now $\mathfrak{P} \subset A[S^{-1}]$ be a prime ideal such that $\mathfrak{P} = \operatorname{Ann}(u/s)$, $\mathfrak{p} = \mathfrak{P} \cap A$. Then $\mathfrak{P} = \mathfrak{p}[S^{-1}]$. If $a \in \mathfrak{p}$, then $(a/1)(u/s) = 0$, i.e. there is $r \in S$ such that $aru = 0$. As $\mathfrak{p}$ is finitely generated, there is a common $r \in S$ such that $\mathfrak{p}(ru) = 0$. On the other hand, if $a(ru) = 0$, then $(a/1)(u/s) = 0$, so $a \in \mathfrak{P} \cap A = \mathfrak{p}$ and $\mathfrak{p} = \operatorname{Ann}(ru)$. □

[5] Sometimes the prime ideals associated to the module A/I are called the *prime ideals assiciated to the ideal I*. We will not use this term to prevent possible misunderstanding.

Proposition 6.6. (1) *If $N \subseteq M$ is a submodule,* $\operatorname{Ass} N \subseteq \operatorname{Ass} M \subseteq \operatorname{Ass} N \cup \operatorname{Ass}(M/N)$.

(2) $\operatorname{Ass}(\bigoplus_{i=1}^k M_k) = \bigcup_{i=1}^k \operatorname{Ass} M_i$.

(3) *If $N_1, N_2, \dots, N_k$ are submodules of M such that $\bigcap_{i=1}^k N_i = 0$, then* $\operatorname{Ass} M \subseteq \bigcup_{i=1}^k \operatorname{Ass}(M/N_i)$.

Proof. (1) Obviously, $\operatorname{Ass} N \subseteq \operatorname{Ass} M$. Let $\mathfrak{p} = \operatorname{Ann} u$ $(u \in M)$. Then $Au \simeq A/\mathfrak{p}$ and $\operatorname{Ann} v = \mathfrak{p}$ for every $v \in Au$. Hence, if $Au \cap N \neq 0$, we have $\mathfrak{p} \in \operatorname{Ass} N$. If $Au \cap N = 0$, the projection $A \to M/N$ gives an embedding $Au \to M/N$. Therefore, $\mathfrak{p} = \operatorname{Ann}(u + N) \in \operatorname{Ass}(M/N)$.

(2,3) **Exercise**. (For (3), construct an embedding $M \hookrightarrow \bigoplus_{i=1}^k (M/N_i)$). □

Theorem 6.7. *Let M be a finite module over a Noetherian ring A.*

(1) *There is a finite filtration*

$$0 = M_0 \subset M_1 \subset M_2 \subset \ldots \subset M_m = M \tag{6.1}$$

such that $M_i/M_{i-1} \simeq A/\mathfrak{p}_i$ for some prime ideals $\mathfrak{p}_i$.

We call such a filtration a *coprime filtration* of M.

(2) *For a coprime filtration* (6.1), $\operatorname{Ass}_A M \subseteq \{\mathfrak{p}_1, \mathfrak{p}_2, \dots, \mathfrak{p}_m\} \subseteq \operatorname{supp} M$ *and the minimal elments of these three sets coincide.*

(3) $\bigcup_{\mathfrak{p} \in \operatorname{Ass}_A M} \mathfrak{p} = Z(M)$, *where $Z(M)$ is the set of* zero divisors on M, *i.e such elements $a \in A$ that $au = 0$ for some nonzero $u \in M$.*

In particular, $\operatorname{Ass} M$ *is finite and contains* $V_{\min}(\operatorname{Ann}_A M)$.

Proof. (1) As we have just seen, there is a prime ideal $\mathfrak{p}_1$ such that M contains a submodule $M_1 \simeq A/\mathfrak{p}_1$. In the same way, M/M_1 contains a submodule $N_2 \simeq A/\mathfrak{p}_2$, where $\mathfrak{p}_2$ is prime. Let M_2 be the preimage of N_2 in M. Then $M_2/M_1 \simeq N_2 \simeq A/\mathfrak{p}_2$. Now $M/M_2 \supseteq N_3 \simeq A/\mathfrak{p}_3$ which gives a submodule $M_3 \supset M_2$ such thar $M_3/M_2 \simeq A/\mathfrak{p}_3$. Itereting this prodedure, we obtain the filtration (6.1). It is finite since M is Noetherian.

(2) It follows from Prop. 6.6 that $\operatorname{Ass} M \subseteq \bigcup_{i=1}^m \operatorname{Ass} M_i/M_{i-1}$. As $M_i/M_{i-1} \simeq A/\mathfrak{p}_i$, $\operatorname{Ass} M_i/M_{i-1} = \{\mathfrak{p}_i\}$. Hence $\operatorname{Ass}_A M \subseteq \{\mathfrak{p}_1, \mathfrak{p}_2, \dots, \mathfrak{p}_m\}$.

Prop. 5.10 implies that the filtration (6.1) gives a filtration of $M_\mathfrak{q}$ with the quotients $(M_i/M_{i-1})_\mathfrak{q} \simeq (A/\mathfrak{p}_i)_\mathfrak{q}$ which is non-zero if and only if $\mathfrak{q} \supseteq \mathfrak{p}_i$. Hence $\{\mathfrak{p}_1, \mathfrak{p}_2, \dots, \mathfrak{p}_m\} \subseteq \operatorname{supp} M$ and these sets have the same minimal elements.

Finally, let $\mathfrak{p}$ be a minimal element of $\operatorname{supp} M$. Then $\mathfrak{p}A_\mathfrak{p} \in \operatorname{supp} M_\mathfrak{p}$ and is minimal there. As it is a unique maximal ideal of $A_\mathfrak{p}$, $\operatorname{supp} M_\mathfrak{p} = \{\mathfrak{p}A_\mathfrak{p}\}$. As $\operatorname{Ass} M_\mathfrak{p} \neq \varnothing$, also $\operatorname{Ass} M_\mathfrak{p} = \{\mathfrak{p}A_\mathfrak{p}\}$. By Prop. 6.5, $\mathfrak{p} = \mathfrak{p}A_\mathfrak{p} \cap A \in \operatorname{Ass} M$.

(3) **Exercise**. □

Corollary 6.8. *Let A be a Noetherian ring.*

(1) $\operatorname{Ass}(A/\sqrt{I}) = V_{\min}(I)$ *for every ideal $I \subset A$.*

(2) *If A is reduced (that is* $\operatorname{nil} A = 0$*), then $Z(A) = \bigcup_{i=1}^s \mathfrak{n}_i$, where $\mathfrak{n}_1, \mathfrak{n}_2, \dots, \mathfrak{n}_s$ are all minimal prime ideals of A.*

Proof. (1) $\sqrt{I} = \bigcap_{\mathfrak{p}\in V_{\min}(I)} \mathfrak{p}$ as $\sqrt{I}$ is a radical ideal. Now use Prop. 6.6(3).
(2) follows from Thm. 6.7(3). □

The following lemma will be often used.

Lemma 6.9 (Prime Avoidness)**.** *Let $\mathfrak{p}_1, \mathfrak{p}_2, \dots, \mathfrak{p}_m$ be ideals of a ring A and at most two of then are not prime, I be an ideal. If $I \subseteq \bigcup_{i=1}^m \mathfrak{p}_i$ then $I \subseteq \mathfrak{p}_i$ for some i.*

Proof. Obviously, we can suppose that $\mathfrak{p}_i \nsubseteq \mathfrak{p}_j$ if $i \neq j$. We use induction by m. Let $m = 2$. Then $I \smallsetminus \mathfrak{p}_i \subseteq \mathfrak{p}_j$ $(j \neq i)$. Suppose there are $a_i \in I \smallsetminus \mathfrak{p}_i$. Then $a_1 + a_2 \notin \mathfrak{p}_1 \cup \mathfrak{p}_2$.

Suppose now that $m \geqslant 3$ and the claim holds for $m-1$ ideals. Let $\mathfrak{p}_1$ be prime. Note that $I = \bigcup_{i=1}^m (I \cap \mathfrak{p}_i)$. If $\mathfrak{p}_1 \cap I \subseteq \mathfrak{p}_j$ for some $j > 1$, then $I \subseteq \bigcup_{i=2}^m \mathfrak{p}_i$, therefore, $I \subseteq \mathfrak{p}_i$ for some i. Suppose that $\mathfrak{p}_1 \cap I \nsubseteq \mathfrak{p}_j$ for any $j > 1$. Then $\mathfrak{p}_1 \cap I \notin \bigcup_{i=2}^m \mathfrak{p}_i$. Choose $a \in (\mathfrak{p}_1 \cap I) \smallsetminus (\bigcup_{i=2}^m \mathfrak{p}_i)$. On the other hand, if $I \nsubseteq \mathfrak{p}_1$, also $I\mathfrak{p}_2 \dots \mathfrak{p}_m \nsubseteq \mathfrak{p}_1$. Choose $b \in (I\mathfrak{p}_2 \dots \mathfrak{p}_m) \smallsetminus \mathfrak{p}_1$. Then $I \ni (a+b) \notin \mathfrak{p}_i$ for any i. □

Corollary 6.10. *Let I be an ideal of a Noetherian ring A, M be a finite A-module. If $Iu \neq 0$ for every nonzero element $u \in M$, there is an element $a \in I$ which is a non-zero-divisor on M.*

Proof. $Iu \neq 0$ for any $u \neq 0$ means that $I \nsubseteq \operatorname{Ann} u$, hence $I \nsubseteq \mathfrak{p}$ for any $\mathfrak{p} \in \operatorname{Ass} M$. Therefore, $I \nsubseteq \bigcup_{\mathfrak{p}\in\operatorname{Ass} M} \mathfrak{p} = Z(M)$, that is contains some a which is a non-zero-divisor on M. □

7. Primary decomposition

Definition 7.1. A submodule $N \subset M$ is called *primary* if, as soon as $au \in N$ for some $a \in A$ and $u \in M \smallsetminus N$, there is m such that $a^m M \subseteq N$. In particular, an ideal $P \subseteq A$ is called *primary* if, as soon as $ab \in P$ for some $a, b \in A$, $b \notin P$, there is m such that $a^m \in I$.

Proposition 7.2. *Let A be a Noetherian ring, M be a finite A-module and $N \subseteq M$ be a submodule. N is primary if and only if $\operatorname{Ass}_A(M/N)$ consists of a unique prime ideal $\mathfrak{p}$. In this case $\mathfrak{p} = \sqrt{\operatorname{Ann}_A M/N}$ and $N = M \cap N_{\mathfrak{p}}$.*
If $\operatorname{Ass}(M/N) = \{\mathfrak{p}\}$, the submodule $N \subseteq M$ is called $\mathfrak{p}$-*primary*. In particular, if $\operatorname{Ass}(A/P) = \{\mathfrak{p}\}$ is a prime ideal, the ideal P is called $\mathfrak{p}$-*primary*.

Proof. Replacing M by M/N we can suppose that $N = 0$. If $\operatorname{Ass}_A(M) = \{\mathfrak{p}\}$, then, by Thm. 6.7(3), $Z(M) = \mathfrak{p}$, hence if $au = 0$ for some $u \neq 0$, then $a \in \mathfrak{p}$. Moreover, by Thm. 6.7(2), $\mathfrak{p}$ is a unique minimal prime ideal containing $\operatorname{Ann}_A M$, hence also $\sqrt{\operatorname{Ann}_A M}$. By Cor. 1.12, $\sqrt{\operatorname{Ann}_A M} = \mathfrak{p}$. Therefore, $a^k M = 0$ for some k, so 0 is a primary submodule. Also, if $v \neq 0$ and $av = 0$, then $a \in \mathfrak{p}$, whence $M \cap 0_{\mathfrak{p}} = \{v \mid sv = 0 \text{ for some } s \notin \mathfrak{p}\} = 0$.

On the contrary, if 0 is a primary submodule in M and $\mathfrak{p} = \operatorname{Ann}_A u$ for some $u \neq 0$, then $a^k M = 0$ for every element $a \in \mathfrak{p}$ and some k. Therefore, $a^k \in \operatorname{Ann}_A M$ and $\mathfrak{p} \subseteq \sqrt{\operatorname{Ann}_A M}$. As any associated prime ideal contains $\sqrt{\operatorname{Ann}_A M}$, it implies that $\mathfrak{p} = \sqrt{\operatorname{Ann}_A M}$ and is unique. □

Remark 7.3. If $\sqrt{\operatorname{Ann}_A(M/N)} = \mathfrak{p}$, where $\mathfrak{p}$ is maximal, then N is $\mathfrak{p}$-primary, but it is not necessarily true if $\mathfrak{p}$ is not maximal. For instance, it is not the case for the ideal $\mathfrak{p}^2$ from Exam. 6.2(4).

Definition 7.4. A submodule $N \subset M$ is called *irreducible* if it cannot be presented as an intersection $N_1 \cap N_2$, where $N_i \neq N$ $(i = 1, 2)$. For ideals it repeats the definition from Rem. 6.1.

In what follows we suppose that the ring A is Noetherian and the module M finite. Then every submodule can be presented as a finite intersection $N_1 \cap N_2 \cap \cdots \cap N_m$, where all N_i are irreducible and $N_i \nsubseteq N_j$ if $i \neq j$.

Proposition 7.5. *An irreducible submodule is primary.*

Proof. Again we can change M to M/N, so suppose that $N = \{0\}$. Let $\operatorname{Ass} M \ni \mathfrak{p}_1, \mathfrak{p}_2$ and $\mathfrak{p}_1 \neq \mathfrak{p}_2$. There are $u_1, u_2 \in M$ such that $\operatorname{Ann} u_i = \mathfrak{p}_i$, that is $Au_i \simeq A/\mathfrak{p}_i$. Then $\operatorname{Ann} v = \mathfrak{p}_i$ for every nonzero $v \in Au_i$. Therefore, $Au_1 \cap Au_2 = \{0\}$ is not irredicible. □

Proposition 7.6. *Every submodule $N \subset M$ is an intersection of irreducible (hence primary) submodules.*

Proof. If N is not irreducible, $N = N_1 \cap N_2$ for some bigger submodules. If both N_1 and N_2 are irreducible, we are done. If N_1 is not irreducible, $N_1 = N_{11} \cap N_{12}$ for some bigger submodules. Iterating this process, we obtain a necessary presentation (it must stop since M is Noetherian). □

Proposition 7.7. *If $N = \bigcap_{i=1}^m N_i$, then $\operatorname{Ass}(M/N) \subseteq \bigcup_{i=1}^m \operatorname{Ass}(M/N_i)$. In particuar, if all $N_1, N_2, \ldots, N_m$ are $\mathfrak{p}$-primary submodules, so is N.*

Proof. The homomorphism $M/N \to \bigoplus_{i=1}^m (M/N_i)$ such that

$$u + N \mapsto (u + N_1, u + N_2, \ldots, u + N_m)$$

is injective. Hence the claim follows from Prop. 6.6. □

Theorem 7.8 (Primary decomposition)**.** *Let $\operatorname{Ass}(M/N) = \{\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_m\}$, where $\mathfrak{p}_i \neq \mathfrak{p}_j$ if $i \neq j$. There are $\mathfrak{p}_i$-primary submodules $N_i \supset N$ such that $N = \bigcap_{i=1}^m N_i$, but $N \neq \bigcap_{i \neq j} N_i$ for any j. Moreover, if $\mathfrak{p}_i$ is a minimal element of $\operatorname{Ass}(M/N)$, then $N_i = M \cap N_{\mathfrak{p}_i}$, hence is uniquely defined.*

A presentation of N as an intersection of $\mathfrak{p}_i$-primary submodules with different $\mathfrak{p}_i$ is called a *primary decomposition* of N and the modules N_i are called *$\mathfrak{p}_i$-primary components* of N.

Proof. From Prop. 7.6 and 7.7 it follows that $N = \bigcap_{i=1}^m N_i$, where each N_i is $\mathfrak{p}_i$-primary for some $\mathfrak{p}_i$, $\mathfrak{p}_i \neq \mathfrak{p}_j$ for $i \neq j$ and $N_i' = \bigcap_{j \neq i} N_j \neq N$. It remains to prove that $\operatorname{Ass}(M/N) = \{\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_m\}$. We use induction. The case $m = 1$ is trivial, so we suppose that the claim holds for intersections of $m - 1$ submodules, hence $\operatorname{Ass}(M/N_i') = \{\mathfrak{p}_j \mid j \neq i\}$. Note first that $M/N \supseteq N_i'/N \simeq N_i' + N_i/N_i \subseteq M/N_i$. As $\operatorname{Ass}(M/N_i) = \{\mathfrak{p}_i\}$, also $\operatorname{Ass}(N_i'/N) = \{\mathfrak{p}_i\}$ and $\mathfrak{p}_i \in \operatorname{Ass}(M/N)$. Therefore, $\operatorname{Ass}(M/N) \supseteq \{\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_m\}$. By Prop. 7.7, also $\operatorname{Ass}(M/N) \subseteq \{\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_m\}$.

Let now $\mathfrak{p}_i$ be minimal. Note that $\mathfrak{p}_j \subseteq \mathfrak{p}$ for every $\mathfrak{p} \in \operatorname{supp}(M/N_j)$. Hence $\mathfrak{p}_i \notin \operatorname{supp}(M/N_j)$ if $j \neq i$, since $\mathfrak{p}_i \not\supseteq \mathfrak{p}_j$ for $j \neq i$. Therefore $(M/N_j)_{\mathfrak{p}_i} = 0$, which means that $(N_j)_{\mathfrak{p}_i} = (M_j)_{\mathfrak{p}_i}$. Then $N_{\mathfrak{p}_i} = \bigcap_{j=1}^m (N_j)_{\mathfrak{p}_i} = (N_i)_{\mathfrak{p}_i}$. As $\operatorname{Ann}(M/N_i) \subseteq \mathfrak{p}_i$, we have that $N_i = M \cap (N_i)_{\mathfrak{p}_i} = M \cap N_{\mathfrak{p}_i}$. □

Exam. 6.2(2) shows that if $\mathfrak{p}_i$ is not mininal in $\operatorname{Ass}_A N$, the $\mathfrak{p}_i$-primary component can be not unquely defined (take $\mathfrak{p}_i = (x, y)$).

Corollary 7.9. *Every nontrivial ideal I is an intersection of primary ideals: $I = \bigcap_{i=1}^m I_i$, where I_i is $\mathfrak{p}_i$-primare and all $\mathfrak{p}_1, \mathfrak{p}_2, \dots, \mathfrak{p}_m$ are different. If $\mathfrak{p}_i$ is minimal among $\mathfrak{p}_1, \mathfrak{p}_2, \dots, \mathfrak{p}_m$, then $I_i = I_{\mathfrak{p}} \cap A$ is uniquely defined. In particular, if I is a radical ideal, this decomposition is unique.*

8. Dimension. Artinian rings. Principal ideal theorem

Definition 8.1. (1) The *height* $\operatorname{ht} \mathfrak{p}$ of a prime ideal $\mathfrak{p}$ is the supremum of such integers h that there is an ascending chain of prime ideals

$$\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \ldots \subset \mathfrak{p}_h = \mathfrak{p}. \tag{8.1}$$

(2) The *dimension* of a ring A is

$$\dim A = \sup\{\operatorname{ht} \mathfrak{m} \mid \mathfrak{m} \in \operatorname{max.spec} A\}$$

We will prove that, if A is Noetherian, $\operatorname{ht} \mathfrak{p} < \infty$ for every prime $\mathfrak{p}$. In particular, if A is local and Noetherian, $\dim A < \infty$. If A is Noetherian, but not local, it is not neccesary so (see Nagata's Example in Appendix F). We will also prove that, if $\Bbbk$ is a field, $\dim \Bbbk[x_1, x_2, \dots, x_n] = n$. It implies that $\dim A < \infty$ for every algebra of finite type over a field.

Suppose that $\Bbbk$ is an algebraically closed field, $I \subset \Bbbk[x_1, x_2, \dots, x_n]$ is an ideal, $A = \Bbbk[x_1, x_2, \dots, x_n]/I$ and $X = \operatorname{var}(I)$. Then $\dim A$ is the maximal length of chain of prime ideals $I = \mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \mathfrak{p}_2 \subset \ldots \subset \mathfrak{p}_d$. It is just the same as the maximal length of chains of irreducible closed subsets $X = X_0 \supset X_1 \supset X_2 \supset \ldots \supset X_d$ (the dimension of X as it is defined in Algebraic Geometry).

We start with Noetherian rings of dimension 0. They happen just to be *Artinian rings*.

Definition 8.2. An A-module M is called *Artinian* if its satisfies the *descending chain condition*, DCC: there are no infinite strictly descending chains of submodules $M = M_0 \supset M_1 \supset M_2 \supset \ldots \supset M_n \supset \ldots$. Equivalently, every subset of submodules of M has a minimal element (with respect to inclusion). If A is Artinian as A-module, that is has no infinite strictly descending chains of ideals, it is called an *Artinian ring*.

Note that a vector space is Artinian if and only if it is Noetherian and if and only if it is finite dimensional. For instance, a finite dimensional algebra over a field is both Artinian and Noetherian.

Proposition 8.3. *Let N be a submodule of M. M is Artinian if and only if both N and N/M are Artinian.*

Proof. Obviously, if M is Artinian, so are N and M/N. Prove the inverse. For a submodule $L \subseteq M$ set $L' = L \cap N$ and $L'' = L + N/N \subseteq M/N$. If $L_1 \supseteq L$, also $L_1' = L'$ and $L_1'' \supseteq L''$. Suppose that $L_1' = L_1$ and $L_1'' = L''$. The latter equiality means that $L_1 + N = L + N$. If $v_1 \in L_1$, then $v_1 = v + u$, where $v \in L$, $u \in N$. Hence $u = v_1 - v \in L_1 \cap N = L \cap N$ and $v_1 \in L$, that is $L_1 = L$. Therefore, any strictly descending chain of submodules of M produces a strictly descending chain of submodules of M/N or of N, which is impossible if both are Artinian. □

Just as for Noetherian modules and rings, we have the following corollary (with the same proof).

Corollary 8.4. (1) *If a ring A is Artinian, so is every finite A-module.*
(2) *If a finite A-module M is Artinian, so is $A/\operatorname{Ann}_A M$.*

Definition 8.5. Ideals I and J are called *coprime* if $I + J = A$. For instance, so is if I is maximal and $J \notin I$.

Note that if I, J_1 are coprime as well as I, J_2, then I is coprime with $J_1 J_2$ (just multiply $(I + J_1)(I + J_2)$).

Proposition 8.6 (Chinese remainder theorem)**.** *Let any two of the ideals $I_1, I_2, \ldots, I_n$ be coprime. Then $\bigcap_{i=1}^n I_i = \prod_{i=1}^n I_i$ and $A/\prod_{i=1}^n I_i \simeq \prod_{i=1}^n A/I_i$.*

Actually, the last assertion means that given any elements $a_1, a_2, \ldots, a_n$ from A, there is an element $a \in A$ such that $a \equiv a_i \pmod{I_i}$ for all i and a is unique up to a summand from $\prod_{i=1}^n I_i$.

Proof. If $n = 2$, let $c_1 + c_2 = 1$, where $c_i \in I_i$. If $b \in I_1 \cap I_2$, then $b = c_1 b + c_2 b \in I_1 I_2$. Therefore, $A/I_1 I_2 = A/I_1 \cap I_2$ and the map $\varphi : A/I_1 I_2 \to A/I_1 \times A/I_2$ is injective. Given $a_i \in A$ $(i = 1, 2)$, set $a = c_1 a_2 + c_2 a_1$. Then $a \equiv a_i \pmod{I_i}$ $(i = 1, 2)$, hence φ is also sutjective.

Now use induction, supposing that the assertion is true for $n - 1$ ideals. Then $J = \bigcap_{i=2}^n I_i = \prod_{i=2}^n$ and is coprime with I_1. Therefore, $\bigcap_{i=1}^n I_i = I_1 \cap J = I_1 J = \prod_{i=1}^n I_i$ and

$$A/\prod_{i=1}^n I_i = A/I_1 J \simeq A/I_1 \times A/J \simeq A/I_1 \times \prod_{i=2}^n A/I_i.$$

(The last isomorphism follows from the inductive conjecture for $I_2, \ldots, I_n$.) □

Theorem 8.7. *The following conditions for a ring A are equivalent*
(1) *A is Artinian.*
(2) *A is Noetherian and* $\dim A = 0$.

Proof. (1)⇒(2). Note that if $\mathfrak{m}_i$ are different maximal ideals of A, then $A \supset \mathfrak{m}_1 \supset \mathfrak{m}_1\mathfrak{m}_2 \supset \mathfrak{m}_1\mathfrak{m}_2\mathfrak{m}_3 \supset \ldots$ is a strictly descending chain. As A is Artinian, it cannot be infinite, so max.spec A is finite: max.spec $A = \{\mathfrak{m}_1, \mathfrak{m}_2, \ldots, \mathfrak{m}_m\}$. Set $\mathfrak{m}_i = \mathfrak{m}_j$ if $i \equiv j \pmod{m}$ and $I_k = \prod_{i=1}^n \mathfrak{m}_i$. Then $I_{k-1}/I_k = I_{k-1}/\mathfrak{m}_k I_{k-1}$ is a vector space over the field $A/\mathfrak{m}_k$. It is Artinian, hence finite dimensional,

hence Noetherian. Let $R = I_m = \operatorname{rad} A$, so $R^n = I_{mn}$. As A is Artinian, the descending chain $R \supseteq R^2 \supseteq R^3 \supseteq \dots$ must stop: $R^n = R^{n+1}$ for some n. Suppose that $R^n \neq 0$ and let $J = \operatorname{Ann}_A R^n = \operatorname{Ann}_A R^{n+1}$. As $J \neq A$, there is an ideal $J' \supset J$ minimal among the ideals properly containing J. Take $a \in J' \setminus J$, then $J' = aA + J$, so J'/J is finitely generated (even cyclic). By Nakayama lemma, $aR + J \neq J'$, hence $aR + J = J$ and $aR \subseteq J = \operatorname{Ann}_A R^n$. Therefore, $a \in \operatorname{Ann}_A R^{n+1} = J$, a contradiction. Hence $R^n = 0$ and we obtain a finite filtration $A = I_0 \supseteq I_1 \supseteq I_2 \supseteq \dots \supseteq I_{mn} = R^n = 0$ with Noetherian quotients I_{k-1}/I_k. Therefore, A is Noetherian. Moreover, as R is nilpotent, $R \subseteq \mathfrak{p}$ for every prime ideal $\mathfrak{p}$, whence $\mathfrak{p} \supseteq \mathfrak{m}_i$ for some i, thus $\mathfrak{p} = \mathfrak{m}_i$. So all prime ideals are maximal and $\dim A = 0$.

(1)⇒(2). As $\dim A = 0$, all prime ideals are maximal, hence also they are minimal, so there are finitely many of them: $\operatorname{spec} A = \operatorname{max.spec} A = \{\mathfrak{m}_1, \mathfrak{m}_2, \dots, \mathfrak{m}_m\}$ and $\operatorname{rad} A = \operatorname{nil} A$. Define I_k and R as above. This time R is nilpotent, so we obtain a finite filtration $A = I_0 \supseteq I_1 \supseteq I_2 \supseteq \dots \supseteq I_{mn} = R^n = 0$ whose quotients I_{k-1}/I_k are Noetherian vector spaces, hence also Artinian. Therefore, A is Artinian. □

Corollary 8.8. *If a ring is Artinian, every element $a \in A$ is either zero divisor or invertible.*

Proof. If $a \notin \mathfrak{m}$ for every maximal ideal $\mathfrak{m}$, it is invertible. As all maximal ideals are minimal, hence associated to 0 by Thm. 6.7), any element belonging to a maximal ideal is zero divisor by the same theorem. □

Corollary 8.9. *If a finite module M is Artinian,* $\operatorname{supp} M$ *is finite.*

Exercise 8.10. Let $\mathfrak{m}$ be a maximal ideal of a Noetherian ring A, M be a finite A-module and $N \subset M$ be its submodule. The following conditions are equivalent::

(1) N is $\mathfrak{m}$-primary.
(2) $\sqrt{\operatorname{Ann}_A(M/N)} = \mathfrak{m}$.
(3) $\operatorname{supp}(M/N) = \{\mathfrak{m}\}$.

If these conditions hold, M/N is Artinian.

We apply these results to prove *Krull principle ideal theorem*. First, a definition and an auxiliary result.

Definition 8.11. For a prime ideal $\mathfrak{p} \subset A$, set

$$\mathfrak{p}^{(n)} = (\mathfrak{p}^n A_{\mathfrak{p}}) \cap A = \{a \in A \mid sa \in \mathfrak{p}^n \text{ for some } s \notin \mathfrak{p}\}$$

and call $\mathfrak{p}^{(n)}$ the *n-th sympolic power* of $\mathfrak{p}$.

Exercise 8.12. Prove that if $\mathfrak{m}$ is a maximal ideal, then $\mathfrak{m}^{(n)} = \mathfrak{m}^n$ for all n.

Lemma 8.13. *Let $\mathfrak{p} \subset A$ be a finitely generated prime ideal. If $\mathfrak{p}^{(n)} = \mathfrak{p}^{(n+1)}$, $\mathfrak{p}$ is a minimal prime ideal.*

Proof. We can replace A by the localization $A_{\mathfrak{p}}$ and suppose that A is local and $\mathfrak{p}$ is its maximal ideal, so $\mathfrak{p} = \operatorname{rad} A$. Then $\mathfrak{p}^{(n)} = \mathfrak{p}^n$. As $\mathfrak{p}$ is finitely generated, so is $\mathfrak{p}^n$ and if $\mathfrak{p}^n = \mathfrak{p}^{n+1}$ Nakayama lemma implies that $\mathfrak{p}^n = 0$. Therefore, $\mathfrak{p} = \operatorname{nil} A$ is minimal. □

Theorem 8.14 (Krull principle ideal theorem)**.** *Let A be a Noetherian ring, $a \in A$ be neither invertible nor zero divisor, $\mathfrak{p}$ be a minimal prime ideal containing a. Then* $\operatorname{ht}\mathfrak{p} = 1$.

Proof. Replacing A by $A_{\mathfrak{p}}$ we can suppose that A is local and $\mathfrak{p}$ is its maximal ideal. Then $\mathfrak{p}$ is a unique prime ideal in A/aA. By Thm. 8.7, A/aA is Artinian. $\mathfrak{p}$ is not a minimal prime ideal of A, since it contains a non-zero-divisor. Hence $\operatorname{ht}\mathfrak{p} \geqslant 1$. Let $\mathfrak{q} \subset \mathfrak{p}$ be a smaller prime ideal. The descending chain of ideals $(\mathfrak{q}^{(n)} + aA)/aA$ of the ring A/aA must stop, so $\mathfrak{q}^{(n)} + aA = \mathfrak{q}^{(n+1)} + aA$ for some n. Let $b \in \mathfrak{q}^{(n)}$, then $b = b' + ac$ for some $b' \in \mathfrak{q}^{(n+1)}$ and $c \in A$. It implies that $ac \in \mathfrak{q}^{(n)}$, so $sac \in \mathfrak{q}^n$ for some $s \notin \mathfrak{q}$. As also $a \notin \mathfrak{q}$, then $c \in \mathfrak{q}^{(n)}$, which gives that $\mathfrak{q}^{(n)} = a\mathfrak{q}^{(n)} + \mathfrak{q}^{(n+1)}$. Note that $a \in \mathfrak{p} = \operatorname{rad} A$. By Nakayama lemma, $\mathfrak{q}^{(n)} = \mathfrak{q}^{(n+1)}$ and $\mathfrak{q}$ is minimal by the preceding lemma. Therefore, $\operatorname{ht}\mathfrak{p} = 1$. □

Corollary 8.15. *A Noetherian domain is factorial if and only if every prime ideal of height* 1 *is principal.*

Proof. **Exercise.** □

9. Parameter sets and dimensions of flat extensions

9.1. **Parameter sets.** From Krull principle ideal theorem we are going to obtain the following results relating heights with generators of ideals.

Theorem 9.1. *Let A be a Noetherian ring, $I = (a_1, a_2, \ldots, a_n)$ be an ideal and $\mathfrak{p}$ be a minimal prime ideal containing I. Then* $\operatorname{ht}\mathfrak{p} \leqslant n$. *In particular,* $\operatorname{ht}\mathfrak{p} < \infty$ *for every prime ideal of A and, if A is local,* $\dim A < \infty$.

Note that this theorem also implies that in a Noetherian ring there are no infinite descending chains of prime ideals.

First we establish the following "bypass lemma."

Lemma 9.2 (Bypass lemma)**.** *Let A be a Noetherian ring, $\mathfrak{q}_1, \mathfrak{q}_2, \ldots, \mathfrak{q}_r$ be prime ideals of A and $\mathfrak{p}_0 \supset \mathfrak{p}_1 \supset \ldots \supset \mathfrak{p}_l$ be a chain of prime ideals such that $\mathfrak{p}_0 \nsubseteq \mathfrak{q}_i$ for all i. There is a chain of prime ideals $\mathfrak{p}_0 \supset \mathfrak{p}'_1 \supset \ldots \supset \mathfrak{p}'_{l-1} \supset \mathfrak{p}_l$ such that $\mathfrak{p}'_j \nsubseteq \mathfrak{q}_i$ for all i, j.*

Proof. Obviously, we can suppose that $\mathfrak{p}_l \subseteq \mathfrak{q}_i$ for all i. So we can replace A by $A/\mathfrak{p}_l$ and suppose that $\mathfrak{p}_l = 0$ and A is a domain. We can also suppose, using induction, that $\mathfrak{p}_{l-2} \nsubseteq \mathfrak{q}_i$ for all i, so, by Prime Avoidness (Lem. 6.9), there is an element $a \in \mathfrak{p}_{l-2}$ such that $a \notin \mathfrak{q}_i$ for all i. Let $\mathfrak{p}'_{l-1}$ be minimal among prime ideals contained in $\mathfrak{p}_{l-2}$ and containing a. Then $\mathfrak{p}'_{l-1} \neq \mathfrak{p}_{l-2}$, since $\operatorname{ht}\mathfrak{p}'_{l-1} = 1$ by Krull principle ideal theorem (Thm. 8.14) and $\operatorname{ht}\mathfrak{p}_{l-2} \geqslant 2$. Therefore, we have obtained the necessary chain. □

Proof of Theorem 9.1. Replaicing A by $A_{\mathfrak{p}}$, we can suppose that A is local and $\mathfrak{p}$ is its unique maximal ideal. Moreover, replacing A be $A/\operatorname{nil} A$, we can suppose that A is reduced, hence, by Cor. 6.8, its zero divisors are just elements of minimal ideals. Then the case $n = 1$ follows from Krull principle ideal theorem. So we use induction. As $\mathfrak{p} \nsubseteq \mathfrak{n}$ for each minimal prime ideal $\mathfrak{n}$, the Prime avoidness lemma 6.9 implies that some of a_i, say a_n, is a non-zero-divisor. Let $J = (a_1, a_2, \dots, a_{n-1})$. and $\mathfrak{q}_1, \mathfrak{q}_2, \dots, \mathfrak{q}_r$ be all minimal prime ideals containing J. If $\mathfrak{p} = \mathfrak{q}_i$, then $\operatorname{ht} \mathfrak{p}_i \leqslant n-1$ by induction. Let $\mathfrak{p} \neq \mathfrak{q}_i$ for all i and $\mathfrak{p} = \mathfrak{p}_0 \supset \mathfrak{p}_1 \supset \dots \mathfrak{p}_l$ be a chain of prime ideals. By Lem. 9.2, we can suppose that $\mathfrak{p}_{l-1} \nsubseteq \mathfrak{q}_i$ for all i. Set $\bar{A} = A/J$, $\bar{a} = a + J$, $\bar{\mathfrak{q}}_i = \mathfrak{q}_i/J$ and $\bar{\mathfrak{p}}_i = \mathfrak{p}_i + J/J$. Then $\bar{\mathfrak{q}}_1, \bar{\mathfrak{q}}_2, \dots, \bar{\mathfrak{q}}_r$ are all minimal prime ideals of $\bar{A}$, and $\bar{\mathfrak{p}}$ is minimal among prime ideals containing $\bar{a}_m$, hence $\operatorname{ht} \bar{\mathfrak{p}} \leqslant 1$. As $\bar{\mathfrak{p}}_{l-1} \nsubseteq \bar{\mathfrak{q}}_i$, $\bar{\mathfrak{p}}$ is minimal among the prime ideals containing $\bar{\mathfrak{p}}_{l-1}$ or, the same, $\mathfrak{p}$ is minimal among the prime ideals containing $J + \mathfrak{p}_{l-1}$. Therefore, in the quotient $A/\mathfrak{p}_{l-1}$ the ideal $\mathfrak{p}/\mathfrak{p}_{l-1}$ is minimal containing $J + \mathfrak{p}_{l-1}/\mathfrak{p}_{l-1}$. By induction, $\operatorname{ht}(\mathfrak{p}/\mathfrak{p}_{l-1}) \leqslant n-1$, hence $l - 1 \leqslant n - 1$ and $l \leqslant n$. □

There is also a result converse to Theorem 9.1.

Theorem 9.3. *Let $\mathfrak{p}$ be a prime ideal of a Noetherian ring A and $\operatorname{ht} \mathfrak{p} = n$. There are elements $a_1, a_2, \dots, a_n \in \mathfrak{p}$ such that every prime ideal containg $(a_1, a_2, \dots, a_n)$ is of height n. In particular, $\mathfrak{p}$ is also minimal prime containing $(a_1, a_2, \dots, a_n)$.*

Such set of elements is called a *parameter set* for the ideal $\mathfrak{p}$.

Proof. Using induction, we will prove the following result which is stronger than the theorem.

Claim. *Let $\mathfrak{p} = \mathfrak{p}_n \supset \mathfrak{p}_{n-1} \supset \dots \supset \mathfrak{p}_1 \supset \mathfrak{p}_0$ be a chain of prime ideals starting with $\mathfrak{p}$., There are elements $a_1, a_2, \dots, a_n \in \mathfrak{p}$ such that, for every $0 < m \leqslant n$, $\mathfrak{p}_m \supseteq I_m = (a_1, a_2, \dots, a_m)$ and all minimal primes containing $(a_1, a_2, \dots, a_m)$ are of height m.*

Replacing A by $A/\operatorname{nil} A$, we can suppose that A is reduced. For $m = 1$, take any non-zero-divisor $a_1 \in \mathfrak{p}_1$. Suppose that $m \leqslant n$ and we have already found $a_1, a_2, \dots, a_{m-1}$ such that $\mathfrak{p}_{m-1} \supseteq I_{m-1}$ and every prime ideal containg I_{m-1} is of height $m - 1$. Let $V_{\min}(I_{m-1}) = \mathfrak{q}_1, \mathfrak{q}_2, \dots, \mathfrak{q}_r$. Then $\mathfrak{p}_m \nsubseteq \mathfrak{q}_i$, hence there is an element $a_m \in \mathfrak{p}_m$ such that $a_m \notin \mathfrak{q}_i$ for every i. Then $I_m = (a_1, a_2, \dots, a_m) \nsubseteq \mathfrak{q}_i$. Let $\mathfrak{q} \in V_{\min}(I_m)$. Then $\mathfrak{q} \supset \mathfrak{q}_i$ for some i. As $\operatorname{ht} \mathfrak{q}_i = m - 1$, $\operatorname{ht} \mathfrak{q} \geqslant m$. But $\operatorname{ht} \mathfrak{q} \leqslant m$ by Thm. 9.1, therefore, $\operatorname{ht} \mathfrak{q} = m$. □

Corollary 9.4. *Let A be a local Noetherian ring with the maximal ideal $\mathfrak{m}$. $\dim A$ equals the minimal n such that $\mathfrak{m} = \sqrt{(a_1, a_2, \dots, a_n)}$ for some elements $a_1, a_2, \dots, a_n$. Equivalently, $A/(a_1, a_2, \dots, a_n)$ is Artinian (**explain it**).*

Such set of elements is called a *parameter set* for the ring A.

Definition 9.5. Let A be a local ring with the maximal ideal n and residue field $\Bbbk$. We call $\operatorname{gen}_A \mathfrak{m} = \dim_{\Bbbk} \mathfrak{m}/\mathfrak{m}^2$ the *embedding dimension* of A and

denote it by $\operatorname{emb.dim} A$. By Cor. 9.4, $\dim A \leqslant \operatorname{emb.dim} A$. If $\dim A = \operatorname{emb.dim} A$, we call A a *regular local ring.* .

Exercise 9.6. Prove that a regular local ring is a domain.

Hint: Use induction by $d = \dim A$, the case $d = 0$ is trivial. Choose $a \in \mathfrak{m}$ such that $a \notin \mathfrak{m}^2$ and $a \notin \mathfrak{q}$ for every minimal prime $\mathfrak{q}$ and prove that a minimal prime $\mathfrak{q} \subset (a)$ is zero.

9.2. **Flat extensions. Polynomial rings.** These results are useful for studying dimensions of extensions of rings, in particular, of polynomial rings.

Theorem 9.7. *Let $A \xrightarrow{\iota} B$ be a homomorphism of Noetherian rings, $\mathfrak{P}$ be a prime ideal of B and $\mathfrak{p} = \iota^{-1}(\mathfrak{P})$. Then*

(1) $\operatorname{ht}\mathfrak{P} \leqslant \operatorname{ht}\mathfrak{p} + \dim B_{\mathfrak{P}}/\mathfrak{p}B_{\mathfrak{P}}$.
(2) *If B is flat over A, the preceding inequality is actually an equality.*

Proof. Replacing A be $A_{\mathfrak{p}}$ and B by $B_{\mathfrak{P}}$, we can suppose that both A and B are local with the maximal ideals, respectively, $\mathfrak{p}$ and $\mathfrak{P}$, so $\operatorname{ht}\mathfrak{p} = \dim A$ and $\operatorname{ht}\mathfrak{P} = \dim B$. Then the assertion becomes $\dim B \leqslant \dim A + \dim B/\mathfrak{p}B$.

(1) Let $\{a_1, a_2, \dots, a_n\}$ be a parameter set for A, $\{\bar{b}_1, \bar{b}_2, \dots, \bar{b}_m\}$ be a parameter set for $B/\mathfrak{p}B$ and b_i be preimages of $\bar{b}_i$ in B. There are integers k, l such that $\mathfrak{p}^k \subseteq (a_1, a_2, \dots, a_n)$ and $\mathfrak{P}^l \subseteq (b_1, b_2, \dots, b_m) + \mathfrak{p}B$. Then $\mathfrak{P}^{kl} \subseteq (a_1, a_2, \dots, a_n, b_1, b_2, \dots, b_m)$, hence $\dim B \leqslant n + m$.

To prove (2) we need a lemma.

Lemma 9.8 (Flat Going-down)**.** *Let $A \xrightarrow{\iota} B$ be a homomorphism of Noetherian rings, $\mathfrak{P}$ be a prime ideal of B and $\mathfrak{p} = \iota^{-1}(\mathfrak{P})$. Suppose that B is flat over A and $\mathfrak{q} \subset \mathfrak{p}$ be a prime ideal in A. There is a prime ideal $\mathfrak{Q} \subset \mathfrak{P}$ such that $\iota^{-1}(\mathfrak{Q}) = \mathfrak{q}$.*

Proof. Again we can suppose that A and B are local with the maximal ideals, respectively, $\mathfrak{p}$ and $\mathfrak{P}$. Moreover, we can suppose that $\mathfrak{q}$ is maximal properly contained in $\mathfrak{p}$. We claim that $M \otimes_A B \neq 0$ for every $M \neq 0$. Indeed, suppose that $M \otimes_A B = 0$. As B is flat, then $N \otimes_A B = 0$ for every submodule of M. Let $N \subseteq M$ be nonzero and finitely generated, $N' \subset N$ be its maximal submodule. Then $N/N' \simeq A/\mathfrak{p}$ and $(N/N') \otimes_A B \simeq B/\mathfrak{p}B = 0$, which is wrong, since $\mathfrak{p}B \subseteq \mathfrak{P}$. Therefore, in particular, $(\mathfrak{p}/\mathfrak{q}) \otimes_A B \simeq \mathfrak{p}B/\mathfrak{q}B \neq 0$, i.e. $\mathfrak{p}B \supset \mathfrak{q}B$. Also $B' = B_{\mathfrak{q}}/\mathfrak{q}B_{\mathfrak{q}} \simeq B \otimes_A (A_{\mathfrak{q}}/\mathfrak{q}A_{\mathfrak{q}}) \neq 0$. Let $\mathfrak{m}'$ be a maximal ideal of B', $\mathfrak{m}$ be its preimage in $B_{\mathfrak{q}}$ and $\mathfrak{Q} = \mathfrak{m} \cap B$. Then $\mathfrak{m} \cap A_{\mathfrak{q}} = \mathfrak{q}A_{\mathfrak{q}}$, so $\mathfrak{Q} \cap A = \mathfrak{q}$. □

Now we prove (2). Let $\mathfrak{P}_0 \supset \mathfrak{P}_1 \supset \ldots \supset \mathfrak{P}_n \supseteq \mathfrak{p}B$ be a chain of prime ideals in B. Then $\mathfrak{P}_n \cap A = \mathfrak{p}$. Let also $\mathfrak{p}_n \supset \mathfrak{p}_{n+1} \supset \ldots \supset \mathfrak{p}_{n+m}$ be a chain of prime ideals of A. Using Lem. 9.8, one can construct a chain $\mathfrak{P}_n \supset \mathfrak{P}_{n+1} \supset \ldots \supset \mathfrak{P}_{n+m}$ of prime ideals of B such that $\mathfrak{P}_k \cap A = \mathfrak{p}_k$ for $k \geqslant n$. Therefore, $\dim B \geqslant \dim A + \dim B/\mathfrak{p}B$. Together with (1) it accomplishes the proof. □

Corollary 9.9. *Let A be a Noetherian ring. Then*

$$\dim A[x_1, x_2, \dots, x_n] = \dim A + n.$$

In particular,

(1) *if $\Bbbk$ is a field, then* $\dim \Bbbk[x_1, x_2, \dots, x_n] = n$;
(2) $\dim \mathbb{Z}[x_1, x_2, \dots, x_n] = n + 1$.

Proof. Obviously, we can suppose that $n = 1$. Let $B = A[x]$, $\mathfrak{P}$ is a maximal ideal in B and $\mathfrak{p} = A \cap \mathfrak{P}$. Then $B/\mathfrak{p}B \simeq \bar{A}[x]$, where $\bar{A} = A/\mathfrak{p}$. Hence $B_{\mathfrak{P}}/\mathfrak{p}B_{\mathfrak{P}} \simeq (B/\mathfrak{p}B)_{\mathfrak{P}} \simeq K[x]_{\mathfrak{P}}$, where $K = \bar{A}_{\mathfrak{p}} \simeq A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}$ is a field, As $\dim K[x] = 1$, $\dim B_{\mathfrak{P}}/\mathfrak{p}B_{\mathfrak{P}} \leqslant 1$ and $\operatorname{ht}\mathfrak{P} \leqslant \operatorname{ht}\mathfrak{p} + 1$. As obviously $\dim B \geqslant \dim A + 1$ (**explain it**), it accomplishes the proof. □

Exercise 9.10. Let A be a Noetherian ring. Prove that

$$\dim A[[x_1, x_2, \dots, x_n]] = \dim A + n.$$

10. Integral extensions and algebras of finite type

Theorem 10.1. *Let $A \subseteq B$ be an integral extension. Then* $\dim A = \dim B$.

The proof consists of several assertions that are also of independent interest.

Claim 1. *For every prime ideal $\mathfrak{p} \subset A$ there is a prime ideal $\mathfrak{P} \subset B$ such that $\mathfrak{P} \cap A = \mathfrak{p}$.*

Proof. Replacing A by $A_{\mathfrak{p}}$ and B by $B_{\mathfrak{p}}$, we can suppose that A is local and $\mathfrak{p} = \operatorname{rad} A$. It is enough to prove that $\mathfrak{p}B \neq B$, since then we can take for $\mathfrak{P}$ a maximal ideal of B containing $\mathfrak{p}B$. Suppose that $\mathfrak{p}B = B$. Then $1 = \sum_{i=1}^{m} a_i b_i$, where $a_i \in \mathfrak{p}$, $b_i \in B$. As B is integral, $B' = A[b_1, b_2, \dots, b_m]$ is a finite A-module and $\mathfrak{p}B' = B'$, which contradicts Nakayama lemma. It accomplishes the proof. □

Claim 2 (Going-up principle)**.** *Let $\mathfrak{p} \supset \mathfrak{q}$ be prime ideals of A, $\mathfrak{Q} \subset B$ be a prime ideal such that $\mathfrak{q} \cap A = \mathfrak{Q}$. There is a prime ideal $\mathfrak{P} \supset \mathfrak{Q}$ such that $\mathfrak{P} \cap A = \mathfrak{p}$.*

Proof. $A/\mathfrak{q} \subseteq B/\mathfrak{Q}$ is also an integral extension, so there is a prime ideal $\bar{\mathfrak{P}} \subset B/\mathfrak{Q}$ such that $\bar{\mathfrak{P}} \cap (A/\mathfrak{q}) = \mathfrak{p}/\mathfrak{q}$. Take for $\mathfrak{P}$ the preimage of $\bar{\mathfrak{P}}$ in B. □

Claim 3. *Let $\mathfrak{p}_0 \supset \mathfrak{p}_1 \supset \ldots \supset \mathfrak{p}_l$ be a chain of prime ideals of A, $\mathfrak{P}_l \subset B$ be a prime ideal such that $\mathfrak{P}_l \cap A = \mathfrak{p}_l$. There is a chain $\mathfrak{P}_0 \supset \mathfrak{P}_1 \supset \ldots \supset \mathfrak{P}_l$ of prime ideals of B such that $\mathfrak{P}_i \cap A = \mathfrak{p}_i$. Therefore,* $\dim B \geqslant \dim A$.

Proof. Case $l = 1$ is just Claim 2. The general case folows by the evident induction □

Claim 4. *Let $A \subseteq B$ be an integral extension, $\mathfrak{P} = \mathfrak{P}_0 \supset \mathfrak{P}_1 \supset \ldots \supset \mathfrak{P}_l$ be a chain of prime ideals of B, $\mathfrak{p} = \mathfrak{P} \cap A$ and $\mathfrak{p}_i = \mathfrak{P}_i \cap A$. Then $\mathfrak{p} = \mathfrak{p}_0 \supset \mathfrak{p}_1 \supset \ldots \supset \mathfrak{p}_l$. Therefore,* $\operatorname{ht}\mathfrak{p} \geqslant \operatorname{ht}\mathfrak{P}$ *and* $\dim A \geqslant \dim B$.

Proof. Obviously, it is enough to prove the assertion for $l = 1$. Replacing A and B by $A/\mathfrak{p}_1$ and $B/\mathfrak{P}_1$, we can suppose that B is a domain and have to prove that if $\mathfrak{P} \subset B$ is non-zero, $\mathfrak{P} \cap A \neq 0$. Take a non-zero $b \in \mathfrak{P}$. Then $b^k + a_1 b^{k-1} + \cdots + a_k = 0$ for some $a_1, a_2, \ldots, a_k \in A$ and if k is minimal, $a_k \neq 0$. But $a_k \in \mathfrak{P} \cap A$. □

Exercise 10.2. Let $A \subseteq B$ be a finite extension of a Noetherian ring A. Prove that $\#\{\mathfrak{P} \in \operatorname{spec} B \mid \mathfrak{P} \cap A = \mathfrak{p}\} \leqslant \operatorname{gen}_A B$.

Remark 10.3. If $\mathfrak{p} \subset A$ is a prime ideal, $h = \operatorname{ht} \mathfrak{p}$, then $\dim A/\mathfrak{p} \leqslant \dim A - h$. Here is an example showing that this inequality can be strict.

Let $A = \Bbbk[[t]][x]$ (polynomials over the formal series ring $\Bbbk[[t]]$) and $a = tx - 1$. Then $A/(a) \simeq \Bbbk((t))$, the field of formal Laurant series (**prove it**). Therefore, (a) is a prime ideal of height 1, but $\dim A/(a) = 0 \neq \dim A - \operatorname{ht}(a)$.

Nevertheless, the situation becomes much better if we consider the "geometrical case," when A is an algebra of finite type over a field. First we consider extensions of *normal rings*, that is integrally closed domains, and establish the so called *Gauss lemma*.

Lemma 10.4 (Gauss lemma)**.** *Let A be a normal ring, K be its field of fractions, $f(x) \in A[x]$ and $g(x) \in K[x]$ be monic polynomials such that $g(x) \mid f(x)$. Then $g(x) \in A[x]$.*

Proof. Let $\deg g = n$. In some extension L of the field K it decomposes as $g(x) = \prod_{i=1}^{n}(x - \lambda_i)$. As $f(\lambda_i) = 0$, all λ_i are intergal over A. Therefore, the coefficiens of g, which are polynomials in λ_i with integral coefficients, also are integral over A. As A is normal, they belong to A. □

We also need a slight generalization of the criterion for integral elements.

Lemma 10.5. *Let $A \subseteq B$ be an extension of rings, $I \subset A$ be an ideal and $b \in B$. The following conditions are equivalent:*

1. *For some n there are elelments $a_1, a_2, \ldots, a_n \in I$ such that $b^n + a_1 b^{n-1} + \cdots + a_n = 0$.*
2. *There is a finitely generated submodule $M \subseteq B$ such that $\operatorname{Ann}_A M = 0$ and $bM \subseteq IM$.*

   If A and B are domains, A is normal and I is prime, these conditions are also equivalent to
3. *The minimal polynomial for b has all coefficients from I, except the leading one.*

Proof. (1) ⇔ (2). Just repeat the proof of Lem. 4.2.

(3) ⇒ (1) is trivial.

(1) ⇒ (3). Let $f(x) = x^n + a_1 x^{n-1} + \cdots + a_n = 0$, where $a_i \in I$, be such that $f(x) = 0$ and $g(x)$ be the minimal polynomial of b. Then $g(x) \in A[x]$ and $f(x) = g(x)h(x)$ for a monic polynomial $h(x)$. By Gauss lemma, $g(x)$ and $h(x)$ are from $A[x]$. Then $x^n \equiv g(x)h(x) \pmod{I}$. As A/I is a domain, $g(x) \equiv x^m \pmod{I}$ for some m. □

Theorem 10.6. *Let $A \subseteq B$ be a finite extension of Noetherian domains, A be normal, $\mathfrak{p}$ be a prime ideal of A and $\mathfrak{P}$ be a prime ideal of B.*

(1) *If $\mathfrak{P}$ is a minimal prime ideal of B containing $\mathfrak{p}$, then $\mathfrak{P} \cap A = \mathfrak{p}$.*
(2) (Going-down for normal rings). *If $\mathfrak{P} \cap A = \mathfrak{p}$ and $\mathfrak{q} \subset \mathfrak{p}$ is a prime ideal of A, there is a prime ideal $\mathfrak{Q}$ of B such that $\mathfrak{P} \supset \mathfrak{Q}$ and $\mathfrak{Q} \cap A = \mathfrak{q}$.*
(3) *If $\mathfrak{P} \cap A = \mathfrak{p}$, then $\operatorname{ht}\mathfrak{P} = \operatorname{ht}\mathfrak{p}$.*

Proof. (1) Let $I = \sqrt{\mathfrak{p}B}$, $\mathfrak{P} = \mathfrak{P}_1, \mathfrak{P}_2, \dots, \mathfrak{P}_k$ be minimal prime ideals of B comtaining I. Then $I = \bigcap_{i=1}^{k} \mathfrak{P}_i$. Suppose that $\mathfrak{p}' = \mathfrak{P} \cap A \neq \mathfrak{p}$. Choose $a \in \bigcap_{i=2}^{k} \mathfrak{P}_i \setminus \mathfrak{P}$ and $b \in \mathfrak{p}' \setminus \mathfrak{p}$. Then $ab \in I$, so $(ab)^r \in \mathfrak{p}B$ for some r. Let $x^n + c_1 x^{n-1} + \dots + c_n \in A[x]$ be the minimal polynomial of a^r. Then the minimal polynomial for $(ab)^r$ is $x^n + c_1 b^r x^{n-1} + \dots + c_n b^{rn}$. By Lem. 10.5(3), $c_i b^{ri} \in \mathfrak{p}$ for all i. As $b \notin \mathfrak{p}$, all $c_i \in \mathfrak{p}$ and $a^r \in \mathfrak{p}B \subset \mathfrak{P}$, a contradiction.

(2) Just take for $\mathfrak{Q}$ a minimal prime ideal such that $\mathfrak{P} \supset \mathfrak{Q} \supseteq \mathfrak{q}B$.

(3) $\operatorname{ht}\mathfrak{p} \geqslant \operatorname{ht}\mathfrak{P}$ is Claim 4 of Thm. 10.1. An obvious induction using (2) shows that if $\mathfrak{p} = \mathfrak{p}_0 \supset \mathfrak{p}_1 \supset \dots \supset \mathfrak{p}_n$ is a chain of prime ideals in A, there is a chain of prime ideals $\mathfrak{P} = \mathfrak{P}_0 \supset \mathfrak{P}_1 \supset \dots \supset \mathfrak{P}_n$ in B such that $\mathfrak{P}_i \cap A = \mathfrak{p}_i$. Therefore, $\operatorname{ht}\mathfrak{P} \geqslant \operatorname{ht}\mathfrak{p}$. □

Now we go to the geometrical situation.

Theorem 10.7. *Let A be an integral algebra of finite type over a field $\Bbbk$. If $\mathfrak{p}$ is a prime ideal in A, then $\operatorname{ht}\mathfrak{p} + \dim A/\mathfrak{p} = \dim A$.*

Proof. By Noether Normalization, there is a subalgebra $N \subseteq A$ such that $N \simeq \Bbbk[a_1, a_2, \dots, a_d]$ and A is integral (hence finite) over N. Then $\dim A = d$. Let $\operatorname{ht}\mathfrak{p} = h$. We will prove the theorem by induction on h. Note that N is factorial, hence normal, therefore, $\operatorname{ht}(\mathfrak{p} \cap N) = h$ by Thm. 10.6(3).

Let $h = 1$. As N is factorial, $\mathfrak{p} \cap N = (f)$, a principal ideal, by Cor. 8.15. Just as in the proof of Thm. 4.9, we can suppose that $f = x_d^n + g_1 x_d^{n+1} + \dots + g_n$, where $g_i \in \Bbbk[x_1, x_2, \dots, x_{n-1}]$. Let $N' = \Bbbk[x_1, x_2, \dots, x_{n-1}, f]$. It is isomorphic to $\Bbbk[x_1, x_2, \dots, x_n]$, hence of dimension d, and N is integral over N', hence so is also A. Moreover, $N' \cap \mathfrak{p} = (f)$, hence $N'/(\mathfrak{p} \cap N') \simeq \Bbbk[x_1, x_2, \dots, x_{n-1}]$, so $\dim N'/(\mathfrak{p} \cap N') = d - 1$. Obviously, $A/\mathfrak{p}$ is integral over $N/(\mathfrak{p} \cap N')$, thus also $\dim A/\mathfrak{p} = d - 1$.

If $h > 1$, consider a chain of prime ideals $0 \subset \mathfrak{p}_1 \subset \mathfrak{p}_2 \subset \dots \subset \mathfrak{p}_h = \mathfrak{p}$. Then $\operatorname{ht}\mathfrak{p}_1 = 1$, therefore, as we have just proved, $\dim A/\mathfrak{p}_1 = d - 1$. Obviously, $\operatorname{ht}\mathfrak{p}/\mathfrak{p}_1 = h - 1$. By induction, $\dim A/\mathfrak{p} = (d-1) - (h-1) = d - h$. □

Corollary 10.8. *Let $A \subseteq B$ be an integral extension of domains that are algebras of finite type over a field, $\mathfrak{p} \in \operatorname{spec} A$, $\mathfrak{P} \in \operatorname{spec} B$ and $\mathfrak{P} \cap A = \mathfrak{p}$. Then $\operatorname{ht}\mathfrak{p} = \operatorname{ht}\mathfrak{P}$.*

Proof. Obviously, $B/\mathfrak{P}$ is an integral extension of $A/\mathfrak{p}$. Hence $\operatorname{ht}\mathfrak{p} = \dim A - \dim A/\mathfrak{p} = \dim B - \dim B/\mathfrak{P} = \operatorname{ht}\mathfrak{P}$. □

Remark 10.9. If $A = \Bbbk[x_1, x_2, \dots, x_n]/I(X)$, where X is an irreducible closed subset in $\mathbb{A}^n$, and Y is the irreducible closed subset in X defined by the ideal $\mathfrak{p}$, they call $\operatorname{ht}\mathfrak{p}$ the *codimension* of Y in X and denote it by $\operatorname{codim} Y$. It is the maximal length of chains $Y = Y_0 \subset Y_1 \subset \ldots \subset Y_l = X$ of irreducible closed subsets of X. Theorem 10.7 claims that $\dim Y + \operatorname{codim} Y = \dim X$. An important corollary is the following. Let Y be a hypersurface in X, that is $Y = V(f)$ for a nonzero element $f \in A$. By Krull principle ideal theorem, all minimal prime ideals $\mathfrak{p} \ni f$ are of height 1, hence, dimensions of all components of Y equal $\dim X - 1$. On the contrary, suppose that A is factorial (for instance, $X = \mathbb{A}^n$) and $\dim Y = \dim X - 1$. Then $\operatorname{ht}\mathfrak{p} = 1$, hence $\mathfrak{p}$ is principle by Cor. 8.15. It means that $Y = V(f)$ is a hypersurface in X, that is defined by 1 equation. In general case, when A is not necessarily factorial, we can only claim that there is one element $f \in A$ such that Y is an irreducible component of a hypersurface $V(f)$ and all other components are also of codimention 1.

11. Normal rings. Dedekind domains

Recall that a *normal ring* is a domain intergrally closed in its field of fractions. First we consider the case of local rings of dimension 1.

Theorem 11.1. *Let A be a local Noetherian ring with the maximal ideal $\mathfrak{m}$. The following conditions are equivalent:*

1. *A is normal and $\dim A = 1$.*
2. *A is a principle ideal domain.*
3. *A is regular of dimension 1.*
4. *A is normal with the field of fractions K and there is an element $q \in K \setminus A$ such that $q\mathfrak{m} \subset A$.*

If these conditions hold, A is called a *discrete valuation ring.*

Proof. (3)⇒(2). Note that (3) means that $\mathfrak{m}$ is of height 1 and is generated by an element a. Then $\mathfrak{m}^n = (a^n)$. Let $\mathfrak{q}$ be a minimal prime ideal. If $b \in \mathfrak{q}$, then $b = ac$ for some c. As $a \notin \mathfrak{q}$, $c \in \mathfrak{q}$, hence $\mathfrak{q} = a\mathfrak{q}$ and $\mathfrak{q} = 0$ by Nakayama lemma, so A is a domain. Since a^n is a non-zero-divisor, $a^n A \simeq A$, hence $\mathfrak{m} \cdot \mathfrak{m}^n = \mathfrak{m}^{n+1}$ is a unique maximal ideal properly contained in $\mathfrak{m}^n$. If I is a nonzero ideal, then $\mathfrak{m}$ is a unique prime ideal containing I, hence $\sqrt{I} = \mathfrak{m}$, i.e. $I \supseteq \mathfrak{m}^k$ for some k, thus $I \nsubseteq \mathfrak{m}^{k+1}$. Let n be the biggest such that $I \subseteq \mathfrak{m}^n$. If $I \subset \mathfrak{m}^n$, it is contained in the unique maximal ideal properly contained in $\mathfrak{m}^n$, that is in $\mathfrak{m}^{n+1}$, which is implossible. Therefore, $I = \mathfrak{m}^n = (a^n)$.

(2)⇒(1). A principle ideal domain is of dimension 1 and factorial, hence normal.

(1)⇒(4). Let $0 \neq a \in \mathfrak{m}$. As $\dim A = 1$, $\sqrt{(a)} = \mathfrak{m}$, i.e. $\mathfrak{m}^n \subseteq (a)$ for some n. Let n be minimal and $b \in \mathfrak{m}^{n-1} \setminus (a)$. Then $q = b/a \notin A$, but $q\mathfrak{m} \subseteq A$.

(4)⇒(3) If $q\mathfrak{m} \subseteq \mathfrak{m}$, then q is integral over A, hence $q \in A$, which is excluded. Therefore, $q\mathfrak{m} = A$ and $\mathfrak{m} = q^{-1}A$. As A is not as field, $\dim A = 1$ and A is regular. □

The following theorem gives a criterion for a Noetherian domain to be normal.

Theorem 11.2. *Let A be a Noetherian domain with the field of fractions K, $\mathbf{P} = \{\mathfrak{p} \in \operatorname{spec} A \mid \operatorname{ht}\mathfrak{p} = 1\}$ (minimal nonzero prime ideals). The following conditions are equivalent:*

(1) *A is normal.*
(2) *For every $\mathfrak{p} \in \mathbf{P}$ the localization $A_\mathfrak{p}$ is a discrete valuation ring and $A = \bigcap_{\mathfrak{p}\in\mathbf{P}} A_\mathfrak{p}$.*

Proof. (2)⇒(1), since all discrete valuation ring are normal and intersection of normal subrings of K is obviously normal.

(1)⇒(2). If A is normal, so is every ring of fractions $A[S^{-1}]$, hence all $A_\mathfrak{p}$ with $\mathfrak{p} \in \mathbf{P}$ are discrete valuation ring. Let $q \in \bigcap_{\mathfrak{p}\in\mathbf{P}} A_\mathfrak{p}$ and $I = \{a \in A \mid aq \in A\}$. Suppose that $q \notin A$, hence $I \neq A$, and let $\mathfrak{p}$ be a minimal prime ideal containing I. Then $q \notin A_\mathfrak{p}$, hence $\mathfrak{p} \notin \mathbf{P}$. Note that $\sqrt{IA_\mathfrak{p}} = \mathfrak{p}A_\mathfrak{p}$, that is $\mathfrak{p}^k A_\mathfrak{p} \subseteq IA_\mathfrak{p}$ for some k and $\mathfrak{p}^k A_\mathfrak{p} \cdot q \in A_\mathfrak{p}$. Let k be minimal and $a \in \mathfrak{p}^{k-1}A_\mathfrak{p}$ be such that $aq \notin A_\mathfrak{p}$. Then $(aq)\mathfrak{p}A_\mathfrak{p} \subseteq A_\mathfrak{p}$. By Thm. 11.1, $A_\mathfrak{p}$ is a discrete valuation ring, hence $\operatorname{ht}\mathfrak{p} = 1$ and $\mathfrak{p} \in \mathbf{P}$, a contradiction. Therefore, $A = \bigcap_{\mathfrak{p}\in\mathbf{P}} A_\mathfrak{p}$. □

Exercise 11.3. We have seen that for local rings of dimension 1 "normal" and "regular" is the same. The following example shows that it is not the case for bigger dimensions. We consider the local ring $A = \Bbbk[[x, y, z]]/(xy - z^2)$, where $\Bbbk$ is a field of characteristic not 2.

(1) Prove that A is normal (use the fact that $\Bbbk[[x, y]]$ is factorial).
(2) Prove that $\dim A = 2$, but $\operatorname{gen}_A \mathfrak{m} = 3$, where $\mathfrak{m}$ is the maximal ideal.

Definition 11.4. A normal Noetherian domain D of dimension 1 (that is such that every nonzero prime ideal is maximal) is called a *Dedekind domain.*

Thm. 11.2 shows that a Dedekind domain is a Noetherian domain such that for every maximal ideal $\mathfrak{m} \subset D$ the localization $D_\mathfrak{m}$ is a discrete valuation ring.

Dedekind domains are just those rings whose arithmetics is the most similar to that of integers or polynomials.

Theorem 11.5. *Let A be a Dedekind domain $\mathbf{M} = \operatorname{max.spec} A$. Every nonzero ideal $I \subseteq A$ uniquely decomposes as*

$$I = \prod_{\mathfrak{p}\in\mathbf{M}} \mathfrak{p}^{k_\mathfrak{p}} = \bigcap_{\mathfrak{p}\in\mathbf{M}} \mathfrak{p}^{k_\mathfrak{p}}, \tag{11.1}$$

where almost all $k_\mathfrak{p} = 0$ (as usually, we denote $\mathfrak{p}^0 = A$).

Proof. Note that, as $\mathfrak{p}$ and $\mathfrak{q}$ are coprime for any two maximal ideals, so are also $\mathfrak{p}^k$ and $\mathfrak{q}^l$, hence the intersection of such powers always coincides with their product. Note also that $\mathfrak{q}A_\mathfrak{p} = A_\mathfrak{p}$, since $\operatorname{Ann}_A(A/\mathfrak{q}) = \mathfrak{q} \notin \mathfrak{p}$. If

I is an arbitrary nonzero ideal in A, for every maximal ideal $\mathfrak{p}$ there is an integer $k_\mathfrak{p} \geqslant 0$ such that $IA_\mathfrak{p} = \mathfrak{p}^{k_\mathfrak{p}}A_\mathfrak{p}$. Moreover, almost all $k_\mathfrak{p} = 0$ (**why?**). Set $I' = \bigcap_{\mathfrak{p}\in\mathbf{P}} \mathfrak{p}^{k_\mathfrak{p}}$. Then $I_\mathfrak{p} = I'_\mathfrak{p}$ for all maximal ideals $\mathfrak{p} \subset A$, hence $I = I'$. Moreover, if any presentation (11.1) is given, $I_\mathfrak{p} = \mathfrak{p}^\mathfrak{p}A_\mathfrak{p}$, hence the powers $k_\mathfrak{p}$ are uniquely defined. □

Definition 11.6. A *fractional ideal* of a domain A is a nonzero A-submodule $J \subset K$, where K is the field of fractions of A such that $aJ \subseteq A$ for some nonzero $a \in A$. Sum and product of fractional ideals are evidently fractional ideals. We denote $J^{-1} = \{q \in K \mid qJ \subseteq A\}$. If $JJ^{-1} = A$, we call J *invertible*.

Exercise 11.7. Prove that

(1) An invertible ideal is always finitely generated.
(2) Let A be a Noetherian domain. Prove that it is a Dedekind domain if and only if every maximal ideal of A is invertible.

Corollary 11.8. *If A is a Dedekind domain, every fractional A-ideal is invertible and is uniquely (up to permutation) is presented as in* (11.1) *(where $k_p \in \mathbb{Z}$ and almost all $k_\mathfrak{p} = 0$).*

Proof. **Exercise.** □

Exercise 11.9. Let A be a Dedekind domain, M be a finite periodic D-module (*periodic* means that $\forall v \in M\ \exists a \in A\ av = 0$). Prove that:

(1) If $\operatorname{Ass}_A M = \{\mathfrak{p}_1, \mathfrak{p}_2, \dots, \mathfrak{p}_n\}$, then $M \simeq \bigoplus_{i=1}^n (M/N_i)$, where N_i is the $\mathfrak{p}_i$-primary component of 0 in M.
(2) If $\operatorname{Ass} M = \{\mathfrak{p}\}$, then $M \simeq M_\mathfrak{p}$.

Let now D be a discrete valuation ring with maximal ideal $\mathfrak{p} = (p)$, M be a finite D-module such that $p^m M = 0$. Prove that:

(3) If $N \subseteq M$ is a submodule and $\varphi : N \to D/p^m D$ is a homomorphism, there is a homomorphism $\psi : M \to D/p^m D$ such that $\psi|_N = \varphi$.
Hint: Let e be the generator of $A/p^m A$. Suppose that $M = N + (u)$ for some u and r is the smallest such that $p^r u = 0$. Then $N \cap (u) = (p^k u)$. If $\varphi(p^k u) = ae$, set $\psi(u) = p^{-k}ae$.
(4) If $p^{m-1}M \neq 0$, then $M \simeq D/p^m D \oplus M'$ for some submodule $M' \subset M$.
(5) $M \simeq \bigoplus_{i=1}^n (D/p^{k_i} D)$ for some k_i.

Deduce that every finite periodic module over a Dedekind domain D is isomorphic to $\bigoplus_{i=1}^n (D/\mathfrak{p}_i^{k_i})$ for some prime ideals $\mathfrak{p}_i$ (not necessarily different) and some k_i.

12. Filtrations. Artin–Rees lemma. Graded rings

Definition 12.1. (1) A *(descending) filtration* of a ring A (of a module M) is a descending chain of ideals (of submodules) $A = I_0 \supseteq I_1 \supseteq I_2 \supseteq \dots$ $(M = M_0 \supseteq M_1 \supseteq M_2 \supseteq \dots)$.
(2) Given a filtration $\mathscr{I} = \{I_n\}$ of a ring A and a filtration $\mathscr{M} = \{M_n\}$ of an A-module M, they say that the filtration $\mathscr{M}$ is

(a) $\mathscr{I}$-*compatible* if $I_mM_n \supseteq M_{m+n}$;
(b) $\mathscr{I}$-*stable* if, moreover, there is an integer n such that $M_{n+k} = I_kM_n$ for every $k \geqslant 0$.

(3) If $\mathfrak{a}$ is an ideal in A, the $\mathfrak{a}$-*adic filtration* of A is the filtration with $I_n = \mathfrak{a}^n$. The $\mathfrak{a}$-*adic filtration* of an A-module M is the filtration with $M_n = \mathfrak{a}^nM$. A filtration $\mathscr{M}$ of M is called $\mathfrak{a}$-*compatible* ($\mathfrak{a}$-*stable*) if its compatible (stable) with respect to the $\mathfrak{a}$-adic filtration.

Definition 12.2. (1) Let $\mathfrak{a}$ be an ideal of a ring A. The *blow-up of A at the ideal* $\mathfrak{a}$ is the ring $\tilde{A} = \bigoplus_{n=0}^{\infty} \mathfrak{a}^n$ with the natural multiplication arising from the equalities $\mathfrak{a}^n\mathfrak{a}^m = \mathfrak{a}^{m+n}$.
(2) If $\mathscr{M}$ is an $\mathfrak{a}$-compatable filtration on an A-module M, we define the $\tilde{A}$-module $\tilde{M} = \bigoplus_{n=0}^{\infty} M_n$ with the natural multiplication arising from the embeddings $\mathfrak{a}^nM^m \subseteq M^{m+n}$.

If A is Noetherian, so is $\tilde{A}$, since, if $\mathfrak{a} = (a_1, a_2, \dots, a_r)$, $\tilde{A} = A[a_1, a_2, \dots, a_n]$, where a_i are considered as elelents from the direct summand $\mathfrak{a}$ of $\tilde{A}$. On the other hand, it is not always the case with $\tilde{M}$.

Lemma 12.3. *Let A be a Noetherian ring, M be a finite A-module $\mathscr{I} = \{I_n\}$ be a filtration on A and $\mathscr{M} = \{M_n\}$ be an $\mathfrak{a}$-compatible filtration of M. The $\tilde{A}$-module $\tilde{M}$ is Noetherian if and only if the filtration $\mathscr{M}$ is $\mathscr{I}$-stable.*

Proof. Consider $\tilde{A}$-submodules $\tilde{M}_n = (\bigoplus_{i=0}^{n} M_i) \oplus (\bigoplus_{k=1}^{\infty} I_kM_n)$ of $\tilde{M}$. Obviously, they are finitely generated and $\tilde{M}_n \subseteq \tilde{M}_{n+1}$. Therefore, $\tilde{M}$ is Noetherian if and only if the ascending chain $\{\tilde{M}_n\}$ stops, that is there is n such that $\tilde{M}_{n+k} = \tilde{M}_n$ for all $k > 0$. But the last equality just means that $I_kM_n = M_{n+k}$ for all $k > 0$. □

Corollary 12.4 (Artin-Rees lemma)**.** *Let A be a Noetherian ring, $\mathscr{I} = \{I_n\}$ be filtration A, M be a finite A-module and $\mathscr{M} = \{M_n\}$ be an $\mathscr{I}$-stable filtration of M. Let also $N \subseteq M$ be a submodule. Then the filtration $\mathscr{N} = \{M_n \cap N\}$ of the module N is also $\mathscr{I}$-stable. In particular, if $\mathfrak{a}$ is an ideal of A, there is an integer n such that $\mathfrak{a}^{n+k}M \cap N = \mathfrak{a}^k(\mathfrak{a}^nM \cap N)$ for all $k > 0$.*

Proof. $\tilde{N}$ is a submodule of $\tilde{M}$. □

Corollary 12.5. [6] *Let A be a Noetherian ring, $\mathfrak{a}$ be an ideal of A, M be a finite A-module and $\bar{M} = \bigcap_{n=1}^{\infty} \mathfrak{a}^nM$. There is $a \in \mathfrak{a}$ such that $(1 - a)u = u$ for all $u \in \bar{M}$. In particular:*

(1) *If $\mathfrak{a} \subseteq \operatorname{rad} A$, then $\bigcap_{n=1}^{\infty} \mathfrak{a}^nM = 0$.*
(2) *If N is a submodule of M and $\mathfrak{a} \subseteq \operatorname{rad} A$, then $\bigcap_{n=1}^{\infty}(\mathfrak{a}^nM + N) = N$.*
(3) *If A is a domain, then $\bigcap_{n=1}^{\infty} \mathfrak{a}^n = 0$.*

Proof. As $\mathfrak{a}^nM \cap \bar{M} = \bar{M}$, so, by Cor. 12.4, $\bar{M} = \mathfrak{a}\bar{M}$. Now use the NAK lemma 3.9. □

[6] This corollary is also cited as Artin–Rees lemma.

Filtrations are closely related to *graded rings*.

Definition 12.6. (1) A *graded ring* is a ring A together with a decomposition of its additive group $A = \bigoplus_{d=0}^{\infty} A_d$ such that $A_d A_{d'} \subseteq A_{d+d'}$.[7] One set $A_+ = \bigoplus_{d=1}^{\infty} A_d$. Obviously, A_0 is a subring and A_+ is an ideal of A.

(2) If $a \in A_d$, they say that a is *homogemeous of degree* d and write $\deg a = d$. If $a = \sum_{d=0}^{\infty} a_d$ (almost all $a_d = 0$), they call a_d *homogeneous components* of a.

(3) A *graded module* over a graded ring A is an A-module together with a decomposition of its additive group $M = \bigoplus_{d=-\infty}^{+\infty} M_d$ such that $A_d M_{d'} \subseteq M_{d+d'}$. Homogeneous elements and homogeeous components of elements of graded modules are defined analogously to elements of graded rings.

(4) A submodule N of a graded module M (for instance, an ideal of a graded ring) is called *homogeneous* if $N = \bigoplus_d N \cap M_d$. Equivalently, if $a \in N$, all its homogeneous components are also in N. Evidently, it means that N can be generated by homogeneous elements. In this case M/N can also be considered as graded setting $(M/N)_d = M_d/N \cap M_d$.

An important class of graded rings and modules arises from filtrations.

Definition 12.7. Let A be a ring with a filtration $\mathscr{I} : A = I_0 \supseteq I_1 \supseteq I_2 \supseteq \dots$. The *associated graded ring* is $\operatorname{gr} A = \bigoplus_{n=0}^{\infty} A_n$, where $A_n = I_n/I_{n+1}$ and the multiplication $A_n \times A_m \to A_{n+m}$ is defined by the rule $(a + I_{n+1})(b + I_{m+1}) = ab + I_{m+n+1}$.

In the same way, given an A-module with an $\mathscr{I}$-compatible filtration $\mathscr{M} : M = M_0 \supseteq M_1 \supseteq M_2 \supseteq \dots$, we define the *associated graded* $\operatorname{gr} A$*-module* $\operatorname{gr} M = \bigoplus_{n=0}^{\infty} M_n/M_{n+1}$.

There is a simple condition for a graded ring to be Noetherian.

Proposition 12.8. *A graded ring A is Noetherian if and only if A_0 is Noetherian and A is an A_0-algebra of finite type.*

Proof. "If" part follows from Cor. 2.4. Prove the"only if" part. As A is Noetherian, the ideal A_+ is finitely generated: $A_+ = (a_1, a_2, \dots, a_m)$, and we can suppose that all a_i are homogeneous. Let $\deg a_i = d_i$, $b \in A_n$ and $b = \sum_{i=1}^{m} c_i a_i$. Obviously, one can suppose that $c_i \in A_{n-d_i}$. Using an obvious induction, one can show that $b \in A_0[a_1, a_2, \dots, a_n]$. □

Obviously, if A is Noetherian, every A_d is a finite A_0-module. Moreover, if M is a finite graded A-module, $M_d = 0$ for $d \ll \infty$ (i.e. for $d < d_0$ for some d_0) and all M_d are finite A_0-modules.

The graded modules and homogeneous ideals behave well with respect to associated primes.

[7] Sometimes one consider graded rings when the components are numbered by elements of more general semigroups.

Proposition 12.9. *Let M be a graded module over a graded ring A, $\mathfrak{p} \in \operatorname{Ass}_A M$. Then $\mathfrak{p}$ is a homogeneous ideal.*

Proof. Let $\mathfrak{p} = \operatorname{Ann}_A u$. If u is homogeneous, so is $\mathfrak{p}$. Let $u = \sum_{i=1}^{k} u_i$, where u_i are homogeneous and $\deg u_1 < \deg u_2 < \dots < \deg u_k$. Use induction by k. Let $a \in \mathfrak{p}$ and $a = \sum_{i=1}^{k} a_i$, where a_i are homogeneous and $\deg a_1 < \deg a_2 < \dots < \deg a_r$. Obviously, it is enough to prove that $a_1 \in \mathfrak{p}$. In any case, $a_1 u_1 = 0$, so $a_1 u = \sum_{i=2}^{k} a_1 u_i$. Let $I = \operatorname{Ann}_A a_1 u$. If $\mathfrak{p} = I$, $\mathfrak{p}$ is homogeneous by induction. If not, let $b \in I \setminus \mathfrak{p}$. As $b a_1 u = 0$, $b a_1 \in \mathfrak{p}$, hence $a_1 \in \mathfrak{p}$, which accomplishes the proof. □

Definition 12.10. A graded ring A is called *connected* if A_0 is a field. For instance, so are associated graded rings of local rings with respect to the filtration defined by the powers of the maximal ideal. Then A_+ is a unique maximal graded ideal of A. The set of graded prime ideals $\mathfrak{p} \neq A_+$ is called the *projective spectrum* of the connected graded ring A.

We will use the so called *shift of grading*.

Definition 12.11. Let M be a graded module over a graded ring A. By $M(k)$ we denote the graded module which coincide with M, but with the grading such that $M(k)_d = M_{d+k}$.

13. Lengths of modules. Poincaré series and Hilbert polynomial.

Definition 13.1. A *composition series* in a module M is a chain of submodules $0 = M_0 \subset M_1 \subset M_2 \subset \dots \subset M_l = M$ such that all quotients M_i/M_{i-1} $(0 < i \leqslant l)$ are simple module. These simple modules are called the *composition factors* of this series.

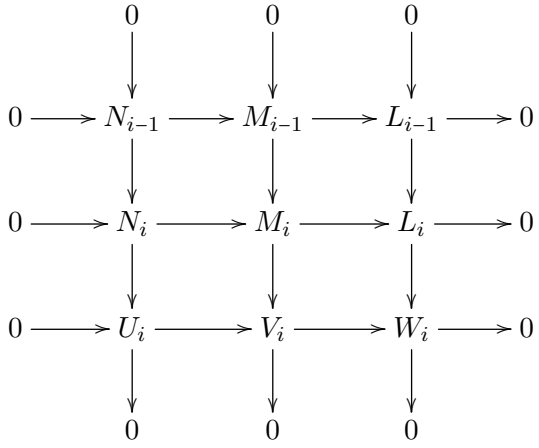
Theorem 13.2 (Jordan–Hölder)**.** (1) *Let $0 = M_0 \subset M_1 \subset M_2 \subset \dots \subset M_l = M$ be a composition series in M, $N \subseteq M$ be a submodule and $L = M/N$. There are composition series in N and L such that the union of the sets of their composition factors coincides with the set of composition factors of the given composition series of M.*

(2) *All composition series of a given module have the same lengths and the same combinations*[8] *of composition series.*

Proof. (1) Set $N_i = N \cap M_i \subseteq N$ and $L_i = M_i + N/N \subseteq L$. Then $M_i/N_i \simeq L_i$. Therefore, we obtain commutative diagrams with exact columns and exact

[8] Recall that *combinations* are finite sequences where the order of elements is not essential, that is two sequences obtained from each other by a permutation of elements are considered as equal.

first and second rows:



where $U_i = N_i/N_{i-1}$, $V_i = M_i/M_{i-1}$, $W_i = L_i/L_{i-1}$. By the 3×3-lemma (Lem. D.10(1)), the third row is also exact. Hence U_i can be considered as a submodule in V_i with the quotient W_i. As V_i is a simple module, either $U_i = V_i$ and $W_i = 0$, or $U_i = 0$ and $W_i = V_i$. Therefore, if we consider the chains of submodules $0 = N_0 \subseteq N_1 \subseteq N_2 \subseteq \ldots \subseteq N_l = N$ and $0 = L_0 \subseteq L_1 \subseteq L_2 \subseteq \ldots \subseteq L_l = L$ and cross out all submodules that coincide with the previous ones, we obtain composition series in N and L with the necessary properties.

(2) follows from (1) by a simple induction (**explain the details**). □

Definition 13.3. If an A-module M has a composition series, it is called a *module of finite length*, the length of a composition series is called the *length* of M and denoted by $\ell_A(M)$ and the composition factors of a composition series are called the *composition factors* of the module M.

Obviously, modules of finite length are just those which are both Noetherian and Artinian. In particular, Thm. 8.7 implies that every finite module over an Artinian ring is of finite length. Assertion (1) of Thm. 13.2 implies that the length is *additive*, i.e. $\ell_A(M) = \ell_A(N) + \ell_A(L)$ if $N \subseteq M$ is a submodule and $L = M/N$.

Exercise 13.4. Let $0 \to M_1 \to M_2 \to \cdots \to M_n \to 0$ be an exact sequence of modules of finite length. Prove that $\sum_{i=1}^{n} (-1)^i \ell_A(M_i) = 0$.

Definition 13.5. Let A be a Noetherian graded ring such that A_0 is Artinian, M be a finite graded A-module. The *Poincaré series* of M is the formal Laurent series

$$P(t, M) = \sum_{d=-\infty}^{+\infty} \ell_{A_0}(M_d) t^d.$$

Note that actually this series only has finitely many terms with negative degrees of t. Note also that if d_0 is the least integer such that $M_{d_0} \neq 0$, then $P(t, M) = t^{-d_0} P(t, M(-d_0))$. Therefore, in what follows we will consider the case of *positibely graded* modules, i.e. such that $M_d = 0$ if $d < 0$.

Theorem 13.6 (Hilbert–Serre)**.** *Let A be a Noetherian graded ring with the Artinian component A_0 and $A = A_0[a_1, a_2, \dots, a_n]$, where a_i are homogeneous with $\deg a_i = d_i > 0$. Let M be a Noetherian positively graded A-module. There is a polynomial $f(t) \in \mathbb{Z}[t]$ such that*

$$P(t, M) = \frac{f(t)}{\prod_{i=1}^{n}(1 - t^{d_i})}.$$

Proof. We use induction on n. If $n = 0$, i.e. $A = A_0$, the module M only has finitely many non-zero components, hence $P(t, M)$ is a polynomial. Thus we can suppose that the theorem holds for the graded ring $A/(a_1) = A_0[a_2, \dots, a_n]$. Consider the map $M \xrightarrow{\alpha} M(d_1)$, $v \mapsto a_1 v$. Let $K = \operatorname{Ker}\alpha$ and $C = \operatorname{Coker}\alpha = M/\operatorname{Im}\alpha$. Then we have an exact sequence

$$0 \to K \to M \xrightarrow{\alpha} M(d_1) \to C \to 0.$$

Recall that $M(d_1)_d = M_{d+d_1}$. By Exer. 13.4,

$$\ell_{A_0}(K_d) - \ell_{A_0}(M_d) + \ell_{A_0}(M_{d+d_1}) - \ell_{A_0}(C_d) = 0.$$

If we multiply all terms by t^{d+d_1} and take the sum, we get

$$t^{d_1}P(t, K) - t^{d_1}P(t, M) + P(t, M) - t^{d_1}P(t, C) = g(t),$$

where $g(t)$ arises from the terms with t^k, $k < d_1$. Note that K and C are actually $A/(a_1)$-modules, so we can suppose that the assertion is valid for their Poincaré series. Therefore, we have

$$P(t, M)(1 - t^{d_1}) = \frac{h(t)}{\prod_{i=2}^{n}(1 - t^{d_i})} + g(t),$$

which implies the necessary result. □

If A is *generated in degree* 1, that is $A = A_0[A_1]$, it implies the following result.

Theorem 13.7. *Let A be a Noetherian graded ring generated in degree 1 with Artinian A_0 and M be a finite A-module. There is an integer r and a polynomial $H_M(t)$ with rational coefiicients such that $\ell_{A_0}(M_d) = H_M(d)$ for all $d \geqslant r$. The leading term of this polynomial is $\dfrac{e(M)t^{m-1}}{(m-1)!}$, where $e(M) > 0$ is an integer and m is the order of the pole of the Poincaré series at $t = 1$.*

The number $e(M)$ is called the *multiplicity* of the module M. If $A = \Bbbk[x_1, x_2, \dots, x_n]/I$, where I is a homogeneous radical ideal, $e(A)$ is called the *multiplicity* of the projective variety $\operatorname{pr.var}(I)$.

Proof. The Poincaré series of M is of the form

$$P(t, M) = \frac{f(t)}{(1 - t)^m}$$

where $f(1) \neq 0$. Let $r = \deg f$.

By the Newton binomial formula

$$(1-t)^{-m} = \sum_{k=0}^{\infty}(-1)^k\binom{-m}{k}t^k = \sum_{k=0}^{\infty}\binom{m+k-1}{m-1}t^k.$$

If $f(t) = \sum_{k=0}^{r} a_k t^k$, its gives us, for $d \geqslant r$,

$$\ell_{A_0}(M_d) = \sum_{k=0}^{r} a_k\binom{m+d-k-1}{m-1},$$

that is $\ell_{A_0}(M_d) = H_M(d)$, where $H_M(d)$ is a polynomial with rational coefficients and the leading term $\dfrac{e(M)t^{m-1}}{(m-1)!}$, where $e(M) = \sum_{k=0}^{r} a_k = f(1) \in \mathbb{Z}$ and $e(M) > 0$, since $H_M(d) \geqslant 0$ for $d \geqslant r$. □

Remark 13.8. Note that if $A = A_0[a_1, a_2, \ldots, a_n]$, the construction implies that $m \leqslant n$.

Example 13.9. (1) If $A = \Bbbk[x_0, x_1, \ldots, x_n]$, where $\Bbbk$ is a field, then $\dim_{\Bbbk} A_d = \binom{n+d}{n} = \dfrac{d^n}{n!} + o(d^n)$. Hence $e(A) = 1$.

(2) Let now $A = \Bbbk[x_0, x_1, \ldots, x_n]/(F)$, where F is a homogeneous polynomial of degree m. Then, for $d \geqslant m$, $\dim_{\Bbbk} A_d = \binom{n+d}{n} - \binom{n+d-m}{n} = \dfrac{md^{n-1}}{(n-1)!} + o(d^{n-1})$. Hence $e(A) = m$. Geometrically, it means that the mupltiplicity of a hypersurface equals the degree of its equation.

Exercise 13.10. They say that an ideal $I \subset \Bbbk[x_0, x_1, \ldots, x_n]$ (or the variety $\operatorname{var}(I)$) is a *complete intersection* if $I = (f_1, f_2, \ldots, f_m)$, where, for every i, the element f_i is not a zero divisor modulo $(f_1, f_2, \ldots, f_{i-1})$ (in particular, f_1 is a non-zero-divisor). Find the multiplicity of the graded ring $\Bbbk[x_1, x_2, \ldots, x_n]/I$ if each f_i is a homogeneous polynomial of degree m_i.

14. Applications to local rings.

Corollary 14.1. *Let A be a Noetherian ring, $\mathfrak{a} \subset A$ be an ideal such that $A/\mathfrak{a}$ is Artinian, M be a finite A-module with an $\mathfrak{a}$-stable filtration $\mathscr{M} = \{M_n\}$.*

(1) *There is a polynomial $\chi_{\mathscr{M}}(t, M) \in \mathbb{Q}[t]$ such that $\ell_A(M/M_n) = \chi_{\mathscr{M}}(n, M)$ for $n \gg 0$.*
The last claim means that there is n_0 such that $\ell_A(M/M_n) = \chi_{\mathscr{M}}(n, M)$ for all $n \geqslant n_0$.

(2) *The leading term of the polynomial $\chi_{\mathscr{M}}(t, M)$ does not depend on the choice of an $\mathfrak{a}$-stable filtration $\mathscr{M}$ and is of the form $\dfrac{e_{\mathfrak{a}}(M)t^m}{m!}$ for some integer $e_A(M) > 0$, where $m \leqslant \operatorname{gen}_A(\mathfrak{a}/\mathfrak{a}^2)$.*

The polynomial $\chi_{\mathscr{M}}(t, M)$ is called the *characteristic polynomial of the filtration $\mathscr{M}$*. The integer $e_{\mathfrak{a}}(M)$ is called the *multiplicity of the ideal A in the module M*. The integer $e_{\mathfrak{a}}(A)$ is called the *multiplicity of the ideal $\mathfrak{a}$*. If A is a local ring with the maximal ideal $\mathfrak{m}$ and $\mathscr{M} = \{\mathfrak{m}^n M\}$ is the $\mathfrak{m}$-adic

filtration, this polynomial is called the *characteristic polynomial or Samuel polynomial of the module* M and denoted by $\chi(t, M)$.

Proof. (1) Applying Thm. 13.7 to the graded module $\operatorname{gr} M = \bigoplus_n M_n/M_{n+1}$ over the graded ring $\operatorname{gr} A = \bigoplus_n \mathfrak{a}^n/\mathfrak{a}^{n+1}$ we see that $\ell_A(M_n/M_{n-1}) = H_{\mathscr{M}}(n, M)$ for some polynomial $H_{\mathscr{M}}(t, M)$ with the leading term $\dfrac{e(M)t^{m-1}}{(m-1)!}$ for $n \geqslant n_0$. Now take for $\chi_{\mathscr{M}}(t, M)$ a polynomial such that $H_{\mathscr{M}}(t, M) = \chi_{\mathscr{M}}(t, M) - \chi_{\mathscr{M}}(t-1, M)$ and $\chi_{\mathscr{M}}(n_0, M) = \ell_A(M/M_{n_0})$ (it exists and is unique).

(2) It is known (and easy to see) that the leading term of $\chi_{\mathscr{M}}(t, M)$ must be $\dfrac{e(M)t^m}{m!}$. Let $\chi_{\mathfrak{a}}(t, M)$ be the corresponding polynomial for the $\mathfrak{a}$-adic filtration $\{\mathfrak{a}^n M\}$. Note that $M_n \supseteq \mathfrak{a}^n M$, hence $\chi_{\mathscr{M}}(n, M) \leqslant \chi_{\mathfrak{a}}(n, M)$. On the other hand, Artin-Rees lemma shows that there is r such that $M_{n+r} = \mathfrak{a}^n M_r \subseteq \mathfrak{a}^n M$, hence $\chi_{\mathscr{M}}(n + r, M) \geqslant \chi_{\mathfrak{a}}(n, M)$. It implies that $\lim_{t\to\infty} \dfrac{\chi_{\mathscr{M}}(t, M)}{\chi_{\mathfrak{a}}(t, M)} = 1$ which means that these polynomials have the same leading terms. □

From now on we suppose that A is Noetherian and local with the maximal ideal $\mathfrak{m}$ and the residue field $\Bbbk$, M is a finitely generated A-module. We denote $\chi(t, M) = \chi_{\mathfrak{m}}(t, M)$, $d(M) = \deg \chi(t, M)$ and are going to prove that $d(M) = \dim M$, where we set $\dim M = \dim A/\operatorname{Ann}_A M$.

Lemma 14.2. (1) *Let $N \subseteq M$ be a submodule, $L = M/N$. Then $d(M) = \max\{d(N), d(L)\}$.*

(2) *$d(M) = d(\bar{A})$, where $\bar{A} = A/\operatorname{Ann}_A M$.*

Proof. (1) Consider the $\mathfrak{m}$-stable filtration $\mathscr{N} = \{N \cap \mathfrak{m}^n M\}$ of N. Note that $\mathfrak{m}^n M/N \cap \mathfrak{m}^n M \simeq \mathfrak{m}^n + N/N = \mathfrak{m}^n L$. As $N/N \cap \mathfrak{m}^n \simeq N + \mathfrak{m}^n/\mathfrak{m}^n$ and $M/N + \mathfrak{m}^n \simeq L/\mathfrak{a}^n L$, we have an exact sequence $0 \to N/N \cap \mathfrak{m}^n M \to M/\mathfrak{m}^n M \to L/\mathfrak{m}^n L \to 0$, whence $\chi(t, M) = \chi_{\mathscr{N}}(t, N) + \chi(t, L)$. As leading coefficients of these polynomials are positive, it implies the claim.

(2) Obviously, $d(M^n) = d(M)$, in particular, $d(F) = d(A)$ if F is a finite free A-module. As every module is a quotient of a free one, $d(M) \leqslant d(\bar{A})$. On the other hand, we have seen that $\bar{A}$ embeds into M^r for some r, whence $d(\bar{A}) \leqslant d(M)$. □

Therefore, from now on we can suppose that M is exact (i.e. $\operatorname{Ann}_A M = 0$) and we only have to prove that $d(A) = \dim A$.

Lemma 14.3. *If an element $a \in \mathfrak{m}$ is a non-zero-divisor on M, then $d(M/aM) \leqslant d(M) - 1$.*

Proof. Consider the submodule $N = aM \simeq M$ (since a is a non-zero-divisor on M). As in the proof above, $\chi(t, M) = \chi_{\mathscr{N}}(t, N) + \chi(t, M/aM)$. As the leading terms of $\chi_{\mathscr{N}}(t, N)$ and $\chi(t, M)$ are the same, $d(M/aM) < d(M)$. □

Theorem 14.4 (Hilbert–Samuel)**.** *$d(M) = \dim M$.*

Proof. Lem. 14.2 shows that it is enough to consider the case $M = A$. Recall that $\dim A$ is the least number n such that there is an $\mathfrak{m}$-primary ideal $\mathfrak{a}$ with n generators. As $\mathfrak{m} \supseteq \mathfrak{a} \supseteq \mathfrak{m}^k$ for some k, $\chi_{\mathfrak{m}}(d, A) \leqslant \chi_{\mathfrak{a}}(d, A) \leqslant \chi_{\mathfrak{m}^k}(d, A) = \chi_{\mathfrak{m}}(kd, A)$ for $d >> 0$. It implies that $\deg \chi_{\mathfrak{m}}(t, A) = \deg \chi_{\mathfrak{a}}(t, A) \leqslant n$ by Cor. 14.1(2).

To prove that $\dim A \leqslant d(A)$ we use induction by $d(A)$. If $d(A) = 0$, $\ell_A(A/\mathfrak{m}^k) = \ell_A(A/\mathfrak{m}^{k+1})$ for some k, that is $\mathfrak{m}^k = \mathfrak{m}^{k+1}$ and $\mathfrak{m}^k = 0$ by Nakayama lemma. Therefore, $\mathfrak{m} = \operatorname{nil} A$ is a unique prime ideal and $\dim A = 0$. Suppose now that the theorem holds for all rings with smaller value of $d(A)$. Choose a chain of prime ideals $\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \ldots \subset \mathfrak{p}_n$, where $n = \dim A$, and consider the ring $A' = A/\mathfrak{p}_0$. Obviously, $\dim A' = \dim A$ and $\ell_{A'}(A'/\mathfrak{m}^k A') \leqslant \ell_A(A/\mathfrak{m}^k A)$, hence $d(A') \leqslant d(A)$. Let $a \in \mathfrak{p}_1 \smallsetminus \mathfrak{p}_0$. It is a non-zero-divisor in A', hence $d(A'/aA') \leqslant d(A') - 1 \leqslant d(A) - 1$. On the other hand, $\dim A'/aA' = \dim A' - 1 = \dim A - 1$. By the inductive conjecture, $\dim A - 1 \leqslant d(A) - 1$, which accomplishes the proof. □

We apply these results to regular local rings, i.e. such that $\mathfrak{m}$ is generated by n elements, where $n = \dim A$.

Theorem 14.5. *If A is a regular local ring of dimension n, then $\operatorname{gr}_{\mathfrak{m}} A \simeq \Bbbk[x_1, x_2, \ldots, x_n]$, hence $\chi(t, A) = \binom{t+n}{n}$.*

Proof. As $\operatorname{gen}_A \mathfrak{m} = n$, there is a natural epimorphism $\varphi : \Bbbk[x_1, x_2, \ldots, x_n] \to \operatorname{gr}_{\mathfrak{m}} A$. Suppose that $\operatorname{Ker} \varphi \ni f$, where f is homogeneous of degree k. Then, for $d \geqslant k$,

$$\dim_{\Bbbk}(\operatorname{gr}_{\mathfrak{m}})_d \leqslant \binom{d+n-1}{n-1} - \binom{d-k+n-1}{n-1} = \frac{kd^{n-2}}{(n-2)!} + o(d^{n-2}).$$

and the degree of the Hilbert polynomial for $\operatorname{gr}_{\mathfrak{m}} A$ is at most $n-2$. Therefore $\deg \chi_{\mathfrak{m}}(t, A) \leqslant n - 1$, which is impossible, since $\dim A = n$. □

The following fact is almost obvious.

Proposition 14.6. *If $\operatorname{gr}_{\mathfrak{m}} A$ is a domain, so is A.*

Proof. **Exercise**. □

Remark. The converse is not true in general, as the example of the ring $A = \Bbbk[[x, y]]/(x^2 - y^3)$ shows, where $\operatorname{gr}_{\mathfrak{m}} A = \Bbbk[x, y]/(x^2)$.

Corollary 14.7. *A regular local ring is a domain.*

15. Completions

Definition 15.1. (1) An *inverse system of groups (rings, modules)* is a set $\mathscr{M} = \{M_i, \phi_i \mid i \in \mathbb{N}\}$, where M_i are groups (rings, modules) and $\phi_i : M_{i+1} \to M_i$ are homomorphisms. It is called *surjective* if all homomorphisms ϕ_i are surjective.

(2) The *inverse limit* $\varprojlim \mathscr{M} = \varprojlim_i M_i$ is the subgroup of the cartesian product $\prod_{i=1}^{\infty} M_i$ consisting of all sequences $(a_i \mid i \in \mathbb{N})$ such that $a_i = \phi_i(a_{i+1})$ for all i.

(3) A *morphism* of inverse systems $\alpha : \mathscr{M} \to \mathscr{N}$, where $\mathscr{N} = \{N, \psi_i\}$ is a set of homomorphisms $\{\alpha_i : M_i \to N_i \mid i \in \mathbb{N}\}$ such that $\alpha_i\phi_i = \psi_i\alpha_{i+1}$ for all i. We define $\operatorname{Ker}\alpha$ ($\operatorname{Im}\alpha$) as the inverse system $\{\operatorname{Ker}\alpha_i, \phi_i|_{\operatorname{Ker}\alpha_{i+1}}\}$ (respectively, $\{\operatorname{Im}\alpha_i, \psi_i|_{\operatorname{Im}\alpha_{i+1}}\}$) (**check that they are well defined**).
Thus *exact sequences* of inverse systems are defined.

(4) If $\alpha : \mathscr{M} \to \mathscr{N}$ is a morphism of inverse systems, its *inverse limit* $\varprojlim \alpha = \varprojlim_i \alpha_i$ is defined as the homomorphism $\varprojlim \mathscr{M} \to \varprojlim \mathscr{N}$ mapping (a_i) to $(\alpha_i(a_i))$.

Inverse limit is a functor from the category of inverse systems to the category of groups. The next results shows that it is *left exact*.

Proposition 15.2. *If a sequence of inverse systems* $0 \to \mathscr{M} \xrightarrow{\alpha} \mathscr{N} \xrightarrow{\beta} \mathscr{L} \to 0$ *is exact, the sequence*

$$0 \to \varprojlim \mathscr{M} \xrightarrow{\varprojlim \alpha} \varprojlim \mathscr{N} \xrightarrow{\varprojlim \beta} \varprojlim \mathscr{L} \tag{15.1}$$

is exact. Moreover, if the inverse system $\mathscr{M}$ *is surjective, the whole sequence*

$$0 \to \varprojlim \mathscr{M} \xrightarrow{\varprojlim \alpha} \varprojlim \mathscr{N} \xrightarrow{\varprojlim \beta} \varprojlim \mathscr{L} \to 0 \tag{15.2}$$

is exact.

Proof. Let $\mathscr{M} = \{M_i, \phi_i\}$, $\mathscr{N} = \{N_i, \psi_i\}$, $\mathscr{L} = \{L_i, \theta_i\}$. Obviously, $\varprojlim \alpha$ is injective and $(\varprojlim \beta)(\varprojlim \alpha) = 0$. If $\varprojlim \beta(a_i) = (\beta_i(a_i)) = 0$ then $a_i = \alpha_i(b_i)$. for each i. As also $\alpha_i\phi_i(b_{i+1}) = \psi_i\alpha_{i+1}(b_{i+1}) = \psi_i(a_{i+1}) = a_i$ and α_i is injective, $\phi_i(b_{i+1}) = b_i$ and $(b_i) \in \varprojlim \mathscr{N}$, hence $(a_i) \in \operatorname{Im}\varprojlim \alpha$ and the sequence (15.1) is exact.

Suppose that all maps $\phi_i : M_{i+1} \to M_i$ are surjective. Let $(a_i) \in \varprojlim \mathscr{L}$. We have to construct $b_i \in N_i$ such that $a_i = \beta_i(b_i)$ and $\psi_i(b_{i+1}) = b_i$. We do it recursively, starting from any choice of b_1. Let we have already constructed $b_1, b_2, \dots, b_i$ and let $a_{i+1} = \beta_{i+1}(c)$. Then $\beta_i\psi_i(c) = \theta_i\beta_{i+1}(c) = a_i = \beta_i(b_i)$, that is $b_i - \psi_i(c) \in \operatorname{Ker}\beta_i = \operatorname{Im}\alpha_i$. Let $b_i - \psi_i(c) = \alpha_i(c')$. There is $c'' \in M_{i+1}$ such that $c' = \varphi_i(c'')$. Then $b_i - \psi_i(c) = \alpha_i\phi_i(c'') = \psi_i\alpha_{i+1}(c'')$. Therefore, if we set $b_{i+1} = c + \alpha_{i+1}(c'')$, we obtain that $\psi_i(b_{i+1}) = b_i$ and $\beta_{i+1}(b_{i+1}) = \beta_{i+1}(c) = a_{i+1}$, just what we need. Hence the sequence (15.2) is exact. □

Definition 15.3. (1) Let $\mathfrak{F} = \{F^iM \mid i \in \mathbb{N}\}$ be a (descending) filtration in M, i.e. a set of subgroups such that $F^iM \subseteq F^{i+1}M$ for all i. Then $\mathscr{F} = \{M/M_i, f_i : M/M_{i+1} \to M/M_i\}$, where f_i is the natural epimorphism, is an inverse system. Its inverse limit $\varprojlim \mathscr{F}$ is called the *completion of* M *with respect to the filtration* $\mathfrak{F}$ and denoted by

$\hat{M}_{\mathfrak{F}}$. We define the homomorphism $\iota_{\mathfrak{F}} : M \to \hat{M}_{\mathfrak{F}}$ mapping an element v to the sequence (v_i), where $v_i = v + F^i M \in M/F^i M$.

(2) Let $\mathfrak{a}$ is an ideal of a ring A, M be an A-module. The filtration $\mathfrak{F}_{\mathfrak{a}}$ such that $F^i M = \mathfrak{a}^i M$ is called the $\mathfrak{a}$-*adic filtration*. Its inverse limit is called the $\mathfrak{a}$-*adic completion* of M and denoted by $\hat{M}_{\mathfrak{a}}$ and write $\iota_{\mathfrak{a}}$ instead of $\iota_{\mathfrak{F}_{\mathfrak{a}}}$.

(3) Every homomorphism $\alpha : M \to N$ induces homomorphisms $M/\mathfrak{a}^i M \to N/\mathfrak{a}^i N$, hence a morphism of inverse systems and a homomorphism of inverse limits $\hat{\alpha}_{\mathfrak{a}} : \hat{M}_{\mathfrak{a}} \to \hat{N}_{\mathfrak{a}}$.

Obviously, $\operatorname{Ker} \iota_{\mathfrak{F}} = \bigcap_{i=1}^{\infty} F^i M$. In particular, $\operatorname{Ker} \iota_{\mathfrak{a}} = \bigcap_{i=1}^{\infty} \mathfrak{a}^i M$. For instance, if A is local Noetherian with maximal ideal $\mathfrak{m}$ and M is finite, $\iota_{\mathfrak{m}}$ is injective due to Artin-Rees lemma (Cor. 12.5).

Example 15.4. If $A = \Bbbk[x_1, x_2, \dots, x_n]$ and $\mathfrak{m} = (x_1, x_2, \dots, x_n)$, then $\hat{A}_{\mathfrak{m}} = \Bbbk[[x_1, x_2, \dots, x_n]]$ (**expalin it**).

If $A = \mathbb{Z}$ and $\mathfrak{p} = (p)$, they write $\mathbb{Z}_p$ instead of $\hat{\mathbb{Z}}_{(p)}$ and call this ring *the ring of p-adic integers*. Its field of quotients is denote by $\mathbb{Q}_p$ and called *the field of p-adic numbers*. One can verify that $\mathbb{Q}_p \simeq \mathbb{Z}_p \otimes_{\mathbb{Z}} \mathbb{Q}$, but $\mathbb{Q}_p$ is not the p-adic completion of $\mathbb{Q}$ (**try to explain it**).

One can check that every p-adic integer can be uniquely written as $c_0 + c_1 p + c_2 p^2 + \dots$, where $0 \leqslant c_i < p$. For instance, $-1 = (p-1) + (p-1)p + (p-1)p^2 + \dots$.

Note that the $\mathfrak{a}$-adic filtrations are always surjective. Nevertheless, we cannot apply Prop. 15.2 to $\mathfrak{a}$-adic completions, since the functor $M \mapsto M/\mathfrak{a}^n M$ is not exact. We are going to fix this fault in Noetherian case.

Example 15.5. Let A be local Noetherian and $\mathfrak{m}$ be its maximal ideal. If $\hat{A}_{\mathfrak{m}}$ is a domain, so is A (since $\iota_{\mathfrak{m}}$ is an embedding). The following example shows that converse is not true.

Let $A = \Bbbk[x, y]/(y^2 - x^2 = x^3)$, where $\Bbbk$ is a field $\mathfrak{m} = (x, y)$. Then $A_{\mathfrak{m}}$ is a domain. $\hat{A}_{\mathfrak{m}} = \Bbbk[[x, y]]/(y^2 - x^2 - x^3)$. One can see that $\Bbbk[[x, y]] \ni z$ such that $z^2 = x^2 + x^3$ (set $z = x\sqrt{1+x}$ and use Newton binomial formula). If $\bar{y}$ and $\bar{z}$ are images of y and z in $\hat{A}_{\mathfrak{m}}$, then $(\bar{y} - \bar{z})(\bar{y} + \bar{z}) = 0$, though $\bar{y} \neq \pm\bar{z}$.

We call two filtrations $\mathfrak{F}$ and $\mathfrak{G}$ on the same module M *commensurate* if for eviery i there are $\nu(i)$ and $\mu(i)$ such that $F^i M \supseteq G^{\nu(i)} M$ and $G^i M \supseteq F^{\mu(i)} M$.

Lemma 15.6. *If two filtrations $\mathfrak{F}$ and $\mathfrak{G}$ on the same group M are commensurate, $\hat{M}_{\mathfrak{F}} \simeq \hat{M}_{\mathfrak{G}}$.*

Proof. We can suppose that $\nu(i+1) \geqslant \nu(i) \geqslant i$. Define a new filtration $\tilde{\mathfrak{G}}$ setting $\tilde{G}^i M = G^{\nu(i)} M$. One can easily see that $\hat{M}_{\tilde{\mathfrak{G}}} \simeq \hat{M}_{\mathfrak{G}}$. On the other hand, the natural epimorphisms $M/\tilde{G}^i M \to M/F^i M$ define a morphism of inverse systems, hence a homomorphism $\hat{M}_{\mathfrak{G}} \to \hat{M}_{\mathfrak{F}}$. Just in the same way one defines a homomorphism $\hat{M}_{\mathfrak{F}} \to \hat{M}_{\mathfrak{G}}$ and one easily verifies that these two homomorphisms are mutually inverse (**restore the details**). □

Corollary 15.7. *Let $\mathfrak{a}$ be an ideal in a ring A. If $\mathfrak{F}$ is an $\mathfrak{a}$-stable filtration in an A-module M, then $\hat{M}_{\mathfrak{F}} \simeq \hat{M}_{\mathfrak{a}}$.*

Corollary 15.8. *Let A be a Noetherian ring, $\mathfrak{a} \subset A$ be an ideal.*

(1) *If $0 \to N \to M \to L \to 0$ is an exact sequence of finite A-modules, then the sequence of completions*

$$0 \to \hat{N}_{\mathfrak{a}} \to \hat{M}_{\mathfrak{a}} \to \hat{L}_{\mathfrak{a}} \to 0 \tag{15.3}$$

is also exact.

(2) *If M is a finite A-module, then the homomorphism $\gamma_M : A_{\mathfrak{a}} \otimes_A M \to \hat{M}_{\mathfrak{a}}$ mapping $(a_i) \otimes v \mapsto (a_i v)$ is an isomorphism.*

(3) *$\hat{A}_{\mathfrak{a}}$ is a flat A-module.*

Proof. (1) As M is Noetherian, we can use the Artin-Rees lemma (Lem. 12.3) and replace $\mathfrak{a}$-adic filtration of N by the $\mathfrak{a}$-stable filtration $\{N \cap \mathfrak{a}^n M\}$. Then there are exact sequences

$$0 \to N/M \cap \mathfrak{a}^n N \to M/\mathfrak{a}^n M \to L/\mathfrak{a}^n L \to 0.$$

and we just have to apply Prop. 15.2.

(2) There is an exact sequence $P' \to P \to M \to 0$, where P and P' are finite free A-modules. Obviously, γ_P is an isomorphism. Therefore, we obtain a commutative diagram with exact rows

$$\begin{array}{ccccccc}
\hat{A}_{\mathfrak{a}} \otimes_A P' & \longrightarrow & \hat{A}_{\mathfrak{a}} \otimes_A P & \longrightarrow & \hat{A}_{\mathfrak{a}} \otimes_A M & \longrightarrow & 0 \\
\downarrow{\scriptstyle \gamma_{P'}} & & \downarrow{\scriptstyle \gamma_P} & & \downarrow{\scriptstyle \gamma_M} & & \\
\hat{P}'_{\mathfrak{a}} & \longrightarrow & \hat{P}_{\mathfrak{a}} & \longrightarrow & \hat{M}_{\mathfrak{a}} & \longrightarrow & 0
\end{array}$$

As γ_P and $\gamma_{P'}$ are isomorphisms, so is γ_M.

(3) By (1) and (2), the map $\hat{A}_{\mathfrak{a}} \otimes_A N \to \hat{A}_{\mathfrak{a}} \otimes_A M$ is injective for every injective map of finite modules $N \to M$. It remains to apply the criterion of flatness (Thm. B.11). □

Corollary 15.9. *Let A be a Noetherian ring, $\mathfrak{a}$ and I be ideals in A, M be a finite A-module.*

(1) $\widehat{(IM)}_{\mathfrak{a}} = I\hat{M}_{\mathfrak{a}}$.

(2) *The map $\iota_{\hat{\mathfrak{a}}}$ is an isomorphism, where $\hat{\mathfrak{a}} = \mathfrak{a}\hat{A}_{\mathfrak{a}}$.*

Proof. We write $\hat{M}$ instead of $\hat{M}_{\mathfrak{a}}$.

(1) Left side of this equality is the image of the map $(I \otimes_A M) \otimes_A \hat{A} \to M \otimes_A \hat{A}$, while the right side is the image of the map $I \otimes_A (M \otimes_A \hat{A}) \to M \otimes_A \hat{A}$. Now use the associativity of tensor product.

(2) Evidently, $\widehat{M/\mathfrak{a}^n M} \simeq M/\mathfrak{a}^n M$. From (1) we see that $\hat{M}/\mathfrak{a}^n \hat{M} \simeq \widehat{M/\mathfrak{a}^n M} \simeq M/\mathfrak{a}^n M$, hence $\hat{\hat{M}} \simeq \hat{M}$. □

Remark 15.10. Note that always $\hat{\mathfrak{a}} = \mathfrak{a}\hat{A}_{\mathfrak{a}} \subseteq \operatorname{rad} \hat{A}$. Indeed, if $a \in \hat{\mathfrak{a}}$, then $1 + a + a^2 + \cdots = (1-a)^{-1}$, so use Prop. 3.11.

Theorem 15.11. *Let A be a Noetherian ring, $\mathfrak{a} \subset A$ be an ideal. The following conditions are equivalent:*

(1) $\mathfrak{a} \subseteq \operatorname{rad} A$.
(2) $M \neq 0$ *implies* $M \otimes_A \hat{A}_\mathfrak{a} \neq 0$.
(3) $\hat{A}_\mathfrak{a}$ *is* faithfully flat *over A, that is a sequence of A-modules $N \xrightarrow{\alpha} M \xrightarrow{\beta} L$ is exact if and only if so is the sequence $N \otimes_A \hat{A}_\mathfrak{a} \xrightarrow{\alpha\otimes 1} M \otimes_A \hat{A}_\mathfrak{a} \xrightarrow{\beta\otimes 1} L \otimes_A \hat{A}_\mathfrak{a}$.*
(4) *If M is an A-module, $N, N' \subseteq M$ its submodules and $\hat{A} \otimes_A N = \hat{A} \otimes_A N'$, then $N = N'$.*
(If M is finite, it means that if $\hat{N}' = \hat{N}$, then $N = N'$.)
(5) $\hat{N} \cap M = N$ *for every submodule N of a finire A-module M; in particular, $I\hat{M}_\mathfrak{a} \cap M = IM$ for every ideal $I \subseteq A$.*
(6) $I\hat{A}_\mathfrak{a} \cap A = I$ *for every ideal $I \subset A$.*

Proof. (1) $\Rightarrow$ (2). Let $M \ni v \neq 0$, $N = Av \subseteq M$. Then $\mathfrak{a}N \neq N$ by Nakayama lemma, hence $N \otimes_A \hat{A}_\mathfrak{a} \simeq N_\mathfrak{a} \neq 0$. As the map $N \otimes_A \hat{A}_\mathfrak{a} \to M \otimes_A \hat{A}_\mathfrak{a}$ is an embedding, $M \otimes_A \hat{A}_\mathfrak{a} \neq 0$.

(2) $\Rightarrow$ (4). Let first $N' \subseteq N$, $L = N'/N$. If $\hat{A} \otimes_A N = \hat{A} \otimes_A N'$, then $\hat{L} = 0$, hence $L = 0$ and $N = N'$. In general case, set $N'' = N + N'$. Then $\hat{A} \otimes_A N'' = \hat{A} \otimes_A N = \hat{A} \otimes_A N'$, whence $N'' = N = N'$.

(4) $\Rightarrow$ (3). As $\hat{A}$ is flat, $\operatorname{Im}(\alpha\otimes 1) = \operatorname{Im}\alpha \otimes_A \hat{A}$ and $\operatorname{Ker}(\beta\otimes 1) = \operatorname{Ker}\beta \otimes_A \hat{A}$. (4) implies that if $\operatorname{Im}(\alpha \otimes 1) = \operatorname{Ker}(\beta \otimes 1)$, then $\operatorname{Im}\alpha = \operatorname{Ker}\beta$.

(3) $\Rightarrow$ (2) is obtained if we consider the sequence $0 \to M \to 0$.

(2) $\Rightarrow$ (1). If $\mathfrak{a} \nsubseteq \mathfrak{m}$ for some maximal ideal $\mathfrak{m}$, then $\mathfrak{a} + \mathfrak{m} = A$, which implies that $\mathfrak{a}\hat{A} + \mathfrak{m}\hat{A} = \hat{A}$. As $\mathfrak{a}\hat{A} \subseteq \operatorname{rad}\hat{A}$, we have that $\mathfrak{m}\hat{A} = \hat{A}$, whence $\hat{A} \otimes_A (A/\mathfrak{m}) = 0$.

(1) $\Rightarrow$ (5). An element $v \in M$ belongs to $\hat{N}$ if and only if for each k there is an element $v_k \in N$ such that $v \equiv v_k \pmod{\mathfrak{a}^k}$, that is $v \in N + \mathfrak{a}^k$. As $\bigcap_{k=1}^\infty (N + \mathfrak{a}^k) = N$, it means that $v \in N$.

(5) $\Rightarrow$ (6) is trivial.

(6) $\Rightarrow$ (1). Suppose that $\mathfrak{a} \nsubseteq \mathfrak{m}$ for some maximal ideal $\mathfrak{m}$. Then $\mathfrak{m} + \mathfrak{a} = A$. Therefore $\mathfrak{a}(A/\mathfrak{m}) = A/\mathfrak{m}$, $\widehat{A/\mathfrak{m}} = 0$ and $\hat{A} = \hat{\mathfrak{m}} = \mathfrak{m}\hat{A}$, so $\mathfrak{m}\hat{A} \cap A = A \neq \mathfrak{m}$ $\square$

16. Complete local rings. Hensel lemma

Definition 16.1. A local ring A with the maximal ideal $\mathfrak{m}$ is called *complete* if the homomorphism $\iota_\mathfrak{m} : A \to \hat{A}_\mathfrak{m}$ is an isomorphism.

Actually it means that, given a sequence $a_1, a_2, \dots, a_k, \dots$ of elements from A such that $a_{k+1} \equiv a_k \pmod{\mathfrak{m}^k}$ for all k, there is a unique element a such that $a \equiv a_k \pmod{\mathfrak{m}^k}$ for all k. Then we write $a = \lim_k a^k$. In particular, $\bigcap_{k=1}^\infty \mathfrak{m}^k = 0$, like in Noetherian case.

Theorem 16.2. *Let A be a complete local ring with the maximal ideal $\mathfrak{m}$, f, g, h be monic polynomials from $A[x]$, and $d \in A$ be such that*

(a) $d \in (g, h)$.
(b) $f \equiv gh \mod d^2\mathfrak{m}$

There are monic polynomials $g, h \in A[t]$ such that

(1) $f = \tilde{g}\tilde{h}$.
(2) $\tilde{g} \equiv g \mod d\mathfrak{m}$ *and* $\tilde{h} \equiv h \mod d\mathfrak{m}$.

Proof. We shall construct monic polynomials g_k, h_k such that

(1_k) $f \equiv g_k h_k \mod d^2\mathfrak{m}^k$.
(2_k) $g_{k+1} \equiv g_k \mod d\mathfrak{m}^k$ and $h_{k+1} \equiv h_k \mod d\mathfrak{m}^k$.

Then, as A is complete, we can set of $\tilde{g} = \lim_k g_k$ and $\tilde{h} = \lim_k h_k$.

We proceed recursively, starting from $g_1 = g$ and $h_1 = h$. Let we have constructed g_k and h_k. Then $f = g_k h_k + r$, where $r \in d^2\mathfrak{m}^k A[t]$. As $d \in (g, h)$, $r = gu + hv$ for some $u, v \in d\mathfrak{m}^k A[x]$. Replacing v by its residue modulo g, we can suppose that $\deg v < \deg g$. Then $\deg u < \deg h$. Set $g_{k+1} = g_k + v$ and $h_{k+1} = h_k + u$. Then $g_{k+1}h_{k+1} = g_k h_k + (g_k u + h_k v) + uv$. Note that $g_k u + h_k v \equiv gu + hv = r \mod d^2\mathfrak{m}^{k+1}$ and $uv \in d^2\mathfrak{m}^{2k}A[x]$. Therefore, $g_{k+1}h_{k+1} \equiv g_k h_k + r = f \mod d^2\mathfrak{m}^{k+1}$ and we are done. □

Remark 16.3. Actually we can always effectively construct an element from A belonging to (g, h). Let $g(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n$ and $h(x) = b_0x^m + b_1x^{n-1} + \cdots + b_m$. Set $R(g, h) = \det \mathbf{R}$, where

$$\mathbf{R} = \begin{pmatrix} a_0 & 0 & 0 & \dots & 0 & b_0 & 0 & 0 & \dots & 0 \\ a_1 & a_0 & 0 & \dots & 0 & b_1 & b_0 & 0 & \dots & 0 \\ a_2 & a_1 & a_0 & \dots & 0 & b_2 & b_1 & b_0 & \dots & 0 \\ a_3 & a_2 & a_1 & \dots & 0 & b_3 & b_2 & b_1 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & a_n & 0 & 0 & 0 & \dots & b_m \end{pmatrix}$$

(of size $(m + n) \times (m + n)$; m columns for a_i and n columns for b_i). Then there are polynomials $u(x), v(x)$ such that $\deg u < m$, $\deg v < n$ and $gu + hv = R(g, h)$. ($R(g, h)$ is called the *resultant* of g and h). To prove it, write u and v with "indeterminate coefficients": $u = \sum_{i=0}^{m-1} u_i x^{m-1-i}$ and $v = \sum_{i=0}^{n-1} v_i x^{n-i-1}$ and obtain a system of linear equations for u_i, v_i with $\mathbf{R}$ as the matrix of coefficients. Now take for $(u_0, u_1, \dots, u_{m-1}, v_0, v_1, \dots, v_{n-1})^\top$ the last column of the adjoint matrix $\tilde{\mathbf{R}}$.

Corollary 16.4 (Hensel lemma)**.**[9] *Let A be a complete local ring with the maximal ideal $\mathfrak{m}$, $f \in A[t]$ be a monic polynomial and $a \in A$ are such that $f(a) \equiv 0 \mod f'(a)^2\mathfrak{m}$. There is $\tilde{a} \in A$ such that $f(\tilde{a}) = 0$ and $\tilde{a} \equiv a \mod f'(a)\mathfrak{m}$.*

[9] We also refer to Thm. 16.2 as to "Hensel lemma".

Proof. Let $f(x) = (x-a)g(x) + r(x)$. Then $r(x) \equiv 0 \mod f'(a)^2\mathfrak{m}$, hence $f'(x) \equiv g(x) + (x-a)g'(x) \mod f'(a)^2\mathfrak{m}$ and $f'(a) \equiv g(a) \mod f'(a)^2\mathfrak{m}$. As always $g(a) \in (x-a, g(x))$, we can apply Thm. 16.2 to the polynomials $f, g, x-a$. It gives us $\tilde{a} \equiv a \mod f'(a)\mathfrak{m}$ and $\tilde{g}$ such that $f(x) = (x-\tilde{a})\tilde{g}$. □

The simplest case of Thm. 16.2 and Cor. 16.4 is when $d = 1$ (respectively, $f'(a) \notin \mathfrak{m}$). Then they can be easily generalized using induction (we leave the details to the reader).

Corollary 16.5. *Let A be a complete local ring with the maximal ideal $\mathfrak{m}$.*

1. *If $f \equiv g_1 g_2 \dots g_m \mod \mathfrak{m}$, where $f, g_1, g_2, \dots, g_m$ are monic polynomials and $g_1, g_2, \dots, g_m$ are pairwise coprime (that is $(g_i, g_j) \ni 1$ for all $i \neq j$), there are polynomials $\tilde{g}_1, \tilde{g}_2, \dots, \tilde{g}_m$ such that $f = \tilde{g}_1\tilde{g}_2\dots\tilde{g}_m$ and $\tilde{g}_i \equiv g_i \mod \mathfrak{m}$.*
2. *Let $\lambda_1, \lambda_2, \dots, \lambda_m \in A$ be such that $f(\lambda_i) \equiv 0 \mod \mathfrak{m}$, $f'(\lambda_i) \not\equiv 0 \mod \mathfrak{m}$ and $\lambda_i \not\equiv \lambda_j \mod \mathfrak{m}$ if $i \neq j$. There are elements $\tilde{\lambda}_1, \tilde{\lambda}_2, \dots, \tilde{\lambda}_m$ such that $f(\tilde{\lambda}_i) = 0$ and $\tilde{\lambda}_i \equiv \lambda_i \mod \mathfrak{m}$.*

Exercise 16.6. Let $f_1, f_2, \dots, f_n \in A[x_1, x_2, \dots, x_n]$, where A is a complete local ring with the maximal ideal $\mathfrak{m}$,

$$J = \begin{pmatrix} \frac{\partial f_1}{\partial x_1} & \frac{\partial f_1}{\partial x_2} & \dots & \frac{\partial f_1}{\partial x_n} \\ \frac{\partial f_2}{\partial x_1} & \frac{\partial f_2}{\partial x_2} & \dots & \frac{\partial f_2}{\partial x_n} \\ \dots\dots & \dots\dots & \dots\dots & \dots\dots \\ \frac{\partial f_n}{\partial x_1} & \frac{\partial f_n}{\partial x_2} & \dots & \frac{\partial f_n}{\partial x_n} \end{pmatrix}$$

and $D = \det J(\mathbf{a})$. Let $\mathbf{a} = (a_1, a_2, \dots, a_n) \in A^n$ be such that $f_i(\mathbf{a}) \equiv 0 \pmod{D^2\mathfrak{m}}$ for all i. Prove that there is $\tilde{\mathbf{a}} = (\tilde{a}_1, \tilde{a}_2, \dots, \tilde{a}_n) \in A^n$ such that $f_i(\tilde{\mathbf{a}}) = 0$ and $\tilde{a}_i \equiv a_i \pmod{D\mathfrak{m}}$ for all i.

Theorem 16.7. *Let A be a ring, B be a local complete A-algebra with the maximal ideal $\mathfrak{n}$ and $b_1, b_2, \dots, b_n$ be elements from $\mathfrak{n}$.*

1. *There is a unique homomorphism of A-algebras $\varphi : A[[x_1, x_2, \dots, x_n]] \to B$ such that $\varphi(x_i) = b_i$.*
2. *If the map $A \to B/\mathfrak{n}$ is surjective and $\mathfrak{n} = (b_1, b_2, \dots, b_n)_B$, then φ is surjective.*
3. *If the induced map of graded rings $A[x_1, x_2, \dots, x_n] \to \operatorname{gr}_{\mathfrak{n}} B$ is a monomorphism, so is φ.*

Proof. (1) There is a homomorphism of A-algebras $\bar{\varphi} : A[x_1, x_2, \dots, x_n] \to B$ mapping $x_i \mapsto b_i$. It induces homomorphisms $\varphi_m : A[x_1, x_2, \dots, x_n]/\mathfrak{m}^m \to B/\mathfrak{n}^m$, where $\mathfrak{m} = (x_1, x_2, \dots, x_n)$. They are compatible with the epimorphisms $A[x_1, x_2, \dots, x_n]/\mathfrak{m}^{n+1} \to A[x_1, x_2, \dots, x_n]/\mathfrak{m}^n$ and $B/\mathfrak{n}^{n+1} \to B/\mathfrak{n}^n$, hence induce a homomorphism of inverse limits $\varphi : A[[x_1, x_2, \dots, x_n]] \to B$. Obviously, φ is unique.

(2) Under these conditions, the induced maps $\mathfrak{m}^k \to \mathfrak{n}^k/\mathfrak{n}^{k+1}$ are surjective. If $b \in \mathfrak{n}$, there is $a_1 \in \mathfrak{m}$ such that $b = \varphi(a_0) + b_1$, where $b_1 \in \mathfrak{n}^2$. In the same way, we construct $b_2, b_3, \dots$ such that $b - \sum_{i=1}^{k} \in \mathfrak{n}^{k+1}$ and $b_k = \varphi(a_k)$, where $a_k \in \mathfrak{m}^k$. Set $a = \sum_{k=0}^{\infty} a_k$. Then $\varphi(a) \equiv b \pmod{\mathfrak{n}^{m+1}}$ for every m. Therefore $\varphi(a) = b$, since $\bigcap_{m=1}^{\infty} \mathfrak{n}^m = 0$.

(3) Note that this condition actually means that the composition $A \to B \to B/\mathfrak{n}$ is injective and $f(b_1, b_2, \dots, b_n) \notin \mathfrak{n}^{d+1}$ for every homogeneous polynomial $f \in A[x_1, x_2, \dots, x_n]$ of degee d. If f consists of nonzero terms of minimal degree from a series $g \in A[[x_1, x_2, \dots, x_n]]$, then $\varphi(g) \equiv \varphi(f) \not\equiv 0 \pmod{\mathfrak{n}^{d+1}}$, hence $\varphi(g) \neq 0$. □

Theorem 16.8. *Let A be Noetherian, $\mathfrak{a} \subset A$ be an ideal, $\mathfrak{a} = (a_1, a_2, \dots, a_n)$. Then $\hat{A}_{\mathfrak{a}} \simeq A[[x_1, x_2, \dots, x_n]]/I$, where $I = (x_1 - a_1, \dots, x_n - a_n)$. In particular, $\hat{A}_{\mathfrak{a}}$ is Noetherian.*

Proof. Consider the ring $A' = A[x_1, x_2, \dots, x_n]$ and its ideals $J = (x_1 - a_1, \dots, x_n - a_n)$ and $\mathfrak{m} = (x_1, x_2, \dots, x_n)$. Then $A[[x_1, x_2, \dots, x_n]] = \hat{A}'_{\mathfrak{m}}$ and $I = J\hat{A}'_{\mathfrak{m}}$. Obviously, $A'/J \simeq A$ and under this isomorphism $\mathfrak{m}$ is mapped to $\mathfrak{a}$. Taking $\mathfrak{m}$-adic completions, we obtain

$$A_{\mathfrak{a}} = A_{\mathfrak{m}} \simeq (\widehat{A'/J})_{\mathfrak{m}} \simeq \hat{A}'_{\mathfrak{m}}/\hat{J}_{\mathfrak{m}} \simeq \hat{A}'_{\mathfrak{m}}/J\hat{A}'_{\mathfrak{m}} = \hat{A}'_{\mathfrak{m}}/I. \qquad \square$$

Definition 16.9. Let A be a local ring with the maximal ideal $\mathfrak{m}$. A *field of representatives* for the ring A is a subfield $\Bbbk \subseteq A$ such that the composition $\Bbbk \hookrightarrow A \to A/\mathfrak{m}$ is an isomorphism.

For instance, if $\Bbbk$ is an algebraically closed field, A is a $\Bbbk$-algebra of finite type and $\mathfrak{m}$ is a maximal ideal of A, then $\Bbbk$ is a field of representatives for the localization $A_{\mathfrak{m}}$ by Cor. 4.11. A theorem of Cohen asserts that if A is a complete local ring and $\operatorname{char} A = \operatorname{char} A/\mathfrak{m}$, then A has a field of representatives. If a field of representatives exists, the structure of the complete ring becomes more simple.

Corollary 16.10. *Let A be a complete local ring, $\mathfrak{m}$ be its maximal ideal, $n = \operatorname{gen}_A \mathfrak{m} < \infty$ and $\Bbbk$ be a field of representatives for A. Then $A \simeq \Bbbk[[x_1, x_2, \dots, x_n]]/I$ for some ideal I. In particular, A is Noetherian. If, moreover, A is regular, $A \simeq \Bbbk[[x_1, x_2, \dots, x_n]]$.*

Proof. Just apply Thm. 16.7 to a set of generators of $\mathfrak{m}$. If A is regular, also use Thm. 14.5. □

One can prove that if $\operatorname{char} A = \operatorname{char} \Bbbk$, where $\Bbbk = A/\mathfrak{m}$ (for instance, $\operatorname{char} \Bbbk = 0$ or $\operatorname{char} A = p$), A has a field of representatives. We shall prove it in the simplest case, when A contains a subfiled such that $\Bbbk$ is *separably generated* over its image. We recall that a field $\Bbbk$ is *separably generated* over a subfiled $\Bbbk'$ if there is a subfield such that $\Bbbk''$ is purely transcendent over $\Bbbk'$ while $\Bbbk$ is algebraic and separable over $\Bbbk''$. Note that if $\Bbbk$ is a finite field of characteristic p, it contains the prime field $\mathbb{F}_p$ and is algebraic and separable

(hence separably generated) over $\mathbb{F}_p$. In what follows we identify a subfield $\Bbbk' \subseteq A$ with its image in $\Bbbk$.

Theorem 16.11. *Let A be a complete local ring, $\mathfrak{m}$ be its maximal ideal and $\Bbbk = A/\mathfrak{m}$. Suppose that A contains a subfield $\Bbbk'$ such that $\Bbbk$ is* separably generated *over $\Bbbk'$. Then A has a field a representatives $F \supseteq \Bbbk'$.*

Proof. Let $\Bbbk' \subseteq \Bbbk'' \subseteq \Bbbk$ be a subfield such that $\Bbbk''$ is purely transcendent over $\Bbbk'$ while $\Bbbk$ is algebraic and separable over $\Bbbk''$, and let $\Bbbk'' = \Bbbk'(x_i \mid i \in \mathscr{I})$, where the elements x_i are algebraically independent over $\Bbbk'$. If a_i is a preimage of x_i in A, then $f(a_{i1}, a_{i2}, \dots, a_{ir}) \not\equiv 0 \pmod{\mathfrak{m}}$ for every nonzero polynomial $f(x_{i1}, x_{i2}, \dots, x_{ir}) \in \Bbbk'(x_i \mid i \in \mathscr{I})$. Therefore, A contains the subfield $\Bbbk'(a_i \mid i \in \mathscr{I})$ that maps isomorphically onto $\Bbbk''$. Hence, we can suppose that $\Bbbk$ is algebraic and separable over $\Bbbk'$.

Zorn lemma implies that there is a maximal subfield F of A containing $\Bbbk'$. If $\alpha \in \Bbbk \setminus F$, $f(x)$ is its minimal polynomial over $\Bbbk'$ and a is a preimage of α in A, we have that $f(a) \equiv 0 \pmod{\mathfrak{m}}$ and $f'(a) \not\equiv 0 \pmod{\mathfrak{m}}$. By Hensel lemma, there is $b \in A$ such that $f(b) = 0$. Then $F(b) \simeq F(\alpha)$ is a bigger subfield of A. Therefore, $F = \Bbbk$. □

Corollary 16.12. *Let A be a complete local ring, $\mathfrak{m}$ be its maximal ideal, $\Bbbk = A/\mathfrak{m}$ and $n = \operatorname{emb.dim} A < \infty$. If $\operatorname{char} \Bbbk = 0$ or $\operatorname{char} A = p$ and $\Bbbk$ is a finite field, then $A \simeq \Bbbk[[x_1, x_2, \dots, x_n]]/I$ for some ideal I. In particular, A is Noetherian. If, moreover, A is regular, $A \simeq \Bbbk[[x_1, x_2, \dots, x_n]]$.*

17. Valuation rings and valuations

Definition 17.1. Let V be a domain, K be its field of fractions. We call V a *valution ring in the field K* if for every elelment $a \in K$ either $a \in A$ or $a^{-1} \in A$.

Example 17.2.
(1) Obviously, if V' is a subring of K containing V, it is also a valuation ring.
(2) Every discrete valuation ring is a valuation ring (**explain it**).
(3) Let $V_n \subset \Bbbk(x_1, x_2, \dots, x_n)$, where $\Bbbk$ is a field, $V = \{f/g \mid \deg f \leqslant \deg g\}$. Obviously, it is a valuation ring.

Exercise 17.3. Prove that V_n from the last example is a discrete valuation ring with the residue field isomorphic to $\Bbbk(x_1, x_2, \dots, x_{n-1})$.

Proposition 17.4. *Let V be a valuation ring with the field of fractions K. Then V is normal and local with the maximal ideal $\mathfrak{m} = \mathfrak{m}_V = \{a \in V \mid a^{-1} \notin V\}$.*

Proof. Suppose that $q \in K$ is integral over V, that is $q^n + a_1 q^{n-1} + \dots + a_n = 0$ for some $a_i \in V$. If $q \notin V$, then $q^{-1} \in V$ and $q = -a_1 - a_2 q^{-1} - \dots - a_n q^{-n} \in V$, a contradiction. So V is normal.

Obviously, if $a \in \mathfrak{m}$, $b \in V$, then $ab \in \mathfrak{m}$. Let a, b be nonzero elements from $\mathfrak{m}$. Either $a/b \in V$ or $b/a \in V$. If $a/b \in V$, then $a + b = b(a/b + 1) \in \mathfrak{m}$. If

$b/a \in V$, then $a + b = a(1 + b/a) \in \mathfrak{m}$. Therefore, $\mathfrak{m}$ is an ideal. As neither proper ideal contains invertible elements, $\mathfrak{m}$ contains all proper ideals. □

Remark 17.5. If V is a valuation ring in the field K, then $\mathfrak{m}_V = \{a \in K \mid a^{-1} \notin V$. In particular, if $V \nsubseteq V'$, then $\mathfrak{m}_V \not\supseteq \mathfrak{m}_{V'}$.

Exercise 17.6. Prove that:

(1) Every valuation ring V is a *Bezout ring*, that is every finitely generated ideal of V is principal.
(2) A Noetherian ring is a valuation ring if and only if it is a discrete valuation ring.
(3) If V is a valuation ring, $\mathfrak{p}$ is its prime ideal, then $A/\mathfrak{p}$ and $A_{\mathfrak{p}}$ are also valuation rings.

We shall show that there are valuation rings between each domain and its field of fractions, and even "many" of them.

Theorem 17.7. *Let A be a domain, K be its field of fractions.*

(1) *For every prime ideal $\mathfrak{p} \in A$ there is a valuation ring V with the maximal ideal $\mathfrak{m}$ such that $\mathfrak{m} \cap A = \mathfrak{p}$.*
(2) *Let $\mathfrak{V} = \{V \mid V$ is a valuation ring and $A \subseteq V \subseteq K\}$. Then $\operatorname{Int}(A, K) = \bigcap_{V \in \mathfrak{V}} V$.*

Proof. (1) Replacing A by $A_{\mathfrak{p}}$, we can suppose that A is local and $\mathfrak{p}$ is its maximal ideal. Then $\mathfrak{m} \cap A = \mathfrak{p}$ means the same as $\mathfrak{p}V \neq V$. Let $\mathfrak{A}$ be the set of subrings $B \subseteq K$ such that $A \subseteq B$ and $\mathfrak{p}B \neq B$. By Zorn's lemma, $\mathfrak{A}$ contains a maximal element V. If $\mathfrak{m} \subset V$ is a maximal ideal containing $\mathfrak{p}V$, then $\mathfrak{p}V_{\mathfrak{m}} \neq V_{\mathfrak{m}}$. As V is maximal, $V = V_{\mathfrak{m}}$, that is V is local with the maximal ideal $\mathfrak{m}$.

Let $q \in K$. If $q \in K$ is integral over V, then $\mathfrak{m}V[q] \neq V[q]$, hence $\mathfrak{p}V[q] \neq V[q]$. As V is maximal, $q \in V$, so V is normal. If $\mathfrak{m}V[q^{-1}] \neq V[q^{-1}]$, then $q^{-1} \in V$, since V is maximal. If $\mathfrak{m}V[q^{-1}] = V[q^{-1}]$, there are elements $a_1, a_2, \dots, a_m \in \mathfrak{m}$ such that $a_0 + a_1 q^{-1} + a_2 q^{-2} + \dots + a_m q^{-m} = 1$, whence $q^m(1 - a_0) = a_1 a^{m-1} + a_2 q^{m-2} + \dots a_m$. As $1 - a_0$ is invertible, it means that q is integral over V, hence $q \in V$ and V is a valuation ring.

(2) As all valuation rings are normal, $\operatorname{Int}(A, K) \subseteq \bigcap_{V \in \mathfrak{V}} V$. Suppose that $a \notin \operatorname{Int}(A, K)$. Then $a \notin A[a^{-1}]$. Choose a maximal ideal $\mathfrak{p} \subset A[a^{-1}]$ containing a^{-1}. There is a valuation ring $V \supseteq A[a^{-1}]$ with the maximal ideal $\mathfrak{m}$ such that $\mathfrak{m} \cap A[a^{-1}] = \mathfrak{p}$. As $a^{-1} \in \mathfrak{m}$, $a \notin V$. □

Valuation rings are closely connected with *valuations* on a field.

Definition 17.8. Let K be a field, Γ be an *ordered abelian group*. It means that there is a total order $\leqslant$ on Γ such that $\alpha \leqslant \beta$ implies $\alpha + \gamma \leqslant \beta + \gamma$ for every γ. A *valuation on K with values in Γ* is a homomorphism $v : K^\times \to \Gamma$ such that $v(a + b) \geqslant \min\{v(a), v(b)\}$.

We shall show that actually there is an "almost" one-to-one correspondence between valuation rings and valuations.

Theorem 17.9. (1) *Let $v : K^\times \to \Gamma$ be a valuation on a field K, $V_v = \{a \in K \mid v(a) \geqslant 0\} \cup \{0\}$. Then V_v is a valuation ring with the maximal ideal $\mathfrak{m} = \{a \in K \mid v(a) > 0\} \cup \{0\}$.*

(2) *Let V be a valuation ring with the field of fractions K, $\Gamma_V = K^\times/V^\times$. For two cosets $\alpha, \beta \in \Gamma_V$ with representatives $a \in \alpha$, $b \in \beta$ set $\alpha \leqslant \beta$ if $b/a \in V$. Set also $v_V(a) = aV^\times \in \Gamma_V$. Then Γ_V is a totally ordered group and $v_V : K^\times \to \Gamma_V$ is a valuation.*

(3) (a) *$V_{v_V} = V$ for every valuation ring V.*

(b) *For every valuation v there is an isomorophism $\gamma : \Gamma_{V_v} \xrightarrow{\sim} \operatorname{Im} v$ such that $v = \gamma \circ v_{V_v}$.*

Proof. (1) One easily sees that V_v is a ring and $\mathfrak{m}$ is an ideal in V_v. If $0 \neq a \notin V$, i.e. $v(a) < 0$, then $v(a^{-1}) = -v(a) > 0$, thus $a \in V_v$ and V_v is a valuation ring. If $a \in \mathfrak{m}$, i.e $v(a) > 0$, then $v(a^{-1}) < 0$, so $a^{-1} \notin A$. If $a \in V_v \setminus \mathfrak{m}$, i.e. $v(a) = 0$, then also $v(a^{-1}) = 0$, hence $a \in V_v^\times$. Therefore, $\mathfrak{m} = V_v \setminus V_v^\times$ is the maximal ideal of V.

(2) By definition, v_V is a homomorphism. If $\alpha = aV^\times$, $\beta = bA^\times$, then either $a/b \in V$ or $b/a \in V$, hence either $\beta \leqslant \alpha$ or $\alpha \leqslant \beta$. So Γ is totally ordered. Let $\alpha \leqslant \beta$. Then $b = ca$, hence $a + b \in aA$ and $v(a + b) \geqslant v(a)$. Therefore, $v(a + b) \geqslant \min\{v(a), v(b)\}$ and v is a valuation.

(3) immediately follows from definitions (**explain the details**). □

Example 17.10. (1) Let D be a discrete valuation ring, K be its field of fractions, $\mathfrak{m} = (p)$ be the maximal ideal of D. Then every element $a \in K^\times$ can be uniquely presented as $up^{v(a)}$, where $u \in D^\times$ and $v(a) \in \mathbb{Z}$. Therefore, $K^\times/D^\times \simeq \mathbb{Z}$ and $a \mapsto v(a)$ is just the valuation v_D. We claim that there are no rings A such that $D \subset A \subset K$. Indeed, if $A \ni a$ and $v(a) = -n$ with $n > 0$, $A \supseteq p^{-m}D$ for all $m > 0$, therefore, $A = K$.

(2) Let now D be a Dedekind ring, K be its field of fractions and $\mathfrak{p} \subset D$ be a maximal ideal of D. Then $D_\mathfrak{p}$ is a discrete valuation ring. We denote by $v_\mathfrak{p}$ the corresponding valuation and call it the *$\mathfrak{p}$-adic valuation* on the field K. Let v be any valuation on K such that $v(a) \geqslant 0$ for every $a \in D$, $\mathfrak{p} = \{a \in D \mid v(a) > 0\}$. It is a prime ideal in D and obviously $V_v \supseteq D_\mathfrak{p}$. Therefore $V = D_\mathfrak{p}$ and $v = v_\mathfrak{p}$. Therefore, $\mathfrak{p}$-adic valuations are the only valuations on K positive on D.

Exercise 17.11. (1) Prove that if v is a valution with values in $\mathbb{Z}$, then V_v is a discrete valuation ring.

18. Krull rings

Definition 18.1. A *Krull ring* is a domain A with the field of fractions K such that there is a set $\mathscr{D}$ of discrete valuation rings $D \subset K$ such that $A = \bigcap_{D \in \mathscr{D}} D$ and for every element $q \in K$ the set $\{D \in \mathscr{D} \mid a \notin D\}$ is finite.

If we denote by v_D the valuation of K corresponding to D, the last condition means that for every $a \in A$ the set $\{D \mid v_D(a) \neq 0\}$ is finite.

As all discrete valuation rings are normal, so is every Krull domain. On the other hand, Theorem 11.2 implies that every Noetherian normal ring is a Krull ring. Considering a Krull domain, we will always mean that the set $\mathscr{D}$ is given. For a discrete valuation ring D we denote by $\mathfrak{m}_D$ its maximal ideal.

Proposition 18.2. *Let A be a Krull ring, $S \subset A$ be a multiplicative subset of A. Then $A[S^{-1}]$ is also a Krull ring. Namely, $A[S^{-1}] = \bigcap_{D\in\mathscr{D}_S} D$, where $\mathscr{D}_S = \{D \in \mathscr{D} \mid D \supseteq A[S^{-1}]\}$, or, the same $\mathscr{D}_S = \{D \in \mathscr{D} \mid S \cap \mathfrak{m}_D = \varnothing\}$.*

Proof. Obviously, $\bigcap_{D\in\mathscr{D}_S} D \supseteq A[S^{-1}]$. Let $a \in \bigcap_{D\in\mathscr{D}_S} D$. There are only finitely many $D \in \mathscr{D}$ such that $v_D(a) < 0$, let they be $D_1, D_2, \dots, D_r$, $\mathfrak{m}_i = \mathfrak{m}_{D_i}$ and $v_i = v_{D_i}$. As $D_i \notin \mathscr{D}_S$, there is $s_i \in S \cap \mathfrak{m}_i$. Then $v_i(s_i) > 0$ and, changing s_i to s_i^k with k rather big, we can suppose that $v_i(s_i a) \geqslant 0$. Let $s = s_1 s_2 \dots s_r$. Then $v_D(sa) \geqslant 0$ for all $D \in \mathscr{D}$, hence $sa \in A$ and $a \in A[S^{-1}]$. □

Lemma 18.3. *Let V be a valuation ring in a field K. For every element $a \in K$ there is an integer d such that for every integer $s \geqslant 2$ such that $d \nmid s$ the elements $a(s) = (1 + a + a^2 + \dots + a^{s-1})^{-1}$ and $aa(s)$ are in V.*

Proof. Let $\mathfrak{m}$ be the maximal ideal of V and $p = \operatorname{char} V/\mathfrak{m}$. Note that $a(s) = \dfrac{1-a}{1-a^s} = a^{-s+1}\dfrac{a^{-1}-1}{a^{-s}-1}$. Therefore, if $a \notin V$, $a(s)$ and $aa(s)$ are in V, so $d = 1$. If $a \in V$ and $a \equiv 1 \pmod{\mathfrak{m}}$, then $d = p$. If $a^k \not\equiv 1 \pmod{\mathfrak{m}}$, for every k, also $d = 1$. If $a \not\equiv 1 \pmod{\mathfrak{m}}$ but $a^k \equiv 1 \pmod{\mathfrak{m}}$ for some $k > 1$, d is the smallest of such k. □

Proposition 18.4. *Let $A = \bigcap_{i=1}^r V_r$ where V_i are valuation rings in a field K with maximal ideals $\mathfrak{m}_i$ and $V_i \nsubseteq V_j$ if $i \neq j$.*

1. *$\mathfrak{p}_i = A \cap \mathfrak{m}_i$ are all maximal ideals of A and $V_i = A_{\mathfrak{p}_i}$.*
2. *If all V_i are discrete valuation ring, A is a principal ideal domain.*

Proof. (1) Obviously, $A_{\mathfrak{p}_i} \subseteq V_i$. Let $a \in V_i$. For every V_j choose d_j such that $a(s)$ and $aa(s)$ are in V_j if $d_j \nmid s$ and choose s such that $d_j \nmid s$ for all j. Then $a(s)$ and $aa(s)$ are in A and $a(s) \in V_i^\times$, hence $a(s) \notin \mathfrak{p}_i$. Therefore, $a = \dfrac{aa(s)}{a(s)} \in A_{\mathfrak{p}_i}$, so $A_{\mathfrak{p}_i} = V_i$. It implies, in particular, that $\mathfrak{p}_i \not\supseteq \mathfrak{p}_j$ if $i \neq j$.

Let I be an ideal in A such that $I \nsubseteq \mathfrak{p}_i$ for all i. Then there is $a \in I$ such that $a \notin \mathfrak{p}_i$ for all i, that is $a \notin \mathfrak{m}_i$. Therefore, a is invertible in all V_i, hence in $\bigcap_{i=1}^r V_i = A$ and $I = A$.

(2) If V_i is a discrete valuation ring, then $\mathfrak{m}_i^2 \neq \mathfrak{m}_i$, hence $\mathfrak{p}_i^{(2)} \neq \mathfrak{p}_i$. Choose $p_i \in \mathfrak{p}_i$ such that $p_i \notin \mathfrak{p}_i^{(2)} \cup \left(\bigcup_{j\neq i} \mathfrak{p}_j\right)$. Then $\mathfrak{p}_i = p_i A$. If $I \subset A$ is an ideal, $IA_{\mathfrak{p}_i} = \mathfrak{p}_i^{m_i}$ for some m_i. Therefore $I = p_1^{m_1} p_2^{m_2} \dots p_r^{m_r}$ (see Claims in Exam. 5.6). □

For a ring A we denote by $\mathscr{P}(A)$ the set of prime ideals in A of height 1.

Theorem 18.5. *Let $A = \bigcap_{D\in\mathscr{D}} D$ be a Krull ring, $\mathscr{P} = \mathscr{P}(A)$.*

(1) *$A_\mathfrak{p} \in \mathscr{D}$ for every $\mathfrak{p} \in \mathscr{P}$.*
(2) *$A = \bigcap_{\mathfrak{p}\in\mathscr{P}} A_\mathfrak{p}$.*

Proof. (1) If $A_\mathfrak{p} \subseteq D$ for some valuation ring D, then $A \setminus \mathfrak{p} \subseteq D^\times$, hence $\mathfrak{m}_D \cap A \subseteq \mathfrak{p}$. If all nonzero elements from A are invertible in D, then $D = K$, which is impossible. Thus $\mathfrak{m}_D \cap A \neq \{0\}$, hence $\mathfrak{m}_D \cap A = \mathfrak{p}$ (since $\operatorname{ht}\mathfrak{p} = 1$) and $v_D(a) > 0$ for every nonzero $a \in \mathfrak{p}$. Therefore the set $\mathscr{D}' = \{D \in \mathscr{D} \mid D \supseteq A_\mathfrak{p}\}$ is finite. By Prop. 18.2, $A_\mathfrak{p} = \bigcap_{D\in\mathscr{D}'} D$. Then $A_\mathfrak{p} \in \mathscr{D}'$ by Prop. 18.4.

(2) Let $a \in A$, $\{D_1, D_2, \dots, D_r\} = \{D \in \mathscr{D} \mid a \in \mathfrak{m}_D\}$ (this set is finite). Denote $\mathfrak{m}_i = \mathfrak{m}_{D_i}$, $\mathfrak{p}_i = \mathfrak{m}_i \cap A$ and $I_i = aD_i \cap A$. Then $aA = \bigcap_{i=1}^r I_i$. As $aD_i = \mathfrak{m}_i^k$ for some k, $\mathfrak{p}_i \supseteq I_i \supseteq \mathfrak{p}_i^k$, so $\mathfrak{p}$ is a unique minimal element from $\operatorname{Ass} I_i$. If $b \in A \setminus \mathfrak{p}_i$, then $b \in D_i^\times$, hence $cb \in I_i$ implies $c \in I_i$. Therefore, no prime ideal $\mathfrak{q} \supset \mathfrak{p}$ is in $\operatorname{Ass} I_i$ and I_i is $\mathfrak{p}_i$-primary. We shall prove that $\operatorname{ht}\mathfrak{p}_i = 1$ for all i, that is $D_i = A_{\mathfrak{p}_i}$.

Denote $\mathfrak{p} = \mathfrak{p}_i$ and suppose that $\operatorname{ht}\mathfrak{p} > 1$. Then $A_\mathfrak{p} = \bigcap_{D\in\mathscr{D}'} D$, where $\mathscr{D}' = \{D \in \mathscr{D} \mid D \subseteq A_\mathfrak{p}\}$. As $A_\mathfrak{p}$ is not a discrete valuation ring, $\mathscr{D}'$ is infinite by Prop. 18.4. Therefore, there is $D_0 \supseteq A_\mathfrak{p}$ such that $a \in D_0^\times$. Let $\mathfrak{q} = \mathfrak{m}_{D_0} \cap A$, then $a \notin \mathfrak{q}$ and $\mathfrak{q} \subseteq \mathfrak{p}$. Note that $aA \not\supseteq J = \bigcap_{j\neq i} I_j$. Let $m > 0$ be the smallest such that $aA \supseteq \mathfrak{p}^m \cap J$ and $c \in \mathfrak{p}^{m-1} \cap J \setminus aA$. Then $c\mathfrak{q} \subseteq aA$. As $a \notin \mathfrak{q}$, it implies that $c\mathfrak{q} \subseteq a\mathfrak{q}$, hence $(c/a)\mathfrak{q} \subseteq \mathfrak{q}$ and $(c/a)^n\mathfrak{q} \subseteq A$ for all n. If $q \in \mathfrak{q}$, it gives that $q(c/a)^n \in A \subset D$ or $D[c/a] \subseteq q^{-1}D$ for every $D \in \mathscr{D}$. As D is Noetherian, it implies that $D[c/a]$ is a finite D-module, that is $c/a \in D$, since D is normal. Therefore, $c/a \in A$, which contradicts the choice of c.

Now let $b \in A$ be such that $b/a \in A_\mathfrak{p}$ for all $\mathfrak{p} \in \mathscr{P}$. Then $b \in aA_{\mathfrak{p}_i}$, hence $b \in I_i$ for all i, that is $b \in aA$ and $b/a \in A$. □

Lemma 18.6 (Approximation lemma)**.** *Let A be a Krull ring with the field of fractions K, $\mathbf{P} = \{\mathfrak{p}_1, \mathfrak{p}_2, \dots, \mathfrak{p}_k\} \subseteq \mathscr{P}(A)$ and $m_1, m_2, \dots, m_k$ be integers. There is an element $a \in K$ such that $v_{\mathfrak{p}_i}(a) = m_i$ $(1 \leqslant i \leqslant k)$ and $v_\mathfrak{p}(a) \geqslant 0$ for $\mathfrak{p} \notin \mathbf{P}$.*

Proof. For every i there is an element a_i such that $a_i \in \mathfrak{p}_i \setminus \big(\bigcap_{j\neq i} \mathfrak{p}_j\big) \cap \mathfrak{p}_i^{(2)}$. Then $v_{\mathfrak{p}_i}(a_i) = 1$, $v_{\mathfrak{p}_j}(a_i) = 0$ for $j \neq i$ and $v_\mathfrak{p}(a_i) \geqslant 0$ if $\mathfrak{p} \notin \mathbf{P}$. Set $b = \prod_{i=1}^k a_i^{m_i}$, then $v_{\mathfrak{p}_i}(b) = m_i$. Let $\mathfrak{q}_1, \mathfrak{q}_2, \dots, \mathfrak{q}_r$ be all primes from $\mathscr{P}(A)$ such that $\mathfrak{q}_j(b) = l_j < 0$. Choose, as above, $c_j \in A$ such that $v_{\mathfrak{q}_j} = 1$, $v_{\mathfrak{q}_{j'}} = 0$ if $j' \neq j$ and $v_{\mathfrak{p}_i}(c_i) = 0$ for all i. Then $a = b\prod_{j=1}^r c_j^{-l_j}$ is what we need. □

Corollary 18.7. (1) *A Krull ring A is Noetherian if and only if $A/\mathfrak{p}$ is Noetherian for every $\mathfrak{p} \in \mathscr{P}(A)$.*
(2) *A ring A is a Dedekind ring if and only if it is a Krull ring of dimension* 1.

Proof. (1) Let $\mathfrak{p} \in \mathscr{P}(A)$. By Lem. 18.6, there is an element $q \in K$ such that $v_\mathfrak{p}(q) = 1$ and $v_\mathfrak{q}(q) \leqslant 0$ for every $\mathfrak{q} \in \mathscr{P}(A) \setminus \{\mathfrak{p}\}$. Then $qA_\mathfrak{p} = \mathfrak{p}A_\mathfrak{p}$. Let

$B = A[q] \subseteq A_{\mathfrak{p}}$. Then

$$\mathfrak{p}^{(n)} = \mathfrak{p}^n A_{\mathfrak{p}} \cap A = q^n B \cap A = \{a \in A \mid v_{\mathfrak{p}}(a) \geqslant n\}.$$

As $q^n B/q^{n+1}B \simeq B/qB \simeq A/\mathfrak{p}$ are Noetherian A-modules, so are also $B/q^n B$ and its submodule $A/\mathfrak{p}^{(n)}$.

Let now $a \in A$. Then $aA = \bigcap_{i=1}^r \mathfrak{p}_i^{(n_i)}$ for some $\{\mathfrak{p}_1, \mathfrak{p}_2, \dots, \mathfrak{p}_r\} \subseteq \mathscr{P}(A)$. It implies that A/aA embeds into $\prod_{i=1}^r A/\mathfrak{p}_i^{(n_i)}$, which is Noetherian. Therefore, A/aA, hence also A are Noetherian.

(2) As Dedekind ring is normal, it is Krull ring, and it is of dimension 1. On the contrary, if A is a Krull ring of dimension 1, every ideal $\mathfrak{p} \in \mathscr{P}(A)$ is maximal, so $A/\mathfrak{p}$ is a field. By (1), A is Noetherian. As it is normal, it is a Dedekind ring. □

19. Normalization

19.1. **Algebras of finite type.** Let A be a normal domain, K its field of fractions, a field $L \supseteq K$ be a finite extension of the field K and $B = \mathrm{Int}(A, L)$. The *normalization problem* asks whether B is a finite extension of A. A partial case of this problem, arising from geometry, is the following. Let A be an algebra of finite type over a field $\Bbbk$, K be its field of fractions. Is its integral closure in K also an algebra of finite type? It is indeed a partial case, since A is finite over a subalgebra $N \simeq \Bbbk[x_1, x_2, \dots, x_d]$, K is a finite extension of $\Bbbk(x_1, x_2, \dots, x_d)$ and $\mathrm{Int}(A, K) = \mathrm{Int}(N, K)$. Therefore, $\mathrm{Int}(A, K)$ is of finite type if and only if it is a finite N-module. There are examples that show that, even if A is a discrete valuation ring, B can be not finite over A (see [8, (E3.2), p.206]). Nevertheless, in the "geometric situation" the answer is positive.

Theorem 19.1 (Noether)**.** *Let A be a domain which is an algebra of finite type over a field $\Bbbk$, L be a finite extension of its field of fractions K (maybe $L = K$). Then $\mathrm{Int}(A, L)$ is a finite A-algebra, hence an algebra of finite type over $\Bbbk$.*

First we recall some facts about separable extensions and traces. Let L be a finite extension of K, $\alpha \in L$. We denote by Φ_α the linear map $v \mapsto \alpha v$ in the K-vector space L and by $\mathrm{tr}_{L/K}\,\alpha$, or by $\mathrm{tr}\,\alpha$ if there can be no ambiguity, the trace $\mathrm{tr}\,\Phi_\alpha$. Let $\mu_\alpha(x) = x^m + a_1 x^{m-1} + \dots + a_m$ be the minimal polynomial of α over K. Chose a basis $\omega_1, \omega_2, \dots, \omega_k$ of L over $K(\alpha)$. Then $\{\alpha^i \omega_j \mid 0 \leqslant i < m, 1 \leqslant j \leqslant k\}$ is a basis of L over K and an easy calculation shows that $\mathrm{tr}_{L/K}\,\alpha = -ka_1$. If A is normal and α is integral over A, then $\mathrm{tr}_{L/K}\,\alpha \in A$.

Lemma 19.2. *If L is a finite separable extension of K, there is $\lambda \in L$ such that $\mathrm{tr}_{L/K}\,\lambda \neq 0$.*

Proof. If $\mathrm{char}\,K = 0$, just set $\lambda = 1$; then $\mathrm{tr}\,\lambda = (L : K) \neq 0$. If $\mathrm{char}\,K > 0$, we must use another consideration. Namely, it is known that $L = K(\theta)$ for

some element θ. Let $f(t)$ be the minimal polynomial of θ over K. In some extension $L' \supseteq L$ it decomposes as $\prod_{i=1}^{n}(x-\theta_i)$, where $\theta_1 = \theta$ and $\theta_i \neq \theta_j$ if $i \neq j$, since θ is separable. Then over the field L' the matrix Φ_θ is similar to $\operatorname{diag}(\theta_1, \theta_2, \ldots, \theta_n)$. Therefore, $\operatorname{tr}\theta^k = \operatorname{tr}\Phi_\theta^k = \sum_{i=1}^{n}\theta_i^k$. As all θ_i are different,

$$\begin{vmatrix} 1 & 1 & \ldots & 1 \\ \theta_1 & \theta_2 & \ldots & \theta_n \\ \theta_1^2 & \theta_2^2 & \ldots & \theta_n^2 \\ \ldots & \ldots & \ldots & \ldots \\ \theta_1^{n-1} & \theta_2^{n-1} & \ldots & \theta_n^{n-1} \end{vmatrix} \neq 0,$$

hence $\operatorname{tr}\theta^k \neq 0$ for some k. □

Remark. One can prove that, on the contrary, if $\operatorname{tr}_{L/K} \neq 0$, the extension L is separable (**try to do it**).

Now we can prove that in separable case (in particular, in characteristic 0) the normalization problem has positive answer for Noetherian domains.

Theorem 19.3. *Let A be a normal Noetherian domain with the field of fractions K, L be a finite separable extension of K and $B = \operatorname{Int}(A, L)$. Then B is a finite A-algebra.*

Proof. For every element $\alpha \in K$ there is $a \in A$ such that $a\alpha$ is integral over A. Hence there is a basis $v_1, v_2, \ldots, v_n$ of L over K consisting of elements integral over A. Consider the symmetric bilinear function $\operatorname{tr}(uv)$ on the K-vector space L. If $\operatorname{tr}\lambda \neq 0$, then $\operatorname{tr}(u \cdot (u^{-1}\lambda) \neq 0$, hence this form is non-degenerate. Therefore, there is a *dual basis* $v_1^*, v_2^*, \ldots, v_n^*$ such that $\operatorname{tr}(v_i v_j^*) = \delta_{ij}$. Let $b \in B$, $b = \sum_{i=1}^{n} c_i v_i^*$ for some $c_i \in K$. Then $\operatorname{tr}(bv_i) = c_i \in A$, hence $B \subseteq (v_1^*, v_2^*, \ldots, v_n^*)_A$. As A is Noetherian, B is a finite A-module. □

In particular, this result implies Thm. 19.1 if $\operatorname{char}\Bbbk = 0$. In positive characteristic the field $\Bbbk(x_1, x_2, \ldots, x_n)$ has non-separable extensions. So we need more information on such extensions. First of all, recall that any finite extension $L \supseteq K$ embeds into a finite *normal* extension $\tilde{L}$, i.e. such that every polynomial $f(x) \in K[x]$ which has a root in $\tilde{L}$ splits in $\tilde{L}[x]$ into linear factors.[10] Therefore, in normalization problem for Noetherian rings we can always suppose that the extension $L \supset K$ is normal.

Lemma 19.4. *Let $\operatorname{char} K = p$, $L \supset K$ be a finite normal extension, $F = \{\alpha \in L \mid \exists k > 0\ \alpha^{p^k} \in K\}$.*[11] *Then L is a separable extension of F.*

Proof. Let $f(x) \in K[x]$ be a minimal polynomial of an element $\alpha \in L$. If $f'(x) \neq 0$, α is separable over K, hence over F. If $f'(x) = 0$, $f(x) = \bar{f}(x^p)$ for some $\bar{f}(x)$. Let $q = p^k$, where k the biggest such that $f(x) = f_0(x^q)$ for some $f_0(x) \in K[x]$ and $\beta_1, \beta_2, \ldots, \beta_r$ be the roots of $f_0(x)$, where $\beta_1 = \alpha^q$. Obviously $f_0'(x) \neq 0$, so β_i are all different and separable over K. The roots

[10] It follows, for instance, from [1, Thm. 16.3.2]

[11] **Check that F is a subfield of L.**

of $f(x)$ are $\alpha = \alpha_1, \alpha_2, \dots, \alpha_r$, where $\alpha_i^q = \beta_i$. They are also all different. Denote by $\sigma_j(\alpha_i)$ the elementary symmetric functions of α_i. Then $\sigma_j(\alpha_i)^q = \sigma_j(\beta_i) \in K$, so $\sigma_j(\alpha_i) \in F$. Note that α_i are the roots of the polynomial $x^r - \sigma_1(\alpha_i)x^{r-1} + \dots + (-1)^r\sigma_r(\alpha_i)$, hence are separable over F. It accomplishes the proof. □

Corollary 19.5. *Let A be a normal Noetherian domain with the field of fractions K of characterisric p. The following conditions are equivalent:*

(1) $\operatorname{Int}(A, L)$ *is a finite A-algebra for every finite extension $L \supset K$.*
(2) $\operatorname{Int}(A, L)$ *is a finite A-algebra for every finite extension $L \supset K$ such that $L^q \subseteq K$ for some $q = p^k$.*

Proof of Theorem 19.1 in the case of characteristic p. By Noether normalization, we can suppose that $A = \Bbbk[x_1, x_2, \dots, x_n]$ and $K = \Bbbk(x_1, x_2, \dots, x_n)$. Let $L = K(\alpha_1, \alpha_2, \dots, \alpha_m)$. By Cor. 19.5 we can suppose that $L = K(\alpha)$, where $\alpha^q = f(x_1, x_2, \dots, x_n) \in K$ for some $q = p^k$. We suppose that q is minimal, so $x^q - f$ is irreducible over K. Let C be the set of coefficients of the polynomial $f(x)$ and $\Bbbk' = \Bbbk[c^{1/q} \mid c \in C]$. Let $L' = \Bbbk'\left(x_1^{1/q}, x_2^{1/q}, \dots, x_n^{1/q}\right)$. Then L embeds into L': just map α to $\tilde{f}\left(x_1^{1/q}, x_2^{1/q}, \dots, x_n^{1/q}\right)$, where $\tilde{f}$ is obtained from f by replacing each coefficient c by $c^{1/q}$. The ring $A' = \Bbbk'[x_1^{1/q}, x_2^{1/q}, \dots, x_n^{1/q}] \simeq \Bbbk'[x_1, x_2, \dots, x_n]$ is normal finite A-algebra, hence $A' = \operatorname{Int}(A, L')$. As $\operatorname{Int}(A, L) \subseteq A'$, it is also a finite A-algebra. □

19.2. **Theorem of Krull-Akizuki. Normalizations of Krull rings.**

Theorem 19.6 (Krull-Akizuki)**.** *Let A be a Noetherian domain of Krull dimension 1, K be its field of fractions, L be a finite extension of K, $n = (L : K)$ and $B \supseteq A$ be a subring of L, which is not a field. Then B is Noetherian of Krull dimension 1 and for every nonzero prime ideal $\mathfrak{p} \subset A$, there is finitely many prime ideals $\mathfrak{P} \subset B$ containing $\mathfrak{p}$. In particular,* $\operatorname{Int}(A, L)$ *is a Dedikind ring.*

First we establish the next lemma.

Lemma 19.7. *Let A be a Noetherian domain of Krull dimension 1, K be its field of fractions and M be an A-submodule of a K-vector space V of dimension n. Then $\ell_A(M/aM) \leqslant n\ell_A(A/aA)$ for every nonzero $a \in A$.*

Proof. We can suppose that $KM = V$, that is M contains a basis $v_1, v_2, \dots, v_n$ of V. Then $(v_1, v_2, \dots, v_n)_A \simeq A^n$ is a submodule of M and we have an exact sequence $0 \to A^n \to M \to N \to 0$, where N is periodic. Suppose first that M is finite. As $\dim A = 1$, N is of finite length. Applying $\otimes_A A/aA$ to this exact sequence and taking into account that $\operatorname{Tor}_1^A(M, A/aA) \simeq \operatorname{Ann}_M a$ (see Exam. D.21), we obtain the exact sequence

$$0 \to \operatorname{Ann}_M a \to \operatorname{Ann}_N a \to (A/aA)^n \to M/aM \to N/aN \to 0.$$

As M is torsion free, $\operatorname{Ann}_M a = 0$. Taking the alternative sum of length and knowing from Exam. D.21 that $\ell_A(N/aN) = \ell_A(Ann_N a)$, we see that $\ell_A(M/aM) = n\ell_A(A/aA)$.

Suppose now that $\ell_A(M/aM) > n\ell_A(A/aA)$ for some M. Then M/aM contains a finitely generated submodule $L = (\bar{u}_1, \bar{u}_2, \dots, \bar{u}_m)_A$ such that $\ell_A(L) > n\ell_A(A/aA)$. Let u_i be a preimage of $\bar{u}_i$ in M and $M' = (u_1, u_2, \dots, u_m)_A$. Then

$$\ell_A(M'/aM') \geqslant \ell_A(M'/aM) = \ell_A(L) > n\ell_A(A/aA),$$

which is impossible, since M' is finite. □

Proof of Krull-Akizuki theorem. Let $I \subset B$ be an ideal. If $b \neq 0$ is an element from I, it satisfies an equation $a_0 b^k + a_1 b^{k-1} + \dots + a_{k-1} b + a_0$, where $a_i \in A$ and $a_0 \neq 0$. Then $a_0 \in A \cap I$. By Lem. 19.7, $B/a_0 B$ is of finite length, hence finite. Therefore, I is also finite and B/I is of finite length, hence Artinian, that is of Krull dimension 0. Hence B is Noetherian and $\dim B = 1$. Moreover, as $B/\mathfrak{p}B$ is Artinian for every nonzero prime ideal $\mathfrak{p} \subset A$, there is finitely many maximal ideals in $B/\mathfrak{p}B$, that is finitely many prime ideals $\mathfrak{P} \subset B$ such that $\mathfrak{P} \supseteq \mathfrak{p}$. □

Corollary 19.8. *Let A be a discrete valuation ring with the maximal ideal $\mathfrak{m}$ and the residue field $\Bbbk$, K be its field of fractions, L be a finite extension of K, $n = (L : K)$ and $B = \operatorname{Int}(A, L)$. Then B is a principle ideal domain with finitely many maximal ideals $\mathfrak{m}_1, \mathfrak{m}_2, \dots, \mathfrak{m}_m$ and $B = \bigcap_{i=1}^m B_{\mathfrak{m}_i}$, where all $B_{\mathfrak{m}_i}$ are discrete valuation rings. Moreover, $m \leqslant n$.*

Proof. Let pA be the maximal ideal of A. We know that B is a Dedekind ring with finitely many maximal ideals $\mathfrak{m}_1, \mathfrak{m}_2, \dots, \mathfrak{m}_m$. Choose $p_i \in \mathfrak{m}_i \setminus \mathfrak{m}_i^2 \cap \left(\bigcap_{j \neq i} \mathfrak{m}_i\right)$. Then $\mathfrak{m}_i = (p_i)$, which implies that B is a principle ideal domain. As B is a Krull ring, $B = \bigcap_{i=1}^m B_{\mathfrak{m}_i}$. As $\ell_A(B/pB) \leqslant n$, also $m \leqslant n$. □

Theorem 19.9. *Let A be a Krull ring with the field of fractions K, L be a finite extension of K, $n = (L : K)$ and $B = \operatorname{Int}(A, L)$. Then B is a Krull ring and for every $\mathfrak{p} \in \mathscr{P}(A)$ there is at most n prime ideals $\mathfrak{P} \in \mathscr{P}(B)$ such that $\mathfrak{P} \cap A = \mathfrak{p}$.*

Proof. Let $\{\mathfrak{p}_i \mid i \in \mathscr{I}\}$ be the set of prime ideals of A of height 1, $A_i = A_{\mathfrak{p}_i}$. Then $A = \bigcap_{i \in \mathscr{I}} A_i$. Let $B_i = \operatorname{Int}(A_i, L)$, $\{\mathfrak{m}_{ij} \mid 1 \leqslant j \leqslant n_i\}$, where $n_i \leqslant n$, be maximal ideals of B_i. Cor. 19.8 shows that $B_i = \bigcap_{j=1}^{n_i} B_{ij}$, where $B_{ij} = (B_i)_{\mathfrak{m}_{ij}}$ are discrete valuation rings and $\mathfrak{m}_{ij} \cap A = \mathfrak{p}_i$. Note that $B = \bigcap_{i \in \mathscr{I}} B_i = \bigcap_{i,j} B_{ij}$. Indeed, an element b is integral over A if and only if the coefficients of its minimal polynomial over K belong to A, i.e. belong to all A_i, which means that b belongs to all B_i or, the same to all B_{ij}. Let $b \in B$ and $b^k + a_{k-1} b + \dots + a_1 b + a_0 = 0$, where all a_l are in A and $a_0 \neq 0$. If $b \in \mathfrak{m}_{ij}$, $a \in \mathfrak{p}_i$, which gives finitely many possibilities for i, Therefore, B is a Krull ring and $\mathfrak{P}_{ij} = \mathfrak{m}_{ij} \cap B$ are all prime ideals of B of height 1. Obviously, $\mathfrak{P}_{ij} \cap A = \mathfrak{p}_i$. □

20. Homological dimensions

Definition 20.1. (1) Let M be an A-module.
- (a) The *projective dimension* $\mathrm{pr.dim}_A M$ of M is defined as $\sup\{n \mid \exists X \ \mathrm{Ext}^n_A(M,X) \neq 0\}$.
- (b) The *injective dimension* $\mathrm{inj.dim}_A M$ of M is defined as $\sup\{n \mid \exists X \ \mathrm{Ext}^n_A(X,M) \neq 0\}$
- (c) The *flat dimension* $\mathrm{fl.dim}_A M$ of M is defined as $\sup\{n \mid \exists X \ \mathrm{Tor}^A_n(M,X) \neq 0\}$.

(2) (a) The *global dimension* $\mathrm{gl.dim}\, A$ of the ring A is defined as $\sup\{\mathrm{pr.dim}_A M \mid M \in A\text{-Mod}\} = \sup\{\mathrm{inj.dim}_A M \mid M \in A\text{-Mod}\}$.[12]
- (b) The *weak dimension* $\mathrm{w.dim}\, A$ of the ring A is defined as $\sup\{\mathrm{fl.dim}_A M \mid M \in A\text{-Mod}\}$.

There are equivalent definitions of these notions.

Proposition 20.2. *The following conditions are equivalent:*

(1) $\mathrm{pr.dim}_A M = p$.
(2) $p = \inf\{n \mid \ \forall X \ \mathrm{Ext}^{n+1}_A(M,X) = 0\}$.
(3) $p = \inf\{n \mid \exists$ projective resolution P_* of M such that $P_n = 0$ for $n > p\}$.
(4) $p = \inf\{n \mid$ as soon as all P_i in an exact sequence $0 \to K \to P_{n-1} \to \cdots \to P_1 \to P_0 \to M \to 0$, are projective, K is also projective$\}$.

We propose the reader to prove this proposition and to formulate analogous results for injective and flat dimensions.

The Baer criterion of injectivity as well as analogous criterion for flatness imply the following results (**prove them**).

Proposition 20.3.

(1) $\mathrm{inj.dim}_A M = \sup\{n \mid$ there is an ideal $I \subset A$ such that $\mathrm{Ext}^n_A(A/I, M) \neq 0\}$.
(2) $\mathrm{fl.dim}_A M = \sup\{n \mid$ there is a finitely generated ideal $I \subset A$ such that $\mathrm{Tor}^A_n(A/I, M) \neq 0\}$.
(3) $\mathrm{gl.dim}\, A = \sup\{\mathrm{pr.dim}\, A/I \mid$ where $I \subset A$ is an ideal$\}$.
(4) $\mathrm{w.dim}\, A = \sup\{\mathrm{fl.dim}\, A/I \mid$ where $I \subset A$ is a finitely generated ideal$\}$.

For Noetherian rings we can say even more. Namely, we shall prove that, first, their global dimensions coincide with weak dimensions and, second, these dimensions can be localized.

Definition 20.4. A module M is called *finitely presented* if there is an epimorphism $\pi : F \to M$, where F is a free module of finte rank and $ker\pi$ is finite.

[12] If the ring is not commutative, one has to distinguish *left global dimension* and *right global dimension*.

Proposition 20.5. *If M is finitely presented, N is finite and $N \xrightarrow{\beta} M$ is an epimorphism, then* $\operatorname{Ker}\beta$ *is finite.*

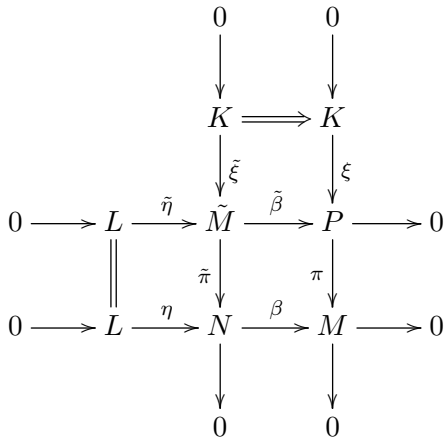
Proof. We have exact sequences

$$0 \to K \xrightarrow{\xi} F \xrightarrow{\pi} M \to 0$$

and

$$0 \to L \xrightarrow{\eta} N \xrightarrow{\beta} M \to 0.$$

Using pull-back, we construct the diagram



Here

$$\tilde{M} = \{(u,p) \mid \beta(u) = \pi(p)\} \subseteq N \oplus P,$$
$$\tilde{\pi}(u,p) = u,\ \ \tilde{\beta}(u,p) = p,$$
$$\tilde{\eta}(v) = (\eta(v), 0)\ \ \tilde{\xi}(k) = (0, \xi(k)).$$

It is commutative with exact rows and columns (**check it**). $\tilde{M}$ is finite, since K and N are finte. As P is projective, $\tilde{M} \simeq L \oplus P$. Therefore, L is finite. □

Exercise 20.6 (Schanuel lemma)**.** Using the same considerations, prove the following assertions.

(1) Let $0 \to N_i \xrightarrow{\alpha_i} P_i \xrightarrow{\beta_i} M \to 0$ $(i = 1,2)$ be exact sequences with proective modules P_i. Then $P_1 \oplus N_2 \simeq P_2 \oplus N_1$.

(2) Let $0 \to M \xrightarrow{\alpha_i} E_i \xrightarrow{\beta_i} N_i \to 0$ $(i = 1,2)$ be exact sequences with injective modules E_i. Then $E_1 \oplus N_2 \simeq E_2 \oplus N_1$.

Lemma 20.7. *Let M be a finitely presented A-module, N be an A-B-bimodule and E be an injective B-module. The map $\phi_M : \operatorname{Hom}_B(N,E) \otimes_A M \to \operatorname{Hom}_B(\operatorname{Hom}_A(M,N),E)$ sending $f \otimes u$ to the homomorphism $g \mapsto f(g(u))$ is an isomorphism.* (**Check that ϕ is well defined**.)

Proof. Fix N and E and denote the right part by $\mathrm{F}(A)$ and the left part by $\mathrm{G}(A)$. As E is injective, the functors F and G are right exact. If $M = A$, both $\mathrm{F}(A)$ and $\mathrm{G}(A)$ are just $\mathrm{Hom}_B(N, E)$ and under this identification ϕ_A is identity. Therefore, ϕ_P is isomorphism for any finite free A-module P. As M is finitely presented, there is an exact sequence $P' \to P \to M \to 0$, where P and P are finite free modules. Then we have a commutative diagram with exact rows

$$\begin{array}{ccccccc} \mathrm{F}P' & \longrightarrow & \mathrm{F}P & \longrightarrow & \mathrm{F}M & \longrightarrow & 0 \\ \downarrow{\scriptstyle \phi_{P'}} & & \downarrow{\scriptstyle \phi_P} & & \downarrow{\scriptstyle \phi_M} & & \\ \mathrm{G}P' & \longrightarrow & \mathrm{G}P & \longrightarrow & \mathrm{G}M & & 0 \end{array}$$

As $\phi_{P'}$ and ϕ_P are isomorphisms, so is ϕ_M by 5 lemma. □

Theorem 20.8. (1) *A finitely presented module M is projective if and only if it is flat.*

(2) *If M is a finite module over a Noetherian ring,* $\mathrm{pr.dim}_A M = \mathrm{fl.dim}_A M$.

(3) *If A is a Noetherian ring,* $\mathrm{gl.dim}\, A = \mathrm{w.dim}\, A$.

Proof. (1) Every projective module is flat. On the other hand, let M be a flat module. In Lem. 20.7, set $B = \mathbb{Z}$ and $E = \mathbb{U} = \mathbb{Q}/\mathbb{Z}$. Then $\mathrm{Hom}_{\mathbb{Z}}(N, \mathbb{U}) \otimes_A M$ is an exact functor of N. Thefore, $\mathrm{Hom}_{\mathbb{Z}}(\mathrm{Hom}_A(M, N), \mathbb{U})$ is also exact. Exer. C.10(1) implies that the functor $\mathrm{Hom}_A(M, N)$ is exact, that is P is projective.

(2) If $\mathrm{fl.dim}_A M = \infty$, also $\mathrm{pr.dim}_A M = \infty$ (**why?**). Suppose that $\mathrm{fl.dim}_A M = n$ and use induction by n. Over a Noetherian ring finite modules are finitely presented. $\mathrm{fl.dim}_A M = 0$ means that M is flat, hence projective, so $\mathrm{pr.dim}_A M = 0$. Suppose that the claim is valid for modules of flat dimension $n-1$ and let $\mathrm{fl.dim}_A M = n$. There is an exact sequence

$$0 \to K \to P_{n-1} \to P_{n-2} \to \cdots \to P_2 \to P_1 \to P_0 \to M,$$

where all modules P_i are projective, hence flat, and all terms are finite. Then K is also flat, hence projective, and $\mathrm{pr.dim}_A M = n$.

(3) now follows from Prop. 20.3(3,4). □

Proposition 20.9. (1) *Let M be a finitely presented A-module. For each A-module N and each multiplicative subset $S \subset A$ the map*

$$\gamma_M : \mathrm{Hom}_A(M, N)[S^{-1}] \to \mathrm{Hom}_{A[S^{-1}]}(M[S^{-1}], N[S^{-1}])$$

which send f/s to homomorphism $u/s \mapsto f(u)/s$ is an isomorphism.

(2) *Let M be a finite module over a Noetherian ring A. Then*

$$\mathrm{Ext}^n_A(M, N)[S^{-1}] \simeq \mathrm{Ext}^n_{A[S^{-1}]}(M[S^{-1}], N[S^{-1}])$$

for each A-module N, each multiplicative subset $S \subset A$ and each n. In particular, $\mathrm{pr.dim}_{A[S^{-1}]} M[S^{-1}] \leqslant \mathrm{pr.dim}_A M$.

Proof. (1) Evidently, γ_A is an isomorphism. Therefore, γ_P is an isomorphism for every finite free A-modiule P. Now just follow the proof of Lem. 20.6.

(2) Let P_* be a projective resolution of M consisting of finite modules. Then $P_*[S^{-1}]$ is a projective resolution of $M[S^{-1}]$ as of $A[S^{-1}]$-module. As taking quotients is an exact functor,

$$\operatorname{Ext}^n_A(M,N)[S^{-1}] = H^n(\operatorname{Hom}_A(P_*,N))[S^{-1}] \simeq H^n(\operatorname{Hom}_A(P_*,N)[S^{-1}]) \simeq$$
$$\simeq H^n(\operatorname{Hom}_{A[S^{-1}]}(P_*[S^{-1}],N[S^{-1}])) = \operatorname{Ext}^n_{A[S^{-1}]}(M[S^{-1}],N[S^{-1}]).$$

□

Theorem 20.10. *Let A be a local Noetherian ring with the maximal ideal $\mathfrak{m}$ and the residue field $\Bbbk = A/\mathfrak{m}$, M be a finite A-module.*

(1) *The following conditions are equivalent:*
   (a) *M is flat.*
   (b) *M is projective.*
   (c) *M is free.*
   (d) $\operatorname{Tor}^A_1(\Bbbk, M) = 0$.

(2) $\operatorname{pr.dim}_A M = \operatorname{fl.dim}_A M = \inf\{n \mid \operatorname{Tor}^A_{n+1}(\Bbbk, M) = 0\}$.

(3) $\operatorname{gl.dim} A = \operatorname{fl.dim}_A \Bbbk = \inf\{n \mid \operatorname{Tor}^A_{n+1}(\Bbbk, \Bbbk) = 0\}$.

Proof. (1) Obviously, we only have to prove that (d)⇒(c). Let $M/\mathfrak{m}M \simeq \Bbbk^m$, $\bar v_1, \bar v_2, \dots, \bar v_m$ be a basis of $M/\mathfrak{m}$, v_i be preimages of $\bar v_i$ in M, $F = A^m$ with the basis $e_1, e_2, \dots, e_m$ and $\pi : F \to M$ maps $e_i \mapsto v_i$. We have the exact sequence $0 \to K \to F \xrightarrow{\pi} M \to 0$, where $K = \operatorname{Ker}\pi$. Tensoring with $\Bbbk$, we obtain the exact sequence $0 \to K/\mathfrak{m}K \to F/\mathfrak{m}F \xrightarrow{\bar\pi} M/\mathfrak{m}M \to 0$. As also $F/\mathfrak{m}M \simeq \Bbbk^m$, $\bar\pi$ is an isomorphism. Therefore, $K/\mathfrak{m}K = 0$ and $K = 0$ by Nakayama lemma. Thus $M \simeq F$.

(2) Let $p = \inf\{n \mid \operatorname{Tor}^A_{n+1}(\Bbbk, M) = 0\}$. There is an exact sequence

$$0 \to K \to P_{p-1} \to P_{p-2} \to \cdots \to P_1 \to P_0 \to M \to 0,$$

where the modules P_i are finite and free. It implies that $\operatorname{Tor}^A_1(K, \Bbbk) \simeq \operatorname{Tor}^A_{p+1}(M, \Bbbk) = 0$. Therefore, K is free and $p = \operatorname{pr.dim} M$. □

This theorem easily globalizes.

Theorem 20.11. *Let A be a Noetherian ring, M be a finite A-module.*

(1) $\operatorname{pr.dim}_A M = \sup\{\operatorname{pr.dim}_{A_\mathfrak{m}} M_\mathfrak{m} \mid \mathfrak{m} \in \operatorname{max.spec} A\} =$
$= \inf\{n \mid \forall\, \mathfrak{m} \in \operatorname{max.spec} A \ \operatorname{Tor}^A_{n+1}(A/\mathfrak{m}, M) = 0\}$.

(2) $\operatorname{gl.dim} A = \sup\{\operatorname{gl.dim}_{A_\mathfrak{m}} M_\mathfrak{m} \mid \mathfrak{m} \in \operatorname{max.spec} A\} =$
$= \sup\{\operatorname{fl.dim}_A A/\mathfrak{m} \mid \mathfrak{m} \in \operatorname{max.spec} A\} =$
$= \inf\{n \mid \forall\, \mathfrak{m} \in \operatorname{max.spec} A \ \operatorname{Tor}^A_{n+1}(A/\mathfrak{m}, A/\mathfrak{m}) = 0\}$.

Proof. (1) $\operatorname{Tor}^A_k(A/\mathfrak{m}, M) \simeq \operatorname{Tor}^{A_\mathfrak{m}}_k(A/\mathfrak{m}, M_\mathfrak{m})$, since $\mathfrak{m}\operatorname{Tor}^A_k(A/\mathfrak{m}, M) = 0$. By Thm. 20.10, if $\operatorname{Tor}^{A_\mathfrak{m}}_{k+1}(A/\mathfrak{m}, M_\mathfrak{m}) = 0$, then $\operatorname{pr.dim}_{A_\mathfrak{m}} M_\mathfrak{m} \leqslant k$. Therefore, $\operatorname{Ext}^{k+1}_A(M,N)_\mathfrak{m} = \operatorname{Ext}^{k+1}_{A_\mathfrak{m}}(M_\mathfrak{m}, N_\mathfrak{m}) = 0$ for every N. If it holds for all $\mathfrak{m} \in \operatorname{max.spec} A$, then $\operatorname{Ext}^{k+1}_A(M,N) = 0$ by Claim (2) from Exam. 5.6, hence $\operatorname{pr.dim} M \leqslant k$. It proves the assertion.

(2) is an immediate consequence of (1). □

21. Koszul complex

21.1. **Regular sequences and depth.** In this section $\underline{\boldsymbol{a}}$ denotes a sequence $(a_1, a_2, \dots, a_n)$ of elements of A, $\mathfrak{a} = (a_1, a_2, \dots, a_n)_A$, $\underline{\boldsymbol{a}}_k = (a_1, a_2, \dots, a_{k-1})$. $\mathfrak{a}_k = (a_1, a_2, \dots, a_{k-1})_A$; in particular, $\mathfrak{a}_1 = 0$ and $\mathfrak{a}_{n+1} = \mathfrak{a}$.

Definition 21.1. (1) We define the *Koszul complex* $\mathrm{K}_*(\underline{\boldsymbol{a}})$ as follows:

- $\mathrm{K}_k(\underline{\boldsymbol{a}})$ is the free A-module with a basis $\{e_{i_1}e_{i_2}\dots e_{i_k} \mid 1 \leqslant i_1 < i_2 < \dots < i_k \leqslant n\}$, where e_i are some symbols. In particular, $\mathrm{K}_0(\underline{\boldsymbol{a}}) = A$ (a basis is an empty symbol) and $\mathrm{K}_k(\underline{\boldsymbol{a}}) = 0$ if $k > n$ or $k < 0$.
- The differential $d_k : \mathrm{K}_k(\underline{\boldsymbol{a}}) \to \mathrm{K}_{k-1}(\underline{\boldsymbol{a}})$ is defined by A-linearity and the rule

$$d_k(e_{i_1}e_{i_2}\dots e_{i_k}) = \sum_{j=1}^{k}(-1)^{j-1}a_{i_j}e_{i_1}e_{i_2}\dots \check{e}_{i_j}\dots e_{i_k},$$

where, as usually, $\check{}$ shows that the corresponding symbol is omitted. In particular, $d_1(e_i) = a_i$.
(**Check that $d^2 = 0$, so it is indeed a complex**.)

(2) For an A-module M we set $\mathrm{K}_*(\underline{\boldsymbol{a}}, M) = \mathrm{K}_*(\underline{\boldsymbol{a}}) \otimes_A M$.
(3) We denote $H_k(\underline{\boldsymbol{a}}, M) = H_k(\mathrm{K}_*(\underline{\boldsymbol{a}}, M))$.
In particular, $H_0(\underline{\boldsymbol{a}}, M) = M/\mathfrak{m}M$ and $H_n(\underline{\boldsymbol{a}}, M) \simeq \mathrm{Ann}_M \mathfrak{a}$ (**explain it**).

Definition 21.2. We say that a sequence $\underline{\boldsymbol{a}}$ is *M-regular* if each a_k is a non-zero-divisor on the module $M/\mathfrak{a}_k M$.

Theorem 21.3. (1) *If $\underline{\boldsymbol{a}}$ is M-regular, $H_k(\underline{\boldsymbol{a}}, M) = 0$ for $k > 0$. In particular, if $\underline{\boldsymbol{a}}$ is A-regular, $\mathrm{K}(\underline{\boldsymbol{a}})$ is a free resolution of $A/\mathfrak{a}$.*
(2) *Conversely, if all $a_i \in \operatorname{rad} A$ and M is finitely generated, the following conditions are equivalent:*
  (a) *$\underline{\boldsymbol{a}}$ is M-regular.*
  (b) *$H_k(\underline{\boldsymbol{a}}, M) = 0$ for $k > 0$.*
  (c) *$H_1(\underline{\boldsymbol{a}}, M) = 0$.*

We need an auxilary result on homologies of complexes. For a complex C_* and an element $a \in A$ we denote by C_*^a the complex such that

$$C_k^a = C_k \oplus C_{k-1} \quad \text{and} \quad d_k^a = \begin{pmatrix} d_k & a\cdot \\ 0 & -d_{k-1} \end{pmatrix}.$$

Exercise 21.4. Prove that $\mathrm{K}_*(\underline{\boldsymbol{a}}, M) \simeq \mathrm{K}_*(\underline{\boldsymbol{a}}_n, M)^{a_n}$.

Lemma 21.5. *For each k there is an exact sequence*

$$0 \to H_k(C_*)/aH_k(C_*) \to H_k(C_*^a) \to \mathrm{Ann}_{H_{k-1}(C_*)} a \to 0.$$

Proof. There is an obvious exact sequence of complexes

$$0 \to C_* \to C_*^a \to C_*[-1] \to 0,$$

where $C[-1]_k = C_{k-1}$ with the differential $-d$. It gives the LES

$$\dots \xrightarrow{\delta} H_k(C_*) \to H_k(C_*^a) \to H_k(C_*[-1]) \xrightarrow{\delta} H_{k-1}(C_*) \to H_{k-1}(C_*^a) \to \dots$$

and one can see that $\delta : H_k(C_*[-1]) = H_{k-1}(C_*) \to H_{k-1}(C_*)$ is just multiplication by a (**check it**). It proves the claim. □

Proof of Thm 21.3. We use induction by the length n of the sequence $\underline{\boldsymbol{a}}$. For $n = 1$ both assertions are evident.

(1) By induction, $H_k(\underline{\boldsymbol{a}}_k, M) = 0$ for $k > 0$. Lem. 21.5 with $C_* = \mathrm{K}(\underline{\boldsymbol{a}}_n, M)$, hence $C_*^a = \mathrm{K}(\underline{\boldsymbol{a}}, M)$, implies that $H_k(\underline{\boldsymbol{a}}, M) = 0$ for $0 < k \leqslant n$ (note that a is non-zero-divisor on $H_0(\underline{\boldsymbol{a}}_n, M) = M/\mathfrak{a}_n M$).

(2) We only have to prove that $(c) \Rightarrow (a)$. For $k = 1$ Lem. 21.5 gives the exact sequence

$$0 \to H_1(\underline{\boldsymbol{a}}_n, M)/aH_1(\underline{\boldsymbol{a}}_n, M) \to H_1(\underline{\boldsymbol{a}}, M) \to \operatorname{Ann}_{H_0(\underline{\boldsymbol{a}}_n, M)} a \to 0.$$

If $H_1(\underline{\boldsymbol{a}}, M) = 0$, then

- $H_1(\underline{\boldsymbol{a}}_n, M) = 0$ by Nakayama lemma;
- a is non-zero-divisor on $M/\mathfrak{a}_n M$.

By induction, the first claim implies that the sequence $\underline{\boldsymbol{a}}_n$ is M-regular. Together with the second claim it implies that $\underline{\boldsymbol{a}}$ is M-regular. □

Corollary 21.6. *Let $\underline{\boldsymbol{a}} = (a_1, a_2, \dots, a_n)$ be an M-regular sequence and σ be a permutation of $\{1, 2, \dots, n\}$. Then the sequence $\underline{\boldsymbol{a}}_\sigma = (a_{\sigma 1}, a_{\sigma 2}, \dots, a_{sin})$ is also M-regular. (**why?**).*

From now on A denotes a local Noetherian ring with the maximal ideal $\mathfrak{m}$ and the residue field $\Bbbk = A/\mathfrak{m}$.

Definition 21.7. The *depth* $\operatorname{dep} M$ of an A-module M is defined as the maximal length of M-regular sequences from $\mathfrak{m}$.

Proposition 21.8. $\operatorname{dep} M \leqslant \dim M$ *for every A-module M.*

If $\operatorname{dep} M = \dim M$, the module M is called a *Cohen-Macaulay module*. If A itself is Cohen-Macaulay as A-module, we call it a *Cohen-Macaulay ring*.

Proof. We use induction by $\dim M = d$. If $d = 0$, then $A/\operatorname{Ann}_A M$ is Artinian, hence all elements from $\mathfrak{m}$ are zero divisors on M, so $\operatorname{dep} M = 0$. If $d > 0$, let $(a_1, a_2, \dots, a_d)$ be an M-regular sequence. Then $(a_2, \dots, a_d)$ is an $M/a_1 M$-regular sequnce. As a_1 is non-zero-divisor on M, $\dim M/aM \leqslant \dim M - 1$ (see Lem. 14.3). Hence $n - 1 \leqslant d - 1$ and $n \leqslant d$. □

Proposition 21.9. $\operatorname{dep} M = 0$ *if and only if M contains a submodule isomorphic to $\Bbbk$, or, equivalently, $\mathfrak{m} \in \operatorname{Ass} M$.*

Proof. If M contains a submodule isomorphic to $\Bbbk$, all elements of $\mathfrak{m}$ annlihilate it, so are zero divisors on M. On the contrary, let $\mathfrak{m} \notin \operatorname{Ass} M = \{\mathfrak{p}_1, \mathfrak{p}_2, \dots, \mathfrak{p}_r\}$. Then $\mathfrak{m} \notin \bigcup_{i=1}^r \mathfrak{p}$ and any element $a \in \mathfrak{m} \setminus \bigcup_{i=1}^r \mathfrak{p}$ is a non-zero-divisor on M, so $\operatorname{dep} M > 0$. □

21.2. **Regular local rings.** Now we are going to prove the fundamental results about regular local Noetherian rings. Namely, we shall prove that they are just the local Noetherian rings of finite global dimension. First we prove the relation between depth and projective dimension. In this section A always denote a local Noetherian ring. We follow the book of Serre [9].

Lemma 21.10. *Suppose that* $\operatorname{gl.dim} A = n < \infty$. *For every finite* A*-module* M

$$\operatorname{dep} M + \operatorname{pr.dim} M = n.$$

Proof. If $\operatorname{dep} M = 0$ there is an embedding $\Bbbk \hookrightarrow M$ (Prop. 21.9), hence an embedding $\operatorname{Tor}_n^A(\Bbbk, \Bbbk) \hookrightarrow \operatorname{Tor}_n(\Bbbk, M)$ (since $\operatorname{Tor}_A^{n+1} = 0$). As $\operatorname{Tor}_n^A(\Bbbk, \Bbbk) \neq 0$ by Thm. 20.10, $\operatorname{Tor}_n^A(\Bbbk, M) \neq 0$ and $\operatorname{pr.dim} M = n$.

Now suppose that $\operatorname{dep} M = d > 0$ and the claim is true for modules of depth $d-1$. There is an element $a \in \mathfrak{m}$ such that a is non-zero-divisor on M and $\operatorname{dep} M/aM = d-1$. The exact sequence $0 \to M \xrightarrow{a\cdot} M \to M/aM \to 0$ gives the exact sequence

$$\operatorname{Tor}_k^A(\Bbbk, M) \xrightarrow{a\cdot} \operatorname{Tor}_k^A(\Bbbk, M) \to \operatorname{Tor}_k^A(\Bbbk, M/aM) \to \\ \to \operatorname{Tor}_{k-1}^A(\Bbbk, M) \xrightarrow{a\cdot} \operatorname{Tor}_{k-1}^A(\Bbbk, M).$$

As $a \in \mathfrak{m}$, multiplications by a in this exact sequence are zero. Therefore, $\operatorname{Tor}_k^A(\Bbbk, M/aM) = 0$ if and only if $\operatorname{Tor}_{k-1}^A(\Bbbk, M) = 0$ (since then also $\operatorname{Tor}_k^A(\Bbbk, M) = 0$) and $\operatorname{pr.dim} M/aM = \operatorname{pr.dim} M + 1$. Using induction, we can suppose that $\operatorname{dep} M/aM + \operatorname{pr.dim} M/aM = n$, whence $\operatorname{dep} M + \operatorname{pr.dim} M = n$. □

We also need the notion of *minimal free resolution.*

Definition 21.11. A free resolution (F_*, π) of a module M is called *minimal* if $\operatorname{Im} d_k \subseteq \mathfrak{m}F_{k-1}$ for all $k > 0$.

For instance, if $\underline{\boldsymbol{a}} = (a_1, a_2, \dots, a_n)$ is an A-regular sequence from $\mathfrak{m}$, $\mathrm{K}(\underline{\boldsymbol{a}})$ is a minimal free resolution of $A/(a_1, a_2, \dots, a_n)_A$.

Proposition 21.12. (1) *Every finite* A*-module has a minimal free resolution.*

(2) *If* F_* *is a minimal and* P_* *is an arbitrary free resolution of* M*, then* F_* *is isomorphic to a direct summand of* P_**. In particular, a minimal resolution is unique up to isomorphism and, if* $\operatorname{pr.dim} M = n < \infty$*, the minimal resolution is of length* n*.*

Proof. (1) The preimages $v_1, v_2, \dots, v_r$ of a basis of $M/\mathfrak{m}M$ generate M. Take $F_0 = A^r$ and $\pi : F_0 \to M$ mapping basic elements $e_i \mapsto v_i$. It is an epimorphism and it induces isomorphism $F_0/\mathfrak{m}F_0 \xrightarrow{\sim} M\mathfrak{m}M$. Therefore, $\operatorname{Ker}\pi \subseteq \mathfrak{m}F_0$. Now apply the same procedure to $\operatorname{Ker}\pi$, then to the kernel of the obtained map $F_1 \to F_0$ etc. It gives a minimal free resolution of M.

(2) Let $\alpha : P_* \to F_*$ and $\beta : F_* \to P_*$ lift the idemtity homomorphism of M. Then $\gamma = \alpha\beta$ also lifts id_M. By definition of minimal resolution, γ_k

induces an epimorphism $F_k \to F_k/\mathfrak{m}F_k$, hence γ_k is an epimorphism. As F_k is Noetherian, γ_k is an isomorphism. Therefore $\alpha(\beta\gamma^{-1}) = \mathrm{id}_P$, which means that $P_* = \operatorname{Ker}\alpha \oplus \operatorname{Im}(\beta\gamma^{-1})$ and the second summand is isomorphic to F_*. □

We will also use the next result.

Lemma 21.13. *Let M be a finite A-module and*

$$\begin{array}{ccc} P_* & \xrightarrow{\varphi} & M \\ {\scriptstyle\alpha}\downarrow & & \| \\ F_* & \xrightarrow{\pi} & M \end{array}$$

be a commutative diagram of complexes such that (F_*, π) is a minimal free resolution of M and (P_*, φ) satisfies the conditions:

1. *All P_k are free of finite rank and $P_k = 0$ for $k < 0$.*
2. *$\operatorname{Im} d_k^P \subseteq \mathfrak{m}P_{k-1}$ for all $k > 0$.*
3. *The map $P_0/\mathfrak{m}P_0 \to M/\mathfrak{m}M$ induced by φ is injective.*
4. *The maps $P_k/\mathfrak{m}P_k \to \mathfrak{m}P_{k-1}/\mathfrak{m}^2P_{k-1}$ induces by d_k^P are injective for all $k > 0$.*

Then all α_k split, i.e there are $\beta_k : F_k \to P_k$ such that $\beta_k\alpha_k = \mathrm{id}$, so P_k is a direct summand of F_k. [13]

Proof. Let $\bar{M}$ denote $M/\mathfrak{m}$ and $\bar{\xi} : \bar{M} \to \bar{N}$ be the map induced by the homomorphism $\xi : M \to N$. We shall prove that all maps $\bar{\alpha}_k$ are monomorphisms. Then there are homomorphisms $\bar{\alpha}'_k : \bar{F}_k \to \bar{P}_k$ such that $\bar{\alpha}_k\bar{\alpha}' = \mathrm{id}$. Lifting $\bar{\alpha}'$ to a homomorphism $\alpha' : F_k \to P_k$, we see that $\alpha_k\alpha' \equiv \mathrm{id} \pmod{\mathfrak{m}}$, hence is surjective, hence is an isomorphism (since P_k is Noetherian), hence α_k splits.

If $\bar{\alpha}_0(\bar{v}) = 0$, also $\bar{\varphi}(\bar{v}) = 0$, hence $\bar{v} = 0$. Suppose that we have proved the claim for $\bar{\alpha}_{k-1}$. Then there is $\beta : F_{k-1} \to P_{k-1}$ such that $\beta\alpha_{k-1} = \mathrm{id}$. If $\bar{\alpha}_k(v) = 0$, then $\alpha_{k-1}d_k(v) = d_k\alpha_k(v) \in \mathfrak{m}^2F_{k-1}$, hence $d_k(v) = \beta\alpha_{k-1}d_k(v) \in \mathfrak{m}^2P_{k-1}$. By (4), $v \in \mathfrak{m}P_k$, so $\bar{v} = 0$. It accomplishes the proof. □

Exercise 21.14. Let $\operatorname{emb.dim} A = n$ and $\mathfrak{m} = (a_1, a_2, \ldots, a_n)_A$. Prove that the Koszul complex $\mathrm{K}_*(\underline{\boldsymbol{a}})$ together with the surjection $\varphi : \mathrm{K}_0(\underline{\boldsymbol{a}}) = A \to \Bbbk$ satisfies the conditions (1)-(4) of Lem. 21.13.

Theorem 21.15 (Serre)**.** *A local Noetherian ring A is regular if and only if* $\operatorname{gl.dim} A < \infty$. *Then* $\operatorname{gl.dim} A = \dim A$.

Proof. Let $\operatorname{emb.dim} A = n$ and $\mathfrak{m} = (a_1, a_2, \ldots, a_n)_A$. Suppose that A is regular, i.e. $\dim A = n$. Then $\operatorname{gr}_{\mathfrak{m}} A \simeq \Bbbk[x_1, x_2, \ldots, x_n]$ is a domain, hence A is a domain, hence a_1 is a non-zero-divisor. Therefore, $\dim A/a_1A = d - 1$. As the images of $a_2, \ldots, a_n$ generated the maximal ideal in A/a_1A, this ring is also regular, thus a_2 is non-zero-divisor on A/a_1A. Iterating this

[13] We do not claim that the complex P_* is a direct summand of F_*.

consideration, we see that $\underline{\boldsymbol{a}} = (a_1, a_2, \dots, a_n)$ is an A-regular sequence. Then $\mathrm{K}(\underline{\boldsymbol{a}})$ is a minimal free resolution of $\Bbbk$, hence $\operatorname{gl.dim} A = \operatorname{pr.dim} \Bbbk = n$.

Let now $\operatorname{gl.dim} A = d < \infty$ and F_* be the minimal free resolution of $\Bbbk$. Then $F_k = 0$ for $k > d$. By Exer. 21.14 and Lem. 21.13, $\mathrm{K}_k(\underline{\boldsymbol{a}})$ are direct summands of F_k, hence $F_n \neq 0$. Therefore, $n \leqslant d$. On the other hand, $\operatorname{dep} A = d - \operatorname{pr.dim}_A A = d$, hence $d \leqslant n$. □

Corollary 21.16. *If A is regular, so is $A[S^{-1}]$ for every multiplicative set S. In particular, so are all localizations $A_{\mathfrak{p}}$.*

Note that it means that every prime ideal $\mathfrak{p} \subset A$ of height h contains h elements whose images in $\mathfrak{p}/\mathfrak{p}^{(2)}$ are linear independent over $A/\mathfrak{p}$.

We also note one corollary for rings which are not necessarily local.

Corollary 21.17. *Let A be a Noetherian ring.* $\operatorname{gl.dim} A < \infty$ *if and only if* $\dim A < \infty$ *and all rings $A_{\mathfrak{m}}$, where $\mathfrak{m} \in \operatorname{max.spec} A$, are regular. In this case* $\operatorname{gl.dim} A = \dim A$.

21.3. **Factoriality of regular local rings.** Now we are going to prove the following theorem of Auslander and Buchsbaum.

Theorem 21.18 (Auslander–Buchbaum)**.** *Every regular local Noetherian ring is factorial.*

Recall that it is equivalent to the claim that in such ring A every prime ideal of height 1 is principal (Cor. 8.15). We shall prove this theorem using induction, since if $\dim A = 1$, then A is a discrete valuation ring, hence factorial. We will use the following fact.

Lemma 21.19. *Let A be a Noetherian domain, $\mathscr{P}$ be a set of prime elements of A. If $A' = A[\mathscr{P}^{-1}]$ is factorial, so is A.*

Proof. Let $\mathfrak{p} \subset A$ be a prime ideal of height 1. If $\mathfrak{p} \cap \mathscr{P} \neq \varnothing$, there is a prime element $p \in \mathscr{P}$. As (p) is also prime, $\mathfrak{p} = (p)$. Suppose that $\mathfrak{p} \cap \mathscr{P} = \varnothing$. Then $\mathfrak{p}A'$ is principal, $\mathfrak{p}A' = (q)$. We can suppose that $q \in A$ and $p \nmid q$ for any $p \in \mathscr{P}$. Let $a \in \mathfrak{p}$. There is an element $s = p_1 p_2 \dots p_k$, where $p_i \in \mathscr{P}$, such that $sa = qb$ for some $b \in A$. Then $p_i \mid b$, since $p_i \nmid q$, hence $s \mid b$ and $q \mid a$. Therefore $\mathfrak{p} = (q)$. □

We also need a generalization of Schanuel lemma (Exer. 20.6).

Lemma 21.20. *Let $0 \to K \to P_n \to \dots \to P_1 \to P_0 \to M \to 0$ and $0 \to K' \to P'_n \to \dots \to P'_1 \to P'_0 \to M \to 0$ be exact sequences with projective modules P_i and P'_i. Then*

$$P_0 \oplus P'_1 \oplus P_2 \oplus P'_3 \oplus \dots \oplus K_1 \simeq P'_0 \oplus P_1 \oplus P'_2 \oplus P_3 \oplus \dots \oplus K_2, \tag{21.1}$$

where $K_1 = K'$, $K_2 = K$ if n is even and $K_1 = K$, $K_2 = K'$ if n is odd.

Proof. We use induction. For $n = 0$ it is Schanuel lemma. If $n > 0$, let $L = \operatorname{Ker}(P_0 \to M)$ and $L = \operatorname{Ker}(P'_0 \to M)$. By Schanuel lemma, $L \oplus P'_0 \simeq L' \oplus P_0$.

Consider exact sequences

$$0 \to K \to P_n \to \cdots \to P_2 \to P_1 \oplus P_0' \to L \oplus P_0' \to 0$$

and

$$0 \to K' \to P_n' \to \cdots \to P_2' \to P_1' \oplus P_0 \to L' \oplus P_0 \to 0$$

and apply the inductive supposition. We obtain just (21.1). □

A finite A-module P is called *stably free* if there are finite free modules F and F' such that $P \oplus F' \simeq F$. Certainly, then P is projective and has a finite free resolution $0 \to F' \to F \to P \to 0$. On the contrary, if a projective module P has a finite free resolution, then, applying Lem. 21.20 to this resolution and to the resolution $0 \to P \to P \to 0$, we see that P is stably free. Therefore, stably free modules are just projective modules that have a finite free resolution.

Lemma 21.21. *If an ideal I of a domain A is stably free, it is principal.*

Proof. Let $\alpha : A^{n+1} \xrightarrow{\sim} I \oplus A^n$. As $I \subseteq A$, we can consider α as a homomorphism $A \oplus A^n \to A^{n+1}$. We choose a basis $e_0, e_1, \ldots, e_n$ of $A \oplus A^n$ such that $I \subseteq Af_0$. Let $f_0, f_1, \ldots, f_n$ be a basis of A^{n+1}. Then we can identify α with the matrix (α_{ij}) such that $\alpha(f_j) = \sum_{i=0}^{n} \alpha_{ij} e_i$. Let $d = \det \alpha$ and $\tilde{\alpha} = (\tilde{\alpha}_{ij})$ be the adjoint matrix, i.e. such that $\alpha\tilde{\alpha} = d \cdot \mathrm{id}$. Consider the vector $v_0 = (\tilde{\alpha}_{10}, \tilde{\alpha}_{20}, \ldots, \tilde{\alpha}_{n0})^\top \in A^{n+1}$. Then $\alpha v_0 = de_0$. There are also vectors $v_i \in A^{n+1}$ $(1 \leqslant i \leqslant n)$ such that $\alpha v_i = e_i$. Let $v_i = \beta f_i$, where $\beta = (\beta_{ij})$. Then

$$\alpha\beta = \begin{pmatrix} d & 0 & 0 & \ldots & 0 \\ 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & \ldots & 1 \end{pmatrix},$$

whence $\det \beta = 1$, so $v_0, v_1, \ldots, v_n$ is a basis of A^{n+1} such that $\alpha v_0 = de_0$ and $\alpha v_i = f_i$ $(1 \leqslant i \leqslant n)$. Therefore, $I \simeq \langle de_0 \rangle_A$ is a principal ideal. □

Proof of Theorem 21.18. Using induction, we can suppose that $\dim A = d > 1$ and the assertion is true for rings of smaller dimensions. Let $\mathfrak{m} = (a_1, a_2, \ldots, a_d)$. Then A/a_1A is regular, hence a domain, so a_1 is prime. By Lem. 21.19, we have to prove that $A' = A[a_1^{-1}]$ is factorial. Prime ideals of A' are $\mathfrak{p}A'$, where $a_1 \notin \mathfrak{p}$, in particular, $\mathfrak{p} \neq \mathfrak{m}$. Therefore, $\dim A' < d$ and if $\mathfrak{n}$ is a maximal ideal of A', the ring $A'_{\mathfrak{n}}$ is factorial. Any ideal of A' is of the form IA', where I is an ideal of A. As $\mathrm{gl.dim}\, A < \infty$, I has a finite free resolution, hence IA' also has a finite free resolution. If $\mathfrak{p} \subset A'$ is prime of height 1, then, for every maximal ideal $\mathfrak{n} \subset A'$ the ideal $\mathfrak{p}A'_{\mathfrak{n}}$ is principal, hence projective. By Thm. 20.11, $\mathfrak{p}$ is projective. As it has a finite free resolution, it is stably free. By Lem. 21.21, it is principal, which accomplishes the proof. □

Appendix A. Functors, Hom and exactness

We denote by A-Mod the category of A-modules. Recall the definition of *functors*.

Definition A.1. A *functor* (*covariant functor*) $\mathrm{F} : A\text{-Mod} \to B\text{-Mod}$ is a map sending every A-module X to a B-module $\mathrm{F}(X)$ and every homomorphism $\alpha : X \to Y$ to a homomorphism $\mathrm{F}(\alpha) : \mathrm{F}(X) \to \mathrm{F}(Y)$ such that

$$\mathrm{F}(\mathrm{id}_X) = \mathrm{id}_{\mathrm{F}(X)},$$
$$\mathrm{F}(\alpha\beta) = \mathrm{F}(\alpha)\mathrm{F}(\beta).$$

It is called *additive* if also

$$\mathrm{F}(\alpha + \beta) = \mathrm{F}(\alpha) + \mathrm{F}(\beta).$$

We usually consider additive functors omitting "additive".

Example A.2. Recall that an *A-B-bimodule* is an abelian group M which is both an A-module and B-module such that the multiplication by elements from A and B commute:

$$a(ub) = (au)b \quad \text{for all} \quad u \in M,\ a \in A,\ b \in B.$$

(For convenience, we write multiplication by elements $b \in B$ on the right side: ub.)

Given such bimodule, we can consider the functor $\mathrm{Hom}_R(M, -) : A\text{-Mod} \to B\text{-Mod}$. It maps an A-module X to $\mathrm{Hom}_A(M, X)$ considered as B-module by the rule $bf(x) = f(xb)$ and a homomorphism $\alpha : X \to Y$ to the homomorphism $\mathrm{Hom}_A(M, \alpha) = \alpha\cdot : \mathrm{Hom}_A(M, X) \to \mathrm{Hom}_A(M, Y),\ f \mapsto \alpha f$. Obviousely, it is indeed an additive functor.

Certainly, we can consider the case when $A = B$ and $au = ua$ for all a. The $\mathrm{Hom}_R(M, -)$ is a functor from A-Mod to itself (an *endofunctor*).

We will also consider a variant of these definitions.

Definition A.3. A *contravariant functor* $\mathrm{F} : A\text{-Mod} \to B\text{-Mod}$ is a map sending every A-module X to a B-module $\mathrm{F}(X)$ and every homomorphism $\alpha : X \to Y$ to a homomorphism $\mathrm{F}(\alpha) : \mathrm{F}(Y) \to \mathrm{F}(X)$ such that

$$\mathrm{F}(\mathrm{id}_X) = \mathrm{id}_{\mathrm{F}(X)},$$
$$\mathrm{F}(\alpha\beta) = \mathrm{F}(\beta)\mathrm{F}(\alpha).$$

It is called *additive* if also

$$\mathrm{F}(\alpha + \beta) = \mathrm{F}(\alpha) + \mathrm{F}(\beta).$$

We usually consider additive contravariant functors omitting "additive".

Example A.4. Given an A-B-bimodule M, we can consider the functor $\mathrm{Hom}_B(M, -) : B\text{-Mod} \to A\text{-Mod}$. It maps a B-module X to $\mathrm{Hom}_B(X, M)$ considered as A-module by the rule $af(x) = f(ax)$ and a homomorphism $\alpha : X \to Y$ to the homomorphism $\mathrm{Hom}_B(\alpha, M) = \cdot\alpha : \mathrm{Hom}_B(Y, M) \to$

$\mathrm{Hom}_B(X, M)$, $f \mapsto f\alpha$. Obviousely, it is indeed an additive contravariat functor.

Remark. Certainly, a contravariant functor A-Mod $\to$ B-Mod is the same as a (covariant) functor from the *dual category* $(A\text{-Mod})^{\mathrm{op}}$, but we do not suppose that the reader is familiar with the theory of categories.

These functors are closely related to the exactness of exact sequences. Recall the corresponding definitions.

A sequence (finite or infinite) of homomorphisms

$$\dots \to M_{n+1} \xrightarrow{\alpha_{n+1}} M_n \xrightarrow{\alpha_n} M_{n-1} \to \dots$$

is *exact* if $\mathrm{Im}\,\alpha_{n+1} = \mathrm{Ker}\,\alpha_n$ for all n.

Exercise A.5. Prove that

(1) $0 \to N \xrightarrow{\alpha} M$ is exact if and only if α is injective.
(2) $N \xrightarrow{\alpha} M \to 0$ is exact if and only if α is surjective.
(3) $0 \to N \xrightarrow{\alpha} M \xrightarrow{\beta} L$ is exact if and only if α is injective and $\mathrm{Im}\,\alpha = \mathrm{Ker}\,\beta$ (then we also say that $\alpha = \mathrm{Ker}\,\beta$).
(4) $N \xrightarrow{\alpha} M \xrightarrow{\beta} L \to$ is exact if and only if β is surjective and $\mathrm{Im}\,\alpha = \mathrm{Ker}\,\beta$, i.e. $L \simeq \mathrm{Coker}\,\alpha = M/\mathrm{Im}\,\alpha$ (then we also say that $\beta = \mathrm{Coker}\,\alpha$).
(5) $0 \to N \xrightarrow{\alpha} M \xrightarrow{\beta} L \to 0$ is exact if and only if $\alpha = \mathrm{Ker}\,\beta$ and $\beta = \mathrm{Coker}\,\alpha$.

An exact sequence of the form $0 \to N \xrightarrow{\alpha} M \xrightarrow{\beta} L \to 0$ is called a *short exact sequence*. It is called *split* if there are homomorphisms $\alpha' : M \to N$ and $\beta' : L \to M$ such that

$$\begin{aligned} &\alpha'\alpha = \mathrm{id}_N, \\ &\beta\beta' = \mathrm{id}_L, \\ &\alpha\alpha' + \beta'\beta = \mathrm{id}_M. \end{aligned} \tag{A.1}$$

Then the maps $M \underset{\psi}{\overset{\phi}{\rightleftarrows}} N \oplus L$, $\phi(u) = (\alpha'(u), \beta(u))$, $\psi(v, w) = \alpha(v) + \beta'(w)$ are mutually inverse isomorphisms (**check it!**). Note that the equalities A.1 imply that the sequence $0 \to N \xrightarrow{\alpha} M \xrightarrow{\beta} L \to 0$ is exact (**verify it**).

Proposition A.6. *Let $0 \to N \xrightarrow{\alpha} M \xrightarrow{\beta} L \to 0$ be a short exact sequence. The following conditions are equivalent:*

(1) $0 \to N \xrightarrow{\alpha} M \xrightarrow{\beta} L \to 0$ *is split.*
(2) *There is $\alpha' : M \to N$ such that $\alpha'\alpha = \mathrm{id}_N$.*
(3) *There is $\beta' : L \to M$ such that $\beta\beta' = \mathrm{id}_L$.*

Proof. We prove that (1) $\Leftrightarrow$ (2), leaving (1) $\Leftrightarrow$ (3) to the reader.

(1) $\Rightarrow$ (2) by definition.

(2) $\Rightarrow$ (1). Let $N' = \operatorname{Im}\alpha$, $L' = \operatorname{Ker}\alpha'$. The equality $u = \alpha\alpha'(u) + (u - \alpha\alpha'(u))$ shows that $N' + L' = M$. If $u \in N' \cap L'$, then $u = \alpha(v) = \alpha\alpha'\alpha(v) = \alpha\alpha'(u) = 0$, hence $M = N' \oplus L'$. Moreover, as $\operatorname{Im}\alpha = \operatorname{Ker}\beta$, β induces an isomorphism $\bar{\beta} : L' \xrightarrow{\sim} L$. The inverse isomorphism $L \to L'$ gives $\beta' : L \to M$ such that $\beta\beta' = \mathrm{id}_L$. Finally, $\beta\alpha = 0$, $\alpha'\beta' = 0$, so if $u = \alpha(v) + \beta'(w)$, then $v = \alpha'(u)$, $w = \beta(u)$, whence $(\alpha\alpha' + \beta'\beta)(u) = u$. □

As every (additive) functor preserves products and sums, it maps split short exact sequences to split short exact sequences.

Exactness is closely connected with the functor Hom.

Theorem A.7. (1) *A sequence*

$$0 \to N' \xrightarrow{\alpha} N \xrightarrow{\beta} N' \tag{A.2}$$

is exact if and only if for every module M the sequence

$$0 \to \operatorname{Hom}_A(M, N') \xrightarrow{\alpha\cdot} \operatorname{Hom}_A(M, N) \xrightarrow{\beta\cdot} \operatorname{Hom}_A(M, N'') \tag{A.3}$$

is exact.

(2) *A sequence*

$$N' \xrightarrow{\alpha} N \xrightarrow{\beta} N'' \to 0 \tag{A.4}$$

is exact if and only if for every module M the sequence

$$0 \to \operatorname{Hom}_A(N'', M) \xrightarrow{\cdot\beta} \operatorname{Hom}_A(N, M) \xrightarrow{\cdot\alpha} \operatorname{Hom}_A(M, N') \tag{A.5}$$

is exact.

Proof. We prove (2) leaving the analogous proof of (1) as **exercise**.

Suppose that the sequence (A.4) is exact. If $(\cdot\beta)(f) = f\beta = 0$, then $f = 0$ since β is surjective. As $\beta\alpha = 0$, also $(\cdot\alpha)(\cdot\beta) = \cdot(\beta\alpha) = 0$, hence $\operatorname{Im}(\cdot\beta) \subseteq \operatorname{Ker}(\cdot\alpha)$. Let $f : N \to M$ lie in $\operatorname{Ker}(\cdot\alpha)$, that is $f\alpha = 0$. Then $\operatorname{Ker} f \supseteq \operatorname{Im}\alpha$, hence f induces a homomorphism $g : N/\operatorname{Im}\alpha \to M$ such that $g(x + \operatorname{Im}\alpha) = f(x)$. But β is actually an isomorphism $\operatorname{Coker}\alpha = N/\operatorname{Im}\alpha \xrightarrow{\sim} N''$. So we can consider g as a homomorphism $N'' \to M$ such that $g\beta(x) = f(x)$, that is $f = (\cdot\beta)(g)$. Therefore $\operatorname{Ker}(\cdot\alpha) = \operatorname{Im}(\cdot\beta)$ and the sequence (A.5) is exact.

On the contrary, let the sequence (A.5) be exact. Consider the natural surjection $f : N'' \to N''/\operatorname{Im}\beta$. Obviously, $f\beta = 0$. As $\cdot\beta$ is injective, $f = 0$, hence $N''/\operatorname{Im}\beta = 0$, which means that β is surjective. As $\beta\alpha = (\cdot\alpha)(\cdot\beta)(1_{N''}) = 0$, $\operatorname{Im}\alpha \subseteq \operatorname{Ker}\beta$. Now consider the natural surjection $f : N \to N/\operatorname{Im}\alpha$. Then $(\cdot\alpha)(f) = f\alpha = 0$, hence $f \in \operatorname{Ker}(\cdot\alpha) = \operatorname{Im}(\cdot\beta)$, that is $f = g\beta$ for some g. It implies that $\operatorname{Ker}\beta \subseteq \operatorname{Ker} f = \operatorname{Im}\alpha$, hence the sequence (A.4) is exact. □

The exactness of the sequences (A.3) and (A.5) means that both functors $\operatorname{Hom}_A(M, -)$ and $\operatorname{Hom}_A(-, M)$ are *left exact* in the sense of the following definition.

Definition A.8. (1) (a) A (covariant) functor F is called *left exact* if as well as $0 \to X \to Y \to Z$ is an exact sequence, so is the sequence $0 \to \mathrm{F}(X) \to \mathrm{F}(Y) \to \mathrm{F}(Z)$.
(b) A contravariant functor F is called *left exact* if as well as $X \to Y \to Z \to 0$ is an exact sequence, so is the sequence $0 \to \mathrm{F}(Z) \to \mathrm{F}(Y) \to \mathrm{F}(X)$.
(2) (a) A (covariant) functor F is called *right exact* if as well as $X \to Y \to Z \to 0$ is an exact sequence, so is the sequence $\mathrm{F}(X) \to \mathrm{F}(Y) \to \mathrm{F}(Z) \to 0$.
(b) A contravariant functor F is called *left exact* if as well as $0 \to X \to Y \to Z$ is an exact sequence, so is the sequence $\mathrm{F}(Z) \to \mathrm{F}(Y) \to \mathrm{F}(X) \to 0$.
(3) A functor is called *exact* if and only if it is both left and right exact.

Proof. We prove (1), remaining (2) as an exercise. (3) and (4) in fact coincide with (1) and (2).

Let $\alpha''(x) = 0$, Choose y such that $x = \xi(y)$. Then $\eta\alpha(y) = \alpha''\xi(y) = 0$, hence $\alpha(y) = \eta'(z)$. As $\zeta'\beta'(z) = \beta\eta'(z) = \beta\alpha(y) = 0$ and ζ' is injective, $\beta'(z) = 0$. Therefore, $z = \alpha'(t)$ and $\alpha\xi'(t) = \eta'\alpha'(t) = \alpha(y)$. As α is injective, $y = \xi'(t)$ and $x = \xi\xi'(t) = 0$. Thus α'' is a monomorphism (exactness at N'').

As $\beta''\eta = \zeta\beta$ is an epimorphism, so is β'' (exactness at L'').

Let $x \in N''$ and $x = \xi(y)$. Then $\alpha''(x) = \eta\alpha(y)$ and $\beta''\alpha''(x) = \beta''\eta\alpha(y) = \zeta\beta\alpha(y) = 0$, that is $\operatorname{Im}\alpha'' \subseteq \operatorname{Ker}\beta''$.

Let now $\beta''(x) = 0$ and $x = \eta(y)$. Then $\zeta\beta(y) = \beta''\eta(y) = 0$, hence $\beta(y) = \zeta'(z)$. Let $z = \beta'(t)$. Then $\beta\eta'(t) = \zeta'\beta'(t) = \beta(y)$, that is $\beta(y - \eta'(t)) = 0$. Therefore, $y - \eta'(t) = \alpha(v)$ and $x = \eta(y - \eta'(t)) = \eta\alpha(v) = \alpha''\zeta(v)$, so $\operatorname{Ker}\beta'' \subseteq \operatorname{Im}\alpha'$, which completes the proof. □

Remark A.9. (1) One can prove that the definitions of right and left exact functors do not change if we only test them on the exact seqeunces $0 \to X \to Y \to Z \to 0$.
(2) One can also prove that if a functor F is exact and a sequence

$$\dots \to M_{n+1} \xrightarrow{\alpha_{n+1}} M_n \xrightarrow{\alpha_n} M_{n-1} \to \dots$$

is exact, so is the sequence

$$\dots \to \mathrm{F}(M_{n+1}) \to \mathrm{F}(M_n) \to \mathrm{F}(M_{n-1}) \to \dots$$

We will not prove these facts here (the reader can try to do), though will use them when we need. We recommend the reader to prove them, since it is a useful exercise on the notion of exactness

Appendix B. Tensor product

Another inportant example of a funcor is *tensor product.*

Definition B.1. Let M, N are A-modules. Its *tensor product* $M \otimes_A N$ is defined as A-module with the set of generators $x \otimes y$, where $x \in M$, $y \in N$,

and the relations

$$(x+x')\otimes y = x\otimes y + x'\otimes y,$$
$$x\otimes(y+y') = x\otimes y + x\otimes y',$$
$$(ax)\otimes y = x\otimes(ay) = a(x\otimes y)$$

for all $x, x' \in M,\ y, y' \in N,\ a \in A$.

The map $\otimes : M\times N \to M\otimes_A N,\ (x,y)\mapsto x\otimes y$ is *bilinear*. Moreover, it is a *universal bilinear map*.

Proposition B.2. *If a map $\varphi : M\times N\to L$ is bilinear, there is a unique homomorphism $\tilde\varphi : M\otimes_A N\to L$ such that $\varphi = \tilde\varphi\circ\otimes$, that is $\varphi(x,y) = \tilde\varphi(x\otimes y)$.*

Proof. It is an easy **exercise**; just check that the map $\tilde\varphi : x\otimes y\mapsto\varphi(x,y)$ preserves the relations, so is well defined. □

As usually, this universality defines the tensor product up to a canonical isomorphism.

Proposition B.3. *Let $\tau : M\times N\to T$ be a bilinear map such that for any bilinear map $\varphi : M\times N\to L$ there is a unique homomorphism $\tilde\varphi : T\to L$ such that $\varphi = \tilde\varphi\circ\tau$. There is a unique isomorphism $\tilde\tau : T\xrightarrow{\sim} M\otimes_A N$ such that $\tau = \tilde\tau\circ\otimes$.*

Proof. The universality of $\otimes$ defines a homomorphism $\tilde\tau$ such that $\tau = \tilde\tau\circ\otimes$. The universality of τ defines a homomorphiosm $\theta : M\otimes_R N\to T$ such that $\otimes = \theta\circ\tau$. Then $\otimes = \theta\circ\tilde\tau\circ\otimes$ and the uniqueness implies that $\theta\circ\tilde\tau = \mathrm{id}_{M\otimes_R N}$. In the same way $\tilde\tau\circ\theta = \mathrm{id}_T$. □

Using universality, one can easily establish the following properties of tensor products.

Proposition B.4. *There are unique isomorphisms*

(1) $M\otimes_R N\xrightarrow{\sim} N\otimes_R M$ *mapping* $x\otimes y\mapsto y\otimes x$.
(2) $M\otimes_R(N\otimes_R L)\xrightarrow{\sim}(M\otimes_R N)\otimes_R L$ *mapping* $x\otimes(y\otimes z)\mapsto(x\otimes y)\otimes z$.
(3) $M\otimes_R(N\oplus L)\xrightarrow{\sim} M\otimes_R N\oplus M\otimes_R L$ *mapping* $x\otimes(y,z)\mapsto(x\otimes y, x\otimes z)$.
(4) $(M+N)\otimes_R L\xrightarrow{\sim} M\otimes_R L\oplus N\otimes_R L$ *mapping* $(x,y)\otimes z\mapsto(x\otimes z, y\otimes z)$.
(5) $A\otimes_A M\simeq M$ *($a\otimes u\mapsto au,\ u\mapsto 1\otimes u$).*

So in what follows we omit brackets, i.e. write $M\otimes_R N\otimes_R L$ instead $M\otimes_R(N\otimes_R L)$ or $(M\otimes_R N)\otimes_R L$ and do the same for longer tensor products.

Proof. (2) Define the map $\varphi : M\times N\times L\to M\otimes_A(N\otimes_A L)$ such that $\varphi(x,y,z) = x\otimes(y\otimes z)$ and check that it is a universal trilinear map. The same for the map $\psi : M\times N\times L\to(M\otimes_A N)\otimes_A L$ such that $\psi(x,y,z) = (x\otimes y)\otimes z$ (**restore the details**).

The other properties are proved analogously. □

Tensor product is a bifunctor: if $\alpha : M \to M'$ and $\beta : N \to N'$ are homomorphisms, they induce a homomorphism $\alpha \otimes \beta : M \otimes_A N \to M' \otimes_A N'$: $u \otimes v \mapsto \alpha(u) \otimes \beta(v)$ and the map $(\alpha, \beta) \mapsto \alpha \otimes \beta$ is bilinear, so induces a homomorphism

$$\mathrm{Hom}_A(M, M') \otimes_A \mathrm{Hom}_A(N, N') \to \mathrm{Hom}_A(M \otimes_A N, M' \otimes_A N').$$

An important fact concerning tensor product is the *adjunction formula*.

If M is an A-B-bimodule and N is a B-module, the tensor product $M \otimes_B N$ can be considered as an A-module setting $a(u \otimes v) = (au) \otimes v$. So we can consider the functor $M \otimes_B - : B\text{-Mod} \to A\text{-Mod}$. In particular, if B is an A-algebra and M is an A-module, we can "lift" it to a B-module $B \otimes_A M$ ("change of rings"). If L is an A-module, the module of homomorphisms $\mathrm{Hom}_A(M, L)$ can be considered as B-module if we define $(bf)(v) = f(vb)$.

Theorem B.5 (Adjunction formula)**.** *If M is an A-B-bimodule, for each B-module N and each A-module L there is an isomorphism*

$$\mathrm{Hom}_A(M \otimes_B N, L) \simeq \mathrm{Hom}_B(N, \mathrm{Hom}_A(M, L)).$$

Proof. We define homomorphisms

$$\mathrm{Hom}_A(M \otimes_B N, L) \underset{\psi}{\overset{\phi}{\rightleftarrows}} \mathrm{Hom}_B(N, \mathrm{Hom}_A(M, L)$$

as follows:

$$\phi(f)(v)(u) = f(u \otimes v),$$
$$\psi(g)(u \otimes v) = g(v)(u)$$

for all $u \in M$, $v \in N$, $f \in \mathrm{Hom}_A(M \otimes_B N, L)$ and $g \in \mathrm{Hom}_B(N, \mathrm{Hom}_A(M, L)$. Certainly, we must verify that

(1) $\phi(f)(v)$ is a homomorphism of A-modules;
(2) $\phi(f)$ is a homomorphism of B-modules;
(3) $\psi(g)$ is well defined, i.e. agrees with the defining relations for $u \otimes v$;
(4) $\psi(g)$ is a homomorphism of A-modules.

We check (1) and (4) and leave (2) and (3) as an easy exercise.

(1): $\phi(f)(v)(au) = f(u \otimes av) = f(a(u \otimes v)) = af(u \otimes v) = a\phi(f)(v)(u)$;

(4): $\psi(g)(a(u \otimes v)) = \psi(g)(au \otimes v) = g(v)(au) = ag(v)(u) = a\psi(g)(u \otimes v)$.

Obviously, ϕ and ψ are mutually inverse. □

Example B.6. Let B be an A-algebra, M be an A-module, L be a B-module. Then

$$\mathrm{Hom}_B(B \otimes_A M, L) \simeq \mathrm{Hom}_A(M, L)$$

(since the map $f \mapsto f(1)$ defines an isomorphism $\mathrm{Hom}_B(B, L) \simeq L$).

This theorem, together with the results of App. A, implies the exactness property of tensor product.

Corollary B.7. *Tensor product is right exact, that is, if the sequence* $M \xrightarrow{\alpha} N \xrightarrow{\beta} L \to 0$ *is exact, so is the sequence*

$$M \otimes_A X \xrightarrow{\alpha\otimes 1} N \otimes_A X \xrightarrow{\beta\otimes 1} L \otimes_A X \to 0 \tag{B.1}$$

for each A*-module* X*.*

Proof. Let Y be an arbitrary A-module. Apply $\mathrm{Hom}_A(-, Y)$ to the sequence B.1. We obtain

$$0 \to \mathrm{Hom}_A(L \otimes_A X, Y) \xrightarrow{\cdot(\beta\otimes 1)} \mathrm{Hom}_A(N \otimes_A X, Y) \xrightarrow{\cdot(\alpha\otimes 1)} \longrightarrow \mathrm{Hom}_A(M \otimes_A X, Y), \tag{B.2}$$

or, using the adjunction formula,

$$0 \to \mathrm{Hom}_A(L, \mathrm{Hom}_A(X, Y)) \xrightarrow{\cdot\beta} \mathrm{Hom}_A(N, \mathrm{Hom}_A(X, Y)) \xrightarrow{\cdot\alpha} \longrightarrow \mathrm{Hom}_A(M, \mathrm{Hom}_A(X, Y)),$$

which is exact by Thm. A.7(2). Therefore, the sequence (B.2) is also exact. By the same theorem, the sequence (B.1) is exact. □

Corollary B.8. *If* I *is an ideal in* A*, then* $M \otimes_A (A/I) \simeq M/IM$*.*

Proof. Just apply $M \otimes_A -$ to the exact sequence $0 \to I \to A \to A/I \to 0$. □

A module F is called *flat* is the functor $F \otimes_A -$ is exact, i.e. for every exact sequence $0 \to M \xrightarrow{\alpha} N \xrightarrow{\beta} L \to 0$ the sequence

$$0 \to M \otimes_A F \xrightarrow{\alpha\otimes 1} N \otimes_A F \xrightarrow{\beta\otimes 1} L \otimes_A F \to 0$$

is also exact. As we already know that $F\otimes -$ is right exact, it actually means that this functor maps monomorphisms to monomorphisms. For instance, any free A-module is flat, since $A^{(\mathfrak{I})} \otimes_A M \simeq M^{(\mathfrak{I})}$.

An A-algebra A' is called *flat* if it is flat as an A-module. For instance, the A-algebra $A[S^{-1}]$ from Sec. 5 is flat, as well as the algebra $\hat{A}_{\mathfrak{a}}$ if A is Noetherian (Cor. 15.8(3)).

The next properties easily follow from the assiciativity of tensor product.

Proposition B.9. (1) *Let* M *be a flat* A*-module,* N *be an* A*-*B*-bimodule flat as* B*-module. Then* $M \otimes_A N$ *is flat as* B*-module.*

(2) *If* B *is a flat* A*-algebra,* M *is a flat* B*-module, it is also flat as* A*-module.*

Remark B.10. In order that F be flat it is enough that for every finite submodule $N \subseteq M$ the map $N \otimes_A F \to M \otimes_A F$ be injective. Indeed, if $N \subseteq M$ is any submodule, u is an element of $N \otimes_A F$, then $u = \sum_{i=1}^{n} v_i \otimes w_i$, where $u_i \in N$, $w_i \in F$. Therefore, it is an element of $N' \otimes_A M$, where $N' = (v_1, v_2, \dots, v_n)$ is a finitely generated submodule.

We establish a criterion of flatness.

Theorem B.11. *An A-module M is flat if and only if for every ideal $I \subseteq A$ the natural map $I \otimes_A M \to M$, $a \otimes m \mapsto am$, is injective (here we identify M with $A \otimes_A M$).*

(As in Rem. B.10, it is enough to consider finitely generated ideals.)

Proof. The necessity is by definition. Prove the sufficiency. First we show that if X is a submodule of a free A-module F, the map $X \otimes_A M \to F \otimes_A M$ is injective.

Let $F = A^2$, $X_1 = \{a \in A \mid (a,0) \in X\}$ and $X_2 = \{a \in A \mid (a,b) \in X \text{ for some } b \in A\}$. Then X_1 and X_2 are ideals in A and there is a commutative diagran with exact rows and split second row

$$\begin{array}{ccccccccc} 0 & \longrightarrow & X_1 & \xrightarrow{\alpha} & X & \xrightarrow{\beta} & X_2 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \xi} & & \downarrow{\scriptstyle \eta} & & \downarrow{\scriptstyle \zeta} & & \\ 0 & \longrightarrow & A & \xrightarrow{\iota} & A^2 & \xrightarrow{\pi} & A & \longrightarrow & 0 \end{array}$$

Tensoring with M we obtain a commutative diagran with exact rows

$$\begin{array}{ccccccccc} & & X_1 \otimes_A M & \xrightarrow{\alpha\otimes 1} & X \otimes_A M & \xrightarrow{\beta\otimes 1} & X_2 \otimes_A M & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \xi\otimes 1} & & \downarrow{\scriptstyle \eta\otimes 1} & & \downarrow{\scriptstyle \zeta\otimes 1} & & \\ 0 & \longrightarrow & A \otimes_A M & \xrightarrow{\iota\otimes 1} & A^2 \otimes_A M & \xrightarrow{\pi\otimes 1} & A \otimes_A M & \longrightarrow & 0, \end{array}$$

where $\xi \otimes 1$ and $\zeta \otimes 1$ are monomorphisms. Let $x \in X \otimes_A M$ be such that $(\eta \otimes 1)(x) = 0$. Then $(\zeta \otimes 1)(\beta \otimes 1)(x) = (\pi \otimes 1)(\eta \otimes 1)(x) = 0$, hence $(\beta\otimes 1)(x) = 0$ and $x = (\alpha\otimes 1)(y)$ for some $y \in X_1 \otimes_A M$. Now $(\iota\otimes 1)(\xi\otimes 1)(y) = (\eta \otimes 1)(\alpha \otimes 1)(y) = (\eta \otimes 1)(x) = 0$, whence $y = 0$ and $x = 0$.

Now induction shows that the claim is true for submodules of A^n. But every finitely generated submodule of $A^{\mathfrak{I}}$ is actually a submodule of $A^{\mathfrak{J}}$ for a finite subset $\mathfrak{J} \subseteq \mathfrak{I}$. Therefore, the claim holds in this case too.

Let now X be arbitrary, $X' \subseteq X$ be a submodule. There is an exact sequence $0 \to Y \xrightarrow{\iota} F \xrightarrow{\pi} X \to 0$ for some free module X. Let $F' = \pi^{-1}(X')$. Then $F' \supseteq Y$ and there is a commutative diagram with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & Y & \xrightarrow{\iota'} & F' & \xrightarrow{\pi'} & X' & \longrightarrow & 0 \\ & & \| & & \downarrow{\scriptstyle \xi} & & \downarrow{\scriptstyle \eta} & & \\ 0 & \longrightarrow & Y & \xrightarrow{\iota} & F & \xrightarrow{\pi} & X & \longrightarrow & 0 \end{array}$$

Tensoring with M we obtain a commutative diagran with exact rows

$$\begin{array}{ccccccccc} Y \otimes_A M & \xrightarrow{\iota'\otimes 1} & F' \otimes_A M & \xrightarrow{\pi'\otimes 1} & X' \otimes_A M & \longrightarrow & 0 \\ \| & & \downarrow{\scriptstyle \xi\otimes 1} & & \downarrow{\scriptstyle \eta\otimes 1} & & \\ Y \otimes_A M & \xrightarrow{\iota\otimes 1} & F \otimes_A M & \xrightarrow{\pi\otimes 1} & X \otimes_A M & \longrightarrow & 0 \end{array}$$

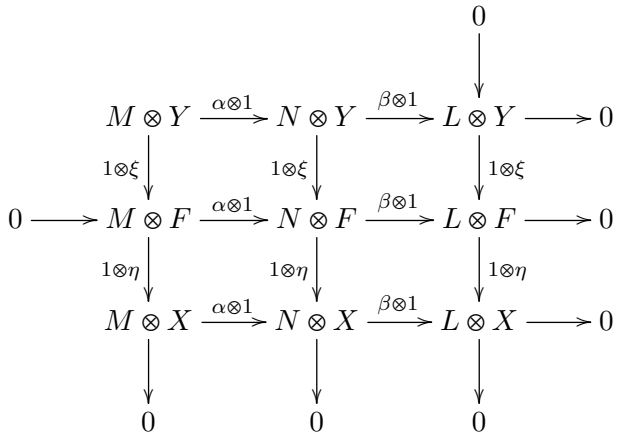
and we already know that $\xi\otimes 1$ is a monomorphism. Let $x\in X'\otimes_A M$ be such that $(\eta\otimes 1)(x)=0$, $f\in F'$ be such that $x=(\pi'\otimes 1)(f)$. Then $(\pi\otimes 1)(\xi\otimes 1)(f)=0$, hence $(\xi\otimes 1)(f)=(\iota\otimes 1)(y)$ for some $Y\in Y\otimes_A M$. Let $f'=(\iota'\otimes 1)(y)$, then $(\xi\otimes 1)(f')=(\iota\otimes 1)(y)=(\xi\otimes 1)(f)$, hence $f'=f$ and $x=(\pi'\otimes 1)(f')=0$. □

The next property of flat modules is also often used.

Proposition B.12. *L is flat if and only if for every exact sequence $0\to M\xrightarrow{\alpha}N\xrightarrow{\beta}L\to 0$ and every module X the sequence $0\to M\otimes_A X\xrightarrow{\alpha\otimes 1}N\otimes_A X\xrightarrow{\beta\otimes 1}L\otimes_A X\to 0$ is also exact.*

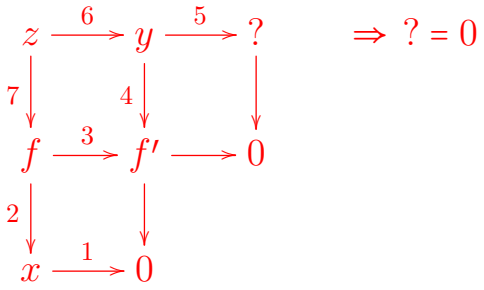
Proof. We prove "⇒" leaving "⇐" to the reader.[14] So we have to prove that $\alpha\otimes 1$ is a monomorphism.

There is an exact sequence $0\to Y\xrightarrow{\xi}F\xrightarrow{\eta}X\to 0$ with a free module F. Tensoring all terms of these two exact sequences, we obtain a commutative diagram with exact rows and columns (we write $\otimes$ instead of $\otimes_A$)



(See the picture in red below to follow the proof.)
Let $x\in M\otimes X$ be such that $(\alpha\otimes 1)(x)=0$, $f\in M\otimes F$ be such that $x=(1\otimes\eta)(f)$. Then $(1\otimes\eta)(\alpha\otimes 1)(f)=0$, hence $(\alpha\otimes 1)(f)=(1\otimes\xi)(y)$ for some $y\in N\otimes Y$. Now $(1\otimes\xi)(\beta\otimes 1)(y)=(\beta\otimes 1)(1\otimes\xi)(y)=0$, hence $(\beta\otimes 1)(y)=0$ and $y=(\alpha\otimes 1)(z)$ for some $z\in M\otimes Y$. As $(\alpha\otimes 1)(1\otimes\xi)(z)=(1\otimes\xi)(\alpha\otimes 1)(z)=(1\otimes\xi)(y)=(\alpha\otimes 1)(f)$ and $\alpha\otimes 1: M\otimes F\to N\otimes F$ is injective, $(1\otimes\xi)(z)=f$ and $x=(1\otimes\eta)(1\otimes\xi)(z)=0$. □

[14] *Hint for "⇐":* Consider such exact sequence with free N.

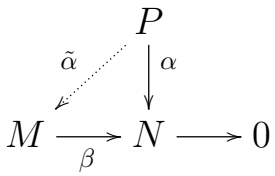


Exercise B.13. Let $0 \to M \xrightarrow{\alpha} N \xrightarrow{\beta} L \to 0$ be an exact sequence with a flat module L. Prove that M is flat if and only if N is flat.

Note that if M and N are flat, L need not to be: consider the sequence $0 \to \mathbb{Z} \xrightarrow{2} \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to 0$.

Appendix C. Projective and injective modules

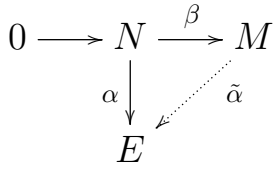
Definition C.1. (1) A module P is called *projective* if for every epimorphism $\beta : M \to N$ and any homomorphism $\alpha : P \to N$ there is a homomorphism $\tilde{\alpha} : P \to M$ such that $\alpha = \beta\tilde{\alpha}$. It it usually presented by the commutative diagram with exact row



where the dotted arrow must be constructed.

(2) A module E is called *injective* if for every monomorphism $\alpha : N \to M$ and any homomorphism $\alpha : N \to P$ there is a homomorphism $\tilde{\alpha} : M \to E$ such that $\alpha = \tilde{\alpha}\beta$. It it usually presented by the commutative

diagram with exact row

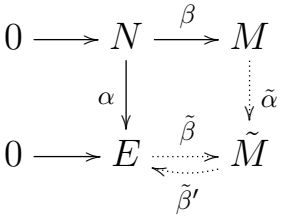


In other words, P is projective if and only if the functor $\mathrm{Hom}_A(P,-)$ is exact, and E is injective if and only if the functor $\mathrm{Hom}_A(-,E)$ is exact.

Proposition C.2. (1) *A module P is projective if and only if every epimorphism $\beta : M \to P$* splits*, i.e. there is $\beta' : P \to M$ such that $\beta\beta' = \mathrm{id}_P$ (then $M \simeq \mathrm{Ker}\,\beta \oplus P$).*

(2) *A module E is injective if and only if every monomorphism $\beta : E \to M$* splits*, i.e. there is $\beta' : M \to E$ such that $\beta'\beta = \mathrm{id}_E$ (then $M \simeq \mathrm{Ker}\,\beta' \oplus E$).*

Proof. (2) By definition, if E is injective, there is such β'. On the contrary, let every monomorphism $E \to M$ splits. For a monomorphism $\beta : N \to M$ and a homomorphism $\alpha : N \to E$, denote by $\tilde{M}$ the quotient $E \oplus M/\{(\alpha(v), -\beta(v)) \mid v \in N\}$. Let $[u,v]$ be the image in $\tilde{M}$ of the pair (u,v). For $u \in E$, $v \in M$ set $\tilde{\beta}(u) = [u,0]$ and $\tilde{\alpha}(v) = [0,v]$. Then $\tilde{\alpha}\beta = \tilde{\beta}\alpha$ and $\tilde{\beta}$ is a monomorphism. Therefore, there is $\tilde{\beta}' : \tilde{M} \to E$ such that $\tilde{\beta}'\tilde{\beta} = \mathrm{id}_E$. It implies that $\alpha = \alpha'\beta$, where $\alpha' = \tilde{\beta}'\tilde{\alpha}$. See the diagram



The analogous proof of (1) is left to the reader. □

The following assertions are evident.

Proposition C.3. (1) *A direct sum (maybe infinite) $\bigoplus_{i\in\mathscr{I}} P_i$ is projective if and only if all modules P_i are projective.*

(2) *A direct product (maybe infinite) $\prod_{i\in\mathscr{I}} P_i$ is injective if and only if all modules P_i are injective.*

The following results immediately follow from the preceding propositions.

Corollary C.4. (1) *A module P is projective if and only if it is isomorphic to a direct summand of a free module (of finite rank if P is finite).*

(2) *For every module M there is an epimorphism $P \to M$, where P is projective.*

(3) *For every module M there is an exact sequence*

$$\cdots \to P_n \to P_{n-1} \to \cdots \to P_2 \to P_1 \to P_0 \to M \to 0,$$

where all modules P_n are projective.

Unfortunately, there are not so evident injective modules analogous to free modules that are evidently projective. Thus, to prove the results dual to Cor. C.4, we have to do some job. It starts from the following criterion of injectivity, due to Baer.

Theorem C.5 (Baer criterion)**.** *An A-module E is injective if and only if for every ideal $I \subseteq A$ and every homomorphism $\alpha : I \to E$ there is an element $q \in E$ such that $\alpha(a) = aq$ for every $a \in I$.*[15]

Proof. This condition is necessary by definition of injective modules. To prove that it is sufficient, consider a module M, its submodule N and a homomorphism $\alpha : N \to E$. We have to extend it to a homomorphism $\beta : M \to E$. Consider the set $\mathfrak{E}$ of extensions of α to bigger submodules, that is

[15] Equivalently, there is $\alpha' : A \to E$ such that $\alpha = \alpha'|_I$: just set $\alpha'(a) = aq$ for all $a \in A$. In this form Baer criterion is analogous to the criterion of flatness (Thm. B.11).

the pairs (N', α') such that $N' \supseteq N$ $\alpha' : N' \to E$ is a homomorphism7 and $\alpha'|_I = \alpha$. We set $(N', \alpha') \leqslant (N'', \alpha'')$ if $N' \subseteq N''$ and $\alpha' = \alpha''|_{I'}$. One easily sees that Zorn lemma can be applied to $\mathfrak{E}$, so there is a maximal extension (N', α'). We must prove that $N' = M$. Suppose that $v \in M \setminus N'$ and set $I = \{a \in A \mid av \in N'\}$. The map α' induces a homomorphism $\beta : I \to E$ such that $\beta(a) = \alpha'(av)$. Therefore, there is an element $q \in E$ such that $\alpha'(a) = aq$ for every $a \in I$. Set $\tilde{\alpha}(u + av) = \alpha(u) + aq$ for all $a \in A$ (**check that this definition is consistent**). We obtain an extension $(N' + Av, \tilde{\alpha}) > (N', \alpha')$ in contradiction with maximality of (N', α'). It accomplishes the proof. □

Exercise C.6. (1) Let M be a finite module. Prove that for any set of modules $\{N_i \mid i \in \mathscr{I}\}$ the natural homomorphism

$$\bigoplus_{i\in\mathscr{I}} \mathrm{Hom}_A(M, N_i) \to \mathrm{Hom}_A(M, \bigoplus_{i\in\mathscr{I}} N_i)$$

is bijective.

(2) Prove that if A is Noetherian, a direct sum $\bigoplus_{i\in\mathscr{I}} E_i$ is injective if and only if each E_i is injective even if $\mathscr{I}$ is infinite. Note that for non-Noetherian rings it is not so.

Corollary C.7. *An A-module M is called* divisible *if for every element $u \in M$ and every non-zero-divisor $a \in A$ there is $v \in M$ such that $av = u$.*

(1) *Each injective module is divisible and the converse is true if A is a principle ideals domain.*
(2) *Let A be a principle ideals domain, K be its field of fractions and $U = K/A$.*
   (a) *Every quotient of an injective A-module is also injective.*

(b) *For every nonzero element v of an A-module M there is a homomorphism $\alpha_v : M \to U$ such that $\alpha_v(v) = 0$.*

(c) *Every A-module embeds into a direct product $U^{\mathscr{I}} = \prod_{i \in \mathscr{I}} U_i$, where $U_i = U$ for every $i \in \mathscr{I}$ (note that this direct product is injective).*

Proof. (1) and (2a) are immediate consequences of Baer criterion. In particular, K and U are injective.

(2b) Since U is injective, it is enough to construct a nonzero homomorphism $\alpha : Av \to U$. Let $\operatorname{Ann}_A v = aA$. If $a = 0$, we can define $\alpha_v(v) = u$ for arbitrary nonzero $u \in U$. If $a \neq 0$, define $\alpha_v(v)$ as the coset $1/a + A \in U$.

(2c) Define $\alpha : M \to U^M$ mapping an element $v \in M$ to the element $(\alpha_v(v)) \in U^M$. □

Lemma C.8. *Let F be an A-B-bimodule flat as A-module and E be an injective B-module. Then $\operatorname{Hom}_B(F, E)$ is an injective A-module.*

Proof. It folows immediately from the Adjunction formula B.5. □

Now we can prove a sort of dual for Cor. C.4. We denote by $\mathbb{U}$ the quotient $\mathbb{Q}/\mathbb{Z}$ which is an injective $\mathbb{Z}$-module and, for any ring A, set $DA = \operatorname{Hom}_{\mathbb{Z}}(A, \mathbb{U})$ (it is an injective A-module).

Corollary C.9. (1) *Every A-module embeds into $DA^{\mathscr{I}}$ for some set $\mathscr{I}$. Thus every A-module embeds into an injective A-module.*

(2) *An A-module is injective if and only if it is a direct summand of $DA^{\mathscr{I}}$ for some $\mathscr{I}$.*

(3) *For every A-module M there is an exact sequence*

$$0 \to M \to E_0 \to E_1 \to E_2 \to \cdots \to E_n \to E_{n+1} \to \dots,$$

where all modules E_n are injective.

Proof. (1) Note that $M \simeq \mathrm{Hom}_A(A, M) \subseteq \mathrm{Hom}_{\mathbb{Z}}(A, M)$ and an embedding $M \to U^{\mathscr{I}}$ induces an embedding $\mathrm{Hom}_{\mathbb{Z}}(A, M) \to \mathrm{Hom}_{\mathbb{Z}}(A, U^{\mathscr{I}}) \simeq DA^{\mathscr{I}}$.

(2) and (3) follow from (1). □

Exercise C.10. For every A-module M denote

$$DM = \mathrm{Hom}_A(M, DA) \simeq \mathrm{Hom}_{\mathbb{Z}}(M, \mathbb{U}).$$

Prove that:

(1) A sequence $N \xrightarrow{\alpha} M \xrightarrow{\beta} L$ is exact if and only if so is the induced sequence $DL \xrightarrow{\cdot\alpha} DM \xrightarrow{\cdot\beta} DN$.
(2) M is flat if and only if DM is injective.
(3) P is projective if and only if for every epimorphism $\beta : DA^{\mathscr{I}} \to N$ and every homomorphism $\alpha : P \to N$ there is $\alpha' : P \to DA^{\mathscr{I}}$ such that $\alpha = \beta\alpha'$.

Theorem C.11. *An injective A-module E is indecomposable if and only if its endomorphism ring $R = End_A E$ is local (that is non-invertible elements of R form an ideal).*

Proof. If $E = E_1 \oplus E_2$, where both summands are nonzero, and π_i is the projection onto E_i, then π_i are not invertible but $\pi_1 + \pi_2 = 1$. Thus $\mathrm{End}_A E$ is not local.

Let now E is indecomposable and $\alpha : E \to E$ be an endomorphism. If α is a monomorphism, then $\mathrm{Im}\,\alpha$ is a direct summand of E, hence $\mathrm{Im}\,\alpha = E$ and α is an isomorphism. If both α and β are not isomorphisms, i.e. $\mathrm{Ker}\,\alpha \neq 0$ and $\mathrm{Ker}\,\beta \neq 0$, then $\mathrm{Ker}(\alpha + \beta) \supseteq \mathrm{Ker}\,\alpha \cap \mathrm{Ker}\,\beta \neq 0$, hence $\alpha + \beta$ is not isomorphism. Therefore, $\mathrm{End}_A E$ is local. □

Krull–Schmidt–Azumaya theorem (Thm. E.1) implies

Corollary C.12. *Let $\bigoplus_{i=1}^{n} E_i \simeq \bigoplus_{j=1}^{m} E'_j$, where E_i and E'_j are indecomposable injective modules. Then $n = m$ and there is a permutation σ of indices such that $E_i \simeq E'_{\sigma i}$ for all i.*

C.1. **Injective envelopes.**

Definition C.13. (1) Let M be a submodule of an A-module M'. They say that M is an *essential submodule* of M' or M' is an *essential extension* of M if $M \cap N \neq 0$ for every nonzero submodule $N \subset M'$. Equivalently, for each nonzero $v \in M'$ there is $a \in A$ such that $av \neq 0$ and $av \in M$.

(2) If there is a monomorphism $\alpha : M \to E$, where E is injective and $\operatorname{Im}\alpha$ is essential in E, they call E (or the embedding $M \overset{\alpha}{\hookrightarrow} E$) the "injective envelope of M.

We shall prove that injective envelope always exists and is unique up to isomorphism. So we will denote it by $E(M)$.

Exercise C.14. (1) Prove that if N_i $(1 \leqslant i \leqslant m)$ are essential submodules of M, then $\bigcap_{i=1}^m N_i$ is essential in M.

(2) Prove that if $N_i \subseteq M_i$ $(1 \leqslant i \leqslant m)$ are essential submodules, then $\bigoplus_{i=1}^m N_i$ is an essential submodule in $\bigoplus_{i=1}^m M_i$.

(3) Deduce that $E(\bigoplus_{i=1}^m M_i) = \bigoplus_{i=1}^m E(M_i)$.

Lemma C.15. *A module M is injective if and only if it has no nontrivial injective extensions.*

Proof. Suppose that M is injective. If $M \subseteq M'$, then $M' = M \oplus N$ for some submodule N, As M is essential, $N = 0$ and $M = M'$.

Suppose now that M has no essential extensions. M embeds into an injective modul E. Consider the set $\mathfrak{N}$ of submodules $N \subset E$ such that $N \cap M = 0$. One easily sees that we can apply Zorn lemma to show that $\mathfrak{N}$ has a maximal element N. Then the composition $M \hookrightarrow E \to E/N$ is a monomorphism, so we can consider M as a submodule of E/N. If $\bar{N}'$ is a submodule of E/N such that $M \cap \bar{N}' = 0$, then $M \cap N' = 0$, where N' is the preimage of $\bar{N}'$ in

E. Therefore, E/N is an essential extension of M, hence $M = E/N$ which means that $M + N = E$, that is $E = M \oplus N$ and M is injective. □

Exercise C.16. (1) Let M be an A-module and N be an $A[S^{-1}]$-module. Prove that

$$\mathrm{Hom}_A(M, N) \simeq \mathrm{Hom}_{A[S^{-1}]}(M[S^{-1}], N).$$

(2) Let S be the set of non-zero-divisors of a ring A, $K = A[S^{-1}]$. Prove that $K = E(A)$.

Theorem C.17. (1) *For every A-module M there is an injective envelope $\alpha : M \to E$.*

(2) *If $\alpha' : M \to E'$ is another monomorphism of M into an injective module E', there is an embedding $\beta : E \hookrightarrow E'$ such that $\mathrm{Im}\,\alpha' = \mathrm{Im}(\beta\alpha)$. In particular, E is a direct summand of E'. If α' is also an injective envelope, β is an isomorphism.*

Proof. (1) Let $M \subseteq Q$, where Q is an injective module. Consider the set $\mathfrak{M}$ of submodules $N \subseteq Q$ which are essential extensions of M. Again we can apply Zorn lemma and choose a maximal element $E \in \mathfrak{M}$. Suppose that $E' \supset E$ is an proper essential extension of E. As Q is injective, the embedding $\alpha : E \hookrightarrow Q$ extends to a homomorphism $\alpha' : E' \to Q$. As $\mathrm{Ker}\,\alpha' \cap E = 0$ and E is essential in E', $\mathrm{Ker}\,\alpha' = 0$. Hence $E \subset \mathrm{Im}\,\alpha' \simeq E'$. Obviously, $\mathrm{Im}\,\alpha'$ is also an essential extension of M, which contradicts the maximality of E. Therefore, E has no essential extensions, so it is injective and is an injective envelope of M.

(2) As E' is injective, $\alpha' : M \to E'$ extends to $\beta : E \to E'$ such that $\alpha' = \beta\alpha$. As M is essential in E, $\mathrm{Ker}\,\beta = 0$, so β is a monomorphism and $\mathrm{Im}\,\beta \simeq E$ is a direct summand of E'. If $\mathrm{Im}\,\alpha' = \mathrm{Im}\,\beta\alpha$ is also essential, $\mathrm{Im}\,\beta$ is essential, so $\mathrm{Im}\,\beta = E'$. essential □

Exercise C.18. Prove the following assertions.

(1) If $N \subseteq M$, then $E(N)$ is a direct summand of $E(M)$.
(2) Let E be an injective module. The following conditions are equivalent:
   (a) E is indecomposable.
   (b) E is an injective envelope of every nonzero submodule $M \subseteq E$.
   (c) There are no nonzero submodules $N, N' \subset E$ such that $N \cap N' = 0$. (Note that if $E = E(M)$, it is enough to consider submodules of M.)

Theorem C.19. *Let $N_1, N_2, \dots, N_n$ be submodules of an A-module M such that $\bigcap_{i=1}^n = 0$ but $N_i' = \bigoplus_{j\neq i} N_j \neq 0$ for every i. The embedding $\iota : M \hookrightarrow \bigoplus_{i=1}^n M_i$, where $M_i = M/N_i$, extends to an isomorphism $E(M) \xrightarrow{\sim} E = \bigoplus_{i=1}^n E(M_i)$.*

Proof. We identify M with $\operatorname{Im}\iota$. Note that $M \cap M_i \neq 0$ for every i. Indeed, if $0 \neq x \in N_i'$, then $\iota(x) \in M_1$. Therefore, $M \cap M_i$ is essential in $E(M_i)$. Let $v = (v_1, v_2, \dots, v_n) \in E$, where $v_i \in E(M_i)$. There is $a \in A$ such that $0 \neq av_1 \in M \cap M_1$. Proceeding recursively, we find $b \in A$ such that $bv \neq 0$ and $bv_i \in M \cap M_i$ for all i, hence $bv \in M$ and M is essential in E, that is ι extends to an isomorphism $E(M) \xrightarrow{\sim} E$. □

C.2. **Injective modules over Noetherian rings.**[16]

Theorem C.20 (Matlis)**.** *Let A be a Noetherian ring. For each prime ideal $\mathfrak{p} \subset A$ denote by $E_\mathfrak{p}$ the injective envelope $E(A/\mathfrak{p})$.*

(1) *$E_\mathfrak{p}$ is indecomposable, every indecomposable injective A-module is isomorphic to $E_\mathfrak{p}$ for some prime ideal $\mathfrak{p}$ and $E_\mathfrak{p} \not\simeq E_\mathfrak{q}$ if $\mathfrak{p} \neq \mathfrak{q}$.*
(2) *$E_\mathfrak{p} \simeq A_\mathfrak{p} \otimes_A E_\mathfrak{p}$ and is an injective $A_\mathfrak{p}$-module.*
(3) $\operatorname{End}_A E_\mathfrak{p} = \operatorname{End}_{A_\mathfrak{p}} E_\mathfrak{p}$.
(4) *$E_\mathfrak{p}$ is the injective envelope (over A and over $A_\mathfrak{p}$) of the residue field $\Bbbk(\mathfrak{p}) = A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$.*

[16] See the paper of Matlis [5].

(5) *Let $N_1, N_2, \dots, N_m$ be irreducible primary submodules of an A-module M, namely, N_i is $\mathfrak{p}_i$-primary. Suppose that $\bigcap_{i=1}^m N_i = 0$ and $\bigcap_{j\neq i} N_j \neq 0$ for every i. Then $E(M) = \bigoplus_{i=1}^m E_{\mathfrak{p}_i}$.*

Proof. (1) If N, N' are submodules of $A/\mathfrak{p}$, then $N \cap N' \neq 0$, hence $E_{\mathfrak{p}}$ is indecomposable by Exer. C.18(2c). On the contrary, let E be an indecomposable module and $\mathfrak{p} \in \operatorname{Ass} E$. Then E contains a submodule M isomorphic to $A/\mathfrak{p}$, hence $E \simeq E_{\mathfrak{p}}$ by Exer. C.18(2b). Finally, $E_{\mathfrak{p}}$ contains no submodule N isomorphic to $A/\mathfrak{q}$, since otherwise $M \cap N = 0$ which is impossible. Therefore, $E_{\mathfrak{p}} \not\simeq E_{\mathfrak{q}}$.

(2) If $q \notin \mathfrak{p}$, the map $q\cdot : a \mapsto qa$ is injective in $A/\mathfrak{p}$, hence also on $E_{\mathfrak{p}}$. Therefore, it is bijective on $E_{\mathfrak{p}}$. If we write a/q for the element b such that $bq = a$, then the isomorphism $\phi : A_{\mathfrak{p}} \otimes_A E_{\mathfrak{p}} \xrightarrow{\sim} E_{\mathfrak{p}}$ is given by the rule $\phi(a/q \otimes e) = ae/q$ (**check that it is indeed an isomorphism**). As $A_{\mathfrak{p}}$ is flat over A,

$$\operatorname{Hom}_{A_{\mathfrak{p}}}(A_{\mathfrak{p}} \otimes_A M, A_{\mathfrak{p}} \otimes_A N) \simeq \operatorname{Hom}_A(M, N) \otimes_A A_{\mathfrak{p}}$$

for every finitely generated A-module M, in particular, for every ideal $M \subseteq A$. Therefore, the Baer criterion implies that $E_{\mathfrak{p}}$ is an injective $A_{\mathfrak{p}}$-module.

(3) is evident, since $q\cdot$ is bijective on $E_{\mathfrak{p}}$ for every $q \notin \mathfrak{p}$.

(4) $E_{\mathfrak{p}}$ contains $A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}} = A_{\mathfrak{p}} \otimes_A A/\mathfrak{p}$, hence is its injective envelope.

(5) By Thm. C.19, $E(M) \simeq \bigoplus_{i=1}^m E(M/N_i)$. As N_i is irreducible, $E(M/N_i)$ is indecomposable by Ex. C.18(2c). As M/N_i is $\mathfrak{p}_i$-primary, it contains a submodule isomorphic to $A/\mathfrak{p}_i$. By Ex. C.18(2b), $E(M/N_i) \simeq E(A/\mathfrak{p}_i) = E_{\mathfrak{p}_i}$. □

Together with Cor. C.12 it implies

Corollary C.21. *Let M be a finite A-module, N be its submodule and $N = \bigcap_{i=1}^n N_i = \bigcap_{j=1}^m N'_j$, where all N_i and N'_j are primary and irreducible, namely, N_i is $\mathfrak{p}_i$-primary and*

N'_j is $\mathfrak{p}'_j$-primary. Then $m = n$ and there is a permutation σ of indices such that $\mathfrak{p}'_{\sigma i} = \mathfrak{p}_i$ for all i. In particular, the number of $\mathfrak{p}$-primary submodules in these decompositions is the same for every $\mathfrak{p}$.

Remark. Matlis has also proved [5] that every injective module over a Noetherian ring is a direct sum (maybe infinite) of indecomposables (that is of modules $E_\mathfrak{p}$) and this decomposition is unique up to isomorphism and permutation of summands.

Exercise C.22. Prove that:

(1) $\operatorname{Ass} E_\mathfrak{p} = \{\mathfrak{p}\}$.
(2) $\operatorname{Hom}_A(E_\mathfrak{p}, E_\mathfrak{q}) \neq 0$ if and only if $\mathfrak{p} \subseteq \mathfrak{q}$.

C.3. **Matlis duality.** In this subsection we suppose that A is a local Noetherian ring with the maximal ideal $\mathfrak{m}$ and the residue fields $\Bbbk = A/\mathfrak{m}$. We denote by $\mathbb{E}$ the injective envelope $E(\Bbbk)$ and set $M^* = \operatorname{Hom}_A(M, \mathbb{E})$. As we have seen, $\operatorname{Ass}\mathbb{E} = \{\mathfrak{m}\}$, hence $\mathbb{E} = \bigcup_{n=1}^\infty \mathbb{E}_n$, where $\mathbb{E}_n = \{e \in \mathbb{E} \mid \mathfrak{m}^n e = 0\} \simeq (A/\mathfrak{p}^n)^*$.

Proposition C.23. *The homomorphism $\varepsilon_M : M \to M^{**}$ mapping $v \in M$ to the homomorphism $v^* : M^* \to \mathbb{E}$ such that $v^*(f) = f(v)$ is a monomorphism.*

Proof. Let $v \neq 0$. There is a maximal submodule $N \subset Av$ and $Av/N \simeq \Bbbk$. Therefore, there is a nonzero homomorphism $Av \to \mathbb{E}$. As $\mathbb{E}$ is injective, it extends to a homomorphism $f : M \to \mathbb{E}$ such that $v^*(f) = f(v) \neq 0$. □

Exercise C.24. Prove that:

(1) A sequence $N \xrightarrow{\alpha} M \xrightarrow{\beta} L$ is exact if and only if so is the induced sequence $L^* \xrightarrow{\beta^*} M^* \xrightarrow{\alpha^*} N^*$ is exact.
(2) M is flat if and only if M^* is injective.

Proposition C.25. *Let M be an A-module of finite length.*

(1) *M^* is of finite length and $\ell_A(M^*) = \ell_A(M)$.*
(2) *$\varepsilon_M : M \to M^{**}$ is an isomorphism.*
(3) *For every n the module $\mathbb{E}_n$ is of finite length and $\mathbb{E}_n^* \simeq A/\mathfrak{m}^n$.*

Proof. (1) Obviously, $\Bbbk^* \simeq \Bbbk$. If $M = M_0 \supset M_1 \supset \ldots \supset M_l = 0$ is a composition series in M, that is $M_i/M_{i+1} \simeq \Bbbk$, it gives a filtration $0 = M'_0 \subset M'_1 \subset \ldots \subset M'_l = M^*$, where $M'_i = \{f \in M^* \mid f(M_i) = 0\}$, and $M'_{i+1}/M'_i \simeq \Bbbk$. Therefore, $\ell_A(M^*) = \ell_A(M)$.

(2) As ε_M is a monomorphism and $\ell_A(M) = \ell_A(M^{**})$ by (1), ε_M is an isomorphism.

(3) is the partial case of (2) for $M = A/\mathfrak{m}^n$. □

We denote by $\hat{A}$ the $\mathfrak{m}$-adic completion of A and set $\hat{M} = \hat{A} \otimes_A M$. If M is finitely generated, it coincides with the $\mathfrak{m}$-adic completion of M. Note that $\hat{\mathbb{E}} \simeq \mathbb{E}$: an element $a \otimes e$, where $e \in \mathbb{E}_n$ is identified with $\bar{a}e$, where $\bar{a}$ is the image of a in $\hat{A}/\mathfrak{m}^n\hat{A} = A/\mathfrak{m}^n$.

Corollary C.26. (1) $\operatorname{End}_A \mathbb{E} = \mathbb{E}^* \simeq \hat{A}$.
(2) *Let M be a finite A-module.*
  (a) $\operatorname{Hom}_A(M, \mathbb{E}) \simeq \operatorname{Hom}_A(\hat{M}, \mathbb{E})$.
  (b) *Homomorphism $\varepsilon_M : M \to M^{**}$ induces an isomorphism $\hat{M} \simeq M^{**}$. In particular, if A is complete, ε_M is an isomorphism for every finite A-module M.*

Proof. (1) As $\mathbb{E} = \bigcup_{i=1}^{\infty} \mathbb{E}_n$, $\mathbb{E}^* = \operatorname{Hom}_A(\mathbb{E}, \mathbb{E})$ is identified with $\varprojlim_n \operatorname{Hom}_A(\mathbb{E}_n, \mathbb{E})$ (**expalin it**). As $\mathbb{E}^* \simeq A/\mathfrak{m}^n$, it implies that $\mathbb{E}^* \simeq \hat{A}$.

(2a) follows from the fact that $M/\mathfrak{m}^n M = \hat{M}/\mathfrak{m}^n\hat{M}$.

(2b) By (1), M^* is always an $\hat{A}$-module and ε_A induces an isomorphism $\hat{A} \xrightarrow{\sim} A^{**}$. Hence the same is true for every free A-module of finite rank. If M is a finite A-module, there is an exact sequence $F' \to F \to M \to 0$, where F and

F' are free A-modules of finite rank. Applying * twice, we obtain a commutative diagram with exact rows

$$\begin{array}{ccccccc} F' & \longrightarrow & F & \longrightarrow & M & \longrightarrow & 0 \\ \downarrow{\scriptstyle \varepsilon_{F'}} & & \downarrow{\scriptstyle \varepsilon_F} & & \downarrow{\scriptstyle \varepsilon_M} & & \\ (F')^{**} & \longrightarrow & F^{**} & \longrightarrow & M^{**} & \longrightarrow & 0 \end{array}$$

As the first two vertical homomorphisms are isomorphisms, so is the third. □

Proposition C.27. *If an A-module M is Artinian, there is a monomorphism $M \to \mathbb{E}^n$ for some n.*

Proof. As M is Artinian, there is a homomorphism $\alpha : M \to \mathbb{E}^n$ with minimal kernel. Let $\operatorname{Ker}\alpha \neq 0$. It is Artinian, hence contains a simple submodule $N \simeq A/\mathfrak{m}$. There is an embedding $\beta : N \to \mathbb{E}$, which can be extended to a homomorphism $\beta' : M \to \mathbb{E}$. Then the kernel of the homomorphism $\binom{\alpha}{\beta'} : M \to \mathbb{E}^{n+1}$ is strictly less than $\operatorname{Ker}\alpha$. This contradiction shows that $\operatorname{Ker}\alpha = 0$. □

Proposition C.28. (1) *If the module M^* is Artinian (Noetherian), M is Noetherian (Artinian).*

(2) *$\mathbb{E}$ is an Artinian module.*

Proof. (1) For every submodule $N \subseteq M$ set $N^\perp = \{f \in M^* \mid f(N) = 0\}$. If $N \subset L$, $N^\perp \supset L^\perp$, since there are nonzero homomorphisms $L/N \to \mathbb{E}$ which can be extended to homomorphisms $M \to \mathbb{E}$. Therefore, each strictly descending (ascending) chain of submodules of M gives a strictly ascending (descending) chain of submodules in M^*.

(2) As $\mathbb{E}^* \simeq \hat{A}$ is a Noetherian $\hat{A}$-module and the structures of A-module and of $\hat{A}$-module on $\mathbb{E}$ are the same, (2) follows from (1). □

Corollary C.29. *If M is an Artinian A-module, the map $\varepsilon_M : M \to M^{**}$ is an isomorphism.*

Proof. Cor. C.26 implies that $\varepsilon_{\mathbb{E}}$ is an isomorphism. On the other hand, Prop. C.27 and C.28 imply that there is an exact sequence $0 \to M \to \mathbb{E}^n \to \mathbb{E}^m$ for some m and n. Now just repeat the proof of Cor. C.26(2b). □

Altogether, these results can be summarize as follows.

Theorem C.30 (Matlis)**.** *The functor * induces an exact duality between the categories of Artinian and Noetherian $\hat{A}$-modules.*

Recall that it means that the following assertions hold:

(1) The functor * is exact.
(2) For every Artinian or Noetherian module M the natural map $M \xrightarrow{\varepsilon_M} M^{**}$ is an isomorphism.
(3) If M is Artinian (Noetherian), M^* is Noetherian (Artinian).

Appendix D. Homological algebra

We present here (mainly without proofs) elelments of homological algebra which are widely used in commutative algebra. We refer to [10] for details and much more.

D.1. **Complexes and homologies.**

Definition D.1. (1) A *complex* $C_* = \{C_n, d_n^C \mid n \in \mathbb{Z}\}$ is a sequence of modules and homomorphisms

$$\cdots \to C_{n+1} \xrightarrow{d_{n+1}^C} C_n \xrightarrow{d_n^C} C_{n-1} \to \dots \tag{D.1}$$

such that $d_n^C d_{n+1}^C = 0$ for every n (that is $\operatorname{Im} d_{n+1}^C \subseteq \operatorname{Ker} d_n^C$). If there can be no ambiguity, they write d_n instead of d_n^C.

(2) The quotients $\operatorname{Ker} d_n^C / \operatorname{Im} d_{n+1}^C$ are called the *n-th homology* of the complex C_* and denoted by $H_n(C_*)$.

(3) If $H_n(C_*) = 0$ for all n, i.e. the sequence D.1 is exact, the complex C_* is called *acyclic*.

(4) A *morphism* of complexes $\varphi_* : C_* \to D_*$ is a set of morhpisms $\{\varphi_n : C_n \to D_n\}$ such that $\varphi_{n-1} d_n^C = d_n^D \varphi_n$ for all n, i.e. all diagrams

$$\begin{array}{ccc} C_n & \xrightarrow{d_n^C} & C_{n-1} \\ {\scriptstyle \varphi_n}\downarrow & & \downarrow{\scriptstyle \varphi_{n-1}} \\ D_n & \xrightarrow{d_n^D} & D_{n-1} \end{array}$$

are commutative. Symbollicaly, they often write $\varphi d = d\varphi$.

(5) A morphism $\varphi_* : C_* \to D_*$ induces a homomorphisms of homologies $H_n(\varphi_*) : H_n(C_*) \to H_n(D_*)$.

(6) If all $H_n(\varphi_*)$ are zero, the morphism φ_* is called *homologically trivial*.

(7) If all $H_n(\varphi_*)$ are isomorphism, they say that φ_* is a *homologism* (or *quasi-isomorphism*) and write $\varphi_* : C_* \rightsquigarrow D_*$.
(Note that in this case it can happen that there are no homologisms $D_* \rightsquigarrow C_*$. It can even happen that there are no non-zero morphisms $D_* \to C_*$.)

Complexes of A-modules and their morphisms form the *category of complexes* $\operatorname{Com} A$. We consider every A-module M as complex whose 0-th component is M and all other components are 0. (**What is a morphism $M \to C_*$ and a morphism $C_* \to M$?**).

Definition D.2. (1) Let φ_* and ψ_* are morphisms of complexes $C_* \to D_*$. We say that they are *homotopic* and write $\varphi_* \sim \psi_*$ if there is a set of homomorphisms $\sigma_* = \{\sigma_n : C_n \to D_{n+1}\}$ such that $\varphi_n - \psi_n = d_{n+1}\sigma_n + \sigma_{n-1} d_n$ for all n. Symbolically $\varphi - \psi = d\sigma + \sigma d$. We say that σ_* is a *homotopy* between φ_* and ψ_*. If $\varphi_* \sim 0$, they say that φ_* is *homotopically trivial*.

(2) If $\mathrm{id}_{C_*} \sim 0$, they say that the complex C_* is *contractible* (or *homotopically trivial*) and a homotopy between id_{C_*} and 0 is called a *contraction* for C_*.
(3) A morphism $\varphi_* : C_* \to D_*$ is called a *homotopism* (or *homotopical equivalence*) if there is a morphism $\psi_* : D_* \to C_*$ such that $\psi_*\varphi_* \sim \mathrm{id}_{C_*}$ and $\varphi_*\psi_* \sim \mathrm{id}_{D_*}$. Then they say that these compexes are *homotopic* and write $C_* \sim D_*$.

One easily verifies that if $\varphi_* \sim \psi_*$, then $H_n(\varphi_*) = H_n(\psi_*)$ for every n (**check it**). In particular, a homotopically trivial morphism is homologically trivial, a contractible complex is acyclic and a homotopism is a homologism.

The following remark is very useful. We highly recommend the reader to prove them.

Remark D.3. (1) Every (additive) functor maps homotopic morphisms to homotopic, hence homotopisms to homotopisms, homotopically equivalent complexes to homotopically equivalent and contractible complexes to contractible)
(2) If a functor F is exact, then $H_n(\mathrm{F}C_*) \simeq \mathrm{F}H_n(C_*)$ for every complex C_*. In particular, such functor maps homologisms to homologisms and acyclic complexes to acyclic.

In what follows we usually omit $*$ and say "complex (C, d)" or even "complex C" as well as "morphism α" and "homotopy σ."

The following "*Snake lemma*" is, perhaps, the cornerstone of homological algebra.

Lemma D.4 (Snake lemma)**.** *Let*

$$\begin{array}{ccccccc} & & M_1 & \xrightarrow{\alpha} & M_2 & \xrightarrow{\beta} & M_3 \longrightarrow 0 \\ & & \xi\downarrow & & \eta\downarrow & & \zeta\downarrow \\ 0 & \longrightarrow & N_1 & \xrightarrow[\alpha']{} & N_2 & \xrightarrow[\beta']{} & N_3 \end{array}$$

be a commutative diagram with exact rows. There is a homomorphism $\delta : \operatorname{Ker}\zeta \to \operatorname{Coker}\xi$ *such that the sequence*

$$\operatorname{Ker}\xi \xrightarrow{\bar\alpha} \operatorname{Ker}\eta \xrightarrow{\bar\beta} \operatorname{Ker}\zeta \xrightarrow{\delta} \operatorname{Coker}\xi \xrightarrow{\bar\alpha'} \operatorname{Coker}\eta \xrightarrow{\bar\beta'} \operatorname{Coker}\zeta$$

is exact.

Sketch of proof. Construction of δ:
Let $\zeta(x) = 0$. There is $y \in M_2$ such that $x = \beta(y)$. Then $\beta'\eta(y) = 0$, hence $\eta(y) = \alpha(z)$ for a unique $z \in N_1$. Set $\delta(x) = z + \operatorname{Im}\xi \in \operatorname{Coker}\xi$. One can verify that another choice of y gives $z' \in N_1$ such that $z' - z \in \operatorname{Im}\xi$, that is $\delta(x)$ does not depend on this choice (**check it**).

It remains to verify that the resulting sequence is exact. It is a useful exercise and we leave it to the reader. □

Using Snake lemma, it is easy to prove the "*5-lemma.*"

Lemma D.5 (5-lemma)**.** *Let*

$$\begin{array}{ccccccccc} M_1 & \xrightarrow{\alpha_1} & M_2 & \xrightarrow{\alpha_2} & M_3 & \xrightarrow{\alpha_3} & M_4 & \xrightarrow{\alpha_4} & M_5 \\ \xi_1\downarrow & & \xi_2\downarrow & & \xi_3\downarrow & & \xi_4\downarrow & & \xi_5\downarrow \\ N_1 & \xrightarrow{\beta_1} & N_2 & \xrightarrow{\beta_2} & N_3 & \xrightarrow{\beta_3} & N_4 & \xrightarrow{\beta_4} & N_5 \end{array}$$

be a commutative diagram with exact rows.

(1) *If* ξ_2 *and* ξ_4 *are epimorphisms and* ξ_5 *is a monomorphism, then* ξ_3 *is an epimorphism.*
(2) *If* ξ_2 *and* ξ_4 *are monomorphisms and* ξ_1 *is an epimorphism, then* ξ_3 *is a monomorphism.*

In particular, if ξ_2 and ξ_4 are isomorphisms, ξ_1 is an epimorphism and ξ_5 is a monomorphism, then ξ_3 is an isomorphism.

Sketch of proof. (Details are left to the reader.)

(1) Apply Snake lemma to the diagram

$$\begin{array}{ccccccc} & & M_3 & \xrightarrow{\alpha_3} & M_4 & \xrightarrow{\alpha_4} & \operatorname{Im}\alpha_4 \longrightarrow 0 \\ & & \downarrow{\scriptstyle \bar\xi_3} & & \downarrow{\scriptstyle \xi_4} & & \downarrow{\scriptstyle \xi_5} \\ 0 & \longrightarrow & N_3/\operatorname{Im}\beta_2 & \xrightarrow[\bar\beta_3]{} & N_4 & \xrightarrow[\beta_4]{} & N_5 \end{array}$$

and take into account that $\operatorname{Im}\xi_3 \supseteq \operatorname{Im}\beta_2$ (**why?**).

(2) Apply Snake lemma to the diagram

$$\begin{array}{ccccccc} & & M_1 & \xrightarrow{\alpha_1} & M_2 & \xrightarrow{\alpha_2} & \operatorname{Ker}\alpha_3 \longrightarrow 0 \\ & & \downarrow{\scriptstyle \bar\xi_1} & & \downarrow{\scriptstyle \xi_2} & & \downarrow{\scriptstyle \xi_3} \\ 0 & \longrightarrow & N_1/\operatorname{Ker}\beta_1 & \xrightarrow[\bar\beta_1]{} & N_2 & \xrightarrow[\beta_2]{} & N_3 \end{array}$$

and take into account that $\operatorname{Ker}\xi_3 \subseteq \operatorname{Ker}\alpha_3$ (**why?**). □

Definition D.6. A sequnce of complexes $\dots \to C^{(n+1)} \xrightarrow{\alpha^{(n)}} C^{(n)} \xrightarrow{\alpha^{(n)}} C^{(n-1)} \to \dots$ us called *exact* if $\operatorname{Ker}\alpha_i^{(n)} = \operatorname{Im}\alpha_i^{(n+1)}$ for all n and i.

Usually we consider short exact sequences. The main result for them is the so called "*long exact sequence*" (LES) of homologies.

Theorem D.7 (LES theorem)**.** *For every short exact sequence of complexes $0 \to C' \xrightarrow{\alpha} C \xrightarrow{\beta} C'' \to 0$ there are*

homomorphisms $\delta_n : H_n(C'') \to H_{n-1}(C')$ *such that the sequence*

$$\begin{aligned} \ldots \to H_n(C') &\xrightarrow{H_n(\alpha)} H_n(C) \xrightarrow{H_n(\beta)} H_n(C'') \xrightarrow{\delta_n} \\ &\to H_{n-1}(C') \xrightarrow{H_{n-1}(\alpha)} H_{n-1}(C) \xrightarrow{H_{n-1}(\beta)} H_{n-1}(C'') \to \ldots \end{aligned}$$

is exact.

Proof. Apply Snake lemma to the diagram

$$\begin{array}{ccccccc} & & C'_n/\operatorname{Im} d'_{n+1} & \longrightarrow & C_n/\operatorname{Im} d_{n+1} & \longrightarrow & C''_n/\operatorname{Im} d''_{n+1} \longrightarrow 0 \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & \operatorname{Ker} d'_{n-1} & \longrightarrow & \operatorname{Ker} d_{n-1} & \longrightarrow & \operatorname{Ker} d''_{n-1} \end{array}$$

where the vertical maps are generated by differentials and the horizontal by α and β.
(**Verify that the rows of this diagram are exact**.)

Note that δ is constructed as follows. Take $x \in C''_n$ such that $dx = 0$ and choose $y \in C'_n$ such that $x = \beta(y)$. Then $\beta(dy) = 0$, hence $dy = \alpha(z)$ for some $z \in C'_{n-1}$ and $dz = 0$. If $\bar{x}$ is the class of x in $H_n(C'')$, then $\delta_n(\bar{x}) = \bar{z}$ (the class of z in $H_{n-1}(C')$) (**check it**). □

Corollary D.8. *Let* $0 \to C' \to C \to C'' \to 0$ *be an exact sequence of complexes. If two of them are acyclic, so is the third.*

Exercise D.9. Let

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

be a commutative diagram of complexes with exact rows. Then the induced diagrams

$$\begin{array}{ccc} H_n(C'') & \xrightarrow{\delta_n} & H_{n-1}(C') \\ \downarrow & & \downarrow \\ H_n(D'') & \xrightarrow{\delta_n} & H_{n-1}(D') \end{array}$$

are commutative for all n.

An immediate consuence of Cor. D.8 is the so called "3×3 *lemma*."

Lemma D.10. *(*3×3*-Lemma). Let*

$$\begin{array}{ccccccccc} & & 0 & & 0 & & 0 & & \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & N' & \xrightarrow{\alpha'} & M' & \xrightarrow{\beta'} & L' & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \xi'} & & \downarrow{\scriptstyle \eta'} & & \downarrow{\scriptstyle \zeta'} & & \\ 0 & \longrightarrow & N & \xrightarrow{\alpha} & M & \xrightarrow{\beta} & L & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \xi} & & \downarrow{\scriptstyle \eta} & & \downarrow{\scriptstyle \zeta} & & \\ 0 & \longrightarrow & N'' & \xrightarrow{\alpha''} & M'' & \xrightarrow{\beta''} & L'' & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ & & 0 & & 0 & & 0 & & \end{array}$$

be a commutative diagram.

(1) *If all columns and the first two rows are exact, so is the third row.*
(2) *If all columns and the last two rows are exact, so is the first row.*
(3) *If all rows and the first two columns are exact, so is the third column.*
(4) *If all rows and the last two columns are exact, so is the first column.*

D.2. **Derived functors.**

Definition D.11. Let M be an A-module.

(1) A *resolution* of M is a pair (C_*, φ), where C_* is a complex such that $C_n = 0$ if $n < 0$ and φ is a homologism $C \rightsquigarrow M$. Actually, such resolution can be written as an exact sequence

$$\cdots \to C_n \xrightarrow{d_n} C_{n-1} \to \cdots \to C_2 \xrightarrow{d_2} C_1 \xrightarrow{d_1} C_0 \xrightarrow{\varphi} M \to 0,$$

(2) A *projective resolution* of M is a resolution (P_*, φ) such that all P_n are projective.

(3) A *coresolution* of M is a pair (C_*, φ), where C_* is a complex such that $C_n = 0$ if $n > 0$ and φ is a homologism $L \rightsquigarrow M$. Actually, such resolution can be written as an exact sequence

$$0 \to M \xrightarrow{\varphi} C^0 \xrightarrow{d^0} C^1 \xrightarrow{d^1} C^2 \to \cdots \to C^n \xrightarrow{d^n} C^{n+1} \to \dots,$$

where we use the "upper notations."

(4) An *injective coresolution*[17] of M is a coresolution (E^*, φ) such that all E^n are injective.

Proposition D.12. *Every module M has a projective resolution and an injective coresolution.*

Proof. It follows from Cor. C.4(3) and C.9(3) (just cross out M from the given exact sequences). □

Certainly, projective and injective resolutions are not unique. Nevertheless, they are *unique up to homotopy* as the next lemma shows.

Theorem D.13. (1) *Let $\psi : P_* \to M$, be a homomorphism of complexes, where all P_n are projective, (C_*, φ) be a resolution of N and $\alpha : M \to N$ be an arbitrary homomorphism.*

[17] More usual is the name *injectice resolution*, but seems more consistent.

(a) *There is a morphism* $\tilde\alpha : P_* \to C_*$ *such that* $\varphi\tilde\alpha = \alpha\psi$ *and every two such morphisms are homotopic.*
(b) *All projective resolutions of* M *are homotopic.*

(2) *Let* $\psi : M \to E^*$ *be a homomorphism of complexes, where all* E^n *are injective,* (C^*, φ) *be a coresolution of* N *and* $\alpha : N \to M$ *be an arbitrary homomorphism.*
(a) *There is a morphism* $\tilde\alpha : C^* \to E^*$ *such that* $\tilde\alpha\varphi = \psi\alpha$ *and every two such morphisms are homotopic.*
(b) *All injective coresolutions of* M *are homotopic.*

We call $\tilde\alpha$ *the* extension of α to resolutions (coresolutions).

Proof. We prove (2) remaining (1) to the reader.

(2a) We have a diagram (without dotted arrows and red letters), where the first row is exact and the second row is a complex:

$$\begin{array}{ccccccccccc}
0 & \longrightarrow & N & \xrightarrow{\varphi} & C^0 & \xrightarrow{d^0} & C^1 & \xrightarrow{d^1} & C^2 & \xrightarrow{d^2} & \dots \\
 & & \downarrow{\scriptstyle\alpha} & & \vdots{\scriptstyle\alpha^0} & & \vdots{\scriptstyle\alpha^1} & & \vdots{\scriptstyle\alpha^2} & & \\
0 & \longrightarrow & M & \xrightarrow{\psi} & E^0 & \xrightarrow{d^0} & E^1 & \xrightarrow{d^1} & E_2 & \xrightarrow{d^2} & \dots
\end{array}$$

As φ is a monomorphism and E^0 is injective, there is α^0 such that $\psi\alpha = \alpha^0\varphi$. Then $d^0\alpha^0\varphi = d^0\psi\alpha = 0$, hence $d^0\alpha^0$ can be considered as a homomorphism from $C^0/\operatorname{Im}\varphi = C^0/\operatorname{Ker} d^0 \simeq \operatorname{Im} d_1$. Therefore there is α^1 such that $\alpha_1 d^0 = d^0\alpha^0$. Iterating these considerations, we obtain a morphism $\tilde\alpha = \{\alpha^n\}$.

If there is another $\tilde\alpha'$ such that $\tilde\alpha'\varphi = \psi\alpha$, then $(\tilde\alpha' - \tilde\alpha)\varphi = 0$, so we have a commutative diagram (without dotted arrows and red letters), where the first row is exact and the second row is a complex:

$$\begin{array}{ccccccccccc}
0 & \longrightarrow & N & \xrightarrow{\varphi} & C^0 & \xrightarrow{d^0} & C^1 & \xrightarrow{d^1} & C^2 & \xrightarrow{d^2} & \dots \\
 & & \downarrow{\scriptstyle 0} & & \downarrow{\scriptstyle\beta^0} & \swarrow{\scriptstyle\sigma_1} & \downarrow{\scriptstyle\beta^1} & \swarrow{\scriptstyle\sigma_2} & \downarrow{\scriptstyle\beta^2} & & \\
0 & \longrightarrow & M & \xrightarrow{\psi} & E^0 & \xrightarrow{d^0} & E^1 & \xrightarrow{d^1} & E_2 & \xrightarrow{d^2} & \dots
\end{array}$$

where $\beta^n = \alpha'^n - \alpha^n$. As $\beta^0\varphi = 0$, β^0 is actually a map from $C^0/\operatorname{Im}\varphi \simeq C^0/\operatorname{Ker} d^0 \simeq \operatorname{Im} d^1$. As E_0 is injective, there is $\sigma^1 : C^1 \to E^0$ such that $\beta^0 = \sigma^1 d^0$. Now $(\beta^1 - d^0\sigma^1)d^0 = \beta^1 d^0 - d^0\beta^0 = 0$, hence, by the same reason, there is $\sigma^2 : C^2 \to E^1$ such that $\beta^1 - d^0\sigma^1 = \sigma^2 d^1$ or $\beta^1 = d^0\sigma_1 + \sigma_2 d_1$. Iterating these condiderations, we obtain a homotopy $\{\sigma^n\}$ between $\tilde{\alpha}'$ and $\tilde{\alpha}$.

(2b) follows immediately from (2a) (**explain it**). □

Let F be a functor A-Mod $\to$ B-Mod. If $C_* = \{C_n, d_n\}$ is a complex from Com A, then $FC_* = \{\mathrm{F}C_n, \mathrm{F}d_n\}$ is a complex from Com B. Note that if $C_* \sim D_*$, then $\mathrm{F}C_* \sim \mathrm{F}D_*$ (**why?**). For every A-module M choose a projective resolution P_*^M and an injective coresolution E_M^*.

Definition D.14. (1) For every A-module M set $\mathrm{L}_n\mathrm{F}(M) = H_n(\mathrm{F}P_*^M)$ and $\mathrm{R}^n\mathrm{F}(M) = H^n(\mathrm{F}E_M^*)$.

(2) For every homomorphism $\alpha : M \to N$ choose its extensions to resolutions and coresolutions $\alpha_*^P : P_*^M \to P_*^N$ and $\alpha_E^* : E_M^* \to E_N^*$. Define $\mathrm{L}_n\mathrm{F}(\alpha) = H_n(\mathrm{F}\alpha_*^P)$ and $\mathrm{R}^n\mathrm{F}(\alpha) = H^n(\mathrm{F}\alpha_E^*)$.

Thm. D.13 implies that these definitions do not depend on the choice of resolutions and extensions of homomorphisms to resolutions. Therefore, we obtain sets of functors $\mathrm{LF} = \{\mathrm{L}_n\mathrm{F}\}$ and $\mathrm{R}^n\mathrm{F} = \{\mathrm{R}^n\mathrm{F}\}$. They are called, respectively, the *left derived* and *right derived* functors of the functor F. If F is a contravariant functor, we define its *right derived* as $H^n(\mathrm{F}P_*^M)$ and *left derived* as $H_n(\mathrm{F}E_M^*)$. Note that, as F reverse the directions of arrows, it is convenient to use upper notations for RF and lower notations for LF.

An immediate cosequence of these definitions are the following properties. We leave their proofs as easy exercises.

Proposition D.15. (1) *If a module P is projective and F is a covariant (contravariant) functor,* $\mathrm{L}_n\mathrm{F}(P) = 0$ *(respectively,* $\mathrm{R}^n\mathrm{F}(P) = 0$*) if* $n > 0$.
(2) *If a module E is injective and F is a covariant (contravariant) functor,* $\mathrm{R}^n\mathrm{F}(E) = 0$ *(respectively,* $\mathrm{L}_n\mathrm{F}(E) = 0$*) if* $n > 0$.
(3) *If the functor F is left exact (right exact), then* $\mathrm{R}^0\mathrm{F} \simeq F$ *(respectively,* $\mathrm{L}_0\mathrm{F} \simeq F$*).*
(4) *If the functor F is exact,* $\mathrm{R}^n\mathrm{F} = 0$ *and* $\mathrm{L}_n\mathrm{F} = 0$ *for all* $n > 0$.

Example D.16. (1) If we fix a module M, we can consider the functor $\mathrm{Hom}_A(M, -)$. Its right derived functors are denoted by $\mathrm{Ext}^n_A(M, -)$. By definition, $\mathrm{Ext}^n_A(M, N)$ is the n-th cohomology of the complex $\mathrm{Hom}_A(M, E^*_N)$.
(2) On the other hand, fixing a module N, we can define right derived functors of $\mathrm{Hom}_A(-, N)$ which are denoted by $\mathrm{Ext}^n_A(-, N)$. This time $\mathrm{Ext}^n_A(M, N)$ is the n-th cohomology of the complex $\mathrm{Hom}_A(P^M_*, N)$. Certainly, it causes ambiguity, but actually both definitions give the same result as we shall see later.
(3) If we fix a module M, we can also consider the functor $M \otimes_A -$. Its left derived functors are denoted by $\mathrm{Tor}^A_n(M, -)$. By definition, $\mathrm{Tor}^A_N(M, N)$ is the n-th homology of the complex $M \otimes_A P^N_*$. Again, the same result is obtained if we fix N and calculate $\mathrm{Tor}^A_N(M, N)$ as the n-th homology of $P^M_* \otimes_A N$.

The main property of derived functors is the long exact sequence arising from the following lemma.

Lemma D.17. *For every exact sequence of modules* $0 \to M_1 \xrightarrow{\alpha} M_2 \xrightarrow{\beta} M_3 \to 0$ *there are commutative diagrams of*

complexes with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M_1 & \xrightarrow{\alpha} & M_2 & \xrightarrow{\beta} & M_3 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \varphi_1} & & \downarrow{\scriptstyle \varphi_2} & & \downarrow{\scriptstyle \varphi_3} & & \\ 0 & \longrightarrow & E_1^* & \xrightarrow{\tilde{\alpha}_E} & E_2^* & \xrightarrow{\tilde{\beta}_E} & E_3^* & \longrightarrow & 0 \end{array} \tag{D.2}$$

and

$$\begin{array}{ccccccccc} 0 & \longrightarrow & P_*^1 & \xrightarrow{\tilde{\alpha}_P} & P_*^2 & \xrightarrow{\tilde{\beta}_P} & P_*^3 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \varphi^1} & & \downarrow{\scriptstyle \varphi^2} & & \downarrow{\scriptstyle \varphi^3} & & \\ 0 & \longrightarrow & M_1 & \xrightarrow{\alpha} & M_2 & \xrightarrow{\beta} & M_3 & \longrightarrow & 0 \end{array} \tag{D.3}$$

where (E_i^*, φ_i) is an injective coresolution and (P_*^i, φ^i) is a projective resolution of M_i.

Proof. We start from the commutative diagram

$$\begin{array}{ccccccccc} & & 0 & & 0 & & 0 & & \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & M_1 & \xrightarrow{\alpha} & M_2 & \xrightarrow{\beta} & M_3 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \varphi_1} & & \downarrow{\scriptstyle \varphi_2} & & \downarrow{\scriptstyle \varphi_3} & & \\ 0 & \longrightarrow & E_1^0 & \xrightarrow{\alpha^0} & E_2^0 & \xrightarrow{\beta^0} & E_3^0 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \psi_1} & & \downarrow{\scriptstyle \psi_2} & & \downarrow{\scriptstyle \psi_3} & & \\ 0 & \longrightarrow & L^1 & \xrightarrow{\alpha'} & L^2 & \xrightarrow{\beta'} & L_3 & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ & & 0 & & 0 & & 0 & & \end{array}$$

where

- φ_1 and φ_3 are some embeddings M_1 and M_3 into injective modules.
- $E_2^0 = E_1^0 \oplus E_3^0$ and $\varphi_2 = \begin{pmatrix} \varphi' \\ \varphi_3\beta \end{pmatrix}$, where $\varphi' : M_2 \to E_1^0$ is such that $\varphi'\alpha = \varphi_1$.
- α^0 and β^0 are the natural embedding and projection.

- $L_i = \operatorname{Coker}\varphi^i$, ψ_i are the natural surjections and α' and β' are induced by α^1 and β^1.

All columns and the first two rows are exact by construction. By 3×3 lemma, the third row is also exact. Now we can apply the same construction to the exact sequence $0\to L_1\xrightarrow{\alpha'} L_2\xrightarrow{\beta'} L_3\to 0$, which gives the terms E_i^1 together with differentials d_i^0 and morphisms α^1 and β^1. Iterating, we obtain diagram (D.2). Diagram (D.3) is constructed analogously (**restore the details**). □

Theorem D.18 (LES theorem)**.** *Let* $0\to M_1\xrightarrow{\alpha} M_2\xrightarrow{\beta} M_3\to 0$ *be an exact sequence of* A*-modules. For every (covariant) functor* $\mathrm{F}: A\text{-Mod}\to B\text{-Mod}$ *there are homomorphisms* $\delta^n: \mathrm{R}^n\mathrm{F}(M_3)\to \mathrm{R}^{n+1}\mathrm{F}(M_1)$ *and* $\delta_n: \mathrm{L}_n\mathrm{F}(M_3)\to \mathrm{L}_{n-1}\mathrm{F}(M_1)$ *such that the sequences*

$$\begin{aligned}
0\longrightarrow \mathrm{R}^0\mathrm{F}(M_1)&\xrightarrow{\mathrm{R}^0\mathrm{F}(\alpha)}\mathrm{R}^0\mathrm{F}(M_2)\xrightarrow{\mathrm{R}^0\mathrm{F}(\beta)}\mathrm{R}^0\mathrm{F}(M_3)\xrightarrow{\delta^0}\\
\longrightarrow \mathrm{R}^1\mathrm{F}(M_1)&\xrightarrow{\mathrm{R}^1\mathrm{F}(\alpha)}\mathrm{R}^1\mathrm{F}(M_2)\xrightarrow{\mathrm{R}^1\mathrm{F}(\beta)}\mathrm{R}^1\mathrm{F}(M_3)\xrightarrow{\delta^1}\dots\\
\dots\longrightarrow \mathrm{R}^n\mathrm{F}(M_1)&\xrightarrow{\mathrm{R}^n\mathrm{F}(\alpha)}\mathrm{R}^n\mathrm{F}(M_2)\xrightarrow{\mathrm{R}^n\mathrm{F}(\beta)}\mathrm{R}^n\mathrm{F}(M_3)\xrightarrow{\delta^n}\\
\longrightarrow \mathrm{R}^{n+1}\mathrm{F}(M_1)&\xrightarrow{\mathrm{R}^{n+1}\mathrm{F}(\alpha)}\mathrm{R}^{n+1}\mathrm{F}(M_2)\xrightarrow{\mathrm{R}^{n+1}\mathrm{F}(\beta)}\mathrm{R}^{n+1}\mathrm{F}(M_3)\xrightarrow{\delta^{n+1}}\dots
\end{aligned}$$

and

$$\begin{aligned}
\dots\longrightarrow \mathrm{L}_{n+1}\mathrm{F}(M_1)&\xrightarrow{\mathrm{L}_{n+1}\mathrm{F}(\alpha)}\mathrm{L}_{n+1}\mathrm{F}(M_2)\xrightarrow{\mathrm{L}_{n+1}\mathrm{F}(\beta)}\mathrm{L}_{n+1}\mathrm{F}(M_3)\xrightarrow{\delta_{n+1}}\\
\longrightarrow \mathrm{L}_n\mathrm{F}(M_1)&\xrightarrow{\mathrm{L}_n\mathrm{F}(\alpha)}\mathrm{L}_n\mathrm{F}(M_2)\xrightarrow{\mathrm{L}_n\mathrm{F}(\beta)}\mathrm{L}_n\mathrm{F}(M_3)\xrightarrow{\delta n}\dots\\
\dots\longrightarrow \mathrm{L}_1\mathrm{F}(M_1)&\xrightarrow{\mathrm{L}_1\mathrm{F}(\alpha)}\mathrm{L}_1\mathrm{F}(M_2)\xrightarrow{\mathrm{L}_1\mathrm{F}(\beta)}\mathrm{L}_1\mathrm{F}(M_3)\xrightarrow{\delta_1}\\
\longrightarrow \mathrm{L}_0\mathrm{F}M_1)&\xrightarrow{\mathrm{L}_0\mathrm{F}(\alpha)}\mathrm{L}_0\mathrm{F}(M_2)\xrightarrow{\mathrm{L}_0\mathrm{F}(\beta)}\mathrm{L}_0\mathrm{F}(M_3)\longrightarrow 0
\end{aligned}$$

are exact.

We propose the reader to formulate the analogous theorem for contravariant functors.

Proof. We use the diargam (D.2). As all modules E_i^n are injective, all sequences $0\to E_1^n\to E_2^n\to E_3^n\to 0$ split, hence remain exact after applying the functor F. Therefore, we obtain the exact sequence of complexes $0\to FE_1^*\to FE_2^*\to FE_3^*\to 0$. The long exact sequence for the right derived

functors is just the long exact sequence for this exact sequence of complexes. For the left derived functor use the diagram (D.3). □

Corollary D.19. (1) *Let* $0 \to M \xrightarrow{\alpha} E \xrightarrow{\beta} M' \to 0$ *be an exact sequence with injective module* E*. Then for every covariant (contravariant) functor* F*,* $\mathrm{R}^n\mathrm{F}(M) \simeq \mathrm{R}^{n-1}\mathrm{F}(M')$ *if* $n > 1$ *and* $\mathrm{R}^1\mathrm{F}(M) \simeq \operatorname{Coker}\mathrm{R}^0\mathrm{F}(\beta)$ *(respectively,* $\mathrm{L}_n\mathrm{F}(M) \simeq \mathrm{L}_{n-1}\mathrm{F}(M')$ *if* $n > 1$ *and* $\mathrm{L}_1\mathrm{F}(M) \simeq \operatorname{Ker}\mathrm{L}_0\mathrm{F}(\beta)$*).*

(2) *Let* $0 \to M' \xrightarrow{\beta} P \xrightarrow{\alpha} M \to 0$ *be an exact sequence with projective module* P*. Then, for every covariant (contravariant) functor* F*,* $\mathrm{R}^n\mathrm{F}(M) \simeq \mathrm{R}^{n-1}\mathrm{F}(M')$ *if* $n > 1$ *and* $\mathrm{R}^1\mathrm{F}(M) \simeq \operatorname{Coker}\mathrm{R}^0\mathrm{F}(\beta)$ *(respectively,* $\mathrm{L}_n\mathrm{F}(M) \simeq \mathrm{L}_{n-1}\mathrm{F}(M')$ *if* $n > 1$ *and* $\mathrm{L}_1\mathrm{F}(M) \simeq \operatorname{Ker}\mathrm{L}_0\mathrm{F}(\beta)$*).*

D.3. **Ext and Tor.** We are going to prove that both definitions of Ext and Tor (whether we fix the first or the second argument) give the same results. For the moment we denote $\operatorname{Ext}^n_A(\underline{M}, -) = \mathrm{R}^n \operatorname{Hom}_A(M, -)$ and $\operatorname{Ext}^n_A(-, \underline{N}) = \mathrm{R}^n \operatorname{Hom}_A(-, N)$, as well as $\operatorname{Tor}^A_n(\underline{M}, -) = \mathrm{L}^n(M \otimes_A -)$ and $\operatorname{Tor}^A_n(-, \underline{N}) = \mathrm{L}^n(- \otimes_A N)$.

Theorem D.20. $\operatorname{Ext}^n_A(\underline{M}, N) \simeq \operatorname{Ext}^n_A(M, \underline{N})$ *and* $\operatorname{Tor}^A_n(\underline{M}, N) \simeq \operatorname{Tor}^A_n(M, \underline{N})$ *for every modules* M, N*.*

Proof. We sketch a proof of the first assertion; the second one can be proved quite analogously. As every homomorphism $\xi : N \to N'$ induces a homomorphism $\xi\cdot : \operatorname{Hom}_A(-, N) \to \operatorname{Hom}_A(-, N')$, it induces a morphism of the derived functors $\operatorname{Ext}^n_A(-, \underline{N}) \to \operatorname{Ext}^n_A(-, \underline{N'})$ which we denote by $\cdot\xi^n$. One easily sees that these morphisms commute with the homomorphisms of the LES for derived functors $\operatorname{Ext}^n_A(-, \underline{N})$ and $\operatorname{Ext}^n_A(-, \underline{N'})$. The following properties hold:

(1) $\operatorname{Ext}^n_A(-, \underline{E}) = 0$ if E is injective (since $\operatorname{Hom}_A(-, E)$ is exact).
(2) If $0 \to N_1 \to N_2 \to N_3 \to 0$ is an exact sequence, then, for every complex P_* with projective components the induced sequence of complexes

$$0 \to \operatorname{Hom}_A(P^*, N_1) \to \operatorname{Hom}_A(P^*, N_2) \to \operatorname{Hom}_A(P^*, N_3) \to 0$$

is also exact. If $P^* = P^*_M$, it gives a LES for $\operatorname{Ext}^n_A(M, \underline{N_i})$ which is of the same shape as the LES for the functors $\operatorname{Ext}^n_A(\underline{M}, N_i)$. Moreover, they both starts from $\operatorname{Hom}_A(M, N_i)$.
(3) Therefore, if $0 \to N' \xrightarrow{\alpha} E \to N \to 0$ is an exact sequence with injective E, $\operatorname{Ext}^n_A(M, \underline{N}) \simeq \operatorname{Ext}^{n-1}_A(M, \underline{N'})$ for $n > 1$ and $\operatorname{Ext}^1_A(M, \underline{N}) \simeq \operatorname{Coker}(\cdot\alpha^1)$.
(4) As the last assertion also holds for $\operatorname{Ext}^n_A(\underline{M}, N)$, we can prove isomorphisms $\operatorname{Ext}^n_A(\underline{M}, N) \simeq \operatorname{Ext}^n_A(M, \underline{N})$ by induction. □

Here are some calculations of Ext and Tor. They will be used in the proof of the theorem of Krull-Akizuki (Thm. 19.6).

Example D.21. Let $I \subset A$ be an ideal. The exact sequence $0 \to I \to A \to A/I \to 0$ induces exact sequences

$$0 \to \operatorname{Ann}_M I \to M \xrightarrow{\eta} \operatorname{Hom}_A(I, M) \to \operatorname{Ext}^1_A(A/I, M) \to 0$$

and

$$0 \to \operatorname{Tor}^A_1(A/I, M) \to I \otimes_A M \to M \to M/IM \to 0,$$

where η maps an element $v \in M$ to the homomorphism $x \mapsto xv$ $(x \in I)$. Hence $\operatorname{Ext}^1_A(A/I, M) \simeq \operatorname{Coker} \eta$ and

$$\operatorname{Tor}_1(A/I, M) \simeq \operatorname{Ker}(I \otimes_A M \to IM).$$

In particular, if $a \in A$ is a non-zero-divisor, then $\operatorname{Ext}^1_A(A/aA, M) \simeq M/aM$, $\operatorname{Tor}^A_1(A/aA, M) \simeq \operatorname{Ann}_M a$, so we obtain the evident exact sequence

$$0 \to \operatorname{Ann}_M a \to M \xrightarrow{a} M \to M/aM \to 0.$$

If M is of finite length, all modules in the last sequence are of finite length. Taking the alternative sum of length, we see that $\ell_A(M/aM) = \ell_A(\operatorname{Ann}_M a)$

Ext^1 is closely related to *extensions of modules*.

Definition D.22. (1) A *extension* of a module M with the kernel N (or an extension of N with the quotient M) is an exact sequence $\mathrm{E} : 0 \to N \xrightarrow{\alpha} X \xrightarrow{\beta} M \to 0$.

(2) The extensions E and $\mathrm{E}' : 0 \to N \xrightarrow{\alpha} X' \xrightarrow{\beta} M \to 0$ are called *equivalent* if there is a homomorphism $\gamma : X \to X'$ such that $\alpha' = \gamma\alpha$ and $\beta = \beta'\gamma$, that is the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & N & \xrightarrow{\alpha} & X & \xrightarrow{\beta} & M & \longrightarrow & 0 \\ & & \| & & \downarrow{\scriptstyle\gamma} & & \| & & \\ 0 & \longrightarrow & N & \xrightarrow{\alpha'} & X' & \xrightarrow{\beta'} & M & \longrightarrow & 0 \end{array} \tag{D.4}$$

is commutative. Then we write $\mathrm{E} \approx \mathrm{E}'$. One easily sees that $\approx$ is an equivalence relation.

(3) We denote by $\operatorname{Ex}(M, N)$ the set of equivalence classes of extensions of M with kernel N.

(4) The extension E induces the connecting map $\delta_{\mathrm{E}} : \operatorname{Hom}_A(M, M) \to \operatorname{Ext}^1_A(M, N)$. We denote by $\underline{\varepsilon}(\mathrm{E})$ the element $\delta_{\mathrm{E}}(\mathrm{id}_M) \in \operatorname{Ext}^1_A(M, N)$.

Theorem D.23. *The map $\underline{\varepsilon}$ establishes a bijection betweem $\operatorname{Ex}(M, N)$ and $\operatorname{Ext}^1_A(M, N)$.*

Proof. The diagram (D.4) induces a commutative diagram

$$\begin{array}{ccc} \operatorname{Hom}_A(M, M) & \xrightarrow{\delta_{\mathrm{E}}} & \operatorname{Ext}^1_A(M, N) \\ \| & & \| \\ \operatorname{Hom}_A(M, M) & \xrightarrow{\delta_{\mathrm{E}'}} & \operatorname{Ext}^1_A(M, N) \end{array}$$

Hence $\underline{\varepsilon}(\mathrm{E}) = \underline{\varepsilon}(\mathrm{E}')$ and $\underline{\varepsilon}$ can be considered as a map $\operatorname{Ex}(M, N) \to \operatorname{Ext}^1_A(M, N)$.

On the other hand, choose an exact sequence $\mathrm{R}: 0 \to K \xrightarrow{\xi} P \xrightarrow{\eta} M \to 0$ with projective P. Then δ_R induces an isomorphism $\mathrm{Coker}(\cdot\xi) \simeq \mathrm{Ext}^1(M,N)$. Given a homomorphism $\phi: K \to N$, let $X = N \oplus P/\{(\phi(v), -\xi(v)\}$, where $v \in K$. We denote by $[u,p]$ the coset of (u,p) in X and define homomorphisms $\alpha: N \to X$ and $\beta: X \to M$ setting $\alpha(u) = [u,0]$ and $\beta[u,p] = \eta(p)$. One easily verifies that the sequence $\mathrm{E}(\phi): 0 \to N \xrightarrow{\alpha} X \xrightarrow{\beta} M \to 0$ is exact, hence is an extension from $\mathrm{Ex}(M,N)$. One can also check that if $\phi' = \phi + \psi\xi$ for some $\psi: P \to N$, then $\mathrm{E}(\phi') \approx \mathrm{E}(\phi)$ (**check it**). Hence, we can write $\mathrm{E}(\varepsilon)$, where $\varepsilon = \delta_R(\phi)$, instead of ϕ.

Exercise D.24. Verify that $\underline{\varepsilon}(\mathrm{E}(\varepsilon)) = \varepsilon$ and $\mathrm{E}(\underline{\varepsilon}(\mathrm{E})) \approx \mathrm{E}$. It means that $\underline{\varepsilon}$ ist indeed a bijection.

□

Appendix E. Krull–Schmidt–Azymaya

Recall that a ring R (maybe noncommutative) is called *local* if the set of non-invertible elements of R is an ideal $\mathfrak{r} = \mathrm{rad}\, A$. Obviously, it is a unique left and a unique right ideal of R and $1-a$ is invertible for every $a \in \mathfrak{r}$.

Theorem E.1 (Krull–Schmidt–Azumaya)**.** *Let M_i $(1 \leqslant i \leqslant n)$ be A-modules such that $B_i = \mathrm{End}_A M_i$ are local rings, $M = \bigoplus_{i=1}^m M_i$.*

1. *If $M \simeq N \oplus N'$, there is a subset $\mathbf{I} \subseteq \{1,2,\dots,n\}$ such that $N \simeq \bigoplus_{i\in\mathbf{I}} M_i$ and $N' \simeq \bigoplus_{i\notin\mathbf{I}} M_i$.*
2. *If $M \simeq \bigoplus_{j=1}^m N_j$, where $\mathrm{End}_A N_j$ are also local, then $i = j$ and there is a permutation σ of indices such that $M_i \simeq N_{\sigma i}$.*

Proof. We do the following steps.

Claim 1. *Let M, N be A-modules such that $\mathrm{End}_A M$ is local with the maximal ideal $\mathfrak{r}$, $\alpha: M \to N$ and $\beta: N \to M$ are*

homomorphisms. If $\beta\alpha \notin \mathfrak{r}$, *there is* $\alpha' : N \to M$ *such that* $\alpha'\alpha = \mathrm{id}_M$, *so* $N = \operatorname{Im}\alpha \oplus \operatorname{Ker}\alpha'$ *and* $\alpha : M \xrightarrow{\sim} \operatorname{Im}\alpha$.

Proof. If $\beta\alpha \notin \mathfrak{r}$, it is invertible: $\gamma\beta\alpha = \mathrm{id}_M$ and we can set $\alpha' = \gamma\beta$. □

Claim 2. *Let* M, M', N, N' *are* A*-modules,* $\operatorname{End}_A M$ *and* $\operatorname{End}_A M'$ *are local and* $M \oplus N \simeq M' \oplus N'$. *Either* $M \simeq M'$ *and* $N \simeq N'$ *or there is a module* L *such that* $N \simeq M' \oplus L$ *and* $N' \simeq M \oplus L$.

Proof. We denote by $\mathfrak{r}$ the maximal ideal of $\operatorname{End}_A M$. Let an isomorphism $\alpha : M \oplus N \xrightarrow{\sim} M' \oplus N'$ is given by the matrix $\left(\begin{smallmatrix} \alpha_1 & \alpha_2 \\ \alpha_3 & \alpha_4 \end{smallmatrix}\right)$ and α^{-1} is given by the matrix $\left(\begin{smallmatrix} \beta_1 & \beta_2 \\ \beta_3 & \beta_4 \end{smallmatrix}\right)$. Then $\beta_1\alpha_1 + \beta_2\alpha_3 = \mathrm{id}_M$. Let first $\beta_1\alpha_1 \notin \mathfrak{r}$. As M' is indecomposable, $\alpha : M \xrightarrow{\sim} M'$. If γ is the automorphism of $M \oplus N$ given by the matrix $\left(\begin{smallmatrix} \mathrm{id}_M & -\alpha_1^{-1}\alpha_2 \\ 0 & \mathrm{id}_N \end{smallmatrix}\right)$, then $\alpha\gamma = \left(\begin{smallmatrix} \alpha_1 & 0 \\ \alpha_3 & \alpha_4' \end{smallmatrix}\right)$. As $\alpha\gamma$ is an isomorphism, so is also $\alpha_4' : N \to N'$.

Let now $\beta_1\alpha_1 \in \mathfrak{r}$. Then $\beta_2\alpha_3 \notin \mathfrak{r}$, hence there is $\gamma : N' \to M$ such that $\gamma\alpha_3 = \mathrm{id}_M$. It implies that $N' = \operatorname{Im}\alpha_3 \oplus L$, where $L = \operatorname{Ker}\gamma$. Moreover, if $\iota : L \to N'$ is the embedding and $\pi : N' \to L$ is the projection, $\alpha_3\gamma + \iota\pi = \mathrm{id}_{N'}$ (**check it**). Then the isomorphism $\alpha : M \oplus N \to M' \oplus M \oplus L \xrightarrow{\sim} M \oplus M' \oplus L$ is given by the matrix

$$\tilde{\alpha} = \begin{pmatrix} \mathrm{id}_M & \gamma\alpha_4 \\ \alpha_1 & \alpha_2 \\ 0 & \pi\alpha_4 \end{pmatrix}$$

and the isomorphism $\alpha^{-1} : M \oplus M' \oplus L \to M \oplus N$ is given by the matrix

$$\tilde{\beta} = \begin{pmatrix} \beta_2\alpha_3 & \beta_1 & \beta_2\iota \\ \beta_4\alpha_3 & \beta_3 & \beta_4\iota \end{pmatrix}.$$

(**Verify that** $\tilde{\beta}\tilde{\alpha} = \mathrm{id}$.) As $\beta_2\alpha_3 \notin \mathfrak{r}$, the first part of the proof shows that $N \simeq M' \oplus L$. □

The theorem is obtained from Claim 2 by an easy induction (**explain the details**). □

Appendix F. Nagata's example

Theorem F.1. *Let $A = \Bbbk[x_1, x_2, \dots, x_n, \dots]$, where $\Bbbk$ is a field, $0 = d_1 < d_2 < d_3 < \dots < d_n < \dots$ be a sequence of integers, $\mathfrak{p}_i = (x_{d_i+1}, \dots, x_{d_{i+1}})$, $S = A \setminus \bigcup_{i=1}^{\infty} \mathfrak{p}_i$ and $\tilde{A} = A[S^{-1}]$. The ring $\tilde{A}$ is Noetherian and $\dim \tilde{A} = \sup_i (d_{i+1} - d_i)$, so it is infinite if these differences are unbounded (for instance, if $d_i = i^2$).*

We prove this result in several steps.

Claim 1. *If $I \subset A$ is an ideal such that $I \cap S = \varnothing$, that is $I \subseteq \bigcup_{i=1}^{\infty} \mathfrak{p}_i$, then $I \subseteq \mathfrak{p}_i$ for some i. Therefore, prime ideals of $\tilde{A}$ are $\mathfrak{p}\tilde{A}$, where $\mathfrak{p}$ is a prime ideal of A contained in some $\mathfrak{p}_i$, and maximal ideals of $\tilde{A}$ are $\mathfrak{p}_i\tilde{A}$.*

Proof. Let $I_k = I \cap \Bbbk[x_1, x_2, \dots, x_{d_{k+1}}]$. Find the smallest k such that $I_k \neq 0$. $I_k \subseteq \bigcup_{i=1}^{k} \mathfrak{p}_i \cap \Bbbk[x_1, x_2, \dots, x_{d_{k+1}}]$. Therefore, $I_k \subseteq \mathfrak{p}_i \cap \Bbbk[x_1, x_2, \dots, x_{d_{k+1}}]$ for some $i \leqslant k$. Choose the minimal possible i. If $l > k$, also $I_l \subseteq \mathfrak{p}_j \cap \Bbbk[x_1, x_2, \dots, x_{d_{l+1}}]$ for some $j \leqslant l$. Obviously $I_k \notin \mathfrak{p}_j \cap \Bbbk[x_1, x_2, \dots, x_{d_{k+1}}]$ if $j > k$. Therefore, $j \leqslant k$ and, as i was chosen minimal, $j = i$ and $I \subseteq \mathfrak{p}_i$. □

Claim 2. *$\tilde{A}$ is Noetherian.*

Proof. Every localization $\tilde{A}_{\mathfrak{p}_i\tilde{A}_i}$ is Noetherian. Evidenly, any element from $\tilde{A}$ is contained only in finitely many of the ideals $\mathfrak{p}_i\tilde{A}$. Therefore, we can apply the following fact.

Lemma F.2. *Let R be a ring such that $R_{\mathfrak{m}}$ is Noetherian for every maximal ideal $\mathfrak{m} \subseteq R$ and every element $a \in R$ is contained only in finitely many maximal ideals. Then R is Noetherian.*

Proof. Let I be an ideal of R, $\mathfrak{m}_1, \mathfrak{m}_2, \dots, \mathfrak{m}_m$ be all maximal ideals containing I. There are elements $a_{ij} \in I$ $(1 \leqslant j \leqslant k_i)$ such that $I_{\mathfrak{m}_i}$ is generated by $a_{ij}/1$. Let $J \subseteq I$ be generated by all elements a_{ij} $(1 \leqslant i \leqslant m, 1 \leqslant j \leqslant k_i)$. Then $I_{\mathfrak{m}} = J_{\mathfrak{m}}$ for

all $\mathfrak{m} \in \operatorname{max.spec} R$. Therefore $I = J$ is finitely generated. □

Claim 3. $\operatorname{ht} \mathfrak{p}_i = d_{i+1} - d_i$. *Therefore,* $\dim \tilde{A} = \sup_i (d_{i+1} - d_i)$.

Proof. $\operatorname{ht} \mathfrak{p}_i \leqslant d_{i+1} - d_i$ since $\mathfrak{p}_i = (x_{d_i+1}, \ldots, x_{d_{i+1}})$. On the other hand, $\operatorname{ht} \mathfrak{p}_i \geqslant d_{i+1} - d_i$, since $\mathfrak{p}_i \supset (x_{d_i+2}, \ldots, x_{d_{i+1}}) \supset (x_{d_i+3}, \ldots, x_{d_{i+1}}) \supset \ldots \supset 0$ is a chain of prime ideals of length $d_{i+1} - d_i$. □

It accomplishes the proof of the Nagata's theorem.

References

[1] Artin, M. *Algebra*. Prentice Hall, Inc., Englewood Cliffs, NJ, 1991.

[2] Atiyah, M. F., and Macdonald, I. G. *Introduction to commutative algebra*, economy ed. Addison-Wesley Series in Mathematics. Westview Press, Boulder, CO, 2016.

[3] Eisenbud, D. *Commutative algebra*, vol. 150 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995.

[4] Greuel, G.-M., and Pfister, G. *A* **Singular** *introduction to commutative algebra*, extended ed. Springer, Berlin, 2008.

[5] Matlis, E. Injective modules over Noetherian rings. *Pac. J. Math. 8* (1958), 511–528.

[6] Matsumura, H. *Commutative algebra*, second ed., vol. 56 of *Mathematics Lecture Note Series*. Benjamin/Cummings Publishing Co., Inc., Reading, MA, 1980.

[7] Matsumura, H. *Commutative ring theory*, second ed., vol. 8 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1989. Translated from the Japanese by M. Reid.

[8] Nagata, M. *Local rings*, vol. No. 13 of *Interscience Tracts in Pure and Applied Mathematics*. Interscience Publishers (a division of John Wiley & Sons, Inc.), New York-London, 1962.

[9] Serre, J.-P. *Local algebra. Transl. from the French by CheeWhye Chin*. Springer Monogr. Math. Berlin: Springer, 2000.

[10] Weibel, C. A. *An introduction to homological algebra*, vol. 38 of *Camb. Stud. Adv. Math.* Cambridge: Cambridge University Press, 1994.

Index