LECTURE NOTES
COMMUTATIVE ALGEBRA

SERGEY MOZGOVOY

Contents

Date: March 28, 2024.

1. Rings and Ideals

1.1. **Prime and maximal ideals.** A ring will always mean a commutative ring unless otherwise stated. Given a ring A, we will usually denote the zero ideal $\{0_A\}$ by 0. We will allow rings A with $1_A = 0_A$. In this case $a = a \cdot 1_A = a \cdot 0_A = 0_A$ for all $a \in A$, hence $A = \{0_A\}$. This ring is called the *zero ring*.

Definition 1.1.
1. An ideal $I \subset A$ is called *proper* if $I \neq A$.
2. A proper ideal $\mathfrak{p} \subset A$ is called *prime* if $ab \in \mathfrak{p} \implies a \in \mathfrak{p}$ or $b \in \mathfrak{p}$.
3. A proper ideal $\mathfrak{m} \subset A$ is called *maximal* if there is no ideal I such that $\mathfrak{m} \subsetneq I \subsetneq A$.
4. The set of all prime ideals of A is denoted by $\operatorname{Spec}(A)$, called the *spectrum* of A.
5. The set of all maximal ideals of A is denoted by $\operatorname{Max}(A)$, called the *maximal spectrum* of A.

Example 1.2 (Maximal and prime ideals in $\mathbb{Z}$)**.** Maximal ideals of $\mathbb{Z}$ have the form $(p) = \mathbb{Z}p$, where $p \geq 2$ is a prime number. The set of prime ideals consists of the maximal ideals and the zero ideal.

Remark 1.3. A nonzero element $p \in A$ is called prime if p is not invertible and if $p \mid ab$ implies $p \mid a$ or $p \mid b$. One can show that $p \in A$ is prime $\iff$ $(p) = Ap$ is a nonzero prime ideal. If A is a PID, then every prime ideal is either zero or of the form (p) for a prime element $p \in A$. The maximal ideals of A are all nonzero prime ideals.

Lemma 1.4.
1. *An ideal $\mathfrak{p}$ is prime $\iff$ $A/\mathfrak{p}$ is an integral domain.*
2. *An ideal $\mathfrak{m}$ is maximal $\iff$ $A/\mathfrak{m}$ is a field.*
3. *A maximal ideal is prime.*

Proof. **(1)** Let $\mathfrak{p}$ be prime and $[a], [b] \in A/\mathfrak{p}$ be nonzero. Then $a, b \notin \mathfrak{p} \implies ab \notin \mathfrak{p}$ (as $\mathfrak{p}$ is prime) $\implies [a] \cdot [b] = [ab] \neq 0$ in $A/\mathfrak{p}$. This means that $A/\mathfrak{p}$ is an integral domain. The converse is similar.
(2) If $\mathfrak{m}$ is maximal, then there are no ideals in $A/\mathfrak{m}$ except 0 and $A/\mathfrak{m}$. If $a \in A/\mathfrak{m}$ is nonzero $\implies$ the principal ideal (a) is nonzero $\implies$ $(a) = A/\mathfrak{m}$ $\implies$ $\exists b \in A/\mathfrak{m}$ such that $ab = 1$ $\implies$ a is invertible. This means that $A/\mathfrak{m}$ is a field. Conversely, if $A/\mathfrak{m}$ is a field, then there are no ideals in $A/\mathfrak{m}$ except 0 and $A/\mathfrak{m}$. This implies that there are no ideals $\mathfrak{m} \subset I \subset A$ except $I = \mathfrak{m}$ or $I = A$.
(3) Using the previous statements we obtain: if $\mathfrak{m}$ is maximal $\implies$ $A/\mathfrak{m}$ is a field $\implies$ $A/\mathfrak{m}$ is an integral domain $\implies$ $\mathfrak{m}$ is prime. Alternatively, assume that $\mathfrak{m}$ is maximal, $ab \in \mathfrak{m}$ and $a \notin \mathfrak{m}$. Then $(a) + \mathfrak{m} = A \implies 1 - ac \in \mathfrak{m}$ for some $c \in A \implies b - abc \in \mathfrak{m} \implies b \in \mathfrak{m}$ as $ab \in \mathfrak{m}$. This proves that $\mathfrak{m}$ is prime. □

Exercise 1.5. Show that if R is a PID and $\mathfrak{p} \subset R$ is a non-zero prime ideal, then $\mathfrak{p}$ is maximal.

Remark 1.6. We know that for any ideal $I \subset A$, there is a bijection between ideals $I \subset J \subset A$ and all ideals of A/I, where an ideal $J \subset A$ is mapped to the ideal J/I of A/I. This implies that there is a bijection between all prime (maximal) ideals $I \subset J \subset A$ and all prime (maximal) ideals of A/I. Indeed, an ideal $I \subset J \subset A$ is prime (maximal) $\iff$ $A/J \simeq (A/I)/(J/I)$ is an integral domain (a field) $\iff$ $J/I \subset A/I$ is prime (maximal).

Remark 1.7. We obtain that $\operatorname{Max} A \subset \operatorname{Spec} A$. The set $\operatorname{Spec} A$ (hence also $\operatorname{Max} A$) can be equipped with a topology as follows. For any subset (or ideal) $I \subset A$, define

$$Z(I) = \{\mathfrak{p} \in \operatorname{Spec} A \mid I \subset \mathfrak{p}\} \tag{1}$$

and define closed sets in $\operatorname{Spec} A$ to be subsets of the form $Z(I)$. This topology is called the *Zariski topology*.

Later we will require the following set-theoretic result.

Lemma 1.8 (Zorn)**.** *Let X be a non-empty poset (partially ordered set) such that every chain $Y \subset X$ (a totally ordered subset, meaning that if $x, y \in Y$, then $x \le y$ or $y \le x$) has an upper bound in X (meaning an element $x \in X$ such that $y \le x$ $\forall y \in Y$). Then X has at least one maximal element (meaning an element $x \in X$ such that $x \le y \implies x = y$).*

Theorem 1.9. *A proper ideal $I \subset A$ is contained in at least one maximal ideal.*

Proof. To apply *Zorn's lemma*, let X be the set all of proper ideals of A that contain I. We define the partial order on X given by inclusion of ideals. The set X is non-empty as $I \in X$.

Given a chain $Y \subset X$ of ideals, we consider the subset $J = \bigcup_{J' \in Y} J' \subset A$. It is an ideal of A. Indeed, if $a, b \in J \implies a \in J'$, $b \in J''$ for some $J', J'' \in Y$. Then $J' \subset J''$ or $J'' \subset J'$ by the chain assumption. Assuming that $J' \subset J''$, we obtain $a, b \in J'' \implies a + b \in J'' \subset J$. Other axioms of an ideal are verified in the same way.

The ideal J is proper, as otherwise $1 \in J \implies 1 \in J'$ for some $J' \in Y \implies J' = A$, which contradicts to the assumption that all elements of X are proper ideals. Therefore $J \in X$ and J is an upper bound of the chain Y. By Zorn's lemma, X has a maximal element, which is the required maximal ideal of A that contains I. □

Definition 1.10. For an ideal $I \subset A$ and a subset $J \subset A$, define the product IJ to be the ideal

$$IJ = \left\{ \sum a_i b_i \,\middle|\, a_i \in I, b_i \in J \ \forall i \right\}.$$

Definition 1.11. Let $f \colon A \to B$ be a ring homomorphism.

1. For an ideal $I \subset A$, define the *extension ideal* $I^e = Bf(I) \subset B$ (ideal generated by $f(I)$).
2. For an ideal $J \subset B$, define the *contraction ideal* $J^c = f^{-1}(J) = \{a \in A \mid f(a) \in J\} \subset A$.

Lemma 1.12. *Let $f \colon A \to B$ be a ring homomorphism and $\mathfrak{q} \subset B$ be a prime ideal. Then $f^{-1}(\mathfrak{q}) \subset A$ is a prime ideal.*

Proof. One can show that $\mathfrak{p} = f^{-1}(\mathfrak{q})$ is an ideal of A. Let $ab \in \mathfrak{p}$. Then $f(ab) = f(a)f(b) \in \mathfrak{q}$, hence $f(a) \in \mathfrak{q}$ or $f(b) \in \mathfrak{q}$. Therefore $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$. □

Example 1.13. There exist ring homomorphisms $f \colon A \to B$ and maximal ideals $\mathfrak{n} \subset B$ such that $f^{-1}(\mathfrak{n})$ is not necessarily maximal. For example, let $f \colon \mathbb{Z} \to \mathbb{Q}$ be the inclusion. Then the zero ideal $\mathfrak{n} = 0 \subset \mathbb{Q}$ is maximal in $\mathbb{Q}$, but $f^{-1}(\mathfrak{n}) = 0 \subset \mathbb{Z}$ is not maximal in $\mathbb{Z}$ (for example, $0 \subset (2) \subset \mathbb{Z}$).

Remark 1.14. We will see later (Hilbert's Nullstellensatz 5.26) that if B is a finitely-generated algebra over a field $\Bbbk$ (meaning that $B \simeq \Bbbk[x_1, \ldots, x_n]/I$ for some ideal I) and $\mathfrak{n} \subset B$ is a maximal ideal, then $B/\mathfrak{n}$ is a finite field extension of $\Bbbk$. If $f \colon A \to B$ is an algebra homomorphism and $\mathfrak{m} = f^{-1}(\mathfrak{n})$, then $\Bbbk \subset A/\mathfrak{m} \subset B/\mathfrak{n}$, hence $A/\mathfrak{m}$ is a finite-dimensional integral domain. This implies that $A/\mathfrak{m}$ is a field (exercise), hence $\mathfrak{m} \subset A$ is a maximal ideal.

1.2. **Radicals.**

Definition 1.15.

(1) An element $a \in A$ is called *nilpotent* if $a^n = 0$ for some $n > 0$.

(2) Define the *nilradical* of A to be the set of all nilpotent elements of A

$$\mathcal{N}(A) = \{a \in A \mid a^n = 0 \text{ for some } n > 0\}.$$

(3) For any ideal $I \subset A$, define the *radical* of I to be

$$\sqrt{I} = \{a \in A \mid a^n \in I \text{ for some } n > 0\}.$$

Note that $\mathcal{N}(A) = \sqrt{0}$, hence $\mathcal{N}(A)$ is an ideal of A by the following result.

Lemma 1.16. *$\sqrt{I}$ is an ideal of A and $\sqrt{\sqrt{I}} = \sqrt{I}$.*

Proof. If $a, b \in \sqrt{I}$, then $a^m \in I$, $b^n \in I$ for some $m, n > 0$. Therefore

$$(a+b)^{m+n} = \sum_{k+l=m+n} \binom{m+n}{k} a^k b^l \in I$$

as either $k \geq m$ or $l \geq n$, hence either $a^k \in I$ or $b^l \in I$. This implies that $a + b \in \sqrt{I}$. Similarly, $-a \in \sqrt{I}$. Finally, for any $c \in A$, we have $(ca)^m = c^m a^m \in I$, hence $ca \in \sqrt{I}$. Therefore $\sqrt{I}$ is an ideal.

If $a \in \sqrt{\sqrt{I}} \implies a^m \in \sqrt{I}$ for some $m > 0 \implies a^{mn} = (a^m)^n \in I$ for some $n > 0 \implies a \in \sqrt{I}$. □

Lemma 1.17. *$\mathcal{N}(A)$ is the intersection of all prime ideals of A.*

Proof. Let $I = \mathcal{N}(A)$ and let I' be the intersection of all prime ideals of A. If $a \in I \implies a^n = 0$ for some $n > 0$. For any prime ideal $\mathfrak{p} \subset A$, we have $a^n = 0 \in \mathfrak{p} \implies a \in \mathfrak{p}$ (by the property of prime ideals). This implies that $a \in I'$ and $I \subset I'$.

Conversely, assume that $c \in I'$ and $c \notin I$. Then $c^n \notin I$ for all $n > 0$, as otherwise $c^n \in I = \mathcal{N}(A)$ $\implies c$ is nilpotent $\implies c \in I$. Consider the set X of all ideals J such that

$$c^n \notin J \qquad \forall n > 0.$$

and order it by inclusion. Then X satisfies the conditions of the Zorn lemma (see Theorem 1.9), in particular $X \neq \varnothing$ as $I \in X$. Therefore X has a maximal element, say $\mathfrak{p}$. We claim that $\mathfrak{p}$ is prime. Assume that $ab \in \mathfrak{p}$ and $a \notin \mathfrak{p}$, $b \notin \mathfrak{p}$. Then $\mathfrak{p} + aA$, $\mathfrak{p} + bA$ are strictly larger than $\mathfrak{p}$, hence

$$c^m \in \mathfrak{p} + aA, \qquad c^n \in \mathfrak{p} + bA$$

for some $m, n > 0$. Therefore $c^{m+n} \in (\mathfrak{p} + aA)(\mathfrak{p} + bA) \subset \mathfrak{p} + abA = \mathfrak{p}$, which contradicts to $\mathfrak{p} \in X$. We found a prime ideal $\mathfrak{p}$ such that $c \notin \mathfrak{p}$, hence $c \notin I'$ (intersection of primes), a contradiction. □

Lemma 1.18. *For any ideal $I \subset A$, we have*

(1) *$\sqrt{I}/I = \mathcal{N}(A/I)$.*

(2) *$\sqrt{I}$ is the intersection of all prime ideals of A that contain I.*

Proof. **(1)** If $[a] \in \sqrt{I}/I \implies a^n \in I$ for some $n > 0 \implies [a]^n = 0$ in $A/I \implies [a] \in \mathcal{N}(A/I)$. The converse is similar.

(2) We know that $\sqrt{I}/I = \mathcal{N}(A/I)$ is the intersection of all prime ideals of A/I. These prime ideals can be identified with prime ideals of A that contain I, hence $\sqrt{I}$ is equal to the intersection of the latter ideals. □

Definition 1.19. Define the *Jacobson radical* $\mathcal{R}(A)$ of a ring A to be the intersection of all maximal ideals of A.

Remark 1.20. We always have $\mathcal{N}(A) \subset \mathcal{R}(A)$ as every maximal ideal is prime. Later we will show that if A is a finitely-generated algebra over a field, then every prime ideal is an intersection of maximal ideals and therefore $\mathcal{N}(A) = \mathcal{R}(A)$. Such rings are called *Jacobson rings*.

Example 1.21.

(1) Consider the ring $\mathbb{Z}$ and $a \in \mathcal{R}(\mathbb{Z})$. For any prime number $p \in \mathbb{Z}$, the ideal $p\mathbb{Z}$ is maximal as $\mathbb{Z}/p\mathbb{Z}$ is a field. This implies that $a \in \mathcal{R}(\mathbb{Z}) \subset p\mathbb{Z}$, hence $p \mid a$. We conclude that $p \mid a$ for all prime p, hence $a = 0$. Therefore $\mathcal{R}(A) = 0$.

(2) Consider the ring $A = \Bbbk[x]/(x^2)$. Every ideal in A can be written as $I/(x^2)$ for some ideal $(x^2) \subset I \subset \Bbbk[x]$. We can write $I = (f)$ for some $f \in \Bbbk[x]$. Then $(x^2) \subset (f)$ implies $f \mid x^2$ $\implies f = 1, x, x^2$ up to a scalar. The corresponding ideal is maximal (or prime) only if $f = x$. We conclude that $\mathcal{N}(A) = \mathcal{R}(A) = (x)/(x^2)$.

(3) Let $A = \Bbbk[\![t]\!]$ be the ring of formal power series over a field $\Bbbk$. A power series $f = \sum_{i \geq 0} f_i t^i$ is invertible $\iff f_0 \neq 0$. Therefore $\mathfrak{m} = \{f \in A \mid f_0 = 0\}$ is a unique maximal ideal of A, hence $\mathcal{R}(A) = \mathfrak{m}$. On the other hand $\mathcal{N}(A) = 0$.

Lemma 1.22. *$a \in \mathcal{R}(A) \iff 1 - ab$ is invertible for all $b \in A$.*

Proof. ($\implies$) If $1 - ab$ is not invertible for some $b \in A \implies (1 - ab) \subset A$ is a proper ideal $\implies$ there exists a maximal ideal $(1 - ab) \subset \mathfrak{m} \subset A$. We have $a \in \mathcal{R}(A) \subset \mathfrak{m} \implies ab \in \mathfrak{m} \implies 1 \in \mathfrak{m}$, a contradiction.

($\impliedby$) We need to show that, for any maximal ideal $\mathfrak{m}$, we have $a \in \mathfrak{m}$. But otherwise $\mathfrak{m} + (a) = A$ $\implies c + ab = 1$ for some $c \in \mathfrak{m}$ and $b \in A \implies 1 - ab = c$ is not invertible, a contradiction. ☐

1.3. **Local rings.**

Definition 1.23. A ring A is called a *local ring* if it has a unique maximal ideal $\mathfrak{m}$. The field $\Bbbk = A/\mathfrak{m}$ is called the *residue field* of A. Sometimes we will write $(A, \mathfrak{m})$ to specify a local ring A with its maximal ideal $\mathfrak{m}$.

Remark 1.24. Let $(A, \mathfrak{m})$ be a local ring.
(1) We have $\mathcal{R}(A) = \mathfrak{m}$.
(2) If $I \subset A$ is a proper ideal, then $I \subset \mathfrak{m}$. Indeed, we know that I is contained in some maximal ideal of A. As there exists a unique maximal ideal $\mathfrak{m}$ in A, we have $I \subset \mathfrak{m}$.

Example 1.25. Let $A = \Bbbk[\![t]\!]$ be the ring of formal power series over a field $\Bbbk$. A power series $f = \sum_{i \geq 0} f_i t^i$ is invertible $\iff$ $f_0 \neq 0$. Therefore $\mathfrak{m} = \{f \in A \mid f_0 = 0\}$ is a unique maximal ideal of A.

Example 1.26. Let X be a topological space and $x \in X$. Consider the set of pairs (U, f), where $x \in U \subset X$ is open and $f \colon U \to \mathbb{R}$ is continuous. Define an equivalence relation on the set of such pairs as $(U, f) \sim (V, g)$ if there exists open $x \in W \subset U \cap V$ such that $f|_W = g|_W$. The corresponding equivalence classes are called *germs* and form a commutative ring A_x (with pointwise addition and multiplication), called the *ring of germs*. The set $\mathfrak{m}_x = \{[f] \in A_x \mid f(x) = 0\}$ is a maximal ideal (it is the kernel of the evaluation map $A_x \to \mathbb{R}$, $[f] \mapsto f(x)$). If $[f] \in A_x \backslash \mathfrak{m}_x$, then $f(x) \neq 0 \implies f$ is nonzero on some open neighborhood V of $x \implies [f]$ is invertible (the inverse is given by $g(y) = f(y)^{-1}$ for $y \in V$). If $\mathfrak{m} \neq \mathfrak{m}_x$ is another maximal ideal $\implies \exists [f] \in \mathfrak{m} \backslash \mathfrak{m}_x$ $\implies [f]$ is invertible $\implies \mathfrak{m} = A_x$, a contradiction. We proved that $\mathfrak{m}_x$ is the unique maximal ideal of A_x, hence A_x is local. This example explains the name "local".

Lemma 1.27. *Let A be a ring and $\mathfrak{m} \subset A$ be a proper ideal. Then f.a.e.*
(1) *A is a local ring with the maximal ideal $\mathfrak{m}$.*
(2) *$\mathfrak{m}$ is maximal and all elements in $1 + \mathfrak{m}$ are invertible.*
(3) *All elements in $A \backslash \mathfrak{m}$ are invertible.*

Proof. **(1) $\implies$ (2).** If $1 + a$ is not invertible for some $a \in \mathfrak{m} \implies (1 + a)$ is a proper ideal $\implies$ it is contained in a maximal ideal $\implies (1 + a) \subset \mathfrak{m} \implies 1 = (1 + a) - a \in \mathfrak{m}$, a contradiction.
(2) $\implies$ (3). If $a \in A \backslash \mathfrak{m} \implies (a) + \mathfrak{m} = A \implies$ there exist $b \in A$ and $c \in \mathfrak{m}$ such that $ab + c = 1$ $\implies ab = 1 - c$ is invertible $\implies a$ is invertible.
(3) $\implies$ (1). Let $I \subset A$ be a proper ideal. If $I \not\subset \mathfrak{m} \implies \exists a \in I \backslash \mathfrak{m}$. By assumption a is invertible, hence $A = (a) = I$, a contradiction. We proved that every proper ideal is contained in $\mathfrak{m}$, hence $\mathfrak{m}$ is the unique maximal ideal. $\square$

1.4. **Rings of fractions.** Recall that one can obtain the field of rational numbers $\mathbb{Q}$ from the ring of integers $\mathbb{Z}$ by formally inverting all non-zero integers. More generally, given an integral domain A, we can construct its field of fractions $Q(A)$ by formally inverting all nonzero elements of A. More precisely, we consider the set of pairs (a, s) with $a, s \in A$ and $s \neq 0$, consider an equivalence relation

$$(a, s) \sim (b, t) \iff at = bs$$

and define a ring structure on the set of equivalence classes, where we interpret the equivalence class of (a, s) as a fraction $\frac{a}{s}$. We would like to generalize this construction for an arbitrary ring A in which we invert an appropriate subset $S \subset A$.

Definition 1.28. A subset $S \subset A$ is called a *multiplicative set* (or multiplicatively closed set) if $1 \in S$ and if S is closed under multiplication (i.e. $a, b \in S \implies ab \in S$).

Remark 1.29. Equivalently, a multiplicative set is a submonoid of the monoid $(A, *)$.

We define the *ring of fractions* $S^{-1}A$ of A with respect to a multiplicative set S as follows: We define an equivalence relation $\sim$ on the set $A \times S$ by the rule

$$(a, s) \sim (b, t) \iff (at - bs)u = 0 \text{ for some } u \in S.$$

This relation is indeed an equivalence relation:

(1) Reflexivity: $(a, s) \sim (a, s)$ is obvious.
(2) Symmetry: $(a, s) \sim (b, t) \iff (b, t) \sim (a, s)$ is obvious.
(3) Transitivity: assume that $(a, s) \sim (b, t)$ and $(b, t) \sim (c, u)$. Then $(at - bs)v = 0$ and $(bu - ct)w = 0$ for some $v, w \in S$. Therefore

$$(atv)uw = (bsv)uw = (buw)sv = (ctw)sv$$

and $(au - cs)tvw = 0$. This implies $(a, s) \sim (c, u)$ as $tvw \in S$.

We denote the equivalence class of (a, s) by $\frac{a}{s} = a/s$ and we denote the set of all equivalence classes by $S^{-1}A$. We define the ring structure on $S^{-1}A$ by the rule

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

This ring is called the *ring of fractions* (or *localization*) of A with respect to S. There is a natural ring homomorphism

$$i \colon A \to S^{-1}A, \qquad a \mapsto \frac{a}{1}.$$

We will usually denote $i(a)$ by a, although the map i is not necessarily injective. In particular, we denote $\frac{0}{1}$ by 0 and $\frac{1}{1}$ by 1.

Example 1.30. Let A be an integral domain and let $S = A\backslash\{0\}$. Then S is a multiplicative set (if $a, b \neq 0 \implies ab \neq 0$) and the fraction ring $S^{-1}A$ is the field of fractions of A.

Example 1.31. Assume that $0 \in S$. Then we always have $(a, s) \sim (0, 1)$. Therefore $S^{-1}A$ consists of one element $\frac{0}{1} = 0$, hence $S^{-1}A$ is the zero ring.

Remark 1.32. The map $i \colon A \to S^{-1}A$ is not always injective. For example, if $0 \in S$, then $S^{-1}A = 0$. For a different example, consider $A = \mathbb{Z}/6\mathbb{Z}$ and $S = \{1, 2, 4\}$. Then $(3, 1) \sim (0, 1)$ as $2(3 - 0) = 0$ in A and $2 \in S$. This implies that $i(3) = 0$.

Lemma 1.33. *The map $i \colon A \to S^{-1}A$ is injective $\iff$ S does not contain zero divisors.*

Proof. ($\Longleftarrow$) If $i(a) = 0$ for some $a \neq 0$, then $(a, 1) \sim (0, 1) \implies ua = 0$ for some $u \in S \implies u \in S$ is a zero divisor. The converse is similar. □

Example 1.34. Let $\mathfrak{p} \subset A$ be a prime ideal and $S = A\backslash\mathfrak{p}$. Then S is a multiplicative set. Indeed, if $a, b \in S \implies a, b \notin \mathfrak{p} \implies ab \notin \mathfrak{p} \implies ab \in S$. We denote the ring $S^{-1}A$ by $A_\mathfrak{p}$ in this case. The set

$$\mathfrak{m}_\mathfrak{p} = S^{-1}\mathfrak{p} = \left\{ \frac{a}{s} \,\middle|\, a \in \mathfrak{p}, s \in S \right\} \subset A_\mathfrak{p}$$

is an ideal in $A_\mathfrak{p}$. Moreover, if $\frac{a}{s} \notin \mathfrak{m}_\mathfrak{p} \implies a \notin \mathfrak{p} \implies a \in S \implies \frac{a}{s}$ is invertible in $A_\mathfrak{p}$ with the inverse $\frac{s}{a}$. This implies that $A_\mathfrak{p}$ is a local ring and $\mathfrak{m}_\mathfrak{p}$ is its maximal ideal. The ring $A_\mathfrak{p}$ is called the *localization* of A at the prime ideal $\mathfrak{p}$. The residue field $\Bbbk_\mathfrak{p} = A_\mathfrak{p}/\mathfrak{m}_\mathfrak{p}$ is called the *residue field at* $\mathfrak{p}$. It is isomorphic to the field of fractions of the integral domain $A/\mathfrak{p}$ (we will show later that $A_\mathfrak{p}/\mathfrak{m}_\mathfrak{p} = S^{-1}A/S^{-1}\mathfrak{p} \simeq S^{-1}(A/\mathfrak{p})$).

Example 1.35. Let $f \in A$ and let $S = \{f^n \mid n \geq 0\}$. Then S is a multiplicative set. We denote $S^{-1}A$ by A_f in this case. The elements of A_f are of the form $\frac{a}{f^n}$ for some $a \in A$ and $n \geq 0$. Note that if f is nilpotent, then $0 \in S$ and $A_f = 0$.

Lemma 1.36 (Universal property)**.** *Let $f\colon A \to B$ be a ring homomorphism such that $f(s)$ is invertible $\forall s \in S$. Then there exists a unique ring homomorphism $\bar{f}\colon S^{-1}A \to B$ such that $f = \bar{f} \circ i$.*

Proof. Uniqueness: $\bar{f}(a/1) = \bar{f}i(a) = f(a) \implies \bar{f}(1/s) = f(s)^{-1} \implies \bar{f}(a/s) = f(a)/f(s)$. Existence: let $\bar{f}(a/s) = f(a)/f(s)$. □

Remark 1.37. Given an ideal $I \subset A$, its extension I^e with respect to $i\colon A \to S^{-1}A$ is given by

$$I^e = S^{-1}A \cdot i(I) = \left\{ \sum\nolimits_{k=1}^n \frac{a_k}{s_k} \,\middle|\, a_k \in I, s_k \in S \right\} = \left\{ \frac{a}{s} \,\middle|\, a \in I, s \in S \right\} = S^{-1}I.$$

Theorem 1.38. *There is a bijection between the set of prime ideals in $S^{-1}A$ and the set of prime ideals in A that don't intersect S:*

$$S^{-1}A \supset \mathfrak{q} \mapsto \mathfrak{q}^c = i^{-1}(\mathfrak{q}) \subset A, \qquad A \supset \mathfrak{p} \mapsto \mathfrak{p}^e = S^{-1}\mathfrak{p} \subset S^{-1}A.$$

Proof. We know that if $\mathfrak{q} \subset S^{-1}A$ is prime, then $\mathfrak{p} = i^{-1}(\mathfrak{q}) \subset A$ is also prime. If $s \in \mathfrak{p} \cap S$, then $i(s) \in \mathfrak{q}$ is invertible, hence $\mathfrak{q} = S^{-1}A$. This is a contradiction, hence $\mathfrak{p} \cap S = \varnothing$.

Conversely, let $\mathfrak{p} \subset A$ be prime and $\mathfrak{p} \cap S = \varnothing$. We claim that $S^{-1}\mathfrak{p} \subset S^{-1}A$ is prime. Indeed, $(S^{-1}A)/(S^{-1}\mathfrak{p}) = \bar{S}^{-1}(A/\mathfrak{p})$, where $\bar{S}$ is the image of S in $A/\mathfrak{p}$ (exercise). The quotient $A/\mathfrak{p}$ is an integral domain (as $\mathfrak{p}$ is prime), hence $\bar{S}^{-1}(A/\mathfrak{p})$ is also an integral domain. Therefore $S^{-1}\mathfrak{p} \subset S^{-1}A$ is prime.

Let us show that if $\mathfrak{q} \subset S^{-1}A$ is prime, then $\mathfrak{q}^{ce} = S^{-1}(\mathfrak{q}^c) = \mathfrak{q}$. We always have $\mathfrak{q}^{ce} \subset \mathfrak{q}$. If $a/s \in \mathfrak{q} \implies a/1 \in \mathfrak{q} \implies a \in \mathfrak{q}^c \implies a/s \in \mathfrak{q}^{ce}$. Therefore $\mathfrak{q}^{ce} = \mathfrak{q}$.

Let us show that if $\mathfrak{p} \subset A$ is prime and $\mathfrak{p} \cap S = \varnothing$, then $\mathfrak{p}^{ec} = (S^{-1}\mathfrak{p})^c = \mathfrak{p}$. We always have $\mathfrak{p} \subset \mathfrak{p}^{ec}$. If $a \in \mathfrak{p}^{ec}$, then $a/1 \in \mathfrak{p}^e = S^{-1}\mathfrak{p}$, hence $a/1 = b/s$ for some $b \in \mathfrak{p}$, $s \in S$. Therefore $(as - b)u = 0$ for some $u \in S$. This implies $a(su) = bu \in \mathfrak{p}$, hence $a \in \mathfrak{p}$ or $su \in \mathfrak{p}$. But $su \in S$ and $S \cap \mathfrak{p} = \varnothing$, hence $a \in \mathfrak{p}$. We conclude that $\mathfrak{p}^{ec} = \mathfrak{p}$. □

Corollary 1.39. *If $\mathfrak{p} \subset A$ is a prime ideal, then there is a $1-1$ correspondence between prime ideals of $A_\mathfrak{p}$ and prime ideals of A contained in $\mathfrak{p}$.*

Remark 1.40. The above bijection does not extend to arbitrary ideals in general. For example, consider the ring $A = \mathbb{Z}$, a prime ideal $\mathfrak{p} = 2\mathbb{Z}$ and the localization $A_\mathfrak{p}$. The element 3 is invertible in $A_\mathfrak{p}$, hence $(6\mathbb{Z})^e = (2\mathbb{Z})^e$. This means that ideals $6\mathbb{Z}$ and $2\mathbb{Z}$ (both contained in $\mathfrak{p}$) are mapped to the same ideal in $A_\mathfrak{p}$.

2. Modules

2.1. **Preliminaries.** We will assume the knowledge of the following notions:

(1) A module over a ring.
(2) A homomorphism between two modules.
(3) A submodule of a module and a quotient module.
(4) The kernel and the image of a homomorphism.

Let M be a module over a ring A.

Definition 2.1.

(1) For an ideal $I \subset A$ and a subset $N \subset M$, we define
$$IN = \left\{ \sum_i a_i x_i \,\middle|\, a_i \in I,\, x_i \in N \right\}$$
which is a submodule of M.
(2) Given submodules $L, N \subset M$, define $(L : N) = \{a \in A \,|\, aN \subset L\}$. It is an ideal of A.
(3) Define the *annihilator* of M to be $\operatorname{Ann} M = \operatorname{Ann}_A M = \{a \in A \,|\, aM = 0\}$.
(4) We will say that M is *faithful* if $\operatorname{Ann} M = 0$.

Remark 2.2.

(1) Let $I \subset A$ be an ideal and $M = A/I$. Then $\operatorname{Ann} M = I$.
(2) If $I \subset \operatorname{Ann} M$ is an ideal, then $IM = 0$ and M can be considered as a module over A/I.
(3) If $I = \operatorname{Ann} M$, then M is faithful as a module over A/I.

Definition 2.3. For a family $(M_i)_{i\in \mathcal{I}}$ of submodules of M, we define the *sum*
$$\sum_i M_i = \left\{ \sum_i x_i \,\middle|\, x_i \in M_i \right\},$$
where all but a finite number of x_i are zero. It is a submodule of M and it is the minimal submodule that contains all the M_i.

Remark 2.4. The intersection $\bigcap_i M_i$ is is the maximal submodule of M contained in all of the M_i.

Definition 2.5.

(1) For any $x \in M$, define $Ax = \{ax \,|\, a \in A\}$. It is a submodule of M.
(2) A module M is said to be generated by a family $(x_i)_{i\in\mathcal{I}}$ of elements in M if $M = \sum_i Ax_i$. The family $(x_i)_i$ is called the set of *generators* of M.
(3) A module M is said to be *finitely generated* if it has a finite set of generators. This means that the exist elements $x_1, \dots, x_n \in M$ such that
$$M = Ax_1 + \dots + Ax_n = \left\{ \sum_{i=1}^n a_i x_i \,\middle|\, a_i \in A\ \forall 1 \le i \le n \right\}.$$

Lemma 2.6 (*Nakayama's lemma*)**.** *Let M be a finitely generated A-module and $I \subset \mathcal{R}(A)$ be an ideal.*

(1) *If $IM = M$, then $M = 0$.*
(2) *If $M = IM + N$ for some submodule N, then $M = N$.*
(3) *If $f\colon N \to M$ is a homomorphism such that $\bar f\colon N/IN \to M/IM$ is surjective, then f is surjective.*

Proof. **(1)** Let $x_1, \dots, x_n$ be a minimal set of generators of M. Then $x_n \in M = IM$ implies $x_n = a_1x_1 + \dots + a_nx_n$ with $a_i \in I$. Therefore $(1 - a_n)x_n = a_1x_1 + \dots + a_{n-1}x_{n-1}$. We have $a_n \in \mathcal{R}(A) \implies 1 - a_n$ is invertible $\implies x_n$ is a linear combination of $x_1, \dots, x_{n-1} \implies M$ is generated by $x_1, \dots, x_{n-1}$, a contradiction to the minimality of n.
(2) If $M = IM + N$, then $M/N = (IM + N)/N = I(M/N) \implies M/N = 0 \implies M = N$.
(3) If $\bar f$ is surjective, then $f(N) + IM = M \implies f(N) = M$. □

Lemma 2.7. *Let* $(A, \mathfrak{m})$ *be a local ring and* M *be a finitely generated* A*-module. If the classes of* $x_1, \ldots, x_n \in M$ *form a basis of* $M/\mathfrak{m}M$ *over* $\Bbbk = A/\mathfrak{m}$*, then* $x_1, \ldots, x_n$ *generate* M *over* A*.*

Proof. Let $N \subset M$ be generated by $x_1, \ldots, x_n$ over A. Then the map $N \to M \to M/\mathfrak{m}M$ is surjective, hence $N + \mathfrak{m}M = M \implies N = M$ by Nakayama's lemma as $\mathfrak{m} = \mathcal{R}(A)$. □

2.2. **Direct sums and products.** Given two A-modules M, N, we define their direct sum $M \oplus N$ to be the set of all pairs (x, y) with $x \in M$ and $y \in N$ and with operations of addition and scalar multiplication

$$(x, y) + (x', y') = (x + x', y + y'), \qquad a \cdot (x, y) = (ax, ay), \qquad x, x' \in M,\ y, y' \in N, a \in A.$$

More generally

Definition 2.8. Let $(M_i)_{i \in \mathcal{I}}$ be a family of A-modules.

(1) Define their *direct sum* $\bigoplus_{i \in \mathcal{I}} M_i = \coprod_{i \in \mathcal{I}} M_i$ to be the set of families $(x_i \in M_i)_i$ with almost all $x_i = 0$ (i.e. all but a finite number).
(2) Define their *direct product* $\prod_{i \in \mathcal{I}} M_i$ to be the set of all families $(x_i \in M_i)_i$ (we allow infinitely many x_i to be nonzero).

These sets are equipped with an A-module structure using pointwise addition and scalar multiplication. Note that if $\mathcal{I}$ is finite, then $\bigoplus_i M_i = \prod_i M_i$.

Remark 2.9. For every $i \in \mathcal{I}$, we define a canonical inclusion

$$\alpha_i \colon M_i \to \bigoplus_j M_j, \qquad x_i \mapsto (0, \ldots, 0, x_i, 0, \ldots, 0)$$

and a canonical projection

$$\pi_i \colon \prod_j M_j \to M_i, \qquad (x_j)_j \mapsto x_i.$$

Lemma 2.10 (Universal properties)**.** *Let M and $(M_i)_{i \in \mathcal{I}}$ be a family of A-modules.*

(1) *Given a family of homomorphisms $(f_i \colon M_i \to M)_i$, there exists a unique homomorphism $\bar{f} \colon \bigoplus_i M_i \to M$ such that $\bar{f} \circ \alpha_i = f_i$.*
(2) *Given a family of homomorphisms $(f_i \colon M \to M_i)_i$, there exists a unique homomorphism $\bar{f} \colon M \to \prod_i M_i$ such that $\pi_i \circ \bar{f} = f_i$.*

Proof. **(1)** We define $\bar{f}((x_i)_i) = \sum_i f_i(x_i) \in M$ for all $(x_i)_i \in \bigoplus_i M_i$. It's not difficult to verify that this is a well-defined homomorphism (note that almost all $x_i = 0$ and the sum on the right is finite) which satisfies the required conditions.
(2) We define $\bar{f}(x) = (f_i(x))_i \in \prod_i M_i$ for all $x \in M$. It's not difficult to verify that this is a well-defined homomorphism which satisfies the required conditions. □

Definition 2.11.

(1) For every $n \geq 0$, we define $A^n = \prod_{i=1}^n A = \bigoplus_{i=1}^n A$, the direct sum of n copies of A.
(2) Given a set $\mathcal{I}$, define $A^{(\mathcal{I})} = \bigoplus_{i \in \mathcal{I}} A$, the direct sum of copies of A indexed by $\mathcal{I}$.
(3) A module M over a ring A is called *free* if it is isomorphic to $A^{(\mathcal{I})}$ for some set $\mathcal{I}$. Equivalently, M has a *basis* $(x_i)_{i \in \mathcal{I}}$, meaning that $(x_i)_{i \in \mathcal{I}}$ generates M and is linearly independent: if $\sum_i a_i x_i = 0$ for some $a_i \in A$, then $a_i = 0$ for all $i \in \mathcal{I}$.

Lemma 2.12. *A module M is finitely generated $\iff$ M is isomorphic to a quotient of A^n for some $n \geq 0$.*

Proof. **($\Longrightarrow$)** Assume that M is finitely generated and let $(x_i)_{i \in I}$ be a set of its generators. Consider the map

$$f \colon A^n \to M, \qquad (a_1, \ldots, a_n) \mapsto \sum_i a_i x_i \in M.$$

This map is surjective, hence $M \simeq A^n / \operatorname{Ker} f$.
($\Longrightarrow$) Under our assumptions there exists a surjective homomorphism $f \colon A^n \to M$ for some $n \geq 0$. Then the elements $x_i = f(e_i)$, where $e_i = (0, \ldots, 0, 1, 0, \ldots, 0) \in A^n$ for $1 \leq i \leq n$, generate M. □

2.3. **Hom and tensor product.** Given modules M, N over A, consider the set of all A-module homomorphisms

$$\operatorname{Hom}(M,N)=\operatorname{Hom}_A(M,N)=\{f\colon M\to N\mid f \text{ is a homomorphism}\}.$$

It has an A-module structure, where the sum and the scalar product are defined by the rules

$$(f+g)(x)=f(x)+g(x),\qquad (af)(x)=a\cdot f(x)\qquad \forall x\in M$$

for $f,g\in\operatorname{Hom}(M,N)$ and $a\in A$. The set of endomorphisms $\operatorname{End}(M)=\operatorname{Hom}(M,M)$ has a (non-commutative) ring structure, where the product is given by composition.

Remark 2.13. Homomorphisms $\alpha\colon M'\to M$ and $\beta\colon N\to N'$ induce maps

(1) $\alpha^*\colon \operatorname{Hom}(M,N)\to\operatorname{Hom}(M',N)$, $f\mapsto f\circ\alpha$,
(2) $\beta_*\colon \operatorname{Hom}(M,N)\to\operatorname{Hom}(M,N')$, $f\mapsto \beta\circ f$

which are again A-module homomorphisms.

We define the *tensor product* $M\otimes N=M\otimes_A N$ of two modules to be an A-module generated by elements of the form $x\otimes y$ for $x\in M$, $y\in N$ subject to the relations

(1) $(x+x')\otimes y=x\otimes y+x'\otimes y$ for $x,x'\in M$ and $y\in N$.
(2) $x\otimes(y+y')=x\otimes y+x\otimes y'$ for $x\in M$ and $y,y'\in N$.
(3) $a(x\otimes y)=(ax)\otimes y=x\otimes(ay)$ for $a\in A$, $x\in M$ and $y\in N$.

Remark 2.14. A general element of $M\otimes N$ can be written in the form $\sum_i x_i\otimes y_i$, where $x_i\in M$ and $y_i\in N$, although this representation is not unique. If $(x_i)_i$ and $(y_j)_j$ are families of generators of M, N respectively, then $x_i\otimes y_j$ generate $M\otimes N$.

Proposition 2.15 (Universal property)**.** *Let M, N be A-modules. Then*

(1) *The map $\phi\colon M\times N\to M\otimes N$, $(x,y)\mapsto x\otimes y$ is A-bilinear.*
(2) *For any A-module L and any A-bilinear map $f\colon M\times N\to L$, there exists a unique A-linear map $\bar f\colon M\otimes N\to L$ such that $f=\bar f\circ g$.*

Proof. **(1)** We have

(1) $\phi(x+x',y)=(x+x')\otimes y=x\otimes y+x'\otimes y=\phi(x,y)+\phi(x',y)$.
(2) $\phi(ax,y)=(ax)\otimes y=a(x\otimes y)=a\phi(x,y)$.

Other axioms of bilinearity are verified in the same way.
(2) Uniqueness follows from the fact that $\bar f(x\otimes y)=\bar f\phi(x,y)=f(x,y)$ and elements $x\otimes y$ generate $M\otimes N$. For the existence we verify that that the map $\bar f$ given by $\bar f(x\otimes y)=f(x,y)$ satisfies all the required properties. □

Remark 2.16. Homomorphisms $\alpha\colon M\to M'$ and $\beta\colon N\to N'$ induce a homomorphism

$$\alpha\otimes\beta\colon M\otimes N\to M'\otimes N',\qquad x\otimes y\mapsto\alpha(x)\otimes\beta(y).$$

In particular, there is a homomorphism $\alpha\otimes 1\colon M\otimes N\to M'\otimes N$, $x\otimes y\mapsto\alpha(x)\otimes y$.

Lemma 2.17. *We have*

(1) $\operatorname{Hom}(A,M)\simeq M$.
(2) $A\otimes M\simeq M$.
(3) $M\otimes N\simeq N\otimes M$.
(4) $L\otimes(M\otimes N)\simeq(L\otimes M)\otimes N$.
(5) $(L\oplus M)\otimes N\simeq(L\otimes N)\oplus(M\otimes N)$.

Lemma 2.18 (Tensor-Hom adjunction)**.** *Given modules L,M,N, there is a natural isomorphism*

$$\operatorname{Hom}(L\otimes M,N)\simeq\operatorname{Hom}(L,\operatorname{Hom}(M,N)).$$

Proof. Given $f\colon L\otimes M\to N$, define $f'\colon L\to\operatorname{Hom}(M,N)$ by the rule

$$f'(l)(m)=f(l\otimes m).$$

Conversely, given $f'\colon L\to\operatorname{Hom}(M,N)$, define $f''\colon L\times M\to N$ by the rule $f(l,m)=f'(l)(m)$. It is easy to see that f is A-bilinear, hence it factors through $f\colon L\otimes M\to N$. □

Definition 2.19 (Restriction and extension of scalars)**.** Let $f\colon A \to B$ be a ring homomorphism.

(1) Given a B-module N, we can equip it with an A-module structure by the rule $ax = f(a)x$ for $a \in A$, $x \in N$. It is said to be obtained from N by *restriction of scalars*. In particular, the ring B is equipped with an A-module structure. We call B an A-*algebra* in this situation.

(2) Given an A-module M, we can equip $M_B = B \otimes_A M$ with a B-module structure by the rule $b(b' \otimes x) = (bb') \otimes x$ for $b, b' \in B$ and $x \in M$. It is said to be obtained from M by *extension of scalars*.

Example 2.20. Consider a natural projection $\pi\colon A = \mathbb{Z} \to B = \mathbb{Z}/2\mathbb{Z}$ and consider a $\mathbb{Z}$-module $M = \mathbb{Z}/3\mathbb{Z}$. Then $M_B = B \otimes_A M = (\mathbb{Z}/2\mathbb{Z}) \otimes_{\mathbb{Z}} (\mathbb{Z}/3\mathbb{Z}) = 0$.

Lemma 2.21. *We have $M_B \otimes_B N_B \simeq (M \otimes N)_B$.*

Proof.

$$M_B \otimes_B (N_B) \simeq M \otimes_A B \otimes_B B \otimes_A N \simeq M \otimes_A B \otimes_A N \simeq (M \otimes N)_B$$

as $B \otimes_B B \simeq B$. □

Lemma 2.22. *Given an A-module M and a B-module N, we have*

$$\mathrm{Hom}_B(M_B, N) \simeq \mathrm{Hom}_A(M, N).$$

Proof. By the adjunction isomorphism

$$\mathrm{Hom}_B(M_B, N) = \mathrm{Hom}_B(B \otimes_A M, N) \simeq \mathrm{Hom}_A(M, \mathrm{Hom}_B(B, N)) \simeq \mathrm{Hom}_A(M, N)$$

as $\mathrm{Hom}_B(B, N) \simeq N$. □

2.4. **Exact sequences.**

Definition 2.23.

(1) A sequence of modules and homomorphisms
$$\dots \to M_{i-1} \xrightarrow{d_{i-1}} M_i \xrightarrow{d_i} M_{i+1} \to \dots$$
is called a (cochain) *complex* if $d_i \circ d_{i-1} = 0$ for all i. This is equivalent to the requirement $\operatorname{Im} d_{i-1} \subset \operatorname{Ker} d_i$.

(2) The complex is said to be *exact* at M_i if $\operatorname{Im} d_{i-1} = \operatorname{Ker} d_i$. The complex (or sequence) is called exact if it is exact at every M_i.

Lemma 2.24.

(1) $0 \to M \xrightarrow{f} N$ *is exact (at* M*)* $\iff$ f *is injective.*

(2) $M \xrightarrow{g} N \to 0$ *is exact (at* N*)* $\iff$ g *is surjective.*

(3) *A complex* $0 \to L \xrightarrow{f} M \xrightarrow{g} N \to 0$ *is exact* $\iff$ f *is injective,* g *is surjective and induces an isomorphism* $g\colon M/\operatorname{Im} f \to N$*. Such sequence is called a short exact sequence.*

Proof. **(3)** If the sequence is exact, then f is injective by (1) and g is surjective by (2). We also have $\operatorname{Im} f = \operatorname{Ker} g$, hence $N \simeq M/\operatorname{Ker} g = M/\operatorname{Im} f$. Conversely, we get injectivity of f by (1) and surjectivity of g by (2). Finally, we have $\operatorname{Im} f = \operatorname{Ker}(M \to M/Imf) = \operatorname{Ker}(M \to N) = \operatorname{Ker} g$. $\square$

Lemma 2.25.

(1) *A complex*
$$0 \to M_1 \to M_2 \to M_3$$
is exact $\iff$ *for any module* N *the following sequence is exact*
$$0 \to \operatorname{Hom}(N, M_1) \to \operatorname{Hom}(N, M_2) \to \operatorname{Hom}(N, M_3)$$

(2) *A complex*
$$M_1 \to M_2 \to M_3 \to 0$$
is exact $\iff$ *for any module* N *the following sequence is exact*
$$0 \to \operatorname{Hom}(M_3, N) \to \operatorname{Hom}(M_2, N) \to \operatorname{Hom}(M_1, N).$$

(3) *If a complex*
$$M_1 \to M_2 \to M_3 \to 0$$
is exact, then for any module N*, the following complex is exact*
$$M_1 \otimes N \to M_2 \otimes N \to M_3 \otimes N \to 0$$

Proof. **(2)** Consider an exact sequence $M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3 \to 0$ and the corresponding sequence
$$0 \to \operatorname{Hom}(M_3, N) \xrightarrow{g^*} \operatorname{Hom}(M_2, N) \xrightarrow{f^*} \operatorname{Hom}(M_1, N).$$
If $\phi \in \operatorname{Hom}(M_3, N)$ is mapped to zero $\implies$ $g^*(\phi) = \phi g = 0$. But g is surjective $\implies$ $\phi = 0$. This means that $\operatorname{Ker} g^* = 0$. If $\phi \in \operatorname{Hom}(M_2, N)$ is mapped to zero $\implies$ $f^*(\phi) = \phi f = 0$ $\implies$ $\phi(\operatorname{Im} f) = 0$ $\implies$ $\phi\colon M_2 \to N$ factorizes through $\bar\phi\colon M_2/\operatorname{Im} f \to N$. But $M_2/\operatorname{Im} f = M_2/\operatorname{Ker} g \simeq M_3$ and we obtain $\bar\phi\colon M_3 \to N$ satisfying $g^*(\bar\phi) = \phi$. This implies $\operatorname{Ker} f^* = \operatorname{Im} g^*$.

The converse statement is proved similarly.

(3) According to (2), the required complex is exact $\iff$ for any module L, the complex
$$0 \to \operatorname{Hom}(M_3 \otimes N, L) \to \operatorname{Hom}(M_2 \otimes N, L) \to \operatorname{Hom}(M_1 \otimes N, L)$$
is exact. Using the isomorphism $\operatorname{Hom}(M \otimes N, L) \simeq \operatorname{Hom}(M, \operatorname{Hom}(N, L))$, we can rewrite the above complex as
$$0 \to \operatorname{Hom}(M_3, L') \to \operatorname{Hom}(M_2, L') \to \operatorname{Hom}(M_1, L'),$$
where $L' = \operatorname{Hom}(N, L)$. The latter complex is exact by (2). $\square$

Remark 2.26. Using categories and functors we can interpret the above result by saying that

(1) The functor $\operatorname{Hom}(N, -)\colon \operatorname{Mod} A \to \operatorname{Mod} A$ is left exact.

(2) The contravariant functor $\operatorname{Hom}(-, N)\colon \operatorname{Mod} A \to \operatorname{Mod} A$ is left exact.

(3) The functor $-\otimes N\colon \operatorname{Mod} A \to \operatorname{Mod} A$ is right exact.

Example 2.27. Let $A = \mathbb{Z}$ and $N = \mathbb{Z}/2\mathbb{Z}$. Then $\operatorname{Hom}(N, -)$ does not preserve exactness. For example, we can apply it to the short exact sequence

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

and observe that $\operatorname{Hom}(N, \mathbb{Z}) = 0$ and $\operatorname{Hom}(N, N) = N$.

Similarly, $N \otimes -$ does not preserve exactness. We can apply $N \otimes -$ to the above sequence and obtain a sequence

$$0 \to N \xrightarrow{0} N \to N \to 0$$

which is not exact on the left.

2.5. **Projective and flat modules.**

Definition 2.28.
(1) A module P is called *projective* if $\operatorname{Hom}(P, -)$ preserves exact sequences.
(2) A module P is called *flat* if $P \otimes -$ preserves exact sequences.

Lemma 2.29. *FAE*
(1) *P is projective.*
(2) *$\operatorname{Hom}(P, -)$ preserves short exact sequences.*
(3) *If $f\colon M \to N$, $g\colon P \to N$ are homomorphisms and f is surjective, then there exists $h\colon P \to M$ such that $g = fh$*

$$\begin{array}{ccc} & & P \\ & \overset{h}{\swarrow} & \downarrow g \\ M & \xrightarrow[f]{} & N \end{array}$$

(4) *Every surjective homomorphism $f\colon M \to P$ splits, that is, there exists $s\colon P \to M$ such that $fs = 1_P$.*
(5) *P is a direct summand of a free module.*

Proof. **(1) $\Longrightarrow$ (2).** is clear.
(2) $\Longrightarrow$ (1). follows from the fact that we can split every exact sequence

$$\cdots \to M_{i-1} \xrightarrow{d_{i-1}} M_i \to M_{i+1} \xrightarrow{d_i} \dots$$

into short exact sequences

$$0 \to K_i \to M_i \to K_{i+1} \to 0,$$

where $K_i = \operatorname{Ker} d_i$ and $K_{i+1} = \operatorname{Ker} d_{i+1} = \operatorname{Im} d_i$.
(2) $\Longrightarrow$ (3). Given a surjective $f\colon M \to N$, we consider a short exact sequence

$$0 \to \operatorname{Ker} f \to M \xrightarrow{f} N \to 0$$

Then $f_*\colon \operatorname{Hom}(P, M) \to \operatorname{Hom}(P, N)$ is surjective, in particular $\exists h \in \operatorname{Hom}(P, M)$ such that $g = f_*(h) = fh$.
(3) $\Longrightarrow$ (4). Considering $g = 1_P$, we can find $h\colon P \to M$ such that $fh = g = 1_P$.
(4) $\Longrightarrow$ (5). Let $(x_i)_{i \in \mathcal{I}}$ be a set of generators of P. Then there exists a surjective homomorphism $f\colon F = A^{(\mathcal{I})} \to P$, $e_i \mapsto x_i$. By assumption, there exists $s\colon P \to F$ such that $fs = 1_P$. We claim that $F = \operatorname{Im} s \oplus \operatorname{Ker} f$. If $x \in \operatorname{Im} s \oplus \operatorname{Ker} f$, then $x = s(y)$ and $f(x) = 0 \implies y = fs(y) = f(x) = 0 \implies x = 0$. On the other for every $x \in F$, consider $x' = sf(x)$. Then $x' \in \operatorname{Im} S$ and $f(x - x') = f(x) - f(x) = 0$, hence $x - x' \in \operatorname{Ker} f$. Finally, note that $P \simeq \operatorname{Im} s$ as $s\colon P \to F$ is injective. Therefore $F \simeq P \oplus \operatorname{Ker} f$.
(5) $\Longrightarrow$ (1). Note that $\operatorname{Hom}(A, M) \simeq M$, hence $\operatorname{Hom}(A, -)$ preserves exactness. Similarly, we have $\operatorname{Hom}(A^{(\mathcal{I})}, M) \simeq M^{\mathcal{I}}$, hence $\operatorname{Hom}(A^{(\mathcal{I})}, -)$ preserves exactness. This implies that for every direct summand P of $A^{(\mathcal{I})}$, $\operatorname{Hom}(P, -)$ preserves exactness. □

Lemma 2.30. *FAE*
(1) *P is flat.*
(2) *$P \otimes -$ preserves short exact sequences.*
(3) *If $f\colon M \to N$ is injective, then $f \otimes 1\colon P \otimes M \to P \otimes N$ is injective.*

Lemma 2.31. *Every projective module is flat.*

Proof. If P is projective, then P is a direct summand of a free module (assume for simplicity that it is finitely generated), say A^n. We have $A^n \otimes M \simeq M^n$, hence $A^n \otimes -$ preserves exactness. This implies that P also preserves exactness. □

2.6. **Localization of modules.** Let $S \subset A$ be a multiplicative system and let M be an A-module. Define an equivalence relation on $M \times S$ by the rule

$$(m, s) \sim (m', t) \iff \exists u \in S\colon\ u(tm - sm') = 0$$

We denote an equivalence class of (m, s) by $\frac{m}{s} = m/s$ and denote the set of all equivalence classes by $S^{-1}M$. It can be equipped with a structure of an $S^{-1}A$-module in an obvious way.

Remark 2.32.

(1) If $\mathfrak{p} \subset A$ is prime and $S = A\backslash\mathfrak{p}$, we denote $S^{-1}M$ by $M_{\mathfrak{p}}$.
(2) If $f \in A$ and $S = \{f^n\}_{n\ge 0}$, we denote $S^{-1}M$ by M_f.

Lemma 2.33. *The map*

$$f\colon S^{-1}A \otimes_A M \to S^{-1}M, \qquad \frac{a}{s} \otimes m \mapsto \frac{am}{s}$$

is well-defined and is an isomorphism of $S^{-1}A$-modules.

Proof. One can see that the map

$$S^{-1}A \times M \to S^{-1}M, \qquad \left(\frac{a}{s}, m\right) \mapsto \frac{am}{s}$$

is A-bilinear, hence induces the required homomorphism f. It is clear that f is surjective. Let $\sum_i \frac{a_i}{s_i} \otimes m_i \in \operatorname{Ker} f$. We can bring it to the form $\frac{1}{s} \otimes m$. As $f\big(\frac{1}{s} \otimes m\big) = \frac{m}{s} = 0$, there exists $u \in S$ such that $um = 0$. But then

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

This implies that f is injective, hence is an isomorphism. □

Lemma 2.34. *The operation S^{-1} preserves exact sequences.*

Proof. Consider an exact sequence $L \xrightarrow{f} M \xrightarrow{g} N$ and the corresponding sequence

$$S^{-1}L \xrightarrow{f'} S^{-1}M \xrightarrow{g'} S^{-1}N$$

We have $gf = 0 \implies$ hence $g'f' = 0 \implies \operatorname{Im}(f') \subset \operatorname{Ker}(g')$. If $m/s \in \operatorname{Ker}(g') \implies g(m)/s = 0$ in $S^{-1}N \implies \exists u \in S,\ ug(m) = 0$ in $N \implies g(um) = 0 \implies um \in \operatorname{Ker} g = \operatorname{Im} f \implies um = f(m')$ for some $m' \in L \implies m/s = f(m')/us = f'(m'/us) \in \operatorname{Im}(f')$. This proves that $\operatorname{Ker}(g') = \operatorname{Im}(f')$. □

Corollary 2.35. *$S^{-1}A$ is a flat A-module.*

Example 2.36. The last corollary implies that $\mathbb{Q}$ is a flat module over $\mathbb{Z}$. On the other hand $\mathbb{Q}$ is not projective: otherwise it is a direct summand of a free module, hence there is an injective map $f\colon \mathbb{Q} \to \mathbb{Z}^{(I)}$ for some set I. Let $f(1) = (x_i)_{i\in I} \in \mathbb{Z}^{(I)}$ and let $n = \max_i |x_i| + 1$. If $f(1/n) = (y_i)_{i\in I}$, then $(x_i)_i = nf(1/n) = (ny_i)_i$. But $|ny_i| > |x_i|$ whenever $y_i \ne 0$. A contradiction.

Lemma 2.37. *Let M be an A module. Then FAE*

(1) $M = 0$.
(2) $M_{\mathfrak{p}} = 0$ *for every prime ideal* $\mathfrak{p} \subset A$.
(3) $M_{\mathfrak{m}} = 0$ *for every maximal ideal* $\mathfrak{m} \subset A$.

Proof. **(1)** $\implies$ **(2)** $\implies$ **(3)** is clear.

Assume that $M_{\mathfrak{m}} = 0$ for every maximal ideal $\mathfrak{m} \subset A$ and $M \ne 0$. Let $0 \ne x \in M$ and $I = \operatorname{Ann}(A)$. Then I is a proper ideal ($1 \cdot x = x \ne 0 \implies 1 \notin I$), hence it is contained in a maximal ideal $\mathfrak{m}$. Since $x/1 = 0$ in $M_{\mathfrak{m}}$, there exists some $u \in A\backslash\mathfrak{m}$ such that $ux = 0$. But then $u \in \operatorname{Ann} x = I \subset \mathfrak{m}$. A contradiction. □

Lemma 2.38. *Let $f\colon M \to N$ be a module homomorphism. Then FAE*

(1) f *is injective/surjective.*
(2) $f_{\mathfrak{p}}\colon M_{\mathfrak{p}} \to N_{\mathfrak{p}}$ *is injective/surjective for every prime ideal* $\mathfrak{p} \subset A$.
(3) $f_{\mathfrak{m}}\colon M_{\mathfrak{m}} \to N_{\mathfrak{m}}$ *is injective/surjective for every maximal ideal* $\mathfrak{m} \subset A$.

Proof. **(1) $\Longrightarrow$ (2).** As localization preserves exact sequences.
(2) $\Longrightarrow$ (3). As every maximal ideal is prime.
(3) $\Longrightarrow$ (1). Assume that $f_{\mathfrak{m}}$ is injective for every maximal ideal $\mathfrak{m}$. Let $L = \operatorname{Ker} f$ and consider an exact sequence $0 \to L \to M \xrightarrow{f} N$. For every maximal ideal $\mathfrak{m}$, the corresponding sequence $0 \to L_{\mathfrak{m}} \to M_{\mathfrak{m}} \xrightarrow{f_{\mathfrak{m}}} N_{\mathfrak{m}}$ is exact $\Longrightarrow$ $L_{\mathfrak{m}} \simeq \operatorname{Ker} f_{\mathfrak{m}} = 0$ as $f_{\mathfrak{m}}$ is injective. This implies that $L = 0$, hence f is injective. The proof for surjectivity is similar. $\square$

3. Chain conditions

3.1. Noetherian rings and modules.

Definition 3.1. Let A be a ring.

(1) An A-module M is called *Noetherian* if every submodule of M is finitely generated.
(2) The ring A is called *Noetherian* if it is Noetherian as a module over itself.

Example 3.2.

(1) A PID A is Noetherian. Indeed, every submodule of A is an ideal, hence a principal ideal, generated by one element.
(2) In particular, the algebra of polynomials $\Bbbk[x]$ over a field $\Bbbk$ is Noetherian. We will see later that $\Bbbk[x_1, \ldots, x_n]$ is also Noetherian. As well as $\Bbbk[x_1, \ldots, x_n]/I$ for every ideal I.

Lemma 3.3. *Let M be an A-module. The following conditions are equivalent*

(1) *Every submodule of M is finitely generated.*
(2) *Every increasing chain of submodules*
$$M_1 \subset M_2 \subset \ldots \subset M$$
stabilizes, that is, $M_n = M_{n+1} = \ldots$ for some $n > 0$.

Proof. **(1) $\Longrightarrow$ (2).** Consider an increasing chain
$$M_1 \subset M_2 \subset \ldots \subset M$$
and let $N = \cup_{n\geq 1} M_n \subset M$. Then N is a submodule of M and by assumption it is finitely generated. Let $x_1, \ldots, x_k$ be generators of N. Then $x_i \in M_{n_i}$ for some $n_i \geq 1$. Taking $n = \max_i n_i$, we obtain $x_i \in M_n$ for all i, hence $N \subset M_n$ and $M_n = M_{n+1} = \ldots$.
(2) $\Longrightarrow$ (1). Let us show that a submodule $N \subset M$ is finitely generated. Choose $x_0 = 0 \in N$ and, assuming that elements $x_0, \ldots, x_k \in N$ are constructed, let $M_k \subset N$ be the module generated by them. If $M_k = N$, then N is finitely generated and we are done. If $M_k \neq N$, we let $x_{k+1} \in N \backslash M_k$ and continue the process. In this way we obtain a chain of modules
$$M_1 \subset M_2 \subset \ldots \subset N \subset M$$
with $M_k \neq M_{k+1}$ for all $k \geq 1$. A contradiction. □

Definition 3.4. Let A be a ring.

(1) An A-module M is called *Artin* if every decreasing chain of submodules
$$M \supset M_1 \supset M_2 \supset \ldots$$
stabilizes, that is, $M_n = M_{n+1} = \ldots$ for some $n > 0$.
(2) The ring A is called *Artin* if it is Artin as a module over itself.

We will see later that every Artin ring is automaticaly Noetherian.

Example 3.5.

(1) The algebra $\Bbbk[x_1, x_2, \ldots]$ is neither Noetherian nor Artin. Indeed, it contains chains of ideals
$$(x_1) \subset (x_1, x_2) \subset \ldots, \qquad (x_1, x_2, \ldots) \supset (x_2, \ldots) \supset \ldots.$$
(2) The algebra $\Bbbk[x]$ is not Artinian: $(x) \supset (x^2) \supset \ldots$.
(3) A vector space over a field is Noetherian $\iff$ it is Artin $\iff$ it is finite-dimensional.
(4) Let $p \in \mathbb{Z}$ be a prime number and let $\mathbb{Z}_p = \{m/p^n \mid m \in \mathbb{Z}, n \geq 0\} \subset \mathbb{Q}$ be the corresponding localization. One can show that the $\mathbb{Z}$-module $\mathbb{Z}_p/\mathbb{Z}$ is Artin, but not Noetherian. To see this one should verify that the only proper submodules of $\mathbb{Z}_p/\mathbb{Z}$ are of the form $M_n = \{[m/p^n] \mid m \in \mathbb{Z}\}$ for $n \geq 0$.

Lemma 3.6. *Let M be an A-module and $L \subset M$ be a submodule. Then M is Noetherian $\iff$ L and M/L are Noetherian.*

Proof. First proof. Assume that M is Noetherian. Every increasing chain in L is a chain in M, hence stabilizes. Given an increasing chain $(M'_n)_n$ in M/L, we consider the chain $(\pi^{-1}(M'_n))_n$ in M, where $\pi\colon M \to M/L$ is the projection. Then $(\pi^{-1}(M'_n))_n$ stabilizes, hence $(M'_n)_n$ also stabilizes as $M'_n = \pi(\pi^{-1}(M'_n))$. Assume now that L and M/L are Noetherian and let $(M_n)_n$ be an increasing chain in M. Then the chain of modules

$$\pi(M_n) = (M_n + L)/L$$

stabilizes in M/L and the chain of modules $M_n \cap L$ stabilizes in L. Therefore there exists $n \geq 0$ such that $M_n + L = M_m + L$ and $M_n \cap L = M_m \cap L$ for all $m \geq n$. This implies that the inclusion $M_n \subset M_m$ is equality (hence the chain stabilizes) as otherwise $\exists x \in M_m \backslash M_n \implies x \in M_m \subset M_n + L \implies x = y + l$ for some $y \in M_n$, $l \in L \implies x - y = l \in M_m \cap L = M_n \cap L \implies x \in M_n$, a contradiction.

Second proof. Let M be Noetherian. If $N \subset L$ is a submodule, then $N \subset M$, hence N is finitely generated and L is Noetherian. Let $N \subset M/L$ be a submodule and let $\pi\colon M \to M/L$ be the projection. The module $N' = \pi^{-1}(N) \subset M$ is finitely generated, hence also $N = \pi(N')$ is finitely generated and M/L is Noetherian.

Assume that L and M/L are Noetherian and let $N \subset M$. Then $N \cap L \subset L$ is finitely generated and $N/(N \cap L) \simeq (N + L)/L \subset M/L$ is finitely generated. This implies that N is also finitely generated. □

Corollary 3.7. *If M, N are Noetherian A-modules, then $M \oplus N$ is also Noetherian.*

Proof. Let $M' = M \oplus N$. Then $N \subset M'$ and $M'/N \simeq M$ are Noetherian. We conclude that M' is Noetherian. □

Corollary 3.8. *If A is a Noetherian ring and M is a finitely generated A-module, then M is Noetherian.*

Proof. Let M have a generator set $(x_1, \ldots, x_n)$. Then there is a surjection $f\colon A^n \to M$, $(a_i)_i \mapsto \sum_i a_i x_i$. The module A^n is Noetherian by Cor. 3.7. Therefore the module $M \simeq A^n/\operatorname{Ker} f$ is Noetherian by Lemma 3.6. □

Lemma 3.9. *Let M be a Noetherian module over A and $S \subset A$ be a multiplicative set. Then $S^{-1}M$ is Noetherian over $S^{-1}A$.*

Proof. Consider the map $i\colon M \to S^{-1}M$, $x \mapsto x/1$. For any submodule $N \subset S^{-1}M$, let $L = i^{-1}(N) \subset M$. It is Noetherian, hence has generators $x_1, \ldots, x_n$ over A. We claim that $x_1/1, \ldots, x_n/1$ generate N over $S^{-1}A$. For any $x/s \in N$, we have $x/1 = s \cdot x/s \in N$, hence $x \in L$. Therefore $x = \sum_i a_i x_i$ for some $a_i \in A$. This implies that $\frac{x}{s} = \sum_i \frac{a_i}{s}\frac{x_i}{1}$. □

Theorem 3.10 (*Hilbert's basis theorem*)**.** *If A is noetherian, then $A[x]$ is noetherian.*

Proof. Let $I \subset A[x]$ be an ideal. For any $f \in A[x]$, let $\operatorname{lc}(f)$ be its leading coefficient. The set $J = \{\operatorname{lc}(f) \mid f \in I\}$ is an ideal in A. As A is noetherian, J is finitely generated, say by elements $a_1, \ldots, a_n$. For every $1 \leq i \leq n$, choose $f_i \in I \subset A[x]$ such that $a_i = \operatorname{lc}(f_i)$ and let $r_i = \deg f_i$. Let $I' = (f_1, \ldots, f_n) \subset I$ and let $r = \max\{r_1, \ldots, r_n\}$. For any $f \in I$, if $m = \deg f \geq r$, consider $a = \operatorname{lc}(f) \in J$ and write $a = \sum_i b_i a_i$ for some $b_i \in A$. Then $f - \sum_i b_i f_i x^{m-r_i}$ has degree $< m$ and is still in I. Note that $\sum_i b_i f_i x^{m-r_i} \in I'$. Proceeding in this way, we obtain a decomposition $f = g + h$, where $\deg g < r$ and $h \in I'$.

Let $M \subset A[x]$ be an A-module generated by $1, x, \ldots, x^{r-1}$. Then $g \in M$ and $g = f - h \in I \implies g \in M \cap I$. We proved that $I = (M \cap I) + I'$. As M is finitely generated over A, it is noetherian $\implies M \cap I$ is finitely generated over A. We also know that $I' = (f_1, \ldots, f_n)$ is finitely generated over $A[x]$. This implies that $I = (M \cap I) + I'$ is finitely generated over $A[x]$. We conclude that $A[x]$ is Noetherian. □

Definition 3.11. Let B be an A-algebra (this means that $A \subset B$ or more generally, we are given a ring homomorphism $\phi\colon A \to B$). We say that B is a *finitely generated* A-algebra if there exists a finite set of elements $b_1, \ldots, b_n \subset B$ such that every element in B can be written in the form $f(b_1, \ldots, b_n)$ for some polynomial $f \in A[x_1, \ldots, x_n]$.

Remark 3.12.

(1) Note that there is a surjective ring homomorphism $A[x_1, \dots, x_n] \to B$, $f \mapsto f(b_1, \dots, b_n)$, hence $B \simeq A[x_1, \dots, x_n]/\operatorname{Ker} f$. Conversely, if $B = A[x_1, \dots, x_n]/I$ for some ideal I, then B is a finitely-generated A-algebra.

(2) Note that $\Bbbk[x_1, \dots, x_n]$ is a finitely-generated $\Bbbk$-algebra, but not a finitely-generated $\Bbbk$-module.

Corollary 3.13. *If A is a Noetherian ring and B is a finitely-generated A-algebra, then B is also Noetherian.*

Proof. There is a surjective ring homomorphism $A[x_1, \dots, x_n] \to B$. By the Hilbert's basis theorem, the ring $A[x_1, \dots, x_n]$ is Noetherian, therefore its quotient is also Noetherian. □

Definition 3.14. A *minimal prime ideal* over an ideal $I \subset A$ is a prime ideal $I \subset \mathfrak{p} \subset A$ minimal among all prime ideals that contain I.

Lemma 3.15 (Noether)**.** *If A is Noetherian and $I \subset A$ is an ideal, then there are only finitely many minimal prime ideals over I (and every prime ideal over I contains one of them). In particular, $\sqrt{I}$ is a finite intersection of prime ideals.*

Proof. Assume that the statement is wrong and let I be a maximal ideal among all ideals that do not satisfy the required condition (it exists as A is Noetherian). Then I is not prime, hence $\exists a, b \notin I$ such that $ab \in I$. Ideals (I, a) and (I, b) are strictly greater than I, hence there are finitely many minimal primes over them. We have $Z(I, a) \cup Z(I, b) \subset Z(I)$. On the other hand, if $\mathfrak{p} \supset I$ is prime, then $ab \in \mathfrak{p} \implies a \in \mathfrak{p}$ or $b \in \mathfrak{p} \implies \mathfrak{p} \in Z(I, a)$ or $\mathfrak{p} \in Z(I, b)$. Therefore $Z(I) = Z(I, a) \cup Z(I, b)$ and minimal prime ideals over I are contained in the union of (finitely many) minimal primes over (I, a) and minimal primes over (I, b). □

3.2. **Artin rings.** Our goal in this section is to get a better understanding of Artin rings and to show that they are always Noetherian.

Lemma 3.16. *In an Artin ring every prime ideal is maximal.*

Proof. Let A be an Artin ring and $\mathfrak{p} \subset A$ be a prime ideal. Then $B = A/\mathfrak{p}$ is an Artin integral domain. For every nonzero $x \in B$, the chain $(x) \supset (x^2) \supset \dots$ stabilzes $\implies (x^n) = (x^{n+1})$ for some $n \geq 1 \implies x^n = x^{n+1}y$ for some $y \in B \implies xy = 1$ and x is invertible. This implies that B is a field and $\mathfrak{p} \subset A$ is maximal. □

Lemma 3.17. *In an Artin ring there are only finitely many maximal ideals.*

Proof. Given an infinite sequence of different maximal ideals $\mathfrak{m}_1, \mathfrak{m}_2, \dots$, consider a decreasing chain of ideals $I_n = \mathfrak{m}_1 \cap \dots \cap \mathfrak{m}_n$ for $n \geq 1$. This chain stabilizes, hence $\mathfrak{m}_1 \cap \dots \cap \mathfrak{m}_n = \mathfrak{m}_1 \cap \dots \cap \mathfrak{m}_n \cap \mathfrak{m}_{n+1} \implies \mathfrak{m}_1 \cap \dots \cap \mathfrak{m}_n \subset \mathfrak{m}_{n+1}$. This implies that $\mathfrak{m}_i \subset \mathfrak{m}_{n+1}$ for some $1 \leq i \leq n$ (otherwise $\exists a_i \in \mathfrak{m}_i \backslash \mathfrak{m}_{n+1}$, $1 \leq i \leq n \implies \prod_{i=1}^n a_i \in \cap_{i=1}^n \mathfrak{m}_i \backslash \mathfrak{m}_{n+1}$ as $\mathfrak{m}_{n+1}$ is prime). But $\mathfrak{m}_i \subset \mathfrak{m}_{n+1}$, implies $\mathfrak{m}_i = \mathfrak{m}_{n+1}$, a contradiction. □

Lemma 3.18. *In an Artin ring the Nilradical is equal to the Jacobson radical and is nilpotent.*

Proof. The nilradical $J = \mathcal{N}(A)$ is equal to $\mathcal{R}(A)$ as every prime ideal is maximal. By the assumption, the chain $J \supset J^2 \supset \dots$ stabilizes, hence $J^n = J^{n+1}$ for some $n \geq 0$. Assume that $J^n \neq 0$ and let $I \subset A$ be the minimal ideal such that $I \cdot J^n \neq 0$. It exists by our assumption on decreasing chains. For any $x \in I$ with $xJ^n \neq 0$, we have $I = Ax$ by minimality of I, hence I is finitely-generated. Moreover, $JI \cdot J^n = IJ^{n+1} = IJ^n \neq 0$, hence $JI = I$ by minimality of I. By Nakayama's lemma, we conclude that $I = 0$, a contradiction to $IJ^n \neq 0$. □

Lemma 3.19. *Let $(\mathfrak{m}_1, \dots, \mathfrak{m}_n)$ be a sequence of maximal ideals in A such that $\prod_i \mathfrak{m}_i = 0$. Then A is Artin $\iff$ A is Noetherian.*

Proof. Assume that A is Artin. Consider a chain of ideals

$$A = I_0 \supset I_1 \supset \dots \supset I_n = 0,$$

where $I_i = \mathfrak{m}_1 \dots \mathfrak{m}_i$ for $0 \leq i \leq n$. As A is Artin, we conclude that I_i and I_{i-1}/I_i are Artin over A. Each factor $I_{i-1}/I_i = I_{i-1}/\mathfrak{m}_i I_{i-1}$ is a vector space over a field $A/\mathfrak{m}_i$. It is finite-dimensional over $A/\mathfrak{m}_i$ as it is Artin over A and over $A/\mathfrak{m}_i$. But this implies that I_{i-1}/I_i is Noetherian over $A/\mathfrak{m}_i$, hence also over A. Assuming that we proved that I_i is Noetherian (it is automatic for $I_n = 0$), we consider an exact sequence $0 \to I_i \to I_{i-1} \to I_{i-1}/I_i \to 0$ with Noetherian modules on the sides and conclude that I_{i-1} is Noetherian. Continuing this process, we prove that A is Noetherian.

Assuming that A is Noetherian, we go through the same lines to show that A is Artin. □

Theorem 3.20. *A ring A is Artin $\iff$ A is Noetherian and every prime ideal of A is maximal.*

Proof. Assume that A is Artin and let $\mathfrak{m}_1, \dots, \mathfrak{m}_n$ be all of its maximal ideals. Then $\mathcal{R}(A) = \cap_i \mathfrak{m}_i$ and $\mathcal{R}(A)^k = 0$ for some $k \geq 0$. Therefore $\prod_i \mathfrak{m}_i^k = 0$ and we can apply the previous lemma.

Assume that A is Noetherian and its every prime ideal is maximal. Then every prime ideal is automatically a minimal prime ideal over 0, hence there are finitely many prime ideals by Lemma 3.15, say $\mathfrak{m}_1, \dots, \mathfrak{m}_n$. The nil-radical $\mathcal{N}(A) = \cap_i \mathfrak{m}_i$ is finitely generated, hence $\mathcal{N}(A)^k = 0$ for some $k > 0$. Indeed, let $\mathcal{N}(A) = (a_1, \dots, a_l)$ with $a_i^{k_i} = 0$ for some $k_i > 0$ and let $k = \sum k_i$. For any element $\sum_i a_i b_i \in \mathcal{N}(A)$, every summand of $(\sum_i a_i b_i)^k$ is of the form $\prod_i (a_i b_i)^{t_i}$ with at least one $t_i \geq k_i$ (otherwise $k = \sum t_i < \sum k_i = k$). Therefore $\prod_i (a_i b_i)^{t_i} = 0$ and $(\sum_i a_i b_i)^k = 0$, hence $\mathcal{N}(A)^k = 0$. This implies that $\prod_i \mathfrak{m}_i^k = 0$ and we can apply the previous lemma. □

Lemma 3.21. *Let $(A, \mathfrak{m})$ be a Noetherian local ring . Then A is Artin $\iff$ $\mathfrak{m}$ is nilpotent.*

Proof. If A is Artin, then $\mathfrak{m} = \mathcal{R}(A)$ is nilpotent. Conversely, if $\mathfrak{m}^n = 0$ for some $n \geq 1$, then we can apply the previous Lemma and conclude that A is Artin. □

Theorem 3.22. *An Artin ring is a finite product of Artin local rings.*

Proof. Let $\mathfrak{m}_1, \ldots, \mathfrak{m}_r$ be all maximal ideals of A. Then $\mathcal{R}(A) = \cap_i \mathfrak{m}_i$ and $\mathcal{R}(A)^k = 0$ for some $k \geq 1$. Therefore $\prod_i \mathfrak{m}_i^k = 0$. For any $i \neq j$, we have $\mathfrak{m}_i, \mathfrak{m}_j \subset \sqrt{\mathfrak{m}_i^k + \mathfrak{m}_j^k}$, hence $A = \mathfrak{m}_i + \mathfrak{m}_j \subset \sqrt{\mathfrak{m}_i^k + \mathfrak{m}_j^k}$. Therefore $\mathfrak{m}_i^k + \mathfrak{m}_j^k = A$ and these ideals are coprime. By the Chinese remainder theorem, there is an isomorphism $A/\cap_i \mathfrak{m}_i^k \to \prod_i A/\mathfrak{m}_i^k$, where $\cap_i \mathfrak{m}_i^k = \prod_i \mathfrak{m}_i^k = 0$. The rings $A/\mathfrak{m}_i^k$ are Artin. They are also local, as the maximal ideal $\bar{\mathfrak{m}}_i = \mathfrak{m}_i/\mathfrak{m}_i^k$ is nilpotent (see the proof of the previous lemma). □

Remark 3.23. Let A be an Artin, finitely generated algebra over a field $\Bbbk$. We will show that A is finite-dimensional over $\Bbbk$. Note that conversely, if A is a finite-dimensional algebra over $\Bbbk$, then A is obviously Artin. By the previous theorem we can assume that A is local, with a maximal ideal $\mathfrak{m}$. Then $\mathfrak{m}^n = 0$ for some $n > 0$. Every quotient $\mathfrak{m}^i/\mathfrak{m}^{i+1}$ is finitely generated over A and over the residue field $A/\mathfrak{m}$. Therefore $\mathfrak{m}^i/\mathfrak{m}^{i+1}$ is finite-dimensional over $A/\mathfrak{m}$. On the other hand $A/\mathfrak{m}$ is finite-dimensional over $\Bbbk$ (Hilbert Nullstellensatz), hence $\mathfrak{m}^i/\mathfrak{m}^{i+1}$ is finite-dimensional over $\Bbbk$. This implies that A is also finite-dimensional over $\Bbbk$.

4. Algebra and Geometry

We start with a topological example that should serve us as a motivation.

Example 4.1. Let X be a compact Hausdorff topological space and $A = C(X)$ be the algebra of continuous functions $f\colon X \to \mathbb{R}$. Then the map

$$\phi\colon X \to \operatorname{Max} A, \qquad x \mapsto \mathfrak{m}_x = \{f \in A \mid f(x) = 0\},$$

is a bijection, where $\operatorname{Max} A$ is the set of maximal ideals of A. The ideal $\mathfrak{m}_x$ is maximal as it is the kernel of the (surjective) evaluation map $\mathrm{ev}_x\colon A \to \mathbb{R}$, $f \mapsto f(x)$. Note that $f(x) = 0 \iff f \in \mathfrak{m}_x$. The map ϕ is injective as by Urysohn's lemma, for any $x \neq y$ in X, there exists $f \in A$ with $f(x) = 0$ and $f(y) = 1$, hence $f \in \mathfrak{m}_x \backslash \mathfrak{m}_y$ and $\mathfrak{m}_x \neq \mathfrak{m}_y$. To see that ϕ is surjective, let $I \in \operatorname{Max} A$ and assume that $I \neq \mathfrak{m}_x$ for all $x \in X$. For every $x \in X$, let us choose $f_x \in I \backslash \mathfrak{m}_x$. Then $f_x(x) \neq 0$, hence $x \in U_x = \{y \in X \mid f_x(y) \neq 0\}$. This implies that $X = \bigcup_x U_x$ is an open cover and we can find a finite subcover $X = U_{x_1} \cup \cdots \cup U_{x_n}$. The function $f = \sum f_{x_i}^2 \in I$ is nowhere zero on X, hence is invertible. Therefore $I = A$, a contradiction.

We claim that the map $\phi\colon X \to \operatorname{Max} A$ is a homeomorphism, where $\operatorname{Max} A$ is equipped with the Zariski topology, meaning that the closed sets are of the form $Z(I) = \{\mathfrak{m} \in \operatorname{Max} A \mid \mathfrak{m} \supset I\}$ for all ideals $I \subset A$. The map $\phi\colon X \to \operatorname{Max} A$ is continuous as

$$\phi^{-1}(Z(I)) = \{x \in X \mid f(x) = 0\ \forall f \in I\} = \bigcap_{f \in I} \{x \in X \mid f(x) = 0\}$$

is closed. To see that ϕ is a homeomorphism it is enough to show that $\operatorname{Max} A$ is Hausdorff (as X is compact). Consider two maximal ideals $\mathfrak{m}_x$, $\mathfrak{m}_y$ with $x \neq y$. There exist open subsets $x \in U \subset X$, $y \in V \subset X$ with $U \cap V = \varnothing$. By Urysohn's lemma $\exists f, g \in A$ such that $f(x) = 1$, $f|_{X\backslash U} = 0$ and $g(y) = 1$, $g|_{X\backslash V} = 0$. Then fg is zero on X. We have $\mathfrak{m}_x \in U' = \operatorname{Max} A \backslash Z(f)$, $\mathfrak{m}_y \in V' = \operatorname{Max} A \backslash Z(g)$ and $U' \cap V' = \operatorname{Max} A \backslash (Z(f) \cup Z(g)) = \operatorname{Max} A \backslash Z(fg) = \varnothing$.

The above example implies that instead of a topological space X we can consider the algebra of functions on X and interpret the points of X as the maximal ideals of this algebra. Next, we will substitute X with an algebraic set and substitute $C(X)$ with an algebra of polynomial functions.

Definition 4.2. Let $\Bbbk$ be a field and $A = \Bbbk[x_1, \ldots, x_n]$. Given a set of polynomials $I \subset A$, we define the corresponding *algebraic subset* of $\Bbbk^n$

$$Z(I) = \{(a_1, \ldots, a_n) \in \Bbbk^n \mid f(a_1, \ldots, a_n) = 0\ \forall f \in I\}. \tag{2}$$

Note that I may be replaced by the ideal it generates without changing $Z(I)$. As A is a Noetherian ring by the Hilbert's basis theorem (see Cor. 3.13), every ideal I has a finite set of generators, hence $I = (f_1, \ldots, f_r)$ for some $f_i \in A$. If $I = (f_1, \ldots, f_r)$, we denote $Z(I)$ by $Z(f_1, \ldots, f_r)$.

Example 4.3.

(1) Let $f(x, y) = x^2 + y^2 - 1 \in \mathbb{R}[x, y]$. Then

$$Z(f) = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 = 1\}$$

is the radius one circle in $\mathbb{R}^2$.

(2) Let $f(x, y) = x^n + y^n - 1 \in \mathbb{C}[x, y]$ for $n \geq 3$. Then

$$Z(f) = \{(x, y) \in \mathbb{C}^2 \mid x^n + y^n = 1\}$$

is called the Fermat curve. Fermat's last theorem asserts that the Fermat curve has no nontrivial rational points (that is, $(x, y) \in \mathbb{Q}^2$ with $xy \neq 0$).

(3) For $a \in \Bbbk^n$, let $\mathfrak{m}_a = (x_1 - a_1, \ldots, x_n - a_n) \subset A = \Bbbk[x_1, \ldots, x_n]$. Then $A/\mathfrak{m}_a \simeq \Bbbk$, hence $\mathfrak{m}_a$ is a maximal ideal. We have

$$Z(\mathfrak{m}_a) = \{b \in \Bbbk^n \mid b_i - a_i = 0\ \forall i\} = \{a\}.$$

This implies that $\mathfrak{m}_a \neq \mathfrak{m}_b$ if $a \neq b$. We will see later that if $\Bbbk$ is algebraically closed, then every maximal ideal of $A = \Bbbk[x_1, \ldots, x_n]$ is of the form $\mathfrak{m}_a$ for some $a \in \Bbbk^n$ (Hilbert's Nulstellensatz). Therefore there is a bijection between $\Bbbk^n$ and the set of maximal ideals $\operatorname{Max} A$.

Lemma 4.4. *Let $A = \Bbbk[x_1, \dots, x_n]$. Then*
1. $Z(0) = \Bbbk^n$, $Z(A) = \varnothing$.
2. $Z(I) \cup Z(J) = Z(I \cap J)$ *for arbitrary ideals* $I, J \subset A$.
3. $\cap_i Z(I_i) = Z(\sum_i I_i)$ *for arbitrary ideals* $I_i \subset A$.
4. $I \subset J \implies Z(I) \supset Z(J)$.

Definition 4.5. Define the *Zariski topology* on $\Bbbk^n$ with closed sets of the form $Z(I)$ for all $I \subset \Bbbk[x_1, \dots, x_n]$. It restricts to a topology on every algebraic subset $X \subset \Bbbk^n$.

Example 4.6. Consider the Zarisky topology on $\Bbbk = \Bbbk^1$, where $\Bbbk$ is an algebraically closed field. Every ideal $I \subset \Bbbk[x]$ is principal, hence is of the form $I = (f)$ for some polynomial $f = c(x - a_1)\dots(x - a_k) \in \Bbbk[x]$. If $c = 0$, then $I = 0$ and $Z(I) = \Bbbk$. If $c \neq 0$, then $Z(I) = Z(f) = \{a_1, \dots, a_k\} \subset \Bbbk$ is a finite set. Hence all algebraic sets in $\Bbbk$ are finite subsets of $\Bbbk$ and the whole space $\Bbbk$. Therefore the open sets in the Zariski topology on $\Bbbk$ are the complements of finite subsets and the empty set.

Definition 4.7. Let $X \subset \Bbbk^n$ be a subset.
1. Define the ideal of X
$$I(X) = \{f \in A \mid f(a_1, \dots, a_n) = 0 \ \forall (a_1, \dots, a_n) \in X\} \subset A.$$
2. Every polynomial $f \in \Bbbk[x_1, \dots, x_n]$ defines a function
$$f \colon \Bbbk^n \to \Bbbk, \qquad (a_1, \dots, a_n) \mapsto f(a_1, \dots, a_n),$$
called a *polynomial function*. Its restriction $f \colon X \to \Bbbk$ is called a polynomial function on X.
3. Two polynomial functions f, g agree on X (that is, $f(x) = g(x)$ for all $x \in X$) if and only if $f - g \in I(X)$. Therefore the ring of different polynomial functions on X can be identified with
$$\Bbbk[X] = \Bbbk[x_1, \dots, x_n]/I(X)$$
called the *coordinate ring* of X.

Example 4.8. Let $a = (a_1, \dots, a_n) \in \Bbbk^n$. Then $\mathfrak{m}_a = (x_1 - a_1, \dots, x_n - a_n) \subset I(a)$ as $x_i - a_i$ vanishes at a. The ideal $\mathfrak{m}_a$ is maximal and $1 \notin I(a)$, hence $I(a) = \mathfrak{m}_a$. Equivalently,
$$f(a) = 0 \iff f \in \mathfrak{m}_a, \qquad f \in \Bbbk[x_1, \dots, x_n].$$

Lemma 4.9.
1. $X \subset Y \implies I(X) \supset I(Y)$.
2. $I(\varnothing) = \Bbbk[x_1, \dots, x_n]$ *and* $I(\Bbbk^n) = 0$ *(if $\Bbbk$ is an infinite field).*
3. $I(\cup X_i) = \cap I(X_i)$.
4. $I(X)$ *is a radical ideal:* $I(X) = \sqrt{I(X)}$.

Proof. **(2)** To prove that $I(\Bbbk^n) = 0$, we need to show that if $f \in \Bbbk[x_1, \dots, x_n]$ is nonzero, then $f(a) \neq 0$ for some $a \in \Bbbk^n$. If $n = 1$, then f can have only a finite number of roots and we are done as $\Bbbk$ is infinite. For $n > 1$, consider f as a polynomial in one variable x_n over $\Bbbk[x_1, \dots, x_{n-1}]$
$$f = \sum_{i \geq 0} f_i x_n^i, \qquad f_i \in \Bbbk[x_1, \dots, x_{n-1}]$$
If $f_i \neq 0$, then by induction there exists $(a_1, \dots, a_{n-1}) \in \Bbbk^{n-1}$ such that $f_i(a_1, \dots, a_{n-1}) \neq 0$. Then the polynomial
$$f(a_1, \dots, a_{n-1}, x_n) = \sum_{i \geq 0} f_i(a_1, \dots, a_{n-1}) x_n^i$$
is nonzero and can have only a finite number of roots. Hence we are done as $\Bbbk$ is infinite.
(4) Assume that $f \in \sqrt{I(X)}$, hence $f^k \in I(X)$ for some $k > 0$. Then $f^k(a) = 0$ for all $a \in X$ $\implies f(a) = 0$ for all $a \in X \implies f \in I(X)$. □

Remark 4.10. Let $\Bbbk = \mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$ and $f(x) = x^2 + x$. Then $f(0) = f(1) = 0 \implies f \in I(\Bbbk) \implies I(\Bbbk) \neq 0$ (one can show that $I(\Bbbk) = (x^2 + x)$). This is an illustration of the fact that $I(\Bbbk^n) \neq 0$ for finite fields $\Bbbk$ and $n \geq 1$.

Lemma 4.11. *Let $\Bbbk$ be a field.*

(1) *For any algebraic subset $X \subset \Bbbk^n$, we have $Z(I(X)) = X$.*
(2) *For any ideal $J \subset \Bbbk[x_1, \dots, x_n]$, we have $I(Z(J)) \supset \sqrt{J}$.*

Proof. **(1)** We always have $X \subset Z(I(X))$. By assumption $X = Z(J)$ for some ideal J. Therefore $J \subset I(Z(J)) = I(X) \implies Z(I(X)) \subset Z(J) = X$. We conclude that $Z(I(X)) = X$.
(2) We know that $J \subset I(Z(J))$ and $I(Z(J))$ is a radical ideal. Therefore $\sqrt{J} \subset I(Z(J))$. □

Example 4.12. For $\Bbbk = \mathbb{F}_2$ and $J = (0) \subset \Bbbk[x]$, we have $Z(J) = \Bbbk$ and $I(Z(J)) = I(\Bbbk) \ni x^2 + x$, while $\sqrt{J} = (0)$. Therefore $I(Z(J)) \neq \sqrt{J}$.

Theorem 4.13 (*Hilbert's Nullstellensatz*)**.** *Let $\Bbbk$ be an algebraically closed field. Then, for every ideal $J \subset \Bbbk[x_1, \dots, x_n]$, we have $I(Z(J)) = \sqrt{J}$.*

Hilbert's Nullstellensatz (zero-points-theorem in german) will be proved later. It implies that there is a 1-1 correspondence between algebraic subsets of $\Bbbk^n$ and radical ideals of $\Bbbk[x_1, \dots, x_n]$ (if $\Bbbk$ is algebraically closed). Let us formulate several equivalent forms of Hilbert's Nullstellensatz (we will prove later the third statement for algebraically closed fields).

Theorem 4.14. *Given an (algebraically closed) field $\Bbbk$, the following are equivalent*

(1) *If $J \subset \Bbbk[x_1, \dots, x_n]$ is an ideal, then $I(Z(J)) = \sqrt{J}$.*
(2) *If $J \subset \Bbbk[x_1, \dots, x_n]$ is a proper ideal, then $Z(J) \neq \varnothing$.*
(3) *Every maximal ideal in $\Bbbk[x_1, \dots, x_n]$ is of the form $\mathfrak{m}_a = (x_1 - a_1, \dots, x_n - a_n)$ for some $a \in \Bbbk^n$.*

Proof. (1) $\implies$ (2). Let $Z(J) = \varnothing$ for some $J \subset A = \Bbbk[x_1, \dots, x_n]$. Then $\sqrt{J} = I(Z(J)) = I(\varnothing) = A \implies 1 \in \sqrt{J} \implies 1^k \in J$ for some $k > 0 \implies J = A$.
(2) $\implies$ (3). Let $J \subset A$ be a maximal ideal. Then $J \neq A \implies Z(J) \neq \varnothing$ and we can choose $a \in Z(J)$. Then $J \subset I(a) = \mathfrak{m}_a \implies J = \mathfrak{m}_a$ as J is maximal.
(3) $\implies$ (2). If $J \neq A$, then there exists a maximal ideal $\mathfrak{m} \supset J$. By (3) we have $\mathfrak{m} = \mathfrak{m}_a$ for some $a \in \Bbbk^n$. Therefore $a \in Z(\mathfrak{m}) \subset Z(J)$ and $Z(J) \neq \varnothing$.
(2) $\implies$ (1) (Rabinowitsch trick). We know that $\sqrt{J} \subset I(Z(J))$. Conversely, assume that $f \in I(Z(J))$. Consider the ideal

$$J' = (J, ft - 1) \subset \Bbbk[x_1, \dots, x_n, t].$$

If $(a_1, \dots, a_n, c) \in Z(J')$, then $(a_1, \dots, a_n) \in Z(J) \implies f(a_1, \dots, a_n) = 0 \implies ft - 1$ does not vanish at this point. Therefore $Z(J') = \varnothing$. By (2) we have $J' = (1)$ and we can write

$$1 = (ft - 1)g_0 + \sum_i f_i g_i$$

for some $g_i \in \Bbbk[x_1, \dots, x_n, t]$ and $f_i \in J$. After substitution $t = 1/f$, we obtain

$$1 = \sum_i f_i g_i(x_1, \dots, x_n, 1/f)$$

and after multiplication with a sufficiently high power of f, we get $f^N = \sum_i f_i h_i \in J$ for some $N > 0$ and $h_i = f^N g_i(x_1, \dots, x_n, 1/f) \in \Bbbk[x_1, \dots, x_n]$. Therefore $f^N \in J \implies f \in \sqrt{J}$. □

Corollary 4.15. *Let $\Bbbk$ be an algebraically closed field and $X \subset \Bbbk^n$ be an algebraic set. Then*

(1) *There is a bijection between $\Bbbk^n$ and the set of maximal ideals of $\Bbbk[x_1, \dots, x_n]$.*
(2) *There is a bijection between X and the set of maximal ideals of $\Bbbk[X] = \Bbbk[x_1, \dots, x_n]/I(X)$.*

Proof. **(1)** Follows from the previous theorem and Hilbert's Nullstellensatz. **(2)** If $J = I(X)$, then $X = Z(I(X)) = Z(J)$. We have $a \in X \iff f(a) = 0\ \forall f \in J \iff f \in \mathfrak{m}_a\ \forall f \in J \iff J \subset \mathfrak{m}_a$. Therefore $a \in X$ corresponds to the maximal ideal $\mathfrak{m}_a/J \subset \Bbbk[x_1, \dots, x_n]/J$. □

5. Integral dependence

5.1. **Integral and finite algebras.** We say that a ring B is an algebra over a ring A if A is a subring of B. If $f\colon A\to B$ is a ring homomorphism, then B is an algebra over $f(A)$ and sometimes we will say that B is an algebra over A.

Definition 5.1. Let B be an algebra over a ring A.

(1) An element $b\in B$ is called *integral* over A if it is a root of a monic polynomial with coefficients in A, meaning that there exist $a_0,\dots,a_{n-1}\in A$ such that

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

(2) The algebra B is called an *integral* algebra over A if all elements of B are integral over A.
(3) The algebra B is called a *finite* algebra over A if B is finitely generated as an A-module, meaning that there exist $b_1,\dots,b_n\in B$ such that $B=\sum_i Ab_i$.
(4) The algebra B is called a *finite type* algebra over A if B is finitely generated as an A-algebra, meaning that there exist $b_1,\dots,b_n\in B$ such that

$$B=A[b_1,\dots,b_n]=\left\{\sum_{i_1,\dots,i_n\ge0}a_{i_1,\dots,i_n}b_1^{i_1}\dots b_n^{i_n}\mid a_{i_1,\dots,i_n}\in A\right\}.$$

Remark 5.2. An algebra B over A, where both A and B are fields, is called a field extension. An element $b\in B$ integral over A is also called algebraic over A. If B is finite over A, then B is called a finite field extension of A.

Example 5.3. An algebra B over a field $\Bbbk$ is a finite algebra (in the above sense) if and only if the dimension of B over $\Bbbk$ is finite. In particular, the algebra of polynomials $\Bbbk[x]$ is not finite over $\Bbbk$. But it is of finite type over $\Bbbk$ as it is generated by a single element x as an algebra over $\Bbbk$. On the other hand, the algebra $B=\Bbbk[x]/(x^n-1)$ is finite over $\Bbbk$. It is generated (as a module over $\Bbbk$) by the elements $1,x,\dots,x^{n-1}$. The element $x\in B$ is integral over $\Bbbk$ as it is a root of the polynomial x^n-1.

Exercise 5.4. Let B be an integral algebra over A.

(1) If $J\subset B$ is an ideal, then B/J is integral over $A/(A\cap J)$.
(2) If $S\subset A$ is a multiplicative set, then $S^{-1}B$ is integral over $S^{-1}A$.

Lemma 5.5. *Let $A\subset B\subset C$ be rings such that B is finite over A and C is finite over B. Then C is finite over A.*

Proof. Let B have generators $b_1,\dots,b_m$ over A and C have generators $c_1,\dots,c_n$ over B. Then $B=\sum_i Ab_i$ and $C=\sum_j Bc_j$. Hence $C=\sum_j Bc_j=\sum_j\sum_i Ab_ic_j=\sum_{i,j}Ab_ic_j$. Therefore the elements b_ic_j (for $1\le i\le m$, $1\le j\le n$) generate C over A as a module. □

Lemma 5.6. *Let B be an algebra over A and $b\in B$ be integral over A. Then the algebra $A[b]=\left\{\sum_i a_ib^i\,\middle|\,a_i\in A\right\}$ is finite over A.*

Proof. We have $b^n=-(a_{n-1}b^{n-1}+\dots+a_0)$ for some $a_0,\dots,a_{n-1}\in A$. Therefore

$$b^{n+k}=-(a_{n-1}b^{n+k-1}+\dots+a_0b^k),\qquad k\ge0.$$

By induction, we can express b^{n+k} as a linear combination of $1,b,\dots,b^{n-1}$ with coefficients in A. This implies that $A[b]$ is generated by $1,b,\dots,b^{n-1}$ as an A-module. □

Corollary 5.7. *Let $b_1,\dots,b_n\in B$ be integral over A. Then $A[b_1,\dots,b_n]\subset B$ is finite over A.*

Proof. We can write $A[b_1,\dots,b_n]=A'[b_n]$, where $A'=A[b_1,\dots,b_{n-1}]$. We have $A\subset A'\subset A'[b_n]$, where $A'=A[b_1,\dots,b_{n-1}]$ is finite over A by induction and $A'[b_n]$ is finite over A' by Lemma 5.6. Therefore $A'[b_n]$ is finite over A by Lemma 5.5. □

Lemma 5.8. *Let B be a finite algebra over A. Then B is integral over A.*

Proof. Let us show that every $b \in B$ is integral over A. Let $u_1, \dots, u_n$ generate B as a module over A. Let $bu_i = \sum_j c_{ij} u_j$ for some $c_{ij} \in A$ and let $C = (c_{ij}) \in M_{n\times n}(A)$. Then

$$(bI_n - C)u = 0, \qquad u = (u_1, \dots, u_n)^t.$$

Multiplying the last equation by the adjoint of the matrix $bI_n - C$, we obtain $\det(bI_n - C)u = 0$. Therefore $\det(bI_n - C)u_i = 0$ for all $i \implies \det(bI_n - C)B = 0 \implies \det(bI_n - C) = 0$. This implies that b is a root of the monic polynomial

$$\det(xI_n - C) = x^n + a_{n-1}x^{n-1} + \dots + a_0 \in A[x].$$

Therefore b is integral over A. □

Remark 5.9. The proof of the last lemma can be generalised as follows. Let B be an algebra over A such that there exists a faithful B-module M (meaning that $\operatorname{Ann} M = \{b \in B \mid bM = 0\} = 0$), finitely generated over A. Then B is integral over A.

Corollary 5.10. *Let B be an algebra over A and $b \in B$. Then the following are equivalent:*

1. *b is integral over A.*
2. *$A[b]$ is finite over A.*
3. *There exists a ring $A[b] \subset C \subset B$ such that C is finite over A.*

Lemma 5.11. *An algebra B is finite over $A \iff$ it is integral and of finite type over A.*

Proof. If B is finite over A, then it is finitely-generated as an A-algebra. It is integral over A by Lemma 5.8. Conversely, let B be integral and of finite type over A. Then $B = A[b_1, \dots, b_n]$ for some $b_i \in B$. The elements b_i are integral over A, hence $B = A[b_1, \dots, b_n]$ is finite over A by Cor. 5.7. □

Lemma 5.12. *Let $A \subset B \subset C$ be rings such that B is integral over A and C is integral over B. Then C is integral over A.*

Proof. For every $c \in C$, there exist $b_0, \dots, b_{n-1} \in B$ such that $c^n + b_{n-1}c^{n-1} \cdots + b_0 = 0$. Then $B' = A[b_0, \dots, b_{n-1}]$ is finite over A by Cor. 5.7 and $B'[c]$ is finite over B' by Lemma 5.6. Therefore $B'[c]$ is finite over A by Lemma 5.5. Then $c \in B'[c]$ is integral over A by Lemma 5.8. □

Lemma 5.13. *For a subring $A \subset B$, the set C of all elements in B integral over A is a subring of B.*

Proof. If $b, b' \in C$, then they are integral over A, hence $A[b, b']$ is finite over A by Cor. 5.7. Therefore $b \pm b, bb' \in A[b, b']$ are integral over A by Lemma 5.8. This implies that $b \pm b', bb' \in C$. □

Definition 5.14.

1. For a subring $A \subset B$, the ring $\bar{A} = \bar{A}_B$ consisting of all elements in B integral over A is called the *integral closure* of A in B.
2. A subring $A \subset B$ is called *integrally closed* in B if $\bar{A} = A$. This means that every element $b \in B$ integral over A is contained in A.
3. A ring A is called *integrally closed* (without a reference to a larger ring) if A is integrally closed in the ring of fractions $\mathcal{F}(A) = S^{-1}A$, where $S \subset A$ is the set of non-zero-divisors of A.

Example 5.15. If B is an integral algebra over A, then $\bar{A} = B$. For example, if $f \in A[x]$ is a monic polynomial, then $B = A[x]/(f)$ is finite over A, hence is integral over A and $\bar{A} = B$.

Example 5.16. Let us show that $\mathbb{Z}$ is integrally closed in $\mathcal{F}(\mathbb{Z}) = \mathbb{Q}$. Let $b = \frac{m}{n} \in \mathbb{Q}$ (with coprime m, n) be integral over $\mathbb{Z}$. Then $b^r + a_{r-1}b^{r-1} + \dots + a_0 = 0$ for some $a_i \in \mathbb{Z}$, hence $m^r + a_{r-1}m^{r-1}n + \dots + a_0 n^r = 0$. This implies $n \mid m^r$. As m, n are coprime, we conclude that $n = \pm 1$, hence $b \in \mathbb{Z}$. This example can be generalized to show that every UFD is integrally closed.

Lemma 5.17. *Let $\bar{A}$ be the integral closure of $A \subset B$. Then $\bar{A}$ is integrally closed in B.*

Proof. Let $b \in B$ be integral over $\bar{A}$. Then $A \subset \bar{A} \subset \bar{A}[b]$ are integral inclusions, hence $\bar{A}[b]$ is integral over A. In particular, $b \in \bar{A}[b]$ is integral over A, hence $b \in \bar{A}$. □

Lemma 5.18. *Let $\bar{A}$ be the integral closure of $A \subset B$ and let $S \subset A$ be a multiplicative set. Then $S^{-1}\bar{A}$ is the integral closure of $S^{-1}A$ in $S^{-1}B$.*

Proof. Every element $\frac{b}{s} \in S^{-1}\bar{A}$ is integral over $S^{-1}A$. Indeed, $b \in \bar{A}$ is integral over A, hence $b^n + \sum_{i=0}^{n-1} a_i b^i = 0$ for some $a_i \in A$. Dividing by s^n, we obtain $\left(\frac{b}{s}\right)^n + \sum_{i=0}^{n-1} \frac{a_i}{s^{n-i}} \left(\frac{b}{s}\right)^i = 0$. This implies that $\frac{b}{s}$ is integral over $S^{-1}A$. Conversely, let $\frac{b}{s} \in S^{-1}B$ be integral over $S^{-1}A$. Then $\left(\frac{b}{s}\right)^n + \sum_{i=0}^{n-1} \frac{a_i}{s_i} \left(\frac{b}{s}\right)^i = 0$ for some $\frac{a_i}{s_i} \in S^{-1}A$. Multiplying this equation by $(st)^n$, where $t = s_0 \dots s_{n-1} \in S$, we obtain integral dependence of bt over A. Therefore $bt \in \bar{A}$ and $\frac{b}{s} = \frac{bt}{st} \in S^{-1}\bar{A}$. □

5.2. Going-up theorem.

Theorem 5.19. *Let $A \subset B$ be integral domains such that B is integral over A. Then A is a field if and only if B is a field.*

Proof. Assume that A is a field. Every $0 \neq b \in B$ is integral over A, hence

$$b^n + a_{n-1}b^{n-1} + \dots + a_1 b + a_0 = 0$$

for some $a_i \in A$. Assume that n is minimal. Then $a_0 \neq 0$ as otherwise $b(b^{n-1} + \dots + a_1) = 0$, hence $b^{n-1} + \dots + a_1 = 0$ and n would be not minimal. We have $a_0 = -b(b^{n-1} + \dots + a_1)$, hence

$$b^{-1} = -a_0^{-1}(b^{n-1} + \dots + a_1) \in B.$$

Therefore B is a field.

Assume that B is a field. For $0 \neq b \in A$, the element $b^{-1} \in B$ is integral over A, hence

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

for some $a_i \in A$. Therefore

$$b^{-1} = -(a_{n-1} + \dots + a_0 b^{n-1}) \in A.$$

This implies that A is a field. □

We say that a ring homomorphism $f\colon A \to B$ is integral if B is integral over $f(A)$.

Lemma 5.20. *Let $f\colon A \to B$ be an integral ring homomorphism. Then a prime ideal $\mathfrak{q} \subset B$ is maximal $\iff$ $\mathfrak{p} = f^{-1}(\mathfrak{q})$ is maximal.*

Proof. The rings $A/\mathfrak{p} \subset B/\mathfrak{q}$ are integral domains and $B/\mathfrak{q}$ is integral over $A/\mathfrak{p}$. By the previous result $B/\mathfrak{q}$ is a field $\iff$ $A/\mathfrak{p}$ is a field. □

Corollary 5.21. *Let $f\colon A \to B$ be an integral ring homomorphism and $\mathfrak{q} \subsetneq \mathfrak{q}' \subset B$ be prime ideals. Then $f^{-1}(\mathfrak{q}) \neq f^{-1}(\mathfrak{q}')$.*

Proof. Considering $f(A)$ instead of A, we can assume that f is injective. Assume that $\mathfrak{p} = f^{-1}(\mathfrak{q}) = f^{-1}(\mathfrak{q}')$. Taking localizations $A_\mathfrak{p}$ and $B_\mathfrak{p}$, we can assume that $\mathfrak{p}$ is maximal (there is a bijection between prime ideals of $B_\mathfrak{p}$ and prime ideals of B that don't intersect $S = A\backslash\mathfrak{p}$; ideals $\mathfrak{q}, \mathfrak{q}'$ don't intersect S). But then $\mathfrak{q}$ and $\mathfrak{q}'$ are maximal by the previous result and $\mathfrak{q} \subsetneq \mathfrak{q}'$, a contradiction. □

Theorem 5.22. *Let $f\colon A \to B$ be an integral ring homomorphism. Then, for every prime ideal $\mathfrak{p} \subset A$, there exists a prime ideal $\mathfrak{q} \subset B$ such that $\mathfrak{p} = f^{-1}(\mathfrak{q})$. Equivalently, the following map is surjective*

$$f^*\colon \operatorname{Spec} B \to \operatorname{Spec} A, \qquad \mathfrak{q} \mapsto f^{-1}(\mathfrak{q}).$$

Proof. Consider $S = A\backslash\mathfrak{p}$, $A_\mathfrak{p} = S^{-1}A$, $B_\mathfrak{p} = S^{-1}B$ and a commutative diagram

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ {\scriptstyle i}\downarrow & & \downarrow{\scriptstyle j} \\ A_\mathfrak{p} & \xrightarrow{f_\mathfrak{p}} & B_\mathfrak{p} \end{array}$$

The induced map $f_\mathfrak{p}\colon A_\mathfrak{p} \to B_\mathfrak{p}$ is integral. Let $\mathfrak{n} \subset B_\mathfrak{p}$ be a maximal ideal. Then $\mathfrak{m} = f_\mathfrak{p}^{-1}(\mathfrak{n}) \subset A_\mathfrak{p}$ is also maximal by Lemma 5.20. Hence $\mathfrak{m} = \mathfrak{p}_\mathfrak{p}$, the unique maximal ideal of $A_\mathfrak{p}$. We have $\mathfrak{p} = i^{-1}(\mathfrak{p}_\mathfrak{p}) = i^{-1}(f_\mathfrak{p}^{-1}(\mathfrak{n})) = f^{-1}(j^{-1}(\mathfrak{n})) = f^{-1}(\mathfrak{q})$ for the prime ideal $\mathfrak{q} = j^{-1}(\mathfrak{n}) \subset B$. □

Corollary 5.23 (Going-up theorem). *If $f\colon A \to B$ is integral, then for any chain of prime ideals $\mathfrak{p}_0 \subset \ldots \subset \mathfrak{p}_n \subset A$, there exists a chain of prime ideals $\mathfrak{q}_0 \subset \ldots \subset \mathfrak{q}_n \subset B$ with $\mathfrak{p}_i = f^{-1}(\mathfrak{q}_i)$.*

Proof. We choose $\mathfrak{q}_0 \subset B$ such that $f^{-1}(\mathfrak{q}_0) = \mathfrak{p}_0$. Then we apply induction to $\bar{f}\colon A/\mathfrak{p}_0 \to B/\mathfrak{q}_0$ and the chain of prime ideals $\mathfrak{p}_1/\mathfrak{p}_0 \subset \ldots \subset \mathfrak{p}_n/\mathfrak{p}_0 \subset A/\mathfrak{p}_0$. □

Exercise 5.24. If $f\colon A \to B$ is finite and $\mathfrak{p} \in \operatorname{Spec} A$, then the set $\left\{\mathfrak{q} \in \operatorname{Spec} B \,\middle|\, f^{-1}(\mathfrak{q}) = \mathfrak{p}\right\}$ is finite.

Hint: Substitute A by $A/\mathfrak{p}$ and B by $B/\mathfrak{p}B$, then invert nonzero elements of A. Use Lemma 3.17.

5.3. Proof of the Nullstellensatz.

Theorem 5.25 (*Noether's normalization theorem*)**.** *For any finitely generated algebra B over a field $\Bbbk$, there exists a polynomial subalgebra $A = \Bbbk[y_1, \dots, y_r] \subset B$ such that B is finite over A.*

Proof. We will assume that $\Bbbk$ is infinite. Let $b_1, \dots, b_n$ be generators of B over $\Bbbk$. If they are algebraically independent (meaning that $f(b_1, \dots, b_n) \ne 0$ for all $0 \ne f \in \Bbbk[x_1, \dots, x_n]$), then $B \simeq \Bbbk[x_1, \dots, x_n]$ and we can take $A = B$.

Otherwise, $f(b_1, \dots, b_n) = 0$ for some $0 \ne f \in \Bbbk[x_1, \dots, x_n]$. For every monomial $m = x_1^{i_1} \dots x_n^{i_n}$, we define its (total) degree $\deg(m) = i_1 + \dots + i_n$. We can write $f = \sum_{k=0}^N f_k$, where f_k has only monomials of degree k and $f_N \ne 0$. Using the substitution $b_i' = b_i - a_i b_n$ for some $a_i \in \Bbbk$, $1 \le i \le n-1$, we obtain

$$0 = f(b_1, \dots, b_n) = \sum_{k=0}^N f_k(b_1' + a_1 b_n, \dots, b_{n-1}' + a_{n-1} b_n, b_n)$$

$$= f_N(a_1, \dots, a_{n-1}, 1) b_n^N + \sum_{i=0}^{N-1} g_i(b_1', \dots, b_{n-1}') b_n^i$$

for some polynomials g_k in $n-1$ variables. We claim that $f_N(x_1, \dots, x_{n-1}, 1) \ne 0$. Indeed, we can write $f_N = \sum_{i=0}^N h_i x_n^{N-i} \ne 0$, where $h_i \in \Bbbk[x_1, \dots, x_{n-1}]$ has total degree i. Then $f_N(x_1, \dots, x_{n-1}, 1) = \sum_i h_i \ne 0$. As $\Bbbk$ is infinite, there exist $a_1, \dots, a_{n-1} \in \Bbbk$ such that $f_N(a_1, \dots, a_{n-1}, 1) \ne 0$ (see Lemma 4.9). Dividing the above equation by $f_N(a_1, \dots, a_{n-1}, 1)$ we obtain that b_n is integral over $A' = \Bbbk[b_1', \dots, b_{n-1}'] \subset B$, hence $B = A'[b_n]$ is finite over A'. By induction on n, there exists a polynomial subalgebra $A = \Bbbk[y_1, \dots, y_r] \subset A'$ such that A' is finite over A. But then B is also finite over A. □

Theorem 5.26 (General Hilbert's Nullstellensatz)**.** *Let $\Bbbk$ be a field. Then*

1. *If A is a finitely-generated $\Bbbk$-algebra and is a field, then A is a finite field extension of $\Bbbk$.*
2. *If A is a finitely-generated $\Bbbk$-algebra and $\mathfrak{m} \subset A$ is a maximal ideal, then $A/\mathfrak{m}$ is a finite field extension of $\Bbbk$.*

Proof. **(1)** By Theorem 5.25, there exists a polynomial subalgebra $B = \Bbbk[y_1, \dots, y_r]$ of A such that A is finite (hence integral) over B. Then B is a field by Theorem 5.19, hence $r = 0$ and $B = \Bbbk$. This implies that A is finite over $\Bbbk$, meaning that it is a finite field extension of $\Bbbk$.
(2) The algebra $A/\mathfrak{m}$ is finitely generated and is a field. By (1) it is a finite field extension of $\Bbbk$. □

Theorem 5.27 (Hilbert's Nullstellensatz)**.** *Let $\Bbbk$ be an algebraically closed field. Then every maximal ideal in $\Bbbk[x_1, \dots, x_n]$ is of the form $(x_1 - a_1, \dots, x_n - a_n)$ for some $a_1, \dots, a_n \in \Bbbk$.*

Proof. Let $\mathfrak{m} \subset \Bbbk[x_1, \dots, x_n]$ be a maximal ideal. Then $L = \Bbbk[x_1, \dots, x_n]/\mathfrak{m}$ is a finite field extension of $\Bbbk$ by the previous theorem. Therefore every element $a \in L$ is algebraic over $\Bbbk$. As $\Bbbk$ is algebraically closed, the minimal polynomial of a is linear. Therefore $a \in \Bbbk$ and we conclude that $L = \Bbbk$. Consider the projection map

$$\pi \colon \Bbbk[x_1, \dots, x_n] \to \Bbbk[x_1, \dots, x_n]/\mathfrak{m} = L = \Bbbk.$$

Let $a_i = \pi(x_i) \in \Bbbk$ for $1 \le i \le n$ and $\mathfrak{m}_a = (x_1 - a_1, \dots, x_n - a_n)$. We have $x_i - a_i \in \operatorname{Ker} \pi = \mathfrak{m}$, hence $\mathfrak{m}_a \subset \mathfrak{m}$. But $\mathfrak{m}_a$ is a maximal ideal, hence $\mathfrak{m} = \mathfrak{m}_a$. □

Theorem 5.28. *Let A be a finitely-generated algebra over a field $\Bbbk$. Then*

1. $\mathcal{N}(A) = \mathcal{R}(A)$.
2. *For every ideal $I \subset A$, the intersection of the maximal ideals containing I is equal to $\sqrt{I}$.*
3. *Every prime ideal of A is an intersection of maximal ideals.*

Proof. **(3) $\Longrightarrow$ (1).** The nilradical $\mathcal{N}(A)$ is equal to the intersection of all prime ideals of A and the Jacobson radical $\mathcal{R}(A)$ is equal to the intersection of all maximal ideals of A. Every maximal ideal is prime, hence $\mathcal{N}(A) \subset \mathcal{R}(A)$. By our assumption, every prime ideal $\mathfrak{p}$ is an intersection of maximal ideals, hence $\mathcal{R}(A) \subset \mathfrak{p}$. Therefore $\mathcal{R}(A) \subset \bigcap_{\mathfrak{p} \in \operatorname{Spec}(A)} \mathfrak{p} = \mathcal{N}(A)$.

(1) $\Longrightarrow$ (2). Let J be the intersection of all maximal ideals containing I. Then $J/I = \mathcal{R}(A/I) = \mathcal{N}(A/I) = \sqrt{I}/I$, hence $J = \sqrt{I}$.

(3) We can substitute A by $A/\mathfrak{p}$ and assume that $\mathfrak{p} = 0$ and A is an integral domain. Then the intersection of all maximal ideals containing $\mathfrak{p}$ is equal to $\mathcal{R}(A)$ and we need to show that $\mathcal{R}(A) = 0$. Let $f \in A$ be nonzero. The algebra $B = A[f^{-1}]$ is finitely-generated over $\Bbbk$, hence for any maximal ideal $\mathfrak{m} \subset B$, the field $B/\mathfrak{m}$ is finite over $\Bbbk$. We have $\Bbbk \subset A/\mathfrak{q} \subset B/\mathfrak{m}$, where $\mathfrak{q} = A \cap \mathfrak{m}$. Therefore $A/\mathfrak{q}$ is an integral domain and $A/\mathfrak{q}$ is finite (hence integral) over $\Bbbk$. By Theorem 5.19, the algebra $A/\mathfrak{q}$ is a field (one can also show directly that an integral domain, finite-dimensional over a field is itself a field). This implies that $\mathfrak{q} \subset A$ is a maximal ideal. We have $f \notin \mathfrak{q}$ as otherwise $f \in \mathfrak{q} \subset \mathfrak{m}$, hence $\mathfrak{m} = A[f^{-1}]$ is not maximal. We conclude that $f \notin \mathcal{R}(A)$, hence $\mathcal{R}(A) = 0$. $\square$

6. Dedekind domains

6.1. Valuation rings.

Definition 6.1. Let A be an integral domain and $K = \mathcal{F}(A)$ be its field of fractions. Then A is called a *valuation ring* of K if for every $0 \neq x \in K$, either $x \in A$ or $x^{-1} \in A$.

Example 6.2. Let $A = \mathbb{Z}$ and $K = \mathcal{F}(\mathbb{Z}) = \mathbb{Q}$ be its field of fractions. Then $x = \frac{2}{3} \in \mathbb{Q}$ and $x^{-1} = \frac{3}{2}$ are not integers, hence $\mathbb{Z}$ is not a valuation ring.

Example 6.3. Let $A = \Bbbk[\![x]\!] = \left\{\sum_{i\geq 0} f_i x^i \,\middle|\, f_i \in \Bbbk\right\}$ be the ring of power series over a field $\Bbbk$. Every nonzero element of $\Bbbk[\![x]\!]$ can be written in the form $x^n g$, where $n \geq 0$ and $g = \sum_{i\geq 0} g_i x^i$, $g_i \in \Bbbk$, satisfies $g_0 \neq 0$ (the element g is invertible in $\Bbbk[\![x]\!]$). To construct the field of fractions $K = \mathcal{F}(A)$, we only need to invert x (for example, $(x^n g)^{-1} = x^{-n} g^{-1}$, where $g^{-1} \in A$). Therefore $\mathcal{F}(A) = \Bbbk(\!(x)\!) = \left\{\sum_{i\geq N} f_i x^i \,\middle|\, f_i \in \Bbbk,\ N \in \mathbb{Z}\right\}$, called the field of Laurent series over $\Bbbk$. Every nonzero element of $\Bbbk(\!(x)\!)$ can be written in the form $f = x^n g$, where $n \in \mathbb{Z}$ and $g = \sum_{i\geq 0} g_i x^i$ satisfies $g_0 \neq 0$. If $n \geq 0$, then $f \in \Bbbk[\![x]\!]$ and if $n < 0$, then $f^{-1} = x^{-n} g^{-1} \in \Bbbk[\![x]\!]$. Therefore $\Bbbk[\![x]\!]$ is a valuation ring.

Example 6.4. Let A be a principal ideal domain, $p \in A$ be a prime element and $\mathfrak{p} = (p)$ (a maximal ideal as $A/(p)$ is a field). Then $A_\mathfrak{p} = S^{-1}A$, $S = A\backslash\mathfrak{p}$, is a valuation ring. Indeed, every nonzero element of $K = \mathcal{F}(A_\mathfrak{p}) = \mathcal{F}(A)$ can be written in the form $x = \frac{a}{b}$, where $a, b \in A$ are coprime. If $b \notin \mathfrak{p}$, then $x = \frac{a}{b} \in A_\mathfrak{p}$. If $a \notin \mathfrak{p}$, then $x^{-1} = \frac{b}{a} \in A_\mathfrak{p}$. If $a, b \in \mathfrak{p}$, then $p \mid a$ and $p \mid b$, a contradiction.

Exercise 6.5. Let A be a valuation ring and $K = \mathcal{F}(A)$. Show that

(1) The group $\Gamma = K^\times/A^\times$ with the relation $x \geq y$ if $x/y \in A$ is a totally ordered set.
(2) If $x \geq y$ in Γ, then $x + z \geq y + z$ (using additive notation for the multiplication in Γ).
(3) The map $v\colon K^\times \to \Gamma$, $x \mapsto [x]$, satisfies
  (a) $v(xy) = v(x) + v(y)$.
  (b) $v(x + y) \geq \min\{v(x), v(y)\}$.

The map v as above is called a valuation of the field K.

Lemma 6.6. *If A is a valuation ring of a field K, then*

(1) *A is a local ring.*
(2) *A is integrally closed in K.*

Proof. **(1)** It is enough to show that the set $\mathfrak{m} \subset A$ of all non-invertible elements is an ideal. Then every proper ideal of A is contained in $\mathfrak{m}$, hence $\mathfrak{m}$ is the unique maximal ideal of A.

If $a \in A$ and $x \in \mathfrak{m}$, then $ax \in \mathfrak{m}$. Indeed, if $ax \notin \mathfrak{m}$, then ax is invertible, hence $bax = 1$ for some $b \in A$. But this implies that x is invertible, a contradiction.

If $x, y \in \mathfrak{m}$ are nonzero, then $x + y \in \mathfrak{m}$. Indeed, either xy^{-1} or $x^{-1}y$ is in A. Assuming that $xy^{-1} \in A$, we get $xy^{-1} + 1 \in A$, hence $x + y = (xy^{-1} + 1)y \in \mathfrak{m}$ by the previous argument.

We conclude that $\mathfrak{m}$ is an ideal.

(2) Assume that $x \in K\backslash A$ is integral over A. Then we have

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

for some $a_i \in A$. As $x \notin A$, we obtain $x^{-1} \in A$, hence $x = -(a_{n-1} + \cdots + a_0 x^{1-n}) \in A$. A contradiction. ∎

6.2. **Discrete valuation rings.**

Definition 6.7. A *discrete valuation* on a field K is a surjective map $v\colon K^* \to \mathbb{Z}$ such that

(1) $v(xy) = v(x) + v(y)$ (that is, v is a group homomorphism).
(2) $v(x + y) \geq \min\{v(x), v(y)\}$.

We define $v(0) = +\infty$ for convenience.

Remark 6.8. An *absolute value* on a field K is a map $|-| : K \to \mathbb{R}$ such that

(1) $|x| \geq 0$ and $|x| = 0 \iff x = 0$.
(2) $|xy| = |x| \cdot |y|$.
(3) $|x + y| \leq |x| + |y|$.

It is called *non-archimedean* if a stronger condition is satisfied:

(3') $|x + y| \leq \max\{|x|, |y|\}$.

Given a discrete valuation v and a constant $0 < c < 1$, we can define a non-archimedean absolute value $|x| = c^{v(x)}$.

Lemma 6.9. *Let v be a discrete valuation on a field K, then*

$$A = \{x \in K \mid v(x) \geq 0\}$$

is a valuation ring (hence local and integrally closed), called the discrete valuation ring (DVR) of v. Its maximal ideal is

$$\mathfrak{m} = \{x \in K \mid v(x) > 0\}.$$

Proof. It is clear that A is a ring. We have $v(1) = 0$. If $0 \neq x \in K$ is not in A, then $v(x) < 0$, hence $v(x^{-1}) = v(1) - v(x) = -v(x) > 0$ and $x^{-1} \in A$. This implies that A is a valuation ring.

It is clear that $\mathfrak{m}$ is an ideal. An element $x \in A$ is invertible $\iff$ $v(x) \geq 0$ and $v(x^{-1}) \geq 0$ $\iff$ $v(x) = 0$. This means that $\mathfrak{m}$ consists of all non-invertible elements of A, hence is the unique maximal ideal of A. □

Example 6.10. Let $K = \mathbb{Q}$ and p be a prime number. Every non-zero $x \in \mathbb{Q}$ can be written in the form $p^k \frac{m}{n}$, where m, n are coprime with p and $k \in \mathbb{Z}$. We define the valuation v_p with $v_p(x) = k$. The valuation ring of v_p consists of fractions $p^k \frac{m}{n}$ with $k \geq 0$ and m, n coprime with p. This is the local ring $\mathbb{Z}_{(p)} = S^{-1}\mathbb{Z}$, where $S = \mathbb{Z} \backslash (p)$.

Example 6.11. Let $K = \Bbbk(\!(x)\!)$ be the field of Laurent power series $f = \sum_{i=N}^{\infty} f_i x^i$ over a field $\Bbbk$. We define the valuation $v(f) = \min\{i \in \mathbb{Z} \mid f_i \neq 0\}$. Its valuation ring is $\Bbbk[\![x]\!]$, the ring of power series.

An element $t \in A$ with $v(t) = 1$ is called a *uniformizer*.

Lemma 6.12. *If $t \in A$ is a uniformizer, then every element $x \in K$ can be expressed uniquely in the form ut^k, where $u \in A$ is a unit and $k \in \mathbb{Z}$.*

Proof. Let $k = v(x)$ and $u = xt^{-k}$. Then $v(u) = 0$, hence $u \in A$ is invertible. Note that if $x = ut^k$, where u is invertible, then $v(x) = k$, hence k is uniquely determined. Therefore $u = xt^{-k}$ is also uniquely determined. □

Lemma 6.13. *Every non-zero ideal $I \subset A$ is of the form $\mathfrak{m}^n = (t^n)$ for some $n \geq 0$.*

Proof. Let $n = \min\{v(a) \mid a \in I\}$ and let $a \in I$ satisfy $v(a) = n$. It is clear, that $(a) \subset I$. Conversely, if $b \in I$, then $v(ba^{-1}) = v(b) - v(a) \geq 0$, hence $ba^{-1} \in A$ and $b = (ba^{-1})a \in (a)$. Therefore $I = (a)$. We can write $a = ut^n$ for some invertible $u \in A$. Then $I = (a) = (t^n)$. In particular, $\mathfrak{m} = (t)$, hence $I = (t^n) = \mathfrak{m}^n$. □

The above result implies that A is a Noetherian local domain of dimension one (every nonzero prime ideal is maximal).

Theorem 6.14. *Let $(A, \mathfrak{m})$ be a Noetherian local domain with the residue field $\Bbbk = A/\mathfrak{m}$. Then FAE*

(1) *A is a DVR*

(2) *A is integrally closed and every nonzero prime ideal is maximal.*
(3) $\mathfrak{m}$ *is principal.*
(4) $\dim_{\Bbbk} \mathfrak{m}/\mathfrak{m}^2 = 1$.
(5) *Every nonzero ideal is a power of* $\mathfrak{m}$.
(6) *There exists* $t \in A$ *such that every nonzero ideal is of the form* (t^n) *for some* $n \geq 0$
(7) *A is a PID.*

Proof. **(1) $\Longrightarrow$ (2).** A is a valuation ring, hence integrally closed by Lemma 6.6. If $\mathfrak{p} \subset A$ is a non-zero prime ideal, then $\mathfrak{p} = \mathfrak{m}^n$ for some $n \geq 0 \implies \mathfrak{m} \subset \mathfrak{p} \implies \mathfrak{p} = \mathfrak{m}$.
(2) $\Longrightarrow$ (3). Let $0 \neq a \in \mathfrak{m}$. Then $\sqrt{(a)}$ is an intersection of prime ideals, hence $\sqrt{(a)} = \mathfrak{m}$. This implies that $\mathfrak{m}^n \subset (a)$ for some $n \geq 1$ and we can assume that $\mathfrak{m}^{n-1} \not\subset (a)$. Let $b \in \mathfrak{m}^{n-1} \backslash (a)$ and $x = \frac{b}{a} \notin A$. If $x\mathfrak{m} \subset \mathfrak{m}$, then $\mathfrak{m}$ is a faithful $A[x]$-module, finitely generated over A. Therefore x in integral over A, hence $x \in A$, a contradiction. On the other hand $x\mathfrak{m} \subset \frac{\mathfrak{m}^{n-1}}{a}\mathfrak{m} \subset \frac{1}{a}(a) = A$. We conclude that $x\mathfrak{m} = A$, hence $\mathfrak{m} = x^{-1}A$ is principal.
(3) $\Longrightarrow$ (4). If $\mathfrak{m}$ is principal, then $\dim \mathfrak{m}/\mathfrak{m}^2 \leq 1$. On the other hand, if $\mathfrak{m}^2 = \mathfrak{m}$, then $\mathfrak{m} = 0$ by Nakayama lemma. Therefore $\dim \mathfrak{m}/\mathfrak{m}^2 = 1$.
(4) $\Longrightarrow$ (3). If $\dim \mathfrak{m}/\mathfrak{m}^2 = 1$, then $Ax + \mathfrak{m}^2 = \mathfrak{m}$ for some $x \in \mathfrak{m}$. By Nakayama lemma, this implies that $Ax = \mathfrak{m}$, hence $\mathfrak{m}$ is principal.
(3) $\Longrightarrow$ (5). Let $\mathfrak{m} = (t)$. We claim that $\cap_n \mathfrak{m}^n = 0$. If $a \in \cap_n \mathfrak{m}^n$, then we can write $a = b_n t^n$ for some $b_n \in A$. This implies $b_n t^n = b_{n+1} t^{n+1} \implies b_n = b_{n+1} t \implies (b_n) \subset (b_{n+1})$. This chain of ideals stabilizes, hence $b_{n+1} = u b_n$ for some invertible u. Therefore $b_n = utb_n$ and $b_n = 0$ as otherwise $ut = 1$ and $\mathfrak{m} = (t) = A$. We conclude that $a = 0$.

Let $0 \neq I \subset A$ be a proper ideal. Then $I \subset \mathfrak{m}$ and $I \not\subset \cap_n \mathfrak{m}^n$, hence there exists $n \geq 0$ such that $I \subset \mathfrak{m}^n$, but $I \not\subset \mathfrak{m}^{n+1}$. If $a \in I \backslash \mathfrak{m}^{n+1} \implies a \in \mathfrak{m}^n = (t^n) \implies a = ut^n$ for some $u \notin \mathfrak{m}$ (otherwise $a \in \mathfrak{m}^{n+1}$). This implies that u is invertible, hence $\mathfrak{m}^n = (t^n) = (a) \subset I \subset \mathfrak{m}^n$ and $I = \mathfrak{m}^n$.
(5) $\Longrightarrow$ (6). We have $\mathfrak{m} \neq \mathfrak{m}^2$ by Nakayama's lemma. Let $t \in \mathfrak{m} \backslash \mathfrak{m}^2$. Then $(t) = \mathfrak{m}^n$ for some $n \geq 1$. If $n \geq 2$, then $(t) = \mathfrak{m}^n \subset \mathfrak{m}^2$, hence $t \in \mathfrak{m}^2$, a contradiction. Therefore $n = 1$ and $(t) = \mathfrak{m}$. By assumption, every nonzero ideal is of the form $\mathfrak{m}^n = (t^n)$ for some $n \geq 0$.
(6) $\Longrightarrow$ (1). We have $\mathfrak{m} = (t)$. If $(t^n) = (t^{n+1}) = \mathfrak{m}(t^n)$, then $(t^n) = 0$ by Nakayama lemma, a contradiction. For every $a \neq 0$, we have $(a) = (t^k)$ for exactly one $k \geq 0$. We define $v(a) = k$ and extend v to K^* by defining $v(a/b) = v(a) - v(b)$. One can check that v is a discrete valuation and A is its valuation ring.
(6) $\Longrightarrow$ (7). Obvious. **(7) $\Longrightarrow$ (3).** Obvious. □

Example 6.15. Let $A = \Bbbk[x]_{(x)}$ (localization of the ring $\Bbbk[x]$ at the prime ideal $\mathfrak{p} = (x)$). This is a Noetherian local domain with the maximal ideal $\mathfrak{m} = (x)$ which is principal. Therefore A is a DVR. Its field of fractions is $\Bbbk(x)$, the field of rational functions over $\Bbbk$. The valuation is given by the formula $v(x^n f/g) = n$ for the polynomials $f, g \in \Bbbk[x]$ with non-trivial constant coefficients.

6.3. Dedekind domains.

Definition 6.16. Let A be an integral domain.

(1) A is said to have dimension one if every nonzero prime ideal of A is maximal. In particular, DVR have dimension one.
(2) A is called *integrally closed* if it is integrally closed in its field of fractions.
(3) An integral domain A is called a *Dedekind domain* if A is Noetherian, integrally closed and has dimension one.

Example 6.17.

(1) Any DVR is a Dedekind domain.
(2) $\mathbb{Z}$ is a Dedekind domain. We proved earlier that $\mathbb{Z}$ is integrally closed. Every nonzero prime ideal if of the form (p) for some prime number $p \in \mathbb{Z}$. But $\mathbb{Z}/(p)$ is a field, hence (p) is a maximal ideal.
(3) More generally, every PID is a Dedekind domain.
(4) $\mathbb{Z}[-\sqrt{5}]$ is a Dedekind domain (although it is not a PID).
(5) Let K be a finite field extension of $\mathbb{Q}$, called a *number field*. The integral closure A of $\mathbb{Z}$ in K is called the *ring of integers* of K. One can prove that A is a Dedekind domain. Moreover, A is a free module of finite rank over $\mathbb{Z}$.

Lemma 6.18. *Let A be an integral domain. Then f.a.e.*

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

Proof. Let K be the field of fractions of A and C be the integral closure of A in K. Then $C_\mathfrak{p}$ is the integral closure of $A_\mathfrak{p}$ in K by 5.18. A is integrally closed $\iff A = C \iff C/A = 0 \iff C_\mathfrak{p}/A_\mathfrak{p} = (C/A)_\mathfrak{p} = 0$ for all prime ideals $\mathfrak{p} \iff A_\mathfrak{p} = C_\mathfrak{p} \iff A_\mathfrak{p}$ is integrally closed for all prime ideals $\mathfrak{p}$. The same proof works for maximal ideals. □

Theorem 6.19. *Let A be a Noetherian domain of dimension one. Then f.a.e.*

(1) *A is a Dedekind domain.*
(2) *$A_\mathfrak{p}$ is a DVR for all prime ideals $\mathfrak{p} \neq 0$.*

Proof. **(1) $\implies$ (2).** By assumption $A_\mathfrak{p}$ has dimension one. We proved in Lemma 5.18 that if $A \subset B$ is integrally closed and $S \subset A$ is a multiplicative system, then $S^{-1}A$ is integrally closed in $S^{-1}B$. Taking $B = K$ and $S = A\backslash\mathfrak{p}$, we obtain that $A_\mathfrak{p}$ is integrally closed. This implies that $A_\mathfrak{p}$ is a DVR.
(2) $\implies$ (1). As $A_\mathfrak{p}$ is a DVR, it is integrally closed. This implies that A is also integrally closed. If $0 \neq \mathfrak{p} \subset \mathfrak{p}$ are prime ideals, then $0 \neq \mathfrak{p}_\mathfrak{q} \subset A_\mathfrak{q}$ is a non-maximal prime ideal. This contradicts to the assumption that A is a DVR. □

6.3.1. *Fractional ideals.* Let A be an integral domain and K be its field of fractions.

Definition 6.20.

(1) An A-submodule $I \subset K$ is called a *fractional ideal* of A if $aI \subset A$ for some $0 \neq a \in A$.
(2) For any A-submodule $I \subset K$, define $I^{-1} = (A : I) = \{a \in K \,|\, aI \subset A\}$.
(3) An A-submodule $I \subset K$ is called *invertible* if there exists an A-submodule $J \subset K$ such that $IJ = A$. We have then $J = I^{-1}$ as $J \subset I^{-1} = I^{-1}IJ \subset AJ = J$.

Remark 6.21. We have $I^{-1}I \subset A$. If $I \subset A$ is an ideal, then $A \subset I^{-1}$.

Remark 6.22. If $I \subset K$ is invertible, then I is a fractional ideal. Indeed, if $I^{-1}I = A$, then $1 = \sum_{i=1}^n x_i y_i$ for some $x_i \in I^{-1}$ and $y_i \in I$. For any $x \in I$, we have $x = \sum_i (xx_i)y_i$ with $xx_i \in A$. This implies that I is generated by $y_1, \ldots, y_n$, hence is a fractional ideal. The same argument implies that I^{-1} is a fractional ideal.

Remark 6.23. If I, J is are fractional ideals, then $aI \subset A$ and $bJ \subset A$ for some nonzero $a, b \in A$. Therefore $ab(IJ) \subset A$ with $ab \neq 0$, hence IJ is also a fractional ideal. This implies that fractional ideals form a commutative monoid (with an identity given by A).

Exercise 6.24. Show that if $KI = K$, then I^{-1} is isomorphic to $\mathrm{Hom}_A(I, A)$.

Lemma 6.25. *Let A be a Noetherian integral domain and $I \subset K$ be an A-submodule. Then I is a fractional ideal $\iff$ I is finitely generated over A.*

Proof. If I is a fraction ideal, then $aI \subset A$ for some $a \in A$, hence $I \subset \frac{1}{a}A$. The A-module $\frac{1}{a}A \subset K$ is Noetherian, hence I is finitely generated. Let I be finitely generated, say by elements a_i/b_i for $1 \le i \le n$. Taking $b = \prod b_i$, we obtain $bI \subset (a_1, \dots, a_n) \subset A$, hence I is a fractional ideal. □

Lemma 6.26. *Let A be a Noetherian ring and $I \subset A$ be an ideal. Then I contains a product of prime ideals $\mathfrak{p}_1 \dots \mathfrak{p}_n$ such that $I \subset \mathfrak{p}_i$ for all i.*

Proof. Assume the contrary and let I be a maximal ideal that does not satisfy the required property (it exists as A is Noetherian). Then I is not prime, hence $\exists a, b \in A$ such that $ab \in I$, $a \notin I$, $b \notin I$. By maximality of I, ideals $I + aA$, $I + bA$ contain products of non-zero prime ideals (all of primes contain I). Then the product of all these prime ideals is contained in $(I + aA)(I + bA) \subset I + abA = I$, a contradiction. □

Lemma 6.27. *Let A be a Dedekind domain. For any prime $0 \ne \mathfrak{p} \subset A$, we have $\mathfrak{p}^{-1} \ne A$ and $\mathfrak{p}^{-1}\mathfrak{p} = A$.*

Proof. We claim that $\mathfrak{p}^{-1} \ne A$. Choose $0 \ne a \in \mathfrak{p}$ and choose the smallest $n > 0$ such that Aa contains a product of non-zero primes $\mathfrak{p}_1 \dots \mathfrak{p}_n$ (there is such n by the previous result). Then $\mathfrak{p}_1 \dots \mathfrak{p}_n \subset aA \subset \mathfrak{p}$ and $\mathfrak{p}$ contains one of the factors, say $\mathfrak{p}_1$. The prime ideal $\mathfrak{p}_1$ is maximal, hence $\mathfrak{p}_1 = \mathfrak{p}$. By minimality of n, we have $\mathfrak{p}_2 \dots \mathfrak{p}_n \not\subset aA$ and we can choose $b \in \mathfrak{p}_2 \dots \mathfrak{p}_n \backslash aA$. Then $b\mathfrak{p} \subset \mathfrak{p}_1 \dots \mathfrak{p}_n \subset aA$, hence $b/a \in \mathfrak{p}^{-1}$. On the other hand $b/a \notin A$ as $b \notin aA$. We conclude that $\mathfrak{p}^{-1} \ne A$.

To show that $\mathfrak{p}^{-1}\mathfrak{p} = A$, we note that $\mathfrak{p} \subset \mathfrak{p}^{-1}\mathfrak{p} \subset A$ and $\mathfrak{p}$ is maximal. Assume that $\mathfrak{p}^{-1}\mathfrak{p} = \mathfrak{p}$. Then, for any $x \in \mathfrak{p}^{-1}$, we have $x\mathfrak{p} \subset \mathfrak{p}$. This implies that x is integral over A (see Lemma 5.10), hence $x \in A$. We conclude that $\mathfrak{p}^{-1} = A$, a contradiction. □

Theorem 6.28. *Let A be a Dedekind domain. Then every ideal $I \subset A$ can be uniquely (up to a permutation of factors) written as a product of prime ideals $I = \mathfrak{p}_1 \dots \mathfrak{p}_n$.*

Proof. Let $I \ne 0$ be a maximal ideal that can not be written as a product of prime ideals. There exists a maximal ideal $\mathfrak{p}$ that contains I. Then $I_1 = \mathfrak{p}^{-1}I \subset \mathfrak{p}^{-1}\mathfrak{p} = A$ is an ideal in A and $\mathfrak{p}I_1 = (\mathfrak{p}\mathfrak{p}^{-1})I = I$. If I_1 can be written as a product of prime ideals, then we are done. Otherwise, from $I \subset \mathfrak{p}^{-1}I = I_1$ and maximality of I, we conclude that $I = I_1 = \mathfrak{p}^{-1}I$. Then for any $x \in \mathfrak{p}^{-1}$, $xI \subset I$, hence x is integral over A and $x \in A$. This implies $\mathfrak{p}^{-1} = A$, a contradiction.

Assume that $I = \mathfrak{p}_1 \dots \mathfrak{p}_m = \mathfrak{q}_1 \dots \mathfrak{q}_n$. Then $\prod \mathfrak{q}_j \subset \mathfrak{p}_1$, hence $\mathfrak{q}_j \subset \mathfrak{p}_1$ for some j, say $j = 1$. By maximality of $\mathfrak{q}_1$, we conclude that $\mathfrak{p}_1 = \mathfrak{q}_1$. Multiplying both sides with $\mathfrak{p}_1^{-1}$, we obtain $\mathfrak{p}_2 \dots \mathfrak{p}_m = \mathfrak{q}_2 \dots \mathfrak{q}_n$ and conclude by induction that $m = n$ and $\mathfrak{p}_i = \mathfrak{q}_i$ up to a permutation. □

Corollary 6.29. *For any non-zero fractional ideal I, we have $I^{-1}I = A$.*

Proof. We have $aI \subset A$ for some $0 \ne a \in A$. Then $(aI)^{-1} = a^{-1}I^{-1}$ and $II^{-1} = (aI)(aI)^{-1}$. Substituting I by aI, we can assume that $I \subset A$. We can write $I = \mathfrak{p}_1 \dots \mathfrak{p}_n$, where $\mathfrak{p}_i$ are prime. Then $I^{-1} = \mathfrak{p}_1^{-1} \dots \mathfrak{p}_n^{-1}$, hence $II^{-1} = A$.. □

6.4. **AKLB setup.**

Theorem 6.30. *Let A be an integrally closed domain and K be its field of fractions with* $\operatorname{char} K = 0$*. Let L/K be a finite field extension and B be the integral closure of A in L. Then*

(1) *$L = KB$ is the field of fractions of B.*
(2) *There exists a basis $v_1, \dots, v_n$ of L over K such that $B \subset \bigoplus_i Av_i$.*
(3) *If A is a Dedekind domain, then B is a Dedekind domain, finite over A.*

Proof. **(1)** If $x \in L$, then x is algebraic over K, hence satisfies an equation of the form

$$a_m x^m + a_{m-1}x^{m-1} + \cdots + a_0 = 0, \qquad a_i \in A,\ a_m \neq 0.$$

Multiplying this equation by a_m^{m-1}, we see that $a_m x$ is integral over A, hence $a_m x \in B$. Applying this procedure to a basis of L over K, we find a new basis $u_1, \dots, u_n$ with $u_i \in B$, hence $L = KB$. The field of fractions of B contains K and B, hence is equal to L.
(2) For any $x \in L$, consider the multiplication operator $x\colon L \to L$, $y \mapsto xy$, which is K-linear (we obtain an embedding $L \subset \operatorname{End}_K(L)$). Define a K-bilinear form $(x, y) = \operatorname{Tr}_{L/K}(xy)$ on L. This bilinear form is non-degenerate as $(x, x^{-1}) = \operatorname{Tr}_{L/K}(\mathrm{id}) = n \neq 0$ for any $0 \neq x \in L$. Consider the basis $v_1, \dots, v_n$ of L over K dual to $u_1, \dots, u_n$, that is, satisfying $(u_i, v_j) = \delta_{ij}$.

For any $x \in B$, consider the characteristic polynomial $\chi_x(t) = \det_{L/K}(t \cdot \mathrm{id} - x) \in K[t]$. Then x is a root of this polynomial. On the other hand x is a root of some monic polynomial $f \in A[t]$, hence $\chi_x(t)$ is a factor of some power of f. All roots of f (in some finite field extension of K) are integral over A, hence all the coefficients of $\chi_x(t)$ (and in particular $\operatorname{Tr}_{L/K}(x)$) are integral over A, hence $\operatorname{Tr}_{L/K}(x) \in A$. We have $u_i \in B$, hence $xu_i \in B$ and $\operatorname{Tr}_{L/K}(xu_i) \in A$. This implies that $x = \sum_i (x, u_i)v_i \in \sum_i Av_i$, hence $B \subset \bigoplus_i Av_i$.
(3) As A is Noetherian, $B \subset \bigoplus_i Av_i$ is Noetherian as an A-module (in particular, finite over A), hence also Noetherian as a B-module. B is integrally closed by its definition. Let $0 \neq \mathfrak{q} \subset B$ be a prime ideal. Given $0 \neq x \in \mathfrak{q}$, we have

$$x^m + a_{m-1}x^{m-1} + \cdots + a_0 = 0$$

for some $a_i \in A$ with $a_0 \neq 0$. This implies that $a_0 \in Bx \cap A \subset \mathfrak{q} \cap A$, so the prime ideal $\mathfrak{q} \cap A$ is nonzero, hence maximal as A is a Dedekind domain. We conclude that $\mathfrak{q}$ is also maximal by Lemma 5.20. □

Corollary 6.31. *Let K be a finite field extension of $\mathbb{Q}$ and A be the integral closure of $\mathbb{Z}$ in K. Then A is a Dedekind domain and is a free $\mathbb{Z}$-module of rank $[K : \mathbb{Q}]$. The corresponding basis of A over $\mathbb{Z}$ is called an integral basis.*

Proof. As $\mathbb{Z}$ is a Dedekind domain, we conclude that A is a Dedekind domain, finite over $\mathbb{Z}$. This implies that A is a free $\mathbb{Z}$-module of finite rank. If $A = \bigoplus_{i=1}^n \mathbb{Z}v_i$, then v_i are linearly independent over $\mathbb{Q}$ (otherwise there would be a linear dependence over $\mathbb{Z}$). The elements $v_1, \dots, v_n$ generate K over $\mathbb{Q}$ as $K = \mathbb{Q}A$, hence they form a basis of K over $\mathbb{Q}$. □

Example 6.32. Let B be the integral closure of $\mathbb{Z}$ in $L = \mathbb{Q}[\sqrt{m}]$, where $m \in \mathbb{Z}$ is square-free. An element $a + b\sqrt{m} \in L$ has a minimal polynomial $p(x) = x^2 - 2ax + (a^2 - mb^2)$. If this element is integral over $\mathbb{Z}$, then $p(x)$ is a factor of some polynomial in $\mathbb{Z}[x]$, hence $p \in \mathbb{Z}[x]$ by Gauss lemma. This implies that $a + b\sqrt{m} \in B \iff 2a \in \mathbb{Z}$ and $a^2 - mb^2 \in \mathbb{Z}$. In particular, $4mb^2 \in \mathbb{Z}$, hence $2b \in \mathbb{Z}$. If $a = \frac{1}{2}k$ and $b = \frac{1}{2}l$ for $k, l \in \mathbb{Z}$, then one requires $4 \mid (k^2 - ml^2)$. For example

(1) If $m = 2$, then we obtain $2 \mid k$ and $2 \mid l$, hence $B = \mathbb{Z}[\sqrt{2}]$.
(2) If $m = 5$, then we obtain $4 \mid (k^2 - l^2) \iff k \equiv l \pmod 2$. Therefore $B = \mathbb{Z}[\frac{1}{2}(1 + \sqrt{5})]$.
(3) If $m = -5$, then we obtain $4 \mid (k^2 + l^2) \iff 2 \mid k,\ 2 \mid l$. Therefore $B = \mathbb{Z}[\sqrt{-5}]$.
(4) Generally, if $m \not\equiv 1 \pmod 4$, then $B = \mathbb{Z}[\sqrt{m}]$. If $m \equiv 1 \pmod 4$, then $B = \mathbb{Z}[\frac{1}{2}(1 + \sqrt{m})]$.

7. Dimension

7.1. Krull dimension.

Remark 7.1. Consider a vector space $\Bbbk^n$ over a field $\Bbbk$. We can interpret its dimension n as the length of the maximal strictly increasing chain of vector spaces $0 \subset \Bbbk \subset \Bbbk^2 \subset \ldots \subset \Bbbk^n$, where

$$\Bbbk^m = \{(x_1, \ldots, x_m, 0, \ldots, 0) \mid x_i \in \Bbbk \ \forall i \le m\} = Z(x_{m+1}, \ldots, x_n) \subset \Bbbk^n.$$

On the level of ideals in $\Bbbk[x_1, \ldots, x_n]$ we have a chain of length n

$$(x_1, \ldots, x_n) \supset (x_2, \ldots, x_n) \supset \ldots \supset (x_n) \supset 0.$$

Note that all these ideals are prime as $\Bbbk[x_1, \ldots, x_n]/(x_{m+1}, \ldots, x_n) \simeq \Bbbk[x_1, \ldots, x_m]$ is an integral domain. We can use this interpretation to define the dimension of $\Bbbk[x_1, \ldots, x_n]$ or any other ring to be the maximal length of a chain of prime ideals. We don't use arbitrary ideals here as, for example, there is an infinite chain of ideals in $\Bbbk[x]$ (only one of them is prime) $(x) \supset (x^2) \supset (x^3) \supset \ldots$

Definition 7.2. Let A be a ring.

1. A finite sequence $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n \subset A$ of prime ideals is called a *prime chain* of length n.
2. For a prime ideal $\mathfrak{p} \subset A$, we define its height $\operatorname{ht}(\mathfrak{p})$ to be the supremum of the lengths of all prime chains contained in $\mathfrak{p}$.
3. We define the *Krull dimension* $\mathbf{dim}(A)$ of A to be the supremum of the lengths of all prime chains in A. Equivalently,
$$\mathbf{dim}(A) = \sup\{\operatorname{ht}(\mathfrak{p}) \mid \mathfrak{p} \in \operatorname{Spec} A\} = \sup\{\operatorname{ht}(\mathfrak{m}) \mid \mathfrak{m} \in \operatorname{Max} A\}.$$

Example 7.3.

1. If $\Bbbk$ is a field, then $\mathbf{dim}(\Bbbk) = 0$. The only prime chain in $\Bbbk$ is $\mathfrak{p}_0 = 0$ which has length 0.
2. if A is a principal ideal domain, then $\mathbf{dim}\, A = 1$. Maximal prime chains in A are of the form $\mathfrak{p}_0 = 0 \subset \mathfrak{p}_1 = (p)$, where $p \in A$ is a prime element. These chains have length 1.
3. If A is a Dedekind domain, then $\mathbf{dim}\, A = 1$.
4. Let $A = \Bbbk[x_1, \ldots, x_n]$, where $\Bbbk$ is a field. Then there is a prime chain
$$0 \subset (x_1) \subset \ldots \subset (x_1, \ldots, x_n),$$
hence $\mathbf{dim}(A) \ge n$. We will see later that $\mathbf{dim}(A) = n$.

Lemma 7.4. *For every prime ideal $\mathfrak{p} \subset A$, we have*

1. $\operatorname{ht}(\mathfrak{p}) = \mathbf{dim}(A_\mathfrak{p})$.
2. $\mathbf{dim}(A) \ge \operatorname{ht}(\mathfrak{p}) + \mathbf{dim}(A/\mathfrak{p})$.

This lemma implies that $\mathbf{dim}(A) = \sup\{\mathbf{dim}(A_\mathfrak{m}) \mid \mathfrak{m} \in \operatorname{Max} A\}$ and it is enough to know Krull dimensions of local rings.

Lemma 7.5. *Let A be a Noetherian ring. Then $\mathbf{dim}(A) = 0 \iff A$ is Artinian.*

Proof. We have $\mathbf{dim}(A) = 0 \iff$ every prime ideal of A is maximal. This is equivalent to A being Artinian by Theorem 3.20. ☐

Theorem 7.6. *Let $f\colon A \to B$ be a finite (or integral) ring homomorphism. Then $\mathbf{dim}\, A = \mathbf{dim}\, B$.*

Proof. Given a prime chain in B, its preimage in A consists of distinct prime ideals by Cor. 5.21, hence $\mathbf{dim}\, A \ge \mathbf{dim}\, B$. Conversely, any prime chain $\mathfrak{p}_0 \subset \ldots \subset \mathfrak{p}_n$ in A can be lifted to a prime chain $\mathfrak{q}_0 \subset \ldots \subset \mathfrak{q}_n$ in B by Cor. 5.23, hence $\mathbf{dim}\, A \le \mathbf{dim}\, B$. ☐

Lemma 7.7. *We have $\mathbf{dim}\, \Bbbk[x_1, \ldots, x_n] = n$ for any field $\Bbbk$.*

Proof. We have seen that $A = \Bbbk[x_1, \ldots, x_n]$ satisfies $\mathbf{dim}\, A \ge n$. Let $0 = \mathfrak{p}_0 \subset \ldots \subset \mathfrak{p}_k \subset A$ be a prime chain and $0 \ne f \in \mathfrak{p}_1$. Then $\mathbf{dim}(A/Af) \ge k - 1$. There exists a polynomial subalgebra $B = \Bbbk[y_1, \ldots, y_r] \subset A/Af$ such that $r < n$ and A/Af is finite over B (Theorem 5.25). Then $k - 1 \le \mathbf{dim}(A/Af) = \mathbf{dim}\, B = r < n$ (we have $\mathbf{dim}\, B = r$ by induction on n), hence $k \le n$. This implies $\mathbf{dim}\, A \le n$. ☐

7.2. **Hilbert-Poincaré series.**

Definition 7.8.

(1) A *graded ring* A is a ring equipped with a decomposition $A = \bigoplus_{n\geq 0} A_n$, where $A_n \subset A$ are subgroups and $A_m A_n \subset A_{m+n}$.
(2) A *graded A-module* M is an A-module equipped with a decomposition $M = \bigoplus_{n\geq 0} M_n$, where $M_n \subset M$ are subgroups and $A_m M_n \subset M_{m+n}$.
(3) An element $x \in M$ is called *homogeneous* of degree $n \in \mathbb{Z}$ if $x \in M_n$.

Example 7.9. **(1)** Every ring can be considered as a graded ring concentrated in degree zero.
(2) Let A be a ring and $I \subset A$ be an ideal. Then $A^* = \bigoplus_{n\geq 0} I^n/I^{n+1}$ is a graded ring, with $A_0^* = A/I$, $A_1^* = I/I^2$. Multiplication $(I^m/I^{m+1}) \times (I^n/I^{n+1}) \to I^{m+n}/I^{m+n+1}$ is induced by the multiplication in A. Similarly, if M is an A-module, then $M^* = \bigoplus_{n\geq 0} I^n M/I^{n+1}M$ is a graded A^*-module.

Lemma 7.10. *Let A be a graded ring. Then FAE*

(1) *A is Noetherian.*
(2) *A_0 is Noetherian and A is finitely generated as an A_0-algebra.*

Proof. **(1) $\Longrightarrow$ (2).** If A is Noetherian, then $A_0 = A/I$, where $I = \bigoplus_{n\geq 1} A_n$, is also Noetherian. The ideal I is finitely generated over A, say by homogeneous elements $x_1, \ldots, x_r$ of degrees $d_1, \ldots, d_r > 0$. Let us show that these elements generate A as an algebra over A_0. For any $x \in A_n$, we can write $x = \sum a_i x_i$ for some $a_i \in A_{n-d_i}$. By induction, A_{n-d_i} is contained in the algebra generated by $x_1, \ldots, x_r$ over A_0, therefore x is also contained in this algebra.
(2) $\Longrightarrow$ (1). This follows from the Hilbert's basis theorem. □

Lemma 7.11. *Let A be a Noetherian graded ring and M be a finitely-generated graded A-module. Then every M_n is a finitely-generated A_0-module.*

Proof. We can assume that $A = A_0[x_1, \ldots, x_r]$, where x_i has degree $d_i > 0$. Let M be generated by homogeneous elements $m_1, \ldots, m_s$ of degree $k_1, \ldots, k_s$. Every element in M_n can be written in the form $\sum_{i=1}^s a_i m_i$, where $a_i \in A_{n-k_i}$. Therefore M_n is generated over A_0 by the elements $f(x_1, \ldots, x_r)m_i$, where f is a monomial in $x_1, \ldots, x_r$ of total degree $n - k_i$ (there are finitely many such monomials for every $1 \leq i \leq s$). □

If the conditions of Lemma 7.11 are satisfied and $\Bbbk = A_0$ is a field, then every M_n is finite-dimensional over $\Bbbk$ and we define the Hilbert-Poincaré series of M

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

Example 7.12. Let $A = \Bbbk[x]$ be a graded ring with $\deg x = d > 0$. Then

$$P(A,t) = \sum_{k\geq 0} t^{kd} = \frac{1}{1-t^d}.$$

More generally, let $A = \Bbbk[x_1, \ldots, x_r]$ be a graded ring with $\deg x_i = d_i > 0$. Then

$$P(A,t) = \sum_{k_1,\ldots,k_r\geq 0} t^{k_1 d_1 + \cdots + k_r d_r} = \prod_{i=1}^r \frac{1}{1-t^{d_i}}.$$

We will need to generalize Hilbert-Poincaré series to the case where A_0 is Artinian.

Theorem 7.13. *Let A be an Artinian ring and M be a finitely-generated A-module. Then*

(1) *M is both Artinian and Noetherian.*
(2) *M has a composition series, meaning a chain of submodules*

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

such that $M_i/M_{i-1} \neq 0$ is simple for all $1 \leq i \leq n$. We say that M has finite length.
(3) *All composition series of M have the same length, called the length of M and denoted by $\ell(M)$.*

Proof. **(1)** A is Artinian, hence also Noetherian. We can represent M as a quotient of A^r for some $r > 0$. Therefore M is also Artinian and Noetherian.
(2) As M is Artinian, we can choose a minimal nonzero submodule $M_1 \subset M$. Then M_1/M_0 is simple. Similarly, we choose a minimal submodule $M_1 \subsetneq M_2 \subset M$ and show that M_2/M_1 is simple. Continuing this process, we obtain a chain of submodules $0 = M_0 \subset M_1 \subset M_2 \subset \cdots = M$ such that $M_i/M_{i-1} \neq 0$ are simple. As M is Noetherian, this chain should stabilize, hence $M_n = M$ for some $n \geq 0$.
(3) This follows from the Jordan-Hölder theorem. □

Example 7.14. If A is a field and M is a finitely-generated A-module, then M is finite-dimensional and $\ell(M) = \dim M$.

Lemma 7.15. *If $0 \to L \to M \to N \to 0$ is an exact sequence, then $\ell(M) = \ell(L) + \ell(N)$.*

Let A be a Noetherian graded ring and M be a f.g. graded A-module. Assume that A_0 is Artinian (for example a field). Then every M_n is finitely generated over A_0, hence has finite length. We define the *Hilbert-Poincaré series* of M

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

Theorem 7.16 (Hilbert-Serre)**.** *Let A be a graded ring generated over Artinian A_0 by homogeneous elements $x_1, \dots, x_r$ of degrees $d_1, \dots, d_r > 0$. For every graded finitely generated A-module M, the series $P(M,t)$ can be written in the form $f(t)/\prod_i(1-t^{d_i})$ for some polynomial $f \in \mathbb{Z}[t]$.*

Proof. We can assume that $A = A_0[x_1, \dots, x_r]$, where x_i has degree d_i. If $r = 0$, then M is f.g. over $A = A_0$, hence $M_n = 0$ for $n \gg 0$. Therefore $P(M,t)$ is a polynomial.

For any $d \in \mathbb{Z}$, we define the shifted graded A-module $M(d)$ by the rule $M(d)_n = M_{d+n}$. It satisfies $P(M(d),t) = t^{-d}P(M,d)$. There is an exact sequence of graded A-modules

$$0 \to K(-d_r) \to M(-d_r) \xrightarrow{x_r} M \to L \to 0$$

As the length ℓ is additive (with respect to exact sequences), we obtain

$$P(K(-d_r),t) - P(M(-d_r),t) + P(M,t) - P(L,t) = 0,$$

hence $(1-t^{d_r})P(M,t) = P(L,t) - t^{d_r}P(K,t)$.

Multiplication by x_r is trivial on K and L, hence we can consider them as modules over the graded ring $A_0[x_1, \dots, x_{r-1}]$ and apply induction on r. □

Corollary 7.17. *Let $d(M)$ be the pole order of $P(M,t)$ at $t = 1$. Then $d(M) \leq r$, where r is the number of homogeneous generators of A over A_0.*

Lemma 7.18. *Assume that A is generated over A_0 by homogeneous elements $x_1, \dots, x_r$ of degree 1. Then $\ell(M_n)$ is a polynomial in n (with rational coefficients) of degree $d(M) - 1$ for $n \gg 0$. It is called the Hilbert polynomial of M.*

Proof. By the previous theorem, we can write $P(M,t) = f(t)/(1-t)^d$, where $d = d(M)$ and $f(t) \in \mathbb{Z}[t]$ with $f(1) \neq 0$. We have Taylor series

$$(1-t)^{-d} = \sum_{k\geq 0} \frac{d(d+1)\dots(d+k-1)}{k!}t^k = \sum_{k\geq 0} \binom{d+k-1}{d-1} t^k$$

If $f(t) = \sum_{i=0}^N f_i t^i$, then

$$P(M,t) = \sum_{i=0}^N f_i t^i (1-t)^{-d} = \sum_{k\geq 0}\sum_{i=0}^N f_i \binom{d+k-1}{d-1} t^{k+i}$$

hence

$$\ell(M_n) = \sum_{i=0}^N f_i \binom{d+n-i+1}{d-1}, \qquad \text{for } n \gg 0.$$

This is a polynomial in n with the leading term $\sum_{i=0}^N f_i \frac{n^{d-1}}{(d-1)!} = f(1)\frac{n^{d-1}}{(d-1)!} \neq 0$. It has degree $d-1$. □

7.3. **Dimension theorem.** Let $(A,\mathfrak{m})$ be a Noetherian local ring, $I\subset A$ be an $\mathfrak{m}$-primary ideal ($\mathfrak{m}^n\subset I\subset\mathfrak{m}$ for some $n>0$) and let M be a finitely-generated A-module. Consider the graded ring and the graded module

$$A^*=\bigoplus_{n\ge0}I^n/I^{n+1},\qquad M^*=\bigoplus_{n\ge0}I^nM/I^{n+1}M.$$

The ring $A_0^*=A/I$ is Artinian as it is a quotient of $A/\mathfrak{m}^n$. If $x_1,\dots,x_r\in I$ generate I over A, then the the classes $[x_i]\in I/I^2=A_1^*$ generate the algebra A^* over A_0^*. The module M^* is finitely-generated over A^*. By the previous results, the pole order $d(M^*)$ of $P(M^*,t)$ at $t=1$ satisfies $d(M^*)\le r$. Moreover, $\ell(M_n^*)$ is a polynomial in $n\gg0$ of degree $d(M^*)-1$. Therefore the function

$$\chi_I(M,n)=\ell(M/I^nM)=\sum_{k=0}^{n-1}\ell(I^kM/I^{k+1}M)=\sum_{k=0}^{n-1}\ell(M_k^*)$$

is a polynomial in $n\gg0$ of degree $d(M^*)$, called the *Hilbert-Samuel function* (polynomial). We denote $\chi_I(A,n)$ by $\chi_I(n)$.

Remark 7.19. The function $p_i(n)=\sum_{k=0}^{n-1}k^i$ is a polynomial of degree $i+1$ in n. For example, $p_0(n)=n$, $p_1(n)=\frac{n(n-1)}{2}$. For any polynomial $f=\sum_{i=0}^d f_it^i\in\mathbb{Q}[t]$ of degree d, we have

$$g(n)=\sum_{k=0}^{n-1}f(k)=\sum_{i=0}^{d}\sum_{k=0}^{n-1}f_ik^i=\sum_{i=0}^{d}f_ip_i(n)$$

which is a polynomial of degree $d+1$ in n.

Lemma 7.20. *If $\mathfrak{m}^r\subset I\subset\mathfrak{m}$, then $\deg\chi_I(M,n)=\deg\chi_{\mathfrak{m}}(M,n)$. We denote it by $d(M)$.*

Proof. We have $\mathfrak{m}^{rn}M\subset I^nM\subset\mathfrak{m}^nM$, hence $\chi_{\mathfrak{m}}(M,rn)\ge\chi_I(M,n)\ge\chi_{\mathfrak{m}}(M,n)$. Therefore these polynomials have equal degrees. □

Lemma 7.21. *Consider a short exact sequence $0\to L\to M\to N\to0$. Then*

(1) $d(M)=\max\{d(L),d(N)\}$.
(2) $\chi_I(M,n)-\chi_I(L,n)-\chi_I(N,n)$ *is a polynomial of degree* $<d(L)$.

Proof. We have $\ell(N/I^nN)=\ell(M/L+I^nM)\le\ell(M/I^nM)$, hence $d(N)\le d(M)$. Moreover,

$$\chi(M,n)-\chi(N,n)=\ell(M/I^nM)-\ell(M/L+I^nM)=\ell(L+I^nM/I^nM)=\ell(L/L\cap I^nM).\tag{3}$$

One can show that $I(L\cap I^kM)=L\cap I^{k+1}M$ for $k\gg0$ (Artin-Rees lemma). Therefore

$$I^nL\subset L\cap I^nM=I^{n-k}(L\cap I^kM)\subset I^{n-k}L$$

for all $n>k$, hence

$$\ell(L/I^nL)\ge\ell(L/L\cap I^nM)\ge\ell(L/I^{n-k}L).\tag{4}$$

We obtain from (3) and (4) that $\chi(M,n)-\chi(N,n)$ and $\chi(L,n)$ have the same degree and the same leading coefficient. This implies the second statement. If $d(N)<d(M)$, we obtain $d(M)=d(L)=\max\{d(L),d(N)\}$. If $d(N)=d(M)$, we obtain $d(L)\le d(M)$, hence $d(M)=\max\{d(L),d(N)\}$. □

Corollary 7.22. *Let $x\in A$ be a non-zero-divisor. Then $d(A/xA)<d(A)$.*

Proof. Consider an exact sequence $0\to A\xrightarrow{x}A\to A/xA\to0$. By the previous result $\chi(A/xA,n)$ is a polynomial of degree $<d(A)$. □

Theorem 7.23 (Dimension theorem)**.** *For a Noetherian local ring $(A,\mathfrak{m})$, let $d(A)$ denote the degree of the polynomial $\ell(A/\mathfrak{m}^n)$ for $n\gg0$ and $\delta(A)$ denote the minimal number of generators of $\mathfrak{m}$-primary ideals of A. Then*

$$\mathbf{dim}(A)=d(A)=\delta(A).$$

Proof. We will prove inequalities $\mathbf{dim}(A) \le d(A) \le \delta(A) \le \mathbf{dim}(A)$.
(1) $\mathbf{dim}(A) \le d(A)$. If $d(A) = 0$, then $\ell(A/\mathfrak{m}^n)$ is constant for $n \gg 0$, hence $\mathfrak{m}^n = \mathfrak{m}^{n+1}$ for $n \gg 0$. By Nakayama lemma, $\mathfrak{m}^n = 0$. Therefore A is Artinian, hence $\mathbf{dim}\, A = 0$. Let $\mathfrak{p} = \mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \ldots \subset \mathfrak{p}_k$, be a prime chain. Choose $x \in \mathfrak{p}_1 \backslash \mathfrak{p}$. Then $\mathbf{dim}(A/Ax + \mathfrak{p}) \ge k - 1$. The element $[x] \in A/\mathfrak{p}$ is a non-zero-divisor, hence $d(A/Ax + \mathfrak{p}) < d(A/\mathfrak{p}) \le d(A)$. Therefore, by induction on $d(A)$,

$$k - 1 \le \mathbf{dim}(A/Ax + \mathfrak{p}) \le d(A/Ax + \mathfrak{p}) < d(A),$$

hence $k \le d(A)$ and $\mathbf{dim}(A) \le d(A)$.
(2) $d(A) \le \delta(A)$. Let I be an $\mathfrak{m}$-primary ideal with $r = \delta(A)$ generators over A. Then the algebra A^* is generated over A/I by r elements. Therefore $d(A) = d(A^*) \le r$ by the previous results.
(3) $\delta(A) \le \mathbf{dim}(A)$. If $\mathbf{dim}(A) = 0$, then A is Artinian, hence $\mathfrak{m}^n = 0$ for some $n > 0$. Taking $I = \mathfrak{m}^n = 0$, we obtain $\delta(A) = 0$. Let $r = \mathbf{dim}(A) > 0$. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ be minimal prime ideals over 0. If $\mathfrak{m} \subset \bigcup_i \mathfrak{p}_i$, then $\mathfrak{m} \subset \mathfrak{p}_i$ for some i (prime avoidance), hence $\mathfrak{m} = \mathfrak{p}_i$ is a minimal prime ideal and $\mathbf{dim}\, A = 0$, a contradiction. Consider any $x \in \mathfrak{m} \backslash \bigcup_i \mathfrak{p}_i$. Then $\mathbf{dim}(A/Ax) \le r - 1$, hence $\delta(A/Ax) \le r - 1$ by induction and there exists an ideal $\mathfrak{m}^n + Ax \subset I \subset \mathfrak{m}$ such that I/Ax has $r - 1$ generators over A/Ax. Then I has r generators over A, hence $\delta(A) \le r$. □

Lemma 7.24 (Prime avoidance)**.** *Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_r \subset A$ be prime ideals and $I \subset A$ be an ideal such that $I \subset \bigcup_i \mathfrak{p}_i$. Then $I \subset \mathfrak{p}_i$ for some i.*

Proof. Let $I \subset \mathfrak{p}_1 \cup \cdots \cup \mathfrak{p}_r$. We may assume that $\mathfrak{p}_i$ are not contained in each other. Assume that $I \not\subset \mathfrak{p}_i$ for all i. Then $I\mathfrak{p}_1 \ldots \mathfrak{p}_{r-1} \not\subset \mathfrak{p}_r$ and $I \not\subset \mathfrak{p}_1 \cup \cdots \cup \mathfrak{p}_{r-1}$ (by induction). Consider $a \in I\mathfrak{p}_1 \ldots \mathfrak{p}_{r-1} \backslash \mathfrak{p}_r$ and $b \in S = I \backslash (\mathfrak{p}_1 \cup \cdots \cup \mathfrak{p}_{r-1}) \subset \mathfrak{p}_r$. Then $a + b \in I$ and $a + b \notin \mathfrak{p}_i$ for $1 \le i < r$. Therefore $a + b \in S \subset \mathfrak{p}_r$, hence $a = (a + b) - b \in \mathfrak{p}_r$, a contradiction. □

Corollary 7.25. *We have $\mathbf{dim}\, A \le \dim_{A/\mathfrak{m}} \mathfrak{m}/\mathfrak{m}^2$. In particular, $\mathbf{dim}\, A$ is finite.*

Proof. Let $x_1, \ldots, x_r \in \mathfrak{m}$ be elements such that their images in $\mathfrak{m}/\mathfrak{m}^2$ form a basis. By Nakayama lemma, these elements generate $\mathfrak{m}$. Therefore $\mathbf{dim}(A) = \delta(A) \le r = \dim \mathfrak{m}/\mathfrak{m}^2$. □

Example 7.26. Let A be a DVR. Then $\mathbf{dim}(A) = 1$ and $\dim \mathfrak{m}/\mathfrak{m}^2 = 1$, hence $\mathbf{dim}\, A = \dim \mathfrak{m}/\mathfrak{m}^2$ in this case.

Theorem 7.27 (Krull's principal ideal theorem)**.** *Let A be a Noetherian ring and $x \in A$ be a non-zero-divisor and not a unit. Then every minimal prime ideal $\mathfrak{p}$ over (x) has height 1.*

Proof. Taking $A_{\mathfrak{p}}$, we can assume that A is local and $\mathfrak{p}$ is its maximal ideal, hence $\operatorname{ht} \mathfrak{p} = \mathbf{dim}(A)$. Then $\mathfrak{p}$ is the only prime ideal containing (x), hence $\sqrt{(x)} = \mathfrak{p}$ and $\mathfrak{p}^n \subset (x) \subset \mathfrak{p}$ for some $n > 0$. Therefore $\mathbf{dim}(A) = \delta(A) \le 1$. If $\mathbf{dim}(A) = 0$, then A is Artinian, hence $\mathfrak{p}^n = 0$ for some $n > 0$. But this would imply that x is a zero-divisor. □

Lemma 7.28. *Let $(A, \mathfrak{m})$ be a Noetherian local ring and $x \in \mathfrak{m}$ be a non-zero divisor. Then $\mathbf{dim}\, A/(x) = \mathbf{dim}\, A - 1$.*

Proof. Let $Ax \subset \mathfrak{p}_0 \subset \ldots \subset \mathfrak{p}_k = \mathfrak{m}$ be a prime chain with $k = \mathbf{dim}(A/Ax)$. Then $\operatorname{ht} \mathfrak{p}_0 = 1$, hence $\mathbf{dim}\, A \ge k + 1$. On the other hand, let $\mathfrak{m}^n + Ax \subset I \subset \mathfrak{m}$ be an ideal such that I/Ax has $\delta(A/Ax) = k$ generators. Then I has $k+1$ generators, hence $\mathbf{dim}\, A = \delta(A) \le k+1$. We conclude that $\mathbf{dim}\, A = k + 1 = \mathbf{dim}(A/Ax) + 1$. □

Lemma 7.29. *Let A be Noetherian and $\mathfrak{p}$ be a minimal prime ideal over $(a_1, \ldots, a_k) \subset A$. Then $\operatorname{ht} \mathfrak{p} \le k$.*

Proof. Taking $A_{\mathfrak{p}}$ we can assume that A is local and $\mathfrak{p}$ is its maximal ideal. As before, $\mathfrak{p}$ is a minimal prime over $I = (a_1, \ldots, a_k)$, hence it is the only prime ideal containing I. Therefore $\sqrt{I} = \mathfrak{p}$ and $\mathfrak{p}^n \subset I \subset \mathfrak{p}$ for some $n > 0$. We conclude that $\operatorname{ht} \mathfrak{p} = \mathbf{dim}\, A = \delta(A) \le k$. □

Corollary 7.30. *If $\Bbbk$ is algebraically closed, then $\mathbf{dim}\, \Bbbk[x_1, \ldots, x_n] = n$.*

Proof. We have seen that $A = \Bbbk[x_1, \ldots, x_n]$ has dimension $\mathbf{dim}\, A \ge n$. Every maximal ideal of A is of the form $\mathfrak{m} = (x_1 - a_1, \ldots, x_n - a_n)$ for some $a_i \in \Bbbk$. Therefore $\operatorname{ht} \mathfrak{m} \le n$, hence $\mathbf{dim}\, A \le n$. We conclude that $\mathbf{dim}\, A = n$. □

7.4. **Transcendence degree.**

Definition 7.31. Let L/K be a field extension.

(1) We say that elements $a_1, \dots, a_n \in L$ are *algebraically independent* over K if $f(a_1, \dots, a_n) \neq 0$ for all nonzero polynomials $f \in K[x_1, \dots, x_n]$.
(2) Define the *transcendence degree* $\operatorname{trdeg}(L/K)$ of L over K to be the maximal number of algebraically independent elements of L over K.
(3) A collection $(a_1, \dots, a_n)$ of elements in L is called a *transcendence base* of L/K if they are algebraically independent over K and L is algebraic over $K(a_1, \dots, a_n)$.

Example 7.32. We will see that $\operatorname{trdeg}(K(x_1, \dots, x_n)/K) = n$.

Lemma 7.33. *Let $a_1, \dots, a_n \in L$ be algebraically independent over K. Then $b \in L$ is algebraic over $K(a_1, \dots, a_n) \iff a_1, \dots, a_n, b$ are algebraically dependent over K.*

Proof. Assume that b is algebraic over $K(a_1, \dots, a_n)$. Multiplying the corresponding polynomial by the common denominator, we obtain $0 \neq f \in K[a_1, \dots, a_n][x]$ such that $f(b) = 0$. It can be interpreted as a polynomial $f \in K[x_1, \dots, x_n, x]$ such that $f(a_1, \dots, a_n, b) = 0$. The converse is similar. □

Lemma 7.34. *Let $a_1, \dots, a_n \in L$ be algebraically independent over K and $b \in L$ be algebraic over $K(a_1, \dots, a_n)$, but not algebraic over $K(a_2, \dots, a_n)$. Then a_1 is algebraic over $K(b, a_2, \dots, a_n)$.*

Proof. By the previous lemma, the elements $b, a_2, \dots, a_n$ are algebraically independent over K, while the elements $b, a_1, \dots, a_n$ are algebraically dependent. Applying the lemma again, we obtain that a_1 is algebraic over $K(b, a_2, \dots, a_n)$. □

Theorem 7.35. *If $a_1, \dots, a_n \in L$ is a transcendence base over K, then $\operatorname{trdeg}(L/K) = n$.*

Proof. We only have to show that $\operatorname{trdeg}(L/K) \leq n$ and we can assume that n is minimal with the property that $a_1, \dots, a_n \in L$ is a transcendence base over K. Assume that $b_1, \dots, b_m \in L$ are algebraically independent over K. We will prove by induction on k that

$$S_k = \{b_1, \dots, b_k, a_{k+1}, \dots, a_n\}$$

is a transcendence base (after reordering a_i). This is true for $k = 0$. Assume that it is true for k. Then b_{k+1} is algebraic over $K(S_k)$. This implies that $b_1, \dots, b_{k+1}, a_{k+1}, \dots, a_n$ are algebraically dependent over K. Then there exists $i \geq k+1$ such that $S = \{b_1, \dots, b_{k+1}, a_{k+1}, \dots, a_{i-1}\}$ is algebraically independent, while $S \cup \{a_i\}$ is algebraically dependent. Then a_i is algebraic over $K(S_{k+1})$, where $S_{k+1} = S_k \cup \{b_{k+1}\} \backslash \{a_i\}$, hence L is also algebraic over $K(S_{k+1})$. The set S_{k+1} is algebraically independent by minimality of n, hence is a transcendence base. If $m > n$, then $S_n = \{b_1, \dots, b_n\}$ is a transcendence base, hence b_{n+1} is algebraic over $K(b_1, \dots, b_n)$, a contradiction. This implies that $\operatorname{trdeg}(L/K) \leq n$. □

Lemma 7.36. *Let $K \subset L \subset M$ be field extensions. Then*

$$\operatorname{trdeg}(M/K) = \operatorname{trdeg}(L/K) + \operatorname{trdeg}(M/L).$$

Proof. Let $S = \{a_1, \dots, a_m\}$ be a transcendence base of L/K and $T = \{b_1, \dots, b_n\}$ be a transcendence base of M/L. Then $S \cup T$ is algebraically independent over K. Moreover, L is algebraic over $K(S)$, hence $L(T)$ is algebraic over $K(S \cup T)$. As M is algebraic over $L(T)$, we obtain that M is algebraic over $K(S \cup T)$. □

Let now A be an integral domain, finitely generated over a field K and let L be the fraction field of A. It is a finitely generated field extension of K, hence $\operatorname{trdeg}(L/K) < \infty$.

Theorem 7.37. *We have $\mathbf{dim}\, A = \operatorname{trdeg}(L/K)$.*

Proof. By Noether normalization theorem, we can embed $B = K[x_1, \dots, x_n] \subset A$ so that A is finite over B. Then $\mathbf{dim}\, A = \mathbf{dim}\, B = n$ by Theorem 7.6 and Cor. 7.30.

Let $L' = K(x_1, \dots, x_n)$ be the field of fractions of B. Then L is a finite field extension of L', hence $\operatorname{trdeg}(L/K) = \operatorname{trdeg}(L'/K) = n$. □

Remark 7.38. One can show that for any maximal ideal $\mathfrak{m} \subset A$, we have $\operatorname{ht} \mathfrak{m} = \operatorname{trdeg}(L/K)$.

Appendix A. Categories and functors

Definition A.1. A *category* $\mathcal{A}$ consists of the following data

(1) A family $\operatorname{Ob}\mathcal{A}$, whose elements are called objects of $\mathcal{A}$.
(2) For all objects X, Y of $\mathcal{A}$, a set $\operatorname{Hom}(X,Y) = \operatorname{Hom}_{\mathcal{A}}(X,Y)$, whose elements are called morphisms from X to Y.
(3) For all objects X, Y, Z of $\mathcal{A}$, a map

$$\operatorname{Hom}(X,Y) \times \operatorname{Hom}(Y,Z) \to \operatorname{Hom}(X,Z), \qquad (f,g) \mapsto g \circ f,$$

called the composition map.

This data should satisfy

(1) $\forall X \in \operatorname{Ob}\mathcal{A}$, $\exists 1_X \in \operatorname{Hom}(X,X)$ s.t. $1_Y \circ f = f \circ 1_X = f$ for any $f \in \operatorname{Hom}(X,Y)$.
(2) The composition of morphisms is associative.

Remark A.2.

(1) The element 1_X is unique for every $X \in \operatorname{Ob}\mathcal{A}$.
(2) We write $f\colon X \to Y$ for $f \in \operatorname{Hom}(X,Y)$.
(3) A morphism $f\colon X \to Y$ is called an isomorphism if $\exists g\colon Y \to X$ such that $gf = 1_X$ and $fg = 1_Y$.

Example A.3.

(1) The category $\operatorname{Mod} A$ of modules over a ring A and homomorphisms between them.
(2) The category Set of sets and all maps between them.
(3) The category Top of topological spaces and continuous maps between them.
(4) The category Com of commutative rings and ring homomorphisms.
(5) The category Grp of groups and group homomorphisms.
(6) The category Ab of abelian groups and group homomorphisms. It can be identified with $\operatorname{Mod}\mathbb{Z}$.

Definition A.4. Let $\mathcal{A}$ and $\mathcal{B}$ be two categories. A *(covariant) functor* F from $\mathcal{A}$ to $\mathcal{B}$ consists of the following data

(1) A map $F\colon \operatorname{Ob}(\mathcal{A}) \to \operatorname{Ob}(\mathcal{B})$.
(2) A map $F\colon \operatorname{Hom}_{\mathcal{A}}(X,Y) \to \operatorname{Hom}_{\mathcal{B}}(FX,FY)$ for all objects $X, Y \in \operatorname{Ob}(\mathcal{A})$.

This data should satisfy

(1) $F(1_X) = 1_{FX}$ for all $X \in \operatorname{Ob}(\mathcal{A})$.
(2) $F(g \circ f) = F(g) \circ F(f)$.

Definition A.5.

(1) Given a category $\mathcal{A}$, we define the *opposite category* $\mathcal{A}^{\mathrm{op}}$ using the data

$$\operatorname{Ob}(\mathcal{A}^{\mathrm{op}}) = \operatorname{Ob}(\mathcal{A}), \qquad \operatorname{Hom}_{\mathcal{A}^{\mathrm{op}}}(X,Y) = \operatorname{Hom}_{\mathcal{A}}(Y,X).$$

(2) A functor from $\mathcal{A}^{\mathrm{op}}$ to $\mathcal{B}$ is called a *contravariant functor* from $\mathcal{A}$ to $\mathcal{B}$.

Example A.6.

(1) Given a category $\mathcal{A}$ and an object X, there is a (covariant) functor

$$\operatorname{Hom}(X,-)\colon \mathcal{A} \to \mathrm{Set}, \qquad Y \mapsto \operatorname{Hom}(X,Y).$$

There is also a contravariant functor

$$\operatorname{Hom}(-,X)\colon \mathcal{A} \to \mathrm{Set}, \qquad Y \mapsto \operatorname{Hom}(Y,X).$$

(2) For the category $\operatorname{Mod} A$ and an A-module M, we have similar functors $\operatorname{Hom}(M,-)$ and $\operatorname{Hom}(-,M)$ from $\operatorname{Mod} A$ to $\operatorname{Mod} A$.
(3) For any A-module N, there is a functor

$$-\otimes N\colon \operatorname{Mod} A \to \operatorname{Mod} A, \qquad M \mapsto M \otimes N.$$

Definition A.7. Let F, G be two functors from $\mathcal{A}$ to $\mathcal{B}$. A *morphism* (or natural transformation) ϕ from F to G consists of the data

(1) Morphism $\phi_X\colon FX \to GX$ for every object $X \in \operatorname{Ob}(\mathcal{B})$

such that for every $f \in \mathrm{Hom}_{\mathcal{A}}(X,Y)$ the following diagram commutes

$$\begin{array}{ccc} FX & \xrightarrow{F(f)} & FY \\ {\scriptstyle \phi_X}\downarrow & & \downarrow{\scriptstyle \phi_Y} \\ GX & \xrightarrow{G(f)} & GY \end{array}$$

Definition A.8. Let $f\colon A \to B$ be a ring homomorphism.

(1) Given a B-module M, we can consider it as an A-module by setting $ax = f(a)x$ for $a \in A$, $x \in M$. In this way we obtain a functor $\mathrm{Mod}\, B \to \mathrm{Mod}\, A$, called a *restriction of scalars*.

(2) Given an A-module M, we consider a B-module

$$M_B = B \otimes_A M, \qquad b(b' \otimes x) = bb' \otimes x, \qquad b, b' \in B,\ x \in M.$$

In this way we obtain a functor $B \otimes_A -\colon \mathrm{Mod}\, A \to \mathrm{Mod}\, B$, called an *extension of scalars*.

Definition A.9. Two functors $F\colon \mathcal{A} \to \mathcal{B}$, $G\colon \mathcal{B} \to \mathcal{A}$ are called *adjoint* if there exist natural bijections

$$\mathrm{Hom}_{\mathcal{B}}(F(X), Y) \simeq \mathrm{Hom}_{\mathcal{A}}(X, G(Y)) \qquad \forall\ X \in \mathrm{Ob}(\mathcal{A}),\ Y \in \mathrm{Ob}(\mathcal{B}).$$

In this case F is called a *left adjoint* functor to G and G is called a *right adjoint* functor to F.

Example A.10. There is a Tensor-Hom adjunction (see Lemma 2.18)

$$\mathrm{Hom}(L \otimes M, N) \simeq \mathrm{Hom}(L, \mathrm{Hom}(M, N)).$$

for A-modules L, M, N. It implies that the functors

$$F\colon\ \mathrm{Mod}\, A \to \mathrm{Mod}\, A, \qquad L \mapsto L \otimes M,$$
$$G\colon\ \mathrm{Mod}\, A \to \mathrm{Mod}\, A, \qquad N \mapsto \mathrm{Hom}(M, N)$$

are adjoint.

Appendix B. Limits

Recall that a *poset* (a *partially ordered set*) $\mathcal{I}$ is a set equipped with a binary relation $\le$ (a subset $R \subseteq \mathcal{I} \times \mathcal{I}$, where $(x, y) \in R$ is denoted as $x \le y$) satisfying

(1) $x \le x$ for $x \in \mathcal{I}$.
(2) $x \le y$ and $y \le x \implies x = y$ for $x, y \in \mathcal{I}$.
(3) $x \le y$ and $y \le z \implies x \le z$ for $x, y, z \in \mathcal{I}$.

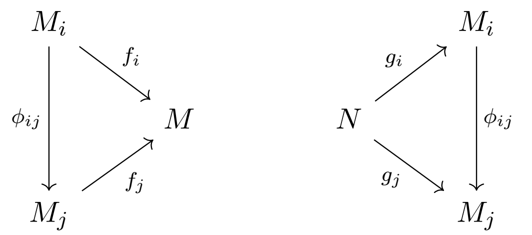
A poset $\mathcal{I}$ is called a *chain* (or a *totally ordered set*) if $x \le y$ or $y \le x$ for all $x, y \in \mathcal{I}$.

Example B.1.

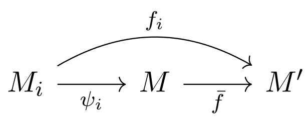
(1) The sets $\mathbb{N}, \mathbb{Z}, \mathbb{R}$ with the usual order are chains.
(2) The set $\mathbb{N}^2$ with the order $(i, j) \le (i', j')$ if $i \le i'$ and $j \le j'$ is a poset. Note that $(1, 0)$ and $(0, 1)$ are incomparable, hence the order is partial.
(3) A set $\mathcal{I}$ with the only relations $x \le x$ for $x \in \mathcal{I}$ is a poset.
(4) The power set 2^X of a set X is the set of all subsets of X. It has the partial order given by inclusion of sets: $U \le V \iff U \subseteq V$. Every subset of 2^X has the induced partial order. In particular, for a commutative ring A, the spectrum $\operatorname{Spec} A \subset 2^A$ is partially ordered.

Definition B.2. Let $\mathcal{I}$ be a poset.

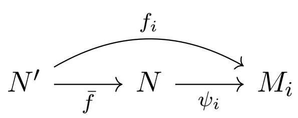
(1) Define an $\mathcal{I}$-*diagram* of modules to be a family $(M_i)_{i \in \mathcal{I}}$ of A-modules together with homomorphisms $\phi_{ij} \colon M_i \to M_j$ for $i \le j$ such that $\phi_{ii} = \mathrm{id}$ for $i \in \mathcal{I}$ and $\phi_{jk} \circ \phi_{ij} = \phi_{ik}$ for all $i \le j \le k$.
(2) Given an $\mathcal{I}$-diagram $(M_i)_{i \in \mathcal{I}}$ and modules M, N, define a morphism $f \colon (M_i)_i \to M$ to be a collection of homomorphisms $(f_i \colon M_i \to M)_i$ such that $f_j \circ \phi_{ij} = f_i$ for all $i \le j$. Define a morphism $g \colon N \to (M_i)_i$ to be a collection of homomorphisms $(g_i \colon N \to M_i)_i$ such that $\phi_{ij} \circ g_i = g_j$ for all $i \le j$.



(3) Given an $\mathcal{I}$-diagram of modules $(M_i)_{i \in \mathcal{I}}$, define its *direct limit* (or colimit) $\varinjlim_{i \in \mathcal{I}} M_i$ to be an A-module M with a morphism $\psi \colon (M_i)_i \to M$ such that, for any module M' with a morphism $f \colon (M_i)_i \to M'$ there exists a unique morphism $\bar{f} \colon M \to M'$ such that $\bar{f} \circ \psi_i = f_i \ \forall i \in \mathcal{I}$.



(4) Given an $\mathcal{I}$-diagram of modules $(M_i)_{i \in \mathcal{I}}$, define its *inverse limit* $\varprojlim_{i \in \mathcal{I}} M_i$ to be an A-module N with a morphism $\psi \colon N \to (M_i)_i$ such that, for any module N' with a morphism $f \colon N' \to (M_i)_i$ there exists a unique morphism $\bar{f} \colon N' \to N$ such that $\psi_i \circ \bar{f} = f_i \ \forall i \in \mathcal{I}$.



Example B.3. Let $(M_i)_{i \in \mathcal{I}}$ be a family of modules. Equip $\mathcal{I}$ with the partial order $i \le i$ for $i \in \mathcal{I}$. Then $\varinjlim_i M_i = \bigoplus_i M_i$ and $\varprojlim_i M_i = \prod_i M_i$.

Remark B.4. Note that direct and inverse limits are unique up to an isomorphism.

Theorem B.5. *Any $\mathcal{I}$-diagram of modules has a direct limit and an inverse limit.*

Theorem B.6. *Given a poset $\mathcal{I}$ and an $\mathcal{I}$-diagram of A-modules $(M_i)_{i\in\mathcal{I}}$, we have*

$$\varprojlim_i M_i = \left\{ x \in \prod_i M_i \;\middle|\; x_j = \phi_{ij}(x_i)\ \forall i \le j \right\}.$$

Proof. It is easy to see that the above subset $M \subset \prod_i M_i$ is an A-submodule. We define $\psi_i \colon M \hookrightarrow \prod_i M_i \xrightarrow{\pi_i} M_i$, where the first map is an embedding and the second map is the canonical projection. If $f \colon M' \to (M_i)_i$ is a morphism, then we obtain a canonical morphism $\bar{f} \colon M' \to \prod_i M_i$ by the universal property of products. Given $y \in M'$ and $x = \bar{f}(y) \in \prod_i M_i$, we have $x_i = f_i(y)$ and $\phi_{ij}(x_i) = \phi_{ij} f_i(y) = f_j(y) = x_j$ for all $i \le j$. This implies that $\bar{f}(y) = x \in M$ and we obtain a homomorphism $\bar{f} \colon M' \to M$ as required in the definition of an inverse limit. □

Theorem B.7. *Let $\mathcal{I}$ be a filtered poset (i.e. $\forall i, j \in \mathcal{I}\ \exists k \in \mathcal{I}$ with $i \le k$, $j \le k$) and $(M_i)_{i\in\mathcal{I}}$ be an $\mathcal{I}$-diagram of A-modules. Then $\varinjlim_i M_i = \bigcup_i M_i / \sim$, where for $x_i \in M_i$, $x_j \in M_j$*

$$x_i \sim x_j \iff \exists k \ge i, j \text{ with } \phi_{ik}(x_i) = \phi_{jk}(x_j).$$

Appendix C. Primary decomposition

Throughout this section we will assume that A is a Noetherian ring. This implies that every set of ideals of A has a maximal element.

Definition C.1. Let M be an A-module.

(1) A prime ideal $\mathfrak{p} \subset A$ is called *associated* to M if $\mathfrak{p} = \operatorname{Ann} x$ for some $x \in M$. Equivalently, M contains a submodule isomorphic to $A/\mathfrak{p}$ (consider $A/\mathfrak{p} \to M$, $[a] \mapsto ax$). The set of all primes associated to M is denoted by $\operatorname{Ass}(M) = \operatorname{Ass}_A(M)$.
(2) M is called *co-primary* if it has only one associated prime.
(3) A submodule $N \subset M$ (or an ideal $I \subset A$) is called *primary* if M/N (respectively A/I) is co-primary. Submodule N is called $\mathfrak{p}$-*primary* if $\operatorname{Ass}(M/N) = \{\mathfrak{p}\}$.

Example C.2. For any prime ideal $\mathfrak{p} \subset A$, we have $\operatorname{Ass}_A(A/\mathfrak{p}) = \{\mathfrak{p}\}$. Indeed, for every $0 \neq [x] \in A/\mathfrak{p}$, we have $\operatorname{Ann}_A[x] = \{a \in A \mid ax \in \mathfrak{p}\} = \mathfrak{p}$: if $a \in \mathfrak{p}$, then $ax \in \mathfrak{p}$ and conversely, if $ax \in \mathfrak{p}$, then $a \in \mathfrak{p}$ as $x \notin \mathfrak{p}$ and $\mathfrak{p}$ is prime.

Remark C.3. We will see later that an ideal $I \subset A$ is primary $\iff$

$$ab \in I \implies a^n \in I \text{ for some } n \geq 1 \text{ or } b \in I. \tag{5}$$

Moreover, the associated prime to A/I is equal to $\sqrt{I}$. Equivalently, every zero divisor in A/I is nilpotent.

Let us show currently that condition (5) implies that $\mathfrak{p} = \sqrt{I}$ is prime and I is $\mathfrak{p}$-primary. If $ab \in \sqrt{I} \implies (ab)^m \in I$ for some $m > 0 \implies a^{mn} \in I$ for some $n > 0$ or $b^m \in I \implies a \in \sqrt{I}$ or $b \in \sqrt{I}$. If $\mathfrak{q} = \operatorname{Ann}_A[b]$ is prime for some $0 \neq [b] \in A/I$, then $I \subset \mathfrak{q} \subset \sqrt{I} = \mathfrak{p}$. The first inclusion implies $\mathfrak{p} = \sqrt{I} \subset \mathfrak{q}$, hence $\mathfrak{q} = \mathfrak{p}$. Therefore $\operatorname{Ass} A/I = \{\mathfrak{p}\}$ (assuming that it is non-empty, which we will prove shortly) and I is $\mathfrak{p}$-primary.

Condition (5) means that a primary ideal is an analogue of an ideal $(p^n) \subset \mathbb{Z}$ for a prime number $p \in \mathbb{Z}$. If $ab \in (p^n)$, then $p^n \mid ab$. Therefore either $p \mid a$ and then $p^n \mid a^n$ or $p \nmid a$ and then $p^n \mid b$. This means that either $a^n \in (p^n)$ or $b \in (p^n)$. The primary decomposition that we will discuss later is an analogue of the fact that every nonzero integer $m \in \mathbb{Z}$ can be written in the form $m = \prod_i p_i^{n_i}$ with distinct p_i. In terms of ideals this means $(m) = \prod_i (p_i^{n_i}) = \bigcap_i (p_i^{n_i})$.

Example C.4.

(1) A prime ideal is primary.
(2) An ideal $(n) \subset \mathbb{Z}$ is primary $\iff$ $n = 0$ or n is a prime power.
(3) If $\mathfrak{m} = \sqrt{I}$ is a maximal ideal, then I is primary and $\mathfrak{m}$ is the associated prime. The maximal ideal $\mathfrak{m}/I = \sqrt{I}/I = \mathcal{N}(A/I)$ is contained in every prime ideal of A/I, hence $\mathfrak{m}/I$ is the only prime ideal. Every zero divisor of A/I is contained in $\mathfrak{m}/I = \mathcal{N}(A/I)$, hence is nilpotent.
(4) Let $A = \Bbbk[x, y]$ and $I = (x, y^2)$. Then $\mathfrak{m} = \sqrt{I} = (x, y)$ is a maximal ideal, hence I is primary. Note that I is not a power of $\mathfrak{m}$.
(5) Let $A = \Bbbk[x, y, z]/(xy - z^2)$ and $\mathfrak{p} = (x, z)_A$. Then $A/\mathfrak{p} \simeq \Bbbk[y]$, hence $\mathfrak{p}$ is prime. The ideal $I = \mathfrak{p}^2 = (x^2, xz, xy)_A = x(x, y, z)_A$ is not primary. The element $x + I \in A/I$ has annihilator $(x, y, z)_A$ which is maximal and different from $\mathfrak{p} = \sqrt{I}$. Another way to see that $\mathfrak{p}^2$ is not primary is to consider $xy = z^2 \in \mathfrak{p}^2$ and note that $x \notin \mathfrak{p}^2$ while $y \notin \sqrt{\mathfrak{p}^2} = \mathfrak{p}$.

Lemma C.5. *Let M be a nonzero A-module.*

(1) *If $\mathfrak{p}$ is a maximal element in the set of ideals $\{\operatorname{Ann} x \mid 0 \neq x \in M\}$, then $\mathfrak{p} \in \operatorname{Ass}(M)$. In particular, $\operatorname{Ass} M$ is nonempty.*
(2) *For every $0 \neq x \in M$, the ideal $\operatorname{Ann} x$ is contained in some prime associated to M.*

Proof. **(1)** We need to show that $\mathfrak{p}$ is prime. Let $\mathfrak{p} = \operatorname{Ann}(x)$, $ab \in \mathfrak{p}$ and $b \notin \mathfrak{p}$. Then $bx \neq 0$ and $abx = 0$. As $\mathfrak{p} = \operatorname{Ann}(x) \subset \operatorname{Ann}(bx)$ is maximal, we obtain $\mathfrak{p} = \operatorname{Ann}(bx)$, hence $a \in \operatorname{Ann}(bx) = \mathfrak{p}$. **(2)** Follows from 1. □

Lemma C.6. *Let $0 \to L \to M \to N \to 0$ be a short exact sequence of A-modules. Then*

$$\operatorname{Ass} L \subset \operatorname{Ass} M \subset \operatorname{Ass} L \cup \operatorname{Ass} N.$$

Proof. If $\mathfrak{p} \in \operatorname{Ass} L$, then $A/\mathfrak{p}$ is isomorphic to a submodule of L, hence to a submodule of M. Therefore $\mathfrak{p} \in \operatorname{Ass} M$.

Let $\mathfrak{p} \subset M$ and $M' \subset M$ be isomorphic to $A/\mathfrak{p}$. If $L \cap M' = 0$, then $M' \to N$ is injective, hence $\mathfrak{p} \in \operatorname{Ass} N$. If $L \cap M' \neq 0$, let $0 \neq x \in L \cap M'$. We have seen that $\operatorname{Ann} x = \mathfrak{p}$ for all $0 \neq x \in M' \simeq A/\mathfrak{p}$, hence $\mathfrak{p} \in \operatorname{Ass} L$. □

Lemma C.7. *If $N, N' \subset M$ are $\mathfrak{p}$-primary, then $N \cap N'$ is also $\mathfrak{p}$-primary.*

Proof. There is an injection $M/N \cap N' \to M/N_1 \oplus M/N_2$, hence $\varnothing \neq \operatorname{Ass}(M/N_1 \cap N_2) \subset \operatorname{Ass}(M/N_1) \cup \operatorname{Ass}(M/N_2) = \{\mathfrak{p}\}$. □

Definition C.8. Let $N \subset M$ be a submodule. A *primary decomposition* of N is an expression of N as a finite intersection

$$N = \bigcap_{i=1}^{n} Q_i$$

of primary submodules $Q_i \subset M$. Such a decomposition is called *irredundant* (or minimal) if no Q_i can be omitted and the associated primes of M/Q_i are all distinct.

Theorem C.9 (Lasker-Noether)**.** *Let M be a finitely-generated module over a Noetherian ring A. Then every (proper) submodule $N \subset M$ has an irredundant primary decomposition.*

Proof. We say that $N \subset M$ is irreducible in M if whenever $N = N_1 \cap N_2$, we have $N = N_1$ or $N = N_2$. Let $N \subset M$ be a maximal submodule that is not a finite intersection of irreducible submodules. Then N is not irreducible, hence $N = N_1 \cap N_2$, where N_1, N_2 are strictly greater than N, hence can be written as finite intersections of irreducibles. This implies that N is also a finite intersection of irreducibles. We claim that if $N \subset M$ is irreducible, then N is primary. Taking M/N, we can assume that $N = 0$. Assume that $\mathfrak{p}, \mathfrak{q} \in \operatorname{Ass}(M)$ and $\mathfrak{p} \neq \mathfrak{q}$. Then M contains submodules isomorphic to $A/\mathfrak{p}$ and $A/\mathfrak{q}$. We have seen that $\operatorname{Ann}_A[x] = \mathfrak{p}$ for every $0 \neq [x] \in A/\mathfrak{p}$ and similarly for $\mathfrak{q}$. Therefore the intersection of these submodules is equal to zero, hence $N = 0$ is not irreducible, a contradiction.

If any Q_i can be removed from the intersection, we omit it. If Q_i, Q_j have the same associated prime, we consider $Q_i \cap Q_j$ which is again primary. □

Lemma C.10. *Let $N \subset M$ be a submodule and $N = \cap_{i=1}^{n} Q_i$ be an irredundant primary decomposition with $\operatorname{Ass} M/Q_i = \{\mathfrak{p}_i\}$. Then $\operatorname{Ass} M/N = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$.*

Proof. There is an injection $M/N \to \bigoplus_i M/Q_i$, hence $\operatorname{Ass} M/N \subset \cup_i \operatorname{Ass} M/Q_i = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$.

Let $N' = Q_2 \cap \ldots Q_n$. Then $N = Q_1 \cap N'$ and $N'/N = N'/Q_1 \cap N' \simeq (Q_1 + N')/Q_1 \subset M/Q_1$, hence $\operatorname{Ass} N'/N \subset \operatorname{Ass} M/Q_1 = \{\mathfrak{p}_1\} \implies \mathfrak{p}_1 \in \operatorname{Ass} N'/N \subset \operatorname{Ass} M/N$. Similarly $\mathfrak{p}_i \in \operatorname{Ass} M/N$ for all i. □

Lemma C.11. *If M is a finitely generated A-module, then there exists a chain of submodules*

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

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

Proof. If $M \neq 0$, choose $\mathfrak{p}_1 \in \operatorname{Ass} M$ and $M_1 \subset M$ isomorphic to $A/\mathfrak{p}_1$. Then apply the same procedure to M/M_1 to find M_2, and so on. As M is finitely-generated and A is Noetherian, we obtain that M is also Noetherian, hence an increasing chain of submodules stabilizes and our process stops after a finite number of steps. □

We have seen already that a Noetherian module has a primary decomposition, hence has a finite number of associated ideals. Here is a direct proof of this fact.

Lemma C.12. *Let M be a finitely-generated A-module. Then $\operatorname{Ass} M$ is a finite set.*

Proof. Consider the chain from Lemma C.11. Then $\operatorname{Ass} M \subset \cup_i \operatorname{Ass} M_i/M_{i-1}$. Moreover, we have $M_i/M_{i-1} \simeq A/\mathfrak{p}_i$, hence $\operatorname{Ass} M_i/M_{i-1} = \{\mathfrak{p}_i\}$. □

Let $S \subset A$ be a multiplicative set and $i\colon A \to S^{-1}A$, $a \mapsto a/1$ be the natural ring homomorphism. We proved in Theorem 1.38 that there is a bijection

$$i^*\colon \operatorname{Spec}(S^{-1}A) \xrightarrow{\sim} \{\mathfrak{p} \in \operatorname{Spec} A \mid \mathfrak{p} \cap S = \varnothing\}, \qquad \mathfrak{q} \mapsto i^{-1}(\mathfrak{q})$$

with an inverse given by $\mathfrak{p} \mapsto S^{-1}\mathfrak{p}$.

Lemma C.13. *Given an A-module M, the map $i^*\colon \operatorname{Spec} S^{-1}A \to \operatorname{Spec} A$ induces a bijection*

$$\operatorname{Ass}_{S^{-1}A} S^{-1}M \simeq \{\mathfrak{p} \in \operatorname{Ass}_A M \mid \mathfrak{p} \cap S = \varnothing\}.$$

Proof. Let $\mathfrak{q} = \operatorname{Ann}_{S^{-1}A}(m/s)$ be prime, for some $m/s \in S^{-1}M$, and let $\mathfrak{p} = i^{-1}(\mathfrak{q}) = (a_1, \dots, a_n)$ ($\mathfrak{p}$ is finitely-generated as A is Noetherian). Then $a_i m/s = 0$ in $S^{-1}M$, hence $a_i t_i m = 0$ for some $t_i \in S$. With $t = \prod_i t_i$, we have $a_i tm = 0 \implies a_i \in \operatorname{Ann}(tm) \implies \mathfrak{p} \subset \operatorname{Ann}(tm)$. Conversely, if $a \in \operatorname{Ann}(tm)$, then $ats \cdot m/s = 0$ in $S^{-1}M \implies ats/1 \in \mathfrak{q} \implies a/1 \in \mathfrak{q}$ and $a \in \mathfrak{p}$.

On the other hand, let $\mathfrak{p} = \operatorname{Ann}_A(m)$ be prime, for some $m \in M$, and let $\mathfrak{p} \cap S = \varnothing$. We claim that $\mathfrak{q} = S^{-1}\mathfrak{p} \subset S^{-1}A$ is equal to $\operatorname{Ann}_{S^{-1}A}(m/1)$. For any $a/s \in S^{-1}\mathfrak{p}$, we have $a/s \cdot m/1 = am/s = 0$, hence $a/s \in \operatorname{Ann}_{S^{-1}A}(m/1)$. Conversely, if $a/s \in \operatorname{Ann}_{S^{-1}A}(m/1)$, then $am/s = 0 \implies atm = 0$ for some $t \in S \implies at \in \operatorname{Ann}_A(m) = \mathfrak{p} \implies a \in \mathfrak{p}$ as $t \in S$ and $S \cap \mathfrak{p} = \varnothing$. ☐

Remark C.14. For any prime ideal $\mathfrak{p} \subset A$, consider the multiplicative set $S = A \backslash \mathfrak{p}$. Then we obtain a bijection between $\operatorname{Ass}_{A_\mathfrak{p}} M_\mathfrak{p}$ and $\{\mathfrak{p}' \in \operatorname{Ass}_A M \mid \mathfrak{p}' \subset \mathfrak{p}\}$.

Theorem C.15. *We have*

$$\operatorname{Ass}(M) \subset \operatorname{Supp}(M) = \{\mathfrak{p} \in \operatorname{Spec} A \mid M_\mathfrak{p} \neq 0\}$$

and every minimal element of $\operatorname{Supp}(M)$ *is in* $\operatorname{Ass}(M)$.

Proof. If $\mathfrak{p} \in \operatorname{Ass} M$, then there exists an exact sequence $0 \to A/\mathfrak{p} \to M$, hence $0 \to (A/\mathfrak{p})_\mathfrak{p} \to M_\mathfrak{p}$. The residue field $(A/\mathfrak{p})_\mathfrak{p} = A_\mathfrak{p}/\mathfrak{p}_\mathfrak{p}$ is nonzero, hence $M_\mathfrak{p} \neq 0$.

Let $\mathfrak{p} \in \operatorname{Supp} M$ be a minimal element. Localizing with respect to $S = A \backslash \mathfrak{p}$, we obtain that $\mathfrak{p} \in \operatorname{Ass}_A M \iff \mathfrak{p}A_\mathfrak{p} \in \operatorname{Ass}_{A_\mathfrak{p}} M_\mathfrak{p}$ (by the previous lemma). After localization we can assume that $A = A_\mathfrak{p}$ and $M = M_\mathfrak{p}$. Then all prime ideals are contained in $\mathfrak{p}$ and by the minimality of $\mathfrak{p}$, $\operatorname{Supp} M = \{\mathfrak{p}\}$. As $\operatorname{Ass} M \subset \operatorname{Supp} M$ is non-empty, we conclude that $\mathfrak{p} \in \operatorname{Ass} M$. ☐

Lemma C.16. *Let M be a finitely-generated non-zero A-module. Then*

1. *M is co-primary* $\iff \operatorname{Ann} x \subset \sqrt{\operatorname{Ann} M}$ *for $0 \neq x \in M$. The associated prime of M is* $\sqrt{\operatorname{Ann} M}$.
2. *Ideal $I \subset A$ is primary $\iff ab \in I$ implies $a \in \sqrt{I}$ or $b \in I$, for $a, b \in A$. The associated prime of A/I is $\sqrt{I}$.*

Proof. **(1)** Let $\operatorname{Ass} M = \{\mathfrak{p}\}$. By Lemma C.5, $\operatorname{Ann} x$ is contained in some prime associated to M, hence $\operatorname{Ann} x \subset \mathfrak{p}$. As M is finitely-generated, we have $\operatorname{Supp} M = Z(\operatorname{Ann} M)$ (prove this!). By Theorem C.15, $\mathfrak{p}$ is the unique minimal prime ideal over $\operatorname{Ann} M$ (see Lemma 3.15), hence $\sqrt{\operatorname{Ann} M} = \mathfrak{p}$ and $\operatorname{Ann} x \subset \mathfrak{p} = \sqrt{\operatorname{Ann} M}$.

Conversely, let $I = \sqrt{\operatorname{Ann} M}$. For every $\mathfrak{p} \in \operatorname{Ass} M$, we have $\mathfrak{p} = \operatorname{Ann} x \subset \sqrt{\operatorname{Ann} M} = I$, for some $0 \neq x \in M$, by our assumption. On the other hand $\operatorname{Ann} M \subset \operatorname{Ann} x = \mathfrak{p}$, hence $I = \sqrt{\operatorname{Ann} M} \subset \mathfrak{p}$. We conclude that $I = \mathfrak{p}$, hence I is prime and $\operatorname{Ass} M = \{I\}$.
(2) Consider $M = A/I$. Then $\operatorname{Ann} M = I$ and we apply the previous statement. ☐