



UiO : **Department of Mathematics**
University of Oslo

MAT4200 Autumn 2025

Commutative algebra revision

December 4, 2025

Rings

A ring is a commutative ring with unity: a set A equipped with addition $a + b$ and multiplication ab such that

- $(A, +)$ is an abelian group
- Multiplication is associative and commutative
- The distributive law $a(b + c) = ab + ac$ holds
- There is an element $1 \in A$ such that $1a = a$ for all a .

Basic examples

- $\mathbb{Z}, \mathbb{Z}/n, \mathbb{Q}, \mathbb{R}, \mathbb{C}$.
- For any ring A , the ring $A[x_1, \dots, x_n]$ of polynomials in n variables.

Homomorphisms

A **homomorphism of rings** is a map $\varphi: A \rightarrow B$ preserving addition, multiplication and 1, i.e. for all $x, y \in A$ we have

$$\varphi(x + y) = \varphi(x) + \varphi(y), \quad \varphi(xy) = \varphi(x)\varphi(y), \quad \varphi(1) = 1.$$

If φ is bijective it is an **isomorphism**; we write $A \cong B$.

Basic examples

- The natural maps $\mathbb{Z} \rightarrow \mathbb{Q} \rightarrow \mathbb{R} \rightarrow \mathbb{C}$ and $\mathbb{Z} \rightarrow \mathbb{Z}/n$ are homomorphisms.
- For a ring A and elements $b_1, \dots, b_n \in A$, a homomorphism $\varphi: A[x_1, \dots, x_n] \rightarrow A$ is given by

$$\varphi\left(\sum a_{i_1 \dots i_n} x_1^{i_1} \cdots x_n^{i_n}\right) = \sum a_{i_1 \dots i_n} b_1^{i_1} \cdots b_n^{i_n}.$$

Ideals and quotient rings

An **ideal** is a subgroup I of $(A, +)$ such that $ax \in I$ for all $a \in A, x \in I$.

The **quotient ring** A/I is the set of cosets of I in $(A, +)$, with addition and multiplication defined by

$$\begin{aligned}(x + I) + (y + I) &= (x + y) + I, \\ (x + I)(y + I) &= xy + I.\end{aligned}$$

The quotient homomorphism $\varphi: A \rightarrow A/I$ is given by

$$\varphi(x) = x + I.$$

Ideals, examples

- For any homomorphism of rings $\varphi: A \rightarrow B$, the kernel

$$\ker \varphi = \varphi^{-1}(0) \subseteq A$$

is an ideal.

- Given $f \in A$, the ideal

$$(f) = \{xf \mid x \in A\}$$

is the **principal ideal** generated by f .

- Given $f_1, \dots, f_n \in A$, the ideal generated by the f_i is

$$(f_1, f_2, \dots, f_n) = \left\{ \sum_{i=1}^n x_i f_i \mid x_i \in A \right\}.$$

Ideals of this form are called **finitely generated**.

Fundamental homomorphism theorem of rings

Theorem (Fundamental homomorphism theorem)

Let $\varphi: A \rightarrow B$ be a ring homomorphism. Then:

- *the image $\text{im } \varphi \subseteq B$ is a subring of B ;*
- *there is a ring isomorphism*

$$\bar{\varphi}: A / \ker \varphi \xrightarrow{\cong} \text{im } \varphi$$

such that $\bar{\varphi}(a + \ker \varphi) = \varphi(a)$ for all $a \in A$.

In particular, every surjective homomorphism $\varphi: A \twoheadrightarrow B$ induces an isomorphism

$$A / \ker \varphi \cong B.$$

Quotient rings, examples

- $\mathbb{Z}/(n)$ = ring of integers mod n .
- For $n \geq 1$ such that n is not a square number,

$$\mathbb{Z}[x]/(x^2 - n) = \mathbb{Z}[\sqrt{n}] \cong \{a + b\sqrt{n} \mid a, b \in \mathbb{Z}\} \subset \mathbb{Q}.$$

- For $n \leq -1$,

$$\mathbb{Z}[x]/(x^2 - n) = \mathbb{Z}[i\sqrt{n}] \cong \{a + ib\sqrt{n} \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}.$$

- Given $a_1, \dots, a_n \in A$,

$$A[x_1, \dots, x_n]/(x_1 - a_1, \dots, x_n - a_n) \cong A.$$

- If k is a field and $f \in k[x]$ is irreducible, then $k[x]/(f)$ is a finite extension field of k .

Prime and maximal ideals

- An element $x \in A$ is a **unit** if there is $y \in A$ such that $yx = 1$.
- An ideal $P \subseteq A$ is **prime** if $P \neq (1)$ and $x, y \notin P$ implies $xy \notin P$.
- An ideal $\mathfrak{m} \subseteq A$ is **maximal** if $\mathfrak{m} \neq (1)$ and there is no ideal $\mathfrak{m} \subsetneq I \subsetneq (1)$.
- A ring A is an **integral domain** if A is not the 0 ring, and $x, y \neq 0$ implies $xy \neq 0$.
- A ring A is a **field** if A is not the 0 ring, and $x \neq 0$ implies x is a unit.

The spectrum of a ring

The set of prime ideals in a ring A is called the **spectrum of A** and is denoted $\text{Spec}(A)$.

Prime and maximal ideals

Theorem

Let $I \subseteq A$ be an ideal.

- *I prime $\iff A/I$ is an integral domain.*
- *I maximal $\iff A/I$ is a field.*
- *I maximal $\Rightarrow I$ prime.*

Prime and maximal ideals, examples

- In $\mathbb{Z}$, the prime ideals are (0) and (p) for all primes p . The maximal ideals are the primes except for (0) .
- If k is a field, then in $k[x]$, the prime ideals are (0) and (f) with f irreducible. The maximal ideals are the prime ideals except for (0) .
- Let k be a field, $a_1, \dots, a_n \in k$. Then

$$(x_1 - a_1, x_2 - a_2, \dots, x_n - a_n) \subset k[x_1, \dots, x_n]$$

is a maximal ideal.

Principal ideal domains

An integral domain A is a **principal ideal domain** (PID) if every ideal is principal.

Examples

- All fields are PIDs.
- $\mathbb{Z}$
- $k[x]$ for k a field.

UFDs

Let A be an integral domain.

Irreducible elements

An element $a \in A$ is irreducible if a is neither 0 nor a unit, and if $bc = a$ implies either b or c is a unit.

Unique Factorisation Domain

An integral domain A is a UFD if every non-zero $a \in A$ admits a factorisation

$$a = p_1 \cdot \dots \cdot p_n$$

where the p_i are irreducible, and moreover this factorisation is unique up to reordering the p_i and multiplying by units.

UFDs, properties and examples

Irreducible versus prime

If A is an UFD and $a \in A \setminus (0)$, then a is irreducible $\iff (a)$ is a prime ideal.

For a general integral domain A , only $\Leftarrow$ holds.

Theorem

Every PID is an UFD.

Gauss' lemma

If A is an UFD, then $A[x]$ is an UFD.

Corollary

$\mathbb{Z}[x_1, \dots, x_n]$ is a UFD. If k is a field, $k[x_1, \dots, x_n]$ is an UFD.

Maximal ideals exist

Theorem (Krull's theorem)

If A is a non-zero ring, then there is a maximal ideal $\mathfrak{m} \subset A$.

Strengthening

If A is a ring and $I \subsetneq A$ an ideal, then there is a maximal ideal $\mathfrak{m} \supseteq I$.

Corollary

For any $f \in A$

f is a unit $\iff (f) = (1) \iff f$ lies in no maximal ideal.

Operations on ideals

Given ideals $I_1, \dots, I_n \subseteq A$, we define new ideals by:

- **Ideal sum**

$$I_1 + \dots + I_n = \{x_1 + \dots + x_n \mid x_i \in I_i\}.$$

- **Intersection** $I_1 \cap \dots \cap I_n$.

- **Product**

$$I_1 \cdots I_n = \{\text{all finite sums of products } x_1 \cdots x_n \mid x_i \in I_i\}.$$

- **Ideal quotient**

$$(I_1 : I_2) = \{x \in A \mid xI_2 \subseteq I_1\}.$$

- **Radical** of an ideal I :

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

Finitely generated ideals

An ideal $I \subseteq A$ is **finitely generated** if we can find $f_1, \dots, f_n \in A$ such that

$$I = (f_1, f_2, \dots, f_n).$$

We say that $f_1, \dots, f_n$ **generate** I .

Rewriting finitely generated ideals

Given $a, f_1, \dots, f_n \in A$, $1 \leq i \neq j \leq n$,

$$(f_1, \dots, f_n) = (f_1, \dots, f_{i-1}, f_i + af_j, f_{i+1}, \dots, f_n).$$

Given a unit $u \in A$, we have

$$(f_1, \dots, f_n) = (f_1, \dots, f_{i-1}, uf_i, f_{i+1}, \dots, f_n).$$

The nilradical

An element $f \in A$ is **nilpotent** if there is an $n \geq 1$ such that $f^n = 0$. The **nilradical** of A is

$$N = \sqrt{(0)} = \{f \in A \mid f \text{ is nilpotent}\}.$$

Theorem

The nilradical of A equals the intersection of all prime ideals of A .

Corollary

For any ideal $I \subseteq A$, we have that $\sqrt{I}$ equals the intersection of all prime ideals containing I .

Extension and contraction of ideals

Let $\varphi: A \rightarrow B$ be a homomorphism. We move ideals between A and B :

- If $J \subseteq B$ is an ideal, its **contraction** along φ is the ideal $\varphi^{-1}(J) \subseteq A$.
- If $I \subseteq A$ is an ideal, its **extension** along φ denoted $\varphi(I)B \subseteq B$, is the smallest ideal of B containing $\varphi(I)$. Concretely

$$\varphi(I)B = \left\{ \sum_{i=1}^n b_i \varphi(x_i) \mid b_i \in B, x_i \in I \right\}.$$

Theorem

If $P \subset B$ is a prime ideal, then so is $\varphi^{-1}(P) \subset A$.

Ideals in quotient rings

Let $I \subseteq A$ be an ideal, and let $\varphi: A \rightarrow A/I$ be the quotient homomorphism. We have a bijection

$$\begin{aligned} \{\text{Ideals of } A/I\} &\leftrightarrow \{\text{Ideals of } A \text{ containing } I\} \\ J &\mapsto \varphi^{-1}(J) \\ K/I &\leftrightarrow K \end{aligned}$$

This sends prime (resp. maximal) ideals to prime (resp. maximal) ideals.

Extension and contraction, examples

- If $\varphi: A \rightarrow B$ is the inclusion of a subring and $J \subseteq B$ an ideal, then $\varphi^{-1}(J) = J \cap A$.
- For $\varphi: A \rightarrow A[x]$ the standard inclusion and $I \subseteq A$, we have

$$\varphi(I)A[x] = I[x] = \left\{ \sum_{i=1}^n a_i x^i \mid a_i \in I \right\} \subseteq A[x].$$

Coprime ideals

Two ideals $I, J \subseteq A$ are **coprime** if $I + J = (1)$.

Theorem (The Chinese remainder theorem)

If $I_1, \dots, I_n$ are pairwise coprime, then $I_1 \cap \dots \cap I_n = I_1 \cdots I_n$ and

$$\begin{aligned} A/(I_1 \cap \dots \cap I_n) &\cong A/I_1 \times \dots \times A/I_n \\ a + I_1 \cap \dots \cap I_n &\mapsto (a + I_1, \dots, a + I_n) \end{aligned}$$

Example

- In $\mathbb{Z}$, ideals (m) and (n) are coprime $\iff m$ and n are coprime.
- If $k_1, \dots, k_n$ are pairwise coprime integers, we get

$$\mathbb{Z}/(k_1 \cdots k_n) \cong \mathbb{Z}/k_1 \times \dots \times \mathbb{Z}/k_n.$$

Local rings

A ring A is **local** if it has a *unique* maximal ideal $\mathfrak{m}$.

Theorem

A ring A is local if and only if its set of non-units forms an ideal. If A is local, then the set of non-units is the maximal ideal.

Examples

- All fields are local.
- $k[x]/(x^n)$ is local, with maximal ideal $(x)/(x^n)$.
- $\mathbb{Z}_{(2)} = \{m/n \mid m \in \mathbb{Z}, n \in \mathbb{Z} \setminus (2)\} \subset \mathbb{Q}$ is local, with maximal ideal

$$\{m/n \mid m \in (2), n \in \mathbb{Z} \setminus (2)\}.$$

Modules

A **module** over a ring A is an abelian group M equipped with an operation of multiplication from A

$$A \times M \rightarrow M, \quad (a, m) \mapsto am$$

satisfying a short list of axioms (distributivity, associativity, etc.).

Examples

- If k is a field, then a k -module is the same thing as a k -vector space (the axioms are the same).
- A $\mathbb{Z}$ -module is the same thing as an abelian group.

Modules, examples

- Every ring A is an A -module in a natural way.
- Every ideal of A is an A -module in a natural way.
- Given A -modules M, N , we get an A -module

$$M \oplus N = \{(m, n) \mid m \in M, n \in N\},$$

with $(m, n) + (m', n') = (m + m', n + n')$ and $a(m, n) = (am, an)$.

- Given a ring homomorphism $\varphi: A \rightarrow B$, B is an A -module via $ab = \varphi(a)b$ for $a \in A, b \in B$.

Homomorphism of modules

A **homomorphism of A -modules** is a map $\varphi: M \rightarrow N$ respecting multiplication from A and addition; for all $a \in A$, $m, n \in M$, we have

$$\varphi(am) = a\varphi(m), \quad \varphi(m + n) = \varphi(m) + \varphi(n).$$

It is an **isomorphism** if it is bijective. The set of homomorphisms from M to N is a module, denoted $\text{Hom}_A(M, N)$ **Examples**

- If M is an A -module and $x \in A$, we have a homomorphism $\varphi: M \rightarrow M$ given by $\varphi(m) = xm$.
- If $m \in M$, we get a homomorphism $\varphi: A \rightarrow M$ by $\varphi(x) = xm$.

Sub- and quotient modules

Let M be an A -module. Then $M' \subseteq M$ is a **submodule** if it is a subgroup of $(M, +)$ and closed under multiplication from A , i.e.

$$x \in M', a \in A \Rightarrow ax \in M'.$$

It follows that M' inherits a module structure from $(M, +)$, and the quotient group M/M' is an A -module by setting

$$a(m + M') = am + M' \quad \forall a \in A, m \in M$$

Example

- Given an ideal $I \subset A$ and an A -module M , we have the submodule

$$IM = \left\{ \sum_{i=1}^n a_i m_i \mid a_i \in I, m_i \in M \right\} \subseteq M.$$

Module isomorphism theorems

- Given a homomorphism of modules $\varphi: M \rightarrow N$, we have that $\operatorname{im} \varphi \subseteq N$ is a submodule, and

$$\operatorname{im}(\varphi) \cong M / \ker \varphi.$$

- Given A -modules $M \subseteq N \subseteq P$, we have that $N/M \subseteq P/M$ is a submodule, and an isomorphism

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

- Given submodules $P, N \subseteq M$, we have an isomorphism

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

Kernels, images and cokernels

Given a homomorphism of modules $\varphi: M \rightarrow N$, there are three main associated modules:

- **Kernel:** $\ker \varphi = \varphi^{-1}(0) \subseteq M$.
- **Image:** $\operatorname{im} \varphi = \{\varphi(m) \mid m \in M\}$.
- **Cokernel:** $\operatorname{cok} \varphi = N / \operatorname{im} \varphi$.

We have

$$\begin{aligned}\varphi \text{ injective} &\iff \ker \varphi = 0 \iff M \rightarrow \operatorname{im} \varphi \text{ is an isomorphism} \\ \varphi \text{ surjective} &\iff \operatorname{cok} \varphi = 0 \iff \operatorname{im} \varphi \rightarrow N \text{ is an isomorphism}\end{aligned}$$

Exact sequences

A sequence of homomorphisms of modules

$$M_1 \xrightarrow{\varphi_1} M_2 \xrightarrow{\varphi_2} \dots \xrightarrow{\varphi_{n-1}} M_n$$

is **exact at** M_i if $\ker \varphi_i = \operatorname{im} \varphi_{i-1}$. It is **exact** if it is exact at M_i for $2 \leq i \leq n-1$.

Examples

- A sequence $M \xrightarrow{\varphi} M'' \rightarrow 0$ is exact if and only if φ is surjective.
- A sequence $0 \rightarrow M' \xrightarrow{\varphi} M$ is exact if and only if φ is injective.
- A sequence $0 \rightarrow M \xrightarrow{\varphi} N \rightarrow 0$ is exact if and only if φ is an isomorphism.

Short exact sequences

An exact sequence of the form

$$0 \rightarrow M' \xrightarrow{i} M \xrightarrow{p} M'' \rightarrow 0$$

is called **short exact**. The sequence being exact is equivalent to:

- 1 i is injective,
- 2 p is surjective, and
- 3 $\text{im}(i) = \ker(p)$.

Standard short exact sequence

Every short exact sequence is isomorphic to one of the form

$$0 \rightarrow M \rightarrow N \rightarrow N/M \rightarrow 0.$$

Additive functions

A function ν defined on some set of modules with values in an abelian group is called **additive** if for every short exact sequence

$$0 \rightarrow M' \rightarrow M \rightarrow M'' \rightarrow 0,$$

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

Examples

- Finite $\mathbb{Z}$ -modules, $\nu(M) = |M| \in \mathbb{Q}^\times$.
- k a field, finite dimensional k -modules, $\nu(M) = \dim_k(M) \in \mathbb{Z}$.

Proposition

If ν is additive and

$$0 \rightarrow M_1 \rightarrow \cdots \rightarrow M_n \rightarrow 0$$

is exact, then $\sum_{i=1}^n (-1)^i \nu(M_i) = 0$.

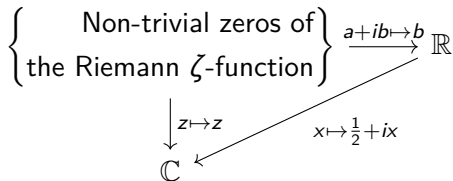
Commutative diagrams

A collection of modules and homomorphisms between them forms a **commutative diagram** if, for any two modules M, N in the diagram, all ways to compose homomorphisms to obtain a homomorphism from M to N agree.

This diagram is commutative if and only if $\gamma \circ \beta = \delta \circ \alpha$:

$$\begin{array}{ccc} M & \xrightarrow{\beta} & N \\ \downarrow \alpha & & \downarrow \gamma \\ P & \xrightarrow{\delta} & Q \end{array}$$

This diagram is commutative if and only if the Riemann hypothesis holds:



Snake lemma

Assume we are given a commutative diagram of A -modules where the rows are exact:

$$\begin{array}{ccccccccc}
 0 & \longrightarrow & M' & \xrightarrow{i_M} & M & \xrightarrow{\pi_M} & M'' & \longrightarrow & 0 \\
 & & \downarrow \varphi' & & \downarrow \varphi & & \downarrow \varphi'' & & \\
 0 & \longrightarrow & N' & \xrightarrow{i_N} & N & \xrightarrow{\pi_N} & N'' & \longrightarrow & 0.
 \end{array}$$

Then we have an exact sequence

$$0 \rightarrow \ker \varphi' \rightarrow \ker \varphi \rightarrow \ker \varphi'' \rightarrow \operatorname{cok} \varphi' \rightarrow \operatorname{cok} \varphi \rightarrow \operatorname{cok} \varphi'' \rightarrow 0.$$

Free modules

An A -module M is **free** if it is isomorphic to $A^{\oplus \Lambda}$ for some set Λ . It is free of **finite rank** n if Λ is a finite set of n elements.

Homomorphisms of finite rank free modules

If A is a ring, then every homomorphism of free A -modules

$$\varphi: A^m \longrightarrow A^n$$

is given by multiplication by a unique $(n \times m)$ -matrix with entries in A , so we have

$$\operatorname{Hom}_A(A^m, A^n) \cong A^{mn}$$

Presentation of modules

A **presentation** of an A -module M is the data of sets G , R , and homomorphisms φ, ψ giving an exact sequence

$$A^{\oplus R} \xrightarrow{\psi} A^{\oplus G} \xrightarrow{\varphi} M \rightarrow 0$$

- We have $M \cong A^{\oplus G} / \operatorname{im} \psi$.
- Every A -module admits a presentation.
- If M has a presentation with G, R finite, we say that M is **finitely presented**.

Finitely generated modules

An A -module M is **finitely generated** if equivalently

- 1 It admits a presentation $A^{\oplus R} \rightarrow A^{\oplus G} \rightarrow M \rightarrow 0$ with G finite.
- 2 there is a surjective homomorphism of A -modules $A^n \rightarrow M$, or
- 3 M is isomorphic to A^n/K for some submodule $K \subseteq A^n$, or
- 4 there are elements $m_1, \dots, m_n \in M$ such that every $m \in M$ can be written as

$$m = a_1 m_1 + \cdots + a_n m_n, \quad a_i \in A.$$

Nakayama's lemma

In all statements, let A be a local ring with maximal ideal $\mathfrak{m}$, and let M be a finitely generated A -module.

Theorem (Nakayama's lemma)

If $\mathfrak{m}M = M$, then $M = 0$.

Corollary

- *A homomorphism $\varphi: N \rightarrow M$ is surjective if and only if the composed map $N \xrightarrow{\varphi} M \rightarrow M/\mathfrak{m}M$ is surjective.*
- *Elements $x_1, \dots, x_n \in M$ generate M as an A -module if and only if $x_1 + \mathfrak{m}M, \dots, x_n + \mathfrak{m}M$ generate $M/\mathfrak{m}M$ as an $A/\mathfrak{m}$ -module.*

Categories

A **category** $\mathcal{C}$ is the data of

- a collection of **objects**, $\text{Ob}(\mathcal{C})$,
- for every pair of objects $X, Y \in \text{Ob}(\mathcal{C})$, a set of **morphisms** $\text{Mor}_{\mathcal{C}}(X, Y)$.
- for all $X, Y, Z \in \text{Ob}(\mathcal{C})$ a **composition map** $\circ$

$$\begin{aligned}\text{Mor}_{\mathcal{C}}(X, Y) \times \text{Mor}_{\mathcal{C}}(Y, Z) &\rightarrow \text{Mor}_{\mathcal{C}}(X, Z) \\ (f, g) &\mapsto g \circ f.\end{aligned}$$

This data must satisfy, for all f, g, h such that composition is defined:

- 1 Associativity: $(f \circ g) \circ h = f \circ (g \circ h)$
- 2 Existence of identity morphisms: For every object X , there is an $\text{id}_X \in \text{Mor}_{\mathcal{C}}(X, X)$ such that $f \circ \text{id}_X = f$, and $\text{id}_X \circ g = g$.

Categories, examples

In this course we care about two examples:

- The category **Ring**:
 - Objects of **Ring** are rings.
 - Given rings A, B , we define

$$\text{Mor}_{\text{Ring}}(A, B) = \{\text{Ring homomorphisms } \varphi: A \rightarrow B\},$$

and composition in the usual way.

- Let A be a ring. The category Mod_A has:
 - Objects of Mod_A are A -modules.
 - Given A -modules M, N , we define

$$\begin{aligned}\text{Mor}_{\text{Mod}_A}(M, N) &= \text{Hom}_A(M, N) \\ &= \{\text{Module homomorphisms } \varphi: M \rightarrow N\},\end{aligned}$$

and composition in the usual way.

Covariant functors

Definition

Given categories $\mathcal{C}, \mathcal{D}$, a **covariant functor** $F: \mathcal{C} \rightarrow \mathcal{D}$ is given by a map $F: \text{Ob } \mathcal{C} \rightarrow \text{Ob } \mathcal{D}$, together with, for each $X, Y \in \text{Ob } \mathcal{C}$, a map $F: \text{Mor}_{\mathcal{C}}(X, Y) \rightarrow \text{Mor}_{\mathcal{D}}(F(X), F(Y))$, such that

- 1 Composition is preserved: Given $X \xrightarrow{f} Y \xrightarrow{g} Z$ in $\mathcal{C}$, we have

$$F(g \circ_{\mathcal{C}} f) = F(g) \circ_{\mathcal{D}} F(f)$$

- 2 Identities are preserved:

$$F(\text{id}_X) = \text{id}_{F(X)} \quad \forall X \in \text{Ob } \mathcal{C}.$$

Contravariant functors

Definition

Given categories $\mathcal{C}, \mathcal{D}$, a **contravariant functor** $F: \mathcal{C} \rightarrow \mathcal{D}$ is given by a map $F: \text{Ob } \mathcal{C} \rightarrow \text{Ob } \mathcal{D}$, together with, for each $X, Y \in \text{Ob } \mathcal{C}$, a map $F: \text{Mor}_{\mathcal{C}}(X, Y) \rightarrow \text{Mor}_{\mathcal{D}}(F(Y), F(X))$, such that

- 1 Composition is preserved: Given $X \xrightarrow{f} Y \xrightarrow{g} Z$ in $\mathcal{C}$, we have

$$F(g \circ_{\mathcal{C}} f) = F(f) \circ_{\mathcal{D}} F(g)$$

- 2 Identities are preserved:

$$F(\text{id}_X) = \text{id}_{F(X)} \quad \forall X \in \text{Ob } \mathcal{C}.$$

Hom functors

Let M be an A -module. We have a *covariant* functor

$\text{Hom}_A(M, -): \text{Mod}_A \rightarrow \text{Mod}_A$ given by

- On objects: $\text{Hom}_A(M, -)(N) = \text{Hom}_A(M, N)$
- On morphisms: Given $\psi \in \text{Hom}_A(N, P)$ have

$$\begin{aligned}\text{Hom}_A(M, -)(\psi): \text{Hom}_A(M, N) &\rightarrow \text{Hom}_A(M, P) \\ \text{Hom}_A(M, -)(\psi)(\varphi) &= \psi \circ \varphi.\end{aligned}$$

We have a *contravariant* functor $\text{Hom}_A(-, M): \text{Mod}_A \rightarrow \text{Mod}_A$ given by

- On objects: $\text{Hom}_A(-, M)(N) = \text{Hom}_A(N, M)$
- On morphisms: Given $\psi \in \text{Hom}_A(N, P)$ have

$$\begin{aligned}\text{Hom}_A(-, M)(\psi): \text{Hom}_A(P, M) &\rightarrow \text{Hom}_A(N, M) \\ \text{Hom}_A(-, M)(\psi)(\varphi) &= \varphi \circ \psi.\end{aligned}$$

Exactness of functors

A covariant functor $F: \text{Mod}_A \rightarrow \text{Mod}_B$ is **left exact** if for all short exact sequences in Mod_A

$$0 \rightarrow M' \rightarrow M \rightarrow M'' \rightarrow 0$$

the sequence

$$0 \rightarrow F(M') \rightarrow F(M) \rightarrow F(M'')$$

in Mod_B is exact.

Exactness of functors

A covariant functor $F: \text{Mod}_A \rightarrow \text{Mod}_B$ is **right exact** if for all short exact sequences in Mod_A

$$0 \rightarrow M' \rightarrow M \rightarrow M'' \rightarrow 0$$

the sequence

$$F(M') \rightarrow F(M) \rightarrow F(M'') \rightarrow 0$$

in Mod_B is exact.

Exactness of functors

A covariant functor $F: \text{Mod}_A \rightarrow \text{Mod}_B$ is **exact** if for all short exact sequences in Mod_A

$$0 \rightarrow M' \rightarrow M \rightarrow M'' \rightarrow 0$$

the sequence

$$0 \rightarrow F(M') \rightarrow F(M) \rightarrow F(M'') \rightarrow 0$$

in Mod_B is exact. If F is exact, then every exact sequence in Mod_A (not necessarily short) is sent to an exact sequence in Mod_B

Exactness of functors

A contravariant functor $F: \text{Mod}_A \rightarrow \text{Mod}_B$ is **left exact** if for all short exact sequences in Mod_A

$$0 \rightarrow M' \rightarrow M \rightarrow M'' \rightarrow 0$$

the sequence

$$0 \rightarrow F(M'') \rightarrow F(M) \rightarrow F(M')$$

in Mod_B is exact.

Exactness of functors

A contravariant functor $F: \text{Mod}_A \rightarrow \text{Mod}_B$ is **right exact** if for all short exact sequences in Mod_A

$$0 \rightarrow M' \rightarrow M \rightarrow M'' \rightarrow 0$$

the sequence

$$F(M'') \rightarrow F(M) \rightarrow F(M') \rightarrow 0$$

in Mod_B is exact.

Exactness of functors

A contravariant functor $F: \text{Mod}_A \rightarrow \text{Mod}_B$ is **exact** if for all short exact sequences in Mod_A

$$0 \rightarrow M' \rightarrow M \rightarrow M'' \rightarrow 0$$

the sequence

$$0 \rightarrow F(M'') \rightarrow F(M) \rightarrow F(M') \rightarrow 0$$

in Mod_B is exact.

If F is exact, then every exact sequence in Mod_A (not necessarily short) is sent to an exact sequence in Mod_B

Exactness of Hom functors

Let M be an A -module. Both $\text{Hom}_A(M, -)$ and $\text{Hom}_A(-, M)$ are left exact: Given an exact sequence

$$0 \rightarrow N' \rightarrow N \rightarrow N'' \rightarrow 0,$$

the sequences

$$0 \rightarrow \text{Hom}_A(M, N') \rightarrow \text{Hom}_A(M, N) \rightarrow \text{Hom}_A(M, N'')$$

and

$$0 \rightarrow \text{Hom}_A(N'', M) \rightarrow \text{Hom}_A(N, M) \rightarrow \text{Hom}_A(N', M)$$

are exact.

Tensor product

Let M, N and P be A -modules. A map $\varphi: M \times N \rightarrow P$ is **A -bilinear** if for $x, x' \in M$, $y, y' \in N$ and $a \in A$ we have

$$\begin{aligned}\varphi(x + x', y) &= \varphi(x, y) + \varphi(x', y), \\ \varphi(x, y + y') &= \varphi(x, y) + \varphi(x, y'), \\ \varphi(ax, y) &= \varphi(x, ay) = a\varphi(x, y).\end{aligned}$$

Theorem

There exists a module $M \otimes_A N$ together with a bilinear map $\chi: M \times N \rightarrow M \otimes_A N$ such that every bilinear map $\varphi: M \times N \rightarrow P$ can be factored uniquely as $\varphi = \psi \circ \chi$ for an A -module homomorphism $\psi: M \otimes_A N \rightarrow P$. The module $M \otimes_A N$ is uniquely defined by this property (up to isomorphism).

Tensor product, description

Elements of $M \otimes_A N$ are formal sums

$$\sum_{i=1}^n x_i \otimes y_i, \quad x_i \in M, y_i \in N,$$

subject to relations (for $x, x' \in M, y, y' \in N, a \in A$):

$$\begin{aligned}(x + x') \otimes y &= x \otimes y + x' \otimes y, \\ x \otimes (y + y') &= x \otimes y + x \otimes y', \\ a(x \otimes y) &= ax \otimes y = x \otimes ay.\end{aligned}$$

Given a bilinear map $\varphi: M \times N \rightarrow P$, the associated homomorphism $\psi: M \otimes_A N \rightarrow P$ has

$$\psi(x \otimes y) = \varphi(x, y).$$

Tensor product and change of ring for modules

If $\varphi: A \rightarrow B$ is a ring homomorphism, then we can turn A -modules into B -modules and vice versa.

- If N is a B -module, the induced A -module is $N_A = N$, with A -module structure given by $an = \varphi(a)n$.
- If M is an A -module, the induced B -module is $M_B = B \otimes_A M$, with B -module structure given by $b(c \otimes m) = bc \otimes m$.

Tensor product, examples

- For any module M , $A \otimes_A M \cong M$, via the map $a \otimes m \mapsto am$.
- Given M, M', N , we have

$$(M \oplus M') \otimes_A N \cong (M \otimes_A N) \oplus (M' \otimes_A N)$$

(tensor product behaves as multiplication).

- For any ideal $I \subseteq A$, we have

$$M \otimes_A A/I \cong M/IM.$$

The tensor functor

Let M be an A -module. There is a covariant functor $M \otimes_A - : \text{Mod}_A \rightarrow \text{Mod}_A$, given by

- On objects: $(M \otimes_A -)(N) = M \otimes_A N$
- On morphisms: Given homomorphism $\varphi: N' \rightarrow N$, get

$$(M \otimes_A -)(\varphi): M \otimes_A N' \rightarrow M \otimes_A N$$
$$(M \otimes_A -)(\varphi)(\sum m_i \otimes n_i) = \sum m_i \otimes \varphi(n_i).$$

Theorem

The functor $M \otimes_A -$ is right exact.

A module M is **flat** if $M \otimes_A -$ is exact, equivalently if whenever $\varphi: N' \rightarrow N$ is injective, then $N' \otimes_A M \rightarrow N \otimes_A M$ is injective.

Flatness, examples

- M and N flat $\iff M \oplus N$ flat.
- A is flat as an A -module.
- Every free module is flat.
- Every fraction ring $S^{-1}A$ is flat as an A -module.
- $\mathbb{Z}/2$ is not flat as a $\mathbb{Z}$ -module, since the map $\varphi: \mathbb{Z} \rightarrow \mathbb{Z}$ given by $\varphi(m) = 2m$ induces

$$\varphi \otimes \text{id}_{\mathbb{Z}/2} = 0: \mathbb{Z} \otimes \mathbb{Z}/2 \rightarrow \mathbb{Z} \otimes \mathbb{Z}/2.$$

Algebras

Let A be a ring. An A -**algebra** is a ring B together with a homomorphism $\varphi: A \rightarrow B$.

An A -algebra is an A -module via $ab = \varphi(a)b$.

An A -algebra B is called

- **finite** if B is finitely generated as an A -module
- **finite type** if B is finitely generated as an A -algebra, that is there exists $b_1, \dots, b_n \in B$ such that every $b \in B$ can be written as

$$b = \sum a_{i_1, \dots, i_n} b_1^{i_1} \dots b_n^{i_n} \quad a_{\bullet} \in A$$

Fact: An A -algebra B is of finite type if and only if it is isomorphic (as an A -algebra) to $A[x_1, \dots, x_n]/I$ for some ideal $I \subseteq A[x_1, \dots, x_n]$.

Fraction rings

A subset $S \subseteq A$ is **multiplicatively closed** if $1 \in S$ and $s, t \in S \Rightarrow st \in S$.

Definition

The **fraction ring** $S^{-1}A$ has elements equivalence classes of symbols a/s with $a \in A$ and $s \in S$, and with equivalence relation defined by

$$a/s = b/t \iff \exists u \in S \text{ such that } (at - bs)u = 0.$$

Addition and multiplication are defined by the usual fraction formulas:

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

Fraction rings, examples (cont.)

Examples

- If A is an integral domain and $S = A \setminus \{0\}$, then $S^{-1}A$ is the fraction field of A .
- If $P \subset A$ is a prime ideal, take $S = A \setminus P$, and write $A_P = S^{-1}A$.
- If $f \in A$, take $S = \{f^k\}_{k \geq 0}$, and write $A_f = S^{-1}A$.
- $\mathbb{Z}_{(0)} = \mathbb{Q}$.
- More generally, if A is an integral domain, $A_{(0)}$ is the fraction field of A .
- For p a prime,

$$\mathbb{Z}_{(p)} = \{m/n \mid m \in \mathbb{Z}, n \notin (p)\} \subset \mathbb{Q}.$$

- $\mathbb{Z}_n = \{m/n^k \mid m \in \mathbb{Z}, k \geq 0\} \subset \mathbb{Q}$.

Fraction modules

If $S \subseteq A$ is multiplicatively closed and M is an A -module, define an $S^{-1}A$ -module as the set of equivalence classes of symbols m/s , with $m \in M$, $s \in S$ and

$$m/s \sim n/t \iff \exists u \in S \text{ such that } (tm - sn)u = 0.$$

This defines a functor $S^{-1}(-): \text{Mod}_A \rightarrow \text{Mod}_{S^{-1}A}$.

Theorem

*We have an isomorphism of $S^{-1}M$ -modules $S^{-1}M \cong S^{-1}A \otimes_A M$.
The functor $S^{-1}(-)$ is exact.
The A -module $S^{-1}A$ is flat.*

Properties of fraction modules

Theorem (“Taking fraction modules commutes with most things”)

Let $S \subset A$ be a multiplicatively closed system. The functor $S^{-1}(-): \text{Mod}_A \rightarrow \text{Mod}_{S^{-1}A}$

- *sends submodules to submodules*

$$M' \subseteq M \Rightarrow S^{-1}M' \subseteq S^{-1}M,$$

- *commutes with taking direct sums*

$$S^{-1}(M \oplus N) = S^{-1}M \oplus S^{-1}N \cong S^{-1}(M \oplus N).$$

Properties of fraction modules (cont.)

For $M, N \subseteq P$:

- S^{-1} commutes with taking intersections and sums, that is

$$S^{-1}(M \cap N) = S^{-1}M \cap S^{-1}N \subseteq S^{-1}P$$

and

$$S^{-1}(M + N) = S^{-1}M + S^{-1}N \subseteq S^{-1}P.$$

- S^{-1} commutes with tensor product

$$S^{-1}(M \otimes_A N) \cong S^{-1}M \otimes_{S^{-1}A} S^{-1}N.$$

Local properties

A property X of modules (rings, homomorphisms, ideals, ...) is **local** if “ X holds for M ” is equivalent to “ X holds for M_P for all prime ideals $P \subset A$ ”.

Theorem

The following are local properties:

- *a module being 0;*
- *a homomorphism being injective;*
- *a homomorphism being surjective;*
- *a homomorphism being an isomorphism;*
- *a module being flat.*

Strengthening: In each case above, the property “ X holds for M ” is equivalent to “ X holds for all $M_{\mathfrak{m}}$ with $\mathfrak{m} \subset A$ maximal”.

Ideals in fraction rings

Let $S \subseteq A$ be multiplicatively closed, and consider the standard homomorphism $\varphi: A \rightarrow S^{-1}A$. For ideals $I \subseteq A$ and $J \subseteq S^{-1}A$, we have

$$\varphi(I)S^{-1}A = S^{-1}I \subseteq S^{-1}A$$

and

$$J = \varphi(\varphi^{-1}(J))S^{-1}A$$

Consequently, the maps

$$\begin{aligned} E: \{\text{Ideals in } A\} &\rightleftharpoons \{\text{Ideals in } S^{-1}A\}: R \\ E(I) &= \varphi(I)S^{-1}A \\ R(J) &= \varphi^{-1}(J) \end{aligned}$$

are such that R is injective and E is surjective.

Prime ideals in fraction rings

Let $S \subseteq A$ be multiplicatively closed and $\varphi: A \rightarrow S^{-1}A$ the standard homomorphism.

Theorem

The operations of extension and contraction along φ (E and R on previous slide) give a bijection between prime ideals of $S^{-1}A$ and the prime ideals of A contained in $A \setminus S$.

Examples

- Let $P \subset A$ be prime. The prime ideals of A_P are in bijection with the prime ideals $Q \subseteq P$ in A . This shows A_P is local with maximal ideal P_P .
- The prime ideals of A_f are in bijection with prime ideals P such that $f \notin P$.

Chain conditions

Definition

Let M be an A -module.

- The module M is **Noetherian** if every sequence of submodules

$$M_1 \subseteq M_2 \subseteq \cdots \subseteq M$$

stabilises, that is there is some $N \geq 0$ such that $M_n = M_N$ for $n \geq N$.

- The module M is **Artinian** if every sequence of submodules

$$M \supseteq M_1 \supseteq M_2 \supseteq \cdots$$

stabilises.

Chain conditions on rings

Definition

A ring A is Noetherian (resp. Artinian) if and only if it is so as an A -module. This means that A is Noetherian (resp. Artinian) if every ascending (resp. descending) chain of ideals in A stabilises.

Theorem (“Chain conditions preserved under ring change operations”)

Let A be Noetherian (resp. Artinian).

- If $I \subseteq A$ is an ideal, then A/I is Noetherian (resp. Artinian).
- If $S \subseteq A$ is multiplicatively closed, then $S^{-1}A$ is Noetherian (resp. Artinian).

Alternative descriptions of Noetherian/Artinian

Definition through maximal/minimal elements

An A -module M is Noetherian (resp. Artinian) if in every set T of submodules of M we can find a maximal (resp. minimal) submodule.

Theorem (Characterisation of Noetherian modules/rings)

An A -module M is Noetherian if and only if every submodule $M' \subseteq M$ is finitely generated.

A ring A is Noetherian if and only if every ideal is finitely generated

Theorem

Let A be a Noetherian ring. An A -module M is Noetherian if and only if it is finitely generated.

Chain conditions and short exact sequences

Theorem

Let

$$0 \rightarrow M' \rightarrow M \rightarrow M'' \rightarrow 0$$

be an exact sequence of A -modules. Then

$$M \text{ Noetherian} \Leftrightarrow M' \text{ \& } M'' \text{ Noetherian}$$

and

$$M \text{ Artinian} \Leftrightarrow M' \text{ \& } M'' \text{ Artinian.}$$

Simple modules

Definition

An A -module $M \neq 0$ is **simple** if its only submodules are 0 and M .

Fact: Every simple module is isomorphic to $A/\mathfrak{m}$ for some maximal ideal $\mathfrak{m} \subset A$.

Definition

Let M be an A -module. We say a sequence of submodules

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

is a **composition series** of **length** l if every quotient M_i/M_{i+1} is simple, or equivalently if we cannot find a submodule $M' \subseteq M$ and $i \in \{0, \dots, l-1\}$ such that

$$M_i \supsetneq M' \supsetneq M_{i+1}.$$

Length

Theorem (“Length is independent of choice of composition series”)

If M admits a composition series, then

- Every composition series of M has the same length, and
- Every sequence

$$M = M_0 \supsetneq M_1 \supsetneq \cdots \supsetneq M_k = 0$$

can be extended to a composition series by adding modules $M_i \subsetneq M' \subsetneq M_{i+1}$.

Definition

If M admits a composition series, then we say it has **finite length**, and its **length** is $l(M)$, defined as the length of any of its composition series.

Additivity of length

Theorem

A module M has finite length if and only if it is both Noetherian and Artinian.

Theorem (“Additivity of length”)

Length is additive, in the sense that if

$$0 \rightarrow M' \rightarrow M \rightarrow M'' \rightarrow 0$$

is an exact sequence of finite length modules, then $l(M) = l(M') + l(M'')$.

Hilbert's basis theorem

Hilbert's basis theorem

If A is a Noetherian ring, then $A[x]$ is Noetherian.

Corollary (“Lots of rings are Noetherian”)

Every localisation of a finite type $\mathbb{Z}$ -algebra is Noetherian.

If k is a field, then every localisation of a finite type k -algebra is Noetherian.

Integral dependence

Definition

Let $A \subseteq B$ be a ring inclusion. An element $b \in B$ is **integral over** A if we can find $a_0, \dots, a_{n-1} \in A$ such that

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

If every $b \in B$ is integral over A , we say $A \subseteq B$ is an **integral ring extension**.

Proposition

An element $b \in B$ is integral over A if and only if the subring

$$A[b] = \left\{ \sum a_i b^i \mid a_i \in A \right\} \subseteq B$$

is a finitely generated A -module.

Integral closures

Theorem/definition

Let $A \subseteq B$ be a ring inclusion. The set

$$C = \{b \in B \mid b \text{ is integral over } A\}$$

is a subring of B , with $A \subseteq C \subseteq B$. The ring C is called the **integral closure of A in B** .

Definition

We say A is **integrally closed in B** if every $b \in B$ which is integral over A lies in A ; equivalently, if A is equal to its integral closure in B .

Integrality of ring extensions preserved

Proposition

Let $A \subseteq B$ be an integral ring extension.

- If $J \subset B$ is an ideal and $I = J \cap A$, then

$$A/I \subseteq B/J$$

is an integral ring extension.

- If $S \subseteq A$ is a multiplicatively closed subset, then

$$S^{-1}A \subseteq S^{-1}B$$

is an integral ring extension.

Primes in integral extensions

Theorem

Let $A \subseteq B$ be an integral ring extension. Then

- 1 A prime ideal $Q \subset B$ is maximal if and only if $Q \cap A$ is maximal in A .
- 2 **Lying over:** For every prime ideal $P \subset A$, there exists a prime ideal $Q \subset B$ such that $Q \cap A = P$.
- 3 **Going up:** If $P \subseteq P' \subset A$ are prime ideals and $Q \subset B$ is a prime ideal such that $Q \cap A = P$, there exists a prime ideal $Q' \supseteq Q$ in B such that $Q' \cap A = P'$.
- 4 If $Q \subsetneq Q'$ are prime ideals in B , then $Q \cap A \subsetneq Q' \cap A$.

Krull dimension

Definition

Let A be a ring. The Krull dimension of A is the supremum (possibly ∞) of the possible lengths n of a chain of prime ideals

$$P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_n \subsetneq A.$$

- $\dim k = 0$ for a field k .
- $\dim A = 1$ for every non-field PID, in particular $\dim \mathbb{Z} = \dim k[x] = 1$.
- $\dim k[x_1, \dots, x_n] = n$.

Theorem

If $A \subseteq B$ is an integral ring extension, then $\dim A = \dim B$.

Algebraic independence

Definition

Let k be a field and let A be a k -algebra. We say that $a_1, \dots, a_n \in A$ are **algebraically independent over k** if, equivalently:

- 1 There is no non-zero $f \in k[x_1, \dots, x_n]$ such that $f(a_1, \dots, a_n) = 0$, or
- 2 The k -algebra homomorphism $\varphi: k[x_1, \dots, x_n] \rightarrow A$ given by $\varphi(f) = f(a_1, \dots, a_n)$ is injective.

If $a_1, \dots, a_n$ are algebraically independent, then the subalgebra $k[a_1, \dots, a_n] \subseteq A$ is isomorphic (via φ) to the polynomial ring $k[x_1, \dots, x_n]$.

Noether normalisation lemma

Theorem

Let k be a field and A a finite type k -algebra. Then there exist elements $a_1, \dots, a_n \in A$ algebraically independent over k such that $k[a_1, \dots, a_n] \subseteq A$ is an integral ring extension.

Corollary

We have $\dim A = \dim k[a_1, \dots, a_n] = n$.

Corollary 2 (Zariski's lemma)

If k is a field and A is a finite type k -algebra such that A is a field, then A is a finite k -algebra.

Hilbert's Nullstellensatz

Hilbert's Nullstellensatz

Let k be an algebraically closed field. There is a bijection

$$\begin{aligned} k^n &\leftrightarrow \{\text{Maximal ideals of } k[x_1, \dots, x_n]\} \\ (a_1, \dots, a_n) &\mapsto (x_1 - a_1, \dots, x_n - a_n) \end{aligned}$$

Corollary

Let k be an algebraically closed field, and let $A = k[x_1, \dots, x_n]/(f_1, \dots, f_m)$. There is a bijection

$$\begin{aligned} \{(a_1, \dots, a_n) \in k^n \mid \forall i, f_i((a_j)) = 0\} &\leftrightarrow \{\text{Maximal ideals of } A\} \\ (a_1, \dots, a_n) &\mapsto (\bar{x}_1 - a_1, \dots, \bar{x}_n - a_n) \end{aligned}$$

Graded rings

Definition

A **graded ring** is a ring A together with subgroups $A_d \subseteq A$ for every $d \geq 0$, such that

- 1 Every element $a \in A$ can be written uniquely as a sum

$$a = \sum_{d \geq 0} a_d \quad a_d \in A_d,$$

with only finitely many $a_d \neq 0$.

- 2 for $a \in A_d, b \in A_e$, we have $ab \in A_{d+e}$.

By the first condition, we have an isomorphism of groups
 $(A, +) \cong \bigoplus_{d \geq 0} A_d$.

Homogeneous elements and ideals

Let A be a graded ring.

Homogeneous elements

An element $a \in A$ is called **homogeneous** of degree d if $a \in A_d$.

Homogeneous ideals

An ideal $I \subseteq A$ is called **homogeneous** if it can be generated by homogeneous elements.

Fact: If $I \subseteq A$ is a homogeneous ideal, then A/I has a structure of graded ring, by

$$(A/I)_d = \{a + I \mid a \in A_d\}$$

An assumption

Let A be a graded ring. Assume from now on that

- A_0 is a field, denoted k .
- As a graded ring, we then have $A \cong k[x_1, \dots, x_n]/(f_1, \dots, f_m)$, where the f_i are homogeneous elements.

The Hilbert function

Hilbert function

For a graded ring A with the above assumption, its **Hilbert function** $H_A: \mathbb{Z} \rightarrow \mathbb{N}$ is defined by

$$H_A(d) = \dim_k A_d.$$

Theorem/definition

Let A be a graded ring satisfying the assumptions above. There exists a polynomial $P_A \in \mathbb{Q}[x]$ and an integer $N \geq 0$ such that

$$H_A(n) = P_A(n)$$

when $n \geq N$. The polynomial P_A is the **Hilbert polynomial** of A .

Tools for computing the Hilbert function

- 1 If $A = k[x_1, \dots, x_n]$, know $H_A(d) = \binom{n+d-1}{n-1}$.
- 2 Describe a k -basis for A . E.g. let $A = k[x, y]/(x^3)$. The k -module A_d has basis

$$\{\bar{x}^2\bar{y}^{d-2}, \bar{x}\bar{y}^{d-1}, \bar{y}^d\}$$

when $d \geq 2$, so $H_A(d) = 3$ when $d \geq 2$.

- 3 If $A = B/(f)$ and $f \in B_i$ is a non-zerodivisor, then

$$0 \rightarrow B_{d-i} \xrightarrow{\cdot f} B_d \rightarrow A_d \rightarrow 0$$

is exact, which gives

$$H_A(d) = H_B(d) - H_B(d-i).$$

The dimension theorem

Theorem

Let A be a graded ring with assumptions as above, and let P_A be its Hilbert polynomial. We then have

$$\deg P_A + 1 = \dim A.$$

Note that if $P_A = 0$, we here define $\deg P_A = -1$, so that

$$P_A = 0 \Leftrightarrow \dim A = 0.$$

UiO : **Department of Mathematics**
University of Oslo



MAT4200 Autumn 2025

Commutative algebra revision

