Commutative Algebra (Math 502)

Rings

Example 1: $0 = \{0\}$ is a commutative ring. In fact, $1 = 0 \iff A = \{0\}$.

Example 2: $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$

Example 3: A a commutative ring. $A[X] = \{ f(x) = \sum_{r=0}^{n} a_r x^r \}$ (polynomial ring).

Example 4: $A[[X]]$ (formal power series).

Example 5: $\{A_i\}_{i \in I}$ collection of rings indexed by I. Then $\prod_{i \in I} A_i$ (cartesian product).

Ideals

$I \subseteq A$ additive sgp s.t. $ax \in I$ $\forall a \in A, \forall x \in I$.

We write $(f_1, \dots, f_n) = \{$ ideal generated by $f_1, \dots, f_n$. $\{ \sum_{i=1}^{n} a_i f_i \mid a_i \in A \} \subseteq A$

The residue class ring is $A/_I$.

Example: $I = (1) = A$, then $A/_I = 0$.

- **Domain**: ring with $1 \neq 0$ and no zero divisors. ($\mathbb{Z}$ is a ring, any subring of a field is).
- **Field**: a ring A such that any nonzero element is a unit.
- **Prime ideals**: proper ideal $P \subseteq A$ s.t. $xy \in P \Rightarrow x \in P$ or $y \in P$. (equivalently, iff A/p is a domain).

If I, J are ideals, define $I \cdot J := \{ \sum f_i g_i \mid f_i \in I, g_i \in J \text{ finite} \}$

Lemma: if P is prime and $I \cdot J \subseteq P$, then $I \subseteq P$ or $J \subseteq P$

Def (maximal ideal): $M \subseteq A$ is maximal if it is proper and is maximal wrt proper ideals (i.e. there's no proper ideal s.t. $I \supsetneq M$). (equivalently, iff $A/_M$ is a field).

If $I \subseteq A$ is an ideal, there's a 1-1 correspondence

$$\{ \text{ideals of } A/_I \} \longleftrightarrow \{ \text{ideals of } A \text{ that contain } I \}$$

and it preserves primality and maximality.

- Homomorphisms of rings:

$f: A \to B$ s.t. $f(x+y) = f(x)+f(y)$, $f(xy) = f(x)f(y)$, $f(1)=1$.

Def An <u>A-algebra</u> is a pair (B, f) s.t. B is a commutative ring, and $f: A \to B$ is a ring homomorphism (ex: $A = \mathbb{Z}$, $B = \mathbb{Z}/n\mathbb{Z}$. $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$)

Def An homomorphism of A-Algebras $B \xrightarrow{g} B'$ is an homomorphism such that

$$\begin{tikzcd} B \arrow[r, "g"] & B' \\ & A \arrow[ul, "f"] \arrow[u, "f'"'] \end{tikzcd}$$

satisfies $gf = f'$.

Ex k = field, $A = k[X_1, \dots, X_n]$, $B = k$-algebra ($k \hookrightarrow B$).

$\mathrm{Hom}_{k\text{-alg}}(A, B) \simeq B^n = B \times \dots \times B$

$\varphi \longmapsto (\varphi(X_1), \dots, \varphi(X_n))$ (i.e. $k[X_1, \dots, X_n]$ is a free k-algebra on n generators).

Ex $A = k[X_1, \dots, X_n]/(f_1, \dots, f_r)$ $\ni \overline{X_i}$ is the image of X_i

$\mathrm{Hom}_{k\text{-alg}}(A, B) \longleftrightarrow \{\underline{b} \mid f_i(\underline{b}) = 0 \ \forall i = 1..r\}$

$\varphi \longmapsto (\varphi(\overline{X_1}), \dots, \varphi(\overline{X_n}))$

<u>Zorn's lemma</u>: Let P be a poset.

If every totally ordered subset $S \subseteq P$ has an upper bound in P, then P has a maximal element (not unique, in general)..

Def A multiplicative subset in a ring A is a subset S s.t. $1 \in S$, and is closed under multiplication.

<u>Prop</u>: Let $S \subseteq A$ be a multiplicative set, $I \subseteq A$ an ideal $S \cap I = \emptyset$. Then $\exists J \subseteq A$, ideal maximal wrt the property $J \supseteq I$, $J \cap S = \emptyset$.

Furthermore, any J maximal wrt this property is prime.

In particular, any proper ideal is contained in a maximal ideal ($S = \{1\}$).
Also, any non-zero ring has maximal ideals ($1 \neq 0$, $I = \{0\}$, $S = \{1\}$).

Proof $\Gamma = \{$ proper ideals $J \subseteq A$ s.t. $J \supseteq I$, $J \cap S = \emptyset\}$

Let S be a totally ordered subset, $S = \{J_\alpha\} \subseteq \Gamma$

Let $\bar{J} := \bigcup_\alpha J_\alpha$ ideal, $\bar{J} \in \Gamma$.

By Zorn's lemma, $\exists J$ maximal in Γ.

Given such a J maximal in Γ, want to show that it is prime.

If $x, y \notin J$, want to show that $xy \notin J$ (see that $S \supseteq \{1\} \Rightarrow 1 \notin J \Rightarrow J$ is proper).

$J + Ax \supsetneq J$, so $\exists \begin{cases} s \in (J + Ax) \cap S \\ t \in (J + Ay) \cap S \end{cases}$ $\quad s = a + bx \quad t = c + dy \quad a, c \in J \quad b, d \in A$

$st = \underbrace{ac + bcx + ady}_{\in J} + bdxy \Rightarrow bdxy \notin J$ since $J \cap S = \emptyset \Rightarrow xy \notin J$.

Def The <u>radical</u> of an ideal I is $\sqrt{I} = \{f \in A \mid f^n \in I$ for some $n \in \mathbb{N}\}$.

Prop: $\sqrt{I} = \bigcap_{\substack{P \supseteq I \\ P \text{ prime}}} P$

Pf $\subseteq)$ if $f \in \sqrt{I}$, $f^n \in I$ for some n.
if $P \supseteq I$, P prime, $f \cdot f^{n-1} \in P \Rightarrow f \in P$ or $f^{n-1} \in P$ + induction //

$\supseteq)$ If $f \notin \sqrt{I}$, let $S = \{1, f, f^2, \dots\}$

$S \cap I = \emptyset$, but then by the lemma, $\exists$ prime P st $P \supseteq I$, $P \cap S = \emptyset$.

Since $f \in S$, $f \notin P$. So $f \notin \bigcap P$.

//

Def The <u>nilradical</u> of a ring A is $nil(A) = \sqrt{0} = \{$nilpotent elements$\}$.

We have that $nil(A) = \bigcap_{\text{prime ideals}} P$.

Def The <u>Jacobson radical</u> of A is $Jrad(A) = \{x \in A \mid 1 + ax$ is a unit $\forall a \in A\}$

Prop: $Jrad(A) = \bigcap_{\substack{\mathfrak{m} \subseteq A \\ \mathfrak{m} \text{ maximal ideals}}} \mathfrak{m}$

Pf $\subseteq$) If $x \in \mathrm{Jrad}(A)$, $\mathfrak{M}$ max ideal, want $x \in \mathfrak{M}$. If not,
$M + Ax = A = (1) \Rightarrow 1 = m + ax$ for some $m \in \mathfrak{M}$, $a \in A \Rightarrow$
$\Rightarrow 1 - ax = m \in M \Rightarrow (1-ax) \neq (1)$ //

$\supseteq$) If $x \in \bigcap \mathfrak{M}$, consider $1 + ax$ for any $a \in A$. For any maximal ideal $\mathfrak{M}$,
$1 + ax \equiv 1 \mod \mathfrak{M} \Rightarrow 1 + ax \notin \mathfrak{M}$ for any $\mathfrak{M} \Rightarrow 1 + ax \in \mathrm{Units}(A)$.

• Factorization

Let A be a domain.

Def $a \in A$ is irreducible iff is not a unit and $a = xy \Rightarrow x$ or y is a unit.
(equivalently, iff (a) is maximal among proper principal ideals).

Def $a \in A$ is prime if (a) is a prime ideal.
(prime $\Rightarrow$ irreducible).

Example: $A = \mathbb{Z}[\sqrt{-5}] = \{a + \sqrt{-5}\, b : a, b \in \mathbb{Z}\}$.
$2 \cdot 3 = 6 = (1+\sqrt{-5})(1-\sqrt{-5})$. So 2 is irreducible in A, but is not prime.

Def: A U.F.D is a domain A such that every non-unit admits a factorization into irreducible elements, unique up to units & ordering.

Def A domain A has the ascending chain condition (acc) for principal ideals: if every chain $(a_1) \subsetneq (a_2) \subsetneq \cdots$ stops after finite steps.

The a.c.c. implies that any non-unit can be factored into irreducibles.

Pf Suppose x is not a unit. So if $x = ab$, where a, b not both units,
$\Rightarrow a, b$ not factorizable into irreducibles.
So $(x) \subsetneq (a)$. And then (a) satisfies the same properties, so can build an infinite ascending chain $\Rightarrow$!!
//

If, additionally, every irreducible in A is prime, then factorization is "unique" (i.e. A is a UFD)

__Prop__: A is a UFD iff A has a.c.c for principal ideals & irr $\Rightarrow$ prime.

Pf/ have seen $\Leftarrow$; $\Rightarrow$ is easy.

__Corollary__: a PID is a UFD.

Pf/ Given a chain, take the union $\bigcup (a_i) = (a)$. But a lives in some (a_i), so it stops there $\Rightarrow$ a.c.c.

__Remark__: $k[x_1, \dots, x_n]$ is a UFD but it is __not__ a PID.

- __Coprimality__

If A is a ring, and $I, J \subseteq A$ are ideals.

$\boxed{\text{Def}}$ We say that I and J are __coprime__ if $I + J = A$.

__Prop__: If I and J are coprime, then $IJ = I \cap J$, and $A/IJ \cong A/I\cap J \cong A/I \times A/J$

Pf/ $IJ \subseteq I \cap J$ clear.

Since $A = (1) = I + J$, $1 = \underset{I}{x} + \underset{J}{y}$

If $a \in I \cap J$, $a = a \cdot 1 = \underbrace{a \cdot x}_{JI} + \underbrace{a \cdot y}_{IJ} \in IJ$.

$$\begin{tikzcd} A/IJ \arrow[r] & A/I\cap J \arrow[r, bend left, "\text{proj}"] & A/I \times A/J \\ & a \arrow[r, mapsto] & (\bar{a}, \bar{a}) \\ A \arrow[uu, two heads] \arrow[uur] \arrow[ur] & & \end{tikzcd}$$

Given $\bar{u}, \bar{v}$, take

$uy + vx \in A$

This is a preimage $\Rightarrow$ surjection //

If $I_1, \dots, I_n$ are pairwise coprime, then

$$A/I_1 \cdots I_n \cong A/I_1 \times \dots \times A/I_n$$

• Modules

A module M is <u>finitely generated</u> if $\exists\, m_1, \dots, m_n \in M$ s.t. $(n < \infty)$

$$M = Am_1 + \dots + Am_n$$

<u>Ex</u>: $F = A^n = Ae_1 \oplus \dots \oplus Ae_n$

<u>Rk</u>: M is f-g iff $\exists$ surjection $F \twoheadrightarrow M$ from a <u>free module</u> to M.

Note that the submodules of a ring A are the ideals of A.

$\boxed{\text{Def}}$ M module, $N, N' \subseteq M$ submodules.

$$(N : N')_A := \{ a \in A \mid aN' \subseteq N \} \quad (\text{it is an ideal of } A).$$

We can then say that $\mathrm{Ann}(M) := (0 : M)_A = \{ a \in A \mid aM = 0 \}$.

<u>Note</u>: M becomes a module over $A/\mathrm{Ann}(M)$.

$\boxed{\text{Def}}$: M is <u>faithful</u> iff $\mathrm{Ann}(M) = 0$.

We can write also $\mathrm{Ann}(m) := (0 : Am)_A = \{ a \in A : am = 0 \}$.

$\mathrm{Hom}_A(M, N)$ and $M \otimes_A N$ are A-modules <u>since A is commutative</u>.

$\mathrm{Hom}_A(M, -)$ to exact sequences $0 \to N' \to N \to N''$ gives exact (right exact)

$\mathrm{Hom}_A(-, N)$ — — — $M' \to M \to M'' \to 0$ gives exact (right exact)

$M \otimes_A -$ — — — $N' \to N \to N'' \to 0$ —

$- \otimes_A N$ — — — $M' \to M \to M'' \to 0$ —

- **The Cayley-Hamilton Theorem.**

Th: If A is a ring, $I \subseteq A$ an ideal, M a f.g. A-module.
If $\varphi : M \to M$ is an A module homomorphism s.t. $\varphi(M) \subseteq IM$,
Then $\exists$ monic polynomial $p(X) = X^n + p_1 X^{n-1} + \cdots + p_n \in A[X]$,
with $p_i \in I^i$ s.t. $p(\varphi) = \varphi^n + p_1 \varphi^{n-1} + \cdots + p_n = 0$ as a homomorphism.

Pf/ Let $m_1, \dots, m_n \in M$ be a generator set.
Then, we can write $\varphi(m_i) = \sum_{j=1}^{n} a_{ij} m_j$ for some a_{ij} (not unique!).
Let $U = (a_{ij})$ be a $n \times n$ matrix given by the a_{ij}'s
Make M a module over $A[X]$, by making $X \cdot m := \varphi(m)$.
Let $\underline{m} = \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix}$ a column vector in M.
Let $V := (b_{ij})$ be the matrix of cofactors (matriz adjunta traspuesta).

We know that $(X \underline{id} - U)\underline{m} = 0$

Then $\underbrace{V(X \cdot \underline{id} - U)}_{\det(X \cdot id - U) \cdot \underline{id}} \cdot \underline{m} = 0$. Write $p(X) := \det(X \cdot \underline{id} - U)$

So $p(X) m_i = 0$. This implies $p(X) \cdot M = 0$.
The formulas for the coefficients in the characteristic polynomial show that p_j is an homogeneous polynomial of degree j in the (a_{ij}). So, $p_{ij} \in I^j$

//

- ## Nakayama Lemma

Th (Nakayama's lemma): Let A be a ring, $I \subseteq A$ an ideal.
Let M be a f.g. A-module. Then,

a) If $M = I \cdot M$, then $\exists\, a \in I$ s.t. $am = m \;\; \forall m \in M$ (Hence, $(1-a)M = 0$).

b) If $I \subseteq \mathrm{Jrad}(A)$, then whenever [$M = IM \Rightarrow M = 0$]

pf/ a) We use Cayley-Hamilton:

$\varphi = id_M : M \to M$ (satisfies $\varphi(M) = IM$).

So $\exists\, p(x) = x^n + p_1 x^{n-1} + \dots + p_n \in A[X]$ s.t. $p(\varphi) = 0$ & $p_j \in I^j$

i.e. $1 + p_1 + \dots + p_n$ annihilates M, and $p_j \in I^j \subseteq I$.

So define $a := -(p_1 + \dots + p_n)$ and we are done //

b) $\exists\, a \in I$ s.t. $(1-a)M = 0$. $a \in I \subseteq \mathrm{Jrad}(A) \Rightarrow$

$\Rightarrow 1 + Aa \subseteq \mathrm{Units}(A) \Rightarrow 1-a$ is a unit $\Rightarrow M = 0$. //

Def A <u>local ring</u> is a ring with a unique maximal ideal.

Ex/ $\mathbb{Z}/p^n\mathbb{Z}$ is a local ring with $\mathfrak{m} = (p)$; $\mathbb{Z}_{(p)} = \{\frac{a}{b} \in \mathbb{Q} \mid p \nmid b\}$ is, with $\mathfrak{m} = (p)$; $A/\mathfrak{m} = \mathbb{F}_p$.

If A is a local ring with maximal ideal $\mathfrak{m}$, then $\mathfrak{m} = \mathrm{Jrad}(A)$. So we get:

Corollary: A be a local ring, M finitely generated. Then $\mathfrak{m}M = M \Leftrightarrow M = 0 \Leftrightarrow$

$\Leftrightarrow M \otimes_A k = 0$ (or $M \otimes_A A/\mathfrak{m} = 0 \Rightarrow M = 0$).

Corollary: If $I \subseteq \mathrm{Jrad}(A)$, M module and $N \subseteq M$ submodule,
and M/N finitely generated, then if $M = N + IM$
we get $M = N$.

Example:

$A = \mathbb{Z}_{(p)}$, $M = \mathbb{Q}$.

$M \otimes_A A/\mathfrak{m} = \mathbb{Q} \otimes_{\mathbb{Z}_{(p)}} \mathbb{F}_p = 0$ but $\mathbb{Q}$ is not zero.

We deduce, thus, that $\mathbb{Q}$ is not finitely generated as $\mathbb{Z}_{(p)}$-module.

Proposition: A a local ring, $\mathfrak{m}$ its maximal ideal, M a f.g. A-module and write $\overline{M} := M \otimes_A A/\mathfrak{m}$ (which is a vectorspace over $A/\mathfrak{m}$).

Then $v_1, \dots, v_n \in M$ is a minimal generator set for $M \Leftrightarrow \bar{v}_1, \dots, \bar{v}_n$ is a basis for $\overline{M}$.

Pf/ If $v_1, \dots, v_n$ generate M, we get a surjection

$$A^n \xrightarrow{f} M \longrightarrow 0$$

So $f \otimes_A A$ is still a surjection, so $\overline{M}$ is generated by its image.

If $v_1, \dots, v_n \in M$: $A^n \xrightarrow{f} M \longrightarrow \underset{\text{coker } f}{\overset{\shortparallel}{C}} \longrightarrow 0$

C is f.g. because M is. So can apply Nakayama's lemma.

If $\bar{v}_1, \dots, \bar{v}_n$ generate $\overline{M}$, then

$C \otimes_A A/\mathfrak{m} = \text{Coker}\left[f \otimes A/\mathfrak{m} \right] = 0$ and then $\overset{(\text{Nak})}{C = 0} \Rightarrow f$ is surjective.

Minimality follows straightforward. //

Recall: an A-module P is <u>projective</u> iff it is a summand of a free module. or, equivalently, if for all surjections $M \xrightarrow{f} P \to 0$ of modules there exists a section $s: P \to M$ st $f \circ s = 1_P$.

Proposition: A be a local ring, M f.g. module over A. Then M is free iff M is projective (it is true without requiring M to be f.g.).

Pf Consider M has a minimal set of generators $u_1, \dots, u_n$. So $A^n \xrightarrow{f} M \to 0$ so there's a section $\Rightarrow A^n \simeq M \oplus N$. $M = sM$, $N = (1 - sf)A^n$.

$\bar{u}_1, \dots, \bar{u}_n$ are a basis for $\overline{M} = M \otimes_A A/\mathfrak{m}$. $A^n \otimes A/\mathfrak{m} = (A/\mathfrak{m})^n \simeq \overline{M} \oplus \overline{N} \Rightarrow \dim_k(A/\mathfrak{m}) = n$

Since N is a summand, it is also finitely generated, so $N=0$. //

(C.H.T. M f.gen. A-module, $I \subseteq M$, $\varphi: M \to M$ st. $\varphi(M) \subseteq IM$. Then, $\exists$ monic $p(x) \in A[x]$ st $p(\varphi)=0$, and $p(x) = x^n + p_1 x^{n-1} + \dots + p_n$ and $p_i \in I^i$).

Prop: Let M be a f.generated A-module
$f: M \to M$ endomorphism.
If f is a surjection, then f is an iso.

Pf Make M into an $A[T]$-module by letting T act as f.
Let $\varphi: M \to M$ be the identity map.
Let $I = (T) \subseteq A[T]$. Since f is surjective,

$$\varphi(M) = TM = f(M) = M \Rightarrow \varphi(M) \subseteq IM.$$

Applying C-H, $\exists$ monic $p(x) \in A[T][x]$ st. $p(\varphi)=0$
As φ is the identity, $p(\varphi) = 1 + p_1 + \dots + p_n$ and $p_i \in I^i = (T^i)$
So $1 = -(p_1 + \dots + p_n) = gT$ for some $g \in A[T]$.
So $id_M = \underbrace{g(f)}_{\text{polynomial in } f} \circ f \Rightarrow$ left inverse to f and, since f is surjective, f is iso. //

Corollary: If $M \simeq A^n$, then any set of n elements that generate M is a free basis.
In particular, the rank of a finite generated free module, is well defined.

Pf If $M \simeq A^n$, there is $\gamma: M \to A^n$ iso.
A gen. set of size n gives $\varphi: A^n \to M$ surjective.
So $\varphi \circ \gamma = f$ is a surjection. Since M is f.g., it is an isomorphism.
So φ is an isomorphism.

Note: this does not hold in general for non-commutative rings!

(counter)-example:

Let V an infinite-dim vec-space over K.

$R = \hom_K(V,V)$ ← free right module over R.

$V \simeq V \oplus V$ as a vector-space.

So $\underset{R}{\underset{\shortparallel}{\hom_K(V, V\oplus V)}} \simeq \hom_K(V,V) \oplus \hom_K(V,V) \simeq R \oplus R$

Review of concepts

• A module M is simple if non-zero and the only submodules are 0 & M.

If M is simple, Take $m \in M$, $m \neq 0$. Then

$$0 \to I \to A \twoheadrightarrow M \to 0 \qquad M = A/I \text{ and } I \text{ has to be maximal.}$$
$$a \mapsto am$$

So M simple $\Leftrightarrow$ $A/\mathfrak{m}$, $\mathfrak{m}$ = max ideal.

• A chain $M = M_0 \supsetneq M_1 \supsetneq M_2 \supsetneq \cdots \supsetneq M_n = 0$ of submodules is a composition series if M_s/M_{s+1} are simple.

Jordan-Hölder Th:

If M has a composition series of length $= n$, then every comp. series of M has length n, and the quotients $\{M_s/M_{s+1}\}$ do not depend on the comp. series, up to reordering.

Def: the length of a module $\ell(M)$ is the length of any comp. series. If no finite composition series exists, $\ell(M) = \infty$.

Obs: If $N \subseteq M$, then $\ell(M) = \ell(N) + \ell(M/N)$.

• Ascending chain conditions.

If Γ is a poset, then the following are equivalent:

(1) Every nonempty $S \subseteq \Gamma$ has a maximal element.

(2) Every ascending chain of elements $x_1 < x_2 < \cdots < x_k < \cdots$ in Γ must stop at some finite step.

Def: We'll say that M is Noetherian if it satisfies the a.c.c. for submodules.

Def: A ring A is Noetherian if it is Noetherian as a module over itself. (i.e. if ideals of A satisfy a.c.c).

Thm: The following are equivalent:

(1) M is a noetherian module.

(2) every submodule of M is finitely generated.

Pf (1)⇒(2). $N \subseteq M$ submodule. ⇒ $\exists$ maximal f.g. $N' \subseteq N$.

If $N' \neq N$, then $N' + An \subseteq N$ $n \in N - N'$ contradicting maximality.

(2)⇒(1)

If we have $N_1 \subseteq N_2 \subseteq \cdots$ a chain of submodules

$N := \bigcup_i N_i$ is f. gen. by elts $x_1, \ldots, x_k$. So there $\exists$ i st.

$x_1, \ldots, x_k \in N_i \Rightarrow N = N_i$.

Def M is Artinian iff it satisfies the descending chain condition.

Prop:

(1) Exact seq. $0 \to M' \to M \to M'' \to 0$. Then

M is Noetherian (resp. Artinian) $\Leftrightarrow$ M' and M'' are Noetherian (resp. Artinian)

(2) If M f.g. A-module, and A is Noeth. (Artinian) then so is M.

Prop: M is Noetherian & Artinian iff it has finite length.

Pf ⇐) easy

⇒) build some ~~infinite~~ finite length by using Artinian. The Noeth. condition says it'll stop.

So I is prime $\Rightarrow$ I is maximal, so $\ell(A/I) = 1 < \infty$ $\Rightarrow$ contradiction.

(b) $\Rightarrow$ (c): done before.

(c) $\Rightarrow$ (a)

Suppose A is Artinian.

Claim: 0 is a product of maximal ideals.

Pf of claim:

Let J be minimal among ideals which are products of maximal ideals (Artinian).

If M is maximal, then $MJ = J$ by minimality of J.

In particular, $J \subseteq M$ $\forall M$ maximal $\Rightarrow$ $J \subseteq \mathrm{Jrad}(A)$.

Also, $J^2 = J$ by minimality.

Claim: $J = 0$.

Pf of claim: Suppose not: $J \neq 0$. Let I be an ideal minimal wrt property that $IJ \neq 0$

(this exists by Artinian ppty and $I = A$ has this property).

In particular, $\exists$ $f \in I$, $f \neq 0$, s.t. $fJ \neq 0$.

So $I = (f)$, by minimality of I.

But $((f)J)J = (f)J^2 = (f)J \neq 0$, so $(f) = (f)J$ by minimality.

Hence, $\exists$ $g \in J$ st $f = fg$ so $\underbrace{(1-g)}_{\text{a unit because } g \in \mathrm{Jrad}(A)} f = 0 \Rightarrow f = 0 \Rightarrow !!$

This proves that 0 is a product of maximals.

$0 = M_1 M_2 \cdots M_t$ for some list of maximal ideals.

$A \supsetneq M_1 \supsetneq M_1M_2 \supsetneq \cdots \supseteq M_1 \ldots M_t = 0$

The quotients $M_1 \cdots M_s / M_1 \cdots M_{s+1}$ are artinian modules.

In fact, an Artinian A/M_{s+1} (field) -module, so it's an A/M_{s+1} -vectorspace

and Artinian means finite dimensional so $\ell(M_1 \ldots M_s / M_1 \ldots M_{s+1}) < \infty \to \ell(A) < \infty$.

So A is Noetherian.

If $P \subseteq A$ prime, $P \supseteq 0 = M_1 \cdots M_t$, so $P \supseteq M_i$ for some $i \Rightarrow$

$\Rightarrow$ $P = M_i$ by maximality so there are finitely many primes, all of which are maximal //

Hints for HW:

3.1 b) A ring is semilocal if it has a finite set of maximal ideals.

If $M \subseteq A$ is maximal, then for any ideal I, either $I \subseteq M$ or $I+M=A$.

In particular, maximal ideals are coprime.

$$I \hookrightarrow A \twoheadrightarrow B \simeq A/I$$

If $M \subseteq A$ maximal, either $f(M)=B$ or $f(M) \subsetneq B$ and is a maximal ideal.

Prop: M module, M Noeth & Art. $\Leftrightarrow$ $l(M) < \infty$ (reminder).

~~Example: $\mathbb{Z}$ is Noetherian~~

Question: is $\mathbb{Q}/\mathbb{Z}$ Artinian as a $\mathbb{Z}$-module? It is <u>not</u> Noetherian: $\frac{1}{p}\mathbb{Z}/\mathbb{Z} \subsetneq \frac{1}{p^2}\mathbb{Z}/\mathbb{Z} \subsetneq \cdots$

Theorem: if <u>A is a ring</u>, TFAE: (Hopkins-Akizuki).

(a) A is Noetherian, and all primes are maximal (and there is a finite amount of them).

(b) A has finite length as an A-module.

(c) A is Artinian.

If these hold, then A has finitely many maximal ideals.

Pf/ (a)$\Rightarrow$(b)

Suppose A is Noetherian and all primes are maximal, but A has not finite length.

Let be $I \subseteq A$ be an ideal maximal wrt the property that $l(A/I)=\infty$.

(0 has this property, so the set is not empty).

Claim: I is prime: suppose not, i.e. $\exists\, a,b \notin I$ st $ab \in I$. Then

$$0 \to A/(I:a) \xrightarrow[x \mapsto ax]{} A/I \twoheadrightarrow \underbrace{A/(I+Aa)}_{\text{finite length, by maximality of } I} \to 0$$

is an exact seq. of A-modules.

Note that $(I:a) \supseteq I$ and $b \in (I:a)$, so $(I:a) \supsetneq I$.

So $A/(I:a)$ has finite length. So A/I has finite length $\Rightarrow\Leftarrow$!!

Note in particular that all Artinian rings are semilocal.

Ex: A a k-algebra, $\dim_k A < \infty$. Then A has finite length as A-module, so is Artinian.

Hilbert Basis Theorem: If A is Noetherian, so is $A[X]$.

Corollary: Say $B \simeq A[X_1, \dots X_n]/J$ is finite-type over A. Then A Noetherian implies that finite-type A-algebras are also Noetherian.

Pf of HBT:

$J \subseteq A[X]$.

Construct elements $f_i \in I$ as follows:

$f_1 \neq 0$, $f_1 \in I$, of minimal degree among elements of I.

$f_s \in I$ is chosen to have minimal degree among $I \setminus (f_1, \dots, f_{s-1})$.

And want to show that this stops.

Let a_i = leading coeff. of f_i. So $f_i = a_i X^n$ + lower degree.

There exists a t s.t. $a_i \in (a_1, \dots, a_t)$ $\forall i$ (since A is Noetherian).

f_{t+1}: $a_{i+1} = \sum_{i=1}^{t} u_i a_i$ $u_i \in A$.

Set $g = \sum_{i=1}^{t} u_i a_i X^{(\deg f_{t+1}) - (\deg f_i)}$. f_{t+1}, g have same degree and l.c.

So $f_{t+1} - g$ has smaller degree, so $f_{t+1} - g \notin I$, contradicting the choice of f_{t+1}. //

Prop: If A Noetherian, then $A[[X]]$ is also Noetherian.

Pf: See Matsumura

Thm (Cohen): A is Noetherian iff every prime ideal is finitely generated.

Pf $\Rightarrow$) ok.

$\Leftarrow$) Consider the set $\Gamma = \{ J \subseteq A \mid I \text{ not f.gen} \}$. Zorn $\Rightarrow$ there is a maximal such I. (Assume first that Γ is not empty)

I is prime ($\Rightarrow$ contradiction). If I is not prime, $\exists\, x, y \notin I$, $xy \in I$.

Then $I + Ax$ is finitely generated. $I + Ax = (\mu_1, \dots, \mu_r, x)$. Can assume $\mu_i \in I$. ~~and have~~ (see after note)

Note: $\mathbb{Q}/\mathbb{Z}_{(p)}$ is Artinian.

$\shortparallel$

$\bigcup_n \frac{1}{p^n}\mathbb{Z}/\mathbb{Z} \simeq \bigcup_n \mathbb{Z}/p^n$. All of its proper subgroups are $\frac{1}{p^n}\mathbb{Z}/\mathbb{Z}$

Regarding $\mathbb{Q}/\mathbb{Z}$,

$\frac{\mathbb{Q}}{\mathbb{Z}} \simeq \bigoplus_p \mathbb{Q}/\mathbb{Z}_{(p)}$ as can write $\frac{a}{b} = n + \sum_p \frac{c_p}{p^{d_p}}$.

It is not Artinian.

In general, if $M = \bigoplus_{i=1}^{\infty} M_n$, $M_n \neq 0$, then can build a sequence $N_k := \bigoplus_{n=k}^{\infty} M_n \subseteq M$, which is an infinite descending $\Rightarrow$ Not artinian.

End of Cohen's proof: $I = (\mu_1, \dots, \mu_r) + (I:x)x$ (check this formula!).
Note that $(I:x) \supseteq I$, and $y \in (I:x) \setminus I$. So $(I:x)$ is finitely generated.
So $I = (\mu_1, \dots, \mu_r, \lambda_1 x, \dots, \lambda_s x) \Rightarrow$!!

//

• Localization

Let A be a ring, $S \subseteq A$ a multiplicatively closed subset.

$A_S (= S^{-1}A = A[S^{-1}] = \cdots) := \{(a,s) \in A \times S\}/\sim$ where $(a,s)\sim(a',s') \Leftrightarrow \exists t \in S$ s.t. $t(as' - a's) = 0$

Claim: A_S is a ring, where $(a,s) + (a',s') := (as' + a's, ss')$, $(a,s)\cdot(a',s') = (aa', ss')$,
and $1 = (1,1)$, $0 = (0,1)$. (check it!)

There's a natural map $f: A \longrightarrow A_S$ by $f(a) = (a,1) = \frac{a}{1}$

The kernel of f is $\{x \in A \mid \exists s \in S \text{ s.t. } sx = 0\}$

⇒ Universal property: given A, S as above and $g: A \to B$ a hom of rings, such that $g(S) \subseteq \mathrm{Unit}(B)$, there exists a unique $h: A_S \to B$ s.t.

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[dr, "g"'] & A_S \arrow[d, "h"] \\ & B \end{tikzcd} \qquad \left(h\left(\frac{a}{s}\right) := \frac{g(a)}{g(s)} \right)$$

If S consists of non-zero divisors (e.g. if A is a domain, and $0 \notin S$) then $A \subseteq A_S$.

$\boxed{\text{Def}}$ The <u>total quotient ring</u> of a ~~ring~~ A is A_S where $S = \{\text{nonzero divisors}\}$. $(K(A))$

$\boxed{\text{Def}}$ When A is a domain, then the total quotient ring is called <u>fractions field</u> of A. $(K(A))$

If $P \subseteq A$ is a prime ideal, $S := A \setminus P$ is a mult. closed subset, and we define:

$\boxed{\text{Def}}$ The localization of A at P is $A_P := A_{A \setminus P}$

<u>Claim</u>: it is a local ring, with unique maximal $PA_P \subseteq A_P$.

<u>Ex</u>: $\cdot\ \mathbb{Z}_{(p)}$

$\cdot\ A = k[X]$, then $K(A) \simeq k(X)$; $A_{(x)} \subseteq k(X)$ is $\{\frac{f}{g} \mid x \nmid g\}$.

Suppose now that $f: A \to B$ is a ring hom.

notation
$\downarrow$

If $I \subseteq A$ an ideal, the <u>extended</u> ideal is $f(I) \cdot B \,(= I^e)(= I \cdot B)$

If $J \subseteq B$ an ideal, the <u>contracted</u> ideal is $f^{-1}(J) \cdot A\ (= J^c)(= J \cap A)$.

In general:

$\cdot\ I \subseteq (I^e)^c$ and $(J^c)^e \subseteq J$.

$\boxed{\text{Def}}$ I is a <u>contracted</u> ideal iff $I = I^{ec}$

J is an <u>extended</u> ideal iff $J = J^{ce}$

<u>Prop</u>: if $f: A \to B$ is a ring hom. and $P \subseteq B$ is prime, then $P^c \subseteq A$ is prime.

Pf If $x, y \in A \setminus P^c$ then $f(x), f(y) \notin P \Rightarrow f(xy) = f(x)f(y) \notin P \Rightarrow$
$\Rightarrow xy \notin P^c$.

Def The prime spectrum of a ring A, $\mathrm{Spec}(A) := \{P \subseteq A \text{ prime ideals}\}$.

Then, a ring hom $f: A \to B$ induces $f^{\#}: \mathrm{Spec}(B) \to \mathrm{Spec}(A)$ by $f^{\#}(P) := f^{-1}(P)$.

Example: If $f: A \twoheadrightarrow B$ is surjective (i.e. $B \simeq A/I$), then every ideal of B is extended.

In particular, $\mathrm{Spec}(B) \longleftrightarrow \{P \text{ primes of } A \text{ containing } I\} \subseteq \mathrm{Spec}(A)$.

Prop: Let A be a ring, S a mult. closed subset. Then, all ideals of A_S are extended from A.

In particular, the primes of A_S are precisely the ideals $P \cdot A_S$ where $P \subseteq A$ is a prime s.t. $P \cap S = \emptyset$. (i.e. $\mathrm{Spec}(A_S) \longleftrightarrow \{P \text{ primes } P \cap S = \emptyset\} \subseteq \mathrm{Spec}(A)$.

Pf Let $J \subseteq A_S$ be an ideal. Need to show $J \supseteq J^{ce}$ (the other inclusion holds always).

Suppose $x \in J$, $x = \frac{a}{s}$ for $a \in A, s \in S$.

So $a = \frac{a}{s} \cdot s = x \cdot s$. $xs \in J$ and $xs \in f(A)$, so $a \in J^c$.

So $x \cdot s \in f(J)$, and so $x \cdot s \cdot \frac{1}{s} \in f(J) A_S$ since $s^{-1} \in A_S$. //

If $P \subseteq A_S$ is prime, then $P = P^{ce}$. But P^c is itself prime, so any prime in A_S is an extension of a prime in A.

Suppose that $Q \subseteq A$ is prime. Then $Q A_S$ is:

$\to$ if $Q \cap S \neq \emptyset \Rightarrow x \in Q \cap S$, so $1 = x \cdot x^{-1} \in Q A_S \Rightarrow Q A_S = A_S$.

$\to$ if $Q \cap S = \emptyset$, then want to show $Q A_S$ is prime:

Let $\frac{a}{s}, \frac{a'}{s'}$ be elements in A_S s.t. $\frac{aa'}{ss'} \in Q A_S$.

$\exists t \in S$ s.t. $taa' \in Q$, so either a or $a' \in Q$. If $a \in Q$, then $\frac{a}{s} \in Q A_S$ ... so $Q A_S$ is prime if it is proper.

But if $1 \in Q A_S$ then $\exists t \in S$ s.t. $t \in Q$. But can't be, as $S \cap Q = \emptyset$. //

If P is prime, then

$$\mathrm{Spec}(A_P) \longleftrightarrow \{\text{primes contained in } P\} \subseteq \mathrm{Spec}(A).$$

Let A be a ring; S a m.c. set; I an ideal of A.

Let $\overline{S}$:= image of S in A/I.

Then $(A/I)_{\overline{S}} \simeq A_S/IA_S$

Pf exercise.

Example: it implies that $k(A/P) \simeq A_P/PA_P$ $\quad$ $k(P)$ (notation).

Prop: $S \subseteq T$ mult. closed, then $A_T \simeq (A_S)_{T'}$ where T' is the image of T in A_S.

Pf Use universal property.

$\boxed{\text{Def}}$ The $\underline{\text{m-Spec}}(A) \subseteq \mathrm{Spec}(A)$ is the set of maximal ideals in A.

Rk: They don't behave well by contraction: $f^{-1}(M)$ need not be maximal!

Rk: $\mathrm{Spec}(A) = \emptyset \Leftrightarrow A = 0 \Leftrightarrow \text{m-Spec}(A) = \emptyset$.

If $I \subseteq A$ an ideal, $V(I) := \{P \supseteq I,\ P \text{ prime}\} \subseteq \mathrm{Spec}(A)$.

Write $\mathcal{F} = \{V(I) : I \subseteq A \text{ ideal}\}$. These are the closed sets of a $\underline{\text{topology}}$ in $\mathrm{Spec}(A)$.

- $V(0) = \mathrm{Spec}(A)$
- $V(A) = \emptyset$
- $V(I) \cup V(J) = V(IJ)$
- $\bigcap V(I_\alpha) = V(\sum I_\alpha)$

Rk: $\{P\} \subseteq \mathrm{Spec}(A)$ is a closed subset iff P is a maximal ideal.

~~If~~ Example A is a PID but not a field. $\mathrm{Spec}(A) = \{0\} \cup \{(p),\ p \text{ prime up to units}\}$.
closed points

If then $f \in A$, $\leadsto V((f)) = \{(p) \mid p \text{ divides } f\}$.

So $\mathcal{F} = \{\mathrm{Spec}(A)\} \cup \{\text{finite subsets of } m\text{-}\mathrm{Spec}(A)\}$.

<u>Note</u>: if A is a domain, the one point set $\{0\} \subseteq \mathrm{Spec}\, A$ <u>is dense</u>.

<u>Example</u>: $f \in A$, $S = \{1, f, f^2, f^3, \dots\}$

$$\mathrm{Spec}(A_S) \hookrightarrow D(f) := \{P \mid f \notin P\} \subseteq \mathrm{Spec}(A)$$
definition

<u>Notation</u>: $A[f^{-1}] = A_{\{1, f, f^2, \dots\}}$

If we have $f_1, \dots, f_n \in A$, call S = mult. set generated by $f_1, \dots, f_n$.

$$A[f_1^{-1}, \dots, f_n^{-1}] := A_S.$$

<u>Fact</u>: $A_S \cong A[g^{-1}]$ where $g = f_1 f_2 \cdots f_n$.

Note that $D(f) = \mathrm{Spec}(A) \setminus V((f))$.

If $I = (f_\alpha)_\alpha$, then $\mathrm{Spec}(A) \setminus V(I) = \bigcup_\alpha D(f_\alpha)$

<u>Conclusion</u>: $D(f)$ are a basis for the open sets for the topology.

<u>Example</u>:

$A = K[X, Y]$.

$I = (X, Y)$ is maximal. $V(I) = \{I\}$.

The complement $\mathrm{Spec}(A) \setminus V(I) = D(X) \cup D(Y)$ so it is not a $D(f)$ for any $f \in A$.

• Localization of modules.

Let M be a module over A, and $S \subseteq A$ a multiplicative closed subset.

$$M_S = \{(m,s) \in M \times S\}/_\sim \quad \text{where } (m,s) \sim (m',s') \text{ iff } \exists\, t \in S : t(s'm - sm') = 0.$$

$$\mathrm{Ker}\,(M \longrightarrow M_S) = \{m \in M : \exists\, s \in S : sm = 0\}.$$

<u>Universal property.</u>

M_S is a module over A_S (check that).

If M is A-module and N is an A_S-module and $\varphi : M \to N$ <u>of A-modules,</u>

then $\exists!$ map of modules $M_S \longrightarrow N$ making

$$\begin{tikzcd} & M_S \arrow[d, dashed] \\ M \arrow[ur, "i"] \arrow[r, "\varphi"'] & N \end{tikzcd}$$

commute.

<u>Prop.</u>

1) $M_S \simeq M \otimes_A A_S$

2) If $N \subseteq M$ is an A-submodule then N_S is a A_S-submodule of M_S.

i.e A_S is <u>flat</u> as an A-module $\left(- \otimes_A A_S \text{ is an exact functor}\right)$.

Pf (1) We use the universal property: $N := M \otimes_A A_S$. Define $\begin{array}{c} M_S \longrightarrow N \\ s^{-1}m \longmapsto m \otimes s^{-1} \end{array}$

(this is the map given by the univ. property).

Define $\left\{ \begin{array}{c} N \longrightarrow M_S \\ m \otimes s^{-1}a \mapsto s^{-1}am \end{array} \right\}$, and check they are inverse one of the other

(2)
$$\begin{tikzcd} N \arrow[r] \arrow[d, "\tilde{\varphi}"'] & N_S \arrow[d, "\varphi"] \\ M \arrow[r] & M_S \end{tikzcd}$$

φ ⟸ inclusion. Given $s^{-1}n \in M_S$ s.t. $\varphi(s^{-1}n) = 0$.

$0 = \varphi(s^{-1}n) = s^{-1}\varphi(n) \Rightarrow \varphi(n) = 0$ in $M_S \Leftrightarrow \exists t \in S : t\tilde{\varphi}(n) = 0$ in M.

$\Leftrightarrow 0 = \tilde{\varphi}(tn) \underset{\tilde{\varphi} \text{ is inj.}}{\Rightarrow} tn = 0 \Rightarrow s^{-1}n = t^{-1}t\,s^{-1}n = 0$ in N_S //

"Corollary": M Noetherian $\Rightarrow M_S$ Noetherian.

(In particular, if A Noeth $\Rightarrow A_S$ Noetherian) (and the same for Artinian's)

Pf: It is enough to show that all submodules of M_S are of the form N_S, for submodules N of M.

In particular, if $K \subseteq M_S$ is a submodule, then $K \simeq \varphi^{-1}(K)_S$ where $\varphi: M \to M_S$

Key fact: any $x \in M_S$ is $\frac{\varphi(m)}{s}$ for $m \in M$, $s \in S$...

Prop: Let M be an A-module, and $x \in M$. Then:

$x = 0$ iff x goes to 0 in M_P for every maximal ideal P of A.

$(M_P = M_{A \setminus P} = M \otimes_A A_P)$

Pf $\Rightarrow$ clear

$\Leftarrow$ if x goes to 0 in M_P, then $sx = 0$ in M for some $s \in A \setminus P$.

i.e. $\operatorname{ann}(x) \notin P \Rightarrow \operatorname{ann}(x) = A$, so $x = 0$.

Corollary: $M = 0 \Leftrightarrow M_P = 0$ for every maximal ideal P.

field!

residue field of A_p: A_P/pA_P (if P maximal, $k(P) = A/P$)

Prop: Let M f.g. A-module.

Then $M = 0$ iff $M \otimes_A k(P) = 0$ for every maximal ideal P.

Pf By Nakayama, if N is a module over a local ring B and N f.g. then $N/mN = 0 \Rightarrow N = 0$

Apply it to A_P the local ring, and $M = M_P$. Then $M_P \otimes_A k(P) = M_P \otimes_A A/P =$

$= M_P \otimes_{A_P} \left(A_P / pA_P \right) = M_P / pA_P M$ //

Remark: $A_S \otimes_A A_S \simeq A_S$, and if M is an A_S-module,

$M \otimes_A A_S \simeq M$.

We can then say that if M is an A_S-module, N an A-module, then $M \otimes_A N \simeq M \otimes_{A_S} N_S$.

$$\left(M \otimes_A N \simeq (M \otimes_A A_S) \otimes_A N = M \otimes_A (A_S \otimes_A N) = M \otimes_A N_S \right).$$

Def M module over A. The <u>support</u> of M over A is

$$\mathrm{Supp}_A(M) := \{ P \in \mathrm{Spec}(A) \mid M_P \neq 0 \}$$

(i.e. $\mathrm{Supp}(M) = \emptyset \Leftrightarrow M = 0$).

If M is finitely generated, then by Nakayama $M_P = 0 \Leftrightarrow M_P/PA_PM_P = 0 \Rightarrow M_P \otimes_A k(P) = 0$

<u>Prop</u>: If M f.gen. A-module, then $M \otimes_A k(m) = 0$ for every maximal $m \subseteq A \Rightarrow M = 0$.

<u>Prop</u>: If M is a f-gen A-module, then $\mathrm{Supp}_A(M)$ is closed in $\mathrm{Spec}(A)$.

Pf Let $m_1, \dots, m_r$ be a set of generators of M.

$P \in \mathrm{Supp}_A(M) \Leftrightarrow M_P \neq 0 \Leftrightarrow m_i$ is nonzero in M_P, for some $1 \le i \le r \Leftrightarrow$

$\Leftrightarrow \mathrm{ann}(m_i) \subseteq P$ for some i $\Leftrightarrow \mathrm{ann}(M) = \bigcap_{i=1}^{n} \mathrm{ann}(m_i) \subseteq P \Leftrightarrow \mathrm{supp}(M) = V(\mathrm{ann}(M))$. //

Note, if M is <u>not</u> fin-generated, $\mathrm{supp}(M) \subseteq V(\mathrm{ann}(M))$.

<u>Prop</u>: $A \xrightarrow{f} B$ homomorphism of rings. M a f.gen B-module.

If $M \otimes_A k(P) = 0$ for all primes $P \subseteq A$, then $M = 0$.

Pf Suppose $M \neq 0$. Then $\exists Q \subseteq B$ prime, such that $M_Q \neq 0$ and in fact such that $M_Q/QB_Q \neq 0$ (by Nakayama).

Let $P = f^{-1}(Q) \subseteq A$ (also a prime).

We have $\overset{\text{image of } P \text{ by } f}{P} M_Q \subseteq Q M_Q$, so $M_Q/PM_Q \neq 0$.

Let $T = B - Q$, $S = A - P$.

<u>Claim</u>: $\underset{\text{as a }B\text{-module}}{M_{f(S)}} \simeq \underset{\text{as an }A\text{-module}}{M_S}$ (exercise)

Since $f(S) \in T$, have $M_Q = M_T = (M_{f(S)})_T \simeq (M_P)_T$

Now, of $M_Q/pM_Q = (M_P)_T/p(M_P)_T = \left(M_P/pM_P\right)_T = \left(M \otimes_A k(P)\right)_T \Rightarrow M \otimes_A k(P) \neq 0$ //

$\longleftarrow$

$$\begin{tikzcd} B & Q \in \mathrm{Spec}(B) \arrow[d, "f^\#"] \\ A \arrow[u, "f"] & \{P\} \in \mathrm{Spec}(A) \end{tikzcd}$$

fiber of $f^\#$ over $\{P\}$.

We're looking for $P' \subseteq B$ that restrict to P in A.

$$\begin{tikzcd} B \arrow[r] & B \otimes_A k(P) \\ A \arrow[u] \arrow[r] & k(P) \arrow[u] \end{tikzcd}$$

it turns out that the fiber $\simeq \mathrm{Spec}(B \otimes_A k(P))$.

$S = A \setminus P$

$B \otimes_A k(P) = B_{f(S)}/pB_{f(S)}$ (exercise)

<u>Example</u>: Let $M = B/I$.

$B/I \otimes_A k(P) = 0$

$$\begin{tikzcd} & & \mathrm{Spec}(B) \arrow[d] \\ \text{fibers} \arrow[r, hook] \arrow[d] & \mathrm{Spec}(B/I) \arrow[ur, hook] \arrow[r] & \mathrm{Spec}(A) \\ \{P\} \arrow[rr, hook] & & \mathrm{Spec}(A) \end{tikzcd}$$

$\Rightarrow B/I = 0$.

<u>Proposition</u>: A ring, M module. Let

(1) $U_r := \{P \in \mathrm{Spec}(A) \mid M_P$ can be generated by r elements over $A_P\}$.

If M is f-gen, then U_r is open.

(2) $U_F := \{P \in \mathrm{Spec}(A) \mid M_P$ is a free A_P-module$\}$.

If M is finitely presented, U_F is open.

Def M is finitely presented if $\exists$ an exact sequence:

$$\underbrace{A^q}_{\text{fin presentn}} \longrightarrow \underbrace{A^p \longrightarrow M \longrightarrow 0}_{\text{fin. generators}}$$

Lemma: If $0 \to K \to M \to N \to 0$ exact, M = f-gen, N = f. pres. Then K is f-generated.

Lemma (Snake lemma):

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & K' \arrow[r] \arrow[d] & K \arrow[r] \arrow[d] & K'' \arrow[d] \arrow[ddll, dashed, bend left, "\delta"] & \\
0 \arrow[r] & M' \arrow[r] \arrow[d] & M \arrow[r] \arrow[d] & M'' \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & N' \arrow[r] \arrow[d] & N \arrow[r] \arrow[d] & N'' \arrow[r] \arrow[d] & 0 \\
 & C' \arrow[r] \arrow[d] & C \arrow[r] \arrow[d] & C'' \arrow[r] \arrow[d] & 0 \\
 & 0 & 0 & 0 &
\end{tikzcd}$$

Given two exact sequences and the kernels & cokernels of vertical maps as shown, there is an exact sequence

$$0 \to K' \to K \to K'' \to C' \to C \to C'' \to 0$$

δ is defined with diagram chasing:
$x \in K''$, $\delta(x) \in C'$ be the unique $y \in C'$ s.t.
$\exists$ $a \in M$, $b \in N'$ s.t.

$$\begin{tikzcd}
 & & x \arrow[d] \\
 & a \arrow[r] \arrow[d] & ? \\
b \arrow[r] \arrow[d] & ? & \\
y & &
\end{tikzcd}$$

Pf/exercise.

Pf (of previous lemma):

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & ? \arrow[r] \arrow[d] & ? \arrow[r] \arrow[d] & U \arrow[d] \arrow[ddll, bend left] & \\
 & A^r \arrow[r] \arrow[d] & A^{p+r} \arrow[r] \arrow[d] & A^p \arrow[r] \arrow[d, "\alpha"] & 0 \\
0 \arrow[r] & K \arrow[r] \arrow[d] & M \arrow[r] \arrow[d] & N \arrow[r] \arrow[d] & 0 \\
 & C \arrow[r] \arrow[d] & 0 \arrow[r] & 0 & \\
 & 0 & & &
\end{tikzcd}$$

finitely generated.

$\alpha(e_i) = n_i$ $i = 1..p$ generate N.
Choose $m_i \in M$ which map to n_i.
Can choose a finite set of additional generators $k_1, \dots, k_r$ that actually lie in K.

By snake lemma, C is f-gen because U is, and so K is f-gen //.

Proof of proposition:

(1) $U_r = \{p : M_p$ can be generated by r elements$\}$. Show that U_r is open if M f-gen.

Show: if $P \in U_r$, then $\exists$ open n-h of P in U_r.

M_p: Let $m_1, \dots, m_r \in M$ s.t. images generate M_p, coming from $m_1', \dots, m_r'$ generators of M_p.

Have $\varphi : A^r \to M$ so that $A^r \to M \to C \to 0$

and $C_p = 0$ since $A^r_p \to M_p \to C_p \to 0$ is exact. $\underset{\text{coker}(\varphi)}{C}$

Consider $\mathrm{Supp}(C)$, a closed set since M is f-gen.

Let $V = \mathrm{Spec}(A) - \mathrm{Spec}(C)$.

$Q \in V \Rightarrow C_Q = 0 \Rightarrow A^r_Q \to M_Q \to \underset{0}{C_Q} \to 0$ so $Q \in U_r$ s.t. $P \in V \subseteq U_r$.

(2) If $P \in U_F$, $\exists m_1, \dots, m_r \in M$ whose images in M_P are a free basis.

In proof of (1), we actually showed that if $m_1, \dots, m_r \in M$ are such that their images generate M_P as an A_P-module, then $\exists V \in \mathrm{Spec}(A)$ open s.t. $Q \in V \Rightarrow m_1, \dots, m_r$ generate M_Q as an A_Q-module.

So $\exists f \in A$ s.t. $P \in D(f) \subseteq V$ since $D(f)$'s are a basis for the topology.

$D(f) = \{Q \mid Q \not\ni f\}$

$m_1, \dots, m_r$ give an homomorphism of modules $A^r \xrightarrow{\varphi} M \to C \to 0$ (exact).

After inverting f, φ becomes surjective:

$$A^r[\tfrac{1}{f}] \xrightarrow{\varphi'} M[\tfrac{1}{f}] \to C[\tfrac{1}{f}] \to 0 \Rightarrow M[\tfrac{1}{f}]_{QA[\frac{1}{f}]} \cong M_Q \text{ for } Q \not\ni f.$$

In particular, $C[\tfrac{1}{f}]_{QA[1/f]} = C_Q = 0$ since $Q \in V$ so φ' is surjective.

$\left(C[\tfrac{1}{f}]_{\tilde{Q}} = 0 \ \forall \text{ prime } \tilde{Q} \text{ of } A[\tfrac{1}{f}] \Rightarrow C[\tfrac{1}{f}] = 0 \right)$.

Consider $K = \ker(A^r \xrightarrow{\varphi} M)$. Have an exact seq. $0 \to K[\tfrac{1}{f}] \to A^r[\tfrac{1}{f}] \to M[\tfrac{1}{f}] \to 0$

(since localization is exact).

$\downarrow$

Since M is finitely presented over A, so is $M[1/g]$ over $A[1/g]$.
(localization of f.pres. module is f.presented).

Since $A^r[1/g]$ is f-gen, $\Rightarrow K[1/g]$ is finitely generated over $A[1/g]$.

Hence, $\mathrm{Supp}_{A[1/g]} K[1/g]$ is closed in $\mathrm{Spec}(A[1/g]) \simeq \underset{\text{open}}{D(g)} \subseteq \mathrm{Spec}\, A$

So $W = \mathrm{Spec}\, A[1/g] - \mathrm{Supp}\, K[1/g]$ is open in $D(g)$ hence open in $\mathrm{Spec}(A)$.

$Q \in W \Rightarrow K[1/g]_{QA[1/g]} \simeq K_Q = 0$, so $A^r_Q \longrightarrow M_Q$ is an isomorphism.

So $Q \in V \Rightarrow M_Q$ free.

Rk: Can define $U_{F,r} := \{ P \mid M_P$ is free of rank r over $A_P \}$.

We have proven that $U_{F,r}$ is open if M is finitely presented.

$\boxed{\text{Def}}$ We say that M is locally free if M_P is free for each $P \in \mathrm{Spec}(A)$.

If M is finitely presented, $\mathrm{Spec}\, A = \bigsqcup_{r=0}^{m} U_{F,r}$ (m = size of a generating set of M).

So $U_{F,r}$ are open and closed subsets.

Rk: Can define $d(P) = \mathrm{rk}_{A_P}(M_P)$ and $d : \mathrm{Spec}\, A \longrightarrow \mathbb{Z}$ is continuous.

It is a locally constant function.

(In particular, if $\mathrm{Spec}\, A$ is connected $\Rightarrow d$ is constant)

Example: $A = k[X,Y] \supseteq M = (X,Y)$. $A/M \cong k$.

$U_2(M) = \mathrm{Spec}(A)$

$U_1(M) = \mathrm{Spec}(A) \setminus \{M\} \simeq U_{F,1}(M)$. $\leftarrow$ Why?

We have $0 \to M \to A \to A/M \to 0$. Localizing,

$0 \to M_P \to A_P \to \underset{A_P/MA_P}{(A/M)_P} \to 0$ exact. $(A/M)_P \overset{?}{=} 0 \Leftrightarrow 1$ goes to 0 in $(A/M)_P \Leftrightarrow$

$\Leftrightarrow \exists s \in A \setminus P$ s.t. $s \cdot 1 \in M$

$\Leftrightarrow A \setminus P \cap M \neq \emptyset \Leftrightarrow M \not\subseteq P$

$((A/M)_P \neq 0 \Leftrightarrow M \subseteq P)$. But M is maximal, so $P = M$.

Integral Extensions ([Mats. §9, Eisenbud §4]).

Prop Let A a ring, B = A-algebra generated over A by one element b.

i.e. $B \simeq A[X]/J$ $(b \Leftrightarrow X)$.

Then,

(1) B is a finite A-module generated by r elements $\Leftrightarrow$ $\exists$ monic polynomial $f \in J$ of degree r.

(2) B is a free A-module of rank r iff $J = (f)$ for some monic f of degree r.

Pf (1) $\Leftarrow$) if $f \in J$ is monic of degree r, $f = X^r + a_{r-1}X^{r-1} + \dots + a_0$

Can do polynomial long division: if $g \in A[X]$, can write

$g = fh + k$ where $\deg k < r$, $h, k \in A[X]$.

In particular, B is generated as A-module by $1, b, b^2, \dots, b^{r-1}$

$\Rightarrow$) By C-H th, $\varphi : B \to B$, $x \mapsto bx$ $\Rightarrow$ obtain $f(x) \in A[X]$ s.t. $f(\varphi)$ acts as 0 on B.

So $f(\varphi) \cdot 1 (=0) = f(b)$, i.e. $f \in J$.

(2) $\Leftarrow$) clear: $1, x, \dots, x^{r-1}$ is a basis of $A[X]/(f)$

$\Rightarrow$) By part (1), $\exists$ monic polynomial f of degree r in J.

$$\underset{\text{free of rank } r}{A[X]/(f)} \twoheadrightarrow \underset{\text{free of rank } r}{A[X]/J} \simeq B$$

$\Rightarrow$ isomorphism.

(a surjective map of free modules is an isomorphism) //

Def: if B is an A-algebra, $b \in B$ is <u>integral over A</u> if $\exists$ some monic polynomial $f \in A[X]$ s.t. $f(b) = 0$.

(or equivalently, if $A[b] \subseteq B$ is finite as an A-module).

Remark :
$$\begin{tikzcd} A \arrow[rr, "f"] \arrow[dr] & & B \\ & A/I \arrow[ur] & \end{tikzcd}$$
$b \in B$ integral over $A \iff \bar{b}$ integral over A/I.

Matsumura Assumes that $A \subseteq B$ (i.e. B is an extension ring of A) when defining integrality.

Lemma: If B is an A-algebra, $b \in B$. Then

b integral over $A \iff \exists$ sub-A-algebra $C \subseteq B$ which is finite as an A-module

Pf
$\Rightarrow$) take $A[b] =: C$

$\Leftarrow$) C-H Th: consider $\varphi : C \to C$, $x \mapsto bx$ map of finite A-modules $\Rightarrow$ get a monic $f \in A[X]$ s.t. $f(\varphi) = 0 \Rightarrow f(\varphi)\cdot 1 = f(b) = 0$ (Same as (1) in prop)

Corollary: the set of elements of B that are integral over A form a sub-A-algebra.

Pf $\operatorname{img}(A)$ consists of integral elements $(X - a)$.

If $b, b' \in B$ are integral over A, consider $C = A[b, b'] \subseteq B$.

Since $A[b]$ is gen by $1, b, \dots, b^{m-1}$
$A[b']$ " " $1, b', \dots, (b')^{n-1}$ $\Rightarrow C$ is generated by $\{ b^i (b')^j \}_{\substack{0 \le i \le m \\ 0 \le j \le n}}$

So $b + b'$ and $bb' \in A[b, b']$.

Def Say B is integral over A iff B consists of elements integral over A (equivalently, if B is generated as A-algebra by integral elements).

If $A \to B$, let $\tilde{A} \subseteq B$ be the set of integral elements, called the integral closure of A in B (it is a subring of B).

Def : if A is a domain, let $B = K(A)$. Say that A is integrally closed if it is its own integral closure in $K(A)$.

Given $K \subseteq L$ a field extension

Def $S \subseteq L$ a subset is <u>algebraically independent</u> over K iff there are no polynomial relations of elements of S (with coeffs. in K).

(i.e if $\alpha_1, \dots, \alpha_r \in S$ distinct, $f \in K[X_1, \dots, X_r]$ then $f(\alpha_1, \dots, \alpha_r) = 0 \Rightarrow f = 0$)

(i.e the K-algebra hom $K[X_1, \dots, X_r] \to L$ determined by $\alpha_1, \dots, \alpha_r$ is <u>injective</u>)

Def A <u>transcendence basis</u> of L over K is a maximal algebraically independent subset. It exists by Zorn's lemma.

If $S \subseteq L$ is alg. indep. over K, then S is a basis iff L is algebraic over $K(S)$.

(Pf: if $\beta \in L$ then $S \cup \{\beta\}$ is <u>not</u> alg. indep., so $\exists f \in K[X_1, \dots, X_r, Y]$ s.t. $f(\alpha_1, \dots, \alpha_r, \beta) = 0$.
write $g(T) := f(\alpha_1, \dots, \alpha_r, T) \in K(S)[T]$ $\Rightarrow$ β is a root of g.
If L is algebraic over $K(S)$, similarly.).

<u>Lemma</u>: if $S \subseteq T \subseteq L$ s.t. S is alg. indep over K and L is algebraic over $K(T)$, then $\exists$ transcendence basis B s.t. $S \subseteq B \subseteq T$.

Pf Zorn's lemma.

<u>Proposition 1</u>: If B, B' are transcendence basis of L over K, and if $|B| = n$, then $|B'| = n$. (so the "cardinality" is well defined).

Def The <u>transcendence degree</u> of L over K, $\mathrm{trdeg}_K L := |B| \in \mathbb{N} \cup \{\infty\}$.

<u>Example</u>: $\mathbb{R}$, $\mathbb{C}$ have ∞ tr. degree over $\mathbb{Q}$. (in fact, uncountable).

Pf (of Prop 1):

Consider $\beta_1, \beta_2, \ldots, \in B'$ distinct. Let B_1 be tr. basis s.t.

$$\{\beta_1\} \subseteq B_1 \subseteq B \cup \{\beta_1\}$$

if $\beta_1 \notin B$, this is proper inclusion; if $\beta_1 \in B$ it is equality.

In either case, $|B_1| \leq |B| = n$.

Define inductively B_j such that:

$$\{\beta_1, \ldots, \beta_j\} \subseteq B_j \subseteq B_{j-1} \cup \{\beta_j\}$$

Check that we discard an element of $B \cap B_{j-1}$ to obtain B_j (except if $\beta_j \in B$).

Thus, $B_n \cap B = B' \cap B \Rightarrow$ since $B_n \subseteq B \cup \{\beta_1, \ldots, \beta_n\}$, must have $B_n \subseteq B'$.

Since B_n & B' are tr. basis, must have $B_n = B'$ and so $|B'| = |B_n| \leq n$. //

Proposition 2: $K \subseteq L \subseteq F$; $\operatorname{trdeg}_K L = m$, $\operatorname{trdeg}_L F = n$. Then

$\operatorname{trdeg}_K F = m + n$ (it will be ∞ if m or n are ∞).

Pf Exercise.

Def if K is alg. closed field, $I \subseteq K[X_1, \ldots, X_r]$, then the variety of I.

$$Z(I) = \{\underline{a} = (a_1, \ldots, a_r) \in K^r \mid f(\underline{a}) = 0 \text{ for all } f \in I\}.$$

Prop: if $A \to B \to C$ ring homomorphisms s.t. B is integral over A, and $c \in C$ s.t. c is integral over B, then c is integral over A.

Pf

$\exists$ monic polynomial $f \in B[X]$ s.t. $f(c) = 0$. $f(X) = X^n + b_{n-1}X^{n-1} + \cdots + b_0$, $b_j \in B$.

$R := A[b_0, \ldots, b_{n-1}] \subseteq B$ it is a finitely-gen A-module, since the b_j are integral over A.

$R[c] \subseteq C$ is finite over R, since c satisfies $f \in R[X]$.

So $R[c]$ is finite over R and R finite over $A \Rightarrow R[c]$ is finite over $A \Rightarrow$

$\Rightarrow c$ is integral over A. //

Prop: Any U.F.D. is an integrally closed domain
(i.e A is its own integral closure in $K = K(A)$).

Pf Let $\alpha \neq 0$ in K, which is integral over A, so satisfies a monic

$$f(X) = X^n + c_{n-1}X^{n-1} + \dots + c_0 \in A[X].$$

write $\alpha = \frac{a}{b}$, $a, b \in A$. Write in lowest terms (i.e. assume a, b to have no common prime factors).
We'll show that $b \in A^\times$ (is a unit), so $\alpha \in A$.

$$0 = \left(\frac{a}{b}\right)^n + c_{n-1}\left(\frac{a}{b}\right)^{n-1} + \dots + c_0 \Rightarrow 0 = a^n + c_{n-1}b\,a^{n-1} + \dots + c_1 b^{n-1}a + c_0 b^n$$

If $p \mid b \Rightarrow p \mid a^n \Rightarrow p \mid a \Rightarrow a, b$ have a common factor $\Rightarrow p$ is a unit. //

Example: $\mathbb{Z}$, $k[X]$, $k[X_1, \dots, X_n]$ are integrally closed.

Prop: Let B be an A-algebra, $f \in A[X]$ monic, and suppose $f = g \cdot h$ where $g, h \in B[X]$ monic. Then, the coefficients of g and h are integral over A.

Corollary: for $A = \mathbb{Z}$, $B = \mathbb{Q}$, Gauss proved if a polynomial factors over the rationals it must factor over the in the integers.

Pf (of prop): In general, if $g \in R[T]$, can construct $R[\alpha] := R[X]/(g(X))$, $\alpha \longleftarrow T$

Then, in $R[\alpha]$, have $g = (T - \alpha)g_1$ where $g_1 \in R[\alpha][T]$. (by pol'l long division)
We can then inductively adjoin roots $\alpha_1, \alpha_2, \dots$ of g to B, and of h.
We get $C = B[\alpha_1, \dots, \alpha_r, \beta_1, \dots, \beta_s]$ s.t.

$$g = \prod(T - \alpha_i) \quad h = \prod(T - \beta_j) \quad \text{over } C[T].$$ (use that g and h are monic)

All α's and β's are in fact roots of $f = gh$. Let $R = A[\alpha_1, \dots, \alpha_r, \beta_1, \dots, \beta_s] \subseteq C$
Then R is integral over A (we've adjoined roots of a monic).
Then g and h still factor completely in $R[T]$. The coeffs of g and h can be written as polynomials in their roots, so done. //

<u>Corollary</u>: Let A be an int. closed domain, $K = K(A)$ its field of fractions. $L \supseteq K$ be an alg extension. Then,

$\alpha \in L$ is integral over A iff its minimal monic irred. poly over K has coefficients in A.

Pf/ $\Leftarrow$) clear.

$\Rightarrow$) Let $\alpha \in L$ integral over A, and $f \in A[T]$ a monic s.t. $f(\alpha) = 0$.
Choose f to be of minimal degree with this property.
If $f = gh$, $g, h \in K[T]$ monic of positive degree, then since A is integrally closed in K, have that $g, h \in A[T]$ by previous proposition, thus contradicting minimality. //

<u>Example</u>: K algebraic ext. over $\mathbb{Q}$. Let $\mathcal{O}_K$:= integral closure of $\mathbb{Z}$ in K.
($\mathcal{O}_K$ are the algebraic integers, i.e. whose monic irr. over $\mathbb{Q}$ have integral coeffs).

Consider $G = \mathrm{Gal}(K/\mathbb{Q})$. If $\varphi \in G$, then $\varphi(\mathcal{O}_K) = \mathcal{O}_K$

$$\begin{array}{ll} \mathrm{Spec}(\mathcal{O}_K) & \mathfrak{P}_1 \; \mathfrak{P}_2 \ldots \quad = \{\mathfrak{P} \subseteq \mathcal{O}_K : \mathfrak{P} \cap \mathbb{Z} = (p)\}. \\ \big\downarrow f^\# & \\ \mathrm{Spec}(\mathbb{Z}) & (p) \end{array}$$

G acts on $(p)\mathcal{O}_K$.

Given $\mathfrak{P} \subseteq \mathcal{O}_K$, $G_{\mathfrak{P}} = \{\varphi \in G : \varphi(\mathfrak{P}) = \mathfrak{P}\}$. Such φ induces an automorphism over $\mathcal{O}_K/\mathfrak{P} \supseteq \mathbb{F}_p$. $I_{\mathfrak{P}} = \{\varphi : \varphi \equiv \mathrm{id} \bmod \mathfrak{P}\} \subseteq G_{\mathfrak{P}}$.

Example: k a field.

$A = k[T^2, T^3] \subseteq B = k[T]$

basis$/k$: $1, T^2, T^3, T^4, \ldots$

$$A \xleftarrow{\approx} \underbrace{k[X,Y]/(Y^2-X^3)}_{C}$$

$T^2 \longleftarrow X$

$T^3 \longleftarrow Y$

$0 \longleftarrow Y^2 - X^3$

$\leftarrow$ as $k[X]$-module, C is free of rank 2.

$C = k[X][Y]/(Y^2-X^3)$ $\leftarrow$ monic in Y

as k-vectorspace, C has basis

$1, X, X^2, X^3, \ldots \longrightarrow 1, T^2, T^4, T^6$

$Y, XY, X^2Y, X^3Y, \ldots \quad T^3, T^5, T^7, \ldots \quad \in A$

So the previous map is actually an isomorphism

Claim: B is the integral closure of A.

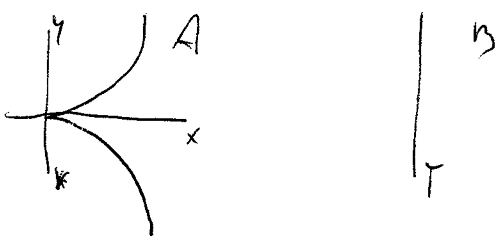
$k(B) = k(T)$ But $k(A) = k(T)$ since $T = \frac{T^3}{T^2} \in k(A)$.

$\cup$

$k(A)$

B is integrally closed. Only need to see that B is integral over A.

But can check for generators, and $T \in B$ satisfies $U^2 - T^2 \in A[U]$.



Example 2: $A = k[T^2-1, T^3-T] \subseteq B = k[T]$.

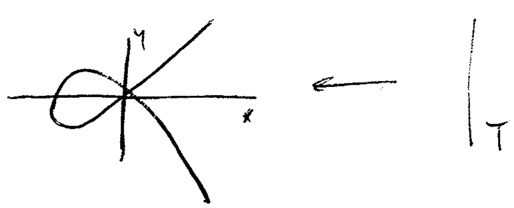
$$A \xleftarrow{\approx} k[X,Y]/(Y^2-X^2(X+1))$$

$T^2-1 \longleftarrow X$

$T^3-T \longleftarrow Y$

check that it is an isomorphism.

And B is also the integral closure of A.



This is called "normalizing the curve", which removes singularities.

Prop: let $B = A$-algebra. $S \subseteq A$ a multiplicatively-closed subset, and suppose $\tilde{B} \subseteq B$ is the integral closure of A in B. Then: $\tilde{B}_S$ is the integral closure of A_S in B_S.

Pf. • Show that $\tilde{B}_S$ is integral over A_S:

As a ring, $\tilde{B}_S$ is generated over A_S by the elements of $\tilde{B}$.

Since $b \in \tilde{B}$ is integral over A, then $\frac{b}{1} \in \tilde{B}_S$ is integral over A_S: it still satisfies a monic with coeff in $A \subseteq A_S$.

• Show now that $\tilde{B}_S$ is the integral closure:

Suppose $\frac{b}{s} \in B_S$ is integral over A_S. want $\frac{b}{s} \in \tilde{B}_S$.

We'll show that $\exists\, t \in S$ s.t. tb is integral over A.

Consider a monic $f(x) = X^n + \left(\frac{c_{n-1}}{d_{n-1}}\right) X^{n-1} + \dots + \frac{c_0}{d_0} \in A_S[X]$ s.t. $f\left(\frac{b}{s}\right) = 0$

So $\left(\frac{b}{s}\right)^n + \frac{c_{n-1}}{d_{n-1}}\left(\frac{b}{s}\right)^{n-1} + \dots + \frac{c_0}{d_0} = 0$ $\qquad (c_i \in A,\ d_i \in S)$.

Multiply by $(s\, d_{n-1} \cdots d_0)^n$ (to clear denominators and more).

$$(b d_0 \cdots d_{n-1})^n + c_{n-1} s\, (d_0 d_1 \cdots d_{n-2})(b d_0 \cdots d_{n-1})^{n-1} + c_{n-2} s^2 (d_0^2 \cdots d_{n-3}^2 d_{n-2} d_{n-1}^2)(b d_0 \cdots d_{n-1})^{n-2}$$
$$+ \dots + c_0 s^n (\ ) = 0$$

Then bt (for $t = d_0 \cdots d_{n-1} \in S$) satisfies a monic over A

$\Rightarrow b = bt(t^{-1})$ is integral over A_S. As $b \in \tilde{B}$, $\frac{b}{s} \in \tilde{B}_S$.

• <u>Lying over / Going Up Theorem:</u>

⇝ If $A \subseteq B$ is an integral extension,

- if $P \subseteq A$ prime, then $\exists$ prime $Q \subseteq B$ s.t. $Q \cap A = P$.
- if $P \subseteq A$ prime and $I \subseteq B$ ideal s.t. $I \cap A \subseteq P$, then $\exists$ prime $Q \subseteq B$, $I \subseteq Q$ s.t. $Q \cap A = P$.

(the first • says that $f^{\#} : \mathrm{Spec}(B) \to \mathrm{Spec}(A)$ is surjective).

Pf: <u>Lying over ⇒ Going up:</u>

Given $A \cap I \subseteq P \subseteq A$, $I \subseteq B$, $A \subseteq B$.

Replace: $A' := A/_{A \cap I}$, $B' := B/_{I}$, $P' := P/_{A \cap I} \subseteq A'$.

Since B integral over A, have B' integral over A'. So lying over gives $Q' \subseteq B'$ s.t. $Q' \cap A' = P'$ and take $Q :=$ preimage of Q' in B. //

<u>Pf of lying over:</u>

Let $S = A \setminus P$. Then $A_p = A_s \subseteq B_s$ since localization is exact.

It is enough to find a prime $\tilde{Q} \subseteq B_s$ s.t. $\tilde{Q} \cap A_p = PA_p$, the maximal of A_p. Why?

$$\begin{tikzcd} B \arrow[r] & B_s \\ A \arrow[r] \arrow[u] & A_s \arrow[u] \end{tikzcd} \qquad \begin{tikzcd} Q \arrow[d, squiggly] & \tilde{Q} \arrow[l, squiggly] \arrow[d, squiggly] \arrow[dl] \\ P & PA_p \arrow[l, squiggly] \end{tikzcd}$$

(Then we can take $Q = B \cap \tilde{Q}$).

Claim: $PA_sB_s (= PB_s)$ is a proper ideal (after that, if its proper it is contd in $\tilde{Q}$ prime, which will restrict to something $\supseteq PA_s$).

Suppose not, i.e. suppose $PB_s = B_s$. Then $1 = \sum_{i=1}^{r} x_i b_i$, $x_i \in PA_s$, $b_i \in B_s$

Since B is integral over A, B_s is integral over A_s

Let $R := A_s[b_1, \dots, b_r] \subseteq B_s$. R is fin. gen as an A_s-module. Still in R, $1 = \sum x_i b_i$ (since $x_i, b_i \in R$). So $(PA_s)R = R$. By Nakayama, $R = 0$.

But $A_s \subseteq R \Rightarrow$!! //

• Hilbert's Nullstellensatz:

k a field. $A = k[X_1, \dots, X_r]$.
Then every prime ideal of A is an intersection of maximal ideals $\mathfrak{m}$ of A which have the property that $A/\mathfrak{m}$ is finite over k.
(in particular, all maximal ideals are s.t. $A/\mathfrak{m}$ is finite over k).

→ Special case: if k is algebraically closed, and $\mathfrak{m} \subseteq A$ maximal,
VIP

$$k \hookrightarrow A \twoheadrightarrow A/\mathfrak{m} \quad \Rightarrow \quad A/\mathfrak{m} \cong k \text{ since } A/\mathfrak{m} \text{ is algebraic.}$$

So $\mathfrak{m}$ is the kernel of

$$\begin{tikzcd} & & & k \arrow[d, "\wr"] \arrow[dl] \\ 0 \arrow[r] & \mathfrak{m} \arrow[r] & A \arrow[r] & A/\mathfrak{m} \end{tikzcd}$$

$$X_j \longmapsto a_j \in k$$

So $\mathfrak{m}_{\underline{a}} = (X_1 - a_1, \dots, X_r - a_r)$.

So $\mathfrak{m}\text{-Spec}(A) \longleftrightarrow k^r$

$$\mathfrak{m}_{\underline{a}} \longleftrightarrow \underline{a}$$

[Corollary of Going Up: Let $A \subseteq B$ be an integral extension of domains.
Then A is a field iff B is a field.

Pf $\Rightarrow$) if A is a field, $b \in B$, $b \neq 0$. Then $A[b]$ is a finite A-module.
Thus $A[b] \simeq A[X]/(f(X))$ f monic irreducible. So $A[b]$ a field $\Rightarrow$
$\Rightarrow b^{-1} \in A[b] \subseteq B$. $\Rightarrow B$ is a field.

$\Leftarrow$) if B is a field, then by lying over thm, all primes $\mathfrak{p}$ of A are of the form $\mathfrak{p} = A \cap Q$, Q prime in B. As B is a field, $\mathfrak{p} = A \cap (0) = (0)$. //

~~Proof of Nullstellensatz~~:

Let, given $J = (f_1, \dots, f_n) \subseteq A$, $Z(J) := \{ \underline{a} \in K^r \mid f(\underline{a}) = 0 \ \forall f \in J \} =$

the zeroes of the ideal J. $= \{ \underline{a} \in K^r \mid f_j(\underline{a}) = 0 \ \forall j = 1 \dots n \}$.

$= \{ \underline{a} \in K^r \mid M_{\underline{a}} \supseteq J \}$.

An algebraic set $X \subseteq K^r$ is any set of the form $Z(J)$ for some ideal J.

(note that if $J' = \sqrt{J} = \{ f \in A \mid f^n \in J$ for some $n \}$. Then $Z(J) = Z(J')$).

Given any subset $X \subseteq K^r$,

$I(X) = \{ f \in A \mid f(\underline{a}) = 0$ for all $\underline{a} \in X \} = \bigcap_{\underline{a} \in X} M_{\underline{a}}$ "ideal of vanishing of X".

Then:

$X \subseteq X' \Rightarrow I(X) \supseteq I(X')$.

$Z(J) \subseteq Z(J') \Leftarrow J \supseteq J'$

Also,

$Z(I(X)) \supseteq X$

$I(Z(J)) \supseteq J$

Algebraic sets are those X s.t. $Z(I(X)) = X$. (all formal)

Also, I, Z give a bijective correspondence:

$\{$alg sets$\} \longleftrightarrow \{$ideals J s.t. $I(Z(J)) = J \}$.

The corollary of Nullstellensatz says that $I(Z(J)) = \sqrt{J}$, and then

$\{$alg sets$\} \longleftrightarrow \{$radical ideals$\}$.

Now, $I(Z(J)) = \bigcap_{M_{\underline{a}} \supseteq J} M_{\underline{a}} \supseteq \bigcap_{P \supseteq J} P = \sqrt{J}$

Nullstellensatz says that this is an equality.

In the case k is not algebraically closed, still know that all maximal ideals are kernels of maps $0 \to M \to A \to L \to 0$ where L is a finite extension of k.

All maximal ideals are kernels of $A \to \bar{k}$ = alg closure of k.
$A = k[x_1, \ldots, x_r]$

Proof of Nullstellensatz:

Def: A is a Jacobson ring if every prime ideal of A is a intersection of maximal ideals. Note that A Jacobson $\Rightarrow$ A/J is Jacobson for any ideal J.

Example: fields are Jacobson.
$\mathbb{Z}$ is Jacobson.
$\mathbb{Z}_{(p)}$ is not a Jacobson ring: $\operatorname{spec}(\mathbb{Z}_{(p)}) = \{p\mathbb{Z}_{(p)}, 0\}$.
So local rings are not Jacobson unless they are fields.

Lemma: A Jacobson, $P \subseteq A$ prime. Then either P is maximal or P is contained in infinitely many distinct maximal ideals.

Pf If P is non-maximal, P contained only in the maximals $M_1, \ldots, M_d$.
So $P = \bigcap_{i=1}^{d} M_i \supseteq M_1 \cdots M_d \Rightarrow \exists i$ s.t. $P \supseteq M_i \Rightarrow P = M_i \Rightarrow$!!
finite intersection! //

Prop: let A be a PID. Then TFAE:
a) A is Jacobson.
b) A is a field or A has infinitely many distinct maximal ideals.

Pf (a) $\Rightarrow$ (b) done: (0) is prime, and use the lemma
(b) $\Rightarrow$ (a):
Suppose A a PID but not a field. $\operatorname{Spec} A = \{0\} \cup \{(p) \mid p \text{ prime element in } A\}$. ← maximal ideals
0 is the only non-maximal.
So A Jacobson $\Leftrightarrow$ $\operatorname{Jrad}(A) = 0$. For such A, will show that A not Jacobson $\Rightarrow$ finite m-Spec.
Let $f \neq 0$ be an element of $\operatorname{Jrad}(A)$. Then f has a prime factorization $f = p_1 \cdots p_d$ p_i primes.
Thus $f \in (p) \Leftrightarrow (p) = (p_i)$ for some $i \Rightarrow$ finite m-Spec because $f \in \bigcap (p)$ //

Corollary: K a field, $K[X]$ is Jacobson (PID and not a field and has infinitely many maximal ideals (by Euclid's proof of ∞ primes)).

Prop: TFAE:

a) A is Jacobson.

b) For p prime in A and $f \in A/p$, $f \neq 0$, s.t. $(A/p)[f^{-1}]$ is a field, then A/p is a field.

Pf (a) $\Rightarrow$ (b)

WLOG, assume A is Jacobson that $A[f^{-1}]$ is a field for some $f \in A$. Want A be a field.

The primes of A, $\operatorname{Spec} A = \{0\} \sqcup \{p \mid p \not\ni f\}$. Suppose A is not a field, and derive a contradiction!

By hypothesis, $f \in \bigcap_{\substack{p \text{ prime} \\ p \neq 0}} p \subseteq \bigcap_{M \text{ maximal}} M = \overset{A \text{ Jacobson}}{\operatorname{Jrad}(A) = 0} \Rightarrow !!$

equality because A is Jacobson and (0) not maximal.

(b) $\Rightarrow$ (a)

Given A satisfying (b), If $Q \subseteq A$ prime, want that Q is intersection of maximal ideals.

Let $I = \bigcap_{Q \subseteq M \text{ maximal}} M$. Want $I = Q$. If not, $\exists f \in I \setminus Q$.

Let p be maximal among the ideals which contain Q and do not touch $\{1, f, f^2, \dots\}$ (by Zorn, and p is prime).

Now $(A/p)[f^{-1}] = A[f^{-1}]/pA[f^{-1}]$

By the way we chose p, $pA[f^{-1}]$ is maximal in $A[f^{-1}]$

So $(A/p)[f^{-1}]$ is a field. By (b), (A/p) is a field,

so p is a maximal ideal, $p \supseteq Q$, so $f \in I \subseteq p$ contradicting $f \notin p$ //.

Def An A-algebra is said to be <u>finite type over A</u> if it is generated as an A-algebra by finitely many elements. (ie. $B \cong A[X_1, \dots, X_r]/J$)

<u>Theorem</u> (General Nullstellensatz):

Let A be a Jacobson ring, and B a finite-type A-algebra. Then

1) B is Jacobson

2) If $N \subseteq B$ is a maximal ideal and $M := N \cap A$, then M is a maximal ideal of A, and B/N is <u>finite</u> over A/M.

(note that if $A = k$ is a field and $B = k[X_1, \dots, X_r]$, get B is Jacobson and that if $N \subseteq B$ maximal then B/N is finite extension of k).

Pf

We need a lemma:

<u>Lemma</u>: Let $A \subseteq B$ be an inclusion of <u>domains</u>, where A is Jacobson and B is generated as an A-algebra by <u>one</u> element. Then,

If there $\exists\, f \neq 0$, $f \in B$ s.t $B[f^{-1}]$ is a field, then

A and B are fields and B is finite over A.

Pf $S := A \setminus \{0\}$; $K := A_S = K(A)$.

$$\begin{tikzcd}
A \arrow[r, hook] \arrow[d] & B \arrow[d] \arrow[dr] & \\
K = A_S \arrow[r, hook] \arrow[rr, bend right] & B_S \arrow[r, hook] & B[f^{-1}] \cong K(B)
\end{tikzcd}$$

Since $B = A[\beta]$, also $B_S = A_S[\beta] = K[\beta]$. Thus,

either $B_S \cong k[X]$ or $B_S \cong k[X]/(p(X))$ where $p(X)$ is monic, irreducible poly $/K$.

Since $B[f^{-1}] (\cong B_S[f^{-1}])$ is a field, then $B_S \not\cong k[X]$ (because $k[X]$ is a Jacobson PID, not a Field).

So we must have $B_S \simeq k[X]/(p(X))$, and $p(\beta)=0$.

There exists $a \in A$ s.t. $a.p \in A[X]$ (by clearing denominators).

So p is actually an element of $A[a^{-1}][X]$.

We have $B[a^{-1}]$ is an $A[a^{-1}]$-algebra generated (as an algebra) by a single element β.

Since β satisfies a monic $p(X) \in A[a^{-1}][X]$, β is integral over $A[a^{-1}]$, so $A[a^{-1}] \subseteq B[a^{-1}]$ is an integral extension.

Now, $f \in B \subseteq B[a^{-1}]$, so f satisfies a monic polynomial $A[a^{-1}]$:

$f^n + c_{n-1} f^{n-1} + \dots + c_1 f + c_0$ with $c_j \in A[a^{-1}]$.

WLOG, $c_0 \neq 0$ as we are in a domain. Multiplying by $c_0^{-1} f^{-n}$ we get:

$\frac{1}{c_0} + \frac{c_{n-1}}{c_0} f^{-1} + \dots + \frac{c_1}{c_0} f^{-(n-1)} + f^{-n} = 0$.

Let $\alpha := a c_0 \in A$, so $A[\alpha^{-1}] = A[a^{-1}][c_0^{-1}]$ and then f^{-1} is integral over $A[\alpha^{-1}]$.

Therefore, $B[f^{-1}] = A[\beta][f^{-1}]$ is integral over $A[\alpha^{-1}]$.

By a corollary of lying over, $A[\alpha^{-1}]$ is a field (because $B[f^{-1}]$ is a field by hypothesis).

But since A is a Jacobson domain, A is a field, and we have $A = A_S$, $B = B_S = B[f^{-1}]$ is free over A as $B_S \simeq k[X]/(p)$ (over $k = A$).

Still need to prove Nullstellensatz:

1) B finite type over A, A Jacobson

to show that B is Jacobson, it is enough to deal with the case $B = A[\beta]$ and then proceed by induction.

Need to show, for every $Q \subseteq B$ prime and $f \neq 0$ in B/Q s.t. $(B/Q)[f^{-1}]$ is a field $\Rightarrow$ B/Q a field.

Set $A' = A/_{Q \cap A}$, $B' = B/Q$. Then $A' \subseteq B'$ is a ~~finite type~~ extension of domains generated by one element, and A' is Jacobson.

Applying the lemma, we are done.

2) Show, if $N \subseteq B$ is maximal, then $M := A \cap N$ is maximal in A and $B/N \supseteq A/M$ finite.

Enough to do the case $B = A[\beta]$ by a (downward) induction, because we already know that B is finite type over A.

$B' = B/N$, $A' = A/M$, then A' is Jacobson and B' is gen by 1 element

B' field $\Rightarrow$ A' field by the lemma, and B' finite over A'.

If k is alg. closed, can consider algebraic sets $X \subseteq k^r$, $Y \subseteq k^s$.

$\boxed{\text{Def}}$: A <u>morphism</u> of algebraic sets $\varphi : X \to Y$ is a function given by polynomials $g_1, \dots, g_s \in k[X_1, \dots, X_r]$, i.e. $\varphi(\underset{\in X}{\underline{a}}) := \underset{\in Y \subseteq k^s}{(g_1(\underline{a}), \dots, g_s(\underline{a}))}$.

Given a morphism φ, define φ^* by:

$$A = k[X_1,\dots,X_r] \longleftarrow B = k[Y_1,\dots,Y_r] : \varphi^*$$

$$g_j \longleftarrow\!\shortmid\; Y_j$$

$$\big(h(g_1,\dots,g_s) \longleftarrow\!\shortmid\; h \big)$$

The fact that $\varphi(X) \subseteq Y$ amounts to the fact that $\varphi^*(I(Y)) \subseteq I(X)$.

(i.e. $h \in I(Y) \Rightarrow h(\underline{b}) = 0 \;\forall\, \underline{b} \in Y \Rightarrow (\varphi^* h)(\underline{a}) = h(g_1(\underline{a}),\dots,g_s(\underline{a})) = h(\varphi(\underline{a})) = 0 \;\forall\, \underline{a}$).

Set $A(X) := A/I(X)$ and $A(Y) := B/I(Y)$, and get:

$\varphi^* : A(Y) \longrightarrow A(X)$ a k-algebra homomorphism.

Conversely, given a ring homomorphism $\varphi^* : A(Y) \to A(X)$, can recover φ:

$X = \text{m-Spec}(A(X))$, $Y = \text{m-Spec}(A(Y))$.

do it as exercise!

$\underline{a} \in X \to M_{\underline{a}} \in \text{m-Spec}(A(X))$. Take $\varphi^{*-1}(M_{\underline{a}})$. It will be a maximal in $A(Y)$,

Can state it as a theorem:

$$\left\{ \begin{array}{c} \underline{\text{affine algebraic sets}} \\ \text{Algebraic sets } X \subseteq k^r \\ \text{morphisms as described} \end{array} \right\} \xleftrightarrow{\text{equiv. of categories}} \left\{ \begin{array}{c} \underline{\text{Affine } k\text{-algebras}} \\ k\text{-alg, finite type over } k, \\ \text{reduced (reduced} \Rightarrow \text{nil}(A) = 0) \end{array} \right\}$$

Dimension (Krull dimension):

$$\dim A := \sup\{ r \mid A \supsetneq P_0 \supsetneq \cdots \supsetneq P_r \},\ P_i \subseteq A \text{ prime.}$$

This can be stated as a property of the space Spec A, but it is not the most useful definition of dimension on Spec A

Def For P a prime **height** of P is $ht(P) := \sup\{r : P \supsetneq P_0 \supsetneq \cdots \supsetneq P_r\}$ P_j prime $= \dim A_P$.

Def The **coheight** is $\operatorname{coht} P := \sup\{ r : A \supsetneq P_0 \supsetneq \cdots \supsetneq P_r = P\} = \dim A/P$

Rk: $ht\, P + \operatorname{coht} P \leq \dim A$.

Examples:

- 0-dim domains are = fields.
- PID's are 1-dim or 0-dim.
- Artinian rings are 0-dim (all primes are maximal).
- $A = k[x_1, \dots, x_r]$, then $(x_1,\dots,x_r) \supsetneq (x_1,\dots,x_{r-1}) \supsetneq \cdots \supsetneq (x_1) \supsetneq 0 \Rightarrow \dim A \geq r$ — will prove equality.

Def: For an ideal I, $\underline{ht\, I} := \inf\{ ht\, P \mid P \supseteq I \}$. ($P$ prime).

Def If M is a module, $\dim M := \dim (A/\operatorname{ann} M)$.

Prop: Let A be a domain of finite-type over a field k.
Let $r := \operatorname{trdeg}_k A$ ($< \infty$) & $\operatorname{trdeg}_k A := \operatorname{trdeg}_k K(A)$.
Then $r = 0 \Leftrightarrow A$ is a field.

Pf
If $r=0$, $A = k[\alpha_1, \dots, \alpha_n]$.
Since $r=0$, α_1 is algebraic over k. So $k[\alpha_1]$ is a field. Then A has tr.deg $=0$ over $k[\alpha_1,\dots,\alpha_d]$, and by induction each $k[\alpha_1,\dots,\alpha_{d+1}]$ is a field $\Rightarrow A$ is a field.
If A is a field, Nullstellensatz implies that A is finite over k, so $\operatorname{trdeg}_k A = 0$. //

Theorem: If k is a field, A a domain of finite-type over k, then:

$$\dim A = \operatorname{trdeg}_k A.$$

(**Corollary:** $\dim k[X_1,\dots,X_r] = r$.)

Pf Let $r := \operatorname{trdeg}_k A$.

1) $r \geq \dim A$:

Claim: If A is a domain, $A \supseteq k$, and $P \neq 0$ is prime, then $\operatorname{trdeg}_k A > \operatorname{trdeg}_k A/P$

The claim proves (1): if $P_0 \supsetneq P_1 \supsetneq \cdots \supsetneq P_s = 0$, then $\operatorname{trdeg} A/P_0 < \operatorname{trdeg} A/P_1 < \cdots < \operatorname{trdeg} A/P_s$

So if P_0 is maximal, $\operatorname{trdeg}_k A/P_0 = 0$. $\Rightarrow$ $\operatorname{trdeg}_k A/P_s = \operatorname{trdeg}_k A \geq s$.

Pf of claim: Choose $\bar\alpha_1, \dots, \bar\alpha_r$ a transcendence basis of A/P (in A/P).

Lift the $\bar\alpha_i$ to $\alpha_i \in A$, and then:

$\alpha_1, \dots, \alpha_r$ are algebraically independent in $K(A)$.

$$\begin{tikzcd} A \arrow[r, two heads] & A/P \\ k[\alpha_1,\dots,\alpha_r] \arrow[u, hook] \arrow[ur, hook] & \end{tikzcd}$$

$k[\alpha_1,\dots,\alpha_r] =: R$ a polynomial ring

Let $S := R \setminus \{0\}$. Note that $S \cap P$ because of the right inclusion of the diagram.

So then, PA_S is a prime ideal in A_S, $PA_S \neq 0$ because A was a domain.

$$\operatorname{trdeg}_k A_S \left(= \operatorname{trdeg}_k K(A)\right) = \operatorname{trdeg}_{R_S} A_S + \underbrace{\operatorname{trdeg}_k R_S}_{r}$$

A_S is a domain with a nontrivial prime (so it's not a field).

Since A_S is finite-type over the field R_S but it's not itself a field,

$\operatorname{trdeg}_{R_S} A_S > 0$. So $\operatorname{trdeg}_k A > r = \operatorname{trdeg}_k A/P$. //

(continues proof).

(2) $\underline{r \leq \dim A}$

Proof by induction on r:

If $r=0$, ok.

Suppose $r>0$. Choose $\alpha \in A$, alg. indep/k. i.e $k[\alpha] \subseteq A$ is a polynomial ring.

Let $S := k[\alpha] \setminus \{0\}$. Let $K := k[\alpha]_S$. Then:

$\underset{(\mathrm{trdeg}_k A)}{\mathrm{trdeg}_k A_S} = \mathrm{trdeg}_K A_S + \mathrm{trdeg}_k K$. So $\mathrm{trdeg}_K A_S = r-1$.

By induction, $\dim A_S = r-1$, so $\exists$ a chain of primes:

$A_S \supsetneq Q_{r-1} \supsetneq \cdots \supsetneq Q_0 = 0$

Let $P_j := A \cap Q_j$ are all different. $P_j \cap S \neq \emptyset$ and $A \supsetneq P_{r-1} \supsetneq \cdots \supsetneq P_0 = 0$

Consider A/P_{r-1}. Since $k[\alpha] \cap P_{r-1} = 0$, have an inclusion

$\underset{\text{polynomial ring}}{k[\bar{\alpha}]} \hookrightarrow A/P_{r-1}$, ($\bar{\alpha}$ = image of α in A/P_{r-1}) we are using the Nullstellensatz here!

So $\mathrm{trdeg}_k A/P_{r-1} \geq 1 \Rightarrow A/P_{r-1}$ is <u>not</u> a field $\Rightarrow \exists P_r \supsetneq P_{r-1}$,

and there $\dim A \geq r$. //

- ## Associated primes & primary decomposition.

Idea: in $\mathbb{Z}$, $(n) = (p_1^{e_1}) \cap \cdots \cap \underline{(p_r^{e_r})}$ ← primary ideal associated to (p_r).

Let A be a ring, M a module over A.

Def: An <u>associated prime</u> of M is a prime ideal of A of the form $\mathrm{ann}(x)$ for some $x \in M$. (note that $\mathrm{ann}(x)$ is <u>not</u> prime, in general).

(note $\mathrm{ann}(x)$ is proper ideal $\Leftrightarrow x \neq 0$).

Def $\mathrm{Ass}(M) = \mathrm{Ass}_A(M) := \{$associated primes of $M\}$.

Define $A \longrightarrow M$, $a \longmapsto ax$. Then if $P = \mathrm{ann}(x)$, $A/p \hookrightarrow M$.

Thm: Every maximal element of $\mathcal{F} = \{\mathrm{ann}(x) \mid x \neq 0, x \in M\}$ is an (associated) prime.

If A is Noetherian, $\mathrm{Ass}_A(M) \neq \phi$, and $\bigcup_{P \in \mathrm{Ass}(M)} P = \{a \in A : \exists x \in M, x \neq 0 \text{ st } ax = 0\}$ "Zero-divisors of M".

Pf/ Let $\mathrm{ann}(x) \in \mathcal{F}$ be a maximal element. So $x \neq 0$.

Suppose $a, b \notin \mathrm{ann}(x)$. We have $bx \neq 0$ and $\mathrm{ann}(bx) \supseteq \mathrm{ann}(x)$.

By maximality, $\mathrm{ann}(bx) = \mathrm{ann}(x)$

Thus $a \notin \mathrm{ann}(bx)$. So $abx \neq 0 \Rightarrow ab \notin \mathrm{ann}(x) \Rightarrow \mathrm{ann}(x)$ is prime.

Since $\mathcal{F} \neq 0$, it must have maximal elements (because A is Noeth.), which are therefore associated primes of M.

$$\{\text{zero divisors of } M\} = \bigcup_{0 \neq x \in M} \mathrm{ann}(x) = \bigcup_{\mathrm{ann}(x) \in \mathcal{F}} \mathrm{ann}(x).$$

A Noetherian $\Rightarrow$ every $\mathrm{ann}(x) \in \mathcal{F}$ is contained in a maximal element, thus

$$\{\text{zero divisors of } M\} = \bigcup_{P \in \mathrm{Ass}(M)} P$$

Thm Let $S \subseteq A$ mult. closed set. Can view $\mathrm{Spec}(A_S)$ as a subset of $\mathrm{Spec}(A)$.

1) If N is an A_S-module, then

$$\mathrm{Ass}_{A_S}(N) = \mathrm{Ass}_A(N).$$

2) If M is an A-module, ~~and~~ A is Noetherian,

$$\mathrm{Ass}_{A_S}(M_S) = \mathrm{Ass}_A(M) \cap \mathrm{Spec}(A_S).$$

Pf/ (1) Let N be an A_S-module, consider $x \in N$, $x \neq 0$.

Have $\mathrm{ann}_A(x) = \mathrm{ann}_{A_S}(x) \cap A$ (contraction).

Thus, if $Q = \mathrm{ann}_{A_S}(x)$ is prime in A_S, then $Q \cap A = \mathrm{ann}_A(x)$ is prime in A, so $\mathrm{ann}_A(N) \supseteq \mathrm{ann}_{A_S}(N)$. But if $P = \mathrm{ann}_A(x)$ is prime, then $P \cap S = \phi$. $s \in S \Rightarrow \begin{array}{c} N \longrightarrow N \\ n \longmapsto sn \end{array}$ is iso.

(cont proof).
Can consider also

$\mathrm{ann}_{A_S}(x) \supseteq PA_S$. But there's equality: $\frac{a}{s}x=0 \Rightarrow s\cdot\frac{a}{s}x=0 \Rightarrow ax=0 \Rightarrow$

$\Rightarrow a\in \mathrm{Ann}_A(x)$. Thus $\frac{a}{s}\in PA_S$ and then get $\mathrm{ann}_{A_S}(x)=PA_S$.

So, $\mathrm{Ass}_A(N) \subseteq \mathrm{Ass}_{A_S}(N)$.

(2). Suppose $P\in \mathrm{Ass}_A(M)\cap \mathrm{Spec}(A_S)$.

So $P=\mathrm{ann}_A(x)$ for some $x\in M$. and also $P\cap S=\emptyset$.

Want to show $PA_S\in \mathrm{Ass}_{A_S}(M_S)$.

Claim: $\mathrm{ann}_{A_S}(\frac{x}{1})=PA_S$:

Pf/ if $\frac{a}{s}x=0$ in M_S, so $\exists t\in S$ s.t. $tax=0$, thus $ta\in \mathrm{ann}_A(x)=P$.

Since $t\notin P \Rightarrow a\in P$, so $\mathrm{ann}_{A_S}(\frac{x}{1})\subseteq PA_S$.

But as $P\subseteq \mathrm{Ann}_{A_S}(\frac{x}{1})$, must have $PA_S\subseteq \mathrm{Ann}_{A_S}(\frac{x}{1})$ //

Now suppose $Q=\mathrm{ann}_{A_S}(x)\in \mathrm{Ass}_{A_S}(M_S)$.

Can assume WLOG that $x\in M$ (by multiplying by some $s\in S$). Now, let

$P=Q\cap A$. Then $Q=PA_S$.

Write $P=(f_1,\dots,f_r)$ (since A is Noetherian).

Since $f_j x=0$ $\forall j$ (in M_S). There is $t_j\in S$ st. $t_j f_j x=0$ in M.

Set $x':=t_1t_2\dots t_r\cdot x(\in M)$, $\mathrm{ann}_M(x')\supseteq P$ clearly by construction.

But also $\mathrm{ann}_A(x')\subseteq \mathrm{ann}_{A_S}(\frac{x'}{1}) \underset{\uparrow}{=} \mathrm{ann}_{A_S}(\frac{x}{1})=Q$

since $x'=(t_1\cdots t_r)x$, unit in A_S

So $\mathrm{ann}_A(x')\subseteq Q\cap A=P$.

Therefore, $\mathrm{ann}_A(x')=P$, and then $\mathrm{Ass}_{A_S}(M_S)\subseteq \mathrm{Ass}_A(M)\cap \mathrm{Spec}(A_S)$ //

Corollary: if A is Noetherian, then

$$P \in \mathrm{Ass}_A(M) \iff PA_p \in \mathrm{Ass}_{A_p}(M_p)$$

Now, take a prime P, $\mathrm{Ass}_A(A/p) = \{P\}$.

Theorem: Let A be a ring.

$0 \to M' \to M \to M'' \to 0$ a short exact seq of A modules.

Then $\mathrm{Ass}_A(M') \subseteq \mathrm{Ass}_A(M) \subseteq \mathrm{Ass}_A(M') \cup \mathrm{Ass}_A(M'')$

Pf/ $\mathrm{Ass}_A(M') \subseteq \mathrm{Ass}_A(M)$:

If $x \in M'$, $\mathrm{ann}_{A,M'}(x) = \mathrm{ann}_{A,M}(x)$ since $M' \subseteq M$

$\mathrm{Ass}_A(M) \subseteq \mathrm{Ass}_A(M') \cup \mathrm{Ass}_A(M'')$:

Let $p = \mathrm{ann}_{A,M}(x) \in \mathrm{Ass}(M)$.

Can map

$$\begin{tikzcd} 0 \arrow[r] & M' \arrow[r] & M \arrow[r] & M'' \arrow[r] & 0 \\ & & A/p \arrow[u, hook] & a \arrow[u, mapsto, "ax"'] \end{tikzcd}$$

Let $N = A\cdot x \subseteq M$. N submodule $\cong A/p$.

If $\exists\, y \in N \cap M'$, $y \neq 0$: $\mathrm{ann}_{M'}(y) = \mathrm{ann}_M(y) = P$. So then $P \in \mathrm{Ass}(M')$.

If ~~NNM~~ $P \notin \mathrm{Ass}(M')$, then $N \cap M' = 0$, so

$$\begin{tikzcd} 0 \arrow[r] & M' \arrow[r] & M \arrow[r] & M'' \arrow[r] & 0 \\ 0 \arrow[r] & 0 \arrow[r] & N \arrow[r] & N \arrow[u, hook] \end{tikzcd}$$

The composite $N \to M''$ is embedding, then $P \in \mathrm{Ass}(M'')$. //

<u>Theorem</u>: If A is Noetherian and M is a finite A-module, then $\exists$

$$0 = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_r = M$$

s.t. $M_j/M_{j-1} \simeq A/p_j$ as A-modules, for some primes p_1 to p_r.

Pf/ Since A is Noetherian, $\mathrm{Ass}_A(M) \neq \emptyset$, so $\exists$ a submodule $M_1 \subseteq M$ s.t. $M_1 \simeq A/p_1$.

Consider M/M_1 and, by induction, find a submodule of M/M_{j-1} which is isomorphic to A/p_j for some p_j.

And let $M_j := \ker\left[M \to M/M_{j-1} \big/ (A/p_j)\right]$, so $M_j/M_{j-1} = A/p_j$.

It stops since M is Noetherian.

//

<u>Theorem</u>: if A is Noetherian, and M is a finite A-module, then:

1) $\mathrm{Ass}(M)$ is finite and nonempty.

2) $\mathrm{Ass}(M) \subseteq \mathrm{Supp}(M)$.

3) {the minimal elements of $\mathrm{Ass}(M)$} = {the minimal elements of $\mathrm{Supp}(M)$}.

(Since M is finite, remember that $\mathrm{Supp}(M) = V(\mathrm{ann}(M)) = \{P \supseteq \mathrm{ann}(M)\}$.)

Pf/ (1): non-empty is already proved. Also, $\mathrm{Ass}(M) \subseteq \bigcup \mathrm{Ass}(M_j/M_{j-1}) \overset{\text{prev. thm.}}{=} \{p_1, \dots, p_r\}$.

(2): clear.

(3) Only have to show that, if P is minimal in $\underset{V(\mathrm{ann}(M))}{\overset{\shortparallel}{\mathrm{Supp}}}(M)$, then $P \in \mathrm{Ass}(M)$.

Given such a P, $M_P \neq 0$.

$$\underset{\text{contains } PA_P}{\emptyset \neq} \mathrm{Ass}_{A_P}(M_P) = \mathrm{Ass}(M) \cap \mathrm{Spec}(A_P) \subseteq \mathrm{Supp}(M) \cap \mathrm{Spec}(A_P) \overset{\text{minimality}}{=} \{P\}$$

So $P \in \mathrm{Ass}(M)$.

//

Special case: $M = A$ Noetherian, then $\mathrm{Supp}_A(A) = \mathrm{Spec}(A)$. Then,

$$\mathrm{Ass}(A) \supseteq \{\text{minimal primes of } A\} \quad (\text{only finitely many}).$$

So $\mathrm{Spec}(A) = V(P_1) \cup \cdots \cup V(P_r)$ where $P_1, \dots, P_r$ are the minimal primes.

Each of the $V(P_i)$ is irreducible (i.e. it's not the union of two proper closeds)

The elements $P_{r+1}, \dots, P_s$ of $\mathrm{Ass}(A)$ which are not minimal are called <u>embedded</u> primes.

<u>Examples</u>

$A = k[X,Y]$, $I = (XY)$.

$$\mathrm{Ass}_A(A/I) \left(\simeq \mathrm{Ass}_{A/I}(A/I)\right)$$

$$P \longmapsto P/I$$

Consider $X \in A/I$.

$$\begin{array}{ccc} A\cdot X & \hookrightarrow & A/I \\ \| & & \| \\ M_1 & & M \\ \wr\| & & \\ A/(I:X) & & \end{array}$$

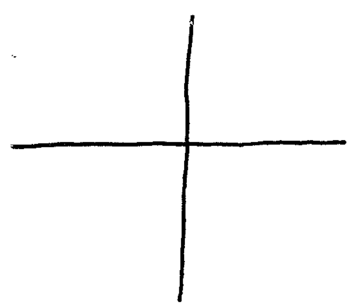
And $(I:X) = (Y)$, so there's one associated prime, $(Y) \in \mathrm{Ass}(A/I)$.

$$M/M_1 = A/(I+AX) \cong A/(X) \Rightarrow (X) \in \mathrm{Ass}(M/M_1).$$

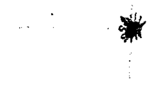
Know that $\mathrm{Ass}(A/I) \subseteq \mathrm{Ass}(M_1) \cup \mathrm{Ass}(M/M_1) = \{(X),(Y)\}$.

Since $(X) = \mathrm{ann}_{A/I}(Y)$, have $\mathrm{Ass}(A/I) = \{(X),(Y)\}$.

They're both minimal.



Example 2: $A = k[X,Y]$, $I = (X^2, XY, Y^2)$, $M = A/I$.



Claim: $\mathrm{Ass}(M) = \{(X,Y)\}$.

Pf

$$\underset{\displaystyle A/(X,Y)}{\overset{\shortparallel}{M_1 := A\cdot X}} \hookrightarrow M$$

Now, $M/M_1 = A/\left((X^2, XY, Y^2) + (X)\right) \cong A/(X, Y^2)$

$$\underset{\displaystyle A/(X,Y)}{\overset{\shortparallel}{M_2 := A\cdot Y}} \hookrightarrow M/M_1 \cong A/(X,Y^2)$$

$(M/M_1)/M_2 \cong A/(X,Y)$

$\Rightarrow$ (X,Y) is the only Associated prime.

Example 3: $A = k[X,Y]$, $I = (X^2, XY)$.

$M = A/I$

$$\underset{\displaystyle A/(X,Y)}{\overset{\shortparallel}{M_1 := A\cdot X}} \hookrightarrow M \quad ; \qquad M/M_1 = A/(X, X^2, XY) = A/(X)$$

So $\mathrm{Ass}(M) \subseteq \{(X,Y), (X)\}$. Need to check whether $(X) \in \mathrm{Ass}(M)$.

$\mathrm{Ann}_{A/I}(Y) = (I : Y) = (X)$

↑ if sth is not a multiple of X, it won't be a multiple after multiplying it by Y, so it won't be in I.

• Primary decomposition.

Def Let A be a ring, M a module, $N \subseteq M$ a submodule. N is <u>primary submodule</u> if, $\forall a \in A$, $\forall m \in M \setminus N$, if $am \in N \Rightarrow a^r M \subseteq N$ for some r.

(equiv, for all $a \in A$ which are zero-divisors of M/N, they are in $\sqrt{\mathrm{Ann}(M/N)}$).
We say also that M/N is, in this case, <u>coprimary</u>.

<u>Theorem</u>: If A is <u>Noetherian</u>, M a <u>finite</u> A-mod, then
$N \subseteq M$ is primary $\Leftrightarrow \mathrm{Ass}(M/N) = \{P\}$.
In this case, if $I := \mathrm{Ann}(M/N)$, then I is a primary ideal, and $\sqrt{I} = P$.

(I primary ideal means that I is a primary sub-A-module). (or that the quotient is P-coprimary.)

We say then that N is a P-primary submodule, in this case.

<u>Pf of th</u>:
$\Leftarrow$) Suppose $\mathrm{Ass}(M/N) = \{P\}$.
We have that P is the <u>unique</u> prime which is minimal amongst primes containing $I := \mathrm{Ann}(M/N)$.
We conclude that $\sqrt{I} = P$ (because of the previous sentence!).
Suppose $a \in A$ is a zero divisor for M/N. So $a \in \bigcup_{P' \in \mathrm{Ass}(M/N)} P' = P = \sqrt{I}$ //

$\Rightarrow$) Suppose M/N coprimary.
Consider any $P \in \mathrm{Ass}(M/N)$ (it is nonempty, we proved it before).
Then, any $a \in P$ is a zero-divisor for M/N, so $a \in \sqrt{\mathrm{Ann}(M/N)} = \sqrt{I}$
So $P \subseteq \sqrt{I}$.
Also $P \supseteq I$ (since $\mathrm{Ass} \subseteq \mathrm{Supp}$)
$\Rightarrow P = \sqrt{I}$ $\Rightarrow$ all such primes are the same!

//

<u>Claim</u>: I is primary ideal: given $a, b \in A$ s.t. $b \notin I$, $ab \in I$. Want that $a^n \in I$.
Since $I := \mathrm{Ann}(M/N)$, $a \cdot b(M/N) = 0$. But $b(M/N) \neq 0$. Therefore, a is a zero divisor for M/N. So $a \in \bigcup \mathrm{Ass} = P = \sqrt{I}$ //

Given $N \subseteq M$ a submodule,

<u>Def</u>: N is <u>reducible</u> if $N = N_1 \cap N_2$ for $N_1 \subseteq M$, $N_2 \subseteq M$ s.t. $N_i \neq N$.
Otherwise, say N is <u>irreducible</u>.

<u>Fact</u>: If N is Noetherian, then every submodule is a finite intersection of irreducibles.

Pf Let $N \subseteq M$ be maximal among submodules which are <u>not</u> finite intersections of irreducibles (use Noetherianness). Thus N is <u>not</u> irreducible, so $N = N_1 \cap N_2$
But since $N_i \supsetneq N \Rightarrow N_i$ have finite irreducible decomposition $\Rightarrow$!! //

<u>Def</u>. A <u>decomposition</u> of N is $N = N_1 \cap \cdots \cap N_r$, and say that
- it is <u>irredundant</u> if $N \neq N_1 \cap \cdots \cap \widehat{N_i} \cap \cdots \cap N_r$ for any $1 \le i \le r$.
- it is a <u>primary decomp.</u> if each N_i is primary.

<u>Thm</u>: if A noeth, M finite, then, if N_1, N_2 are P-primary,
$N_1 \cap N_2$ is P-primary.

Pf

$$M/_{N_1 \cap N_2} \hookrightarrow M/_{N_1} \oplus M/_{N_2}$$

So $\quad \mathrm{Ass}\left(M/_{N_1 \cap N_2}\right) \subseteq \mathrm{Ass}\left(M/_{N_1} \oplus M/_{N_2}\right) \subseteq \mathrm{Ass}\left(M/_{N_1}\right) \cup \mathrm{Ass}\left(M/_{N_2}\right) = \{P\}$

And as it is nonempty, $\mathrm{Ass}\left(M/_{N_1 \cap N_2}\right) = \{P\}$ //

So we have the notion of "shortest" primary decomposition, where if $P_i = \mathrm{Ass}(M/N_i)$, then $P_i \neq P_j$ for $i \neq j$.

<u>Thm</u>: if A is Noeth, M a finite A-mod, then:

1) The irreducible submodules are primary.

2) If $N = N_1 \cap \cdots \cap N_r$ is an irredundant primary decomposition of $N \subsetneq M$, then $\mathrm{Ass}(M/N) = \{P_1, .., P_r\}$ - where $\{P_i\} = \mathrm{Ass}(M/N_i)$.

3) Every $N \subsetneq M$ has a primary decomposition.
Furthermore, if $P \in \mathrm{Ass}(M/N)$ is <u>minimal</u>, then the P-primary component in any shortest primary decomposition of N is $\varphi_p^{-1}(N_p)$, where
$\varphi_p : M \to M_p$ is the localization map.
(i.e. uniqueness of minimal primes).

Pf (1) Show that if $N \subseteq M$ is <u>not</u> primary, then it is reducible:
Consider M/N. want to find $K_1, K_2 \subset M/N$ s.t. $K_1 \cap K_2 = \emptyset$, but $K_i \neq 0$.
Since N is not primary, have $P_1 \neq P_2 \in \mathrm{Ass}(M/N)$. So $\exists$ submodules $K_1, K_2 \in M/N$ with $K_i \simeq A/P_i$ $i=1,2$.
If $x \in K_1 \cap K_2$, $x \neq 0$, then $\mathrm{Ann}(x) = P_1 = P_2 \Rightarrow$!! So $K_1 \cap K_2 = 0_{/N}$

(2) Replace M with M/N, so $0 = N_1 \cap .. \cap N_r$ is irredundant prim. decomp, $\{P_i\} = \mathrm{Ass}(M/N)$.
Since $M \hookrightarrow M/N_1 \oplus \cdots \oplus M/N_r$ is an inclusion (ker is zero).
we have $\mathrm{Ass}(M) \subseteq \mathrm{Ass}(M/N_1 \oplus \cdots \oplus M/N_r) = \bigcup_{i=1}^{r} \mathrm{Ass}(M/N_i)$

• $\subseteq$] have seen because $\mathrm{Ass}(M) \subseteq \mathrm{Ass}(M') \cup \mathrm{Ass}(M'')$
• $\supseteq$] they are submodules of M, so ...

Need to show now that each P_i (say, P_1) is an Associated prime of M.
Since the decomp. is irredundant, $N_2 \cap .. \cap N_r \neq 0$. since $N_1 \cap (N_2 \cap .. \cap N_r) = 0$
Take $x \neq 0$, $x \in N_2 \cap .. \cap N_r$. So $\mathrm{ann}_M(x) = (N_1 : x)$
$(N_1 : M) = \mathrm{Ann}(M/N_1) = I$ is a primary ideal in A, with $\sqrt{I} = P_1$
We have $P_1^n M \subseteq N_1$ for some n. So $P_1^n \cdot x = 0$. Suppose we chose n s.t. $\begin{cases} P_1^n x = 0 \\ P_1^{n-1} x \neq 0 \end{cases}$

choose now $\overset{\neq 0}{y} \in P_1^{n-1}x$. So $\underline{\mathrm{Ann}(y) \supseteq P_1}$.

Also, $y \in N_2 \cap \cdots N_r$, and thus since $y \neq 0$, $y \notin N_1$

$\mathrm{ann}(y) = P_1$ & $P_1 \in \mathrm{Ass}(M)$

Since N_1 is P_1-primary, thus $\left[P_1 \supseteq \mathrm{Ann}_{M/N_1}(y) = (N_1 : y)_M = (0 : y)_M = \mathrm{ann}_M(y)\right.$ //

(B) That any $N \subseteq M$ has a primary decomp. is clear, by the previous discussion.

Let $N = N_1 \cap \cdots \cap N_r$ be a shortest primary decomposition.

Let N_i be associated to P_i.

Suppose that $P = P_1$ is a minimal element of $\mathrm{Ass}(M/N)$.

As localization is an exact functor, $N_P = (N_1)_P \cap \cdots \cap (N_r)_P \subseteq M_P$.

For $i > 1$, $P_i^{n_i} \subseteq \mathrm{Ann}(M/N_i)$ for some $n_i > 0$.

Since $P = P_1$ is minimal, $P_i \not\subseteq P$ for $i = 2, \ldots, r$,

the localization $(M/N_i)_P = M_P / N_{iP} = 0$ for $i = 2, \ldots, r$

So $M_P = (N_i)_P$ $\forall i = 2 \ldots r$, so $N_P = (N_1)_P \cap \cdots \cap (N_r)_P = (N_1)_P$

If $\varphi_P : M \to M_P$ is the localization hom., $\varphi_P^{-1}(N_P) = \varphi_P^{-1}((N_1)_P)$

To show that $\varphi_P^{-1}((N_1)_P) = N_1$, use: $\quad$ ($N_1 \subseteq \varphi^{-1}((N_1)_P)$ is clear)

if $m \in M$ s.t. $\varphi_P(m) \in (N_1)_P \Rightarrow \exists s \in A \setminus P$ s.t. $sm \in N_1$.

So either $m \in N_1$ or $m \notin N_1$, $sm \in N_1$.

Since N_1 is a primary submodule, $s^r m \in N_1$ for some r

Hence $s \in \sqrt{\mathrm{ann}(M/N_1)} = P_1 = P \Rightarrow\!\Leftarrow$!! Thus $m \in N_1$ //

Example:

Let $A = k[X,Y]$. $I = (X^2, XY)$

$P_1 = (X)$, $P_2 = (X,Y)$. (P_1 minimal, P_2 embedded).

$I = (X) \cap (X^2, XY, Y^2)$ is a primary decom (note $A/(X^2,XY,Y^2)$ is a P_2-coprimary).

Also, $I = (X) \cap (X^2, Y)$.

$A/(X^2,Y)$ is also P_2-coprimary. (So it is not unique).

• Flatness

Def: An A-mod M is flat (A-flat) if $M \otimes_A (-)$ preserves exact sequences of A-modules.

(equivalently, require only that $M \otimes_A -$ preserves injective homomorphisms).

If $f: A \to B$ is a ring-hom, say that B is flat over A if it is flat as an A-module.

Examples: • A_S is flat over A.

- Free modules are flat. ($F = \bigoplus_I A \Rightarrow F \otimes_A N = \bigoplus_I N$.)
- Projective modules are flat. (P is s.t. $F = P \oplus P'$ and use previous).
- $B = A[X_1, \dots, X_r]$ is flat over A: it is free as an A-module, monomial basis.
- $B = A[X]/(f(X))$ for f monic, is flat over A.

Thm: Let $f: A \to B$ a ring homomorphism, M a B-module. Then

M is flat over $A \iff$ for every maximal ideal $Q \subseteq B$, M_Q is A_p-flat ($p = Q \cap A$, Q^c).

(so if $f = id: A \to A$, then M is A-flat iff M_p is A_p-flat for every maximal ideal $p \subseteq A$).

Pf: If $S \subseteq A$ is a mult. closed set and M, N are A_S-modules, then $M \otimes_{A_S} N \cong M \otimes_A N$ (canonical isomorphism).

(because $M \otimes_A A_S = M_S = M$).

↓

(Pf of Local crit. for flatness).

$\Rightarrow$] Suppose M is A-flat, Let $Q \subseteq B$ be prime in B, $p = Q \cap A$.
Need to show that $M_Q \otimes_{A_p} (-)$ is an exact functor (on A_p-modules!).

~~$M_Q \otimes_{A_p} N = (M \otimes_B B_Q) \otimes_{A_p} N = (B_Q \otimes_B M) \otimes_{A_p} N$~~

$$M_Q \otimes_{A_p} N \simeq M_Q \otimes_A N = (B_Q \otimes_B M) \otimes_A N = B_Q \otimes_B (M \otimes_A N)$$

So the functor $M_Q \otimes_{A_p} (-)$ is the composite of two functors:

$$N \longrightarrow M \otimes_A N \text{, and } \longmapsto B_Q \otimes_B (M \otimes_A N).$$

So $M \otimes_A (-)$ is exact and B_Q is B-flat so $B_Q \otimes_B (-)$ is exact. //

$\Leftarrow$] Suppose M is a B-module, and that M_Q is A_p flat for all maximals Q.
Let ~~N where~~ $0 \to N \to N'$ be an exact sequence of A-modules.
Let $K = \ker [M \otimes_A N \longrightarrow M \otimes_A N']$. Want to show that $K = 0$.
The sequence $0 \to K \to M \otimes_A N \to M \otimes_A N'$ is an exact seq. of B-modules.
(because M is a B-module).

Localising at Q, $0 \to K_Q \to (M \otimes_A N)_Q \to (M \otimes_A N')_Q$ is exact.

$$(M \otimes_A N)_Q = B_Q \otimes_B (M \otimes_A N) = (B_Q \otimes_B M) \otimes_A N = M_Q \otimes_A N \simeq (M_Q \otimes_{A_p} A_p) \otimes_A N =$$

$$= M_Q \otimes_{A_p} (A_p \otimes_A N) = M_Q \otimes_{A_p} N_p \quad \text{so it } (M \otimes_A (-))_Q \simeq \underbrace{\underbrace{(-)_p}_{\text{exact functor}} \otimes_{A_p} M_Q}_{\text{exact functor}}.$$

So $K_Q = 0$ for all maximals, and this means $K = 0$. //

Prop: Let A be a ring.

1) Let M be a flat A-module. Let $N_1, N_2 \subseteq N$ A-modules. Then,
$$M\otimes_A(N_1\cap N_2) \simeq (M\otimes_A N_1)\cap(M\otimes_A N_2)$$
can think $M\otimes_A N_i \subseteq M\otimes_A N$ because M is flat.

2) If $A \to B$ is a flat ring-homomorphism, $I_1, I_2 \subseteq A$ ideals. Then,
$$(I_1\cap I_2)B = I_1B \cap I_2B.$$

3) If I_1 is <u>finitely-generated</u>, then $(I_2 : I_1)B = (I_2B : I_1B)$.

Pf 1) $0 \to N_1\cap N_2 \to N \xrightarrow{p} N/N_1 \oplus N/N_2$ is exact of A-mod.
Apply $M\otimes_A -$ and done.

2) If $I \subseteq A$ an ideal, then for any ring hom $f: A\to B$.

$$\begin{tikzcd} I\otimes_A B \arrow[r, two heads] \arrow[d] & IB \arrow[dl] \\ A\otimes_A B & \end{tikzcd}$$

surjection, in general

$A\otimes_A B \cong B$, $a\otimes b \mapsto ab$

If B is A-flat, the map $I\otimes_A B \twoheadrightarrow IB$ is an inclusion (thus iso), and thus Now (2) follows from (1).

3) If $I_1 = (x) \subseteq A$, then $0 \to (I_2 : x) \to A \xrightarrow{\cdot x} A/I_2$ is exact of A modules.
If B is A-flat $0 \to B\otimes_A(I_2:x) \to \underbrace{B\otimes_A A}_{\cong B} \xrightarrow{\cdot x} B\otimes_A A/I_2$

$B\otimes_A A/I_2 \cong B/B\otimes_A I_2 = B/I_2B$

So $B\otimes_A(I_2 : x) = (I_2B : x)_B = (I_2B : I_1B)_B$

Also, $B\otimes_A(I_2 : x) = (I_2 : x)_B B$. So if $I_1 = (x)$, $(I_2 : I_1)B = (I_2B : I_1B)_B$.

Now if $I_1 = (x_1, \dots, x_r)$, then
$(I_2 : I_1) = \bigcap_{i=1}^{r} (I_2 : x_i)$ and use the fact just proven for principals.

~~Def~~ A <u>directed set Λ</u> is a poset s.t $\forall \alpha,\beta \in \Lambda$, $\exists \gamma \in \Lambda$ s.t $\alpha \leq \gamma$, $\beta \leq \gamma$.

~~Def~~ A <u>directed system</u> is a collection $\{X_\lambda\}_{\lambda\in\Lambda}$ of sets, together with, for every pair $\alpha \leq \beta \in \Lambda$, a function $f_{\beta\alpha} : X_\alpha \to X_\beta$, such that $f_{\alpha\alpha} : X_\alpha \to X_\alpha$ is the identity and $f_{\gamma\beta} \circ f_{\beta\alpha} = f_{\gamma\alpha}$ $\forall\, \alpha \leq \beta \leq \gamma$.

<u>Example</u>: $\Lambda = \mathbb{N}$.

$$X_0 \xrightarrow{f_{10}} X_1 \xrightarrow{f_{21}} X_2 \xrightarrow{f_{32}} X_3 \to \cdots$$

<u>Def</u> The <u>direct limit</u> (or directed colimits) is:

Let $\varinjlim_\Lambda X_\lambda := \coprod_{\lambda\in\Lambda} X_\lambda \big/ \sim$ where $(a \in X_\alpha) \sim (b \in X_\beta)$ iff $\exists c \in X_\gamma$, $\alpha,\beta \leq \gamma$ and $f_{\gamma\alpha}(a) = c = f_{\gamma\beta}(b)$.

Exercise: check that $\sim$ is an equivalence relation.

~~Prop~~ Let $\underline{i_\alpha} : X_\alpha \to \varinjlim_\Lambda X_\lambda$ be the obvious map $(i_\alpha(a) := [a \in X_\alpha])$.

~~Claim~~ Def A <u>cone</u> on the directed system $\{X_\lambda\}_{\lambda\in\Lambda}$ is a ~~set~~ Y and functions $g_\lambda : X_\lambda \to Y$ $\forall \lambda \in \Lambda$, s.t. $g_\beta \circ f_{\beta\alpha} = g_\alpha$ $\forall \alpha \leq \beta \in \Lambda$.

$$\begin{tikzcd} X_\alpha \arrow[r, "f_{\beta\alpha}"] \arrow[dr, "g_\alpha"'] & X_\beta \arrow[d, "g_\beta"] \\ & Y \arrow[u, phantom, "\circlearrowleft" near start, shift right=3] \end{tikzcd}$$

<u>Prop</u>: There is a bijective correspondence:

$$\{\text{functions on } \varinjlim_\Lambda X_\lambda \to Y\} \longleftrightarrow \{\text{cones on } \{X_\lambda\}_\Lambda \text{ to } Y\}$$

$$g \longmapsto (g_\alpha := g \circ i_\alpha)$$

<u>Rk</u>: (i_λ) are a cone to $\varinjlim X_\lambda$ and is the <u>initial cone</u> to the directed system.

<u>Rk</u>: Require that the directed sets Λ are <u>nonempty</u>!

$$\begin{tikzcd}
X_\alpha \arrow[d, "f_{\beta\alpha}"'] \arrow[dr, "i_\alpha"] \arrow[drr, bend left, "g_\alpha"] & & \\
 & \varinjlim X \arrow[r, dashed, "\exists! h"] & Y \\
X_\beta \arrow[ur, "i_\beta"'] \arrow[urr, bend right, "g_\beta"'] & &
\end{tikzcd}$$

~~Defn~~

Prop: If $\{X_\lambda, f_{\alpha\beta}\}_\Lambda$ is a <u>constant</u> directed system (i.e. $\exists S$ s.t. $X_\lambda = S$, $f_{\alpha\beta} = \mathrm{id}_S$)

(1) then $\varinjlim_\Lambda S \cong S$.

(2) If $\{X, f\}_\Lambda$, $\{Y, g\}_\Lambda$ are directed systems, then can define $\{X \times Y, f \times g\}$ is a directed system, and $\varinjlim X_\lambda \times Y_\lambda \cong (\varinjlim X_\lambda) \times (\varinjlim Y_\lambda)$

Defn → (3) A map $\varphi : \{X, f\}_\Lambda \to \{Y, g\}_\Lambda$ of Λ-directed systems is a collection of functions $\varphi_\lambda : X_\lambda \to Y_\lambda$ s.t. $\forall \alpha \leq \beta \in \Lambda$,

$$\begin{tikzcd}
X_\alpha \arrow[r, "f_{\beta\alpha}"] \arrow[d, "\varphi_\alpha"'] & X_\beta \arrow[d, "\varphi_\beta"] \\
Y_\alpha \arrow[r, "g_{\beta\alpha}"'] & Y_\beta
\end{tikzcd}$$

Defn: If $u, v : X \to Y$ are two functions of sets, the <u>equalizer</u> or <u>kernel</u> of the pair (u, v) is $\ker(u, v) := \{x \in X : u(x) = v(x)\}$. (the "good kernels" are $\ker(u, 0)$.)

If $\varphi, \psi : \{X, f\}_\Lambda \to \{Y, g\}_\Lambda$ are maps of Λ-directed systems, let $K_\lambda := \ker(\varphi_\lambda, \psi_\lambda)$. Then (K_λ, h) is a directed system, where $h_{\beta\alpha} : K_\alpha \to K_\beta$ are $h_{\beta\alpha} = f_{\beta\alpha}|_{K_\alpha}$.

And $\varinjlim_\Lambda K_\lambda \cong \ker\left[\varinjlim_\Lambda X_\lambda \overset{\varinjlim \varphi}{\underset{\varinjlim \psi}{\rightrightarrows}} \varinjlim_\Lambda Y_\lambda \right]$

Proof: Exercise!

An <u>abelian group</u> is $\left(A \text{ a set}, \mu : A \times A \to A,\ i : A \to A,\ z : \overset{\{0\}}{*} \to A\right)$ s.t. the following diagrams commute:

$$\begin{tikzcd} * \times A \arrow[r, "z \times id"] \arrow[dr, bend right, "pr_2"'] & A \times A \arrow[d, "\mu"] & A \times * \arrow[l, "id \times z"'] \arrow[dl, "pr_1"] \\ & A & \end{tikzcd}$$

identity →

$$\begin{tikzcd} A \arrow[r, "(id, i)"] \arrow[d, "pr"'] \arrow[dr, phantom, "\#"] & A \times A \arrow[d, "\mu"] \\ * \arrow[r, "z"] & A \end{tikzcd}$$

instead of ← inverse

$$\begin{tikzcd} A \times A \times A \arrow[r, "\mu \times id"] \arrow[d, "id \times \mu"'] \arrow[dr, phantom, "\#"] & A \times A \arrow[d, "\mu"] \\ A \times A \arrow[r, "\mu"'] & A \end{tikzcd}$$

(associativity)

$$\begin{tikzcd} A \times A \arrow[rr, "\tau"] \arrow[dr, "\mu"'] & \# & A \times A \arrow[dl, "\mu"] \\ & A & \end{tikzcd}$$

$\tau : (x, y) \longmapsto (y, x)$

(commutativity)

<u>Def</u> A <u>directed system of Abelian Groups</u> $\{A_\lambda, f_{\alpha\beta}\}_\Lambda$ is a directed system of sets, s.t. each A_λ has an ab.gp structure and each $f_{\alpha\beta}$ is a group homomorphism.

$$\begin{tikzcd} A \times A \arrow[r, "f \times f"] \arrow[d, "\mu_A"'] & B \times B \arrow[d, "\mu_B"] \\ A \arrow[r, "f"] & B \end{tikzcd}$$

<u>Prop</u>: If $\{A_\lambda, f_{\alpha\beta}\}$ is a directed system of AbGp, then $\varinjlim_\Lambda A_\lambda$ is an abelian group, $i_\lambda : A_\lambda \to \varinjlim A_\lambda$ are group homomorphisms, and these are the universal cone on $\{A_\lambda\}$ in the category of AbGp. (i.e. if B ab gp, $\cancel{\exists!}\ g_\lambda : A_\lambda \to B$ gp hom s.t. $g_\beta \circ f_{\beta\alpha} = g_\alpha$ $\forall \alpha \leq \beta \in \Lambda$) $\exists!$ s.t.

$$\begin{tikzcd} \varinjlim_\Lambda A_\lambda \arrow[r, "g"] & B \\ A_\lambda \arrow[u, "i_\lambda"] \arrow[ur, "g_\lambda"'] \arrow[ur, phantom, "\#"] & \end{tikzcd} \quad (\forall \lambda).$$

Pf <u>Exercise!</u>

Def An R-module is an abelian group M with $\psi : R \times M \to M$ making some diagrams commute.

Prop: Same result as prev. prop. holds if we replace AbGp with $_R$Mod, and "gphom" with "$_R$Mod-hom".

Prop: Let $\{M'_\lambda\}_\Lambda \xrightarrow{u} \{M_\lambda\}_\Lambda \xrightarrow{v} \{M''_\lambda\}_\Lambda$ be an exact sequence of directed systems of R-modules (i.e. $\forall \lambda$, $M'_\lambda \xrightarrow{u_\lambda} M_\lambda \xrightarrow{v_\lambda} M''$ is exact).
Then, $\varinjlim_\Lambda M'_\lambda \xrightarrow{\bar{u}} \varinjlim_\Lambda M_\lambda \xrightarrow{\bar{v}} \varinjlim_\Lambda M''_\lambda$ is exact.

Pf Given $y \in \varinjlim M_\lambda$ s.t $\bar{v}(y) = 0$, want $x \in \varinjlim M'_\lambda$ s.t $\bar{u}(x) = y$.
We have $y = [b \in M_\beta]$ for some $\beta \in \Lambda$.
So $\bar{v}(y) = [v_\beta(b) \in M''_\beta] = 0 = [0 \in M''_\beta] \Rightarrow \exists\, \gamma \geq \beta$ s.t $f''_{\gamma\beta}(v_\beta(b)) = f''_{\gamma\beta}(0) = 0$
$\Rightarrow f''_{\gamma\beta}(v_\beta(b)) = v_\gamma(f_{\gamma\beta}(b)) = 0$
Since $y = [b \in M_\beta] = [f_{\gamma\beta}(b) \in M_\gamma]$.
Notice that $f_{\gamma\beta}(b) \in \ker v$: $\exists\, a \in M'_\gamma$ s.t $\bar{u}(a) = f_{\gamma\beta}(b)$.
Let $x := [a \in M'_\gamma]$ then $\bar{u}(x) = y$. //

Thm: Let A be a commutative ring. Let $\{M_\lambda\}_\Lambda$ be a directed system of A-modules, and let N be an A-module. Then,
$$\varinjlim_\Lambda (M_\lambda \otimes_A N) \simeq \left(\varinjlim_\Lambda M_\lambda\right) \otimes_A N$$

Proof: Consider $g_\lambda = i_\lambda \otimes id : M_\lambda \otimes_A N \to (\varinjlim_\Lambda M_\lambda) \otimes N$.
By univ. property, this gives a map $g : \varinjlim_\Lambda (M_\lambda \otimes_A N) \to (\varinjlim_\Lambda M_\lambda) \otimes N$

HOMOLOGICAL ALGEBRA

CHARLES REZK

1. Introduction

This is a brief exposition of the basic ideas of homological algebra, for the most part without proofs (which can be easily supplied by the reader, or looked up in a standard reference, such as Weibel's *An Introduction to Homological Algebra*). It is geared towards defining Tor groups.

We write Mod_A for the category of right A-modules.

2. Chain complexes

Let $\mathbf{A} = \mathrm{Mod}_A$.

A **chain complex** C in $\mathbf{A}$ is a sequence C_n, $n \geq 0$ of objects of $\mathbf{A}$ (by convention $C_n = 0$ for $n < 0$), together with maps $d_n \colon C_n \to C_{n-1}$ for each n, such that $d_{n-1}d_n = 0$. For the most part, we suppress the lower indexing on maps, and will just write d for d_n, so the condition becomes $d^2 = 0$.

A **chain map** $f \colon C \to D$ of chain complexes is a sequence of homomorphisms $f = f_n \colon C_n \to D_n$ for each n such that $df = fd$. Chain complexes in $\mathbf{A}$ form a category, denoted $\mathrm{Ch}_{\mathbf{A}}$. A **chain homotopy** between chain maps $f, g \colon C \to D$ is a sequence of maps $s = s_n \colon C_n \to D_{n+1}$ such that $ds + sd = f - g$.

The n**th homology group** H_nC of a chain complex C is the quotient

$$H_nC \stackrel{\text{def}}{=} (\ker d \colon C_n \to C_{n-1})/(\operatorname{im} d \colon C_{n+1} \to C_n).$$

Proposition 2.1. *H_n is a functor from $\mathrm{Ch}_{\mathbf{A}}$ to $\mathbf{A}$. Furthermore, if $f, g \colon C \to D$ are chain homotopic, then $H_nf = H_ng$ as homomorphisms $H_nC \to H_nD$.*

We say that a sequence $C \to D \to E$ of chain maps is **exact** if each sequence $C_n \to D_n \to E_n$ is exact.

If $0 \to C \xrightarrow{f} D \xrightarrow{g} E \to 0$ is a short exact sequence of chain complexes, the **connecting map** $\delta \colon H_nE \to H_{n-1}C$ is defined and characterized by the following property: $\delta([z]) = [x]$ for $z \in \ker(E_n \to E_{n-1})$, $x \in \ker(C_{n-1} \to C_{n-2})$ if and only if there exists $y \in D_n$ such that $z = g(y)$ and $f(x) = d(y)$.

Proposition 2.2. *If $0 \to C \xrightarrow{f} D \xrightarrow{g} E \to 0$ is a short exact sequence of chain complexes, there is an exact sequence*

$$\cdots \to H_nC \to H_nD \to H_nE \to H_{n-1}C \to H_{n-1}D \to \cdots \to H_0D \to H_0E \to 0,$$

where the maps in the sequence are H_nf, H_ng, and δ.

Date: September 21, 2005.

This proposition, and the definition of the connecting map, basically amount to the snake lemma.

3. Projective resolutions

A **resolution** of a module $M \in \mathbf{A}$ consists of a chain complex C in $\mathbf{A}$, together with a homomorphism $\epsilon_C\colon H_0C \to M$, such that ϵ_C is an isomorphism, and $H_nC \approx 0$ for $n > 0$. (One often expresses this by saying that the sequence

$$\cdots C_3 \to C_2 \to C_1 \to C_0 \to M \to 0$$

is exact.)

If $f\colon M \to N$ is a map of modules, and (C, ϵ_C) and (D, ϵ_D) are resolutions of M and N respectively, we say that a chain map $g\colon C \to D$ **covers** f if $(\epsilon_D)(H_0g) = f\epsilon_C$ as maps $H_0C \to N$.

A module P is **projective** if it is a summand of a free module. Equivalently, P is projective if it has the **left lifting property** with respect to surjections; that is, for every surjection $q\colon M \to N$ and every map $g\colon P \to N$, there is a map $f\colon P \to M$ such that $qf = g$.

A **projective resolution** is a resolution C of M such that each C_n is a projective module. Likewise, a **free resolution** is one in which each C_n is a free module.

free module

$$\begin{tikzcd} \cdots \arrow[r] & C_1 \arrow[rr] \arrow[dr] & & C_0 \arrow[r] & M \arrow[r] & 0 \\ & 0 \arrow[r] & \operatorname{Ker} d_0 \arrow[ur] \arrow[r] & 0 \end{tikzcd}$$

Proposition 3.1. *Let M be a module.*

(a) *There exists a free resolution, and hence a projective resolution, of M.*

(b) *Let C be a* projective *resolution of M, let D be a resolution of N, and let $f\colon M \to N$ be a map of modules. Then there exists a chain map $g\colon C \to D$ covering f.*

(c) *Let C be a* projective *resolution of M, let D be a resolution of N, let $g, h\colon C \to D$ be two chain maps which both cover the map $f\colon M \to N$. Then g and h are chain homotopic.*

In particular, for every two projective resolutions C and D of a module M, there exists a chain map $f\colon C \to D$ covering the identity map of M, and any two such chain maps are chain homotopic.

4. Left derived functors

Let $\mathbf{B} = \mathrm{Mod}_B$ be another category of modules.

An **additive functor** $T\colon \mathbf{A} \to \mathbf{B}$ is a functor such that $T(f+g) = Tf + Tg$ for any $f, g\colon M \to N$ in $\mathbf{A}$. Additive functors carry chain complexes to chain complexes, chain maps to chain maps, and chain homotopies to chain homotopies.

Given an additive functor T, we define the n**th left derived functors** L_nT, for $n \geq 0$, as follows. For each module M, choose a fixed projective resolution (C, ϵ_C) of M. Set

$$L_nT(M) \stackrel{\text{def}}{=} H_nT(C).$$

Proposition 4.1. *Let T be an additive functor.*

(a) *The expression $L_nT(M)$ is well-defined, in that it does not depend on the choice of resolution C, up to unique isomorphism. That is, if (D, ϵ_D) is another projective resolution of M, then there is a canonical isomorphism $L_nT(M) = H_nT(C) \to$*

$H_nT(D)$, defined to be the unique map obtained from any chain map $C \to D$ covering the identity of M.

(b) *L_nT defines a functor $\mathbf{A} \to \mathbf{B}$.*

5. Properties of left derived functors

The following is a "relative" version of the existence of projective resolutions. The non-relative version corresponds to the special case of $M = 0$ and $C = 0$.

Proposition 5.1. *Let $f\colon M \to N$ be a map of modules, and let (C, ϵ_C) be a resolution of M. Then there exists a resolution (D, ϵ_D) of N, together with a chain map $g\colon C \to D$ covering f, such that the groups of the complex D have the form $D_n \approx C_n \oplus P_n$, the map $g_n\colon C_n \to D_n$ is the inclusion of the first summand, and P_n is projective.*

Proposition 5.2. *Let $0 \to M' \to M \to M'' \to 0$ be a short exact sequence of modules. Then this sequence is covered by a short exact sequence $0 \to C' \to C \to C'' \to 0$ of projective resolutions.*

Proposition 5.3. *Let $T\colon \mathbf{A} \to \mathbf{B}$ be an additive functor, and let $0 \to M' \to M \to M'' \to 0$ be a short exact sequence in $\mathbf{A}$. Then there is an exact sequence*

$$\cdots \to L_nT(M') \to L_nT(M) \to L_nT(M'') \to L_{n-1}T(M') \to \cdots \to L_0(M'') \to 0.$$

An additive functor T is **right exact** if $M' \to M \to M'' \to 0$ exact implies $TM' \to TM \to TM'' \to 0$ is exact. An additive functor T is **exact** if it is right exact and if it preserves injections; equivalently, T is exact if it takes exact sequences to exact sequences.

Proposition 5.4. *Let $T\colon \mathbf{A} \to \mathbf{B}$ be an additive functor.*

(a) *The 0th derived functor $L_0T\colon \mathbf{A} \to \mathbf{B}$ is right exact.*
(b) *There is a natural transformation of functors $\eta\colon L_0T \to T$. If P is a projective module, then $\eta_P\colon L_0T(P) \to T(P)$ is an isomorphism.*
(c) *The functor T is right exact if and only if η is an isomorphism on all objects.*

Proposition 5.5. *Let $T\colon \mathbf{A} \to \mathbf{B}$ be a right exact additive functor. The following are equivalent.*

(a) *T is an exact functor.*
(b) *$L_nT \equiv 0$ for all $n > 0$.*
(c) *$L_1T \equiv 0$.*

A module M is called **T-acyclic** if $L_nT(M) = 0$ for all $n > 0$. A **T-acyclic resolution** of M is a resolution C such that every C_n is T-acyclic.

Proposition 5.6. *If (C, ϵ_C) is a T-acyclic resolution of M, then $H_nT(C) \approx L_nT(M)$ for all n.*

Proof. Let $K_n = \operatorname{im}(d\colon C_n \to C_{n-1})$ with $K_0 = M$, and consider the long exact sequence of derived functors associated to the short exact sequences $0 \to K_{n+1} \to C_n \to K_n \to 0$. □

6. Tor

Fix a left A-module N, and let $T_N\colon \mathbf{A} \to \mathbf{B}$ be the functor defined by $T(M) \stackrel{\text{def}}{=} M \otimes_A N$. (If A is a commutative ring, we can take $B = A$; however, if A is not commutative, we can only take B to be the center of A.) The functor T_N is right exact.

We define the Tor groups to be the left derived functors of T_N. That is, we set

$$\mathrm{Tor}^A_n(M, N) \stackrel{\text{def}}{=} L_n T_N(M).$$

Proposition 6.1. *We have*

(a) $\mathrm{Tor}^0_A(M, N) \approx M \otimes_A N$.

(b) *N is flat as a left A-module,* iff $\mathrm{Tor}^n_A(M, N) = 0$ *for all right modules M and all $n > 0$,* iff $\mathrm{Tor}^1_A(M, N) = 0$ *for all right modules M.*

(c) *If $0 \to M' \to M \to M'' \to 0$ is a short exact sequence of right modules, there is a long exact sequence*

$$\cdots \to \mathrm{Tor}^n_A(M', N) \to \mathrm{Tor}^n_A(M, N) \to \mathrm{Tor}^n_A(M'', N) \to \mathrm{Tor}^{n-1}_A(M', N) \to \cdots$$

ending in

$$\cdots \to \mathrm{Tor}^1_A(M'', N) \to M' \otimes_A N \to M \otimes_A N \to M'' \otimes_A N \to 0.$$

(d) *If (C, ϵ_C) is a resolution of M by flat right A-modules, then we have* $\mathrm{Tor}^n_A(M, N) \approx H_n(C \otimes_A N)$.

7. Balancing Tor

Let $\mathbf{A}'$ denote the category of *left* A-modules.

Fix a right A-module M, and let $U_M\colon \mathbf{A}\text{'} \to \mathbf{B}$ be the functor defined by $U_M(N) \stackrel{\text{def}}{=} M \otimes_A N$. The functor U_M is right exact.

We define the Tor' groups to be the left derived functors of U_M. That is, we set

$$\mathrm{Tor}'^A_n(M, N) \stackrel{\text{def}}{=} L_n U_M(N).$$

A **double complex** K is a collection of modules $K_{p,q}$ for $p, q \geq 0$, together with maps $d'\colon K_{p,q} \to K_{p-1,q}$ and $d''\colon K_{p,q} \to K_{p,q-1}$ such that $d'^2 = 0$, $d''^2 = 0$, and $d'd'' = d''d'$.

Let K be a double complex. For each p, we obtain a chain complex $K_{p,\bullet}$ whose groups are $K_{p,q}$ (with fixed p) and differentials are the d''. Likewise, for each q, we obtain a chain complex $K_{\bullet,q}$ whose groups are $K_{p,q}$ (with fixed q) and differentials are the d'.

The **total complex** of a double complex K is the complex ΔK defined by

$$(\Delta K)_n \stackrel{\text{def}}{=} \bigoplus_{p+q=n} K_{p,q}, \qquad dx = d'x + (-1)^p d''x \quad \text{if } x \in K_{p,q}.$$

Proposition 7.1. *Let K be a double complex.*

(a) *Let C be the chain complex defined by $C_p = H_0(K_{p,\bullet})$, with chain map induced by d'; there is an evident map of complexes $\Delta K \to C$. If for each $p \geq 0$ we have $H_q(K_{p,\bullet}) = 0$ for all $q > 0$, then this map of complexes induces an isomorphism $H_n(\Delta K) \to H_n(C)$ for all n.*

(b) *Let D be the chain complex defined by $D_q = H_0(K_{\bullet,q})$, with chain map induced by d''; there is an evident map of complexes $\Delta K \to D$. If for each $q > 0$ we have $H_p(K_{\bullet,q}) = 0$ for all $p > 0$, then this map of complexes induces an isomorphism $H_n(\Delta K) \to H_n(D)$ for all n.*

Proof. Let L be the double complex with $L_{p,q} = K_{p,q}$ for $q > 0$, $L_{p,0} = \mathrm{im}(d''\colon K_{p,1} \to K_{p,0})$. Then there is a short exact sequence $0 \to \Delta L \to \Delta K \to C \to 0$ of chain complexes, and thus we have reduced to a special case: if $H_q(K_{p,\bullet}) = 0$ for all p and q, then $H_n \Delta K = 0$ for all n. □

Proposition 7.2. *Let M be a left A-module, and C a projective resolution of M by left modules. Let N be a right A-module, and D a projective resolution by right modules. Let K be the double complex defined by $K_{p,q} \stackrel{\text{def}}{=} C_p \otimes_A D_q$. Then*

$$\mathrm{Tor}'^A_n(M, N) \approx H_n(\Delta K) \approx \mathrm{Tor}^A_n(M, N).$$

Department of Mathematics, University of Illinois at Urbana-Champaign, Urbana, IL
E-mail address: `rezk@math.uiuc.edu`

(cont. proof).

Recall that if K & L, P are A-modules, an A-bilinear map $K \times L \xrightarrow{\varphi} P$ is a function s.t. $\varphi(x_1+x_2, y) = \varphi(x_1,y) + \varphi(x_2,y)$ and $\varphi(ax,y) = \varphi(x,ay)\ \forall a \in A$.

$$\varphi(x, y_1+y_2) = \varphi(x,y_1) + \varphi(x,y_2)$$

We have a function $r : K \times L \to K \otimes_A L$, $(x,y) \mapsto (x \otimes y)$ is bilinear and,

given any $\varphi : K \times L \to P$, φ bilinear, $\exists!\ h$ homomorphism $h : K \otimes_A L \to P$ making the following diagram commute:

$$\begin{tikzcd} K \times L \arrow[r, "\varphi"] \arrow[d, "r"'] \arrow[dr, phantom, "\#"] & P \\ K \otimes_A L \arrow[ur, "h"'] & \end{tikzcd}$$

So to get a ~~map~~ $\left(\varinjlim_\Lambda M_\lambda\right) \otimes N \to \varinjlim_\Lambda (M_\lambda \otimes_A N)$, we define first a bilinear map from $\varinjlim_\Lambda M_\lambda \times N$:

Given $n \in N$, let $\varphi_n : \varinjlim_\Lambda M_\lambda \to \varinjlim (M_\lambda \otimes_A N)$ s.t. $\underset{M_\lambda}{x} \mapsto \underset{M_\lambda \otimes_A N}{x \otimes n}$

This is a A-mod homomorphism.

Define $\varphi : \left(\varinjlim_\Lambda M_\lambda\right) \times N \to \varinjlim (M_\lambda \otimes_A N)$

$$(x, n) \longmapsto \varphi_n(x)$$

it is certainly left-linear. Can show that φ is A-bilinear.

Therefore, $\exists\ h : \varinjlim M_\lambda \otimes_A N \to \varinjlim (M_\lambda \otimes N)$ a homomorphism, by the universal property of tensor product.

Need to check that $h \circ g = id$, $g \circ h = id$ (exercise!)

Prop: If $\{M_\lambda\}_\Lambda$ is a directed system of flat A-modules, then $\varinjlim_\Lambda M_\lambda$ is also flat over A.

Pf If $N' \to N \to N''$ is exact,

$$(\varinjlim_\Lambda M_\lambda) \otimes N' \longrightarrow (\varinjlim_\Lambda M_\lambda) \otimes N \longrightarrow (\varinjlim_\Lambda M_\lambda) \otimes N''$$

$$(\varinjlim_\Lambda M_\lambda) \otimes N = \varinjlim (M_\lambda \otimes N)$$

use previous theorems //

There is a collection of functors $\mathrm{Tor}_A^q(-,-)$ s.that:

- $\mathrm{Tor}_A^0(M,N) \simeq M \otimes_A N$
- $\mathrm{Tor}_A^q(M,N)$ is bilinear in M & N.
- If $0 \to N' \to N \to N'' \to 0$ is a s.e.s. of A-modules, then there is a long exact sequence of A-modules:

$$\cdots \to \mathrm{Tor}_A^q(M,N') \to \mathrm{Tor}_A^q(M,N) \to \mathrm{Tor}_A^q(M,N'') \to$$
$$\to \mathrm{Tor}_A^{q-1}(M,N') \to \mathrm{Tor}_A^{q-1}(M,N) \to \mathrm{Tor}_A^{q-1}(M,N'') \to$$
$$\cdots \to \mathrm{Tor}_A^0(M,N') \to \mathrm{Tor}_A^0(M,N) \to \mathrm{Tor}_A^0(M,N'') \to 0$$

$$\mathrm{Tor}_A^0(M,N) = M \otimes_A N$$

- Tor is balanced: $\mathrm{Tor}_A^q(M,N) \simeq \mathrm{Tor}_A^q(N,M)$ if A is a commutative ring.

Example: Let $M = A/xA$, where x is a non-zero divisor of A.

A projective resolution for M is $\cdots 0 \to 0 \to 0 \to A \xrightarrow{1 \mapsto x} A \to M$

$$A \to xA \to 0, \quad 0 \to xA \to A$$

$$N \otimes_A \begin{pmatrix} 0 \\ \downarrow \\ A \\ \downarrow \\ A \\ \downarrow \\ 0 \end{pmatrix} = TC = \begin{pmatrix} 0 \\ \downarrow \\ N \\ \downarrow \cdot x \\ N \end{pmatrix} \Rightarrow \mathrm{Tor}_0^A(N,M) = H_0 TC = N/xN \; (\simeq N \otimes A/xA)$$

$$\mathrm{Tor}_1^A(N,M) = H_1 TC = \ker[N \xrightarrow{x} N]$$ and $\mathrm{Tor}_q^A(N,M) = 0 \;\; \forall q \geq 2$.

If M is an A-module, $I \subseteq A$ an ideal.

We have a map:

$$I \otimes_A M \twoheadrightarrow IM \subseteq M$$
$$x \otimes m \longmapsto xm$$

It is a surjection, in general.

Claim: if M is flat, then this is a bijection:

Pf/ $(I \hookrightarrow A) \otimes_A M = I \otimes_A M \hookrightarrow A \otimes_A M \simeq M$ //

Thm: Let A be a ring, M an A-module. Then,

M is A-flat iff for every fin-gen ideal $I \subseteq A$, $I \otimes_A M \hookrightarrow A \otimes_A M$ is injective.

Pf/ $\Rightarrow$/ done in the claim.

$\Leftarrow$/ First - show that the condition implies it holds for any I (not necessarily fin gen).

Let $I \subseteq A$ be any ideal.

Let $\Lambda :=$ set of fin-gen ideals $\subseteq I$.

Λ is a directed set: $\Lambda \neq \emptyset$ $(0 \in \Lambda)$, $J_1, J_2 \in \Lambda \Rightarrow J_1 + J_2 \in \Lambda$.

Take now $\varinjlim_{J \in \Lambda} J \cong I$ (check it, it is easy).

Consider the exact sequence of directed systems (constant 0 and A).

$0 \to J \to A$ ~~$\Rightarrow$ get $0 \to I \to A$ exact sequence~~

Get a directed Λ-system:

$\underset{\substack{\shortparallel \\ 0}}{0 \otimes_A M} \to J \otimes_A M \to A \otimes_A M$ is exact since J is f-gen.

& taking the directed limit, $0 \to \varinjlim_{\Lambda} J \otimes_A M \to A \otimes_A M$

As tensor is compatible with direct limits, get

$0 \to I \otimes_A M \to A \otimes_A M$ exact because $\varinjlim_{\Lambda}$ is exact.

(cont proof)

Now let $N' \subseteq N$ an inclusion of modules.

Want $N' \otimes M \to N \otimes M$ be an inclusion.

Can say $N \cong \varinjlim_{\Lambda} N'_\alpha$, $\Lambda = \{N'_\alpha \subseteq N$ of form $N'_\alpha = N' + A\omega_1 + \dots + A\omega_r\}$ (check it again).

<u>Claim</u>: it suffices to show that $N' \otimes M \to N'_\alpha \otimes M$ is injective $\forall N'_\alpha \in \Lambda$.

Pf (then, consider $0 \to N' \otimes M \to N'_\alpha \otimes M$ is exact, then take the direct limit and get $0 \to N' \otimes M \to N \otimes M$ exact //).

So we are reduced to the case where N is fin. gen over N', i.e. $N = N' + A\omega_1 + \dots + A\omega_r$.

By induction on r, can reduce to the case $N = N' + A\omega$

Need to show that $0 \to N' \otimes M \to N \otimes M$ is exact.

As $N = N' + A\omega$, have $0 \to N' \to N \to A/I \to 0$ where

$I = \{a \in A : a\omega \in N'\} = (N' : \omega)_A$.

Taking $\mathrm{Tor}_*^A(\cdot, M)$, get:

$$\cdots \quad \cdots \mathrm{Tor}_1^A(A/I, M) \to N' \otimes M \to N \otimes M \to A/I \otimes M \to 0$$

Since this is exact, need to show that $\mathrm{Tor}_1^A(A/I, M)$

The sequence $0 \to I \to A \to A/I \to 0$ gives

$$\mathrm{Tor}_1^A(A,M) \to \mathrm{Tor}_1^A(A/I, M) \xrightarrow[\partial\text{-map!}]{} I \otimes M \xrightarrow{\text{injective by hypothesis}} A \otimes M \to A/I \otimes M \to 0$$

So $\mathrm{Tor}_1^A(A,M) \twoheadrightarrow \mathrm{Tor}_1^A(A/I, M)$ is a surjection

And $\mathrm{Tor}_1^A(A,M) = 0$ because A is flat (so $\mathrm{Tor}_q^A(A,M) = 0 \ \forall q \geq 1$).

So $\mathrm{Tor}_1^A(A/I, M) = 0$ ⇒ ///

Theorem: Let A be a ring, M an A-module. TFAE:

(1) M is A-flat.

(2) $\forall a_{ij} \in A$, $x_j \in M$ s.t. $\sum_{j=1}^{n} a_{ij} x_j = 0$ $\forall i$ $(i=1..r)$, $\exists b_{jk} \in A$, $y_k \in M$ $(k=1..s$ for some $s)$.

s.t. $\sum_j a_{ij} b_{jk} = 0$ $\forall i,k$, and $x_j = \sum_{k=1}^{s} b_{jk} y_k$ $\forall j$

(3) (2) in the special case that $r=1$.

Pf

1⇒2: Let $\varphi: A^n \to A^r$ be the homomorphism given by matrix (a_{ij}).

Consider $\varphi \otimes id_M : \underset{\underset{M^r}{\cong}}{A^n \otimes_A M} \to \underset{\underset{M^n}{\cong}}{A^r \otimes_A M}$, called φ_M.

The element $\underline{x} = (x_1, \dots, x_n) \in M^n$ is in $\operatorname{Ker} \varphi_M$ (this is exactly the hypo. in (2)).

Let $K = \ker[\varphi : A^n \to A^r]$.

$-\otimes_A M$ gives $0 \to K\otimes M \to A^n \otimes_A M \to A^r \otimes_A M$ (by flatness of M).

Write $\rho : K \to A^n$ the inclusion of the kernel.

So $\underline{x} = (\rho \otimes id_M)\left(\sum_{k=1}^{s} \beta_k \otimes y_k\right)$ for some $y_k \in M$, $\beta_k \in K$

Write $\rho(\beta_k) = (b_{1k}, \dots, b_{nk}) \in A^n$.

Then $\underset{\underset{(x_1,\dots,x_n)}{\parallel}}{\underline{x}} = \sum_k \rho(\beta_k) \otimes y_k \cong \sum_k (b_{1k}, \dots, b_{nk}) \otimes y_k = \sum_k (b_{1k} y_k, \dots, b_{nk} y_k)$

$= (\dots, \underbrace{\sum_k b_{jk} y_k}_{j^{th} \text{ entry}}, \dots)$.

As $\beta_k \in K$, the b_{jk} are in the kernel of φ, so done //

2⇒3 is clear.

(cont proof)

(3 ⇒ 1): Given M satisfying (3). Want to show that M is flat.
As we have seen, need to show that, given any finitely-generated ideal $I \subseteq A$, that $I \otimes_A M \xrightarrow{f} A \otimes_A M \simeq M$ is injective.

Consider $u = \sum_{j=1}^{n} a_j \otimes x_j$ in $I \otimes_A M$ (u a general element in $I \otimes M$).

Suppose $f(u) = 0$. $\iff 0 = \sum_{j=1}^{n} a_j x_j$. So by (3),

$\exists\ b_{jk} \in A$, $y_k \in M$ s.t. $x_j = \sum_k b_{jk} y_k$, $\sum_j a_j b_{jk} = 0$

Now $u = \sum_{j=1}^{n} a_j \otimes x_j = \sum_{\substack{j=1\\k=1}} a_j \otimes (b_{jk} y_k) = \sum_{j,k} \underbrace{(a_j b_{jk})}_{=0} \otimes y_k = 0$ //

We now restate condition (2):

(*) For every hom $\beta : F \to M$ where F is a f-gen free A-module, and for every finitely-gen submodule $K \subseteq Ker(\beta)$,
There exists a diagram

$$\begin{tikzcd} F \arrow[r, "\gamma"] \arrow[dr, "\beta"'] & G \arrow[d, "\delta"] \\ & M \end{tikzcd}$$

of module homs s.t.
→ $\delta\gamma = \beta$
→ G is fin-gen & free
→ $K \subseteq Ker(\gamma)$.

Claim: (*) is equivalent to (2):

(2)⇒(*): Given (a_{ij}), (x_j), let ~~$F = A^n$~~, ~~and let~~
let $F = Ae_1 \oplus \cdots \oplus Ae_m$, a free module on generators $e_1, \ldots, e_m$.
~~Let K be the submodule of F generated by~~
Let $\beta : F \to M$ be defined by $\beta(e_j) = x_j$.
Let $K \subseteq F$ be the submodule given by $k_1, \ldots, k_r$; $k_i = \sum_j a_{ij} e_j$
Then $K \subseteq Ker(\beta)$, and K is finitely-generated.

↓

Now suppose $\exists\, G, \gamma, \delta$

$$\begin{tikzcd} F \arrow[r, "\gamma"] \arrow[d, "\beta"'] & G \arrow[dl, "\delta"] \\ M & \end{tikzcd} \quad G = Ae_1' \oplus \cdots \oplus Ae_s' \quad \text{with} \quad K \subseteq \ker(\gamma)$$

Then let b_{jk} be defined by $\gamma(e_j) = \sum_k b_{jk} e_k'$, and y_k is defined by $y_k = \delta(e_k')$.

$\delta\gamma = \beta \Rightarrow \sum b_{jk} y_k = x_j$.

$K \subseteq \ker \gamma \Rightarrow \sum a_{ij} b_{jk} = 0$.

$(\ast\ast) \Rightarrow (\ast)$: exercise.

So now we have $(\ast) \Leftrightarrow M$ flat.

<u>Corollary</u>: Let M be a module of finite presentation. Then,
M is flat $\Leftrightarrow$ M is projective.
(in particular, if A is Noetherian, M f.gen flat $\Leftrightarrow$ M f.gen. projective).

<u>Example</u>: We need finiteness!
Let $A = \mathbb{Z}$, $M = \mathbb{Q}$ as a $\mathbb{Z}$-module. $\mathbb{Q}$ is flat (because $\mathbb{Q}$ is divisible!) but not projective.
The problem is that $\mathbb{Q}$ is not finitely-generated over $\mathbb{Z}$!..

<u>Pf of corollary</u>:
$\Leftarrow$ clear without restriction.
$\Rightarrow$ Let $F_1 \to F_0 \xrightarrow{\beta} M \to 0$ be a finite presentation. (F_0, F_1 are f-gen free)
Let $K := \operatorname{Im}(F_1 \to F_0) = \ker \beta$. K is f.gen (it's the image of a F-gen).

$$\begin{tikzcd} K \subseteq F_0 \arrow[r, "\gamma"] \arrow[d, "\beta"'] & G \arrow[dl, "\delta"] \\ M & \end{tikzcd} \exists \quad \text{s.t.} \quad K \subseteq \ker(\gamma).$$

We will construct a retract $M \xrightarrow{\varepsilon} G$. But by construction, $M \cong \operatorname{Coker}(F_1 \to F_0)$ $= F_0/K$
So there $\exists$ hom $\varepsilon: M \to G$ s.t.
$$\begin{tikzcd} F_0 \arrow[r, "\gamma"] \arrow[d, "\beta"'] & G \\ M \arrow[ur, "\varepsilon"'] & \end{tikzcd}$$
In particular, $\varepsilon\beta = \gamma$.
$$\begin{tikzcd} F_0 \arrow[r, "\mathrm{id}"] \arrow[d, "\beta"] & F_0 \arrow[r, "\mathrm{id}"] \arrow[d, "\gamma"] & F_0 \arrow[d, "\beta"] \\ M \arrow[r, "\varepsilon"] & G \arrow[r] & M \end{tikzcd}$$ commutes.

<u>Corollary</u>: Let A be a local ring, with maximal ideal P.
Let M be a finitely-gen flat A-module. Then <u>M is free</u>.

<u>Proof</u>: M/PM is a fin-gen A/p-module (so it's a vectorspace).

If $\bar{x}_1, \dots, \bar{x}_n$ is a basis for M/PM and $x_j \in M$ are lifts of $\bar{x}_j$,

then the $x_1, \dots, x_n$ generate M as an A-module (Nakayama's lemma).

Need to show that the x_i are linearly-indep.

If $x_1, \dots, x_r \in M$ are s.t. $\bar{x}_j \in M/PM$ are lin. indep over A/p,

then x_j's are linearly indep over A.

. By induction on r:

<u>$r=1$</u>: $x_1 \in M$ s.t. $\bar{x}_1 \neq 0$. Suppose $a_1 x_1 = 0$ in M for some $a_1 \in A$.

Since M is flat, $\exists\, y_k \in M$, $b_{1k} \in A$ s.t. $a_1 b_{1k} = 0$, $x_1 = \sum_k b_{1k} y_k$

As $x_1 \notin PM$, at least one of the b_{1k} is not in P, for some k.

Thus b_{1k} is a unit, and $a_1 b_{1k} = 0 \Rightarrow a_1 = 0$

<u>$r>1$</u>: $x_1, \dots, x_r \in M$ s.t. $\bar{x}_1, \dots, \bar{x}_r$ lin. indep. Suppose $\sum_j a_j x_j = 0$ for some a_j.

Then $\exists$ y's & b's s.t.

$$\sum_j a_j b_{jk} = 0, \quad \sum_k b_{jk} y_k = x_j$$

(all of them)

Since the $\bar{x}_j$ are l.i., at least one, say x_r s.t. $x_r \notin PM$

So $b_{rk} \notin P$ for some k.

So $a_r b_{rk} = -a_1 b_{1k} - \dots - a_{r-1} b_{r-1,k}$ with b_{rk} a unit,

So a_r is a linear combination of the a_i's for $(a_1, \dots a_{r-1})$.

$$0 = \sum_{j=1}^{r} a_j x_j = a_1 (x_1 + c_1 x_r) + \dots + a_{r-1} (x_{r-1} + c_{r-1} x_r)$$

mod P, gives $0 = a_1 (\overline{x_1 + c_1 x_r}) + \dots + a_{r-1} (\overline{x_{r-1} + c_{r-1} x_r})$, so

as $\{(x_i + c_i x_r)\}$ are linear indep, by induction have $a_1 = 0, \dots, a_{r-1} = 0 \Rightarrow a_r = 0$ //

Def A module M over a ring A is <u>faithfully flat</u> if for every sequence $N' \xrightarrow{f} N \xrightarrow{g} N''$ of A-modules, then
$N' \to N \to N''$ is exact iff $N' \otimes M \to N \otimes M \to N'' \otimes M$ is exact.

Rk: Faithfully flat $\Rightarrow$ flat.

We say that <u>a ring homomorphism</u> $A \to B$ is <u>faithfully flat</u> if B is faith-flat as an A-module.

<u>Example</u>: If F is a free A-module, then it is faithfully-flat.

<u>Thm</u>: TFAE:

1) M is faithfully flat.
2) M is flat and, for all A-modules $N \neq 0$, $M \otimes_A N \neq 0$.
3) M is flat and, for all ~~A-modules~~ maximal ideals $\mathfrak{m} \subseteq A$, $M/\mathfrak{m}M \neq 0$.

Pf
<u>1⇒2</u>: Consider $0 \to N \to 0$ ~~exact~~ $\Rightarrow (0 \to N \to 0) \otimes M = (0 \to N\otimes M \to 0)$ ~~is exact~~. If $N \otimes M = 0$ then the 2nd one is exact, so $0 \to N \to 0$ is also exact by f-flatness $\Rightarrow N = 0$.

<u>2⇒3</u>: $M \otimes A/\mathfrak{m} \simeq M/\mathfrak{m}M$. Since $A/\mathfrak{m} \neq 0$, $\Rightarrow M/\mathfrak{m}M \neq 0$ if M is f-flat.

<u>3⇒2</u>: If $N \neq 0$, pick $x \in N$, $x \neq 0$,

$$\left[\begin{array}{ccc} A/\mathrm{ann}(x) & \hookrightarrow & N \\ \downarrow & & \\ A/\mathfrak{p} & & \end{array}\right] \underset{A}{\otimes} M \Rightarrow \begin{array}{ccc} M \otimes A/\mathrm{ann}(x) & \hookrightarrow & M \otimes_A N \\ \downarrow & & \\ M \otimes A/\mathfrak{p} & & \end{array} \Rightarrow M \otimes_A N \neq 0.$$

for some maximal ideal $\mathfrak{p} \supseteq \mathrm{ann}(x)$

$M\otimes A/\mathfrak{p} = M/\mathfrak{p}M \neq 0$

<u>2⇒1</u>: Let $N' \xrightarrow{f} N \xrightarrow{g} N''$ be a sequence s.t. $M\otimes N' \to M \otimes N \to M \otimes N''$ is exact.

a) Show $g\circ f = 0$ (i.e. show $\mathrm{Im}(g\circ f) = 0$). Consider $K = \mathrm{Im}(g\circ f) \subseteq N''$

$$\begin{tikzcd} N' \arrow[rr, "g\circ f"] \arrow[dr] & & N'' \\ & K \arrow[ur] & \end{tikzcd} \overset{\otimes M}{\Rightarrow} \begin{tikzcd} M\otimes N' \arrow[rr, "id_M \otimes (g\circ f)"] \arrow[dr, two heads, "\text{true in general}"'] & & M\otimes N'' \\ & M\otimes K \arrow[ur, hook, "\text{since } M \text{ is flat}"'] & \end{tikzcd}$$

So $M \otimes K \simeq \mathrm{Im}(id_M \otimes (g\circ f))$
Since $id_M \otimes gf = 0 \Rightarrow M\otimes K = 0 \Rightarrow K = 0$

(cont pf)

b) Need to show that $\operatorname{Im} f \simeq \ker g$.

Let $H := \frac{\ker g}{\operatorname{Im} f}$. (want $H=0$).

Have exact sequence $0 \to \ker f \xrightarrow{\varphi} N' \to \operatorname{Im}(f) \to 0$.

$\operatorname{Im} f \subseteq \ker g$, so $0 \to \operatorname{Im} f \to \ker g \to H \to 0$ is exact.

Also, $0 \to \ker(g) \to N \to N''$.

Tensoring by M, get:

~~$M \otimes N' \xrightarrow{\otimes f} M \otimes N \to M \otimes \operatorname{Im}(f) \to 0$~~

$$0 \to \underset{\substack{\shortparallel \\ \ker(id \otimes f)}}{M \otimes \ker f} \to M \otimes N' \to M \otimes \overset{\substack{\operatorname{Im}(id \otimes f) \\ \shortparallel}}{\operatorname{Im}(f)} \to 0$$

$$0 \to \underset{\substack{\shortparallel \\ \operatorname{Im}(id \otimes f)}}{M \otimes \operatorname{Im}(f)} \to \underset{\substack{\shortparallel \\ \ker(id \otimes g)}}{M \otimes \ker(g)} \to M \otimes H \to 0$$

Since $M \otimes N' \to M \otimes N \to M \otimes N''$ is exact, $M \otimes \operatorname{Im}(f) \simeq M \otimes \ker g$, so $M \otimes H = 0. \Rightarrow H = 0$. //

Thm 7.3: Let $f: A \to B$ be a ring homomorphism, M a B-module. Then,

1) If M is faithfully flat $/A \Rightarrow f^{\#}(\operatorname{Supp}_B(M)) \simeq \operatorname{Spec}(A)$.

2) If M is finite over B, then

M is faithfully-flat $/A \iff M$ is A flat and $f^{\#}(\operatorname{Supp}(M)) \supseteq m\text{-}\operatorname{Spec}(A)$.

Example: $A \to B = A_S$ is always flat, but not usually faithfully-flat:

if p is a prime touching S, $A_S \otimes (A/p) = A_S/pA_S \simeq 0$, so not f-flat.

Corollary: (if $f = id : A \to A$):

1) If M is faithfully flat $/A$, then $\mathrm{Supp}_A(M) = \mathrm{Spec}(A)$.

2) If M is finite $/A$, then M is faithfully flat $/A \iff M$ flat & $\mathrm{Supp}(M) \supseteq \text{m-}\mathrm{Spec}(A)$.

Pf (of thm):

(1) Given $P \subseteq A$ a prime, need to find $Q \subseteq B$, prime, s.t. $M_Q \neq 0$, $\overset{f^{\#}(Q)}{Q \cap A} = P$.

Define $C := B \otimes_A k(P)$ (where $k(P) := K(A/p)$).

Then have

$$\begin{tikzcd} B \arrow[rrr] & & & C \\ A \arrow[u] \arrow[r] & A/p \arrow[r] & A_p/pA_p \cong K(A/p) = k(P) \arrow[ur] & \end{tikzcd}$$

$M \otimes_B C \cong M \otimes_B (B \otimes_A k(P)) = M \otimes_A k(P)$. Since M is faith. flat $/A$,

$M \otimes_A k(P) \neq 0$. So $M \otimes_B C \neq 0$, so $C \neq 0$.

Let $\tilde{Q} \subseteq C$ be any prime ideal s.t. $M'_{\tilde{Q}} \neq 0$ (any (nonzero) module has nonzero support) and define $Q := \tilde{Q} \cap B$.

Then $P = (\tilde{Q} \cap k(P)) \cap A = Q \cap A$.

Let $M' := M \otimes_B C \cong M \otimes_A k(P)$. Then $\cancel{M \otimes \tilde{Q}}$

$M'_{\tilde{Q}} = (M \otimes_B C) \otimes_C C_{\tilde{Q}} \cong M \otimes_B C_{\tilde{Q}} \cong M_Q \otimes_{B_Q} C_{\tilde{Q}}$ (because have $B_Q \to C_{\tilde{Q}}$). Thus $M_Q \neq 0$.

(2) M finite B-module. ~~Know~~ Suppose M is A-flat and $f^{\#}(\mathrm{Supp}_B(M)) \supseteq \text{m-}\mathrm{Spec}(A)$.

Want to show that M is faithfully-flat $/A$.

i.e. Need to show that, if $P \subseteq A$ is maximal ideal, then $M/PM \neq 0$.

So $\exists\, Q \subseteq B$, prime, s.t. $M_Q \neq 0$, $Q \cap A = P$. So $M_P \neq 0$

(since $A \setminus P$ "$\subseteq$" $B \setminus Q$).

By Nakayama, $M_Q/QM_Q \neq 0$ (M is finite B-mod). So $M_Q/PM_Q \neq 0$ since $PM_Q \subseteq QM_Q$

So $(M/PM)_Q \neq 0$ and hence $M/PM \neq 0$.

Prop: Let M, N be A-modules, B a flat A-algebra. If M is finitely-presented, then $\mathrm{Hom}_A(M,N)\otimes_A B \simeq \mathrm{Hom}_B(M\otimes_A B, N\otimes_A B)$ as B-modules.

Pf Have contravariant functors $F, G : A\text{mod} \to B\text{-mod}$

$F(M) := \mathrm{Hom}_A(M,N)\otimes_A B$

$G(M) := \mathrm{Hom}_B(M\otimes_A B, N\otimes_A B)$ (N is fixed).

Have a natural map $F(M) \xrightarrow{\lambda(M)} G(M)$

$f\otimes b \longmapsto [m\otimes x \mapsto f(m)\otimes xb]$ $(= b\cdot(f\otimes \mathrm{id}_B))$

It is natural in the following sense:

if $g : M \to M'$ hom of A-modules,

$$\begin{array}{ccc} F(M) & \xrightarrow{\lambda(M)} & G(M) \\ {\scriptstyle F(g)}\uparrow & \circlearrowleft & \uparrow{\scriptstyle G(g)} \\ F(M') & \xrightarrow{\lambda(M')} & G(M') \end{array}$$ commutes.

If $M = A$, $F(M) = \mathrm{Hom}_A(A,N)\otimes_A B$

$G(M) = \mathrm{Hom}_B(A\otimes_A B, N\otimes_A B)$

Claim: $F(M) \simeq N\otimes_A B \simeq G(M)$

$f\otimes b \longmapsto f(1)\otimes b \;\; \leftarrow\!\shortmid\; g$

$g(1\otimes 1)$

$\Rightarrow \lambda(A)$ is iso.

If $M = A^p$,

$$\begin{array}{ccc} F(A^p) & \longrightarrow & G(A^p) \\ \downarrow\simeq & & \downarrow\simeq \\ \prod_p (F(A)) & \xrightarrow[\prod \lambda(A)]{} & \prod G(A^p) \end{array}$$

$\Rightarrow \lambda(A^p)$ is iso

Finally, if $A^p \to A^q \to M \to 0$ is exact, obtain

$$\begin{array}{ccccccc} 0 \to & F(M) & \to & F(A^q) & \to & F(A^p) & \text{exact} \\ & \lambda(M)\downarrow & & \downarrow\simeq & & \downarrow\simeq & \\ 0 \to & G(M) & \to & G(A^q) & \to & G(A^p) & \text{exact} \end{array}$$

$\Rightarrow \lambda(M)$ is iso.

Corollary: $B = A_S$. If M is finitely presented,

$\mathrm{Hom}_A(M,N)_S \xrightarrow{\sim} \mathrm{Hom}_{A_S}(M_S, N_S)$ (localization commutes with Hom).

• Completion

Let Λ be a directed set.

Def An inverse system of sets consists of sets X_λ, $\lambda \in \Lambda$, and functions $f_{\lambda\mu} : X_\mu \to X_\lambda$ for $\lambda \leq \mu$ in Λ.

Such that:

$$f_{\lambda\lambda} = \mathrm{id}_{X_\lambda}, \quad f_{\lambda\mu} f_{\mu\nu} = f_{\lambda\nu} \quad \text{for all } \lambda \leq \mu \leq \nu \text{ in } \Lambda.$$

Example: $\Lambda = \mathbb{N}$, $X_0 \leftarrow X_1 \leftarrow X_2 \leftarrow \cdots$

Def: The inverse limit of an inverse system $\{X_\lambda, f_{\mu\lambda}\}$ is:

$$\varprojlim_{\Lambda} X_\lambda := \{(x_\lambda) \in \prod_{\lambda\in\Lambda} X_\lambda : f_{\lambda\mu}(x_\mu) = x_\lambda \ \forall \lambda \leq \mu \text{ in } \Lambda\}.$$

Proposition: Given a "cocone" $\{S \xrightarrow{g_\lambda} X_\lambda\}_{\lambda\in\Lambda}$ from a set S, there exists a unique factorization through the universal cocone p_λ.

$$\begin{tikzcd} S \arrow[r, "g_\lambda"] \arrow[dr, dashed, "h"'] & X_\lambda & x_\lambda \\ & \varprojlim_{\Lambda} X_\lambda \arrow[u, "p_\lambda"'] & (x_\mu) \arrow[u, mapsto] \end{tikzcd}$$

Let M be an A-module, and let Λ be a directed set.
Write $\mathcal{F} = \{M_\lambda\}_{\lambda\in\Lambda}$ a family of submodules of M,
such that if $\lambda \leq \mu$, $M_\lambda \supseteq M_\mu$.
We will give a topology for M; called $\mathcal{T}$.
The basis of this topology is $\{x + M_\lambda\}_{\lambda\in\Lambda, x\in M}$ (cosets of elements of $\mathcal{F}$).
($U \subseteq M$ is open iff $\forall x \in U$, $\exists \lambda$ s.t. $x + M_\lambda \subseteq U$).
The addition $M\times M \to M$, and $\begin{array}{c} M \to M \\ x \mapsto ax \end{array}$ are continuous maps.
Such topology is called a <u>linear topology</u>.

Def Say that M is <u>separated</u> (Hausdorff) if $\bigcap_{\lambda\in\Lambda} M_\lambda = 0$

Given a topological module, can form an inverse system:

$N_\lambda := M/M_\lambda$

Def The <u>completion of M</u>, is $\hat{M} := \varprojlim_{\Lambda} M/M_\lambda$, with the map
$M \to \hat{M}$ associated to the cocone $M \xrightarrow{p_\lambda} M/M_\lambda$ the obvious projection.

<u>Example</u>: $A = \mathbb{Z}$, p a prime number, $M = \mathbb{Z}$.
$\mathcal{F} = \{p^k\mathbb{Z}\}_{k\in\mathbb{N}}$. $\hat{A} = \hat{\mathbb{Z}}_p = \varprojlim_{\mathbb{N}} \mathbb{Z}/p^k\mathbb{Z}$, the p-adic integers.
So $\hat{\mathbb{Z}}_p = \{(a_k) : a_k \in \mathbb{Z}/p^k\mathbb{Z},\ a_{k+1} \equiv a_k \bmod p^k\ \forall k\}$.
As $a \in \mathbb{Z}/p^k\mathbb{Z}$ can be uniquely written as $a = a_0 + a_1 p + \cdots + a_{k-1}p^{k-1}$, $a_i \in \{0,\ldots,p-1\}$
can think $\hat{\mathbb{Z}}_p = \{c_0 + c_1 p + c_2 p^2 + \cdots \mid c_i \in \{0,\ldots,p-1\}\}$.

Ex: $B = A[X]$.

$\mathcal{F} = \{X^k \cdot B\}_{k \in \mathbb{N}}$.

$\hat{B} = \varprojlim_{k \in \mathbb{N}} A[X]/(X^k) \simeq A[[X]] = \{\sum_{i \geq 0}^{\infty} a_i x^i, \ a_i \in A\}$.

Ex: $\Lambda = \{1, 2, 3, \dots\}$, with "$a \leq b$" iff $a \mid b$

$A = M = \mathbb{Z}$, $\mathcal{F} = \{n\mathbb{Z}\}_{n \in \Lambda}$

$\hat{\mathbb{Z}} = \varprojlim_{n \in \Lambda} \mathbb{Z}/n\mathbb{Z}$ are called the <u>profinite integers</u>. $\left(\hat{\mathbb{Z}} \simeq \prod_{p \text{ prime}} \hat{\mathbb{Z}}_p \right)$.

$\hat{M}$ has a topology, also:

$\hat{M} \xrightarrow{q_\lambda} M/M_\lambda$. Define $M_\lambda^* := \operatorname{Ker}(q_\lambda) \subseteq \hat{M}$.

$\mathcal{F}^* := \{M_\lambda^*\}_{\lambda \in \Lambda}$ gives a linear topology on $\hat{M}$.

As $\hat{M} \hookrightarrow \prod_{\lambda \in \Lambda} M/M_\lambda$, can make M/M_λ have the discrete topology, and then the given topology on $\hat{M}$ is exactly the subspace topology of the product topology on M/M_λ.

<u>Rk</u>: $M \xrightarrow{q} \hat{M}$ is continuous (in fact, $q^{-1}(M_\lambda^*) = M_\lambda$).

Def A topological module M is <u>complete</u> if $M \simeq \hat{M}$.

Given families $\mathcal{F} = \{M_\lambda\}_\Lambda$, $\mathcal{F}' = \{M'_\gamma\}_\Gamma$, they give the same topology on M iff
$$\begin{cases} \forall \lambda \in \Lambda, \exists \gamma \in \Gamma \text{ s.t. } M'_\gamma \subseteq M_\lambda \\ \forall \gamma \in \Gamma, \exists \mu \in \Lambda \text{ s.t. } M_\mu \subseteq M'_\gamma \end{cases}$$

(ex: $\{n\mathbb{Z}\}$ and $\{p^k\mathbb{Z}\}$ are <u>not</u> the same topology on $\mathbb{Z}$).

Suppose we have the exact sequence:

$$0 \to N \xrightarrow{\alpha} M \xrightarrow{\beta} \underset{\underset{Q}{\shortparallel}}{M/N} \to 0$$

If $\mathcal{F}_M = \{M_\lambda\}_{\lambda \in \Lambda}$ is a basis for open nbh of 0 for M (giving a topology on M), then get:

- Submodule Topology: $\mathcal{F}_N = \{N_\lambda : N \cap M_\lambda\}$
- Quotient topology: $\mathcal{F}_Q = \{Q_\lambda := \beta(M_\lambda) = N + M_\lambda / N\}$

Note that, under this topology,

$\alpha^{-1}(M_\lambda) = N_\lambda$. $\implies \alpha$ and β are continuous.

$\beta^{-1}(Q_\lambda) = N + M_\lambda \supseteq M_\lambda$

<u>Theorem</u>: $0 \to \hat{N} \xrightarrow{\tilde{\alpha}} \hat{M} \xrightarrow{\tilde{\beta}} \hat{Q}$ is exact, and $\hat{N}$ is the closure of $\Psi(N)$ in $\hat{M}$ ($\Psi : M \to \hat{M}$).

Pf

exact here because of the definition of N_λ.

$0 \to N/N_\lambda \to M/M_\lambda \to Q/Q_\lambda \to 0$ exact?

$Q/Q_\lambda = M/N \big/ (N + M_\lambda/N) = \dfrac{M}{N + M_\lambda}$ Yes! Check it.

exercise!

Take $\varprojlim_\lambda$. Inverse limits are left-exact. So get:

$0 \to \hat{N} \to \hat{M} \to \hat{Q}$

Need to show that $\hat{N}$ is the closure of $\Psi(N)$ in $\hat{M}$.

I.e. $\forall x \in \hat{N}$, ~~there is a small~~ any open neighborhood $\mathcal{U}$ of x is s.t. $\mathcal{U} \cap \Psi(N) \neq \phi$.

(<u>Rk</u>: if $S \subseteq X$, $\bar{S} = \bigcap_{\substack{C \text{ closed} \\ C \supseteq S}} C$ - so it always exist).

$\downarrow$

(41)

(cont. proof)

So, as we have a basis for the topology, any open n-h of $x \in \hat{N}$ contains $x + M_\lambda^*$ for some λ. $\left(0 \to M^* \to \hat{M} \xrightarrow{P_\lambda} M/M_\lambda \to 0 \right)$

So, given $x = (x_\mu \in \cancel{M/M_\mu})$ and a given λ, need to find an element of $\Psi(N) \cap (x + M_\lambda^*)$.

Note that if $x \in \hat{N}$, then can represent $x = (x'_\mu \in N/N_\mu)$.

Let $\tilde{x}'_\mu \in N$ be any lift of x'_μ to N.

$\Psi(\tilde{x}'_\mu) \in \Psi(N)$. Want to show that $\Psi(\tilde{x}'_\mu) - x \in M_\lambda^*$.

$$P_\mu(x - \Psi(\tilde{x}'_\mu)) = x_\mu - P_\mu(\Psi(\tilde{x}'_\mu)) = x_\mu - x_\mu \mod M_\mu^* \quad (\text{so } \Psi(\tilde{x}'_\mu) \in x + M_\mu^*)$$

<u>Prop</u>: if $\mathcal{F}_M = \{M_n\}_{n \in \mathbb{N}}$, then $0 \to \hat{N} \xrightarrow{\hat{\alpha}} \hat{M} \xrightarrow{\hat{\beta}} \hat{Q} \to 0$ is exact.

Pf: $\hat{Q} = (\widehat{M/N}) = \varprojlim_n Q/Q_n = \varprojlim_n M/(N+M_n)$.

Let $y = (y_n) \in \hat{Q}$ (i.e. $y_n \in M/(N+M_n)$).

Want $x = (x_n) \in \hat{M} = \varprojlim M/M_n$ s.t. $\hat{\beta}(x) = y$.

$$\begin{tikzcd}
M/M_1 \ni x_1 \arrow[d, "\beta"] & M/M_2 \ni x_2 \arrow[l, "P_2"'] \arrow[d, "\beta"] & M/M_3 \ni x_3 \arrow[l, "P_3"'] \arrow[d, "\beta"] & \cdots \arrow[l, "P_4"'] \\
Q/Q_1 & Q/Q_2 \arrow[l, "P_2"'] & Q/Q_3 \arrow[l, "P_3"'] & \cdots \arrow[l, "P_4"'] \\
y_1 & y_2 \arrow[l, mapsto] & y_3 \arrow[l, mapsto] &
\end{tikzcd}$$

Construct x by induction. Let x_1 be any elt of M/M_1 s.t. $\beta(x_1) = y_1$.

Given $x_1, \dots, x_{n-1}$, let $\varepsilon \in M/M_n$ s.t. $\beta(\varepsilon) = y_n$. Note that it may happen that $P_n(\varepsilon) \neq x_{n-1}$!

$P_n(\varepsilon) - x_{n-1} \in M/M_{n-1}$. $\hat{\beta}(P_n(\varepsilon) - x_{n-1}) = P_n(\hat{\beta}(\varepsilon)) - \hat{\beta}(x_{n-1}) = y_{n-1} - y_{n-1} = 0$.

So $\varepsilon \equiv x_{n-1} \mod N + M_{n-1}$.

write then $\varepsilon - x_{n-1} \equiv t + u$, $\quad t \in N,\ u \in M_{n-1}$ $\quad$ (mod M_{n-1}).

Set $x_n := \varepsilon - t \in M/M_n$.

Now $\hat{\beta}(x_n) = \hat{\beta}(\varepsilon) - \hat{\beta}(t) = y_n - 0 = y_n$

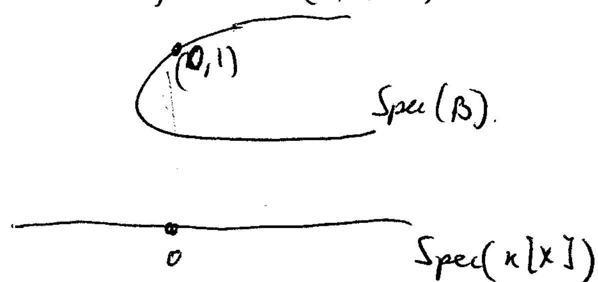
And also $p(x_n) = p(\varepsilon) - p(t) = p(x_{n-1}) + p(u) = p(x_{n-1}) = x_{n-1}$ //

• I-adic topology:

If $I \subseteq A$ is an ideal, then $\{I^n M\}_{n \in \mathbb{N}}$ is the I-adic topology.
write $\hat{M}_I$ for the I-adic completion of M.

Example: $A = k[X] \hookrightarrow B = k[X,Y]/(Y^2 - X - 1)$ $\quad$ (suppose char $k \neq 2$).

$I := J \cap A = (X)$ $\quad J := (X, Y-1)$



Claim: $\hat{A}_I \to \hat{B}_J$ is an isomorphism of topological rings.

Pf Define
$$\begin{tikzcd} B \arrow[r, "\beta"] & \hat{A}_I = k[[X]] \\ A \arrow[u, hook] \arrow[ur, "\psi"'] & \end{tikzcd}$$
such that $\beta(X) = X$
$\beta(Y) = $ "$\sqrt{1+X}$"

So $\beta(Y) = \sum_{k=0}^{\infty} \binom{1/2}{k} X^k = 1 - \frac{X}{2} + \frac{X^2}{8} + \dots \in k[[X]]$.

So $\beta : B \to \hat{A}_I$ is a ring homomorphism. It is also continuous:

The topology on $\hat{A}_I$ is $\{\ker(\hat{A}_I \to A/I^k A)\} = \{(X^k)\}$.

$\beta^{-1}((X^k)) \supseteq J^k$ (since $\beta(X) \in X\hat{A}_I$, and $\beta(Y-1) \in X\hat{A}_J$).

Can finally show that β is injective.

<u>Example:</u> $A = k[X]$, $B = k[X,Y]/(Y^2-X-1)$

$I = J \cap A = (X+1)$ $\quad J = (X+1, Y)$

If $T = X+1$, $A = k[X] = k[T] \Rightarrow \hat{A}_I = k[[T]]$

Now, $\hat{B}_J = k[[U]]$ and <u>will get</u> $T \mapsto U^2$ + higher degree $\Rightarrow$ not isomorphic.

Let A be a ring, $I \subseteq A$ an ideal, M a module. Consider the I-adic topology $\{I^n M\}_{n \geq 0}$, and $\hat{M}_I = \varprojlim_{n \geq 0} M/I^n M$.

<u>Def</u>: M is I-adically complete if $M \cong \hat{M}_I$ (note that $\hat{M}_I$ is an $\hat{A}_I$-module).

<u>Def</u>: A <u>Cauchy sequence</u> is $(x_n)_{n \geq 0}$, $x_n \in M$ s.t. $\forall k$, $\exists N$ s.t. $x_m - x_n \in I^k M$ for all $m, n \geq N$.

If M is I-adically complete and separate (i.e. $\bigcap I^n M = 0$), write $x := \lim x_n$ for the unique element $x \in M$ s.t.
$\forall k \geq 0$, $\exists N \geq 0$ s.t. $\forall n \geq N$ $x - x_n \in I^k M$.

<u>Prop</u>: $I \subseteq A$.

a) If $A \cong \hat{A}_I$ then $I \subseteq \mathrm{Jrad}(A)$.

b) If $M = \hat{M}_I$, $a \in I$, then multiplication by $1+a$ is an iso on M.

<u>Pf</u>

a) Let $a \in I$, $b := \lim (1 + xa + x^2a^2 + \dots + x^n a^n) \in A$.

Then $(1 - xa) b = 1 \Rightarrow 1 - xa \in A^\times$ $\forall x \in A \Rightarrow a \in \mathrm{Jrad}(A)$.

b) $M = \hat{M}_I$ is an $\hat{A}_I$-module. Also, the image of a in $\hat{A}_I$ by the previous part is in Jrad $\Rightarrow$ acts as a unit on M.

Hensel's lemma: Let $A \simeq \hat{A}_I$, $f(X) \in A[X]$. Let $a \in A$ s.t. $f(a) \equiv 0 \mod I$ and $f'(a) \equiv$ unit $\mod I$.

Then, $\exists!\ b \in A$ s.t. $f(b) = 0$, and $b \equiv a \mod I$.

Pf/

aside: if $f(x) = x^n$, $f^{(k)}(x) = n \cdot (n-1) \cdots (n-k+1)\, x^{n-k}$.

Let $f^{[k]}(x) := \binom{n}{k} x^{n-k}$ for $f(x) = x^n$, and extend $[k]$ linearly over A.

Then, $f(X+Y) = \sum_k f^{[k]}(X) Y^k$ (and $f(X+Y) \equiv f(X) + f'(X) Y \mod Y^2$)

Set $b_1 := a$, so $f(b_1) \in I$.

Consider $f(b_1 + \varepsilon) \equiv f(b_1) + f'(b_1)\varepsilon \mod I^2$ for some $\varepsilon \in I$.

Set $\varepsilon :=$ "$- f(b_1) \cdot (f'(b_1))^{-1}$"

(i.e. consider residues $\overline{f(b_1)} \in I/I^2$, $-\overline{f(b_1)}\ \overline{f'(b_1)}^{-1} \in I/I^2$

Let ε be any lift to I s.t. $\varepsilon f'(b_1) \equiv -f(b_1) \mod I^2$.)

Then, set $b_2 := b_1 + \varepsilon$, so $f(b_2) \equiv 0 \mod I^2$,

and $b_2 \equiv a \mod I$.

Given b_n s.t. $f(b_n) \equiv 0 \mod I^n$, $b_n \equiv a$, let

$b_{n+1} := b_n + \varepsilon$ where ε is any lift to I^n of

$-\overline{f(b_n)} \cdot (f'(b_n))^{-1}$ in I^n/I^{n+1}

Then $(b_n)_n$ is a Cauchy sequence, so $b \in A$, $f(b) \in I^n$ for all n, so $f(b) = 0$.

//

(cont pf)

Uniqueness: If b and b' are two different solutions, there is a smallest n s.t. $b \equiv b' \mod I^n$ $(n \geq 2)$.

Let $\varepsilon := b' - b \in I^{n-1}$. $f(b') = f(b+\varepsilon) \equiv \underbrace{f(b)}_{0} + \underbrace{f'(b)\varepsilon}_{\text{unit mod } I} \mod I^{2(n-1)}$

So $f'(b)\varepsilon \equiv 0 \mod I^{2(n-1)} \subseteq I^n \Rightarrow \varepsilon \in I^n$, so $b = b'$ //

Hensel's lemma, version 2: If $A \simeq \hat{A}_I$, $F(X) \in A[X]$ monic. Let $f := \bar{F} \in (A/I)[X]$. Suppose $f = g \cdot h$ for some monic $g, h \in (A/I)[X]$. $(g,h) = (1)$. Then $\exists$ monics $G, H \in A[X]$ s.t. $g \equiv \bar{G}$, $h \equiv \bar{H}$ and $F = G \cdot H$.

Corollary: Let $A \simeq \hat{A}_I$. Let B be a ring, $f(x) \in B[X]$ s.t. $(f(x), f'(x)) = B[X]$. Given a commutative diagram

$$\begin{tikzcd} B \arrow[r] \arrow[d] & A \arrow[d] \\ B[X]/(f(x)) \arrow[r] \arrow[ur, dashed] & A/I \end{tikzcd} \qquad x \longmapsto \bar{a}$$

$\exists$ a dotted arrow making all commute.

(reason: $f(\bar{a}) = 0$ & $f'(\bar{a})$ is a unit, so $x \mapsto b$)

Corollary (lifting idempotents): If $A \simeq \hat{A}_I$ s.t. $\bar{e}^2 = \bar{e}$, then $\exists!\, e \in A$ s.t. $e \equiv \bar{e} \mod I$, and $e^2 = e$.

Pf/ $f(x) = x^2 - x \in A[X]$, $f'(x) = 2x - 1$.
$f(\bar{e}) = 0 \mod I$, $f'(\bar{e}) = 2\bar{e} - 1$.
$(2\bar{e} - 1)^2 = 4\bar{e}^2 - 4\bar{e} + 1 = 1$. So $\exists!\, e \in A$ s.t. $e \equiv \bar{e} \mod I$, and $f(e) = 0$ //.

Note: If $A \simeq \hat{A}_I$, $A/I \simeq B_1 \times \dots \times B_r$ product of rings, then $\exists\ A \simeq A_1 \times \dots \times A_r$, product decomposition.

Example: $R = k[X]$, $I = (X(X-1))$, $A = \hat{R}_I$ is J-adically complete wrt $J = IA$, and $A \simeq k[[X]] \times k[[X-1]]$. $R \to A$, $R \to R_S$, $S = R \setminus \{(x) \cup (x-1)\}$.

Prop: if A is I-adically complete, M an A-module, separated in I-adic topology.
If $\omega_1, \dots, \omega_n \in M$ s.t. $\bar{\omega}_1, \dots, \bar{\omega}_n \in M/IM$ generate A/I-module. Then:
$\omega_1, \dots, \omega_n$ generate M as A-module.

Pf/ Know that $M = \sum_{i=1}^{n} A\omega_i + IM$

Given $y \in M$, write $y = \sum_{i=1}^{n} a_{i,0}\omega_i + x_1$ for some $a_{i,0} \in A$, $x_i \in IM$.

$x_1 \in IM = I(\sum A\omega_i + IM) = \sum I\omega_i + I^2 M$.

write $x_1 = \sum a_{i,1}\omega_i + x_2$, $a_{i,1} \in I$, $x_2 \in I^2 M$.

By induction, $x_m = \sum a_{i,m}\omega_i + x_{m+1}$, $a_{i,m} \in I^m$, $x_{i+1} \in I^{m+1}M$

Set $a_i := a_{i,0} + a_{i,1} + a_{i,2} + \dots \in A$ (converges by Cauchy).

Claim: $y = \sum a_i \omega_i$.

Note that $y \equiv \overbrace{\sum_i (a_{i,0} + a_{i,1} + \dots + a_{i,m})\omega_i}^{y_m}$ mod $I^{m+1}M$

So let $z := \sum a_i \omega_i$.

So $y - z \in I^{m+1}M$: $y = \sum (a_{i,0} + \dots + a_{i,m})\omega_i + x_{m+1}$ $\Rightarrow$

$\Rightarrow$ $y - z = \sum \underbrace{(a_{i,0} + \dots a_{i,m} - a_i)}_{\in I^{m+1}}\omega_i + \underbrace{x_{m+1}}_{\in I^{m+1}M} \in I^{m+1}M$,

So $y - z \in \bigcap_{m \geq 0} I^m M = 0$ because M is separated.

Remark: it is a version of Nakayama's lemma, not requiring M be finite but instead requiring M be separated in the I-adic top.

Example: $A = \mathbb{Z}_p$, $M = K(\mathbb{Z}_p) = \mathbb{Q}_p$.

$I = p\mathbb{Z}_p \subseteq A$ and A is I-adically complete.

$M/IM = \mathbb{Q}_p/p\mathbb{Q}_p \simeq 0$

So M is not separated: $I^k M = p^k \mathbb{Q}_p \cong \mathbb{Q}_p$ not separated.

$A \supseteq I$, I-adically complete.

M a module, get I-adic topology $\{I^k M\}$.

$N \subseteq M$. $Q := M/N$. Q has a I-adic topology: $\{I^k Q = (I^k M + N)/N\}$ = quotient topology

But in general, submodules are not as nice:

N has $\left\{ \begin{array}{ll} I\text{-adic topology}: & \{I^k N\} \\ \text{Subspace topology}: & \{I^k M \cap N\} \end{array} \right.$

Theorem (Artin-Rees Lemma): Let A be a Noetherian ring, M a finite A-module, $N \subseteq M$ a submodule. Let $I \subseteq A$ an ideal. Then:

$$\exists\, c \geq 0 \text{ s.t. } \forall n > c, \quad I^n M \cap N = I^{n-c}(I^c M \cap N)$$

Corollary: I-adic topology $=$ submodule topology on N.

Pf/ $\forall k$, $I^k N \subseteq (I^k M) \cap N$ (true always).

$\forall n > c$, $I^n M \cap N = I^{n-c}(I^c M \cap N) \subseteq I^{n-c} N$

So for given k, let $n := c + k$, get $I^{n-c} N = I^k N \supseteq I^{c+k} M \cap N$ //

Proof (of Artin-Rees):

It is clear that for any c, $I^{n-c}(I^cM \cap N) \subseteq I^nM \cap N$

Write $I=(a_1,\dots,a_r)$ $\quad M = Aw_1+\dots+Aw_s$

Given $x \in I^nM$, can write $\quad x = \sum_{i=1}^{s} f_i(\underline{a})\,w_i$, where $f_i \in A[X_1,\dots,X_r]$ ($=B$) is a homogeneous polynomial of degree n.

Consider $J_n := \{(f_1,\dots,f_s) \in B^s \mid f_i \text{ hom. of deg. } n \text{ and } \sum f_i(\underline{a})w_i \in N\}$.

(J_n is a subset of B^s (not necessarily an ideal)).

Note that $\exists$ function $J_n \longrightarrow I^nM$.

Let $C :=$ B-submodule of B^S generated by $\bigcup_{n\geq 0} J_n$

B is Noetherian (because A is), and so C is a finite B-module.

Write $\quad C = \sum B u_j$ (finite sum).

Each $u_j = (u_{j,1},\dots,u_{j,s})$, $\quad u_{j,i} \in B$

WLOG, assume $u_j \in \bigcup_{n\geq 0} J_n$, and let d_j s.t. $u_j \in J_{d_j}$ and $c := \max\{d_j\}$.

Suppose now that $n \geq c$, and $x \in I^nM \cap N$. Want $x \in I^{n-c}(I^cM \cap N)$.

Write $x = \sum f_i(\underline{a})w_i$ $\quad (f_1,\dots,f_s) \in J_n \subseteq C$

Write $(f_1,\dots,f_s) = \sum p_j(\underline{x})\,\underset{\substack{\shortparallel\\ J_{d_j}}}{u_j}$ $\quad$, $p_j \in B = A[x_1,\dots,x_r]$

WLOG, can take $p_j(x)$ be homogeneous of degree $n-d_j \geq 0$ because $n \geq \underset{\substack{\shortparallel\\ c}}{\max\{d_j\}}$ (think about it).

$$x = \sum_{i=1}^{s} f_i(\underline{a})w_i = \sum_i\Big(\sum_j p_j(\underline{a})u_{j,i}(\underline{a})\Big)w_i = \sum_j p_j(\underline{a})\underbrace{\Big(\sum_i u_{j,i}(\underline{a})w_i\Big)}_{\in\, I^{d_j}M \cap N \text{ by construction}}$$

Also, $p_j(\underline{a}) \in I^{n-d_j} = I^{n-c}\cdot I^{c-d_j}$

So $p_j(\underline{a})\sum_i u_{j,i}(\underline{a})w_i \in I^{n-c}I^{c-d_j}(I^{d_j}M \cap N) \subseteq I^{n-c}(I^cM \cap N)$ //

Corollary: if A is Noetherian, M a finite A-module, then:

$$M \otimes_A \hat{A}_I \simeq \hat{M}_I$$

Pf If $M = A$, $A \otimes_A \hat{A}_I = \hat{A}_I$ //

If $M = M_1 \oplus \cdots \oplus M_r$, as both tensoring and completion preserve direct sums,

$$M \otimes_A \hat{A}_I = \bigoplus M_i \otimes \hat{A}_I \text{, and } \hat{M} \simeq \bigoplus \hat{M}_i \;//$$

So corollary is true if M is finite and free.

Consider a finite presentation:

$$\begin{tikzcd} A^p \arrow[r] & A^q \arrow[r] & M \arrow[r] & 0 & \Rightarrow & A^p \otimes \hat{A} \arrow[r] \arrow[d, phantom, "\wr"] & A^q \otimes \hat{A} \arrow[r] \arrow[d, phantom, "\wr"] & M \otimes \hat{A} \arrow[r] \arrow[d, phantom, "\wr"] & 0 \text{ is exact.} \\ & & & & & \hat{A^p} \arrow[r] & \hat{A^q} \arrow[r] & ? \arrow[r] & 0 \end{tikzcd}$$

Need to know that $\hat{A^p} \to \hat{A^q} \to \hat{M} \to 0$ is exact

$$\begin{tikzcd} & & A^q \arrow[r] \arrow[dr] & A^p \arrow[r] & M \arrow[r] & 0 \\ 0 \arrow[r] & K \arrow[ur] & & N \arrow[u] & \\ & & 0 \arrow[ur] & & \end{tikzcd}$$

$\leftarrow$ subspace topology $=$ I-adic topology

$$\begin{tikzcd} & \hat{A^q} \arrow[d] & & & \\ 0 \arrow[r] & \hat{N} \arrow[r] \arrow[d] & \hat{A^p} \arrow[r] & \hat{M} \arrow[r] & 0 \\ & 0 & & & \end{tikzcd}$$

//

(So we get the following, looking at same part of the proof:)

Lemma: A Noetherian, $I \subseteq A$, $M' \to M \to M''$ an exact sequence of finitely-generated A-modules. Then, $\hat{M}'_I \to \hat{M}_I \to \hat{M}''_I$ is exact.

Pf Uses Artin-Rees, (submod top $=$ I-adic top) and that completion preserves short exact sequences:

$$\begin{tikzcd} & M \arrow[r] \arrow[dr] & M' \arrow[r] \arrow[dr] & M'' \arrow[dr] & \\ K \arrow[ur, hook] & & L \arrow[ur, hook] & & P \arrow[ul, hook] & Q \end{tikzcd}$$

Example: $A = \mathbb{Z}$, $I = p\mathbb{Z}$, $\hat{A}_I = \hat{\mathbb{Z}}_p \supseteq \mathbb{Z}_{(p)}$

$M = \mathbb{Q}$, $\hat{M}_I = 0$, but $M \otimes_{\mathbb{Z}} \hat{\mathbb{Z}}_p \neq 0$:

$\mathbb{Q} \otimes_{\mathbb{Z}} \hat{\mathbb{Z}}_p \simeq (\hat{\mathbb{Z}}_p)[\frac{1}{p}] = \mathbb{Q}_p$ (fraction field of $\hat{\mathbb{Z}}_p$). ($\neq 0$ because $\hat{\mathbb{Z}}_p$ is a domain).

(previous proposition does not apply, because $\mathbb{Q}$ is not fin-gen over $\mathbb{Z}$).

Prop: A Noetherian. Then $\hat{A}_I$ is flat over A

Pf Need to show that, given an ideal $J \subseteq A$, $J \otimes_A \hat{A} \to A \otimes_A \hat{A}$ is injective.

$$A \otimes_A \hat{A} \cong \hat{A}_I$$

Since J is fin-gen, $J \otimes_A \hat{A} \simeq \hat{J}_I$. So:

So get $0 \to \hat{J}_I \to \hat{A}_I$ is exact, because $0 \to J \to A$ was (A-R) //

Example: $A[[X]]$ is flat over $A[X]$. And $A[X]$ is flat over A. So $A[[X]]$ is flat over A.

Krull Intersection

Prop: A Noetherian, $I \subsetneq A$, M finite A-module. Let $N := \bigcap_n I^n M$.

Then, $\exists a \in A$, $a \equiv 1 \bmod I$ and $aN = 0$.

Pf By NAK, it is enough to show that $N = IN$.

By Artin-Rees, $\exists c$ s.t. $I^n M \cap N = I^{n-c}(I^c M \cap N) \subseteq IN$ (if $n > c+1$)

By definition of N, $I^n M \cap N = N$, so get $N \subseteq IN$ $\Rightarrow$ //

Corollary: If A is Noetherian and $I \subseteq \mathrm{Jrad}(A)$, M finite A-mod, then the I-adic topology on M is separated, and every submodule of M is closed. (Pf: if $I \subset \mathrm{Jrad}(A)$, then "a" in prop is a unit, so $aN = 0 \Rightarrow N = 0$. $N \subseteq M$ closed iff M/N separated),

Note: why $N \subseteq M$ closed iff M/N is separated?

Pf/ **Remark:** if a module Q is separated, then $\{0\}$ is closed:

$\{I^n Q\}$ a basic open neighborhoods of Q.

All open ~~sets~~ submodules are also closed, because can take the union of all the cosets not equal to the given submodule.

Exercise: prove then the note.

Note: If A is I-adically complete, and Noetherian! then $I \subseteq \mathrm{Jrad}(A)$, and so for any finite module M, it is separated and all of its submodules are closed.

Corollary: If A is a Noetherian domain, and $I \subsetneq A$, then $\bigcap I^n = 0$.

Pf/ In the Krull intersection prop., take $M = A$, $N = \bigcap I^n$.

there is $a \in A$ s.t. $a \equiv 1 \bmod I$ s.t. $aN = 0$.

But since $a \neq 0$, a is not a zero divisor and thus $N = 0$.

(but if $A = B \times C$, $I = 0 \times C$, then $I^n = I$ and so $\bigcap I^n = 0 \times C$!).

Prop: Let A be a Noetherian ring. $I, J \subseteq A$, M a finite A-module.

$\hat{M} = \hat{M}_I$, $\psi : M \to \hat{M}_I$. Then,

$$\widehat{(JM)}_I = J\hat{M}_I = \overline{\psi(JM)}$$

$\downarrow$

Proof
Consider the exact sequence: (of finite A-modules).

$$0 \to JM \to M \to M/JM \to 0.$$

So $0 \to \widehat{(JM)}_I \to \hat{M}_I \to \widehat{(M/JM)}_I \to 0$ exact

So we get $\widehat{(JM)}_I = \overline{\Psi(JM)}$.

Write $J = \sum_{i=1}^{r} Aa_i$.

$$JM = \operatorname{Im}\Big[M^r \xrightarrow{\varphi} M \Big] \quad . \text{ Then:}$$
$$(x_1, \dots, x_r) \mapsto \sum_{i=1}^{r} a_i x_i$$

$M^r \xrightarrow{\varphi} M \to M/JM \to 0$ exact of A-mod. Take $\widehat{(\ )}_I$ and get:

$$\hat{M}_I^r \xrightarrow{\hat{\varphi}} \hat{M}_I \to \widehat{(M/JM)}_I \to 0 \quad \text{exact}.$$
$$(y_1, \dots, y_r) \mapsto \sum a_i y_i \qquad \text{"} \ \hat{M}_I / \widehat{(JM)}_I \ \text{(by prev seq)}.$$

So $\widehat{JM} = \operatorname{Im} \hat{\varphi} = J \cdot \hat{M}_I$. //

Remark: If A is Noetherian, in $\hat{A}_I$, the completion topology is the same as the $I\hat{A}_I$-adic topology.

Prop: if A is Noetherian, $I \subseteq A$, then $\hat{A}_I \cong A[[X_1, \dots, X_n]] / (X_1 - a_1, \dots, X_n - a_n)$ where $I = (a_1, \dots, a_n)$.

Corollary: if A is Noetherian, then $\hat{A}_I$ is also Noetherian (since $A[[X_1, \dots, X_n]]$ is Noeth by Hilbert's Basis).

Pf (of prop):

$B := A[X_1, \dots, X_n]$.

$P := (X_1, \dots, X_n) \subseteq B$.

Then $\hat{B}_P = A[[X_1, \dots, X_n]]$.

Take $J := (X_1 - a_1, \dots, X_n - a_n) \subseteq B$. Note that $B/J \cong A$.

$P^n(B/J) = P^n A$ ← makes A into a B-module. $(P^n A = I^n A)$.

So the P-adic topology in B/J coincides with the I-adic top on A

Thus, $\hat{A}_I = \widehat{(B/J)}_P \cong \hat{B}_P / \hat{J}_P \cong \dfrac{\hat{B}_P}{J\hat{B}_P} \cong \dfrac{A[[X_1, \dots, X_n]]}{(X_1 - a_1, \dots, X_n - a_n)}$ //

Example: $\mathbb{Z}$, $I = p\mathbb{Z}$. $\mathbb{Z}_p \cong \mathbb{Z}[[X]]/(X-p)$

Prop: A Noeth., $I \subseteq A$, M a finite A-module. Then:

Completion top on $\hat{M}_I$ = I-adic topology on $\hat{M}_I$ as an A-module = $I\hat{A}_I$-adic top on $\hat{M}_I$

Pf/ $M_n^* := \operatorname{Ker}[\hat{M}_I \to M/I^n M]$.

$0 \to I^n M \to M \to M/I^n M \to 0$ exact seq of A-modules. Then, A-R ⇒

⇒ $0 \to \widehat{I^n M} \to \hat{M} \to \widehat{M/I^n M} \to 0$ exact.

Obs: $M/I^n M$ is discrete in the I-adic topology (i.e. $\{0\}$ is open).

Since $I^k(M/I^n M) = 0$ for large k, $\widehat{M/I^n M} = M/I^n M$.

Then $M_n^* = (\widehat{I^n M})_I = I^n(\hat{M}_I)$. So the I-adic top = completion top.

Finally, $I^n \hat{M} = (I^n \hat{A})\hat{M} = (I\hat{A})^n \hat{M}$, so it is also the $I\hat{A}$-adic topology //

amounts to prove that $I^n \hat{M}$ is a sub-$\hat{A}$-module. But $I^n \hat{M}$ is some kernel so OK.

Proposition: Let A be Noetherian, $I \subseteq A$ an ideal. Then TFAE:

1) $I \subseteq \mathrm{Jrad}(A)$.
2) Every ideal is closed in the I-adic topology.
3) $\hat{A}_I$ is faithfully flat $/A$.

Def: A is Zariski if it satisfies the above (depends on the I: ideal of definition).

Rk: usually used when A is a local ring, $I := m_A$.

Pf: (1) $\Rightarrow$ (2) (done by Krull intersection).

(2) $\Rightarrow$ (3).

$\hat{A}_I$ is A-flat by Artin-Rees.

To show faithful, need to show $P\hat{A}_I \neq \hat{A}_I$ for all $P \subseteq A$ maximal.

Since $0 \subseteq A$ is closed, A is separated, so $\psi: A \to \hat{A}_I$ is injective.

$P\hat{A} = \overline{\psi(P)}$ (by Artin-Rees).

But $\overline{\psi(P)} = P\hat{A}_I \subseteq \hat{A}_I$

Since $P \subseteq A$ is closed, $\overline{\psi(PA)} \cap A = P\hat{A}_I \cap A$

Claim: $1 \notin P\hat{A}_I \cap A$. (and so, as P is maximal, $P\hat{A}_I \cap A = P$).

Pf Since, if $1 \in \overline{\psi(P)}$, $\exists\, n \gg 0$ s.t. $(1 + I^n\hat{A}) \cap \psi(P) \neq \phi$,

so $(1 + I^nA) \cap P \neq 0$, contradicting P being a proper ideal.

(3) $\Rightarrow$ (1)

If $P \subseteq A$ is maximal, since $\hat{A}_I$ is f. flat $\Rightarrow P\hat{A}_I \cap A = P$.

So we have that $P\hat{A}_I = \overline{\psi(P)}$ is closed in $\hat{A}_I$.

In general, we know we know $I\hat{A}_I \subset \mathrm{Jrad}(\hat{A}_I)$.

By the Krull intersection thm., every ideal in $\hat{A}_I$ is closed.

Since $\psi: A \to \hat{A}_I$ is continuous, it implies that $\psi^{-1}(P\hat{A}_I) = P$ is closed in A.

Suppose $I \not\subseteq P$ for some maximal P of A. Then, $I^n + P = A$ $\forall n > 0$ (because P maximal)

But $I^n + P = A$ $\forall n > 0$ says that P is not closed $\Rightarrow$!!
(because $1 = p + x$, $x \in I^n$ for some $n \Rightarrow$ every small nbh touches P !)

//

Proposition: If A is semilocal (i.e. if $m\text{-Spec} = \{\mathfrak{m}_1, \dots, \mathfrak{m}_r\}$), and $I := \mathrm{Jrad}(A) = \mathfrak{m}_1 \cap \dots \cap \mathfrak{m}_r$ $(= \mathfrak{m}_1 \cdots \mathfrak{m}_r)$. Then:

$\to \hat{A}_I \cong \hat{A}_1 \times \dots \times \hat{A}_r$, where $\hat{A}_i = \widehat{(A_{\mathfrak{m}_i})}_{\mathfrak{m}_i}$.

Example: $\mathbb{Z}$. $S = \mathbb{Z} - (p_1) \cup \dots \cup (p_r)$. $\mathbb{Z}_S$ is a semilocal ring, with maximals $p_i \mathbb{Z}_S$.

Then $(\hat{\mathbb{Z}_S})_I = \hat{\mathbb{Z}}_{p_1} \times \dots \times \hat{\mathbb{Z}}_{p_r}$. $(I = p_1 \cdots p_r)$.

Pf Note that $\mathfrak{m}_i^n + \mathfrak{m}_j^n = A$ for $i \neq j$, $n > 0$. (distinct maximals).

$$A/I^n = A/\mathfrak{m}_1^n \cdots \mathfrak{m}_r^n \simeq A/\mathfrak{m}_1^n \times \dots \times A/\mathfrak{m}_r^n$$

Taking inverse limits,

$$\varprojlim A/I^n = \prod_i \varprojlim A/\mathfrak{m}_i^n = \hat{A}_{\mathfrak{m}_1} \times \dots \times \hat{A}_{\mathfrak{m}_r}$$

But note that

$$A/\mathfrak{m}_i^n = (A/\mathfrak{m}_i^n)_{\mathfrak{m}_i} = A_{\mathfrak{m}_i}/\mathfrak{m}_i^n A_{\mathfrak{m}_i}, \text{ so } \varprojlim A/\mathfrak{m}_i^n = \varprojlim \left(A_{\mathfrak{m}_i}/\mathfrak{m}_i^n A_{\mathfrak{m}_i}\right) = \hat{A}_i.$$

Valuation Rings.

Let R be a domain, $K = k(R)$ its fraction field.

Def R is a valuation ring if $x \in K - R \Rightarrow x^{-1} \in R$.

Let $G := \{xR : x \in K - \{0\}\} \cong K^\times/R^\times$ ← group quotient (with additive notation: $[xR] + [yR] = [xyR]$).

Def G is called the value group of R.

Def An abelian group G is a totally ~~ordered~~ group if it has $\leq$, a total order relation, and if $x \leq y$, $a \leq b$ then $x + a \leq y + b$.

Given $x, y \in K \setminus \{0\}$, then either $\frac{x}{y} \in R$ or $\frac{y}{x} \in R$.

$\frac{x}{y} \in R \Rightarrow xR = \frac{x}{y} yR \subseteq yR$ (and $\frac{y}{x} \in R \Rightarrow yR \subseteq xR$)

So it defines an ordering $\Rightarrow$ G is a totally ordered group.

Write $v : K \to G \cup \{\infty\}$ for

$$x \longmapsto \begin{cases} [xR] & \text{if } x \neq 0 \\ \infty & \text{if } x = 0 \end{cases}.$$

The order we give is backwards: $xR \subseteq yR$, then say that $[xR] \geq [yR]$.

The function $v : K \to G \cup \{\infty\}$ satisfies:

(1) $v(xy) = v(x) + v(y)$ $\quad \forall x, y \in K$

(2) $v(x+y) \geq \min\{v(x), v(y)\}$ $\quad \forall x, y \in K$.

(3) $v(x) = \infty$ iff $x = 0$

Def: Such a v is called a <u>valuation on K.</u>

More generally, given $v : K \to H \cup \{\infty\}$ a valuation, where H is a totally ordered ~~addition~~ group, can define

$$R_v := \{x \in K \mid v(x) \geq 0\}$$, and R_v is a valuation ring.

<u>Exercise</u>: prove this.

In such a case, the value group is $v(K^\times) \subseteq H$.

<u>Rk</u>: given an integral domain R and an ordered group H, and a function $v : R \to H \cup \{\infty\}$ satisfying (1), (2), (3), then there is a unique extension to $v : K \to H \cup \{\infty\}$, which is a valuation.

(by $v(\frac{x}{y}) := v(x) - v(y)$, and using $\frac{x}{y} + \frac{x'}{y'} = \frac{xy' + x'y}{yy'}$).

Example: $R = \mathbb{Z}$. $v(n) = \#$ of powers of p in n (p-adic valuation, v_p).

$\mathbb{Z}_{v_p} = \mathbb{Z}_{(p)}$ is bigger than $\mathbb{Z}$!!

Example: $R = k[X]$. $f(X)$ an irreducible monic polynomial.

$v_f(g) = \#$ of factors of f in g.

$v_f : k(X) \longrightarrow \mathbb{Z} \cup \{\infty\}$. and $R_{v_f} = \cancel{k[X]}\ k[X]_{(f(X))}$

Let R be a valuation ring, $v : K \to G \cup \{\infty\}$ a valuation.

Given $I \subseteq R$, $I = \bigcup_{x \in I} xR \Leftrightarrow$ a half-interval in G (in fact, in $[0, \infty) \subseteq G$).

More generally, any R-submodule $I \subseteq K \Leftrightarrow$ half intervals of G (of all G, or $[\infty]$)

Let $m_R = \bigcup_{v(x) > 0} xR$ is the unique maximal ideal of R.

Corollary: Valuation rings are local rings.

Example: $R = k[X, Y]$, $K = k(X, Y)$.

Define $v : R^\times \longrightarrow \mathbb{R} \cup \{\infty\}$ by (fix $\alpha > 0, \alpha \in \mathbb{R}$)

$$v\Big(\sum_{i,j \geq 0} c_{i,j} X^i Y^j\Big) := \begin{cases} m + \alpha n = \min\{i + \alpha j : c_{i,j} \neq 0\}. \\ 0 \quad \text{for the zero-poly.} \end{cases}$$

Suppose that α is irrational.

$$R_v = \{\tfrac{f}{g} \in K \mid v(f) \geq v(g)\} \cup \{0\}.$$

Claim: $R_v / m_{R_v} \simeq k$ (if α is irrational)

Pf

$\varphi : R_v \longrightarrow k$

$$f/g \longmapsto \begin{cases} 0 \text{ if } v(f/g) > 0 \\ \frac{c_{m,n}}{d_{m,n}} \text{ if } v(f) = v(g) = m + \alpha n \end{cases}$$ (check that, as α is irrational, there's a unique)

Check that φ defines a ring hom, and it is exhaustive. //

In particular, if $k = \mathbb{R}$,

$$\lim_{t\to 0} \frac{f(t^{*},t^{\alpha})}{g(t^{*},t^{\alpha})} = \varphi\left(\frac{f}{g}\right) \quad \leftarrow \text{well defined only if } \alpha \notin \mathbb{Q}.$$

What happens when α is rational: say $\alpha = 1$.

$\cancel{v\left(\frac{x}{y}\right) = v\left(\frac{-y}{x}\right) = 0, \text{ then } \lim_{t\to 0} \frac{f(t,t)}{g(t,t)}}$

Then $\frac{x}{x-y}$ does not work if plug $x = t$, $y = t^{\alpha} = t$.

In this case, $k\left(\frac{x}{y}, \frac{y}{x}\right) \subseteq R_v$, $k\left(x/y\right) \subseteq R_v/m$ //

Prop: Valuation rings are integrally closed.

Pf R, $K = K(R)$.

Suppose $x \in K \setminus R$. want to show that x is <u>not</u> integral over R.

if $x \in K - R$, $\frac{1}{x} \in R$. In fact, $v: R \to G \cup \{\infty\}$ is the valuation function, then $v(x) < 0$, $v(x^{-1}) > 0 \Rightarrow x^{-1} \in m_{R}$.

If x was integral over R, then

$$\exists\, a_i \in R: \quad a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + x^n = 0$$

Multiplying by x^{-n}, $0 = \underbrace{a_0 x^{-n} + \cdots + a_{n-1} x^{-1}}_{\in m_R} + 1 \Rightarrow 1 \in m_R \Rightarrow$ contradiction. //

Prop: Let A be an integral domain, $K = K(A)$.

Let B the integral closure of A in K.

Then $$B = \bigcap_{\substack{A \subseteq R \\ R \text{ is a val. ring of } K}} R$$

We need first to prove a lemma:

<u>Lemma</u>: Let K be a field, $A \subseteq K$ a subring, $P \subsetneq A$ prime. Then there exists a valuation ring R of K s.t.

$m_R \cap A = P$.

Pf/ WLOG, can assume $A = A_P \subseteq K$ (a local ring).

Let $\mathcal{F} := \{$ subrings $B \subseteq K$: $A \subseteq B$, $1 \notin PB\}$.

Zorn's lemma applies on $\mathcal{F}$, to give a maximal element $R \in \mathcal{F}$.

Since $PR \neq R$, $\exists\, m \supseteq PR$, m maximal in R.

Since $R_m \in \mathcal{F}$, $R = R_m$, so R is a local ring.

Since $m \cap A \supseteq P$, then $m \cap A = P$ because A is local ring.

Only have to show that R is a valuation ring:

Let $x \in K - R$.

Consider $R[x] \subseteq K$. ($R[x] \supsetneq R$).

Also, $R[x] \notin \mathcal{F}$, so $1 \in P \cdot R[x]$.

Thus $1 = a_0 + a_1 x + \cdots + a_n x^n$ for some $a_0 \in PR \subseteq m$

$1 - a_0 \notin m$, so $1 - a_0$ is a unit. Get (dividing by $1 - a_0$)

$1 = b_1 x + \cdots + b_n x^n$ $\quad b_i \in m$.

Suppose neither x nor x^{-1} is in R.

Then $1 = b_1 x + \cdots + b_n x^n = c_1 x^{-1} + \cdots + c_m x^{-m}$ $\quad$ ($b_i, c_i \in m$). (doing the same with x^{-1}).

Choose them with smallest degrees n, m.

If $n \geq m$, then $b_n x^{n} \cdot 1 = b_n c_1 x^{n-1} + \cdots + b_n c_m x^{n-m}$

So $1 = b_1 x + \cdots + b_{n-1} x^{n-1} + (b_n c_1 x^{n-1} + \cdots + b_n c_m x^{n-m})$ get an expression for 1 in less degree, contradicting minimality.

If $n = m$, get $1 = a_0 + \cdots + a_{n-1} x^{n-1}$, $a_n \in m$ (Divide $(1-a_0)^{-1}$ to get an expr form) //

Pf of the Prop ($B = \bigcap_{\substack{R \supseteq A \\ R \text{ val. ring}}} R$).

Define $B' := \bigcap_{\substack{R \supseteq A \\ R \text{ val. ring}}} R$, B be the integral closure of A in K.

Want $B = B'$.

Have $B \subseteq B'$, because valuation rings are integrally closed.

Suppose $x \in K \setminus B$.

Let $y = x^{-1}$, and consider $A[y] \subseteq K$

$A[y] \supseteq yA[y] \not\ni 1$ (if $1 \in yA[y]$, have $0 = 1 + a_1 y + \dots + a_n y^n$, $a_i \in A$, and then $y = x^{-1} \Rightarrow 0 = x^n + a_1 x^{n-1} + \dots + a_n \Rightarrow x \in B \Rightarrow !!$).

By the Lemma, $\exists$ a valuation ring $R \subseteq K$ s.t.

- $R \supseteq A[y]$
- $m_R \supseteq yA[y]$.

So $y \in m_R \Rightarrow x^{-1} \in m_R$. So $x \notin R$! ($v(x^{-1}) > 0 \Rightarrow v(x) < 0 \Rightarrow x \notin R$). //

Given G an ordered abelian group,

Def G is Archimedean if, for $x, y \in G$, $x > 0$, there is $n \in \mathbb{N}$ s.t. $nx > y$.

pf. in Mats.

(Equivalently, there is an embedding $G \hookrightarrow \mathbb{R}$ as an ordered group)

Prop: Let R be a val. ring with value group $G \neq 0$. Then G Archimedean $\Leftrightarrow \dim R = 1$ (Krull dimension).

($G = 0 \Leftrightarrow \dim R = 0$ (i.e. $R = K$))

Pf $\Rightarrow$] To show $\dim R = 1$, only need to show that $\{(0), m\}$ are the only primes in R.

Let $P \subseteq R$ prime, $P \neq 0$.

Pick $y \in P$, $y \neq 0$. Let $x \in m$, $x \neq 0$. ($v(x) = a > 0$, $v(y) = b > 0$).

$\exists n$ s.t. $an > b \Rightarrow v\left(\frac{x^n}{y}\right) > 0 \Rightarrow \frac{x^n}{y} \in R \Rightarrow x^n \in yR \subseteq P \Rightarrow x \in P \Rightarrow \checkmark$

$\Leftarrow$] Let $y \neq 0$, $y \in m$, $\sqrt{yR} = m$. So $x \in m, x \neq 0$, $\exists n$ s.t. $x^n \in yR \Rightarrow \frac{x^n}{y} \in R \Rightarrow v\left(\frac{x^n}{y}\right) \geq 0 \Rightarrow n v(x) \geq y$ //

Def: A <u>discrete valuation ring</u> (DVR) is a valuation ring with value group $\simeq \mathbb{Z}$.

Prop: If R is a valuation ring, TFAE:

(1) R is a DVR.

(2) R is a PID.

(3) R is Noetherian.

~~Pf~~

<u>(1) ⇒ (2)</u>:

Since $\mathbb{Z}$ is discrete, every ideal is principal.

<u>(2) ⇒ (3)</u>: trivial

<u>(3) ⇒ (1)</u>:

Let $I = a_1R + \dots + a_rR$

Since R is a valuation ring, there is some i s.t

$$a_iR \supseteq a_jR \quad \forall j = 1..r$$

So $I = a_iR$. In particular, R is a PID (so (3)⇒(2)).

~~Pick any element~~ $m_R = xR$ for some $x \in m_R$.

$\bigcap_{n \geq 0} m^n = 0$ by Krull intersection thm. (R is a Noetherian Domain).

Given $0 \neq y \in R$, $\exists$ largest n s.t $y \in x^nR = m^n$

Consider yR. $yR \subseteq m^n$, so $y = ux^n$ for some $u \in R$.

It must have $u \notin m$ (if not, n is not the largest).

So v is a unit. so $yR = (\frac{y}{u})R = x^nR = m^n$.

So $G_{\geq 0} = \mathbb{N}$.

In a DVR,

<u>Def</u>: Any generator of m, is called a <u>uniformizer</u>.

So any $y \in R$ can be <u>uniquely</u> as $y = u x^n$, for some $n \geq 0$, $u \in R^\times$.

<u>Theorem</u>: TFAE:

1) R is a DVR.

2) R is a local PID, not a field.

3) R is a Noetherian local ring, $\dim R > 0$, m_R principal.

4) R is a 1-dimensional integrally closed Noetherian local domain.

Pf/ (1) ⇒ (2) already done.

(2) ⇒ (3) clear.

(3) ⇒ (1).

Let $m_R = xR$.

If x was nilpotent, $m_R = \sqrt{0} \Rightarrow m_R$ is only prime ideal ⇒ !! $\dim R > 0$.

Thus x is not nilpotent.

$xR = m_R = \mathrm{Jrad}(R)$, so:

By Krull intersection, $\bigcap_{n \geq 0} m^n = 0$ (R Noeth, $m \subseteq \mathrm{Jrad}(R)$)

If $y \in R$, $y \neq 0 \Rightarrow \exists!\, n$ s.t. $y \in m^n \setminus m^{n+1}$

So $y = u x^n$ for some $u \in R$. $u \in m \Rightarrow y \in m^{n+1} \Rightarrow !! \Rightarrow u \notin m \Rightarrow$

$\Rightarrow u$ is a unit.

Also, R is an integral domain: $(u x^n)(v x^m) = uv\, x^{n+m} \neq 0$ since x not nilpotent.

So a general element of $K = K(R)$ has the form $u x^n$, $u \in R^\times$, $n \in \mathbb{Z}$.

So either $u x^n \in R$ or $u^{-1} x^{-n} \in R \Rightarrow$ valuation ring.

↓

(cont proof)

Need to prove $1 \Leftrightarrow 4$ (R DVR $\Rightarrow R$ is a 1-dim integrally closed Noetherian Local Dom.)

$\Rightarrow$) clear.

$\Leftarrow$) Consider $m_R \subseteq R$, $K = K(R)$. We will prove $4 \Rightarrow 3$ (that m_R is principal).

Claim. $\exists$ an R-submodule, $m^{-1} \subseteq K$ such that $m \cdot m^{-1} = R$

Given the claim, then:

$m \neq m^2$ (if $m = m^2$, then $m^2 \cdot m^{-1} = R \Rightarrow mR = R \Rightarrow !!$).

Pick $x \in m \setminus m^2$:

$x m^{-1} \subseteq m m^{-1} \subseteq R$ so $x m^{-1}$ is an ideal in R.

So either $x m^{-1} = R$ or it is proper (if it's proper, it is contained in m)

if $x m^{-1} \subseteq m$, then $xR \subseteq m^2 \Rightarrow x \in m^2 \Rightarrow !!$

So $x m^{-1} = R$ and thus $x m^{-1} m = mR \Rightarrow (x) = m$. //

<u>Pf of the claim</u>:

Let $m^{-1} := \{ b \in K : mb \subseteq R \} = (R : m)_K$

Clearly, $R \subseteq m^{-1}$

Want $R \neq m^{-1}$:

Pick $x \in m \setminus m^2$ ($m \neq m^2$ by Nakayama (m is finitely generated!)).

Consider $\mathrm{Ass}_R(R/xR)$.

The element $x^{\in R}$ is a 0-divisor for R/xR. So $x \in P$, some associated prime.

~~So therefore~~ But $\dim R = 1$, so $P = m$.

So $m = (xR : yR)_R$ for some $y \in R$. ($m = \mathrm{ann}_{R/xR}(y)$)

Let $a = yx^{-1} \in K$. So $a \notin R$ ($a \in R \Rightarrow y \in xR \Rightarrow m = R \Rightarrow !!$).

Also, $a \in m^{-1}$: $am = yx^{-1}m = x^{-1} y m \subseteq x^{-1}(xR) = R$.

Now, knowing $m m^{-1} \subseteq R$ and that $R \subsetneq m^{-1}$. Suppose $m = m m^{-1}$. Then $am \subseteq m$

So multiplication-by-a gives $\varphi : m \to m$, $b \mapsto ab$, a R-module hom.

So, as m is finitely-generated, by CHT gives:

a monic polynomial over R satisfied by φ (ie by $a \in K$).

Since R is integrally closed $\Rightarrow a \in R$. $\Rightarrow$!!

So $m \neq m\, m^{-1}$.

We deduce, as $m m^{-1} \supseteq m$ and $m m^{-1} \neq m \Rightarrow m m^{-1} = R$ $\Rightarrow$ proves the claim

Let R be an integral domain.

<u>Def</u>: A <u>fractional ideal</u> is a non-zero R-submodule $I \subseteq K$ s.t.

$\exists\, \alpha \neq 0$, $\alpha \in K$ s.t. $\alpha I \subseteq R$.

<u>Note</u>: As R-modules, $I \simeq \alpha I$. So R noetherian $\Rightarrow$ all fractional ideals are finitely generated.

<u>Example</u>: if $\beta \in K$, $I = R\beta \subseteq K$ is a fractional ideal.

<u>Def</u>: $I \subseteq K$ a fractional ideal is <u>invertible</u> if, for

$I^{-1} := \{ \alpha \in K : \alpha I \subseteq R \} = (R : I)_K$, $\leftarrow$ a fractional ideal.

the module $I I^{-1} = R$.

<u>Rk</u>: If R is a DVR, then all fractional ideals are Rx^n, $n \in \mathbb{Z}$,

So they are all invertible.

Prop: Let R be a domain, $K = k(R)$, $I \subseteq K$ a fractional ideal. TFAE:

1) I is invertible (finitely generated).
2) I is a projective R-module (finitely generated)
3) I is f.gen $/R$ and $I_P = IR_P \subseteq K$ is a <u>principal</u> R_P-module for each <u>maximal ideal</u> $P \subseteq R$. (i.e. I is locally free of rank-1).

~~Pf~~

<u>(1)⇒(2)</u>:

$II^{-1} = R$.

So $1 = \sum_{i=1}^{n} a_i b_i$ for some $a_i \in I$, $b_i \in I^{-1}$.

Let $F = \bigoplus_{i=1}^{n} Re_i$ a free-rank-n module.

Define $\varphi : F \to I$
$e_i \mapsto a_i$

<u>claim</u>: φ is surjective: i.e. $I = Ra_1 + \cdots + Ra_n$.

$\left(x \in I \Rightarrow 1 \cdot x = \sum a_i \underbrace{b_i x}_{\in R} \right)$

Define $\psi : I \to F$ and note $\varphi \circ \psi(x) = \sum b_i x a_i = 1 \cdot x = x$.
$x \mapsto \sum_{i=1}^{n} (b_i x) e_i$

So I is a retract of F.

(Notice also that we proved that I is finitely generated).

<u>Note</u>: also shown that $I^{-1} = \sum Rb_i$ (possibly not free).

(cont pf)

$2 \Rightarrow 1$: Assume I is projective fractional.

Claim: $I^{-1} \simeq Hom_R(I,R)$

(Clear if $I = R\alpha$ for some $\alpha \in K, \alpha \neq 0$).

In general, if I is fractional, need to show that any hom $I \to R$ is given by multiplication by some $\beta \in K$ (β unique).

($I = \sum R\alpha_i$ sum of principal fractional ideals,

given $\varphi: I \to R$, $\exists$ unique $\beta_i \in K$ s.t. $\varphi|_{R\alpha_i}$ is mult by β_i).

Need to show that those β_i are all the same.

It is enough to show that any $R\alpha_i \cap R\alpha_j \neq \phi$.

Since I is fractional, can replace it by the ideal $\alpha I \subseteq R$ (ideal).

And in domain, for any two nonzero ideals $J_1, J_2 \subseteq R$, $J_1 \cap J_2 \supseteq J_1 J_2 \neq \phi$.

Now, since I is projective, $\exists$ a free module F and hom's

$$I \xrightarrow{\psi} F \xrightarrow{\varphi} I \quad \text{s.t. } \varphi \circ \psi = id.$$

Write $F = \bigoplus Re_i$ (possibly infinite).

Write $\psi(x) = \sum \psi_i(x) e_i$ (the sum is finite, for any x).

Since $\psi_i \in Hom_R(I,R) \simeq I^{-1}$, let $b_i \in I^{-1}$ s.t. $\psi_i(x) = b_i x$

$\Rightarrow$ almost all b_i are 0.

Set $a_i = \varphi(e_i) \in I$.

~~Then $\sum a_i b_i$~~ = Now $\varphi\psi(x) = \sum \psi_i(x) e_i = \varphi\left(\sum (b_i x) e_i\right) = \sum (b_i x) a_i =$

$$= \left(\sum a_i b_i\right) x$$

Since $\varphi\psi = id$, have $\sum a_i b_i = 1$ (since everything inside K, a field).

This shows that $I^{-1} I \ni 1 \Rightarrow I$ is invertible.

(cont proof of equivalence).

1 ⇒ 3:

The proof already given shows that I is finitely-generated.

Let $a_1, \dots, a_n \in I$ be a generating set.

Let $b_1, \dots, b_n \in I^{-1}$ s.t. $1 = \sum \underbrace{a_i b_i}_{\in R}$.

In $R_\mathfrak{p}$, since $1 = \sum a_i b_i \in R_\mathfrak{p}$, $\exists i$ s.t. $a_i b_i \notin \mathfrak{p} R_\mathfrak{p}$

(i.e. $a_i b_i$ is a unit in $R_\mathfrak{p}$).

$$I_\mathfrak{p} = (a_i b_i) I_\mathfrak{p} = a_i (b_i I_\mathfrak{p}) = a_i b_i I R_\mathfrak{p} \subseteq a_i R R_\mathfrak{p} = a_i R_\mathfrak{p} \subseteq I_\mathfrak{p}.$$

So $I_\mathfrak{p} = a_i R_\mathfrak{p}$ (as $R_\mathfrak{p}$ as a module) as a submodule of K. //

3 ⇒ 1:

Let $I \subseteq K$ be a f.gen. fractional ideal, with $I_\mathfrak{p}$ principal $\forall \mathfrak{p}$.

Claim: $(I^{-1})_\mathfrak{p} = (I_\mathfrak{p})^{-1}$:

$\Rightarrow$ $(I^{-1})_\mathfrak{p} \subseteq (I_\mathfrak{p})^{-1}$ clear (think about it, need only that $I^{-1} \subseteq (I_\mathfrak{p})^{-1}$ (and then, locality is preserving because $(I_\mathfrak{p})^{-1}$ is an $R_\mathfrak{p}$-mod)

$\Leftarrow$ $(I_\mathfrak{p})^{-1} \subseteq (I^{-1})_\mathfrak{p}$

Suppose $I = a_1 R + \dots + a_n R$, $a_1, \dots, a_n \in K$. $(I_\mathfrak{p} = a_1 R_\mathfrak{p} + \dots + a_n R_\mathfrak{p})$.

If $x \in (I_\mathfrak{p})^{-1}$ $x \cdot a_i \in R_\mathfrak{p}$ $\forall i$

So $\exists c_i \in R \setminus \mathfrak{p}$ s.t. $x a_i c_i \in R$ $\forall i$

Let $c = c_1 \cdots c_n \in R \setminus \mathfrak{p}$ then $x a_i c \in R$ $\forall i$

So $cx \in I^{-1}$. Then $x \in (I^{-1})_\mathfrak{p}$ since $c \in R \setminus \mathfrak{p}$ $(\Rightarrow (I^{-1})_\mathfrak{p} = (I_\mathfrak{p})^{-1})$ //

Now suppose $I I^{-1} \neq R$. Consider a maximal $\mathfrak{p}$ s.t. $\mathfrak{p} \supseteq I I^{-1}$.

then $(I^{-1})_\mathfrak{p} I_\mathfrak{p} \subseteq \mathfrak{p} R_\mathfrak{p}$ $\quad (\mathfrak{p} R_\mathfrak{p} \supseteq (I^{-1} I)_\mathfrak{p} = (I^{-1})_\mathfrak{p} I_\mathfrak{p})$.

And by the claim, $(I_\mathfrak{p})^{-1} I_\mathfrak{p} \subseteq \mathfrak{p} R_\mathfrak{p}$. Since $I_\mathfrak{p}$ is principal, $(I_\mathfrak{p})^{-1} I_\mathfrak{p} = R_\mathfrak{p}$, (principal ⇒ invertible)

⇒ contradiction //.

Invertible Modules

Let R be a ring.

Def An R-module M is <u>invertible</u> if it is finitely-presented and $M_{\mathfrak{p}} \simeq R_{\mathfrak{p}}$ as an $R_{\mathfrak{p}}$-module, for each maximal ideal $\mathfrak{p}$.

Define then $M^* := \hom_R(M, R)$. and
$$\mu : M^* \otimes M \to R$$
$$(\varphi \otimes m) \longmapsto \varphi(m)$$

<u>Prop</u>: A module M is invertible iff μ is an isomorphism.

Furthermore, if M is invertible, then M and M^* are projective modules.

(notice that $(M^*)_{\mathfrak{p}} \simeq (M_{\mathfrak{p}})^*$, because $\hom_R(M,R)_{\mathfrak{p}} \simeq \hom_{R_{\mathfrak{p}}}(M_{\mathfrak{p}}, R_{\mathfrak{p}})$)

Pf $\Rightarrow$) Suppose M invertible. $\left[M^* \otimes_R M \xrightarrow{\mu} R\right]_{\mathfrak{p}} = \left[(M^*)_{\mathfrak{p}} \otimes_{R_{\mathfrak{p}}} M_{\mathfrak{p}} \to R_{\mathfrak{p}}\right] =$

$= \left[(M_{\mathfrak{p}})^* \otimes_{R_{\mathfrak{p}}} M_{\mathfrak{p}} \to R_{\mathfrak{p}}\right]$.

Since $M_{\mathfrak{p}} \simeq R_{\mathfrak{p}}$, $(M_{\mathfrak{p}})^* \simeq \hom_{R_{\mathfrak{p}}}(R_{\mathfrak{p}}, R_{\mathfrak{p}}) \simeq R_{\mathfrak{p}}{}^*$.

And then $R_{\mathfrak{p}} \otimes_{R_{\mathfrak{p}}} R_{\mathfrak{p}} \to R_{\mathfrak{p}}$ is iso. //

$\Leftarrow$) Given $\mu : M^* \otimes_R M \to R$ iso.

<u>Note</u>: $(M^*)_{\mathfrak{p}} \longrightarrow (M_{\mathfrak{p}})^* = \hom_{R_{\mathfrak{p}}}(M_{\mathfrak{p}}, R_{\mathfrak{p}})$ is not necessarily an iso.

Write $1 = \mu\left(\sum \varphi_i \otimes m_i\right) = \sum \varphi_i(m_i)$ (in R).

After localizing at $\mathfrak{p}$, get $\exists\, i$ s.t. $\overbrace{\varphi_i(m_i)}^{c} \in R \setminus \mathfrak{p}$

Let $x = c^{-1} m_i \in M_{\mathfrak{p}}$. Let $\varphi = \varphi_i$

$$\begin{tikzcd} R_{\mathfrak{p}} \arrow[r] \arrow[rr, bend left, "id"] & M_{\mathfrak{p}} \arrow[r, "\varphi"] & R_{\mathfrak{p}} \end{tikzcd} \quad \text{So} \quad R_{\mathfrak{p}} \simeq \overbrace{R_{\mathfrak{p}} x}^{\simeq R_{\mathfrak{p}}} \oplus \ker\varphi$$
$$1 \longmapsto x$$

Similarly, $R_{\mathfrak{p}} \to (M^*)_{\mathfrak{p}} \xrightarrow{ev_x} R_{\mathfrak{p}}$ So $(M^*)_{\mathfrak{p}} \simeq \overbrace{R_{\mathfrak{p}} \varphi}^{\simeq R_{\mathfrak{p}}} \oplus \ker(ev_x)$
$$1 \longmapsto \varphi \qquad x \longmapsto 1$$

$\Rightarrow (R_{\mathfrak{p}}\varphi \oplus \ker ev) \otimes (R_{\mathfrak{p}} x \oplus \ker\varphi)$
$\Rightarrow \ker\varphi = 0$
$\Rightarrow \varphi : M_{\mathfrak{p}} \to R_{\mathfrak{p}}$ is an iso.
Thus $M_{\mathfrak{p}} \simeq R_{\mathfrak{p}}$.

(cont proof)

We need to show that M is finitely presented.

Recall: $1 = \sum_{i=1}^{r} \varphi_i(m_i)$, $\varphi_i \in M^*$, $m_i \in M$, and that at least one of the m_i's was a generator for M_p.

So $m_1, \dots, m_r$ generate M as an R-module (local generators $\Rightarrow$ global gen).

So M is finitely generated - but need finitely presented! (if M noetherian, done).

We will show that M is projective. Then proj + fin gen $\Rightarrow$ fin. pres.

Let $\mathcal{C}$ be the category of R-modules.

Define two functors: $F : \mathcal{C} \to \mathcal{C}$, $F(N) = M \otimes_R N$.

$G : \mathcal{C} \to \mathcal{C}$, $G(N) = M^* \otimes_R N$.

Then $GF(N) = M^* \otimes (M \otimes N) \simeq (M^* \otimes M) \otimes N \xrightarrow[\simeq]{M \otimes id_N} R \otimes N = N$

So $GF \simeq$ id. functor.

Also, $FG \simeq (M \otimes M^*) \otimes N \simeq (M^* \otimes M) \otimes N \xrightarrow{\simeq} R \otimes N \simeq N$

So $FG \simeq$ id. functor.

And hence F and G are self-equivalences of $\mathcal{C}$.

So $\hom_R(N, N') \xrightarrow{\simeq} \hom_R(GN, GN')$.

So $\hom_R(M, N) \simeq \hom_R(M^* \otimes M, M^* \otimes N) = \hom(R, M^* \otimes N) \simeq M^* \otimes N$

Thus $\hom_R(M, -) \simeq M^* \otimes_R (-)$ (isomorphic as functors).

(tensoring is right-exact, so $\hom_R(M, -)$ is right exact, so M is projective.

Since M is projective, $R^n = M \oplus N$.

So $(R^n)^* \simeq M^* \oplus N^*$ $\leftarrow$ M^* is f.-gen proj $\Rightarrow$ f. pres.

$\hom(R^n, R) \cong R^n$ (not canonical)

So can do $(M^*)_{\mathfrak{p}} \simeq (M_{\mathfrak{p}})^* \simeq (R_{\mathfrak{p}})^* \simeq R_{\mathfrak{p}}$ (since M is invertible).

So M^* is invertible. //

Prop: R be a Noetherian domain. M is an invertible module iff M isom. to an invertible fractional ideal.

Noetherian ← true without this, but don't need it.

Pf $\Leftarrow$) If $I \subseteq K$ is invertible fractional ideal, recall $I^{-1} = I^*$.

We showed that I is a finitely-gen. R-module, so I is f. presented and $I_{\mathfrak{p}}$ is a principal frac. ideal, so $\simeq R_{\mathfrak{p}}$.

$\Rightarrow$) Let M be an invertible module.

Let $\varphi \in M^*$, $\varphi \neq 0$. $\varphi : M \to R$.

Claim: φ is injective (and so M is isom. to an ideal I).

Pf Let $\mathfrak{p}$ be a prime, consider $\varphi_{\mathfrak{p}} : \underset{\underset{R_{\mathfrak{p}}}{\wr\wr}}{M_{\mathfrak{p}}} \to R_{\mathfrak{p}}$.

So $\varphi_{\mathfrak{p}}$ is either 0 map or injective. So need only to show that $\varphi_{\mathfrak{p}} \neq 0$ $\forall \mathfrak{p}$.

$$\underset{\varphi}{\overset{\in}{M^*}} \longrightarrow (M^*)_{\mathfrak{p}} \simeq \underbrace{(M_{\mathfrak{p}})^*}_{\ni \varphi_{\mathfrak{p}}}$$

M^* invertible, so projective.

$F \simeq M^* \oplus N$ and $F \to F_{\mathfrak{p}}$ is injective $\forall \mathfrak{p}$ (since R is a domain)

So $M^* \to M^*_{\mathfrak{p}}$ is injective, so $\varphi_{\mathfrak{p}}$ is injective. $\Rightarrow \varphi$ injective.

Since $M \simeq I$, I is an invertible module, so

$I^* \otimes I \longrightarrow R$ is an isomorphism, and $I^* \simeq I^{-1}$

$\overset{\wr\wr}{I^{-1} \otimes I}$ ↗ So multiplication has to be surjective. So $I^{-1} I = R$ //

If R is a ring, noetherian, define:

$$\mathrm{Pic}(R) = \left\{ \begin{matrix} \text{invertible} \\ R\text{-modules} \end{matrix} \right\} \Big/ \text{isomorphism},$$ the Picard group. (Abelian gp).

The group structure is given by tensor products:

$$(M, N) \longmapsto M \otimes_R N$$

Inverses are given ~~as~~ $M \mapsto M^*$, (identity $= R$)

If R is a Noetherian domain,

then $\mathscr{C}(R) := \left\{ \begin{matrix} \text{invertible fractional} \\ \text{ideals in } K \end{matrix} \right\}$. (Cartier Divisors).

It is an abelian group for multiplication: $(I, J) \subset K \mapsto I \cdot J \subseteq K$.

$$(IJ)^{-1} \supseteq I^{-1} J^{-1}.$$

So $(IJ)^{-1} \cdot (IJ) \supseteq I^{-1} J^{-1} I J = R$ if I, J are invertible, so

$(IJ)^{-1}(IJ) = R$.

So have an isomorphism of groups, which is surjective: $C(R) \twoheadrightarrow \mathrm{Pic}(R) \to 0$

Observe that get the exact sequence:

$$0 \to K^\times / R^\times \to C(R) \to \mathrm{Pic}(R) \to 0$$

$\uparrow$ principal Cartier divisors (= principals fractional ideals).

<u>Remark</u>. The group $\mathscr{C}(R)$ is generated by invertible "true" ideals.

Every element in $\mathscr{C}(R)$ is $\alpha^{-1} I = (\alpha R)^{-1} I$ where

I is an invertible honest ideal, $\alpha \in R^\times$.

- Invertible primes

Prop: Let R a Noetherian domain, $P \neq 0$ prime. Then,

P invertible $\Rightarrow ht(P) = 1$ and R_P is a DVR.

Pf/ P invertible $\Rightarrow PR_P$ is principal in R_P.

So, as R_P is a Noeth. local domain, $\dim R_P > 0$ and PR_P is principal, so R_P is a DVR (this is one of the characterizations we had).

$ht_R(P) = ht_{R_P}(PR_P) = 1$ because R_P is a DVR. //

Prop: Let R be an integrally closed domain (Mats. says Normal).

1) Then all prime divisors of nonzero principal ideals have $ht = 1$,

2) and $R = \bigcap_{ht P = 1} R_P$

Pf/ (1) $\overset{0}{\underset{a}{\neq}}R \subseteq R$.

$\{P_1, \dots, P_r\} = Ass_R(R/aR)$

prime divisors.

So need to show that $ht(P_i) = 1$.

Pick $P \in Ass_R(R/aR)$.

Then $P = ann_{R/aR}(b) = (aR : bR)_R$

Let $m = PR_P$, then $(aR_P : bR_P)_{R_P} = PR_P = m$

Claim: $ba^{-1} \in m^{-1}$: $ba^{-1}m \subseteq a^{-1} \cdot (aR_P) = R_P$

$\cdot ba^{-1} \notin R_P$: if $ba^{-1} \in R$, then $b \cdot 1 = ba^{-1} \cdot a \subseteq aR_P \Rightarrow 1 \in m \Rightarrow !!$

If ~~$ba^{-1} \in m$, then~~ $ba^{-1}m \subseteq m$ then by CHT ba^{-1} is integral over R_P

But R_P integrally closed, so $ba^{-1} \in R_P \Rightarrow !!$

Thus $ba^{-1}m = R_P$. so $m^{-1}m \supseteq ba^{-1}m = R$, so m is invertible.

Since R_p is Noetherian domain m invertible $\Rightarrow m$ has $ht = 1$.
But m is pR_p, so $ht_R P = 1$.

(2) Claim: $a, b \in R$, $a \neq 0$, $b \in aR_p$ for all ht 1 primes P, then $b \in aR$ $\quad [\frac{b}{a} \in \bigcap_{ht 1} R_p \Rightarrow b/a \in R]$.

Pf/ $Ass(R/aR) = \{p_1, \dots, p_n\}$.

So $aR = q_1 \cap \dots \cap q_n$, where q_i is p_i-primary.

$ht\, p_i = 1$ by part (1),

Note that $0 \notin Ass(A/aR)$, so the p_i are minimal associated (because they have ht 1)

So $q_i = aR_{p_i} \cap R$.

So if $b \in aR_{p_i} \Rightarrow b \in q_i \ \forall i \Rightarrow b \in \bigcap q_i = (\bigcap aR_{p_i}) \cap R$ //

Theorem: Let R be a domain. TFAE:

(1) R is Dedekind

(2) R is Noetherian and, for each nonzero prime P, R_P is a DVR.

(3) R is Noetherian, integrally closed of dim ≤ 1.

If these hold, then every nonzero ideal $I \subseteq R$ has a unique factorization as a product of prime ideals

Def: A domain R is Dedekind if every nonzero ideal is invertible.

Pf: $1 \Rightarrow 2$: Since invertible ideals are fin-gen $\Rightarrow R$ is Noetherian.

If $p \neq 0$, we proved that if p is invertible then R_p is a DVR, so done //

$2 \Rightarrow 3$: is dim ≤ 1 because for $ht\, p = 1 \ \forall p$. In general, for a domain R have $R = \bigcap_{\substack{\text{max ideals} \\ P}} R_P$. Each R_P is integrally closed, so is the intersection //

$\underline{3 \Rightarrow 2}$: For each nonzero prime $P \subseteq R$, R_P is a Noetherian 1-dim integrally-closed domain, so R_P is a DVR.

$\underline{2 \Rightarrow 1}$: Given $I \neq 0$ an ideal, I is fin-gen by Noetherianness, and $IR_P \supseteq I \Rightarrow$ $\Rightarrow IR_P \neq 0$. For a criterion we proved, it is enough to prove that IR_P is principal. Since R_P is a DVR,

$$IR_P = \pi^n R_P \text{ for } (\pi) = PR_P, \text{ so done.}$$

We still need to prove the existence and uniqueness of the factorization!

Given $I \subseteq R$ nonzero ideal, want to show it is a product of primes.

If not, then acc gives an ideal I maximal wrt "not a product of primes".

$I \neq R$ since R is an (empty) product of primes, and $I \neq$ prime.

So $\exists$ prime $P \supseteq I$. (P maximal, in fact).

$$\underbrace{I \subseteq}_{R \subseteq P^{-1}} IP^{-1} \underbrace{\subseteq}_{I \subseteq P \text{ and } P \text{ invertible}} R$$

If $IP^{-1} = I$, then $I = IP$ $\Rightarrow I_P = I_P PR_P$. By Nakayama, $I_P = 0$.

As R is a domain, $I_P = 0 \Rightarrow I = 0 \Rightarrow$ contradiction.

So $I \subsetneq IP^{-1}$ and hence IP^{-1} is a product of primes.

So $IP^{-1} = Q_1 \cdots Q_r \Rightarrow I = Q_1 \cdots Q_r \cdot P$ is a factorization $\Rightarrow\Leftarrow$!!

To prove uniqueness, given Q a nonzero prime, I a nonzero ideal,

$IR_Q = (QR_Q)^n$ for a unique $n \in \mathbb{N}$.

Write $v_Q(I) := n$

Claim: $v_Q(IJ) = v_Q(I) + v_Q(J)$ (because $IJR_Q = (IR_Q)(JR_Q)$).

Write $C^+(R)$ = set of nonzero ideals of R, an abelian monoid under mult.

and have $C^+(R) \to \prod\limits_{Q \text{ max. ideal}} \mathbb{Z}$

If $P \subseteq R$ is prime, then $v_Q(P) = \begin{cases} 1 & \text{if } P = Q \\ 0 & \text{if } P \neq Q \end{cases}$. So we are done.

As a conclusion, we get also:

For R a Dedekind domain, then $\overset{\text{cartier divisors}}{C^{\bullet}(R)} \simeq \prod_{\text{m-Spec}(R) = \text{Spec}(R) \setminus \{0\}} \mathbb{Z}$.

It is also true, but we will not prove, that if a domain has the property of Unique Factorization, then it is a Dedekind Domain.

Examples:

1) $R = \mathbb{Z}[\sqrt{m}]$, m squarefree, $m \not\equiv 1\ (4)$.

For $m = -5$,

$$\begin{array}{cc} \mathbb{Z}[\sqrt{-5}] & P \\ | & | \\ \mathbb{Z} & (p) \end{array}$$

For $P = (2, 1+\sqrt{-5})$, $R/P = \mathbb{Z}/2\mathbb{Z}$

P is not principal, but of course invertible.
can check it.

~~So the primes in R are:~~

~~• Over 2:~~

In fact $C(R) \to \operatorname{Pic}(R) \to 0$

$\operatorname{Pic}(R) \cong \mathbb{Z}/2\mathbb{Z}$ ← Class group.

and $P = (2, 1+\sqrt{-5})$ is a representative of the nonzero class of $\operatorname{Pic}(R)$.

2) $R = \mathbb{Z}[\sqrt{-1}] = \mathbb{Z}[i]$ Gauss integers.

$$\begin{array}{cc} \mathbb{Z}[i] & P \\ | & | \\ \mathbb{Z} & (p) \end{array}$$

Over (2): $(1+i)$, $(1-i)$

Over p, $p \equiv 3\ (4)$ $\to$ p

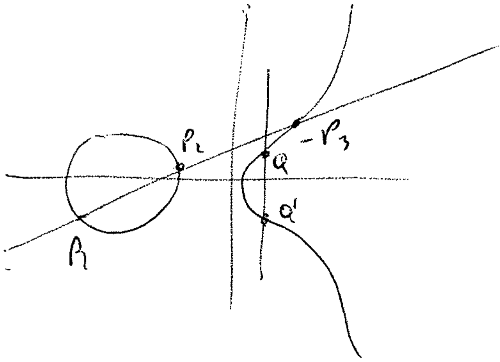
Over p, $p \equiv 1\ (4)$ $\to$ $(a+bi)$, $(a-bi)$ $\quad a, b \in \mathbb{Z}$, $a^2+b^2 = p$ (Fermat's theorem).

3) $R = \mathbb{C}[X,Y] / (\overbrace{Y^2 - (X^2-1)X}^{f(x,y)})$ (an elliptic curve).

R is a Dedekind ideal, and $\text{m-Spec}(R) \longleftrightarrow \{(a,b) \in \mathbb{C}^2 \mid f(a,b) = 0\} = V((f))$

Note that if $g \in R$, $(g) = \underbrace{Q_1 \cdots Q_r}$ ← intersection of $V((f))$ and $V((g))$ with multiplicities.

The $\operatorname{Pic}(R) = \bigoplus_{V((f))} \mathbb{Z} \Big/ \operatorname{div}((g))$



$[P_1]+[P_2] = -[P_3]$ in $\mathrm{Pic}(R)$.

$[Q]+[Q'] = 0$ in $\mathrm{Pic}(R)$

(so $[Q'] = -[Q]$.

So
$$\begin{tikzcd} \mathrm{Pic}(R) \arrow[r, phantom, "\simeq"] & X\cup\{\infty\} \arrow[dl] \\ C(R) \arrow[u, two heads] & \end{tikzcd}$$
$P \longleftrightarrow p$

- Dimension theory.

Recall: $\dim A := \sup\{r \mid A \supseteq \mathfrak{p}_0 \supsetneq \cdots \supsetneq \mathfrak{p}_r\} = \sup\{\dim A_{\mathfrak{p}}\}$ (prime ideals.)

So dimension is a local property.

Result: Let A be a Noetherian local ring, $\mathfrak{m} \subseteq A$, $k = A/\mathfrak{m}$.

Let $d = \dim_{\mathrm{Krull}}(A)$.

Also, can compute $\mathrm{length}_A(A/\mathfrak{m}^{n+1})$ (if $k \subseteq A$, length $= \dim_k(A/\mathfrak{m}^{n+1})$).

Then: $\mathrm{length}(A/\mathfrak{m}^{n+1}) \sim \mathcal{O}(n^d)$

(if A is not local, and $\mathfrak{p}$ is a maximal ideal, $\mathrm{length}\left(\underbrace{A_{\mathfrak{p}}/(\mathfrak{p}A_{\mathfrak{p}})^{n+1}}_{= A/\mathfrak{p}^{n+1}\ ::}\right)$).

In fact, $\chi(n) = \mathrm{length}(A/\mathfrak{m}^{n+1})$ is a polynomial in n (for n large).

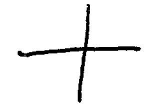
Example: $A = k[X_1, \ldots, X_r]_{(X_1,\ldots,X_r)}$, $\mathfrak{m} = (X_1, \ldots, X_n)$

$\ell(A/\mathfrak{m}^{n+1}) = \dim_k(A/\mathfrak{m}^{n+1}) = \binom{r+n}{r}$

(if $r=1$, $\dim k[X]/X^{n+1} = \binom{1+n}{1} = n+1$, for $r=2$, $\dim k[X,Y]/(X,Y)^{n+1} = \binom{2+n}{2}$).

(Convention: $\binom{u}{v} = 0$ if $u<v$).

In this case, $\ell(A/\mathfrak{m}^{n+1}) = \dfrac{(n+r)(n+r-1)\cdots(n+1)}{r!}$ for $n \geq -r$.

Example 2: $k[X,Y]_{(X,Y)}/(XY)$ $\quad m=(X,Y) \to$ 

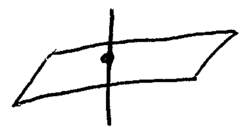
$$\begin{array}{cccccc} & X & X^2 & X^3 & \\ 1 & & & & \\ & Y & Y^2 & Y^3 & \\ n=0 & 1 & 2 & 3 & \cdots \end{array}$$

$$\dim\left(A/m^{n+1}\right) = \begin{cases} 2n+1 & \text{if } n \geq 0. \\ \cancel{2n+1 \text{ if } n \geq} \end{cases}$$

A polynomial of deg 1, so $\dim A = 1$.

In these two examples, we have $\frac{1}{1!} n^1 + \cdots$ (← 1 component) and $\frac{2}{1!} n, \cdots$ (two components)

Those numbers are called the __multiplicity__.

Example 3: $A = k[X,Y,Z]_{(X,Y,Z)}/(XZ, YZ) \longrightarrow$ 

$$\begin{array}{cccc} & X & X^2 & X^3 \\ & & & X^2Y \\ 1 & Y & XY & XY^2 \\ & & Y^2 & Y^3 \\ & Z & & \\ & & Z^2 & \\ & & & Z^3 \end{array} \cdots$$

~~Length~~. $\dim A/m^{n+1} = \binom{2+n}{2} + \binom{1+n}{1} - 1$

So $\dim_{Krull} = 2$ (degree-2 poly.)

Def A __system of parameters__ for a local ring A is a sequence $y_1, y_2, \ldots, y_d \in m$ s.t. $\ell\left(A/(y_1,\ldots,y_d)\right) < \infty$.

Result: the minimal length for a system of parameters of m is exactly $\dim A$.

(Note that in example 2, if $u = X-Y$, $\ell(A/uA) = 2 < \infty$, so $\dim A = 1$)

In example 1, we had that the maximal ideal was generated by a minimal set of parameters. This is then called a normal local ring.

- <u>Graded rings and modules.</u>

Let G be a commutative monoid $(+)$.

Def: A G-graded ring R is $R = \bigoplus_{i \in G} R_i$ s.t. $R_i \cdot R_j \subseteq R_{i+j}$

A G graded module M is $M = \bigoplus_{i \in G} M_i$ s.t. $R_i M_j \subseteq M_{i+j}$

(usually, $G = \mathbb{N}, \mathbb{Z}$).

Def: An element $x \in M$ is <u>homogeneous</u> if $\exists i \in G$ s.t. $x \in M_i$.

we write $|x| = i$ if $x \in M_i$ $(x \neq 0)$.

Def. A submodule $N \subseteq M$ is <u>homogeneous</u> if it is generated by homogeneous elements (as an abelian group).

In such a case, $N_i := N \cap M_i$, $N \simeq \bigoplus_{i \in G} N_i$.

<u>Example</u>: $R = R_0[X_1, \dots, X_n]$, R_0 a ring, $|X_i| = d_i > 0$ (degrees of polynomials).

<u>Note</u>: M_i is a R_0-module, $\forall i$. (And R_0 is a ring, always).

<u>Prop</u>: $R = \bigoplus_{n \geq 0} R_n$ is Noetherian iff $\left| \begin{array}{l} R_0 \text{ is Noetherian and } R \text{ is finitely-generated} \\ \text{as a ring over } R_0. \end{array} \right.$

Pf $(\Leftarrow)$ HBT.

$\Rightarrow)$ $R_{\geq 1} := R^+ = \bigoplus_{n > 0} R_n \subseteq R$ (an ideal (homogeneous)).

So $R_0 \simeq R/R^+$ is Noetherian.

$R^+ = x_1 R + \dots + x_r R$ (know that R^+ is f.gen)

Can take the x_i's to be homogeneous (think about it).

Consider $R_0[x_1, \dots, x_r] \subseteq R$.

The ring $R_0[x_1, \dots, x_r]$ is homogeneous ring, so will show that $R_n \subseteq R_0[x_1, \dots, x_r]$ $\forall n$.

<u>$n=0$ clear</u>. In general, since $R_n \subseteq R^+$, $R_n \overset{\text{can always write in this way}}{=} x_1 R_{n-d_1} + \dots + x_r R_{n-d_r}$ where $x_i \in R_{d_i}$

Since $R_{n-e} \subseteq R[x_1, \dots, x_r]$ by induction, we're done.

Let R be a graded Noetherian ring, M a finitely-generated R-module.
(so $\exists$ homog. elts $m_i \in M_{d_i}$ which generate).

Def: $N[d]$ is the module s.t. $N[d]_n := N_{n+d}$ (shift down by d).

We have

$$\bigoplus_{i=1}^{r} R[-d_i]\underset{\substack{\text{formal}\\ \text{generator},\ |e_i|=d_i}}{e_i} \xrightarrow{e_i \mapsto m_i} M \longrightarrow 0$$

(because $\left(\bigoplus_{i=1}^{r} R[-d_i]e_i\right)_n \longrightarrow M_n$)

$$\left(\bigoplus_{i=1}^{r} R[-d_i]e_i\right)_n \cong \bigoplus_{i=1}^{r} (R_{n-d_i})e_i$$

Note: R Noetherian $\Rightarrow$ each R_n is a finite R_0-module.

Suppose that R_0 is Artinian. Then, $\ell(R_0) < \infty$ (as R_0-module), and thus each $\ell(M_n) < \infty$.

Rk: usually, $R_0 = k$ (it is Artinian), and $\ell(M_n) = \dim_k(M_n)$.

Hilbert Series:
$P(M,t) := \sum_{n=0}^{\infty} \ell(M_n).t^n \in \mathbb{Z}[[t]]$. it is called the Hilbert series.

The Hilbert function is $H_M(n) := \ell(M_n)$.

Prop: If R is a Noetherian graded ring, R_0 Artinian and M a finite R-module, then if $R = R_0[x_1,\dots,x_r]$, $|x_i| = d_i$ hom generators (not nec. free).
Then $P(M,t) = \dfrac{f(t)}{\prod_{i=1}^{r}(1-t^{d_i})}$ where $f(t) \in \mathbb{Z}[t]$.

Pf induction on r.
$r=0$: $R=R_0$. Then $\ell_M(n)=0$ for $n>>0$. So $P(M,t) \in \mathbb{Z}[t]$ already.

For $r>0$, note that

$0 \to \underset{k[-d_r]}{\mathrm{Ker}} \to M[-d_r] \xrightarrow{\cdot x_r} M \to L \to 0$ is a degree-0-hom

So have $0 \to K_{n-d_r} \to M_{n-d_r} \to M_n \to L_n \to 0$

K and L are modules over R/x_rR

Notice that $L_n=0$ if $n<0$
$K_n=0$ if $n<d_r$

By additiveness of length, have

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

So $$P(M,t) - P(M[-d_r],t) = \underbrace{P(L,t) - P(K[-d_r],t)}_{\text{OK by induction}}$$

$$P(M,t) - P(M,t)\cdot t^{d_r} = \frac{g(t)}{\prod_{i=1}^{r-1}(1-t^{d_i})}$$

Note: • $P(M[-d],t) = P(M,t)\,t^d$.

• $0 \to M' \to M \to M'' \to 0 \Rightarrow P(M,t) = P(M',t) + P(M'',t)$.

Special case: $d_1 = \dots = d_r = 1$. Then R is generated over R_0 by R_1.

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

We'll write $P(M,t) = \dfrac{f(t)}{(1-t)^d}$, where either $d=0$ or $f(1)\neq 0$ (unique such expression)

We have an invariant $d(M) := d$.

Def: The Hilbert function of M is $H_M(n) = \ell(M_n)$ (and $H_M(n)=0$ for $n<0$).

$$(1-t)^{-d} = \sum_{n=0}^{\infty} \binom{d-1+n}{d-1} t^n$$

So if $f(t) = \sum_{i=0}^{s} a_i t^i$, then $\ell(M_n) = a_0\binom{d-1+n}{d-1} + a_1\binom{d-2+n}{d-1} + \dots + a_s\binom{d-s-1}{d-1}$ th.

So from the previous expression, $H(n)$ is a fixed polynomial $\varphi(n)$, for φ of degree $\leq d-1$, for $n \geq s+1-d$.

In fact, $\varphi(X) = \frac{f(1)}{(d-1)!} X^{d-1}$ + lower degree.

(Rk: ~~$f(1) \neq 0$~~ if d is chosen minimally, $\deg \varphi = d-1$ or $\varphi \equiv 0$ (when $d=0$)).

Def: The Hilbert Polynomial for M is $\varphi_M(X)$.

Example: $A = k[X_0, \dots, X_r]$, $|X_i| = 1$ ($r+1$ - variables).

$$\ell(A_n) = \binom{n+r}{r}, \quad \text{so} \quad \varphi_A = \frac{(X+r)(X+r-1)\cdots(X+1)}{r!}$$

If $B = A/(F)$, $F \overset{\neq 0}{\in} A_d$, $d>0$,

then $$0 \to A[-d] \xrightarrow{\cdot F} A \to B \to 0$$

$$\Rightarrow \ell(B_n) = \binom{n+r}{r} - \binom{n+r-d}{r} \Rightarrow \varphi_B(X) = \frac{d}{(r-1)!} X^{r-1} + \dots$$

If $A = k[X_0, \dots, X_r]$, $|X_i| = 1$

and have a ~~graded~~ homogeneous ideal $I \subseteq A^+$, then $Z(I) \subseteq \mathbb{P}^r(k)$

(i.e. define $\mathbb{P}^r(k) = \{(a_0, \dots, a_r) \in k^{r+1} \mid a_i \neq 0 \text{ for some } i\} / (a_0, \dots, a_r) \sim (\lambda a_0, \dots, \lambda a_r)$)

And $Z(I) := \{[a_0 : \dots : a_r] : F(a_0, \dots, a_r) = 0 \ \forall F$ homogeneous element in $I\}$.

If $I \subseteq A^+$ is a homogeneous ideal, can consider $\overline{I}_n := \{F \in A_n \mid \forall m \gg 0, A_m F \subseteq I\}$ ($n \geq 0$). $\overline{I}_n$ is called the saturation of I.

Can show that $I_n = \overline{I}_n$ for all $n \gg 0$.

The projective scheme associated to I depends only on $\overline{I}$.

So for projective geometry, we use the Hilbert Polynomial as invariant, depending only on the saturation of ideals.

Variation: Given R and M as before, define

$$H'_M(n) := \sum_{i=0}^{n} \ell(M_i) \quad \left(= \ell\left(\bigoplus_{i=0}^{n} M_i\right)\right)$$

Can consider $P'(M,t) = \sum H'_M(n) t^n$.

Then $P'(M,t) = P(M,t)\,(1+t+t^2+\cdots) = \dfrac{P(M,t)}{1-t}$

So then $\exists$ a polynomial φ'_M s.t. $\varphi'_M(n) = H'_M(n)$ for large n.

And $\varphi_M(X) = \varphi'_M(X) - \varphi'_M(X-1)$

And thus, $\deg \varphi'_M = \deg \varphi_M + 1$.

In general, $H'_M(n) = a_0\binom{d+n}{d} + a_1\binom{d+n-1}{d} + \cdots + a_s\binom{d+n-s}{d}$

where $d = d(M)$ is the same as before.

- Samuel function.

Let A be a Noetherian semilocal ring.

Write $\mathfrak{m} := \mathrm{Jrad}(A) \left(= \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_t\right) \left(= \mathfrak{m}_1 \cdots \mathfrak{m}_t\right)$.

(think of A being a local ring).

Let $I \subseteq \mathfrak{m}$ s.t. $\mathfrak{m} \supseteq I \supseteq \mathfrak{m}^\nu$ for some $\nu \geq 1$.

We call I an "ideal of definition". (because I-adic topology $=$ $\mathfrak{m}$-adic topology)

(think of $I = \mathfrak{m}$).

Def: The associated graded ring is $gr_I(A) := \bigoplus_{n \geq 0} I^n/I^{n+1} \simeq A/I \oplus I/I^2 \oplus \cdots$

$\left(gr_I(A)_n = I^n/I^{n+1}\right)$.

Def: For M an A-module, $gr_A(M) := \bigoplus_{n\geq 0} I^n M/I^{n+1}M$ is a graded module over $gr_I(A)$.

Write $A' := gr_I(A)$, $M' := gr_I(M)$.

Note that A' is generated in degree 1 over deg $0 = A/I$.

Note that A Noetherian semilocal, I ideal of definition $\Rightarrow A/I$ is Artinian,

So if M is a finite A-module, define

$$\chi_M^I(n) := \ell\left(M/I^{n+1}M\right) = \sum_{i=0}^{n} \ell\left(gr_I(M)_i\right). \quad \left(\begin{array}{l}\text{length as a } A/I^e\text{-module} \\ \text{where } e \geq n+1\end{array}\right)$$

We have

$$\chi_M^I(n) = a_0\binom{d+n}{d} + \cdots + a_s\binom{d+n-s}{d} \quad \text{where } a_i \in \mathbb{Z}, \text{ with minimal } d.$$

And define $d(M) := d$.

If I, J are two ideals of definition, $\exists\, e>0$ s.t. $I^e \subseteq J$, $J^e \subseteq I$.

So $\ell(M/I^{n+1}M) \geq \ell(M/J^{e(n+1)}M) \Rightarrow \begin{cases} \chi_M^I(n) \geq \chi_M^J(en+e-1) \\ \chi_M^J(n) \geq \chi_M^I(en+e-1) \end{cases}$

This implies that χ_M^I and χ_M^J have the same degree d, so $d(M)=d$ is well defined.

<u>Prop</u>: A as above, $0 \to M' \to M \to M'' \to 0$ exact seq of <u>finite</u> A-modules. Then $d(M) = \max\{d(M'), d(M'')\}$, and for I = ideal of def,

$\chi_M^I - \chi_{M''}^I$ and $\chi_{M'}^I$ have the same degree and the same leading coefficient.

Pf

$$0 \to M'/M'\cap I^{n+1}M \to M/I^{n+1}M \to M''/I^{n+1}M'' \to 0$$

write $\varphi(n) = \ell\left(M'/M'\cap I^{n+1}M\right) = \chi_M^I(n) - \chi_{M''}^I(n)$, so

φ is a polynomial for large n.

By Artin-Rees, $\exists\, c \geq 0$ s.t. ~~$M'\cap I$~~

$$I^{n+1}M' \subseteq M'\cap I^{n+1}M \subseteq I^{(n+1)-c}M'$$

So $\chi_{M'}(n) \leq \varphi(n) \leq \chi_{M'}(n-c) \Rightarrow$ ~~$\deg \varphi(n)$~~ $\deg\varphi = \deg \chi_{M'}$, and have the same leading coeff.

(note that χ's and φ take non-negative values for large n, that gives $d(M) = \max\{\ \}$. //

If M is a (finite) module, can define $\dim(M) := \dim\left(A/_{ann(M)}\right)$.
(so as $V(ann(M)) = Supp(M) \subseteq Spec(A)$, the dimension of M is the dim. of $Supp(M)$).

If A is Noetherian, $\exists$ filtration

$$0 \hookrightarrow M_1 \hookrightarrow M_2 \hookrightarrow \cdots \hookrightarrow M_r = M \quad \text{s.t.} \quad M_i/_{M_{i-1}} \simeq A/_{P_i}, \quad P_i \text{ prime.}$$

As $Supp(M) = \{Q \in Spec\, A \mid M_Q \neq 0\}$, then $Supp(M) = \bigcup_{i=1}^{r} V(P_i)$.

(and so $\sqrt{ann(M)} = \sqrt{P_1 \cdots P_r}$)

We get that $\dim(M) = \dim\left(A/_{ann(M)}\right) = \max\{\dim(A/_{P_i})\}$.

In particular, if we have $0 \to M' \to M \to M'' \to 0$,

then $\dim(M) = \max\{\dim(M'), \dim(M'')\}$.

We'll show now that $\dim(M) = d$ in case of (semi) local rings.

Let A a semilocal Noetherian ring., $\mathfrak{m} = Jrad(A)$.

Def A system of parameters for M is a sequence $y_1, \ldots, y_r \in \mathfrak{m}$

s.t. $\ell\left[M/_{(y_1M + \cdots + y_rM)}\right] < \infty$

Define $\delta(M) :=$ shortest length of a system of parameters.

(if $\ell(M) < \infty$, then $\delta(M) = 0$).

Note: if I is an ideal of definition, then $\delta(M) \leq \#$ generators of I.

(because $\ell(A/I) < \infty$, so $\ell(M/IM) < \infty$).

Note: if A is a local ring and $I \subseteq A$ is any proper ideal,

then $\ell(A/I) < \infty \Leftrightarrow I$ is $\mathfrak{m}$-primary.

So $\delta(A) =$ minimal $\#$ of generators for any $\mathfrak{m}$-primary ideal.

Theorem: Let A be semilocal Noeth. ring, M a finite A-module.

Then $\dim M = d(M) = \delta(M)$.

Corollary: $\dim M$ is finite! In particular, if A is a semilocal ring then its Krull dimension is finite.
(So Noetherian rings are locally finite dimensional)

Proof: (I): $d \geq \dim$, (II): $\delta \geq d$, (III) $\dim \geq \delta$.

(I) First, show that $d(A) \geq \dim(A)$, by induction on $d(A)$.

If $d(A)=0$, then $\chi_i(n) = \ell(A/m^{n+1})$ is constant for large n.

So $m^n = m^{n+1}$ for $n \gg 0$. By Noeth., NAK $\Rightarrow m^n = 0$.

Thus A is Artinian $\Rightarrow$ 0-dimensional. (can write 0 as finite prod. of maximals).

If $d(A) > 0$, If $\dim(A)=0$ done, so suppose $\dim(A) > 0$.

So $\exists$ chain $P_0 \subsetneq P_1 \subseteq A$ of primes.

Pick $x \in P_1 \setminus P_0$, and set $B := A/_{P_0 + Ax}$

Have the exact sequence:

$$0 \to A/_{P_0} \xrightarrow{\cdot x} A/_{P_0} \to B \to 0$$

(recall: if $A \twoheadrightarrow B$ and A is semi-local, then $f(\mathrm{Jrad}(A)) = \mathrm{Jrad}(B)$)
So $\dim(B)$ is the same if we think of it as a ring ~~or~~ as an A-module)

By the previous lemma, $\chi^m_{A/P_0} - \chi^m_B$ and χ^m_{A/P_0} have the same degree & l.c. (as polynomials), so $\deg(\chi^m_B) < \deg(\chi^m_{A/P_0})$.

So $d(B) < d(A/P_0) \leq d(A)$. We can apply induction,

$d(B) \geq \dim(B)$ - so $d(A) - 1 \geq \dim(B)$

Consider an arbitrary $P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_e$ chain of primes in A.

$\Rightarrow P_1 B \subsetneq \cdots \subsetneq P_e B$ chain of primes in B.

$\dim(A) \geq e \Rightarrow \dim(B) \geq e-1$.

We get $\dim B \geq \dim A - 1$ (if P_0 is the minimal element of a chain of primes of maximal length in A)

So $d(A) \geq \dim(A)$.

Now if M is a finite A-module, given a filtration $M_0 = 0 \subset M_1 \subset \dots \subset M_q = M$ ~~for~~ $M_i/M_{i-1} \simeq A/p_i$. So:

$$\dim(M) = \sup\{\dim A/p_i\}$$
$$\wedge \qquad\qquad \wedge \text{ by lemma}$$
$$d(M) = \sup\{d(A/p_i)\}$$

//

(II) $\delta(M) \geq d(M)$.

If $\delta(M) = 0 \Rightarrow \ell(M) < \infty$, $\chi_M^{m}(n)$ bounded $\Rightarrow d(M) = 0$.

Suppose $\delta(M) = s > 0$. Then, $\exists\, x_1, \dots, x_s \in \mathfrak{m}$ s.t.

$$\ell\left(M/_{x_1M + \dots + x_sM}\right) < \infty.$$

Write $M_i := \dfrac{M}{x_1M + \dots + x_iM}$. Then $\delta(M_i) = s - i$ by minimality of length.

$$\begin{tikzcd} 0 \arrow[r] & M/(\mathfrak{m}^nM : x_1) \arrow[r, "\cdot x_1"] & M/\mathfrak{m}^nM \arrow[r] & M_1/\mathfrak{m}^nM_1 = \frac{M}{x_1M + \mathfrak{m}^nM} \arrow[r] & 0 \\ & M/\mathfrak{m}^{n-1}M \arrow[u, two heads] & & & \end{tikzcd}$$

~~Observe that $\mathfrak{m}^{n-1}M$~~ (because $\mathfrak{m}^{n-1}M \subseteq (\mathfrak{m}^nM : x_1)$).

$$\overbrace{\ell\left(M_1/\mathfrak{m}^nM_1\right)}^{\chi_{M_1}(n-1)} = \ell\left(M/\mathfrak{m}^nM\right) - \ell\left(M/(\mathfrak{m}^nM : x_1)\right) \geq \ell\left(M/\mathfrak{m}^nM\right) - \ell\left(M/\mathfrak{m}^{n-1}M\right) = \chi_M(n-1) - \chi_M(n-2)$$

$\Rightarrow \deg \chi_{M_1} \geq \deg \chi_M - 1$, so $d(M_1) \geq d(M) - 1$.

By induction, $\underbrace{d(M_s)}_{=0} \geq d(M) - s$, so $\overset{\delta(M)}{\overset{=}{s}} \geq d(M)$

//

(cont pf)

(III): $\dim M \geq \delta(M)$.

Induction on $\dim(M)$.

$\dim(M) = 0 \Rightarrow \dim(A/\mathrm{ann}(M)) = 0$. So $\sqrt{\mathrm{ann}(M)}$ = intersection of finite # of maximals,

so $\mathfrak{m}^n \subseteq \mathrm{ann}(M)$ for some $n > 0$, so $\ell(A/\mathrm{ann}(M)) < \infty \overset{\text{and}}{\Rightarrow} \ell(M) < \infty$

(M is built from finitely many $A/\mathrm{ann}(M)$ - modules.)

Suppose now $\dim(M) > 0$.

Let $P_1, \ldots, P_6$ be primes, divisors of $\mathrm{ann}(M)$, such that $\mathrm{coht}\, P_i \left(= \dim A/P_i\right) = \dim M$.

Since $\dim(M) > 0$, then P_i are not maximal, so don't contain $\mathfrak{m}$.

Let $x_1 \in \mathfrak{m} \setminus \bigcup P_i$ (by prime avoidance). $M_1 := M/x_1 M$

$\dim M_1 < \dim M$ since $\mathrm{ann}(M_1) \supseteq x_1 A + \mathrm{ann}(M)$, so $P_i \not\supseteq \mathrm{ann}(M_1)$

$\dim(M) - 1 \geq \dim(M_1) \underset{\text{induction}}{\geq} \delta(M_1) \geq \delta(M) - 1$

from a minimal system of params for M_1, add x_1 and get a system (possibly not minimal) for M.

Th (Krull's Principal Ideal Theorem):

A Noetherian, $I = (a_1, \ldots, a_r) \subseteq A$.

If P is a minimal prime divisor of I, then $ht(P) \leq r$.

(so $ht(I) \leq r$, recalling $ht(J) := \inf\{ht\, P \mid P \supseteq I \text{ prime}\}$.

Pf/ Consider $IA_P \subseteq A_P$. It is PA_P-primary if P is a minimal prime divisor.

[$P \in \mathrm{Ass}(A/I)$, and so $\mathrm{Ass}(A_P/IA_P) \overset{\text{Noeth}}{=} \underbrace{\mathrm{Ass}(A/I) \cap \mathrm{Spec}(A_P)}_{\{P\}}$]

$ht(P) = \dim(A_P) = \delta(A_P)$

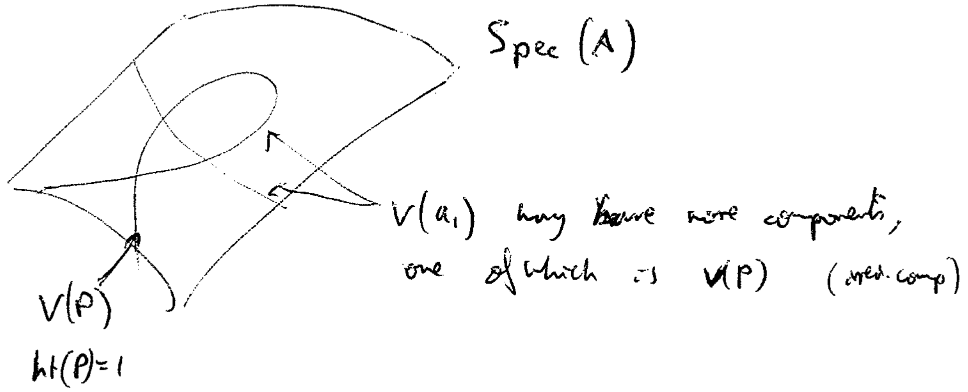
Since $IA_P = (a_1, \ldots, a_r)A_P$ is PA_P-primary, $\delta(A_P) \leq r \Rightarrow$ //

Prop: $P \subseteq A$ a prime, A a Noeth. ring, $ht(P) = r$. Then:

i) P is a minimal prime divisor of some $I = (a_1, \dots, a_r)$

ii) if $b_1, \dots, b_s \in P$, then $ht_{A/(b_1,\dots,b_s)}\left(P/(b_1,\dots,b_s)\right) \geq r - s$

iii) if $a_1, \dots, a_r$ are as in (i), then $ht\left(P/(a_1,\dots,a_i)\right) = r - i$



Pf (i) $\dim A_P = r$, so $\exists\, a_1, \dots, a_r \in PA_P$ s.t. $(a_1, \dots, a_r)A_P$ is PA_P-primary

$(\delta(A_P) = \dim(A_P))$

Write $a_i = \frac{a_i'}{s_i}$ $(a_i' \in P,\ s_i \in A \setminus P)$. so $(a_1', \dots, a_r')A_P = (a_1, \dots, a_r)A_P$.

So WLOG, can assume $a_i \in A$.

Let $I = (a_1, \dots, a_r) \subseteq A$.

$Ass(A_P/IA_P) = \{P\}$, so P is minimal assoc. prime of A/I.

$\quad \shortparallel$

$Ass(A/I) \cap Spec(A_P)$ //

(ii) $\bar{A} := A/(b_1,\dots,b_s)$, $\bar{P} = P/(b_1,\dots,b_s)$, $t := ht\,\bar{P}$.

By (i), $\exists\, c_1, \dots, c_t \in P$ s.t. $\bar{P}$ is a minimal prime divisor of $(c_1, \dots, c_t)\bar{A} \subseteq \bar{A}$.

So $(b_1, \dots, b_s, c_1, \dots, c_t) \subseteq A$ has P as a minimal prime divisor.

Thus $ht(P) = r \leq s + t$ by KPI th., so $r - s \leq t = ht\,\bar{P}$ //

(iii) $ht\ P/(a_1,\dots,a_i) \geq r - i$ by (ii).

$\bar{A} := A/(a_1,\dots,a_i)$

But $P/(a_1,\dots,a_i)$ is a minimal prime divisor of $(a_{i+1}, \dots, a_r)\bar{A}$. By KPI th. done //

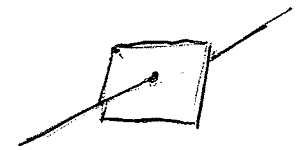
<u>Remark</u>: By KPI th., if $I=(x_1,\dots,x_s)\subseteq \mathfrak{m}$ where $A\supseteq\mathfrak{m}$ is local Noeth.

Then $ht(I)\leq s$

Even if $x_1,\dots,x_s$ is part of a system of parameters for $\mathfrak{m}$,

it need not be the case that $ht(I)=s$:

<u>Example</u>: $k[X,Y,Z]_{(X,Y,Z)}$ $\quad(\mathfrak{m}=(X,Y,Z)A)$.



$I=\big((X)\cap(Y,Z)\big)A$.

$B:=A/I$. minimals of B are $(X)B$ and $(Y,Z)B$.

$$\left.\begin{aligned} &\text{So } \dim\left(B/XB\right)=\dim\left(A/XA\right)=2 \\ &\dim\left(B/(Y,Z)B\right)=\dim\left(A/(Y,Z)A\right)=1\end{aligned}\right\}\Rightarrow \dim(B)=2.$$

A system of parameters for B can be $x_1=Y,\ x_2=X+Z$.

$\frac{B}{(x_1B+x_2B)}\cong\ 1\quad X\quad Z \quad\to\quad \frac{B}{x_1B+x_2B}$ has rank 2 over k.

Let $J:=(x_1)=(Y)B\subseteq B$.

Then $ht\,J\leq 1$. Note that we don't have equality:

$Y\in(Y,Z)B\leftarrow$ minimal prime of B.

$J=YB\subseteq(Y,Z)B\Rightarrow ht(J)\leq ht(Y,Z)B=0\quad\Rightarrow ht(J)=0$ //

The problem was that the choice of the parameters for $\mathfrak{m}$ was too special. We will see next that one can make always the good choice.

Prop: $A \supsetneq m$ a local Noetherian ring. Then there exists a system of parameters for m, $x_1, \dots, x_r \in m$, s.t. every $F \subseteq \{x_1, \dots, x_r\}$ is such that $ht(F A) = \# F$.

pf $r = 0$ easy.

$r \geq 1$

Let P_{0j}, $1 \leq j \leq e_0$ be all minimal primes of A (i.e. all primes of ht 0).

Let $x_1 \in m \setminus \bigcup_{j=1}^{e_0} P_{0j}$ (if $m = \bigcup P_{0j}$, then by prime avoidance $m = P_{0k}$ for some k!)

$ht((x_1)) = 1$ [≤ 1 by KPI th. and (x_1) is not contained in the ht 0 primes].

(if $r = 1$, done!).

otherwise, P_{1j} $1 \leq j \leq e_1$ be all minimal prime divisors of (x_1) of minimal height.

So $ht(P_{1j}) = 1$

Let $x_2 \in m \setminus (\bigcup P_{0j} \cup \bigcup P_{1j}) \Rightarrow ht((x_2)) = 1$ as before

Also, $ht((x_1, x_2)) = 2$ (by KPI, ≤ 2 and $=$ by construction).

(If $r = 2$, done!)

otherwise, $x_3 \in m$ but not in the minimal prime divisors of $0, (x_1), (x_2), (x_1, x_2)$.

$(\dots)$

//

Let a system of parameters of (A, m) (noeth local of dim r), be a sequence $a_1, \dots, a_r \in m$ which generate.

$k = A/m$.

Let $n := \operatorname{rank} m/m^2$, it is called the <u>embedding dimension of A</u>.

<u>Rk</u>: emb dim $\geq$ dim A.

<u>Ex</u>: $A = k[X,Y]_{(X,Y)}$, then $A/(XY)$ has dim 1 but emb. dim. $= 2$.

Def: A is a regular local ring if dim = emb dim.

(i.e. if $\exists$ a system of parameters which generates $\mathfrak{m}$ itself).

Such a system of parameters is called a <u>regular system of params.</u>

Lemma: $(A, \mathfrak{m})$, n dimensional local ring.

Let $x_1, \dots, x_i \in \mathfrak{m}$. TFAE:

1) $x_1, \dots, x_i$ is a subset of a regular system of params.

2) The images of $x_1, \dots, x_i$ in $\mathfrak{m}/\mathfrak{m}^2$ are l.i over k.

3) $A/(x_1, \dots, x_i)$ is a regular local ring of dim. $n-i$

Pf

(1)$\Rightarrow$(2): clear.

(1)$\Rightarrow$(3): $x_1, \dots, x_n$ ~~local~~ reg. system of param. $\bar{A} := A/(x_1, \dots, x_i)$.

$\bar{\mathfrak{m}} = (x_1, \dots, x_n)\bar{A} = (x_{i+1}, \dots, x_n)\bar{A}$.

Then $x_{i+1}, \dots, x_n$ is a minimal system of params. for $\bar{\mathfrak{m}}$ ($\Rightarrow \bar{A}$ is regular).

So $\dim \bar{A} = n-i$

(3)$\Rightarrow$(1): $\bar{\mathfrak{m}} := \mathfrak{m}/(x_1, \dots, x_i)$ in $\bar{A}$. If $\bar{\mathfrak{m}}$ is generated by images of elts $y_1, \dots, y_{n-i}$ in A,

then $\mathfrak{m}$ is generated by $(x_1, \dots, x_i, y_1, \dots, y_{n-i})$

Since $\dim A = n$, $i + n - i = n \Rightarrow$ this is a subset of a reg. system of params.

(2)$\Rightarrow$(1): $\operatorname{rank}_k \mathfrak{m}/\mathfrak{m}^2 = n$. Since $x_1, \dots, x_i$ are l.i in $\mathfrak{m}/\mathfrak{m}^2$, can extend

to $x_1, \dots, x_n \in \mathfrak{m}$ s.t. they are a k-basis for $\mathfrak{m}/\mathfrak{m}^2$

$\Rightarrow x_1, \dots, x_n$ is a reg. system of params.

Theorem: A regular local ring is a domain.

Remark: Suppose A is a regular local ring. $\dim A = 0 \Leftrightarrow A$ is a field.

Also, if $\dim A = 1 \Leftrightarrow A$ is a DVR.

Pf of theorem:

Will do it by induction on $n = \dim A$. ($n \leq 1$ clear by remark).

Suppose then $n > 1$.

Let $P_1, \dots, P_r$ be the minimal primes of A.

Have $\mathfrak{m} \not\subseteq P_i$ for any i (by dimension).

Also, $\mathfrak{m} \not\subseteq \mathfrak{m}^2$ (by NAK, $\dim > 0$).

By prime avoidance (ex. 1.6). $\exists\, x$

$x \in \mathfrak{m} \setminus \mathfrak{m}^2 \cup (\bigcup P_i)$ (don't need all to be primes!)

By previous lemma, A/xA is a reg. local ring of dimension $n-1$. So it is a domain, by induction.

Thus, xA is prime.

There is a $P_i \subseteq xA$ (P_i are minimal). As $x \notin P_i$, $P_i \subsetneq xA$.

Given $y \in P_i$, $y = ax$ for some $a \in A$. As $x \notin P_i \Rightarrow a \in P_i$.

So $P_i = xP_i$. By NAK, $P_i = 0$, so 0 is a prime $\Rightarrow A$ is a domain //.

Theorem: If $(A, \mathfrak{m})$ is a d-dimensional regular local ring, $k = A/\mathfrak{m}$.

Then $gr_{\mathfrak{m}}(A) \simeq k[X_1, \dots, X_d]$, $|X_i| = 1$.

and $\chi_A(n) = \binom{n+d}{d}$ $n \geq 0$.

Pf/ Since $\mathfrak{m} = (x_1, \dots, x_d)$, then $gr_{\mathfrak{m}}(A) = k[X_1, \dots, X_d]/I$, I a homog. ideal.

So only need to show $I = 0$.

Suppose $f \in I$, $f \neq 0$. f hom of degree r.

$$\frac{k[X_1, \dots, X_d]}{(f)} \twoheadrightarrow \frac{k[X_1, \dots, X_d]}{I} = gr_A(\mathfrak{m}).$$

the samuel poly?. If $R = k[X_1, \dots, X_d]$, there is an exact seq. of graded rings:

$$0 \to R[-r] \xrightarrow{\cdot f} R \to R/(f) \to 0$$

So $\chi_{R/f}(n) = \ell\left(\frac{R/(f)}{(R/(f))_+^{n+1}} \right) = \binom{n+d}{d} - \binom{n+d-r}{d} \geq \chi_A(n)$ $\forall n$

(cont pf)

So $\deg \chi_A \leq d-1$.
But we must have $\deg \chi_A = \dim A = d$ $\Big\} \Rightarrow$!! . So $I = 0$ //

Remark: The same proof shows that if A is a Noeth local ring s.t. $gr_{m} A = k[X_1, \ldots, X_d]$, then A is regular, of dimension d.

Examples: $A = k[X_1, \ldots, X_d]_{(X_1, \ldots, X_d)}$
$B = k[[X_1, \ldots, X_d]]$ are regular local rings.

(If A is regular local ring, so is $\hat{A}_{m}$).

Also, $\mathbb{Z}_{(p)}$, $\hat{\mathbb{Z}}_p$ are regular local rings.

Prop: Let A be a complete regular local ring, $\dim A = d$, $k = A/m$.
If A contains a field isomorphic to k, then $A \simeq k[[X_1, \ldots, X_d]]$
(i.e. ask $k \hookrightarrow A/m$ is iso).

Pf
Can define $k[X_1, \ldots, X_d] \longrightarrow A$ by $X_i \mapsto x_i$ where $\{x_i\}$ is a reg. system of params.
Have $k[X_1, \ldots, X_d]/(X_1, \ldots, X_d)^n \longrightarrow A/m^n$ is surjective because $\{x_i\}$ is syst of params.

The dimensions coincide $\Rightarrow$ they are isomorphic. $\Rightarrow \hat{A} = k[[X_1, \ldots, X_d]]$. //

In fact, the proposition is true under the hypothesis that A contains <u>any</u> field.
(Look it at Eisenbud).

• Multiplicity

Let $(A, \mathfrak{m})$ be a d-dim Noeth. local ring, M a finite A-module,
I an ideal of definition ($\mathfrak{m}$-primary).

Then $\chi_M^I(n) = \ell(M/I^{n+1}M)$ for large $n \gg 0$ is a polynomial of degree $\dim M \leq d$.

So $\chi_M^I(n) = \frac{e}{d!} n^d$ + lower degrees where $e \in \mathbb{Z}$ $\left(\binom{n+d}{d} = \frac{(n+d)\cdots(n+1)}{d!} \right)$.

If $\dim M < d$, $e = 0$. In general, $e \geq 0$.

Write $e(I) := e(I, A)$ the multiplicity of A wrt I.

For $I = \mathfrak{m}$, if A is a regular local ring, $e(\mathfrak{m}) = 1$ (since $\chi_A^{\mathfrak{m}} = \binom{n+d}{d}$).

Ex: $k[X,Y]_{(X,Y)}/(XY)$, $e((X,Y)) = 2$.

Prop: $0 \to M' \to M \to M'' \to 0$ exact, then $e(I, M) = e(I, M') + e(I, M'')$.

Given M with a filtration $0 = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_r = M$ so that $M_i/M_{i-1} \cong A/\mathfrak{p}_i$ (for primes $\mathfrak{p}_i$).

Then $e(I, M) = \sum e(I, A/\mathfrak{p}_i)$

Note that $e(I, A/\mathfrak{p}_i) = 0$ unless $\dim A/\mathfrak{p}_i = d$, so in particular need only to consider the minimal $\mathfrak{p}_i$.

Prop: $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_t\}$ the subset of minimal primes of A s.t. $\dim A/\mathfrak{p}_i = d$.

Then $e_A(I, M) = \sum e_{A/\mathfrak{p}_j}(\bar{I}_j, A/\mathfrak{p}_j) \cdot \ell_{A_{\mathfrak{p}_j}}(M_{\mathfrak{p}_j})$

where $\bar{I}_j$ = image of I in $A/\mathfrak{p}_j$.

(Note that $A_{\mathfrak{p}_j}$ is a field, so $\ell_{A_{\mathfrak{p}_j}}(M_{\mathfrak{p}_j})$ = rank as vector space over $A_{\mathfrak{p}_j}$).

Cor: If A is a domain, $e(I, M) = e(I) \cdot s$ where $s = \operatorname{rank}_K(M \otimes_A K)$ $(K = k(A))$.

Pf of prop:

Induction on $\sigma := \sum_j \ell_{A_{P_j}}(M_{P_j})$.

If $\sigma = 0$ it means $M_{P_j} = 0 \;\forall P_j \Rightarrow P_j \notin \mathrm{Supp}(M) = V(\mathrm{ann}(M))$.

So $\mathrm{ann}(M) \not\subseteq P_j \;\forall j$. As $\dim M = \dim A/\mathrm{ann}(M) < d \Rightarrow e(I, M) = 0$. ✓

Given M, let $P \in \mathrm{Ass}_A(M)$, $\underset{\substack{\cong\\ A/P}}{N} \hookrightarrow M \twoheadrightarrow M/N$. So

$$e_A(I, M) = e_A(I, \underbrace{A/P}_{N}) + e_A(I, M/N).$$

Note that $e_A(I, A/P) = e_{A/P}(I, A/P)$ since $\ell_A\left((A/P)/I^n(A/P)\right) = \ell_{A/P}\left((A/P)/I^n(A/P)\right)$.

If $\dim A/P < d$, these lengths $= 0$, so if $P \notin \{P_1, \dots, P_t\}$. So only need to worry about $\{P_1, \dots, P_t\}$.

If $P \in \{P_1, \dots, P_t\}$, $N_{P_j} = \begin{cases} A_{P_j}/P_j A_{P_j} & P = P_j \\ 0 & P \neq P_j \end{cases} \Rightarrow \ell(N_{P_j}) = \begin{cases} 1 & P = P_j \\ 0 & P \neq P_j \end{cases}$ //

• Fiber dimension

Let $\varphi : A \to B$ a ring homomorphism.

The going-up property is: given $Q_0 \subseteq B$ s.t. $Q_0 \cap A = P_0$, and $P_1 \supseteq P_0$, then $\exists\, Q_1 \supseteq Q_0$ in B s.t. $Q_1 \cap A = P_1$.

Recall that if $A \subseteq B$ is integral, it has the going-up property.

The going-down property is, given $P_0 \subsetneq P_1 \subseteq A$, $Q_1 \subsetneq B$ s.t. $Q_1 \cap A = P_1$, then $\exists\, Q_0 \subsetneq Q_1$ s.t. $Q_0 \cap A = P_0$.

Prop: if B is flat over A, then the going-down property holds.

Pf:
$$\begin{array}{ccccc} ? & - & Q_1 & \subsetneq & B \\ | & & | & & | \\ P_0 & \subsetneq & P_1 & \subsetneq & A \end{array}$$
Localize at Q_1 and P_1:
$$\begin{array}{ccccc} ? & \subseteq & Q_1 B_{Q_1} & \subsetneq & B_{Q_1} \\ | & & & & \\ P_0 A_{P_1} & \subseteq & P_1 A_{P_1} & \subsetneq & A_{P_1} \end{array}$$

As $B_{Q_1} = (B_{P_1})_{Q_1}$ and B is A-flat, $\Rightarrow A_{P_1} \to B_{P_1} \to (B_{P_1})_{Q_1} \Rightarrow$

$\Rightarrow B_{Q_1}$ is flat over A_{P_1}.

Since for the maximal ideal $P_1 A_{P_1}$ of A_{P_1} we have $P_1 B_{Q_1} \neq B_{Q_1}$, the maximal ideal criterion for faithful-flatness $\Rightarrow A_{P_1} \to B_{Q_1}$ is faithfully-flat.

So

$$\begin{tikzcd}
\tilde{Q}_0 \arrow[d, mapsto] & \operatorname{Spec}(B_{Q_1}) \arrow[r, two heads] \arrow[d, hook] & \operatorname{Spec}(A_{P_1}) \arrow[d, hook] & \ni P_0 A_{P_1} \arrow[d, mapsto] \\
\tilde{Q}_0 \cap B = Q_0 & \operatorname{Spec}(B) \arrow[r] & \operatorname{Spec}(A) & P_0
\end{tikzcd}$$

is surjective

Given $P \in \operatorname{Spec}(A)$, let $k(P) = A_P / PA_P = K(A/P)$.

Given $\varphi : A \to B$, define

Def: The fiber ring over P is $B \otimes_A k(P)$.

Prop: $\varphi : A \to B$ of Noetherian rings. Let $Q \subseteq B$ prime, $P = A \cap Q$.

Then:

1) $\underbrace{\operatorname{ht} Q}_{\dim B_Q} \leq \underbrace{\operatorname{ht} P}_{\dim A_P} + \dim \overbrace{\left(B_Q / PB_Q \right)}^{(B \otimes_A k(P))_Q}$

2) If the Going Down Property holds, then it is an equality: $\operatorname{ht} Q = \operatorname{ht} P + \dim (B_Q / PB_Q)$.

Pf WLOG can take $A := A_P$, $B := B_Q$ (local rings). $A \to B$ is a local hom

(i.e. $\mathfrak{m}_B^{Q} \cap A = \mathfrak{m}_A^{P}$).

Want to see $\dim B \leq \dim A + \dim B/PB$.

Let $x_1, \dots, x_r$ be a system of params. for A ($r = \dim A$).

Let $y_1, \dots, y_s \in B$ are elements whose images in B/PB are a system of parameters.

(cont pf)

Note that $(y_1,\dots,y_s)(B/PB)$ is a $\overline{Q} = Q(B/PB)$ primary ideal, so $\exists \mu$ s.t. $\overline{Q}^{\mu} \subseteq (y_1,\dots,y_s)B/PB$.

So $Q^{\mu} \subseteq (y_1,\dots,y_s)B + PB$.

Also, $\exists \nu$ s.t. $P^{\nu} \subseteq (x_1,\dots,x_r)A$

$\Big\}\ Q^{\mu\nu} \subseteq \overbrace{(y_1,\dots,y_s,x_1,\dots,x_r)}^{\text{it is } Q\text{-primary}}B$

$\therefore \dim B \leq s+r$

(2) Write $\dim B/PB = s$, $\dim A = r$

$\exists\ Q = Q_0 \supsetneq \cdots \supsetneq Q_s \supseteq PB$ maximal chain of primes.

All the Q_i's restrict to P: $Q_i \cap A = P$.

Have also $P = P_0 \supsetneq P_1 \supsetneq \cdots \supsetneq P_r \supseteq A$ a maximal chain of primes.

By the going down, we can extend the chain $Q_0 \dots Q_s$ in B to one of length $r+s$: $Q_{s+i} \subseteq B$, $Q_{s+i} \cap A = P_i$

$Q_0 \supsetneq Q_1 \supsetneq \cdots \supsetneq Q_{s+r} \Rightarrow \dim B \geq r+s$

<u>Convention</u>: $\dim(0) = -\infty$

<u>Corollary</u>: If $\varphi: A \to B$ is flat, then $\dim B = \sup\{ht(P) + \dim(B \otimes_A k(P))\}$ where the sup is taken over all $P = A \cap Q$ for Q all maximal ideals of B.

Pf $\dim B = \sup\{ht(Q) \mid Q \in m\text{-}Spec(B)\}$.

By prop, $ht(Q) = ht(P) + \dim((B \otimes_A k(P))_Q)$

and $\dim(B \otimes_A k(P)) = \sup\{\dim((B \otimes_A k(P))_Q) \mid Q$ max. ideals of B lying over $P\}$.

<u>Corollary</u>: If, additionally, $\varphi^*(m\text{-}Spec(B)) \subseteq m\text{-}Spec(A)$, then $\dim(B) = \sup\{\ \}$ where sup is taken for $P \in m\text{-}Spec(A)$.

Example: A a domain, not a field; $B = K(A)$. $\quad (\dim A \geq 1, \ \dim B = 0)$.

The localization $A \to B$ is flat, then;

$$\dim B = \underset{\overset{\shortparallel}{0}}{ht_A(0)} + \dim B \quad (\text{because } 0 \in A, \ B \otimes_A A_0 \simeq B).$$

^ trivial equality...

Consequences: If A is Noetherian, then $A[X_1, \ldots, X_n] =: B$ has dimension $n + \dim A$.

pf/ $P \in \operatorname{Spec}(A)$, $B \otimes_A K(P) = K(P)[X_1, \ldots, X_n]$ — field, $\dim = n$. //

Also, $\dim A[[X_1 \ldots X_n]] = n + \dim A$;

We don't know, in general, that $B \otimes_A A' \overset{?}{\simeq} A'[[X_1, \ldots, X_n]]$.

However, if $A' = A/I$, then $B \otimes_A A/I \simeq A/I[[X_1, \ldots, X_n]]$.

$A \to A[[X_1 \ldots X_n]]$ is flat, and then for all $Q \in m\text{-}\operatorname{Spec}(B)$, then $Q = (P, X_1, \ldots, X_n)$, where $P \in m\text{-}\operatorname{Spec}(A)$, so $Q \cap A = P$ and can use the corollary. //

Regular Sequences.

A a ring, M an A-module.

Def $a \in A$ is M-regular if a is not a zero-divisor on M.

So if a is regular, have exact sequence $0 \to M \xrightarrow{\cdot a} M \to M/aM \to 0$

Def $a_1, \ldots, a_n \in A$ is an M-(regular) sequence if: (order matters!)

1) a_i is $M/(a_1 M + \cdots + a_{i-1} M)$ - regular, and

2) $M/(\sum a_i M) \neq 0$.

So get

$$0 \to M \xrightarrow{\cdot a_1} M \to \underbrace{M/a_1 M}_{= M_1} \to 0$$

$$0 \to M_1 \xrightarrow{\cdot a_2} M_1 \to \underbrace{M_1/a_2 M}_{M_2} \to 0$$

$\vdots$

<u>Example</u>: If A is a regular local ring and $x_1,\dots,x_n$ is a regular system of parameters, it is an A-regular sequence.

∘ The Koszul Complex:

Let $x_1,\dots,x_n \in A$. Define a chain complex $K_\bullet = K_\bullet(x_1,\dots,x_n) = K_\bullet(\underline{x})$ as:

$$K_p = \bigoplus_{1\le i_1<i_2<\dots<i_p\le n} A e_{i_1\dots i_p} \qquad \left(\text{free on } \binom{n}{p} \text{ generators}\right).$$

$$d(e_{i_1\dots i_p}) := \sum_{r=1}^{p} (-1)^{r-1} x_{i_r} e_{i_1,\dots,\hat{i_r},\dots,i_p}$$

$$0 \to K_n \xrightarrow{d} K_{n-1} \xrightarrow{d} \cdots \xrightarrow{d} K_1 \xrightarrow{d} K_0 \to 0$$

<u>Ex</u>: x_1, x_2. $\quad K_2 = Ae_{1,2}$, $K_1 = Ae_1 \oplus Ae_2$

And $e_{12} \mapsto x_1 e_2 - x_2 e_1$

$$\begin{array}{c} K_2 \\ \downarrow \begin{bmatrix} -x_2 \\ x_1 \end{bmatrix} \\ K_1 \\ \downarrow [\,x_1 \ \ x_2\,] \\ K_0 \end{array}$$

<u>Notation</u>: If M is an A-module, write

$$K_\bullet(\underline{x}, M) := K_\bullet(\underline{x}) \otimes_A M \quad , d = d \otimes id_M \qquad \text{it is also a chain complex.}$$

<u>Def</u> $H_p(\underline{x}, M) := H_p(K_\bullet(\underline{x}, M))$.

In particular,
$$H_0(\underline{x}, M) = \operatorname{coker}\left[K_1(\underline{x}) \otimes_A M \longrightarrow K_0(\underline{x}) \otimes_A M\right] \cong M/(x_1,\dots,x_n)M$$
$$\begin{array}{ccc} \| & & A\otimes M \\ & & \cong \\ \bigoplus Me_i & \xrightarrow[m e_i \mapsto x_i m]{} & M \end{array}$$

Also, $H_n(\underline{x}, M) = \ker\left(K_n(\underline{x}) \otimes M \to K_{n-1}(\underline{x}) \otimes M\right)$
$$\begin{array}{ccc} \cong & & \\ e_{1\dots n} \otimes M & & \bigoplus \hat{e}_i M \quad (\hat{e}_i = e_1 \cdots \hat{e}_i \cdots e_n) \\ m & \longmapsto & (x_1 m, -x_2 m, x_3 m, \dots) \end{array}$$

So $H_n(\underline{x}, M) \cong \{ m \in M : (x_1,\dots,x_n)\cdot m = 0 \}$.

Recall that, if C, D are chain complexes of A-modules, so is $C_\bullet \otimes_A D_\bullet$,

as $[C_\bullet \otimes D_\bullet]_r = \bigoplus_{p+q=r} C_p \otimes_A D_q$ and $d(\underset{C_p}{x} \otimes \underset{D_q}{y}) = dx \otimes y + (-1)^p x \otimes dy$.

Obs: $K(\underline{x}) = K(x_1) \otimes \cdots \otimes K(x_n)$!

Example: $K_\bullet(x_1) = [Ae_1 \longrightarrow A\cdot 1]$, $e_1 \longmapsto x_1$, $K_\bullet(x_2) = [Ae_2 \longrightarrow A\cdot 1]$, $e_2 \longmapsto x_2$

Then $K_\bullet(x_1) \otimes K_\bullet(x_2) = \left[A\cdot e_1 \otimes e_2 \longrightarrow \begin{array}{c} Ae_1 \otimes 1 \\ \oplus \\ A\cdot 1 \otimes e_2 \end{array} \longrightarrow A\cdot 1 \otimes 1 \to 0 \right]$ //

$\underbrace{e_1 \otimes e_2}_{e_{12}} \longmapsto d(e_1) \otimes e_2 + e_1 \otimes d(e_2) = x_1 \cdot \underbrace{1 \otimes e_2}_{e_2} + x_2 \cdot \underbrace{e_1 \otimes 1}_{e_1}$

Lemma: Let $C_\bullet$ be a complex of A-modules.

$K_\bullet(x) := [Ae_1 \xrightarrow{\cdot x} A\cdot 1]$

(Notation: $C_\bullet(x) := C_\bullet \otimes K_\bullet(x)$).

Then there exist a sequence of chain complexes:

$$0 \to C_\bullet \to C_\bullet(x) \to C_\bullet[-1] \to 0$$

where $(C_\bullet[-1])_p := C_{p-1}$ and $d_{C[-1]} = \pm d_C$ depending on the degree.

Hence we have a long exact sequence on the homology:

$$\cdots \to H_p(C_\bullet) \to H_p(C_\bullet(x)) \to \underset{H_p(C_\bullet[-1])}{H_{p-1}(C_\bullet)} \xrightarrow{\cdot x} H_{p-1}(C_\bullet) \to \cdots$$

Pf exercise.

(rk for the pf:

$$\begin{tikzcd} 0 \arrow[r] & C_p \arrow[r, hook] \arrow[d, "d_c"] & {[C.(x)]_p = C_p \otimes A\cdot 1 \oplus C_{p-1} \otimes Ae} \arrow[r] \arrow[d, "d_c\otimes id \quad \pm id\otimes d_K \quad d_c \otimes id"] & C_{p-1} \arrow[r] \arrow[d, "d_c"] & 0 \\ 0 \arrow[r] & C_{p-1} \arrow[r, hook] & {[C.(x)]_{p-1} = C_{p-1} \otimes A\cdot 1 \oplus C_{p-2} \otimes Ae} \arrow[r] & C_{p-2} \arrow[r] & 0 \end{tikzcd}$$

Prop: If $x_1, \dots, x_n \in A$ is an M-regular sequence, then

$H_0(\underline{x}, M) \cong M/(x_1, \dots, x_n)M$ and

$H_p(\underline{x}, M) \cong 0 \quad \forall p > 0$.

Theorem: $(A, \mathfrak{m})$ is a local ring and $x_1, \dots, x_n \in \mathfrak{m}$, and

M a finite A-module.

If $H_1(\underline{x}, M) = 0$, then $x_1, \dots, x_n$ is an M-regular sequence.

Remark: in general, $(x_1, \dots, x_n) \cdot H_*(\underline{x}, M) = 0$.

because $x_i \cdot H_*(C.(x_i)) = 0$:

Note that taking twice x_i (rename it x):

$$\dots \to H_{p-1}(C.(x,x)) \to H_p(C.(x)) \to H_p(C.(x)) \to H_p(C.(x,x)) \to \dots$$

we can find

$$\begin{tikzcd} K(x) \arrow[r, hook] \arrow[dr, equal] & K(x,x) \arrow[d] \\ & K(x) \end{tikzcd}$$

, so $K(x,x) \cong K(x) \oplus K(x)[-1]$.

Prop: Let A be a ring, M a module, $x_1,\dots,x_n \in A$ is an M-regular sequence, then:

$$H_0(\underline{x}, M) = M/(x_1,\dots,x_n)M \quad \text{and} \quad H_q(\underline{x},M)=0 \quad \forall q>0.$$

Pf $\underline{n=1}$

$$0 \to \underbrace{H_1(x_1,M)}_{=0} \to M \xrightarrow{\cdot x_1} M \to \overbrace{M/x_1M}^{=H_0(x_1,M)} \to 0$$

since x_1 is M-regular.

$\underline{n>1}$: by induction:

$$\cdots \to H_{p+1}(\underline{x},M) \to H_p(x_1,\dots,x_{n-1};M) \xrightarrow{\cdot x_n} H_p(x_1,\dots,x_{n-1};M) \to H_p(\underline{x},M) \to \cdots$$

$=0$ if $p \geq 1$ by induction.

So $H_{p+1}(\underline{x},M)=0$ $\forall p \geq 1$. $\Rightarrow H_q(\underline{x},M)=0$ for $q \geq 2$.

For $q=1$,

$$\overset{0}{\overset{\shortparallel}{H_1(x_1,\dots,x_{n-1};M)}} \to H_1(\underline{x},M) \to H_0(x_1,\dots,x_{n-1};M) \xrightarrow{\cdot x_n} H_0(x_1,\dots,x_{n-1}) \to H_0(\underline{x},M) \to 0$$

$\Rightarrow H_1(\underline{x},M)$ because $\cdot x_n$ is injective. (x_n regular).

(Assume A is Noetherian)

Thm $(A,\mathfrak{m})$ local ring, $x_1,\dots,x_n \in \mathfrak{m}$. Then $M^{\neq 0}$ finite A-module,

If $H_1(\underline{x},M)=0$ then $x_1,\dots,x_n$ is an M-regular sequence.

Pf Induction on n. ($n=1$ clear).

$\underline{n>1}$: Consider $\cdots \to H_1(x_1,\dots,x_{n-1};M) \xrightarrow{\cdot x_n} H_1(x_1,\dots,x_{n-1};M) \to \underset{0}{\overset{\shortparallel}{H_1(\underline{x},M)}}$

By Noetherianness, $\longrightarrow$ finite A-modules.

So by Nakayama's lemma, $H_1(x_1,\dots,x_{n-1};M)=0$.

By induction, $x_1,\dots,x_{n-1}$ is regular. Then

$$\underset{0}{\overset{\shortparallel}{H_1(\underline{x},M)}} \to H_0(x_1,\dots,x_{n-1},M) \to H_0(x_1,\dots,x_{n-1},M) \to H_0(\underline{x},M) \to 0 \Rightarrow x_1,\dots,x_n \text{ is regular}$$ //

Def: $A \supseteq I$ an ideal, M an A-module.

A sequence $x_1, \ldots, x_r \in I$ is <u>a maximal M-regular sequence in I</u> if $\nexists\, y \in I$ s.t. $x_1, \ldots, x_r, y$ is M-regular.

Prop: If A is Noetherian, $I = (y_1, \ldots, y_n)$ and M a finite A-module s.t. $IM \neq M$.

Write $q := \sup\{ i : H_i(\underline{y}; M) \neq 0 \}$.

Then any maximal M-regular sequence in I has length $n-q$.

(in particular, the length doesnot depend on the sequence)

Def: The <u>depth</u> of I is the length of any maximal M-reg-seq in I.

write $\operatorname{depth}(I, M)$.

<u>Pf of prop:</u>

Let $x_1, \ldots, x_s$ be a maximal M-reg seq in I. want $s = n-q$.

Induction on s.

<u>$s=0$:</u> Every element of I is a zero-divisor. So $I \subseteq P = \operatorname{ann}(m)$, $m \neq 0$

an Associated prime.

by prime avoidance.

So $I \cdot m = 0$.

Then $H_n(\underline{y}, M) = \{ x \in M \mid y_1 x = \cdots = y_n x = 0 \}$.

and $m \in H_n(\underline{y}, M)$. So $q = n \Rightarrow \checkmark$.

<u>$s>0$:</u> Write $M_1 = M/x_1M$. $x_2, \ldots, x_s$ is a maximal M_1-reg. sequence in I.

So by induction,

$$0 \to M \xrightarrow{\cdot x_1} M \to M_1 \to 0 \Rightarrow 0 \to K(\underline{y}) \otimes M \to K(\underline{y}) \otimes M \to K(\underline{y}) \otimes M_1 \to 0$$

is exact. (at every degree).

So $\exists$ l.e.s.

$$\underset{\overset{\parallel}{0}}{H_{q+1}(\underline{y}, M)} \to H_{q+1}(\underline{y}, M_1) \to \underset{\overset{\nparallel}{0}}{H_q(\underline{y}, M)} \underset{\overset{\parallel}{0}}{\xrightarrow{\cdot x_1}} H_q(\underline{y}, M) \to \cdots$$

$\Rightarrow H_{q+1}(\underline{y}, M_1) \cong H_q(\underline{y}, M) \neq 0$

but $H_{q+1}(\underline{y}, M_1) \neq 0$ and $H_i(\underline{y}, M_1) = 0$ if $i > q+1$.

So $s-1 = n - \sup\{\} = n-(q+1) \Rightarrow s = n-q$. //

Prop: Let A be a Noetherian ring, $I \subseteq A$. Then:

$$\operatorname{depth}(I) \leq \operatorname{ht}(I) \left(= \inf\{ \mathfrak{p} : \mathfrak{p} \underset{\text{prime}}{\supseteq} I \}\right)$$

Pf: If $x_1, \dots, x_n$ max A regular seq.

x_1 is not a zero divisor, so it is not contained in any minimal prime of A.

So $\operatorname{ht}_{A/(x_1)} I/(x_1) < \operatorname{ht}(I)$.

But the images of $x_2, \dots, x_n$ are a maximal $A/(x_1)$ - reg seq. in $I/(x_1)$.

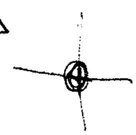
By induction, $\underbrace{\operatorname{depth}(I/(x_1))}_{= n-1} \leq \operatorname{ht}(I/(x_1)) \leq \operatorname{ht}(I) - 1$ //

Def: A ring A is <u>Cohen-Macaulay</u> (CM) if, for every <u>maximal ideal</u> P,

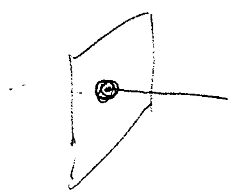
$\operatorname{depth}(P) = \operatorname{ht}(P)$.

(for A a local ring, Cohen-Macaulay iff $\operatorname{depth}(\mathfrak{m}) = \dim A$).

We know that if A is a regular local ring it is Cohen-Macaulay.

Example: $k[X,Y]_{(X,Y)}/(XY) = A$  $\dim A = 1$.

Take $x_1 := X+Y$. It is a regular sequence in $\mathfrak{m}$, which is necessarily maximal. So it is CM.

Example: $A := k[X,Y,Z]_{(X,Y,Z)}/\underbrace{(XY, XZ)}_{= (X) \cap (Y,Z)}$  Call $R := k[X,Y,Z]_{(X,Y,Z)}$

$\dim A = 2$.

Let $\mathfrak{m} = (\overset{x_1}{X-Y}, \overset{x_2}{Y}, \overset{x_3}{Z})$ (try that $\cdot x_1$ is injective ($\cdot X$ is not!)).

$$0 \to A \xrightarrow{\cdot x_1} A \to \underbrace{A/x_1}_{= R/(XY, XZ, X-Y)} \to 0$$

$$R/(XY, XZ, X-Y) \cong k[Y,Z]_{(Y,Z)}/(Y^2, YZ) = A_1$$

Want to show that $H_2 \neq 0$ (the Koszul homology).

$$H_*(x_1, A) = \begin{cases} 0 & \text{if } * > 0 \\ A_1 & \text{if } * = 0 \end{cases}$$

Since $H_i(x_1, A) = 0$ $\forall i \geq 0$, have: $A_1 = k[Z]_{(Z)}$

$$0 \to H_1(x_1, x_2; A) \to A_1 \xrightarrow{\cdot x_2} A_1 \to H_0(x_1, x_2, A) \to 0$$

$$(Y, Z) \cdot A_1 \simeq k[Y,Z]_{(x,y)}/Y \oplus k[Y,Z]_{(Y,Z)}/(Y,Z)$$

$$0 \to H_2(x_1, x_2, x_3) \to H_1(x_1, x_2) \xrightarrow{\cdot x_3} H_1(x_1, x_2). \Rightarrow \text{depth } A = 1.$$

$\cancel{\neq} 0$

Def: A Noeth ring is <u>catenary</u> if $\forall P \supsetneq Q$ primes, all maximal chains between P and Q have the same length.

~~Rk: ... a catenary ring~~

Thm: CM rings are catenary.

Thm: if A is CM, then $A[X]$ is CM.

Lemma: If $P \subseteq A$ is a prime, M a finite A-module and $P \supseteq \text{ann}(M)$,

1) An M-reg sequence in P localizes to an M_P-reg seq in PA_P.

2) If $I \subseteq P$, $\text{depth}(I, M) \leq \text{depth}(I_P, M_P)$.

3) For any ideal I, $\exists Q$ maximal, $Q \supseteq I$, $Q \supseteq \text{ann}(M)$ s.t. $\text{depth}(I, M) = \text{depth}(I_Q, M_Q)$.

Pf (1) clear, localization is exact. $I := (x_1, \dots, x_r)$, M-reg seq in P. $I_P M_P \neq M_P$

As P is in the support of M/IM ($P \supseteq \text{ann}(M/IM) = \text{ann}(M) + I$).

(2) follows from (1).

(3) $I = (x_1, \dots, x_n)$, $r = \text{depth}(I, M)$. So $H := H^A_{n-r}(\underline{x}, M) \neq 0$. in the ring A.

Then if $Q \subseteq A$ is any prime, $H_Q := H \otimes A_Q \simeq H^{A_Q}_{n-r}(\underline{x}, M_Q)$.

Since $H \neq 0$, $I \subseteq \text{ann}(H) \Rightarrow \exists$ maximal ideal in $\text{Supp}(H)$. (so $H_Q \neq 0$).

So $\text{depth}(I_Q, M_Q) \leq r \Rightarrow$ equality using (2).

Prop: (A, m) a local ring, M a finite A-module. $I \subsetneq A$, $y \in m$.

Then $\operatorname{depth}((I, y); M) \leq \operatorname{depth}(I; M) + 1$.

Pf/ $I = (x_1, \ldots, x_n)$. $r = \operatorname{depth}(I + (y); M)$.

Then $H_i(x_1, \ldots, x_n, y; M) = 0$ if $i > (n+1) - r$ (and $\neq 0$ when $i = n+1-r$).

LES:

$H_{i+1}(\underline{x}, y; M) \to H_i(\underline{x}, M) \xrightarrow{\cdot y} H_i(\underline{x}, M) \to H_i(\underline{x}, y; M) \to H_{i-1}(\underline{x}, M) \to \cdots$

So for $i > n+1-r$, $\cdot y$ is an iso between $H_i(\underline{x}, M) \xrightarrow{\sim} H_i(\underline{x}, M)$.

By NAK, $H_i(\underline{x}, M) = 0$ for $i > n+1-r$. So

$\operatorname{depth}((I, y), M) \leq \operatorname{depth}(I, M) + 1$.

Now suppose A local, $Q \subsetneq P$, $\operatorname{ht}_{A/Q} P/Q = 1$.

The principal ideal theorem implies that $\exists\, y \in P$ s.t. P is minimal prime divisor of (Q, y).

Suppose $\operatorname{depth}(Q, y) = r$. $\exists$ max reg. seq. $x_1, \ldots, x_r \in (Q, y) \subseteq P$.

If we wanted to extend this sequence to P.

Take $0 \to A/(x_1, \ldots, x_r) \xrightarrow{\cdot x_{r+1}} A/(x_1, \ldots, x_{r+1})$ for some $x_{r+1} \in P$.

Since P is in $\operatorname{Ass}(A/(Q, y))$, $P = \operatorname{ann}(\bar{z})$, $\underset{\neq 0}{\bar{z}} \in A/(Q, y)$.

So $\bar{z}$ ...

⋮

work with it, and it should work.

E.O.C.