Commutative Algebra

Michaelmas 2021

Why commutative algebra?

Chief motivations

- Algebraic Geometry

$$A = \frac{k[x_1, \ldots, x_n]}{I}$$

(a finitely generated k-algebra, where k is a field).

- Algebraic Number Theory

$\mathbb{Z}$ = integers

$\mathbb{Q} \subseteq K$ a finite field extension,

$$\mathcal{O}_K := \{ t \in K \mid \exists a_1, \ldots, a_n \in \mathbb{Z} \text{ with } t^n + a_1 t^{n-1} + \cdots + a_n = 0 \}$$

the <u>number ring</u> of K

$\mathbb{Q} \subseteq \mathbb{Q}(i)$

$\mathbb{Z} \subseteq \mathbb{Z}[i]$

§ New modules from old

- A be a ring, $(M_i)_{i\in I}$ a collection of A-modules.

Then the direct product

$\prod_{i\in I} M_i$ is the Cartesian product of the M_i with module structure

$$a\cdot(m_i)_{i\in I} = (a\cdot m_i)_{i\in I}$$

The direct sum

$$\bigoplus_{i \in I} M_i \subseteq \prod_{i \in I} M_i$$

is the submodule

$$\left\{ (m_i)_{i \in I} \;\middle|\; \begin{array}{l} \text{all but a finite} \\ \#\text{ of } m_i \text{ are zero} \end{array} \right\}$$

- If M, N are A-modules, so is

$$\mathrm{Hom}_A(M, N) = \{ \varphi : M \to N \mid \varphi \text{ an } A\text{-module hom.} \}$$

A-module structure:

$$(a \cdot \varphi)(m) = a \cdot \varphi(m).$$

- Given $\varphi : M \to N$ an A-module hom.,

$$\ker \varphi = \{ m \in M \mid \varphi(m) = 0 \}$$

$$\operatorname{Im} \varphi = \{ \varphi(m) \mid m \in M \}$$

are A-submodules of M and N respectively.

The <u>cokernel</u> of φ is

$$\operatorname{coker} \varphi := N / \operatorname{Im} \varphi .$$

- A sequence of A-modules and A-module homomorphisms

$$\cdots \longrightarrow M_{i-1} \xrightarrow{\varphi_i} M_i \xrightarrow{\varphi_{i+1}} M_{i+1} \longrightarrow \cdots$$

is *exact* at M_i if

$$\operatorname{im} \varphi_i = \ker \varphi_{i+1}.$$

If the sequence is exact at M_i for every i, we say the sequence is *exact*.

$$0 \to M_1 \xrightarrow{\varphi} M_2 \quad \text{exact}$$

$$\Longleftrightarrow \ker \varphi = 0 \Longleftrightarrow \varphi \text{ is injective.}$$

$$M_1 \xrightarrow{\varphi} M_2 \to 0 \quad \text{is exact}$$

$$\Longleftrightarrow \operatorname{Im} \varphi = M_2 \Longleftrightarrow \varphi \text{ is surjective}$$

$$0 \to M_1 \xrightarrow{\varphi} M_2 \xrightarrow{\psi} M_3 \to 0$$

(a <u>short</u> <u>exact</u> <u>sequence</u>)

is exact if and only if

- φ injective
- ψ surjective,
- ψ induces an isomorphism

$$\frac{M_2}{\ker\psi} = M_2/\operatorname{Im}\varphi = \operatorname{coker}\varphi \cong M_3.$$

(Restatement of Noether's first isomorphism theorem.)

<u>Prop</u>: $M_1 \xrightarrow{\varphi} M_2 \xrightarrow{\psi} M_3 \to 0$ is exact $\iff$ $\forall$ A-modules N

$$0 \to \operatorname{Hom}_A(M_3, N) \xrightarrow{\overline{\psi}} \operatorname{Hom}_A(M_2, N) \xrightarrow{\overline{\varphi}} \operatorname{Hom}_A(M_1, N)$$

where $\overline{\psi}(f) = f \circ \psi$

$$\overline{\varphi}(g) = g \circ \varphi.$$

Pf: Exercise! $\boxtimes$

Prop: $0 \to M_1 \xrightarrow{\varphi} M_2 \xrightarrow{\psi} M_3$ is exact $\Longleftrightarrow$ $\forall$ A-modules N,

$$0 \to \mathrm{Hom}(N, M_1) \xrightarrow{\overline{\varphi}} \mathrm{Hom}(N, M_2) \xrightarrow{\overline{\psi}} \mathrm{Hom}(N, M_3)$$

is exact

$$\overline{\varphi}(f) = \varphi \circ f$$

$$\overline{\psi}(g) = \psi \circ g.$$

Pf: Exercise! $\boxtimes$

Tensor products.

Def: If M, N, P are A-modules, an *A-bilinear map* $f : M \times N \to P$ is a map such that $\forall x \in M$, the map

$$y \mapsto f(x,y)$$

is an A-module hom. $N \to P$

$\forall y \in N$, the map

$$x \mapsto f(x,y)$$

is an A-module hom. $M \to P$.

Prop: M, N A-modules. Then there exists a pair (T, g) where T is an A-module and $g: M \times N \to T$ is bilinear,

satisfying the following universal property:

Given any A-bilinear map $f: M \times N \to P$, there exists a unique A-module homomorphism $f': T \to P$ such that

$$\begin{tikzcd}
M \times N \arrow[r, "g"] \arrow[dr, "f"'] & T \arrow[d, "f'"] \\
& P
\end{tikzcd}$$

$(f' \circ g = f)$ is commutative.

Such data (T, g) is

unique up to unique isomorphism.

<u>Pf:</u> <u>Uniqueness:</u>

Suppose we have two such pairs (T, g), (T', g').

Apply the universal property for (T, g) to the bilinear map $g' : M \times N \to P'$:

$$\begin{tikzcd} M \times N \arrow[r, "g"] \arrow[dr, bend right, "g'"'] & T \arrow[d, "\exists! \varphi"] \\ & T' \end{tikzcd}$$

Reversing roles of (T, g), (T', g')

gives similarly a hom. $\varphi : T' \to T$.

$\varphi \circ \psi$ fits into a commutative diagram

$$
\begin{tikzcd}
M \times N \arrow[r, "g"] \arrow[dr, "g'"'] \arrow[ddr, "g"'] & T \arrow[d, "\psi"] \arrow[dd, bend left=60, "\varphi \circ \psi"] \\
& T' \arrow[d, "\varphi"] \\
& T
\end{tikzcd}
$$

By the universal property for (T, g) applied to $g : M \times N \to T$,

we must have $\varphi \circ \psi = id_T$

by uniqueness of map.

Similarly $\psi \circ \varphi = id_{T'}$.

Existence:

$$C = \bigoplus_{i \in M \times N} A \quad (\text{H-ge!})$$

i.e., formal (finite) linear combinations of elements of $M \times N$ with coefficients in A, i.e.,

$$\sum_{i=1}^{k} a_i (m_i, n_i).$$

Let $D \subseteq C$ be the submodule generated by all elements of C of the form

$$(m+m', n) - (m,n) - (m',n)$$

$$(m, n+n') - (m,n) - (m,n')$$

$$(am, n) - a\cdot(m,n)$$

$$(m, an) - a\cdot(m,n)$$

(all $m \in M$, $n \in N$.)

Set $T = C/D$.

Let's denote by $m \otimes n$ the image (m,n) in T.

The above relations translate to

$$(m+m')\otimes n = m\otimes n + m'\otimes n$$

$(*)$ $$m\otimes(n+n') = m\otimes n + m\otimes n'$$

$$(am)\otimes n = a(m\otimes n) = m\otimes(an)$$

Define $g: M\times N \to T$

by $g(m,n) = m\otimes n$.

$\circledast \Rightarrow g$ is A-bilinear.

This gives the pair (T, g).

Check this satisfies the universal property:

Let $f : M \times N \longrightarrow P$ be given.

Then define

$$\bar{f} : C \longrightarrow P$$

$$\bar{f}\left(\sum_i a_i (m_i, n_i) \right) = \sum_i a_i f(m_i, n_i).$$

By bilinearity of f,

$$D \subseteq \ker \bar{f}.$$

Hence $\bar{f}$ induces a map

$$f' : T = C/D \longrightarrow P, \quad \text{and}$$

$$f'(g(m,n)) = f'(m \otimes n) = \bar{f}(m,n)$$
$$= f(m,n)$$

so $f' \circ g = f$.

The requirement that $f' \circ g = f$ uniquely determines f'.

$\blacksquare$

<u>Def</u>: We write T as constructed above as $M \otimes_A N$. the <u>tensor product</u> of M and N.

<u>Remark</u>: This extends to multilinear maps

$$f : M_1 \times \cdots \times M_r \longrightarrow P$$

giving $M_1 \otimes_A M_2 \otimes_A \cdots \otimes_A M_r \to P.$

Remark: There exists canonical isomorphisms

① $M \otimes_A N \xrightarrow{\cong} N \otimes_A M$

$m \otimes n \longmapsto n \otimes m$

② $(M \otimes_A N) \otimes_A P \xrightarrow{\cong} M \otimes_A (N \otimes_A P)$

$\xrightarrow{\cong} M \otimes_A N \otimes_A P.$

③ $(M \oplus N) \otimes_A P \cong (M \otimes_A P) \oplus (N \otimes_A P)$

$(m, n) \otimes p \longmapsto (m \otimes p, n \otimes p)$

(i.e., first define a bilinear map

$(M \oplus N) \times P \longrightarrow (M \otimes_A P) \oplus (N \otimes_A P)$

and then use universal property.)

(4) $A \otimes_A M \xrightarrow{\cong} M$

$a \otimes x \longmapsto ax$

Remark: $\varphi : A \to B$ a ring homomorphism

M an A-module.

Then $B \otimes_A M$ is a B-module

via $b \cdot (b' \otimes m) := (bb') \otimes m$

This gives a way of going

from A-modules to B-modules.

Remark: $\varphi : A \to B$ a ring hom,

N a B-module, then N is

also an A-module via

$$a \cdot n = \varphi(a) \cdot n.$$

<u>Remark</u>: Let $\varphi_i : A \to B_i$ be ring homomorphisms, $i = 1, 2$. Then $B_1 \otimes_A B_2$ has the structure of a ring via

$$(b_1 \otimes b_2)(b_1' \otimes b_2') = b_1 b_1' \otimes b_2 b_2'.$$

[<u>Exercise</u>: Check this is well-defined and gives a ring structure on $B_1 \otimes_A B_2$.]

In fact, this tensor product of rings satisfies the following universal property:

There exists a diagram

$$\begin{tikzcd}
b_1 \otimes 1 & B_1 \otimes_A B_2 & B_2 \arrow[l] \\
b_1 \arrow[u, mapsto] & B_1 \arrow[u] & A \arrow[l, "\varphi_1"] \arrow[u, "\varphi_2"']
\end{tikzcd}$$

$$1 \otimes b_2 \longleftarrow b_2$$

Commutative:

$\varphi_1(a) \otimes 1 =$

$(a \cdot 1) \otimes 1$

$= 1 \otimes (a \cdot 1)$

$= 1 \otimes \varphi_2(a)$

such that for any commutative diagram of rings

$$\begin{tikzcd}
R & B_2 \arrow[l, "f_2"'] \\
B_1 \arrow[u, "f_1"] & A \arrow[l, "\varphi_1"] \arrow[u, "\varphi_2"']
\end{tikzcd}$$

there exists a unique $g : B_1 \otimes_A B_2 \longrightarrow R$

making

$$\begin{tikzcd}
R & & \\
& B_1 \otimes_A B_2 \arrow[ul, "g"'] & B_1 \arrow[l] \arrow[ull, bend right, "f_2"'] \\
& B_2 \arrow[u] \arrow[uul, bend left, "f_1"] & A \arrow[l, "\varphi_1"] \arrow[u, "\varphi_2"']
\end{tikzcd}$$

commute. Note $g(b_1 \otimes b_2) = f_1(b_1) \cdot f_2(b_2)$

[*Exercise*: Check this!]

Remark: This says $\otimes$ is the fibred sum in the category of rings.

Prop: Let M, N, P be A-modules.

Then $\exists$ a canonical isomorphism

$$\mathrm{Hom}_A(M \otimes_A N, P) \cong \mathrm{Hom}_A(M, \mathrm{Hom}_A(N, P))$$

[Hom, $\otimes$ are adjoint functors.]

Pf: $\mathrm{Hom}_A(M \otimes_A N, P) = \mathrm{Bil}_A(M \times N, P)$,

where Bil_A denotes the set of bilinear maps $M \times N \to P$. (Universal property)

We also have a map

$$\mathrm{Bil}_A(M \times N, P) \longrightarrow \mathrm{Hom}_A(M, \mathrm{Hom}_A(N, P))$$

$$f \longmapsto (m \mapsto (n \mapsto f(m,n)))$$

(that the latter map is an A-module hom. is the def'n of bilinear.)

Conversely, we have a map

$$\mathrm{Hom}_A(M, \mathrm{Hom}_A(N,P)) \longrightarrow \mathrm{Bil}_A(M \times N, P)$$

$$f \longmapsto ((m,n) \mapsto f(m)(n))$$

Check these maps are inverse to

each other. $\blacksquare$

<u>Prop</u>: Let

$$M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3 \to 0$$

be ~~an~~ exact sequence of A-modules, N an A-module. Then

$$(*) \quad M_1 \otimes_A N \xrightarrow[f\otimes 1]{} M_2 \otimes_A N \xrightarrow[g \otimes 1]{} M_3 \otimes_A N \to 0$$

is exact

where
$$(f \otimes 1)(m_1 \otimes n) = f(m_1) \otimes n$$
$$(g \otimes 1)(m_2 \otimes n) = g(m_2) \otimes n.$$

<u>Pf</u>: By Prop. about exactness properties of $\mathrm{Hom}_A(\cdot, P)$, $(*)$ is exact if and only if

$$0 \to \mathrm{Hom}(M_3 \otimes N, P) \to \mathrm{Hom}(M_2 \otimes N, P)$$

$$\to \mathrm{Hom}(M_1 \otimes N, P)$$

is exact for all A-modules P.

But this is

$$0 \to \mathrm{Hom}(M_3, \mathrm{Hom}(N, P)) \to \mathrm{Hom}(M_2, \mathrm{Hom}(N, P))$$

$$\to \mathrm{Hom}(M_1, \mathrm{Hom}(N, P))$$

which is exact because

$M_1 \to M_2 \to M_3 \to 0$ is exact.

<u>Example</u>: $\otimes$ does not preserve injectivity in general:

$$0 \to \mathbb{Z} \xrightarrow[f]{\cdot 2} \mathbb{Z}$$

(hom. of $\mathbb{Z}$-modules)

Apply $\otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z}$

$$\begin{tikzcd}
\mathbb{Z}\otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z} \arrow[r, "f\otimes 1", "\text{i.e. } 0"'] \arrow[d, phantom, "\wr"] & \mathbb{Z}\otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z} \arrow[d, phantom, "\wr"] \\
\mathbb{Z}/2\mathbb{Z} & \mathbb{Z}/2\mathbb{Z}
\end{tikzcd}$$

$$\begin{aligned}
(f\otimes 1)(a\otimes b) &= f(a)\otimes b \\
&= 2a\otimes b \\
&= a\otimes (2\cdot b) \\
&= a\otimes 0 \\
&= 0.
\end{aligned}$$

Thus $\otimes$ doesn't preserve injectivity.

<u>Def</u>: An A-module N is <u>flat</u>

if whenever $0\to M_1\to M_2$ is exact,

$$0\to M_1\otimes_A N\to M_2\otimes_A N \text{ is exact.}$$

Examples: $N = A$.

$$N = A \oplus \cdots \oplus A$$

$$M_i \otimes_A N = (M_i \otimes_A A) \oplus \cdots \oplus (M_i \otimes_A A)$$

$$= M_i \oplus \cdots \oplus M_i$$

Def: A free A-module is a module isomorphic to

$\bigoplus_{i \in I} A$ for some index set I

(I may be infinite.)

Prop: M is a finitely generated A-module (f.g. A-module)

$\iff$ M is isomorphic to a quotient of $A^n = \underbrace{A \oplus \cdots \oplus A}_{n \text{ copies}}$ for some n.

Pf: $\Rightarrow$ Let $m_1, \dots, m_n$ generate M.

Define $\varphi : A^n \longrightarrow M$

$$(a_1, \dots, a_n) \longmapsto \sum_{i=1}^{n} a_i m_i .$$

φ is surjective, so

$M \cong A^n / \ker \varphi$, by Noether's first isomorphism theorem.

$\Leftarrow$ Have a surjection

$$A^n \to M$$

$$(0, \dots, 1, \dots 0) \longmapsto m_i$$

$\uparrow$

i^{th} place

(since M is assumed ~~to~~ be a quotient of A^n).

Then $m_1, \dots, m_n$ generate M since the quotient map is surjective. $\boxtimes$

Prop: Let M be a f.g. A-module, $I \subseteq A$ an ideal, $\phi : M \to M$ an A-module homomorphism such that

$$\phi(M) \subseteq I \cdot M = \left\{ \sum a_i m_i \mid a_i \in I, m_i \in M \right\}$$

Then ϕ satisfies an equation of the form

$$\phi^n + a_1 \phi^{n-1} + \cdots + a_n = 0$$

with all $a_i \in I$.

Pf: Let $m_1, \ldots, m_n$ be generators of M, so since $\phi(m_i) \in I \cdot M$,

i.e., $\phi(m_i) = \sum_{j=1}^{n} a_{ij} m_j$ with $a_{ij} \in I$.

So $$\sum_{j=1}^{n} (\delta_{ij} \phi - a_{ij}) m_j = 0$$

$$\delta_{ij} = \begin{cases} 0 & i \neq j \\ 1 & i = j \end{cases}$$

Multiply this equation on the left

by the adjoint matrix to

$$(\delta_{ij}\phi - a_{ij})_{\substack{1 \le i \le n \\ 1 \le j \le n}}$$

This gives

$$\det(\delta_{ij}\phi - a_{ij}) \cdot m_j = 0$$

$\forall j$.

Thus $\det(\delta_{ij}\phi - a_{ij})$ is the

0 endomorphism of M,

and expanding determinant gives

the desired equation. $\square$

Cor: Let M be a f.g. A-module, $I \subseteq A$ an ideal such that $IM = M$. Then there exists $a \equiv 1 \mod I$ such that $aM = 0$.

Pf: Take $\phi = id$. Take

$$a = 1 + a_1 + \cdots + a_n, \quad a_1, \ldots, a_n \in I$$

So $a \equiv 1 \mod I$

and $a \cdot M = 0$. ▧

Def: The Jacobson radical of a ring A is the intersection of all maximal ideals of A.

Nakayama's Lemma: Let M be f.g. A-module, $I \subseteq A$ an ideal contained in the Jacobson radical of A.

Then $IM = M$ implies $M = 0$.

Pf: By Cor., there exists an $a \in A$ with $a \equiv 1 \mod I$ and $a \cdot M = 0$.

So $1 - a \in I$. If a is not invertible, there exists a maximal ideal $m \subseteq A$ containing a.

But $1 - a \in I \subseteq m$. Thus $a, 1-a \in m$, so $1 \in m$, a contradiction.

Thus a is invertible, and

$$M = a^{-1}(aM) = 0. \quad \boxtimes$$

Cor: Let M be a f.g. A-module, $N \subseteq M$ a submodule, $I \subseteq A$

an ideal contained in the Jackson radical of A. Then

$$M = IM + N \Rightarrow M = N.$$

<u>Pf</u>: Apply Nakayama's Lemma to M/N, using

$$I(M/N) = (IM+N)/N,$$

so $M = IM + N \Rightarrow I(M/N) = M/N$

$$\Rightarrow M/N = 0$$

$$\Rightarrow M = N. \quad \blacksquare$$

<u>Def</u>: A ring A is <u>local</u> if it has a unique maximal ideal. We usually write (A, m) where m is the unique maximal ideal of A.

Prop: Let (A, m) be a local ring, M a f.g. A-module, and let $m_1, \dots, m_n \in M$ such that their images $\bar{m}_1, \dots, \bar{m}_n \in M/mM$ form a basis for M/mM as an A/m-vector space. Then the m_i generate M as an A-module.

Pf: Let $N \subseteq M$ be the submodule generated by $m_1, \dots, m_n$. $= \{\sum a_i m_i \mid a_i \in m, m_i \in M\}$

Have a composition

$$N \hookrightarrow M \longrightarrow M/mM$$

which is surjective by assumption.

Thus $N + mM = M$, so $N = M$ by Cor. to Nakayama's Lemma. ∎

Localization:

A an integral domain

$\rightsquigarrow K(A)$ = field of fractions of A

$= \{(a,t) \mid a, t \in A,\ t \neq 0\}/\sim$

with $(a,t) \sim (a', t')$ if

$at' = a't$.

We write the equivalence class of (a,t)

as a/t.

<u>Note</u>: If A were not an integral domain, this would not be an equivalence relation.

<u>Def</u>: Let A be any ring. A <u>multiplicatively closed subset</u> $S \subseteq A$

is a subset with $1 \in S$ and

$s_1 \cdot s_2 \in S$ whenever $s_1, s_2 \in S$.

$$\frac{a}{1}$$

$$\frac{a}{s} \cdot \frac{a'}{s'} = \frac{aa'}{ss'}$$

Given $S \subseteq A$ multiplicatively closed, define a relation on $A \times S$

by $(a, s) \sim (b, t)$

$$\iff (at - bs)u = 0$$

for some $u \in S$.

<u>Check this is an equivalence relation:</u>

Reflexive, symmetric ✓

<u>Transitivity:</u> $(a, s) \sim (b, t)$, $(b, t) \sim (c, u)$

$\Rightarrow \exists\, v, w \in S$ such that

$$(at - bs)v = 0 \quad \text{and} \quad (bu - tc)w = 0$$

Multiply first equation by uw and

second equation by sv and add:

$$0 = atvuw - ctwsv$$

$$= (au - cs)\,tvw$$

hence $(a,s) \sim (u,c)$.

Remark: If $0 \in S$, then $A \times S$ consists of a single equivalence class.

We write $S^{-1}A$ for the set of equivalence classes of $\sim$ on $A \times S$, and write the equivalence class of (a,s) as $\frac{a}{s}$.

We give $S^{-1}A$ a ring structure

$$\frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st}, \quad -\left(\frac{a}{s}\right) = \frac{-a}{s}$$

$$\left(\frac{a}{s}\right)\left(\frac{b}{t}\right) = \frac{ab}{st}.$$

Exercise: Check these operations satisfy the ring axioms.

Def: We say $S^{-1}A$ is the **localization** of A at S.

Example: A an integral domain,

$S = A \setminus \{0\}$,

$S^{-1}A$ = field of fractions of A.

Examples (key) (1) Let $\mathfrak{p} \subseteq A$ be a prime ideal (A arbitrary).

Then $S = A \setminus \mathfrak{p}$ is multiplicatively closed ($s_1, s_2 \notin \mathfrak{p} \Rightarrow s_1 \cdot s_2 \notin \mathfrak{p}$)

We write
$$A_{\mathfrak{p}} := S^{-1}A,$$
the <u>localization</u> of A at $\mathfrak{p}$.

(2) If $f \in A$, then

$S = \{1, f, f^2, \dots\}$ is multiplicatively closed.

We write
$$A_f := S^{-1}A,$$
the localization of A at f.

<u>Example</u>: $A = \mathbb{Z}$,

$\mathfrak{p} = (2)$

$$A_{\mathfrak{p}} = \left\{ \frac{a}{b} \in \mathbb{Q} \;\middle|\; 2 \nmid b \right\}.$$

$f = 2$

$$A_2 := \left\{ \frac{a}{2^n} \in \mathbb{Q} \;\middle|\; n \geq 0 \right\}.$$

<u>Universal property</u>: Let $S \subseteq A$ be multiplicatively closed. Then for every ring hom. $g: A \to B$ with $g(s)$ is invertible $\forall s \in S$, $\exists$ a unique factorization

$$A \xrightarrow{f} S^{-1}A \xrightarrow{h} B$$

of g, where $f(a) = \frac{a}{1}$

<u>Pf: Uniqueness:</u> If h satisfies the condition, then

$$h\left(\frac{a}{1}\right) = h(f(a)) = g(a)$$

$$h\left(\frac{1}{s}\right) = h\left(\left(\frac{s}{1}\right)^{-1}\right) = h\left(\frac{s}{1}\right)^{-1}$$

$$= g(s)^{-1}$$

Thus $h\left(\frac{a}{s}\right) = h\left(\frac{a}{1} \cdot \frac{1}{s}\right) = g(a) \cdot g(s)^{-1}$.

<u>Existence:</u> Need to check that if

we define $h\left(\frac{a}{s}\right) := g(a)\, g(s)^{-1}$,

then h is well-defined, and a <u>ring hom.</u>

Exercise

So if $\frac{a}{s} = \frac{a'}{s'}$, i.e., $\exists\, t \in S$

with $(as' - a's)\, t = 0$. Then

$$(g(a)g(s') - g(a')g(s))\, g(t) = 0$$

Since $g(t)$ is invertible, we get

$$g(a)g(s') - g(a')g(s) = 0$$

or $$g(a)g(s)^{-1} = g(a')g(s')^{-1}$$

This shows well-definedness. $\boxtimes$

Localization of modules:

$S \subseteq A$ mult. closed,

M an A-module.

Define $S^{-1}M = M \times S / \sim$

where $(m, s) \sim (m', s')$ if $\exists t \in S$

such that $t(ms' - m's) = 0$.

Write the equivalence class of (m, s)

as $\frac{m}{s}$, define addition

$$\frac{m}{s} + \frac{m'}{s'} = \frac{s'm + sm'}{ss'}$$

and $S^{-1}A$-module structure by

$$\frac{a}{s} \cdot \frac{m}{s'} = \frac{a \cdot m}{ss'}.$$

So $S^{-1}M$ is an $S^{-1}A$-module.

Prop: There exists a unique isomorphism

$$f : S^{-1}A \otimes_A M \longrightarrow S^{-1}M$$

such that $f\left(\frac{a}{s} \otimes m\right) = \frac{am}{s}$.

Pf: Have a bilinear map

$$S^{-1}A \times M \longrightarrow S^{-1}M$$

$$\left(\frac{a}{s}, m\right) \longmapsto \frac{am}{s},$$

hence inducing an A-module homomorphism f.

- Surjectivity of f is obvious
$$f\left(\frac{1}{s} \otimes m\right) = \frac{m}{s}.$$
- Uniqueness of f follows from the universal property of the tensor product.

• Injective: An arbitrary element of $S^{-1}A \otimes_A M$ can be written as

$$\sum_i \frac{a_i}{s_i} \otimes m_i$$

Let $t_i = \prod_{j \neq i} s_j$, $s = \prod_j s_j$

Then

$$\sum_i \frac{a_i}{s_i} \otimes m_i = \sum_i \frac{a_i t_i}{s_i t_i} \otimes m_i$$

$$= \sum_i \frac{a_i t_i}{s} \otimes m_i$$

$$= \sum_i \frac{1}{s} \otimes a_i t_i m_i$$

$$= \frac{1}{s} \otimes \sum_i a_i t_i m_i .$$

So every element of $S^{-1}A \otimes_A M$

is of the form $\frac{1}{s} \otimes m$ for some

$s \in S$, $m \in M$.

Suppose $f\left(\frac{1}{s} \otimes m\right) = 0$.

Then $\frac{m}{s} = \frac{0}{1}$, $\exists\, t \in S$ such that

$$(m \cdot 1 - s \cdot 0)t = 0, \quad \text{i.e.,} \quad mt = 0.$$

So $$\frac{1}{s} \otimes m = \frac{t}{st} \otimes m = \frac{1}{st} \otimes tm$$
$$= \frac{1}{st} \otimes 0 = 0.$$

Thus f is injective. $\blacksquare$

Remark: This is defined as a map of A-modules, but is also a map of $S^{-1}A$-modules:

$$f\left(\frac{a}{s} \cdot \left(\frac{a'}{s'} \otimes m\right)\right) = f\left(\frac{aa'}{ss'} \otimes m\right)$$
$$= \frac{aa'm}{ss'} = \frac{a}{s} \cdot f\left(\frac{a'}{s'} \otimes m\right)$$

Remark: $S^{-1}M$ is also an A-module

via $a \cdot \left(\frac{m}{s}\right) = \frac{am}{s}$.

Prop: S^{-1} preserves exact sequences,

i.e., if [S^{-1} is an exact functor]

$$M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3$$

is exact, so is

$$S^{-1}M_1 \xrightarrow{S^{-1}f} S^{-1}M_2 \xrightarrow{S^{-1}g} S^{-1}M_3$$

where $(S^{-1}f)\left(\frac{m}{s}\right) = \frac{f(m)}{s}$.

($S^{-1}f$ is an $S^{-1}A$-module homomorphism.)

Pf: $g \circ f = 0$ since $\operatorname{im} f \subseteq \ker g$,

so $S^{-1}g \circ S^{-1}f = 0$, so

$\operatorname{im} S^{-1}f \subseteq \operatorname{Ker} S^{-1}g.$

If $\frac{m}{s} \in \operatorname{Ker} S^{-1}g$, so

$$\frac{g(m)}{s} = 0 \quad \text{in} \quad S^{-1}M_3$$

i.e., $\exists\, t \in S$ with $t\,g(m) = 0$, in M_3.

But $0 = t\,g(m) = g(tm)$, so

$tm \in \operatorname{Ker} g$ so $\exists\, m' \in M_1$ with

$f(m') = tm$ (since $\operatorname{Ker} g = \operatorname{im} f$).

In $S^{-1}M_2$

$$\frac{m}{s} = \frac{mt}{st} = \frac{f(m')}{st} = (S^{-1}f)\left(\frac{m'}{st}\right).$$

So $\frac{m}{s} \in \operatorname{Im} S^{-1}f.$

Thus $\operatorname{Ker} S^{-1}f = \operatorname{Im} S^{-1}f.$ ☒

<u>Cor</u>: $S^{-1}A$ is a flat A-module.

<u>Local properties</u>: A property P of A (or M or $f: M \to N$) is <u>local</u> if A (M, f etc.) has property P if and only if $A_{\mathfrak{p}}$ ($M_{\mathfrak{p}}$, $f_{\mathfrak{p}}$ etc.) has property P for all primes $\mathfrak{p}$ of A.

<u>Prop</u>: Let M be an A-module. Then the following are equivalent:

1. $M = 0$.
2. $M_{\mathfrak{p}} = 0$ $\forall \mathfrak{p}$ prime
3. $M_{\mathfrak{m}} = 0$ $\forall \mathfrak{m}$ maximal.

Pf: ① $\Rightarrow$ ② $\Rightarrow$ ③ Trivial.

③ $\Rightarrow$ ①. Suppose ③ holds but $M \neq 0$.

Let $x \in M$, $x \neq 0$, and let

$$I = \mathrm{Ann}(x) := \{ a \in A \mid ax = 0 \}.$$

(This is an ideal.) Note $I \neq (1) = A$

since $x \neq 0$.

We have $I \subseteq m$ a maximal ideal.

Then $0 = \frac{x}{1} \in M_m$, so there exists

$a \in A \setminus m$ with $ax = 0$. So $a \in \mathrm{Ann}(x) = I$,

but $a \notin m$, a contradiction. ▨

Prop: Let $\varphi: M \to N$ be an A-module hom. Then the following are equivalent:

① φ is injective (surjective)

② $\varphi_{\mathfrak{p}} : M_{\mathfrak{p}} \to N_{\mathfrak{p}}$ is injective (surjective) $\forall$ primes $\mathfrak{p}$.

③ $\varphi_{\mathfrak{m}} : M_{\mathfrak{m}} \to N_{\mathfrak{m}}$ is injective (surjective) $\forall$ maximal ideals $\mathfrak{m}$.

Pf (for injective)

① $\Rightarrow$ ② $\quad 0 \to M \xrightarrow{\varphi} N$ is exact

$\Rightarrow \quad 0 \to M_{\mathfrak{p}} \to N_{\mathfrak{p}}$ is exact $\forall \mathfrak{p}$.

② $\Rightarrow$ ③ ✓

③ $\Rightarrow$ ①. Let $M' = \ker \varphi$.

so $0 \to M' \to M \to N$ exact, so

$0 \to M'_{\mathfrak{m}} \to M_{\mathfrak{m}} \xrightarrow{\varphi_{\mathfrak{m}}} N_{\mathfrak{m}}$ is exact.

So $M'_m = 0$ $\forall m$ maximal.

Thus $M' = 0$, so φ is injective. $\square$

Behavior of ideals under localization

Given a ring hom. $\varphi : A \to B$, we can go between ideals in the two rings:

$I \subseteq A \rightsquigarrow I^e =$ "the extended ideal"

$=$ ideal generated by $\varphi(I)$.

[In general, $\varphi(I)$ won't be an ideal!

e.g. $\varphi : \mathbb{Z} \to \mathbb{Q}$, $\varphi((n)) = n\mathbb{Z}$

$(n)^e = \mathbb{Q}$.]

$J \subseteq B \rightsquigarrow J^c = \varphi^{-1}(J)$.

an ideal of A.

= "the contracted ideal."

$I \subseteq A$, I^{ece}

Apply this notation to the canonical

map $\varphi : A \longrightarrow S^{-1}A$

$$\varphi(a) = \frac{a}{1}.$$

<u>Def</u>: $I, J \subseteq A$ are ideals, the <u>ideal quotient</u>

$$(I : J) = \{ x \in A \mid xJ \subseteq I \}$$

<u>Example</u>: $A = \mathbb{Z}$

$$((n_1) : (n_2)) = \{ n \in \mathbb{Z} \mid n n_2 \in I \}$$

$$= \{ n \in \mathbb{Z} \mid n_1 \mid n n_2 \}$$

$$= \left(\frac{\operatorname{lcm}(n_1, n_2)}{n_2} \right).$$

Prop: ① Every ideal in $S^{-1}A$ is an extended ideal under the map $\varphi : A \to S^{-1}A$.

② If $I \subseteq A$ then

$$I^{ec} = \bigcup_{s \in S} (I : (s))$$

and $I^e = (1) \iff I \cap S \neq \emptyset$.

③ Let C be the set of contracted ideals in A. Then

$I \in C \iff$ no element of S is a 0-divisor in A/I.

④ The prime ideals of $S^{-1}A$ are in one-to-one correspondence with the prime ideals of A disjoint from S.

Remark: We usually write for $I \subseteq A$,

$I^e = S^{-1} I$, thinking I as an

A-module.

Pf: (1) Let $I \subseteq S^{-1}A$ be an ideal, $\frac{a}{s} \in I$. Then $\frac{a}{1} = s \cdot \left(\frac{a}{s}\right) \in I$,

so $a \in I^c \subseteq A$. So $\frac{a}{s} \in I^{ce}$.

Thus $I \subseteq I^{ce}$. On the other hand $I^{ce} \subseteq I$ for any $\varphi : A \to B$. Thus $I = I^{ce}$.

(2) $a \in I^{ec} = (S^{-1} I)^c$

$\iff \frac{a}{1} = \frac{b}{s}$ for some $b \in I$, $s \in S$

$\iff (as - b)t = 0$ for some $t \in S$

$\Leftrightarrow$ $ast \in I$ for some $s, t \in S$

$\Leftrightarrow$ $a \in (I : (st))$ for some $s, t \in S$.

$\Leftrightarrow$ $a \in \bigcup_{s \in S} (I : (s))$.

In particular, $I^e = (1)$

$\Leftrightarrow$ $I^{ec} = (1)$

$\Leftrightarrow$ $1 \in \bigcup_{s \in S} (I : s)$

$\Leftrightarrow$ $\exists s$ such that $s \in I$

$\Leftrightarrow$ $I \cap S \neq \phi$.

③ Note $I \subseteq I^{ec}$ always. Then first I claim that

$I \in C \Leftrightarrow I^{ec} \subseteq I$.

[$\Rightarrow$): If $I = J^c$, then $J \underset{\uparrow \text{ by ①}}{=} J^{ce} = I^e$,

so $I^{ec} = J^c = I$.

$\Leftarrow$: $I^{ec} \subseteq I \Rightarrow I^{ec} = I \Rightarrow I \in C]$.

Note $I^{ec} \subseteq I$ is equivalent, by (2)

to the statement

$$s \cdot a \in I \text{ for some } s \in S \Rightarrow a \in I,$$

which is equivalent to no element

of S being a 0-divisor in A/I.

(4) If $\varphi : A \to B$ is any ring hom,

$\mathfrak{p} \subseteq B$ is a prime ideal, then

$\varphi^{-1}(\mathfrak{p})$ is prime [See first example sheet.]

Conversely, if $\mathfrak{p} \subseteq A$ is prime,

then $A/\mathfrak{p}$ is an integral domain,

and $S^{-1}A / S^{-1}\mathfrak{p} \cong S^{-1}(A/\mathfrak{p})$

$\cong \bar{S}^{-1}(A/\mathfrak{p})$ where $\bar{S}$ is the image of S in $A/\mathfrak{p}$.

Now $\bar{S}^{-1}(A/\mathfrak{p}) = 0 \iff \frac{1}{1} = 0$

$\iff 0 \in \bar{S}$

Otherwise, $\bar{S}^{-1}(A/\mathfrak{p})$ is contained in the field of fractions of $A/\mathfrak{p}$, thus $\bar{S}^{-1}(A/\mathfrak{p})$ is an integral domain, so $S^{-1}\mathfrak{p} = \mathfrak{p}^e$ is prime.

Note $0 \in \bar{S} \iff \mathfrak{p} \cap S \neq \emptyset$.

This gives 1-1 correspondence:

$$\left\{\begin{array}{c}\text{primes in } A \\ \text{disjoint from } S\end{array}\right\} \qquad \left\{\begin{array}{c}\text{primes of} \\ S^{-1}A\end{array}\right\} \quad \blacksquare$$

$$\mathfrak{p}^c \longleftarrow\!\shortmid \ \mathfrak{p}$$

$$\mathfrak{p} \longmapsto S^{-1}\mathfrak{p} = \mathfrak{p}^e.$$

<u>Remark</u>: If $\mathfrak{p} \subseteq A$ is prime,

$$A_{\mathfrak{p}} := (A \setminus \mathfrak{p})^{-1} A,$$

and the primes of $A_{\mathfrak{p}}$ are in 1-1 correspondence with primes of A contained in $\mathfrak{p}$.

So in this case $\mathfrak{p}^e$ is the unique maximal ideal.

Often we write this maximal ideal as $\mathfrak{p} A_{\mathfrak{p}}$.

So $(A_{\mathfrak{p}}, \mathfrak{p} A_{\mathfrak{p}})$ is a local ring.

<u>Remark</u>: Local rings appear naturally

in geometry

Geometry = topological space + some notion of function on this space.

<u>e.g.</u> X a top. space, cts. $\mathbb{R}$-valued functions,

X a C^∞ manifold, C^∞ $\mathbb{R}$-valued functions

X a complex manifold, holomorphic $\mathbb{C}$-valued functions

X an algebraic variety, regular (polynomial) functions.

$x \in X$,

$$\mathcal{O}_{X,x} = \{ (U, f) \mid x \in U \subseteq X, \ U \text{ open}, \ f \text{ a function on } U \} / \sim$$

$(U, f) \sim (V, g)$ if

$\exists\ x \in W \subseteq U \cap V$ with $f|_W = g|_W$.

$\mathcal{O}_{X,x}$ is a local ring, with maximal ideal $m_x = \{ (U, f) \mid f(x) = 0 \}$

If $(U, f) \in \mathcal{O}_{X,x} \setminus m_x$, then

(U, f) is invertable, i.e.,

$(U, f)^{-1} = (U \setminus \{ y \mid f(y) = 0 \}, f^{-1})$

Thus m_x is the only maximal ideal.

Primary Decomposition

Motivation: Suppose A is a UFD (e.g. $A = \mathbb{Z}$)

$a \in A$ factors as

$$a = u \prod_i p_i^{e_i}$$

with p_i distinct primes, $(p_i) \neq (p_j)$

Could write this as

$$(a) = \bigcap_i (p_i^{e_i})$$

Note $(p_i^{e_i})$ is not a prime ideal, but "close" to being a prime ideal. (It's called a *primary* ideal.)

Generalization: We will look for decompositions

$$I = \bigcap_i q_i$$

where $I \subseteq A$ is an arbitrary ideal

and the q_i are primary ideals

<u>Def</u>: An ideal $I \subseteq A$ is <u>primary</u>

if whenever $a \cdot b \in I$, either $a \in I$

or $b^n \in I$ for some $n > 0$.

<u>Note</u>: We may generalize further,

replacing A and I by

an A-module M and a submodule N.

Then we look for for decompositions

$$N = \bigcap_i N_i$$

where the N_i are "primary submodules"

Fix now a Noetherian ring A.

Def: Let M be an A-module. We say a prime $\mathfrak{p}$ of A is an associated prime of M if one of the following equivalent conditions holds:

① $\exists\, x \in M$ with

$$\mathfrak{p} = \mathrm{Ann}(x) := \{a \in A \mid ax = 0\}.$$

② M has a submodule isomorphic to $A/\mathfrak{p}$.

[① $\Rightarrow$ ② The submodule generated by $x \in M$ is $A/\mathrm{Ann}(x) = A/\mathfrak{p}$.

② $\Rightarrow$ ① If $N \subseteq M$ with $N \cong A/\mathfrak{p}$, then if $x \in N$, $x \neq 0$, $\mathrm{Ann}(x) = \mathfrak{p}$.]

The set of associated primes of M is written $\mathrm{Ass}(M)$ or $\mathrm{Ass}_A(M)$.

<u>Prop</u>: Let $\mathfrak{p}$ be a maximal element of the set of ideals

$$\{ \mathrm{Ann}(x) \mid x \in M, \ x \neq 0 \}.$$ Then

$\mathfrak{p} \in \mathrm{Ass}(M)$

<u>Pf</u>: We need to show $\mathfrak{p}$ is prime.

Let $\mathfrak{p} = \mathrm{Ann}(x)$, and suppose $ab \in \mathfrak{p}$, $b \notin \mathfrak{p}$. Then $bx \neq 0$, and $abx = 0$, so $a \in \mathrm{Ann}(bx)$. But $\mathrm{Ann}(x) \subseteq \mathrm{Ann}(bx)$ so $\mathrm{Ann}(x) = \mathrm{Ann}(bx)$ by maximality of $\mathfrak{p}$. So $a \in \mathrm{Ann}(x) = \mathfrak{p}$. So $\mathfrak{p}$ is prime. $\blacksquare$

Cor: $\mathrm{Ass}(M) = \phi \iff M = 0$.

Pf: $\Leftarrow$ ✓

$\Rightarrow$ $M \neq 0 \Rightarrow$ set $\{\mathrm{Ann}(x) \mid x \in M \setminus \{0\}\}$
$\neq \phi$,

and this set necessarily has maximal elements since A is Noetherian. ∎

Cor: The set of zero-divisors for M,

$\{a \in A \mid \exists m \in M,\ m \neq 0 \text{ with } am = 0\}$

is the union of associated primes of M.

Pf: The set of zero-divisors is

$$\bigcup_{\substack{x \in M \\ x \neq 0}} \mathrm{Ann}(x) = \bigcup_{p \in \mathrm{Ass}(M)} p$$

since every $\mathrm{Ann}(x)$ is contained in a maximal annihilator, i.e., an associated prime. $\boxtimes$

<u>Recall:</u> A a ring

$$\operatorname{Spec} A = \text{"the spectrum of } A\text{"}$$
$$= \{ \mathfrak{p} \subseteq A \mid \mathfrak{p} \text{ prime} \}.$$

[See 1st example sheet.]

If $S \subseteq A$ is a multiplicatively closed subset, we may write

$$\operatorname{Spec}(S^{-1}A) \subseteq \operatorname{Spec} A$$
$$\mathfrak{p} \longmapsto \mathfrak{p}^c$$

<u>Theorem:</u> Let $S \subseteq A$ be a mult. closed subset.

① If N is an $S^{-1}A$-module, then under the above inclusion

$$\mathrm{Ass}_{S^{-1}A}(N) = \mathrm{Ass}_A(N)$$

viewing N as an A-module under the canonical map $A \to S^{-1}A$.

(2) For an A-module M, we have

$$\mathrm{Ass}_{S^{-1}A}(S^{-1}M) = \mathrm{Ass}_A(M) \cap \mathrm{Spec}\, S^{-1}A.$$

Pf: (1) For $x \in N$, we have

$$\mathrm{Ann}_A(x) = \left(\mathrm{Ann}_{S^{-1}A}(x)\right)^c$$

[$\subseteq$: If $a \cdot x = 0$, then $\frac{a}{1} \cdot x = 0$,

so $\frac{a}{1} \in \mathrm{Ann}_{S^{-1}A}(x)$

$\supseteq$: If $\frac{a}{s} \cdot x = 0$, then $\frac{a \cdot x}{1} = 0$,

so $a \cdot x = 0$ by def'n of module structure.]

Thus if $\mathfrak{P} \in \mathrm{Ass}_{S^{-1}A}(N)$,

$\mathfrak{P}^c \in \mathrm{Ass}_A(N)$.

Conversely if $\mathfrak{p} \in \mathrm{Ass}_A(N)$

with $0 \neq x \in N$, $\mathfrak{p} = \mathrm{Ann}_A(x)$,

so $\mathfrak{p} \cap S = \phi$ (as invertible elts

of $S^{-1}A$ can't kill x.)

Thus $S^{-1}\mathfrak{p}$ is a prime ideal of

$S^{-1}A$ and

$$\mathrm{Ann}_{S^{-1}A}(x) = S^{-1}\mathfrak{p}$$

[Certainly $S^{-1}\mathfrak{p} \subseteq \mathrm{Ann}_{S^{-1}A}(x)$

If $\frac{b}{s} \in \mathrm{Ann}_{S^{-1}A}(x)$, then $tb \in \mathrm{Ann}_A(x)$

for some $t \in S$, so $b \in \mathrm{Ann}_A(x) = \mathfrak{p}$

since $\mathfrak{p}$ is prime and $t \notin \mathfrak{p}$.]

Thus $S^{-1}\mathfrak{p} \in \mathrm{Ass}_{S^{-1}A} N$.

② Want to show

$$\mathrm{Ass}_{S^{-1}A}(S^{-1}M) = \mathrm{Ass}_A(M) \cap \mathrm{Spec}(S^{-1}A).$$

If $p \in \mathrm{Ass}_A(M) \cap \mathrm{Spec}(S^{-1}A)$,

$p \cap S = \emptyset$ and $p = \mathrm{Ann}_A(x)$ for

some $x \in M$, $0 \neq x$. Now if

$\left(\frac{a}{s}\right) \cdot \left(\frac{x}{1}\right) = 0$ in $S^{-1}M$, $\exists t \in S$

such that $tax = 0$, in M.

Now $t \notin p$ but $ta \in p$, so $a \in p$,

so $\mathrm{Ann}_{S^{-1}A}(x) = S^{-1}p$, so

$S^{-1}p \in \mathrm{Ass}_{S^{-1}A}(S^{-1}M)$.

$$\boxed{\begin{aligned} p &= \mathrm{Ann}_{S^{-1}A}\left(\frac{x}{s}\right) \\ &= \mathrm{Ann}_{S^{-1}A}\left(\frac{x}{1}\right) \end{aligned}}$$

since s is invertible

Conversely, if $p \in \mathrm{Ass}_{S^{-1}A}(S^{-1}M)$,

$p = \mathrm{Ann}\left(\frac{x}{1}\right)$ for some $x \in M$.

Let $q = p^c$, so $p = q^e$.

Since A is Noetherian, q is finitely generated, so $\exists t \in S$ such that $q = \mathrm{Ann}_A(tx)$

[If $a_1, \dots, a_n$ generate q, $\frac{a_i}{1} \cdot \frac{x}{1} = \frac{a_i \cdot x}{1} = 0$

so $\exists\, t_i$ s.t. $t_i a_i x = 0$.

Take $t = \prod t_i$, and everything in q annihilates tx.]

So $q \in \mathrm{Ass}_A(M)$. $\blacksquare$

Def: For M an A-module, the **support** of M is

$$\mathrm{Supp}(M) := \{ p \in \mathrm{Spec}\, A \mid M_p \neq 0 \}.$$

<u>theorem</u>: $\mathrm{Ass}(M) \subseteq \mathrm{Supp}(M)$, and any minimal element of $\mathrm{Supp}(M)$ is an associated prime of M.

<u>pf</u>: If $\mathfrak{p} \in \mathrm{Ass}(M)$, have an exact sequence

$$0 \to A/\mathfrak{p} \to M, \qquad 1 \mapsto x$$

$$\boxed{\begin{gathered} \mathfrak{p} \in \mathrm{Ass}(M) \\ \iff \mathfrak{p} = \mathrm{Ann}(x) \\ \iff A/\mathfrak{p} \subseteq M. \end{gathered}}$$

hence have exact sequence

$$0 \to (A/\mathfrak{p})_{\mathfrak{p}} \to M_{\mathfrak{p}}$$

$$(A/\mathfrak{p})_{\mathfrak{p}} = A_{\mathfrak{p}} / \underbrace{\mathfrak{p} A_{\mathfrak{p}}}_{= \mathfrak{p}^e = (A \backslash \mathfrak{p})^{-1} \mathfrak{p}} \neq 0.$$

$= $ maximal ideal of $A_{\mathfrak{p}}$

Thus $M_{\mathfrak{p}} \neq 0$, and $\mathfrak{p} \in \mathrm{Supp}(M)$.

If $\mathfrak{p}$ is a minimal element of $\mathrm{Supp}(M)$ note by the previous theorem, (2), that $\mathfrak{p} \in \mathrm{Ass}(M)$ if and only if $\mathfrak{p} A_{\mathfrak{p}} \in \mathrm{Ass}_{A_{\mathfrak{p}}}(M_{\mathfrak{p}})$

Thus we may replace A, M by $A_{\mathfrak{p}}$, $M_{\mathfrak{p}}$. so we can assume $(A, \mathfrak{p})$ is a local ring and $M \neq 0$, and $M_q = 0$ for any $q \subsetneq \mathfrak{p}$. (This follows from the first example sheet.)

So $\mathrm{Supp}(M) = \{\mathfrak{p}\}$. Since $\mathrm{Ass}(M) \neq \emptyset$ since $M \neq 0$.

Thus $\mathrm{Ass}(M) = \{\mathfrak{p}\}$. $\blacksquare$

<u>Cor</u>: Let $I \subseteq A$ be an ideal.

Then the minimal associated primes of the A-module A/I are precisely the minimal elements of

$$V(I) = \{ \mathfrak{p} \in \operatorname{Spec} A \mid I \subseteq \mathfrak{p} \}.$$

<u>Pf</u>: Enough to show

$$\operatorname{Supp}(A/I) = V(I).$$

But $(A/I)_{\mathfrak{p}} = A_{\mathfrak{p}} / I^e$,

and $I^e \neq (1) \iff I \cap (A \setminus \mathfrak{p}) = \emptyset$

$\iff I \subseteq \mathfrak{p}$. $\blacksquare$

<u>Remark</u>: The theorem says the minimal associated primes are the minimal elements of $\operatorname{Supp} M$. The non-minimal associated

primes are called <u>embedded primes</u>.

<u>Note</u>: This requires the existence of a minimal element of $\mathrm{Supp}\, M$ contained in any given element. Then if $\mathfrak{p} \in \mathrm{Ass}\, M$ is minimal, $\exists\, \mathfrak{q} \in \mathrm{Supp}\, M$ minimal with $\mathfrak{q} \subseteq \mathfrak{p}$, so $\mathfrak{q} \in \mathrm{Ass}\, M$, so $\mathfrak{p} = \mathfrak{q}$.

For this fact, we could use that in a Noetherian ring, all chains of primes are finite (requires dimension theory)

<u>Lemma</u>: If M is a finitely generated A-module, then

$$\mathrm{Supp}\, M = V(\mathrm{Ann}_A M)$$
$$= \{\mathfrak{p} \in \mathrm{Spec}\, A \mid \mathfrak{p} \supseteq \mathrm{Ann}_A M\}$$

where $\mathrm{Ann}_A M = \{x \in A \mid xM = 0\}$.

Pf: If $\mathfrak{p} \not\supseteq \mathrm{Ann}_A(M)$ then $\exists$ $s \in \mathrm{Ann}_A(M) \cap S$

where $S = A \setminus \mathfrak{p}$ and $M_{\mathfrak{p}} = S^{-1}M$.

But then for $\frac{x}{t} \in M_{\mathfrak{p}}$, $x \cdot s = 0$,

so $\frac{x}{1} = 0$ in $M_{\mathfrak{p}}$, and so $M_{\mathfrak{p}} = 0$.

Conversely, if $\mathfrak{p} \supseteq \mathrm{Ann}_A(M)$ but

$M_{\mathfrak{p}} = 0$. Let $x_1, \dots, x_n$ generate M as

an A-module. Then $\exists s_i \in S = A \setminus \mathfrak{p}$

such that $s_i x_i = 0$ $\forall i$

But then $s = \prod_{i=1}^{n} s_i$ satisfies

$s x_i = 0$ $\forall i$, so $s \in \mathrm{Ann}_A M$.

This contradicts $\mathfrak{p} \supseteq \mathrm{Ann}_A(M)$. $\blacksquare$

Example! We need M to be finitely generated! $A = \mathbb{Z}$

$$M = \bigoplus_{p \text{ prime}} \mathbb{Z}/p\mathbb{Z}$$

$\mathrm{Ann}_A(M) = 0$, but

$$\mathrm{Supp}\, M = \{(p) \mid p \text{ prime}\}.$$

and $(0) \in V(\mathrm{Ann}_A(M))$

$(0) \notin \mathrm{Supp}\, M.$

Note: This gives a 1-1 correspondence between minimal primes of $\mathrm{Supp}\, M$ and minimal primes of $A/\mathrm{Ann}_A M$.

Minimal primes in rings exist using Zorn's lemma

$p_1 \supseteq p_2 \supseteq \dots$ all prime

$\Rightarrow p = \bigcap p_i$ is prime

Example: Let $A = k[x,y]$, k a field,

$M = A/I$, $\quad I = (x^2, xy)$.

Two associated primes:

1. $\mathfrak{m} = (x,y)$, as $\mathrm{Ann}_A(x+I) = (x,y)$

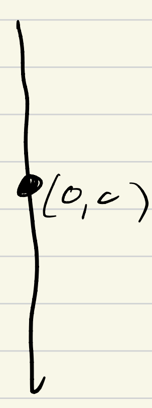
2. $\mathfrak{p} = (x)$, as $\mathrm{Ann}_A(y+I) = (x)$.

Geometric interpretation:

Consider $Z(I) \subseteq k^2$

$$Z(I) = \{(a,b) \in k^2 \mid f(a,b) = 0 \ \forall f \in I\}.$$

In our case, we get the

y-axis  $\subseteq k^2$

Note if we localize at y, so y becomes invertible, the ideal $I^e \subseteq k[x,y]_y$ just becomes (x).

"Origin has fuzz."

Will eventually see that the primary decomposition of I is

$$I = (x) \cap (x,y)^2.$$

m is an embedded associated prime.

<u>Theorem</u>: Let M be a f.g. A-module (A still Noetherian), $M \neq 0$. Then there exists a chain of submodules

$$(0) = M_0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_n = M$$

such that $M_i / M_{i-1} \cong A/\mathfrak{p}_i$

for some prime $\mathfrak{p}_i$.

Pf: Since $M \neq 0$, $\exists\, \mathfrak{p}_1 \in \mathrm{Ass}(M)$ and hence can find submodule $M_1 \subseteq M$ with $M_1 \cong A/\mathfrak{p}_1$.

If $M_1 \neq M$, apply the same procedure to M/M_1 to get chain

$$0 = M_0 \subsetneq M_1 \subsetneq M_2 \subsetneq \cdots$$

with $M_i/M_{i-1} \cong A/\mathfrak{p}_i$

Since M is f.g. over a Noetherian ring, M is Noetherian and this process stops. $\boxtimes$

Lemma: If $0 \to M_1 \to M_2 \to M_3 \to 0$ is exact, then

$$\mathrm{Ass}(M_2) \subseteq \mathrm{Ass}(M_1) \cup \mathrm{Ass}(M_3).$$

pf: Let $\mathfrak{p} \in \mathrm{Ass}(M_2)$, $N \subseteq M_2$ with $N \cong A/\mathfrak{p}$. If $N \cap M_1 = (0)$, then N is isomorphic to a submodule of M_3, so $\mathfrak{p} \in \mathrm{Ass}(M_3)$.

If $N \cap M_1 \neq (0)$, pick $0 \neq x \in N \cap M_1$. Since $A/\mathfrak{p}$ is an integral domain, $\mathrm{Ann}(x) = \mathfrak{p}$, so $\mathfrak{p} \in \mathrm{Ass}(M_1)$. $\boxtimes$

Cor: If M is a f.g. A-module, then $\mathrm{Ass}(M)$ is finite.

pf: Have $0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_n = M$ with $M_i/M_{i-1} \cong A/\mathfrak{p}_i$, so repeated use of the lemma applied to

$$0 \to M_{i-1} \to M_i \to M_i/M_{i-1} \to 0$$

shows $\mathrm{Ass}(M) \subseteq \mathrm{Ass}(M_1) \cup \mathrm{Ass}(M_2/M_1)$

$$\cup \cdots \cup \mathrm{Ass}(M_n/M_{n-1}).$$

But $\mathrm{Ass}(M_i/M_{i-1}) = \mathrm{Ass}(A/\mathfrak{p}_i)$

$$= \{\mathfrak{p}_i\}$$

So $\mathrm{Ass}(M) \subseteq \{\mathfrak{p}_1, \dots, \mathfrak{p}_n\}$. $\square$

<u>Def</u>: An A-module is <u>coprimary</u> if it has a unique associated prime.

A submodule $N \subseteq M$ is <u>primary</u> if M/N is coprimary.

<u>Radicals</u>

<u>Def</u>: $I \subseteq A$ an ideal. The <u>radical</u> of I is

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

<u>Prop</u>: $\sqrt{I} = \bigcap_{\substack{\mathfrak{p} \in \operatorname{Spec} A \\ I \subseteq \mathfrak{p}}} \mathfrak{p}$

$$= \bigcap_{\mathfrak{p} \in V(I)} \mathfrak{p}.$$

<u>Pf</u>: Let I' be the right-hand-side.

$a \in \sqrt{I} \iff a^n \in I$ for some $n > 0$

$\Longrightarrow a^n \in \mathfrak{p}$ for any $\mathfrak{p} \supseteq I$

$\Longrightarrow a \in \mathfrak{p}$ for any $\mathfrak{p} \supseteq I$

$\Longrightarrow a \in I'$.

Conversely, suppose $a^n \notin I$ for any n.

Let Σ be the set of ideals $J \subseteq A$

with $I \subseteq J$ and $a^n \notin J$ for

any $n > 0$.

Σ is non-empty $(I \in \Sigma)$

Σ is ordered by inclusion and satisfies the upper bound property

($J_1 \subseteq J_2 \subseteq \ldots$, sequence of ideals in Σ, then $\bigcup J_i \in \Sigma$.)

By Zorn, have a maximal element $P \in \Sigma$.

<u>Claim</u>: P is prime.

<u>Pf</u>: Suppose $x, y \notin P$.

Then $P + (x)$, $P + (y)$ are ideals strictly containing P, and hence $\exists\, m, n > 0$ such that

$$a^m \in P + (x), \quad a^n \in P + (y).$$

Thus $a^{m+n} \in P + (xy)$ so

$\mathfrak{P} + (xy) \notin \Sigma$, so $xy \notin \mathfrak{P}$.

Hence $\mathfrak{P}$ is prime. $\square$

So we have constructed $\mathfrak{p} \supseteq I$

with $a^n \notin \mathfrak{p}$, i.e., $a \notin \mathfrak{p}$, so $a \notin I'$.

$\square$