Math 742
Andrei Caldararu
VV 605
andreic@math

1/23 Textbooks:
"Commutative Alg": Atiyah-Macdonald (Eisenbud long, Matsumura dry)
Galois Theory - Lecture notes by Artin (Dover)

Commutative Algebra

Ring: A a set with $+,\cdot$ s.t. $(A,+,0)$ an abel gp, $\cdot$ is assoc, $1 \exists\ 1\cdot x = x\cdot 1 = x\ \forall x \in A$, & $x(y+z) = xy+xz$

Commutative Ring: $xy = yx\ \ \forall x,y \in A$

Ring homomorphism: If A,B rings, $f: A \to B$ is a ring homo. if
a) $f(a+b) = f(a)+f(b)$ b) $f(xy) = f(x)f(y)$, c) $f(1) = 1$.
$\Downarrow$
$f(0) = 0$

Note: We don't assume $0 \neq 1$. But if $0 = 1 \Rightarrow A = \{0\}$, the zero ring. The zero ring can't map into any nonzero ring b/c $f(1) = 1$.

f, g ring hom. $\Rightarrow$ $f \circ g$ is

Ex: ① $\mathbb{Z}$
② $k[x_1, \dots, x_n]$, k a field
* $\forall$ ring R, $\exists!$ hom $f: \mathbb{Z} \to R$. $(1 \to 1,\ 7 \to \overbrace{1+1+\cdots+1}^{7})$
$\mathbb{Z}$ is an initial object in category of rings
$\exists!$ hom $g: R \to 0$
0 is a terminal object in cat. of rings
③ $k[x] \hookrightarrow k[x,y]$
④ $\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$
⑤ $\mathbb{Z}/8\mathbb{Z} \longrightarrow \mathbb{Z}/4\mathbb{Z}$

Ideals: $I \subseteq A$ is an ideal if:

(1) $x+y \in I \quad \forall x,y \in I$

(2) $ax \in I \quad \forall x \in I \ \forall a \in A$

Ex: If $x \in A$, the principal ideal gen by x, $(x) = \{ax \mid a \in A\} \subseteq A$.

Ex: $\{f \in \mathbb{Z}[x] \mid f(0) \in 2\mathbb{Z}\}$ is a non-principal ideal.

I' $I = (2,x) = \{2f + xg \mid f,g \in A = \mathbb{Z}[x]\}$

Note: Very rarely does $1 \in I$. In fact, if $1 \in I$, then $I = A$.

Facts:

* ① If $f: A \to B$ a ring hom & $I \subseteq B$ an ideal, then $f^{-1}(I) \subseteq A$ is an ideal.

② $(0) = \{0\} \subseteq B$ is always an ideal.

③ $f^{-1}(0) := \ker f \subseteq A$ is an ideal.

(analogue to Ker of gp hom is normal, & preimage of normal is normal)

④ $f(A) \subseteq B$ is a subring (contains 1, closed under $+$ & $\cdot$)

& $A/\ker f \cong \operatorname{Im} f$ (First Iso. Thm)

Sketch of Pf: Check the gp hom's respect $\cdot$.

Ex: ① $K[x] \xrightarrow{\phi} K$, $f \mapsto f(1)$ a ring hom.

Sur? $\operatorname{Im}\phi = K$, so yes.

$\ker \phi = (x-1)$

$\{f \mid f(1) = 0\} \Leftrightarrow \{f \mid (x-1) \mid f\} = (x-1)$

$\Rightarrow K[x]/(x-1) \cong K$ (not a unique quotient, ex: $K[x]/(x-2) \cong K$, $f \mapsto f(2)$)

Zero-divisors: x is a zero-div. if $\exists y \neq 0$ s.t. $xy = 0$.

(0 is always a zero-div.)

A ring A s.t. $A \neq 0$ and $\forall x \in A$, $x \neq 0$, x is not a zero div. is called an integral domain.

Ex: $\mathbb{Z}$, $K[x_1, \dots, x_n)$ Non-ex: $\mathbb{Z}/6\mathbb{Z}$, b/c $2 \cdot 3 = 0$

$K[x]/(x-1)(x-2)$ b/c $(x-1)(x-2) = 0$

x is <u>nilpotent</u> if $\exists n>0$ s.t. $x^n=0$.

x nilp $\Rightarrow$ x a zero-div. $(x \cdot x^{n-1}=0)$

<u>Unit</u>: x is a <u>unit</u> if $\exists y$ s.t. $xy=1$

<u>Ex</u>: In $\mathbb{Z}$, units are $\{\pm 1\}$.

In $\mathbb{Q}$, units are $\mathbb{Q}\setminus\{0\}$

- The set of units forms an abelian gp

- If p is prime, units in $\mathbb{Z}/p\mathbb{Z}$ form a cyclic gp. (<u>Thm</u>)
  (nontrivial, & hard to find a generator)
  (true for any finite field)

- a is a unit iff $(a)=(1)$

<u>Fields</u>: A is a <u>field</u> if $\forall x \in A$, $x \neq 0$, x is a unit; and $A \neq 0$.

<u>Prop</u>: A a ring, $A \neq 0$. TFAE:

(1) A is a field

(2) The only ideals in A are (0) & (1)

(3) If B is any non-0 ring & $f: A \to B$ a ring hom, then f is injective. (ale ring homs from field are inclusions)

<u>Pf</u>: (1)$\Rightarrow$(2): If I a non-0 ideal then $\exists x \neq 0, x \in I$
$\Rightarrow (x) \subseteq I$, but $(x)=(1)=A \Rightarrow I=(1)$

(2)$\Rightarrow$(3): Given f, look at $\ker f \subseteq A$. $\ker f \neq A$, b/c $1 \notin \ker f$ ($f(1)=1$, & $1 \neq 0$ in B b/c $B \neq 0$) $\Rightarrow$ $\ker f = (0)$
$\Rightarrow f$ is injective.

(3)$\Rightarrow$(1): If $x \in A, x \neq 0$, look at $(x) \subseteq A$
$A \to A/(x)$ not injective b/c $x \mapsto 0$. By (3),
$A/(x)=0 \Leftrightarrow (x)=A \Rightarrow x$ a unit.

1/25 Prime & Maximal Ideals

Def: An ideal $\mathfrak{p} \subseteq A$ is prime if:
(1) $\mathfrak{p} \neq A$
(2) $ab \in \mathfrak{p} \Rightarrow a \in \mathfrak{p}$ or $b \in \mathfrak{p}$.
(analogous to $p \in \mathbb{Z}$ prime iff $p|ab \Rightarrow p|a \vee p|b$).
- in $\mathbb{Z}$, (p) prime iff p prime, b/c $ab \in (p) \Leftrightarrow p|ab$ $\overset{\text{if } p \text{ prime}}{\Leftrightarrow} p|a$ or $p|b \Leftrightarrow a \in (p)$ or $b \in (p)$.
- $(0) \subseteq \mathbb{Z}$ is definitely prime

Prop: $(0) \subseteq A$ is prime iff A is an integral domain.

Claim: If $I \subseteq A$ an ideal, $\exists$ a bijective corresp. btwn
$\{$ideals in $A/I\} \longleftrightarrow \{$ideals $J \subseteq A$ s.t. $I \subseteq J\}$

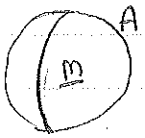
$p: A \to A/I$

$\overline{J} \longmapsto p^{-1}(\overline{J})$ ideal in A (b/c preimage of ideal is ideal)
contains J b/c $(0) \subseteq \overline{J}$.

$p(J) \longmapsto J$

Thm: $\mathfrak{p}$ is prime iff $A/\mathfrak{p}$ is an int. domain.
Pf: $A/\mathfrak{p}$ int. dom. $\Leftrightarrow$ ($\bar{x}\bar{y} = 0 \Rightarrow \bar{x} = 0$ or $\bar{y} = 0$ for $\bar{x}\bar{y} \in A/\mathfrak{p}$ and $A/\mathfrak{p} \neq 0$.)
$\Leftrightarrow$ ($xy \in \mathfrak{p} \Rightarrow x \in \mathfrak{p}$ or $y \in \mathfrak{p}$ for $x, y \in A$ & $\mathfrak{p} \neq A$)
$\Leftrightarrow \mathfrak{p}$ prime.

Def: An ideal $\mathfrak{m} \subseteq A$ is called maximal if $\mathfrak{m} \neq A$ and $\mathfrak{m} \subseteq \mathfrak{a} \Rightarrow \mathfrak{a} = \mathfrak{m}$ or $\mathfrak{a} = A$.



Ex: ① If p a prime $\neq$ in $\mathbb{Z}$ ($p \neq 0$), then (p) is max. in $\mathbb{Z}$!
w/c If not, add coprime #, so all lin combs in ideal, & so 1 in ideal, so ideal $= \mathbb{Z}$.

② $(x-a) \subseteq k[x]$ is max. for any $a \in k$. (same proof - in $k[x]$ ∃ div. alg. w/ remainder)
③ $(x-a, y-b) \subseteq k[x,y]$ is max. for $a, b \in k$. (prove later)
④ $(x-a) \subseteq k[x,y]$ is prime but not max.
⑤ $(0) \subseteq \mathbb{Z}$ is prime but not max.

Thm: $\underline{m} \subseteq A$ is max. iff $A/\underline{m}$ is a field.
Cor: $\underline{m}$ max $\Rightarrow$ $\underline{m}$ prime (b/c fields are int. dom)
Pf: $\underline{m}$ max $\Leftrightarrow$ no ideals btwn $\underline{m}$ & A
$\Leftrightarrow$ only ideals in $A/\underline{m}$ are (0) & $A/(\underline{m}) \Leftrightarrow A/\underline{m}$ field.

Thm: If $A \neq 0$, ∃ max. ideals in A. In fact, $\forall I \subsetneq A$, ∃ $\underline{m}$ max s.t. $\underline{m} \supseteq I$.
Pf: Look at part. ordered set of all proper ideals containing I. This sat. conditions of Zorn's Lemma, b/c given increasing ideals, union of all is an ideal, not everything (b/c $1 \notin$ any, so $1 \notin$ union), so all chains have max $\Rightarrow$ max. elt of set.
Cor: Every non-unit is contained in some max ideal.
Pf: the principal ideal gen by nonunit is $\subseteq$ max ideal (by thm).

Digression: What are max. & prime ideals in $\mathbb{C}[x_1, \ldots, x_n]$?
(1) Max. ideals: $(x_1 - a_1, \ldots, x_n - a_n)$ for $a_1, \ldots, a_n \in \mathbb{C}$.
(2) Prime ideals: If $I \subseteq \mathbb{C}[x_1, \ldots, x_n]$ an ideal, define $z(I) \subseteq \mathbb{C}^n$ by $z(I) = \{(x_1, \ldots, x_n) \in \mathbb{C}^n \mid f(x_1, \ldots, x_n) = 0 \ \forall f \in I\}$
ex: $z((x_1 - a_1, \ldots, x_n - a_n)) = \{(a_1, \ldots, a_n)\}$
For $\mathbb{C}[x,y]$: $z((x)) = 0 \times \mathbb{C} = y$-axis
$\{$max. ideals in $k[x_1, \ldots, x_n]\} \xleftrightarrow{z} \{$pts in $\mathbb{C}^n\}$

Ex: $\mathbb{R}[x]/(x^2+1) \cong \mathbb{C}$

$\mathbb{R}[x] \longrightarrow \mathbb{C}$, $\ker = (x^2+1)$

$x \longmapsto i$

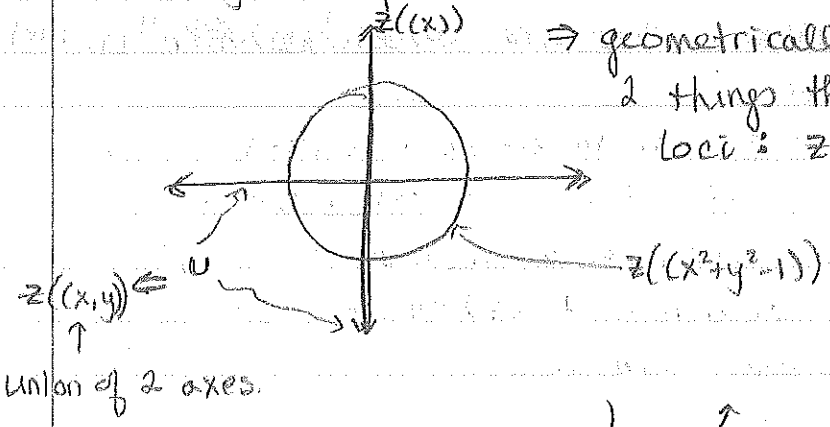
So $(x^2+1) \subseteq \mathbb{R}[x]$ is max. (b/c quot. is field).
but not of form $(x-a)$!.

Ex of primes & nonprimes in $\mathbb{C}[x,y]$:

(1) (x) prime: If $x \mid fg$, then $x \mid f$ or $x \mid g$.

(2) (x^2+y^2-1) prime

(3) (xy) not prime. (b/c neither x nor y in ideal)

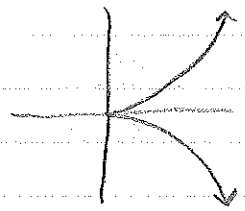


Union of 2 axes.

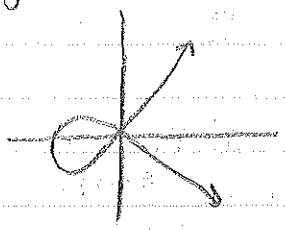
⇒ geometrically, it is the union of 2 things that are themselves zero-loci: $Z((xy)) = Z((x)) \cup Z((y))$

Note: $Z(I)$ is the zero locus of a set of polynomials.

(4) (x^2-y^3) prime



(5) $(y^2-x^2(x-1))$ prime



Def: Subsets of $\mathbb{C}^n$ of the form $Z(I)$ are called closed in the Zariski topology.

Exercise: These are the closed sets in a topology on $\mathbb{C}^n$

- A closed set Y is <u>irreducible</u> if $Y \neq Y_1 \cup Y_2$ w/ Y_1, Y_2 closed, $Y_1 \neq Y$, $Y_2 \neq Y$.

<u>Prop</u>: $\mathfrak{p}$ is prime $\Rightarrow$ $Z(\mathfrak{p})$ is irred.

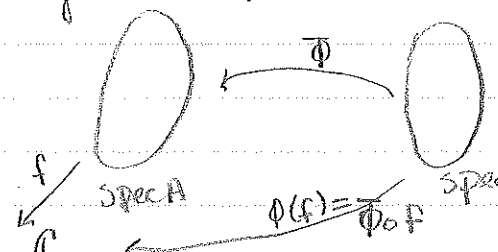
<u>Ex</u>: $(x^2) \subseteq k[x]$ not prime (b/c $x \notin (x^2)$) but $Z((x^2)) = Z((x)) = \{0\} \subseteq \mathbb{C}$ is irred, so not $\Leftrightarrow$ in prop.

1/28 <u>Fact</u>: If $f: A \to B$ a ring hom & $\mathfrak{p} \subseteq B$ prime, then $f^{-1}(\mathfrak{p}) \subseteq A$ is prime.

<u>Pf</u>: $A/f^{-1}(\mathfrak{p}) \longrightarrow B/\mathfrak{p}$ is injective ring hom.
[$A \to B \to B/\mathfrak{p}$ $f^{-1}(\mathfrak{p}) \to 0$, so $\exists$ this map]
$\Rightarrow A/f^{-1}(\mathfrak{p})$ is a subring of an integral dom, (b/c $B/\mathfrak{p}$ int dom), so $A/f^{-1}(\mathfrak{p})$ an int dom $\Rightarrow$ $f^{-1}(\mathfrak{p})$ prime.
[can also be done directly]

- Same <u>fails</u> for max. ideals.
<u>ex</u>: $\mathbb{Z} \hookrightarrow \mathbb{Q}$
(0) not max. (0) is max.

<u>Big Idea</u>: Given ring A, make up a space, Spec A s.t. elts of A are "fcns" on Spec A.
- First approx: If $A = \mathbb{C}[x_1, \dots, x_n]$, would like Spec A to be close to $\mathbb{C}^n$. Define Specm A = $\{\underline{m} \subseteq A \mid \underline{m} \text{ maximal}\}$. [Spec $A = \{\mathfrak{p} \subseteq A \mid \mathfrak{p} \text{ prime}\}$]
Specm $\mathbb{C}[x_1, \dots, x_n] = \mathbb{C}^n$.
- We'd also like to assoc. to a map $A \xrightarrow{\phi} B$ of rings a map Spec $A \xleftarrow{\Phi}$ Spec B (define a <u>contravariant</u> functor)



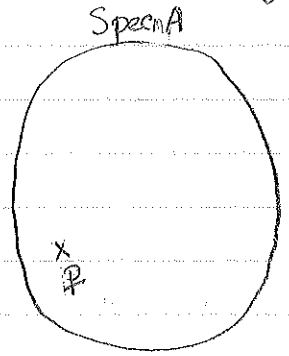
ie, $\left\{\begin{matrix}\text{maps} \\ X \to Y\end{matrix}\right\}$ induce $\left\{\begin{matrix}\text{maps} \\ (\text{fcns on } Y) \to (\text{fcns on})\end{matrix}\right\}$

Indeed, a hom. of rings $\varphi: A \to B$ induces $\overline{\varphi}: \operatorname{Spec} B \to \operatorname{Spec} A$
$\mathfrak{p} \longmapsto \varphi^{-1}(\mathfrak{p})$.

Def: A ring A is said to be **local** iff $\exists!$ maximal ideal in A.
(ie, $\operatorname{Spec_m} A$ is a single pt)

Prop: If A is a ring & $\underline{m} \subseteq A$ an ideal:
(1) $\underline{m}$ is max. & A is local iff $\forall x \notin \underline{m}$, x is a unit.
(2) If $\underline{m}$ is max & $\forall x \in \underline{m}$, $1+x$ is a unit $\iff$ A local.

Pf: (1): $\Rightarrow$: Assume $x \notin \underline{m}$ is not a unit. Then $\exists\, \underline{m}'$ max. s.t. $x \in \underline{m}'$. But then $\underline{m} \neq \underline{m}'$, contradicting A local.
$\Leftarrow$: Assume $\forall x \notin \underline{m}$, x a unit. Then every ideal $\underline{m}' \supsetneq \underline{m}$ has a unit, so $\underline{m}' = (1)$. So $\underline{m}$ is max. If $\underline{m}'$ is another max ideal, we can't have $\underline{m}' \subseteq \underline{m}$, so $\underline{m}'$ contains an $x \notin \underline{m} \Rightarrow \underline{m}'$ contains a unit, contradiction.
(2): $\Leftarrow$: If $x \in \underline{m}$, then $1+x \notin \underline{m}$ (b/c else $\underline{m} = (1)$), so $1+x$ is a unit.
$\Rightarrow$: Let $y \in A \setminus \underline{m}$. Then $(\underline{m}, y) = A$
$\Rightarrow 1 = x + by$, $x \in \underline{m}$, $b \in A$. (b/c $1 \in A$)
$\Rightarrow by = 1 - x$ a unit $(1 + (-x)) \Rightarrow y$ a unit.
$\Rightarrow$ by (1), done.



- each fcn has local operation near each pt $\mathfrak{p}$.
- **localization**: Start w/ ring A & prime ideal $\mathfrak{p}$ & produces a local ring $A_{\mathfrak{p}}$ which captures the behavior of fcns on $\operatorname{Spec} A$ only around $\mathfrak{p}$. (focus on germ at $\mathfrak{p}$)

Ex: (1) A field is a local ring

~~(2)~~ $R = \{\frac{m}{2^n} \mid m \in \mathbb{Z}, n \in \mathbb{N}\} \subseteq \mathbb{Q}$ is a local ring (not a field b/c w/ inversion $m \neq 2^n$, nec.)

- $\frac{1}{2}$ is a unit, 2 is a unit.

→ pick set of all nonunits

Let $I = \{m/2^n \mid m/2^n \text{ not a unit}\}$ ie, in lowest terms, $m \neq \pm 1$.

$= \{m/2^n \mid \text{if } 2 \nmid m \text{ then } m \neq \pm 1\}$

Units in R are 2^i, $i \in \mathbb{Z}$.

Max. ideal: (3) max, (5) max, ... num. div. is. by 3 / $\mathbb{Z}$ & throws out 2.

(2) $R = \{\frac{m}{n} \mid 2 \nmid n\} \subseteq \mathbb{Q}$ is a local ring

(throws out all prime ideals of $\mathbb{Z}$ except (2))

- (2) is the only max. ideal.

CK! (2) is set of fracs in lowest terms w/ $2 \mid m$.

If $x \notin (2)$, m is not even, so a unit.

- works for any prime $(p \nmid n)$.

→ Given int. dom., embed in its field of fracs, given prime ideal, look at things w/ denom. not in prime ideal ⇒ will be local ring.

1/30 Nilradical

Def: $\mathcal{N} = \{x \in A \mid x \text{ is nilpotent, ie } \exists n \geq 0 \text{ s.t. } x^n = 0\}$ is the nilradical.

- This is an ideal.

We'll say a ring A is reduced if it has no nilpotents ($\neq 0$)

- $A/\mathcal{N}$ is reduced. If $\bar{x} \in A/\mathcal{N}$ is nilp, $\Rightarrow \bar{x}^n = 0$ for some n

$\Rightarrow x^n \in \mathcal{N} \Rightarrow \exists k$ s.t. $(x^n)^k = 0 \Rightarrow x$ is nilp $\Rightarrow x \in \mathcal{N} \Rightarrow \bar{x} = 0$.

Def: If $I \subseteq A$ is an ideal, the radical of I,

$r(I) = \sqrt{I} = \{x \in A \mid \exists n \geq 0 \text{ s.t. } x^n \in I\}$

- $r(I) \supseteq I$ ($n = 1$), but in general it's bigger.

Prop: $A/r(I)$ is reduced.
b/c $r(r(I)) = r(I)$, & $\bar{x} \in A/r(I)$ nilp if $\bar{x} \in r(r(I)) \Rightarrow \bar{x} = 0$.

Ex: If $x = p_1^{\alpha_1} \cdots p_n^{\alpha_n} \in \mathbb{Z}$, then $r((x)) = (p_1 p_2 \cdots p_n)$

Def: I is said to be radical iff $I = \sqrt{I}$.

If $I \subseteq \mathbb{C}[x_1, \ldots, x_n]$, we associated a set $Z(I) \subseteq \mathbb{C}^n$,
where $Z(I) = \{\underline{x} \mid f(\underline{x}) = 0 \ \forall f \in I\}$ $(\underline{x} = (x_1, \ldots, x_n))$.
Given a subset of $\mathbb{C}^n$, can we produce an ideal?
If $S \subseteq \mathbb{C}^n \overset{?}{\rightsquigarrow} I \subseteq \mathbb{C}[x_1, \ldots, x_n]$.
Define $I(S) = \{f \in \mathbb{C}[x_1, \ldots, x_n] \mid f(\underline{x}) = 0 \ \forall \underline{x} \in S\}$. This is an ideal, always.

In $\mathbb{C}$, what sets can be $Z(I)$? everything (if $f = 0$) or a finite set of pts. (not $\mathbb{Z} \subseteq \mathbb{C}$, for example).
- A subset of $\mathbb{C}^n$ is said to be algebraic if it is of the form $Z(I)$ for some I (equivalently if it is closed in the Zariski top. on $\mathbb{C}^n$).

ideal $\Rightarrow$ algebraic set & any set $\Rightarrow$ ideal.
Not inverses...: $Z(I(S)) = \bar{S}$ in z. top.
$I(Z(\underline{a})) \supseteq \sqrt{\underline{a}}$ • must contain $\underline{a}$

→ If instead of $\mathbb{C}$ we put $\mathbb{R}$, this is no longer true.
ex: $Z((x^2+1)) = \emptyset$, so $I(Z((x^2+1))) = (1)$
but $\sqrt{(x^2+1)} = (x^2+1)$ (b/c (x^2+1) max & prime)
Note: If I is a prime ideal, it is a radical.
b/c if $a^n \in I$, $a(a^{n-1}) \in I \Rightarrow a \in I$ ✓ or $a^{n-1} \in I$ &, continue.

Prop: I is radical iff A/I has no nilpotents
(*no nilp's in an int. dom.)

Note: ① $\underline{a} \subseteq I(Z(\underline{a}))$ ② $I(S)$ is radical $\forall S$.
b/c if f^n vanishes, f vanishes

$\{$ alg subsets of $\mathbb{C}^n\}$ $\xrightarrow{I}$ $\xleftarrow{Z}$ $\{$ radical ideals of $\mathbb{C}[x_1,\dots,x_n]\}$ (inverses)

Fact: $Z(\sqrt{a}) = Z(a)$.

Ex: $Z((x^2)) = \{x \in \mathbb{C} \mid x^2 = 0\}$
$= \{x \in \mathbb{C} \mid x = 0\}$
$= Z((x))$

Thm: $\eta = \bigcap_{\substack{\mathfrak{p} \subseteq A \\ \mathfrak{p} \text{ prime}}} \mathfrak{p}$, ie, the nilrad is the int of all prime ideals.

Pf: "$\subseteq$": If $x^n = 0 \Rightarrow x^n \in \mathfrak{p}\ \forall \mathfrak{p} \Rightarrow x \in \mathfrak{p}\ \forall \mathfrak{p} \Rightarrow x \in \cap \mathfrak{p}$

"$\supseteq$": Let $\eta' = \cap \mathfrak{p}$. [WTS if f not nilp $\Rightarrow f \notin \eta'$, ie $\exists \mathfrak{p}$ prime s.t. $f \notin \mathfrak{p}$].

Let $\Sigma = \{\underline{a} \subsetneq A \mid \underline{a}$ ideal s.t. $f^n \notin \underline{a}\ \forall n\}$.

- $\Sigma \neq \emptyset$ b/c $(0) \in \Sigma$. (b/c f not nilp)
- $(\Sigma, \subseteq)$ satisfies the chain condition in Zorn's lemma b/c given chain, the union an ideal (b/c nested) & is maximal s.t. $f^n \notin \cup$.

$\Rightarrow \exists$ max. elements of the ordered set $(\Sigma, \subseteq)$.

Let $\mathfrak{q}$ be such a max. elt. [WTS $\mathfrak{q}$ prime - if ok, done b/c if $f^n \notin \mathfrak{q}\ \forall n$, $f \notin \mathfrak{q}$].

* alt. charac. of prime * $\Longrightarrow$ To show $\mathfrak{q}$ prime, it's enough to show that if $x \notin \mathfrak{q}$ & $y \notin \mathfrak{q}$, $\Rightarrow xy \notin \mathfrak{q}$.

Let $x, y \notin \mathfrak{q}$. Then $\mathfrak{q} + (x) \supsetneq \mathfrak{q} \Rightarrow \mathfrak{q} + (x) \notin \Sigma$

$\Rightarrow \exists n$ s.t. $f^n \in \mathfrak{q} + (x)$. Similarly, $\exists n'$ s.t. $f^{n'} \in \mathfrak{q} + (y)$. $\Rightarrow f^{n+n'} \in \mathfrak{q} + (xy)$ b/c:

$f^n = q_1 + ax$ & $f^{n'} = q_2 + by \Rightarrow f^{n+n'} = (q_1 q_2 + q_1 by + q_2 ax + abxy) \in (xy)$ ✓

$\Rightarrow \mathfrak{q} + (xy) \notin \Sigma$

$\Rightarrow (xy) \notin \mathfrak{q}$ □

Cor: $\sqrt{\underline{a}} = \bigcap_{\substack{\underline{p} \text{ prime} \\ \underline{p} \supseteq \underline{a}}} \underline{p}$.

Pf: Look at $A \xrightarrow{\phi} A/\underline{a}$. $\phi^{-1}(\eta_{A/\underline{a}}) = \sqrt{\underline{a}}$ b/c

- $A/\phi^{-1}(\eta_{A/\underline{a}}) \simeq (A/\underline{a})/\eta_{A/\underline{a}}$ & this is a reduced ring; and
- $\phi^{-1}(\eta_{A/\underline{a}}) \supseteq \underline{a}$, & is smallest radical that contains $\underline{a}$.

(details ...)

- Read rest of Ch. 1
- Start problems #15-22

before Friday, when there will be a discussion.

Two important pieces:

(1) $a_1, \ldots, a_n \subseteq A$ ideals. Have map:

$A \to A/a_1 \times A/a_2 \times \cdots \times A/a_n$

$a \mapsto (a \bmod a_1, \ldots, a \bmod a_n)$ Neither inj. or surj.

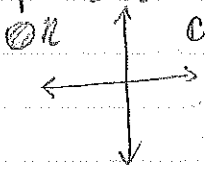
Surj: ideals are rel. prime (Chinese Remainder Thm)

inj: $\bigcap a_i = (0)$

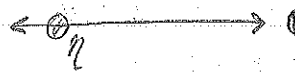
(2) Extension & contraction of ideals, esp. example of $\mathbb{Z} \subseteq \mathbb{Z}[i]$.

2/1 (0) → represented by η, the generic pt

Spec $\mathbb{C}[x]$



or, better:



(one-dim. vector sp)

What is the topology on Spec $\mathbb{C}[x]$?

- closed sets: $V(\underline{a})$ - closed for any $\underline{a} \subseteq \mathbb{C}[x]$ an ideal

$V(\underline{a}) = \{\underline{p} \in \operatorname{Spec} \mathbb{C}[x] \mid \underline{a} \subseteq \underline{p}\}$

If $\underline{a} = (f)$, $f \neq 0$, then $V(\underline{a}) = \{(x-a) \mid f(a) = 0\}$, finite

⇒ closed sets are finite subsets of closed pts (ie $(x-a)$)

If $\underline{a} = (f)$, $f = 0$, then $V(f) = X$. or X.

What about η? $\overline{\{\eta\}} = X$, b/c $\Rightarrow$ int. of all cl. sets containing it $\ni X$ contains it.

Spec $\mathbb{Z}$ = $\{(0), (p) \text{ for } p \text{ prime}\}$.

Closed subsets:

What is $V((35)) = \{(5), (7)\}$

Closed sets in Spec $\mathbb{Z}$ are either Spec $\mathbb{Z}$ or finite sets of (p)'s.

(p) - closed

(0) - not closed, $\overline{(0)} = \text{Spec } \mathbb{Z}$

$\rightarrow$ not Hausdorff. In fact, all open sets contain η.

Q: If $f \in \mathbb{C}[x]$, can we think of f as a function on Specm $\mathbb{C}[x]$?

- If $\mathfrak{m} \subseteq \mathbb{C}[x]$ is maximal ideal $(x-a)$, what does it mean to evaluate f at a? Take the residue.

A: $\mathbb{C}[x] \to \mathbb{C}[x]/(x-a) \cong \mathbb{C}$; $\phi_a : \mathbb{C}[x] \to \mathbb{C}$, $\ker \phi_a$ is $(x-a)$

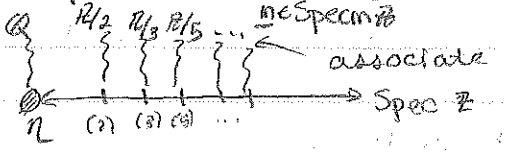
$f \mapsto \overline{f} \cong f(a)$ $\qquad f \mapsto f(a)$

So $f \in A$ gives rise to a fcn $\tilde{f}$: Specm $\mathbb{C}[x] \to \mathbb{C}$

$(x-a) \mapsto f \bmod (x-a)$

Same in $\mathbb{Z}$: An elt of $\mathbb{Z}$ ($n \in \mathbb{Z}$) gives a fcn.

$\tilde{n}$: Specm $(\mathbb{Z}) \to \coprod \mathbb{Z}/\mathfrak{m}$



$\tilde{9}$: $\bar{1}$ $\bar{0}$ $\bar{1}$ $\bar{2}$

First mod out by ideal (an int. dom) then η is its field of fractions (p. 13 # 21(vii))

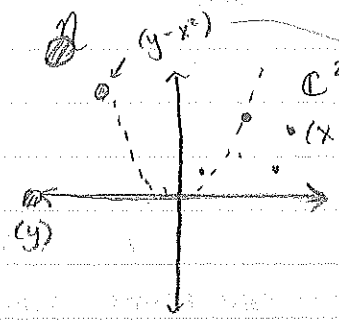
- $n \in \mathbb{Z}$, $V((n)) =$ zero locus of $\tilde{n} = \{x \in \text{Spec } \mathbb{Z} \mid \tilde{n}(x) = 0\}$

Two-dim example: Spec $\mathbb{C}[x,y]$

prime ideals $\leftarrow$ $(x-a, y-b) \rightsquigarrow$ pts in $\mathbb{C}^2 \Rightarrow$ only closed pts

(x), $(y-x^2)$, $(y^2 - x(x-1)(x-2)) \Rightarrow$ non-closed pts

$(0) \rightsquigarrow \eta$ single pt whose closure is the parabola



$V(x-y^2) = \{(x-y^2), (x-a, y-b) \text{ s.t. } a = b^2\}$

Is $(x-y^2) \subseteq (x-a, y-b)$? yes, for all a, b that satisfy the eqn

$\overline{\{x-y^2\}} = V(x-y^2)$

- $(x-y^2)$ is a non-closed pt whose closure gives an irreducible subvariety.

(Schemes : Manifolds :: Comm. rings : $\mathbb{R}^n$) $\leftarrow$ local vs. global props

Ex: $\mathbb{C}[x,y]/(x-y^2)$ an integral domain b/c $(x-y^2)$ prime

Spec$(\mathbb{C}[x,y]/(y-x^2))$ = prime ideals in $\mathbb{C}[x,y]$ which contain $(x-y^2) = V(y-x^2)$ = parabola + generic pt $(y-x^2)$

- If R is a ring f.g. over $\mathbb{C}$, ie $\mathbb{C}[x_1, \ldots, x_n]/I$ (map each gen. to $x_1, \ldots, x_n$; map's kernel identifies I)

Then Spec( ) $= V(I) \subseteq$ Spec $\mathbb{C}[x_1, \ldots, x_n] = \mathbb{C}^n \cup$ extra nebulous pts.

- Spec $\mathbb{C}[x]/(x) \simeq$ Spec $\mathbb{C}[x]/(x^2)$ as top. sp's

$\downarrow$ $\qquad$ $\downarrow$ $\qquad$ $\uparrow$ unique prime ideal

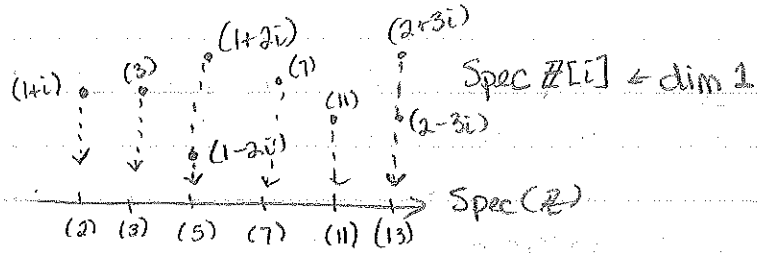
Spec $\mathbb{C}$ $\qquad$ $\{(x)\}$

$\downarrow$ $\qquad$ $\downarrow$ $\qquad$ $\uparrow$ fat pt, not generic pt.

$\{*\}$ $\qquad$ $\{*\}$

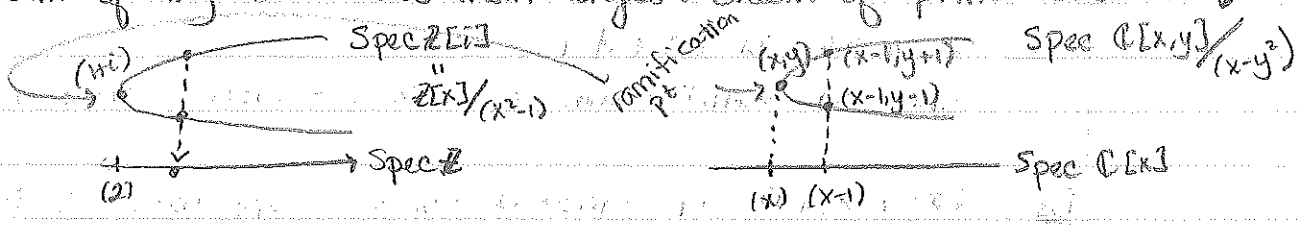
But fcns on 2 sets are different — schemes give this extra info.

2/4 $\mathbb{Z} \hookrightarrow \mathbb{Z}[i]$



- $(1+i)^2 = 2 \Rightarrow (2) \subseteq (1+i)^c$. Actually, only get even ints, so $(2) = (1+i)^c$
- $5 = 1+4 = 1^2+2^2 = (1+2i)(1-2i)$, both are prime
  $13 = 4+9 = 2^2+3^2 = (2+3i)(2-3i)$ $(3 \bmod 4)$...

dimension 1: (0), max ideals only. ie, $\mathbb{C}[x]$
dimension 2: (0), prime, max, ie $\mathbb{Z}[x]$ ext. $(0) \subsetneq (x) \subsetneq (2,x)$
codim. of ring is 1 less than longest chain of prime ideals.



- $\mathbb{Z}[i]/(3)$ & $\mathbb{Z}[i]/(1+2i)$ give different fields, b/c $\mathbb{Z}$ not alg. closed & allows finite field extensions.
- Spec $\mathbb{Z}[i]$ is parabola b/c in a field extension, ie $\mathbb{Q}$, (3) will split into 2 pts. $(1+i)$ never will split — it's 2 copies of $(1+i)$ already. $(1+i)^2 = 2$. ↑ $(1+\sqrt{2}i)$ & $(1-\sqrt{2}i)$

Modules

module : ring :: vector bundle : space

- abelian gp $(+)$ & operation $(\cdot)$ of ring on it.

Examples:

(1) If $I \subseteq A$ is an ideal, then I is a submodule of A
(2) A is a module of itself.
(3) Vector sp. over a field
(4) $\mathbb{Z}$-modules $\Leftrightarrow$ abelian gp (ie, $2x = x + x$)
(5) If G a gp, $k[G]$ (the gp algebra) over a field k.
left $k[G]$-modules are G-representations.
(needs to be R-mod, ie vector sp, w/ an action of G)

Def: $\phi : M \to N$ is an A-mod. homomorphism if
$\phi(m+n) = \phi(m) + \phi(n)$ & $\phi(am) = a\phi(m)$ $\forall a \in A$, $m \in M, n \in N$.

- $\ker \phi = \{m \in M \mid \phi(m) = 0\}$ is a submodule of M.
- If $N \subseteq M$ a submod, then M/N a mod. if $a \cdot \bar{m} := \overline{a \cdot m}$. Well-def b/c if $m \equiv m' \pmod N$, then $m' = m + n$ for some $n \in N$
$a\bar{m'} = \overline{am'} = \overline{a(m+n)} = \overline{am + an} = \overline{am}$ ✓.
- $\operatorname{Im}\phi = \{x \in N \mid \exists m \in M \text{ s.t. } \phi(m) = x\} \subseteq N$ submod.
- Cokernel: $\operatorname{coker}\phi = N/\operatorname{im}\phi$
- $\operatorname{Hom}(M,N) = \{\phi : M \to N \mid \phi \text{ a mod. hom's on } A\text{-mod.}$
$((a\phi)(m) = a \cdot \phi(m))$.
- $M \xrightarrow{f} M' \overset{\text{(induces)}}{\rightsquigarrow} \operatorname{Hom}(M',N) \longrightarrow \operatorname{Hom}(M,N)$
$\phi \longmapsto \phi \circ f$

ie, $\operatorname{Hom}(-,N)$ is a contravariant functor:
$A\text{-mod} \to A\text{-mod}$, but in opp. direction.

- $N \xrightarrow{g} N' \rightsquigarrow \operatorname{Hom}(M,N) \longrightarrow \operatorname{Hom}(M,N')$
$\phi \longmapsto g \circ \phi$

ie, $\operatorname{Hom}(M,-)$ is a covariant functor:
direction of induced map is same.

Can take sum of submods, their intersection (a submod), not their product, only prod. of ideal & submod., can do quotients.

- If $M, N \subseteq P$ submodules, then $[M:N] = \{a \in A \mid aN \subseteq M\} \subseteq A$ is an ideal. In part, $[0:N] = \operatorname{Ann} N$, the annihilator of N.

- If $S \subseteq M$, S a subset of M a module, then $\langle S \rangle = \{x \in M \mid x = \sum_{i=1}^{n} a_i s_i$ for some $n \geq 0$, $a_i \in A$, $s_i \in S\} \subseteq M$ is the smallest submod of M containing S.

Def: M is finitely generated if $\exists$ an $S \subseteq M$, S finite, s.t. $\langle S \rangle = M$.
(somewhat analogous to f.d. vector sp's)

Ex: $\mathbb{Z}/2\mathbb{Z}$ as a $\mathbb{Z}$-module does not have a basis. 1 is a generator, but not lin. ind, bc $2 \cdot 1 = 0$ (ie $2x = 0 \not\Rightarrow x = 0$), so not a basis.

Prop: M is f.g. $\Leftrightarrow$ $M \simeq$ quotient of A^n.
($A^n = \bigoplus_{i=1}^{n} A$)

Pf: If $M = A^n/N$ for some $N \subseteq A^n$ a submod, then $\{\overline{e_i}\}_{i=1}^{n}$, $e_i = (0, 0, \ldots, \overset{i^{th}\text{ position}}{1}, 0, 0, \ldots 0) \in A^n$ form a finite set of generators.

If M is f.g. by $\{x_1, \ldots, x_n\} \subseteq M$, then map $A^n \to M$ by $\phi(e_i) = x_i$, & extend by linearity.
Then ϕ a mod. hom, & onto.
$\Rightarrow M \simeq A^n/\ker\phi$ ✓

2/6 Nakayama's Lemma: (NAK Lemma) → Goal

Prop: Let M be a f.g. A-mod, $\mathfrak{a} \subseteq A$ an ideal, $\phi: M \to M$ a mod. hom. w/ property $\phi(M) \subseteq \mathfrak{a}M$.
Then $\exists\, a_1, \dots, a_n \in \mathfrak{a}$ s.t. $\phi^n + a_1\phi^{n-1} + \cdots + a_n = 0$.
(fcnal eqn in $\mathrm{Hom}(M,M) = \mathrm{End}(M) \leftarrow$ a comm. ring)
[similar to "a matrix satisfies its characteristic poly"].
Pf: Let $x_1, \dots, x_n$ be a set of generators of M.
Write $\phi(x_i) = \sum_{j=1}^{n} a_{ij} x_j$, $a_{ij} \in \mathfrak{a}$.

$$\Rightarrow \sum_{j=1}^{n} (\phi \cdot \delta_{ij} - a_{ij})(x_j) = 0$$

$$\Rightarrow \underbrace{\begin{pmatrix} \phi - a_{11} & -a_{12} & -a_{13} & \cdots & -a_{1n} \\ -a_{21} & \phi - a_{22} & -a_{23} & & \\ & & & \ddots & \\ & & & & \phi - a_{nn} \end{pmatrix}}_{X} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = 0$$

Mult by X-adjoint (take all det's of minors) ↙ w/ transpose & sign change
[Given sq. matrix X, $\exists$ adjoint X^+ s.t. $X^+X = \det X \cdot I$]
$\Rightarrow (\det X)\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = 0 \Rightarrow \det X = 0 \in \mathrm{End}(M)$ (b/c $=0$ $\forall$ gens)
($\det X \in \mathrm{End}(M)$)
$\Rightarrow$! $\det X$ = product of diag. $= 0$ → eqn of correct form. □

Cor 1: If $\mathfrak{a}M = M$, then $\exists\, x \in A$, $x \equiv 1 \bmod \mathfrak{a}$ s.t. $xM = 0$.
Pf: Take $\phi = id \Rightarrow \underbrace{(1 + a_1 + \cdots + a_n)}_{= x} m = 0 \quad \forall m \in M$
Then $x \equiv 1 \bmod \mathfrak{a}$ & $xm = 0 \ \forall m \in M$ □

Jacobson radical, $\mathcal{R} = \bigcap \mathfrak{m}$, $\mathfrak{m} \subseteq A$, $\mathfrak{m}$ maxl.

Fact: If $x \equiv 1 \bmod \mathcal{R} \Rightarrow x$ unit.

Nakayama's Lemma: Let M be f.g. A-mod & $\underline{a} \subsetneq A$ an ideal, $\underline{a} \subseteq \mathcal{R}$. Then $\underline{a}M = M \Rightarrow M = 0$.

Pf 1: $\underline{a}M = M \Rightarrow \exists x \in A$ $x \equiv 1 \bmod \underline{a}$ s.t. $xM = 0$,
But $x \equiv 1 \bmod \mathcal{R} \Rightarrow x$ a unit, $yx = 1 \Rightarrow M = yxM$
$= y(0) = 0$. ✓

Pf 2: Assume $M \neq 0$. Then let $\{x_0, \dots, x_n\} \neq \emptyset$ be a minimal set of generators (minimal exists b/c M f.g.) ($\neq \emptyset$ b/c $M \neq 0$). $x_n \in \underline{a}M = M \Rightarrow x_n = a_1x_1 + \cdots + a_nx_n$, $a_i \in \underline{a}$
$\Rightarrow (1-a_n)x_n = a_1x_1 + \cdots + a_{n-1}x_{n-1}$. But $1-a_n$ is a unit, so mult by inverse & $x_n = a_1(1-a_n)^{-1}x_1 + \cdots + a_{n-1}(1-a_n)^{-1}x_{n-1}$
$\Rightarrow x_n \in \operatorname{span}\{x_1, \dots, x_{n-1}\}$, contradiction of minimality.
(ie, can throw out all gen's, so $M = 0$)

Cor: If M f.g., $N \subseteq M$ submodule, $\underline{a} \subseteq \mathcal{R}$, then $M = \underline{a}M + N \Rightarrow M = N$.

Pf: Mod out by N:
$M/N = (\underline{a}M+N)/N \overset{?}{=} \underline{a}(M/N) \Rightarrow M/N = 0 \Rightarrow M = N$.

Prop: Let A be a local ring w/ max. ideal $\underline{m}$, M a f.g. A-mod. $A/\underline{m} = k$ (residue field). Notice that $M/\underline{m}M$ is a k-vector sp. (b/c action of $\underline{m} = 0$; so really an action of $A/\underline{m} = k$). Let $x_1, \dots, x_n \in M$ s.t. $\overline{x}_1, \dots, \overline{x}_n$ generate $M/\underline{m}M$ as a k-vector sp. Then $x_1, \dots, x_n$ gen. M.

Pf: Let $N = \langle x_1, \dots, x_n \rangle$. WTS $M = N$. [Note that $N/\underline{m}(M \cap N) \subseteq M/\underline{m}M$, and the assumption that $\overline{x}_1, \dots, \overline{x}_n$ implies that they are $=$.]

Claim: $M = N + \underline{m}M$.

Pf: Let $x_1 \in M$. Look at $\overline{x} \in M/\underline{m}M$. Then
$\overline{x} = \overline{a}_1\overline{x}_1 + \cdots + \overline{a}_n\overline{x}_n$ $(\overline{a}_i \in k)$
$\Rightarrow x - (a_1x_1 + \cdots + a_nx_n) \in \underline{m}M$
$\Rightarrow x \in N + \underline{m}M$, ($a_nx_n \in N$) Since $\underline{m} = \mathcal{R}$ (local) $\Rightarrow M = N$ □

This prop. gives a way to choose basis of module, b/c we know how to pick basis of vector sp's: just lift it to M.

Short Exact Sequences

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

- if these were vector sp's, $0 \to A \to B \to C \to 0$, then $B = A \oplus C$, ie $\mathbb{Z} = \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.
- But in modules, B is not uniquely determined by $A \oplus C$.

Also true that $0 \to \mathbb{Z} \to B \oplus \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to 0$ a s.e.s.

So S.e.S's give us ways to build new modules (extensions) from A & C, ie, B.
or a way to decompose a more complicated module, B, into A & C.

2/8 $0 \to A \to B \to C \to 0$ exact means Ker = Im

(A: injective, B→C: surj.)

B is an extension of C by A

$B \supseteq A$ and $B/A \cong C$.

Ex: (Abelian gps) In $\mathbb{Z}$-mod, extensions of $\mathbb{Z}/2$ by $\mathbb{Z}/2$ are: $\mathbb{Z}/2 \oplus \mathbb{Z}/2$ and $\mathbb{Z}/4$ (These are the only 2 gps of order 4)

($\oplus$ always works; ($\not\cong$))

Exactness: We say a functor $F: R\text{-Mod} \to S\text{-Mod}$ is left/right exact if whenever we have a s.e.s. $0 \to A \to B \to C \to 0$, the sequence $0 \to f(A) \to f(B) \to f(C)$ is still exact. or $f(A) \to f(B) \to f(C) \to 0$

(ie, may not be surj.; may not be inj.; still exact)

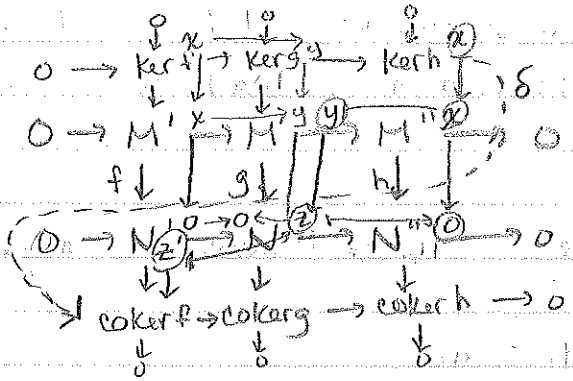
for a covariant (direction of arrows stays same) functor.

For a contravariant functor G,
G left exact: $0 \to G(C) \to G(B) \to G(A)$ exact
G right exact: $G(C) \to G(B) \to G(A) \to 0$ exact

Thm: ① $\mathrm{Hom}(-, M): R\text{-mod} \to R\text{-mod}$ is contravariant left exact
② $\mathrm{Hom}(N, -): R\text{-mod} \to R\text{-mod}$ is covariant left exact

Pf (part) Let $0 \to M' \xrightarrow{g} M \to M'' \to 0$ exact & N an R-mod. ②: $0 \to \mathrm{Hom}(N, M') \xrightarrow{\phi} \mathrm{Hom}(N, M) \to \mathrm{Hom}(N, M'')$
WTS: exact. First, show ϕ is injective.
$\phi(f) = g \circ f$ for $f \in \mathrm{Hom}(N, M')$
If $\phi(f) = \phi(f') \Rightarrow g \circ f = g \circ f'$ but g was injective
$\Rightarrow f = f'$!

Snake Lemma: Let λ w/ all squares commute



$\exists z' \in N'$ b/c $z \mapsto 0$, b/c $x \in \ker h$
so can get from x to z',
well-def? (check $0 \to 0$)
(b/c z' must $= f(y)$, so $z' \in \mathrm{Im} f \Rightarrow z' \to 0$.)

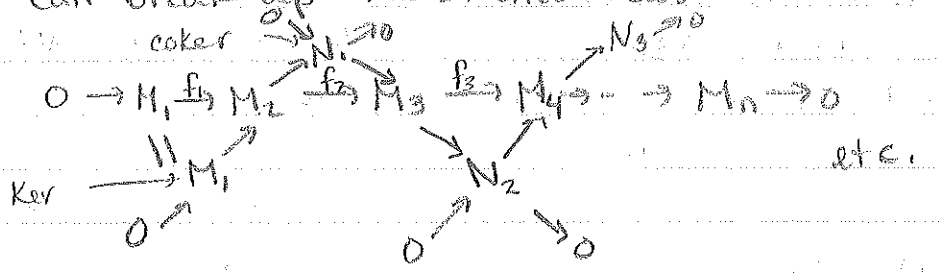
Then $\exists$ a long exact sequence:
$0 \to \ker f \to \ker g \to \ker h \xrightarrow{\delta} \mathrm{coker}\, f \to \mathrm{coker}\, g \to \mathrm{coker}\, h \to 0$

"Diagram Chasing" Why $\ker f \to \ker g$?

If $\lambda: R\text{-mod} \to \mathbb{Z}$ (abel gp) s.t. $\lambda(M) = \lambda(M') + \lambda(M'')$ $\forall$ s.es, $0 \to M' \to M \to M'' \to 0$.
(ex: $\dim: K\text{-}\overset{f.d.}{\mathrm{mod}} \to \mathbb{Z}$ applies)

Prop: If λ as before, & $0 \to M_1 \to M_2 \to \cdots \to M_n \to 0$ is exact, then $\sum_{i=1}^{n} (-1)^i \lambda(M_i) = 0$. (alternating sum $= 0$)

Pf: Can break up l.e.s. into ses:



$N_1 = M_2/\operatorname{Im} f_1 = M_2/\operatorname{Ker} f_2 \cong \operatorname{Im} f_2$, so $N_1 \hookrightarrow M_3$

$N_2 = M_3/\operatorname{Im} f_2 = M_3/\operatorname{Ker} f_3 \cong \operatorname{Im} f_3$, so $N_2 \hookrightarrow M_4$

So break up the les into ses's. So,

$\lambda(M_2) = \lambda(M_1) + \lambda(N_1)$

$-\lambda(M_3) = \lambda(N_1) + \lambda(N_2)$

$-\lambda(M_1) + \lambda(M_2) - \lambda(M_3) = -\lambda(N_2)$

$+\lambda(M_4) = \lambda(N_2) + \lambda(N_3)$

$-\lambda(M_1) + \lambda(M_2) - \lambda(M_3) + \lambda(M_4) = \lambda(N_3)$

$\vdots$

etc.

Read p. 24-27 and review. (Tensor products of modules)

Def: ${}_AM_B$ means A ring, B ring, M is a left A-mod, M right B-mod, & $(a \cdot m) \cdot b = a \cdot (m \cdot b)$ $\forall a \in A, b \in B, m \in M$.

M is called an A-B bimodule.

Thm If ${}_AM_B$ & ${}_BN_C$, then ${}_A(M \otimes_B N)_C$ is an A-C bimod.

Pf: $a \cdot (m \otimes n) = (a \cdot m) \otimes n$ and $(m \otimes n) \cdot c = m \otimes (n \cdot c)$

(& some more checking - is this well-def?)

(NTS

$a(mb) \otimes n \overset{\text{def}}{=} a(mb \otimes_B n) = a(m \otimes bn) \overset{\text{def}}{=} (am) \otimes bn$

$= (am)b \otimes n$

OK, b/c M is A-B bimod.

Reason this is important:

If ${}_AM_B$, then $M \otimes_B - : B\text{-mod} \to A\text{-mod}$ functor.

If $N \in B\text{-mod}$, ${}_BN_{\mathbb{Z}}$ & ${}_AM_B$

$\rightsquigarrow {}_A(M \otimes_B N)_{\mathbb{Z}}$

2/11 ${}_AM_B$ gives rise to a functor, A, B not nec comm. rings

Ob: $\text{Mod-}A \longrightarrow \text{Mod-}B$

$N \longmapsto N \otimes_A M$

Morph: $f: N_1 \to N_2 \longmapsto N_1 \otimes_A M \to N_2 \otimes_A M$ by $f \otimes id$

Rudiments of Morita Theory

Def: Two rings, A & B, are said to be Morita equivalent if the categories Mod-A & Mod-B are equivalent.

- Two categories $\mathcal{C}$ & $\mathcal{D}$.

  $F: \mathcal{C} \to \mathcal{D}$ is a functor if it assoc to each object, $C \in Ob(\mathcal{C})$, $F(C) \in Ob(\mathcal{D})$ & for every $C_1, C_2 \in \mathcal{C}$ a map $Hom_{\mathcal{C}}(C_1, C_2) \to Hom_{\mathcal{D}}(F(C_1), F(C_2))$ s.t. compositions are respected.

  [Given M_1, N_1, get $M_1 \otimes N_1$ $(f \otimes g)(m \otimes n)$
  $\downarrow f$ $\downarrow g$ $\downarrow f \otimes g$ $= f(m) \otimes g(n)$
  M_2 N_2 $M_2 \otimes N_2$]

- Two categories $\mathcal{C}, \mathcal{D}$ are equivalent if there are functors in both directions s.t. the composition is isomorphic to the id in both ways. (see below)

Ex: $\text{Mod-}A \longrightarrow \text{Mod-}A$

$M \longrightarrow M \otimes_A A \cong M$, but $M \neq M \otimes_A A$

→ A pair of functors $F: \mathcal{C} \to \mathcal{D}$ & $G: \mathcal{D} \to \mathcal{C}$ are said to be inverse equivalences if $G \circ F: \mathcal{C} \to \mathcal{C}$ is isomorphic to $1_{\mathcal{C}}$ & $F \circ G \cong 1_{\mathcal{D}}$.

ie, $\forall C \in \mathcal{C}$ a choice of iso Φ_C $(G \circ F)(C) \cong C$ one for each C.

s.t. $C \xrightarrow{f} C'$ commutes.
$\Phi_{C'}$

$(G \circ F)(f)$ $\Phi_{C'}$ $(G \circ F)(C) \to (G \circ F)(C')$

ex: 2 categories w/ only one obj. & all morph's are iso (ie, each is a gp). Need the commutative diagram b/c only looking at functor's action on obj's is trivial. Here, need functors to be gp homomorphisms - ie inverse equivalences.

Look at functors induced by bimods.
Start w/ 2 rings A & B, & try to understand how they could be Morita equiv:

$$\text{Mod-}A \underset{G=\cdot\otimes_B N}{\overset{F=\cdot\otimes_A M}{\rightleftarrows}} \text{Mod-}B \qquad {}_AM_B,\ {}_BN_A \leftarrow A\text{-}A \text{ bimod.}$$

$G\circ F(X) = (X\otimes_A M)\otimes_B(N) \cong X\otimes_A(M\otimes_B N)$

Would like $M\otimes_B N \cong A$ as an A-A bimod.
(b/c then $G\circ F \cong id$, ie $X\otimes_A(M\otimes_B N)\cong X$)
Similarly, want $N\otimes_A M \cong B$ as B-B bimod.

Example (fundamental) $A = k$, a field, $B = M_n(k) = \text{End}_k(V)$, for $V \in A\text{-Mod}$. (b/c an A-mod is a vector sp) & f.g.
Want to write $\text{End}(V) = V^\vee \otimes_k V$
($V^\vee$ = V-dual)

In general, there is a map

$$V^\vee\otimes V \longrightarrow \text{End}(V)$$
$$\varphi = \sum_i f_i\otimes v_i \longmapsto (\tilde{\varphi}: V\to V,\ \tilde{\varphi}(v) = \sum_i f_i(v)\cdot v_i)$$
$$f_i \in \text{Hom}(V,k)$$
$$v_i \in V$$

Claim: This is an iso. ($\varphi \longmapsto \tilde{\varphi}$) of v.s. if V f.d.
Pick a basis $e_1,\dots,e_n$ of V. Given any $\Psi: V\to V$, define φ as follows.
$\forall v\in V$, $\Psi(v) = \sum_i a_i(v)\cdot e_i$. Note, $a_i(v)$ is a linear fcn of v!! Take $\varphi = \sum_i a_i\otimes e_i$, then $\Psi = \tilde{\varphi}$, so map is surj. & is an iso.
$\Rightarrow M = V$ & $N = V^\vee$ so $N\otimes_A M \cong B$.

as k-k bimod.

Is $M \otimes_B N \cong A$? ie, what is $V \otimes_{End(V)} V^\vee$?

If $= k$, then $k \cong M_n(k)$ are Morita equivalent.

(V a left k-mod. why a right $M_n(k)$ mod? mult by matrices on right. So $V^\vee$ is the approp. bi-mod)

Ex: Prove that $V \otimes_{End(V)} V^\vee$ is the same thing as matrices in $End(V)$ which commute w/ everything, ie k.

(HW)

2/13 $\operatorname{Spec} A = Z_1 \amalg Z_2$, $Z_1 = V(I_1)$ $Z_2 = V(I_2)$

$Z_1 \cup Z_2 = \operatorname{Spec} A \Rightarrow I_1 \cap I_2 \subseteq \eta$

$Z_1 \cap Z_2 = \emptyset \Rightarrow I_1 + I_2 = A$

I_1, I_2 coprime, $A/I_1 \times A/I_2 \cong A/I_1 \cap I_2$

$\Rightarrow$ in A/η there are nontrivial idempotents

So $\bar{x}^2 = \bar{x}$ in $A/\eta \Rightarrow x^2 = x + n$ for some $x \in A$, $n \in \eta$

Hint: Try to find smth in A which is idempotent up to n^2. Repeat process, & through induction will get a true idempotent. Try $y = x + an$ for some $a \in A$. (good choice of a!)

=

k a field, V = f.d. k-vector sp. Think of elts of V as column vectors. $End(V) = B$ ($B = M_n(k)$)

${}_B V_k$. Claim: ${}_k V^\vee_B$, B acts if $M \in B$, $f: V \to k$ ($f \in V^\vee$) define $f \cdot M : V \to k$ by $(f \cdot M)(v) = f(M \cdot v)$, a

Check this is a right action.

Get functors

$$\text{Mod-}k \underset{Y \otimes_B V}{\overset{X \mapsto X \otimes_k V^\vee}{\rightleftarrows}} \text{Mod-}B$$

"$\subset$": easy: $Y \longmapsto Y \otimes_B V \longrightarrow Y \otimes_B (V \otimes_k V^\vee) \simeq Y \otimes_B B \cong Y$

"$\supseteq$": $X \to X \otimes_k V^\vee \to X \otimes_k (V^\vee \otimes_B V) \simeq X \otimes_k k \simeq X$

$V^\vee \otimes_B V \ni \sum_i \alpha_i \otimes_B v_i$, $\alpha_i \in V^\vee$, $v_i \in V$

$\downarrow$

If B were k, can turn it into a lin. transf. ϕ.
$x \mapsto \phi \to \sum_i \alpha_i(x) \otimes v_i$

This ϕ is constrained by $\otimes_B$ b/c need
$(\alpha_i \cdot M) \otimes_B v_i = \alpha_i \otimes_B (M \cdot v_i)$ $\forall M \in B$.
So $\phi(Mx) = M \cdot \phi(x)$, ie ϕ commutes w/ any matrix $M \Rightarrow \phi$ is a scalar matrix

* This argument is not quite correct, b/c suggested $\exists$ map $V^\vee \otimes_B V \to V^\vee \otimes_k V$ but arrow actually goes in other direction., b/c $V^\vee \otimes_B V = V^\vee \otimes_k V /$ relation $\alpha_i M \otimes v_i = \alpha_i \otimes M v_i$

Ex: So $\exists$ surj $\uparrow$, i NTS every endomorphism gets identified w/ a scalar matrix in $V^\vee \otimes_B V$.

Applications of Tensor Product in Comm Alg

① Extension of Scalars

$A \xrightarrow{\phi} B$ a map of rings

restriction of scalars:
$B\text{-Mod} \longrightarrow A\text{-mod}$: a acts via $\phi(a)$
(ie, restricting to scalars in $\operatorname{im}\phi$.)
${}_B M$ Then ${}_A M$ b/c $a \cdot m = \phi(a) \cdot m$.

How to get from an A-mod to a B-mod?

If ${}_AN$, we could look at pairs (b,n) s.t. $b \in B, n \in N$. This is a B-mod, b/c B acts on 1st component. Naive, b/c forgets about action of A.
Better, look at $b \otimes_A n$. Get a functor,

$$A\text{-mod} \longrightarrow B\text{-mod}$$
$$N \longmapsto B \otimes_A N$$

(we just use ${}_BB_A$, where right A-mod. structure comes from ϕ).

Ex: Prove: ($\leftarrow$ extension)

$$\mathrm{Hom}_{B\text{-mod}}(B \otimes_A N, N') \cong \mathrm{Hom}_{A\text{-mod}}(N, {}_AN')$$

for any $N \in A$-mod, $N' \in B$-mod ($\uparrow$ restriction of scalars)
We say extension is left adjoint to restriction

Def: If $F: \mathcal{C} \to \mathcal{D}$ & $G: \mathcal{D} \to \mathcal{C}$, F is left adjoint to G if $\mathrm{Hom}_{\mathcal{D}}(FC, D) \cong \mathrm{Hom}_{\mathcal{C}}(C, GD)$ $\forall C \in \mathcal{C}, D \in \mathcal{D}$.

(can be substitute for inverse, if inv. doesn't exist)

Ex: Check that the functor "Forget": Groups $\longrightarrow$ Sets admits a left adjoint F: Sets $\longrightarrow$ Groups, w/
$F(S)$ = free gp on S.
(simply unwinding the def. of free gp)

Natural isomorphism: F, G 2 functors $\mathcal{C} \to \mathcal{D}$ w/ $F(A) \overset{\alpha_A}{\cong} G(A)$ $\forall A$ a natural iso. means
$\forall A \xrightarrow{\varphi} A'$ in $\mathcal{C}$, the following diagram commutes

$$\begin{array}{ccc} F(A) & \xrightarrow{\alpha_A} & G(A) \\ {\scriptstyle F(\varphi)}\downarrow & & \downarrow{\scriptstyle G(\varphi)} \\ F(A') & \xrightarrow[\cong]{\alpha_{A'}} & G(A') \end{array} \qquad (F = {}^{\vee},\ G = \mathrm{id})$$

Ex: Thm: If A a f.d. vector sp, $A^{\vee} \cong A$, but not naturally.
However, $A^{\vee\vee} \cong A$ naturally
($F = {}^{\vee\vee}$ $G = \mathrm{id}$.)

Thm: The functor $-\otimes N$ is right exact, $\forall N$.

Def: We say N is flat if the functor $-\otimes N$ is exact.

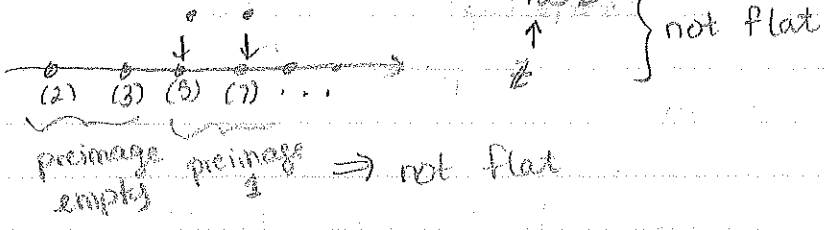
Ex: $\mathbb{Z}/2\mathbb{Z}$ is not a flat $\mathbb{Z}$-mod.

$$0 \longrightarrow \mathbb{Z} \xrightarrow{\cdot 2} \mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow 0 \quad \Big| \otimes \mathbb{Z}/2\mathbb{Z}$$

$$\Rightarrow \quad \mathbb{Z}/2\mathbb{Z} \xrightarrow{\cdot 2} \mathbb{Z}/2\mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow 0$$

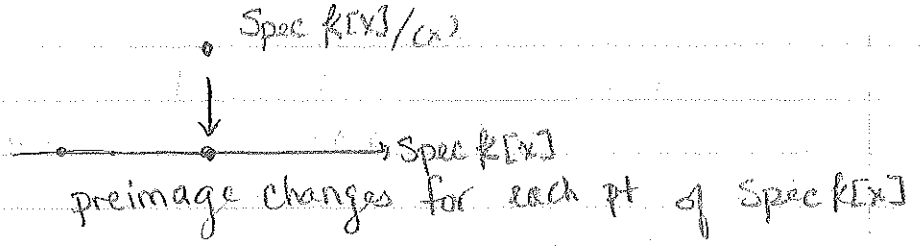
$\cdot 2$ map, so can't be injective

2/15 **Ex**: ① $\mathbb{Z}/n\mathbb{Z}$ is not a flat $\mathbb{Z}$-mod.
but $\mathbb{Z}$ is. b/c tensoring w/ $\mathbb{Z}$ is identity functor



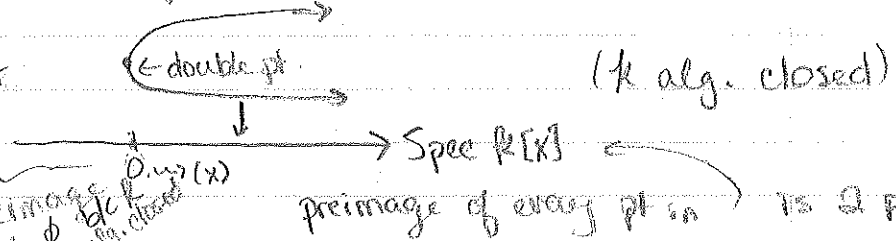
$\Rightarrow$ not flat

② $k[x]/(x)$ is not a flat $k[x]$-mod, but $k[x]$ is
(same argument)



③ Consider the ring map $k[x] \to k[x,y]/(x-y^2)$. This makes $k[x,y]/(x-y^2)$ into a flat $k[x]$ mod.

$(x) \subsetneq k[x,y]/(x-y^2)$ is not prime (b/c $y \cdot y \in (x)$)
$(x) = (x,y)^2$ maximal



(k alg. closed)

Def: Let k be a commutative ring. A *k-algebra* is a ring (possibly non-comm) A and a ring hom. $k \to Z(A)$

- Know how to act on A by scalars (elts of k) by moving them into the center & then multiplying.

Ex: ① $M_n(k)$ is a k-alg. w/ $k \to \begin{pmatrix} k & & 0 \\ & \ddots & \\ 0 & & k \end{pmatrix}$

② $k[x,y]/(x-y^2)$ is a $k[x]$-alg.

Geometrically, if A is commutative, a k-alg. is a space/Spec k, ie a space X plus a map $X \to \operatorname{Spec} k$.

Def: A k-alg. map $A \to B$ is a ring hom $A \xrightarrow{\Phi} B$ s.t.

$$\begin{array}{ccc} & k & \\ \swarrow & & \searrow \\ Z(A) & & Z(B) \\ \searrow & & \nearrow \\ & \Phi \to B & \end{array} \quad \text{commutes.}$$

Thm: If A & B are k-algs, then we can make $A \otimes_k B$, which is also a k-algebra.

Pf: Define $(a \otimes b) \cdot (a' \otimes b') = aa' \otimes bb'$

Ex: Check well-def. & assoc.

Ex: ① Say smth interesting about $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$

- vector sp over $\mathbb{R}$ of dim 4
- comm. ring
- not a field: $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} = \mathbb{R}[x]/(x^2+1) \otimes_{\mathbb{R}} \mathbb{R}[y]/(y^2+1)$
  $= \mathbb{R}[x,y]/(x^2+1, y^2+1)$
  $= \mathbb{C}[y]/(y^2+1) \cong \mathbb{C}[y]/(y-i) \times \mathbb{C}[y]/(y+i)$ (coprime ideals; Chinese remainder Thm)
  (Spec is 2 pts)
- has 0 divisors: $(i \otimes 1 + 1 \otimes i)(i \otimes 1 - 1 \otimes i) = (i \otimes 1)^2 - (1 \otimes i)^2$
  $= (-1) \otimes 1 - (1 \otimes -1)$
  $= 0$

non-zero b/c $\mathbb{C}$ has basis over $\mathbb{R}$ $(1, i)$ & $i \otimes 1, 1 \otimes i$ are lin. ind. $\Rightarrow$ So basis $(i \otimes 1, 1 \otimes i, 1 \otimes 1, i \otimes i)$

Detour through Non-comm. Alg

Def: An irreducible (simple) module (left/right) M is one which has no other (L/R) submods but 0 or M.
(irred. mods correspond exactly to irreps of gp algs)

Schur's Lemma: If M is simple & $\phi: M \to M$ is a nonzero module hom, then ϕ is an iso.

Pf: Note: $\ker\phi$ & $\operatorname{Im}\phi$ are submods of M.

$\phi \neq 0 \Rightarrow \operatorname{Im}\phi \neq 0 \Rightarrow \operatorname{Im}\phi = M \Rightarrow$ Surj.

$\phi \neq 0 \Rightarrow \ker\phi \neq M \Rightarrow \ker\phi = 0 \Rightarrow$ Inj. $\square$

(Also true $\phi: M \to N$, M & N are both simple)

* Simple mods are $\cong$, or there are no homs btwn them & all homs are isos.

Cor: If M is simple, $\operatorname{End}(M)$ is a division algebra (or a skew-ring – a field, but not nec. comm.: a poss. non-comm. ring where every $\neq$ elt. is invertible)

Pf: all end's are iso's ✓

Ex: If D is a division alg (simple as a mod over self – b/c submods = ideals & all ideals contain unit) then D^n is a simple $M_n(D)$-mod.
(module – multiply vectors by matrices)
simple; can get all matrices from one vector & elementary matrices.

Def: A ring A is simple if it is simple as a 2-sided mod over itself
$\Rightarrow$ 2-sided submods = 2-sided ideals of A.
(similar to that of gps)

Ex: Show $M_n(D)$ is simple.

2/18 Simple ring: no 2-sided ideals (other than 0 & R).

Simple, f.d. k-alg's, k a fixed field.

Ex: $k = \mathbb{R}$: $\mathbb{C}$, $\mathbb{H}$: } all f.d. div. alg's over $\mathbb{R}$ (Frobenius)
(↑ f.d. skew-field over $\mathbb{R}$ (ie, division alg))
Also $M_n(\mathbb{R})$, $M_n(\mathbb{C})$, $M_n(\mathbb{H})$ } all simple f.d. k-alg.

Aim: Wedderburn's Thm: If k a field, every f.d. simple k-alg is of the form $M_n(D)$, D is a f.d. division k-alg., $n > 0$.

Def: A central simple k-alg is a f.d. k-alg. A, which is simple & $Z(A) = k$.
(always $k \subseteq Z(A)$)
- above, $\mathbb{C}$ & $M_n(\mathbb{C})$ are not central.

We will see that if A, B are central simple k-alg's, so is $A \otimes_k B$.

- It follows that we get a gp, Brauer gp of k:
$Br(k) = (\{\text{central simple algs}\}/\sim, \otimes)$ (up to Morita equivalence)
$A \sim B$ if $\exists\, n, m \in \mathbb{Z}$ s.t. $M_n(A) \cong M_m(B)$.
(an alg & the matrices over it are same in $Br(k)$)
$\Leftrightarrow A \overset{k}{\sim} B$ Morita equiv.

Ex: $\mathbb{H} \otimes_{\mathbb{R}} \mathbb{H} \cong M_4(\mathbb{R})$ ← id in $Br(\mathbb{R})$ (prove this) (4 b/c $\dim \mathbb{H}_{\mathbb{R}} = 4$)
$\Rightarrow Br(\mathbb{R}) = \mathbb{Z}/2\mathbb{Z}$ so $\mathbb{H}$ has order 2, & $\mathbb{H}$ the only non-trivial elt in $Br(\mathbb{R})$

Lemma: Let A be a non-comm. k-alg. which is f.d. over k. (in particular, it's a k-vector sp). Then:
(1) A has a simple right module
(2) Any non-zero mod contains a simple sub-mod.
(3) A simple mod has f.d. over k.
(4) If M is simple, $End_A(M)$ is a k-division alg

Pf: [(2) ⇒ (1) b/c $A \neq 0$.]

(2): Any minimal $\neq 0$ submod is simple. Why is there such a submod?

Start w/ $m \in M$, $m \neq 0$, look at $mA \subseteq M$ ← cyclic submod of M

f.d. vector spaces satisfy the descending chain condition. $mA \neq 0$, f.d. over k b/c $\exists$ surj $A \to mA$, quotient of A. ⇒ f.d.

(3): (It must be contained in a cyclic submod, which is f.d.) OR

If M is simple, $0 \neq m \in M$, then $mA = M$, & mA f.d. as above.

(4) Follows from Schur's Lemma.

Lemma: Assume A simple, $M \subseteq A$ a $\neq 0$ right ideal. Then A = bicommutant of M.

Def: If M an A-mod, $A' = \mathrm{End}_A(M)$ is the commutant of M, & $A'' = \mathrm{End}_{A'}(M)$ is the bicommutant. ⇒ M is an A'-mod.

Ex: k a field, M a f.d. vector sp. over k. Then

$A' = \mathrm{End}_k(M) = M_n(k)$

$A'' = \mathrm{End}_{M_n(k)}(M) = k$

Ex: If $A = M_n(k)$, $M = k^n$ (column vectors)

$A' = \mathrm{End}_A(M) = k$

$A'' = \mathrm{End}_k(M) = A$

$\begin{pmatrix} 0 & | & * \\ & | & \vdots \\ & | & * \end{pmatrix}$ ← copy of M; ½ left ideal

b/c $\begin{pmatrix} * & * \\ * & * \end{pmatrix}\begin{pmatrix} 0 & * \\ & \vdots \\ & * \end{pmatrix} = \begin{pmatrix} 0 & * \\ & \vdots \\ & * \end{pmatrix}$

Thm (Wedderburn): Any simple f.d. k-alg is of the form $M_n(D)$ for D a division k-alg.

Pf: Pick a simple (right) submod. M inside A. (M a nonzero rt ideal b/c submod).
$A' = \mathrm{End}_A(M)$ is a divion alg by Schur's Lemma.
Call $A' = D$. So, by lemma,
$A = \mathrm{End}_D(M)$.
But M is f.g. over D b/c f.g. over $k \subseteq D$ b/c M a f.d. vector sp over k. (Every max. set of lin. ind elts is a basis → true for skew-fields, as well)
D a skew-field ⇒ M is free over D ⇒
$A = \mathrm{End}_D(M) = M_n(D)$, where $n = \dim_D M$.

Ex (of an ∞-dim. simple ring) W = Weyl alg.
$W = D_{\mathbb{A}^1} = \underbrace{k\langle x, \partial\rangle}/\langle \partial x - x\partial = 1\rangle$
free, n.c. alg over k in x & ∂

Ring of all differential operators on the line.
$\partial = \frac{\partial}{\partial x}$, $x = \cdot x$, $1 = \cdot 1$
$\frac{\partial}{\partial x}(x^n \cdot x) = (n+1)x^n$ } $(n+1)x^n - nx^n = 1\cdot x^n$ ✓
$x \cdot (\frac{\partial}{\partial x} x^n) = n x^n$ }

$(\partial^{m_1} x^{n_1})(\partial^{m_2} x^{n_2}) = \partial^{m_1+m_2} x^{n_1+n_2} + \text{l.o.t's}$.

· deformation of polynomial ring
If $\langle \partial x - x\partial = 0\rangle$, get poly. ring in 2 var's.
$W_t = k\langle x, \partial\rangle / \langle x\partial - \partial x = t\rangle$

Then $W_0 = k[x, \partial]$ = fcns on cotangent bundle of the line. ($\Omega^1_{\mathbb{A}^1}$ ← symplectic manifold)
↳ 2 copies of line

W_1 is a quantization of the fcns on $\Omega^1_{\mathbb{A}^1}$.

2/20 **Lemma** (from last time): If A simple, $M \subseteq A$ a non-zero right ideal, then $A'' = A$, where A'' = bicommutant, $A'' = \mathrm{End}_{A'}(M)$, $A' = \mathrm{End}_A(M)$.

Pf: Define the map $R: A \to A''$

$R(a)\cdot(m) = ma$ (check this ends over A')

This is a ring hom. WTS inj & surj.

① Injective: $R(1) = \mathrm{Id}_M \neq 0 \Rightarrow R \neq 0$, so $\ker(R)$ is 2-sided in A & not everything, so $\ker(R) = 0$

② Surjective: (i) $R(M)$ a rt ideal in A'':

WTS if $a'' \in A''$ and $m \in M$, then $R(m)\cdot a'' = R(m\cdot a'')$

ie WTS $\forall n \in M$ we have $(a'' \circ R(m))(n) = (R(m\cdot a''))(n)$.

$a'' \circ R(m) = a''(m)$

$= (nm)\cdot a'' \iff = n(m)\,a''$

$= n\cdot a''(m)$ b/c a'' an A'-mod hom., so comm. w/ elts of A', & consider $n\cdot -$ as a endo. of M.

ie, $a''(nm) = n\cdot a''(m)$ ✓

(ii) $R(A)$ a rt ideal in A''. (⇒ done, b/c it's a right ideal that contains $1_{A''}$, so must be everything.)

M was a right ideal in $A \Rightarrow A\cdot M$ a 2-sided ideal in A. $\Rightarrow A\cdot M \supseteq M \neq 0 \Rightarrow A\cdot M = A$ (since A simple) $\Rightarrow R(A) = R(A\cdot M) = R(M)\cdot R(A) = R(M)$

↑ b/c right mult. switches order.

Thm: The tensor prod of 2 central simple alg's is again central simple.

Pf: (read in notes)

⇒ The Brauer gp exists.

- $B_r(\mathbb{R}) = \mathbb{Z}/2\mathbb{Z}$

Thm: If k an alg. closed field, $Br(k) = 0$.
(ex, $Br(\mathbb{C}) = 0$)
ie, every f.d. div. alg. over $\mathbb{C}$ must be $\mathbb{C}$.

Def: Let A be a k-alg., $B \subseteq A$ a sub. alg. Then the centralizer of B is: $C = \{x \in A \mid xy = yx \ \forall y \in B\}$, C is a subalg.

Lemma: If A, A' algs, $B \subseteq A$, $B' \subseteq A'$ subalgs w/ centralizers C, C', then the centralizer of $B \otimes B' \subseteq A \otimes A'$ is $C \otimes C'$.
Pf: $C \otimes C' \subseteq C''$ obvious.
read $C'' \subseteq C \otimes C'$. □

Lemma: If A is a simple k-alg, then $Z(A)$ is a finite extension of k, ie $Z(A)$ is a field, $k \subseteq Z(A)$, & $\dim_k Z(A) < \infty$.
Pf: Note that $A = M_n(D)$, D a f.d. div. alg. over k, by Wedderburn. $M_n(D) = M_n(k) \otimes_k D$ (extension of scalars, check!)
By lemma, $Z(A) = Z(M_n(k)) \otimes_k Z(D)$
$= k \otimes_k Z(D) = Z(D)$, a field.
$k \subseteq Z(A)$ by def.
f.d. over k b/c A was f.d, so its center must be. □

Cor: If $k = \bar{k}$, $Z(A) = k$. (b/c no finite field ext's since alg. closed)

Pf of Thm: Let D be a f.d. div. alg. over k (assume $k = \bar{k}$). Pick any $x \in D$. Look at $k[x] \subseteq D$ (subring of D gen by k & x). $k[x]$ f.d over k (b/c D was) Comm. subring, b/c k are scalars & D div alg. over k, & powers of x always comm.

Thus $k[x]$ a f. field ext. of $k \Rightarrow k[x] = k$
$\Rightarrow x \in k. \Rightarrow k = D.$ □

Cor: Any simple alg. over $k = \bar{k}$ is $M_n(k)$ for some n.

Fact (w/o proof): Let A be a f.d. alg over a field k. If $A \otimes_k \bar{k} = M_n(\bar{k})$, then A is central simple over k.

Almost pf (of existence of Br gp): ie c.s.a. $\otimes$ c.s.a = c.s.a.
Let A, B be central simple algs over k, $\bar{k}$
$\bar{A}, \bar{B}$ be $A \otimes_k \bar{k}$, $B \otimes_k \bar{k} \Rightarrow \bar{A} = M_n(\bar{k})$, $\bar{B} = M_{n'}(\bar{k})$
$\Rightarrow \bar{A} \otimes_{\bar{k}} \bar{B} = M_{nn'}(\bar{k}) = (A \otimes_k \bar{k}) \otimes_{\bar{k}} (B \otimes_k \bar{k})$

check! tensor prod of 2 matrix algs is a matrix alg

$= (A \otimes_k B) \otimes_k \bar{k} = \overbrace{A \otimes B}$ = matrix alg. ← extended.
By fact, $A \otimes B$ is central simple.

Semi-Simplicity
- a simple ring has a ! irred. mod., & all other mods are sums of it.

Def: A module is semi-simple if it is a direct sum of irreducibles. A ring is s-s if every f.g. mod. is semi-simple.

2/22 HW

(11b) True that $m \leq n$. $\phi: R^m \to R^n$ inj $\Rightarrow$ $m \leq n$.

(If R int dom, tensor w/ field of fracs of R $\to$ exact)

(Baltach) Assume $m > n$,

$$R^m \hookrightarrow R^n \hookrightarrow R^m$$

(ψ is injective & $\operatorname{Im}\psi$ has last coord. 0)

ψ an endo of R^m, so it satisfies a poly:

$\psi^k + a_1\psi^{k-1} + \cdots + a_k = 0$ $\quad a_i \in R$. of minimal degree

$\Rightarrow a_k \neq 0$. b/c ψ inj, else $\psi(\psi^{n-1} + \cdots + a_{n-1}) = 0$ & have left cancelation b/c ψ inj.

On the other hand, plug in $(0, 0, \ldots, 1)$

LHS has a_k in last coord, so $\neq 0$ $\lightning$.

Farb & Dennis, Noncommutative Alg, Ch. 1.

Def: A module M is s.s. if it is a direct sum of simple modules. It is s.s. & of finite length if this direct sum is finite.

Ex: v.sp's (sum of 1-D v.sp's) & f. length = f. dim.

Prop: Assume $M_i \subseteq M$ are simple ($i \in I$) s.t. $\sum_{i \in I} M_i = M$. (ie, every elt in M can be written as sum of M_i's, not nec. uniquely), then M is s.s. & $\exists$ $J \subseteq I$ s.t. $M = \bigoplus_{i \in J} M_j$.

Pf: Say $J \subseteq I$ is lin. ind. if $\sum_{j \in J \text{ finite}} m_j = 0 \Rightarrow m_j = 0$ $\forall j \in J$ if $m_j \in M_j$ $\forall j$ (ie, modules form dir. sum $\to$ there's no $\cap$)

Let J be maximal s.t. it's lin. ind. (use Zorn's Lemma to show such a J exists). Then J generates, ie. $\bigoplus_{j \in J} M_j = M$: Denote $N = \bigoplus_{j \in J} M_j$

$\forall i \in I$, look at $M_i \cap N$ (a submod of M_i) if $= 0$, can add i to J & stay lin. ind. $\lightning$ ($\Leftarrow$ $J \cup \{i\}$ is lin. ind.)

$\Rightarrow M_i \cap N = M_i$ b/c M_i is simple. $\Rightarrow M_i \subseteq N$, so $M = \sum M_i \subseteq N$ ✓

Cor: Submodules & quotients of ss are ss.

Pf: If M ss & $N \subseteq M$ sub, $\exists$ surj $M \xrightarrow{\phi} M/N \to 0$

$$M = \bigoplus_{i \in I} M_i$$

$\Rightarrow \phi(M_i)$ generate M/N, & they are 0 or simple ✓

Look at $N \cap M_i$. N is gen. by $N \cap M_i$, which are 0 or simple (b/c they're submods of M_i, simple)

Cor: If $N \subseteq M$ sub, then N is a direct summand of M. (M s.s.)

Pf: Write $M = \bigoplus M_i$. Then $N = \bigoplus (M_i \cap N)$

non-zero for a subset of M_i's

Let $J = \{i \in I \mid M_i \cap N \neq 0\}$. Then $M = N \oplus \left(\bigoplus_{i \neq j} M_j\right)$

(exercise) **Prop**: Converse is true, ie, if every submod is a direct summand, then M is s.s.

Prop: If M s.s. & of finite length, then $\mathrm{End}(M) = \bigoplus_{i=1}^{n} M_{n_i}(D_i)$

$n_i \in \mathbb{Z}$, D_i is a div. alg.

Pf: $M = \bigoplus M_i$ (finite). Collect all by iso. type. No hom's btwn types. $M_{n_i}(\mathrm{End}(M_i))$, n_i = # of M_i's of that type.

↑ a div. alg. by Schur's Lemma.

$\mathrm{End}(M_i^{\oplus n_i}) = M_{n_i}(D_i)$

Def: R is <u>s.s.</u> if it is s.s. as a left module over itself.

Thm: TFAE

(1) R is s.s.

(2) Every left R-mod. is ss

(3) Every s.e.s. of R-mod's splits

Detour: Consider a ses

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

TFAE: (1) $M \cong M' \oplus M''$

HW: prove this

(2) $\exists\ p' : M \to M'$ s.t. $p' \circ i = id_{M'}$

(3) $\exists\ i' : M'' \to M$ s.t. $p \circ i' = id_{M''}$

ie, $0 \longrightarrow M' \xrightarrow{i} M \xrightarrow{p} M'' \longrightarrow 0$ with $\exists\ p'$ or $\exists\ i'$

We then say the ses <u>splits</u> & i' & p' are called <u>splittings</u>

<u>Pf of thm</u>:

(1) $\Rightarrow$ (2): If M an R-mod, then M is a quotient of R^I so R^I s.s. b/c R is $\Rightarrow M$ s.s. by prop.

(2) $\Rightarrow$ (3): Obvious b/c $M' \cong M$ is a direct summand

(3) $\Rightarrow$ (1): Pick any submod I of R fits in a s.e.s $0 \to I \to R \to \frac{R}{I} \to 0$ which splits by (3) $\Rightarrow$ I is a direct summand $\forall$ submods I.

$\Rightarrow R$ s.s.

<u>Ex</u>: ① D a div. alg. (b/c all we know a bases carries through to div. alg's, so all mod's s.s.

② $M_n(D)$ ← module theory same as that for D (Morita equivalent ? s.s. is invariant under Morita equivalence)

③ $\mathbb{Z}/n\mathbb{Z}$ s.s. iff n is square-free, (product of distinct primes to power 1)

④ $k[G]$ is ss iff $\text{char } k \nmid |G|$: <u>Maschke's Thm</u>
$|G| < \infty$ gp. (note, if $\text{char } k = 0$, $k[G]$ is ss)

(Artin-Wedderburn Thm)

Structure Thm 1: If R ss, $R \cong \prod_{i=1}^{n} M_{n_i}(D_i)$

$n_i \in \mathbb{Z}$, D_i div. alg.

Pf: $R = \mathrm{End}_R(R)$ and R fg. by 1 so R fin. length

$\frac{1}{1}$ ↗ is of the correct form (earlier prop.)

$R = \bigoplus_{i \in I} M_i$, M_i simple

1 = finite sum of elts in M_i, but can get R by mult w/ 1, so no other M_i can show up

$\Rightarrow$ fin. length

Cor: R comm & ss $\Rightarrow R = \prod_{i=1}^{n}$ fields

Thm: If R is ss, then $R = \bigoplus_{i=1}^{n} R_i$, R_i simple R-mod and these are all the irred (simple) R mods.

(analogue to regular rep. of gp = $\oplus$ of all irreps)

Pf: Let M be a simple R-mod. Then $\exists$ a map (surj)

$$\bigoplus R_i = R \to M \to 0$$

$\mathrm{Im}(R_i)$ in M is either 0 or M, & at least one nonzero b/c map surj. But then that nonzero map $R_i \to M$ must be an iso (Schur's Lemma)

b/c cyclic submod of M gen. by $m \in M$ is M.

2/25 A an R-alg, R comm. We say A is Azumaya if $\forall \mathfrak{m} \subseteq R$ maximal, $A_{\mathfrak{m}} = A \otimes_R R/\mathfrak{m}$ (a field) is central simple, ie it becomes a matrix alg. after a finite unramified extension of $R/\mathfrak{m}$. (A way to extend Brauer gp to schemes)

Recall: Matrix algs over division rings are simple.

Thm (2^{nd} Artin-Wedderburn) If A a ss k-alg & $A = A_1 \times \cdots \times A_m$ & $A = A_1' \times \cdots \times A_n'$, A_i, A_j' simple, then $m=n$ & $\forall i \; \exists j$ s.t. $A_i = A_j'$ (actually $=$, not $\cong$!)

Pf: Each A_i, A_j' are 2-sided ideals in A. So,

$$A_1 = A_1 \cdot A = \prod_{j=1}^{n} \underbrace{A_1 \cdot A_j'}_{\text{2-sided ideal in } A_1, \text{ which is simple} \Rightarrow = 0 \text{ or } A_1}$$

If more than 1 $A_j' = A_1$, it wouldn't be a direct prod. so, $\exists! j$ s.t. $A_1 \cdot A_j' = A_1 \Rightarrow A_j' = A$. (b/c $A_1 A_j'$ also a 2-sided ideal in A_j'.)

Thm: Let G be a finite gp, k a field, $\operatorname{char} k \nmid |G|$. Then $k[G]$ is ss.

Pf: We'll show that any ses of $k[G]$-mods (which are same as G-reps, ss vector sp's w/ a multiplication by G) splits. Let

$$0 \to M' \to M \underset{s}{\overset{p}{\rightleftarrows}} M'' \to 0 \quad \text{be a ses of } k[G]\text{-mods}$$

B/c every ses of v. sp's splits (pick a basis of M'', lift it to M by p, since p surj, then define s by mapping basis elts to basis elts.), can always find an s s.t. $p \circ s = \mathrm{id}_{M''}$, & s is a map of v. sp's. We'd need $s(g \cdot m'') = g \cdot s(m'')$ for s to be a map of G-mods. or, that $g^{-1} s(g \cdot m'') = s(m'')$ $\forall g \in G$. No reason for this to be so.

Define $S: M'' \to M$ by $S(m'') = \sum_{g \in G} g^{-1} s(gm'')$

Claims: ① S is G-equivariant, ie $S(hm'') = hS(m'')$.

Pf: Just summing over hg's, so same.

② $p \circ S = |G| \cdot id_{M''}$.

$$p(S(m'')) = \sum_{g \in G} g^{-1} p \cdot s(gm'')$$
$$= \sum_{g \in G} g^{-1} g m''$$
$$= |G| m''$$

So if $|G|$ is invertible in $k[G]$ (i.e., if $\operatorname{char} k \nmid |G|$), then $\frac{1}{|G|} S$ is a G-equivariant splitting.

Ex: Consider the surj. map of $k[G]$-mods, "augmentation"

$$k[G] \xrightarrow{\varepsilon} k$$
$$\sum_{g \in G} a_g \cdot g \longmapsto \sum a_g$$

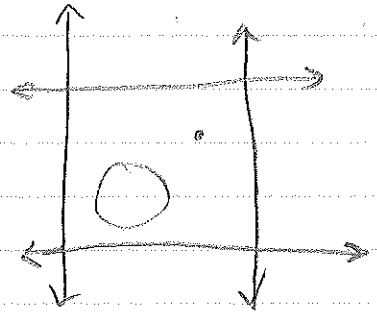
Claim: This splits if $\operatorname{char} k \nmid |G|$

Tensor Products of Comm Alg

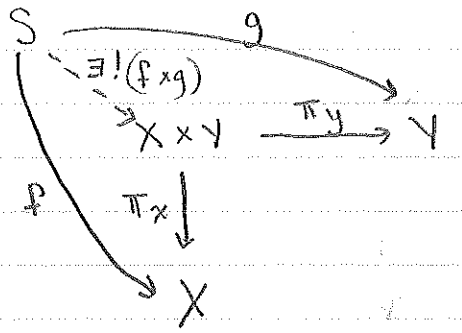
$$k[x_1, \dots, x_n] \otimes_k k[y_1, \dots, y_m] = k[x_1, \dots, x_n, y_1, \dots, y_m]$$

Specm: $k[x_1, \dots, x_n] \to k^n$; Specm: $k[y_1, \dots, y_m] \to k^m$; Specm: $k[x_1, \dots, x_n, y_1, \dots, y_m] \to k^{n+m}$

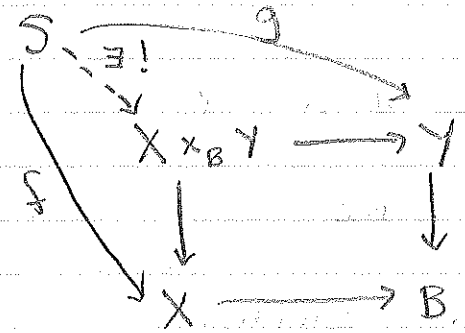
- need Specm, not Spec, b/c in each line, prime ideals are pts, so products are pts & lines, but ∃ more irred. curves (the ⊙, for ex)



For Sets: The universal property of $X \times Y$: $\forall f: S \to X$ & $\forall g: S \to Y$, $\exists!$ $(f \times g): S \to X \times Y$ s.t. $\pi_X \circ (f \times g) = f$ & $\pi_Y \circ (f \times g) = g$.



For Fiber Products: Now f, g are maps over B, ie $= id$ when go all the way to B.
$X \times_B Y$ is called the fiber product

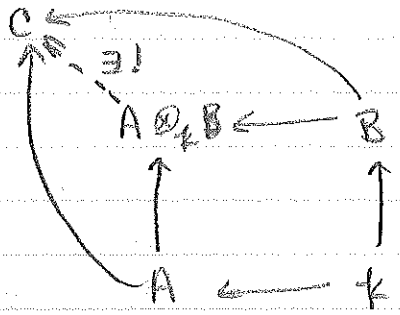


Exercise:
① $X \times_B Y$ is unique up to unique isomorphisms
② If $B = \{*\}$, then $X \times_B Y = X \times Y$
③ If $X \subseteq B$, $Y \subseteq B$, then $X \times_B Y = ?$
④ If $X = \{b\}$, $b \in B$, $Y \to B$ arbitrary, then $X \times_B Y = ?$

Thm: $\mathrm{Spec}(A \otimes_k B) = \mathrm{Spec}\, A \times_{\mathrm{Spec}\, k} \mathrm{Spec}\, B$ (in affine schemes). Ie, Spec satisfies the universal property for affine schemes.

Pf For A, B comm. alg over a comm. ring k,
⊗ is the categorical fiber coproduct in comm. rings. ↳ b/c arrows reversed.

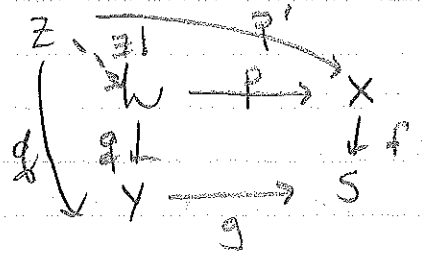
ie,



(Check!)

Then replacing everything w/ Spec reverses the arrows, & so it satisfies the univ. prop. for fiber products.

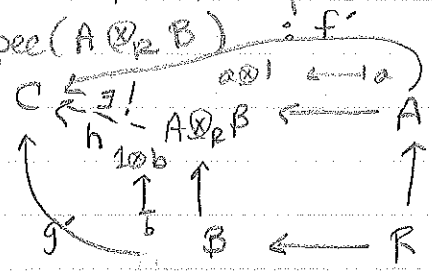
2/27 A space W with maps p & q over S (ie $f \circ p = g \circ q$) is called a fiber product of X & Y over S if it satisfies: $\forall Z$ & maps p' & q' over S (ie $f \circ p' = g \circ q'$) there exists a unique map $Z \to W$ making the diagram commute.



So to show the fiber product exists, need to exhibit a W and maps p, q.

In the category Sets, $W = \{(x,y) \in X \times Y \mid f(x) = g(y)\}$
In the category Top, same.
Define the category Affine Schemes $= (\text{Comm Rings})^{op}$
ie, same objects, but all arrows reversed.
(had an exercise which showed $X, Y \subseteq \mathbb{A}^n$ (algebraic a poly (regular) map $X \to Y \Leftrightarrow$ ring map $R_Y \to R_X$)

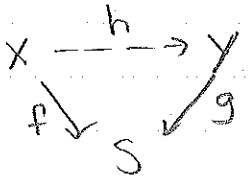
In AffSch, fiber products exist & $\operatorname{Spec} A \times_{\operatorname{Spec} R} \operatorname{Spec} B = \operatorname{Spec}(A \otimes_R B)$



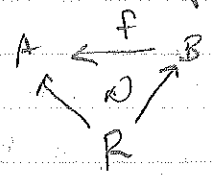
$h(a \otimes b) = f'(a) \cdot g'(b)$

(NTC well-def, ring map, unique)

Fix a space S. A <u>space over S</u>, X, is a pair (X, f) w/ $f: X \to S$. If (X,f) & (Y,g) are spaces over S, then a map $h: X \to Y$ is a <u>map over S</u> if $f = g \circ h$ (ie, preserves the structure map)



Similar to a map of R-algebras vs. a ring map



- If $S = \{*\}$, $X \times_S Y = X \times Y$.

- $X_s = X \times_S \{s\} \longrightarrow X$; $X_s = f^{-1}(s)$ (the fiber of f over s)

$$\begin{array}{ccc} X_s & \longrightarrow & X \\ \downarrow & & \downarrow f \\ \{s\} & \longrightarrow & S \end{array}$$

- If $X, Y \subseteq S$, $X \times_S Y \to X$; $X \times_S Y = X \cap Y$ (pts must lie in X & in Y)

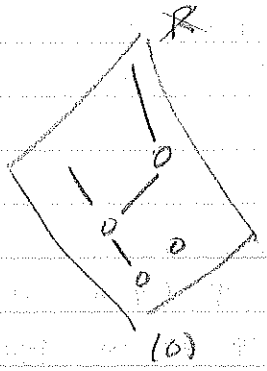
$$\begin{array}{ccc} X \times_S Y & \longrightarrow & X \\ \downarrow & & \downarrow \\ Y & \hookrightarrow & S \end{array}$$

- If $I, J \subseteq R$ ideals (in AffSch) $R/I \otimes_R R/J =$

$$\begin{array}{ccc} R/(I+J) & \leftarrow & R/I \\ \uparrow & & \uparrow \\ R/J & \leftarrow & R \end{array} \xrightarrow{\operatorname{Spec}} \begin{array}{ccc} V(I) \cap V(J) & & \\ = & & \\ V(I+J) & \hookrightarrow & V(J) \\ \downarrow & & \downarrow \\ V(J) & \hookrightarrow & S \end{array}$$

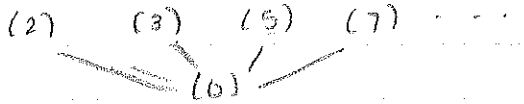
Rings & Modules of Fractions

R a ring. Draw all prime ideals

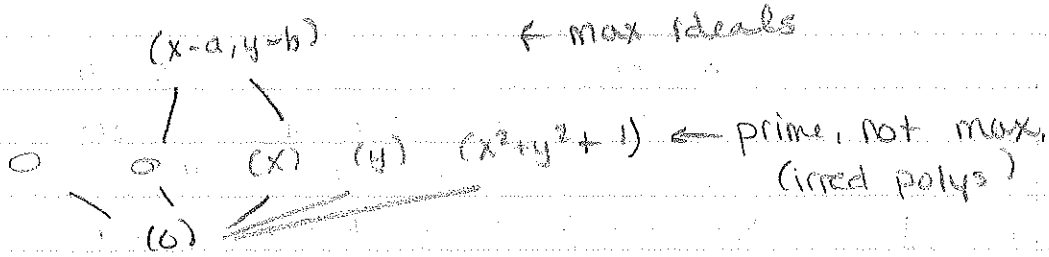


ie, draw the lattice based on inclusion.

Spec $\mathbb{R}$:



Spec $k[x,y]$



Modding out by an ideal throws out everything below it & keeps only the part of tree from that ideal.
What if want to kill everything not below it?
- Note, the ideal becomes maximal, & the only one b/c rest of that level thrown out ⇒ ring local.

Spec $\mathbb{Z}$: will construct a field, b/c (0) will be max, & only field to assoc. to $\mathbb{Z}$ is $\mathbb{Q}$.

Def: A a ring. $S \subseteq R$ is called a multiplicative system if:

(1) $1 \in S$

(2) $a, b \in S \Rightarrow a \cdot b \in S$.

(not nec. cl. under $+$)

Ex: In $\mathbb{Z}$, a mult. sys. is all $\neq 0$ #'s.

First try at inverting all elts in S:

Take the set of pairs $\{(a,s) \mid a \in A, s \in S\}$

- but $1/2 = 2/4$, so can't take all pairs (a,s)...

Need:

$(a,s) \sim (b,t) \Leftrightarrow at = bs$. Doesn't work b/c not trans.

Ck: obviously sym & refl; transitive...

Trans: Say $(a,s) \sim (b,t)$ & $(b,t) \sim (c,u)$

Then $at = bs$ & $bu = ct$. Want $au = cs$

$\Downarrow$ $\Downarrow$

$atu = bsu$ & $bsu = cst \Rightarrow t(au - cs) = 0$

If t not a zero-div, ok, but t could be zero-div.

Instead: $(a,s) \sim (b,t) \Leftrightarrow (at - bs) \cdot u = 0$ for some $u \in S$.

then, trans. ok. If S has no 0-div, then equiv. to original def.

Then $S^{-1}A/\sim$

Introduce $+, \cdot$ on $S^{-1}A$ by $\frac{a}{s} + \frac{b}{t} = \frac{at+bs}{st}$ & $\frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st}$

(we write $\frac{a}{s} = \overline{(a,s)}$)

Ex: Check this is well-def., makes $S^{-1}A$ into a ring.

Universal Property of $S^{-1}A$:

(1) $\exists$ canonical ring map $f: A \to S^{-1}A$
$a \mapsto a/1$ (why needed $1 \in$ mult sys)

(2) $\forall s \in S$, $f(s)$ is a unit in $S^{-1}A$.
b/c $f(s) = s/1$ & $s/1 \cdot 1/s = s/s = 1/1 = 1_{S^{-1}A}$
(need $s \in S$ b/c need to write it in denom)

(3) This is universal:

Prop: Let A be a comm. ring, $S \subseteq A$ a mult. sys, $f: A \to S^{-1}A$ the canonical map. Then given any comm. ring B & any ring map $g: A \to B$ s.t. $g(s)$ is a unit $\forall s \in S$, then $\exists!$ ring map $S^{-1}A \to B$ s.t. the diagram commutes:

$$\begin{array}{ccc} A & \xrightarrow{f} & S^{-1}A \\ {\scriptstyle g}\downarrow & \swarrow_{\exists! \, h} & \\ B & & \end{array}$$

ie, $S^{-1}A$ is the best ring in which have inverted all elts of S & have a map from A.

Pf: Define $h(a/s) = g(a)\,g(s)^{-1}$.
NTS: h well-def, ring map, & !.
!: $h(a/s) = h(a/1 \cdot 1/s) = h(a/1)\,h(1/s) = h(f(a)) \cdot h(f(s)^{-1})$
$= g(a)\,g(s)^{-1}$ (b/c ring map takes inv. to inv of image).
So this is the only choice for h.

Ex: (1) $\mathfrak{p} \subseteq A$ prime, $S = A \setminus \mathfrak{p}$ is a multiplicative sys. $1 \notin \mathfrak{p}$, & if $rs \notin \mathfrak{p}$, $r \in \mathfrak{p}$ & $s \notin \mathfrak{p}$.
We define $A_{\mathfrak{p}} = S^{-1}A$. we call it the <u>localization of A at $\mathfrak{p}$</u>.
Note: $A_{\mathfrak{p}}$ is a local ring & $\mathfrak{p}A_{\mathfrak{p}}$ is its ! max. ideal.
if $\mathfrak{q} \not\subseteq \mathfrak{p}$, contains $s \in S \Rightarrow$ becomes a unit $\Rightarrow$
$\mathfrak{q} = A_{\mathfrak{p}}$.

3/1 Examples of rings of fractions:

① $\mathfrak{p} \subseteq A$ prime, $S = A \setminus \mathfrak{p}$, then $S^{-1}A =: A_{\mathfrak{p}}$.

$\mathfrak{p}A_{\mathfrak{p}} = \mathfrak{p}^e$ (extension of $\mathfrak{p}$) $A \to A_{\mathfrak{p}}$, $\mathfrak{p} \dashrightarrow \mathfrak{p}^e$ a max ideal.

$\mathfrak{p}^e$ is the only max ideal in $A_{\mathfrak{p}}$.

Caveat:

② $f \in A$, $S = \{1, f, f^2, \dots\}$, then $S^{-1}A = A_f$ (not a localization)
(If a prime ideal is principal, & $\mathfrak{p} = (f)$, then it could be a localization - careful of notation)

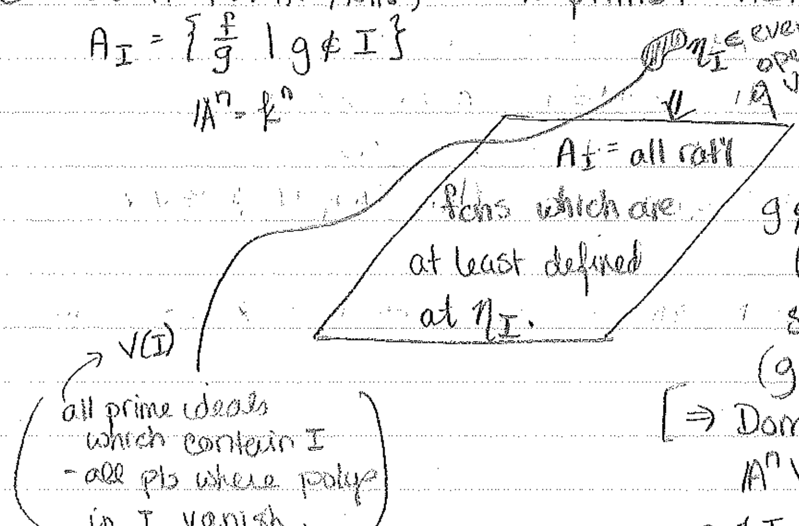
$\mathfrak{p} = (2) \subseteq \mathbb{Z}$ — $A_{\mathfrak{p}}$ = fracs where denom is even. (? Check?)

$2 \in \mathbb{Z}$ — A_2 = fracs where denom is power of 2

③ $S^{-1}A = 0 \Leftrightarrow 0 \in S$
need $\frac{1}{1} = \frac{0}{1} \Leftrightarrow (1\cdot 1 - 1 \cdot 0)s = 0$ for some $s \in S \Leftrightarrow s = 0 \in S$.

Caveat: In general, the map $A \to S^{-1}A$ may not be injective. (true when A is an integral domain)

④ Let $A = k[x_1, \dots, x_n]$, $I \subseteq A$ prime. Then
$A_I = \{ \frac{f}{g} \mid g \notin I \}$



$\frac{f}{g}$ gives a rat'l fcn on k^n, defined on some open subset.
$g \notin I \Rightarrow \frac{f}{g}$ defined along at least a non-empty open subset of $V(I)$.
$(g \notin I \Rightarrow V(I) \not\subseteq V(g))$
[$\Rightarrow$ Domain of def. of f/g is $\mathbb{A}^n \setminus V(g) =: U$ open.
$g \notin I \Rightarrow U \cap V(I) \neq \emptyset$.]
(actually defined on most of $V(I)$ b/c open sets dense)

• Geometric Interpretation of Localization:

If $\mathfrak{p} \subseteq k[x_1, \ldots, x_n]$ is max'l, ie $(x_1 - a_1, \ldots, x_n - a_n)$ (k alg. cl)

$\frac{f}{g} \in A_{\mathfrak{p}}$ Being $A_{\mathfrak{p}}$ means as a rat'l fcn on $\mathbb{A}^n$ which is defined at $(a_1, \ldots, a_n)$.

→ ie ratl fcns which are defined around my pt.

→ will allow singularities at pts far away.

$\mathfrak{p}$ ◦ look only at germ of space around $\mathfrak{p}$

→ will retain information that's recovered near $\mathfrak{p}$

(keep in mind ex. of deriv - only need to know values of fcn in some open set around the pt you're interested in

⇒ local information → any one will do)

ie, can get info about $f \in A$ near $\mathfrak{p}$ from its image in $A_{\mathfrak{p}}$.

Analogue in Real Analysis:

Let $X = \mathbb{R}^n$, $x = (x_1, \ldots, x_n) \in \mathbb{R}^n$. The ring of germs of fcns ($\mathcal{C}^\infty$, cts, etc) at x is defined as

$$\mathcal{C}^\infty_x = \{(U, f) \mid U \subseteq \mathbb{R}^n \text{ open}, x \in U \text{ (nbhd of } x), f \in \mathcal{C}^\infty \text{ defined on } U\} / \sim$$

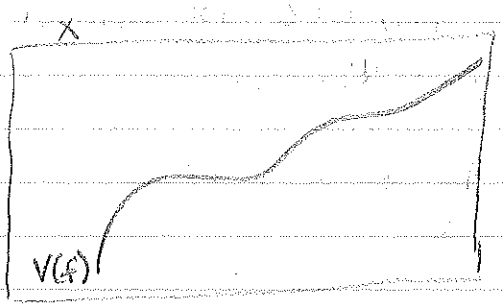
$(U, f) \sim (V, g) \Leftrightarrow \exists$ open W, $W \subseteq U$, $W \subseteq V$ s.t. $f|_W = g|_W$.

($x \in W$)

(If $f = g$ in some small nbhd of x, in same germ)

• Passing to $A_f = \left\{ \frac{g}{f^n} \mid g \in k[x_1, \dots, x_n] \right\}$
fcns defined on $X_f = \mathbb{A}^n \setminus V(f)$ (ie, have to avoid 0's of f)

$X_f = \operatorname{Spec} A_f$.



A_f = defined everywhere but $V(f)$ (the open set = $V(f)^c$)
$A_{\mathfrak{p}}$ = defined almost everywhere on $V(f)$

Modules of Fractions

Say A a ring, M an A-mod, $S \subseteq A$ a multiplicative set,
Define $S^{-1}M = \left\{ \frac{m}{s} \mid m \in M, s \in S \right\} / \sim$

↑ same as for rings of fracs
$\frac{m}{s} \sim \frac{m'}{s'} \iff (s'm - sm')\, s'' = 0$
for some $s'' \in S$

(note: don't mult. elts of M, so doesn't make sense to invert elts of M)

Note: $S^{-1}M$ is a module over $S^{-1}A$.

If $f : M \to M'$ is a map of modules, get a map $S^{-1}f : S^{-1}M \to S^{-1}M'$ of $S^{-1}A$-mods.

$$\frac{m}{s} \longmapsto \frac{f(m)}{s}$$

$\Rightarrow$ S^{-1} is a functor from A-Mod to $S^{-1}A$-mod

Prop (1) S^{-1} is an exact functor
(2) $S^{-1}M \simeq M \otimes_A S^{-1}A$
(3) $S^{-1}A$ is a flat A-mod.

Pf: (1) Let $M' \xrightarrow{f} M \xrightarrow{g} M''$ be exact, ie $\ker g = \operatorname{im} f$.

Look at

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

What is $\ker(S^{-1}g)$?

$\ker(S^{-1}g) = \left\{ \frac{m}{s} \mid \frac{g(m)}{s} = 0 \text{ in } S^{-1}M'' \right\}$. Let $m/s \in \ker(S^{-1}g)$

$\frac{g(m)}{s} = \frac{0}{1} \Leftrightarrow g(m)\cdot t = 0$ for some $t \in S$

$\Downarrow$

$g(tm) = 0 \Rightarrow tm \in \ker g = \operatorname{im} f$

$\Rightarrow tm = f(m')$ for some $m' \in M'$

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

$\Rightarrow m/s \in \operatorname{im}(S^{-1}f) \Rightarrow \ker(S^{-1}g) \subseteq \operatorname{im}(S^{-1}f)$

"$\supseteq$": NTS composite map $= 0$

$S^{-1}g \circ S^{-1}f = S^{-1}(g \circ f) = 0$ since $g \circ f = 0$.

(2) Define a map

$$M \otimes_A S^{-1}A \longrightarrow S^{-1}M \qquad m \otimes \frac{f}{s} \longmapsto \frac{fm}{s}$$

Ck: well-def $((m, \frac{f}{s}) \to \frac{fm}{s}$ is A-bilinear)

doesn't depend on which rep you pick

Ex: Prove its an isomorphism:

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

$$\frac{m}{s} \longmapsto m \otimes_A \frac{1}{s}$$

(3) Automatic.

Ex: If A an int. dom., $A^m \to A^n$ an injective map $\Rightarrow m \leq n$

Pf: $(0) \subseteq A$ prime ($\Leftrightarrow A$ int dom), $S = A \setminus \{0\}$

$\Rightarrow K = A_{(0)}$ a field (b/c (0) max. ideal)

exactness of localization (S^{-1})

$\Rightarrow K^m \to K^n$ is injective $\Rightarrow m \leq n$ by v. sp. theory

3/4 Tensor products commute w/ S^{-1}:

Prop: If M, N are A-mods & $S \subseteq A$ a mult. sup, then

$$S^{-1}(M \otimes_A N) \simeq S^{-1}M \underset{S^{-1}A}{\otimes} S^{-1}N$$

(modules of $S^{-1}A$)

In particular, $(M \otimes_A N)_{\mathfrak{p}} \simeq M_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} N_{\mathfrak{p}}$.

Pf: "$\longrightarrow$" $\frac{m \otimes n}{s} \longmapsto \frac{m}{s} \otimes \frac{n}{1}$ (map extends by linearity to all tensors)

Define a map $M \times N \longrightarrow S^{-1}M \underset{S^{-1}A}{\otimes} S^{-1}N$

$$(m,n) \longmapsto \frac{m}{1} \otimes \frac{n}{1}$$

This is an A-bilinear map $\Rightarrow$ (Univ. Prop. of $\otimes$) $\Rightarrow$! map $M \underset{A}{\otimes} N \longrightarrow S^{-1}M \underset{S^{-1}A}{\otimes} S^{-1}N$ ... (every elt in $M \otimes N$ maps to an elt which can be divided by any elt of S)

$\Rightarrow$ this map extends to a ! map $S^{-1}(M \otimes_A N) \to S^{-1}M \underset{S^{-1}A}{\otimes} S^{-1}N$

"$\longleftarrow$" $\frac{m}{s} \otimes \frac{n}{s'} \longrightarrow \frac{m \otimes n}{s \cdot s'}$ well-def & an inverse. □

Local Properties

Prop: TFAE:

(1) $M = 0$

(2) $M_{\mathfrak{p}} = 0$ $\forall \mathfrak{p}$ prime

(3) $M_{\mathfrak{m}} = 0$ $\forall \mathfrak{m}$ max.

Pf: (1) $\Rightarrow$ (2) $\Rightarrow$ (3): Obvious.

(3) $\Rightarrow$ (1): Assume by contradiction that $M \neq 0$

Pick $x \in M$, $x \neq 0$. $\frac{x}{1} = 0$ in $M_{\mathfrak{m}} \Leftrightarrow \exists \underbrace{s \in A, s \notin \mathfrak{m}}_{s \in S}$ s.t. $s \cdot x = 0$

Look at $\mathrm{Ann}(x) = \{a \in A \mid ax = 0\}$, an ideal in A, $\mathrm{Ann}(x) \subsetneq A$ (b/c $1 \notin \mathrm{Ann}(x)$). So let $\mathfrak{m} \supseteq \mathrm{Ann}(x)$ be a max'l ideal.

$\Rightarrow$ Then $\frac{x}{1} \neq 0$ in $M_{\mathfrak{m}}$ ↯ □

Prop: If $f: M \to N$ is a map of modules, Ker & Coker are computed locally: $(f_{\mathfrak{p}}: M_{\mathfrak{p}} \to N_{\mathfrak{p}})$

$(\ker f)_{\mathfrak{p}} \cong \ker(f_{\mathfrak{p}})$ (similarly for coker)

Pf: $0 \to \ker f \to M \xrightarrow{f} N \to \operatorname{coker} f \to 0$ is exact

Localization is exact; so we get an exact seq

$$0 \to (\ker f)_{\mathfrak{p}} \to M_{\mathfrak{p}} \xrightarrow{f_{\mathfrak{p}}} N_{\mathfrak{p}} \to (\operatorname{coker} f)_{\mathfrak{p}} \to 0$$

exactness tells us that $(\ker f)_{\mathfrak{p}} \cong \ker(f_{\mathfrak{p}})$ & for coker. □

Prop: Injectivity of a map is a local property, ie TFAE:

(1) $f: M \to N$ injective

(2) $f_{\mathfrak{p}}: M_{\mathfrak{p}} \to N_{\mathfrak{p}}$ injective $\forall \mathfrak{p}$ prime

(3) $f_{\mathfrak{m}}: M_{\mathfrak{m}} \to N_{\mathfrak{m}}$ injective $\forall \mathfrak{m}$ maxl

Pf: (1) $\Leftrightarrow (\ker f) = 0 \Leftrightarrow (\ker f)_{\mathfrak{p}} = 0 \ \forall \mathfrak{p}$ (by prev. prop)

$\Leftrightarrow f_{\mathfrak{p}}$ inj. (or replace $\mathfrak{p}$ by $\mathfrak{m}$)

* Same for surjectivity. (w/ coker)

* "Isomorphic" is not a local prop.

Ex: Flatness is a local property.

Prop: Let M be an A-mod. TFAE:

(1) M is flat as an A-mod

(2) $M_{\mathfrak{p}}$ is flat as an $A_{\mathfrak{p}}$-mod $\forall \mathfrak{p}$ prime

(3) $M_{\mathfrak{m}}$ is flat as an $A_{\mathfrak{m}}$-mod $\forall \mathfrak{m}$ maxl.

Pf: (1) $\Rightarrow$ (2) $\Rightarrow$ (3): If M flat over A, so is $M \otimes_A A_{\mathfrak{p}}$ b/c $A_{\mathfrak{p}}$ always flat.

(3) $\Rightarrow$ (1) Assume M is not flat. $\Rightarrow \exists$ injective map $N \to N'$ s.t. $M \otimes N \to M \otimes N'$ is not injective. So we have the exact seq.

$0 \to N \to N'$ but $0 \to K \to M \otimes N \to M \otimes N'$ (*)

$K \neq 0$ ← Kernel.

$K \neq 0 \Rightarrow \exists\ \underline{m}$ maxl s.t. $K_{\underline{m}} \neq 0$. Look at (*) & localize at $\underline{m}$:

$$0 \to K_{\underline{m}} \to (M \otimes N)_{\underline{m}} \longrightarrow (M \otimes N')_{\underline{m}}$$

$\neq 0$

ie $0 \to \underset{\neq 0}{K_{\underline{m}}} \to M_{\underline{m}} \otimes N_{\underline{m}} \longrightarrow M_{\underline{m}} \otimes N'_{\underline{m}}$

but $0 \to N_{\underline{m}} \to N'_{\underline{m}}$ is exact & $M_{\underline{m}}$ flat

$\Rightarrow K_{\underline{m}} = 0$ ↯. □

3/16 **Prop:** (i) Every ideal in $S^{-1}A$ is an extended ideal

ie, for every $\underline{a} \subseteq S^{-1}A$ an ideal, $\exists\ \underline{b} \subseteq A$ an ideal s.t. $\underline{b}^e = \underline{a}$.

(ii) $\underline{a} \subseteq A$, $\underline{a}^{ec} = \bigcup_{s \in S} (\underline{a} : s)$

Cor: $\underline{a}^e = (1) \Leftrightarrow \underline{a} \cap S \neq \emptyset$

(iii) Prime ideals in $S^{-1}A$ are in 1-1 corresp. w/ $\underline{p} \subseteq A$ prime s.t. $\underline{p} \cap S = \emptyset$.

Pf: (i) Let $\underline{a} \subseteq S^{-1}A$ an ideal. Look at $\underline{a}^{ce}$. WTS $\underline{a}^{ce} = \underline{a}$. One inclusion always holds: $\underline{a}^{ce} \subseteq \underline{a}$.

> **Pf:** $f : B \to A$, $\underline{a} \subseteq A$,
> $f(\underline{a}^c) = f f^{-1}(\underline{a}) = \underline{a} \cap f(B) \subseteq \underline{a}$
> So $\underline{a}^{ce} = \langle f(\underline{a}^c) \rangle \subseteq \underline{a}$. □

For $\underline{a} \subseteq \underline{a}^{ce}$: Let $\frac{x}{s} \in \underline{a}$. $\Rightarrow \frac{x}{1} \in \underline{a}$ (mult. by s) $\Rightarrow x \in \underline{a}^c$ (b/c $f(x) = \frac{x}{1} \in \underline{a}$) $\Rightarrow \frac{x}{1} \in \underline{a}^{ce}$. Since s invert, $\frac{1}{s} \cdot \frac{x}{1} \in \underline{a}^{ce}$ □

Ex: $\mathbb{Z} \hookrightarrow \mathbb{Q}$ (i)

$(0)^{ce} = (0)$

$\mathbb{Q}^{ce} = \langle 1 \rangle = (1)$

(ii)

$(0)^{ec} = (0)$

$(m)^e = (1) \Rightarrow (m)^{ec} = \mathbb{Z}$ (b/c m invert.)

(ii) Let $\underline{a} \subseteq A$ be an ideal, $x \in \underline{a}^{ec} \Leftrightarrow \frac{x}{1} \in \underline{a}^e = S^{-1}\underline{a}$

[b/c $0 \to \underline{a} \to A$ $\quad S^{-1}: 0 \to S^{-1}\underline{a} \to S^{-1}A$]

$S^{-1}\underline{a} = \{\frac{a}{s} \mid a \in \underline{a}, s \in S\} \Leftrightarrow \frac{x}{1} = \frac{a}{s}$ for some $a \in \underline{a}$, $s \in S$

$\Leftrightarrow \exists\ t \in S$ s.t. $(xs - a)t = 0$

$\Leftrightarrow$ $xst \in \underline{a}$ for some $s,t \in S$

$\Leftrightarrow$ $x \in (\underline{a} : s')$ for some $s' \in S$

$= \{r \in A \mid rs' \in \underline{a}\}$

(iii) $\mathfrak{q} \longmapsto \mathfrak{q}^c$. If $\mathfrak{q} \subseteq S^{-1}A$, then $\mathfrak{q}^c$ is prime in A

$\in S^{-1}A$ prime $\subseteq A$ prime $\quad$ & $\mathfrak{q}^c \cap S = \emptyset$ b/c if $s \in \mathfrak{q}^c \cap S$

$\Rightarrow \frac{s}{1} \in \mathfrak{q} \overset{\cdot 1/s}{\Rightarrow} 1 \in \mathfrak{q}$ ↯

Let $\mathfrak{p} \subseteq A$ prime be s.t. $\mathfrak{p} \cap S = \emptyset$. Define $\mathfrak{q} = \mathfrak{p}^e$.

Look at $A/\mathfrak{p}$, an int. dom. Let $\bar{S}$ = Image of S under $A \to A/\mathfrak{p}$. ($\bar{S}$ is mult. sys. in $A/\mathfrak{p}$)

$\bar{S}^{-1}(A/\mathfrak{p}) \cong S^{-1}A/S^{-1}\mathfrak{p}$ b/c:

$0 \to \mathfrak{p} \to A \to A/\mathfrak{p} \to 0$, apply S^{-1}:

$0 \to S^{-1}\mathfrak{p} \to S^{-1}A \to S^{-1}(A/\mathfrak{p}) \to 0$ is exact

$\Rightarrow S^{-1}(A/\mathfrak{p}) \cong S^{-1}A/S^{-1}\mathfrak{p}$ & S^{-1} acts on $A/\mathfrak{p}$ by proj.

$\bar{S}^{-1}(A/\mathfrak{p})$ is either the 0 ring or $\subseteq (A/\mathfrak{p})_{(0)}$ then mult. so $S^{-1}(A/\mathfrak{p}) = \bar{S}^{-1}(A/\mathfrak{p})$

↑ field of fracs → invert everything & $\bar{S}$ only inverted some

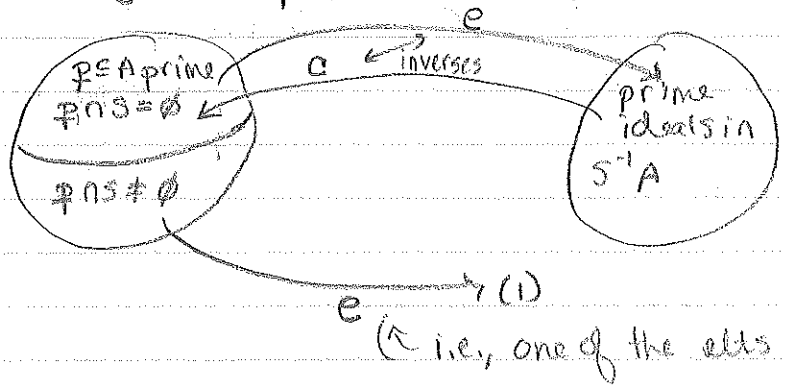
~~$S^{-1}A$~~

So, $S^{-1}\mathfrak{p}$ is either 0 or int. dom. (b/c $\subseteq$ field)

$\Rightarrow S^{-1}\mathfrak{p} = \mathfrak{p}^e = \mathfrak{q}$ is either (1) or a prime ideal.

$\Rightarrow \mathfrak{q}$ is either (1) or prime.

By (ii) $\mathfrak{q} = \mathfrak{p}^e = (1)$ iff $\mathfrak{p} \cap S \neq \emptyset$ ↯ $\Rightarrow \mathfrak{q}$ prime.



(↑ i.e., one of the elts became invertible)

Thm: Let $f \in A$, f not nilp. Then $\exists \mathfrak{p} \subseteq A$ prime s.t. $f \notin \mathfrak{p}$.

Pf: Take $S = \{1, f, f^2, \ldots\}$. f not nilp $\Rightarrow 0 \notin S$.
$\Leftrightarrow S^{-1}A \neq 0 \Leftrightarrow \exists \underline{m}$ max'l in $S^{-1}A$. Look at $\underline{m}^c$.
$\underline{m}^c$ is prime in A & $\underline{m}^c \cap S = \emptyset \Rightarrow f \notin \underline{m}^c$, so $\underline{m}^c$ the desired prime.
(different proof in this in pf of nilrad $= \cap \mathfrak{p}$)

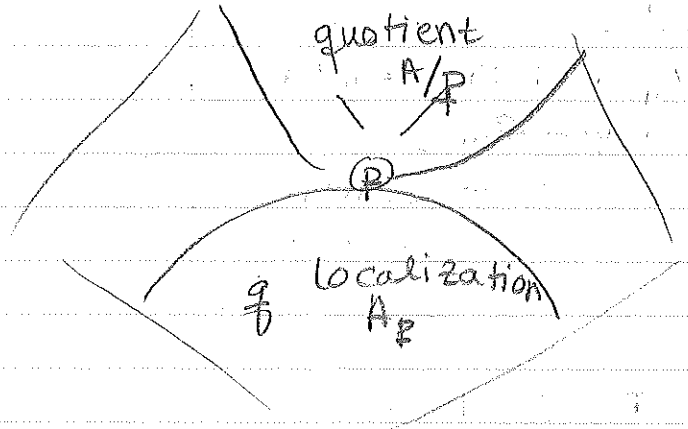
Cor: $\mathcal{N}_{S^{-1}A} = S^{-1}\mathcal{N}_A$

$$\cap \mathfrak{p} = (\underbrace{\cap \mathfrak{p}^c}_{\text{subset of } \mathfrak{p} \subseteq A, \text{ only those that } \cap S = \emptyset,})^e$$
but if $\cap S \neq \emptyset$, $(\ )^e = (1)$, so don't contribute to intersection

Cor: $\{\text{primes in } A_{\mathfrak{p}}\} \xleftrightarrow{1\text{-}1} \{\text{primes } \mathfrak{q} \subseteq A \text{ s.t. } \mathfrak{q} \subseteq \mathfrak{p}\}$

b/c $S = A \setminus \mathfrak{p}$, so $\mathfrak{q} \cap S = \emptyset \Leftrightarrow \mathfrak{q} \subseteq \mathfrak{p}$.

. Lattice



- In quotient, all primes containing $\mathfrak{p}$ survive.
- In localization, all primes contained in $\mathfrak{p}$ survive

3/8 **Def**: Let $A \subseteq B$ be rings, $x \in B$ is said to be <u>integral over</u> A if there exists $a_1, \dots, a_n \in A$ s.t.
$x^n + a_1 x^{n-1} + \cdots + a_n = 0$.

· <u>Integral closure</u> - add all elts that are int. over A

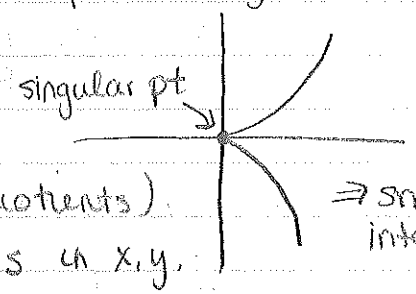
Ex: ① $\mathbb{Z} \subseteq \mathbb{Q}$. Assume $\frac{m}{n} \in \mathbb{Q}$ is integral over $\mathbb{Z}$.
wlog, $(m,n) = 1$. $\frac{m}{n}$ int. over $\mathbb{Z} \Rightarrow \exists\, a_1, \dots, a_t \in \mathbb{Z}$
s.t. $\frac{m^t}{n^t} + a_1 \frac{m^{t-1}}{n^{t-1}} + \cdots + a_t = 0$. Clear denoms:
$m^t + a_1 m^{t-1} n + \cdots + a_t n^t = 0$
$\Rightarrow n \mid m^t$ (b/c $m^t = (-a_1 m^{t-1} + \cdots + a_t n^{t-1})\, n$)
$\Rightarrow n = \pm 1$ b/c $\gcd(m,n) = 1$
$\Rightarrow \frac{m}{n} \in \mathbb{Z}$.

Obs: Always $a \in A$ is integral over A (A satisfies $x - a = 0$)
We say a ring A is <u>integrally closed in B</u> if:
$A = \{x \in B \mid x \text{ int. } /A\}$
We say A is <u>integrally closed</u> if it's int. cl. in its field of fractions.
· Thus $\mathbb{Z}$ is integrally closed

② $A = k[x,y]/(y^2 - x^3)$
an integral domain
Is A int. cl.? (in its field of fracs)
(localization commutes w/ quotients)
· FqF of $k[x,y]$ = rat'l fcns in x, y.
Look at $f = y/x$
$f^2 = y^2/x^2 = x^3/x^2 = x$
This $f \in k = \text{FofF in } A$. is int over A b/c satisfies
$z^2 - x = 0$. but $f \notin A$.
Thus A is <u>not</u> integrally closed.

In u.f.d., $\langle f(x) \rangle$ prime iff $f(x)$ irred

Spec A: $y = \pm x^{3/2}$



Irreducible.
$\Rightarrow$ smooth in the integral closure.

integral closure = normalization:

Prop: For $A \subseteq B$, $x \in B$, TFAE:

(1) x is int/A

(2) $A[x]$ = (subring of B gen by $A \cup x$) is a f.g. A-mod.

(3) $A[x] \subseteq C \subseteq B$ where C is a subring of B which is a f.g. A-mod.

(4) $\exists$ a faithful $A[x]$-mod M that is f.g. as an A-mod.

Pf: (1)$\Rightarrow$(2): $A[x]$ is gen by $\{1, x, x^2, \dots\}$ but integral dependence/A $\Rightarrow x^n \in \text{span}\{1, x, \dots, x^{n-1}\} \Rightarrow$ $A[x]$ is gen by $\{1, x, \dots, x^{n-1}\}$.

(2)$\Rightarrow$(3) Take $C = A[x]$.

(3)$\Rightarrow$(4) Take $M = C$. C clearly an $A[x]$-mod b/c $A[x] \subseteq C$. Faithful: If $y \in A[x]$ is such that $cy = 0$ $\forall c \in C$, then $1 \cdot y = 0 \Rightarrow y = 0 \Rightarrow$ faithful

(4)$\Rightarrow$(1): Take $a = A$, $\phi = \cdot x$. ϕ an automorph. of M. (Regard M as an A-mod) By prop, $\exists$ an identity $\phi^n + a_1\phi^{n-1} + \cdots + a_n = 0$ for $a_i \in A$
But $(\phi^n + \cdots + a_n)(m) = (x^n + \cdots + a_n) \cdot m = 0$ $\forall m \in M$
$\Rightarrow x^n + \cdots + a_n = 0$ b/c M faithful $\Rightarrow$ x is int/A.

□

Prop: If $x_1, \dots, x_n$ are int/A, then $A[x_1, \dots, x_n]$ f.g./A.

Pf: by induction on n. □ (in book)

Cor: $C = \{x \in B \mid x \text{ int/} A\}$ is a subring of B.

Pf: $x, y \in C \Rightarrow A[x,y]$ f.g/A $\Rightarrow A[x+y]$ and $A[x \cdot y]$ f.g./A
$\Rightarrow x+y, x \cdot y$ int/A.

Def: If $A \subseteq B$, $C = \{x \in B \mid x \text{ int/} A\}$. We say

(1) if $C = A$, A is <u>integrally closed</u>.

(2) if $C = B$, B is <u>integral over A</u>.

Prop: $A \subseteq B \subseteq C$, B int/A, C int/B $\Rightarrow$ C int/A.

Pf: Let $x \in C$. WTS x int./A. Because C int/B, $\exists$ an eqn $x^n + b_1 x^{n-1} + \cdots + b_n = 0$ w/ $b_i \in B$. Look at $B' = A[b_1, \ldots, b_n] \subseteq B$. B' is a f.g. A-mod (by prop.) & x is int./$B' \Rightarrow B'[x]$ is a f.g. B'-mod $\Rightarrow$ f.g. A-mod (which is obviously faithful over $A[x]$) & is a subring of C containing A. $\Rightarrow x$ int. over A (Lemma part (3)).

Prop: If $A \subseteq B$, C is the integral closure of A in B, Then C is integrally closed in B. (ie. $\overline{A} = \overline{A}$)

Pf: Let $b \in B$ be integral over C. $\overset{\text{by prev. prop.}}{\Rightarrow}$ b int. over A $\Rightarrow b \in C$

Prop: If $A \subseteq B$, B int. over A

(1) If $\underline{b} \subseteq B$ an ideal, $\underline{a} = \underline{b} \cap A$, then $B/\underline{b}$ is integral over $A/\underline{a}$.

(2) If S is multiplicatively closed in A. Then $S^{-1}B$ is int. over $S^{-1}A$.

Pf (1) Let $\bar{x} \in B/\underline{b}$. Then x is int/$A \Rightarrow \exists\, a_1, \ldots, a_n$ s.t. $x^n + a_1 x^{n-1} + \cdots + a_n = 0$ in B. $\Rightarrow \bar{x}^n + \bar{a}_1 \bar{x}^{n-1} + \cdots + \bar{a}_n = 0$ in $B/\underline{b}$, (w/ $\bar{a}_i \in A/\underline{a}$).

(2) Let $\frac{x}{s} \in S^{-1}B$. x int over $A \Rightarrow \exists\, a_1, \ldots, a_n$ s.t. $x^m + a_1 x^{n-1} + \cdots + a_n = 0$ $(\div s^n)$

$\Rightarrow \left(\frac{x}{s}\right)^n + \frac{a_1}{s}\left(\frac{x}{s}\right)^{n-1} + \cdots + \frac{a_n}{s^n} = 0$, $\frac{a_i}{s^i} \in S^{-1}A \Rightarrow$ x/s int. over $S^{-1}A$. □

3/11 f surj $\Rightarrow$ f^* inj. ; f inj $\Rightarrow$ f^* dominant, image is dense in Spec(A). (not nec. surj.)

today: $f: A \to$ field of fracs
& f^* is not just dom., but surj.

Going Up

Prop: Let $A \subseteq B$ be an int doms, B integral /A. Then A is a field iff B is a field.

Pf: ($\Rightarrow$): Assume A is a field, $y \in B$, $y \neq 0$. B/c y is integral over A, $\exists\ y^n + a_1 y^{n-1} + \cdots + a_n = 0$, $a_i \in A$. Pick it of minimal degree. $\Rightarrow a_n \neq 0$ (else $y(y^{n-1} + \cdots + a_{n-1}) = 0$ & no zero div $\Rightarrow y^{n-1} + \cdots + a_{n-1} = 0$ ↯). $\Rightarrow a_n^{-1} \in A$ b/c A field. $-a_n = y(y^{n-1} + \cdots) + a_{n-1})$. Mult by $\frac{1}{-a_n}$:

$1 = y\underbrace{(y^{n-1} + \cdots + a_{n-1}) \cdot \frac{1}{-a_n}}_{\in B} \Rightarrow y$ a unit. ✓

($\Leftarrow$): Assume B a field, $x \in A$, $x \neq 0$. Then $x^{-1} \in B \Rightarrow x^{-1}$ integral /A $\Rightarrow x^{-n} + a_1 x^{-n+1} + \cdots + a_n = 0$

$x^{-n} = -a_1 x^{-n+1} - \cdots - a_n$. Mult by x^{n-1}

$x^{-1} = \underbrace{-a_1 - \cdots - a_1 x^{n-1}}_{\in A} \Rightarrow x^{-1} \in A$ ✓

□

Cor: Let $A \subseteq B$ be rings, B int /A, $\mathfrak{q} \subseteq B$ prime, $\mathfrak{p} = \mathfrak{q}^c = \mathfrak{q} \cap A$ prime in A. Then $\mathfrak{q}$ is maximal iff $\mathfrak{p}$ is maximal.
(ie, closed pts go to closed pts under integral maps)

Pf: Look at $B/\mathfrak{q} \supseteq A/\mathfrak{p}$ ($A \to B \to B/\mathfrak{q}$, $\underbrace{\ker = \mathfrak{p}}$ $\Rightarrow A/\mathfrak{p} \to B/\mathfrak{q}$ inj.

By what we did last time, $B/\mathfrak{q}$ is int. over $A/\mathfrak{p}$ & both are int. domains. Apply prop.

$\mathfrak{q}$ max $\Leftrightarrow$ $B/\mathfrak{q}$ field $\Leftrightarrow$ $A/\mathfrak{p}$ field $\Leftrightarrow$ $\mathfrak{p}$ max. □

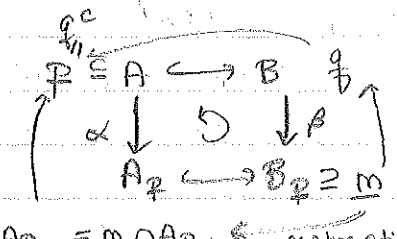
Cor: $A \subseteq B$ rings, B int $/A$, $\mathfrak{q} \subseteq \mathfrak{q}'$ prime in B s.t. $\mathfrak{q}^c = \mathfrak{q}'^c$. Then $\mathfrak{q} = \mathfrak{q}'$.
(ie, if containment of contraction is strict, then containment of ideals is strict).

Pf: Let $\mathfrak{p} = \mathfrak{q}^c = \mathfrak{q}'^c \subseteq A$ prime. Look at $S = A \setminus \mathfrak{p} \subseteq A$
$S^{-1}A = A_{\mathfrak{p}}$, $S^{-1}B = B_{\mathfrak{p}}$ (although $\mathfrak{p}$ not nec. prime ideal of B)
↑ book's notation.

We have $B_{\mathfrak{p}}$ int. over $A_{\mathfrak{p}}$. Let $\underline{m}$ = extension of $\mathfrak{p} \subseteq A$ to $A_{\mathfrak{p}}$ ($\underline{m} = \mathfrak{p}A_{\mathfrak{p}}$) = unique max. ideal of $A_{\mathfrak{p}}$.
Let $\underline{n}, \underline{n}'$ be extensions of $\mathfrak{q}, \mathfrak{q}'$ to $B_{\mathfrak{p}}$.
So $\underline{n} \subseteq \underline{n}'$. But $\mathfrak{q} \cap A = \mathfrak{p} \Rightarrow \underline{n} \cap A_{\mathfrak{p}} = \underline{m} = \underline{n}' \cap A_{\mathfrak{p}}$
$\Rightarrow$ (by cor) $\underline{n}, \underline{n}'$ max'l (b/c their restrictions are max)
But $\underline{n} \subseteq \underline{n}' \Rightarrow \underline{n} = \underline{n}'$. (So $\mathfrak{q}, \mathfrak{q}'$ did not meet mult sup, so they survived localization, so there's a 1-1 corresp.). By thm on primes in rings of fracs, $\mathfrak{q} = \mathfrak{q}'$. □

Thm: Let $A \subseteq B$ be rings, B int $/A$, $\mathfrak{p} \subseteq A$ prime. Then $\exists\, \mathfrak{q} \subseteq B$ prime s.t. $\mathfrak{q}^c = \mathfrak{p}$.
(ie f^* is surj).
* Not generally true: $\mathbb{Z} \hookrightarrow \mathbb{Q}$, f^* not surj. *

Pf: $B_{\mathfrak{p}}$ still int. $/A_{\mathfrak{p}}$, & have diagram of rings



· Pick $\underline{m} \subseteq B_{\mathfrak{p}}$ max.

$\mathfrak{p}A_{\mathfrak{p}} = \underline{m} \cap A_{\mathfrak{p}}$ ← contraction

prime & max'l $\Rightarrow \underline{m} \cap A_{\mathfrak{p}} = \mathfrak{p}A_{\mathfrak{p}}$

So $\alpha^{-1}(\mathfrak{p}A_{\mathfrak{p}}) = \mathfrak{p} \Rightarrow$ if we let $\mathfrak{q} = \beta^{-1}(\underline{m})$, we have $\mathfrak{q}^c = \mathfrak{p}$. □

Read Going Up Thm & proof. Read Going Down Thm (skip proof)

Valuations

Def: Let B be an int. dom, k = field of fr. We say B is a valuation ring (of k) if $\forall x \neq 0$ in k, either $x \in B$ or $x^{-1} \in B$ or both.
(ie, the ring fills up a lot of the field).

Ex: $\mathbb{Z}$ not a valuation ring of $\mathbb{Q}$, $\mathbb{Z}_{(2)}$ is a val. ring of $\mathbb{Q}$.
(fracs whose denoms not div by 2)

Prop: (1) B is a local ring
(2) If $B \subsetneq B' \subsetneq K \Rightarrow B'$ a valuation ring
(3) B int. closed in K.

Pf: (1) Let $\underline{m} \subseteq B$ be the set of all non-units.
WTS $\underline{m}$ an ideal (in a non-local ring, this is not an ideal).
If $x \neq 0$, $x \in \underline{m}$, $a \in B$. Then ax not a unit, (b/c if ax unit, $(ax)^{-1} \in B$ contr. $x \in \underline{m}$).
$\Rightarrow ax \in \underline{m}$. If $x, y \in \underline{m}$, $x, y \neq 0$
xy^{-1} or $x^{-1}y \in B$ (b/c B val. ring)
If $xy^{-1} \in B$, $y(1 + xy^{-1}) = y + x \in \underline{m}$ ($y \in \underline{m}$, $1 + xy^{-1} \in B$)

($x \in \mathbb{Q}$, either 2 ∤ denom, $\Rightarrow x \in \mathbb{Z}_{(2)}$, or 2 ∤ denom $\Rightarrow$ 2 ∤ num $\Rightarrow x^{-1} \in \mathbb{Z}_{(2)}$.)

(2) Obvious
(3) If $x \in K$ is s.t. x is int over B. (WTS $x \in B$)
$\Rightarrow \exists\ x^n + b_1 x^{n-1} + \cdots + b_n = 0$, $b_i \in B$
if $x \in B$, done. if $x^{-1} \in B$, then
$x^n = -b_1 x^{n-1} - \cdots - b_n$. mult by x^{1-n}
$\Rightarrow x = -b_1 - b_2 x^{-1} - \cdots - b_n x^{1-n} \in B$ b/c $x^{-1} \in B$

□

Define a fcn $v_2 : \mathbb{Q} \to \mathbb{Z}$
$v_2(m/n) =$ (highest power of 2 dividing m) − (—"— dividing n)
($v_2(4/6) = 1$)
1) $v_2(xy) = v_2(x) + v_2(y)$
2) $v_2(x+y) \leq \max(v_2(x), v_2(y))$
Such fcns called a valuation

Exercise: All valuations on $\mathbb{Q}$ are like v_2 for some prime (ie v_p)

$$\mathbb{Z}_{(2)} = \{ x \in \mathbb{Q} \mid v_2(x) \geq 0 \}$$

$v_p \Rightarrow$ valuation ring as above.

3/13 Valuation Rings:

K = field, subring $B \subseteq K$ is called a valuation ring if any $x \in K - B$ satisfies $x^{-1} \in B$.

Properties: B is local & integrally closed.

Ex: K (= $\mathbb{Q}$) ① $B = \{ \frac{m}{n} \mid m \in \mathbb{Z}, p \nmid n \}$ p a fixed prime.

② $B = \mathbb{Q}$

① & ② are discrete valuation rings, val. ring that came from a map $K \setminus \{0\} \to \mathbb{Z}$ (that satisfies certain props)

[as set of elts in which map non-neg → in the map from last time]

max ideal $\underline{m} \subseteq B$, field of fracs $B/\underline{m}$ → for ①, $\underline{m} = pB$, $B/\underline{m} = \mathbb{Z}/p\mathbb{Z}$ ($\underline{m} = pB$ b/c if unit in B, need num not ÷ by p)

for ②, $\underline{m} = (0)$, field of fracs = $\mathbb{Q}$.

③

K	$B \subseteq K$	$\underline{m} \subseteq B$	$B/\underline{m}$
$\mathbb{C}(z)$	$\{ \frac{f}{g} \mid g(a) \neq 0 \}$	$\{ \frac{f}{g} \mid \substack{f(a)=0 \\ g(a)\neq 0} \}$	$\mathbb{C}$
	$\mathbb{C} \ni a$ fixed.	↑ if invert, not in B	
$\mathbb{C}(z)$	0	$\mathbb{C}(z)$	

(These are only val. rings in $\mathbb{Q}$ & $\mathbb{C}(z)$, resp.)

Fix K a field, and fix an alg. cl. field Ω. Consider pairs (A, f), $A \subseteq K$ subring, $f: A \to \Omega$.

Ex: $B \subseteq K$ (local) val. ring, $B \to B/\underline{m} \subseteq \overline{(B/\underline{m})}$ (= Ω)

These pairs are max such pairs.

$\mathbb{Q}$ ∪ $\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ → map can be extended to a val. ring B (from ①), but no further.

Order (A,f)'s : $(A_1, f_1) \geq (A_2, f_2)$ if ① $A_1 \supset A_2$ &
② $f_1|_{A_2} = f_2$.

Thm: A pair (B,g) is maximal iff B is a val. ring & and $\mathrm{Ker}(g) = \underline{m}$ (ie $g: B \to B/\underline{m} \hookrightarrow \Omega$; so g factors through $B/\underline{m}$)

Pf: $(\Leftarrow)$: Suppose g extends to $B' \supset B$. Take $x \in B' - B, \subset K - B$.
Then $x^{-1} \in B$ (b/c val. ring) & not a unit
$\Rightarrow x^{-1} \in \underline{m} \Rightarrow g(x^{-1}) = 0$, but $g(x) = (g(x^{-1}))^{-1}$ ↯.
ie $g(x^{-1}) = 0$
$\quad \quad \| $
$\quad \frac{1}{g(x)}$

$(\Rightarrow)$: $g: B \to \Omega$ is max'l.

Step 1: B is local & $\mathrm{Ker}(g)$ is the max ideal
ie $\mathrm{Ker}(g) = \underline{m}$.

Pf: g extends easily to $B_{\underline{m}} = \{ \frac{x}{y} \mid x \in B, y \in B \setminus \underline{m} \}$
So $B_m = B$, b/c B max'l. ie, $(B - \underline{m})^{-1} \subset B$
$\Rightarrow$ claim. (all elts not in $\underline{m}$ are invert).

Take $x \in K - \{0\}$

Step 2: Either $1 \notin \underline{m}[x]$ or $1 \notin m[x^{-1}]$. (ie, one of the 2 is a proper ideal)
$\underline{m}[x] \subset B \subset B[x]$, $m[x^{-1}] \subset B[x]$

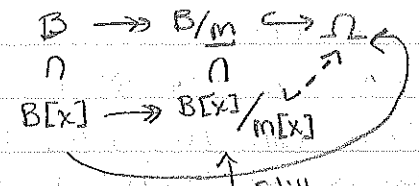
Pf: Suppose otherwise. Then, $1 = a_0 + a_1 x + \cdots + a_m x^m \quad a_i \in \underline{m}$
and $1 = b_0 + b_1 x^{-1} + \cdots + b_n x^{-n} \quad b_i \in \underline{m}$

Assume m, n minimal, and $m \geq n$.
Mult. 2nd by x^m: $x^m = b_0 x^m + b_1 x^{m-1} + \cdots b_n x^{m-n}$
$(1 - b_0) x^m = \cdots$
↑ invertible b/c $b_0 \in \underline{m}$ (& all $1 + \underline{m}$ are units)
$(1 + b_0)^{-1} \in B$

$\Rightarrow x^m = * x^{m-1} + \cdots + * x^{m-1}$, & simplifies 1st eqn
which contradicts m minimal.

Step 3: Suppose $m[x] \neq 1$, so $B[x] \neq m[x]$. If x is transcendental, then g extends to $B[x]$ as $B[x] \to B \xrightarrow{g} \Omega$, $p(x) \mapsto p(0)$. Contradicts maximality of (B, g).

If x is algebraic,



ie, is an algebraic extn of B/m

$\bar{g}$ is an extension of g unless $x \in B$. & $B[x] = B$.
By symmetry, if $\frac{1}{x} \notin m[x^{-1}]$, $x^{-1} \in B$. □

Cor: $A \subset k$, A a ring, k a field. The integral closure $\overline{A} = \bigcap_{\substack{B \subset k \text{ val. ring} \\ A \subseteq B}} B$ (ie intersection of all val rings containing A)

Pf: ($\subseteq$): B/c $\overline{B} = B$, so must contain $\overline{A}$.

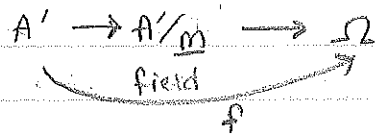
($\supseteq$): Suppose $x \notin \overline{A}$. (WTS $\exists$ val ring B s.t. $x \notin B$)

Then $x \notin A[x^{-1}] = A'$

B/c $x^d + \cdots$, divide by x^{d-1} & get poly for x^{-1} & vice versa.

$x^{-1} \in A'$ is not a unit (b/c $x \notin A$).

Take max. ideal $m \ni x^{-1}$ & consider



Gives (A', f). There is a $(B, g) \geq (A', f)$, so $B \supset A'$ & g extends f, B a val. ring.
But $x \notin B$ (f annihilated $x^{-1} \Rightarrow g(x^{-1}) = 0$ $\Rightarrow g(x)$ not defined $\Rightarrow x$ not in domain of $g \Rightarrow x \notin B$). □

In particular, any hom. $A \to \Omega$ (Ω alg. cl. field) extends to $\bar{A}$.
(b/c can be extended to a val. ring, & any val. ring contains $\bar{A}$).

Hilbert's Nullstellensatz (Zero-Locus Thm)
K a field, $B \supset K$ a f.g. alg and a field, then B is an alg. ext'n of K., (so $[B:K] < \infty$.
*any transcendental ext'n from an alg (ie w/ div) is infinite.

3/15 Prop: Let $A \subseteq K$ be an inclusion of rings, K a field. Then $\bar{A} = \bigcap_{A' \supseteq A} A'$ s.t. A' a val. ring of K.

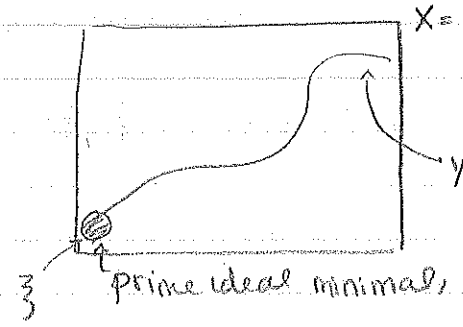
Hartogs's Thm: Every holomorphic fcn $f: B^n \setminus \{0\} \to \mathbb{C}$ (where B^n = unit ball in $\mathbb{C}^n$) extends to a holomorphic fcn on B^n if $n \geq 2$.
(all singularities in codim-2 are removable)
(the prop. is the algebraic analogue of the thm).

Algebraic Analogue: If X is a normal variety
(ex: Spec R, R int. cl. domain)
[variety $\rightsquigarrow$ R a domain, normal $\rightsquigarrow$ integrally closed in FF],
then any rat'l fcn on X regular in codimension 1 is regular $\leftarrow$ holo. ↳(meromorphic fcn)
[If $X = \operatorname{Spec} R$, rat'l fcns on X are elts of the FF $k = R_{(0)}$]
[Ex: If $X = \mathbb{A}^n$ ($X = \operatorname{Spec} k[x_1, .., x_n]$) $f \in k[x_1, .., x_n]$ are "regular" fcns on X, $FF = k = k(x_1, .., x_n)$ ← rat'l fcns in k]
$\frac{x^2+1}{xy}$ a rat'l fcn on $\mathbb{A}^2$. singularities on axes, which is codim 1.

Prop: If A is nice (ex: f.g. over a field), then $\forall \mathfrak{p}$ minimal in A (above (0)), $A_{\mathfrak{p}}$ is a valuation ring of $K = A_{(0)}$.
↑ field of fracs.

Ex: $\mathbb{Z}_{(p)}$ are val rings of $\mathbb{Q}$ b/c (p) are all min. primes.

rat'l fcn $\Rightarrow$ elt of K. regular in codim 1 $\Rightarrow$ in every $A_{\mathfrak{p}}$ for $\mathfrak{p}$ min. prime.



$f \in A_{(0)}$ regular in codim 1 $\Rightarrow$ f defined along open U which intersects Y.

$\Rightarrow U \ni \xi$

$\Rightarrow f \in A_{\mathfrak{p}}$.

So rat'l fcn $f \Leftrightarrow f \in K$

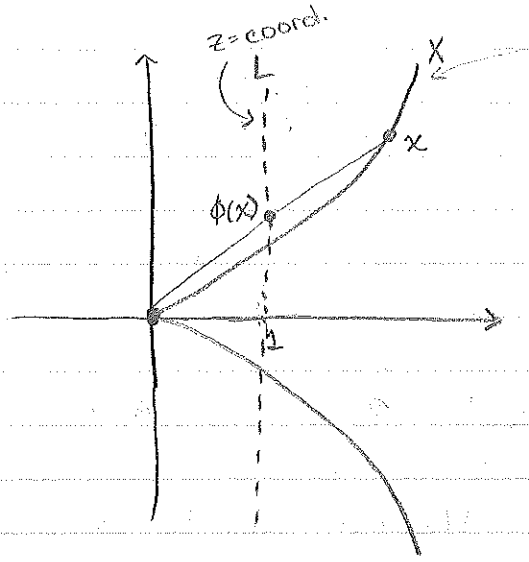
reg. in codim 1 $\Leftrightarrow f \in A_{\mathfrak{p}}$ $\forall \mathfrak{p}$ min., $\mathfrak{p} \neq (0)$

$\Rightarrow f \in \bigcap A_{\mathfrak{p}}$, $A_{\mathfrak{p}}$ val. rings of K, $A_{\mathfrak{p}} \supseteq A$.
$\mathfrak{p}$ height 1 ← minimal above 0

$\Rightarrow f \in \overline{A}$. If X is normal (ie A is int. closed), then $f \in A \Rightarrow f$ is regular.

Ex: $k[x,y]/(y^2 - x^3) = A$

Claim: $\overline{A} \simeq k[z]$, $z = y/x$.



$z(y^2 - x^3)$

Define a map $X \setminus \{0\} \xrightarrow{\phi} L \setminus \{(1,0)\}$
$\phi((x,y)) = (1, y/x)$

ϕ is bijective (expect a line to intersect a cubic (x^3) 3 times. - but $(0,0)$ is a double pt - so only one place left to hit curve)

- Can write a formula for ϕ^{-1}, only involving rat'l fcns:
$\phi^{-1}((1,z)) = (z^2, z^3)$

Cor: $\exists$ an iso of rings
$A_y \cong k[z]_z$

- removing $y=0 \Leftrightarrow$ localizing at y.
$\mathrm{Spec}(A_y) = \mathrm{Spec}(A) \setminus V(y) = X \setminus (0,0)$
$\wr$
$\mathrm{Spec}(k[z]_z)$

ϕ^{-1} is a regular map (defined everywhere) $L \to X$
$\rightsquigarrow$ expect a map of rings in the other direction.

$A \xrightarrow{f} k[z]$ (both int dom's)

$k[x,y]/(y^2 - x^3)$ well-def b/c $y^2 - x^3 \longrightarrow 0$.

$x \longmapsto z^2$
$y \longmapsto z^3$

Claim: f injective (Ck)

(generic pt of L & X are same)

② f induces an isom. on rings of fracs

③ $k[z]$ is integrally closed. (poly ring in 1 var - same proof as for $\mathbb{Z}$) $\Rightarrow \overline{A} \subseteq k[z]$

④ $\overline{A} = k[z]$ b/c z is integral over A.
$z = y/x$ satisfies $z^2 - x = 0$ (integrality eqn / A)
$\Rightarrow k[z] \subseteq \overline{A}$. ✓

3/18 If A int. closed, integral domain $A = \bigcap_{ht\,\mathfrak{p}=1} A_{\mathfrak{p}}$ & $A = \bigcap_{\substack{C \text{ val. ring} \\ \text{of } k,\ C \supseteq A}} C$

($A_{\mathfrak{p}}$ is a val. ring, but not all of them.) (k the f.g fr. of A) ↑ intersection over larger class.

Prop: Let $A \subseteq B$ be int. dom's, B a f.g. A-alg. Let Ω be an alg. cl. field & $v \neq 0 \in B$. Then $\exists\, u \neq 0 \in A$ s.t. every hom $f: A \to \Omega$ s.t. $f(u) \neq 0$ can be extended to $g: B \to \Omega$ s.t. $g(v) \neq 0$.

Cor: (Nullstellensatz) Let k be a field & B a f.g. alg. over k which is also a field. Then B is algebraic over k (ie B is a finite alg. ext'n of k).

(B a f.g. alg over k: $\{b_1, \dots, b_n\}$ s.t. $\sum k_i b_i^n$ are all elts of B — can't pick inverses

ie: $\mathbb{Q}$ is not a f.g. $\mathbb{Z}$-alg — b/c only finitely many primes in denoms of generators.

If smth is f.g. as a field, allows inverses as well.

B finite alg. / k — all elts of B are sol'ns to polys in k of finite degree

$k[x]/(f)$, f irred. poly. $k[x]$ f.g. alg. over k, & $k[x]/(f)$ a finite alg. ext'n of k b/c x satisfies f.)

Pf: Let $\Omega = \overline{k}$, $A = k$, $B = B$, $v = 1$. By prop, $\exists\, u \neq 0 \in k$ s.t. $f: k \hookrightarrow \Omega$, ... can be extended to a $g: B \to \Omega$ s.t. $g(1) \neq 0$. Since B a field, every hom. either 0 or injective $\Rightarrow g$ is injective. $B \subseteq \Omega$ $\Rightarrow$ all elts of B are alg. over k (b/c all elts of Ω are). □

(every f.g. alg. over a field is integral)

Pf of prop: By easy induction, reduce to B is gen. by 1 elt $x \in B$ over A.

Case 1: x is transcendental over A, ie no eqn w/ coeffs in A is satisfied by x, ie $B = A[x]$ in the usual sense (ie $A[y] \to B$ has no kernel
$A \hookrightarrow A$, $y \mapsto x$; ↑ surj b/c B gen by x $\Rightarrow A[y] \cong B$.)

Look at $v \in B$. v is a polynomial in x; ie $\exists$ $a_0, \dots, a_n \in A$ s.t. $a_0 x^n + \cdots + a_n = v$. Pick $u = a_0$.

$x^p - x$ in $\mathbb{F}_p$ is identically 0 $\forall x$

Then given $f: A \to \Omega$ s.t. $f(u) \neq 0$, ie $f(a_0) \neq 0$, look at poly $f(a_0)z^n + \cdots + f(a_n)$ w/ coeffs in Ω. This takes at least some non-zero value for some $z \in \Omega$ b/c it can have at most n roots, but Ω is infinite (b/c alg. closed fields are infinite). Pick $\xi \in \Omega$ s.t. $f(a_0)\xi^n + \cdots + f(a_n) \neq 0$. Extend $f: A \to \Omega$ to a $g: \underset{\| A[x]}{B} \to \Omega$ by setting $g(x) = \xi$.

Then $g(v) = f(a_0)\xi^n + \cdots + f(a_n) \neq 0$.

[We've used: given $f: A \to C$ & any elt $c \in C$, $\exists!$ ring map $g: A[x] \to C$ s.t. $g|_A = f$ & $g(x) = c$. However, if x alg. over A, can't send x to any elt of C b/c must satisfy same relations.]

Case 2: x is algebraic over A, ie $\exists$ an eqn (*) $a_0 x^n + \cdots + a_n = 0$ w/ $a_i \in A$ (as before, $A[y] \to B$ has kernel, so $B \cong A[y]/\text{kernel}$).

Note: $v \in B \Rightarrow v^{-1}$ is also algebraic over k, so $\exists$ $a_0', \dots, a_m' \in A$ s.t. $a_0' v^{-m} + \cdots + a_m' = 0$ (**)

Take $u = a_0 a_0' \in A$. Given any hom $f: A \to \Omega$ s.t. $f(u) \neq 0$. First extend f to $\bar{f}: A[u^{-1}] \to \Omega$ by $\bar{f}(a) = f(a)$ for $a \in A$ & $\bar{f}(u^{-1}) = f(u)^{-1}$ (& b/c Ω a field, so $f(u)$ has an inverse.

Version 1: Let C be the int. closure of $A[u^{-1}]$. By prop. proven by Dima, $\overline{f}$ extends to a $\overline{g}: C \to \Omega$.

Claim (1): $x \in C$: In (*), a_0 is invertible in C (since add u^{-1}, add a_0^{-1} & a_0^{-1}), so dividing (*) by a_0 gives an integrality condition for x over C. But C int. cl. $\Rightarrow x \in C$.

$\Rightarrow B \subseteq C$ (b/c every poly. comb. of x is in C)

Define $g = \overline{g}|_B$.

Claim (2): Note v^{-1} is also integral / C: b/c of eqn (**) dividing by a_0'.

$\Rightarrow v^{-1} \in C$, $v \in C$ (b/c $v \in B \subseteq C$)

$\Rightarrow g(v) \neq 0$: b/c $g(v)g(v^{-1}) = g(1) = 1$.

Version 2: with valuations in book

3/20 $\mathrm{Spec}\,\mathbb{R}[x]$ all ideals 0 or max

max: $(x-a)$, $a \in \mathbb{R}$ ← corresp. to pts in $\mathbb{R}$ ⇝ res. field $\mathbb{R}$ $\left(\frac{\mathbb{R}[x]}{(x-a)} \cong \mathbb{R}\right)$

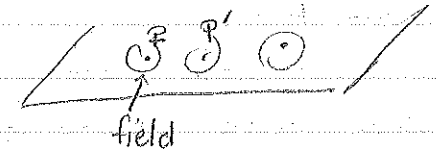
(x^2+ax+b), $\Delta < 0$ ← extra pts ⇝ $\mathbb{C}$ const. polys survive & lin. poly's gone ⇓ 2 dim ext'n of $\mathbb{R}$

(0) ⇝ $\mathbb{R}(x)$ (rational fcns)

If k alg. closed,

$\mathfrak{p}$ prime in $\mathrm{Spec}\,R$, we defined the residue field at $\mathfrak{p}$ as $R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}} \cong (R/\mathfrak{p})_{(0)}$ ($R/\mathfrak{p}$ int dom)

← the unique max ideal in $R_{\mathfrak{p}}$.



- attach a field over each prime
- elts of ring are fcns & take values in field above.

In $\mathbb{A}^1_k$, at gen pt get $k(x)$ as field

Null: all residue fields will give fin. alg. ext'n of k (res. field at $\mathfrak{m}$ ≅ $k[x_1,\dots,x_n]/\mathfrak{m}$ f.g. k-alg & field ⇒ fin. alg. ext'n of k) ← f.g. k-alg

If $k = \overline{k}$, res. field at $\mathfrak{m} = k$

Dichotomy of res. fields can't happen if $k = K$.

Chain Conditions

Prop: Let S be an partially ordered set, $\leq$. TFAE:

(1) Every increasing sequence eventually stabilizes

(2) Every subset has a max. elt.

If $S \subseteq \mathcal{P}(A)$ (ie, S a collection of subsets of A), "$\subseteq$" order & S satisfies (1) or (2), we say S satisfies the ascending chain condition (ACC); an "$\supseteq$" ... descending chain conditon (DCC).

Ex: ① A = fin. abel. gp, $S = \{\text{subgps of } A\}$
S has ACC, DCC

② A = any finite set

③ $\mathbb{Z}$ with subgps (or ideals) has ACC but not DCC.
$(52) \subseteq (26) \subseteq (13) \subseteq (2)$ ACC: every integer has only finitely many factors.
$(2) \supsetneq (4) \supsetneq (8) \supsetneq (16) \supsetneq \cdots$

④ $k[x]$ has ACC but not DCC (same as $\mathbb{Z}$)
- any poly. has finitely many prime factors,

⑤ $k[x_1, x_2, \ldots]$ has neither ACC nor DCC.
$(x_1) \subsetneq (x_1, x_2) \subsetneq (x_1, x_2, x_3) \subsetneq \cdots$

⑥ $k[x]/(x^n)$ has both ACC & DCC (Spec = 1 pt. (one prime ideal $= (x)$))
[If a ring has ACC, quot. has ACC]
fin. dim. as a k-mod. — no ∞ decr. sequence b/c $\dim_k k[x] < \infty$, so dim. must decrease.

Def: A ring A is Noetherian if it satisfies ACC for its ideals; it is Artinian if it satisfies DCC for its ideals.

- to be Artinian, must be fin. dim. over a field, corresp. 0-dim schemes.
- for modules, "ideals" is replaced w/ "submodules"

Ex: infinite dim. simple k-alg. not ss. semi-simple:
$k\langle x,\partial\rangle/\langle x\partial - \partial x = 1\rangle$ is not a matrix alg, but it is simple (no 2-sided ideals)
Check - not semi-simple!

Thm (Artin-Wedderburn): A simple Artinian ring is a matrix alg over a div. alg, $M_n(D)$.
Pf: similar to orig. pf.
(If f.d. over field, then Artinian)

Prop: An R-module M is Noetherian $\Leftrightarrow$ every submod. $N \subseteq M$ is f.g.
Pf: ($\Rightarrow$): Assume by contradiction N is not f.g. Then $\{P \subseteq N \mid P \text{ is f.g.}\}$ has no maximum. $\Rightarrow$ contradicting Acc. (subset of set of submods of M).
(look at max, $P \neq N$, add one more elt not in P)
($\Leftarrow$): Let $N_1 \subseteq N_2 \subseteq \cdots \subseteq N_k \subseteq \cdots$ be an increasing chain of submodules of M. Take $N = \bigcup_i N_i \subseteq M$ submodule. By assumption, N is f.g., so pick $n_1, \ldots, n_k$ which generate. $\exists\ t_i$ s.t. $n_i \in N_{t_i}$ $\forall i$.
Let $t = \max_{1 \le i \le k} \{t_i\}$. At N_t, all generators have appeared,

So sequence must stabilize at t. $\square$

Thm: If $0 \to M' \to M \to M'' \to 0$ is a ses, then M is Noeth/Artin. iff M' and M'' are Noeth/Artin.
Pf: ($\Rightarrow$): seq. of submods in M''; pull back to M, that stabilizes. for M', push it forward
($\Leftarrow$): seq. in M, proj to M'' & pull back to M', both stabilize take max of times, then seq. stabilizes in M.

3/22 **Lemma**: If $0 \to N' \xrightarrow{\alpha} N \xrightarrow{\beta} N'' \to 0$ is short exact and M_1, M_2 are submods N s.t. $\alpha^{-1}(M_1) = \alpha^{-1}(M_2)$ and $\beta(M_1) = \beta(M_2)$, then $M_1 = M_2$.
(use this lemma to finish prev. pf – if stabilizes in N'' & N', then stabilizes in N)

Hint: Look at $M = M_1 + M_2$ & $\alpha^{-1}(M_1) = \alpha^{-1}(M)$, $\beta(M_1) = \beta(M)$
$\cup$
M_1

- If $M_1 = M_1 + M_2$, then $M_1 = M_2$, so can assume $M_1 \subseteq M_2$ by replacing M_2 by $M_1 + M_2$

Prop ① If A is Noetherian, $\phi: A \to B$ onto, then B is Noetherian.
② If $A \subseteq B$, A is Noeth, & B f.g. as an A-mod, then B is Noeth.
③ $S \subseteq A$ a multiplicative set, A Noeth $\Rightarrow S^{-1}A$ is Noeth.

Prop: A Noeth, M f.g. A-mod, $N \subseteq M$ submod $\Rightarrow$ N is f.g., ie M is Noeth.
Pf: (1) A Noeth $\Leftrightarrow$ A is Noeth. as an A-module
(2) A Noeth. A-mod $\Rightarrow$ $A^{\oplus n}$ Noeth.:
$0 \to A \to A \oplus A^{n-1} \to A^{n-1} \to 0$ a s.e.s., induction.
(3) M f.g. $\Leftrightarrow \exists$ surj. map $A^{\oplus n} \to M \to 0$
(map each basis vector in $A^{\oplus n}$ to a gen. of M)
$\Rightarrow \exists$ s.e.s. $0 \to \ker \to A^{\oplus n} \to M \to 0$
$\Rightarrow M$ Noeth. (if middle is Noeth, 2 sides are)
(4) N f.g.
Counterex if A not Noeth: $A = k[x_1, x_2, \ldots] = M$, $N = \langle x_1, x_2, \ldots \rangle$
(ring always f.g. over self $\to$ gen. by 1)

Pf of 1st prop: (1) $0 \to \ker \to A \to B \to 0$ s.e.s.
(ideals in B are ideals of A that contain kernel.)
(2) B f.g. as A-mod $\Rightarrow$ B Noeth. A-mod
ideals in B are subset of A-submods of B
($\neq \mathbb{Z} \hookrightarrow \mathbb{Q}$ ideals $(0) \subseteq \mathbb{Q}$, but not a $\mathbb{Z}$-submod)
$\Rightarrow$ {A-submods} satisfy ACC $\Rightarrow$ {ideals of B} satisfies ACC.
(3) {ideals in $S^{-1}A$} $\xleftrightarrow{1:1}$ {contracted ideals in A}
(contraction from $S^{-1}A$ to A is inj.)
$\Rightarrow$ (Ideals in $S^{-1}A$) $\subseteq$ (ideals in A) ✓ □

Ex: A Noeth $\Rightarrow A_{\mathfrak{p}}$ Noeth.

Thm (Hilbert Basis Thm): If A Noeth $\Rightarrow A[x]$ is Noeth.
(Induct to any poly. ring in finitely many vars)
(ie, if B f.g. as an A-alg, then Noeth, as an A-mod, $A[x]$ gen by $1, x, x^2, \ldots$)
Pf: Let $\underline{a} \subseteq A[x]$ an ideal. WTS $\underline{a}$ f.g.
Define $I \subseteq A$, $I = \{a \in A \mid a$ is a leading coeff of some $f \in \underline{a}\}$
Claim: I is an ideal of A.
- to add, mult. one poly by x^k so have same degree
- to mult by $r \in A$, mult f by r.

A Noeth $\Rightarrow$ I f.g. $I = (a_1, \ldots, a_n)$
Let $f_1, \ldots, f_n \in \underline{a}$ be such that the leading coeffs of f_i is a_i.
Define $\underline{a}' = (f_1, \ldots, f_n) \subseteq \underline{a}$, Let $r_i = \deg f_i$,
$r = \max_{1 \le i \le n} r_i$. Claim: $\forall f \in \underline{a}$, we can write
$f = g + h$, $g \in \underline{a}'$, $\deg h < r$. ← subset, not ideal
(pf deferred). Look at $M \subseteq A[x]$, $M = A$-mod.
gen by $1, x, x^2, \ldots, x^{r-1}$ (ie, all polys of deg $\le r-1$)
Regard everything as A-mods:
Claim $\Rightarrow \underline{a} = \underline{a}' + (\underline{a} \cap M)$. M is f.g $\Rightarrow$ M Noeth as an A-mod. $\Rightarrow \underline{a} \cap M$ a submod is f.g. as

an A-mod. Pick $g_1, \dots, g_k$ gen's for $\underline{a}$ as an A-mod. $\Rightarrow$ $(f_1, \dots, f_n, g_1, \dots, g_k)$ generate $\underline{a}$ as an ideal.

Pf of claim: Pick $f \in \underline{a}$. Then if $\deg f < r$, done ($g = 0$).

If $\deg f \geq r$, look at leading coeff of f:

$f(x) = bx^m + \text{l.o.t.}$, $b \in I \Rightarrow b = \sum a_i c_i$ for some $c_i \in A$. (I f.g.). Then leading term of $\sum c_i f_i x^{m-r_i}$ is exactly bx^m. $\Rightarrow f - \sum c_i f_i x^{m-r_i} \in \underline{a}$ & has lower degree. Repeat — you'll get stuck when $\deg f < r$. Done.

Thm: A Artinian $\Leftrightarrow$ A Noetherian and $\dim A = 0$.
(Pf in book)

Thm: A Artinian $\Rightarrow$ every prime is maximal (ie $\dim A = 0$)

Pf: Let $\mathfrak{p} \subseteq A$ be prime. Then $A/\mathfrak{p}$ an int. dom.

WTS field. Let $x \neq 0 \in A/\mathfrak{p}$. Look at $(x) \supseteq (x^2) \supseteq \cdots \supseteq (x^n) \supseteq \cdots$

Artinian $\Rightarrow x^n = x^{n+1} y$ for some y. No zero divisors, can cancel $x^n \Rightarrow xy = 1 \Rightarrow x$ a unit. $\Rightarrow A/\mathfrak{p}$ field $\square$.

4/1 Artin notes, Stewart Galois Theory

Thm (Hilbert Basis Thm): If A is Noetherian, then $A[x]$ is Noetherian.

Cor: If A is Noeth & B is a f.g. A-alg, then B Noeth.

Pf: B f.g. A-alg $\Leftrightarrow \exists$ surj. map $A[x_1, \dots, x_r] \to B$. If I = kernel, $x_i \mapsto b_i$

$\Rightarrow B = A[x_1, \dots, x_r]/I$, so B a quotient of a Noeth. ring $\Rightarrow$ B Noeth.

Prop: Let $A \subseteq B \subseteq C$ be rings with A Noeth, C f.g. A-alg. Moreover, assume C is a f.g. B-module. Then B is a f.g. A-alg.

Pf: Let $x_1, \dots, x_m \in C$ be A-alg. generators for C.
(every elt in C can be written as a poly. in $x_1, \dots, x_m$ w/ coeff's in A)
Let $y_1, \dots, y_n \in C$ be B-mod gens for C. We have
$x_i = \sum b_{ij} y_j$ for some $b_{ij} \in B$. (mn b_{ij}'s)
$y_i y_j = \sum b_{ijk} y_k \quad b_{ijk} \in B$. ($n^3$ b_{ijk}'s)

Let $B_0 = A[b_{ij}, b_{ijk}]$. We have $A \subseteq B_0 \subseteq B$.
B_0 a f.g. A-alg, A Noeth $\Rightarrow B_0$ Noeth.

Steps: (1) C a f.g. B_0-mod
(2) (1) & B_0 Noeth $\Rightarrow B$, a submod of C, a f.g. B_0-mod
(3) B_0 f.g. A-alg, & (2) $\Rightarrow B$ f.g. A-alg

(2) obvious, (3) obvious.

Pf of (1): We'll show that $\{y_i\}$ generate C as a B_0-mod.
Why? We know every $z \in C$ is a polynomial in the x_i's w/ coeff's in A, but x_i's are lin combs of y's. Open parentheses, & get poly that involves prods of $y_i y_j \Rightarrow$ replace w/ lin. comb. of y_k.
$\Rightarrow z$ a lin. comb. of y_i's w/ coeff's in B_0. $\Rightarrow C$ a B_0-mod. □

[Ex: $z = a_1 x_1 x_2 + a_2 x_3$
$= a_1 (\sum b_{1j} y_j)(\sum b_{2k} y_k) + a_2 (\sum b_{3\ell} y_\ell)$
$= a_1 \sum_{jk} b_{1j} b_{2k} y_j y_k + a_2 \cdots$
$= a_1 \sum_{j,k,s} \underbrace{b_{ij} b_{2k} b_{ijks}}_{\in B_0} y_s + \cdots$]

Thm (Nullstellensatz): Let k be a field, $k \subseteq E$, E a f.g. k-alg & E a field. Then E is a finite algebraic extension of k.

[If you a finitely many elts & get field, then elts you added were algebraic]

Field extn: Can add elts & their inverses

Pf: Let $x_1, \dots, x_n$ be generators of E as a k-alg. Assume some are not algebraic. We can renumber $x_1, \dots, x_n$ so that $x_1, \dots, x_r$ are algebraically independent over k & $x_{r+1}, \dots, x_n$ are algebraic over $k(x_1, \dots, x_r) = F$.

$k \subseteq F \subseteq E$ fields, F a purely transcendental ext'n (ie, can regard $x_1, \dots, x_r$ as abstract variables - they don't satisfy any rel's), E alg. / F.

$k \subseteq F \subseteq E$ (f.g. k-alg; E f.g. F-mod) $\Rightarrow F$ a f.g. k-alg. by prev. prop.

WTS $k(x_1, \dots, x_r)$ is not a f.g. k-alg. This gives contradiction.

Assume $\{f_i/g_i\}$ gen. $k(x_1, \dots, x_r)$ as a k-alg. Take $h = (\prod g_i) + 1$. Then h cannot appear as a denom. in any alg. comb. of $\{f_i/g_i\}$. $\Rightarrow 1/h \in k(x_1, \dots, x_r)$ is not an alg. comb. of $\{f_i/g_i\} \Rightarrow k(x_1, \dots, x_r)$ cannot be f.g. as a k-alg. $\square$.

Field Theory

4/3 J.S. Milne - online notes on field theory & Galois theory

Def: The characteristic of a field k is $\min\{n \mid n\cdot 1 = \overbrace{1+\cdots+1}^{n} = 0\}$
$n>0$, $n\in\mathbb{Z}$
$= \mathrm{Char}\, k$.

$\mathrm{char}\, k = 0 \iff n\cdot 1 \neq 0 \ \forall n \neq 0$.

map $\mathbb{Z} \xrightarrow{f} k$, $1 \mapsto 1$ $\quad \ker f = 0$ if $\mathrm{char}\, k = 0$
but $\ker f$ = prime ideal (preimage of prime is prime)
so $\mathrm{char}\, k = p$, a prime

Binomial Thm: $(a+b)^n = a^n + \binom{n}{1}a^{n-1}b + \binom{n}{2}a^{n-2}b^2 + \cdots + b^n$
true in any ring. ← image of $\binom{n}{2}$ under f into field.

- If $n = p^m$, $p = \mathrm{char}\, k > 0$,
then $p \mid \binom{p^m}{i}$ $\forall\, i \neq p^m, 0$.
$\Rightarrow (a+b)^{p^m} = a^{p^m} + b^{p^m}$
and $(ab)^{p^m} = a^{p^m}b^{p^m}$
$\Rightarrow$ If $\mathrm{char}\, k = p$, then $f: k \to k$, $F(x) = x^p$ is a field homomorphism. $\to$ takes 1 to 1 & is additive & mult.
F is called the Frobenius homomorphism

Ex: $k = \mathbb{Z}/p\mathbb{Z}$, $F = \mathrm{id}$. hom. b/c of Fermat's Little Thm.
- fixed pts of F are the images of $\mathbb{Z}$ under f

Claim: If $\mathrm{char}\, k = p$, then $\mathrm{Fix}(F) = \{x \in k \mid F(x) = x\}$
is $\mathrm{Im}(\mathbb{Z}/p\mathbb{Z} \to k)$.
Why are there no other fixed pts? Look at eqn $X^p = X$ in k, a polynomial eqn, so cannot have more than p roots, those we found above. □

(Weyl Conjecture)