Commotative Algebra

www.math.cmu.edu/users/jcumming/teaching/commalg13

Office hours immediately before/after class

HW every day + Take Home Tests (Midterm + Final)

Notation:

Ring means commotative with identity

If S is a ring, R a sobring includes the identity of S

$\phi: R \to S$ is a homomorphism means: $\phi(1_R) = 1_S$

Zorn's Lemma: $(\mathbb{P}, \leq)$ a poset, nonempty

If every chain has an upper bound, then the poset has a maximal element.

Or: If $\mathbb{P}$ a poset and every chain has an upper bound, then for all $p \in \mathbb{P}$ there is a maximal $q \geq p$.

potentially empty.

Category $\mathcal{C}$: Objects

Arrows $a \xrightarrow{f} b$

Axioms: identity arrow

$$\begin{tikzcd} a \arrow[r, "f"] \arrow[rr, bend right, "g \circ f"'] & b \arrow[r, "g"] & c \end{tikzcd}$$

$$\begin{tikzcd} a \arrow[loop right, "1_a"] \end{tikzcd}$$

associativity

Examples of Categories:

Groups + HMs

Rings + HMs

Metric Space + Isometries

Metric Space + Cts maps

Topological Spaces + Cts maps

Functor: $F: \mathcal{C} \to \mathcal{D}$

map between objects of $\mathcal{C}$ and objects of $\mathcal{D}$, preserves compostion and identity

Consider two functors $F, G : \mathcal{C} \to D$. A natural transformation from F to G does the following:

For each object X of $\mathcal{C}$, $\exists\, FX \xrightarrow{\nu_x} GX$, ν_X an arrow

$$
\begin{tikzcd}
Fx \arrow[r, "\nu_x"] \arrow[d, "Ff"'] & Gx \arrow[d, "Gf"] \\
Fy \arrow[r, "\nu_x"] & Gy
\end{tikzcd}
\qquad X \xrightarrow{f} Y
$$

<u>Initial Object</u>: Let $\mathcal{C}$ be a category. An object x of $\mathcal{C}$ is initial iff for all y objects of $\mathcal{C}$, there is exactly one arrow $X \xrightarrow{f} Y$

<u>Examples:</u> Empty Topological Space

<u>Not</u> the ~~empty Ring~~ zero Ring, b/c we require $0 \mapsto 0$, $1 \mapsto 1$

<u>Theorem:</u> Let $\mathcal{C}$ be a category; X, Y initial. There is a unique isomorphism $X \xrightarrow{g} Y$.

An isomorphism in $\mathcal{C}$ is $X \xrightarrow{g} Y$ s.t. there is $X \xrightarrow{h} Y$ with $hg = 1_X$ and $gh = 1_Y$.

<u>Proof:</u> Since X, Y initial, $X \xrightarrow{f} Y$ and $Y \xrightarrow{g} X$ exist and are unique. $gf = 1_X$, the unique map $X \to X$, and similarly $fg = 1_Y$. ∎

Field of Fractions:

~~Suppose F and F' are both fields~~

Say F is the field of fractions of a ring R, F' a field, with

$$\begin{tikzcd} R \arrow[r, "\phi"] \arrow[dr, "\phi'"'] & F \arrow[d, "\psi"] \\ & F' \end{tikzcd}$$

, then ψ exists and is unique

$$\psi: \frac{\phi(a)}{\phi(b)} \mapsto \frac{\phi'(a)}{\phi'(b)}$$

Consider the category $\mathcal{C}: R \xrightarrow{\psi} G$, ψ injective HM, G a field. (ψ is the object). Then the field of fractions construction is initial in this wacky category.

For a ring R, $I \subseteq R$ is an ideal $\iff I \neq \emptyset$, closed under R-linear combinations.

R/I quotient ring, $\phi: R \to R/I$ is the quotient HM defined by

$\phi: r \mapsto r + I$.

Let $X \subseteq R$. The least ideal containing X is the ideal generated by X, or the set of R-linear combinations of elts. of X.

Ideals of R/I are in bijection with $\{J \text{ ideal of } R, J \supseteq I\}$

A <u>maximal ideal</u> I of R is an ideal such that I is a maximal element in the poset $(\{J \neq R : J \text{ ideal}\}, \subseteq)$.

A <u>prime</u> <u>ideal</u> I of R is an ideal such that $I \neq R$, and if $a, b \notin I$ then $ab \notin I$.

I maximal $\iff R/I$ a field (consider the only ideals of R/I are trivial and R/I)

I prime $\iff R/I$ an integral domain

Fact: If I is a proper ideal, then there is a maximal ideal M such that $I \subseteq M$.

Proof: Apply Zorn's Lemma. Verify (proper ideals, $\subseteq$) satisfies hypothesis of Zorn's Lemma. Since $1 \notin I$ for all I ~~and~~ in the chain, then the union of the chain of proper ideals is proper. ∎

Note: I is proper iff $1 \notin I$.

Defn: Let R be a ring. The <u>prime spectrum</u> of R is

$$\mathrm{Spec}(R) = \{P : P \text{ is a prime ideal of } R\}.$$

Defn: Let (X, τ) be a topological space. A <u>basis</u> for τ is a subset $B \subseteq \tau$ such that τ = unions of elements of B.

Fact: B is a basis for τ iff $\bigcup B = X$ and $\forall\, c, d \in B$, $c \cap d$ is a union of elements of B.

Then $\{A : A \text{ is a union of elts of } B\}$ is a topology.

Defn: Let R be a ring. The Zariski topology on $\mathrm{Spec}(R)$ is the topology with basis $\{O_a : a \in R\}$, $O_a = \{P \in \mathrm{Spec}(R) : a \notin P\}$

A set $Y \subseteq \mathrm{Spec}(R)$ is closed $\iff Y^c$ is open

$\iff Y^c$ is of the form $\bigcup_{a \in A} O_a$, $A \subseteq R$

$\iff Y = \{P \in \mathrm{Spec}(R) : A \subseteq P\}$

<u>Verify that O_a is a basis:</u>

$$O_0 = \{\}, \quad O_1 = \mathrm{Spec}(R)$$

$$O_a \cap O_b \overset{\text{equal}}{=} O_{ab}$$

Let R be a ring. $a \in R$ nilpotent if $\exists n>0$, $a^n = 0$.

<u>Fact</u>: The collection $\{a \in R,\ a \text{ nilpotent}\}$ forms an ideal.

<u>Fact</u>: If a is nilpotent, P prime, $a \in P$.

<u>proof</u>: Let $n>0$ be least such that $a^n \in P$. If $n>1$, then $a^1, a^{n-1} \notin P$ but $a^n = a\, a^{n-1} \in P$ $\divideontimes$.

<u>proof</u>: $a+P$ is nilpotent in integral domain R/P, so $a+P = 0_{R/P}$, so $a \in P$.

So $\underset{\{a \in R,\ a \text{ nilpotent}\}}{\text{"nil ideal" of } R} \subseteq \bigcap\{P : P \text{ prime ideals of } R\}$.

<u>Theorem</u>: Let R be a ring. a is nilpotent $\iff$, for every prime ideal, $a \in P$

<u>Proof</u>; Enough to show that if a is not nilpotent, there is prime P, $a \notin P$.

Consider the poset $\mathbb{P} = \{I : I \text{ ideal of } R,\ \forall n\ a^n \notin I\}$

The poset is nonempty because $0 \in \mathbb{P}$.

Zorn's Lemma applies because union of chains is in the poset. By Zorn, there is a maximal ideal in $\mathbb{P}$.

<u>Last time</u>: $\mathrm{Nil}(R) = \{a \in R : a \text{ nilpotent}\}$ is an ideal.

$\mathrm{Nil}(R) \subseteq P$ for all $P \in \mathrm{Spec}(R)$

Theorem: $Nil(R) = \bigcap Spec(R)$

Proof: Let $a \notin Nil(R)$, let $S = \{a^n : n > 0\}$. $0 \notin S$.
Let $\mathbb{P} = \{I : I \text{ ideal and } I \cap S = \emptyset\}$. $(0) \in \mathbb{P}$, so $\mathbb{P}$ nonempty.
Order $\mathbb{P}$ by $\subseteq$. Use Zorn's Lemma to get $P \in \mathbb{P}$, P maximal in $\mathbb{P}$.

Since $a \notin P$, $P \neq R$. Let $b, c \notin P$. $P + (b) \supsetneq P$ since P maximal, so $P + (b) \notin \mathbb{P}$, so $\exists\, m : a^m \in P + (b)$.
Similarly $\exists\, n : a^n \in P + (c)$

$a^m a^n \in P + (bc) \implies P + (bc) \notin \mathbb{P}$ so $bc \notin P$. Hence P is prime.
thus, $a \notin P$ as well. Hence $\bigcap Spec(R) \subseteq Nil(R)$.

Defn: Let I be an ideal of R. The radical of I is
$\sqrt{I} = \{a : a^n \in I \text{ for } n > 0\}$. I is a radical ideal iff $I = \sqrt{I}$.

$I + J$ is the least ideal containing I, J
$I \cap J$ is the greatest ideal contained in I, J

Remark: $a \in \sqrt{I} \iff a + I \in Nil(R/I) = \bigcap \{P^* : P^* \text{ prime ideal of } R/I\}$

~~Theor~~ **Theorem:** Prime ideals of R/I correspond to prime ideals of R containing I.

Proof: Under the correspondance between ideals of R containing I and ideals of R/I, If J corresponds to J^*, then $R/J \simeq \dfrac{R/I}{J^*}$, Quotient by prime ideal is ID.

<u>Theorem</u>: $\sqrt{I} = \bigcap \{P : P \text{ prime}, I \subseteq P\}$.

<u>R-Modules</u>:

M is an R-module iff

(1) $(M, +)$ is an abelian group.

(2) We have a scalar multiplication map $R \times M \to M$, w/

(i) $r(m_1 + m_2) = rm_1 + rm_2$

(ii) $(r_1 + r_2)m = r_1 m + r_2 m$

(iii) $r_1(r_2 m) = (r_1 r_2) m$

(iv) $0_R m = 0_M$

(v) $1m = m$

If R is a ring, then R is an R-Module.

<u>Category</u> <u>R-Mod</u>

Objects are R-modules

Arrows are R-module HMs (linear maps)

If $\phi: M \to N$ linear, $\ker(\phi) = \{m \in M : \phi(m) = 0_N\}$.

<u>Submodules</u>: a subset, nonempty, closed under linear combination

If R is a ring, the submodules of R (as an R-Module) are the ideals.

If $M \leq N$ (M is a submodule of N), the quotient module N/M is formed by first considering abelian groups $(M, +) \leq (N, +)$, so we have an abelian group $(N/M, +)$, and define $r(n + M) = rn + M$.

First IM theorem for modules

$\phi : M \to N \quad im(\phi) = \{\phi(m) : m \in M\} \leq N$

$\qquad\qquad\quad ker(\phi) \leq M$

Then there is an isomorphism ψ from $\dfrac{M}{ker\,\phi}$ to $im(\phi)$

$\psi : m + ker(\phi) \longmapsto \phi(m)$

Proof: Considering as abelian groups, this is true, so just check works for the scalar multiplication too. Easy.

$$\begin{tikzcd} M \arrow[r, "\phi"] \arrow[d] & N \\ M/ker(\phi) \arrow[ur, "\psi"'] & \end{tikzcd}$$

Submodules of N/M correspond to submodules of N containing M.

Rings of Fractions

Defn: Let R be a ring. $S \subseteq R$ is multiplicatively closed iff

(a) S is closed under multiplication

(b) $1_R \in S$

Example: Let P be a prime ideal of R, $S = R \setminus P$

If S is a multiplicatively closed set and $\mathbb{P} = (\{I \text{ ideal}; I \cap S = \emptyset\}, \subseteq)$ then all maximal elements $\mathbb{P}$ are prime ideals.

Proof similar to the proof that nilpotents are in all prime ideals.

Define a ring RS^{-1} and a homomorphism $\phi: R \to RS^{-1}$ such that for all $s \in S$, $\phi(s)$ is a unit in RS^{-1}!

$\phi: R \to RS^{-1}$ will have the following universal property:
$\forall \left(\psi: R \to T\right)$ s.t $\forall s$ $\psi(s)$ unit of T, $\exists!$ $\chi: RS^{-1} \to T$ with $\chi \circ \phi = \psi$

$$\begin{tikzcd} R \arrow[r, "\phi"] \arrow[dr, "\psi"'] & RS^{-1} \arrow[d, "\chi"] \\ & T \end{tikzcd}$$

Unique b/c initial object in a category w/ objects are HM's from R to another ring, arrows are HM's between targets.

Construct RS^{-1} by forming $R \times S$ and defining the relation $\sim$ on $R \times S$ by $(r_1, s_1) \sim (r_2, s_2)$ iff $\exists a \in S$ such that $a(r_1 s_2 - s_2 r_1) = 0$.

<u>Claim</u>: $\sim$ is an equivalence relation

(1) S is nonempty, $1 \in S$ and $(r,s) \sim (r,s) \Rightarrow a(rs - rs) = 0$.
(2) Clearly symmetric.
(3) $(r_1, s_1) \sim (r_2, s_2)$ and $(r_2, s_2) \sim (r_3, s_3)$
$a(r_1 s_2 - r_2 s_1) = 0$ $\qquad$ $b(r_2 s_3 - r_3 s_2) = 0$

then
$$abs_2(r_1 s_3 - r_3 s_1) = abs_1 r_2 s_3 - abs_3 r_2 s_1 = 0 \quad \blacksquare$$
and $abs_2 \in S$.

<u>Defn</u>: $\frac{r}{s} = [(r,s)]_\sim$ $\qquad$ $\frac{r_1}{s_1} \cdot \frac{r_2}{s_2} = \frac{r_1 r_2}{s_1 s_2}$ $\qquad$ $\frac{r_1}{s_1} + \frac{r_2}{s_2} = \frac{r_1 s_2 + r_2 s_1}{s_1 s_2}$

equivalence class in $\sim$

$RS^{-1} = \{\frac{r}{s} : (r,s) \in R \times S\}$, the HM $\phi : R \to RS^{-1}$ is defined by $\phi(r) = \frac{r}{1}$. For all $s \in S$, $\phi(s) = \frac{s}{1}$ is a unit b/c $\frac{1}{s} \in RS^{-1}$!

If $0 \in S$, $RS^{-1} \cong (0)$.

Check the desired universal property:

$$\begin{tikzcd} R \arrow[r, "\phi"] \arrow[dr, "\psi"'] & RS^{-1} \arrow[d] \\ & T \end{tikzcd}$$

Assume $\psi(s)$ unit in T for all $s \in S$.

If χ exists, $\chi(\frac{r}{s}) = \chi(\phi(r)\phi(s)^{-1})$

$\Rightarrow \chi(\frac{r}{s}) = \psi(r)\psi(s)^{-1}$

Shows uniqueness, check well-defined, HM

Localization: Special case; if P is a prime ideal of R

$R_P = RS^{-1}$ for $S = R \setminus P$.

Remarks: If $0 \in S$, RS^{-1} is the zero ring.

If S contains zerodivisors, ϕ is not injective

$\left(\ker(\phi) = \{r : \frac{r}{1} = \frac{0}{1}\} = \{r : \exists a \in S, ra = 0\}\right)$

If R is an integral domain and $0 \notin S$, then RS^{-1} is isomorphic to the subring of the field of fractions $\{\frac{r}{s} : s \in S\}$.

Ideals of RS^{-1}:

In general, if $\phi: R_1 \to R_2$ is a ring HM. If J an ideal of R_2, J^c (the contraction of J) is $\{r \in R_1 : \phi(r) \in J\}$
$= \phi^{-1}[J]$.

$\frac{R_1}{J^c} \hookrightarrow \frac{R_2}{J}$. If J prime, then J^c prime too.

If I is an ideal of R_1, then I^e (the extension of I) is the ideal generated by $\phi[I]$.

I an ideal of R_1 $I^{ec} \supseteq I$.
J an ideal of R_2, $J^{ce} \subseteq J$.
Also, these are proper inclusions.

$I^{ece} = I^e$ and $J^{cec} = J^c$

Fact: Every ideal of RS^{-1} is of the form I^e for some ideal I of R. $I^e = \{\frac{r}{s} : r \in I, s \in S\}$.

New Notation: $S^{-1}R$ is standard notation for what was RS^{-1}!

Remark: If R is an ID and $0 \notin S$, then $S^{-1}R$ is IM'ic to a subring of the field of fractions of R, namely $\{\frac{a}{b}, a \in R, b \in S\}$.

In particular, in this case, $S^{-1}R$ is also an ID.

Given an R-module M, define $S^{-1}M$ which will be an ~~$S^{-1}R$~~ $S^{-1}R$-module.

Introduce an equivalence relation on $M \times S$:

$(m_1, s_1) \sim (m_2, s_2) \iff \exists\, a \in S \quad a(m_1 s_2 - m_2 s_1) = 0.$
$\qquad\qquad a(s_2 m_1 - s_1 m_2) = 0$ same thing since two sided module.

Some facts:

(1) $\sim$ is an equivalence relation, write $\frac{m}{s}$ for equivalence class of $[(m,s)]$ under $\sim$

(2) $S^{-1}M = \{\frac{m}{s} : m \in M, s \in S\}$

(3) Defining $\frac{m_1}{s_1} + \frac{m_2}{s_2} = \frac{s_2 m_1 + s_1 m_2}{s_1 s_2}$,

(4) $S^{-1}M$ becomes an $S^{-1}R$ module. $\quad \frac{r}{s_1} \cdot \frac{m}{s_2} = \frac{rm}{s_1 s_2}$

Let $\phi : M_1 \to M_2$ be an R-linear map.

Define $S^{-1}\phi : S^{-1}M_1 \to S^{-1}M_2 \qquad S^{-1}\phi : \frac{m}{s} \mapsto \frac{\phi(m)}{s}$

The operation "S^{-1}" is a functor from R-modules ~~and~~ to $S^{-1}R$ modules. $\quad S^{-1} : R\text{-mod} \to S^{-1}R\text{-mod}$.

<u>Exact Sequence</u>: A sequence as for abelian groups can be defined for modules by considering abelian groups as $\mathbb{Z}$-modules.

<u>Key fact</u>: If $A \xrightarrow{\alpha} B \xrightarrow{\beta} C$ is exact, then
$S^{-1}A \xrightarrow{S^{-1}\alpha} S^{-1}B \xrightarrow{S^{-1}\beta} S^{-1}C$ is exact as well.

<u>Proof</u>: Need to show $\operatorname{im}(S^{-1}\alpha) = \ker(S^{-1}\beta)$. $\beta \circ \alpha = 0$

$0 = S^{-1}(0) = S^{-1}(\beta \circ \alpha) = S^{-1}(\beta) \circ S^{-1}(\alpha) \implies \operatorname{im}(S^{-1}\alpha) \subseteq \ker(S^{-1}\beta)$

Look at $\frac{b}{s} \in \ker(S^{-1}\beta)$, so $S^{-1}\beta(\frac{b}{s}) = \frac{\beta(b)}{s} = \frac{0}{1}$ in $S^{-1}C$.

So $\exists\, t \in S$, $t\beta(b) = 0 = \beta(tb) \implies tb \in \operatorname{im}(\alpha)$

so $\exists\, a \in A$ s.t. $\alpha(a) = tb$. So $S^{-1}\alpha : \frac{a}{st} \mapsto \frac{\alpha(a)}{st}$

$\frac{\alpha(a)}{st} = \frac{tb}{st} = \frac{b}{s}$. So $\frac{b}{s} \in \mathrm{Im}(S^{-1}\alpha)$. $\blacksquare$

Recall: If $\phi: R_1 \to R_2$ a ring HM, $I^e = (\phi[I])$
$J^c = \phi^{-1}[J]$

Analyze ideals of $S^{-1}R$ using $\phi: R \to S^{-1}R$ the natural HM.

Theorem: If J is an ideal of $S^{-1}R$, $J = J^{ce}$.

Proof: $J^{ce} \subseteq J$ for some defn of obvious. $((J^c)^e = (\phi[J^c])$
$(\phi[J^c]) = (\phi[\phi^{-1}[J]]) \subseteq (J).$)

Let $\frac{r}{s} \in S^{-1}R$, $r \in R$, $s \in S$, with $\frac{r}{s} \in J$. $\frac{s}{1} \cdot \frac{r}{s} = \frac{r}{1} \in im(\phi)$
so $r \in J^c$, so $\frac{r}{s} \in J^{ce}$. $\Rightarrow J \subseteq J^{ce}$. ∎

Observation: I an ideal of R. If $I \cap S = \emptyset$, $\frac{s}{1} \in I^e$ (a unit),
so $I^e = S^{-1}R$.

What is the spectrum of $S^{-1}R$?

Claim: Prime ideals of $S^{-1}R$ are in bijection with prime ideals of R disjoint from S.

If Q prime and $S = R \setminus Q$, the primes of $S^{-1}R$ correspond to primes contained in Q.

Proof: Let J be prime in $S^{-1}R$. Let $I = J^c$, so $J = I^e$.
I is prime in R and $I \cap S = \emptyset$.

claim: If I is prime in R and $I \cap S = \emptyset$, then $I = I^{ec}$ and I^e is prime in $S^{-1}R$.

Proof of claim;

$I \subseteq I^{ec}$. Conversely, let $r \in I^{ec}$. Then $\frac{r}{1} \in I^e$, and $I^e = \{\frac{a}{b} : a \in I, b \in S\} := S^{-1}I$. So $\frac{r}{1} = \frac{a}{b} \Rightarrow \exists c \in S$ s.t. $c(rb-a) = 0$. As I is prime, $I \cap S = \emptyset$, $c \notin I$ so $rb - a \in I$. And $a \in I \Rightarrow rb \in I$, $b \in S$ and $I \cap S = \emptyset \Rightarrow b \notin I$, so therefore $r \in I$. $\blacksquare$

Since S^{-1} is exact, it can be argued that ~~$S^{-1}R$~~ $S^{-1}\left(\frac{R}{I}\right) \cong \frac{S^{-1}R}{S^{-1}I} = \frac{S^{-1}R}{I^e}$. $S^{-1}\left(\frac{R}{I}\right)$ is an ID since I prime $\Rightarrow$ R/I an integral domain so therefore $S^{-1}\left(\frac{R}{I}\right)$ is an integral domain. $\blacksquare$

Recall $\alpha \in \mathbb{C}$ is an algebraic integer iff $\exists f \in \mathbb{Z}[x]$ $f(\alpha)=0$.

Algebraic integers form a subring of $\mathbb{C}$.

If f is monic and coefficients are algebraic integers, then so are the roots.

Defn: Let $F \subseteq \mathbb{C}$ be a subfield. F is a number field iff $\dim_{\mathbb{Q}} F$ is finite.

Fact: If F is a number field, then every $\alpha \in F$ is algebraic.

pf: Let $n = \dim_{\mathbb{Q}} F$ and consider $\alpha^0, \alpha^1, \ldots, \alpha^n$. There are $n+1$ elements in a n-dimensional vector space, so there is a nontrivial linear dependence among them, $\exists g \in \mathbb{Q}[x]$ $g(\alpha)=0$ ∎

Defn: Let F be a number field. Then $\mathcal{O}_F$ (ring of integers of F) is $\mathcal{O}_F = \{\alpha \in F : \alpha \text{ algebraic integer}\}$.

Examples $F = \mathbb{Q}(i) = \{a+bi : a,b \in \mathbb{Q}\}$ $\mathcal{O}_F = \mathbb{Z}[i] = \{m+ni, \; m,n \in \mathbb{Z}\}$

In general, $\mathcal{O}_F$ need not be a UFD.

Fact: Ideals in $\mathcal{O}_F$ have unique prime factorizations into prime ideals.

Let k be an algebraically closed field.

We study algebraic subsets of k^n.

Given $A \subseteq k[x_1, \ldots, x_n]$ let $V(A) = \{x \in k^n : f(x) = 0 \; \forall f \in A\}$

Note that $V(A)$ ~~is~~ is $V(I)$ for $I = (A)$.

Let $Y \subseteq k^n$, then $I(Y) = \{f : f(a) = 0 \;\; \forall a \in Y\}$.

$I(Y)$ is an ideal.

Facts about ideals and varieties

$V(I(Y)) \supseteq Y$. $\quad I(V(J)) \supseteq J$ (and also $I(V(J)) = \sqrt{J}$).

Hilbert's Nullstellensatz

Implies:

(1) The maximal ideals of $k[x_1, \dots, x_n]$ are of the form $I(\{(a_1, \dots, a_n)\}) = \{f : f(a_1, \dots, a_n) = 0\}$
$$= (x_1 - a_1, x_2 - a_2, \dots, x_n - a_n).$$

(2) $I(V(J)) = \sqrt{J}$.
($r(J)$ in book)

Defn: In any ring A, an ideal J is radical $\iff \sqrt{J} = J$.

Defn: A subset $Y \subseteq k^n$ is called algebraic (or a variety) if $Y = V(J)$ for some J ideal in A.

We have an inclusion reversing bijection between $\{Y : Y \text{ variety in } k^n\}$ and $\{J : J \text{ radical ideal}\}$

Decomposition of Ideals

Defn: An ideal Q of a ring A is called primary iff $Q \neq A$ and $\forall\, x, y \in A$ if $xy \in Q$, then $x \in Q$ or $y \in \sqrt{Q}$.

Prime ideals are primary.

Q is primary iff $\dfrac{A}{Q}$ has only nilpotent zerodivisors and $A/Q \neq 0$.

__Theorem:__ If Q is primary then $\sqrt{Q}$ is the least prime ideal containing Q.

__Proof:__ A priori, $\sqrt{Q} \subseteq P$ for all prime P with $Q \subseteq P$.

Enough to show $\sqrt{Q}$ prime. $xy \in \sqrt{Q} \Rightarrow \exists n \; x^n y^n \in Q \Rightarrow x^n \in Q$ or $y^n \in \sqrt{Q}$

$x^n \in Q \Rightarrow x \in \sqrt{Q}$ or $y \in \sqrt{\sqrt{Q}} = \sqrt{Q}$.

__Fact:__ $\sqrt{I} = \bigcap_{\substack{P \text{ prime} \\ I \subseteq P}} P$.

In general, primary has no relation to power of prime ideal

$$\not\Longrightarrow$$
$$\not\Longleftarrow$$

__Recall:__ In $\frac{A}{Q}$ for Q a primary ideal, all zerodivisors are nilpotent.

__Fact:__ If Q primary, then $\sqrt{Q}$ is prime.

If $\sqrt{Q} = P$ say Q belongs to P, or Q is P-primary.

$\sqrt{Q}$ is prime $\not\Rightarrow$ Q primary. Primary ideals belong to unique prime ideal.

$$\sqrt{Q_1 \cap Q_2 \cap \cdots \cap Q_n} = \sqrt{Q_1} \cap \sqrt{Q_2} \cap \cdots \cap \sqrt{Q_n}$$

__Defns__ $(I : J) = \{a : aJ \subseteq I\}$ $\quad (I : y) = \{a : ay \in I\}$

__Fact:__ If P is prime and $P \supseteq \bigcap_{i=1}^{n} I_i$, then $P \supseteq I_i$ for some i.

__Proof:__ If $P \not\supseteq I_i$ for all i, choose $a_i \in I_i \setminus P$ $\quad \prod a_i \in \bigcap I_i, \notin P$ $\divideontimes$

__Fact:__ If $P = I_1 \cap I_2 \cap \cdots \cap I_n$ then $P = I_i$ for some i.

__Proof:__ from previous fact

Theorem: If $Q_1, \dots, Q_n$ are P-primary ideals, then $Q_1 \cap Q_2 \cap \dots \cap Q_n$ is a P-primary ideal.

Proof: Let $xy \in \bigcap_{i=1}^{n} Q_i$ If $x \in \bigcap_{i=1}^{n} Q_i$ ok, otherwise $x \notin \bigcap_{i=1}^{n} Q_i$. Fix i such that $x \notin Q_i$. So $y \in \sqrt{Q_i} \Rightarrow y \in P$, but $\sqrt{Q_1 \cap Q_2 \cap \dots \cap Q_n}$ is $\sqrt{Q_1} \cap \sqrt{Q_2} \cap \dots \cap \sqrt{Q_n} = \bigcap_{i=1}^{n} P = P \Rightarrow y \in \sqrt{\bigcap_i Q_i}$. ∎

Theorem: If $\sqrt{Q}$ is a maximal ideal M, then Q is M-primary.

Proof: In A/Q, $\sqrt{Q}$ corresponds to $Nil(A/Q)$. $Nil(A/Q)$ is a maximal ideal of A/Q, since $\sqrt{Q}$ maximal in A. Since $Nil(A/Q)$ is the intersection of prime ideals, $Nil(A/Q)$ is unique prime ideal and unique maximal ideal of A/Q. Since A/Q is local, everything not in the nilradical is a unit, since the nilradical is maximal. So zerodivisors are nilpotents.

Writing ideals of A as intersections of primary ideals.

Defn: An ideal I is decomposable iff I is a finite intersection of primary ideals.

Defn: Let I be a decomposable ideal. Then a decomposition of I as $Q_1 \cap Q_2 \cap \dots \cap Q_n$ with Q_i primary is irredundant if

(1) $\sqrt{Q_1}, \sqrt{Q_2}, \dots \sqrt{Q_n}$ are distinct prime ideals.

(2) For each i, $Q_i \not\supseteq \bigcap_{j \neq i} Q_j$

Goal 1: The set of prime ideals which appear as radicals in an irredundant decomposition of I is unique.

Let Q be P-primary in A and let $r \in A$. Analyze $(Q:r)$.

Let $r \in Q$, then $(Q:r) = A$. Let $r \notin Q$. $Q \subseteq (Q:r)$

If $s \in (Q:r)$, then $sr \in Q \Rightarrow r \in Q$ or $s \in \sqrt{Q}$, but $r \notin Q$ so $s \in \sqrt{Q}$. So $Q \subseteq (Q:r) \subseteq \sqrt{Q} = P$. Taking radicals,

$\sqrt{Q} = P \subseteq \sqrt{(Q:r)} = \sqrt{P} = P \Rightarrow \sqrt{(Q:r)} = P$.

So is $(Q:r)$ primary? If $st \in (Q:r)$ then $rst \in Q$

If $rs \in Q$ then $s \in (Q:r)$ otherwise $t \in \sqrt{Q} = P = \sqrt{(Q:r)}$

So $(Q:r)$ is primary.

If $r \notin P$ and $s \in (Q:r)$ then $rs \in Q \Rightarrow s \in Q$. by primary-ness.

So then $(Q:r) \subseteq Q \Rightarrow (Q:r) = Q$.

$$(I_1 \cap I_2 \cap \dots \cap I_n : x) = (I_1 : x) \cap (I_2 : x) \cap \dots \cap (I_n : x).$$

Fact: A contraction of a primary ideal is primary.

proof: Let $\phi: A \to B$ a ring HM, Q a primary ideal of B.

$Q^c = \{a \in A : \phi(a) \in Q\}$ Consider $\frac{A}{Q^c} \hookrightarrow \frac{B}{Q}$ (injective)

so $\frac{B}{Q}$ only has zerodivisors which are nilpotent, and $\frac{A}{Q^c}$ inherits the property w/ the injective map. ∎

Recall: An ideal I is decomposable iff I is an intersection of primary ideals. If $I = Q_1 \cap Q_2 \cap \cdots \cap Q_m$, Q_i primary, this is irredundant iff

(1) $\sqrt{Q_i}$ are distinct prime ideals

(2) $Q_i \not\supseteq \bigcap_{j \neq i} Q_j$ ~~for~~ each i.

Theorem: The set of prime ideals P such that some P-primary ideal appears in an irredundant decomposition of I is equal to $\{P : P \text{ prime and there is } x \ \ P = \sqrt{(I:x)}\}$ (1st uniqueness theorem)

Proof: Fix an irredundant decomposition $I = Q_1 \cap \cdots \cap Q_m$. Set $P_i = \sqrt{Q_i}$. For each i, Fix $x \in \bigcap_{j \neq i} Q_j$ but $x \notin Q_i$.

$(Q_j : x) = A$. $x \notin Q_i \implies Q_i \subseteq (Q_i : x) \subseteq P_i$ and $\sqrt{(Q_i : x)} = P_i$

$$\sqrt{(I:x)} = \sqrt{\bigcap_j (Q_j : x)} = \bigcap_j \sqrt{(Q_j : x)} = P_j \cap \left(\bigcap_{i \neq j} A\right) = P_j.$$ ∎

Conversely, if P is prime and $P = \sqrt{(I:x)}$ then $x \notin I$,

so $x \notin Q_j$ for some j. $P = \bigcap_j \sqrt{(Q_j : x)}$

$\implies P = \sqrt{(Q_j : x)}$ for some j. $x \notin Q_j$, so $P = P_j$. ∎

Terminology: The primes which appear as radicals of primary ideals in an irredundant decomposition of I are said to "belong to I."

Defns A prime P belonging to I is <u>minimal</u> iff P is minimal under inclusion among primes belonging to I. The other primes which are not minimal and belong to I are said to be <u>embedded</u>.

<u>Defn</u>: A set X of prime ideals belonging to I is <u>isolated</u> iff for all $P \in X$, if $Q \subseteq P$ is another prime belonging to I then $Q \in X$.

General facts about $S^{-1}A$ when S is a multiplicatively closed subset of A.

(1) Ideals of $S^{-1}A$ are $S^{-1}I$, that is, extensions of ideals of I.

(2) If $S \cap I$ is nonempty, $S^{-1}I$ contains a unit so $S^{-1}I = S^{-1}A$.

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

(4) $(I : x) = I$ iff $x + I$ is not a zerodivisor in $\frac{A}{I}$.

(5) $I = I^{ec}$ iff S contains no elements s such that $s + I$ is a zerodivisor in A/I.

(6) $S^{-1}\sqrt{I} = \sqrt{S^{-1}I}$.

<u>Theorem</u>: Let Q be P-primary in A, $S \subseteq A$ multiplicatively closed. There are two cases:

(1) If $S \cap P \neq \emptyset$ then $S^{-1}Q = S^{-1}A$.

(2) If $S \cap P = \emptyset$ then Q is the contraction of $S^{-1}Q$, and $S^{-1}Q$ is $S^{-1}P$ primary.

Proof of theorem: (1) $S \cap Q$ is nonempty.

(2) $S^{-1}P = S^{-1}\sqrt{Q} = \sqrt{S^{-1}Q}$ and $S^{-1}P$ is still prime and $S^{-1}Q$ is still primary (check this!). ■

To show $Q = (S^{-1}Q)^c$, need to show that $\forall s \in S$, $s + Q$ is not a zerodivisor in A/Q. ~~If it were, it would be nilpotent, so~~

Q primary $\Longrightarrow$ all zerodivisors are nilpotent, but $s \notin P$ so $s+Q$ is not nilpotent.

Thm Let I be decomposable, $I = Q_1 \cap Q_2 \cap \dots \cap Q_n$, Q_i primary. Let $S \subseteq A$ be multiplicatively closed $S \cap Q_i = \emptyset$ $1 \le i \le m$

$\underbrace{S \cap Q_i \neq \emptyset}_{}$ $m+1 \le i \le n$.

equivalent to $S \cap P_i = \emptyset$, $S \cap P_i \neq \emptyset$

~~So then~~

So then $S^{-1}I = \bigcap_{i \le n} S^{-1}Q_i = \bigcap_{i \le m} S^{-1}Q_i$

$$(S^{-1}I)^c = \bigcap_{1 \le i \le m} (S^{-1}Q_i)^c = \bigcap_{1 \le i \le m} Q_i.$$ ■

Theorem (2nd uniqueness thm): Let X be an isolated set of prime ideals belonging to I. In an irredundant decomposition of I, the intersection of primary ideals whose radicals belong to X is independent of the choice of decomposition.

Proof: Choose the right S and use the previous theorem.

Defn: An R-module M is <u>faithful</u> if $rm=0 \ \forall m \Rightarrow r=0$.

Defn: Let A be a subring of B. $b \in B$ is integral over A iff there is a monic $f \in A[x]$ s.t. $f(b)=0$.

Theorem: The following are equivalent for A subring of B, $b \in B$:

(1) b is integral over A

(2) $A[b]$ is finitely generated as an A-module

[Digression; $A[b]$ is least subring of B containing $A \cup \{b\}$]
$A[b] = \{f(b) : f \in A[x]\}$ evaluate at b is ring HM.

(3) There is a subring C such that $A \subseteq C \subseteq B$, C is finitely generated as an A-module.

(4) There is a faithful $A[b]$-module which is finitely generated as an A-module.

Proof:

$(1) \Rightarrow (2)$ Just like an old homework

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

$(3) \Rightarrow (4)$ $A[b] \subseteq C$ so C is an $A[b]$ module, C is finitely generated as an A-module, $1 \in C \Rightarrow C$ faithful $(\mathrm{Ann}(1) = \{0\})$.

$(4) \Rightarrow (1)$ Let M be a faithful $A[b]$-module, finitely generated as an A-module. Fix $m_1, \dots, m_n$ generating M as an A-module. Consider M^n:

$$b\begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = \begin{pmatrix} \text{matrix } \underline{F} \\ \text{w/ entries in } A \end{pmatrix}\begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix}$$

proof continued:

By the Cayley Hamilton theorem, there is a monic $f \in A[x]$ such that $\underbrace{f(b) = 0}$.

in noncommutative ring of matrices w/ entries in A.

$$f(b)\begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = 0\begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = 0_{M^n} \implies f(b) \text{ annihilates } M \text{ b/c it annihilates generators.}$$

Faithful $\implies f(b) = 0$. So b is a root of the monic polynomial f, so b is integral over A. ∎

Facts about integrality:

(1) If b is integral over A all elements of $A[b]$ are integral over A.

(2) If $b_1, \dots b_n$ are integral over A, then all elements of $A[b_1, \dots b_n]$ are integral over A.

(3) If A subring of B, $\{c \in B : c \text{ integral over } A\}$ is a subring of B.

(4) If A is a subring of B, B a subring of C, B is integral over A (all $b \in B$ are integral over A) and C is integral over B, then C is integral over A.

Theorem: Let A be a subring of B, let B be an integral extension of A. Let J be an ideal of B and let $I = J^c$.

$$\frac{A}{I} \hookrightarrow \frac{B}{J}. \quad \text{Viewing } \frac{A}{I} \text{ as a subring of } \frac{B}{J},$$

$\frac{B}{J}$ is an integral extension of $\frac{A}{I}$.

Theorem: Let A be a subring of B, B an integral extension of A. Let S be a multiplicatively closed subset of A.

$$S^{-1}A \hookrightarrow S^{-1}B \quad (\text{b/c } S^{-1} \text{ is exact})$$

Viewing $S^{-1}A$ as a subring of $S^{-1}B$, $S^{-1}B$ is an integral extension of $S^{-1}A$.

Proof: Let $b/s \in S^{-1}B$ $\quad b \in B, s \in S$. As b is integral over A,

$$b^n = \sum_{i<n} a_i b^i \quad a_i \in A$$

$$\left(\frac{b}{s}\right)^n = \sum_{i<n} \underbrace{\left(\frac{a_i}{s^{n-i}}\right)}_{\in S^{-1}A} \left(\frac{b}{s}\right)^i \Longrightarrow \text{~~$S^{-1}B$ finitely generated as a $S^{-1}A$ module.~~} \ ?$$

subtract then polynomial has b/s as root

Notation: Let A be a subring of B, Let P be a prime ideal of A. Then $B_P = S^{-1}B$ where $S = A \setminus P$.

Lemma: Let A, B be integral domains and let B be an integral extension of A. Then A is a field iff B is a field.

Proof of Lemma:

($\Longrightarrow$) Let A be a field, let $b \neq 0$. $b \in B$.

$$b^n = \sum_{i<n} a_i b^i \quad \text{with } n \text{ minimal.}$$

As B is an ID, we know $a_0 \neq 0$.

Since A is a field $1/a_0$ exists, then

$$a_0^{-1} b^n - \sum_{i=1}^{n-1} a_i a_0^{-1} b_i = 1 = b \left(\begin{matrix} \text{algebraic} \\ \text{mess in } B \end{matrix} \right). \blacksquare$$

($\Longleftarrow$) let B be a field, $a \in A$, $a \neq 0$, $1/a \in B$

$$\left(\frac{1}{a}\right)^n = \sum_{i<n} a_i \left(\frac{1}{a}\right)^i \quad \text{Multiply by } a^{n-1} \text{ to get}$$

$$\frac{1}{a} = \left(\begin{matrix} \text{algebraic} \\ \text{mess in } A \end{matrix} \right) \in A \quad \blacksquare$$

Recall: If A, B are integral domains and B is an integral extension of A, then A is a field iff B is a field.

Corollary: Let A, B rings, B an integral extension of A. Let Q be a prime ideal of B and $P = Q^c = Q \cap A$. Then P is a maximal ideal of A iff Q is a maximal ideal of B.

Proof: Take quotients, use previous fact.

$\frac{A}{P}$ subring of $\frac{B}{Q}$, also integral extension.

P, Q prime so $\frac{A}{P}$, B/Q integral domains.

<u>Theorem</u>: Let A, B be rings, B integral extension of A. Let P be a prime ideal of A. Then there is a prime ideal Q of B such that $Q \cap A = P$. $Q^c = Q \cap A$.

<u>Proof</u>: Let $S = A \setminus P$. $B_p := S^{-1}B$. View $S^{-1}A$ as a subring of $S^{-1}B$ and $S^{-1}B$ is integral extension of $S^{-1}A$.

Prime ideals of $S^{-1}B$ are in bijection with $\{P' : P' \cap A \subseteq P\}$.

$$\begin{tikzcd} A \arrow[r, hook] \arrow[d, "\alpha"'] & B \arrow[d, "\beta"] \\ S^{-1}A \arrow[r, hook] & S^{-1}B \end{tikzcd}$$

local

Let $\bar{Q}$ be a maximal ideal of $S^{-1}B$. $\bar{Q} = S^{-1}Q$ for Q a prime of B such that $Q \cap A \subseteq P$.

$S^{-1}A$

As $B_p = S^{-1}B$ is an integral extension of A_p, $\bar{Q} \cap A_p$ is a maximal ideal of A_p. Since A_p is local, it only has one maximal ideal $\Longrightarrow$ $\bar{Q} \cap A_p = S^{-1}P$.

Now verify that $Q \cap A = P$. ∎

<u>Theorem (Going up theorem)</u>: Let A, B be be rings, B an integral extension of A. Let $P_1 \subseteq \dots \subseteq P_n$ be an increasing sequence of prime ideals of A. Then there exist $Q_1 \subseteq \dots \subseteq Q_n$ of prime ideals of B such that $Q_i \cap A = P_i$.

Let $m \leq n$ $Q_1 \subseteq \dots \subseteq Q_m$ chain of primes of B, $Q_i \cap A = P_i$ $1 \leq i \leq m$. Then $\exists$ $Q_{m+1} \subseteq \dots \subseteq Q_n$ s.t. $Q_i \cap A = P_i$.

Proof: Enough to show for $m=1, n=2$.

$$\begin{array}{ccc} P_2 & \sim & Q_2 \\ \cup\!| & & \cup\!| \\ P_1 & \sim & Q_1 \end{array}$$

For this, let $A' = \frac{A}{P_1}$, $B' = \frac{B}{Q_1}$ and use previous theorem.

Defn: Let A be a subring of B. The <u>integral closure</u> of A in B is $\{b \in B : b \text{ integral over } A\}$. A is <u>integrally closed</u> in B iff $A =$ integral closure of A in B.

Defn: An integral domain A is <u>integrally closed</u> iff A is integrally closed in ~~in~~ its field of fractions.

Example: $\mathbb{Z}$ is integrally closed.

Theorem: Let A be a subring of B, let C be the integral closure of A in B. $A \subseteq C \subseteq B$. Let $S \subseteq A$ be multiplicatively closed, then $S^{-1}C$ is the integral closure of $S^{-1}A$ in $S^{-1}B$.

Theorem: Let A be an integral domain. Then the following are equivalent:

(1) A is integrally closed.

(2) A_P is integrally closed for all prime ideals P of A

(3) A_M is integrally closed for all maximal ideals M of A.

K field of fractions of A, also FOF of A_P and A_M

Review: (Field Theory)

Let K be a subfield of L. Then the degree of L over K is $[L:K] = \dim_K L$.

Fact: If $K_1 \leq K_2 \leq K_3$ then $[K_3:K_1] = [K_3:K_2][K_2:K_1]$

Proof: Combine bases to get one for K_3 over K_1.

Defn: Let K be a subfield of L.

Then $\alpha \in L$ is algebraic over K iff there is $f \in K[x]$ $f \neq 0$ $f(\alpha) = 0$.

Fact: If $[L:K] < \infty$, all $\alpha \in L$ are algebraic over K.

Proof: $[L:K] = n$, $1, \alpha^1 \ldots \alpha^n$ have a non trivial linear dependence. ∎

Fact: A field K is algebraically closed iff every nonzero $f \in K[x]$ splits (that is product of linear polynomials).

Defn: L is an algebraic closure of K iff

(1) L is algebraically closed

(2) K is subfield of L

(3) L is an algebraic extension of K (all $\alpha \in L$ algebraic over K).

Theorem: Every K has an algebraic closure.

Defn: L is algebraic ~~extension~~ extension of k if $k \subseteq L$ and all $a \in L$ algebraic over k.

Fact: If L_1, L_2 are both algebraic closures of k then there is $\alpha : L_1 \cong L_2$ $\alpha \upharpoonright k = id_k$.

Let $k \subseteq L$ $\alpha \in L$ algebraic over k. Let M_α^k be the unique monic polynomial $m \in k[x]$ s.t. $(m) = \{f \in k[x] : f(a) = 0\}$.
Since PID generator is unique.

Let $\phi_\alpha : k[x] \longrightarrow L$ $\phi_\alpha : f \longmapsto f(\alpha)$
So $im(\phi_\alpha) = k[\alpha] \cong \dfrac{k[x]}{(M_\alpha^k)}$ $(m) = ker(\phi_\alpha)$

$im(\phi_\alpha)$ integral domain $\implies (M_\alpha)$ prime $\implies (M_\alpha)$ maximal.
$\implies k[\alpha]$ field.

$k(\alpha)$ is least subfield of L containing $k \cup \{\alpha\}$

If $M_\alpha = M_\beta$, then there is $\phi : k(\alpha) \cong k(\beta)$ $\phi(\alpha) = \beta$
$\phi \upharpoonright k = id_k$.

Defn: Let α be algebraic over k, $\bar{k}$ the algebraic closure.
The conjugates of α are roots of M_α^k in $\bar{k}$.

In $\bar{k}[x]$, $m_\alpha^k = (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$

May ~~[illegible]~~ not be unique.

Let $\phi: A \to B$ be a ring HM. If J ideal of B, $J^{cec} = J^c$.

So I is a contraction of some $J \iff I = I^{ec}$.

<u>Theorem:</u> Let $\phi: A \to B$ be a ring HM. Let P prime in A. P is the contraction of some prime Q of B iff $P = P^{ec}$. (i.e. P is a contracted ideal)

<u>Proof:</u> ($\Leftarrow$) Let $S = \phi[A \setminus P]$, S is moltaplicatively closed in B and S avoids P^e. In $S^{-1}B$, $S^{-1}P^e$ is a proper ideal. Extend to ~~prime~~ maximal ideal $S^{-1}Q$ where Q is prime in B and $Q \cap S = \emptyset$. $S^{-1}P^e \subseteq S^{-1}Q$ so easily $Q \supseteq P^e$, $Q \cap S = \emptyset$.

So then $Q^c = P$. ∎

Let A be a subring of B, I ideal of A. Then $b \in B$ is <u>integral</u> over $I \iff$ there is $a_i \in I$ such that $b^n = \sum_{i<n} a_i b^i$, $n > 0$.

<u>Theorem:</u> The following are equivalent

(1) b is integral over I

(2) There is a faithful $A[b]$-module M, fg as an A-module and $bM \subseteq IM$.

Theorem: Let A be a subring of B. I ideal of A. Let C be the integral closure of A in B. $[A \subseteq C \subseteq B]$.

For $b \in B$, b is integral over $I \iff b$ is in $\sqrt{I^e}$ where I^e is the extension of I to C.

Corollary: $\{b : b \text{ integral over } I\}$ forms an ideal of C.

Proof: If b integral over I, then let $b^n = \sum_{i<n} a_i b^i \quad a_i \in I$.

integrality over I $\implies b$ integral over $A \implies b \in C \implies b^n \in I^e \implies b \in \sqrt{I^e}$.

Conversely, if $b \in \sqrt{I^e}$, $b^m \in I^e$ for some n, so

$$b^m = \sum_{i=1}^{n} a_i c_i \qquad a_i \in I,\ c_i \in C$$ ~~Consider the subring of A~~

Consider $A[c_1, \dots, c_n]$: As each c_i integral over A, so $A[c_1, \dots, c_n]$ is fg as an A-module.

$$A[b^m] \subseteq A[c_1, \dots, c_n] \implies A[c_1, \dots, c_n] \text{ faithful } A[b^m]\text{-module.}$$

Let $M = A[c_1, \dots, c_n]$, then $b^m M \subseteq IM$. So by a previous theorem, b^m integral over $I \implies b$ integral over I.

Special case of the above

Let A be an integrally closed integral domain, B is the field of fractions of A. Integral closure C of A is $C=A$.
If $b \in B$ is integral over I, then $b \in \sqrt{I}$.

<u>Lemma:</u> Let A be an integrally closed ID, $A \leq B$ where B is also an ID. Let k be the field of fractions of A, L the field of fractions of B, then $k \leq L$. Let I be an ideal of A, let $b \in B$ integral over I. Then b, viewed as an element of L, is algebraic over k, and the coefficients of the minimal polynomial m_b^k of b over k are elements of $\sqrt{I}$ (except the leading coefficient).

<u>Proof:</u> b algebraic over k obvious. The coefficients of m_b^k are symmetric polynomials in the conjugates of b. For each conjugate $\bar{b}$ of b, there is an IM $\phi: k(b) \to k(\bar{b})$ which is constant on k. So $\bar{b}$ integral over I as well, meaning coefficients of m_b^k are in k and integral over I, and so coefficients are in A and by previous theorem, they are in $\sqrt{I}$. ∎

<u>Exercise:</u> The following are equivalent for $\alpha \in \mathbb{C}$

(1) α algebraic integer

(2) $m_\alpha^{\mathbb{Q}} \in \mathbb{Z}[x]$, α is algebraic.

Going Down Theorem:

Let A be an integrally closed integral domain, let $B \supseteq A$ be an ID and B integral over A. Let $P_1 \supseteq \dots \supseteq P_n$, P_i prime in A, $Q_1 \supseteq \dots \supseteq Q_m$, Q_i prime in B, $n \geq m$, $Q_i \cap A = P_i$, Q_i prime,

Proof: Reduce to $n=2$, $m=1$

$$\begin{array}{ll} A & P_2 \subseteq P_1 \\ B & ? \subseteq Q_1 \end{array} \qquad \text{Find } ?.$$

Use localization: $A \subseteq B \subseteq B_{Q_1} \subseteq$ field of fractions of B
$A \subseteq K = \underset{\text{fractions of } A}{\text{field of}} \subseteq$ field of fractions of B.

We will find a prime ideal of B_{Q_1} which contracts to P_2. The contraction of this ideal to B will be Q_2.

By previous theorems, it is enough to show that $P_2^{ec} = P_2$, where e,c done between A and B_{Q_1}.

Extension of P_2 to B is BP_2 (B-linear combinations of P_2)
P_2^e (extension to B_{Q_1}) is $\{\frac{x}{s} : x \in BP_2, s \in B \setminus Q_1\}$

General Analysis for elements of P_2^e. Let $y \in P_2^e$, $y = \frac{x}{s}$
$x \in BP_2$, $s \in B \setminus Q_1$. x integral over P_2, so m_x^k, the minimal polynomial of x over k is

$$m_x^k(y) = y^n + \sum_{i<n} u_i y^i \qquad u_i \in P_2.$$

Proof (continued)

$$\gamma \in P_2^{ec} = P_2^e \cap A.$$

Suppose that $\gamma = \frac{x}{s} \in A$, so $s = x\gamma^{-1}$.

~~Want to show~~ $m_s^k = s^n + \sum_{i<n} v_i s^i \quad v_i = \frac{u_i}{\gamma^{n-i}}$

s is integral over A, so coefficients of m_s^k are in A,

that is, $v_i = \frac{u_i}{\gamma^{n-i}} \in A \qquad u_i = v_i \gamma^{n-i}$

$u_i \in P_2$ a prime ideal $\Rightarrow$ ~~v_i or γ is in A.~~

$v_i \in P_2$ or $\gamma \in P_2$.

If $\gamma \notin P_2$, then $v_i \in P_2$ for all i.

Using $s^n = -\sum_{i<n} v_i s^i \in BP_2 \subseteq BP_1 \subseteq Q_1 \Rightarrow s \in Q_1$ since Q_1 prime.

Contradiction, as $s \in B \setminus Q_1$. Hence, $\gamma \in P_2$, so

$P_2^{ec} = P_2$. ∎

Valuation Rings

Defns Let B be an ID, let K be the field of fractions of B.

B is a valuation ring of K if and only if for all $k \in K$,

either $k \in B$ or $k^{-1} \in B$.

Examples: $\mathbb{Z}_{(p)} \subseteq \mathbb{Q}$

$\mathbb{Z}_p \subseteq \mathbb{Q}_p$

Theorem: Let B be a valuation ring of K.

Then (a) B is a local ring

(b) If $B \subseteq B' \subseteq K$, then B' is a valuation ring of K

(c) B is integrally closed.

Proof: (a) Prove nonunits form an ideal.

Let $M = \{b \in B, b \text{ not a unit}\}$. Easily $BM \subseteq M$.

Let $x, y \in M$. WTS: $x+y \in M$. WLOG $x \neq 0, y \neq 0$.

$\frac{x}{y} \in K$ nonzero $\Rightarrow$ $\frac{x}{y}$ or $\frac{y}{x} \in B$. WLOG $\frac{x}{y} \in B$.

$(x+y) = \underbrace{y}_{\in M}\underbrace{\left(\frac{x}{y}+1\right)}_{\in B}$ ~~etc~~ so $y\left(\frac{x}{y}+1\right) = x+y \in M$. ■

(b) Easy

(c) Let $k \in K$ be integral over B, $k^n = \sum_{i<n} b_i k^i$

If $k \notin B$ then $k^{-1} \in B$, multiply by $\left(\frac{1}{k}\right)^{n-1}$ to get

$k = \sum_{i<n} \frac{b_i}{k^{n-i-1}} \in B$. $\ast$. So $k \in B$. ■

Given a field K, want to construct $B \subseteq K$ which is a valuation of K.

Fix Ω an algebraically closed field. Define a poset $\mathbb{P}$ whose elements are pairs (B, g), B a subring of K and $g: B \to \Omega$ is a ring HM.

$$(B_1, g_1) \leq (B_2, g_2) \iff B_1 \subseteq B_2 \text{ and } g_2 \restriction B_1 = g_1.$$

Zorn's Lemma applies and so there are maximal elts of $\mathbb{P}$.

Field Theory

(1) If K, L are fields and $\phi: K \to L$ is a ring HM, then ϕ is injective.

(2) Let K subfield of L, let $\alpha \in L$, then $K(\alpha) = K[\alpha]$ iff α is algebraic over K.

$K(\alpha)$: least subfield of L w/ K, α. $K[\alpha]$: least subring of L w/ K, α.

(3) $K \leq L$, $\alpha \in L$ algebraic over K, if $\psi: K \hookrightarrow \Omega$ is an embedding of K into algebraically closed Ω, then can find $\psi^+: K(\alpha) \to \Omega$ extending ψ.

Proof of (3):

$$\text{Let } m = m_\alpha^K, \text{ let } K_0 = \psi[K], \ m_0 = \psi(m).$$

Let β be a root of m_0 in Ω. Extend ψ so $\psi^+(\alpha) = \beta$.

For all $f \in K[x]$, $\psi^+: f(\alpha) \longmapsto \psi(f)(\beta)$.

Lemma: Let K be a field, B a valuation ring of K. There is an algebraically closed field Ω and a HM $g: B \to \Omega$ such that g is maximal.

Proof of Lemma: B is a local ring.

Let M be the maximal ideal of B, $M = \{\text{nonunits}\}$.
Consider B/M a field. Let Ω be an algebraic closure of B/M. Let $g: B \to \Omega$ be the composition of quotient map $B \to B/M$ and inclusion $B/M \to \Omega$.
Claim g is maximal. If not, $B' \supsetneq B$ and $g' \supsetneq g$ then $g': B' \to \Omega$. Let $c \in B' \setminus B$. Since B is a valuation ring, $1/c \in B$, so $1/c \in M$ is not a unit. Then $g(1/c) = 0$, but $g'(1/c) \neq 0$. $\divideontimes$.

Other way: Fix fields K, Ω with Ω algebraically closed. The poset of $\mathbb{P} = \{(B, g)\}$: B subring of K, $g: B \to \Omega\}$.
Claim: If (B, g) is maximal in $\mathbb{P}$, then B is a valuation ring of K.
Proof:

Claim 1: B is local and $\ker(g)$ is the maximal ideal.
Proof: $M = \ker(g)$ is prime because $\mathrm{im}(g) \leq \Omega$ a subring, and hence ID.
$B/\ker(g) \cong \mathrm{im}(g)$ an ID.

$B \leq B_M \leq K$ where B_M is localization $\{\frac{b}{c} : b \in B, c \in B/M\}$.

Define $g^+: B_M \to \Omega$, $g^+(\frac{b}{c}) = \dfrac{g^+(b)}{g^+(c)}$ $\quad g(c) \neq 0$ when $c \notin M$.
$M = \ker(c)$.

By maximality of g, $B = B_M$. So M must be maximal, and M is the set of nonunits, and unique since B_M is local.

Let $b \in K$, $b \neq 0$. $B[b]$ is the least subring of K containing $\{b\}, B$.
$M[b] = M^e = \{$polynomials in b, coefficients in $M\}$

Claim 2: If $b \in K$, $b \neq 0$ then either $M[b] \neq B[b]$ or $M[1/b] \neq B[1/b]$.

Proof: Otherwise, $1 \in M[b]$, $1 \in M[b^{-1}]$. Then $1 = \sum_{i=0}^{m} a_i b^i$ and $1 = \sum_{j=0}^{n} a_j' b^{-j}$. Take m, n to be minimal among such values. $a_i, a_j' \in M$. Note $m, n > 0$ since otherwise $1 \in M$.

WLOG $m \geq n$. $b^n = a_0' b^n + \dots + a_n' b^0$. $(1-a_0')b^n = a_1' b^{n-1} + \dots + a_n'$.
Since $a_0' \in M$, then $1 - a_0'$ is a unit. So thus
$b^n = (1-a_0')^{-1}(a_1' b^{n-1} + \dots + a_n')$. Substituting ~~...~~ $b^{m-n}(1-a_0')^{-1}(a_1' b^{n-1} + \dots + a_n')$ into expression for b^m, contradict minimality of M.

Claim 3: B is a valuation ring of K.

Proof: Let $b \in K$, $b \neq 0$. WLOG $M[b] \neq B[b]$, so $M[1/b] = B[1/b]$.
As $M[b]$ is a proper ideal of $B[b]$, find M' extending $M[b]$, M' maximal in $B[b]$. So $M' \cap B \supseteq M$ and is an ideal, but M maximal, so $M' \cap B = M$. Get an injective map $\frac{B}{M} \hookrightarrow \frac{B[b]}{M'}$, both of these are fields. View B/M as a subfield of $\frac{B[b]}{M'} = \frac{B}{M}[x]$ where $x = b + M'$.

So by field theory fact, $B/M[x] = B/M(x)$, and so x is algebraic over B/M. g induces an injective map
$h: \frac{B}{M} \hookrightarrow \Omega$. So h lifts to $\frac{B[b]}{M'} \Rightarrow g$ lifts to $B[b]$

~~proof~~ continued. By maximality of g. $B = B[b]$, so therefore $b \in B$, ~~for any~~

So for any ~~$b \in B$~~, $b \in K$, either $b \in B$ or $b^{-1} \in B$. ∎

Theorem: Let K be a field, A a subring of K.
Then $\{c \in K : c \text{ integral over } A\} = \bigcap \{B : B \text{ valuation ring of } K,\ B \supseteq A\}$

The integral closure of A in K.

Proof: ($\subseteq$) Let c be integral over A, $B \supseteq A$ be valuation ring. As B is integrally closed, $c \in B$.

($\supseteq$) Let c be not integral over A. Then $c \notin A[1/c]$.
So c^{-1} is not a unit of $A[c^{-1}]$. Let N be ~~the~~ a maximal ideal in $A[c^{-1}]$, $c \in N$.

Embed $\frac{A[c^{-1}]}{N} \hookrightarrow \Omega$, Ω be the algebraic closure of $A[c^{-1}]/N$.

Define a HM $g_0 : A[c^{-1}] \to \Omega$, $\ker(g_0) = N$.
Extend to maximal HM $g : B \to \Omega$.
g is maximal, so B is a valuation ring.
But $c \notin B$ since $g(c^{-1}) = g_0(c^{-1}) = 0$.

$c \notin \bigcap \{B \text{ valuation rings of } K\}$. ∎

Notherian and Artinian Modules

Defn: Let M be an R-module. M is
(a) Noetherian iff every increasing sequence $(M_i)_{i\in\mathbb{N}}$ of submodules is eventually constant.
(b) Artinian iff every decreasing sequence $(M_i)_{i\in\mathbb{N}}$ of submodules is eventually constant.

Fact: If K is a field, then Artinian = Noetherian = finite dimension.

Theorem: Let $0 \to M_1 \to M_2 \to M_3 \to 0$ be an exact sequence of ~~modules~~. R-modules. M_2 is Noetherian (or Artinian) iff both M_1, M_3 are Noetherian (or Artinian).

Proof: WLOG $M_1 \leq M_2$ and $M_3 = \frac{M_2}{M_1}$

($\Rightarrow$) Let M_2 be Noetherian. Clearly M_1 is also Noetherian, and M_3 is Noetherian because submodules are submodules of M_2 containing M_1 so M_3 is also Noetherian.

($\Leftarrow$) Let M_1, M_3 be Noetherian. Let $(N_j)_{j\in\mathbb{N}}$ be an increasing sequence of M_2. Both sequences $(N_j \cap M_1)_{j\in\mathbb{N}}$ and $\left(\frac{N_j+M_1}{M_1}\right)_{j\in\mathbb{N}}$ are both eventually constant, say for ~~∃~~ $j \geq J$.

image of N_j under $M_2 \to \frac{M_2}{M_1}$

Let $j \geq J$. Since $j \geq J$, $N_j \supseteq N_J$, so enough to show $N_j \subseteq N_J$. Let $n \in N_j$.

$$n + M_1 \in \frac{N_j + M_1}{M_1} = \frac{N_J + M_1}{M_1}.$$ So $n + M_1 = \bar{n} + M_1$ & $\bar{n} \in N_J$

Hence $n - \bar{n} \in M_1$ and $n - \bar{n} \in N_j$, so $n - \bar{n} \in M_1 \cap N_j = M_1 \cap N_J$

So $\bar{n} \in N_J \Rightarrow n \in N_J \Rightarrow N_j = N_J$ ∎

Theorem: The following are equivalent for M an R-module:

(1) Every submodule of M is finitely generated

(2) M is Noetherian

(3) Every nonempty set of submodules of M has an element which is maximal under inclusion.

Proof: (1) $\Rightarrow$ (2).

Consider the sequence $M_1 \subseteq M_2 \subseteq M_3 \subseteq \dots$

Let $M_\infty = \bigcup_{i \in \mathbb{N}} M_i$. M_∞ is a submodule of M, and so finitely generated. $M_\infty = \langle F \rangle$. Fix N such that $F \subseteq M_N$. Since F generates M_∞, then $M_n = M_N$ for all $n \geq N$.

(2) $\Rightarrow$ (1)

If there is a not finitely generated submodule N. Choose by induction elements $n_i \in N$ such that $n_i \notin \langle n_j : j < i \rangle = N_i$. Then the sequence $(N_i)_{i \in \mathbb{N}}$ is increasing but does not stabilize. $\divideontimes$.

(2) $\Rightarrow$ (3)

Suppose not. Let F be a set of submodules with no maximal element under inclusion. Choose $N_i \in F$, $N_i \subsetneq N_{i+1}$ inductively to find an increasing chain w/ no upper bound.

(3) $\Rightarrow$ (2) Consider increasing chain $M_1 \subseteq M_2 \subseteq M_3 \subseteq \dots$ by (3) has a maximal element and thus upper bound.

<u>Defn</u>: Let R be a ring. R is <u>Noetherian</u> (resp. <u>Artinian</u>) if R is a <u>Noetherian</u> (resp. <u>Artinian</u>) R-module.

<u>Example</u>: (Not all rings are Noetherian).

Let $R = \bigcup_{n \in \mathbb{N}} \mathbb{Z}[x_1, x_2, \ldots, x_n] = \mathbb{Z}[x_1, x_2, \ldots]$ ✓ bad notation b/c each polynomial has only finitely many variables.

Let $I = \langle x_n : n \in \mathbb{N} \rangle = \langle f : f \text{ has zero constant term} \rangle = \langle f : f(\vec{0}) = 0 \rangle$.

<u>Claim</u>: I is not finitely generated.

<u>Proof</u>: Let I be generated by $f_1 \cdots f_t$. Let j be such that $j \geq k$ for all k such that x appears in some f_i.
Let k be such that $f_1 \cdots f_t \in \mathbb{Z}[x_1, \ldots, x_k]$, so then $x_{k+1} = \sum_{i=1}^{t} f_i h_i$. Set $x_i = 0$ for $i \leq k$ and $x_{k+1} = 1$, so then $1 = \sum_{i=1}^{t} f_i(0) h_i(0) = 0$ $\divideontimes$.

<u>Theorem</u>: Let R be Noetherian. Then
(1) For every ideal I, R/I is a Noetherian Ring
(2) For every multiplicatively closed set $S \subseteq R$, $S^{-1}R$ is Noetherian.
(3) Every finitely generated R-module is Noetherian.

<u>Proof</u>:

(3) for every n, R^n is Noetherian. $\dfrac{R^n}{R^{n-1} \times \{0\}} \cong R$ and R^{n-1} Noetherian by induction $\Longrightarrow R^n$ Noetherian.

Every finitely generated R-module is a quotient of R^n by a submodule, and so Noetherian.

Theorem (Hilbert's Basissatz): If R is a Noetherian ring, then $R[x]$ is Noetherian ring. (but not as an R-module!)

Corollary (1): If R noetherian, then $R[x_1, \dots x_n]$ is Noetherian $\forall n$.

Corollary (2): If $R \leq S$ and $S = R[a_1, \dots a_n]$ and R Noetherian, then S is Noetherian too.

Proof of (2): $S \cong \dfrac{R[x_1, \dots x_n]}{\ker(f)}$ where f is "evaluate at $(a_1, \dots a_n)$".

Proof: Let I be an ideal of $R[x]$ and for each n, let

$I_n = \{ a \in R : \exists a_0 \dots a_{n-1},\ a x^n + \sum_{i<n} a_i x^i \in I \}$.

I_n is an ideal of R.

$I_n \subseteq I_{n+1}$ (multiply by x) $(xI \subseteq I)$

Fix N such that $I_n = I_N$ for $n \geq N$. ~~Fix $f_1 \dots f_t \in I$ with degree N such that~~ For each $j \leq N$, fix $f_1^j \dots f_{t_j}^j \in I$ with degree j such that their leading coefficients generate I_j

Claim: $\{ f_k^j : j \leq N, 1 \leq k \leq t_j \}$ generate I.

Proof: Let $g \in I$, prove by induction on $\deg(g)$ that g is $R[x]$-linear combination of f_k^j s.

Easy if $g = 0$ or g constant.

Let $\deg(g) = J$, let $a =$ coefficient of x^J on g.

Case 1: $J \leq N$

Leading coefficients of f_k^J $1 \leq k \leq t_J$ generate I_J as an ideal of R, so subtract a suitable R-linear combination to lower degree and use induction hypothesis.

Case 2: $J > N$. Then $I_J = I_N$, so $a \in I_N$, and we can subtract a suitable R-linear combination of $f_k^N x^{J-N}$ to reduce degree of g, and use IH again. ∎

Theorem: If R is Noetherian, all ideals have primary decomposition.

Defn: An ideal I of R is irreducible iff whenever $I = J \cap K$, for ideals J, K, either $I = J$ or $I = K$.

Lemma: If R is Noetherian, every ideal is a finite intersection of irreducible ideals.

Proof: Passing from R to R/I, it is enough to show that the zero ideal is an intersection of irreducible ideals in a Notherian ring.

Or don't do it, and keep the general ideal I.

If not, let I be a maximal counterexample. So I is not irreducible, $I = J \cap K$, $I \subsetneq J$, $I \subsetneq K$. J, K are each finite intersections of irreducible ideals, hence so is I. $\divideontimes$

Lemma: If R is Noetherian and I irreducible, $I \neq R$, then I is primary.

Proof: Passing from R to R/I, enough to show that in a nonzero Noetherian ring, ~~the~~ if zero ideal is irreducible, then all zerodivisors are nilpotent.

Let x be a zerodivisor, $xy = 0$ for $y \neq 0$.

Consider $\text{Ann}(x^n)$. This is an increasing chain with n, so $\text{Ann}(x^n) = \text{Ann}(x^{n+1})$. Choose the least n with this property.

Claim: $(y) \cap (x^n) = (0)$.

Let $z = ay = bx^n$. Then $zx = bx^{n+1} = axy = 0$

So $b \in \text{Ann}(x^{n+1}) \Longrightarrow b \in \text{Ann}(x^n) \Rightarrow bx^n = 0$.

So $z = 0$.

As $y \neq 0$, and (0) irreducible, then $(x^n) = (0)$ and so x is nilpotent.

Hilbert's Nullstellensatz:

For any field k and point $a = (a_1 \dots a_n) \in k^n$, polynomials which vanish at a are $f \in (x_i - a_i : 1 \leq i \leq n) \subseteq k[x_1 \dots x_n]$

The Nullstellensatz is the converse:

If k is an algebraically closed field and M a maximal ideal of $k[x_1, \dots x_n]$, then M has the above form for a unique point $a \in k^n$.

Corollary: If I is a proper ideal of $k[x_1 \cdots x_n]$, $\exists a \in k^n$
$\forall f \in I,\ f(a) = 0$

Corollary: If $f_1 \cdots f_k$ have no common zero in k^n,
$\exists\, g_1 \cdots g_k$ such that $1 = \sum g_i f_i$.

Hilbert's Nullstellensatz

"Module finite over A"

Let A, B be rings, $A \leq B$. B is finitely generated as an A-module iff $\exists\, b_1 \dots b_n \in B$ such that $B = (b_1 \cdots b_n)_A \leftarrow$ linear combo

B is finitely generated as an A-algebra iff $\exists\, b_1 \cdots b_n$ st. $B = A[b_1 \cdots b_n] \leftarrow$ polynomials. "Ring finite over A"

Let K, L be fields, $K \leq L$. Then $a_1 \cdots a_n \in L$ are algebraically independent over K iff $\forall f \in K[x_1 \cdots x_n]$ $f(a_1 \cdots a_n) = 0 \Rightarrow f = 0$.

Easy fact: If $a_1 \cdots a_n \in L$ are algebraically independent over K, then $K(a_1 \cdots a_n) \cong K(x_1 \cdots x_n) \leftarrow$ the FOF of $K[x_1 \cdots x_n]$.

Fact: If $a_1 \cdots a_n$ are algebraically independent over K and $n > 0$, then $K(a_1 \cdots a_n)$ is not ring-finite over K.

Proof: ETS $K(x_1 \cdots x_n)$ is not ring-finite over K. Suppose it is.
Let $K(x_1 \cdots x_n) = K\left[\frac{f_1}{g_1}, \cdots, \frac{f_t}{g_t}\right]$. Let h be irreducible in $K[x_1, \cdots x_n]$, such that $h \nmid g_i$ for all i. Then $\frac{1}{h} \notin$ RHS. $\divideontimes$

Technical Lemma: Let $A \subseteq B \subseteq C$ be rings. Assume A is Noetherian, and C is ring-finite over A and module finite over B. Then B is ring finite over A.

Proof: Let $C = A[x_1 \cdots x_n] = (d_1 \cdots d_t)_B$.

Let $c_i = \sum_{j=1}^{t} \lambda_{ij} d_j$. Let $d_i d_k = \sum_{j=1}^{t} \mu_{ikj} d_j$ since $\{d_i\}$ generates B.

Let $B_0 = A[\{\lambda_{ij}\}, \{\mu_{ikj}\}]$. Key point: $C = (d_1 \cdots d_t)_{B_0}$

B_0 is ring-finite over A, A Noetherian, so B_0 is Noetherian.

C is a finitely-generated B_0-module and B is a B_0-submodule of C. So B is module-finite over B_0. Since B_0 is ring-finite over A, then B is ring-finite over A. ∎

Lemma: Let K, L be fields. $K \subseteq L$ If L is ring-finite over K, then L is module-finite over K. $([L:K] < \infty)$

Proof: Let $L = K[a_1, \ldots, a_t]$. If all a_i are algebraic over K, we're done, b/c then they generate an extension of finite degree.

If not, reorder the a_i's so that for some $0 < s \leq t$, $\{a_1 \cdots a_s\}$ is a maximal algebraically independent subset of $\{a_1 \cdots a_t\}$.

Note for some $s+1 \leq i \leq t$, a_i is algebraic over $K(a_1 \cdots a_s)$. This implies that L is module-finite over $K(a_1 \cdots a_s)$. Apply the previous Lemma w/ $A = K$, $B = K(a_1, \ldots, a_s)$ and $C = L = K[a_1 \cdots a_t]$
$= K(a_1 \cdots a_t)$

Conclude B is ring-finite over K. $\divideontimes$.

Hilbert's Nullstellensatz: K algebraically closed.

If M is a maximal ideal, in $K[x_1, \dots, x_n]$.

Then $M = (x_i - a_i : 1 \le i \le n)$.

Proofs Let K be algebraically closed, M maximal in $K[x_1, \dots, x_n]$

Let $L = \dfrac{K[x_1 \dots x_n]}{M}$. As $M \cap K = (0)$, then L contains isomorphic copy of K.

Let $y_i = x_i + M$, so $L = K[y_1 \dots y_n]$. So L is ring-finite over K, hence L is module-finite over K. So L is an algebraic extension of K, hence $L \cong K$, that is, for each i, $y_i = a_i + M$ for some $a_i \in K$. So $x_i - a_i \in M$ for all i, so $(x_1 - a_1, \dots, x_n - a_n) \subseteq M$.

The LHS is maximal, so $(x_1 - a_1, x_2 - a_2, \dots, x_n - a_n) = M$. ∎

Chains

Defn: Let M be an R-module. A chain of submodules is a finite sequence M_i, $i \le n$, $M_0 = M$ $\quad M_{i+1} \subsetneq M_i$.

Defn: A chain as above is a composition series for M iff it is maximal ~~under inserting~~ (no more submodules can be inserted)

no nontrivial submodules

Fact: A chain is maximall iff $M_n = 0$ and $\dfrac{M_i}{M_{i+1}}$ is simple for all i

Defn: M is simple iff $M \neq 0$ and only submodules of M are 0 and M.

The length of M is the least length of a composition series if one exists, or ∞ otherwise

$M_0 \supsetneq \dots \supsetneq M_n$ has length n.

(Re) Defn: A chain in M is $M_0 = M \supsetneq M_1 \supseteq \dots \supseteq M_n = 0$

Remark: A chain is maximal iff $\frac{M_i}{M_{i+1}}$ is simple for all i.

Remark: Given a chain M is Nöetherian (resp Artinian) iff M_i/M_{i+1} is Noetherian (resp Artinian).

Remark: M is Artinian iff every nonempty family of submodules has a minimal element under inclusion.

A composition series is a maximal chain, and the length of an A-Module is the least length of ~~its~~ a composition series. $L(M)$

Lemma: If $N < M$ ($N \subseteq M, N \neq M$) and $L(M) < \infty$, then $L(N) < L(M)$.

Proof: Fix a composition series $0 = M_n \subseteq \dots \subseteq M_0 = M$, $n = L(M)$ for M. Intersect with N and show the quotients remain simple.

Consider the natural map $M_i \cap N \xrightarrow{\phi} \frac{M_i}{M_{i+1}}$ (restriction of quotient HM)

~~kernel(ϕ~~ ~~$\ker(\phi) = M_i \cap N$~~

$\ker(\phi) = M_{i+1} \cap N$, so induce an injective map

$$\frac{M_i \cap N}{M_{i+1} \cap N} \hookrightarrow \frac{M_i}{M_{i+1}}$$

Proof (continued):

$$\operatorname{im}(\phi) = 0 \quad \text{or} \quad \operatorname{im}(\phi) = \frac{M_i}{M_{i+1}}$$

if $\operatorname{im}(\phi) = 0$, then $M_i \cap N = M_{i+1} \cap N$

if $\operatorname{im}(\phi) \neq 0$, then $\dfrac{M_i \cap N}{M_{i+1} \cap N}$ is simple.

Deleting repetitions, we find a composition series for N, and by deleting the repetition, we find $L(N) \leq L(M)$.

Claim: There is i such that $M_i \cap N = M_{i+1} \cap N$.

Proof: Otherwise $\dfrac{M_i \cap N}{M_{i+1} \cap N} \cong \dfrac{M_i}{M_{i+1}}$, in which case we can show by backwards induction that $M_i \cap N = M_i$ for all i. But then for $i=0$, $M_0 \cap N = M \Rightarrow N = M$ $*$ since N is a proper submodule. Hence $L(N) < L(M)$.

Lemma: Let $L(M) = r < \infty$. Then every chain in M has length $\leq r$.

Proof: Let $M_0 = M \supsetneq M_1 \supsetneq \cdots \supsetneq M_t = 0$. $L(M_0) = r > L(M_1)$. Similarly $L(M_1) > L(M_2) > \cdots > L(M_t) = 0$.

So $t \leq r$.

Lemma: If $L(M) = r < \infty$, then all composition series have length r, and every chain can be extended to a composition series.

Theorem: The following are equivalent:

(1) M has a composition series

(2) M is both Noetherian and Artinian.

Proof: (1) $\Rightarrow$ (2)

Chains have bounded length, both increasing and decreasing.

(2) $\Rightarrow$ (1)

Let $M_0 = M$. So given $M_0 \ldots M_i$ such that $\frac{M_j}{M_{j+1}}$ is simple for $j < i$. If $M_i = 0$ then done.

Else consider $\{N : N < M_i\}$, note it is nonempty.

M is Noetherian $\Rightarrow$ M_i Noetherian $\Rightarrow$ choose maximal N to be M_{i+1}. As M is Artinian, must halt after a finite number of steps. $\blacksquare$

Theorem: Let k be a field, M a k-module. Then TFAE:

(1) M Noetherian

(2) M Artinian

(3) $\dim(M) < \infty$

(4) $L(M) = \dim(M) < \infty$.

Lemma: If I and J are ideals of R, then $\frac{I}{IJ}$ is naturally an R/J-module.

Lemma: Let R be a ring such that $0 = M_1 M_2 \cdots M_n$ ~~$0 = M_1 \cap \dots \cap M_n$~~ where M_i is maximal in R for all i, M_i, M_j not necessarily distinct. Then R is Artinian iff R is Noetherian.

Proof: Consider the chain $R \supsetneq M_1 \supsetneq M_1M_2 \supsetneq M_1M_2M_3 \supsetneq \cdots \supsetneq M_1M_2 \cdots M_n = 0$. WLOG it is strictly decreasing b/c delete repitition.

$\frac{M_1 \cdots M_i}{M_1 \cdots M_{i+1}}$ is an $\frac{R}{M_{i+1}}$-module, so it is Artinian iff Noetherian.

R is Artinian $\Leftrightarrow$ each quotient is Artinian
$\Leftrightarrow$ each quotient is Noetherian
$\Leftrightarrow$ R is Noetherian.

Lemma: If R is ~~an ideal~~ Noetherian ring, I an ideal of R, then there is n such that $\sqrt{I}^n \subseteq I$. In particular, if $I = 0$, then $Nil(R)^n = 0$.

Proof: ~~Let $Nil(R)$~~ $\sqrt{I} = (a_1, \dots, a_t)$, with $a_i^{n_i} \in I$. Then let $n = \sum_{i=1}^{t} n_i$ use binomial theorem to see (any combination of a_i) to the n is in I.

Lemma: Let R be Noetherian, M a maximal ideal of R. Let Q be an ideal of R. Then TFAE

(1) Q is M-primary.
(2) $\sqrt{Q} = M$.
(3) There is n such that $M^n \subseteq Q \subseteq M$.

Proof of previous Lemma:

(1) $\Leftrightarrow$ (2) true for any ring.

(2) $\Longrightarrow$ (3) there is $n \in \mathbb{N}$ $\sqrt{Q}^n \subseteq Q \to M^n \subseteq Q$.

(3) $\Longrightarrow$ (2) $\sqrt{M^n} \subseteq \sqrt{Q} \subseteq \sqrt{M} = M$, and $\sqrt{M^m} = M \subseteq Q$, so $\blacksquare$

<u>Fact</u>: If p prime, $n \geq 1$, then $\sqrt{p^n} = p$.

<u>Lemma:</u> An artinian ID is a field.

<u>Proof:</u> Let $x \neq 0$. Consider (x^n) forms a decreasing sequence of ideals, so $\exists m$ $(x^m) = (x^{m+1})$, so $x^m = yx^{m+1}$ $x^m \neq 0$, so $yx = 1 \Longrightarrow x$ is a unit. Hence, every nonzero element is a unit.

<u>Lemma:</u> In an artinian ring, prime ideals are maximal.

<u>Proof:</u> I prime $\Longrightarrow \frac{R}{I}$ is ID, $\frac{R}{I}$ is artinian $\Longrightarrow \frac{R}{I}$ field.

<u>Digression:</u> The <u>dimension</u> of a ring R is the largest $n \in \mathbb{N}$ such that there is a strict increasing chain

$$P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_n, \quad P_i \text{ prime}.$$

If every prime ideal is maximal, then dimension 0.

<u>Lemma:</u> If R is Artinian, R has finitely many maximal ideals.

Lemma: If R is Artinian, R has finitely many maximal (prime) ideals.

Proof: Consider finite intersections of maximal ideals, when $R \neq 0$.
Let $M_1 \cap \cdots \cap M_n$ be a minimal such ideal. Let M be maximal.
By minimality, $M_1 \cap \cdots \cap M_n \subseteq M$, as M is prime, M contains M_i for some i $M \supseteq M_i$. Since M_i is maximal, then $M = M_i$.

Lemma: If R is an Artinian Ring, $N = Nil(R)$, then $N^k = 0$ for some k.

Proof: $N \supseteq N^2 \supseteq \cdots \supseteq N^k \supseteq \cdots$

Since the ring is Artinian, there is k, $N^k = N^{k+1}$. Suppose that $I = N^k \neq 0$. Let J be minimal among ideals such that $IJ \neq 0$.
Choose $c \in J$ such that $Ic \neq 0$. As $J \supseteq (c)$ and $I(c) \neq 0$, $J = (c)$
Consider $cI \subseteq I$ and $cI \subseteq J$. $(cI)I = cI^2 = cI \neq 0$, so $(c) = J = cI$. Then $c = cd$ for some $d \in I$.

So $c = cd = cd^2 = cd^3 = \cdots$

Hence $d \in I = N^k \Rightarrow d$ nilpotent, so $c = 0$ $\ast$.

Recall: If 0 is a product of maximal ideals, R Noetherian iff R is Artinian.

Theorem: For $R \neq 0$, then the following are equivalent.

(1) R is Artinian

(2) R is Noetherian of dimension zero (Prime ideals are maximal)

Proof of Theorem:

(1) $\Longrightarrow$ (2)

Let $M_1 \cdots M_n$ be the maximal ideals of R.

Then $M_1 \cap M_2 \cap \cdots \cap M_n$ is both the Jacobson Radical and Nilradical, so $(M_1 \cap \cdots \cap M_n)^k = 0$ for some k.

$$M_1^k M_2^k \cdots M_n^k = (M_1 \cdots M_n)^k \subseteq (M_1 \cap \cdots \cap M_n)^k = 0$$

Since 0 is a product of maximal ideals, R Artinian, then R is Noetherian. ∎

(2) $\Longrightarrow$ (1).

As R is Noetherian, $0 = Q_1 \cap \cdots \cap Q_n$ for Q_i primary.

$\sqrt{Q_i} = M_i$, M_i prime and therefore maximal.

As R is Noetherian, there is k_i $M_i^{k_i} \subseteq Q_i$

$\prod_{i=1}^{n} M_i^{k_i} \subseteq \bigcap_{i=1}^{n} M_i^{k_i} \subseteq \bigcap_{i=1}^{n} Q_i$. So by some technical lemma somewhere, and R Noetherian, then R Artinian. ∎

Examples of Artinian Rings

(1) $\frac{\mathbb{Z}}{p^n\mathbb{Z}}$ Both local

(2) $\mathbb{Z}_{(p)} = \{\frac{a}{b} \mid p \text{ doesn't divide } b\}$

Noetherian since localization of Noetherian

not Artinian, ideals are (p^n).

Nakayama's Lemma:

If M is finitely generated and $I \subseteq \mathrm{Jac}(R)$,
$M = IM \Rightarrow M = 0$.

$I \subseteq \mathrm{Jac}(R)$

Fact: If M is finitely generated, $N \subseteq M$ and $M = IM + N$, Then $M = N$.

Proof: $\frac{M}{N}$ is finitely generated $\frac{M}{N} = I \frac{M}{N} \Rightarrow \frac{M}{N} = 0 \rightarrow M = N$.

Fact: Let R be local with maximal ideal I. $\left(I = \mathrm{Jac}(R)\right)$ $\frac{R}{I}$ a field.
Let M be a finitely generated R-module.
If $m_1 + IM, \ldots, m_t + IM$ span $\frac{M}{IM}$, then $m_1 \ldots m_t$ generate M.

Theorem: Let R be a Noetherian local ring with maximal ideal I.
Then either
(a) $I^n \neq I^{n+1}$ for all n (so R not Artinian)
(b) $I^n = 0$ for some n and R is Artinian.

Proof: If not in case (a), then $I^n = I^{n+1} = I I^n$
I^n is finitely generated b/c Noetherian. Nakayama $\Rightarrow I^n = 0$.
0 is product of maximal ideals $\Rightarrow$ R Noetherian.

Recall: I, J ideals of R are coprime iff $I+J=R$

If I, J coprime then $IJ = I \cap J$

Chinese Remainder Theorem:

Ideals $I_1, I_2, \ldots, I_n$ pairwise coprime

$$I_1 I_2 \cdots I_n = I_1 \cap I_2 \cap I_3 \cap \cdots \cap I_n$$

And $$\frac{R}{I_1 I_2 \cdots I_n} \cong \frac{R}{I_1} \oplus \frac{R}{I_2} \oplus \cdots \oplus \frac{R}{I_n}$$

Fact:

If I, J are distinct maximal ideals, $I+J$ strictly larger than each of I, J, but I and J are maximal so $I+J=R$.

Fact: If $\sqrt{I} + \sqrt{J} = R$ then $I+J=R$.

Proof: $1 = a+b$ $\quad a \in \sqrt{I}, b \in \sqrt{J}$ $\quad a^n \in I$ $\quad b^k \in J$

$1^{k+n} \in I+J$ so $I+J$ coprime.

Theorem: If A is an Artinian Ring, then A is isomorphic to a finite product of local Artinian Rings.

Theorem: If A is an Artinian Ring, then A is isomorphic to a finite product of local Artinian Rings.

Proof: By previous work, there are finitely many maximal ideals $M_1, \dots, M_n$ in A, and $M_1^k M_2^k \cdots M_n^k = 0$ for some $k \in \mathbb{N}$.

$\sqrt{M_i^k} = M_i$ Also, each of $M_1^k \dots M_n^k$ are pairwise coprime, so by the Chinese Remainder theorem,

$$A \cong \frac{A}{0} = \frac{A}{M_1^k M_2^k \cdots M_n^k} \cong \frac{A}{M_1^k} \oplus \frac{A}{M_2^k} \oplus \cdots \oplus \frac{A}{M_n^k}$$

Claim: $\frac{A}{M_i^k}$ is an Artinian Local Ring

Proof: Artinian b/c quotient of Artinian Ring.

Maximal ideals of $\frac{A}{M_i^k}$ are maximal ideals of A that contain M_i^k. Let N be maximal in A and contain M_i^k.

Then $N \supseteq M_i^k \Longrightarrow \sqrt{N} = N \supseteq \sqrt{M_i^k} = M_i$

M_i maximal $\Rightarrow N = M_i$. ■

Theorem: Let R be an Artinian local ring.

[If M is the unique maximal ideal, then $M^k = 0$ for some k, $R \setminus M$ is set of units]

TFAE: (1) Every ideal of R is principal

(2) M is principal

(3) $\dim_k \frac{M}{M^2} \leq 1$ where $k = \frac{R}{M}$

Proof of theorem:

(1) $\Rightarrow$ (2) Easy

(2) $\Rightarrow$ (3) If $M=(x)$ then $\{x+M^2\}$ spans $\frac{M}{M^2}$.

(3) $\Rightarrow$ (2) If $\frac{M}{M^2}$ has dimension 0, so $M=M^2$

by Nakayama, ~~R~~ R Artinian $\Rightarrow$ M fg
$M = Jac(R)$

So $M=0$.

If $\dim_k\left(\frac{M}{M^2}\right)=1$, choose a basis $\{x+M^2\}$ and use Nakayama to show $M=(x)$, use lemma from last time.

(2) $\Rightarrow$ (1) Let $M=(x)$. $I \neq (0),(1)$. Let k be such that $M^k=0$.

As M is the unique maximal ideal, $I \subseteq M=(x)$

also $I \neq (0) \Rightarrow I \nsubseteq (0)=M^k=(x^k)$

Let j be such that $I \subseteq (x^j)$ and $I \nsubseteq (x^{j+1})$.

Let $y \in I \setminus (x^{j+1})$. $y = z x^j$ $z \notin (x)=M$, so z is a unit.

~~$x^j z z^{-1}(y)$~~ $x^j = z^{-1} y$ so $x^j \in I$, so $(x^j) \subseteq I$.

Hence $I = (x^j)$ ∎

Moreover, A artin, local has only finitely many ideals.

Recall: Artinian $\iff$ Noetherian and dimension 0

Let R be a Noetherian ID. If R has dimension 1 iff every nonzero prime ideal is maximal and R not a field.

Defn: Let K be a field, ~~and~~ ~~is~~ a discrete valuation ~~ring~~ is a surjective $v: K^* \twoheadrightarrow \mathbb{Z}$ such that $v(a) \in \mathbb{Z}$ $a \neq 0$

$v(0) = +\infty$ by convention.

$v(xy) = v(x) + v(y)$

$v(x+y) \geq \min(v(x), v(y))$

Defn: A ring A is a Discrete Valuation Ring (DVR) iff there is a discrete valuation on the field of fractions of K such that $A = \{x \in K : v(x) \geq 0\}$.

Fact: A a valuation ring, the unique maximal ideal is $M = \{x \in FoF(A) : v(x) > 0\}$

Fact: DVR are integrally closed.

Example: let $k = \mathbb{Q}$, p prime

$v_p(x)$ = unique n s.t. p^n appears in factorization of x.

$d_p(x,y) = p^{-v_p(x-y)}$ defines a metric on $\mathbb{Q}$, plays well w/ field.

Complete $\mathbb{Q}$ with respect to this field to get $\mathbb{Q}_p$

The valuation extends

11/4/13

Theorem: Let A be a Noetherian domain of dimension 1. Then every ideal $I \neq (0),(1)$ I can be written uniquely in the form $Q_1 \cdots Q_n$ where Q_i is primary and $\sqrt{Q_1} \cdots \sqrt{Q_n}$ are distinct.

Proof: As A is Noetherian, I has a minimal representation $Q_1 \cap Q_2 \cap \ldots \cap Q_n$ where Q_i primary $\sqrt{Q_i} = P_i$. P_i is prime and nonzero, dimension $1 \Longrightarrow P_i$ maximal, so P_i are pairwise coprime, hence Q_i pairwise coprime. Hence,

$$Q_1 \cap Q_2 \cap \cdots \cap Q_n = Q_1 Q_2 \cdots Q_n.$$

So existence holds, now for uniqueness;

$P_1, \ldots, P_n$ is an isolated set of primes (no one includes another) because P_i is maximal $\forall i$. So the Q_i are unique. ∎

$v: K \longrightarrow \mathbb{Z} \cup \{\infty\}$ is a valuation

$V(0) = +\infty \qquad V(x) \in \mathbb{Z} \quad x \neq 0$

$v(xy) = v(x) + v(y)$

$v(x+y) \geq \min(v(x), v(y))$

A is a <u>discrete</u> <u>valuation</u> <u>ring</u> if $A = \{x \in K : v(x) \geq 0\}$

Recall: A is a DVR:

$\forall x \in K \setminus \{0\}$ $x \in A$ or $x^{-1} \in A$

A is <u>local</u>

units of A are $\{x \in K : v(x) = 0\}$

nonunits of A are $\{x \in K : v(x) > 0\}$ = maximal ideal.

A is integrally closed

Let I be a nonzero ideal of A, where A is a DVR.

Let $a \in I$, $a \neq 0$, $v(a) = k$ minimal

$$v(b) \geq k \iff v(ba^{-1}) \geq 0 \iff \overset{ba^{-1} \in A}{\cancel{ba^{-1} \in A}} \iff b \in (a)$$

So $I = \{b : v(b) \geq a\} = (a)$

Every ideal is of the form $I_k = \{b : v(b) \geq k\}$

$$I_0 \supsetneq I_1 \supsetneq I_2 \supsetneq \cdots$$

Ideals are linearly ordered by inclusion.

Let $v(c) = 1$, so $(c) = \{b : v(b) > 0\}$ is the unique maximal ideal.

If M is unique maximal ideal, all ideals have form M^k.

M is only maximal and only prime ideal.

So A has dimension 1.

Theorem: Let A be a local Noetherian domain of dimension 1.

M is unique maximal ideal

$k = A/M$

K = F.F of A

TFAE:

(1) A is a DVR

(2) A is integrally closed

(3) M is principal

(4) $\dim_k \frac{M}{M^2} = 1$

(5) Every ideal $I \neq (0),(1)$ has form M^n for $n > 0$

(6) There is c such that every ideal $I \neq (0),(1)$ has form (c^k) for some $k > 0$.

~~Proof:~~

Comments:

(1) From hypothesis, we have

$$M \supsetneq M^2 \supsetneq M^3 \supsetneq M^4 \supsetneq \cdots$$

since otherwise A would be artinian and thus have dimension 0.

(2) If $I \neq 0, (1)$, then I is M-primary, since I is product of primary ideals, but M is the only prime, so I must be M-primary, so there is n, $M^n \subseteq I$

Proof:

(1) $\Rightarrow$ (2) A is a valuation ring and so integrally closed.

(2) $\Rightarrow$ (3) Let $a \in M$, $a \neq 0$. $\sqrt{(a)} = M$, so we can find minimal n such that $M^n \subseteq (a)$. If $n=1$, $M=(a)$ so consider case $n>1$.

$M^{n-1} \not\subseteq (a)$, choose $b \in M^{n-1} \setminus (a)$. In K, let $x = \frac{a}{b}$. $x^{-1} = \frac{b}{a} \notin A$

x^{-1} is not integral over A. So $x^{-1}M \not\subseteq M$.

[M is a fg A-module, if $x^{-1}M \subseteq M$ then M is a faithful $A[x^{-1}]$-module by old facts about integrality.]

However $x^{-1}M \subseteq A$. [$x^{-1} = \frac{b}{a}$, so $x^{-1}M = \frac{b}{a}M \subseteq \frac{M^n}{a} \subseteq A$. Since $b \in M^{n-1}$]

$x^{-1}M$ is an ideal of A, and yet $x^{-1}M \not\subseteq M$, so $M = Ax = (x)$

(3) $\Rightarrow$ (4) M is principal, $\dim_k \frac{M}{M^2} \leq 1$, as in previous argument.

$\dim_k \frac{M}{M^2} = 0 \Rightarrow M = M^2 \Rightarrow$ chain stabilizes $\Rightarrow$ Artin w/ dim 0 $\divideontimes$.

(4) $\Rightarrow$ (5) Let $I \neq (0), (1)$. Find n with $M^n \subseteq I$.

Form the ring $\frac{A}{M^n}$ is an artinian local ring. Use old lemma.

(5) $\Rightarrow$ (6) Let $c \in M \setminus M^2$, then $(c) = M^n$ for some n. Then $(c) = M^1 = M$ because $c \notin M^2$. Hence every ideal is $I = M^k = (c^k)$ if $I \neq (0), (1)$

(6) $\Rightarrow$ (1) Construct v by hand, knowing ideals are I_k.

Define $v(a) = k$ if $(a) = (c^k)$

Extend to K.

11/06/13

Recall: If A is a Noetherian domain of dimension 1, every $I \neq (0), (1)$, every ideal is uniquely the product of primary ideals with distinct radicals.

Remark: If A is a Noetherian domain of dimension 1 and $P \neq 0$ is a prime ideal of A, then A_P is a local Noetherian domain of dimension 1.

Theorem: Let A be a Noetherian domain of dimension 1.
Then TFAE:
(1) A is integrally closed
(2) All nonzero primary ideals of A are powers of nonzero prime ideals
(3) For all nonzero primes P, A_P is a DVR.

Defn: A is a dedekind domain iff A is a Noetherian domain of dimension 1 and A has any of (1), (2), (3)

Easy: In a Dedekind domain, any nonzero ideal $I \neq A$ is uniquely the product of powers of prime ideals.

Proof (1) $\Leftrightarrow$ (3) $\Leftrightarrow$ (2)

Recall (A) A being an integrally closed ID is a local property.
(B) If A is a local Noetherian Domain of dim 1,
A DVR $\Leftrightarrow$ A integrally closed.

(1) $\Leftrightarrow$ Every A_P integrally closed N'ian domain dim=1 $\Leftrightarrow$ every localization is DVR.

Proof (3) ⟹ (2)

Let Q be a primary ideal of A. Let $P = \sqrt{Q}$

Form A_P. Q^e is a primary ideal of A_P, $Q^e \subseteq P^e \leftarrow$ maximal.

Therefore, $Q^e = (P^e)^k$ for some $k \geq 1$, by older theorems

Claim: $Q = P^k$

Proof: P^k is P-primary, because P maximal ($\dim A = 1$)

Since Q, P^k are primary and contained in P, they are contractions of their extensions.

$$Q = Q^{ec} = ((P^e)^k)^c = (P^k)^{ec} = P^k \qquad \blacksquare$$

(2) ⟹ (3)

Let P be nonzero prime ideal, let $I \neq (0), (1)$, I an ideal in A_P. Show that I is a power of the maximal ideal P^e.

$I = I^{ce}$. Let $J = I^c$. $J \neq (0), (1)$ in A. $J \subseteq P$.

by assumption (2), $J = P_1^{k_1} \cdots P_n^{k_n}$ with $P_1 = P$.

$$I = J^e = (P_1^e)^{k_1} (P_2^e)^{k_2} \cdots (P_n^e)^{k_n}$$

Since $P = P_1$ is maximal, for each $j > 1$ P_j is maximal and $P_j \neq P_1 = P$, so $P_j \nsubseteq P$ and $P_j^e \cap (A \setminus P) \neq \emptyset$

Hence $P_j^e = A_P$. So $I = (P^e)^{k_1}$, and by old theorem A_P is a DVR. $\blacksquare$

Example: The ring of integers of a number field is a dedekind domain.

<u>Theorem</u>: If F is a number field, the ring of integers $\mathcal{O}_F$ is a Dedekind domain. ($\mathbb{Q} \subseteq F \subseteq \mathbb{C}$ and $[F:\mathbb{Q}] < \infty$)

$\mathcal{O}_F = \{\alpha \in F, \alpha \text{ algebraic integer}\}$

α is an algebraic integer $\Longleftrightarrow$ α algebraic over $\mathbb{Q}$ and the minimal polynomial $m_\alpha^{\mathbb{Q}} \in \mathbb{Z}[x]$.

<u>Proof:</u>

Need to show $\dim \mathcal{O}_F = 1$, $\mathcal{O}_F$ Noetherian, $\mathcal{O}_F$ integrally closed.

(1) $\mathcal{O}_F$ has field of fractions F.

<u>proof:</u> If $\beta \in F$, let m be the minimal polynomial of β over $\mathbb{Q}$. Find $n \in \mathbb{Z} \setminus \{0\}$ such that $m_{n\beta}^{\mathbb{Q}}$ has integer coefficients. So then $\beta = \frac{n\beta}{n}$, where $n, n\beta \in \mathcal{O}_F$. ∎

If $\gamma \in F$ and γ integral over $\mathcal{O}_F$, then γ integral over F, so $\gamma \in \mathcal{O}_F$.

Let P be a nonzero prime ideal of $\mathcal{O}_F$. $P \cap \mathbb{Z}$ is prime.

(?) Let $\alpha \in P$, $\alpha \neq 0$. Let m be the minimal polynomial of α over $\mathbb{Q}$.

$m = m_\alpha^{\mathbb{Q}} = (x-\alpha_1)\cdots(x-\alpha_n)$, $\alpha_1 = \alpha$ α_i are algebraic integers, as root of m.

$\prod \alpha_i$ = constant term of $m \in \mathbb{Z}$ ...

See email

11/08/13

F is a number field, $\mathcal{O}_F$ the ring of integers.

Last time: $\mathcal{O}_F$ dimension one, $\mathcal{O}_F$ integrally closed

Will Prove: $(\mathcal{O}_F, +)$ is a free abelian group of rank $n = [F:\mathbb{Q}]$

Need: $\mathcal{O}_F$ is Noetherian.

$\mathcal{O}_F$ will be Noetherian $\mathbb{Z}$-mod
$\mathbb{Z} \subseteq \mathcal{O}_F$
$\Rightarrow \mathcal{O}_F$ Noetherian ring

Field Theory: If F_0 is a field and ~~its~~ has characteristic 0
$\alpha: F_0 \hookrightarrow \mathbb{C}$ is a monomorphism
and $F_0 \subseteq F_1$ and $[F_1 : F_1] = t$, α has exacty t extensions onto F_1.

Proof: by induction on t.
If $t=1$, $F_0 = F_1$ and okay.
If $t>1$ choose $\gamma \in F_1 \setminus F_0$, let $m = m_\gamma^{F_0}$ ← distinct roots b/c characteristic 0
$\alpha(m)$ has distinct roots $s = \deg(m) = [F_0(\gamma) : F_0]$
Call these roots $\delta_1 \dots \delta_s$.

For each i, $1 \leq i \leq s$, there is a unique map
$\beta_i : F_0(\gamma) \hookrightarrow \mathbb{C}$ $\quad \beta_i : \gamma \mapsto \delta_i$ These are all extensions of α to $F_0(\gamma)$

Then $F_0 \subseteq F_0(\gamma) \subseteq F_1$ $\quad [F_1 : F_0(\gamma)] = t/s < t$.
So use induction.

Defn: Let $\beta_1 \dots \beta_n$ be the n embeddings of $F \hookrightarrow \mathbb{C}$, $\beta_1 = id_F$.
Where F is a number field and $n = [F:\mathbb{Q}]$. Let $a \in F$.
Then $tr_F(a) = \sum_{i=1}^{n} \beta_i(a)$ $\quad N_F(a) = \prod_{i=1}^{n} \beta_i(a)$

Fact: $Tr_F : F \to \mathbb{Q}$ and $N_F(a) : F \to \mathbb{Q}$.

<u>Proof of facts:</u> Let $a \in F$ $[\mathbb{Q}(a):\mathbb{Q}]=s$ let $m=m_a^{\mathbb{Q}}$, let $a_1 \dots a_s$ be complex roots of m. For each j, $1 \le j \le s$ $\beta_i(a)=a_j$ for n/s values of i.

$$\sum_{i=1}^{n} a_i \in \mathbb{Q} \qquad Tr_F(a) = \frac{n}{s}\sum_{i=1}^{n} a_i \in \mathbb{Q}$$

Consider, given a list $a_1 \dots a_n \in F$, the matrix A with (i,j)-entry $\beta_j(a_i)$

AA^T has i,k entry $\sum_{i=1}^{n} \beta_j(a_i)\beta_j(a_k) = Tr_F(a_i a_k)$

~~det(A)²~~ $\det(A)^2 = \det(AA^T) = \det(Tr_F(a_i a_j)) \in \mathbb{Q}$

$$a_1 \dots a_n \in \mathcal{O}_F \Longrightarrow \det(A)^2 \in \mathbb{Z}$$

discriminant of $a_1 \dots a_n$

<u>Remarks</u> $\det(A)=0 \Longleftrightarrow a_1 \dots a_n$ are linearly dependent over $\mathbb{Q}$.

$a_1 \dots a_n$ independent over $\mathbb{Q} \Longleftrightarrow$ discriminant is zero

<u>Recall:</u> For every $a \in F$, there is $n \in \mathbb{Z}$, $n \neq 0$ $na \in \mathcal{O}_F$. Taking any $\mathbb{Q}$-basis for F as a $\mathbb{Q}$-VS and scaling, we find $a_1 \dots a_n$ which are in $\mathcal{O}_F$ and form a $\mathbb{Q}$-basis.

<u>Claim:</u> The $\mathbb{Z}$-span of $\{\alpha_1 \dots \alpha_n\} \subseteq \mathcal{O}_F \subseteq \mathrm{Span}_{\mathbb{Z}}\{\frac{\alpha_1}{d} \dots \frac{\alpha_n}{d}\}$ where d is the discriminant of $\alpha_1 \dots \alpha_n$.

Then $\mathrm{Span}_{\mathbb{Z}}\{\alpha_1 \cdots \alpha_n\}$ is free of rank n.

also $\mathrm{Span}_{\mathbb{Z}}\{\frac{\alpha_1}{d} \cdots \frac{\alpha_n}{d}\}$ is free of rank n.

So $\mathcal{O}_F$ is a free group of rank n.

Proof: 1^{st} inclusion easy.

2^{nd} inclusion. ~~Let $a \in F, a \neq 0$~~ Let $a \in \mathcal{O}_F$, $a \neq 0$.

$$a = \sum_{i=1}^{n} q_i \alpha_i \qquad q_i \in \mathbb{Q} \qquad \text{So } \beta_j(a) = \sum_{i=1}^{n} q_i \beta_j(\alpha_i)$$

$$\begin{pmatrix} \beta_1(a) \\ \vdots \\ \beta_n(a) \end{pmatrix} = \begin{pmatrix} & A & \end{pmatrix} \begin{pmatrix} q_1 \\ \vdots \\ q_n \end{pmatrix}$$

Since $\{\alpha_i\}$ is lin. indep, A is invertible.

Use Cramer's Rule!

$$\begin{pmatrix} q_1 \\ \vdots \\ q_n \end{pmatrix} = A^{-1} \begin{pmatrix} \beta_1(a) \\ \vdots \\ \beta_n(a) \end{pmatrix}$$

entries in A^{-1} are of the form $\dfrac{\text{alg. integer} \; \cancel{(\text{thing in } \mathcal{O}_F)}}{\delta}$ $\quad \delta = \det(A)$

Each q_i has form $\dfrac{\text{algebraic integer}}{\delta} = \dfrac{\delta\,(\text{alg. integer})}{\delta^2}$

So q_i has form $\dfrac{\text{rational algebraic integer}}{d} \in \dfrac{\mathbb{Z}}{d}$.

Coefficient q_i of $a = \sum_{i=1}^{n} q_i \alpha_i$ is $\dfrac{q_i'}{d}$, with $q_i' \in \mathbb{Z}$

$$a = \sum_{i=1}^{n} q_i' \frac{\alpha_i}{d}.$$

∎

Conclusion: $\mathcal{O}_F$ is a dedekind domain, so ideals $I \neq (0), (1)$ in $\mathcal{O}_F$ are uniquely products of prime ideals.

Fractional Ideals in an Integral Domain

A is an Integral Domain, K is field of fractions of A

A fractional ideal of A is an A-submodule M of K, such that $M = x^{-1}I$ for some $x \in A$ $x \neq 0$, I an ideal of A.

Remark: A finitely generated A-submodule of K is a fractional ideal. (Clear denominators of generators).

Remark: If A is Noetherian, then fractional ideals are finitely generated submodules of K.

If M, N are fractional ideals, MN is the submodule generated by $\{mn : m \in M, n \in N\}$.

M is invertible $\iff$ there is an A-submodule N such that $MN = A$

If M is an A-submodule of K, $(A : M) = \{x \in K : xM \subseteq A\}$

Fact: If M is invertible, $(A:M)$ is the unique N such that $MN=A$. Let N be such that $MN=A$. Then $N \subseteq (A:M)$.

Now $\cancel{N=NA\subseteq}$ $N=NA \subseteq (A:M)A = (A:M)MN \subseteq A:N = N$.

So $N \subseteq (A:M) \subseteq N$.

An A-submodule M is invertible when it has an inverse.

Fact: M invertible $\Longrightarrow$ M fg ($\Longrightarrow$ M a fractional ideal)

Proof: A invertible, $A = M(A:M)$ So $1 \in M(A:M)$, and then $1 = \sum_{i=1}^{n} x_i y_i$ $x_i \in M$, $y_i \in (A:M)$

For every $m \in M$, $m = \sum_{i=1}^{n} x_i (my_i) \in \mathrm{Span}_A \{x_1, \ldots x_n\}$

If a fractional ideal is principal, it is invertible.

$(x)(x^{-1}) = (1)$.

11/11/13

Goal: In a dedekind domain, fractional ideals are all invertible. Define the "ideal class group": nonzero fractional ideals modulo principal nonzero fractional ideals.

Let A be an integral domain, K the field of fractions of A, M an A-submodule of K, P a ~~principal~~ prime ideal of A.

$M_P = \{\frac{m}{s} : s \in A \setminus P\}$.

Recall: Let R be a ring

(1) Let M be an fg R-module, S multiplicatively closed set $\subseteq R$. Then $\mathrm{Ann}(S^{-1}M) = S^{-1}\mathrm{Ann}(M)$

Recall:

(2) Let $M, N \subseteq P$ be R-modules

$(M:N) := \{r \in R : rN \subseteq M\}$ is an ideal of R

If N is fg, then $S^{-1}(M:N) = (S^{-1}M : S^{-1}N)$

Proof: $(M:N) = \operatorname{Ann}\left(\frac{M+N}{N}\right)$, use previous fact.

Theorem: Let A be an ID, K the FoF of A, M an A-submodule of K. Then TFAE

(1) M is invertible

(2) For all prime ideals P, M_P is invertible

(3) For all maximal ideals P, M_P is invertible.

(M is fg)

Recall: Invertible $\Rightarrow$ fg $\Rightarrow$ fractional ideal.

(1) $\Rightarrow$ (2) Let M be invertible, so M is fg. So then $A = M(A:M)$. Localize at $S = A \setminus P$.

$A_P = M_P(A_P : M_P) \Rightarrow M_P$ is invertible.

(2) $\Rightarrow$ (3) Easy.

(3) $\Rightarrow$ (1) Let M be fg, M_P invertible for all maximal P. If M is not invertible, $M(A:M) \subsetneq A$ and $M(A:M)$ is a proper ideal of A.

Let P maximal, $P \supseteq M(A:M)$.

Localize $M_P(A_P : M_P) \subseteq$ "P_P" $\leftarrow$ unique maximal ideal of A_P

but M_P is invertible, so $\divideontimes$.

Theorem: Let A be a DVR. Then all nonzero fractional ideals of A are invertible, ~~[illegible]~~

Proof: Prime ideals are principal.

Theorem: Let A be a dedekind domain. Then all nonzero fractional ideals of A are invertible.

Proof: Let M be a nonzero fractional ideal of A. A is Noetherian so M is finitely generated. M_p is invertible for all maximal p, so apply previous theorem.

Defn: A <u>topological group</u> is a group G equipped with a topology such that the map $G \times G \longrightarrow G$ given by $(g,h) \longmapsto gh^{-1}$ is continuous. Equivalently, multiplication and inversion are cts.

Fact: If G is a topological group, $h \in G$, then $g \mapsto gh$ is a homeomorphism from G to G. Conjugation is a group HM and a homeomorphism.

Remark: If X is a hausdorff space, $\{x\}$ is closed for each x.

Fact: If G is a topological group, G is Hausdorff iff $\{e\}$ is closed.

Proof: ($\Longrightarrow$) easy

($\Longleftarrow$) Consider $\phi: (g,h) \mapsto gh^{-1}$ This is cts, inverse image $\phi^{-1}(\{e\}) = \{(g,g) : g \in G\}$, which is closed $\Longleftrightarrow$ Hausdorff.

is closed.

Let G be a topological group, $N \trianglelefteq G$.

G/N is the quotient group, $\phi_N : G \to G/N$ $\quad \phi_N(g) = \cancel{gN}$ gN.

Give G/N the quotient topology, in which $A \subseteq G/N$ is open $\iff$ $\phi_N^{-1}[A]$ is open in G. Guarantees ϕ_N is continuous.

<u>Claim:</u> ϕ_N is open map.

<u>Proof:</u> Let $U \subseteq G$ be open. Then $\phi_N[U] = \{uN : u \in U\}$.

Then $\phi_N^{-1}\left[\phi_N[U]\right] = UN$. UN is open because

$UN = \bigcup_{n \in N} Un$ is the union of open sets.

<u>Goal:</u> $(gN, hN) \mapsto (gN)(hN)^{-1} = gh^{-1}N$ is cts.

$\phi_N : G \to G/N$ is continuous, open, surjective

So $\phi_N^2 : G \times G \to \frac{G}{N} \times \frac{G}{N}$ is surjective, cts, open.

$$\begin{tikzcd}
(g,h) \arrow[r, "\text{cts}"] \arrow[d, "\phi_N^2"', "\substack{\text{cts}\\ \text{open}\\ \text{surj.}}"] & gh^{-1} \arrow[d, "\phi_N \ \text{cts, open, surjective}"] \\
(gN, hN) \arrow[r] & (gh^{-1}N)
\end{tikzcd}$$

this map is guaranteed to be cts by the diagram.

Convention: Groups are topological and abelian, with $(+, -, 0)$

Recall: Group G is Hausdorff iff $\{0\}$ is closed.

Let G be a topological group, $H =$ intersection of all open sets U containing zero.

Claim 1: $H \leq G$.

H is nonempty, b/c $0 \in H$. The map $g \mapsto -g$ is a Homeomorphism, so $g \in H \Rightarrow -g \in H$.

Let $g_1, g_2 \in H$. ~~Let~~ Let U contain $0 = 0+0$. $+$ is continuous, so there is an open set $V \ni (0,0)$ such that $\forall (a,b) \in V$, $a+b \in U$. Then there is a basic open set $V_1 \times V_2$ containing $(0,0)$. Then $g_1 \in V_1$ and $g_2 \in V_2$ so $g_1 + g_2 \in U$. for all U.

Claim 2: $H = \overline{\{0\}}$

Proof: For each $h \in G$, consider $\phi: g \mapsto h - g$. This is a homeomorphism of G. $h \in H \Leftrightarrow h$ is in every open nbhd of 0 $\Leftrightarrow$ 0 is in every open nbhd of h $\Leftrightarrow h \in \overline{\{0\}}$.

Claim 3: G/H is Hausdorff.

Proof: ~~$\{0\}$~~ $\{0+H\}$ closed in G/H b/c $\overline{\{0\}}$ closed in G.

Claim 4: G is Hausdorff iff H is trivial group.

Proof: Easy.

Assume G is first countable.

Assume G is first countable. (every $x \in G$ has a countable nbhd basis)

<u>Defn:</u> Let $(g_n)_{n \in \mathbb{N}}$ be a sequence in G, a topogroup.

(1) $g_n \longrightarrow g$ iff $\forall$ open $U \ni g$ $\exists N$ $\forall n \geq N$ $g_n \in U$.

(2) (g_n) Cauchy iff $\forall$ open $U \ni 0$, $\exists N$ $\forall m, n \geq N$ $g_m - g_n \in U$.

<u>Exercise:</u> Convergent $\Longrightarrow$ Cauchy

Let $(g_n), (g_n')$ be Cauchy sequences.

$(g_n) \sim (g_n')$ iff $g_n - g_n' \longrightarrow 0$

~~Defn~~ Let $g \in G$, $\phi(g)$ = class of (g_n), $g_n = g$ $\forall n$.

Let $\hat{G}$ be the set of equivalence classes of Cauchy Sequences.

$\phi : G \to \hat{G}$ is a HM with $\ker(\phi) = H = \{0\}$

$\hat{G}$ is complete, which needs 1^{st} countable to prove.

<u>Specialize to following case:</u>

Assume there exists a decreasing sequence of subgroups

$G_0 \geq G_1 \geq G_2 \geq \cdots$

such that the G_i form a nbhd basis for 0.

<u>Note:</u> $U \subseteq G$ is open iff $\forall g \in U$ $\exists n$, $g + G_n \subseteq U$.

For each $n \in \mathbb{N}$, G_n is open. But G_n is also closed.
(If H is open, $H \leq G$, $G \setminus H$ is union of cosets of H, each also closed).

G is Hausdorff iff $\bigcap_{n=0}^{\infty} G_n = \{0\}$. gives intersection of open sets containing zero is $\overline{\{0\}} = \{0\}$, so Hausdorff.

<u>Example:</u> $G = \mathbb{Z}$ $G_n = p^n \mathbb{Z}$, p prime.

Consider $\frac{G}{G_n}$. It has the discrete topology, B/C $\{0\}$ open so under homeomorphism $\{g + G_n\}$ is open $\forall g \in G$.

What is $\hat{G}$ in this case? (The completion of G).

A sequence is Cauchy iff $\forall n$, $(g_i + G_n)$ is eventually constant for large i.

$$\begin{tikzcd}
\frac{G}{G_0} & \frac{G}{G_1} \arrow[l] & \frac{G}{G_2} \arrow[l] & \frac{G}{G_3} \arrow[l] & \cdots \arrow[l] \\
& & (\text{Limit?}) \arrow[ull, dashed] \arrow[ul, dashed] \arrow[u, dashed] \arrow[ur, dashed] &
\end{tikzcd}$$

G an abelian topological group $(G_n)_{n\in\mathbb{N}}$ $G_n \geq G_{n+1}$

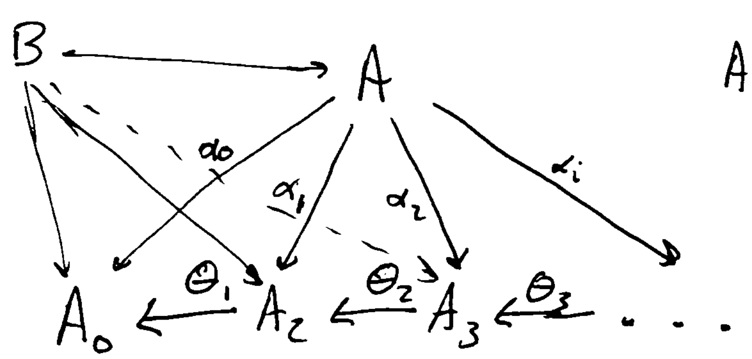
U open $\Leftrightarrow$ $\forall g \in U \ \exists n \quad g + G_n \subseteq U$.

Inverse System of Groups

$$A_0 \xleftarrow{\theta_1} A_1 \xleftarrow{\theta_2} A_2 \xleftarrow{\theta_3} \dots$$

A_i abelian group, θ_i HMs.

System is **surjective** iff θ_i surjective for all i



A cone over (A_n, θ_{n+1}) is $(A, (\alpha_n)_{n\in\mathbb{N}})$

$\alpha_n : A \to A_n$ such that

$\alpha_n = \theta_{n+1} \circ \alpha_{n+1}$

Limits are terminal cones

If B is a limit, there is unique arrow $B \xrightarrow{\Phi} A$ such that everything commutes $\beta_i = \alpha_i \circ \phi$

Every inverse sequence (A_n, θ_{n+1}) has a limit, called the inverse limit.

Elements are sequences $(a_n)_{n\in\mathbb{N}}$ with $a_n \in A_n$, $\theta_{n+1}(a_{n+1}) = a_n$ for all n.

Operation is pointwise $+$, α_i is projection to ith coordinate

This is called the inverse limit of (A_n, θ_{n+1}), denoted

$$\varprojlim (A_n, \theta_{n+1})_{n\in\mathbb{N}} \leq \prod_{n\in\mathbb{N}} A_n$$

In fact, $\varprojlim A_n$ is the kernel of a map $d^{(A_n, \theta_{n+1})}$ from

$$\prod_{n\in\mathbb{N}} A_n \longrightarrow \prod_{n\in\mathbb{N}} A_n \qquad d: (a_n)_{n\in\mathbb{N}} \longmapsto (a_n - \theta_{n+1}(a_{n+1}))_{n\in\mathbb{N}} .$$

Make the collection of inverse systems into a category by an arrow

$$\begin{tikzcd}
A_0 \arrow[d, "\phi_0"'] & A_1 \arrow[l, "\theta_1"'] \arrow[d, "\phi_1"'] & A_2 \arrow[l, "\theta_2"'] \arrow[d, "\phi_2"'] & \cdots \arrow[l] \\
A_0' & A_1' \arrow[l, "\theta_1'"'] & A_2' \arrow[l, "\theta_2'"'] & \cdots \arrow[l]
\end{tikzcd}$$

the map from (A_n, θ_{n+1}) to (A_n', θ_{n+1}') is a collection $(\phi_n : A_n \to A_n')$ such that everything commutes

$$\phi_n \circ \theta_{n+1} = \theta_{n+1}' \circ \phi_{n+1}$$

The inverse limit for the (A_n', θ_{n+1}') is

$$\begin{tikzcd}
 & \varprojlim (A_n, \theta_{n+1}) \arrow[dl] \arrow[d] \arrow[dr] \arrow[drr, bend left] & & \\
A_0 \arrow[d, "f_0"] & A_1 \arrow[l, "\theta_1"'] \arrow[d, "f_1"] & A_2 \arrow[l, "\theta_2"'] \arrow[d, "f_2"] & \cdots \arrow[l] \quad \varprojlim (A_n', \theta_{n+1}') \arrow[dlll, bend right] \arrow[dll, bend right] \arrow[dl] \\
A_0' & A_1' \arrow[l, "\theta_1'"'] & A_2 \arrow[l, "\theta_2'"'] & \cdots \arrow[l]
\end{tikzcd}$$

$\varprojlim (f_n)$ is the map which takes $(a_n) \in \varprojlim (A_n, \theta_{n+1})$ to $(f_n(a_n)) \in \varprojlim A_n'$

Zero element in category of inverse systems,

0 is $0 \xleftarrow{0} 0 \xleftarrow{0} 0 \leftarrow \cdots$

A short exact sequence $0 \to (A_n) \to (B_n) \to (C_n) \to 0$ has the form

$$\begin{tikzcd}
0 \arrow[d] & 0 \arrow[l] \arrow[d] & 0 \arrow[l] \arrow[d] & \cdots \arrow[l] \\
A_0 \arrow[d] & A_1 \arrow[l] \arrow[d] & A_2 \arrow[l] \arrow[d] & \cdots \arrow[l] \\
B_0 \arrow[d] & B_1 \arrow[l] \arrow[d] & B_2 \arrow[l] \arrow[d] & \cdots \arrow[l] \\
C_0 \arrow[d] & C_1 \arrow[l] \arrow[d] & C_2 \arrow[l] \arrow[d] & \cdots \arrow[l] \\
0 & 0 \arrow[l] & 0 \arrow[l] & \cdots \arrow[l]
\end{tikzcd}$$

Columns are short exact sequences of groups

In general is $0 \to \varprojlim A_n \to \varprojlim B_n \to \varprojlim C_n \to 0$ exact? Not in general, but under certain circumstances.

Consider the sequence $0 \to \prod A_n \to \prod B_n \to \prod C_n \to 0$

It is an exact sequence. Consider the map of SES

$$\begin{tikzcd}
0 \arrow[r] \arrow[d, "d^{(0)}"] & \prod A_n \arrow[r] \arrow[d, "d^{(A_n)}"] & \prod B_n \arrow[r] \arrow[d, "d^{(B_n)}"] & \prod C_n \arrow[r] \arrow[d, "d^{(C_n)}"] & 0 \arrow[d, "d^{(0)}"] \\
0 \arrow[r] & \prod A_n \arrow[r] & \prod B_n \arrow[r] & \prod C_n \arrow[r] & 0
\end{tikzcd}$$

General Fact: Exact sequences along rows

$$\begin{array}{ccccccccc} 0 & \to & A & \to & B & \to & C & \to & 0 \\ \downarrow 0 & & \downarrow \alpha & & \downarrow \beta & & \downarrow \gamma & & \downarrow 0 \\ 0 & \to & A' & \to & B' & \to & C' & \to & 0 \end{array}$$

gives exact sequence

$$0 \to \ker(\alpha) \to \ker(\beta) \to \ker(\gamma) \to \operatorname{coker}(\alpha)$$
$$\to \operatorname{coker}(\beta) \to \operatorname{coker}(\gamma) \to 0$$

Applying general fact gives

$$\begin{array}{ccccccccc} 0 & \to & \ker(d^{(A_n)}) & \to & \ker(d^{(B_n)}) & \to & \ker(d^{(C_n)}) & \to & \operatorname{coker}(d^{(A_n)}) \\ & & \| & & \| & & \| & & \\ 0 & \to & \varprojlim (A_n) & \to & \varprojlim (B_n) & \to & \varprojlim (C_n) & \to & ? \end{array}$$

For the sequence $0 \to \varprojlim (A_n) \to \varprojlim (B_n) \to \varprojlim (C_n) \to 0$ to be exact, it is necessary and sufficient for $\operatorname{coker}(d^{(A_n)}) = 0$, that is, $d^{(A_n)}$ is a surjective map from $\prod(A_n) \to \prod(A_n)$.

If then (A_n, θ_{n+1}) system has θ_{n+1} surjective for all n, that is, the inverse system (A_n, θ_{n+1}) is surjective, then $d^{(A_n)}$ is surjective and the sequence exact.

Recall: if we induce a ~~sequence on~~ topology on G by $(G_n)_{n \in \mathbb{N}}$, $G_n \supseteq G_{n+1}$, then G_i is Cauchy iff $\forall n$ $(g_i + G_n)$ is eventually constant.

Consider the surjective inverse system

$$\frac{G}{G_0} \xleftarrow{\theta_1} \frac{G}{G_1} \xleftarrow{\theta_2} \frac{G}{G_2} \xleftarrow{\theta_3} \cdots$$

$$\theta_{n+1} : \frac{G}{G_{n+1}} \longrightarrow \frac{G}{G_n} \qquad \theta_{n+1} : g + G_{n+1} \longmapsto g + G_n .$$

θ_n is surjective. If $\hat{G}$ is the completion wrt Cauchy seqs, then $\hat{G} \cong \varprojlim \left(\frac{G}{G_n}, \theta_{n+1} \right)$

$$\begin{tikzcd} g \in G^* \arrow[r] \arrow[dr, bend right] & {[(g, g, \ldots)]} \in \hat{G} \\ & (g+G_0, g+G_1, \ldots) \in \varprojlim \frac{G}{G_n} . \end{tikzcd}$$

11/18/13

<u>Recall</u>: G an abelian group $G = G_0 \geq G_1 \geq G_2 \geq \ldots$

Topology on G given by U open in G iff $\forall g \in U, \exists n, g + G_n \subseteq U$

$$\begin{tikzcd} & & \hat{G} \arrow[dll, bend right] \arrow[dl] \arrow[d, bend left] \arrow[dr, bend left] & \\ \frac{G}{G_0} & \frac{G}{G_1} \arrow[l] & \frac{G}{G_2} \arrow[l] & \cdots \arrow[l] \end{tikzcd}$$

$$\hat{G} = \left\{ (h_i)_{i \in \mathbb{N}} : h_i \in \frac{G}{G_i} \text{ and } h_{i+1} \mapsto h_i \text{ for all } i \right\}$$

Consider $H \leq G$ and G/H. Gives exact sequence

$$0 \to H \to G \to G/H \to 0 .$$

Topologize H by using $(G_i \cap H)$ as a sequence, as with G.

By results from last time, and exactness of

$$0 \to A_n \to B_n \to C_n \to 0 \qquad A_n = \frac{H}{H \cap G_n} \quad B_n = \frac{G}{G_n}$$

$$C_n = \frac{G/H}{(G_n + H)/H}$$

This gives an exact sequence $0 \to \hat{H} \to \hat{G} \to \widehat{G/H} \to 0.$

which shows $\widehat{G/H} \cong \dfrac{\hat{G}}{\hat{H}}$

Special Case: $H = G_n$

$$\widehat{G/G_n} \cong \hat{G}/\widehat{G_n}$$

Recall that G/G_n is discrete, so that $\widehat{G/G_n} = G/G_n$. The completion is the same.

So now we topologize $\hat{G}$ by using the sequence of $(\widehat{G_n})_{n \in \mathbb{N}}$. So $\hat{\hat{G}} = \varprojlim \dfrac{\hat{G}}{\widehat{G_n}} = \varprojlim \dfrac{G}{G_n} = \hat{G}$.

[A bit of dishonesty here, because this should in principle be a giant diagram chase].

So now we do this for rings + modules.

Key Idea: R is a ring, I an ideal of R, $I^n \leq (R, +)$, $I^0 = R$.

The I-adic topology on R is generated by $(I^n)_{n \in \mathbb{N}}$

Form as a group $\hat{R} = \varprojlim \dfrac{R}{I^n}$

$(\hat{R},+) = \varprojlim \frac{R}{I^n}$ s as an abelian group.

<u>Goal:</u> Make $\hat{R}$ into a topological ring.

Certainly, R is already a topological ring w/ topology given by the sequence $(I_n)_{n\in\mathbb{N}}$.

Let M be an R-module. Topologize M via $(I^n M)_{n\in\mathbb{N}}$. Form $\hat{M} = \varprojlim \frac{M}{I^n M}$. $\hat{M}$ makes sense as an R-module, but $\hat{M}$ is actually an $\hat{R}$-module. This construction is a **functor**, from R-mod to $\hat{R}$-mod.

Is the functor exact? Not always. How ~~exact~~ is it?

<u>Defn:</u> Let M be an R-module.

(1) A <u>filtration</u> of M is a sequence $(M_n)_{n\in\mathbb{N}}$ such that $M_0 = M$, $M_n \leq M$, $M_{n+1} \leq M_n$.

(2) If I is an ideal of R, an <u>I-filtration</u> is a <u>filtration</u> (M_n) such that $IM_n \subseteq M_{n+1}$

(3) A <u>stable</u> <u>I-filtration</u> is an I-filtration (M_n) such that for some n_0, $IM_n = M_{n+1}$ for $n \geq n_0$

(4) Two <u>filtrations</u> (M_n), (M_n') of M have <u>bounded difference</u> if there is t such that $\forall n$, $M_n \supseteq M'_{n+t}$ and $M_n' \supseteq M_{n+t}$

<u>Remarks:</u> If (M_n) and (M_n') have bounded difference, they generate the same topology.

Bounded Difference is an equivalence relation on filtrations.

<u>Lemma:</u> Any two stable I-filtrations of M have bounded difference. In particular, any stable I-filtration gives the same topology as $(I^n M)_{n \in \mathbb{N}}$.

<u>Motivation:</u>

Consider exact sequence $0 \to M_1 \to M_2 \to \frac{M_2}{M_1} \to 0$. Form I-adic completion. In general, the I-adic topology on M_1 may not be equal to the subspace topology of the I-adic topology on M_2. Want to see when they are the same.

<u>Proof of Lemma:</u> $M_0 = M$ so $I^n M = I^n M_0 \subseteq M_n$ since (M_n) is an I-filtration.

Since bdd diff is equivalence relation, suffices to show that (M_n), $(I^n M)$ have bounded difference. Let M_n be stable.

Fix n_0 such that $M_{n+1} = I M_n$ for $n \geq 0$.

Then $M_{n_0+t} = I^t M_{n_0} \subseteq \cancel{M} \; I^t M$.

Hence bdd diff. $\blacksquare$

<u>Defn</u>: A <u>graded Ring</u> is a ring A equipped with a sequence $(A_n)_{n \in \mathbb{N}}$, $A_n \leq (A,+)$, $A \cong \bigoplus_n A_n$ as groups.
$A_s A_t \subseteq A_{s+t}$.

Elements of A_s are called <u>homogeneous of degree s</u>.

<u>Example</u>: Let $A = k[x_1, \dots, x_n]$
$A_s = \{\text{homogeneous polynomials of degree } s\}$
all terms w/ same degree.

Each A_t is an A_0 module.

<u>Defn</u>: A <u>graded module</u> M over graded ring A is module M with a sequence $(M_n)_{n \in \mathbb{N}}$, $M = \bigoplus_n M_n$, such that
$A_s M_t \subseteq M_{s+t}$.

If A is graded, $A_+ = \bigoplus_{i>0} A_i$ is an ideal of A, and
$\frac{A}{A^+} \cong A_0$

<u>Theorem:</u> TFAE for A a graded ring.
(1) A Noetherian
(2) A_0 Noetherian and $A = A_0[b_1, b_2, \dots, b_n]$ $b_i \in A$

A is fg as A_0-algebra.

Proof: ~~(1) ⟹ (2)~~.

(2) ⟹ (1) Basissatz, A_0 Noetherian

(1) ⟹ (2) A_0 is Noetherian and A^+ is an ideal of A, A^+ is fg, fix $b_1 \dots b_n \in A^+$ generators. Then $A = A_0[b_1, b_2 \dots b_n]$.

11/20/13

$$0 \to G \to G' \to G'' \to 0$$

Topologize G' via $(G'_n)_{n \in \mathbb{N}}$, induce topology via maps

$$0 \to \hat{G} \to \hat{G'} \to \hat{G''} \to 0$$

The above Induces exact sequence of completions

But if $0 \to M \to M' \to M'' \to 0$, then I-adic topology on M' via $(I^n M)$ does induce I-adic topology on M'', maybe not on M.

Theorem: A graded, Noetherian ⟹ $A = A_0[b_1, \dots, b_n]$, $b_1 \dots b_n \in A$ "finitely generated A_0-algebra"

Proof: $A^+ = \bigoplus_{i>0} A_i$ is an ideal, A^+ is fg as an A-module, by Noetherian hypothesis. Choose $b_1, \dots, b_n \in A^+$ generating A^+ as an A-module; $A^+ = (b_1, b_2, \dots, b_n)$. Show by induction on t that $A_t \subseteq A_0[b_1, \dots, b_n]$. Also WLOG, $b_i \in A_{k_i}$ $k_i > 0$, (break up sums).

$t = 0$ is easy. If $t > 0$, let $y \in A_t$, $y \in A^+$. So $y = \sum_{i=1}^{n} \lambda_i b_i$, $\lambda_i \in A$. By graded property, $\lambda_i \in A_{t-k_i}$. By induction, $\lambda_i \in A_0[b_1 \dots b_n]$. ∎

Goal: (Artin-Rees Lemma) I an ideal of R

Let R be Noetherian, Let M' be an fg R-module, and let $M \leq M'$. Let (M'_n) be a stable I-filtration of M'. Then $(M \cap M'_n)$ is a stable I-filtration of M.

Corollary: Subspace topology induced on M by I-topology on M' is the I-adic topology on M.

Corollary: If $0 \to M_1 \to M_2 \to M_3 \to 0$ exact seq. of fg R-modules, I an ideal of R, R Noetherian.

Then $0 \to \hat{M}_1 \to \hat{M}_2 \to \hat{M}_3 \to 0$ is exact.

I-adic completions

Defn: Let R be a ring, I an ideal.

R^* is the graded ring with group $(R^*, +) = \bigoplus_{n \in \mathbb{N}} I^n$, $I^0 = R$.

This is made into a ring by

$$\left(\sum_{i=0}^{\infty} a_i\right)\left(\sum_{j=0}^{\infty} b_i\right) = \sum_{k=0}^{\infty}\left(\sum_{i,j:i+j=k} a_i b_j\right).$$

Let (M_n) be an I-filtration of R. Then

$(M^*, +) = \bigoplus_{n \in \mathbb{N}} M_n$. Make M^* into a graded R^* module

using $I^s M_t \subseteq M_{s+t}$ $\left(\sum_{i=0}^{\infty} r_i\right)\left(\sum_{j=0}^{\infty} m_j\right) = \sum_k \sum_{i+j=k} r_i m_j$.

__Theorem:__ Let R be a Noetherian ring, let M be an fg R-module. Let (M_n) be an I-filtration of M. Then TFAE

(1) (M_n) is stable

(2) M^* is an fg R^*-module

__Note:__ If R is Noetherian, then R^* is Noetherian because $R^* = R[b_0 \dots b_n]$ with $I = (b_0, \dots, b_n)$.

__Proof:__ Note that M and each M_n are finitely generated and Noetherian. Given n_0, define Q_{n_0} an R^*-submodule of M^*

$$Q_{n_0} = M_0 \oplus \dots \oplus M_{n_0} \oplus I M_{n_0} \oplus I^2 M_{n_0} \oplus \dots$$

__Verify:__

(1) $Q_{n_0} \leq M^*$ as an R^*-module

(2) As each M_i, $i \leq n_0$ is fg R-module, Q_{n_0} is a fg R^*-module.

(3) $M^* = \bigcup_{n \in \mathbb{N}} Q_n$

$$\begin{tikzcd}
(M_n) \text{ is stable} \arrow[r, Leftrightarrow] & \boxed{\exists\, n_0,\ M^* = Q_{n_0}} \arrow[r, Rightarrow] & \boxed{M^* \text{ is fg}} \arrow[d, Rightarrow, "(R^* \text{ N'ian})"] \\
& \boxed{\text{Sequence } (Q_n) \text{ is eventually stable (constant)}} \arrow[u, Rightarrow] & \boxed{M^* \text{ N'ian } R^*\text{-module}} \arrow[l, Rightarrow]
\end{tikzcd}$$

<u>Proof of Artin-Rees Lemma:</u> $M \leq M'$, (M_n') stable filtration of M'

$I(M_n' \cap M) \subseteq M_{n+1}' \cap M$, so $(M_n' \cap M)$ is an I-filtration of M

Form $(M')^*$ and M^*.

$M^* \leq (M')^*$ as an R^*-module.

(M_n') stable $\Rightarrow (M')^*$ fg $\Rightarrow M^*$ fg $\Rightarrow (M_n)$ stable. ■

[R^* N'ian so fg R^*-mod are N'ian]

<u>Next Goal:</u> R Noetherian, I an ideal $\Rightarrow \hat{R}$ Noetherian.

Let R be a ring, I an ideal. For each $M \in R$-mod, there is a natural map $\phi: \hat{R} \otimes_R M \to \hat{M}$.

Map $R \to \hat{R}$ given by $r \mapsto (r + I^n)$ (or $r \mapsto [(r, r, \ldots)]$.)
This makes $\hat{R}$ into an R-algebra.

$\hat{R} \otimes_R M$ is an $\hat{R}$-module, so is $\hat{M}$. The natural map is some sort of $\hat{R}$-module homomorphism.

$(r_n \in I^n) \in \hat{R}$, $m \in M$ goes to $(r_n m + I^n M) \in \hat{M}$

$\phi(r_n + I^n, m) = (r_n m + I^n M)$

Let R be a ring, I an ideal, M an R-module

Theorem:

(1) If M is fg the map $\hat{R} \otimes_R M \to \hat{M}$ is surjective.

(2) If M is fg and R is Noetherian, $\hat{R} \otimes_R M \to \hat{M}$ is an isomorphism of $\hat{R}$-modules.

Proof:

(1) Special Case: M is free of rank t, that is, $\cancel{\hat{R} \otimes R^t}$
$M \cong R^t$ as an R-module. $\hat{M} \cong (\hat{R})^t$.

If M is generated by t generators, then $M \cong F/N$ where F is free of rank t, and N is a submodule.

$$0 \to N \to F \to M \to 0.$$

$$\boxed{\hat{R} \otimes R^t \cong (\hat{R} \otimes R)^t \cong \hat{R}^t}$$

- Tensoring w/ $\hat{R}$ induces an exact sequence

$$\begin{tikzcd}
 & \hat{R} \otimes N \arrow[r] \arrow[d] & \hat{R} \otimes F \arrow[r] \arrow[d, "\wr"] & \hat{R} \otimes M \arrow[r] \arrow[d] & 0 \arrow[d] \\
0 \arrow[r] & \hat{N} \arrow[r] & \hat{F} \arrow[r, two heads] & \hat{M} \arrow[r] & 0
\end{tikzcd}$$

exact

may not be exact in general, given by I-adic completion being functorial. (I think...)

exact by boring and brute force calculation / diagram chase

11/22/13

Consider the natural map $\hat{R} \otimes_R M \longrightarrow \hat{M}$.

If F is free of rank $n < \infty$, $\hat{R} \otimes F \cong \hat{F}$.

If M is finitely generated, M is a quotient of some F.
$M = F/N$

$$0 \longrightarrow N \longrightarrow F \longrightarrow M \longrightarrow 0$$

$$\begin{tikzcd}
& \hat{R} \otimes N \arrow[r] \arrow[d] & \hat{R} \otimes F \arrow[r] \arrow[d, "\wr"] & \hat{R} \otimes M \arrow[r] \arrow[d] & 0 & \text{exact} \\
0 \arrow[r] & \hat{N} \arrow[r] & \hat{F} \arrow[r, two heads] & \hat{M} \arrow[r] & 0 & \text{Not necessarily exact}
\end{tikzcd}$$

$\longleftarrow$ conclude this map surjective

$\uparrow$ exact here

If we add the assumption that R is N'ian, then F is N'ian and so N is fg. so the map $\hat{R} \otimes N \twoheadrightarrow \hat{N}$ is surjective. Under this assumption, the bottom row of the above diagram is now exact

$$\begin{tikzcd}
& \hat{R} \otimes N \arrow[r] \arrow[d, two heads] & \hat{R} \otimes F \arrow[r] \arrow[d, "\wr"] & \hat{R} \otimes M \arrow[r] \arrow[d, two heads] & 0 & \text{exact} \\
0 \arrow[r] & \hat{N} \arrow[r, hook] & \hat{F} \arrow[r, two heads] & \hat{M} \arrow[r] & 0 & \text{exact}
\end{tikzcd}$$

From now on, R is Noetherian, I an ideal, $\hat{R}$ is I-adic completion.

(a) I fg, as an R-module, so $\hat{I} \cong \hat{R} \otimes I$, and in fact $\hat{I} = I^e$ wrt $R \to \hat{R}$.

(b) I^n fg R-module, so $\widehat{I^n} = (I^n)^e = (I^e)^n = (\hat{I})^n$

Two natural ways to complete $\hat{R}$: $\hat{I}$-adic topology or topology induced by sequence of $(I^n)^e$ and $R \to \hat{R}$. These are the same by (b). In particular, $\hat{R}$ is complete in $\hat{I}$-adic topology.

(c) $\dfrac{R}{I^n} \cong \dfrac{\hat{R}}{(\hat{I})^n}$, so $\dfrac{I^n}{I^{n+1}} \cong \dfrac{\hat{I}^n}{\hat{I}^{n+1}}$

(d) For all $a \in I$, $1+a+a^2+a^3+\dots = (1, 1+a, 1+a+a^2, 1+a+a^2+a^3, \dots)$
This converges to an inverse for $1-a$, which is a unit in the I-adic topology on $\hat{R}$. So $I^e = \hat{I} \subseteq \mathrm{Jac}(\hat{R})$.

In particular, if R is a Noetherian Local ring w/ unique max'l ideal M, and we complete wrt the M-adic topology, then
$\dfrac{\hat{R}}{\hat{M}} \cong \dfrac{R}{M} \leftarrow$ is a field! $\hat{M}$ is maximal in $\hat{R}$. By (d) also
$\hat{M} \subseteq \mathrm{Jac}(\hat{R}) \implies \hat{M} = \mathrm{Jac}(\hat{R})$, so $\hat{R}$ is local with unique maximal ideal $\hat{M}$.

Intuition: How far $\hat{R}$ is from Hausdorff. If $\bigcap_n I^n M = 0$, then Hausdorff.

<u>Krull's Theorem:</u> Let R be a Noetherian ring, let I be an ideal of R, let M be a fg module. Then the kernel of the map $\phi: M \longrightarrow \hat{M}$ $\left(= \bigcap_{n \in \mathbb{N}} I^n M\right)$ is

$$\ker(\phi) = \{ m \in M : \exists a \in I \ \ (1+a)m = 0 \}.$$

<u>Proof:</u> $(\supseteq)$ Let $b = -a \in I$, let $(1+a)m = (1-b)m = 0$, so $mb = m$. So $m = b^n m \in I^n M$ for all $n \in \mathbb{N}$.

$(\subseteq)$ Let $E = \bigcap_{n \in \mathbb{N}} I^n M \leq M$. M is Noetherian, so E is fg. The subspace topology is the indiscrete topology given by $\tau = \{E, \emptyset\}$.

By Artin-Rees, the subspace topology is the same as the subspace topology on E. IE is open, and $IE \neq \emptyset$, so $IE = E$.

By the preamble to Nakayama, we find $\alpha \in I$ such that $(1+\alpha)E = 0$, ~~so if $\phi(m) = 0$, then~~ $\blacksquare$

<u>Corollary:</u> If R is a Noetherian domain, I an ideal of R, proper, then $\bigcap_{n \in \mathbb{N}} I^n = 0$ (So I-adic topology on R is Hausdorff).
[View R as an fg module over itself]

<u>Corollary:</u> If R is aN'ian ring, and $I \subseteq \mathrm{Jac}(R)$, then $\bigcap I^n = 0$.

Associated Graded Ring:

<u>Defn:</u> R a ring, I an ideal, M an R-module, (M_n) I-filtration ~~filtration~~ of M. The <u>Associated Graded Ring</u> of R is

$$G_I(R) = \bigoplus_{n \in \mathbb{N}} \frac{I^n}{I^{n+1}}$$, made into a graded ring in the usual way.

Similarly

$$G(M) = \bigoplus_{n \in \mathbb{N}} \frac{M^n}{M^{n+1}}$$ $G(M)$ is a $G_I(R)$-module.

<u>Lemma:</u> Let R be Noetherian, I an ideal of R, M an fg R-module, (M_n) a filtration. Then

(a) $G_I(R)$ is Noetherian

(b) $G_I(R) \cong G_{\hat{I}}(\hat{R})$

(c) If (M_n) is stable I-filtration, then $G(M)$ is a fg $G_I(R)$-module

<u>Proof (sketch):</u>

(a) fix $b_1, \ldots, b_n$ generators for I as an R-module.
Verify that $\{b_i + I^2\}$ generate $G_I(R)$ in the sense that $G_I(R) = \frac{R}{I}[b_1 + I^2, \ldots, b_n + I^2]$

(b) $\frac{\hat{I}^n}{\hat{I}^{n+1}} \cong \frac{I^n}{I^{n+1}}$ as earlier.

(c) Let $M_{n+1} = IM_n$ $n \geq n_0$ (stability pt.). For each $i \leq n_0$, fix a generating set Y_n for M_n as an R-module. Then verify that

$$\bigcup_{i \leq n_0} (Y_i + M_{i+1})$$ generates $G(M)$.

Defn: A ~~filtered~~ R-module is an R-module M together with filtration (M_n). (resp. I-filtration).

If M, N are filtered R-modules, then a HM of filtered R-modules is $\phi: M \to N$ an R-mod HM such that

$$\phi[M_n] \subseteq N_n$$

ϕ will be continuous, so ϕ induces $\hat{\phi}: \hat{M} \to \hat{N}$

Verify ϕ induces a map $G(\phi): G(M) \to G(N)$

Goal: If R is N'ian and I an ideal, I-adic completion $\hat{R}$ is also N'ian.

11/25/13

Remark: $\hat{R}$ is Hausdorff in $\hat{I}$-adic topology.

Proof: Let (g_n) be a cauchy sequence representing an element of $\bigcap_{n \in \mathbb{N}} \hat{I}^n$. Enough to show $\bigcap_{n \in \mathbb{N}} \hat{I}^n = 0$.

$\bigcap_{n \in \mathbb{N}} \hat{I}^n = \bigcap_{n \in \mathbb{N}} \widehat{I^n}$. For each n, $g_i \in I^n$ for large i, so $g_i \to 0$

Hence, $\bigcap_{n \in \mathbb{N}} \hat{I}^n = 0$. ∎

Category of filtered groups.

Morphism of filtered groups. $A \quad (A_n) \quad \phi[A_n] \subseteq B_n$
$$\begin{array}{ll} A & (A_n) \\ \downarrow \phi & \\ B & (B_n) \end{array}$$

$$G(A) = \bigoplus_n \frac{A_n}{A_{n+1}} \qquad G(\phi): G(A) \to G(B)$$

$$\hat{A} = \varprojlim \left(\frac{A}{A_0} \leftarrow \frac{A}{A_1} \leftarrow \frac{A}{A_2} \leftarrow \cdots \right)$$

$\hat{\phi}: \hat{A} \to \hat{B}$ induced by ϕ.

<u>Lemma:</u> $G(\phi)$ surjective $\Longrightarrow$ $\hat{\phi}$ surjective
$G(\phi)$ injective $\Longrightarrow$ $\hat{\phi}$ injective.

<u>Proof:</u> Have an exact sequence

$$\begin{tikzcd} 0 \arrow[r] & \frac{A_n}{A_{n+1}} \arrow[r] \arrow[d, "\beta_n"] & \frac{A}{A_{n+1}} \arrow[r] \arrow[d, "\alpha_{n+1}"] & \frac{A}{A_n} \arrow[r] \arrow[d, "\alpha_n"] & 0 \\ 0 \arrow[r] & \frac{B_n}{B_{n+1}} \arrow[r] & \frac{B}{B_{n+1}} \arrow[r] & \frac{B}{B_n} \arrow[r] & 0 \end{tikzcd}$$

exact
induced by ϕ.
exact

β_n are components of $G(\phi)$
α_n are maps between things in inverse limits (or something)

"By the usual crap, we get long exact sequence"

$$0 \to \ker(\beta_n) \to \ker(\alpha_{n+1}) \to \ker(\alpha_n) \to \mathrm{coker}(\beta_n) \to \mathrm{coker}(\alpha_{n+1}) \to \mathrm{coker}(\alpha_n) \to 0$$

$G(\phi)$ injective $\Longleftrightarrow$ $\forall n$ β_n injective
$\Longleftrightarrow$ $\forall n$ $\ker(\beta_n) = 0$

proceed by induction on n $\ker(\hat{\phi}) = 0$.
similar for surjective.

Lemma: R is a ring, I an ideal, R is complete in I-adic topology. M an R-module, (M_n) an I-filtration of M, M is Hausdorff in (M_n) topology $(\bigcap_n M_n = 0)$

Then (a) $G(M)$ fg as $G_I(R)$-module $\Rightarrow$ M fg in R-mod

(b) $G(M)$ N'ian as $G_I(R)$-module $\Rightarrow$ M N'ian

Proof: Let $b_1, b_2, \ldots b_n$ generate $G(M)$.

WLOG $b_i \in G(M)_{n_i} \leq \dfrac{M_{n_i}}{M_{n_i+1}}$, say $b_i = m_i + M_{n_i+1}$

Let $F = (R^n, +)$, view it as a filtered group with $(\underbrace{I^t \times I^t \times \cdots \times I^t}_{n \text{ times}}, +)$. Define $\phi: R^n \longrightarrow M$

$\phi(r_1, \ldots, r_n) = \sum_i r_i m_i$ ϕ is morphism of filtered grp.

$G(\phi)$ is surjective as the b's generate $G(M)$.

$\hat{\phi}$ surjective, by previous lemma.

$$\begin{tikzcd} F \arrow[r, "\phi"] \arrow[d, "\wr"] & M \arrow[d, hook, "\psi"] \\ \hat{F} \arrow[r, two heads, "\hat{\phi}"] & \hat{M} \end{tikzcd}$$

This diagram commutes. also $\hat{\phi}$ surjective. Furthermore since R is complete, $F \cong \hat{F}$.

$\ker(\psi) = \bigcap_n M_n = 0$, so ψ is injective.

It follows that ϕ is surjective by diagram chase. So M is fg since ϕ surjective, generated by $\{m_i\}$.

For part (b), need to show all $M' \subseteq M$ are fg. Define a filtration $M_n' = M' \cap M_n$, and argue that $G(M') \hookrightarrow G(M)$, so now $G(M)$ is Noetherian $\Longrightarrow G(M')$ fg $\Longrightarrow M'$ fg by part (a), and $\bigcap_n M_n' \subseteq \bigcap_n M_n = 0$ ■

<u>Thm:</u> Let R be Noetherian, I an ideal, $\hat{R}$ the I-adic completion. Then $\hat{R}$ Noetherian.

<u>Proof:</u> $G_I(R) \cong G_{\hat{I}}(\hat{R})$, $\hat{R}$ Hausdorff and complete in $\hat{I}$-adic topology, and $G_I(R)$ is a Noetherian ring. So $G_{\hat{I}}(\hat{R})$ is a Noetherian $G_{\hat{I}}(\hat{R})$-module.

Appeal to last lemma w/ ring $= \hat{R}$, ideal $= \hat{I}$, module $= \hat{R}$, all w/ $\hat{I}$-adic topology. Then by the previous lemma, $\hat{R}$ is an fg $\hat{R}$ module and $\hat{R}$ is Noetherian. ■

<u>Algebraic Geometry</u>:

Let k be an algebraically closed field.

Points $a \in k^n$ correspond to maximal ideals

If P a prime ideal, then $V(P)$ irreducible variety, and in fact $P = \{f : f(a) = 0 \ \forall a \in V(P)\}$.

<u>Field Theory:</u>

Let K be a subfield of L. Let $\alpha_1, \ldots, \alpha_n \in L$. $\{\alpha_i\}$ are algebraically independent over K iff for all $f \in K[x_1, \ldots, x_n]$, $f(\alpha_1, \ldots, \alpha_n) = 0 \Longrightarrow f = 0$.

Given $X \subseteq L$, $cl(X) = \{\beta \in L : \beta \text{ algebraic over } K(X)\}$

<u>Note:</u> For X algebraically independent, X is algebraically independent set iff $cl(X) = L$.

Cardinality of maximal independent set (transcendence basis) is transcendence degree, and it is always the same.

Defn: λ is additive (function R-mod to $\mathbb{Z}$) $\iff$ for all exact $0 \to M_0 \to M_1 \to M_2 \to 0$,
$\lambda(M_0) - \lambda(M_1) + \lambda(M_2) = 0$. If λ additive, then for all exact $0 \to M_0 \to M_1 \to \dots \to M_{n-1} \to 0$,
$\lambda(M_0) - \lambda(M_1) + \dots \pm \lambda(M_{n-1}) = 0$.

If R is Artinian, then all fg modules have finite length.
Length is additive on $\{M : M \text{ an } R\text{-module of finite length}\}$
$\phi : A \to B$ gives exact $0 \to \ker(\phi) \hookrightarrow A \xrightarrow{\phi} B \twoheadrightarrow \operatorname{coker}(\phi) \to 0$.

R is graded + Noetherian $\iff$ R_0 Noetherian, and R fg as R_0-algebra

Assume: R is a graded Noetherian ring and M an fg, graded R-module.

Easy: For each n, M_n is a fg R_0-module

Fix λ an additive function on class of fg R_0-modules.

$$P(M,t) = \sum_{n=0}^{\infty} \lambda(M_n)\, t^n \in \mathbb{Z}[[t]]$$

because ID,

$$P(M,t) = \frac{\text{poly}}{\prod(1-t^{k_i})}$$

Theorem: If $R = R_0[x_1, \dots, x_s]$, $x_i \in R_{k_i}$, then
$\prod_{i=1}^{s} (1-t^{k_i}) P(M,t)$ is a polynomial in t.

Proof: by induction on s

Base Case: $s=0$, $R=R_0$, M fg as R_0-module. Then for large n,
$M_n = 0$, $\Longrightarrow \lambda(M_n)=0$ for large n.

Assume for $s>0$, holds for rings w/ $s-1$ generators.

Given x_s, define the R_0-module HM $\phi_n : M_n \longrightarrow M_{k_s+n}$.

$\phi_n : m \longmapsto x_s m$. Gives sequence

$$0 \longrightarrow \underset{K_n}{\overset{}{\ker(\phi_n)}} \longrightarrow M_n \longrightarrow M_{n+k_s} \longrightarrow \underset{}{\overset{C_{n+k_s}}{\operatorname{coker}(\phi_n)}} \longrightarrow 0.$$

$C_i = 0$ for $i < k_s$. Then $\lambda(K_n) - \lambda(M_n) + \lambda(M_{n+k_s}) - \lambda(C_{n+k_s}) = 0$

Let $K = \oplus K_n$ and $C = \oplus C_n$, both graded R-modules

Multiply the alternating sum λ-thing by t^{n+k_s} and sum

$$P(K,t)\,t^{k_s} - P(M,t)\,t^{k_s} + P(M,t) - P(C,t) + \text{poly} = 0$$

comes from missing 1st k_s terms

$x_s K = x_s(\oplus K_n) = \oplus(x_s K_n) = 0$ kernel of ϕ_n

$x_s C_{n+k_s} = 0$

So K and C can be regarded as an $R[x_1 \dots x_{s-1}]$-module

Apply IH, $P(K,t)$, $P(C,t)$ are polynomials by IH,

get $(1-t^{k_s}) P(M,t) = \text{poly}$. ■

Restrict to special case:

$k_i = 1$ for all i $\qquad P(M,t) = \dfrac{f(t)}{(1-t)^s}$

$\dfrac{g(t)}{(1-t)^d}$ $d \leq s$ and $g(1) \neq 0$, by factoring out common factors in numerator/denominator

Define $d = d(M)$

Claim: In this case, there is a polynomial h of degree $d-1$ such that $\lambda(M_n) = h(n)$ for all large n. $(\deg(0) = -1)$

Proof: Brute force, binomial thm, equate coefficients

Related Calculation. Let $x \in R_k$ for some $k > 0$ and let x be such that $\phi_k : M \to M$, $\phi_k(m) = xm$, is injective. "x is not a zerodivisor of M". Repeat calculation from above for ϕ.

$$0 \to M_n \to M_{n+k} \to \underbrace{\operatorname{coker}(\phi_k)}_{\cong \frac{M_{n+k}}{xM_n}} \to 0$$

$C \cong \dfrac{M}{xM}$ and $d(C) = d(M) - 1$

Specialize Further: R a Noetherian local ring, I the unique maximal ideal, Q is I-primary ideal, M a fg R-module, (M_n) a stable Q-filtration.

$$G_Q(R) = \bigoplus_n \frac{Q^n}{Q^{n+1}} \qquad G_Q(M) = \bigoplus_n \frac{M_n}{M_{n+1}} \qquad Q^0 = R$$

$$G(R)_0 = \frac{R}{Q} \quad \text{is Artinian (Noetherian, dimension zero)}$$

Each $\frac{M_n}{M_{n+1}}$ is a fg. $G(R)_0$-module. Let λ = length function, as R/Q-module

$$P(G_Q(M), t) = \sum_{n=0}^{\infty} \ell\left(\frac{M_n}{M_{n+1}}\right) t^n$$

$$G_Q(R) = G_Q(R)_0 [x_1, \ldots, x_s] \quad \text{where } x_i = b_i + Q^i$$

b_i generate Q as R-module

There is a polynomial h_0 such that for all large n,
$h_0(n) = \ell\left(\frac{M_n}{M_{n+1}}\right) \quad \deg(h_0) \leq s-1.$

Then $\ell\left(\frac{M}{M_n}\right) = \sum_{i<n} \ell\left(\frac{M_i}{M_{i+1}}\right)$, and there is a polynomial h of degree $\deg(h) \leq s$, $\ell\left(\frac{M}{M_n}\right) = h(n)$ for all large n.

(I) **Recall:** R Noetherian, graded and $R = R_0[x_1, \ldots, x_s]$
$x_i \in R_1$ M fg R-module. λ additive on fg R_0-modules

$$P(M,t) = \sum_n \lambda(M_n) t^n = \frac{g(t)}{(1-t)^d} \qquad 0 \le d \le s$$

$\Longrightarrow \exists h$ $\deg(h) = d-1$ and $\forall$ large n $\lambda(M_n) = h(n)$, $d(M) = d$
h is the Hilbert polynomial.

Remark: If $\alpha: M \twoheadrightarrow M'$, $d(M) \geq d(M')$

Remark: If R_0 is Artinian, R is polynomial ring
$R_0[t_1, \ldots, t_s]$, λ is length, $M = R$, then
$P(R,t) = (1-t)^{-s}$ so $d(R) = s$.

(II)

R Noetherian local ring w/ maximal ideal I, Q is I-primary,
Q generated as R module by s elements.

$$G_Q(R) := \bigoplus_{n \in \mathbb{N}} \frac{Q^n}{Q^{n+1}}$$

If M is a fg R-module w/ stable Q-filtration (M_n),
$$G_Q(M) = \bigoplus_{n \in \mathbb{N}} \frac{M_n}{M_{n+1}}$$

Recall: $\exists$ polynomial H $\forall$ large n $H(n) = \ell\left(\frac{M}{M_n}\right)$

$$\ell\left(\frac{M}{M_n}\right) = \sum_{i<n} \ell\left(\frac{M_i}{M_{i+1}}\right) \qquad d(M) = \deg(H) \le s.$$

not graded, but as in I, we take $d(G_Q(M))$ to be $d(M)$

Let $M = R$ and $M_n = Q^n$

χ_Q is polynomial s.t. $\chi_Q(n) = \ell\left(\frac{R}{Q^n}\right)$ for large n.

In the setting of II, let $(\tilde{M}_n)$ be another stable Q-filtration. By Artin-Rees, $(\tilde{M}_n), (M_n)$ have bounded difference

Hence there is n_0 s.t. $H(n) \leq \tilde{H}(n+n_0)$

$\tilde{H}(n) \leq H(n+n_0)$

$\Longrightarrow$ H and $\tilde{H}$ have the same degree, leading term.

So $d(M)$ is independent of the choice of filtration.

Claim $\deg(\chi_Q)$ is independent of choice of Q.

$\sqrt{Q} = I$ and R Noetherian, so for some r $I^r \subseteq Q \subseteq I$.

$\Longrightarrow$ $I^{rn} \subseteq Q^n \subseteq I^n$

$\Longrightarrow$ $\forall$ large n, $\chi_I(rn) \geq \chi_Q(n) \geq \chi_I(n)$

$\Longrightarrow$ $\deg(\chi_Q) = \deg(\chi_I)$

Defn: $d(R) := \deg(\chi_Q)$ for any I-primary Q.

R Noetherian, local:

$\dim(R)$ = supremum of length of chains of prime ideals

$d(R) = \deg(\chi_M)$ $\quad M$ maximal ideal.

$\delta(R)$ = least number of generators (as R-module) of any I-primary ideal.

Dimension Theorem: $\dim(R) = d(R) = \delta(R)$

Proof: $\delta(R) \geq d(R) \geq \dim(R) \geq \delta(R)$

$\delta(R) \geq d(R)$

$d(R) \geq \dim(R)$

Lemma: R N'ian, local, I max'l ideal, Q is I-primary, M fg R-module $(M_n = Q^n M)$ is filtration

Let $a \in R$, a not zerodivisor for M.

Let $N = aM$ $(\cong M$ as R-mod$)$ and $M' = M/N$

$M'_n = Q^n M'$ $\qquad N_n = M_n \cap N = Q^n M \cap N$.

Then: $d(M') \leq d(M) - 1$

Proof: $0 \to N \to M \to M' \to 0$ is exact, induces a diagram

$$0 \to \frac{N}{N_n} \to \frac{M}{M_n} \to \frac{M'}{N'_n} \to 0$$

By additivity, $\ell\left(\frac{N}{N_n}\right) - \ell\left(\frac{M}{M_n}\right) + \ell\left(\frac{M'}{M'_n}\right) = 0$

Since $N \cong M$, so Hilbert polynomials for M, N have same leading term, so $\underbrace{\ell\left(\frac{N}{N_n}\right) - \ell\left(\frac{M}{M_n}\right)}_{\text{lesser degree then } \ell\left(\frac{N}{N_n}\right) \text{ poly}} = -\ell\left(\frac{M'}{M'_n}\right)$ ∎

Corollary: If R is Noetherian and local, $a \in R$ not a zerodivisor

$d\left(\frac{R}{(a)}\right) \leq d(R) - 1$.

Back to proof

$d(R) \geq \dim(R)$.

Proof: by induction on $d = d(R)$.

$d = 0 \Rightarrow \ell\left(\frac{R}{I^n}\right)$ is eventually constant

$\Rightarrow I^n = I^{n+1}$ for all large N,

(Nakayama) $\Rightarrow I^n = 0$ for all large n

$\Rightarrow R$ artinian $\Rightarrow \dim(R) = 0$.

IH: claim established for $d(R) < d$ $\lneq d$

Induction step: Let $P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_t$ be a chain of primes of length $= t$. (WLOG $t > 0$)

Let $a \in P_1 \setminus P_0$. Let $R' = R/P_0$ (an ID).

$a' = a + P_0 \neq 0$ is not zerodivisor in R'.

Since $\exists$ surjective HM $R \twoheadrightarrow R'$, $d(R) \geq d(R')$

$d\left(\frac{R'}{(a')}\right) \leq d - 1$

$P_1, \ldots, P_t$ induces chain of length $t-1$ in $\frac{R'}{(a')}$

By induction $t - 1 \leq d\left(R'/(a')\right) \leq d - 1$. ∎

Let R be N'ian, P prime of R

height(P) = $\dim(R_P)$

= max length of chains contained in P

Final Claim: $\dim(R) \geq \delta(R)$

Note: if $\dim(R) = d$

I is the unique prime ideal of height d.

Construct inductively $x_1, x_2, \ldots$ $\quad x_i \in I$

and every prime ideal containing $(x_1, x_2 \ldots x_i)$

has height $\geq i$.

For some $k \leq d$, obtain $Q = (x_1, \ldots, x_i)$ s.t. I is only prime ideal containing Q.

Then verify that Q is I-primary (follows from theory of primary decomposition).

Do some other stuff. Get that $\dim(R) \geq \delta(R)$.

stuff involves induction and an exercise from ch. 1.

Algebraic Geometry

k an algebraically closed field, P prime in $k[t_1, \dots, t_n]$

$V = V(P) = \{a \in k^n : f(a) = 0 \ \forall f \in P\}$

$P = I(V) = \{f \in k[t] : f(a) = 0 \ \forall a \in V\}$

$A = A(V) =$ polynomial functions on V $\cong \dfrac{k[t_1, \dots t_n]}{P}$
coordinate ring of variety

Points of $\vec{a} \in k^n$ correspond to max'l ideals in A, $M_{\vec{a}} = \{F : F(a) = 0\}$

$k(V) =$ field of fractions of $A(V)$ $\quad k(V) \supseteq k$

$A_{\vec{a}}$ = localization at $M_{\vec{a}}$ $= \{\frac{f}{g} \in k(V) : g(a) \neq 0\}$

$A_{\vec{a}}$ is a local Noetherian ring, max'l ideal $= \{\frac{f}{g} : f(a) = 0, g(a) \neq 0\}$.

Defn: Dimension of variety V is the transcendence degree of $k(V)$ as a field extension of k (max'l # of algebraically independent elements)

Theorem: For all $\vec{a} \in V$, $\dim(A_{\vec{a}}) = \dim(V)$.

Proof:

Step 1: $\dim(V) \geq \dim(A_{\vec{a}})$

Lemma: R a Noetherian local ring, $I \subseteq R$ maximal, Q is I-primary, $Q = (r_1, \dots, r_d)$ where $d = \dim(R)$.

also assume f is homogenoos $\longrightarrow$ Let $f \in R[t_1, \dots, t_d]$, $\deg(f) = s$. Let $f(r_1, \dots, r_d) \in Q^{s+1}$

Then coefficients of f are in I.

$$G_Q(R) = \bigoplus_{n\in\mathbb{N}} \frac{Q^n}{Q^{n+1}} \qquad Q^0 = R$$

Proof of Lemma: Consider the HM of graded rings $\alpha: \frac{R}{Q}[t_1,\dots,t_d] \twoheadrightarrow G_Q(R)$ defined by evaluation at $(r_1,\dots,r_d)$ level-by-level. If f' is the polynomial in $\frac{R}{Q}[t_1,\dots,t_d]$ corresponding to f, then $f' \in \ker(\alpha)$.

So induce another HM $\dfrac{\frac{R}{Q}[t_1,\dots,t_d]}{(f')} \twoheadrightarrow G_Q(R)$.

Assume for contradiction not all coefficients of f are in I. Some coefficient of f' is a unit in R/Q. Hence f' is not a zerodivisor. By facts from the last lecture, $d\left(\frac{T}{(f')}\right) \leq d-1$, but by definition

$T = \frac{R}{Q}[t_1,\dots,t_d]$ $\quad d(G_Q(R)) = d \quad$ ⁂.

Proof of step 1: $R = A_{\bar{a}}$. Note that $k \subseteq R$ and

$k \cap$ (unique maximal ideal of R) $= 0$.

Let $d = \dim(R)$ choose $r_1,\dots,r_d$ generating an I-Primary ideal Q.

Claim: $r_1 \dots r_d$ algebraically independent over k

($\Longrightarrow d \leq$ trancendence degree of $k(V)$ over $k = \dim(V)$)

Assume for contradiction $F \neq 0$

<u>Proof</u>: Let $F(r_1, \dots, r_d) = 0$. Let F = sum of homogeneous f_i, where $\deg(f_i) = i$. Let s be the least s such that $f_s \neq 0$. $F(r_1, \dots, r_d) = 0 \Rightarrow f_s(r_1, \dots, r_d) \in Q^{s+1}$

(by Lemma) $\Longrightarrow$ Coefficients of f_s lie in $I \Rightarrow f_s = 0$ $\divideontimes$

■ Step 1.

<u>Step 2</u>: $\dim(V) \leq \dim(A_{\bar{a}})$

<u>Easy corollary of going down theorem</u>:

Let $A \subseteq B$, A, B integral domains, Noetherian A integrally closed and B an integral extension of A. Let J be a maximal ideal of B, $I = A \cap J$. Then

(a) I maximal in A

(b) $\dim(B_J) = \dim(A_I)$.

<u>Proof</u>: Use the defn of dimension by lengths of chains of prime ideals, use going-down theorem.

<u>Exercise 16 on pg 69</u>: (Max Noether's normalization theorem)

$A = k[T_1, \dots, T_n]$ $T_i = t_i + P$ A is fg k-algebra.

Then $\exists\ \bar{n} \leq n$ and $U_1, \dots, U_{\bar{n}}$ ~~linearly~~ linear combinations of $T_1, \dots, T_n$ such that $U_1 \dots U_n$ algebraically independent over k and A is an integral extension of ~~$k[U_1, \dots, U_{\bar{n}}]$.~~ $k[U_1, \dots, U_{\bar{n}}]$.

<u>Check</u> (really!) $\bar{n} = \dim(V)$, where k = field of fractions of A.

$k[U_1, \dots, U_{\bar{n}}] = k[s_1, \dots, s_d]$ is a Noetherian ID, and integrally closed since UFD.

$\cap|$

A, A is an integral extension of $k[U_1, \dots, U_{\bar{n}}]$.

Affine Algebraic Geometry

Move the coordinates such that $\vec{a} = 0$.

~~$M_{\vec{a}} = (t_1, \ldots, t_d)$ and~~

$$M_{\vec{a}} = (T_1, \ldots, T_n)$$

$$M_{\vec{a}} \cap k[U_1, \ldots, U_{\bar{n}}] = (u_1, \ldots, u_{\bar{n}})$$

$\bar{n} = \dim(V)$ but also $\bar{n} = \dim k[S_1 \ldots S_{\bar{n}}]_{(s_1 \ldots s_{\bar{n}})}$

$= \dim A(V)_{M_{\vec{a}}}$

■ Step 2. So $\bar{n} = d$.