Commutative Algebra (559) First class 9/3/2010

Tue + Fri 10:20 – 11:40 in Hill 425.
Head count: $\boxed{}$
Background? Interests? Gröbner bases, Int. mult.

Anders Buch
office: Hill 234
asbuch@math.rutgers.edu

A ring R is commutative with 1.

R is Noetherian if every ideal is f.g.

$\Leftrightarrow$ every asc. chain of ideals $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ stabilizes:
$\exists N > 0 : I_N = I_{N+1} = \cdots$

k field $\Rightarrow$ $k[x_1, \dots, x_n]$ is Noetherian.

Hilbert's Basis Thm

R Noetherian $\Rightarrow$ $R[X]$ Noetherian.

Proof: Assume $I \subseteq R[X]$ NOT f.g.

Choose $f_1 \in I$, $f_1 \neq 0$, of minimal degree.
Given $f_1, \dots, f_{i-1}$, choose $f_i \in I \setminus (f_1, \dots, f_{i-1})$ of minimal degree.
Set a_i = leading. coef. of f_i.
R Noetherian $\Rightarrow$ $J := (a_1, a_2, a_3, \dots) \subseteq R$ f.g., $J = (a_1, a_2, \dots, a_m)$.
Write $a_{m+1} = \sum_{i=1}^{m} r_i a_i$, $r_i \in R$.
Set $f' = f_{m+1} - \sum_{i=1}^{m} r_i \cdot f_i \cdot X^{\deg(f_{m+1}) - \deg(f_i)}$.
Now $f' \in I \setminus (f_1, \dots, f_m)$ and $\deg(f') < \deg(f_{m+1})$. ↯.
□

Primary interest: Relation to algebraic geometry.
AG = the study of geometric figures def. by poly equations.

k field. $\mathbb{A}^n = k^n = k \times k \times \cdots \times k$ affine space of dim n.

Given $f \in k[x_1, \dots, x_n]$, define function
$f : \mathbb{A}^n \to k$, $(a_1, \dots, a_n) \mapsto f(a_1, \dots, a_n)$.

Exercise: Assume k infinite field.
Then $f = 0$ as function $\Leftrightarrow$ $f = 0$ as polynomium.

Cor If $f \neq g \in k[x_1, \dots, x_n]$ then $f \neq g : \mathbb{A}^n \longrightarrow k$.

$\therefore$ $k[x_1, \dots, x_n]$ = ring of polynomial fcns on $\mathbb{A}^n$.

Def Given subset $I \subseteq k[x_1, \dots, x_n]$, def. $Z(I) = \{a \in \mathbb{A}^n \mid f(a) = 0 \ \forall f \in I\}$
algebraic set.

Example $I = \{y - x^2\} \subseteq \mathbb{R}[x, y]$.

$Z(y - x^2)$ =  $\subseteq \mathbb{R}^2$

Note: 1) If $J = \langle I \rangle \subseteq k[x_1, \dots, x_n]$ then $Z(J) = Z(I)$.

2) $\bigcap Z(I_\alpha) = Z(\bigcup I_\alpha)$

$Z(I_1) \cup \dots \cup Z(I_m) = Z(I_1 \cdot I_2 \cdots I_m)$

$I_1 \cdot I_2 \cdots I_m = \{a_1 \cdot a_2 \cdots a_m \mid a_i \in I_i\}$

$Z(0) = \mathbb{A}^n$, $Z(1) = \emptyset$

$\therefore$ The algebraic subsets define a topology on $\mathbb{A}^n$, called Zariski topology.

Q: What is a Zariski-open subset of $\mathbb{R}$?

Given $X \subseteq \mathbb{A}^n$ subset, define $I(X) = \{f \in k[x_1, \dots, x_n] \mid f(a) = 0 \ \forall a \in X\}$

$I(X) \subseteq k[x_1, \dots, x_n]$ is an ideal.

Note If $f, g \in k[x_1, \dots, x_n]$ define same fcn. $X \longrightarrow k$, then $f - g \in I(X)$

$\Rightarrow \bar{f} = \bar{g} \in k[x_1, \dots, x_n]/I(X)$.

Def $A(X) = k[x_1, \dots, x_n]/I(X)$ coordinate ring of X (esp. if X closed!).

Alg. Geo $\longleftrightarrow$ Com. Alg.

$X \longleftrightarrow A(X)$.

Exercise 1) $I \subseteq I(Z(I))$

2) $X \subseteq Z(I(X))$ = Zariski closure of X.

Def $I \subseteq R$ ideal.

$\sqrt{I} = \{f \in R \mid \exists n \geq 1 : f^n \in I\}$ radical of I.

I is radical if $I = \sqrt{I}$ $\Leftrightarrow$ $\forall f \in I, n \in \mathbb{N}_+ : f^n \in I \Rightarrow f \in I$.

Exercise 1) $\sqrt{I} \subseteq R$ is radical.

2) Prime ideals are radical.

Hilbert's Nullstellensatz

$k = \bar{k}$ alg. closed field, $I \subseteq k[x_1, \dots, x_n]$ ideal. Then $I(V(I)) = \sqrt{I}$.

Cor $k = \bar{k}$, $f_1, \dots, f_m \in k[x_1, \dots, x_n]$.
$(f_1, \dots, f_m) = (1) \iff Z(f_1, \dots, f_m) = \emptyset$

Pf $\Rightarrow$: clear. $\Leftarrow$: $I = (f_1, \dots, f_m)$. $(1) = I(\emptyset) = I(Z(I)) = \sqrt{I} \Rightarrow 1^n \in I$
$\Rightarrow I = (1)$.

Cor $k = \bar{k}$. Every max ideal $I \subseteq k[x_1, \dots, x_n]$ has the form $I = (x_1 - a_1, \dots, x_n - a_n)$

Pf $I \neq (1) \Rightarrow \exists\ (a_1, \dots, a_n) \in Z(I)$.
$I = \sqrt{I} = I(Z(I)) \subseteq I(\{(a_1, \dots, a_n)\}) = (x_1 - a_1, \dots, x_n - a_n)$.
$\square$

Localization

Def R ring, $U \subseteq R$ subset. U is multiplicatively closed if
$1 \in U$ and $f, g \in U \Rightarrow fg \in U$.

Given R-module M, def.
$$U^{-1}M = (M \times U)/\sim \quad \text{where } (m,u) \sim (m',u') \iff \exists\, v \in U : v(u'm - um') = 0$$

Notation: $\frac{m}{u} = [(m,u)] \in U^{-1}M$.

Exercise $U^{-1}R$ commutative ring, $U^{-1}M$ is a $U^{-1}R$-module.
$$\frac{m}{u} + \frac{m'}{u'} = \frac{u'm + um'}{uu'} \quad \text{and} \quad \frac{r}{u} \cdot \frac{m'}{u'} = \frac{rm'}{uu'}$$

Notation For $F \in R$, set $M_F = \{F^n \mid n \in \mathbb{N}\}^{-1} M = \{\frac{m}{F^n}\}$

Exercise $\varphi : M \to N$ R-hom $\Rightarrow \tilde{\varphi} : U^{-1}M \to U^{-1}N$, $\frac{m}{u} \mapsto \frac{\varphi(m)}{u}$ $U^{-1}R$-hom

Note $\pi : R \to U^{-1}R$, $r \mapsto r/1$ ring. hom.

Universal property

Let $\varphi : R \to S$ be a ring hom. such that $\varphi(u)$ is a unit in S $\forall u \in U$. Then $\exists!$ ring hom. $\tilde{\varphi} : U^{-1}R \to S$ such that

$$\begin{tikzcd} R \arrow[r, "\varphi"] \arrow[dr, "\pi"'] & S \\ & U^{-1}R \arrow[u, "\tilde{\varphi}"'] \end{tikzcd}$$
commutes.

Def Let $\varphi : R \longrightarrow S$ ring hom.

1) If $J \subseteq S$ ideal, then $\varphi^{-1}(J) \subseteq R$ is an ideal.
2) If $I \subseteq R$ ideal, then set $\varphi(I)S = IS = \langle \varphi(I) \rangle \subseteq S$.

Note: $I \subseteq \varphi^{-1}(\varphi(I)S)$ and $\varphi^{-1}(J)\cdot S \subseteq J$.

Def $\operatorname{Spec}(R) = \{\text{prime ideals in } R\}$

Prop $\pi : R \longrightarrow U^{-1}R$.

1) $J \subseteq U^{-1}R$ ideal. Then $\pi^{-1}(J)\cdot(U^{-1}R) = J \subseteq U^{-1}R$.
2) $Q \longmapsto \pi^{-1}(Q)$ is a bijection
$\operatorname{Spec}(U^{-1}R) \xrightarrow{\cong} \{P \in \operatorname{Spec}(R) \mid P \cap U = \varnothing\}$

Proof
1) We know $\pi^{-1}(J)\cdot(U^{-1}R) \subseteq J$.
Let $\frac{r}{u} \in J$. Then $\frac{r}{1} \in J \Rightarrow r \in \pi^{-1}(J) \Rightarrow \frac{r}{1} \in \pi^{-1}(J)\cdot(U^{-1}R)$.

2) The function is well def. and injective.
Let $P \subseteq R$ prime ideal, $U \cap P = \varnothing$.
Exercise: 1) $P\cdot U^{-1}R \subseteq U^{-1}R$ prime ideal.
2) $P = \pi^{-1}(P\cdot U^{-1}R)$

$\square$

Cor R Noetherian $\Rightarrow U^{-1}R$ Noetherian

Pf $J \subseteq U^{-1}R$ ideal. Then $\pi^{-1}(J) \subseteq R$ f.g. $\Rightarrow J = \pi^{-1}(J)\cdot U^{-1}R$ f.g.

Notation $P \subseteq R$ prime ideal. Then $R - P \subseteq R$ is mult. closed.
Set $R_P = (R \setminus P)^{-1}R$.

Def A *local ring* is a ring with exactly one maximal ideal.

R_P is local with max ideal $P\cdot R_P$

Example $X \subseteq \mathbb{A}^n$ alg. subset. $a = (a_1, \dots, a_n) \in X$.

$I(\{a\}) = (x_1 - a_1, \dots, x_n - a_n) \subseteq k[x_1, \dots, x_n]$ max ideal.

$m = I(\{a\})/I(X) \subseteq A(X)$ max ideal.

$A(X) \setminus m = \{f \in A(X) \mid f(a) \neq 0\}$

$A(X)_m = \{f/g \mid f, g \in A(X),\ f/g \text{ defined at } a \in X\}$ "local ring of X at a".

Tensor products

R ring, M, N, P R-modules.

$\varphi : M \times N \longrightarrow P$ is bilinear if ...

Def A tensor product of M and N over R is an R-module T together with a universal bilinear map $\alpha : M\times N \longrightarrow T$.

$$\begin{tikzcd} M\times N \arrow[r, "\varphi"] \arrow[d, "\alpha"'] & P \\ T \arrow[ur, dashed, "\exists!\,\tilde{\varphi}"'] & \end{tikzcd}$$

Notation: $M\otimes_R N = M\otimes N = T$, $\quad M\times N \xrightarrow{\alpha} M\otimes N$, $\quad (m,n)\mapsto m\otimes n$

Construction: $M\otimes_R N$ = free R-mod with basis $M\times N$ / rels.

Properties
(1) $M\otimes_R N$ generated by $\{m\otimes n\}$ as R-module.
(2) $M\otimes_R R = M$.
(3) $M\otimes_R N \cong N\otimes_R M$.
(4) $(M\otimes N)\otimes P = M\otimes(N\otimes P)$
(5) $(M\oplus N)\otimes P = (M\otimes P)\oplus(N\otimes P)$.
(6) $M\longrightarrow N\longrightarrow P\longrightarrow 0$ exact $\Rightarrow$ $M\otimes Q\longrightarrow N\otimes Q\longrightarrow N\otimes Q\longrightarrow 0$ exact.
(7) $\varphi : M\longrightarrow N$ and $\varphi' : M'\longrightarrow N'$ R-homs
$\Rightarrow \exists!\ \varphi\otimes\varphi' : M\otimes M'\longrightarrow N\otimes N'$, $\varphi\otimes\varphi'(m\otimes m') = \varphi(m)\otimes\varphi'(m')$

Follows from univ. property. (1): construction. (6) exercise.
$\mathrm{coker}(M\otimes Q\longrightarrow N\otimes Q)$ = tensor prod.

Example

Assume $N = R^n := R\oplus R\oplus\cdots\oplus R$

$$M\otimes_R N = M\otimes(R\oplus\cdots\oplus R) = (M\otimes R)\oplus\cdots\oplus(M\otimes R) = M\oplus\cdots\oplus M = M^n.$$

Com. Alg. 9/7/2010

Base change $\pi: R \to S$ ring hom.

N S-module $\Rightarrow$ N also R-module : $r \cdot n = \pi(r) \cdot n$

M R-module : $M \otimes_R S$ is an S-module. $s \cdot (m \otimes s') = m \otimes (ss')$.

Exercise

1) $U \subseteq R$ mult. subset, M R-module. Then

$M \otimes_R (U^{-1}R) \cong U^{-1}M$, $m \otimes \frac{r}{u} \mapsto \frac{rm}{u}$

2) $\varphi: M \to N$ injective $\Rightarrow$ $\tilde{\varphi}: U^{-1}M \to U^{-1}N$ injective.

3) $0 \to M' \to M \to M'' \to 0$ exact $\Rightarrow$ $0 \to U^{-1}M' \to U^{-1}M \to U^{-1}M'' \to 0$ exact.

Def M R-module. $\mathrm{Ann}(M) = \{ r \in R \mid r \cdot m = 0 \ \forall m \in M \}$. $\mathrm{Ann}(M) \subseteq R$ ideal.

Prop $U \subseteq R$ mult. closed. M R-module.

(a) Let $m \in M$. Then $\frac{m}{1} = 0 \in U^{-1}M \Leftrightarrow \exists u \in U : um = 0 \in M$

(b) M f.g. Then $U^{-1}M = 0 \Leftrightarrow \mathrm{Ann}(M) \cap U \neq \emptyset$

(c) M f.g., $P \subseteq R$ prime ideal. Then $M_P \neq \emptyset \Leftrightarrow \mathrm{Ann}(M) \subseteq P$.

Proof $\boxed{(b) \Rightarrow}$ M gen. by $m_1, \dots, m_n$.

$\frac{m_i}{1} = 0 \Rightarrow \exists u_i \in U : u_i m_i = 0$. Then $u_1 u_2 \cdots u_n \in \mathrm{Ann}(M) \cap U$

□

Def $\mathrm{Supp}(M) = \{ P \in \mathrm{Spec}(R) \mid M_P \neq 0 \}$

If $I \subseteq R$ ideal, then set $Z(I) = \{ p \in \mathrm{Spec}(R) \mid I \subseteq P \}$

Note: M f.g. $\Rightarrow$ $\mathrm{Supp}(M) = Z(\mathrm{Ann}(M)) \subseteq \mathrm{Spec}(R)$.

Lemma R ring. M R-module.

(a) $m \in M$. $m = 0 \Leftrightarrow \frac{m}{1} = 0 \in M_{\mathfrak{m}}$ $\forall \mathfrak{m} \subseteq R$ max. ideal

(b) $M = 0 \Leftrightarrow M_{\mathfrak{m}} = 0$ $\forall \mathfrak{m} \subseteq R$ max ideal.

Proof

"$\Rightarrow$" trivial in both cases.

(a) $\frac{m}{1} = 0 \in M_{\mathfrak{m}}$ $\forall \mathfrak{m}$ $\Rightarrow$ $\mathrm{Ann}(m) \not\subseteq \mathfrak{m}$ $\forall \mathfrak{m}$

$\Rightarrow \mathrm{Ann}(m) = R \Rightarrow m = 0$.

(b) If $M_{\mathfrak{m}} = 0$ $\forall \mathfrak{m}$ then (a) implies that $M = 0$.

□

Cor $\varphi: M \to N$ R-hom.

φ is injective/surjective/bijective $\Leftrightarrow$ $\varphi_m : M_m \to N_m$ inj/surj/bijective $\forall\, m \subseteq R$ max.

Proof Set $K = \ker(\varphi)$. $0 \to K \to M \to N$ exact $\Rightarrow$ $0 \to K_m \to M_m \to N_m$ exact

φ injective $\Leftrightarrow$ $K = 0$ $\Leftrightarrow$ $K_m = 0\ \forall m$ $\Leftrightarrow$ φ_m injective $\forall m$.

□

Prop $U \subseteq R$ mult. closed subset.

Assume $I \subseteq R$ is an ideal that is maximal among the ideals disjoint from U.

Then I is a prime ideal in R.

Proof Let $r, s \in R \setminus I$.

$(r, I) \cap U \neq \emptyset \Rightarrow \exists\, a \in R,\ a' \in I : \quad ar + a' \in U.$

$(s, I) \cap U \neq \emptyset \Rightarrow \exists\, b \in R,\ b' \in I : \quad bs + b' \in U.$

$(ar + a')(bs + b') = abrs + arb' + a'sb + a'b' \in U$

$\Rightarrow abrs \notin I \Rightarrow rs \notin I.$

□

Cor $I \subseteq R$ ideal. Then $\sqrt{I} = \bigcap_{P \in Z(I)} P \subseteq R$.

Proof

$\subseteq$: $P \in Z(I) \Rightarrow I \subseteq P \Rightarrow \sqrt{I} \subseteq \sqrt{P} = P$

$\supseteq$: Let $f \in R \setminus \sqrt{I}$. Then $U = \{f^n \mid n \geq 0\}$ disjoint from I.

Choose $P \supseteq I$ maximal among ideals disjoint from U

Then $P \in Z(I)$ and $f \notin P$. $\quad \therefore f \notin \bigcap_{P \in Z(I)} P$.

□

Q: Why does P exist?

Let $(A, \leq)$ partially ordered set.

$S \subseteq A$ is <u>totally ordered</u> if $\forall s, t \in S$: $s \leq t$ or $t \leq s$.

$S \subseteq A$ is <u>dominated</u> by $x \in A$ if $s \leq x\ \forall s \in S$.

Zorn's Lemma If every totally ordered subset of A is dominated by an element of A, then A contains a maximal element.

$A = \{\text{ideals } J \subseteq R \mid J \cap \{f^n\} = \emptyset\}$. Order by inclusion.

Assume $S = \{J_\alpha\} \subseteq A$ totally ordered. Then dominated by $\hat{J} = \bigcup_\alpha J_\alpha \in A$.

Zorn $\Rightarrow$ $\exists$ max elt. $P \in A$.

Length

Def A non-zero R-module M is simple if M has no submodules other than $0, M$.

Note Assume M simpel, $0 \neq m \in M$.
Then $R \longrightarrow M$, $r \longmapsto rm$ is surjective $\Rightarrow$ $M \cong R/I$ for some ideal
R/I simple $\Rightarrow$ $I \subseteq R$ max. ideal.

$\therefore$ Any simple R-module is $\cong R/p$, $p \subseteq R$ max. ideal.

Def M R-module. A decomposition series for M is a chain
$M = M_r \supsetneq M_{r-1} \supsetneq \cdots \supsetneq M_0 = 0$ such that M_i/M_{i-1} simple $\forall i$.
r = length of series.

Prop Any two decomp. series for M have same length.

Proof Let $M = N_s \supsetneq N_{s-1} \supsetneq \cdots \supsetneq N_0 = 0$ be another decomp series.

$$\begin{array}{ccccccc}
M = M_r \cap N_s & \supset & M_r \cap N_{s-1} & \supset & \cdots & \supset & M_r \cap N_0 \\
\cup & & \cup & & & & \cup \\
M_{r-1} \cap N_s & \supset & M_{r-1} \cap N_{s-1} & \supset & \cdots & \supset & M_{r-1} \cap N_0 \\
\cup & & \cup & & & & \cup \\
\vdots & & \vdots & & & & \vdots \\
\cup & & \cup & & & & \cup \\
M_0 \cap N_s & \supset & M_0 \cap N_{s-1} & \supset & \cdots & \supset & M_0 \cap N_0 = 0
\end{array}$$

Note 1 Every path from M to 0 is a decomp. series, if repetitions are discarded.

$$(M_i \cap N_j)/(M_i \cap N_{j-1}) = (M_i \cap N_j + N_{j-1})/N_{j-1} \subseteq N_j/N_{j-1} \text{ is simple.}$$

Note 2 All these decomp. series have same length. $\boxed{A/A\cap B = A+B/B}$

$$\begin{array}{ccc} A & \supsetneq & B \\ \cup\!\!\!\!\!\not\;\; & & \cup\!\!\!\!\!\not\;\; \\ C & \supsetneq & D \end{array} \qquad
\begin{array}{ccc} A & \supsetneq & B \\ \| & & \| \\ C & \supsetneq & D \end{array} \qquad
\begin{array}{ccc} A & \supsetneq & B \\ \cup\!\!\!\!\!\not\;\; & & \| \\ C & = & D \end{array} \qquad
\begin{array}{ccc} A & = & B \\ \cup\!\!\!\!\!\not\;\; & & \cup\!\!\!\!\!\not\;\; \\ C & = & D \end{array} \qquad
\begin{array}{ccc} A & = & B \\ \| & & \cup\!\!\!\!\!\not\;\; \\ C & \supsetneq & D \end{array} \qquad
\begin{array}{ccc} A & = & B \\ \| & & \| \\ C & = & D \end{array}$$

$\square$

Def $$\text{length}(M) = \begin{cases} r & \text{if } M = M_r \supsetneq \cdots \supsetneq M_0 = 0 \text{ decomp. series} \\ \infty & \text{if } \nexists \text{ decomp. series.} \end{cases}$$

~~Exercise~~ Exercise

1) $N \subseteq M$ submodule $\Rightarrow$ $\text{length}(M) = \text{length}(N) + \text{length}(M/N)$.
2) $\text{length}(M) < \infty$ $\Rightarrow$ any chain of submodules of M can be refined to decomp. series.

Def The R-module M is Noetherian if every submodule of M is f.g.
$\Leftrightarrow$ every ascending chain $N_1 \subseteq N_2 \subseteq N_3 \subseteq \cdots \subseteq M$ stabilizes.

Exercise R Noetherian ring, M f.g. R-module. Then M is Noetherian.

Def M is Artinian if every descending chain $M_1 \supseteq M_2 \supseteq M_3 \supseteq \cdots$ of submodules stabilizes $M_N = M_{N+1} = \cdots$.

Prop $\text{length}(M) < \infty \Leftrightarrow M$ is Noetherian & Artinian.

Proof $\Leftarrow$: Choose max submodule $M_1 \subsetneq M$.
Choose max submodule $M_2 \subsetneq M_1$
$\vdots$
$M \supsetneq M_1 \supsetneq M_2 \supsetneq \cdots$ stabilizes to decomp series.

$\Rightarrow$: If M Not Noetherian or not Artinian, then $\exists$ infinite strict chain of submodules $\Rightarrow \text{length}(M) = \infty$.

$\square$

Thm 1 Assume $\text{length}(M) < \infty$

(a) $M \cong \bigoplus_{P \subseteq R \text{ max.}} M_P$

(b) $M = M_n \supsetneq M_{n-1} \supsetneq \cdots \supsetneq M_0 = 0$ decomp. series.
Then $\text{length}_{R_P}(M_P) = \#\{i : M_i/M_{i-1} \cong R/P\}$

(c) $M = M_P \Leftrightarrow P^s \cdot M = 0$ for some $s \in \mathbb{N}$.

Proof

Recall: $(M/N)_P = M_P/N_P$. $\quad 0 \to N \to M \to M/N \to 0$.

Assume $N = R/P$ simple, $P \subseteq R$ max ideal. Let $Q \subseteq R$ other max ideal.

Then $N_Q = \begin{cases} N & \text{if } Q = P \\ 0 & \text{if } Q \neq P. \end{cases}$

$(Q \neq P \Rightarrow P \not\subseteq Q \Rightarrow \exists f \in P \setminus Q. \quad f \cdot N = 0 \Rightarrow N_Q = 0.)$

$\therefore$ N simple, $Q \neq P \subseteq R$ max ideals $\Rightarrow (N_P)_Q = 0$

$\therefore$ $\text{length}(M) < \infty \Rightarrow (M_P)_Q = 0$

(a) $\varphi : M \longrightarrow \bigoplus_{P \text{ max}} M_P$, $\quad \varphi(m) = \bigoplus \frac{m}{1}$.

$Q \subseteq R$ max $\Rightarrow \varphi_Q : M_Q \longrightarrow \left(\bigoplus M_P\right)_Q = M_Q$ identity.

$\therefore$ φ isomorphism.

(b) $M = M_n \supsetneq M_{n-1} \supsetneq \cdots \supsetneq M_0 = 0$ decomp. series, $P \subseteq R$ max ideal.

Assume $M_i/M_{i-1} \cong R/Q$.

If $Q = P$: $(M_i)_P \supsetneq (M_{i-1})_P$ and $(M_i/M_{i-1})_P = (M_i)_P/(M_{i-1})_P$ simple R_P-module

If $Q \neq P$: $(M_i)_P = (M_{i-1})_P$ $\qquad (M_i/M_{i-1})_P = (R/Q)_P$

$\therefore M_P = (M_n)_P \supseteq \cdots \supseteq (M_0)_P = 0$ decomp series after repetitions skipped.

length $= \#\{i : M_i/M_{i-1} \cong R/P\}$.

(c) $\Leftarrow$: Assume $P^s \cdot M = 0$.

If $Q \subseteq R$ max, $Q \neq P$, then $\exists f \in P \setminus Q$.

$f^n \cdot M = 0 \Rightarrow M_Q = 0$.

Now (a) $\Rightarrow M \cong M_P$.

$\Rightarrow$: length(M) = length(M_P) $\Rightarrow$

M has decomp series $M = M_n \supsetneq \cdots \supsetneq M_0 = 0$ with $M_i/M_{i-1} \cong R/P$ $\forall i$

$P \cdot M \subseteq M_{n-1}$, $P^2 \cdot M \subseteq M_{n-2}$, ..., $P^n \cdot M \subseteq M_0 = 0$.

$\square$

Example $R = \mathbb{Z}$, $M = \mathbb{Z}/(a)$, $a = p_1^{r_1} \cdots p_k^{r_k}$.

$P = (p) \subseteq \mathbb{Z}$ max ideal.

$(p, a) = 1 \Rightarrow M_P = 0$

$p = p_i$: $M_P = \left(\mathbb{Z}/(p_i^{r_i})\right)_P = \mathbb{Z}/(p_i^{r_i})$

$\therefore\ \mathbb{Z}/(a) = \oplus M_P = \mathbb{Z}/(p_1^{r_1}) \oplus \cdots \oplus \mathbb{Z}/(p_k^{r_k})$

Thm2 R ring; TFAE:

(a) R Noetherian and all prime ideals are maximal

(b) $\text{length}_R(R) < \infty$

(c) R is Artinian

Proof

(a) $\Rightarrow$ (b): Assume R Noeth. and $\text{length}_R(R) = \infty$.

Choose $I \subseteq R$ max among ideals s.t. $\text{length}(R/I) = \infty$. (Noeth.)

Claim: I prime ideal.

Let $ab \in I$, $a \notin I$.

Set $(I:a) = \{r \in R \mid ar \in I\} \supseteq I$.

$$0 \longrightarrow R/(I:a) \xrightarrow{a\cdot} R/I \longrightarrow R/(a)+I \longrightarrow 0$$

$\text{length}(R/I) = \infty$ and $\text{length}(R/(a)+I) < \infty \Rightarrow \text{length}(R/(I:a)) = \infty$

$\therefore\ I:a = I \Rightarrow b \in I:a = I$.

Claim + hypothesis $\Rightarrow I \subseteq R$ max ideal $\Rightarrow \text{length}(R/I) = 1$ $\lightning$.

(b) $\Rightarrow$ (c): Already proved.

(c) $\Rightarrow$ (a): Assume R Artinian.

Claim: $0 \subseteq R$ is a product of max ideals.

Choose $J \subseteq R$ minimal ideal that is a product of max ideals.

If $M \subseteq R$ max ideal, then $MJ \subseteq J \Rightarrow MJ = J$.

$J^2 \subseteq J \Rightarrow J^2 = J$.

Assume $J \neq 0$.

Choose $I \subseteq R$ minimal s.t. $I \cdot J \neq 0$

$I \cdot J \subseteq I$ and $(IJ) \cdot J = IJ^2 = IJ \neq 0 \Rightarrow IJ = I$.

$\exists f \in I: \ f \cdot J \neq 0. \quad (f) \subseteq I \Rightarrow I = (f).$

$(f) \cdot J = IJ = I = (f) \quad \Rightarrow \quad \exists\ g \in J: \ fg = f.$

$\Rightarrow (g-1)f = 0.$

$g \in J \subseteq M \quad \forall\ M \subseteq R$ max ideal $\Rightarrow \quad g-1$ unit in R.

$\therefore\ f = 0, \quad I = 0$ ↯.

Have shown: $0 = M_1 M_2 \cdots M_t$, $\quad M_i \subseteq R$ max ideal.

Note: $M_1 \cdots M_i / M_1 \cdots M_{i+1}$ = vector space over R/M_{i+1}

R Artinian $\Rightarrow$ dim $< \infty$ $\Rightarrow$ length $< \infty$.

$\therefore$ length$(R) < \infty$ $\Rightarrow$ R Noetherian.

Let $P \subseteq R$ prime ideal.

Then $M_1 \cdot M_2 \cdots M_t \subseteq P \Rightarrow M_i \subseteq P$ for some $i \Rightarrow P = M_i$

$\therefore$ All prime ideals are maximal, and there are finitely many of them.

□

Cor $X \subseteq \mathbb{A}^n$ alg. subset. TFAE:

(a) X is finite

(b) $\dim_k A(X) < \infty$

(c) $A(X)$ Artinian

Proof

(a) $\Rightarrow$ (b): $A(X) = \{\text{poly. fcns on } X\} = \{\text{all fcns } X \to k\} = k^{\#X}$.

(b) $\Rightarrow$ (c): length $A(X) \leq \dim_k A(X)$.

(c) $\Rightarrow$ (a): Thm 2 implies $A(X)$ has finitely many max ideals $\Rightarrow \#X < \infty$.

□

Cor Any Artinian ring is a direct product of finitely many local Artinian rings.

Proof Thm 2 $\Rightarrow$ length$(R) < \infty$.

Thm 1 $\Rightarrow$ $R \cong \bigoplus_{P \max} R_P = \prod_{P \max} R_P$

Note: finitely many factors, iso of rings.

□

Cor R Noetherian ring, M f.g. R-module. TFAE:

(a) $\text{length}(M) < \infty$

(b) $\exists$ max ideals $P_1, \to P_n \subseteq R$ s.t. $P_1 \cdot P_2 \cdots P_n \cdot M = 0$

(c) All prime ideals $P \supseteq \text{Ann}(M)$ are maximal.

(d) $R/\text{Ann}(M)$ Artinian ring.

Proof

(a) $\Rightarrow$ (b): $M = M_n \supsetneq M_{n-1} \supsetneq \cdots \supsetneq M_0 = 0$ decomp series.

$M_i/M_{i-1} = R/P_i$. Then $P_1 P_2 \cdots P_n \cdot M = 0$

(b) $\Rightarrow$ (c): Assume $P_1 \cdots P_n \cdot M = 0$, $P_i \subseteq R$ max.

If $P \supseteq \text{Ann}(M) \supseteq P_1 \cdots P_n$ then $P_i \subseteq P$ for some $i \Rightarrow P = P_i$ max.

(c) $\Rightarrow$ (d): All prime ideals in $R/\text{Ann}(M)$ are maximal.

(d) $\Rightarrow$ (a): $S = R/\text{Ann}(M)$. Then M is an S-module.

M f.g. $\Rightarrow$ $M = S^n/N$ $\Rightarrow$ $\text{length}(M) < \text{length}(S^n) < \infty$.

$\square$

Cor $I \subseteq P \subseteq R$ ideals, R Noetherian, P prime. TFAE:

(a) P min. prime over I

(b) R_P/I_P Artinian

(c) $P_P{}^n \subseteq I_P$ (inside R_P) for some $n \in \mathbb{N}$.

> **Remark**
> $I \subseteq R$ ideal, $S \subseteq R$ mult. closed.
> $S^{-1}I := I \cdot (S^{-1}R)$.
> I also R-module.
> $0 \to I \to R \Rightarrow$
> $0 \to S^{-1}I \to S^{-1}R$
> $\therefore$ Same def.

Proof

(a) $\Rightarrow$ (b): R_P/I_P is Noetherian and

P_P/I_P only prime ideal.

(b) $\Rightarrow$ (c): $(0) \subseteq R_P/I_P$. $\sqrt{(0)} = P_P/I_P \subseteq R_P/I_P$. (since all prime ideals are max.)

$P = (f_1, \to f_n) \subseteq R$.

$f_i^N \in I_P \quad \forall i. \Rightarrow P_P^{n \cdot N} \subseteq I_P$

(c) $\Rightarrow$ (a): Assume $I \subseteq Q \subseteq P$.

$P_P^n \subseteq Q_P \Rightarrow P_P \subseteq Q_P \Rightarrow Q_P = P_P \Rightarrow Q = P$.

$\square$

Lemma (Prime Avoidance)

$I_1, \dots, I_n, J \subseteq R$ ideals. Assume $J \subseteq \bigcup_{i=1}^{n} I_i$

If $I_3, I_4, \dots, I_n$ are prime ideals, or if R contains infinite field, then $J \subseteq I_i$ for some i.

Proof Assume $J \not\subseteq \bigcup_{i \neq j} I_i$ for every j.

Choose $x_j \in J$ s.t. $x_j \notin I_i$ for $i \neq j$.

Then $x_j \in I_j$.

$n = 2$: $x_1 + x_2 \notin I_1 \cup I_2$ ↯.

$n \geq 3$: I_n prime ideal.

$x_1 x_2 \cdots x_{n-1} + x_n \notin I_j$ for every j ↯

Conclude: $J \subseteq \bigcup_{i \neq j} I_i$ for some j.

Induction $\Rightarrow$ $J \subseteq I_i$ for some $i \neq j$.

□

Geometry $X \subseteq \mathbb{A}^n$ alg. subset, $k = \bar{k}$.

$A(X) = k[x_1, \dots, x_n]/I(X)$ coordinate ring.

If $Y \subseteq X$ closed subset, then $I(X) \subseteq I(Y)$

$\bar{I}(Y) := I(Y)/I(X) \subseteq A(X)$ radical ideal.

An algebraic set Y is irreducible if:

$Y = Y_1 \cup Y_2$, Y_1, Y_2 closed $\Rightarrow$ $Y = Y_1$ or $Y = Y_2$.

Example: $Z(xy) \subseteq \mathbb{A}^2$ is NOT irreducible. 

Exercise Y is irreducible $\Leftrightarrow$ $\bar{I}(Y) \subseteq A(X)$ prime ideal.

$$\{\text{closed subsets of } X\} \longleftrightarrow \{\text{radical ideals in } A(X)\}$$

$$\{\text{irreducible subsets}\} \longleftrightarrow \{\text{prime ideals}\} = \operatorname{Spec} A(X)$$

$$\{\text{points}\} \longleftrightarrow \{\text{max ideals}\}$$

$$Y \longmapsto I(Y)$$

$$Z(J) \longleftarrow J$$

<u>Exercise</u> Every alg. subset $X \subseteq \mathbb{A}^n$ is union of finitely many irreducible alg. sets.

Set $R = k[x_1, \dots, x_n]$.

1) Assume $I \subseteq R$ radical ideal.

$Z(I) = X_1 \cup \dots \cup X_m \subseteq \mathbb{A}^n$.

$I = \sqrt{I} = I(X_1) \cap \dots \cap I(X_m)$ – intersection of finitely many prime ideals.

$= \{ f \in R \mid f \equiv 0 \text{ on } X_i \ \forall i \}$

2) $R = k[x,y]$. $I = (x^2, xy)$ not radical ideal. $\sqrt{I} = (x)$.

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

$= \{ f \in R \mid f \equiv 0 \text{ on } Z(x)$ <u>and</u> f has zero of order 2 at $(0,0) \}$

<u>Note:</u> $M = R/I$. $x + I = \bar{x}$.

$\mathrm{Ann}(x+I) = (x,y) = \sqrt{(x^2, xy, y^2)}$ ⟷ point

$\mathrm{Ann}(y+I) = (x) = \sqrt{(x)}$ ⟷ line.

<u>Note:</u> Also have $I = (x) \cap (x^2, y)$, intersection not unique.

<u>Def</u> R ring, M R-module.

A prime ideal $P \subseteq R$ is <u>associated</u> to M if $\exists\, m \in M : P = \mathrm{Ann}(m)$.

$\mathrm{Ass}(M) = \mathrm{Ass}_R(M) = \{ P \in \mathrm{Spec}\, R \mid P \text{ associated to } M \}$.

<u>EXCEPTION:</u> $\mathrm{Ass}(I) := \mathrm{Ass}(R/I)$ when $I \subseteq R$ ideal!

<u>Note:</u> 1) If $P = \mathrm{Ann}(m)$, then $R/P \longrightarrow Rm \subseteq M$ is injective.

$\bar{r} \mapsto r \cdot m$

$\therefore\ P \in \mathrm{Ass}(M) \Leftrightarrow R/P \subseteq M$.

2) $\mathrm{Ass}(P) = \mathrm{Ass}(R/P) = \{P\}$. $\mathrm{Ann}(r+P) = P \quad \forall\, r \notin P$.

<u>Prop</u> R ring, M R-module.

If $I \subseteq R$ is maximal among proper ideals that are annihilators for elts. of M, then $I \in \mathrm{Ass}(M)$.

<u>Proof</u> Let $I = \mathrm{Ann}(m)$ be maximal, $m \neq 0 \in M$.

Assume $rs \in I$, $r \notin I$.

$\mathrm{Ann}(m) \subseteq \mathrm{Ann}(rm) \neq R \Rightarrow \mathrm{Ann}(m) = \mathrm{Ann}(rm)$.

$s \in \mathrm{Ann}(rm) = I$.

□

Note: R Noetherian, $M \neq 0 \Rightarrow \mathrm{Ass}(M) \neq \emptyset$.

Cor M R-module, R Noetherian.

(a) $m \in M$. Then $m = 0 \iff \frac{m}{1} = 0 \in M_p \ \forall p \in \mathrm{Ass}(M)$.

(b) $K \subseteq M$ submodule. $K = 0 \iff K_p = 0 \ \forall p \in \mathrm{Ass}(M)$.

Proof $2 \times \Rightarrow$ trivial.

(a) $\Leftarrow$: If $m \neq 0$ then choose $P \subsetneq R$ max. s.t. $P \supseteq \mathrm{Ann}(m)$ and P annihilator of some elt.

Then $P \in \mathrm{Ass}(M)$ and $\frac{m}{1} \neq 0 \in M_P$.

(b) $\Leftarrow$: All elts of K are zero by (a).

□

Lemma (a) $M = M' \oplus M'' \Rightarrow \mathrm{Ass}(M) = \mathrm{Ass}(M') \cup \mathrm{Ass}(M'')$

(b) $0 \to M' \to M \to M'' \to 0 \Rightarrow \mathrm{Ass}(M') \subseteq \mathrm{Ass}(M) \subseteq \mathrm{Ass}(M') \cup \mathrm{Ass}(M'')$.

Proof

(b) $\Rightarrow$ (a).

(a): $p \in \mathrm{Ass}(M') \Rightarrow R/p \subseteq M' \subseteq M \Rightarrow p \in \mathrm{Ass}(M)$.

Let $p \in \mathrm{Ass}(M) \setminus \mathrm{Ass}(M')$.

$R/p \cong R\cdot m \subseteq M$.

If $0 \neq m' \in R\cdot m \cap M'$ then $p = \mathrm{Ann}(m') \in \mathrm{Ass}(M')$ $\lightning$.

$\therefore$ $R\cdot m \cap M' = 0 \Rightarrow R/p \cong R\cdot m \hookrightarrow M''$.

□

Prop R Noetherian, M f.g. R-module.

Then $\exists\ 0 = M_0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_n = M$ s.t. $M_i/M_{i-1} \cong R/p_i$, p_i prime.

Proof If $M \neq 0$ then $\mathrm{Ass}(M) \neq \emptyset \Rightarrow \exists M_1 \subseteq M$ s.t. $M_1 \cong R/p_1$.

If $M/M_1 \neq 0$ then $\exists M_2/M_1 \subseteq M/M_1$ s.t. $M_2/M_1 \cong R/p_2$.

$0 = M_0 \subsetneq M_1 \subsetneq M_2 \subsetneq \cdots$ must stop because M Noetherian.

□

Thm R Noetherian, $M \neq 0$ f.g. R-module.

(a) $\mathrm{Ass}(M)$ is a finite non-empty set containing all minimal primes over $\mathrm{Ann}(M)$.

(b) $\bigcup_{p \in \mathrm{Ass}(M)} p = \{r \in R \mid \exists\ 0 \neq m \in M : rm = 0\}$ zero divisors on M.

(c) $U \subseteq R$ mult. subset $\Rightarrow \mathrm{Ass}_{U^{-1}R}(U^{-1}M) = \{U^{-1}p \mid p \in \mathrm{Ass}(M) \text{ and } p \cap U = \emptyset\}$

Thm R Noetherian, M f.g. R-module.

(a) $\mathrm{Ass}(M)$ is finite and contains all minimal primes over $\mathrm{Ann}(M)$.
Every prime ideal containing $\mathrm{Ann}(M)$ contains a minimal prime over $\mathrm{Ann}(M)$.

(b) $\bigcup_{P \in \mathrm{Ass}(M)} P = \{r \in R \mid \exists\, 0 \neq m \in M : rm = 0\} = \{\text{zero divisors on } M\}$.

(c) $U \subseteq R$ mult. closed $\Rightarrow \mathrm{Ass}_{U^{-1}R}(U^{-1}M) = \{U^{-1}P \mid P \in \mathrm{Ass}(M) \text{ and } P \cap U = \emptyset\}$.

Proof

(a) Choose $0 = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_n = M$, $M_i/M_{i-1} \cong R/P_i$.
Then $\mathrm{Ass}(M) \subseteq \{P_1, \dots, P_n\}$ is finite. Note: $P_1 P_2 \cdots P_n \cdot M = 0$.
Let $Q \subseteq R$ be a prime, $\mathrm{Ann}(M) \subseteq Q$.
Then $P_1 P_2 \cdots P_n \subseteq Q \Rightarrow P_j \subseteq Q$ for some j.
If Q is minimal over $\mathrm{Ann}(M)$, then $Q = P_j$.

(b) $\subseteq$ is clear.
$\supseteq$: Assume $r \in R$, $0 \neq m \in M$, $rm = 0 \in M$.
Let $P \supseteq \mathrm{Ann}(m)$ be max. among annihilator ideals.
Then $r \in P \in \mathrm{Ass}(M)$.

(c) Recall: $\mathrm{Spec}(U^{-1}R) = \{U^{-1}P \mid P \in \mathrm{Spec}(A),\ P \cap U = \emptyset\}$.
$\supseteq$: Assume $P \in \mathrm{Ass}(M)$ and $P \cap U = \emptyset$. Then $U^{-1}P \subseteq U^{-1}R$ prime ideal.
$0 \to R/P \to M \Rightarrow 0 \to U^{-1}R/U^{-1}P \to U^{-1}M$.
$\subseteq$: Assume $P \subseteq R$ prime ideal, $P \cap U = \emptyset$, $U^{-1}P \in \mathrm{Ass}(U^{-1}M)$.
$U^{-1}P = \mathrm{Ann}(\frac{m}{u}) \subseteq U^{-1}R$, $\frac{m}{u} \in U^{-1}M$. $\Rightarrow U^{-1}P = \mathrm{Ann}(\frac{m}{1})$.
Choose $u' \in U$ s.t. $\mathrm{Ann}(u'm) \subseteq R$ is as large as possible.
Claim: $P = \mathrm{Ann}(u'm)$.
$\supseteq$: $r \cdot u'm = 0 \Rightarrow \frac{r}{1} \in \mathrm{Ann}(\frac{u'm}{1}) = U^{-1}P \Rightarrow r \in R \cap U^{-1}P = P$.
$\subseteq$: Let $r \in P$.
$\frac{r}{1} \cdot \frac{u'm}{1} = 0 \in U^{-1}M \Rightarrow \exists\, u'' \in U : r u'' u' m = 0$, i.e. $r \in \mathrm{Ann}(u''u'm)$.
$\mathrm{Ann}(u''u'm) \supseteq \mathrm{Ann}(u'm) \Rightarrow \mathrm{Ann}(u''u'm) = \mathrm{Ann}(u'm)$.

$\square$

Cor R Noetherian, $I \subseteq R$ ideal. There are finitely many minimal primes over I, and $\sqrt{I}$ is the intersection of these min. primes.

Proof Apply part (a) to $M = R/I$, use $\sqrt{I} = \bigcap_{P \supseteq I} P$.

Com. Alg. 9/17/2010

Primary Decomposition

R Noetherian, M f.g. R-module.

Def M is P-coprimary if $\mathrm{Ass}(M) = \{P\}$.

Prop $P \subseteq R$ prime ideal. TFAE:

(a) M is P-coprimary.

(b) P is minimal over $\mathrm{Ann}(M)$ and all elts. in $R \setminus P$ are nonzero divisors on M.

(c) $P^n \cdot M = 0$ for some n, and all elts in $R \setminus P$ are nzds on M.

Proof

(a) $\Rightarrow$ (c): zero-divs$(M) = P$.

P only min. prime over $\mathrm{Ann}(M)$

$\Rightarrow P = \sqrt{\mathrm{Ann}(M)} \Rightarrow P^n \subseteq \mathrm{Ann}(M)$, some n.

(c) $\Rightarrow$ (b): $\mathrm{Ann}(M) \subseteq$ zero-divs$(M) \subseteq P$.

$P^n \cdot M = 0 \Rightarrow P \subseteq \sqrt{\mathrm{Ann}(M)} \Rightarrow P$ minimal over $\mathrm{Ann}(M)$.

(b) $\Rightarrow$ (a): $Q \in \mathrm{Ass}(M) \Rightarrow \mathrm{Ann}(M) \subseteq Q \subseteq$ zero-divs$(M) \subseteq P$.

P minimal over $\mathrm{Ann}(M) \Rightarrow Q = P$.

$\square$

Def R Noetherian, M f.g. R-module, $N \subseteq M$ submodule.

N is a P-primary submodule if M/N is P-coprimary, i.e. $\mathrm{Ass}(M/N) = \{P\}$

Example $M = R = k[x,y]$, $I = (x^2, xy, y^2) \subseteq M$.

$\mathrm{Ass}(I) = \mathrm{Ass}(R/I) = \{(x,y)\} \Rightarrow I$ is an (x,y)-primary ideal/submod.

Cor R Noetherian, $I \subsetneq R$ proper ideal, $P \subseteq R$ prime ideal.

Then I is P-primary $\Leftrightarrow$ $P^n \subseteq I$ for some n and $rs \in I, r \notin P \Rightarrow s \in I$.

Proof Take $M = R/I$ and use (a)$\Leftrightarrow$(c) in Prop. $\square$

Lemma $N_1, \dots, N_t \subseteq M$ P-primary submods $\Rightarrow$ $\bigcap N_i \subseteq M$ P-primary.

Proof WLOG $t=2$.

$$M/_{N_1 \cap N_2} \subseteq M/_{N_1} \oplus M/_{N_2} \Rightarrow \mathrm{Ass}(M/_{N_1\cap N_2}) \subseteq \{P\}.$$

$\square$

Thm R Noetherian, M f.g. R-module. Every submodule $M' \subseteq M$ has a primary decomposition: $(*)$ $M' = M_1 \cap \dots \cap M_n$

where $M_i \subseteq M$ is P_i-primary, $P_i \in \mathrm{Spec}(R)$.

Furthermore:

(a) $\mathrm{Ass}(M/_{M'}) \subseteq \{P_1, \dots, P_n\}$

(b) If $(*)$ is non-redundant (i.e. $M' \subsetneq \bigcap_{i \neq j} M_i \ \forall j$)

then $\mathrm{Ass}(M/_{M'}) = \{P_1, \dots, P_n\}$

(c) If $(*)$ is minimal (i.e. n is minimal), then $n = \#\mathrm{Ass}(M/_{M'})$

In this case we have when P_i is minimal over $\mathrm{Ann}(M/_{M'})$ that

$M_i = \ker(M \longrightarrow (M/_{M'})_{P_i})$ "P_i-primary component of M'".

(d) Assume $(*)$ is minimal and let $U \subseteq R$ be mult. closed.

Let $P_1, \dots, P_t$ be elts of $\mathrm{Ass}(M/_{M'})$ that are disjoint from U.

Then $U^{-1}M' = U^{-1}M_1 \cap \dots \cap U^{-1}M_t$ is a minimal primary decomposition of $U^{-1}M' \subseteq U^{-1}M$ over $U^{-1}R$.

Proof

A submodule $N \subseteq M$ is irreducible if $N = N_1 \cap N_2 \Rightarrow N = N_1$ or $N = N_2$.

M Noetherian $\Rightarrow$ $M' = M_1 \cap \dots \cap M_n$, M_i irreducible.

(Else take $M' \subseteq M$ max s.t. M' not intersection of irreds $\Rightarrow M = M_1 \cap M_2$, $M \subsetneq M_i$. M_i = intersection of irreds. $\lightning$.)

Claim: $N \subseteq M$ irred. $\Rightarrow$ N is primary.

otherwise take $P \neq Q \in \mathrm{Ass}(M/_N)$.

$R/P \cong K_1 \subseteq M/_N$, $R/Q \cong K_2 \subseteq M/_N$.

If $0 \neq x \in K_1 \cap K_2$, then $P = \mathrm{Ann}(x) = Q$ $\lightning$.

$\therefore$ $K_1 \cap K_2 = 0 \Rightarrow N$ not irreducible.

Have proved: $\exists$ primary decomposition

$$(*)\quad M' = M_1 \cap M_2 \cap \dots \cap M_n, \qquad M_i \ \ P_i\text{-primary}.$$

(a) – (d) are statements about M/M'. WLOG $M' = 0$.

(a): $M \subseteq \bigoplus_{i=1}^{n} M/M_i \Rightarrow \mathrm{Ass}(M) \subseteq \mathrm{Ass}(\oplus M/M_i) = \{P_1, \dots, P_n\}$.

(b): $(*)$ not redundant $\Rightarrow N_j = \bigcap_{i \neq j} M_i \neq 0 \quad \forall j$.

$$M_j \cap N_j = 0 \Rightarrow N_j = N_j/N_j \cap M_j \cong N_j + M_j/M_j \subseteq M/M_j$$

$$\Rightarrow \{P_j\} = \mathrm{Ass}(N_j) \subseteq \mathrm{Ass}(M).$$

(c): Assume $(*)$ is minimal.

If $P_i = P_j$ then we can replace M_i, M_j with $M_i \cap M_j$ $\lightning$.

This proves $n = \# \mathrm{Ass}(M)$.

Assume that P_i is minimal over $\mathrm{Ann}(M)$.

$$\begin{tikzcd} & M_{P_i} \arrow[dr, "\gamma"] & \\ M \arrow[ur, "\alpha"] \arrow[dr, "\beta"'] & & (M/M_i)_{P_i} \\ & M/M_i \arrow[ur, "\delta"'] & \end{tikzcd}$$

<u>Claim:</u> γ and δ are injective.

δ injective: $\mathrm{Ass}(M/M_i) = \{P_i\} \Rightarrow R \setminus P_i$ nzds on M/M_i

$$\Rightarrow M/M_i \subseteq (M/M_i)_{P_i}.$$

γ injective: $M \hookrightarrow \bigoplus_{j=1}^{n} M/M_j$

$$\Rightarrow M_{P_i} \hookrightarrow \bigoplus_{j=1}^{n} (M/M_j)_{P_i}$$

$j \neq i \Rightarrow P_j \not\subseteq P_i$ (since P_i min. over $\mathrm{Ann}(M)$)

$\Rightarrow \exists\, r \in P_j \setminus P_i$.

$r^k \cdot (M/M_j) = 0$ for some k (by Prop.) $\Rightarrow (M/M_j)_{P_i} = 0$.

$\therefore\ \gamma : M_{P_i} \hookrightarrow (M/M_i)_{P_i}$

Claim $\Rightarrow$ $\ker(M \xrightarrow{\alpha} M_{P_i}) = \ker(\beta) = M_i$

(d): Assume $M = M_1 \cap \dots \cap M_n$ minimal.

$$\mathrm{Ass}(U^{-1}(M/M_i)) = \{U^{-1}P \mid P \in \mathrm{Ass}(M/M_i) \text{ and } P \cap U = \emptyset\}$$

$$= \begin{cases} \{U^{-1}P_i\} & \text{if } P_i \cap U = \emptyset \\ \emptyset & \text{else} \end{cases}$$

$\therefore$ $U^{-1}M_i \subseteq U^{-1}M$ is $U^{-1}P_i$ - primary for $P_i \cap U = \emptyset$, $(i \le t)$ and

$U^{-1}M_i = U^{-1}M$ for $P_i \cap U \neq \emptyset$. $(i > t)$

$0 = U^{-1}M_1 \cap \cdots \cap U^{-1}M_t$ primary decomp. over $U^{-1}R$.

Minimal because $\operatorname{Ass}(U^{-1}M) = \{U^{-1}P_1, \ldots, U^{-1}P_t\}$.

$\square$

Com. Alg. 9/21/2010

Primary Decomp. and unique factorization

Recall: R domain. $x \in R$.

x irreducible $\Leftrightarrow$ $(\forall a,b \in R: x = ab \Rightarrow (a) = R$ or $(b) = R)$

x prime elt. $\Leftrightarrow$ $(x) \subseteq R$ prime ideal.

x prime elt. $\Rightarrow$ x irreducible

Lemma R Noetherian domain. Then R is a UFD $\Leftrightarrow$ all irred. elts are also prime elts.

Proof
(1) Every $a \in R$ is product of prime elts.
Otherwise choose counter example with $(a) \subseteq R$ maximal.
Then a is not irreducible $\Rightarrow$ $a = a_1 \cdot a_2$, $(a_i) \neq R$.
WLOG a_1 not product of primes.
$(a) \subseteq (a_1)$ $\Rightarrow$ $(a) = (a_1)$ $\Rightarrow$ $\exists r \in R:$ $a_1 = ra = a_1 a_2 r$

But then $a_2 r = 1$ $\lightning$.

(2) Factorization unique: Exercise.

$\square$

Prop R Noeth. domain.
(a) ~~Write~~ $f = p_1^{e_1} \cdots p_n^{e_n}$, $p_i \in R$ prime elt., $(p_i) \neq (p_j)$ for $i \neq j$.
Then $(f) = (p_1^{e_1}) \cap \cdots \cap (p_n^{e_n})$ is minimal primary decomp of (f).
(b) R is a UFD $\Leftrightarrow$ All minimal primes over principal ideals are principal.

Proof
(a) $(p_i^{e_i})$ is (p_i)-primary because $(p_i)^{e_i} \subseteq (p_i^{e_i})$ and

$rs \in (p_i^{e_i})$, $r \notin (p_i)$ $\Rightarrow$ $s \in (p_i^{e_i})$.

($rs = a p_i^{e_i}$. $rs \in (p_i)$, $r \notin (p_i) \Rightarrow s \in (p_i)$ $\Rightarrow$ $s = s' p_i$.
$r s' = a p_i^{e_i - 1}$ Induction $\Rightarrow$ $s' \in (p_i^{e_i-1})$ $\Rightarrow$ $s \in (p_i^{e_i})$.)

Claim: $(f) = (p_1^{e_1}) \cap \cdots \cap (p_n^{e_n})$.

Enough to show: $p \in R$ prime elt. and $p \nmid g \in R$ $\Rightarrow$ $(p^e g) = (p^e) \cap (g)$.

$\subseteq$: clear.

$\supseteq$: Let $h \in R$, assume $gh \in (p^e)$. Will show $gh \in (p^e g)$.

Then $gh \in (p) \Rightarrow h \in (p)$.

$g \cdot \frac{h}{p} \in (p^{e-1}) \Rightarrow$ (Induction) $g \cdot \frac{h}{p} \in (g p^{e-1}) \Rightarrow gh \in (p^e g)$.

(b): $\Rightarrow$: ~~[illegible]~~ Assume P min. over (f).

Write $f = p_1^{e_1} \cdots p_n^{e_n}$, $p_i \in R$ prime elt.

Then $p_i \in P$ for some i.

$(f) \subseteq (p_i) \subseteq P \Rightarrow P = (p_i)$. principal.

$\Leftarrow$: Let $x \in R$ be irreducible.

Let P min prime over (x).

Then $P = (p)$ principal.

$x = ap \Rightarrow (a) = R$, $P = (x)$, x prime.

□

<u>Thm</u> (Cayley-Hamilton)

R ring, $J \subseteq R$ ideal, M R-module gen. by n elts.

$\varphi : M \longrightarrow M$ R-homomorphism.

Assume that $\varphi(M) \subseteq J \cdot M$.

Then $\exists$ polynomium $p(x) = x^n + a_1 x^{n-1} + \cdots + a_n \in R[x]$

such that $p(\varphi) = 0 \in \mathrm{End}(M)$ and $a_i \in J^i$

~~[illegible]~~

<u>Remark</u> If $M = R^n$ then φ is given by matrix $A \in \mathrm{Mat}_{n \times n}(R)$.

C.H. $\Rightarrow p(\varphi) = 0$ where $p(x) = \chi_A(x) = \det(xI - A)$

$\varphi(M) \subseteq JM \Rightarrow A \in \mathrm{Mat}_n(J) \Rightarrow a_i \in J^i$.

<u>Proof</u> M gen. by $m_1, \dots, m_n \in M$.

Write $\varphi(m_j) = \sum_i a_{ij} m_i$, $a_{ij} \in J$.

Set $A = (a_{ij}) \in \mathrm{Mat}_n(R)$.

M module over $R[x]$: $x \cdot m = \varphi(m)$, $p(x) \cdot m = p(\varphi)(m)$.

$(xI - A) \begin{bmatrix} m_1 \\ \vdots \\ m_n \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix} \Rightarrow \det(xI - A) \cdot m_i = 0 \quad \forall i$ $\therefore \chi_A(\varphi) = 0 \in \mathrm{End}(M)$

□

Thm (Cayley-Hamilton)

R ring, $J \subseteq R$ ideal, M R-module gen. by n elts.
$\varphi : M \to M$ R-hom. Assume $\varphi(M) \subseteq J \cdot M$.
Then $\exists$ polynomial $p(x) = x^n + a_1 x^{n-1} + \dots + a_n \in R[x]$
such that $p(\varphi) = 0 \in \mathrm{End}(M)$ and $a_i \in J^i$ $\forall i$.

Cor R ring, M f.g. R-module.
(a) Every surjective R-hom. $\alpha : M \to M$ is an isomorphism.
(b) If $M \cong R^n$ and $\{m_1, \dots, m_n\}$ generate M, then $\{m_1, \dots, m_n\}$ is basis.

Proof

M is an $R[t]$-module, $p(t) \cdot m = p(\alpha)(m)$.
$\varphi := id : M \to M$.
α surjective $\Rightarrow \varphi(M) \subseteq (t) \cdot M$.
C.H. $\Rightarrow \exists$ $p(x) = x^n + a_1 x^{n-1} + \dots + a_n$ so that
$p(id) = 0 \in \mathrm{End}(M)$ and $a_i \in (t^i) \subseteq R[t]$
Note: $p(1) = 1 - q(t) \cdot t$, $q(t) \in R[t]$.
$(1 - q(t) \cdot t) \cdot M = p(1) \cdot M = p(id)(M) = 0$
$\Rightarrow$ $q(\alpha) \circ \alpha = id : M \to M$ $\Rightarrow$ α injective, iso.

(b) Assume $\gamma : M \to R^n$ iso and $m_1, \dots, m_n$ generate M.
$\beta : R^n \twoheadrightarrow M$ surjective, $\beta(e_i) = m_i$.
$\beta\gamma : M \to M$ surjective $\Rightarrow \beta\gamma$ iso $\Rightarrow \beta = (\beta\gamma)\gamma^{-1}$ iso
$\Rightarrow \{m_1, \dots, m_n\}$ basis.

□

Prop R ring, $J \subseteq R[x]$ ideal, $S = R[x]/J$, $s = x + J \in S$.

(a) S is generated by $\leq n$ elts. as R-module
$\Leftrightarrow$ J contains a monic polynomial of degree n.
In this case, S is gen. by $1, s, \dots, s^{n-1}$.

(b) S is a f.g. free R-module
$\Leftrightarrow$ J is generated by a monic polynomial.
In this case, $\{1, s, s^2, \dots, s^{n-1}\}$ is a basis, $n = \mathrm{rank}_R(S)$.

Proof

(a) $\Leftarrow$: Assume $p(x) = x^n + a_1 x + \dots + a_n \in J$.

$d \geq n \Rightarrow s^d = -a_1 s^{d-1} - \dots - a_n s^{d-n}$

$\therefore$ S generated by $1, s, \dots, s^{n-1}$.

$\Rightarrow$: $\varphi : S \longrightarrow S$, $\varphi(m) = sm$ satisfies $\varphi(S) \subseteq R \cdot S$.

$\Rightarrow \varphi^n + a_1 \varphi^{n-1} + \dots + a_n = 0 \in \mathrm{End}_R(S)$ by C.H.

$\Rightarrow s^n + a_1 s^{n-1} + \dots + a_n = 0 \in S$

$\Rightarrow x^n + a_1 x^{n-1} + \dots + a_n \in J$.

(b) $\Leftarrow$: Assume $J = (p(x))$, $p(x) = x^n + a_1 x^{n-1} + \dots + a_n$.

Then S gen. by $1, s, \dots, s^{n-1}$ as R-module.

Linearly independent:

$\sum_{i=0}^{n-1} b_i s^i = 0 \Rightarrow \sum_{i=0}^{n-1} b_i x^i \in (p(x)) \Rightarrow b_i = 0 \ \forall i$.

$\therefore$ $\{1, s, \dots, s^{n-1}\}$ basis for S.

$\Rightarrow$: Assume $S \cong R^n$. Then $\exists$ $p(x) = x^n + a_1 x^{n-1} + \dots + a_n \in J$.

$1, s, s^2, \dots, s^{n-1}$ generate S $\Rightarrow$ basis for S by Cor.

Claim: $J = (p(x))$.

Let $f(x) \in J$. Write $f(x) = g(x) p(x) + h(x)$, $\deg(h) < n$.

$h(x) = \sum_{i=0}^{n-1} b_i x^i \in J \Rightarrow \sum_{i=0}^{n-1} b_i s^i = 0 \Rightarrow b_i = 0 \ \forall i$.

$\therefore$ $f(x) \in (p(x))$.

$\square$

<u>Def</u> R ring, S (commutative) R-algebra.
I.e. S ring with ring hom. $R \to S$.

1) Let $s \in S$. s is <u>integral over R</u> if s is a root of a monic polynomium with coefs. in R.
2) S is <u>integral over R</u> if all elts in S are integral over R.
3) S is <u>finite over R</u> if S f.g. as R-module.

<u>Lemma</u> S finite over R $\Rightarrow$ S integral over R.

<u>Proof</u> Let $s \in S$. Def. $\varphi : S \to S$, $\varphi(m) = sm$.
C.H. $\Rightarrow$ $p(\varphi) = 0 \in \mathrm{End}(S)$ for some monic $p(x) \in R[x]$.
Now $p(s) = p(\varphi)(1) = 0 \in S$.
□

<u>Cor</u> S finite over R $\Leftrightarrow$
S generated as R-algebra by finitely many integral elements.

<u>Proof</u>
$\Rightarrow$: clear from Lemma.
$\Leftarrow$: Assume $S = R[a_1, \dots, a_n]$, a_i integral over R.
Induction $\Rightarrow$ $S' = R[a_1, \dots, a_{n-1}]$ finite over R.
Prop $\Rightarrow$ $S = S'[a_n]$ finite over S'.
$\therefore$ S finite over R.
□

<u>Thm</u> R ring, S R-algebra.
Then $\bar{R} = \{ s \in S \mid s \text{ integral over } R \}$ is a subalgebra of S.

<u>Proof</u> Let $s, t \in \bar{R}$.
Then $R[s,t] \subseteq S$ is a f.g. R-module
$\Rightarrow$ $R[s,t]$ is integral over R
$\Rightarrow$ $s+t$, $s-t$, $st \in \bar{R}$.
□

<u>Def</u> $\bar{R} = \{ s \in S \mid s \text{ integral over } R \}$ is called the <u>integral closure</u> of R in S.

The following implies that $\bar{\bar{R}} = \bar{R} \subseteq S$.

<u>Prop</u> Let $R \subseteq S \subseteq T$ be (sub) rings.
If S integral over R and T integral over S, then T integral over R.

Proof Let $t \in T$.

Write $t^n + a_1 t^{n-1} + \dots + a_n = 0$, with $a_i \in S$.

$R' := R[a_1, \dots, a_n]$ is finite over R.

$R'[t]$ is finite over R'.

Conclude $R'[t]$ is finite over R $\Rightarrow$ t is integral over R.

□

Cor M f.g. R-module, $I \subseteq R$ ideal.

If $M = IM$, then $\exists\, r \in I$: $rm = m$ $\forall m \in M$.

Proof

$\varphi = \mathrm{id} : M \longrightarrow M$ satisfies $\varphi(M) \subseteq IM$.

C.H. $\Rightarrow$ $\varphi^n + a_1 \varphi^{n-1} + \dots + a_n = 0 \in \mathrm{End}(M)$, $a_i \in I$.

$\Rightarrow$ $r = (-a_1 - a_2 - \dots - a_n) = 1 \in \mathrm{End}(M)$.

□

Def The Jacobson radical of a ring R is the intersection of all max. ideals

Nakayama's lemma (NAK)

R ring, M f.g. R-module, $I \subseteq R$ ideal. Assume $I \subseteq$ Jacobson radical.

(a) $IM = M$ $\Rightarrow$ $M = 0$

(b) Let $m_1, \dots, m_n \in M$.

If $\overline{m_1}, \dots, \overline{m_n}$ generate M/IM then $m_1, \dots, m_n$ generate M.

Proof

(a) Choose $r \in I$ s.t. $rm = m$ $\forall m \in M$. Then $(r-1) \cdot M = 0$.

Since $r \in$ all max ideals, $r-1 \in R$ is a unit, so $M = 0$.

(b) Set $N = M/\langle m_1, \dots, m_n \rangle$.

M/IM gen. by $\overline{m_1}, \dots, \overline{m_n}$ $\Rightarrow$ $M = IM + \langle m_1, \dots, m_n \rangle$

$\Rightarrow$ $N = IN$ $\Rightarrow$ $N = 0$.

□

Remark Often applied when (R, m) local ring:

M f.g. R-module and $M/mM = 0$ $\Rightarrow$ $M = 0$.

Example $R = \mathbb{Z}_{(p)} = \{ \frac{a}{b} \in \mathbb{Q} \mid (p, b) = 1 \}$. $M = \mathbb{Q}$.

$\mathbb{Q}/(p)\mathbb{Q} = 0$ but $\mathbb{Q} \neq 0$.

Cor Let M and N be f.g. R-modules.
If $M \otimes_R N = 0$ then $\mathrm{Ann}(M) + \mathrm{Ann}(N) = R$.
If R is local then this means that $M=0$ or $N=0$.

Proof

Assume $M \otimes N = 0$ and $\mathrm{Ann}(M) + \mathrm{Ann}(N) \subsetneq R$ proper.

Choose prime ideal $P \supseteq \mathrm{Ann}(M) + \mathrm{Ann}(N)$.

Note: $\mathrm{Ann}(M_P) + \mathrm{Ann}(N_P) \underset{\text{f.g.}}{=} \mathrm{Ann}(M)_P + \mathrm{Ann}(N)_P \subseteq P_P$.

Replace (R, M, N) with (R_P, M_P, N_P). WLOG (R, P) local.

Since $M \neq 0$, must have $M/PM \neq 0$ by NAK.

M/PM vector space over $R/P \Rightarrow \exists$ linear map $M/PM \twoheadrightarrow R/P$.

$0 = M \otimes_R N \twoheadrightarrow R/P \otimes_R N \cong N/PN$

$\Rightarrow N = PN \Rightarrow N = 0$ (by NAK).

$\lightning$ since $\mathrm{Ann}(N) \subseteq P$.

$\square$

Com. Alg. 9/28/2010 Normalization (1)

R domain with field of fractions $K = K(R) = R_0$.

Def The normalization of R is $\overline{R} = \{s \in K \mid s \text{ integral over } R\}$

R is normal if $\overline{R} = R \subseteq K$

Note $K(\overline{R}) = K$ and $\overline{\overline{R}} = \overline{R} \subseteq K$. So $\overline{R}$ is normal.

Example
$\mathbb{Z} \subseteq \mathbb{Q}$ is normal.

Prop R UFD $\Rightarrow$ R normal.

Proof Assume $\frac{r}{s} \in K$ integral over R.

WLOG r, s relatively prime.

$\exists \ (\frac{r}{s})^n + a_1 (\frac{r}{s})^{n-1} + \dots + a_n = 0, \quad a_i \in R.$

$\Rightarrow r^n + s a_1 r^{n-1} + \dots + s^n a = 0$

$\Rightarrow s \mid r^n \Rightarrow s \in R$ unit $\Rightarrow \frac{r}{s} \in R$.

□

Prop $R \subseteq S$ rings, $f(x) \in R[x]$ monic polynomial.
Assume that $f(x) = g(x) \cdot h(x)$ where $g(x), h(x) \in S[x]$ are monic.
Then the coefs of $g(x)$ and $h(x)$ are integral over R. $(g(x), h(x) \in \overline{R}[x])$

Proof Induction on $\deg(g(x))$.

If $\deg(g(x)) = 0$ then $g(x) = 1$ and $h(x) = f(x) \in R[x]$.

Assume $\deg(g(x)) \geq 1$.

Set $S' = S[t]/(g(t))$, $\alpha = \overline{t} \in S'$.

Write $g(x) = g_1(x) \cdot (x - \alpha) \in S'[x]$.

$f(x) = f_1(x) \cdot (x - \alpha) \in R'[x]$, $\quad R' = R[\alpha] \subseteq S'$.

$f_1(x) = g_1(x) \cdot h(x) \Rightarrow g_1(x), h(x) \in \overline{R'}[x] \subseteq S'[x]$.

$f(\alpha) = 0 \Rightarrow \alpha \in \overline{R} \Rightarrow \overline{R'} = \overline{R}. \subseteq S'$

$\therefore g(x), h(x) \in \overline{R}[x]$.

□

Cor R normal domain with fraction field K, $f(x) \in R[x]$ monic.
$f(x)$ irred. in $R[x]$ $\Leftrightarrow$ $f(x)$ irred. in $K[x]$.

Cor R normal domain. Every irreducible monic polynomial in $R[x]$ is a prime element. ②

Proof Let $f(x) \in R[x]$ be irred and monic.

Then $f(x) \in K[x]$ is irred., so $(f(x)) \subseteq K[x]$ prime ideal.

$R[x]/(f(x))$ free R-module $\Rightarrow R[x]/(f(x)) \subseteq R[x]/(f(x)) \otimes_R K = \underbrace{K[x]/(f(x))}_{\text{field}}$

$\Rightarrow R[x]/(f(x))$ domain $\Rightarrow (f(x)) \subseteq R[x]$ prime ideal.

□

Prop Let $R \subseteq S$ be rings, $U \subseteq R$ mult. closed.

Then $\overline{U^{-1}R} = U^{-1}(\overline{R}) \subseteq U^{-1}S$.

$\boxed{\begin{array}{l} \overline{U^{-1}R} = \text{int. closure of } U^{-1}R \text{ in } U^{-1}S \\ \overline{R} = \text{int. closure of } R \text{ in } S. \end{array}}$

Proof

$\supseteq$: U^{-1} and $\overline{R}$ integral over $U^{-1}R$

$\Rightarrow U^{-1}\overline{R} \subseteq \overline{U^{-1}R}$.

$\subseteq$: Assume $\frac{s}{u} \in U^{-1}S$ is integral over $U^{-1}R$.

$\left(\frac{s}{u}\right)^n + \frac{a_1}{u_1}\left(\frac{s}{u}\right)^{n-1} + \dots + \frac{a_n}{u_n} = 0$, $a_i \in R$, $u_i \in U$.

Set $t = s \cdot u_1 u_2 \cdots u_n$. Multiply with $(u \cdot u_1 u_2 \cdots u_n)^n$:

$t^n + a_1 u \frac{u_1 \cdots u_n}{u_1} t^{n-1} + \dots + a_n u^n \frac{(u_1 \cdots u_n)^n}{u_n} = 0$

$\therefore t \in \overline{R} \Rightarrow \frac{s}{u} \in U^{-1}\overline{R}$.

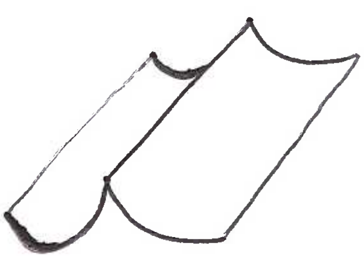
□

Cor R normal domain $\Rightarrow U^{-1}R$ normal domain.

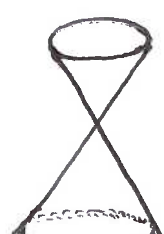
Proof $K(U^{-1}R) = K(R)$. $\overline{U^{-1}R} = U^{-1}\overline{R} = U^{-1}R$. □

Geometric meaning: $X \subseteq \mathbb{A}^n$ alg. subset, $A(X) = k[x_1, \dots, x_n]/I(X)$, $k = \overline{k}$.

$A(X)$ normal $\Rightarrow$ singularities of X is closed subset of codim. ≥ 2.



$A(X)$ not normal.



$A(X)$ is normal

X curve: X non-singular $\Leftrightarrow A(X)$ normal.

Soon: (Finiteness of integral closure) R f.g. domain over k $\Rightarrow$ $\overline{R}$ f.g. domain over k.

Let $X \subseteq \mathbb{A}^n$ be an irred. alg. set.

Write $\overline{A(X)} \cong k[y_1, \dots, y_m]/J$, J prime ideal.

Def. $\overline{X} = Z(J) \subseteq \mathbb{A}^m$. The <u>normalization</u> of X.

$x_i \in \overline{A(X)} \Rightarrow x_i = f_i(y_1, \dots, y_m)$.

Def. $\pi : \overline{X} \longrightarrow X$, $\pi(b_1, \dots, b_m) = (f_1(b), \dots, f_n(b))$

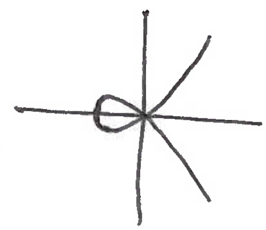
Remark π is "bijective most places."

I.e. $y_j = \dfrac{p_j(x_1, \dots, x_n)}{q_j(x_1, \dots, x_n)}$ rational function on X.

$X \dashrightarrow \overline{X}$, $(a_1, \dots, a_n) \mapsto (y_1(a), \dots, y_m(a))$ defined when $q_j(a) \neq 0 \ \forall j$.

Result: $\overline{X}$ = "X with worst singularities straightened out".

Example $X = Z(y^2 - x^2 - x^3) \subseteq \mathbb{A}^2$



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

Set $t = \frac{y}{x}$.

$t^2 - 1 - x = 0 \Rightarrow t$ integral over $A(X)$.

$\overline{A(X)} = k[t] \subseteq k(t)$. $\overline{X} = \mathbb{A}^1$.

$x = t^2 - 1$, $y = tx = t^3 - t$

$\pi : \overline{X} \longrightarrow X$, $t \longmapsto (t^2 - 1, t^3 - t)$

<u>Significance of $\overline{U^{-1}R} = U^{-1}\overline{R}$:</u>

If X glued together from alg. sets (i.e. X alg. variety) then one can normalize the pieces and glue them together to obtain $\pi : \overline{X} \longrightarrow X$.

Def An <u>affine ring</u> is a ring that is f.g. over a field.

I.e. $k[x_1, \dots, x_n]/I$.

Remark Let $f \in k[x_1, \dots, x_n]$. $f = f_0 + f_1 x_n + \dots + f_d x_n^d$, $f_i \in k[x_1, \dots, x_{n-1}]$.
If f monic in x_n (i.e. $f_d \in k$) then $k[x_1, \dots, x_n]$ finite over $k[x_1, \dots, x_{n-1}, f]$.
x_n integral over $k[x_1, \dots, x_{n-1}, f]$ because $f_d x_n^d + \dots + f_1 x_1 + (f_0 - f) = 0$.

Noether's Normalization Theorem (Lite)

Every affine ring is a finite extension of a polynomial ring.

I.e. R affine ring$/_k$ $\Rightarrow$ $\exists\, S \subseteq R$ subring such that R f.g. S-module and $S \cong k[x_1, \dots, x_r]$.

Proof

Induction on # generators of R/k.

zero generators: $R = k$, $S = k$ works.

Assume R generated by n elts. $R = k[x_1, \dots, x_n]/I$.

WLOG $I \neq 0$.

Let $0 \neq f \in I$.

Assume f is monic in x_n: Then $k[x_1, \dots, x_n]$ finite over $T = k[x_1, \dots, x_{n-1}, f]$

$\Rightarrow R = k[x_1, \dots, x_n]/I$ finite over $T/I \cap T$.

T/IT generated by $\overline{x_1}, \dots, \overline{x_{n-1}}$.

Induction $\Rightarrow$ $T/I \cap T$ finite extension of polynomial ring.

Write $f = \sum c_{\underline{a}} x^{\underline{a}}$, $\quad x^{\underline{a}} = x_1^{a_1} \cdots x_n^{a_n}$, $\quad c_{\underline{a}} \in k$.

Choose $e \in \mathbb{N}$ s.t. $e > \max\{a_i\}$ for all $\underline{a}$ s.t. $c_{\underline{a}} \neq 0$.

Set $x_i' = x_i - x_n^{e^i}$ for $1 \leq i \leq n-1$.

Then $k[x_1, \dots, x_n] = k[x_1', \dots, x_{n-1}', x_n]$

Claim: f is monic in x_n as poly. in $k[x_1', \dots, x_{n-1}', x_n]$.

$$x_1^{a_1} \cdots x_n^{a_n} = (x_1' + x_n^{e})^{a_1} (x_2' + x_n^{e^2})^{a_2} \cdots (x_{n-1}' + x_n^{e^{n-1}})^{a_{n-1}} \cdot x_n^{a_n}$$

is monic in x_n, largest term is $x_n^{a_n + a_1 e + \cdots + a_{n-1} e^{n-1}}$.

Choice of e $\Rightarrow$ All monomials occurring in f have distinct highest terms (so they don't cancel!)

$\therefore$ $f \in k[x_1', \dots, x_{n-1}', x_n]$ monic in x_n.

$\Rightarrow$ $k[x_1, \dots, x_n]$ finite over $k[x_1', \dots, x_{n-1}', f] =: T$

R finite over $T/I \cap T$, $\quad T/I \cap T$ gen. by $\overline{x_1'}, \dots, \overline{x_{n-1}'}$,

so finite over poly. ring.

$\square$

Galois theory Quiz

Do you know:

$K \subseteq L$ field ext.

Alg. closure $\overline{K}$?

$\alpha \in L$ alg. over K. $\mathrm{Irr}(\alpha, K) = ?$

L/K separable extension ?

L/K purely inseparable ?

L/K normal ?

Fact: $K \subseteq N$ finite normal extension, $\alpha, \beta \in N$ conjugate $/K$.
Then $\exists\ \varphi \in \mathrm{Aut}_K(N)$ s.t. $\varphi(\alpha) = \beta$.

Fact: N field, $G \subseteq \mathrm{Aut}(N)$ finite subgroup.
Then N/N^G finite Galois extension
with $\mathrm{Gal}(N/N^G) = G$.

Noether's Normalization Theorem

R affine ring over k. Then $\exists$ subring $S \subseteq R$ s.t. R f.g. S-module and $S \cong k[x_1, \dots, x_p]$.

Proof

Induction on # gens.

Assume $R = k[x_1, \dots, x_n]/I$, $I \neq 0$.

Let $0 \neq f \in I$.

Write $f = \sum c_{\underline{a}} x^{\underline{a}}$, $x^{\underline{a}} = x_1^{a_1} \cdots x_n^{a_n}$, $c_{\underline{a}} \in k$.

Choose $e \in \mathbb{N}$ s.t. $e > \max\{a_1, \dots, a_n\}$ for all $\underline{a}$ s.t. $c_{\underline{a}} \neq 0$.

Set $x_i' = x_i - x_n^{e^i}$ for $1 \le i \le n-1$.

Then $k[x_1, \dots, x_n] = k[x_1', \dots, x_{n-1}', x_n]$

Claim: f is monic in x_n as poly in $k[x_1', \dots, x_{n-1}', x_n]$

$$x_1^{a_1} \cdots x_n^{a_n} = (x_1' + x_n^{e})^{a_1} (x_2' + x_n^{e^2})^{a_2} \cdots (x_{n-1}' + x_n^{e^{n-1}})^{a_{n-1}} x_n^{a_n}$$

is monic in x_n, largest term is $x_n^{a_n + a_1 e + \cdots + a_{n-1} e^{n-1}}$

Choice of $e \Rightarrow$ All monomials occurring in f have distinct highest terms (so they don't cancel!)

$\therefore$ $f \in k[x_1', \dots, x_{n-1}', x_n]$ monic in x_n.

$\Rightarrow$ $k[x_1, \dots, x_n]$ finite over $k[x_1', \dots, x_{n-1}', f] =: T$.

$\Rightarrow$ R finite over T/IT.

T/IT gen. by $\overline{x_1'}, \dots, \overline{x_{n-1}'}$, so finite over poly ring.

$\square$

Com. Alg. 10/1/2010 ①

Weak Nullstellensatz

$k=\bar{k}$ alg. closed, $I \subsetneq k[x_1,\dots,x_n]$ proper ideal. Then $Z(I) \neq \emptyset \subseteq \mathbb{A}^n$.

Proof WLOG I max. ideal. $L = k[x_1,\dots,x_n]/I$ field.

NNT $\Rightarrow$ $\exists$ finite ring extension $k[y_1,\dots,y_m] \subseteq L$.

Assume $m>0$. Then $y_1^{-1} \in L$ is integral over $k[y_1,\dots,y_m]$. But $k[y_1,\dots,y_m]$ is normal. ↯

$\therefore$ $k \subseteq k[x_1,\dots,x_n]/I$ finite extension.

$k=\bar{k} \Rightarrow k \xrightarrow{\cong} k[x_1,\dots,x_n]/I$ isomorphism.

Choose $a_i \in k$ s.t. $x_i \equiv a_i \pmod{I}$.

$(x_1-a_1,\dots,x_n-a_n) \subseteq I \Rightarrow I=(x_1-a_1,\dots,x_n-a_n) \Rightarrow Z(I)=\{(a_1,\dots,a_n)\}$

□

Nullstellensatz $k=\bar{k}$, $I \subseteq k[x_1,\dots,x_n]$ ideal. Then $I(Z(I))=\sqrt{I}$.

Proof $\subseteq$: $I=(f_1,\dots,f_m)$. Let $g \in I(Z(I))$.

Set $J=(f_1,\dots,f_m, yg-1) \subseteq k[x_1,\dots,x_n,y]$

Then $Z(J)=\emptyset \subseteq \mathbb{A}^{n+1}$.

Weak NSS $\Rightarrow$ $1 = a_1f_1+\dots+a_mf_m + a_{m+1}(yg-1)$, $a_i \in k[x_1,\dots,x_n,y]$

Set $y=g^{-1}$: $1 = a_1(x_1,\dots,x_n,g^{-1})\cdot f_1 + \dots + a_m(x_1,\dots,x_n,g^{-1})\cdot f_m$

Multiply with g^N: $g^N \in (f_1,\dots,f_m)=I \Rightarrow g\in\sqrt{I}$.

□

Prop (Going up). $R\subseteq S$ integral ring extension, $P \subseteq R$ prime ideal, $J \subsetneq S$ ideal. Assume $J \cap R \subseteq P$.

Then $\exists$ prime $Q \subseteq S$ s.t. $J \subseteq Q$ and $Q\cap R = P$.

$$\begin{array}{ccc} R & \subseteq & S \\ \cup\!\!| & & \cup\!\!| \\ P & \longleftrightarrow & Q \\ & & \cup\!\!| \\ & & J \end{array}$$

Proof Replace R with $R/J\cap R$ and S with S/J.

WLOG: $J=0$.

Replace R with R_P and S with $(R\setminus P)^{-1}S$.

WLOG: (R,P) local ring.

Claim: $PS \neq S$.

Otherwise write $1 = p_1 s_1 + \dots + p_n s_n$, $p_i \in P$, $s_i \in S$.

$S' = R[s_1, \dots, s_n]$ finite over R and $PS' = S'$.

NAK $\Rightarrow S' = 0$ ↯

Let $Q \subseteq S$ max ideal with $Q \supseteq PS$.

Then $P \subseteq Q \cap R \neq R \Rightarrow P = Q \cap R$.

□

<u>Lemma</u> Assume $R \subseteq S$ domains, $K(R) \subseteq K(S)$ alg. extension, $0 \neq J \subseteq S$ ideal.
Then $J \cap R \neq 0$.

<u>Proof</u> Let $0 \neq x \in J$.

x alg. over $K(R) \Rightarrow x^n + \frac{a_1}{b_1} x^{n-1} + \dots + \frac{a_n}{b_n} = 0$, $a_i, b_i \in R$.

Replace x with $b_1 b_2 \dots b_n x$: $x^n + a_1' x^{n-1} + \dots + a_n' = 0$, $a_i' \in R$.

WLOG: $a_n' \neq 0$.

But then $a_n' \in (x) \subseteq J \subseteq S \Rightarrow a_n' \in J \cap R$.

□

<u>Cor</u> $R \subseteq S$ integral extension of domains. Then R field $\Leftrightarrow$ S field.

<u>Proof</u> $\Leftarrow$: Let $P \subseteq R$ max. ideal.

Going up $\Rightarrow \exists Q \subseteq S$ prime ideal s.t. $P = Q \cap R$.

S field $\Rightarrow Q = 0 \Rightarrow P = 0 \Rightarrow R$ field.

$\Rightarrow$: Let $0 \neq x \in S$.

Lemma $\Rightarrow xS \cap R \neq 0$.

I.e. $\exists y \in S$: $xy \in R \setminus \{0\}$.

R field $\Rightarrow \exists z \in R$: $xyz = 1$.

□

<u>Cor</u> (Incomparability) Let $R \subseteq S$ be an integral extension of rings.

(1) Let $Q \subseteq S$ prime ideal. Then $Q \subseteq S$ max. $\Leftrightarrow$ $Q \cap R \subseteq R$ max ideal.

(2) Let $Q_1 \subsetneq Q \subseteq S$ prime ideals. Then $Q_1 \cap R \subsetneq Q \cap R$.

<u>Proof</u> (1) S/Q integral extension of $R/Q \cap R$.

S/Q field $\Leftrightarrow$ $R/Q \cap R$ field.

(2) Replace R with $R/Q_1 \cap R$ and S with S/Q_1. WLOG: $Q_1 = 0$.

If $Q \neq 0$ then Lemma $\Rightarrow Q \cap R \neq 0$.

□

Geometry

Def. R ring. $\text{Spec-m}(R) = \{ P \subseteq R \mid P \text{ ~~prime~~ max. ideal} \}$

Let $k = \bar{k}$ alg. closed.

$\mathbb{A}^n \longleftrightarrow \text{Spec-m}(k[x_1, \dots, x_n])$; $(a_1, \dots, a_n) \longleftrightarrow (x_1 - a_1, \dots, x_n - a_n)$

$X \subseteq \mathbb{A}^n$ alg. subset. $A(X) = k[x_1, \dots, x_n]/I(X)$.

Note: $(a_1, \dots, a_n) \in X \iff (x_1 - a_1, \dots, x_n - a_n) \supseteq I(X)$.

$X \leftrightarrow \{ P \in \text{Spec-m}(k[x_1, \dots, x_n]) \mid P \supseteq I(X) \} \longleftrightarrow \text{Spec-m}(A(X))$

Let A be any reduced affine ring over k.

Let $f \in A$. Def. function $f : \text{Spec-m}(A) \longrightarrow k$ as follows:

$P \subseteq A$ max. ideal. $\Rightarrow$ $k \xrightarrow{\cong} A/P$ isomorphism.

$f(P) := f + P \in k$.

Claim: $\text{Spec-m}(A)$ is an algebraic set with coordinate ring A.

$A \cong k[x_1, \dots, x_n]/I$, I radical ideal.

$\text{Spec-m}(A) \longleftrightarrow Z(I) \subseteq \mathbb{A}^n$. $A(Z(I)) \cong A$.

Note: $f \in k[x_1, \dots, x_n]$: $f - f(a) \in I(\{a\}) \Rightarrow f(a) = f + I(\{a\}) \in k[x_1 \dots x_n]/I(a)$.

Let A and B be reduced affine rings over k.

Let $\varphi : A \longrightarrow B$ k-algebra hom:

$$\begin{array}{ccc} A & \xrightarrow{\varphi} & B \\ \cup\!\shortmid & & \cup\!\shortmid \\ k & = & k \end{array}$$

Note $Q \subseteq B$ max ideal $\Rightarrow$

$k \subseteq A \twoheadrightarrow B/Q = k$ $\Rightarrow$ $Q \cap A \subseteq A$ max ideal.

Def $\tilde{\varphi} : \text{Spec-m}(B) \longrightarrow \text{Spec-m}(A)$, $\tilde{\varphi}(Q) = Q \cap A$.

Assume $A = k[x_1, \dots, x_n]/I$, $B = k[Y_1, \dots, Y_m]/J$.

$\varphi(\bar{x}_i) = f_i(\bar{Y}_1, \dots, \bar{Y}_m)$ for $1 \le i \le n$.

Def $\tilde{\varphi} : \mathbb{A}^m \longrightarrow \mathbb{A}^n$, $\tilde{\varphi}(b_1, \dots, b_m) = (f_1(b), \dots, f_n(b))$

Claim : $\tilde{\varphi}(Z(J)) \subseteq Z(I)$ and

$$\begin{array}{ccc} Z(J) & \xrightarrow{\tilde{\varphi}} & Z(I) \\ \updownarrow & \circlearrowleft & \updownarrow \\ \text{Spec-m}(B) & \xrightarrow[\tilde{\varphi}]{} & \text{Spec-m}(A) \end{array}$$

We can lift φ to

$\varphi : k[x_1, \dots, x_n] \longrightarrow k[Y_1, \dots, Y_m]$

$\varphi(x_i) = f_i$. Note : $\varphi(I) \subseteq J$.

Let $b \in Z(J)$, $h \in I$. Show : $h(\tilde{\varphi}(b)) = 0$

$h(\tilde{\varphi}(b)) = \varphi(h)(b) = 0$ since $\varphi(h) \in J$.

Galois Theory

Let $k \subseteq L$ be an alg. field extension, $\alpha \in L$.

$k[x] \longrightarrow k(\alpha) \subseteq L$, $x \mapsto \alpha$. $k(\alpha) \cong k[x]/(\mathrm{Irr}(\alpha, k, X))$

$\mathrm{Irr}(\alpha, k, X) \in k[X]$ unique monic. irred. polynomial with α as root.

Fact $\exists$ alg. closed field $\bar{k}$ s.t. $k \subseteq \bar{k}$ alg. ext.
$\mathrm{Irr}(\alpha, k, X) = \prod_{i=1}^{n} (X - \alpha_i)$, $\alpha_i \in \bar{k}$.

Def α is separable over k if $\mathrm{Irr}(\alpha, k, X)$ has no multiple roots in $\bar{k}$.
α is purely inseparable if $\mathrm{char}(k) = p$ and $\alpha^{p^n} \in k$ for some n.

Note If $\mathrm{char}(k) = 0$ then α separable:
$f(X) = \mathrm{Irr}(\alpha, k, X) = \prod (X - \alpha_i)$.
If $\alpha_1 = \alpha_2$ then $f'(\alpha_1) = f(\alpha_1) = 0$.
$\Rightarrow$ $\gcd(f(x), f'(x))$ has pos. degree and divides $f(X)$. $\lightning$

Def L/k is separable if all elts of L separable over k.
L/k is purely insep. if all elts of L purely insep $/k$.

L/k is normal if ~~[illegible]~~
$\forall \alpha \in L \ \exists \alpha_1, \dots, \alpha_n \in L$: $\mathrm{Irr}(\alpha, k, X) = \prod_{i=1}^{n} (X - \alpha_i) \in L[X]$.

L/k is Galois if normal + separable.

Fact: L/k Galois $\Leftrightarrow$ $\# \mathrm{Aut}_k(L) = [L:k]$

Fact: If $L = k(\alpha_1, \dots, \alpha_n)$ and each α_i separable $/k$ then L/k separable

Fact $k \subseteq L$ finite separable extension.
Then $\exists \alpha \in L$ s.t. $L = k(\alpha)$.

Def $\alpha, \beta \in L$ are conjugate over k if $\mathrm{Irr}(\alpha, k, X) = \mathrm{Irr}(\beta, k, X)$.

Lemma $k \subseteq N$ finite normal ext., $\alpha, \beta \in N$ conjugate over k.
Then $\exists \varphi \in \mathrm{Aut}_k(N)$ s.t. $\varphi(\alpha) = \beta$

Proof $\varphi : k(\alpha) \xrightarrow{\cong} k[x]/\mathrm{Irr}(\alpha, k, X) \xrightarrow{\cong} k(\beta)$, $\varphi(\alpha) = \beta$.

Write $k \subseteq N \subseteq \bar{k}$. Extend φ to $\varphi : N \longrightarrow \bar{k}$.

Claim: $\varphi(N) = N$, i.e. $\varphi \in \mathrm{Aut}_k(N)$

Let $\gamma \in N$. $\varphi(\gamma) \in \overline{k}$ must be root in $\mathrm{Irr}(\gamma, k, X)$.

N/k normal $\Rightarrow \varphi(\gamma) \in N$.

□

Thm N field, $G \subseteq \mathrm{Aut}(N)$ any finite subgroup.

Set $N^G = \{ \alpha \in N \mid \sigma(\alpha) = \alpha \ \forall \sigma \in G \}$.

Then N/N^G is Galois and $\mathrm{Aut}_{N^G}(N) = G$.

Proof

Let $\alpha \in N$. Set $A = \{\sigma(\alpha) \mid \sigma \in G\} \subseteq N$. $\sigma(A) = A$. for $\sigma \in G$.

Set $f(X) = \prod_{\beta \in A} (X - \beta)$.

$\sigma(f(X)) = f(X)$ for all $\sigma \in G \Rightarrow f(X) \in N^G[X]$.

All roots distinct, and all roots in N:

$\therefore N^G \subseteq N$ Galois extension.

Choose $\alpha \in N$ s.t. $N = N^G[\alpha]$.

$\# \mathrm{Aut}_{N^G}(N) \leq \deg \mathrm{Irr}(\alpha, N^G, X) \leq \# G$ and $G \subseteq \mathrm{Aut}_{N^G}(N)$.

$\therefore G = \mathrm{Aut}_{N^G}(N)$

□

Normal closure

$K \subseteq L$ finite extension, $L = K[\alpha_1, \dots, \alpha_n]$.

Set $f(X) = \prod_{i=1}^{n} \mathrm{Irr}(\alpha_i, K, X) \in K[X]$.

Write $f(X) = \prod_{j=1}^{m} (X - \beta_j)$, $\beta_j \in \overline{K}$

Def $N = K[\beta_1, \beta_2, \dots, \beta_m]$ is the normal closure of L over K.

Note: L/K separable $\Rightarrow \alpha_i$ separable $/K \Rightarrow \beta_j$ separable $/K$ $\forall j$

$\Rightarrow N/K$ Galois.

Assume N/K finite normal extension.

$G = \mathrm{Aut}_K(N) \subseteq \mathrm{Aut}(N)$ finite subgroup. $(|G| \leq [N:k])$

Thm $\Rightarrow$ $N^G \subseteq N$ Galois extension.

Claim: $K \subseteq N^G$ is purely inseparable.

Pf
Assume $\alpha \in N$ is not purely insep. over K.
Then α conjugate to $\beta \in N$, $\beta \neq \alpha$.
Lemma $\Rightarrow$ $\exists\, \varphi \in \mathrm{Aut}_K(N)$: $\varphi(\alpha) = \beta$.
$\therefore$ $\alpha \notin N^G$.
□

Let R be a domain. $K = K(R)$. $K \subseteq L$ alg. extension.
Let $\overline{R} \subseteq L$ be integral closure of R in L.

Claim: $L = K \cdot \overline{R}$ In particular, $K(\overline{R}) = L$.

Pf
Let $x \in L$. $x^n + \frac{a_1}{b_1} x^{n-1} + \dots + \frac{a_n}{b_n} = 0$, $a_i, b_i \in R$.
$\Rightarrow$ $b_1 \cdots b_n x$ integral over R
$\Rightarrow$ $x = (b_1 \cdots b_n)^{-1} (b_1 \cdots b_n x) \in K \cdot \overline{R}$.
□

Thm (Finiteness of Integral closure)
R affine domain, $K = K(R)$ fraction field, $K \subseteq L$ finite extension.
$\overline{R} \subseteq L$ integral closure of R in L.
Then $\overline{R}$ is a f.g. R-module.

WARNING: TYPOS!

Proof
WLOG: $R = k[x_1, \dots, x_n]$, $K = k(x_1, \dots, x_n)$. (N.N.T.)
WLOG: L/K normal ext. (replace L with normal closure.)

Set $G = \mathrm{Aut}_K(L)$.

Then $K \subseteq L^G$ purely inseparable, $L^G \subseteq L$ is Galois.

Let $T \subseteq L^G$ be integral closure of R in L^G.

Claim T f.g. R-module.

$L^G = K(\alpha_1, \dots, \alpha_m)$

$\alpha_i^q \in K$ for all i, $q = p^r$, $p = \mathrm{char}(K)$.

I.e. $L^G = K(\sqrt[q]{f_1}, \dots, \sqrt[q]{f_m})$, $f_i = \alpha_i^q = \dfrac{g_i(x_1, \dots, x_n)}{h_i(x_1, \dots, x_n)}$

Let k' be k extended with q-th roots of all coefs in g_i, h_i.

$\Rightarrow \sqrt[q]{f_i} \in k'(\sqrt[q]{x_1}, \dots, \sqrt[q]{x_n})$.

Note: p-th roots are well def. in char. p. $(a+b)^p = a^p + b^p \Rightarrow \sqrt[p]{a+b} = \sqrt[p]{a} + \sqrt[p]{b}$.

$\therefore$ $L^G \subseteq k'(\sqrt[q]{x_1}, \dots, \sqrt[q]{x_n})$

Integral closure of R in $k'(\sqrt[q]{x_i})$ is $k'[\sqrt[q]{x_1}, \dots, \sqrt[q]{x_n}]$, which is finite R-module. Hence T finite R-module.

* Remains to prove:
  Integral closure of T in L is a f.g. T-module.
  More generally:

Prop R Noetherian normal ring. $K \subseteq L$ finite separable extension. $\bar{R} \subseteq L$ integral closure of R in L. Then $\bar{R}$ f.g. R-module.

Proof WLOG: L/K is Galois (replace L with normal closure)

$G = \mathrm{Aut}_K(L) = \{\sigma_1, \dots, \sigma_n\}$

Choose $b_1, \dots, b_n \in \bar{R}$ basis for L over K. (Recall $L = K \cdot \bar{R}$.)

Set $M = [\sigma_i(b_j)]_{i,j} \in \mathrm{Mat}_n(\bar{R})$.

$d = \det(M) \in \bar{R}$. $\sigma_1, \dots, \sigma_n$ lin. indep. $/K \Rightarrow d \neq 0$.

Claim: $\bar{R} \subseteq R \cdot \dfrac{b_1}{d^2} + \dots + R \cdot \dfrac{b_n}{d^2}$

$\sigma_i(d) = \pm d \Rightarrow d^2 \in L^G = K$.

Let $x \in \overline{R}$. $x = c_1 b_1 + \cdots + c_n b_n$, $c_i \in K$.

$$M \cdot \begin{bmatrix} c_1 \\ \vdots \\ c_n \end{bmatrix} = \begin{bmatrix} \sum \sigma_1(b_j) c_j \\ \vdots \\ \sum \sigma_n(b_j) c_j \end{bmatrix} = \begin{bmatrix} \sigma_1(x) \\ \vdots \\ \sigma_n(x) \end{bmatrix} \in \overline{R}^{\oplus n}.$$

$\Rightarrow d \cdot c_i \in \overline{R} \quad \forall i.$

$\therefore d^2 c_i \in \overline{R} \cap K = R$ since R normal.

$\Rightarrow x = \sum d^2 c_i \cdot \frac{b_i}{d^2} \in R \cdot \frac{b_1}{d^2} + \cdots + R \cdot \frac{b_n}{d^2}.$

$\square$

<u>Example</u> $\mathbb{Q} \subseteq L$ finite extension (number field)

$\overline{\mathbb{Z}} \subseteq L$ ring of integers.

Prop $\Rightarrow$ $\overline{\mathbb{Z}}$ f.g. $\mathbb{Z}$-module. (in fact, $\overline{\mathbb{Z}}$ = f.g. <u>free</u> $\mathbb{Z}$-mod.)

Eg. $\overline{\mathbb{Z}}$ Noetherian

Com. Alg. 10/8/2010

Prop R Noetherian normal ring, $K = K(R)$, $K \subseteq L$ finite separable ext. $\overline{R} \subseteq L$ integral closure of R in L. Then $\overline{R}$ f.g. R-module.

Proof WLOG: L/K Galois (replace L with normal closure.)

$G = \mathrm{Aut}_K(L) = \{\sigma_1, \dots, \sigma_n\}$

Choose $b_1, \dots, b_n \in \overline{R}$ basis for L over K. (Recall $L = K \cdot \overline{R}$.)

Set $M = \left[\sigma_i(b_j)\right]_{i,j} \in \mathrm{Mat}_n(\overline{R})$.

$d = \det(M) \in \overline{R}$

$\sigma_1, \dots, \sigma_n$ lin. indep. $/K \Rightarrow d \neq 0$.

Claim: $\overline{R} \subseteq R \cdot \frac{b_1}{d^2} + \dots + R \cdot \frac{b_n}{d^2}$

$\sigma_i(d) = \pm d \Rightarrow d^2 \in L^G = K$

Let $x \in \overline{R}$. $x = c_1 b_1 + \dots + c_n b_n$, $c_i \in K$.

$$M \begin{bmatrix} c_1 \\ \vdots \\ c_n \end{bmatrix} = \begin{bmatrix} \sum \sigma_1(b_j) c_j \\ \vdots \\ \sum \sigma_n(b_j) c_j \end{bmatrix} = \begin{bmatrix} \sigma_1(x) \\ \vdots \\ \sigma_n(x) \end{bmatrix} \in \overline{R}^{\oplus n}$$

$\Rightarrow d c_i \in \overline{R} \ \forall i$

$\Rightarrow d^2 c_i \in \overline{R} \cap K = R$ (since R normal.)

$\therefore x = \sum d^2 c_i \cdot \frac{b_i}{d^2} \in R \cdot \frac{b_1}{d^2} + \dots + R \cdot \frac{b_n}{d^2}$.

$\square$

Example $\mathbb{Q} \subseteq L$ finite extension (number field)

$\overline{\mathbb{Z}} \subseteq L$ ring of integers.

Prop $\Rightarrow$ $\overline{\mathbb{Z}}$ f.g. $\mathbb{Z}$-module. In fact f.g. free $\mathbb{Z}$-module!

E.g. $\overline{\mathbb{Z}}$ Noetherian.

<u>Normalization</u> $k = \bar{k}$, A affine domain $/k$.

$X = \text{Spec-m}(A)$ irreducible alg. set.

$\bar{A} \subseteq K(A)$ normalization of A.

Finiteness of integral closure $\Rightarrow$ $\bar{A}$ affine domain $/k$.

Set $\bar{X} = \text{Spec-m}(\bar{A})$ – also irred. alg. set.

k-alg. hom. $A \longrightarrow \bar{A}$ gives polynomial map $\pi : \bar{X} \longrightarrow X$, $\pi(Q) = Q \cap A$.

<u>$\pi : \bar{X} \twoheadrightarrow X$ surjective</u>:

$P \subseteq A$ max. ideal. $P \in X$.

Going up $\Rightarrow$ $\exists\, Q \subseteq \bar{A}$ prime ideal s.t. $P = Q \cap A$.

Incomparability $\Rightarrow$ Q max. ideal, $Q \in \bar{X}$. $\pi(Q) = P$.

<u>π has finite fibers:</u> i.e. $\pi^{-1}(P)$ finite $\forall\, P \in X$.

$Q \in \pi^{-1}(P) \iff Q \supseteq P \cdot \bar{A}$

Incomparability $\Rightarrow$ Q must be minimal over $P \cdot \bar{A}$.

$\therefore\ \pi^{-1}(P) = \text{Ass}(P \cdot \bar{A}) \subseteq \text{Spec-m}(\bar{A})$.

<u>Remark</u> Let $0 \neq f \in A$. $X_f = \{P \in X \mid f(P) \neq 0\} = \text{Spec-m}(A_f)$.

$\text{Spec-m}(A_f) \subseteq \text{Spec-m}(A)$ open subset.

Write $\bar{A} = A[\frac{g_1}{h_1}, \dots, \frac{g_r}{h_r}] \subseteq K(A)$.

Set $f = h_1 h_2 \cdots h_r$.

Then $\bar{A}_f = A_f \subseteq K(A)$ $\Rightarrow$ $\bar{X}_f = X_f$.

$$\begin{array}{ccc} \bar{X} & \xrightarrow{\pi} & X \\ \cup\! \! \mid & & \cup \\ \bar{X}_f & \xrightarrow{\cong} & X_f \end{array}$$

<u>Exercise</u>: $X_f \subseteq X$ dense open subset.

Hilbert Polynomials.

Def A *graded ring* is a ring R with decomposition $R = \bigoplus_{d \geq 0} R_d$ as abelian group, s.t. $R_i \cdot R_j \subseteq R_{i+j}$.

Example $R = k[x_1, \dots, x_n]$.

Exercise $1 \in R_0 \subseteq R$.

Def A *graded R-module* is an R-module M with decomp. $M = \bigoplus_{d \in \mathbb{Z}} M_d$ as R_0-module, s.t. $R_i \cdot M_j \subseteq M_{i+j}$.

$N \subseteq M$ is a *graded submodule* if $N = \bigoplus_{d \in \mathbb{Z}} (N \cap M_d)$.

In this case $M/N = \bigoplus_{d \in \mathbb{Z}} M_d / N_d$ is also graded.

Def M f.g. graded module over $R = k[x_1, \dots, x_n]$.

Set $H_M(d) = \dim_k(M_d)$. – Hilbert function of M.

Def. $\binom{x}{r} = \frac{x(x-1)\cdots(x-r+1)}{r!} \in \mathbb{Q}[x]$

$\mathbb{Q}[x] = \bigoplus_{d \geq 0} \mathbb{Q} \cdot x^d = \bigoplus_{d \geq 0} \mathbb{Q} \cdot \binom{x}{d}$

Note $\sum_{i=0}^{m-1} \binom{i}{r} = \binom{m}{r+1}$. Induction on m: $\binom{m}{r+1} + \binom{m}{r} = \binom{m+1}{r+1}$

Lemma $H : \mathbb{N} \longrightarrow \mathbb{Z}$ any function. Set $\Delta H(x) = H(x+1) - H(x)$.

Then $H \in \mathbb{Q}[x] \iff \Delta H \in \mathbb{Q}[x]$

Proof $\Rightarrow$ is clear.

$\Leftarrow$: Assume $\Delta H(x) = \sum_{r=0}^{d} a_r \binom{x}{r}$, $a_r \in \mathbb{Q}$.

$$H(x) = H(0) + \sum_{i=0}^{x-1} \Delta H(i) = H(0) + \sum_{r=0}^{d} a_r \sum_{i=0}^{x-1} \binom{i}{r} = H(0) + \sum_{r=0}^{d} a_r \binom{x}{r+1} \in \mathbb{Q}[x].$$

$\square$

Thm (Hilbert)

M f.g. graded module over $R = k[x_1, \dots, x_n]$.

Then $\exists$ *Hilbert polynomial* $P_M(x) \in \mathbb{Q}[x]$ s.t. $H_M(d) = P_M(d)$ $\forall d \gg 0$.

Proof Induction on n.

$n = 0 \Rightarrow M$ finite dim. vector space $\Rightarrow P_M(x) = 0$.

Let $n > 0$:

Exact sequence $0 \to K \to M \xrightarrow{x_n \cdot} M \to M/x_nM \to 0$

$\Rightarrow \quad 0 \to K_d \to M_d \to M_{d+1} \to (M/x_nM)_{d+1} \to 0$ exact $\forall d \in \mathbb{Z}$

$\Rightarrow \quad \Delta H_M(d) = H_M(d+1) - H_M(d) = H_{M/x_nM}(d+1) - H_K(d)$

K and M/x_nM f.g. modules over $k[x_1, \dots, x_{n-1}]$

Induction $\Rightarrow H_K(d) = P_K(d)$ and $H_{M/x_nM}(d) = P_{M/x_nM}(d)$ for $d \gg 0$.

$\Rightarrow \Delta H_M(d) =$ polynomial in d for $d \gg 0$

$\Rightarrow H_M(d) =$ polynomial in d for $d \gg 0$.

$\square$

Exercise Let $H(x) = \sum_{r=0}^{d} a_r \binom{x}{r} \in \mathbb{Q}[x]$. TFAE:

(a) $a_r \in \mathbb{Z} \quad \forall r$

(b) $H(d) \in \mathbb{Z} \quad \forall d \in \mathbb{Z}$

(c) $H(d) \in \mathbb{Z} \quad \forall d \in \mathbb{N}, \ d \gg 0$.

$$\boxed{\Delta H(x) = \sum_{r=1}^{d} a_r \binom{x}{r-1}}$$

Consequence

$P_M(x) = \sum_{r=0}^{d} a_r \binom{x}{r}$, $\quad a_0, \dots, a_d \in \mathbb{Z}$ important invariants of M.

Projective varieties

$k = \bar{k}$. $k^* = k - \{0\}$ mult. group.

$k^* \curvearrowright \mathbb{A}^{n+1} - \{0\}$: $t.(a_0, \dots, a_n) = (ta_0, \dots, ta_n)$.

$\mathbb{P}^n := (\mathbb{A}^{n+1} - \{0\})/k^* \qquad \pi : \mathbb{A}^{n+1} - \{0\} \longrightarrow \mathbb{P}^n$.

Let $I \subseteq S := k[x_0, \dots, x_n]$ homogeneous ideal.

Then $Z(I) \subseteq \mathbb{A}^{n+1}$ is k^*-stable.

$Z(I) := Z(I)/k^* \subseteq \mathbb{P}^n$ alg. subset.

If $X \subseteq \mathbb{P}^n$ any subset, set $I(X) = I(\pi^{-1}(X) \cup \{0\}) \subseteq S$.

Let $X \subseteq \mathbb{P}^n$ alg. subset. Proj. coord. ring: $S/I(X)$. $\boxed{\text{DEPENDS ON EMBEDDING } X \subseteq \mathbb{P}^n}$

Write $P_{S/I(X)}(x) = a_0 + a_1\binom{x}{1} + \cdots + a_d\binom{x}{d}$, $a_d \neq 0$.

Def $\dim(X) = d$.
$\deg(X) = a_d \in \mathbb{N}_+$.

Exercise $X \subseteq \mathbb{P}^n$ finite subset of m points.
Then $P_{S/I(X)}(x) = m$. So $\dim(X) = 0$, $\deg(X) = m$.

Bezout's Thm
Let $h_1, h_2, \dots, h_r \in S = k[x_0, \dots, x_n]$ be homogeneous polynomials of degrees $d_1, \dots, d_r$. Set $I = (h_1, \dots, h_r) \subseteq S$.
Assume $\dim Z(I) = n-r$, $Z(I) \subseteq \mathbb{P}^n$.
Then $\deg(S/I) = d_1 d_2 \cdots d_r$.

In particular, if $r = n$ and I radical ideal, then $Z(I) \subseteq \mathbb{P}^n$ finite set with $d_1 d_2 \cdots d_n$ points.

Com. Alg. 10/12/2010 Filtrations

Def R ring, $I \subseteq R$ ideal. The associated graded ring is
$$gr_I(R) = \bigoplus_{j \geq 0} I^j/I^{j+1} = R/I \oplus I/I^2 \oplus \cdots$$

Multiplication: Let $a \in I^m$, $b \in I^n$, $\bar{a} \in I^m/I^{m+1}$, $\bar{b} \in I^n/I^{n+1}$.
Then $\bar{a} \cdot \bar{b} = \overline{ab} \in I^{m+n}/I^{m+n+1}$.

Examples

1) $R = k[x_1, \ldots, x_n]$, $I = (x_1, \ldots, x_n) \subseteq R$.
$I^j = \text{span}\{x_1^{a_1} \cdots x_n^{a_n} \mid \sum a_i \geq j\}$
$I^j/I^{j+1} = \{\text{forms of degree } j\}$
$gr_I R = k[x_1, \ldots, x_n]$

2) $R = k[x, y]$, $I = (xy) \subseteq R$.
Then $gr_I(R)$ is not a domain since $R/I \subseteq gr_I R$.

3) R local ring with max ideal I. Assume I f.g. ideal.
Then $gr_I(R)$ affine ring over $k = R/I$.

Def $I \subseteq R$ ideal, M R-module.
An I-filtration of M is a sequence of submodules
$M = M_0 \supseteq M_1 \supseteq M_2 \supseteq \cdots$ such that $I \cdot M_j \subseteq M_{j+1}$ $\forall j$.
The filtration is I-stable if $I \cdot M_j = M_{j+1}$ $\forall j >> 0$.

Note If $M_{j+1} = I \cdot M_j$ for $j \geq n$, then the filtration is determined by $I, M_1, \ldots, M_n$.

Def Given I-filtration, $\mathcal{J} : M = M_0 \supseteq M_1 \supseteq M_2 \supseteq \cdots$
Set $$gr_{\mathcal{J}} M = \bigoplus_{j \geq 0} M_j/M_{j+1} = M/M_1 \oplus M_1/M_2 \oplus \cdots$$

Note: $gr_{\mathcal{J}} M$ is a $gr_I R$-module:
Let $a \in I^s$, $m \in M_t$, $\bar{a} \in I^s/I^{s+1}$, $\bar{m} \in M_t/M_{t+1}$.
I-Filtration $\Rightarrow$ $am \in M_{s+t}$. $\bar{a} \cdot \bar{m} = \overline{am} \in M_{s+t}/M_{s+t+1}$.

Prop M f.g. R-module, $\mathcal{J} : M = M_0 \supseteq M_1 \supseteq M_2 \supseteq \cdots$ I-stable filtration by f.g. submodules. Then $gr_{\mathcal{J}} M$ is a f.g. $gr_I R$-module.

Proof Assume $IM_i = M_{i+1}$ for $i \geq n$.

Then $(I/I^2) \cdot (M_i/M_{i+1}) = M_{i+1}/M_{i+2} \subseteq gr_{\mathcal{J}} M$ for $i \geq n$.

$\therefore$ $gr_{\mathcal{J}} M$ generated by generators of M/M_1, $M_1/M_2, \dots, M_n/M_{n+1}$.

Def (Hilbert function)

R local ring with f.g. max ideal $I \subseteq R$.

Set $H_R(n) = \dim_{R/I} (I^n/I^{n+1})$ for $n \in \mathbb{N}$.

If M f.g. R-module, set $H_M(n) = \dim_{R/I} (I^n M/I^{n+1} M)$

Cor $\exists\ P_M(x) \in \mathbb{Q}[x]$: $H_M(n) = P_M(n)$ $\forall\ n \gg 0$.

Proof

$gr_I(R)$ affine ring over $k = R/I$, $gr_I(R) = k[x_1, \dots, x_r]/J$.

$\mathcal{J} : M_j = I^j M$ I-stable filtration by f.g. R-submodules.

$\Rightarrow gr_{\mathcal{J}}(M)$ f.g. graded $k[x_1, \dots, x_r]$-module.

$\square$

Note Only one obvious module hom. $M \longrightarrow gr_{\mathcal{J}} M$: $M \longrightarrow M/M_1 \subseteq gr_{\mathcal{J}} M$.
Boring! Too much info. lost.

Def Map of sets: $in : M \longrightarrow gr_{\mathcal{J}}(M)$

$$in(m) = \begin{cases} \bar{m} \in M_j/M_{j+1} & \text{if } \exists\, j : m \in M_j \setminus M_{j+1} \\ 0 & \text{if } m \in \bigcap_{j \geq 0} M_j. \end{cases}$$

Example

$M = R = k[x_1, \dots, x_n]$, $I = (x_1, \dots, x_n)$.

Set $M_j = I^j \subseteq M$.

Given $0 \neq f \in M$, write $f = f_d + f_{d+1} + \dots + f_e$, f_i form of total degree i, $f_d \neq 0$.

Then $f \in M_d \setminus M_{d+1}$ and $in(f) = f_d \in gr_{\mathcal{J}} M = k[x_1, \dots, x_n]$.

Def $M' \subseteq M$ submodule, $\mathcal{J} : M = M_0 \supset M_1 \supset \cdots$ I-filtration.

Set $in(M') = \langle in(m') : m' \in M' \rangle \subseteq gr_{\mathcal{J}}(M)$.

Example $R = M = k[x,y]$. $I = (x,y)$. $M_j = I^j$.

$M' = (xy + y^3,\ x^2) \subseteq M$.

Then $in(M') \neq (xy,\ x^2) \subseteq gr_J(M)$:

$$x(xy + y^3) - y \cdot x^2 = xy^3 \in M'.$$

$$y^2(xy + y^3) - xy^3 = y^5 \in M'.$$

Exercise: $in(M') = (xy, x^2, y^5)$

Blowup-algebra R ring. $I \subseteq R$ ideal.

$$B_I R = \bigoplus_{j \geq 0} I^j = R \oplus I \oplus I^2 \oplus \cdots$$

Graded ring: $a \in I^i$, $b \in I^j \Rightarrow ab \in I^{i+j}$.

Example $I = R$: $B_I R = R \oplus R \oplus R \oplus \cdots = R[t]$.

In general: $B_I R = R[tI] \subseteq R[t]$

Note: 1) $B_I R / I \cdot B_I R = R/I \oplus I/I^2 \oplus \cdots = gr_I R$.

2) R Noetherian $\Rightarrow$ $B_I R$ Noetherian.

Geometry of Blowups

Y affine variety, $X \subseteq Y$ closed subvariety.

$I = I(X) = (f_0, \dots, f_n) \subseteq k[Y]$.

$\varphi : Y \setminus X \longrightarrow \mathbb{P}^n$, $\varphi(y) = (f_0(y) : \cdots : f_n(y))$

Def $Bl_X(Y) = \overline{\{(y, \varphi(y)) \mid y \in Y \setminus X\}} \subseteq Y \times \mathbb{P}^n$ Blowup of Y along X.

$\pi : Bl_X(Y) \longrightarrow Y$ projection.

Note: $\pi : \pi^{-1}(Y \setminus X) \xrightarrow{\cong} Y \setminus X$ iso. of varieties.

If $Y \setminus X$ dense in Y, then π is surjective.

Point: If Y singular along X, then $Bl_X(Y)$ is often "less singular".

Example $Y = Z(y^2 - x^2(x+1)) \subseteq \mathbb{A}^2$. $X = \{(0,0)\} \subseteq Y$.

$I(X) = (x,y) \subseteq k[Y] = k[x,y]/I(Y)$.

$\varphi : Y \setminus \{0\} \longrightarrow \mathbb{P}^1$, $P \mapsto$ line through 0 and P.

$Bl_X(Y) = \{(P, \varphi(P)) \mid P \in Y \setminus X\} \cup \{(0, (1:1)),\ (0, (1:-1))\}$

$Bl_X(Y) \subseteq Y \times \mathbb{P}^n$ closed subset.

Set $J = I(Bl_X(Y)) \subseteq k[Y][z_0, \ldots, z_n]$ graded ideal.

Claim: $k[Y][z_0,\ldots,z_n]/J \cong B_I\, k[Y] = \bigoplus_{d \geq 0} I^d \cdot t^d \subseteq k[Y][t]$.

In particular, $Bl_X(Y)$ depends only on X, Y, not on chosen generators for I.

Def. $\psi : Y \times \mathbb{A}^1 \longrightarrow Y \times \mathbb{A}^{n+1}$, $\psi(y,t) = (y, (tf_0(y), \ldots, t f_n(y)))$

$\psi(Y \times \mathbb{A}^1)$ = affine cone over $Bl_X(Y)$ $\Rightarrow$ $J = I(\psi(Y\times\mathbb{A}^1)) \subseteq k[Y][z_0,\ldots,z_n]$

$\psi^* : k[Y][z_0,\ldots,z_n] \longrightarrow k[Y][t]$, $z_i \longmapsto t f_i$

$J = \ker(\psi^*)$

$\Rightarrow$ $k[Y][z_0,\ldots,z_n]/J \cong \operatorname{Image}(\psi^*) = B_I\, k[Y]$

Com Alg. 10/15/2010

R ring, $I \subseteq R$ ideal

$$gr_I(R) = \bigoplus_{d \geq 0} I^d / I^{d+1}$$

$$B_I(R) = \bigoplus_{d \geq 0} I^d \cong \bigoplus_{d \geq 0} t^d I^d \subseteq R[t].$$

$\mathcal{J}: M = M_0 \supset M_1 \supset M_2 \supset \cdots$ filtration of R-mod M.

I-filtration : $I^s \cdot M_t \subseteq M_{s+t}$

I-stable : $I \cdot M_t = M_{t+1}$ for $t \gg 0$.

$$gr_I(M) = \bigoplus_{d \geq 0} M_d / M_{d+1} \qquad gr_I(R)\text{-module.}$$

Com Alg. 10/15/2010

Def $J: M = M_0 \supseteq M_1 \supseteq \cdots$ I-filtration.

$$B_J M = \bigoplus_{j \geq 0} M_j$$ is a graded $B_I R$-module.

Prop R ring; $I \subseteq R$ ideal, M f.g. R-module with I-filtration $J: M = M_0 \supseteq M_1 \supseteq \cdots$. Assume M_j f.g. $\forall j$.

Then J I-stable $\Leftrightarrow$ $B_J M$ f.g. $B_I R$-module.

Proof

$\Leftarrow$: WLOG $B_J M$ generated by homogeneous elts of degree $\leq n$.

Then $M_n \oplus M_{n+1} \oplus \cdots$ generated by M_n, i.e.

$M_{n+i} = I^i \cdot M_n$ for all $i \geq 0$.

$\therefore$ J is I-stable.

$\Rightarrow$: If $M_{n+i} = I^i \cdot M_n$ for all $i \geq 0$ then $B_J M$ is gen. by generators of $M_0, \ldots, M_n$.

$\square$

Let $J: M = M^0 \supseteq M^1 \supseteq \cdots$ be an I-filtration.

$M' \subseteq M$ submodule.

Set $M'_j = M' \cap M_j$.

Then $J': M' = M'_0 \supseteq M'_1 \supseteq \cdots$ is an I-filtration.

$(I \cdot M'_j = I \cdot (M' \cap M_j) \subseteq M' \cap M_{j+1} = M'_{j+1}.)$

Note: $I \cdot M_j = M_{j+1} \not\Rightarrow I \cdot M'_j = M'_{j+1}$. (E.g. $M' = M_{j+1}$)

Artin-Rees Lemma

R Noetherian ring, $I \subseteq R$ ideal, M f.g. R-module, $M' \subseteq M$ submodule.

If $J: M = M_0 \supseteq M_1 \supseteq \cdots$ is I-stable, then

$J': M'_j = M' \cap M_j$ is also I-stable.

<u>Proof</u> $B_I R$ is Noetherian!

$B_{J'}(M') \subseteq B_J(M)$ submodule.

J I-stable $\Leftrightarrow$ $B_J M$ f.g. $B_I R$-module

$\Rightarrow$ $B_{J'} M'$ f.g. $B_I R$-module $\Leftrightarrow$ J' I-stable.

□

<u>Note</u> More generally:
If $J' : M' = M'_0 \supset M'_1 \supset \cdots$ any I-filtration of M'
so that $M'_j \subseteq M_j$, then we have: J I-stable $\Rightarrow$ J' I-stable.
} Not clear.

<u>Cor</u> (Krull Intersection Thm)

$I \subseteq R$ ideal, R Noeth. M f.g. R-module.

(a) $\exists\, r \in I :$ $(1-r) \cdot \left(\bigcap_{j \geq 0} I^j \cdot M \right) = 0$

(b) If R domain or R local ring, ~~[illegible]~~
and $I \subsetneq R$, then $\bigcap_{j \geq 0} I^j = 0 \subseteq R$.

<u>Proof</u>

Set $M' = \bigcap_{j \geq 0} I^j M$. M Noetherian $\Rightarrow$ M' f.g. R-module.

Def. $J : M_j = I^j \cdot M$. $J' : M'_j = M' \cap M_j . = M'$.

Artin-Rees: J I-stable $\Rightarrow$ J' I-stable.

Thus $I \cdot (M' \cap I^p \cdot M) = M' \cap I^{p+1} \cdot M$ for some $p \in \mathbb{N}$.

$\Rightarrow$ $I \cdot M' = M'$.

C.H. $\Rightarrow$ $\exists\, r \in I :$ $(1-r) \cdot M' = 0$

(b) R local/domain and I proper ideal $\Rightarrow$ $1-r \in R$ nzd.

□

<u>Cor</u> R ~~[illegible]~~ Noetherian local ring, $I \subsetneq R$ proper ideal.

If $\mathrm{gr}_I R$ is a domain, then R is a domain.

<u>Pf</u> Assume $fg = 0$, $f, g \in R$. Then $\mathrm{in}(f) \cdot \mathrm{in}(g) = 0 \in \mathrm{gr}_I R$

$\Rightarrow$ $\mathrm{in}(f) = 0$ or $\mathrm{in}(g) = 0$. $\mathrm{in}(f) = 0 \Rightarrow f \in \bigcap I^j = 0$ □

<u>Kor</u> R Noethersk lokal ring. $I \subsetneq R$ ægte ideal.

$gr_I R$ domæne $\Rightarrow$ R domæne.

<u>Bevis</u> Antag $fg = 0$, $f, g \in R$.

Så er $in(f) \cdot in(g) = 0 \in gr_I R$

$\Rightarrow$ $in(f) = 0$ eller $in(g) = 0$.

$in(f) = 0 \Rightarrow f \in \bigcap_{j \geq 0} I^j = 0 \Rightarrow f = 0$.

□

<u>Eksempel</u> R ikke Noethersk $\Rightarrow$ Krull Int Thm falsk.

$C^\infty(\mathbb{R}) = C^\infty$-funktioner $\mathbb{R} \to \mathbb{R}$.

Sæt $R = \{$kim af C^∞-funktioner i $0 \in \mathbb{R}\}$

$= C^\infty(\mathbb{R})/\sim$

hvor $f \sim g \Leftrightarrow \exists$ $\varepsilon > 0 : f(a) = g(a) \quad \forall a \in (-\varepsilon, \varepsilon)$. ~~åbent interval $\ni 0 \subseteq \mathbb{R}$: $f(a) = g(a)$~~.

$\boxed{\text{Q: Er R lokal?}}$ R lokal ring med maks. ideal

$I = \{f \in R \mid f(0) = 0\}$.

(Hvis $f \in R$, $f(0) \neq 0$, så $\exists$ $\varepsilon > 0$

så $f(a) \neq 0$. $\forall a \in (-\varepsilon, \varepsilon)$.

$1/f$ def. på $(-\varepsilon, \varepsilon)$ giver en invers til f.

$\boxed{\text{Q: Er I e.f.?}}$ $I = (x) \subseteq R$, $x : \mathbb{R} \to \mathbb{R}$ identitetsfcn.

Hvis $f \in I$ så er $f(0) = 0$.

$g = \frac{\Delta f}{\Delta x} = \frac{f(x)}{x}$ har grænseværdi i 0. $g(x) = \begin{cases} \frac{f(x)}{x} & x \neq 0 \\ f'(0) & x = 0 \end{cases}$

Dette definerer $g : \mathbb{R} \to \mathbb{R}$ i C^∞ og $f = xg \in (x)$.

Q: Er R et domæne? Nej:

Sæt $f(x) = \begin{cases} e^{-1/x^2}, & x \geq 0 \\ 0, & x \leq 0. \end{cases}$

Så er $f(x) \cdot f(-x) = 0 \in R$ men $f(x), f(-x) \neq 0$.

Q: Er $\bigcap_{j \geq 0} I^j = 0$?

Nej, $f(x) \in \bigcap_{j \geq 0} I^j$:

$$h(x) = \frac{f(x)}{x^j} \in C^\infty, \quad h(0) = f^{(j)}(0) = 0.$$

Q: Er $gr_I R$ et domæne?

$$I^n = \{f \in R \mid f^{(j)}(0) = 0 \text{ for } 0 \leq j < n\}.$$
$$= \{f \in R \mid f(0) = f'(0) = \cdots = f^{(n-1)}(0) = 0\}.$$

$$I^n/I^{n+1} \xrightarrow{\sim} \mathbb{R}, \quad f \mapsto f^{(n)}(0).$$

$\therefore \; gr_I R = \mathbb{R}[t]$ polynomiumsring.
$\Rightarrow$ domæne!

Flatness.

<u>Exercise</u> $0 \to M' \to M \to M'' \to 0$ exact of R-modules. N R-mod.

Then $M'\otimes N \to M\otimes N \to M''\otimes N \to 0$ also exact.

Let $0 \leftarrow M \leftarrow F_0 \leftarrow F_1 \leftarrow \cdots$ be a free resolution of M.

Complex: $F_\bullet \otimes N$: $F_0\otimes N \leftarrow F_1 \otimes N \leftarrow \cdots$

<u>Def</u> $\mathrm{Tor}_i(M,N) = H_i(F_\bullet \otimes N)$.

<u>Note:</u> $\mathrm{Tor}_0(M,N) = M\otimes_R N$.

<u>Fact 1:</u> $\mathrm{Tor}_i(M,N) = \mathrm{Tor}_i(N,M)$.

<u>Fact 2:</u> Long exact seq:

$0 \to M' \to M \to M'' \to 0$ exact $\Rightarrow$

$$\to M'\otimes N \to M\otimes N \to M''\otimes N \to 0$$
$$\to \mathrm{Tor}_1(M',N) \to \mathrm{Tor}_1(M,N) \to \mathrm{Tor}_1(M'',N)$$
$$\mathrm{Tor}_2(\quad)$$

is exact.

<u>Note:</u> $U \subseteq R$ mult. subset. $U^{-1}(M\otimes_R N) = U^{-1}M \otimes_{U^{-1}R} U^{-1}N$.

$\Rightarrow U^{-1}\mathrm{Tor}_i^R(M,N) = \mathrm{Tor}_i^{U^{-1}R}(U^{-1}M, U^{-1}N)$.

<u>Def</u> An R-module N is <u>flat</u> if $\otimes_N$ exact functor.

I.e. $0\to M' \to M \to M'' \to 0$ exact $\Rightarrow 0 \to M'\otimes N \to M\otimes N \to M''\otimes N \to 0$ exact.

<u>Examples</u> 1) Free R-modules are flat.

2) N flat, $U \subseteq R$ mult. subset $\Rightarrow U^{-1}N$ flat R-module / $U^{-1}R$-module

Com. Alg. 10/19/2010

R ring, M, N R-modules. $F_\bullet \to M \to 0$ free resolution.

<u>Def</u> $\operatorname{Tor}_i(M,N) = H_i(F_\bullet \otimes N)$

$\operatorname{Tor}_0(M,N) = M \otimes N$, $\operatorname{Tor}_i(M,N) = \operatorname{Tor}_i(N,M)$.

Long exact: $0 \to M' \to M \to M'' \to 0$ gives

$$\cdots \to \operatorname{Tor}_1(M'',N) \to M' \otimes N \to M \otimes N \to M'' \otimes N \to 0$$

<u>Def</u> M is <u>flat</u> if $M \otimes_R$ is exact.

<u>Thm</u> M R-module. TFAE:

(1) M flat (2) $\operatorname{Tor}_i(M,N) = 0$ $\forall i > 0$, $\forall$ R-modules N

(3) $I \otimes M \to M$ injective $\forall$ f.g. ideals $I \subseteq R$.

<u>Proof</u> (3) $\Rightarrow$ (1):

Must show: $N' \to N$ injective $\Rightarrow$ $N' \otimes M \to N \otimes M$ injective.

<u>Claim 1</u>: If $J \subseteq R$ any ideal, then $J \otimes M \to M$ injective.

Let $x = \sum_{i=1}^n a_i \otimes m_i \in J \otimes M$. $a_i \in J$, $m_i \in M$.

Assume $x \mapsto \sum_{i=1}^n a_i m_i = 0 \in M$.

Set $I = (a_1, \ldots, a_n) \subseteq J$.

By assumption: $I \otimes M \to J \otimes M \to M$ is injective.

$x = 0 \in I \otimes M \Rightarrow x = 0 \in J \otimes M$.

<u>Claim 2</u>: If $N' \to N$ injective and N f.g. R-module, then $N' \otimes M \to N \otimes M$ injective.

$\exists$ $N' = N_0 \subseteq N_1 \subseteq N_2 \subseteq \cdots \subseteq N_p = N$ such that N_j/N_{j-1} gen. by one elt.

Then $N_j/N_{j-1} \cong R/I_j$.

$0 \to I_j \to R \to R/I_j \to 0$ gives $\underset{\overset{\|}{0}}{\operatorname{Tor}_1(R,M)} \to \operatorname{Tor}_1(R/I_j, M) \to I_j \otimes M \xrightarrow{\subseteq} M$

Conclude $\operatorname{Tor}_1(R/I_j, M) = 0$

$0 = \operatorname{Tor}_1(N_j/N_{j-1}, M) \to N_{j-1} \otimes M \to N_j \otimes M$ Implies $N_{j-1} \otimes M \xrightarrow{\subseteq} N_j \otimes M$ injective.

$\therefore$ $N' \otimes M = N_0 \otimes M \hookrightarrow N_1 \otimes M \hookrightarrow \cdots \hookrightarrow N_p \otimes M = N \otimes M$.

<u>Claim 3</u>: $N' \to N$ injective $\Rightarrow$ $N' \otimes M \to N \otimes M$ injective.

Let $x = \sum_{i=1}^{k} n_i' \otimes m_i \in N' \otimes M$. Assume $x \mapsto 0 \in N \otimes M$.

$N \otimes M$ = free R-module gen. by $\{[n,m] \mid n \in N, m \in M\}$ modulo

$$(*) \begin{cases} a[n,m] - [an, m] \\ a[n,m] - [n, am] \\ [n_1+n_2, m] - [n_1, m] - [n_2, m] \\ [n, m_1+m_2] - [n, m_1] - [n, m_2] \end{cases}$$

$x \mapsto 0 \in N \otimes M \Rightarrow \sum_{i=1}^{k} [n_i', m_i] = \sum$ relations of the form $(*)$.

Let $Q \subseteq N$ be submodule generated by $n_1', \dots, n_k'$ plus all elts used in relations. Set $Q' = Q \cap N'$.

$x = \sum n_i' \otimes m_i \in Q' \otimes M$ and $x \mapsto 0 \in Q \otimes M$.

Claim 2 $\Rightarrow$ $x = 0 \in Q' \otimes M \Rightarrow x = 0 \in N' \otimes M$.

□

<u>Cor</u> $R = k[t]/(t^2)$, M R-module.

M is flat $\Leftrightarrow$ $0 \to tM \to M \xrightarrow{t\cdot} tM \to 0$ is exact.

<u>Proof</u> $0 \to (t) \to R \xrightarrow{t\cdot} (t) \to 0$ exact.

$$\begin{tikzcd} & (t)\otimes M \arrow[r] \arrow[d] & M \arrow[r, "t\otimes"] \arrow[d, equal] & (t)\otimes M \arrow[r] \arrow[d] & 0 \\ 0 \arrow[r] & tM \arrow[r] & M \arrow[r, "t\cdot"] & tM \arrow[r] & 0 \end{tikzcd}$$

$\Rightarrow$: If M flat then $(t)\otimes M \xrightarrow{\cong} tM$ and top row exact $\Rightarrow$ bottom exact.

$\Leftarrow$: If bottom row exact, then $\mathrm{Ker}(M \to (t)\otimes M) = \mathrm{Ker}(M \to tM)$ and hence $(t)\otimes M \cong tM$, and $(t)\otimes M \hookrightarrow M$.

This implies M flat, since $(t) \subseteq R$ only non-trivial ideal.

□

<u>Note</u> M flat R-module, $a \in R$ nzd.

$0 \to R \xrightarrow{a\cdot} R$ exact $\Rightarrow$ $0 \to M \xrightarrow{a\cdot} M$ exact. $\Rightarrow a$ nzd on M.

<u>Cor</u> R PID, M R-module. M flat $\Leftrightarrow$ M torsion free.

<u>Proof</u> $\Rightarrow$: Follows from Note.

$\Leftarrow$: Let $I = (a) \subseteq R$ be an ideal.

$$\begin{tikzcd} 0 \arrow[r] & I \arrow[r] & R \\ 0 \arrow[r] & R \arrow[r, "a\cdot"] \arrow[u, "a\cdot", "\cong"'] & R \arrow[u, equal] \end{tikzcd} \Rightarrow \begin{tikzcd} & I\otimes M \arrow[r] & M \\ 0 \arrow[r] & M \arrow[r, "a\cdot"] \arrow[u, "\cong", "a\otimes"'] & M \arrow[u, equal] \end{tikzcd}$$

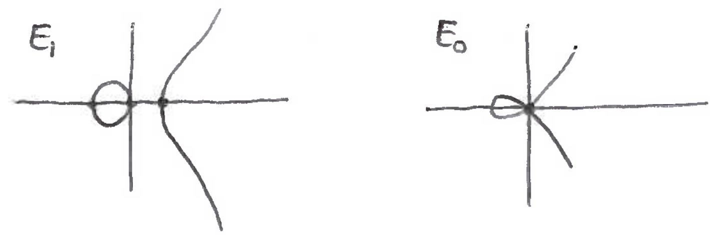
Def An R-algebra S is <u>flat</u> if S is a flat R-module.

Examples 1) $U^{-1}R$. 2) $R[x_1, \dots, x_n]$. 3) $R \xrightarrow{\text{flat}} S \xrightarrow{\text{flat}} T \Rightarrow R \to T$ flat.

Families of varieties

Let $k = \bar{k}$, $\mathrm{char}(k) \neq 2, 3$. For $\lambda \in k$, define curve

$$E_\lambda = Z(y^2 - x(x+1)(x-\lambda)) \subseteq \mathbb{A}^2.$$



Want to consider $\{E_\lambda\}$ as family of alg. sets depending on $\lambda \in k$.

Def. $E = Z(y^2 - x(x+1)(x-t)) \subseteq \mathbb{A}^3$.

$\pi : E \longrightarrow \mathbb{A}^1$, $\pi(a, b, \lambda) = \lambda$.

Then $E_\lambda = \pi^{-1}(\lambda) \subseteq E$.

Def A <u>family of alg. sets</u> is a morphism $\pi : X \longrightarrow B$ of alg. sets.

Consider it as the family $\{\pi^{-1}(b)\}_{b \in B}$.

<u>Recall</u>: π corresponds to k-alg. hom. $\pi^* : A(B) \longrightarrow A(X)$.

Def $\pi : X \longrightarrow B$ is a flat family if $A(X)$ is a flat $A(B)$-algebra.

If $\pi : X \to B$ is a flat family, then $X_b = \pi^{-1}(b)$ depends on b in a "nice"/"continuous" way. E.g. $\dim X_b$ is constant.

Examples

1) $\pi : E \to \mathbb{A}^1$ is flat. $k[t] \xrightarrow{\text{flat}} k[t, x] \xrightarrow{\text{flat}} k[t,x][y]/(y^2 - x(x+1)(x-t))$

2) $X = Z(tx - t)$. $\pi : X \longrightarrow \mathbb{A}^1$, $\pi(x, t) = t$ is NOT flat.

$k[t] \longrightarrow k[x, t]/(tx - t)$

$t \in k[t]$ nzd. $t \in k[x,t]/(tx-t)$ zero divisor.

Note X any irred. alg. set, $\pi : X \longrightarrow \mathbb{A}^1$ dominant morphism. Then π is a flat family.

$k[t] \subseteq A(X)$ domain $\Rightarrow$ $A(X)$ torsion free as $k[t]$-module.

Completion

R ring. $R \supseteq m_1 \supseteq m_2 \supseteq m_3 \supseteq \cdots$ ideals in R.

$$R/m_1 \leftarrow R/m_2 \leftarrow R/m_3 \leftarrow \cdots$$

Def $\hat{R} = \varprojlim R/m_i = \{(g_1, g_2, \ldots) \in \prod_i R/m_i \mid g_i \equiv g_j \pmod{m_i} \text{ for } j > i\}$

$\hat{m}_i = \{(g_1, g_2, \ldots) \in \hat{R} \mid g_j = 0 \in R/m_j \text{ for } j \leq i\}$

Note:

$R \longrightarrow \hat{R}$, $r \mapsto (r + m_1, r + m_2, \ldots)$

$0 \longrightarrow m_i \longrightarrow R \longrightarrow \hat{R}/\hat{m}_i \longrightarrow 0 \quad \Rightarrow \quad \hat{R}/\hat{m}_i = R/m_i$.

$\therefore \hat{\hat{R}} = \hat{R}$.

Def R is called complete wrt. $\{m_i\}$ if $R \xrightarrow{\cong} \hat{R}$.

E.g. $\hat{R}$ is complete.

Def $m \subseteq R$ ideal. m-adic filtration: $R \supseteq m^1 \supseteq m^2 \supseteq m^3 \supseteq \cdots$

$\hat{R}_m :=$ completion wrt. m-adic filtration.

Write $\hat{m} = \hat{m}_1 \subseteq \hat{R}_m$

Lemma $m \subseteq R$ max ideal $\Rightarrow (\hat{R}_m, \hat{m})$ local ring.

Proof $\hat{R}_m/\hat{m} = R/m$ is a field.

$\Rightarrow \hat{m} \subseteq \hat{R}_m$ max. ideal.

Assume $(g_1, g_2, \ldots) \in \hat{R}_m \setminus \hat{m}$.

Then $g_1 \neq 0 \in R/m \Rightarrow g_i \notin m R/m^i$ for $i \geq 1$.

Note: R/m^i local ring with max ideal mR/m^i.

$\therefore g_i$ unit in R/m^i. $\forall i$

$g_i \equiv g_j \pmod{m^i}\ \forall j \geq i \Rightarrow g_i^{-1} \equiv g_j^{-1} \pmod{m^i}\ \forall j \geq i$

$\therefore (g_1^{-1}, g_2^{-1}, \ldots) \in \hat{R}_m$ inverse elt. to $(g_1, g_2, \ldots)$

$\square$

Note: R/m^i local $\Rightarrow$ $R/m^i = (R/m^i)_m = R_m/m_m^i$

$\therefore$ $\hat{R}_m$ = completion of R_m wrt. m_m-adic filtration.

<u>Example</u> S ring, $R = S[x_1, \dots, x_n]$ polynomial ring, $m = (x_1, \dots, x_n) \subseteq R$.
Then $\hat{R}_m = S[[x_1, \dots, x_n]] = \{$formal power series with coefs in $S\}$

<u>Example</u> (Ring of p-adic numbers)
$p \in \mathbb{Z}$ prime number.
$\mathbb{Z}_p := \hat{\mathbb{Z}}_{(p)} = \{(g_1, g_2, \dots) \in \prod \mathbb{Z}/(p^i) \mid g_i \equiv g_{i+1} \pmod{p^i}\}$

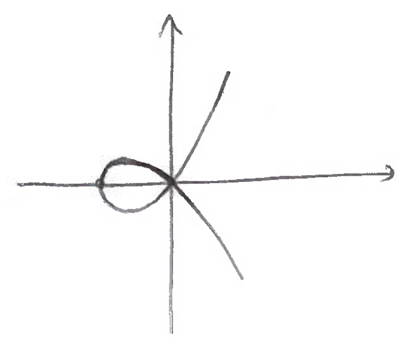
$g_i \in \mathbb{Z}/(p^i)$ can be written $g_i = a_0 + a_1 p + \dots + a_{i-1} p^{i-1} + (p^i)$
with $0 \le a_k < p$.

$g_i \equiv g_j \pmod{p^i}$ for $j \ge i$ $\Rightarrow$ each a_k well defined.

Notation: $(g_1, g_2, \dots) = a_0 + a_1 p + a_2 p^2 + a_3 p^3 + \dots$

<u>Exercise</u>: $p = 2$: $1 + 2 + 2^2 + 2^3 + \dots = -1 \in \mathbb{Z}_2$.

<u>Example</u> $X = Z(y^2 - x^2(1+x)) \subseteq \mathbb{A}^2$. $P = (0,0)$.



X irreducible.
$R = k[x,y]/(y^2 - x^2(x+1))$ domain.
All Zariski nbhds of P are irreducible
$\Rightarrow$ $R_P = R_{(x,y)}$ is a domain.

BUT: X is not irreducible close to P in finer topologies.
$\hat{R}_P = \widehat{R_{(x,y)}} = k[[x,y]]/(y^2 - x^2(x+1))$ is NOT a domain!
$y^2 - x^2(1+x) = (y - x\sqrt{1+x}) \cdot (y + x\sqrt{1+x})$
$\therefore$ $\hat{R}_P \leftrightarrow$ sub-Zariski nbhds. of P.

<u>Properties</u>
R ring, $m \subseteq R$ ideal, $\hat{R} = \hat{R}_m$ m-adic completion.
$\hat{m}_n = \{(g_1, g_2, \dots) \in \hat{R} \mid g_j = 0 \in R/m^j \text{ for } j \le n\}$.

1) $\hat{m}_n = \ker(\hat{R}_m \longrightarrow R/m^n)$

2) $m^n \cdot \hat{R} \subseteq (\hat{m}_1)^n \subseteq \hat{m}_n$

3) $\hat{R} = \varprojlim \hat{R}/\hat{m}_n$

4) $gr(\hat{R}_m) = \bigoplus_{n\geq 0} \hat{m}_n/\hat{m}_{n+1} = \bigoplus_{n\geq 0} m^n/m^{n+1} = gr_m(R)$

Def A sequence $\{a_i\} = \{a_1, a_2, a_3, \dots\}$ of elts in $\hat{R}$ converges to $a \in \hat{R}$ if

$\forall n>0 \ \exists \ i(n) > 0 : \ a_j \equiv a \pmod{\hat{m}_n} \ \forall j \geq i(n)$.

Note: $a \in \hat{R}$ is uniquely determined:

$a_j \longrightarrow a' \Rightarrow a - a' \in \bigcap_n \hat{m}_n = 0$.

Def $\{a_i\} \subseteq \hat{R}$ is a Cauchy sequence if

$\forall \ n>0 \ \exists \ i(n)>0 \ \forall i,j \geq i(n) : \ a_i - a_j \in \hat{m}_n$.

Note: $\{a_i\}$ Cauchy $\Rightarrow$ $\{a_i\}$ converges to

$a = (a_{i(1)} + \hat{m}_1, \ a_{i(2)} + \hat{m}_2, \dots) \in \hat{R}$.

Lemma

$\{a_i\}, \{b_i\} \subseteq \hat{R}$ sequences, $a_i \longrightarrow a$, $b_i \longrightarrow b$.

Then $(a_i + b_i) \longrightarrow a+b$, and $a_i b_i \longrightarrow ab$, and $(-a_i) \longrightarrow -a$.

Exercise

Define the Krull topology (or m-adic topology) on $\hat{R}$ by using the sets $\{a + \hat{m}_n\}$ as a basis of open subsets.

Then convergence and Cauchy sequences agree with usual defs.

Notation Let $b_0, b_1, b_2, \dots \in R$ be elts s.t. $b_i \in m^i$.

Set $a_i = \sum_{j=0}^{i} b_j$. Then $\{a_i\}$ is a Cauchy sequence.

Def $\sum_{j=0}^{\infty} b_j = \lim_{i\to\infty} a_i = (b_0 + m, \ b_0 + b_1 + m^2, \ b_0+b_1+b_2 + m^3, \dots) \in \hat{R}$

Prop If R is complete wrt. $m \subseteq R$, then $1-a \in R$ is a unit $\forall a \in m$.

Proof $(1-a)\cdot\left(\sum_{j=0}^{\infty} a^j\right) = 1 \in \hat{R} = R$. $\square$

Cor (R, P) local ring. $\Rightarrow$ $R[[x_1, \ldots, x_n]]$ local ring with max ideal $P + (x_1, \ldots, x_n)$.

Proof let $f \in R[[x_1, \ldots, x_n]] \setminus P + (x_1, \ldots, x_n)$.

f has constant term $f_0 \in R \setminus P$. unit in R.

$f_0^{-1} f$ has const term 1.

$f_0^{-1} f = 1 - a$, $a \in (x_1, \ldots, x_n) \subseteq R[[x_1, \ldots, x_n]]$.

$\therefore$ $f_0^{-1} f \in R[[x_i]]$ unit $\Rightarrow$ f unit.

$\square$

Prop R complete wrt.

Com. Alg. 11/12/2010

R regular local ring. $m \subseteq R$

$\dim(R) = d > 0$.

$P_1, \ldots, P_t \subseteq R$ min prime ideals.

Prime avoidance: Choose $x \in m$ s.t. $x \notin m^2$ and $x \notin P_i \ \forall i$

Set $S = R/(x)$. $n = m/(x) \subseteq S$.

Claim: $\dim(S) = \dim(R) - 1$

$\dim(S) \leq \dim(R) - 1$:

If $Q_0/(x) \subsetneq \cdots \subsetneq Q_r/(x)$ chain in S then have some chain $P_i \subsetneq Q_0 \subsetneq \cdots \subsetneq Q_r$ in R.

$\dim(S) \geq \dim(R) - 1$:

Set $e = \dim(S)$.

Let $y_1, \ldots, y_e \in m$ be a system of parameters for S.

I.e. $S/(y_1, \ldots, y_e)$ has finite length.

$\Rightarrow R/(x, y_1, \ldots, y_e)$ has finite length

$\Rightarrow \dim R = \operatorname{codim} m \leq e+1. = \dim(S) + 1$

$\therefore \dim(S) = \dim(R) - 1$.

$\square$

Com. Alg. 11/30/2010

$R = k[x_1, \dots, x_n]$, $I \subseteq R$ ideal.

$I = (f_1, \dots, f_m)$.

Let $h \in R$.

Q: Is $h \in I$?

<u>Def</u> A <u>monomial order</u> on R is a total order on $\{x^\alpha\}$ such that
- $x^\alpha \leq x^\beta \Rightarrow x^{\alpha+\gamma} \leq x^{\beta+\gamma}$
- $\leq$ is a well ordering. $\exists$ smallest elt.

<u>Example</u> Lexicographic order:

$x^\alpha < x^\beta \iff (\alpha_1 < \beta_1)$ or $(\alpha_1 = \beta_1$ and $\alpha_2 < \beta_2)$ or ...

$\iff$ first non-zero elt. of $\beta - \alpha$ is positive.

Given monomial order, $LT(f) = LC(f) \cdot LM(f)$ leading term.

<u>Division algo</u> Let $(f_1, \dots, f_s) \subseteq R$. Let $h \in R$.

Then $\exists\ a_1, \dots, a_s, r \in R$ such that

$$h = a_1 f_1 + \dots + a_s f_s + r$$

and all monomials of r are NOT divisible by $LM(f_1), \dots, LM(f_s)$.

<u>Idea</u>: ~~Let~~ $I = (f_1, \dots, f_s) \subseteq R$.

We say I is a <u>Gröbner basis</u> iff $h \in I \iff r = 0$.

<u>Def</u> $LT(I) = \{ LT(h) \mid h \in I \}$.

$\langle LT(I) \rangle$ = ideal generated by $LT(I)$.

<u>Def</u> Let $G = \{g_1, \dots, g_s\} \subseteq I$. G is a Gröbner basis for I if $\langle LT(g_1), \dots, LT(g_s) \rangle = \langle LT(I) \rangle$.

$R = k[x_1, \dots, x_n]$, k field.

Monomial order $\leq$: Total order, well ordering, $x^\alpha \leq x^\beta \Rightarrow x^{\alpha+\gamma} \leq x^{\beta+\gamma}$.

$f \in R$. $f = \sum_\alpha a_\alpha x^\alpha$, $a_\alpha \in k$.

$LM(f) = \max\{x^\alpha \mid a_\alpha \neq 0\}$

$LC(f) = a_\alpha$ where $x^\alpha = LM(f)$

$LT(f) = LC(f) \cdot LM(f)$.

Division Algorithm $F = (f_1, \dots, f_s)$, $f_i \in R$, $h \in R$.

Then $\exists$ $a_1, \dots, a_s, r \in R$ such that

$h = a_1 f_1 + \dots + a_s f_s + r$, every monomial occuring in r is NOT divisible by $LM(f_i)$ for each i, and $LM(h) \geq LM(a_i f_i)$ $\forall i$.

Def $I \subseteq R$ ideal.

$LT(I) = \{LT(f) \mid f \in I\}$ SET!

$\langle LT(I) \rangle$ = ideal generated by $LT(I)$ $\subseteq R$.

Def $G = \{g_1, g_2, \dots, g_s\}$ is a Gröbner basis for I if $g_i \in I$ $\forall i$ and $\langle LT(I) \rangle = \langle LT(g_1), \dots, LT(g_s) \rangle$

Note: Hilbert basis Thm $\Rightarrow$ Every ideal has a Gröbner basis.

Thm $I \subseteq R$ ideal, $G = \{g_1, \dots, g_s\}$ Gröbner basis for I. Let $h \in R$.

Write $h = a_1 g_1 + \dots + a_s g_s + r$, $a_i, r \in R$, division algo.

Then $h \in I \Leftrightarrow r = 0$

Proof

$\Leftarrow$: clear.

$\Rightarrow$: Assume $h \in I$ and $r \neq 0$. Then $r \in I$. $\Rightarrow LT(r) \in LT(I)$.

$\Rightarrow LT(r) \in \langle LT(I) \rangle = \langle LT(g_1), \dots, LT(g_s) \rangle$

$\Rightarrow LT(r)$ divisible by $LT(g_i)$ for some i $\lightning$.

Must have $r = 0$.

□

Prop $G = \{g_1, \dots, g_s\}$ GB for $I \subseteq R$. Let $h \in R$.
Then $\exists!\, r \in R$ such that
(1) $h - r \in I$
(2) Every term of r is NOT divisible by $LT(g_i)$ $\forall i$.

Proof Uniqueness: Assume $r \neq r' \in R$ both sat this.
$0 \neq r - r' \in I$. $LT(r - r') \in \langle LT(g_1), \dots, LT(g_s) \rangle$. $\lightning$.
$\square$

Note: r is called the <u>normal form</u> of f.

Def Let $f, g \in R$, $f, g \neq 0$.
$LM(f) = x^{\alpha}$, $LM(g) = x^{\beta}$. Set $\gamma = (\gamma_1, \dots, \gamma_n)$, $\gamma_i = \max(\alpha_i, \beta_i)$.
Then $LCM(x^{\alpha}, x^{\beta}) = x^{\gamma}$.
The S-polynomial of f and g is
$$S(f,g) = \frac{x^{\gamma}}{LT(f)} \cdot f - \frac{x^{\gamma}}{LT(g)} \cdot g \in R.$$

Example
$f = x^3y^2 - x^2y^3 + x$, $g = 3x^4y + y^2 \in \mathbb{R}[x,y]$.
Use <u>grlex order</u>: $x^{\alpha} \geq x^{\beta}$ iff $|\alpha| > |\beta|$ or $\left(|\alpha| = |\beta| \text{ and } x^{\alpha} \geq_{lex} x^{\beta}\right)$.

$LT(f) = x^3y^2$. $LT(g) = 3x^4y$. $x^{\gamma} = x^4y^2$.
$$S(f,g) = \frac{x^4y^2}{x^3y^2} f - \frac{x^4y^2}{3x^4y} g = x \cdot f - \frac{1}{3} y \cdot g = -x^3y^3 + x^2 - \frac{y^3}{3}.$$

Lemma Let $f_1, \dots, f_s \in R$ and assume $LM(f_i) = x^{\delta}$ $\forall i$.
Let $c_1, \dots, c_s \in k$. If $LM(\sum c_i f_i) < x^{\delta}$, then
$\sum c_i f_i$ is a lin. comb. of the S-polys $S(f_j, f_k)$, $1 \leq j < k \leq s$.
Furthermore, $LM(S(f_j, f_k)) < x^{\delta}$ $\forall j, k$.

Proof $S(f_j, f_k) = \frac{1}{LC(f_j)} f_j - \frac{1}{LC(f_k)} f_k$.
$\square$

Thm $I \subseteq R$ ideal, $G = \{g_1, \ldots, g_s\} \subseteq I$ subset.
Assume that $I = \langle G \rangle$.
Then G is a Gröbner basis $\Leftrightarrow$ $S(g_i, g_j)$ has remainder 0 when divided by G, $\forall i,j$.

Proof

$\Rightarrow$: Clear since $S(g_i, g_j) \in I$.

$\Leftarrow$: Let $f \in I$. Must show $LT(f) \in \langle LT(g_1), \ldots, LT(g_s) \rangle$.

Write $f = \sum h_i g_i$, $h_i \in R$.

Set $x^\delta = \max(LM(h_1 g_1), \ldots, LM(h_s g_s))$. Then $x^\delta \geq LM(f)$.

Choose $\sum h_i g_i$ such that x^δ is as small as possible.

Enough to show $x^\delta = LM(f)$, since then

$$LM(f) = x^\delta = LM(h_i g_i) = LM(h_i)\, LM(g_i) \in \langle LT(g_i) \rangle$$

Assume $x^\delta > LM(f)$.

$$f = \sum_{LM(h_i g_i) = x^\delta} h_i g_i + \sum_{LM(h_i g_i) < x^\delta} h_i g_i$$

$$= \sum_{LM(h_i g_i) = x^\delta} LT(h_i)\, g_i + \sum_{LM(h_i g_i) = x^\delta} (h_i - LT(h_i))\, g_i + \sum_{LM(h_i g_i) < x^\delta} h_i g_i$$

Lemma $\Rightarrow$ first sum is lin. comb. of S-polys.

$$S(LT(h_j) g_j, LT(h_k) g_k) =$$

$$\frac{1}{LC(h_j g_j)} LT(h_j) g_j - \frac{1}{LC(h_k g_k)} LT(h_k g_k) =$$

$$\frac{x^\delta}{LT(g_j)} g_j - \frac{x^\delta}{LT(g_k)} g_k = \frac{x^\delta}{LCM(LT(g_j), LT(g_k))} S(g_j, g_k).$$

Note: $LM(\text{S-poly}) < x^\delta$.

Assumption $\Rightarrow$

can write $S(g_j, g_k) = \sum a_i^{kj} g_i$

such that $LM(a_i^{kj} g_i) \leq LM(S(g_j, g_k))$.

$\therefore$ Can rewrite first sum as $\sum h_i' g_i$ s.t. $LM(h_i' g_i) < x^\delta$.

$\square$ $\lightning$.

~~Algorith~~ <u>Buchberger's Algorithm</u>

$I = (f_1, .., f_s) \subseteq R$ ideal.

Set $G = \{f_1, .., f_s\}$.

For each pair $p, q \in G$, Let $\overline{S}(p,q)$ be the remainder of $S(p,q)$ by division with G.

If $\overline{S}(p,q) \neq 0$ then replace G with $G \cup \{\overline{S}(p,q)\}$.

Repeat until $\overline{S}(p,q) = 0 \quad \forall\, p, q \in G$.

At this point G is a G.B. for I.

<u>Termination</u>: Notice that $LM(\overline{S}(p,q)) \notin \langle LT(G) \rangle$.

$\Rightarrow \langle LT(G) \rangle$ becomes larger every time we add $\overline{S}(p,q)$.

Ascending chain condition $\Rightarrow$ Algorithm terminates.

$R = k[x_1, .., x_n]$. $\leq$ monomial order. $G = \{g_1, .., g_s\}$ g.b. for I if $G \subseteq I$ and $\langle LT(I) \rangle = \langle LT(G) \rangle$.

<u>In practise</u>: Buchbergers algorithm can take a LONG TIME!

<u>Note</u>: Let G be a gb. of I. Let $p \in G$.

If $LT(p) \in \langle LT(G - \{p\}) \rangle$ then $G - \{p\}$ is also GB.

<u>Def</u> A <u>minimal Grobner basis</u> for I is a GB G such that

(i) $LC(p) = 1 \quad \forall\, p \in G$. (ii) $LT(p) \notin \langle LT(G - \{p\}) \rangle \quad \forall\, p \in G$.

<u>Def</u> A <u>reduced GB</u> for I is a GB G such that

(i) $LC(p) = 1 \quad \forall\, p \in G$.

(ii) For all $p \in G$, no monomial of p is in $\langle LT(G - \{p\}) \rangle$.

<u>Existence</u>: Let G be any minimal GB for I.
Replace each $p \in G$ with the remainder $\bar{p}$ when p is divided by $G - \{p\}$.
(Note: $LT(p) = LT(\bar{p})$.)

<u>Thm</u> Let $I \subseteq R$ be an ideal. Then the reduced GB for I is unique.

<u>Proof</u> Let $G = \{g_1, \ldots, g_s\}$ and $G' = \{g_1', \ldots, g_t'\}$ be red. GB for I.

$\langle LT(I) \rangle = \langle LT(G) \rangle = \langle LT(G') \rangle$.

Partial order: $x^\alpha < x^\beta \iff \alpha_i \le \beta_i \;\; \forall i$.

Must have: $\{LT(g_1), \ldots, LT(g_s)\} = \{LT(g_1'), \ldots, LT(g_t')\}$ is set of minimal monomials of $\langle LT(I) \rangle$ wrt. $<$.

WLOG: $s = t$ and $LT(g_i) = LT(g_i')$.

Note: $g_i - g_i' \in I$, and $LM(g_i - g_i') < LM(g_i)$

So not divisible by $LM(g_k)$ for any k.

$\therefore\; g_i - g_i' = 0$, and $G = G'$.

$\square$

<u>Linear algebra</u> ~~Let $a_1x_1 + a_2x_2 + \cdots + a_nx_n$ b_1x_1 b_nx_n c_1x_1~~

Let $f_i = a_{i1}x_1 + \cdots + a_{in}x_n$, $\quad 1 \le i \le s$.

Solve $f_i(x_1, \ldots, x_n) = c_i \;\; \forall i$.

Compute reduced GB for $I = \langle f_1 - c_1, \ldots, f_s - c_s \rangle$.

$G = (g_1, \ldots, g_t)$.

~~Note: $LT(g_j) = x_k$ for some k~~

If $g_j \in k$ for some j: No sols.

Else $LT(g_j) = x_{k_j}$ for some k_j. $\boxed{\text{EXERCISE.}}$

Note: x_{k_j} does not occur in any other g_ℓ.

$\therefore$ $g_1, \dots, g_t$ are in row echelon form!

Com Alg. 12/7/2010 AG. class

Example Solve the equations $\begin{cases} x^2+y^2+z^2=1 \\ x^2+z^2 = y \\ x = z \end{cases}$

$I = \langle x^2+y^2+z^2-1,\ x^2+z^2-y,\ x-z \rangle \subseteq k[x,y,z]$. Lex order: $x>y>z$.

Gröbner basis: $G = \{g_1, g_2, g_3\}$

$g_1 = x-z$, $g_2 = -y+2z^2$, $g_3 = z^4 + \frac{1}{2}z^2 - \frac{1}{4}$

Solve for z, then solve for y, then solve for x.

Elimination Theory.

$\pi : \mathbb{A}^n \longrightarrow \mathbb{A}^{n-l}$, $\pi(x_1,\ldots,x_n) = (x_{l+1},\ldots,x_n)$.

$X \subseteq \mathbb{A}^n$ alg. subset. $\overline{\pi(X)} \subseteq \mathbb{A}^{n-l}$.

$I(\overline{\pi(X)}) = I(\pi(X)) = I(X) \cap k[x_{l+1},\ldots,x_n]$.

Def Let $I \subseteq R = k[x_1,\ldots,x_n]$. ~~Set $S = k[x_{l+1},\ldots,x_n]$~~ The l-th elimination ideal of I is $I_l = I \cap k[x_{l+1},\ldots,x_n]$

Thm Let G be a Gröbner basis for I wrt. lex order, with $x_1 > x_2 > \cdots > x_n$. Then $G_l = G \cap k[x_{l+1},\ldots,x_n]$ is a g.b. for I_l.

Proof Since $G_l \subseteq I_l$, must show $\langle LT(I_l)\rangle = \langle LT(G_l)\rangle$.

$\supseteq$: clear.

$\subseteq$: Let $f \in I_l$. Then $f \in I$, so $LT(f)$ is divisible by $LT(g)$ for some $g \in G$.

$f \in k[x_{l+1},\ldots,x_n] \Rightarrow g \in k[x_{l+1},\ldots,x_n]$ because we use lex order.

$\therefore g \in G_l$.

□

Application: Find $Z(I) \subseteq \mathbb{A}^n$.

First "find" $Z(I_1) \subseteq \mathbb{A}^{n-1}$.

For each point $(a_2,\ldots,a_n) \in Z(I_1)$, find all a_1 such that $(a_1,a_2,\ldots,a_n) \in Z(I)$.

Application $f: X \longrightarrow Y$ morphism of affine varieties. (2)

Find $\overline{f(X)}$. Find $I(f(X)) \subseteq k[Y]$

$X \subseteq \mathbb{A}^n$, $Y \subseteq \mathbb{A}^m$ closed subsets.

$f = (f_1, \dots, f_m) : X \longrightarrow \mathbb{A}^m$.

Find $I(f(X))$.

$\Gamma = \{ (x, f(x)) \subseteq \mathbb{A}^n \times \mathbb{A}^m \mid x \in X \} \subseteq \mathbb{A}^n \times \mathbb{A}^m$

$$f : X \longrightarrow \Gamma \xrightarrow{\pi} \mathbb{A}^m$$
$$x \longmapsto (x, f(x)) \longmapsto f(x).$$

Find $I(\pi(\Gamma))$.

$I(\Gamma) = \langle I(X), Y_1 - F_1, Y_2 - F_2, \dots, Y_m - F_m \rangle \subseteq k[\mathbb{A}^n \times \mathbb{A}^m]$

$I(\pi(\Gamma)) = I(\Gamma) \cap k[Y_1, \dots, Y_m]$.

Q: what if $f : X \dashrightarrow Y$ rational function? $f_i = g_i / h_i$

Solve equations $I \subseteq k[x_1, \dots, x_n]$ ideal. Find $Z(I) \subseteq \mathbb{A}^n$.

Idea: ~~For each point~~

$\pi : \mathbb{A}^n \longrightarrow \mathbb{A}^{n-1}$, $\pi(a_1, a_2, \dots, a_n) = (a_2, \dots, a_n)$

For each point $(a_2, \dots, a_n) \in \pi(Z(I))$, solve for a_1.

Note: $\overline{\pi(Z(I))} = Z(I_1)$, $I_1 = I \cap k[x_2, \dots, x_n]$.

AG fact: $\pi(Z(I))$ contains dense open subset of $Z(I_1)$.

i.e. $\exists$ closed $W \subsetneq Z(I_1)$ such that $Z(I_1) \setminus W \subseteq \pi(Z(I))$.

$\therefore$ For $(a_2, \dots, a_n) \in Z(I_1) \setminus W$, can find set of a_1 s.t. $(a_1, a_2, \dots, a_n) \in Z(I)$.

Remark Assume $I = (f_1, \dots, f_s) \subseteq R = k[x_1, \dots, x_n]$, and for some i we have $f_i = c\, x_1^N +$ terms in which x_1 has degree $< N$.

Then $R'/_{I \cap R'} \hookrightarrow R/_I$ finite extension of rings.

$\Rightarrow$ $\pi : Z(I) \twoheadrightarrow Z(I_1)$ surjective.

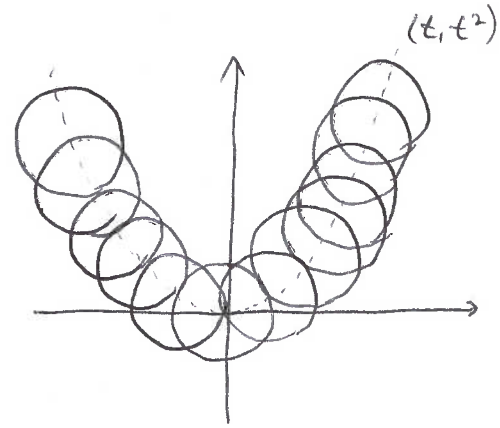
$\therefore$ For every $(a_2, \dots, a_n) \in Z(I_1)$ one can find $a_1 \in k$ s.t. $(a_1, a_2, \dots, a_n) \in Z(I)$.

Envelopes of families of curves.

Let $F \in k[x,y,t]$.

For each $t \in k$, set $C_t = \{(x,y) \in \mathbb{A}^2 \mid F(x,y,t) = 0\}$.

Example $\quad F(x,y,t) = (x-t)^2 + (y-t^2)^2 - 4$



"Def" A curve $E \subseteq \mathbb{A}^2$ is an envelope of the family $\{C_t\}_{t\in k}$ if E is tangent to each of the curves C_t.

Def The envelope of $\{C_t\}$ is the set

$$E = \{(x,y) \in \mathbb{A}^2 \mid \exists t \in k : F(x,y,t) = 0 \text{ and } \tfrac{\partial}{\partial t}F(x,y,t) = 0\}$$

Justification: suppose $t \mapsto (f(t), g(t))$ parametrizes a curve that is tangent to C_t at $(f(t), g(t))$ $\forall t$.

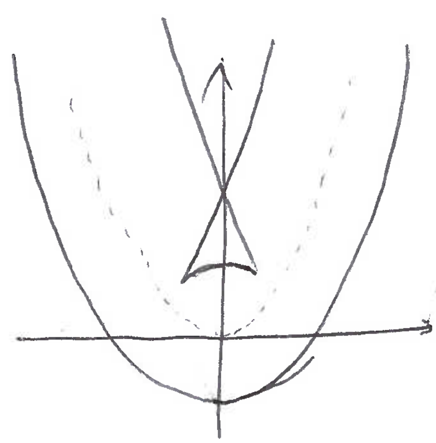
Then $F(f(t), g(t), t) = 0$. and

$$\left(\frac{\partial F}{\partial x}(f(t), g(t), t),\ \frac{\partial F}{\partial y}(f(t), g(t), t)\right) \cdot (f'(t), g'(t)) = 0$$

Since $\frac{\partial}{\partial t} F(f(t), g(t), t) = 0$, we obtain

$$\frac{\partial F}{\partial t}(f(t), g(t), t) = 0 \quad \forall t.$$

Compute: $\quad I(E) = \left(F, \frac{\partial F}{\partial t}\right) \cap k[x,y]$.



Example $\quad \frac{\partial F}{\partial t} = -2(x-t) - 4t(y-t^2)$

OBS: $\left(F, \frac{\partial}{\partial t}F\right)$ contains polynomial of the form

$$t^2 + h_1(x,y)\cdot t + h_0(x,y).$$

$\therefore$ Each point $(x,y) \in E$ is tangent to at most two circles C_t.

Resultants Let $f, g \in k[x]$, $f = a_0 x^\ell + a_1 x^{\ell-1} + \cdots + a_\ell$,
$g = b_0 x^m + b_1 x^{m-1} + \cdots + b_m$.

Does f and g have a common root?

Sylvester matrix:

$$\mathrm{Syl}(f,g,x) = \underbrace{\begin{bmatrix} a_0 & & & \\ a_1 & a_0 & & \\ a_2 & a_1 & \ddots & \\ \vdots & a_2 & & a_0 \\ a_\ell & \vdots & & a_1 \\ & a_\ell & & \vdots \\ & & & a_\ell \end{bmatrix}}_{m}\underbrace{\begin{bmatrix} b_0 & & \\ b_1 & b_0 & \\ b_2 & b_1 & b_0 \\ \vdots & b_2 & b_1 \\ b_m & \vdots & b_2 \\ & b_m & \vdots \\ & & b_m \end{bmatrix}}_{\ell} \quad (\ell+m)\times(\ell+m).$$

Def $\mathrm{Res}(f,g,x) = \det(\mathrm{Syl}(f,g,x))$.

Prop $\mathrm{Res}(f,g,x)$ is a polynomial with integer coefs in $a_0, \ldots, a_\ell, b_0, \ldots, b_m$.
Furthermore, f and g have a common factor in $k[x]$ iff $\mathrm{Res}(f,g) = 0$.

Proof
Let $p = p_0 x^{m-1} + p_1 x^{m-2} + \cdots + p_{m-1}$
$q = q_0 x^{\ell-1} + q_1 x^{\ell-2} + \cdots + q_{\ell-1}$.

Write $pf + qg = c_0 x^{\ell+m-1} + c_1 x^{\ell+m-2} + \cdots + c_{m+\ell-1}$.

Then
$$\begin{bmatrix} c_0 \\ c_1 \\ \vdots \\ c_{m+\ell-1} \end{bmatrix} = \mathrm{Syl}(f,g,x) \begin{bmatrix} p_0 \\ \vdots \\ p_{m-1} \\ q_0 \\ \vdots \\ q_{\ell-1} \end{bmatrix}$$

Note: f and g have a common factor
$\Updownarrow$
$\exists\, p, q \neq 0 : pf + qg = 0$
$\Updownarrow$
$\mathrm{Res}(f,g,x) = 0$.

□

Prop $\exists\, p(x)$ and $q(x)$ of degrees $\le m-1, \ell-1$ such that $pf + qg = \mathrm{Res}(f,g)$.

Proof clear if $\mathrm{Res}(f,g,x) = 0$.
Otherwise solve for p, q s.t. $[c_0, c_1, \ldots, c_{m+\ell-1}] = [0, 0, \ldots, 0, 1]$.

□

Com Alg. 4/3/2014 All rings Noetherian.

PIT Let $x_1, \dots, x_c \in R$ and let $P \subseteq R$ min. prime over $(x_1, \dots, x_c)$. Then $\operatorname{codim}(P) \le c$.

Reverse PIT $P \subseteq R$ any prime. Then P minimal over ideal gen. by $\operatorname{codim}(P)$ elts.

Cor R Noeth. domain. Then R UFD $\Leftrightarrow$ all prime ideals of codim 1 are principal.

Proof
$\operatorname{codim}(P) = 1 \iff P$ min. over principal ideal (by PIT + reverse PIT)

Earlier proved: R UFD $\Leftrightarrow$ all primes min over principal ideals are principal.

$\square$

Systems of Parameters

R local Noetherian ring, $\mathfrak{m} \subseteq R$ max ideal.

Cor $\dim(R)$ = smallest d s.t. $\exists\, x_1, \dots, x_d \in \mathfrak{m}$: $\mathfrak{m}^n \subseteq (x_1, \dots, x_d)$ $\forall n \gg 0$

Proof If $\mathfrak{m}^n \subseteq (x_1, \dots, x_d)$ then $R/(x_1, \dots, x_d)$ Artinian $\Rightarrow \mathfrak{m}$ min over $(x_1, \dots, x_d)$
$\Rightarrow \dim(R) \le d$.

Set $d = \dim(R)$.
Reverse PIT $\Rightarrow$ $\exists\, x_1, \dots, x_d \in \mathfrak{m}$ s.t. $\mathfrak{m}$ min over $(x_1, \dots, x_d)$.
$\Rightarrow \mathfrak{m}^n \subseteq (x_1, \dots, x_d)$ $\forall n \gg 0$.

$\square$

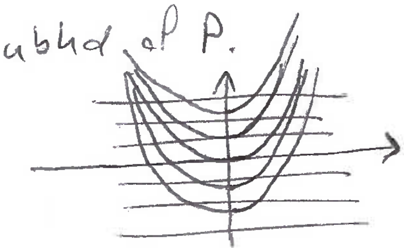
Def An ideal $I \subseteq \mathfrak{m}$ has <u>finite colength</u> if
R/I Artinian $\Leftrightarrow$ $\operatorname{length}(R/I) < \infty$ $\Leftrightarrow$ $\mathfrak{m}^n \subseteq I$ $\forall n \gg 0$.

A seq. $x_1, \dots, x_d$ with $d = \dim(R)$ is called a <u>system of parameters</u> if $(x_1, \dots, x_d)$ has finite colength.

Geometry $X \subseteq \mathbb{A}^n$, $p \in X$ point. $P \subseteq A(X)$ max ideal.
If $x_1, \dots, x_d \in P$ is systems of params for $A(X)_P$, then $x_1, \dots, x_d$ is "almost" a coordinate system in nbhd. of p:

$A(X)/(x_1 - x_1(Q), \dots, x_d - x_d(Q))$ is Artinian for $Q \in$ nbhd of P

$\Rightarrow Z(x_1 - x_1(Q), \dots, x_d - x_d(Q))$ is <u>finite</u> for $Q \in$ nbhd of P.



Example $(0,0) \in \mathbb{A}^2 \leftrightarrow P = (x, y) \subseteq k[x,y]$
$y,\ x^2 - y$ system of parameters for $k[x,y]_P$.

Def M f.g. R-module, $I \subseteq \mathfrak{m}$ ideal.
I has finite colength on M if $\operatorname{length}(M/IM) < \infty$.

Recall: M/IM has finite length
$\iff$ M/IM annihilated by product of max ideals
$\iff$ $\mathfrak{m}^n \subseteq \operatorname{ann}(M/IM)$
$\iff$ $\mathfrak{m} = \sqrt{\operatorname{ann}(M/IM)}$.

Prop R Noeth. ring, M f.g. R-module. $I \subseteq R$ ideal. Then $\sqrt{\operatorname{ann}(M/IM)} = \sqrt{I + \operatorname{ann}(M)}$.
Furthermore, if R local with max ideal $\mathfrak{m}$, then
(a) I has finite colength on M
$\iff$ $\mathfrak{m}^n \subseteq I + \operatorname{ann}(M)$ $\forall n \gg 0$
$\iff$ I has finite colength on $R/\operatorname{ann}(M)$.
(b) $0 \to M' \to M \to M'' \to 0$ exact.
Then I finite colength on M $\iff$ I has finite colength on M' and M''.
(c) $\dim(M) := \dim R/\operatorname{ann}(M)$ is min. # of generators of ideal with finite colength on M.

Proof
$\sqrt{\operatorname{ann}(M/IM)} = \sqrt{I + \operatorname{ann}(M)}$:

$p \supseteq \operatorname{ann}(M/IM) \iff (M/IM)_p = M_p/I_pM_p \neq 0$
$\iff M_p \neq 0$ and $I_p \subseteq P_p$ (NAK)
$\iff p \supseteq \operatorname{ann}(M) + I$.

(a) Set $\overline{R} = R/\operatorname{ann}(M)$.
$\operatorname{ann}(\overline{R}/I\overline{R}) = \operatorname{ann}(M) + I$.
I finite colength on M $\iff$ $\mathfrak{m}^n \subseteq \operatorname{ann}(M/IM)$ $\forall n \gg 0$
$\iff \mathfrak{m}^n \subseteq I + \operatorname{ann}(M)$ $\forall n \gg 0$
$\iff I$ finite colength on $\overline{R}$.

(b) $M'/IM' \to M/IM \to M''/IM'' \to 0$.
I finite colength on M' and M'' $\Rightarrow$
I finite colength on M $\Rightarrow$
I finite colength on M''.

Since $\operatorname{ann}(M') \supseteq \operatorname{ann}(M)$ we have
I fin colen on $M \Rightarrow I$ fin. colen. on M'.

(c) Follows from (a) + result about dim of local ring.

$\square$

Cor $(R, \mathfrak{m})$ local Noeth ring, M f.g. R-module.
$x \in \mathfrak{m} \Rightarrow \dim(M/xM) \geq \dim(M) - 1$.

Proof Set $d = \dim(M/xM)$.
Prop $\Rightarrow \exists\, x_1, \dots, x_d \in \mathfrak{m}$ s.t. $(x_1, \dots, x_d)$ has finite colength on M/xM.
$\Rightarrow (x, x_1, x_2, \dots, x_d)$ finite colength on $M \Rightarrow \dim M \leq d+1$.
□

Recall: Going Up: $R \subseteq S$ integral ext.

$$\begin{array}{ccc} R & \subseteq & S \\ \cup\!\mid & & \\ P & & \exists Q \;:\; P = R \cap Q. \\ \cup\!\mid & & \cup\!\mid \\ J \cap R & - & J \end{array}$$

OBS $R \to S$ flat ring hom,
$R \to \tilde{R}$ ring hom
$\Rightarrow \tilde{R} \longrightarrow S \otimes_R \tilde{R}$ flat.

Going Down (flat version)
$\varphi : R \longrightarrow S$ flat ring hom. R, S Noetherian. $p' \subseteq P \subseteq R$ prime ideals.
$Q \subseteq S$ prime ideal s.t. $P = \varphi^{-1}(Q)$. Then $\exists\, Q' \subseteq Q$ prime s.t. $p' = \varphi^{-1}(Q')$.

$$\begin{array}{ccc} R & \xrightarrow{\varphi} & S \\ \cup\!\mid & & \cup\!\mid \\ P & \text{———} & Q \\ \cup\!\mid & & \cup\!\mid \\ p' & \text{——} & \exists\, Q' \end{array}$$

Proof
$p'S \subseteq Q \Rightarrow \exists\, Q' \subseteq Q$ min prime over $p'S$.
$S/p'S = S \otimes_R R/p'$ is flat over R/p'.
Replace R with R/p', S with $S/p'S$. WLOG $p' = 0$.
Every $x \neq 0$ in R is nzd on $R \Rightarrow \varphi(x)$ is nzd on S (since S flat).
Q' min. prime in $S \Rightarrow Q' \in \mathrm{Ass}(S) \Rightarrow Q'$ consists of zero divisors.
$\therefore \varphi^{-1}(Q') = 0 = p'$.
□