Cayley-Hamilton-Nakayama continued

Thm (CHN) $\{\sum x_i m_i \mid x_i \in I, m_i \in M\} = IM$

Let $I \trianglelefteq R$, M f.g. R-module & suppose $\varphi: M \to IM < M$ is an R-module map. Then $\exists$ polynomial

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

w/ $a_i \in I^i$ such that

$p(\varphi) = 0 \in \operatorname{End} M$

Cor: If M is f.g. R-mod, $f: M \to M$ surjective $\Rightarrow f$ iso.

Pf: Consider M an $R[t]$ module, t acts as f.

as $M = tM = (tR)M$ $\quad$ CHK $\Rightarrow \exists p$ s.t. $p(\varphi) = 0$ in $\operatorname{End} M$.

($t \xrightarrow{\text{id}} \varphi$)

$\Rightarrow \varphi = \text{id} \Rightarrow p(1) = 0$ $\quad p(x) = x^n + a_1 x^{n-1} + \cdots + a_n$

$a_i \in t^i R$ $\quad = x^n + t b_1 x^{n-1} + \cdots + t^n b_n$

$\Rightarrow p(1) = 1 + t(\underbrace{b_1 + t b_2 + \cdots + t^{n-1} b_n}_{g \in \operatorname{End} M}) = 0$

note f & g commute $\longrightarrow$ $+$

$1 + fg = 0 \Rightarrow (-g) f = 1 \in \operatorname{End} M$

$f(-g)$

$\Rightarrow f$ is invertible $\Rightarrow$ isn. $\square$

Cor: if M is f.g. free rk n $\Rightarrow$ every order n gen set is a basis.

Pf: choose $m_1, \dots, m_n$ order n gen set.

$M \cong R^n \twoheadrightarrow M$ is an iso by previous $\Rightarrow$

$e_i \longrightarrow m_i$ $\qquad$ $R^n \to M$ iso. $\square$

Cor Comm. rgs have invariant Basis number

i.e. $R^n \cong R^m \iff m = n$.

Pf: if $R^n \cong R^m$ $m < n$ let $x_1, \dots, x_m$ be a basis,

extend to a map $R^n \to R^m$ surjective. $\Rightarrow$ iso.

R^m $e_1 \hookrightarrow x_1$

$\vdots \qquad \vdots$

$e_m \hookrightarrow x_m$

$e_{m+1} \to 0$

$\vdots \qquad \vdots$

$e_n \to 0$

$\Rightarrow R^n \to R^m$ is injective.

by $\square$

Next: Integrality

Mantra: Integral extensions of comm. rgs are the ring analog of algebraic field exts.

Def Given an extension of comm rgs S/R we say that $a \in S$ is integral over R if a is the root of a monic poly in $R[x]$.

Original motivation:

$$\begin{array}{ccc} \mathbb{Q} & - & \mathbb{Q}(i) \\ | & & | \\ \mathbb{Z} & - & \mathbb{Z}[i] \end{array} \qquad i^2+1=0$$

Def An extension of comm rgs S/R is integral if every $s \in S$ is integral over R.

Side note: generally want to consider $\varphi: R \to S$ hom instead of restricting to φ an inclusion.

$a \in S$ is integral over R if $\exists\, f \in R[x]$ s.t. f monic.

$$\varphi(f)(a) = 0.$$

ex: $\mathbb{Z}/3\mathbb{Z}$ is integral over $\mathbb{Z}$.

$\bar{a} \in \mathbb{Z}/3\mathbb{Z}$ $\quad x - \bar{a} = \varphi(x-a)$

Aside: in geometry ~ corresp to "finite maps" preimages of pts are finite sets. fin. integral algebras

Def S/R an R-alg is finite. if S is f.g. as an R-module.

Lem (compare to 28.7)
S/R is integral if and only if ev $s \in S$ is contained in a subalgebra of S which is finitely generated as an R-module.

Pf: if S/R integral and $s \in S$ satisfies a monic deg n poly then $\{1, s, s^2, \dots, s^{n-1}\} = R[s]$ f.g. subalgebra of S.

Conversely, if $s \in S' \subseteq S$ S' finite subalgebra.
mult. by s gives a hom $S' \xrightarrow{\varphi} S'$, $\varphi(x) = sx$.

CHN $\Rightarrow$ $\exists$ monic poly $p \in R[x]$ w/ $p(\varphi) = 0$

$p(s)$ induces 0 by mult. in $S' \Rightarrow p(s) \cdot 1 = 0 \Rightarrow p(s) = 0$.
□

Observation: if $a \in S$ integral over R then $R[a]$ is finite R-alg.

Observe: if S/R fin alg & T/S fin alg $\Rightarrow T/R$ fin.

Pf: if $s_1, \dots, s_n$ gen S/R & $t_1, \dots, t_m$ gen T/S

then $\{s_i t_j\}$ gen T/R

Cor: if $x, y \in S$ are integral / R then so are all the elements of $R[x,y]$.

Pf: x integral / $R \Rightarrow R[x]/R$ fin $\quad y$ int / R

$\Rightarrow y$ int / $R[x] \Rightarrow R[x,y]/R[x]$ fin.

as an elt of $R[x,y] = R[x][y]$

algebra $\Rightarrow R[x,y]/R$ fin $\Rightarrow R[x,y]/R$ integral.

Cor: If S/R is f.g. & integral then it is finite.

Def: If S/R is an algebra. Let $R' = \{a \in S \mid a \text{ is integral over } R\}$

call R' the integral closure of R in S.

Def: R is integrally closed in S if its integral closure is itself.

Lem: if R' is the integral closure of R in S then R' is integrally closed in S.

exercise

Lem: Let R be a domain w/ frac field F and let E/F be algebraic.

Let S be the int. closure of R in E then $\mathrm{Frac}\, S = E$.

Pf: if $a \in E$ let f be its min poly

$$f(x) = \sum c_i x^i \qquad c_i = \frac{u_i}{v_i}$$

multiply by $(\prod v_i)^n$

$$x^n + \frac{u_1}{v_1} x^{n-1} + \cdots + \frac{u_n}{v_n}$$

$$\left((\prod v_i)x\right)^n + u_1 \prod v_i \left((\prod v_i)x\right)^{n-1} + \cdots + u_n \prod \cdots)$$

$\Rightarrow$ αa is integral over R since $\alpha \in R$.

$\Rightarrow$ $\alpha a \in$ int. closure $\Rightarrow a \in$ (int. closure $(R \setminus \{0\})^{-1} R$)

Def R is int. closed (or normal) if it is int. closed in its fraction field.

R: domain.

Q: given

$$\begin{array}{ccc} E & & \text{finite} \\ | & & \\ S & & \text{int. closure} \\ | & & \\ R & & \end{array} \qquad F = \mathrm{Frac}(R)$$

is S/R finite?

Def we say R is Japanese (N_2) if S/R is always finite.

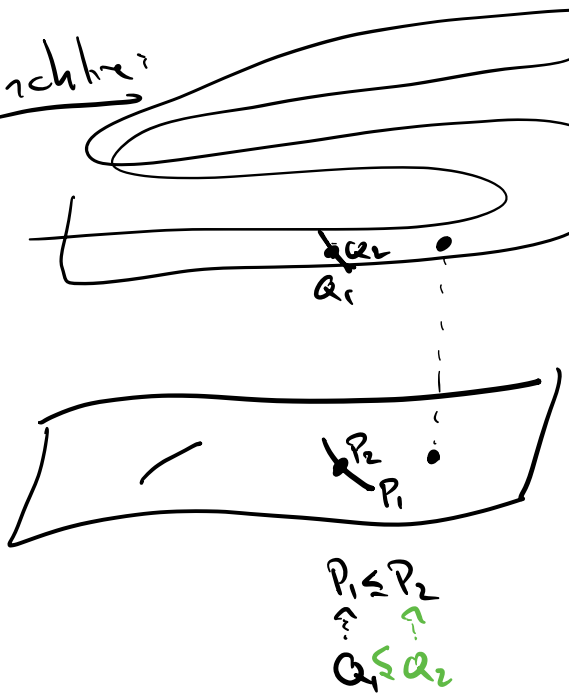
Def we say R is N_1 if the int. closure of R (in its frac field) is finite over R.

Honorable mention:

factorial = UFD $\Rightarrow$ normal (Prop 4.10)

Extended Eisenbud exercise

Punchline:



S

$\uparrow$

R

given $P \subseteq R$ prime

$\exists Q \subseteq S$ prime s.t.

$Q \cap R = P$.

"lying over"

$P_1 \subseteq P_2$

$\uparrow$ $\uparrow$

$Q_1 \subsetneq Q_2$
