Lecture 10. Cayley-Hamilton thm.

Thm (Determinant trick) M an R-module generated by $m_1, \dots, m_n$, $\varphi: M \to M$ an endom. let $\varphi(m_i) = \sum a_{ij} m_j$, and $A = (a_{ij})$. Let $P_A(T) = \det(T - A)$. Then $P_A(A) = 0$.

Remark. This is equivalent to the spec. case $M = R^n$, the usual CH theorem.

Pf. Let Δ be the matrix with entries $\delta_{ij}\varphi - \mu_{a_{ij}}$ with entries in the commutative subring $R[\varphi] \subset \operatorname{End} M$, and X the column vector with entries m_i. Then $\Delta X = 0$. Multiply this on the left by the matrix Γ of cofactors of Δ: $\Gamma \Delta X = 0$. But $\Gamma\Delta = \det(\Delta)$. So we get $\det(\Delta) m_i = 0$, hence $\det(\Delta) = 0$. But $\det(\Delta) = P_A(\varphi)$. So $P_A(\varphi) = 0$.

Prop. M f.gen, $\mathfrak{a} \subset R$ ideal. Then $M = \mathfrak{a}M$ iff $\exists a \in \mathfrak{a}$ s.t. $(1+a)M = 0$.

Pf. $\Rightarrow$: $M = \mathfrak{a}M$. Let $m_1, \dots, m_n$ generate M, $m_i = \sum a_{ij} m_j$ $a_{ij} \in \mathfrak{a}$. Let $A = (a_{ij})$. Let $P_A(T) = T^n + a_1 T^{n-1} + \dots + a_n$. Let $a = a_1 + \dots + a_n$. We use CH for $\varphi = 1$, so $P_A(1) = 0 \Rightarrow (1+a)M = 0$. Conversely if $\exists a$ with $(1+a)M = 0$ then $m = -am \Rightarrow M \subset \mathfrak{a}M$. ∎

Cor. M f.g. R-module, $\varphi: M \to M$ endom. If φ is surjective then φ is an isom.

Pf. Let $P = R[X]$ be the polyn. ring in one var. $\mu: P \to \mathrm{End}\, M$, $\mu(X) = \varphi$. Then M is a P-module. Let $\alpha = \langle X \rangle \subset P$. Since φ is surj, $M = \alpha M$. So by Prop $\exists a \in \alpha$ with $(1+a)M = 0$. Say $a = Xq(X)$, so $(1 + Xq(X))M = 0$, i.e. $(1 + \varphi q(\varphi))M = 0$. Let $\psi = -q(\varphi)$. Then $\varphi\psi = 1$ and $\psi\varphi = 1$. So φ is an isom.

Cor. $R \neq 0$, m, n positive integers. Then

(1) any n generators $(v_1, \ldots, v_n)$ form a free basis for R^n

(2) If $R^m \cong R^n$ then $m = n$.

Pf. (1) Let $\varphi: R^n \to R^n$ be the surjection mapping e_i to v_i. Then φ is surjective, hence an isom. So v_i are independent.

(2) Say $m \leq n$. Then R^n has m generators. Add to them $n - m$ zeros. The result is a free basis, so there can be no zeros, hence $n = m$.

Lemma. (Nakayama). R a ring, $m \subset \mathrm{rad}(R)$ an ideal, and M a f.g. module. Assume $M = mM$. Then $M = 0$.

Pf. $\exists a \in m$ s.t. $(1+a)M = 0$. But $1+a$ is a unit since $m \subset \mathrm{Rad}(R)$. So $M = (1+a)^{-1}(1+a)M = 0$.

Ex. Nakayama lemma may fail if the module is not f.gen. E.g. let $A = \mathbb{C}[[x]]$, $m = (x)$, $K = \mathbb{C}((x))$. So $K = mK$, but $K \neq 0$.

Prop. $m \subset \mathrm{rad}(R)$ ideal, $N \subset M$ modules.

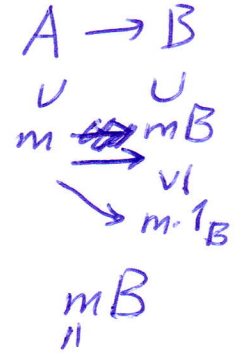
(1) If M/N is f.gen and $N + mM = M \Rightarrow N = M$.

(2) If M is f.gen. then $m_1, \dots, m_n$ generate M $\Leftrightarrow$ images $m_1', \dots, m_n'$ generate M/mM.

Pf. (1) Apply Nakayama to M/N. We have $m \cdot M/N = M/N$, so $M/N = 0$, and $N = M$

(2) $\Leftarrow$ let $N \subset M$ be gen. by $m_1, \dots, m_n$. Since M is f.gen, so is M/N. So by (i) $N = M$ if m_i' generate M/mM. The other direction is obvious.

Local homomorphisms. Let $\varphi : A \to B$ be a map of local rings, m^{cA} and n^{cB} their max. ideals.



Lemma TFAE:

(1) $\varphi^{-1} n = m$

(2) $1 \notin mB$

(3) $mB \subset n$

Pf. (1) $\Rightarrow$ (2) : (1) implies that $\varphi(m) = n \neq 1$. $\Rightarrow$ (2)

(2) $\Rightarrow$ (3) $mB \subset n'$, some max. ideal, but $n' = n$ so get $mB \subset n$, i.e. (3). Also (3) $\Rightarrow m \subset \varphi^{-1}(mB) \subset \varphi^{-1}(n)$. So (1) holds since m is maximal.

Def. A homom. satisfying any of these is called local.

Ex: $\varphi: k[[x]] \to k[[x]]$ $\varphi(x) = p(x)$ $p(0) = 0$
is local. But $\varphi: \underset{A}{k[[x]]} \hookrightarrow \underset{B}{k((x))}$ not local
since $m \cdot B = B$, so $1 \in mB$.

Prop. Consider the following conditions on an R-module P:
(1) P is free of finite rank
(2) P is proj and f.gen.
(3) P is flat and finitely presented.
Then (1) $\Rightarrow$ (2) $\Rightarrow$ (3), and they are equivalent if R is local.

Pf. (1) $\Rightarrow$ (2) known before. (2) $\Rightarrow$ (3) know proj. is flat. also $P \oplus Q = R^n$, and Q is a quot of R^n, so $0 \to Q \to R^n \to P \to 0$, and Q f.gen.
$\Rightarrow P$ fin. pres.
Now supp. R is local, show (3) $\Rightarrow$ (1).
Let P flat, R local. Let $R/m = k$ (residue field).
Then $0 \to L \otimes k \to F \otimes k \to P \otimes k \to 0$ is exact,
where $0 \to L \to F \to P \to 0$ is exact and F is free.
~~Can k be flat~~ $\{e_i\} \to \{p_i\}$
Now, F is fin.gen, so $F \otimes k = k^n$. Can choose F so n is minimal. Then free basis e_i of F map to p_i which is a min. set of gen. of P.

Lemma A loc. ring, $m \subset A$ max. ideal, M f.g. A-module, $m_1, \dots, m_n \in M$. $k = A/m$, $M' = M \otimes k = M/mM$, m_i' images m_i in M'. Then $m_1', \dots, m_n'$ form a basis of $M/mM \iff m_1, \dots, m_n$ form a minimal

generating set for M. In partic, every min. generating set has the same # of elements.

Pf. $m_1', \dots, m_n'$ a basis $\Rightarrow$ $m_1, \dots, m_n$ a generating set, which is clearly minimal. (by Nakayama) Conversely, if $m_1, \dots, m_n$ a min gen. set, then $m_1', \dots, m_n'$ span M/mM. Assume ~~$\sum \alpha_i m_i' = 0$. Say~~ $m_n' = \sum_{i=1}^{n-1} \beta_i m_i'$. Then

$m_n - \sum \beta_i m_i \in mM$, i.e. $m_n - \sum_{i=1}^{n-1} \beta_i m_i = \sum_{j=1}^{n} \alpha_i m_i$,

$\alpha_i \in m$. So $(1 + \alpha_n) m_n = \sum_{i=1}^{n-1} (\alpha_i + \beta_i) m_i$,

$m_n = \sum (1+\alpha_n)^{-1} (\alpha_i + \beta_i) m_i \Rightarrow$ the set is not minimal.

~~This means that the basis e_i of F maps to a min. set of generators p_i for P.~~

By lemma, $p_i \otimes 1$ are a basis of $P \otimes k$, so $\dim P \otimes k = n = \dim F \otimes k \Rightarrow L \otimes k = 0$.

Assume P is finitely presented. Then L is f.generated. Hence $L = 0$ by Nakayama (if ~~$L \neq 0$~~ lift of generators of $L \otimes k = L/mL$). So $P = F$, as desired $\square$.

Def. R' an R-algebra. Then R' is module finite over R if R' is a f.g. R-module.

Def. $x \in R'$ is *integral* over R (integrally dependent) if $\exists a_1, \ldots, a_n \in R$ s.t. $x^n + a_1 x^{n-1} + \cdots + a_n = 0$ on R.

If $\forall x \in R'$ is integral over R, say R' *integral* over R

Prop. $R \to R'$, $n \in \mathbb{N}$, $x \in R'$. TFAE:

(1) x satisfies an eqn of int. dep. of degree n.

(2) $R[x]$ is gen. as an R-mod by $1, x, x^2, \ldots, x^{n-1}$

(3) x lies in a subalg R'' gen. by n elts as a mod over R

(4) $\exists$ a faithful $R[x]$-module M generated over R by n elements.

Pf. Ass. (1). Then $x^n = -a_1 x^{n-1} - \cdots - a_n$. Then can express x^{n+1}, etc. to get (2).

Ass. (2) $\Rightarrow$ (3) with $R'' = R[x]$

Ass (3) $\Rightarrow$ Can take $M = R''$ and get (4)

Ass. (4) $\Rightarrow$ Take $\varphi = \mu_x$ in the det. trick. We obt. monic p s.t. $p(x)M = 0$. Since M is faithful, $p(x) = 0$. $\Rightarrow$ (1). ∎

Cor. R a dom, $P = R[X]$, $\alpha \subset P$. $R' = P/\alpha$, x image of X in R'. Let $n \in \mathbb{N}$. TFAE:

(1) $\alpha = (p)$, p monic of degree n.

(2) $1, x, \ldots, x^{n-1}$ form a free basis of R' over R.

(3) R' is a free R-module of rank n.

Pf. Ass. (1). Then $1, x, \ldots, x^{n-1}$ generate, and are lin. indep.

(2) $\Rightarrow$ (3) trivial

(3) $\Rightarrow$ (1). Consider the char poly of mult. by x on R'. Then get $P/(p(x)) \twoheadrightarrow R'$ surjective. This is a morphism $R^n \to R^n$, so it's an isom, giving (1).

Lemma. $R \subset R'$ finite module, M f.g. $/R' \Rightarrow M$ f.g. $/R$.

Pf. x_i gen. R'/R, m_j gen. M/R' then $x_i m_j$ generate M/R.

Thm. (Tower law of integrality) $R \to R' \to R''$. If $x \in R''$ is integral over R' and R' is integral over R. Then x is integral over R.

Pf. Say $x^n + a_1 x^{n-1} + \cdots + a_n = 0$, $a_i \in R'$.
Let $R_m = R[a_1, \ldots, a_m] \subset R'$. Then
R_m is module finite over R_{m-1},
so R_m is module finite over R
by induction in m. Now x is integral
over R_n. So $R_n[x]$ is module finite
over R_n i.e. $R_n[x]$ is module finite
over R. So x is integral over R
by the above prop.

Thm. $R \to R'$. TFAE:
(1) R' f.g. as an R-alg and integral /R.
(2) $R' = R[x_1, \ldots, x_n]$, x_i integral /R.
(3) R' is module finit /R.

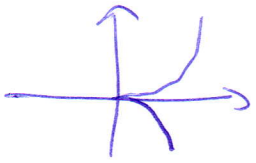
Pf. (1) $\Rightarrow$ (2). $R' = R[x_1, \ldots, x_n)$, x_i int.
(2) $\Rightarrow$ (3) $R[x_1]$ module finite $\Rightarrow$ $R[x_1, x_2]$ mod.
finite $\Rightarrow$ ... (by induction)
(3) $\Rightarrow$ (1) R' integral /R by the above Prop.

Def. $R \to R'$. Integral closure or
normalization of R in R' is the
subset of the elements $\overline{R} \subset R'$ that
are integral over R. If $R \subset R'$ and
$\overline{R} = R$ then say R is integrally closed in R'.

If R is a domain, then $\overline{R} \subset \mathrm{Frac}(R)$ is called <u>normalization</u> of R, and R is <u>normal</u> if $R = \overline{R}$.

<u>Ex.</u> $R = \mathbb{C}[x]$, $R' = \mathbb{C}(x)$ integrally closed (normal).

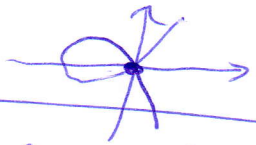
$R = \mathbb{C}[\underset{\|}{x^2}, \underset{\|}{x^3}] = \mathbb{C}[\underset{u}{u}, \underset{v}{v}] / u^3 = v^2$.



Then $\overline{R} \ni x : \; x^2 = u$. So $\overline{R} = \mathbb{C}[x]$.

$R = \mathbb{C}[u,v] / u^2 = v^2(v+1) = \mathbb{C}[\underset{v}{x^2 - 1}, \underset{u}{x(x^2-1)}]$.

$\overline{R} = \mathbb{C}[x] \quad (x^2 = 1 + v)$.



<u>Thm.</u> $R \to R'$, $\overline{R}$ integral closure of R in R'. Then $\overline{R}$ is an R-algebra and $\overline{R}$ is integrally closed in R'.

<u>Pf.</u> Take $a \in R$, $x, y \in \overline{R}$. Then $R[x,y] \subset R'$ is integral over R. So ax, $x+y$, xy are integral over R. ~~by the above prop.~~ Thus $\overline{R}$ is an R-algebra. Also if x is integral over $\overline{R}$ then it's integral over R, so get $\overline{\overline{R}} = \overline{R}$.

<u>Thm.</u> (Gauss) A UFD is normal.

<u>Pf.</u> Let R be a UFD. Given $x \in \mathrm{Frac}(R)$,

Say $x = r/s$ with $r, s \in R$, rel. prime.
Supp. x sat. a polynomial eqn
$x^n = -(a_1 x^{n-1} + \cdots + a_n)$.
Then $r^n = -(a_1 r^{n-1} + \cdots + a_n s^{n-1})s$.
So any prime dividing s also divides r.
So s is a unit, and $x \in R$.

Ex. 1) Polyn. rly in n variables is normal.

2) $R = \mathbb{Z}[\sqrt{5}]$ not a UFD $(1+\sqrt{5})(1-\sqrt{5}) = 2 \cdot 2$
$(\tau^2 - \tau - 1 = 0)$
However, $\tau = \frac{1+\sqrt{5}}{2}$ is an alg. integer.
It's known that $\mathbb{Z}[\tau]$ is a PID $\Rightarrow$ UFD
$\Rightarrow \mathbb{Z}[\tau] \supset \bar{R}$. So $\mathbb{Z}[\tau] = \bar{R}$.

3) $d \in \mathbb{Z}$ square free. $K = \mathbb{Q}(\sqrt{d})$.
$R = \mathbb{Z} \oplus \mathbb{Z}\delta$, $\delta = \begin{cases} \frac{1+\sqrt{d}}{2}, & d \equiv 1 \bmod 4 \\ \sqrt{d}, & \text{if not.} \end{cases}$
Then R is the normalization $\bar{\mathbb{Z}}$ of $\mathbb{Z}$ in K.
(ring of integers).