Lecture 40 Friday April 29

The Smith Normal Form

Let $F =$ field

Given matrix $A \in Mat_n(F)$ $\quad n \geq 1$

Consider matrix

$$xI - A \qquad *$$

where $x =$ indeterminate.

Recall

$$\det(xI - A) = \text{char poly of } A$$
$$\parallel$$
$$c(x)$$

View $*$ as an element of $Mat_n(R)$ where

$$R = F[x]$$

Suppose we try to make $*$ diagonal by applying elementary row and column operations.

Elementary row operations:

(a) For distinct i, j $(1 \le i, j \le n)$

interchange row i, row j

(b) For distinct i, j $(1 \le i, j \le n)$ and $s \in R$,

replace row i by row i + s row j

(c) For $1 \le i \le n$ and a unit $\alpha \in R$

replace row i by α row i

Elem column operations are similar.

Effect of elem row/col ops on det:

(a) $\det' = -\det$

(b) $\det' = \det$

(c) $\det' = \alpha \det$

So $\det, \det'$ are associates in R

Using above row/col operations,

one can put $xI-A$ into the form

"Smith normal form"

$$\begin{pmatrix} 1 & & & & & & & \\ & 1 & & & & & 0 & \\ & & \ddots & & & & & \\ & & & 1 & & & & \\ & & & & m_1(x) & & & \\ & 0 & & & & m_2(x) & & \\ & & & & & & \ddots & \\ & & & & & & & m_r(x) \end{pmatrix}$$

**

with $m_1(x), m_2(x), \ldots, m_r(x) \in F[x]$ all

monic of degree ≥ 1 and

$$m_1(x) \mid m_2(x) \mid \ldots \mid m_r(x)$$

the polynomials $m_i(x)$ are the invariant factors

from the rational canonical form of A.

— ∘ —

To explain, we return to free R-modules

and their R-submodules.

Until further notice

R is any PID

Consider free R-module R^n

Given an R-submodule W of R^n

Write $m = \operatorname{rank}(W)$

Recall $\exists$ R-module iso $W \cong R^m$

So $\exists$ lin indep $w_1, w_2, \dots, w_m \in W$ st

$$W = Rw_1 + Rw_2 + \dots + Rw_m$$

View

$$R^n = \left\{ \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} \;\middle|\; \alpha_i \in R \quad 1 \le i \le n \right\}$$

Define $B \in \operatorname{Mat}_{n \times m}(R)$ such that

column i of B $= w_i$ $\qquad 1 \le i \le m$

By thm 25 $\exists$ linearly indep generators

$v_1, v_2, \ldots, v_n$ for R^n and nonzero $d_1, d_2, \ldots, d_m$ in R

such that both

(i) $d_1 / d_2 / \cdots / d_m$

(ii) $W = Rd_1v_1 + Rd_2v_2 + \cdots + Rd_mv_m$

Consider the matrix in $\mathrm{Mat}_n(R)$ with column $i = v_i$

for $1 \le i \le n$. This matrix is invertible

since $v_1, v_2, \ldots, v_n$ are lin indep generators for R^n.

Call the matrix P^{-1}

Next write

$$d_1v_1, \; d_2v_2, \; \ldots, \; d_mv_m \qquad ☆$$

in terms of

$$w_1, \; w_2, \; \ldots, \; w_m. \qquad ☆☆$$

$\exists$ $Q \in \mathrm{Mat}_m(R)$ st for $1 \le j \le m$,

$$d_jv_j = \sum_{i=1}^{m} Q_{ij} w_i$$

Obs Q is invertible since each of ☆, ☆☆ are lin indep

gens for W

Define $D \in Mat_{n \times m}(R)$ by

$$D = \left(\begin{array}{c} \begin{matrix} d_1 & & 0 \\ & d_2 & \\ 0 & & \ddots \\ & & & d_m \end{matrix} \\ \hline 0 \end{array} \right)$$

We get

$$P^{-1} D = B Q$$

So

$$D = P B Q$$

Since P is invertible, left-mult by P can be achieved via a sequence of row operations.

Since Q is invertible, right-mult by Q can be achieved via a sequence of column operations.

So the equation

$$D = PBQ$$

implies that we can turn B into D via a sequence of row/col operations.

— o —

Return to our matrix $A \in Mat_n(F)$

and ring $R = F[x]$

$m_1(x), m_2(x), \ldots, m_\ell(x)$ are inv factors for Rat. Can. form of A.

Consider vector space $V = F^n$ over F (col vectors)

Define

$$e_i = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \end{pmatrix} \leftarrow i \qquad \in V$$

So $e_1, e_2, \ldots, e_n$ is basis for V

View V as an R-module on which x acts as

$$x: \begin{array}{ccc} V & \longrightarrow & V \\ v & \longrightarrow & \underset{\substack{\uparrow \\ \text{matrix mult}}}{Av} \end{array}$$

The R-module V is generated by $e_1, e_2, \ldots, e_n$

But $e_1, e_2, \ldots, e_n$ are lin dependent over R.

Indeed

$$x e_j = \sum_{i=1}^{n} A_{ij} e_i \qquad 1 \le j \le n$$

The map

$$\varphi : \begin{array}{ccc} R^n & \longrightarrow & V \\ \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} & \longrightarrow & a_1 e_1 + a_2 e_2 + \cdots + a_n e_n \end{array}$$

is surj R-module hom.

Define $W = \ker(\varphi)$

The map φ induces an R-module iso

$$R^n / W \simeq V$$

The R-module V is torsion since $\dim_F(V) < \infty$

So R-module V has rank 0

So R-module W has rank n

For $1 \leq i \leq n$ define

$$w_i := \text{column } i \text{ of } xI - A$$

$$\in R^n$$

One checks

$$w_1, w_2, \dots, w_n \quad \text{are lin indep over } R$$

and

$$W = Rw_1 + Rw_2 + \dots + Rw_n$$

In our earlier discussion $B \in \mathrm{Mat}_n(R)$ satisfies

$$\text{column } i \text{ of } B = w_i \qquad 1 \le i \le n$$

So

$$B = xI - A$$

By Th 25 $\exists$ R-linearly indep gens $v_1, v_2, \dots, v_n$ for R^n and nonzero $d_1, d_2, \dots, d_n$ in R st both

(i) $d_1 \mid d_2 \mid \dots \mid d_n$

(ii) $W = Rd_1v_1 + Rd_2v_2 + \dots + Rd_nv_n$

WLOG $d_i \in R = F[x]$ is monic for $1 \le i \le n$

By the construction of the $m_i(x)$ the sequence

$$d_1, d_2, \ldots, d_n$$

is equal to

$$1, 1, \ldots, 1, m_1(x), m_2(x), \ldots, m_r(x)$$

Define a matrix $D \in Mat_n(R)$ by

$$D = \begin{pmatrix} d_1 & & & 0 \\ & d_2 & & \\ & & \ddots & \\ 0 & & & d_n \end{pmatrix}$$

So D is the Smith normal form for A

By our previous discussion we can turn $\underset{\beta}{\overset{}{xI - A}}$ "

into D via a sequence of row/col operations.

$\square$

Ex $n=3$

$$A = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

A is permutation matrix

$$A^3 = I$$

$$x^3 - 1 = \text{min poly of } A$$
$$= \text{char poly of } A$$

Smith Normal form for A is

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & x^3-1 \end{pmatrix}$$

We can send

$$\begin{pmatrix} x & 0 & -1 \\ -1 & x & 0 \\ 0 & -1 & x \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & x^3-1 \end{pmatrix}$$

via a sequence of elem row/col ops (try it)

$\square$