5/8/2019 >
(115)

§14.4 Diagonalizing matrices over a PID

THEOREM (14.4.6): For R a PID and $A \in R^{m \times n}$, $\exists \; P \in GL_n(R), \; Q \in GL_m(R)$

such that
$$Q^{-1}AP = \left[\begin{array}{c|c} \begin{matrix} d_1 & & 0 \\ & d_2 & \\ & & \ddots \\ 0 & & d_r \end{matrix} & 0 \\ \hline 0 & 0 \end{array}\right] \quad (m \times n)$$
with $d_1 | d_2$, $d_2 | d_3$, ..., $d_{r-1} | d_r$

called the Smith normal form for A.

proof (only for R a Euclidean domain with size function $R \xrightarrow{\sigma} \{0,1,2,\ldots\}$, but the general idea is similar) P.I.D

Induction on the smallest size function $\sigma(a_{ij})$ of any nonzero entry $a_{ij} \neq 0$ occurring in A.

We will repeatedly apply these row & column operations to A that are invertible over R, corresponding to multiplying by elementary matrices on the left and right that are in $GL_m(R)$, $GL_n(R)$:

- swap rows or columns $\longleftrightarrow$ $\begin{bmatrix} 1 & & & 0 \\ & 0 & 1 & \\ & 1 & 0 & \\ 0 & & & 1 \end{bmatrix}$
- add a multiple of a row/col to another $\longleftrightarrow$ $\begin{bmatrix} 1 & & 0 \\ & \ddots & \\ a & & 1 \end{bmatrix}$
- scale a row or column by some $u \in R^\times$ $\longleftrightarrow$ $\begin{bmatrix} 1 & & & 0 \\ & u & & \\ & & \ddots & \\ 0 & & & 1 \end{bmatrix}$

e.g. $A = \begin{bmatrix} -10 & 0 & 6 \\ 8 & 4 & 4 \end{bmatrix} \in \mathbb{Z}^{2 \times 3}$ (so $R = \mathbb{Z}$)

(1st) Find the nonzero entry $a_{ij} \in A$ with smallest size function $\sigma(a_{ij})$; permute rows and cols to make it a_{11}.

e.g. $\begin{bmatrix} -10 & 0 & 6 \\ 8 & 4 & 4 \end{bmatrix} \rightsquigarrow \begin{bmatrix} (4) & 4 & 8 \\ 6 & 0 & -10 \end{bmatrix}$

(2nd) Use a_{11} as a pivot to replace entries in 1st row or column by their remainder r having $\sigma(r) < \sigma(a_{11})$ or $r = 0$

e.g. $\begin{bmatrix} (4) & 4 & 8 \\ 6 & 0 & -10 \end{bmatrix} \rightsquigarrow \begin{bmatrix} (4) & 0 & 0 \\ 6 & -6 & -22 \end{bmatrix} \rightsquigarrow \begin{bmatrix} (4) & 0 & 0 \\ 2 & -6 & -22 \end{bmatrix}$

(3rd) Go back to 1st step if any entries now have $\sigma(a_{ij}) < \sigma(a_{11})$

e.g. $\begin{bmatrix} (4) & 0 & 0 \\ 2 & -6 & -22 \end{bmatrix} \rightsquigarrow \begin{bmatrix} (2) & -6 & -22 \\ 4 & 0 & 0 \end{bmatrix}$

$\rightsquigarrow \begin{bmatrix} (2) & -6 & -22 \\ 0 & -12 & -44 \end{bmatrix} \rightsquigarrow \begin{bmatrix} (2) & 0 & 0 \\ 0 & -12 & -44 \end{bmatrix} = \begin{bmatrix} (2) & 0 & 0 \\ 0 & \vdots & \vdots \end{bmatrix}$ both divisible by (2)

(4th) Repeat until every entry is divisible by a_{11} and 1st row/column are 0 except for a_{11}, so $A = \begin{bmatrix} a_{11} & 0 \cdots 0 \\ 0 & \\ \vdots & \hat{A} \\ 0 & \end{bmatrix}$ ← all entries divisible by a_{11}

(5th) Apply the algorithm inductively to $\hat{A}$.

$\begin{bmatrix} (2) & 0 & 0 \\ 0 & -12 & -44 \end{bmatrix} \rightsquigarrow \begin{bmatrix} (2) & 0 & 0 \\ 0 & (12) & 44 \end{bmatrix} \rightsquigarrow \begin{bmatrix} (2) & 0 & 0 \\ 0 & (12) & 8 \end{bmatrix} \rightsquigarrow \begin{bmatrix} (2) & 0 & 0 \\ 0 & (8) & 12 \end{bmatrix} \rightsquigarrow \begin{bmatrix} (2) & 0 & 0 \\ 0 & (8) & 4 \end{bmatrix}$

$\rightsquigarrow \begin{bmatrix} (2) & 0 & 0 \\ 0 & (4) & 8 \end{bmatrix}$

Smith normal form $= \left[\begin{array}{cc|c} (2) & 0 & 0 \\ 0 & (4) & 0 \end{array}\right] \leftarrow$ ■

PROPOSITION: In the above setting where $Q^{-1}AP = S = \left[\begin{array}{c|c} d_1 \ddots d_r & 0 \\ \hline 0 & 0 \end{array}\right] \in A^{m \times n}$

then as R-modules, $R^m / \mathrm{im}\, A \cong R^m / \mathrm{im}\, S \cong R/(d_1) \times \cdots \times R/(d_r) \times R^{m-r}$

EXAMPLES: (1) $\mathbb{Z}^3 \xrightarrow{\begin{bmatrix} -10 & 0 & 6 \\ 8 & 4 & 4 \end{bmatrix} = A} \mathbb{Z}^2$ has $\mathbb{Z}^2/\mathrm{im}\, A \cong \mathbb{Z}^2/\mathrm{im}\, S$ where $S = \left[\begin{array}{cc|c} 2 & 0 & 0 \\ 0 & 4 & 0 \end{array}\right]$

$\cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$

(2) Transposing these matrices

$\mathbb{Z}^2 \xrightarrow{\begin{bmatrix} -10 & 8 \\ 0 & 4 \\ 6 & 4 \end{bmatrix} = B} \mathbb{Z}^3$ has $\mathbb{Z}^3/\mathrm{im}\, B \cong \mathbb{Z}^3/\mathrm{im} \begin{bmatrix} 2 & 0 \\ 0 & 4 \\ 0 & 0 \end{bmatrix} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}^1$

<u>proof of PROP:</u> Note that since $Q^{-1}AP = S$

then $A = QSP^{-1}$,

and $\operatorname{im} A = \operatorname{im}(QSP^{-1}) = \operatorname{im}(QS)$: $\quad \underline{y} \in \operatorname{im}(QSP^{-1})$

$\Leftrightarrow \underline{y} = QSP^{-1}\underline{x}$ for some $\underline{x} \in R^n$

let $\underline{x}' = P^{-1}\underline{x}$ / let $\underline{x} = P\underline{x}'$ $\quad \Leftrightarrow \underline{y} = QS\underline{x}'$ for some $\underline{x}' \in R^2$

$\Leftrightarrow \underline{y} \in \operatorname{im}(QS)$

Then we claim the composite R-module homom.

$$R^m \xrightarrow{Q} R^m \twoheadrightarrow R^m/\operatorname{im}(QS), \qquad \varphi : R^m \to R^m/\operatorname{im}(QS)$$

is <u>surjective</u> because Q is an isomorphism and $R^m \to R^m/\operatorname{im}QS$ surjects,

and has $\ker\varphi = \operatorname{im}(S)$ because $\varphi(\underline{y}) = 0$

$\Leftrightarrow Q\underline{y} \in \operatorname{im}(QS)$

$\Leftrightarrow Q\underline{y} = QS\underline{x}$ for some $\underline{x} \in R^n$

apply Q^{-1} $\quad \Leftrightarrow \underline{y} = S\underline{x}$ for some $\underline{x} \in R^n$

$\Leftrightarrow \underline{y} \in \operatorname{im}(S)$

Hence $R^m/\operatorname{im}(S) \cong R^m/\underbrace{\operatorname{im}(QS)}_{=\operatorname{im}(A)}$

and $R^m/\operatorname{im}(S) = R\times\cdots\times R \Big/ R\begin{bmatrix} d_1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} + R\begin{bmatrix} 0 \\ d_2 \\ 0 \\ \vdots \\ 0 \end{bmatrix} + \cdots + R\begin{bmatrix} 0 \\ \vdots \\ 0 \\ d_r \\ 0 \\ \vdots \\ 0 \end{bmatrix}$

$$\cong R/(d_1) \times \cdots \times R/(d_r) \times \underbrace{R\times\cdots\times R}_{m-r} \qquad \blacksquare$$

(118) To show PID's R have all fin. gen'd modules $M = R^m/\text{im}A$, need a key idea of Noether.

DEF'N/PROPOSITION: The following are equivalent for an R-module M, and define M being a Noetherian R-module:

(i) $\nexists$ R-submodules $\overbrace{M_1 \subsetneq M_2 \subsetneq \cdots\cdots}^{\infty \text{ sequence}} (\subset M)$
(the ascending chain condition or ACC on submodules)

(ii) every R-submodule $N \subseteq M$ is finitely generated.

proof: (i)⇒(ii): Assuming the ACC, if $N \subseteq M$ is a submodule, either $N = \{0\}$ and we're done since $N = \text{span}_R(\emptyset)$, or $\exists\, n_1 \neq 0$ in N and maybe we're done with $N = \text{span}_R(\{n_1\}) = Rn_1$ or $\exists\, n_2 \in N - Rn_1$ and maybe we're done with $N = \text{span}_R(\{n_1, n_2\}) = Rn_1 + Rn_2$

⋮

This must terminate, else $Rn_1 \subsetneq Rn_1 + Rn_2 \subsetneq \cdots\cdots$ is an infinite ascending chain of submodules.
(with $N = Rn_1 + Rn_2 + \cdots + Rn_t$)

5/5/2019 > (ii)⇒(i): Assuming (ii), given an ascending chain

$$M_1 \subseteq M_2 \subseteq \cdots\cdots \subset M,$$

let $N := \bigcup_{i=1}^{\infty} M_i$, and check that is an R-submodule (easy)
so finitely generated by (ii) as $N = Rn_1 + \cdots + Rn_t$

and each $n_i \in M_{f(i)}$ for $i = 1, 2, \ldots, t$,

so $N \subseteq M_{i_0}$ where $i_0 = \max\{f(1), f(2), \ldots, f(t)\}$

and $M_{i_0} = M_{i_0+1} = \cdots\cdots$ ■

How to use this?

DEF'N: A ring R is a Noetherian ring if it is Noetherian as an R-module, i.e. (i) $\nexists$ ideals $I_1 \subsetneq I_2 \subsetneq \cdots\cdots \subset R$
or equivalently (ii) every ideal $I \subset R$ is fin. gen'd, i.e. $I = Rr_1 + \cdots + Rr_t = (r_1, \ldots, r_t)$ for some $r_1, \ldots, r_t \in R$