4.6 Smith Normal Form

Definition: Two $m \times n$ matrices A, B are *equivalent* if there exist $m \times m$ invertible matrix P and $n \times n$ invertible matrix Q such that $B = PAQ$, where matrices are over D.

Four ways to obtain equivalent matrices.

Type 1:

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} c & d \\ a & b \end{bmatrix}$$

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} b & a \\ d & c \end{bmatrix}$$

and $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = I.$

Type 2:

$$\begin{bmatrix} \alpha & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} \alpha a & \alpha b \\ c & d \end{bmatrix}$$

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} \alpha & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} a\alpha & b \\ c\alpha & d \end{bmatrix}$$

$\begin{bmatrix} \alpha & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} \alpha^{-1} & 0 \\ 0 & 1 \end{bmatrix} = I$, where $\alpha \in D$ is a unit.

Type 3:

$$\begin{bmatrix} 1 & \beta \\ 0 & 1 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} \alpha + \beta c & b + \beta d \\ c & d \end{bmatrix}$$

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 1 & \beta \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} a & a\beta + b \\ c & c\beta + d \end{bmatrix}$$

$\begin{bmatrix} 1 & \beta \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & -\beta \\ 0 & 1 \end{bmatrix} = I$, where $\beta \in D$.

Extra type :

Suppose $g.c.d(a, b) = e$. Then $ax + by = e$ for some x, $y \in D$.

Note $g.c.d(x, y) = 1$. Then $ux + vy = 1$ for u, $v \in D$.

Hence $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} x & v \\ y & -u \end{bmatrix} = \begin{bmatrix} e & av - bu \\ cx + dy & cv - du \end{bmatrix}$ and $\begin{bmatrix} x & v \\ y & -u \end{bmatrix} \begin{bmatrix} u & v \\ y & -x \end{bmatrix} = I.$

Similar for left multiplication.

Theorem (Smith Normal Form):

Any matrix over D is equivalent to $diag(d_1, d_2, \ldots, d_r, 0, \ldots, 0) = \begin{pmatrix} d_1 & & & & & & 0 \\ & d_2 & & & & & \\ & & \ddots & & & & \\ & & & d_r & & & \\ & & & & 0 & & \\ & & & & & \ddots & \\ 0 & & & & & & 0 \end{pmatrix}$,

where $d_i \mid d_i + 1$ for $1 \leq i \leq r-1$.

Proof. Let $A = (a_{ij})$ be a matrix. Let $l(a_{ij})$ be the number of primes (count repeatedly) in the unique factorization of a_{ij}.

(a) By type 1 operation, we can assume $l(a_{11}) \leq l(a_{ij})$.

(b) By extra type repeatedly, we can assume $a_{11} \mid a_{1i}$ and $a_{11} \mid a_{k1}$.

(c) By type 2, we can assume $a_{1i} = 0 = a_{k1}$ for $i,k \neq 1$.

(d) For each a_{ij}, we can use type 2 and extra type to have $a_{11} \mid a_{ij}$.

(e) Go back to step (a) until $a_{1i} = 0 = a_{k1}$ for $i,k \neq 1$ and $a_{11} \mid a_{ij}$.

(f) Go to step (a) doing the submatrix without lst row and 1st column.

□

Comments about the proof of SNF Theorem.

1. D is ED $\Rightarrow$ there exists $\delta : D - \{0\} \longrightarrow \mathbb{N}$ such that for any a, $0 \neq b$ in D, there exists $x \in D$ with $a = bx + r$, where $r = 0$ or $\delta(r) \leq \delta(b)$.
2. If we assume D is ED, we can use $l = \delta$ in the proof and find that the extra type is not necessary.