Proof of Smith Normal Form Theorem

Jiang-Hua Lu

The University of Hong Kong

Algebra II, HKU

Monday Feb 17, 2025

In this file:

- Proof of Smith Normal Form Theorem.

Idea:

- Perform row or column operations to diagonalize a matrix $A \in M_{m,n}$.
- Row operations $\Leftrightarrow$ changing A to PA for some $P \in GL(m, R)$;
- Column operations $\Leftrightarrow$ changing A to AQ for some $Q \in GL(n, R)$.

Recall Smith Normal Form Theorem (SNF).

Theorem

Let R be a PID. Let $A \in M_{m,n}(R)$ be non-zero.

1. *There exist $P \in GL(m, R)$ and $Q \in GL(n, R)$, an integer $1 \leq s \leq n$, and $d_1, \ldots, d_s \in R \setminus \{0\}$ with $d_1 | d_2 | \cdots | d_s$, such that*

$$PAQ = \mathrm{diag}(d_1, d_2, \ldots, d_s, 0, \ldots, 0).$$

2. *The integer s is unique and the elements $d_1, \ldots, d_s$ of R are unique up to associates: $s = \max\{1 \leq k \leq n : I_k(A) \neq \emptyset\}$, and*

$$d_k = m_k(A)/m_{k-1}(A), \quad 1 \leq k \leq s,$$

where $I_k(A)$ is the ideal generated by all $k \times k$ minors of A, and

$$\boxed{m_k(A) = \text{a generator of } I_k(A).}$$

We have proved the second part of the SNF Theorem.

Row operations.

- Type I. Replace Row_i by $\mathrm{Row}_i + \alpha \mathrm{Row}_j$, $\alpha \in R$;
- Type II. Replace some Row_i by $u\mathrm{Row}_i$, where u is a unit in R;
- Type III. Interchange two rows;

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 3 \\ 7 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

Type IV. (PID assumption on R needed!.)

- Assume that $\alpha \in R \backslash \{0\}$, $\beta \in R$, and $\alpha \nmid \beta$.

$-2 \times 3 + 7 = 1$

$$\begin{pmatrix} -2 & 1 \\ -7 & 3 \end{pmatrix}\begin{pmatrix} 3 \\ 7 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

- Let $\delta = \gcd(\alpha, \beta)$.
- As R is a PID, there exist $s, t \in R$ such that $\delta = s\alpha + t\beta$. Then

$$\det \begin{pmatrix} s & t \\ -\beta/\delta & \alpha/\delta \end{pmatrix} = 1 \quad \text{and} \quad \begin{pmatrix} s & t \\ -\beta/\delta & \alpha/\delta \end{pmatrix} \underline{\begin{pmatrix} \alpha \\ \beta \end{pmatrix}} = \begin{pmatrix} \delta \\ 0 \end{pmatrix}.$$

- Performing this operation to the i'th and the j'th entries in a given column replaces the original entries α and β respectively by δ and 0.

Similar four types of column operations.

Definition. Say $A, B \in M_{m,n}(R)$ are equivalent if there is a sequence of row or column operations of the above four types that starts with A and ends with B.

Restatement of first part of Smith Normal Form Theorem: Every non-zero $A \in M_{m,n}(R)$ is equivalent to a

$$\mathrm{diag}(d_1, \ldots, d_s, 0, \ldots, 0),$$

where $d_i \neq 0$ for every $1 \leq i \leq s$ and $d_1 | d_2 | \cdots | d_s$.

A tool:

- Recall for $a \in R \backslash \{0\}$, length $l(a)$ is the number of prime factors (counting multiplicity) in the prime decomposition of a.
- For $a, b \in R \backslash \{0\}$, we say that a is smaller than b if $l(a) < l(b)$.

Properties: for $a, b \in R \backslash \{0\}$,

1. $l(ab) \geq \max(l(a), l(b))$;
2. $l(a) = l(b)$ if a and b are associates;
3. If $l(a) \leq l(b)$ and a does not divide b, then any greatest common divisor c of a and b satisfies $l(c) < l(a)$.

Lemma 0. Suppose that A has a nonzero $(1,1)$-entry α.

1. If there is an element β in the first row or column of A such that $\alpha \nmid \beta$, then A is equivalent to a matrix with smaller $(1,1)$-entry.
2. If α divides all entries in the first row and column, then A is equivalent to a matrix with $(1,1)$-entry equal to α and all other entries in the first row and column equal to zero.

Main step in proving the Smith Normal Form Theorem.

Lemma. For any non-zero $A \in M_{m,n}(R)$, there exists $B \in M_{m,n}(R)$ which is equivalent to A and is of the form

$$B = \begin{pmatrix} d_1 & 0 \\ 0 & C \end{pmatrix},$$

where $d_1 \in R \backslash \{0\}$, $C \in M_{m-1,n-1}(R)$, and d_1 divides all the ~~non-zero~~ entries of C.

Outline of proof.

- Let $\mathcal{A}$ be the set of all matrices in $M_{m,n}(R)$ equivalent to A. Let

$$E = \{e \in R : e \text{ is a non-zero entry of some } A' \text{ in } \mathcal{A}\}.$$

- Then there exists $d_1 \in E$ such that $l(d_1) = \min\{l(e) : e \in E\}$.
- Let $A' \in \mathcal{A}$ be such that d_1 is an entry of A'.

Proof cont'd:

- Switching the rows and columns of A' if necessary, may assume that d_1 is the $(1,1)$-entry of A'.
- By 1) of Lemma 0, d_1 divides entries of the first row and the first column of A';
- By 2) of Lemma 0, can find $B = \begin{pmatrix} d_1 & 0 \\ 0 & C \end{pmatrix}$;
- d_1 must divide every non-zero entry of C: otherwise get $B' \in \mathcal{A}$ whose $(1,1)$-entry is smaller than d_1, contradiction.

Q.E.D.

Proof of Smith Normal Form Theorem. Induction on $m+n$:

- If $m+n=2$, i.e., $m=n=1$, nothing to prove.
- Assume $m+n>2$. Then there exist $P_1 \in GL(m,R)$, $Q_1 \in GL(n,R)$ and $C \in M_{m-1,n-1}$ such that

$$P_1 A Q_1 = \begin{pmatrix} d_1 & 0 \\ 0 & C \end{pmatrix}.$$

- If $C=0$, or if $m=1$ or $n=1$, done.
- Assume $C \neq 0$ and $m \geq 2$ and $n \geq 2$.
- By induction assumption, there exist an integer $2 \leq s \leq \min(m,n)$, elements $d_2,\ldots,d_s \in R\backslash\{0\}$ with $d_2|\cdots|d_s$, and matrices $P_2 \in GL(m-1,R), Q_2 \in GL(n-1,R)$ such that

$$P_2 C Q_2 = \mathrm{diag}(d_2,\ldots,d_s,0,\ldots,0).$$

Proof of Smith Normal Form Theorem, cont'd:

- As d_1 divides every entry of C, have $d_1 | d_2 | \cdots | d_s$.
- Let
$$P = \begin{pmatrix} 1 & 0 \\ 0 & P_2 \end{pmatrix} P_1 \quad \text{and} \quad Q = Q_1 \begin{pmatrix} 1 & 0 \\ 0 & Q_2 \end{pmatrix}.$$
- Then $P \in GL(m, R), Q \in GL(n, R)$ and $PAQ = \mathrm{diag}(d_1, \ldots, d_s, 0, \ldots, 0)$ as desired.

Q.E.D.