Computing Smith Normal Form

Jiang-Hua Lu

The University of Hong Kong

Algebra II, HKU

Monday Feb 17, 2025

In this file:

- §2.1.1. Cauchy-Binet Formula;
- §2.1.2: Statement of Smith Normal Form Theorem.

Definitions. Let R be any commutative ring, and $m, n \geq 1$ integers.

- $M_{m,n}(R)$ is the set of all $m \times n$ matrices with entries in R.
- $M_{n,n}(R)$ is a ring with matrix addition and multiplication.

$$\begin{pmatrix} A & I \\ 0 & B \end{pmatrix}$$

- For $A = (a_{i,j}) \in M_{n,n}(R)$,
$$\det(A) = \sum_{\sigma \in S_n} \operatorname{sign}(\sigma) a_{1,\sigma(1)} a_{2,\sigma(2)} \cdots a_{n,\sigma(n)} \in R.$$
- $\det(AB) = \det(A)\det(B)$ for any $A, B \in M_{n,n}(R)$.

Notation. For any commutative ring R and any $A \in M_{m,n}(R)$ and

$$I \subset \{1, \dots, m\}, \qquad J \subset \{1, \dots, n\}, \qquad |I| = |J| = k,$$

- let $[A]_{I,J}$ be determinant of the sub-matrix of A formed by the rows from I and columns from J;
- call $[A]_{I,J}$ a $(k \times k)$-minor of A.

Lemma. Cauchy-Binet formula. For $A \in M_{m,n}(R), B \in M_{n,p}(R)$, and $I \subset \{1, \dots, m\}$ and $J \subset \{1, \dots, p\}$ with $|I| = |J| = k$, one has

$$[AB]_{I,J} = \sum_{K \subset \{1,\dots,n\}, |K|=k} [A]_{I,K}[B]_{K,J}. \tag{1}$$

Proof. Assume R is an integral domain and let $F = \mathrm{Frac}(R)$. Have

$$A: \ \wedge^k F^n \longrightarrow \wedge^k F^m, \qquad B: \ \wedge^k F^p \longrightarrow \wedge^k F^n.$$

Continue in tutorial

Notation: Let R be any commutative ring. $AB = I \Rightarrow \det A \det B = 1$

- $A \in M_{n,n}(R)$ has an inverse if and only if $\det(A) \in R$ is a unit:

$$AA^{\text{co}-\text{factor}} = A^{\text{co}-\text{factor}}A = \det(A)I_n.$$

- $GL(n, R) := \{A \in M_{n,n}(R) : \det(A) \text{ is a unit in } R\}$ is a group.
  $GL(n, \mathbb{Z}) = \{A \in M_{n,n}(\mathbb{Z}) ; \det A = \pm 1\}$
- For $1 \le s \le \min(m, n)$ and $d_1, \dots, d_s \in R$, have

$$\operatorname{diag}(d_1, d_2, \dots, d_s, 0, \dots, 0) = \begin{pmatrix} d_1 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & d_2 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots & \vdots & \vdots & 0 \\ 0 & 0 & \cdots & d_s & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots & \vdots & \vdots & 0 \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \end{pmatrix},$$

diagonal matrix of size $m \times n$.

SNF Thm:

$$A \in M_{m\times n}(R)$$

$$BAB^{-1}$$

PID

$$P A_{m\times n} Q$$

$GL(m, R)$ $\qquad$ $GL(n, R)$

Smith Normal Form Theorem (SNF Theorem).

Theorem

Let R be a PID. For any $A \in M_{m,n}(R)$, there exist $P \in GL(m, R)$ and $Q \in GL(n, R)$, an integer $1 \leq s \leq \min(m, n)$, and $d_1, \ldots, d_s \in R \backslash \{0\}$ with $d_1 | d_2 | \cdots | d_s$, such that

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

Moreover, the integer s is unique and the elements $d_1, \ldots, d_s$ of R are unique up to up to associates.

$r(A)$

- The integer s is called the rank of A and denoted as $s(A)$;
- the non-zero $d_1, \ldots, d_s \in R$ are called the invariant factors of A.
- $\mathrm{diag}(d_1, d_2, \ldots, d_s, 0, \ldots, 0)$ is called the Smith normal form of A.

Notation. For $A \in M_{m,n}(R)$ and an integer $1 \leq k \leq \min(m,n)$,

1. Let $I_k(A)$ be the ideal generated by all $(k \times k)$-minors of A;
2. Let $m_k(A)$ be a generator of $I_k(A)$. Let $m_0(A) = 1$.
3. When $I_k(A) \neq 0$, $m_k(A)$ is a gcd of all non-zero $k \times k$ minors of A.
4. Let $s(A) = \max\{1 \leq k \leq \min(m,n) : I_k(A) \neq 0\}$.

Lemma: Let R be a PID. For any $A \in M_{m,n}(R)$, $P \in GL(m,R)$, $Q \in GL(n,R)$, and $1 \leq k \leq \min(m,n)$, one has

$$s(PAQ) = s(A) \quad \text{and} \quad I_k(PAQ) = I_k(A).$$

Proof. Let $1 \leq k \leq \min(m,n)$. By Cauchy-Binet,

$$I_k(PA) \subset I_k(A), \qquad I_k(A) = I_k(P^{-1}PA) \subset I_k(PA),$$

so $I_k(PA) = I_k(A)$. Similarly, $I_k(AQ) = I_k(A)$.

Q.E.D.

Proposition

Let R be a PID. If $A \in M_{m,n}(R)$ is non-zero, and if $P \in GL(m,R)$ and $Q \in GL(n,R)$, integer $1 \le s \le \min(m,n)$, and elements $d_1, \dots, d_s \in R \backslash \{0\}$ are such that $d_1 | d_2 | \cdots | d_s$ and

$$PAQ = \mathrm{diag}(d_1, \dots, d_s, 0, \dots, 0),$$

then $s = \max\{1 \le k \le \min(m,n) : I_k(A) \neq 0\}$, and

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

where $u_1, \dots, u_s$ can be any units of R.

Proof. For $1 \le k \le \min(m,n)$, $I_k(A) = I_k(PAD)$, so

$$s = \max\{1 \le k \le \min(m,n) : I_k (A) \neq 0\}$$

and $m_k(A) = m_k(PAQ) = d_1 \cdots d_k$ for $1 \le k \le s$.

$m_k = d_1 \cdots d_{k-1} \Rightarrow d_k = \dfrac{m_k}{m_{k-1}}$ **Q.E.D.**

Example. $R=\mathbb{Z}$ $A=\begin{pmatrix}4&&&\\&2&&\\&&6&\\&&&3\end{pmatrix}$

$$A = \mathrm{diag}(4,2,6,3) = P^{-1}\underline{\mathrm{diag}(1,2,6,12)}Q^{-1} \in M_{4,4}(\mathbb{Z})$$

for some $P, Q \in GL(4,\mathbb{Z})$.

$$PAQ=\begin{pmatrix}1&&&\\&2&&\\&&6&\\&&&12\end{pmatrix}$$

$m_1 = \gcd(4,2,6,3) = 1$

$m_2 = \gcd(\_\ \_\ \_) = 2$

$m_3 = \gcd(\underline{4\times2\times6,\ 4\times2\times3,\ 2\times6\times3},\ 4\times6\times3) = 12$

$m_4 = \det = 4\times2\times6\times3$

$d_1 = m_1/m_0 = 1$ $d_2 = m_2/m_1 = 2$, $d_3 = m_3/m_2 = 6$, $d_4 = \frac{m_4}{m_3} = 12$

Example.

$$A = \mathrm{diag}(4,2,6,3) = P^{-1}\mathrm{diag}(1,2,6,12)Q^{-1} \in M_{4,4}(\mathbb{Z})$$

for some $P, Q \in GL(4,\mathbb{Z})$.

$$A = \begin{pmatrix} x-1 & x+2 & 1 \\ 4 & x^2-1 & x^3+3 \\ 1 & x & x-1 \end{pmatrix} \qquad R = \mathbb{Q}[x]$$

$-x^2+4x+1$

$x^2-2x = x(x-2)$

$m_1 = 1 \qquad m_2 = 1 \qquad m_3 = \det$

$$\begin{pmatrix} 1 & & \\ & 1 & \\ & & \det \end{pmatrix}$$