Uniqueness of Smith Normal Form

Let R be a commutative ring. Then the *determinant* $\det : \mathbb{M}_n(R) \to R$ is a map that has the following properties:

(1) det is *n-multilinear* (or *n-linear* as a function of the rows (respectively, columns) of matrices in $\mathbb{M}_n(R)$. This means that it is R-linear (i.e., an R-homomorphism) in each of the n entries fixing the others, i.e.,

$$\det(\alpha_1, \ldots, r\alpha_i + \alpha_i', \ldots, \alpha_n) \\ = r\det(\alpha_1, \ldots, \alpha_i, \ldots, \alpha_n) + \det(\alpha_1, \ldots, \alpha_i', \ldots, \alpha_n)$$

for all r in R, and rows (respectively columns) of matrices A in $\mathbb{M}_n(R)$.

(2) det is *alternating* as a function of the rows (respectively, columns) of matrices in $\mathbb{M}_n(R)$, i.e., if A has two identical rows (respectively, columns), then $\det A = 0$.

[Note: This implies that the matrix obtained by interchanging two rows (respectively columns) of A has determinant $-\det A$.

(3) $\det I = 1$

Indeed it can be shown that $\det : \mathbb{M}_n(R) \to R$ is the unique function satisfying (1), (2), and (3); and it is given by

$$\det(a_{ij}) = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) a_{1\sigma(1)} \cdots a_{n\sigma(n)}$$

Here the sum is computed over all permutations σ of the ordered set of integers $\{1, 2, \ldots, n\}$. A *permutation* is a bijection of this ordered set, so the value in the ith position after the reordering σ is denoted by $\sigma(i)$. For example, for $n = 3$, the original ordered sequence $\{1, 2, 3\}$ might be reordered by σ to $\{2, 3, 1\}$, where $\sigma(1) = 2$, $\sigma(2) = 3$, and $\sigma(3) = 1$. The set of all such permutations (also known as the *symmetric group* on n elements) is denoted by S_n. We define the *sign function* $\operatorname{sgn} : S_n \to \{\pm 1\}$ by $\operatorname{sgn}(\sigma)$ is $+1$ whenever the reordering given by σ can be achieved by successively interchanging two entries an even number of times, and -1 otherwise. It can be shown that $\operatorname{sgn}(\sigma)$ is independent of how this achieved, i.e., the parity of the number of interchanges to reorder $\{1, \ldots, n\}$ by σ is invariant.

Let A be an $m \times n$ matrix in $R^{m \times n}$ and $1 \leq l \leq \min\{m, n\}$. An *$l$-order minor* of A is a determinant of an $l \times l$ submatrix of A, i.e., a matrix obtained from A be deleting $m - l$ rows and $n - l$ columns of A. The key to proving our uniqueness statement is the following lemma:

Lemma 1. *Suppose that F be a field and A an $m \times n$ matrix in $F[t]^{m \times n}$. Let P and Q be invertible matrices in $\mathrm{GL}_m(F[t])$ and $\mathrm{GL}_n(F[t])$ respectively. Set $B = PAQ$. If $1 \leq l \leq \min\{m, n\}$ and*

(1) if the element a in $F[t]$ is a gcd of all the l-order minors of A, and

(2) if the element b in $F[t]$ a gcd of all the l-order minors of B,

then $a = b$.

Proof. Let $P = (p_{ij})$, $A = (a_{ij})$, $Q = (q_{ij})$ and c in $F[t]$ a gcd of all the l-order minors of PA. Then the kith entry of PA is $\sum_j p_{kj} a_{ji}$, so the kth row of PA is $\sum_j p_{kj}(a_{j1}\, a_{j2} \cdots a_{jn})$ (with the obvious notation). As the determinant is multilinear as a function of the rows, we have $a \mid c$ in $F[t]$. As the determinant is multilinear as a function of the columns, an analogous argument shows that $c \mid b$ in $F[t]$, hence $a \mid b$ in $F[t]$. But we also have $A = P^{-1}BQ^{-1}$, so arguing in the same way, we conclude that we also have $b \mid a$. As both are gcd's $a = b$. □

Corollary 2. *Let A be an $m \times n$ matrix in $F[t]^{m\times n}$ with B a diagonal matrix, write $B = \mathrm{diag}(d_1, \ldots, d_r, 0 \ldots, 0)$ in $F[t]^{m\times n}$, where $d_1, \ldots d_r, 0, \ldots$ are the diagonal entries, satisfying $d_1 \mid \cdots \mid d_r$ and $d_r \neq 0$ in $F[t]$ a Smith Normal Form of A. Let*

$$\Delta_l \text{ be a gcd of all the } l\text{-order minors of } A \text{ in } F[t] \text{ for } 1 \leq l \leq r$$

and $\Delta_0 = 1$. Then

$$\Delta_0 \mid \Delta_1 \mid \cdots \mid \Delta_r \quad \text{and} \quad d_l = \frac{\Delta_l}{\Delta_{l-1}} \text{ in } F[t] \text{ for all } l > 0.$$

Putting this all together, we obtain the following theorem:

Theorem 3. *Let A be an $m \times n$ matrix in $F[t]^{m\times n}$. Then A is equivalent to a matrix in Smith Normal Form. Moreover, if $\mathrm{diag}(a_1, \ldots, a_r, 0, \ldots, 0)$ and $\mathrm{diag}(b_1, \ldots, b_s, 0, \ldots, 0)$ are two Smith Normal Forms for A, then $r = s$ and $a_i = b_i$ for $1 \leq i \leq r$. In particular, the sequence of monic polynomials in $F[t]$*

$$a_1 \mid a_2 \mid \cdots \mid a_r$$

completely determine a Smith Normal Form of A with $a_l = \Delta_l/\Delta_{l-1}$ where Δ_l is a gcd of all the l-order minors of A in $F[t]$ for $1 \leq l \leq r$ and $\Delta_0 = 1$.

The elements $a_1 \mid \cdots \mid a_r$ in the theorem are called the *invariants factors* of A.