Beginning of Oct. 3, 2022

Smith Normal Form

Theorem

If $A \in M_{m\times n}(F[x])$, then there exists invertible U, V matrices over $F[x]$ with UAV = block diagonal $g_1, \ldots, g_t, 0, \ldots$ where $g_1(x) \neq 0$ and $g_1 \mid g_2 \mid \ldots \mid g_t$.

Proof. We induct on $m+n$. Base case $m = n = 1$ trivial. Let $A = [a_{i,j}(x)]$ with entry polynomials. If $A = 0$ there is nothing to prove.

Let $h(x) = \gcd(a_{i,j}(x))$ over all i, j. This is nonzero by assumption. We component-wise divide A by h. Then the gcd of all entries is 1.

Among all matrices B with $B \sim A$ (by UAV), choose one with $b_{11} \neq 0$ of smallest possible degree (exists because A is nonzero and we can exchange rows and also columns).

Claim: b_{11} divides everything in the first row, i.e. $b_{11} \mid b_{1,j}$. If not, $b_{i,j} = qb_{11} + r$ where $\deg r(x) \leqslant \deg b_{11}(x)$. Multiplying the first column by $-q$ and adding it to the j^{th} column, we obtain the j^{th} column with row 1 entry $b_{i,j} - qb_{11} = r(x)$. After swapping columns we obtain a new matrix with even smaller $1, 1$ entry.

Since b_{11} divides $b_{12}, \ldots$, we can add a multiple of the first column to the remaining columns so that the first row becomes $b_{11}, 0, 0, \ldots$. Similarly for the first column. Then we have

$$B = \begin{bmatrix} b_{11} & 0 \\ 0 & C \end{bmatrix}.$$

Claim: b_{11} divides everything in C. For any entry not divisible by b_{11}, we can apply the same argument by adding multiples to the first row (first column is 0 except b_{11} so it remains unaffected) and obtain a contradiction.

We assume the fact that equivalent matrices have the same entry-wise gcd. Therefore b_{11} is the gcd of all entries, so it is constant. By induction, C is equivalent to diagonal $g_2, \ldots, g_r, 0, \ldots$ where $g_2 \mid \ldots \mid g_r$. Then we are done since $g_1(x) := b_{11} \mid g_2(x)$. □

Remark. Here $r = \text{rank}(A)$. $g_1(x)$ is the component-wise gcd of all entries of B. $g_1 g_2$ is the gcd of all determinents of 2×2 minors of B, namely $g_i g_j$ for $i \neq j$. Similarly, $g_1 g_2 \ldots g_\ell$ is the gcd of all $\ell \times \ell$ minor determinents of B.

Lemma

Let $A, B \in M_{m\times n}(R)$ where R is commutative. Let $B = SA$ or AT where S, T are squares. Then any entry of B is a linear combination of entries of A. In particular, the gcd of entries of B is a multiple of gcd of entries of A.

In particular, if S is invertible, we see the gcd of entries of B must equal to that of A, since $A = S^{-1}B$.