Equivalence of Matrices in a Principal Ideal Domain

Math 520B Handout: November 11, 2005

Let R denote a given principal ideal domain.

Definition. Two $m \times n$ matrices A, B in R will be called *equivalent* if there exist matrices $U \in \mathrm{GL}_m(R)$ and $V \in \mathrm{GL}_n(R)$ such $B = UAV$. To indicate that A and B are equivalent one may write $A \sim B$.

Observe that the ideal in R generated by the entries of A and the ideal generated by the entries of B are the same when A and B are equivalent. Since R is a principal ideal domain, it follows that the entries of A and the entries of B share the same greatest common divisors inasmuch as these greatest common divisors serve as single generators for these ideals.

By *rank* of a matrix A in R one understands the rank of A when it is regarded as a matrix in the fraction field of R.

Lemma 1. *If a and b are non-zero entries sharing either a row or a column in an $m \times n$ matrix over R, then there is an equivalent matrix having a greatest common divisor of a and b as entries.*

Proof. The case where they share a row is the transpose of the case where they share a column. If they share a column one may narrow the scope to that column and the two rows that are involved, i.e., it is essentially a question about the case $m = 2, n = 1$. If $Ra + Rb = Rd$, then one may choose $e, f \in R$ such that $ea + fb = d$. If $a' = a/d$ and $b' = b/d$, then

$$\begin{pmatrix} e & f \\ -b' & a' \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} d \\ 0 \end{pmatrix} .$$

Theorem 1. *Every $m \times n$ matrix in R of rank r is equivalent to a matrix C for which $C_{ii} = c_i$ for $1 \le i \le r$ and $C_{ij} = 0$ for all other pairs (i, j) where the non-zero entries c_i are successively divisible, i.e., $c_i | c_{i+1}$ for $1 \le i \le r-1$.*

Proof. Let $k = \max(m, n)$. Use induction on k. The result is trivially true if $k = 1$ or if the given matrix $A = 0$. Assume $k > 1$. Among the non-zero entries in all of the matrices equivalent to A there is an entry in one of those matrices having the minimum number of prime factors occuring among those entries. Let m be an entry having the said minimum number of prime factors, and replace A, if necessary, by an equivalent matrix in which m is an entry. Since any entry may be moved to position $(1, 1)$ using row and column operations, replacing A again, if necessary, by an equivalent matrix, one may assume that m is the $(1, 1)$ entry of A. By the lemma, in view of the choice of m, m must divide all entries in the first row and the first column of A. For each entry in the first column of A other than the m in position $(1, 1)$, performing an elementary row operation on A, hence replacing A by an equivalent matrix, will zero that entry. Likewise elementary column operations will zero entries in the first row of A beyond the $(1, 1)$ position. Thus, one may assume that the m in position $(1, 1)$ is the only non-zero entry in either the first row or the first column of A. By the inductive hypothesis the $(m - 1) \times (n - 1)$ matrix A_1 formed by deleting the first row and the first column of A satisfies $U_1 A_1 V_1 = C_1$ where the only non-zero entries in C_1 are successively divisible elements $c_2, \ldots, c_r$ in positions $(1, 1), \ldots (r - 1, r - 1)$ of C_1. Taking

$$U = \begin{pmatrix} 1 & 0 \\ 0 & U_1 \end{pmatrix} \quad \text{and} \quad V = \begin{pmatrix} 1 & 0 \\ 0 & V_1 \end{pmatrix}$$

one obtains

$$UAV = C$$

with the only non-zero entries being $C_{11} = m$, $C_{22} = c_2$, $\ldots$, $C_{rr} = c_r$. There is still, however, the question of whether m divides c_2. Let d be a greatest common divisor of m and c_2, and let $em + fc_2 = d$. Replacing the first row of C with the sum of itself and the second row multiplied by f and then replacing the second column of that by the sum of itself and the first column multiplied by e yields a matrix equivalent to C, hence equivalent to A, having the entry $d = em + fc_2$. Since d divides m but, in view of the choice of m, has no fewer prime factors than m, one sees that m is the product of a unit in R with d. Therefore, m divides c_2 since d divides c_2.