A SPECIAL CLASS OF MATRICES

K. ROGERS AND E. G. STRAUS

1. Introduction. Let D be an integral domain, K its quotient field, D^n the set of all n-by-1 matrices over D, and A an n-by-n matrix over a field containing K. We say that A has *property* P_D if and only if, for all nonzero u in D^n, the vector Au has at least one component in $D^* = D - \{0\}$. The setting in which this property arose is detailed in [**1**], where we investigated the case where D was either Z, the rational integers, or the ring of integers of an algebraic number field of class-number one. Now, if P is a permutation matrix, T is lower triangular with only ones in the diagonal, and N is nonsingular and over D, then $A = PTN$ has property P_D. It was shown in [**1**] that for $D = Z$ there are matrices not of the form PTN which have property P_D; but, at least in the case of the ring of integers of an algebraic number field of class-number one, we found the necessary but far from sufficient condition, that $\det A$ be in D^*. Our present purpose is to extend this to all algebraic number fields and also to prove necessary and sufficient conditions for property P_D in certain cases.

THEOREM I. *Let D be a domain whose quotient field K is algebraic over its prime field. Let A be an n-by-n matrix, where $n \leqq \#(K)$.*[1] *Then:*

(i) *If K is of prime characteristic, then A has property P_D if and only if $A = PTN$, where P, T and N are as above:*

(ii) *If D is Dedekind and K is a finite algebraic extension of the rationals, then for A to have P_D we must have $\det A \in D^*$.*

THEOREM II. *If $D = D_1[t]$, where t is transcendental over D_1, if $\#(D_1) > n$, and if A has P_D, then the rows of A can be so ordered that the matrices A_r of the first r rows of A have all r-by-r minors in D and not all zero, for $r = 1, 2, \cdots, n$. In particular, the first row is over D, and $\det A \in D^*$.*

If in addition we have only principal ideals, then we can reduce all but one element of the first row to zero and prove by induction:

COROLLARY. *If $D = F[t]$, where $\#(F) > n$, so K is a simple transcendental extension, then A has P_D if and only if $A = PTN$, where P, T and N are as above.*

Received August 11, 1961.

[1] $\#(K)$ = cardinality of K.

We can improve Theorem II to an if and only if statement, as long as $D_1[t]$ is a Gaussian domain.

THEOREM III. *If* $D = F[t_1, t_2 \cdots, t_k]$, *where the* t_i *are algebraically independent over the field* F, *and* $\sharp(F) > n$, *then a matrix* A *has* P_D *if and only if* $A = PLV$, *where* P *is a permutation matrix*, L *is a diagonal matrix over* D^*, *while* V *is nonsingular and such that for* $r = 1, 2, \cdots, n$, *the first* r *rows of* V *have their* r*-by-*r *minors in* D *and without common divisor.*

2. We try to reduce down to the case that A is over K.

LEMMA. I. *Let* B *be an* r*-by-*n *matrix over a field containing* K, *where* $\sharp(K) \geqq n \geqq r$, *and assume that there is a subspace* V *of* K^n *of dimension* r *such that, for all nonzero* $\underline{u}$ *in* V, $B\underline{u}$ *has a component in* K^*. *Then* $B = PTB_1$, *where* P *is a permutation matrix*, T *is triangular with only ones on the diagonal, and* B_1 *is* r*-by-*n *and such that, for all* u *in* V, *the product* B_1u *has all its components in* K *and is* 0 *only when* $u = 0$.

Proof. Let L_i note the subspace of V consisting of those u in V such that the ith component of Bu is in K. Then the relation between B and V implies that $V = \bigcup' L_i$, the union over those i such that for u in L_i the component $(Bu)_i$ is not always zero. We first show that some $L_i = V$. Assume that to be false: hence V is the union of at most r proper subspaces, say $V = H_1 \cup \cdots \cup H_m, m \leqq r \leqq n, m$ minimal. By choosing u, v so that $u \in H_1$, $v \in H_2 \cup \cdots \cup H_m$, $u \notin H_2 \cdots \cup H_m$, $v \notin H_1$, we ensure that the plane $Ku + Kv$ equals the union of at most m lines through the origin. This is clearly impossible if the field K is infinite. If $\sharp(K) = q$, then we should require that $q^2 \leqq n(q-1)+1$, that is, $q + 1 \leqq m \leqq n$, whereas we assumed that $q \geqq n$. Hence some row of B has all its inner products with V in K and not all zero. Permute the rows so that the first row, R_1^t, has this property. Then the lemma is proved for $r = 1$, and we are ready for induction on r; the matrix C of the last $r-1$ rows of B has the correct inner product property relative to $W = V \cap (KR_1)^\perp$, a space of dimension $r-1$. Hence, $C = T_1C_1$, where T_1 is triangular of order $r-1$ with only ones on the diagonal, while the rows $S_2^t, \cdots, S_r^t$ of C_1 are such that all S_j^tu are in K whenever $u \in W$. Since we have not yet chosen the first column of our final T, we can still modify the S_j by multiples of R: for all a_j in any field containing K, the row $S_j^t - a_jR_1^t$ has the same inner product on W as S_j^t. Let S_1 be a vector in V but not in W, so that R and S_1 are not perpendicular. We can then choose a_j so that $(S_j^t a_jR_1^t)S_1 - 0$, so that the rows $R_j^t = S_j^t - a_jR_1^t$ have all inner products in K with a basis for V over K, hence the same with all vectors in V. The result now follows, with T obtained from T_1 by putting the row $(1, 0, \cdots, 0)$ on top and the column $(1, a_2, \cdots, a_n)^t$ to the left, while B_1 has rows $R_1^t, \cdots, R_r^t$. Finally, if some nonzero u in V were perpendicular to all the R, it would be perpendicular to all the rows of B and thus violate the hypothesis.

COROLLARY 1. *If* $\sharp(K) \geqq n$, *and if* A *has property* P_K, *then* $A = PTA_1$, *where* T *is lower triangular with only ones on the diagonal, while* A_1 *is nonsingular over* K. *As usual,* P *is a permutation matrix.*

Proof. This is the case $r = n$, so $V = K^n$ and the deduction is immediate.

COROLLARY 2. *If* $\sharp(K) \geqq n$, *then* A *has* P_D *implies* $\det A \in K^*$.

3. *Proof of Theorem* I. We note first that, if A has P_D and R is any sub-domain of D, then A has property P relative to the intersection of D with the ring obtained from R by adjoining the elements of A. Hence we can take D to be a sub-domain of a finite extension of the prime field. In case K is purely algebraic, this intersection is a finite algebraic extension of the prime field. However, this procedure may spoil the Dedekind property, so we only use this for *part* (i). There, we are now down to the case where D is a sub-domain of a finite field and therefore is itself a finite field. This part of Theorem I follows now from Corollary 1 above, with $D = K$. For *part* (ii) we proceed as follows. In the preceding section we saw that if A has P_D then $\det A \in K^*$, and now we shall show that $\det A \in D^*$ in the case that D is a Dedekind ring and K is an algebraic number field. The usual case is when D is the ring of integers of K, of course. First, we shall replace A by a matrix over K. Permute the rows so that $A = TA_1$, as in Corollary 1. Now, if $1, \xi_1, \cdots, \xi_N$ is a basis for the K-module obtained by adjoining to K all the elements of T, then $A = (T_1 + \xi_2 T_2 + \cdots + \xi_N T_N)A_1$, where the T_i are over K, are strictly lower triangular for $i \geqq 2$, and T_1 is lower triangular with only ones on the diagonal. The matrix $T_1 A_1$ is over K, has the same determinant as A, and it has P_D. For, by the independence of $1, \xi_2, \cdots, \xi_N$ over K, $(Au)_i \in K$ if and only if $(Au)_i = (T_1 A_1 u)_i \in K$, for $u \in K^n$. So we are down to the case that A is over K. If $\det A$ is not in D, some prime ideal $\mathfrak{P}$ must occur to a negative power in the factorisation of the ideal $(\det A)$. Since every element of D can be expressed as $\pi^\nu u/v$, where $\pi \in \mathfrak{P}$, $\pi \notin \mathfrak{P}^2$, u and v are in D but not in $\mathfrak{P}$, while ν is a rational integer, the ring $D_{\mathfrak{P}} = \{a/b \mid a, b \in D, b \notin \mathfrak{P}\}$ is a discrete valuation ring in which every element is a unit times a power of π the only ideals being $D \supset (\pi) \supset (\pi^2) \supset$ etc. Since it is easily shown that A has property P relative to $D_{\mathfrak{P}}$, we are now down to the

case that D is a discrete valuation ring with prime element π, and $\det A$ is a unit times a negative power of π. By multiplying a row of A by an appropriate element of D^*, we can ensure that $\det A = \pi^{-1}$, if we wish. Things now proceed as in Lemma 3 of [1]. Multiply the ith row of A by π^{d_i}, where the d_i are such that the ensuing matrix is over D. Since D is a principal ideal ring, we can triangularize this new matrix B. It has the property that for all nonzero u in D^n, some component $(B\underline{u})_i$ is a nonzero multiple of π^{d_i}; also, $\det B = \pi^{\Sigma d_i - 1}$. These properties are shown to be contradictory. If the residue class field $D/\mathfrak{P}$ has degree f over $Z/\mathfrak{P} \cap Z = Z/pZ$, it has p^f elements. Then, the mumber of residue classes mod $\mathfrak{P}^a$ is p^{af}. By absorbing unit factors, we can assume that the diagonal elements of B are $\pi^{a_i}, i = 1, \cdots, n$, so that $\Sigma a_i < \Sigma d_i$. We let α_i, δ_i run over complete residue systems mod π^{a_i} and mod π^{d_i}, respectively: then the number of vectors α is $(p^f)^{\Sigma a_i}$ and the number of δ is $(p^f)^{\Sigma d_i}$. Hence there are more δ than α. As in [1], one now shows that for given δ there is one and only one α such that the equation $Bu = \alpha + \delta$ is solvable with u in D^n. Then, we find distinct δ, δ' and some α such that $Bu = \delta + \alpha$ and $Bu' = \delta' + \alpha$, where u and u' are in D^n. Hence, $B(u - u') = \delta - \delta'$, and each component of $\delta - \delta'$ is either zero or indivisible by π^{d_i}. This contradicts the P-property for B and establishes at last that we must have had *det* $A \in D^*$.

4. *The case* $D = D_1[t]$. We saw in Lemma I, Corollary 2, that if A has P_D then we can permute the rows and reduce A to the form TA_1, where T is lower triangular with only ones on the diagonal, while A_1 is nonsingular and over K. We now note that $TA_1 = TEEA_1$, where E is any elementary matrix with $E^2 = I$; hence we can add K-multiples of columns of T to other columns, doing the corresponding row-operation on A_1. Hence, we may assume that the sub-diagonal elements of T are either zero or outside K.

LEMMA II. *If A has P_D, where $D = D_1[t]$, $\sharp(D_1) > n$ and t is transcendental over D_1, then some row of A must have all its elements in D.*

Proof. We have $A = TA_1$, as above. Some rows of T, such as the first, have only one nonzero component, and it is 1. By permutation of the columns of T (and hence of the rows of A_1) and also the rows of T, we can put things in the form:

$$A = \begin{pmatrix} I_s & & & 0 \\ t_{s+1,1} \cdots 1 & & & 0 \\ & & 1 & \\ t_{n1} & & & 1 \end{pmatrix} A_1 \, .$$

Thus, the first s rows of A_1 are also rows of A, and the last $n-s$ rows of T involve elements outside K. We shall show that if none of the first s rows in over D, then we can find a vector $u \in D^n$ such that the first s components of Au are in K but not in D, while the last $n-s$ components are not even in K. In general, if we want an element $\underline{u}$ of K^n to be such that the last $n-s$ components of Au are not in K, we want $b = A_1u$ to be in K^n but such that none of $t_{i1}b_1 + \cdots t_{i,i-1}b_{i-1} + b_1$ is in K, for $s < i \leqq n$. Since the coefficients $t_{i1}, \cdots, t_{i,i-1}$ are not all zero and the nonzero ones are outside K, these conditions amount to making b avoid $n-s$ subspaces of K^n. Thus, $u = A_1^{-1}b$ must avoid at most $n-1$ hyperplanes of K^n. So we are finished as soon as we have found u in D^n such that the first s components of A_1u are outside D, and with u avoiding a given set of hyperplanes. There are two cases, according as the matrix A_s of the first s rows of A has a common denominator out of D_1 or not.

(1) *Case when*

$$A_s = \begin{pmatrix} \dfrac{a_{11}(t)}{d}, & \cdots, & \dfrac{a_{1n}(t)}{d} \\ \dfrac{a_{s1}(t)}{d}, & \cdots, & \dfrac{a_{sn}(t)}{d} \end{pmatrix}$$

where $d \in D_1$, $a_{ij}(t) \in D_1[t]$, for $1 \leqq 1 \leqq s$, $1 \leqq j \leqq n$, and d is not a divisor of all the coefficients of $a_{i1}, \cdots, a_{in}$, for each i from 1 to s. We choose $u^t = (t, t^{N_2}, \cdots, t^{N_n})$, where 1 $N_2, \cdots, N_n$ are in ascending order and so far apart that the terms in $\sum_j a_{ij}(t)t^{N_j}$ do not combine, since their terms are of vastly different degrees. Hence, d does not divide all the coefficients of $\sum_j a_{ij}t^{N_j}$, as required.

(ii) *Case when*

$$A_s = \begin{pmatrix} \dfrac{a_{11}(t)}{a(t)} \cdots & \\ & \dfrac{a_{sn}(t)}{a(t)} \end{pmatrix}, \ s \leqq n,$$

where for no value of i does $d(t)$ divide all of $a_{i1}(t), \cdots, a_{in}(t)$. The approach in (i) needs modification, since $d(t)$ might be just a power of t. We begin by showing that if $\sum_{i=1}^n a_i(t)(t-\alpha)^{N_i}$ is divisible by $d(t)$, then, for $N_1, \cdots, N_n$ sufficiently spaced, each $a_i(t)(t-\alpha)^{N_i}$ is divisible by $d(t)$. Since we could change to the new transcendental $t-\alpha$ over D_1, we need only treat the case $\alpha = 0$. Let $d =$ max degree among $d(t), a_1(t), \cdots$. If

$$d(t)(q_i(t) + \cdots + q_n(t)) = \sum_{i=1}^n a_i(t)t^{N_i}, \cdots_{(*)}$$

where $N_{i-1} + d < N_i$, $i = 2, \cdots, n$, and $q_\nu(t)$ involves only terms of degree greater then $N_{\nu-1}$ but not greater than $N_\nu + d$, then:

The terms on the right side of (*) of degree not greater than $N_1 + d$
$= a_1(t)t^{N_1}$
$=$ terms on left side of (*) of degree less than N_2
$= d(t)q_1(t)$.

Thus $d(t) \mid a_1(t)t^{N_1}$, and so on. Hence, if for some i we have $\sum_{\nu=1}^{n} a_{i\nu}(t)(t - \alpha)^{N_\nu}$ divisible by $d(t)$, then $d(t) \mid a_{i\nu}(t)(t-\alpha)^{N_\nu}$, $1 \leqq \nu \leqq n$. By cancelling the factors $t - \alpha$ which may occur in $d(t)$, we deduce that the complementary factor in $d(t)$ must divide some row of the $a_{i\nu}$. So, if we can pick more α than there are rows, we'd need some row divisible by so much that $d(t)$ would have to divide each $a_{i\nu}(t)$. We assumed that $\#(D_1) > n$ for exactly this reason. So, for some $\alpha \in D_1$ and for all $N_1, \cdots, N_n$ sufficiently large and far apart, all of $\sum_{\nu=1}^{n} a_{i\nu}(t)(t-\alpha)^{N_\nu}$ are indivisible by $d(t)$. As to avoiding hyperplanes of K^n: these have the form $h_1x_1 + \cdots + h_nx_n = 0$, where $h_i \in D_1[t]$. Since for $N_1, \cdots, N_n$ far enough apart, the terms of the $h_i(t)t^{N_i}$ don't overlap, we cannot have $\sum h_i(t)t^{N_i} = 0$. As usual, the change $t \to t - \alpha$ is no problem, so Lemma II is proved.

For our purpose, somewhat more than the above is needed. A mild generalisation of Lemma II is now proved.

LEMMA III. *Let B be an r-by-n matrix over a field containing $D_1(t)$, and assume that there is an r-dimensional subspace V of K^n, where $K = D_1(t)$, such that for all nonzero u in $D_1[t]^n \cap V$ some component of Bu is in $D_1[t]$ and is nonzero. Then, some row of B is such that its inner product with $D_1[t]^n \cap V$ is always in $D_1[t]$ and is not always zero.*

Proof. Since every nonzero element of V goes into D^n, where $D = D_1[t]$, on being multiplied by a suitable element of D, we know that Lemma I applies to B and V. Hence, as in the remarks immediately before Lemma II, we know that by permuting the rows of B we can put it in the form $B = TB_1$, where T is r-by-r, is triangular with only ones on the diagonal and every sub-diagonal entry is either 0 or outside K, while B_1 is such that for all nonzero u in V, the product B_1u is nonzero and in K^r. As in Lemma II, we can order the rows of T so that the ones in K come first:

$$B = \begin{pmatrix} I & & \\ t_{s1}, 1 & & \\ & 1 & \\ t_{r1}, & & 1 \end{pmatrix} B_1 \,,$$

where the last $r - s$ (posssibly 0) rows of T involves elements outside K.

The first $s(\geqq 1)$ rows of B_1 coincide with those of B, and we now show that one of these has the desired property. If not, then for the ith row R_i^t, $1 \leqq 1 \leqq s$, we can find a nonzero u_i in $D^n \cap V$, such that $R_i^t u_i$ is not in D. Consider now the matrix $B_1 U$, where U is n-by-s, consisting of the columns $u_1, \cdots, u_s$; $B_1 U$ is r-by-s, is over K, and the first s rows each contain an element outside D. Hence, as before, we can choose $N_1, \cdots, N_s$ so far apart that $B_1 U((t-\alpha)^{N_1}, \cdots, (t-\alpha)^{N_s})^t$ has its first s components outside D and such that the last $r-s$ components of $TB_1 U((t-\alpha)^{N_1}, \cdots, (t-\alpha)^{N_s})_t$ are not even in K. But the vector $u = \sum_{i=1}^s (t-\alpha)^{N_1} u_i \in D^n \cap V$, and we've just shown that Bu has no component in D. This contradiction shows that one of the first s rows of B has its inner product with $D^n \cap V$ always in D. It cannot be perpendicular to V, as there are nonzero elements of V perpendicular to all the other rows of B, by dimensions, and we excluded having all rows of B perpendicular to some nonzero element of V.

COROLLARY. *If A has property P_D, where $D = D_1[t]$ and $\sharp(D_1) > n$, as before, then the rows of A can be so arranged that R_1^t is over D, and for $k = 1, \cdots, n-1$, for all u in D^n and perpendicular to the first k rows of A, we have $R_{k+1}^t \cdot u$ in D, not always zero.*

Proof. By Lemma II we may assume the first row is over D. Assume that the first k rows have been arranged as desired, for some $k \geqq 1$; we can then proceed to the choice of R_{k+1}^t by applying Lemma III to the matrix of the last $n-k$ rows of A, with V the subspace of K^n orthogonal to the first k rows of A.

This necessary condition for P_D, in the simple transcendental case, has the virtue of being patently sufficient. It also makes evident the Corollary to Theorem II: when $D = F[t]$, so that all ideals are principal, matrices with P_D are essentially just nonsingular matrices over D, apart from permuting the rows and pre-multiplying by the usual triangular T. However, it is not easy to see how this criterion for general $D_1[t]$ would be checked, nor does it seem an obvious deduction that $\det A \in D^*$.

Theorem II will now be deduced. Since we already know that det $A \neq 0$, the r-by-r minors of the first r rows of A cannot all be zero. Hence, we need only show that if the rows have been arranged as in the corollary above, then all the r-by-r minors of the first r rows are in D, for $1 \leqq r \leqq n$. By looking at an r-by-r sub-matrix of the first r rows of A, we see that its orthogonality properties should imply that its determinant is in D, and so it will suffice to prove:

LEMMA IV. *Let B be r-by-r over some field containing K, such that the first row is over D and, for $k = 1, \cdots, r-1$, all u perpen-*

dicular to the first k rows of B and in D^r have an inner product with the $k+1$st row in D. Then $\det B \in D$.

Proof. The case $r = 1$ is trivial, so induction can begin. By the case $r-1$, all the minors of the last row are in D. Since these numbers give a vector in D^r perpendicular to the first $r-1$ rows and having inner product $\det B$ with the last row, we are done. The proof of Theorem II is now complete.

It is not a sufficient condition on A for P_D, to have all these r-by-r minors in D and not all zero, for $1 \leqq r \leqq n$, as the example

$$A = \begin{pmatrix} x^2 & -xy \\ 0 & x^{-2} \end{pmatrix}$$

soon shows. In preparation for the proof of the last theorem, we shall show that the extra condition, that the r-by-r minors be in D and without common divisor, is sufficient in the cases when $D = D_1[t]$ is a unique factorisation ring, for example when $D = F[t_1, t_2, \cdots, t_k]$.

LEMMA V. *Let D be a unique factorisation domain with quotient field K, and let A be an r-by-n matrix of rank r such that, for $1 \leqq k \leqq r$, the k-by-k minors of the first k rows of A are all in D and without common divisor. Then the first row is, of course, over D and, for $1 \leqq k < r$, and for all u in D^n and perpendicular to the first k rows of A, the inner product $R^t_{k+1}\cdot u$ is in D.*

Proof. Since we use induction on r, it is necessary only to deal with the case of u perpendicular to the first $r-1$ rows of A. Consider the equations

$$\begin{pmatrix} a_{11}, \cdots, a_{1n} \\ \cdot \quad \cdots \quad \cdot \\ a_{r1}, \cdots, a_{rn} \\ \\ I_{n-r} \\ \end{pmatrix} \begin{pmatrix} u_1 \\ \\ \cdot \\ \cdot \\ \cdot \\ u_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ p \\ u_{r+1} \\ u_n \end{pmatrix}$$

To show $p \in D$, we multiply both sides by $(C_1, \cdots C_n)$, these being the co-factors of the rth column of the n-by-n matrix: hence

$$\begin{vmatrix} a_{11} \cdots a_{1r} \\ a_{ri} \cdots a_{rr} \end{vmatrix} u_r = C_r p + C_{r+1}u_{r+1} + \cdots + C_n u_n \, .$$

But C_r equals the minor formed with the first $r-1$ rows and columns, while $C_{r+1}, \cdots, C_n$ are also equal to cofactors from the first $r-1$ rows. Thus, $C_r p \in D$. Since changing the order of the columns of A does not alter the truth of the hypotheses, we know that for all the minors C at the $(r-1)$st stage, $Cp \in D$. But these minors are without common divisor. Hence $p \in D$, as required.

COROLLARY. *Every matrix of the form PLV, as in Theorem* III, *has property P_D.*

Proof. Since P serves only to permute the rows, we may ignore it. Then we observe that since L is triangular with elements of D^* on the diagonal, the orthogonality property for V of Lemma III, Corollary, is not changed by going to LV. Thus, it is enough to use Lemma V with $r = n$.

Proof of Theorem III. We have just proved the "sufficienty" part of the theorem. So now assume A has P_D. By Lemma III we can order the rows of A so that for all $u \in D^n$ and perpendicular to the first k rows, $R_{k+1}^t \cdot u \in D$ and is not always zero. By using only those u with $n-k$ entries $u_{i1}, \cdots, u_{i_{n-k}}$ equal to zero, we see that the matrix obtained by erasing columns $i_i, \cdots, i_{n-k}$ and the last $n-k$ rows of A has the orthogonality property. By Lemma IV we deduce that the first k rows of A have all k-by-k minors in D. We now put A in the form LV by taking common factors as follows. We examine the first row of A: it is over D, so we take out the common factors. Proceed inductively: assume that factors have been take out so that the co-factors for the first k rows are without common divisor, for $1 \leqq k < r$, and the new matrix still has the orthogonality property. If the minors of the r rows are not relatively prime, divide the rth row by the common factor. Lemma V shows that the orthogonaltiy property is not lost by this process, so we can continue. This completes the proof of Theorem III.

REFERENCE

1. K. Rogers and E. G. Straus, *A class of geometric lattices*, Bull. Amer. Math. Soc., **66** (1960), 118-123.