NORMAL MATRICES AND THE NORMAL BASIS IN ABELIAN NUMBER FIELDS

R. C. THOMPSON

1. Introduction. Throughout this note F denotes a normal field of algebraic numbers of finite degree n over the rational number field. Let $G_1, G_2, \cdots, G_n$ denote the elements of the Galois group G of F. It is known [2] that F may possess a "normal" basis for the integers consisting of the conjugates $\alpha^{G_1}, \alpha^{G_2}, \cdots, \alpha^{G_n}$ of an integer α. In [4] the question of the uniqueness of the normal basis was answered when G is cyclic. (See also [1, 6].) If $\beta_1, \beta_2, \cdots, \beta_n$ is any integral basis of F then the matrix $(\beta_i^{G_j})$, $1 \leqq i, j \leqq n$, is called a discriminant matrix. It was shown in [4] that if G is abelian then the discriminant matrix of the normal basis $\beta_1 = \alpha^{G_1}, \cdots, \beta_n = \alpha^{G_n}$ is a normal matrix and, if G is cyclic and F has a normal basis, then any integral basis $\beta_1, \cdots, \beta_n$ for which the discriminant matrix is normal is of the form $\beta_{\sigma(1)} = \pm\alpha^{G_1}, \cdots, \beta_{\sigma(n)} = \pm\alpha^{G_n}$ for a suitable choice of the $\pm$ signs, where σ is a permutation of $1, 2, \cdots, n$.

It is the purpose of this note to use the methods of [4] to extend these results for cyclic fields to abelian fields. In particular, in Theorem 1, we shall give a new proof of a result obtained by G. Higman in [1]. The author wishes to thank Dr. O. Taussky-Todd for drawing the problems considered here to his attention.

2. Preliminary material. We suppose throughout that

$$G = (S_1) \times (S_2) \times \cdots \times (S_k)$$

is the direct product of k cyclic groups (S_i) of order n_i. Of course, each $n_i > 1$ and $n = n_1 n_2 \cdots n_k$. If X and $Y = (y_{i,j})$ are two matrices with elements in a group or a ring then we define $X \times Y = (Xy_{i,j})$. $X \times Y$ is the Kronecker product [3] of X and Y. Henceforth, in this paper, the symbol $\times$ will always be used to denote the Kronecker product of vectors or matrices. A matrix A is said to be a circulant of type (n_1) if

$$A = [a_1, a_2, \cdots, a_{n_1}]_{n_1} = \begin{bmatrix} a_1 & a_2 & a_3 & \cdots & a_{n_1} \\ a_{n_1} & a_1 & a_2 & \cdots & a_{n_1 - 1} \\ \cdot & \cdot & \cdot & \cdots & \cdot \\ a_2 & a_3 & a_4 & \cdots & a_1 \end{bmatrix} .$$

Here $a_1, a_2, \cdots, a_{n_1}$ may lie in a group or a ring. For $i > 1$ we define

Received June 15, 1961, and in revised form October 13, 1961.

by induction $[A_1, A_2, \cdots, A_{n_i}]_{n_i}$ to be a circulant of type $(n_1, n_2, \cdots, n_i)$ if each of $A_1, A_2, \cdots, A_{n_i}$ is a circulant of type $(n_1, n_2, \cdots, n_{i-1})$. For $1 \leqq i \leqq k$ let $H_i = (1, S_i, S_i^2, \cdots, S_i^{n_i-1})$ and $D_i = [1, S_i^{n_i-1}, S_i^{n_i-2}, \cdots, S_i]_{n_i}$. Henceforth we shall always let $G_1, G_2, \cdots, G_n$ denote the elements of G in the order implied by the vector equality

$$(G_1, G_2, \cdots, G_n) = H_1 \times H_2 \times \cdots \times H_k. \tag{1}$$

Let $y(G_1), y(G_2), \cdots, y(G_n)$ be commuting indeterminants and define the matrix Y by $Y = (y(G_iG_j^{-1})), 1 \leqq i, j \leqq n$. Then it can be proved by induction on k that $D_1 \times D_2 \times \cdots \times D_k = (G_iG_j^{-1}), 1 \leqq i, j \leqq n$, and hence that Y is a circulant of type $(n_1, n_2, \cdots, n_k)$. Since any circulant of type $(n_1, n_2, \cdots, n_k)$ is determined by its first row, it follows that any circulant of type $(n_1, n_2, \cdots, n_k)$ may be obtained by assigning particular values to the indeterminants $y(G_1), \cdots, y(G_n)$ in Y.

LEMMA 1. *Circulants of type $(n_1, n_2, \cdots, n_k)$ with coefficients in a field K form a commutative matrix algebra containing the inverse of each of its invertible elements. For fixed m, all matrices $X = (X_{i,j})$, $1 \leqq i, j \leqq m$, in which each $X_{i,j}$ is a circulant of type $(n_1, n_2, \cdots, n_k)$ with coefficients in K, form a matrix algebra containing the inverse of each of its invertible elements.*

Proof. Let $W = (w(G_iG_j^{-1}))$, $1 \leqq i, j \leqq m$. Then $W + Y$ and aW for $a \in K$ are clearly circulants of type $(n_1, n_2, \cdots, n_k)$. The (i, j) element of WY is

$$\begin{aligned}\sum_{t=1}^{n} w(G_iG_t^{-1})y(G_tG_j^{-1}) &= \sum_{t=1}^{n} w(G_i(G_t^{-1}G_iG_j)^{-1})y((G_t^{-1}G_iG_j)G_j^{-1}) \\ &= \sum_{t=1}^{n} y(G_iG_t^{-1})w(G_tG_j^{-1}) .\end{aligned}$$

But this is the (i, j) element of YW. Hence $WY = YW$. Define

$$z(G_iG_j^{-1}) = \sum_{t=1}^{n} w(G_iG_t^{-1})y(G_tG_j^{-1}) .$$

Then a straightforward calculation shows that $z(G_iG_j^{-1}) = z(G_pG_q^{-1})$ if $G_iG_j^{-1} = G_pG_q^{-1}$. Hence the variables $z(G_iG_j^{-1})$, $1 \leqq i, j \leqq n$, are unambiguously defined, so that WY is a circulant of type $(n_1, n_2, \cdots, n_k)$. This proves the first half of the first assertion of the lemma. The rest of the first assertion follows from the fact that the inverse of a matrix is a polynomial in the matrix. The other assertion of the lemma is now clear.

We let B' and B^* denote, respectively, the transpose and the complex conjugate transpose of the matrix B. The diagonal matrix whose diagonal entries are $\lambda_1, \lambda_2, \cdots, \lambda_n$ is denoted by diag $(\lambda_1, \lambda_2, \cdots, \lambda_n)$. The zero and identity matrices with s rows and columns are denoted by 0_s and I_s, respectively, and for $i = 1, 2, \cdots, k$, the companion matrix of the polynomial $x^{n_i} - 1$ is denoted by $F_i = [0, 1, 0, \cdots, 0]_{n_i}$.

Let ζ_u be a primitive root of unity of order n_u for $1 \leqq u \leqq k$. Set $\Omega_u = (\zeta_u^{(i-1)(j-1)})$, $1 \leqq i, j \leqq n_u$, and set $\Omega = \Omega_1 \times \Omega_2 \times \cdots \times \Omega_k$. Define $T_u = n_u^{-1/2}\Omega_u$ and $T = n^{-1/2}\Omega$. It can be shown by direct computation that T_u is a unitary matrix. Hence, using the basic properties $(X \times Y)(Z \times W) = XZ \times YW$ and $(X \times Y)^* = X^* \times Y^*$ of the Kronecker product, it follows immediately that T is a unitary matrix.

LEMMA 2. *If A is a circulant of type $(n_1, n_2, \cdots, n_k)$ with first row $a = (a_1, a_2, \cdots, a_n)$ and complex coefficients, then $T^*AT =$ diag $(\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_n)$ where the vector $\varepsilon = (\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_n)$ is linked to the vector a by $\varepsilon' = \Omega a'$.*

Proof. The proof is by induction on k. For $k = 1$ it is well known (and straightforward to check) that $AT_1 = T_1 \operatorname{diag}(\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_{n_1})$. Suppose the result known for $k - 1$. If

$$A = [A_1, A_2, \cdots, A_{n_k}]_{n_k} = \sum_{i=1}^{n_k} A_i \times F_k^{i-1}$$

and if we set $d = n_1 n_2 \cdots n_{k-1}$ and define $(\gamma_{(i-1)d+1}, \gamma_{(i-1)d+2}, \cdots, \gamma_{id})$ by

$$\begin{aligned} \text{(2)} \qquad & \Omega_1 \times \cdots \times \Omega_{k-1}(a_{(i-1)d+1}, a_{(i-1)d+2}, \cdots, a_{id})' \\ & = (\gamma_{(i-1)d+1}, \gamma_{(i-1)d+2}, \cdots, \gamma_{id})', \qquad 1 \leqq i \leqq n_k , \end{aligned}$$

then, by the induction assumption,

$$\begin{aligned} & (T_1 \times \cdots \times T_{k-1})^* A_i (T_1 \times \cdots \times T_{k-1}) \\ & \quad = \operatorname{diag}(\gamma_{(i-1)d+1}, \gamma_{(i-1)d+2}, \cdots, \gamma_{id}), \qquad 1 \leqq i \leqq n_k . \end{aligned}$$

Then

$$\begin{aligned} T^*AT &= \sum_{i=1}^{n_k} (T_1 \times \cdots \times T_{k-1} \times T_k)^* (A_i \times F_k^{i-1})(T_1 \times \cdots \times T_{k-1} \times T_k) \\ &= \sum_{i=1}^{n_k} (\{(T_1 \times \cdots \times T_{k-1})^* A_i (T_1 \times \cdots \times T_{k-1})\} \times \{T_k^* F_k T_k\}^{i-1}) \\ &= \sum_{i=1}^{n_k} (\{\operatorname{diag}(\gamma_{(i-1)d+1}, \gamma_{(i-1)d+2}, \cdots, \gamma_{id})\} \\ & \qquad \times \{\operatorname{diag}(1, \zeta_k^{i-1}, \zeta_k^{2(i-1)}, \cdots, \zeta_k^{(n_k-1)(i-1)})\}) . \end{aligned}$$

Thus T^*AT is diagonal. If $r = (b - 1)d + c$ where $1 \leqq c \leqq d$ and $1 \leqq b \leqq n_k$, then the (r, r) diagonal element of T^*AT is

$$\text{(3)} \qquad \varepsilon_r = \sum_{i=1}^{n_k} \gamma_{(i-1)d+c} \zeta_k^{(b-1)(i-1)} , \qquad 1 \leqq r \leqq n .$$

Setting $\varepsilon = (\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_n)$ and $\gamma = (\gamma_1, \gamma_2, \cdots, \gamma_n)$, equations (3) are the same as the matrix equation $\varepsilon' = (I_d \times \Omega_k)\gamma'$ and equations (2) are the same as $((\Omega_1 \times \cdots \times \Omega_{k-1}) \times I_{n_k})a' = \gamma'$. Combining these two facts, we obtain $\varepsilon' = \Omega a'$, as required.

3. **The uniqueness of the normal basis.** If $\beta^{a_1}, \cdots, \beta^{a_n}$ is another normal basis of F then $(\beta^{a_1}, \cdots, \beta^{a_n})' = (a_{i,j})(\alpha^{a_1}, \cdots, \alpha^{a_n})'$ so that $(\beta^{a_i a_j^{-1}}) = (a_{i,j})(\alpha^{a_i a_j^{-1}})$, $1 \leqq i, j \leqq n$, where $(\beta^{a_i a_j^{-1}})$ and $(\alpha^{a_i a_j^{-1}})$ are both circulants of type $(n_1, n_2, \cdots, n_k)$ and $(a_{i,j})$ is a unimodular matrix of rational integers. By Lemma 1, $(a_{i,j}) = (\beta^{a_i a_j^{-1}})(\alpha^{a_i a_j^{-1}})^{-1}$ is also a circulant of type $(n_1, n_2, \cdots, n_k)$. Conversely, if $\beta_1, \cdots, \beta_n$ is an integral basis such that $(\beta_1, \cdots, \beta_n)' = (a_{i,j})(\alpha^{a_1}, \cdots, \alpha^{a_n})'$ where $(a_{i,j})$ is a unimodular circulant of rational integers of type $(n_1, n_2, \cdots, n_k)$, then $(\beta_{i}^{a_j^{-1}}) = (a_{i,j})(\alpha^{a_i a_j^{-1}})$ so that, by Lemma 1, $(\beta_{i}^{a_j^{-1}})$ is also a circulant. Then, in $(\beta_{i}^{a_j^{-1}})$, the elements in the first column are a permutation on those in the first row. Hence $\beta_1, \cdots, \beta_n$ is a permutation of a normal basis. Following [4], we call a circulant trivial if it has but a single nonzero entry in each row. Thus $\beta_1, \cdots, \beta_n$ is necessarily a permutation of $\alpha^{a_1}, \cdots, \alpha^{a_n}$ or of $-\alpha^{a_1}, \cdots, -\alpha^{a_n}$ precisely when all unimodular circulants of rational integers of type $(n_1, n_2, \cdots, n_k)$ are trivial.

If G has a cyclic direct factor of order other than 2, 3, 4, or 6, we may choose the notation so that (S_1) is this cyclic direct factor. By [4] there exists a nontrivial unimodular circulant B of rational integers of type (n_1). Then $B \times I_{n_2 \cdots n_k}$ is a nontrivial unimodular integral circulant of type $(n_1, n_2, \cdots, n_k)$ and so the normal basis is not unique. Hence only the following two cases remain to be considered:

(i) each $n_i = 4$ or 2;

(ii) each $n_i = 3$ or 2; $1 \leqq i \leqq k$.

In either case (i) or case (ii) let A be a unimodular circulant of rational integers of type $(n_1, n_2, \cdots, n_k)$. Then, by Lemma 2, the determinant of A is $\varepsilon_1\varepsilon_2 \cdots \varepsilon_n$ where each ε_i is an integer and hence a unit in the field K generated by $\zeta_1, \cdots, \zeta_k$. K is generated by the root of unity whose order is the least common multiple of $n_1, n_2, \cdots, n_k$. Since this least common multiple is 2, 3, 4, or 6, by the fundamental theorem on units K contains no units of infinite order and hence each ε_i is a root of unity. By Lemma 2,

$$Ta' = n^{-1/2}\varepsilon' . \tag{4}$$

Since the first row T consists of ones only, ε_1 is rational. In (4) we replace, if necessary, each a_i with $-a_i$ and each ε_i with $-\varepsilon_i$ to ensure that $\varepsilon_1 = 1$. Since T is unitary,

$$a' = n^{-1/2}T^*\varepsilon' = n^{-1}\Omega^*\varepsilon' . \tag{5}$$

Let $\Omega = (r_{i,j})$, $1 \leqq i, j \leqq n$. Then, using (5), the triangle inequality, and the fact that each $| r_{j,i} |$ and each $| \varepsilon_j |$ is one, we find that

$$(6) \qquad | a_i | \leqq n^{-1}\sum_{j=1}^{n} | \bar{r}_{j,i}\varepsilon_j | = 1 , \qquad 1 \leqq i \leqq n .$$

If we have $a_q \neq 0$ for some q, then $| a_q | \geqq 1$, so that in (6) for $i = q$ we have equality. Since $r_{1,q} = \varepsilon_1 = 1$, the condition for equality in the triangle inequality forces $\bar{r}_{j,q}\varepsilon_j = 1$ for each j so that $\varepsilon_j = r_{j,q}$ for $j = 1, 2, \cdots, n$. Then, for $i \neq q$,

$$na_i = \sum_{j=1}^{n}\bar{r}_{j,i}r_{j,q} = 0$$

since the columns of Ω are pairwise orthogonal. Thus, in A, there is but a single nonzero entry in each row.

THEOREM 1. *The normal basis for the integers of F is unique* (*up to permutation and change of sign*) *precisely when either* (i) *or* (ii) *below is satisfied*:

(i) *G is the direct product of cyclic groups of order* 4 *and/or order* 2;

(ii) *G is the direct product of cyclic groups of order* 3 *and/or order* 2.

Another form of this theorem is given in [1, Theorem 6].

4. **Normal discriminant matrices.** Let $\alpha^{G_1}, \cdots, \alpha^{G_n}$ be a normal integral basis of F and let Δ be any normal discriminant matrix. Permuting the row and columns of Δ in the same way (this preserves normality) we may assume $\Delta = (\beta_{ij}^{G_j^{-1}})\, 1 \leqq i, j \leqq n$, where $G_1, \cdots, G_n$ are given by (1). Now $\Delta = (a_{i,j})D$ where $D = (\alpha^{G_iG_j})$, $1 \leqq i, j \leqq n$, and where $(a_{i,j})$ is a unimodular matrix of rational integers. From $\Delta\Delta^* = \Delta^*\Delta$ we get $(a_{i,j})DD^*(a_{i,j})' = D^*(a_{i,j})'(a_{i,j})D$. As in [4], DD^* is rational so that $D^*(a_{i,j})'(a_{i,j})D$ is left fixed by every element of G. Let

$$P_s = I_{n_0n_1\cdots n_{s-1}} \times F_s \times I_{n_{s+1}n_{s+2}\cdots n_{k+1}} , \qquad 1 \leqq \varepsilon \leqq k ,$$

where, here and henceforth, $n_0 = n_{k+1} = 1$. The effect of replacing α with α^{S_s} in D may be determined by noting that

$$\begin{aligned} S_s(D_1 \times \cdots \times D_k) &= D_1 \times \cdots \times (S_sD_s) \times \cdots \times D_k \\ &= D_1 \times \cdots \times (F_sD_s) \times \cdots \times D_k \\ &= I_{n_1} \times \cdots \times I_{n_{s-1}} \times F_s \times I_{n_{s+1}} \times \cdots \times I_{n_k}D_1 \times \cdots \times D_k \\ &= P_s(D_1 \times \cdots \times D_k) . \end{aligned}$$

Hence, replacing α with α^{S_s} in D changes D into P_sD. Therefore $D^*(a_{i,j})'(a_{i,j})D = (P_sD)^*(a_{i,j})'(a_{i,j})(P_sD)$ so that $P_s(a_{i,j})'(a_{i,j})P_s' = (a_{i,j})'(a_{i,j})$, for $s = 1, 2, \cdots, k$. Following [4] we define a generalized permutation matrix to be a permutation matrix in which the nonzero entries are permitted to be ± 1. Then Lemma 3 below shows that $(a_{i,j}) = QC$ where Q is a generalized permutation matrix and C is a circulant of type $(n_1, n_2, \cdots, n_k)$. Since $(\beta_1, \cdots, \beta_n)' = (a_{i,j})(\alpha^{\sigma_1}, \cdots, \alpha^{\sigma_n})'$, this implies (by remarks made in § 2) that $\beta_1, \cdots, \beta_n$ is a generalized permutation of a normal basis.

THEOREM 2. *Let F be a field with a normal integral basis. Then only generalized permutations of a normal basis can give rise to normal discriminant matrices.*

THEOREM 3. *If A is a unimodular matrix of rational integers such that AA' is a circulant of type $(n_1, n_2, \cdots, n_k)$, then $A = CQ$ where C is a unimodular circulant of rational integers of type $(n_1, n_2, \cdots, n_k)$ and Q is a generalized permutation matrix.*

Proof. Since each P_i is a circulant of type $(n_1, n_2, \cdots, n_k)$, it follows from Lemma 1 that $P_iAA'P_i' = AA'$ for $i = 1, 2, \cdots, k$, so that Theorem 3 follows from Lemma 3.

LEMMA 3. *If A is a unimodular matrix of rational integers such that $P_iAA'P_i' = AA'$ for $i = 1, 2, \cdots, k$, then $A = CQ$ where C and Q are as in Theorem 3.*

Proof. Let $A_0 = A$ and $Q_0 = I_n$. We shall prove by induction on i that, for $1 \leqq i \leqq k$, $A = A_iQ_i$ where Q_i is a generalized permutation matrix and A_i may be so partitioned that $A_i = (X_{s,t})$, $1 \leqq s, t \leqq n_{i+1}n_{i+2} \cdots n_kn_{k+1}$, where each $X_{s,t}$ is a circulant of type $(n_1, n_2, \cdots, n_i)$. The case $i = k$ is the statement of the lemma. To avoid having to give a special discussion of the case $i = 1$ we make the following definitions and changes in notation. Recall that $n_0 = n_{k+1} = 1$.

A one row, one column matrix is said to be a circulant of type (n_0). A circulant of type $(n_1, \cdots, n_i)$ will now be called a circulant of type $(n_0, n_1, \cdots, n_i)$. We then know that $A = A_0Q_0$ where A_0 is composed of one row, one column blocks which are circulants of type (n_0) and where Q_0 is a generalized permutation matrix. Our induction assumption is that for a fixed value of i with $1 \leqq i \leqq k$ we have $A = A_{i-1}Q_{i-1}$ where we may partition $A_{i-1} = (A_{s,t})$, $1 \leqq s, t \leqq n_in_{i+1} \cdots n_{k+1}$, so that each $A_{s,t}$ is a circulant of type $(n_0, n_1, \cdots, n_{i-1})$, and where Q_{i-1} is a generalized permutation matrix. We shall then deduce that $A = A_iQ_i$. For notational simplicity we set $f = n_0n_1 \cdots n_{i-1}$, $g = n_in_{i+1} \cdots n_k$, $h = n_{i+1}n_{i+2} \cdots n_{k+1}$, $m = n_1n_2 \cdots n_i$.

Now $AA' = A_{i-1}A'_{i-1}$ so that from $P_iAA'P'_i = AA'$ we deduce that $M_iM'_i = I_n$, where $M_i = A_{i-1}^{-1}P_iA_{i-1}$. Since M_i is a matrix of rational integers it follows that M_i is a generalized permutation matrix. Since P_i and A_{i-1} may, after partitioning, be viewed as matrices with g rows and columns in elements which are circulants of type $(n_0, n_1 \cdots, n_{i-1})$, it follows from Lemma 1 that M_i is also a matrix with g rows and columns in elements which are circulants of type $(n_0, n_1, \cdots, n_{i-1})$. From this point of view M_i must be a "generalized permutation matrix" in that it has but a single nonzero entry in each of its g rows and columns. Each of these nonzero entries is of course both a circulant of type $(n_0, n_1, \cdots, n_{i-1})$ and a generalized permutation matrix.

We now digress for a moment to note that if M is a permutation matrix whose coefficients lie in a ring with identity then a permutation matrix R exists with coefficients in the same ring such that $R'MR$ is a direct sum of one row identity matrices and/or matrices like $[0, 1, 0, \cdots, 0]_t$ for $t > 1$. This assertion is a consequence of the fact that a permutation may be decomposed into disjoint cycles.

Applying this fact to the "generalized permutation matrix" M_i, we find that a permutation matrix R_i exists with g rows and columns in elements which are either 0_f or I_f such that $R'_iM_iR_i = N_i$ is a direct sum of r matrices of the following type:

$$E_j = \begin{bmatrix} 0 & E_{j,1} & 0 & 0 & \cdots & 0 \\ 0 & 0 & E_{j,2} & 0 & \cdots & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdots & \cdot \\ 0 & 0 & 0 & \cdot & \cdots & E_{j,e_j-1} \\ E_{j,e_j} & 0 & 0 & 0 & \cdots & 0 \end{bmatrix}$$

if $e_j > 1$, and $E_j = (E_{j,1})$ if $e_j = 1$. Here each $0 = 0_f$ and each $E_{j,q}$ is both a circulant of type $(n_0, n_1, \cdots, n_{i-1})$ (since R_i has circulants of this type as "elements") and a generalized permutation matrix. Moreover, $e_1 + e_2 + \cdots + e_r = g$. Since N_i is similar to P_i and $P_i^{n_i} = I_n$, then $N_i^{n_i} = I_n$. This implies that each $e_j \leqq n_i$. We shall prove that each $e_j = n_i$. The proof is by contradiction. Suppose for at least one j that $e_j < n_i$. We know that $f(e_1 + e_2 + \cdots e_r) = fg = n$. Hence $fn_ir > n$ and so $r > h$. Now

$$\mathrm{P}_i = [0_f, I_f, 0_f, \cdots, O_f]_{n_i} \times I_h$$

and $P_iA_{i-1} = A_{i-1}M_i$. Let $H_s = (A_{s,1}, A_{s,2}, \cdots, A_{s,g})$ for $1 \leqq s \leqq g$. Then from $P_iA_{i-1} = A_{i-1}M_i$ it follows that: $H_2 = H_1M_i, H_3 = H_2M_i, \cdots, H_{n_i} = H_{n_i-1}M_i; H_{n_i+2} = H_{n_i+1}M_i, H_{n_i+3} = H_{n_i+2}M_i, \cdots, H_{2n_i} = H_{2n_i-1}M_i; \cdots; H_{(h-1)n_i+2} = H_{(h-1)n_i+1}M_i, H_{(h-1)n_i+3} = H_{(h-1)n_i+2}M_i, \cdots, H_{hn_i} = H_{hn_i-1}M_i$. Hence, if $B_j = H_{(j-1)n_i+1}$ for $1 \leqq j \leqq h$, then $H_{(j-1)n_i+q} = B_jM_i^{q-1}$ for $2 \leqq q \leqq n_i$.

Consequently,

$$A_{i-1}R_i = \begin{bmatrix} B_1 \\ B_1M_i \\ B_1M_i^2 \\ \cdots \\ B_1M_i^{n_i-1} \\ \cdots \\ B_h \\ B_hM_i \\ \cdots \\ B_hM_i^{n_i-1} \end{bmatrix} R_i = \begin{bmatrix} B_1R_i \\ B_1M_iR_i \\ B_1M_i^2R_i \\ \cdots \\ B_1M_i^{n_i-1}R_i \\ \cdots \\ B_hR_i \\ B_hM_iR_i \\ \cdots \\ B_hM_i^{n_i-1}R_i \end{bmatrix} = \begin{bmatrix} B_1R_i \\ B_1R_iN_i \\ B_1R_iN_i^2 \\ \cdots \\ B_1R_iN_i^{n_i-1} \\ \cdots \\ B_hR_i \\ B_hR_iN_i \\ \cdots \\ B_hR_iN_i^{n_i-1} \end{bmatrix} .$$

Here each B_jR_i $1 \leqq j \leqq h$, may also be regarded as a row vector with g coordinates in elements which are circulants of type $(n_0, n_1, \cdots, n_{i-1})$. This is so because both B_j and R_i have circulants of this type as "elements".

Let $X = (X_1, X_2, \cdots, X_g)$ be a row vector in which the X_i are square matrices with f rows and columns. Then

$$\begin{aligned} XN_i = (&X_{e_1}E_{1,e_1}, X_1E_{1,1}, X_2E_{1,2}, \cdots, X_{e_1-1}E_{1,e_1-1}, \\ &X_{e_1+e_2}E_{2,e_2}, X_{e_1+1}E_{2,1}, X_{e_1+2}E_{2,2}, \cdots, X_{e_1+e_2-1}E_{2,e_2-1} \\ &\cdots, X_gE_{r,e_r}, \cdots, X_{g-1}E_{r,e_r-1}) \, . \end{aligned}$$

Since each $E_{j,q}$ is a generalized permutation matrix, it follows that the first fe_1 columns of XN_i are, apart from order and possible change of sign, just the first fe_1 columns of X; the next fe_2 columns of XN_i are, up to order and sign, just the next fe_2 columns of X; and, in general, columns

$$\begin{aligned} (7) \qquad & f(e_0 + e_1 + \cdots + e_{s-1}) + 1, f(e_0 + e \cdots + e_{s-1}) + 2, \cdots, \\ & f(e_0 + e_1 + \cdots + e_s) \end{aligned}$$

of XN_i are, apart from order and sign, just these same columns in X. Here $e_0 = 0$. This holds for $s = 1, 2, \cdots, r$.

Hence, in $B_jR_iN_i^v$ for $1 \leqq v \leqq n_i - 1$ and fixed j, columns (7) (for a fixed value of s) are just a generalized permutation of columns (7) in B_jR_i. Moreover, the elements appearing in columns (7) and row q of B_jR_i for $2 \leqq q \leqq f$ are just a permutation of the elements in columns (7) and the first row of B_jR_i, since B_jR_i is composed of blocks which are circulants of type $(n_0, n_1, \cdots, n_{i-1})$. All this means that the elements in columns (7) (for a fixed value of s) and row q (for $2 \leqq q \leqq m$) of the matrix

$$\begin{bmatrix} B_jR_i \\ B_jR_iN_i \\ B_jR_iN_i^2 \\ \cdots \\ B_jR_iN_i^{n_i-1} \end{bmatrix} \tag{8}$$

are generalized permutations of the elements in columns (7) and the first row of this matrix. Hence the integers in row q (for $2 \leqq q \leqq m$) and columns (7) of the matrix (8) are congruent (modulo 2) to a permutation of the integers in column (7) and the first row of (8).

In the matrix $A_{i-1}R_i$ add columns $f(e_0 + e_1 + \cdots + e_{s-1}) + 1$, $f(e_0 + e_1 + \cdots + e_{s-1}) + 2, \cdots, f(e_0 + e_1 + \cdots + e_s) - 1$ to column $f(e_0 + e_1 + \cdots + e_s)$ for $s = 1, 2, \cdots, r$. The integers appearing in rows $mp + 2$, $mp + 3, \cdots, m(p + 1)$ of column $f(e_0 + e_1 + \cdots + e)$ are now congruent (modulo 2) to the integer in row $mp + 1$ and column $f(e_0 + e_1 + \cdots + e_s)$. This holds for $p = 0, 1, \cdots, h - 1$, and $s = 1, 2, \cdots, r$. Now add row $mp + 1$ to rows $mp + 2, mp + 3, \cdots, m(p + 1)$ for $p = 0, 1, \cdots, h - 1$. The integer in row $mp + q$ and column $f(e_1 + e_2 + \cdots + e_s)$ is now congruent to zero (modulo 2), for $2 \leqq q \leqq m; 0 \leqq p \leqq h - 1; 1 \leqq s \leqq r$. Hence columns $f(e_1 + e_2 + \cdots + e_s)$ for $1 \leqq s \leqq r$ may be regarded as lying in the same vector space of dimension h over the field of two elements. Since $r > h$, these vectors are dependent. Consequently the determinant of $A_{i-1}R_i$ is congruent to zero (modulo 2). This is a contradiction as the determinant of $A_{i-1}R_i$ is ± 1.

Hence each $e_j = n_i$. Let Z_j be the block diagonal matrix diag $(I_f, E_{j,1}, E_{j,1}E_{j,2}, \cdots, E_{j,1}E_{j,2} \cdots E_{j,n_i-1})$. Since $E_{j,1}E_{j,2} \cdots E_{j,n_i}$ is a diagonal block in $E_j^{n_i}$ and since $E_j^{n_i} = I_m$, it follows that $E_{j,1}E_{j,2} \cdots E_{j,n_i} = I_f$. From this fact and the fact that the $E_{j,q}$ are generalized permutation matrices we find that $Z_jE_jZ_j' = [0_f, I_f, 0_f, \cdots, 0_f]_{n_i}$. Hence, if $Z = \mathrm{diag}\,(Z_1, Z_2, \cdots, Z_r)$, then $ZN_iZ' = P_i$. Morever, Z is a matrix with g rows and columns in elements which are circulants of type $(n_0, n_1, \cdots, n_{i-1})$. We now have $M_i = U_i'P_iU_i$ where $U_i' = R_iZ'$ is a generalized permutation matrix and a matrix with g rows and columns in elements which are circulants of type $(n_0, n_1, \cdots, n_{i-1})$. Then

$$A_{i-1} = \begin{bmatrix} B_1U_i'U_i \\ B_1U_i'P_iU_i \\ \cdots \\ B_1U_i'P_i^{n_i-1}U_i \\ \cdots \\ B_hU_i'U_i \\ \cdots \\ B_hU_i'P_i^{n_i-1}U_i \end{bmatrix} = \begin{bmatrix} B_1U_i' \\ B_1U_i'P_i \\ \cdots \\ B_1U_i'P_i^{n_i-1} \\ \cdots \\ B_hU_i' \\ \cdots \\ B_hU_i'P_i^{n_i-1} \end{bmatrix} U_i = A_iU_i\ ,$$

say. Here each $B_j U'_i$ is a vector with g coordinates in elements which are circulants of type $(n_0, n_1, \cdots, n_{i-1})$. From the form of A_i it follows that A_i may be partitioned into blocks which are circulants of type $(n_0, n_1, \cdots, n_i)$.

The proof is now complete.

References

1. G. Higman, *The units of group rings*, Proc. London Math. Soc., **46** (1940), 231-248.
2. D. Hilbert, *Théorie des corps de nombres algébriques*, Paris, (1913), 164.
3. C. C. MacDuffee, *The theory of matrices*, New York, (1956), 81.
4. M. Newman and O. Taussky, *A generalization of the normal basis in abelian algebraic number fields*, Comm. Pure Appl. Math., **9** (1956), 85-91.
5. O. Taussky, *Unimodular integral circulants*, Math. Z., **63** (1955), 286-289.
6. O. Taussky, *Matrices of rational integers*, Bull. Amer. Math. Soc., **66** (1960), 327-345.

University of British Columbia