GROUP MATRICES

by

William T. Iwata

A THESIS SUBMITTED IN PARTIAL FULFILMENT OF

THE REQUIREMENTS FOR THE DEGREE OF

MASTER OF ARTS

in the Department

of

Mathematics.

We accept this thesis as conforming to the required standard from candidates for the degree of MASTER OF ARTS

THE UNIVERSITY OF BRITISH COLUMBIA

September, 1965

ABSTRACT

A new proof is given of Newman and Taussky's result: if A is a unimodular integral $n \times n$ matrix such that $A'A$ is a circulant, then $A = QC$ where Q is a generalized permutation matrix and C is a circulant. A similar result is proved for unimodular integral skew circulants.

Certain additional new results are obtained, the most interesting of which are: 1) Given any nonsingular group matrix A there exist unique real group matrices U and H such that U is orthogonal and H is positive definite and $A = UH$; 2) If A is any unimodular integral circulant, then integers k and s exist such that $A' = P^k A$ and $P^s A$ is symmetric, where P is the companion matrix of the polynomial $x^n - 1$.

Finally, all the $n \times n$ positive definite integral and unimodular skew circulants are determined for values of $n \leq 6$: they are shown to be trivial for $n = 1,2,3$ and are explicitly described for $n = 4,5,6$.

I hereby certify that this abstract is satisfactory.

TABLE OF CONTENTS

ACKNOWLEDGEMENTS

It is a pleasure to acknowledge my indebtedness to my supervisor Dr. R. C. Thompson for suggesting the study of skew circulants and of circulants in general and for his encouragement and advice in preparing this thesis.

1. Group Rings

Let G be a finite group of order n with elements $g_1,\ldots,g_n$ and let K be an integral domain and let F be a field containing K as a subring. Let $R(G,F)$ denote a vector space over F which admits the elements $g_1,\ldots,g_n$ of G as a basis and in which, additionally, products are defined by $\sum_{i=1}^{n} a_i g_i \sum_{j=1}^{n} b_j g_j = \sum_{i,j=1}^{n} a_i b_j g_{i,j}$ where a_i, b_j are in F and $g_{i,j} = g_i g_j$. It is well known that these operations make $R(G,F)$ into an associative algebra. Let $R_{G,K}$ denote the set of all elements of the form $\sum_{i=1}^{n} a_i g_i$ in $R(G,F)$ where the scalars a_i are in K.

Let 1_G and 1_K be the identities of G and K respectively; and let $1 = 1_K \cdot 1_G$ denote the identity of $R_{G,K}$ and of G and of K as well except under anomalous situations. It is clear that $R_{G,K}$ is a subring of $R(G,F)$. Since $g_1,\ldots,g_n$ is a basis for $R(G,F)$, every element of $R_{G,K}$ is uniquely determined by the scalars in K. We shall refer to $R_{G,K}$ as a group ring of G over K.

2. Matrix Representations and Group Matrices.

A <u>matrix representation</u> of degree n of G is a homomorphism of G into the full linear group $L_n(F)$, the $n \times n$ nonsingular matrices over F.

We introduce the left regular representation of G as follows. If $g \in G$, then

$$gg_i = \sum_{j=1}^{n} a_{ij}(g) g_j \quad , \qquad 1 \leq i \leq n \tag{1}$$

where each $a_{ij}(g)$ is 0 or 1. Let

$$L(g)' = (a_{ij}(g)) , \tag{2}$$

the prime denoting transpose. $L(g)$ is a permutation matrix. Moreover, $L(hg) = L(h)L(g)$, for h,g in G, as the following computation shows. Premultiply eq. 1 by h to get

$$\begin{aligned} h(gg_i) &= \sum_{j=1}^{n} a_{ij}(g) hg_j \\ &= \sum_{j} a_{ij}(g) \sum_{k} a_{jk}(h) g_k \\ &= \sum_{k=1}^{n} \Big(\sum_{j=1}^{n} a_{ij}(g) a_{jk}(h) \Big) g_k \\ &= (hg) g_i \\ &= \sum_{k=1}^{n} a_{ik}(hg) g_k . \end{aligned}$$

Thus $a_{ik}(hg) = \sum_{j=1}^{n} a_{ij}(g)a_{jk}(h)$, hence $L(hg)' = L(g)'L(h)'$, and so $L(hg) = L(h)L(g)$.

If $L(g) = I_n$, then $a_{ij}(g) = 0$, if $i \neq j$, and $a_{ij}(g) = 1$, if $i = j$; and so, $gg_i = g_i$, hence g is the identity. Thus

Lemma 1. G is isomorphic to the group of permutation matrices $L(g)$, g in G, where $L(g)$ is defined relative to the ordering $g_1, \ldots, g_n$ of the elements of G.

We shall call $L(g)$ the <u>left regular matrix representation</u> of G (relative to a particular ordering of the elements of G). We may extend $L(g)$ to a representation of the group ring $R_{G,K}$: for every

$u = \sum_{k=1}^{n} a_k g_k$, a_k in K, set

$$L(u) = \sum_{k=1}^{n} a_k L(g_k) \,. \tag{3}$$

This gives us, by Lemma 1 and the rule for multiplication in $R_{G,K}$,

<u>Lemma</u> 2. For elements u,v in $R_{G,F}$ and a and b in F

$$L(uv) = L(u)L(v),$$

$$L(au+bv) = aL(u) + bL(v) \,.$$

For each g in G the right representation of G is given by

$$g_i g = \sum_{j=1}^{n} b_{ij}(g) g_j, \qquad i = 1,\ldots,n \tag{4}$$

and this corresponds to the mapping

$$R\colon g \to R(g) = (b_{ij}(g)), \quad 1 \le i,\ j \le n,$$

of G onto n distinct permutation matrices of degree n. Eq. 4 implies that G is isomorphic to the matrices $R(g)$, g in G; they form the <u>right regular matrix representation</u> of G.

<u>Theorem</u> 1. Any linear combination of the matrices of the left regular matrix representation commutes with any linear combination of the matrices of the right regular matrix representation.

Proof. By eq.'s 1 and 4 respectively we have for elements g and h in G

$$(gg_1,\ldots,gg_n)' = L'(g)(g_1,\ldots,g_n)' \tag{5}$$

$$(g_1h,\ldots,g_nh)' = R(h)(g_1,\ldots,g_n)' \tag{6}$$

Post-multiplication of eq. 5 by h gives us

$$\begin{aligned}(gg_1h,\ldots,gg_nh)' &= L'(g)(g_1h,\ldots,g_nh)' \\ &= L'(g)R(h)(g_1,\ldots,g_n)'\end{aligned}$$

where the latter result follows from eq. 6. Premultiplying this by g^{-1} and using eq. 5 produces

$$\begin{aligned}(g_1h,\ldots,g_nh)' &= L'(g)R(h)(g^{-1}g_1,\ldots,g^{-1}g_n)' \\ &= L'(g)R(h)L'(g^{-1})(g_1,\ldots,g_n)' \ .\end{aligned}$$

Comparing this with eq. 6 we get $R(h) = L'(g)R(h)L'(g^{-1})$. Since $L(g)L(g^{-1}) = I = L(g)L(g)'$, we get $L(g)R(h) = R(h)L(g)$, as required.

Any linear combination of the left regular matrix representation of G over K is called a <u>group matrix</u> of G over K. This of course presupposes an ordering of the elements of G. Consider the permutation matrix $L(g)$ in eq. 2 in view of eq. 1. We have a one at the (j,i) position of $L(g)'$ precisely when $gg_j = g_i$, hence precisely when $g = g_i g_j^{-1}$. Thus a one appears at the (i,j) position of $L(g)$ precisely when $g = g_i g_j^{-1}$. Thus in $L(u) = \sum_{g_k \text{ in } G} a_{g_k} L(g_k)$, we have a_{g_k} appearing exactly at those positions (i,j) for which $g_k = g_i g_j^{-1}$. In other words, a group matrix of G relative to $g_1,\ldots,g_n$ of G is of the form

$$L(u) = (a_{g_i g_j^{-1}}), \quad 1 \leq i,\ j \leq n . \tag{7}$$

<u>Theorem</u> 2. Any matrix over F which commutes with all matrices of the right regular matrix representation of G is a group matrix of G; that is, it is a linear combination of the matrices of the left regular matrix representation of G.

Proof. Let $C = (c_{ij})$, $1 \leq i,\ j \leq n$, c_{ij} in K, be such that $C = R(g_k)CR(g_k)'$, $k = 1,\ldots,n$, where $R(g_k) = (b_{ij}(g_k))$ as defined in eq. 4 is the right regular matrix representation of G. Let u_j be the n-tuple row vector in which a one occurs in column j and 0's elsewhere. Then for fixed i,j, $1 \leq i,\ j \leq n$, and each k, we have,

$$c_{ij} = u_i C u_j' = u_i R(g_k) C R(g_k)' u_j'$$
$$= \sum_{s,t=1}^{n} b_{is}(g_k) c_{st} b_{jt}(g_k). \tag{8}$$

This sum may be simplified. For, by eq. 4, $b_{ij}(g_k) = 1$, if $g_i^{-1} g_j = g_k$ and $b_{ij}(g_k) = 0$, if $g_i^{-1} g_j \neq g_k$. Hence $c_{ij} = c_{st}$ where s,t are such that $g_i^{-1} g_s = g_k = g_j^{-1} g_t$. Thus $g_i = g_s g_k^{-1}$ and $g_j^{-1} = g_k g_t^{-1}$, so that $g_i g_j^{-1} = g_s g_t^{-1}$. Hence, by eq. 7, C is a group matrix.

Since the matrices $L(g)$ form a group isomorphic to G, and since the matrices are also linearly independent over F, we have Theorem 3.

Theorem 3. $R(G,F)$ is isomorphic to the algebra over F generated by the $L(g)$, g in G. $R_{G,K}$ is isomorphic to the ring generated over K by the $L(g)$, g in G.

Corollary 1. The inverse and the transpose of a group matrix is a group matrix.

Proof. The inverse of any matrix is a polynomial in that matrix. Hence by Theorem 3 the inverse of a group matrix is a group matrix.

Since $L(g^{-1}) = L(g)'$, g in G, the transpose of a linear combination of $L(g_1),\ldots,L(g_n)$ over F is again a linear combination of $L(g_1),\ldots,L(g_n)$ although in a different order. This proves that the transpose of a group matrix is a group matrix.

3. Units and Unimodular Group Matrices.

Elements u and v in $R_{G,K}$ satisfying uv = 1 are called <u>left</u> <u>and</u> <u>right</u> <u>units</u> of $R_{G,K}$, respectively. An element which is both a left and right unit of $R_{G,K}$ is called a <u>unit</u> of $R_{G,K}$. Any square matrix defined over K is said to be unimodular if its determinant is a unit in K. Given the elements u,v above, Lemma 2 and the definition given in eq. 3 imply $L(u)L(v) = L(uv) = L(1) = I_n$. Therefore, L(u) is unimodular. Conversely, let L(u) be unimodular over K. Then $L(u)^{-1}$ exists and by Corollary 1 it is a group matrix with elements in F. In fact, $L(u)^{-1}$ has elements in K since any element of $L(u)^{-1}$ is of the form $S(\det L(u))^{-1}$ in K where S is a cofactor of L(u) and $(\det L(u))^{-1}$ is in K. Thus an element v in $R_{G,K}$ exists such that $L(u)^{-1} = L(v)$, $L(uv) = L(u)L(v) = I_n$; and so, by Theorem 3 uv = 1. This proves "Theorem 4".

<u>Theorem</u> 4. An element is a left unit of $R_{G,K}$ if and only if the corresponding group matrix is unimodular.

<u>Corollary</u> 2. Every left (right) unit is a unit.

Proof. $L(u)L(v) = I_n = L(v)L(u)$.

<u>Theorem</u> 5. The set of all units of $R_{G,K}$ under multiplication forms a group isomorphic to the multiplication group of all unimodular group matrices of G over K.

4. Circulants and Skew Circulants.

When G is a cyclic group with an element g of order n, the group matrix of G over K relative to the elements $1,g,\ldots,g^{n-1}$ is called a <u>circulant</u> over K. Let $g_i = g^{i-1}$, $i = 1,\ldots,n$. Then $g_i g_j^{-1} = g^{i-1-(j-1)} = g^{i-j}$. Thus, $C_{g_i g_j^{-1}} = C_{g^{i-j}}$ and so the elements of the group matrix are constant along each diagonal parallel to the main diagonal.

Let P be the companion matrix of the polynomial x^n-1. Then $P^n = I_n$ and

$$P^i = \begin{array}{c} \\ \\ \\ n-i+1 \\ \\ \\ \end{array} \begin{array}{c} \begin{array}{cccccccc} & & & i+1 & & & & \end{array} \\ \left(\begin{array}{cccccccc} 0 & \ldots & 0 & 1 & 0 & \ldots & & 0 \\ \cdot & \cdots & \cdot & & & & & \\ 0 & \ldots & 0 & 0 & \ldots & & 0 & 1 \\ \hline 1 & 0 & \ldots & 0 & 0 & & \ldots & 0 \\ \cdot & \cdot & \cdots & \cdot & \cdot & & \cdots & \cdot \\ 0 & 0 & \ldots & 1 & 0 & & \ldots & 0 \end{array}\right) \end{array} \tag{9}$$

where $1 \leq i \leq n-1$. It follows that any circulant C is a polynomial in P. Moreover, Theorem 2 in the special case of circulants becomes

<u>Lemma</u> 3. The matrices of the left and right regular representations of G relative to the elements $1,g,\ldots,g^{n-1}$ are circulants. Any matrix commuting with P is a circulant.

If the first row of the circulant C is given by $(c_1,\ldots,c_n)$ we write

$$C = [c_1,\ldots,c_n]_n \tag{10}$$

for brevity. Let the conjugate transpose of a matrix A be denoted by A^*.

Theorem 5. Let $C = [c_1,\ldots,c_n]_n$ be a circulant of order n defined over the complex number field. Let $T = n^{-1/2}(\rho^{(i-1)(j-1)})$, $i \leq i$, $j \leq n$

where ρ is a primitive nth root of unity. Then

$$T^*CT = \mathrm{diag}(\epsilon_1,\ldots,\epsilon_n) \tag{11}$$

where the eigenvalues $\epsilon_1,\ldots,\epsilon_n$ of C are given by the vector matrix equation

$$(\epsilon_1,\ldots,\epsilon_n)' = n^{1/2}T(c_1,\ldots,c_n)' . \tag{12}$$

Proof. Since $x^n-1 = (x-1)g(x)$ where $g(x) = 1 + x + \cdots + x^{n-1}$, $g(\rho^k) = 0$, if n does not divide k. Thus T is unitary; that is, $T^*T = I_n$. For, the (j,i) term of T^*T is given by

$$n^{-1}\sum_{k=1}^{n} \bar{\rho}^{(k-1)(j-1)}\rho^{(k-1)(i-1)} = n^{-1}\sum_{k=1}^{n} \rho^{(k-i)(i-j)}$$

The RHS equals 1, if $i = j$ and equals $g(\rho^{i-j}) = 0$, if $i \neq j$.

Now, since P is the companion matrix of polynomial x^n-1, the eigenvalues of P are the roots of x^n-1; namely, $1, \rho, \rho^2, \ldots, \rho^{n-1}$. Thus if λ_j equals the jth column of T we get

$$P\lambda_j = n^{-1/2}(\rho^{j-1}, \rho^{2(j-1)}, \ldots, \rho^{(n-1)(j-1)}, 1)'$$
$$= \rho^{j-1} \lambda_j$$

so that, the jth column of T is an eigenvector corresponding to the eigenvalue ρ^{j-1} of P, $j = 1,\ldots,n$. Thus, $T^*PT = \mathrm{diag}(1,\rho,\ldots,\rho^{n-1})$. Consequently $C = \sum_{j=1}^{n} c_j P^{j-1}$ implies

$$T^*CT = \sum_{j=1}^{n} c_j \ \mathrm{diag}(1,\rho^{(j-1)}, \rho^{2(j-1)},\ldots,\rho^{(n-1)(j-1)}) .$$

Therefore, if we set

$$\epsilon_i = \sum_{j=1}^{n} c_j \rho^{(i-1)(j-1)} \tag{13}$$

we get eq. 11 and 12 as desired.

The polynomials over K in the $n \times n$ matrix

$$P = \begin{pmatrix} 0 & 1 & 0 & \ldots & 0 \\ \vdots & & & & 0 \\ 0 & 0 & & & 1 \\ -1 & 0 & . & \ldots & 0 \end{pmatrix} \tag{14}$$

are called skew circulants of degree n over K. Skew circulants are not group matrices because in any group matrix the elements in row i are permutations of the elements in row one, $1 \leq i \leq n$. However, the powers of P_- constitute a matrix representation for the cyclic group of order 2n.

Since P_- is the companion matrix of the polynomial $f(x) = x^n + 1$, its eigenvalues are $\rho, \rho^3, \ldots, \rho^{2n-1}$ where ρ is the 2nth primitive root of unity. If $h(x) = x^{2n}-1$, then $h(x) = (x-1)(x+1)g(x)$ where $g(x) = 1 + x^2 + \cdots + x^{2n-2}$. Therefore $g(\rho^k) = 0$, if n does not divide k; otherwise $g(\rho^k) = n$. Therefore, if $T = n^{-1/2}(\rho^{(i-1)(2j-1)})$, $1 \leq i, j \leq n$, the (i,j) element of T^*T being

$$n^{-1} \sum_{k=1}^{n} \bar{\rho}^{(2i-1)(k-1)} \rho^{(k-1)(2j-1)} = n^{-1} \sum_{k=1}^{n} \rho^{2(k-1)(j-i)}$$

$$= n^{-1} g(\rho^{j-i}),$$

implies $T^*T = I_n$. Moreover, the product of P_- and λ_j, the jth column of T, yields

$$P_- \lambda_j = n^{-1/2}(\rho^{2j-1}, \rho^{2(2j-1)}, \ldots, \rho^{(n-1)(2j-1)}, -1)'$$

$$= \rho^{2j-1} \lambda_j$$

since $\rho^n = -1$ implies $\rho^{n(2j-1)} = (-1)^{2j-1} = -1$. In other words, the jth column of T is an eigenvector of P_- corresponding to its eigenvalue ρ^{2j-1}, $j = 1, \ldots, n$. Therefore, $T^*PT = \mathrm{diag}(\rho, \rho^3, \ldots, \rho^{2n-1})$.

<u>Theorem</u> 6. If $A = \sum_{j=1}^{n} a_j P_-^{j-1}$ is a skew circulant over K, then

$$T^* AT = \text{diag}(\epsilon_1, \ldots, \epsilon_n) \tag{15}$$

where $(\epsilon_1, \ldots, \epsilon_n)' = n^{1/2} T'(a_1, \ldots, a_n)'$. (16)

5. Existence of Nontrivial Unimodular Integral Circulants and Skew Circulants.

A unimodular integral (skew) circulant is called trivial if all elements in any row are zero except for a single ± 1; otherwise, it is called nontrivial. We know trivial unimodular (skew) circulants always exist: see (eq. 14) eq. 9. It is shown in [7] that nontrivial unimodular circulants exist if $n \neq 2,3,4,6$.

What about nontrivial unimodular integral skew circulants? This problem is not settled. However, if A were such a matrix then so would be the matrix AA'. For, a diagonal element in AA' is the sum of the squares of the elements in any row of A; and so, off diagonal elements must occur in AA' since it is unimodular. Therefore, the solution is in the answer to another question: For which values of n do nontrivial unimodular skew circulants exist when they are positive definite? This question will be taken up in the sequel for values of $n < 7$.

6. A New Proof of a Theorem on Positive Definite Circulants and Skew Circulants.

In this section G is always a cyclic group of order n and all $n \times n$

matrices are assumed to be integral and unimodular. An $n \times n$ matrix is called a generalized permutation matrix if it has exactly one non zero element, $+1$ or -1, occuring in each row and column.

Theorem 7. If G is a cyclic group of order n and $A'A$ is a unimodular integral group matrix of G, where A is an $n \times n$ matrix of rational integers, then $A = QC$ where Q is a generalized permutation matrix and C is a unimodular group matrix of G.

The proof proceeds by way of Lemmas. For $n > 1$, let $[0,1,0,\ldots,0]_n^-$ denote the matrix in eq. 14.

Lemma 4. Let P and A be $n \times n$ unimodular matrices of rational integers such that

$$P'A'AP = A'A. \tag{17}$$

Then a generalized permutation matrix R exists such that

$$RAPA^{-1}R' = \mathrm{diag}(P_{n_1},\ldots,P_{n_s}) \tag{18}$$

where $n = n_1 + \cdots + n_s$ and for each $i = 1,\ldots,s$, P_{n_i} is $n_i \times n_i$ and is a one rowed submatrix of the form (1) or (-1) if $n_i = 1$, or if $n_i > 1$, of the form $[0,1,0,\ldots,0]_{n_i}$ or $[0,1,0,\ldots,0]_{n_i}^-$.

Proof. The matrix $B = APA^{-1}$ is orthogonal since $(APA^{-1})'APA^{-1} = I_n$; it is also an integral matrix since A is unimodular. Therefore, $B = (b_{ij})$, $1 \leq i, j \leq n$ is a generalized permutation matrix.

Let T be a linear transformation of an n-dimensional space R_n whose matrix is B relative to a basis $e_1,\ldots,e_n$ of R. Then,

$$T(e_i) = b_{i,\pi(i)} e_{\pi(i)}, \quad i = 1,\ldots,n \tag{19}$$

where π is a suitable permutation on $1,\ldots,n$ and $b_{i,\pi(i)} = \pm 1$. Let

$$\pi = (j(1)j(2)\cdots j(r_1))(j(r_1+1)j(r_1+2)\cdots j(r_2))\cdots$$

$$\cdots(j(r_{s-1}+1)j(r_{s-1}+2)\cdots j(r_s)) \tag{20}$$

be a decomposition into s disjoint cyclic products of lengths, say, $n_1,\ldots,n_s$ respectively where $r_0 = 0$, $n_i = r_i - r_{i-1}$, $i = 1,\ldots,s$ and $r_s = n$ and where $j(1),\ldots,j(n)$ is a permutation of $1,\ldots,n$ with $j(1) = 1$. This gives us another basis of R_n:

$$(f_1,\ldots,f_n) = (e_1, e_{j(2)},\ldots,e_{j(n)}) \tag{21}$$

$$= S(e_1,\ldots,e_n)' \tag{22}$$

where S is some permutation matrix. Moreover by eq. 21, 19 and 20 consecutively for $k = 1,\ldots,s$ we get

$$T(f_{r_{k-1}+n_k}) = T(f_{r_k}) = b_{j(r_k),j(r_k)} f_{r_k}$$

when $n_k = 1$; and when $n_k > 1$,

$$T(f_i) = b_{j(i),j(i+1)} f_{i+1}, \quad r_{k-1} < i < r_{k-1} + n_k,$$

with

$$T(f_{r_k}) = b_{j(r_k),j(r_{k-1}+1)} f_{r_{k-1}+1} \cdot$$

In other words except for change in signs T permutes $f_{r_{k-1}+1}, f_{r_{k-1}+2}, \dots, f_{r_k}$ cyclically. In matrix notation this amounts to

$$(T(f_1),\dots,T(f_n))' = H(f_1,\dots,f_n)' \tag{23}$$

where $H = \text{diag}\,(B_1,\dots,B_s)$ is a direct sum of $n_k \times n_k$ matrices B_k whose typical form is the following: $B_k = (\pm 1)$ when $n_k = 1$ and when $n_k > 1$,

$$B_k = \begin{pmatrix} 0 & b_1 & & \\ & & \cdot & \\ & & b_2 & \\ \vdots & & & \\ & & & b_{n_k-1} \\ 0 & & & \\ b_{n_k} & 0 & \dots & 0 \end{pmatrix}$$

where of course the b_i's are equal to $\pm$ 1. Let $Z = \text{diag}\,(1, b_1, b_1 b_s, \dots, b_1 \dots b_{n_k})$.

Then, since $b_i = \pm 1$ we get

$$ZB_kZ' = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ \vdots & & & & \vdots \\ & & & & 0 \\ 0 & & & & 1 \\ b_1 \cdots b_{n_k} & & 0 & \cdots & 0 \end{pmatrix} \quad (\text{if } n_k > 1).$$

Thus we may construct a matrix W, a direct sum of s blocks analogous in form to Z, such that

$$\begin{aligned} WHW' &= W \operatorname{diag}(B_1,\ldots,B_s)W' \\ &= \operatorname{diag}(P_{n_1},\ldots,P_{n_s}) \end{aligned} \tag{24}$$

where P_{n_i} are the matrices defined in eq. 1. But

$$\begin{aligned} (T(f_1),\ldots,T(f_n))' &= S(T(e_1),\ldots,T(e_n))' \\ &= SB(e_1,\ldots,e_n)' \\ &= SBS'(f_1,\ldots,f_n)' \end{aligned}$$

as a result of eq.'s 22, 19, and 22 respectively. Comparing this to eq. 23 we get $H = SBS'$. Therefore, by eq. 24, $WSBS'W' = \operatorname{diag}(P_{n_1},\ldots,P_{n_s})$, and the lemma is proved since $R = WS$ is a generalized permutation matrix and $B = APA^{-1}$.

If, in Lemma 4: 1) the matrix A satisfies the hypothesis in Theorem 7; 2) P is a matrix of the left regular matrix representation of G where n is the order of P; i.e. $P^n = I_n$; 3) the right hand sides of eq. 18 equals $[0,1,0,\ldots,0]_n$, then Theorem 7 is true. For, let L(h), h in G, be the left regular matrix representation which define the group matrix $A'A$ relative, say, to the ordering $g_1,\ldots,g_n$ of the elements of G; let $L_o(h)$, h in G be the left regular matric representation relative to $1, g, \ldots, g^{n-1}$ where g in G is of order n. Then,

$$L_o(g) = [0,1,0,\ldots,0]_n \text{ and } L(h) = SL_o(h)S', \tag{25}$$

h in G, where S is a permutation matrix such that $(g_1,\ldots,g_n)' = S(1,g,\ldots,g^n)'$. But conditions 2) and 3) imply $RAL(g)A^{-1}R' = [0,1,0,\ldots,0]_n$; whence, by eq.'s 25 $SRAL(g)A^{-1}R'S' = L(g)$ and so, SRA commutes with $L(h)$, h in G. From Theorem 2, observing that the left and right regular matrix representations are identical when G is abelian, we infer that SRA is group matrix C of G relative to $g_1,\ldots,g_n$. Put $Q = (SR)'$. This proves Theorem 7 given assumptions 1), 2) and 3) above which are justified as the next lemma shows.

Lemma 5. Let G,A,n be defined as in Theorem 7. Let $A'A$ be a group matrix, a linear combination of the left regular representation matrices $L(h)$, h in G, of G. Then a generalized permutation matrix R exists such that

$$RAL(g)A^{-1}R' = [0,1,0,\ldots,0]_n \tag{26}$$

where g in G is of order n.

Proof. Since G is abelian Lemma 1 and 2 imply $A'A$ and $L(g)$ commute. Therefore, in particular. $P'A'AP = A'A$, where $P = L(g)$. This permits us to use eq. 18 in Lemma 4; that is, condition 1) is satisfied. Also note that $P^n = I_n$ and $P^r \neq I_n$ if $r < n$.

To show condition 3) holds, let $D = RA$ in eq. 18. Then by taking sums of powers from 1 to n and noting that $P^i = L(g^i)$, $i = 1,\ldots,n$ and $L(1) + L(g) + \cdots + L(g^{n-1}) = [1,1,\ldots,1]_n$ we get the similarity relation

$$D[1,\ldots,1]_n\ D^{-1} = \text{diag}\ (B_1,\ldots,B_s) \tag{27}$$

where $B_i = \sum_{j=1}^{n} P_{n_i}{}^j$, $i = 1,\ldots,s$. Using eq. 18, again. $P^n = I_n$ implies $P_{n_i}^n = I_{n_i}$, so that, for some integer m_i, $n = n_i m_i$. In fact, when P_{n_i} is a skew circulant, $2n_i$ is the smallest positive integer such that $P_{n_i}{}^{2n_i} = I_{n_i}$ so that, if $m_i = 2q_i$, then $B_i = \sum_{j=1}^{n} P_{n_i}{}^j = q_i \sum_{j=1}^{2n_i} P_{n_i}{}^j = 0$.

When P_{n_i} is a circulant, $B_i = \sum_{j=1}^{n} P_{n_i}{}^j = m_i \sum_{j=1}^{n_i} P_{n_i}{}^j = m_i[1,\ldots,1]_{n_i}$.

Thus rank B_i is 1 or 0 according as P_{n_i} is a circulant or a skew circulant. However, the rank of the left side of eq. 27 is 1 so that on the right side one and only one non zero component exists; say, $m_k\ [1,\ldots,1]_{n_k}$ arising from a circulant P_{n_k}. Thus n_k divides each element on the right side. But D is a unimodular matrix of rational integers and so m_k divides each element of D^{-1} diag $(B_1,\ldots,B_s)D$, hence m_k divides 1. Therefore $m_k = 1$, $n_k = n$ and eq. 27 implies $RAPA^{-1}R^{-1} = P_{n_k} = [0,1,0,\ldots,0]_n$.

Corollary 2. If A is a unimodular integral matrix and $A'A$ is a circulant, then

$$A = QC \tag{28}$$

where Q is a generalized permutation matrix and C is a unimodular integral circulant.

Theorem 8. If A is a unimodular integral matrix and $A'A$ is a skew circulant, then $A = QC$ where Q is a generalized permutation matrix and C is a unimodular integral skew circulant.

Proof. Let $P = [0,1,0,\ldots,0]^{-}_{n}$. Then, since $A'A$ is by definition a linear combination of powers of P, $P'A'AP = A'A$. Thus, eq. 18 in Lemma 4 can be used. We shall show $s = 1$ and therefore $P_{n_1} = P$ and this would establish Theorem 8 since a matrix which commutes with a nonderogatory matrix is a polynomial in it.

Observe that, if P_{n_i} is a skew circulant, then by adding the first column of the matrix sum

$$P_{n_i} + P_{n_i}^{\;2} + \cdots + P_{n_i}^{\;n_i} = \begin{pmatrix} -1 & 1 & \cdots & 1 \\ \vdots & & & \vdots \\ & & & 1 \\ -1 & . & \cdots & -1 \end{pmatrix}$$

to every other column we get a triangular matrix with -1 as the first diagonal element and -2 for the remaining diagonal elements. Thus

$$\det \sum_{j=1}^{n_i} P_{n_i}^{\;j} = (-1)^{n_i} 2^{n_i - 1} \tag{29}$$

Also, $\sum_{j=1}^{2n_i} P_{n_i}{}^j = 0$, so that if m is odd

$$\sum_{j=1}^{mn_i} P_{n_i}{}^j = \sum_{j=1}^{n_i} P_{n_i}{}^j \quad . \tag{30}$$

Returning to eq. 18, we see that $P^n = -I_n$ implies $P_{n_i}{}^n = -I_{n_i}$,

$i = 1,\ldots,s$ so that each P_{n_i} is a skew circulant and n equals an odd multiple of n_i. Therefore, by eq. 18, again

$$\begin{aligned}
\det \sum_{j=1}^{n} P^j &= \det \sum_{j=1}^{n} \operatorname{diag}(P_{n_1},\ldots,P_{n_s})^j \\
&= \prod_{i=1}^{s} \det \sum_{j=1}^{n} P_{n_i}{}^j \\
&= \prod_{i=1}^{s} \det \sum_{j=1}^{n_i} P_{n_i}{}^j \\
&= (-1)^n 2^{n-s}
\end{aligned}$$

where the last two equations follow directly from eq.'s 30 and 29 respectively. But eq. 29 also implies above that the left hand side equals $(-1)^n 2^{n-1}$. Therefore s = 1 and Theorem 8 is proved.

7. New Results on Group Matrices and Symmetric Circulants.

In what follows, the letters i, u, p, d, s stand for integral, unimodular, positive, definite, symmetric, respectively. With this notational convention Theorem 8 (Theorem 7) states that an pdiu (skew) circulant of the form $A'A$ where A is iu equals $C'C$ where C is an iu (skew) circulant. In view of this it would be interesting to note for what values of n are pdiu (skew) circulants of the form $C'C$ where C is an iu (skew) circulant.

So far, very little is known about this for circulants of degree $n > 13$. In an unpublished work E.C.Dade@ has shown it to be true for circulants of prime order less than 100, with one exception; in [6] it is shown to be false for $n = 5$ where equations 11 and 12 are used to demonstrate that the pdiu circulant $[2,1,0,-1,-1,-1,0,1]_8$ is not of the form $C'C$ where C is an iu circulant. A result of Minkowski in [5] settles the question, in general, for $n \leq 7$; that is, if A is a pdiu $n \times n$ matrix, then $A = B'B$ where B is an iu $n \times n$ matrix, $n \leq 7$. A study in [7] on the uniqueness of the normal basis for normal cyclic fields produced the result that all ui circulants are trivial for $n = 2,3,4,6$. This of course is consistent with Minkowski's result. Also for $n = 5$, an incomplete proof appears in [11] with corrections in [1]. Recently in a paper presently in press [12] R.C.Thompson solved the question for all values of n up to 13 inclusive by considering a more general problem which we shall define in section 8.

As for skew circulants nothing has been written on them. In fact I am indebted to Dr. R.C.Thompson for his conjectures on skew circulants, especially for proposing Theorem 8, the parallel to Corollary 2, and the question of the existence of nontrivial pdiu skew circulants. We shall discuss several cases in the next section.

Instead, we consider whether every nontrivial **ui** circulant is of the form P^kC where $1 \leq k \leq n$, $P = [0,1,0,\ldots,0]_n$ and C is a pdiu circulant; and additionally, if P^kC is symmetric, then either $k = 1$ or $n = 2k$. This is only a conjecture on my part. However, in consonance with it the following facts are obtained. Let G be a group of order n. Let $(c_1,\ldots,c_n)$ be the first row of a group matrix C of G defined over the ring of rational integers. Then, without ambiguity we may write $C = [c_1,\ldots,c_n]_G$.

Lemma 6. Let $C = [c_1,\ldots,c_n]_G$ be a symmetric real nonsingular group matrix with principal idempotent decomposition

$$C = s_1E_1 + \cdots + s_tE_t \tag{31}$$

and let e_i denote the row sum of the first row of E_i. Then, for $i = 1,\ldots,t$:

1) E_i is a symmetric real group matrix;
2) the diagonal element of E_i is a positive rational number equal to r_in^{-1} where r_i is the rank of E_i, the number of eigenvalues of C equal to s_i;
3) $e_i^2 = e_i$ and $e_ie_j = 0$, if $i \neq j$;
4) if eigenvalue $s_1 = c_1 + \cdots + c_n$, then $e_j = 0$ for $j \neq 1$ and $e_1 = 1$.

Note: $c_1+\cdots+c_n$ is always an eigenvalue of C.

Proof. $(E'_i)^2 = E'_i$, $i = 1,\ldots,n$ and $E'_iE'_j = 0$, $i \neq j$. Hence, since $C' = C$ and the principal idempotent decomposition of C is unique, eq.31 implies $E'_i = E_i$. It is known, e.g. see [8], that for principal idempotent decompositions a matrix which commutes with C commutes with every E_i. Therefore, since by definition, C is a left regular representation, Theorem 1 implies all matrices in the right regular representations commute with the E_i and so, by Theorem 2, the E_i are group matrices of G. This proves 1) since the E_i are real by definition of the decomposition.

The principal idempotent decomposition requires that E_i are similar to a diagonal matrix of 1's and possibly 0's. By taking the trace of E_i and the corresponding diagonal matrix and taking cognizance of 1), that is, the main diagonal of E_i is constant, 2) follows immediately. Let

$$x = \text{col}\ (1,\ldots,1)$$

be an n-tuple column vector all of whose elements equal 1. Then, since the E_i's are idempotents, 3) follows directly from 1) and the fact that $E_i^2 x = E_i x$ and $E_i E_j x = 0$. (Note: For any i, $E_i x = (e_1,\ldots,e_1)' = e_1 x$, hence $E_i^2 x = E_i(e_i x) = e_i(E_i x) = e_i e_i x$, whence $e_i = e_i^2$. These results are a consequence of the fact that the row sum of any group matrix is independent of the row.)

From eq. 31, $Cx = s_1 E_1 x + \cdots + s_t E_t x$ so, $c_1 + \cdots + c_n = s_1 e_1 + \cdots + s_t e_t$. By 3) it is possible for only one of the e_i's to be non zero, say e_1, whence the preceding equation reduces to

$$c_1 + \cdots + c_n = s_1 e_1 \quad .$$

But, since C is nonsingular the left side is non zero, so, $e_i \neq 0$. Since e_1 is a row sum of the real matrix E_1, $e_1 = e_1^2 > 0$, and this implies $e_1 = 1$.

Therefore $c_1 + \cdots + c_n = s_1$.

The next result is an integral circulant analogue of the polar factorization theorem.

Theorem 9. If A is an $n \times n$ nonsingular real group matrix then there are unique real matrices H and U such that $A = UH$ where H is a pd group matrix and U is an orthogonal group matrix.

Proof. Let $C = A'A$ be the group matrix in eq. 31 and let $H = \sqrt{s_1}E_1 + \cdots + \sqrt{s_t}E_t$ where we note that the eigenvalues s_i of C are positive since C is pd. Therefore, by 1) in Lemma 6, H is a real positive definite group matrix. Moreover,

$$A'A = H^2 \tag{33}$$

where H is the only positive definite matrix for which this is true by virtue of the uniqueness of equation 31. In [8] it is shown that for nonsingular A there are unique real matrices U and H_o such that U is orthogonal and H_o is positive definite with $A = UH_o$. But this implies $A'A = H_o^2 = H^2$ which by uniqueness of H in eq. 33, in turn implies, $H = H_o$; and therefore U is a group matrix by Corollary 1 and multiplicative closure. Following this, the terms A,H,U in Corollaries 4,5,6 are assumed to be the group matrices in Theorem 9.

Corollary 3. If det A = $\pm$ 1, then det H = 1 and det U = det A. (A,H,U are real).

Proof. By eq. 33 $(\det H)^2 = 1$, hence det H = $\pm$ 1, so, it equals + 1 since H is positive definite. Therefore det UH = det U = det A.

<u>Corollary</u> 4. A is normal iff $A = HU = UH$.

Proof. Consider the commutativity property with regard to the idempotent decomposition and the equality of H^2U and UH^2.

<u>Corollary</u> 5. If in Theorem 9, $A = [a_1,\ldots,a_n]_G$ is an integral unimodular group matrix and $U = [u_1,\ldots,u_n]_G$ and $H = [h_1,\ldots,h_n]_G$, then

$h = h_1 + \cdots + h_n > 1$ and $u_1 + \cdots + u_n = a_1 + \cdots + a_n = \pm 1$.

Proof. Let $u = u_1 + \cdots + u_n$ and $a = a_1 + \cdots + a_n$. The equation $Ax = UHx$ where x is an n-tuple column vector all of whose elements equal 1, implies $a = uh$. Since A is unimodular and integral its row sum equals ± 1; for, $xAA^{-1}x' = naa^{-1} = xI_nx' = n$. Since U is orthogonal, $u^2 = 1$, because $nu^2 = x'U'Ux = x'I_nx = n$. Consequently, $h = \pm 1$ which perforce equals $+1$ since H is positive definite.

<u>Theorem</u> 10. If A is a <u>unimodular</u> <u>integral</u> circulant then there is an integer s such that P^sA is symmetric where $P = [0,1,0,\ldots,0]_n$.

Proof. Let K be the $n \times n$ matrix

$$K = \begin{pmatrix} 0 & & & & 1 \\ & & & 1 & \\ & & \cdot^{\cdot^{\cdot}} & & \\ & 1 & & & \\ 1 & & & & 0 \end{pmatrix}$$

Then $KK = I_n$ and $KPK = P'$. Hence $KA'AK = (A'A)' = A'A$ so that AKA^{-1} is an integral orthogonal matrix, hence a generalized permutation matrix. In fact, if $Q = AKA^{-1}$ then

$$KQ = KAKA^{-1} = A'A^{-1} \tag{34}$$

so that KQ is a circulant, and being trivial implies there is an integer k such that $1 \leq k \leq n$ and $KQ = \pm P^k$. Thus by eq. 34

$$A' = \pm P^k A \ . \tag{35}$$

But since the row sum of A and A' are equal,

$$A' = P^k A. \tag{36}$$

Suppose n is odd. Let r be an integer such that $2r = 2n-k$ or $2r = n-k$ according as k is even or odd. Let s be the nonnegative integer

$$s = n-r \ , \tag{37}$$

This means $r + k = n + s$ or $r + k = s$ according as k is even or odd. Therefore by eq. 36

$$P^r A' = P^{r+k} A = P^s A \ ,$$

and so by eq. 37

$$(P^s A)' = A' P^{n-s} = A' P^r = P^r A' = P^s A,$$

which proves that $P^s A$ is symmetric.

Now suppose n is even. Since the trace of $AKA^{-1} = KP^k$ is zero on the left, it follows that the number of elements in the nontrivial diagonal(s) of P^k is zero, or what is the same k is even. Hence, letting $r = (n-k)/2$ and $s = n-r$, we get from eq. 36

$$P^r A' = P^{r+k} A = P^{r+n-2r} A = P^s A,$$

whence

$$(P^s A)' = A' P^{n-s} = A' P^r$$

and so, $P^s A$ is symmetric.

<u>Corollary</u> 6. If A is a unimodular integral circulant then there is an integer k such that $A' = P^k A$ (where k is even if n is even).

<u>Theorem</u> 11. Let A be a unimodular integral circulant. Then the eigenvalues of the symmetric matrix KA are the square roots of the eigenvalues of the positive definite circulant $A'A$.

Proof. Observe that KP^i is obviously symmetric for each $i = 1,\ldots,n$. Hence KA is symmetric. Then consider the principal idempotent decomposition of KA and $A'A = (KA)'KA$; and the proof follows.

8. Positive Definite Skew Circulants.

In this section B_n always denotes an $n \times n$ symmetric unimodular integral skew circulant.

By definition of B_n, we may write, for $k \geq 1$,

$$B_n = [b_o, b_1, b_2, \ldots, b_k, -b_k, -b_{k-1}, \ldots, -b_1]_n^- \tag{38}$$

if $n = 2k + 1$, and

$$B_n = [b_o, b_1, b_2, \ldots, b_k, 0, -b_k, -b_{k-1}, \ldots, -b_1]_n^- \tag{39}$$

if $n = 2k + 2$. Then, by eq. 16 if $B_n = A$, we get for the ith eigenvalue of B_n

$$\epsilon_i = \sum_{j=1}^{n} a_j \rho^{(2i-1)(j-1)} \tag{40}$$

which, by substitutions of the a_j's with the b's in eq. 38 or 39, yields for any $n \geq 3$,

$$\epsilon_i = b_o + \sum_{j=1}^{k} b_j \rho^{(2i-1)j} - \sum_{j=1}^{k} b_j \rho^{(2i-1)(n-j)} \tag{41}$$

<u>Lemma</u> 7. If B_n is the symmetric $n \times n$ skew circulant given by eq.'s 38 or 39, where $n = 2k+1$ or $2k+2$ then it's eigenvalues are given by

$$\epsilon_i = b_o + \sum_{j=1}^{k} b_j (\rho^{(2i-1)j} - \rho^{(2i-1)(n-j)}) \tag{42}$$

$i = 1,\ldots,n$ and

$$\epsilon_i = \epsilon_{n-i+1} \tag{43}$$

for $i = 1,2,\ldots,k+1$.

Proof. Eq. 42, of course, follows directly from eq. 41. Eq. 43 follows from eq. 39 and the fact that the eigenvalues of a symmetric real matrix are all real. For, $\rho^{2(n-i+1)-1} = \rho^{1-2i}$ and so, by substituting $n - i + 1$ for i in eq. 40 we get,

$$\epsilon_{n-i+1} = \sum_{j=1}^{n} a_j \rho^{(1-2i)(j-1)}$$

and so, by comparing this with eq. 40, $\epsilon_i = \bar{\epsilon}_i = e_{n-i+1}$ for $i = 1,\ldots,k+1$, whether n is odd or even. This evidently implies

<u>Lemma</u> 8. For $n \geq 3$

$$\det B_n = (\epsilon_1 \epsilon_2 \cdots \epsilon_k)^2 \epsilon(n) = \pm 1$$

where

$$\epsilon(n) = \begin{cases} \epsilon_{k+1}^2 & , \text{ if } n = 2k+2 \\ \epsilon_{k+1} & , \text{ if } n = 2k+1 \end{cases} .$$

Given a square matrix A we denote its trace by tr(A). From eq. 15 where $A=B_n$ and eq. 43 we have

Lemma 9. For $n \geq 3$

$$tr(B_n) = nb_o = 2 \sum_{i=1}^{k} \epsilon_i + \delta(n)$$

where $\delta(n) = \begin{cases} 2\epsilon_{k+1}, & \text{if } n = 2k + 2 \\ \epsilon_{k+1}, & \text{if } n = 2k + 1 \end{cases} .$

Lemma 10. If $n = 2k+1$ and $A_n = [a_1, \ldots, a_n]_n^-$ is a unimodular integral skew circulant with eigenvalues defined as in eq. 15, then

$$\epsilon_{k+1} = a_1 + \sum_{j=2}^{n} (-1)^{j-1} a_j = \pm 1.$$

Proof. By eq. 16, keeping in mind that $\rho^n = -1$, we get

$$\epsilon_{k+1} = a_1 + \sum_{j=2}^{n} a_j \rho^{(2k+1)(j-1)}$$
$$= a_1 + \sum_{j=2}^{n} (-1)^{j-1} a_j \ .$$

Therefore, ϵ_{k+1} is a rational integer; similarly with ϵ_{k+1}^{-1}, the k+1 eigenvalue of the inverse of A_n, which as with A_n is a unimodular integral skew circulant. Therefore, since ϵ_{k+1} divides 1 [illegible], $\epsilon_{k+1} = \pm 1$ as desired.

Corollary 7. If n = 2k+1, B_n is as in eq. 38 then

$$\epsilon_{k+1} = b_o + 2 \sum_{j=1}^{k} (-1)^j b_j = \pm 1.$$

Proof. Since B_n by definition is symmetric the corollary follows directly from Lemma 10.

We now proceed to show for which values of n is B_n trivial or nontrivial. Obviously it is trivial for n = 1,2.

Case 3: $$B_3 = I_3 \ .$$

Proof. Let $B_3 = [a,b,-b]_3^-$. By Lemma 7 and

$$\epsilon_1 = a + b\ (\rho - \rho^2)$$

$$\epsilon_2 = a - 2b = 1$$

and so, since $-1 + \rho - \rho^2 = 0$, $\epsilon_1 = a + b$, whence, by Lemma 8

$$\det B_3 = \epsilon_1^{\,2}\,\epsilon_2 = (a + b)^2(a - 2b) = 1.$$

Therefore, $a = 1 + 2b$ implies $a + b = 1 + 3b = \pm 1$; which holds only if $b = 0$ and $a = \pm 1$. Since B_3 is pd, $a = 1$.

<u>Case</u> 4. $B_4 = [a,b,0,-b]_4^-$ is nontrivial for integral solutions of the equation $a^2 - 2b^2 = 1$ when $b \neq 0$, $a > 1$. For example $[3,2,0,-2]_4^-$.

Proof. By Lemma 7, eq. 42,

$$\epsilon_1 = a + b\ (\rho-\rho^3)$$
$$\epsilon_2 = a + b\ (\rho^3-\rho^9) = a + b\ (\rho^3-\rho)$$

and so, since $(\rho-\rho^3)^2 = 2$, by Lemma 2,

$$\det B_4 = (\epsilon_1\epsilon_2)^2 = (a^2 - 2b^2)^2 = 1$$

we have $a^2 - 2b^2 = \pm 1$ which equals $+ 1$ since $\epsilon_1\epsilon_2 > 0$.

Conversely if a and b are solutions such that $a > 0$, $b \neq 0$. Then $a^2 > 2b^2$ implies $a > \pm\sqrt{2}b$ so that $a \pm \sqrt{2}b > 0$ and hence $\epsilon_1, \epsilon_2 > 0$. Therefore B_4 is a pdsiu skew circulant and nontrivial.

<u>Case</u> 5. $B_5 = [a,b,c,-c,-b]_5^-$ is nontrivial iff a,b,c are solutions to

$$a^2 - 4bc = 1 \qquad (44)$$

$$(b-c)(1+b-c) = bc \qquad (45)$$

where $a > 1$. For example $[3,2,1,-1,-2]_5^-$.

Proof. By Lemma 7 and Corollary 7

$$\begin{aligned} \epsilon_1 &= a + b\lambda_1 - c\lambda_2 \\ \epsilon_2 &= a + b\lambda_2 - c\lambda_1 \\ \epsilon_3 &= a - 2b + 2c = 1 \end{aligned} \tag{46}$$

where $\lambda_1 = \rho-\rho^4$ and $\lambda_2 = \rho^3-\rho^2$ and ρ is the 10th primitive root of unity. Using the fact that $-1 + \rho - \rho^2 + \rho^3 - \rho^4 = 0$ a straight forward computation will show that $\epsilon_1\epsilon_2$ is an integer and hence from Lemma 8 $\epsilon_1\epsilon_2 = 1$; indeed,

$$\epsilon_1\epsilon_2 = a^2-b^2-c^2 + ab-ac-3bc = 1.$$

But

$$\begin{aligned} 4\epsilon_1\epsilon_2 + \epsilon_3^2 &= 5a^2-20bc = 5 \\ \epsilon_3 - \epsilon_1\epsilon_2 &= 5(b^2+c^2 - ab+ac - bc) = 0. \end{aligned} \tag{47}$$

The latter equation gives

$$(b-c)(b-c-a) = -bc$$

which reduces to

$$(b-c)(1+b-c) = bc$$

by eq. 46. Eq. 47 implies that if B_5 is nontrivial then $a > 1$.

Conversely if a,b,c are integral solutions to eq.'s 44 and 45 such that $a > 1$, then B_5 is a nontrivial pd unimodular skew circulant. For,

$$4\epsilon_1\epsilon_2 + \epsilon_3^2 = 5a^2 - 20bc$$

which by equation 44 equals 5. Thus solving for the integer $\epsilon_1\epsilon_2$ we get $\epsilon_1\epsilon_2 = 1$. Hence by Corollary 7, $\epsilon_3 = \pm 1$ and so by Lemma 8 B_5 is unimodular; moreover, since 5 divides the difference $\epsilon_3 - \epsilon_1\epsilon_2 = \epsilon_3 - 1$, $\epsilon_3 = 1$; which is eq. 46. To show that all the eigenvalues of B_5 are positive we note that λ_1 and λ_2 are the roots of the polynomial $\lambda(x) = x^2 - x - 1$ which means

$$\lambda_1 = \frac{1-\sqrt{5}}{2} \;,\quad \lambda_2 = \frac{1+\sqrt{5}}{2} \;.$$

So that

$$\epsilon_1 = a + \frac{b-c}{2} - \frac{b+c}{2}\sqrt{5}$$

$$\epsilon_2 = a + \frac{b-c}{2} + \frac{b+c}{2}\sqrt{5} \;.$$

We must show $a + \frac{b-c}{2} > \pm \frac{b+c}{2}\sqrt{5}$. By eq. 44, since $a > 1$, $bc > 0$ and so by eq. 45 $b-c > 0$. Hence we only need to show $a + \frac{b-c}{2} < \frac{b+c}{2}\sqrt{5}$ is false when $b,c > 0$. By squaring both sides and transposing terms we get

$$a^2 + a(b-c) < (b-c)^2 - bc \;.$$

But the right hand side is negative according to eq. 45. This is a contradiction. Hence $\epsilon_1, \epsilon_2 > 0$ and so, B_5 is pd.

Case 6. $B_6 = [a,b,c,0,-c,-b]_6^-$ is nontrivial iff a,b,c are integral solutions of the equations

$$a - 2c = 1 \tag{48}$$

$$\left(\frac{3a-1}{2}\right)^2 - 3b^2 = 1 \tag{49}$$

where $a > 1$. For example $[5,4,2,0,-2,-4]_6^-$.

Proof. We have by Lemma 7

$$\epsilon_1 = a+b(\rho-\rho^5) + c(\rho^2-\rho^4)$$

$$\epsilon_2 = a-2c$$

$$\epsilon_3 = a-b(\rho-\rho^5) + c(\rho^2-\rho^4).$$

But by Lemma 9 and eq. 43 in Lemma 7

$$\mathrm{tr}(B_6) = 6a = 4(a+c(\rho^2-\rho^4)) + 2(a-2c)$$

implies

$$c = c(\rho^2-\rho^4) .$$

To show $c \neq 0$. Let $H_6 = [1,0,-1,0,1,0]_6^-$. Then

$$\begin{aligned} B_6H_6B_6^{-1} &= (B_6H_6)B_6^{-1} \\ &= (a-2c)H_6B_6^{-1} \\ &= H_6 . \end{aligned}$$

Since B_6^{-1} is an integral matrix $a-2c$ divides one, and so,

$$\epsilon_2 = a-2c = 1$$

since B_6 is pd. Therefore, if $c = 0$, $B_6 = I_6$. It follows that $\rho^2-\rho^4 = 1$, and so,

$$\epsilon_1\epsilon_3 = (a+c)^2 - 3b^2. \tag{50}$$

By Lemma 8, $\epsilon_1\epsilon_3 = 1$.

Conversely, suppose a,b,c satisfy equations 48 and 49 such that $a > 1$. Then $a-2c = 1$ implies $c \neq 0$ so that

$$\rho^4-\rho^2+1=0 . \tag{51}$$

Therefore, $\epsilon_1\epsilon_3$ equals one by eq. 49 so that by Lemma 8, B_6 is unimodular.

A solution to eq. 51 is $\rho = \frac{i+\sqrt{3}}{2}$ which is a 12th primitive root of unity. Thus $\rho^5 = \frac{i-\sqrt{3}}{2}$ implies

$$\epsilon_1 = a+\sqrt{3}b + c$$

$$\epsilon_3 = a-\sqrt{3}b + c.$$

By eq. 48, $c > 0$ and hence by eq. 50 it follows that

$$a + c > \pm\sqrt{3}b$$

so that $\epsilon_1, \epsilon_3 > 0$. This proves that B_6 is pd.

Case 7. For $A_7 = [a,b,c,d,-d,-c,-d]_7^-$ the only facts known are:

$$\epsilon_1 = a + b\eta_1 - c\eta_2 + d\eta_3$$

$$\epsilon_2 = a + b\eta_3 - c\eta_1 + d\eta_2$$

$$\epsilon_3 = a + b\eta_2 - c\eta_3 + d\eta_1$$

where $\eta_1 = \rho-\rho^6$, $\eta_2 = \rho^5-\rho^2$, $\eta_3 = \rho^3-\rho^4$, are solutions of the equation

$$x^3 - x^2 - 2x + 1$$

and $\eta_1 - \eta_2 + \eta_3 = 1$ when ρ is the 14th primitive root of unity. A solution of the cubic equation is

$$\frac{1}{3} + \left(\frac{2}{3}\sqrt{7}\right)\cos\left(\frac{1}{3}\cos^{-1}\left(\frac{1}{2\sqrt{7}}\right)\right).$$

Result: We have shown that $[3,2,0,-2]_4$, $[3,2,1,-1,-2]_5$, and $[5,4,2,0,-2,-4]_6$ are positive definite unimodular skew circulants. The diagonal elements 3,3,5 in these matrices are minimal for this class of nontrivial matrices. Hence it is impossible for these matrices to be of the form $C'C$ where C is a nontrivial unimodular positive definite integral skew circulant since the diagonal elements of $C'C$ would otherwise exceed 3,3,5.

9. Appendix.

Let $C = \begin{pmatrix} m & n \\ n & m \end{pmatrix}$ where m and n are integers. Then $m + n$ and $m - n$ are square integers if and only if there is a unique matrix A of rational integers of the form $\begin{pmatrix} r & s \\ s & r \end{pmatrix}$ such that $C = A'A$. This comes as direct consequence of the fact: The relatively prime solutions of the equation $x^2 + y^2 = z^2$ with y even are $x = r^2 - s^2$, $y = 2rs$, $z = r^2 + s^2$, where $r > s > 0$, $(r,s) = 1$.

The above proposition can be violated, if the conditions on m and n are relaxed. For example

$$\begin{pmatrix} 65 & 60 \\ 60 & 65 \end{pmatrix} = \begin{pmatrix} 8 & 1 \\ 7 & 4 \end{pmatrix} \begin{pmatrix} 8 & 7 \\ 1 & 4 \end{pmatrix} .$$

The case for 2×2 skew circulants turns out to be trivial.

BIBLIOGRAPHY

1. E.C.Dade and O. Taussky, Some new results connected with matrices of rational integers, Proc. Symposium in Pure Math. of the Am.Math.Soc., 8(1965), 78-88.

2. G. Higman, The units of group rings, Proc.London Math.Soc., 46 (1940), 231-248.

3. D. Hilbert, Theorie des corps de nombres algebriques,Paris,(1913),164.

4. M. Kneser, Klassenzahlen definites Quadratischer Formen, Archiv der Mathematik, VIII (1957), 241-250.

5. H. Minkowski, Grundlagen fur eine theorie der quadratischen Formen mit ganzzahliget Koeffizienten, Gesammelte Abhandlungen 1 (1911),3-144.

6. M. Newman and O. Taussky, Classes of Positive Definite Unimodular Circulants, 9 (1956), 71-73.

7. M. Newman and O. Taussky, On a generalization of the normal basis in abelian algebraic number fields, Comm. on Pure and Applied Math. 9 (1956), 85-91.

8. S. Perlis, The Theory of Matrices, Cambridge 1952.

9. O. Taussky, Matrices of rational integers, Bull.Amer.Math.Soc.,66 (1960), 327-345.

10. O. Taussky, Normal matrices in some problems in algebraic number theory, Proc. Intern. Congress, Amsterdam, 1954.

11. O. Taussky, Unimodular integral circulants, Math. Z., 63 (1955),286-289.

12. R.C.Thompson, Classes of Definite Group Matrices, Pac.Journ.of Math.

13. R.C.Thompson, Normal Matrices and the Normal Basis in Abelian Number Fields, 12 (1962), 1115-1124.

14. R.C.Thompson, Unimodular Group Matrices with Rational Integers as Elements, 14(1964), 719-726.