PACIFIC JOURNAL OF MATHEMATICS
Vol. 43, No. 3, 1972

CLASSES OF UNIMODULAR ABELIAN GROUP MATRICES

DENNIS GARBANATI AND ROBERT C. THOMPSON

Let G be a finite abelian group, let G_0 be the set of unimodular group matrices for G with rational integer entries, let G_1 be the symmetric members of G_0, and G_2 the positive definite symmetric members of G_0. Let K be either G_1 or G_2. On K impose the equivalence relation of group matrix congruence by asserting $A \sim B$ (for $A, B \in K$) if and only if $C \in G_0$ exists such that $A = CBC^{\mathscr{T}}$, where $^{\mathscr{T}}$ denotes transposition. M. Newman has estimated the number of classes under this equivalence relation, when G is cyclic. In this paper his study is continued for abelian groups. As part of the results it is shown that the class number of K is always a power of two, and when K is G_1 the exact value of this class number is obtained. When K is G_2 an upper bound for class number is found and shown to be sharp by exhibiting an infinite class of groups for which it is achieved.

We now give a more detailed summary of our results. Let the abelian group G have order n and for $g \in G$ let $g \to P(g)$ be the regular representation of G into the group of n-square permutation matrices. Let $\mathfrak{A}$ denote the enveloping algebra over the complex numbers $\mathfrak{C}$ of the permutation matrices $P(g)$, that is,

$$\mathfrak{A} = \left\{\sum_{g \in G} a_g P(g) \,|\, a_g \in \mathfrak{C}\right\} .$$

The group matrices for G are by definition the elements of $\mathfrak{A}$. When G is a cyclic group, the elements of $\mathfrak{A}$ are circulants. Mostly we shall be concerned with the subring $\mathfrak{A}_0$ consisting of those elements of $\mathfrak{A}$ whose entries lie in the rational integers Z. Within $\mathfrak{A}_0$ lie the groups G_0, G_1, G_2 consisting respectively of the unimodular, symmetric unimodular, and positive definite symmetric unimodular elements of $\mathfrak{A}_0$.

If $A, B \in K$ and $A \sim B$ we say A and B are G-congruent. The number of G-congruence classes in K is known [5, 8] to be finite, and upper bounds and exact values for these class numbers in a number of special cases may be found in [5, 6, 9].

In another direction, the rank of the group G_2 is given in [1] in the special case when G is cyclic. Estimates of the rank of G_0 for cyclic G were previously obtained in [5]. However, in earlier work [4] the rank of G_0 (for all abelian G) was essentially determined, although an explicit formula was not given.

In this paper we shall compute the rank of all three groups G_0,

G_1, G_2. Then we shall show that the number of G-congruence classes in K is a power of two, and, using our knowledge of the rank, we shall compute the precise power of two in the case $K = G_1$, and we shall estimate from above the power of two when K is G_2. Next, we exhibit a class of groups for which this estimate gives the exact result. Other results that will be obtained include an interesting analogue of the polar factorization theorem, valid within G_0. At the end of the paper we summarize the corresponding results for the group of unimodular integral skew circulants. (The congruence classes within this group were recently studied in [3].)

We wish to acknowledge that the results of §§2–4 in the special case when G is a cyclic have also been obtained by M. Newman, and will appear in a forthcoming book by him.

1. Notation. The entries of the group matrix A will henceforth be in Q (the rational numbers) and usually in Z (the rational integers). Let $\hat{G}$ denote the group of complex valued characters on G and let χ denote the typical character. Of course, $\hat{G}$ is isomorphic to G. Let

$$A = \sum_{g \in G} a_g P(g) \in \mathfrak{A} . \tag{1}$$

For definiteness we let P be the left regular representation of G. Using the elements of G to index the rows and columns of P, it then follows that the (k, h)-entry of $P(g)$ is one if $gh = k$, and zero if $gh \neq k$. Let Ω denote the matrix

$$\Omega = (\chi(g))_{\chi \in \hat{G}, g \in G} .$$

Here the rows of Ω are indexed by the characters $\chi \in \hat{G}$ and the columns are indexed by the group elements $g \in G$. Then the matrix $U = n^{-1/2}\Omega$ is unitary and furthermore $UAU^* = UAU^{-1}$ is a diagonal matrix in which the diagonal entries (the eigenvalues of A) are the numbers λ_χ defined by

$$\lambda_\chi = \lambda_\chi(A) = \sum_{g \in G} a_g \chi(g) , \quad \chi \in \hat{G} . \tag{2}$$

We may write this relation as

$$(\cdots, \lambda_\chi(A), \cdots)^{\mathcal{T}} = \Omega(\cdots, a_g, \cdots)^{\mathcal{T}} \tag{3}$$

where the vector on the left-hand side has the λ_χ as entries and the vector on the right-hand side has the a_g as entries.

Notice that each character χ determines and is completely determined by the entries in a particular row of Ω.

Let $G = \langle g_1 \rangle \times \cdots \times \langle g_k \rangle$ be the direct product of cyclic groups $\langle g_1 \rangle, \cdots, \langle g_k \rangle$ of orders $n_1, \cdots, n_k$ respectively. Define the basic characters χ_t by

$$\chi_t(g_t) = \exp(2\pi i/n_t) , \qquad \chi_t(g_j) = 1 \quad \text{for} \quad j \neq t ;$$

$t = 1, \cdots, k$. The typical character $\chi \in \hat{G}$ is then uniquely representable as

$$\chi = \chi_1^{e_1} \cdots \chi_k^{e_k}$$

where $e_1, \cdots, e_k$ are integers with $0 \leqq e_t < n_t$, $t = 1, \cdots, k$. Analogously the typical element g of G has the form

$$g = g_1^{e_1} \cdots g_k^{e_k}$$

where again $0 \leqq e_t < n_t$, for $t = 1, \cdots, k$.

The symbol A^* will denote the complex conjugate transpose of matrix A.

2. The ranks of the groups G_0, G_1, G_2.

LEMMA 1. *Rank* $G_0 =$ *rank* $G_1 =$ *rank* $G_2 < \infty$.

Proof. If $A \in G_0$ then each eigenvalue of A is a unit in a cyclotomic number field, hence G_0 is contrained in the direct product of a number of groups of finite rank, hence rank $G_0 < \infty$. (See [5].) We clearly have $G_0 \supseteqq G_1 \supseteqq G_2$. It will suffice to find an exponent m such that $G_2 \supseteqq G_0^m$. Let $A \in G_0$. Then each eigenvalue $\lambda_\chi(A)$ of A is a unit in the algebraic integer ring of the cyclotomic field $Q(\zeta_n)$. Here $\zeta_n = e^{2\pi i/n}$. It is known [10] that an exponent m exists such that for any unit u in $Q(\zeta_n)$, the unit u^m is real and positive. Thus each eigenvalue of A^m is real and positive. Since A^m is a real normal matrix, if it has positive real eigenvalues it must be symmetric and definite. Thus $A^m \in G_2$.

If $A \in G_0$ then each eigenvalue $\lambda_\chi(A)$ is a unit in $Q(\zeta_n)$. But these eigenvalues are not independent of one another, since any conjugate of $\lambda_\chi(A)$ under an automorphism of $Q(\zeta_n)$ will also be an eigenvalue of A. We wish to identify the conjugacy classes of the eigenvalues of $\lambda_\chi(A)$ of A. For this we use formula (2).

First we observe that if character χ has order d (as a member of the group $\hat{G}$) then for each $g \in G$, the cemplex number $\chi(g)$ is a d^{th} root of unity. Furthermore, for at least one $g \in G$ the complex number $\chi(g)$ is a primitive d^{th} root of unity. For the map $g \rightarrow \chi(g)$ is a homomorphism from G into the complex number field and so the range of χ, as group in this field, is a cyclic group. Let $g_0 \in G$ be such that $\chi(g_0)$ generates the range of χ. Then the order of χ in $\hat{G}$ is the order of $\chi(g_0)$ in the multiplicative group of $\mathfrak{C}$. Thus $\chi(g_0)$ is a primitive d^{th}

root of unity. Because at least one entry of the vector $(\cdots, \chi(g), \cdots)_{g \in G}$ (a row of Ω) has order d, the conjugates of this vector (obtained by applying to the entries the automorphisms of the field $Q(\zeta_d)$) are exactly $\varphi(d)$ in number. Consequently it follows that each character χ of order d belongs to a class of $\varphi(d)$ distinct conjugate characters.

From each such class of conjugate characters select one representative character. We call these selected characters the *independent characters*, and as χ ranges over the independent characters we call the associated eigenvalues $\lambda_\chi(A)$ the *independent eigenvalues* of A.

How many independent characters (or eigenvalues) are there? Each independent character of order d belongs to a class of $\varphi(d)$ characters, each having order d. Let $\mathcal{O}(d)$ denote the number of elements of order d is $\hat{G}$. The elements of order d in $\hat{G}$ thus produce exactly $\mathcal{O}(d)/\varphi(d)$ independent characters. We may make this calculation for each $d \mid n$. It is a simple matter to see that $\mathcal{O}(d)/\varphi(d) = N(d)$, where $N(d)$ denotes the number of cyclic subgroups of order d in G. We thus arrive at the following conclusion.

LEMMA 2. *The independent eigenvalues of A are in one-to-one correspondence with the cyclic subgroups of G.*

If we know the values of the independent eigenvalues of the group matrix A (for which the entries are in Q) then the values of all other eigenvalues of A are determined. Conversely, suppose we assign to each independent eigenvalue λ_χ an arbitrary value from the field $Q(\zeta_d)$ (where d is the order of χ) and use the conjugacy relations to determine from these independent eigenvalues values to be assigned to the nonindependent eigenvalues. Rewriting (3) as

$$(4) \qquad (\cdots, a_g, \cdots)^\tau = n^{-1}\Omega^*(\cdots, \lambda_\chi, \cdots)^\tau$$

we may determine a group matrix A which has the assigned λ_χ as its eigenvalues. We claim that this A must have rational numbers as entries. From (4) we see that

$$\begin{aligned} a_g &= n^{-1} \sum_{\chi \in \hat{G}} \bar{\chi}(g)\lambda_\chi \\ &= n^{-1} \sum_1 \sum_2 \bar{\chi}(g)\lambda_\chi \end{aligned}$$

where, for a fixed independent character χ, the sum $\sum_2$ is over all characters conjugate to it, and $\sum_1$ is the sum over the different independent characters. Since the λ_χ take conjugate values in exactly the same manner as the χ do, the sum $\sum_2$ is fixed under each automorphism and therefore is a rational number. Consequently, a_g is a sum of rational numbers and hence $a_g \in Q$.

Let G_{-1} denote the set of group matrices A having rational entries, obtained as follows. For each independent character χ let λ_χ be an arbitrary unit in the group of units of the algebraic integer ring of the number field $Q(\zeta_d)$, d being the order of χ. Use the conjugacy relations to obtain values to assign to the remaining λ_χ. Let G_{-1} be the group matrices with rational entries obtained in this way. Thus G_{-1} is isomorphic to a direct product of N abelian groups, where N is the number of cyclic subgroups of G. Let us compute the rank of G_{-1}. This rank is the sum of the ranks of the constituent direct factors of G_{-1}, and the constituent direct factor associated with λ_χ has rank

$$\frac{1}{2}\varphi(d) - 1 \quad \text{if} \quad d > 2\,, \quad 0 \quad \text{if} \quad d = 1 \quad \text{or} \quad 2\,. \tag{5}$$

The number (5) contributes to the sum giving the rank of G_{-1} precisely as many times as there are cyclic subgroups in G of order d. This yields Lemma 3.

LEMMA 3. *Rank* $G_{-1} = r$ *where*

$$r = \sum_{\substack{d \mid n \\ d>2}} \left(\frac{1}{2}\varphi(d) - 1\right) N(d)\,. \tag{6}$$

Here $N(d)$ denotes the number of cyclic subgroups in G of order d.

We are now ready to prove our first main result.

THEOREM 1. *The common rank of the groups* G_0, G_1, G_2 *is the number* r *given by* (6).

Proof. Clearly G_0 is a subgroup of G_{-1}, and G_{-1} has rank r. To prove that rank $G_0 = r$ it will suffice to prove that $G_{-1}^m \subseteq G_0$ for some exponent m. For this we use a device from [4]. Let R be the algebraic integer ring of $Q(\zeta_n)$, and let R' be the quotient ring $R/(n)$. Each independent eigenvalue λ_χ, being a unit in R, determines a unit in the finite group of units of the finite ring R'. Hence for some fixed exponent m we have $\lambda_\chi^m \equiv 1 \pmod{n}$. Therefore $\lambda_\chi^m = 1 + i_\chi n$ where i_χ is an algebrac integer. For the matrix A^m the associated eigenvalues are the λ_χ^m, and if we apply formula (4) to find the entries of A^m, we find that they take the form

$$n^{-1} \sum_{\chi \in \hat{G}} \bar{\chi}(g)\lambda_\chi^m = n^{-1} \sum_{\chi \in \hat{G}} \bar{\chi}(g) + \sum_{\chi \in \hat{G}} i_\chi \bar{\chi}(g)\,.$$

Here $\sum_\chi i_\chi \chi$ is an algebraic integer, and $n^{-1} \sum_\chi \chi(g) = 0$ or 1 according as g is not or is the identity. Thus the entries of A^m are algebraic integers. Since A^m has rational entries, it follows that $A^m \in G_0$ Therefore $G_{-1}^m \subseteqq G_0$, completing the proof. (This trick is taken from [4, page 238].)

3. The quotient group G_0/G_1.

THEOREM 2. *$G_0/G_1 \cong G^2$, where G^2 is the group of squares in G.*

Proof. Let $A \in G_0$, say

$$A = \sum_{g \in G} a_g P(g) , \qquad a_g \in Z . \tag{7}$$

Define a map $\sigma: G_0 \to G_0$ by $\sigma(A) = A^{-1}A^{\mathcal{T}}$. Clearly σ is a homomorphism since G_0 is abelian. Because $\lambda_\chi(AB) = \lambda_\chi(A)\lambda_\chi(B)$ and $\lambda_\chi(A^{\mathcal{T}}) = \lambda_\chi(A^*) = \overline{\lambda_\chi(A)}$, we see that

$$\lambda_\chi(\sigma(A)) = \overline{\lambda_\chi(A)}/\lambda_\chi(A) .$$

Thus $|\lambda_\chi(\sigma(A))| = 1$ for each $\chi \in \hat{G}$. We already know that $\lambda_\chi(A)$ is a unit in $Q(\zeta_n)$. Therefore $\lambda_\chi(\sigma(A))$ is a root of unity, and hence $\sigma(A)$ has finite order. In order to exploit this fact we now give the following lemma, a special case of a result in [4].

LEMMA 4. *If $B \in G_0$ has finite order then $B = \pm P(g)$ for some $g \in G$.*

Proof. There is an element $g \in G$ such that $C = \pm P(g)B$ has a positive entry in the (1, 1) position. Since the only $P(h)$, $h \in G$, which has a nonzero entry in the main diagonal is $P(e)$ (e is the identity of G) and since C is a linear combination of the $P(h)$, we see that C has a positive integer, call it c_0, as its common entry down the main diagonal. Since C has finite order each $\lambda_\chi(C)$ is a root of unity. Therefore,

$$\text{trace } C = nc_0 = |\sum_\chi \lambda_\chi(C)| \leqq \sum_\chi |\lambda_\chi(C)| = n .$$

Thus $0 < c_0 \leqq 1$, hence $c_0 = 1$, hence equality holds in this application of the triangle inequality, hence the $\lambda_\chi(C)$ are equal, and hence C is scalar. Since C is integral and unimodular, we get $C = \pm I_n$. Thus $B = \pm P(g^{-1})$, as desired.

Applying Lemma 4 to $\sigma(A)$, we see that $\sigma(A) = \pm P(h)$ for some $h \in G$. We now exclude the possibility of the minus sign. If we had $\sigma(A) = -P(h)$, then from $A^{\mathcal{T}} = -P(h)A$ we get

$$\sum_{g \in G} a_g P(g^{-1}) = -\sum_{g \in G} a_g P(gh) ,$$

or

$$\sum_{g \in G} a_g P(g^{-1}) = -\sum_{g \in G} a_{g^{-1}h^{-1}} P(g^{-1}) .$$

Thus

$$a_g = -a_{g^{-1}h^{-1}} , \quad \text{all} \quad g \in G , \tag{8}$$

since the matrices $P(g)$ are linearly independent.

Let f denote the permutation on G defined by $f\colon g \to g^{-1}h^{-1}$. Then f^2 is the identity, and hence f is a product of one cycles and two cycles. For each g fixed by f we obtain from (8) that

$$a_g = 0 \tag{9.1}$$

and for each g moved by f we obtain from (8) that

$$a_g + a_{f(g)} = 0 . \tag{9.2}$$

On A perform the elementary operations in which we add to the first column of A all the other columns of A. The common entry down the first column of the resulting matrix is $\sum_g a_g$ and this sum, by (9), equals 0. Thus A is singular, a contradiction.

Consequently $\sigma(A) = P(h)$. Suppose h is not a square in G. Then the permutation f above has no fixed points. From $A^{\mathscr{T}} = P(h)A$ we obtain (in place of (8)) the formula

$$a_g = a_{f(g)} , \quad \text{and} \quad g \neq f(g) . \tag{10}$$

Adding together, as above, all the columns of A, we see from (10) that the common entry $\sum_g a_g$ in the first column must be an even integer. Thus $\det A \equiv 0 \pmod 2$. This contradicts the unimodularity of A.

We now know that $\sigma(A) = P(h)$ and $h = g^2$ for some element $g \in G$. Since $\sigma(P(g^{-1})) = P(g^2)$, it follows that σ is a homomorphism from G_0 onto the group of all $P(g^2)$, $g \in G$. What is kernel of σ? A short calculation shows it to be G. Thus $G_0/G_1 \cong$ the group of all $P(g^2)$ for $g \in G$. This completes the proof of Theorem 2.

Theorem 2 yields the following interesting variant of the polar factorization theorem.

THEOREM 3. *Let* $A \in G_0$. *Then* $A = P(g)B$, *for some* $g \in G$ *and some* $B \in G_1$.

Proof. Let $\sigma(A) = P(g^{-2})$. Then $A^{\mathscr{T}} = P(g^{-2})A$, hence $(P(g^{-1})A)^{\mathscr{T}} = P(g^{-1})A$. Thus $B = P(g^{-1})A$ is symmetric so that $B \in G_1$. Since $A = P(g)B$, the result is at hand.

4. The class numbers.

THEOREM 4. *Let K be either G_1 or G_2. Then the number of G-congruence classes in K is $[K: G_1^2]$*

Proof. If $A, B \in K$ and are G-congruent then $B = CAC^{\mathscr{T}}$ where $C \in G_0$. By Theorem 3, $C = P(g)C_1$ where $C_1 \in G_1$. Hence $B = C_1AC_1^{\mathscr{T}} = C_1^2A$. Thus B and A are in the same residue class of A modulo G_1^2. Conversely, if $A \equiv B \bmod G_1^2$ then $A = BC_1^2$ for $C_1 \in G_1$, hence $A = C_1BC_1^{\mathscr{T}}$ and so A and B are G-congruent. Thus the number of G-congruence classes is exactly $[K: G_1^2]$.

COROLLARY 1. *If two group matrices in G_0 are G-congruent, they are G-congruent by a matrix from G_1.*

THEOREM 5. *The number of congruence classes in G_1 by elements of G_0 equals the number of congruence classes in G_1 by elements of G_1, and is 2^{r+t+1}, where r is given by* (6) *and t is the number of basis elements in the Sylow* 2 *subgroup of G.*

Proof. This number is $[G_1: G_1^2]$. The rank of G_1 is r, and hence G_1 is a direct product of its subgroup of finite order elements and r cyclic groups of infinite order. The finite order elements in G_1 are, by Lemma 4, of the form $\pm P(g)$ and in order for $P(g)$ to be symmetric, we must have $P(g) = P(g^{-1})$, that is, $g^2 = e$. Thus the finite order subgroup of G_1 is the direct product of t cyclic groups of order 2 and the group $\langle -I_n \rangle$. The only finite order element in G_1^2 is I_n. Hence the finite order part of G_1 contributes 2^{t+1} to $[G_1: G_1^2]$. The infinite order generators contribute 2^r to $[G_1: G_1^2]$. This yields the result.

THEOREM 6. *The number of congruence classes in G_2 by elements of G_0 equals the number of congruence classes in G_2 by elements of G_1 and this class number is a divisor of 2^r, where r is given by* (6).

Proof. This number is $[G_2: G_1^2]$. Now $G_1/G_2 \cong (G_1/G_1^2)/(G_2/G_1^2)$ and hence

$$[G_2: G_1^2] = [G_1: G_1^2]/[G_1: G_2] .$$

By the proof of Theorem 5, $[G_1: G_1^2] = 2^{r+t+1}$, and thus $[G_2: G_1^2]$ is a divisor of 2^{r+t+1}. Thus $[G_2: G_1^2]$ is a power of two. However, all of the group matrices of the form $\pm P(g)$ for $g^2 = e$ lie in different cosets of $G_1 \bmod G_2$. For if $g_1^2 = g_2^2 = e$ and $\pm P(g_1g_2^{-1})$ is positive definite, it follows that each eigenvalue of $\pm P(g_1g_2^{-1})$ (being a positive real root of unity) must be one, and hence $\pm P(g_1g_2^{-1}) = I_n = P(e)$. This says $g_1 = g_2$, and the $\pm$ sign is $+$. Consequently the 2^{t+1} matrices $\pm P(g)$ as g ranges over the solutions of $g^2 = e$ are distinct mod G_2. Since these matrices form a subgroup of G_1, we see that $2^{t+1} \mid [G_1: G_2]$. Thus $[G_2: G_1^2]$ is divisor of 2^r.

5. An example. One may ask how close to the actual class number is the upper estimate 2^r for the number of G-congruence classes in G_2. In some instances it is too high; as an example take G to be the cyclic group of odd prime order p. In this case $r = (p-3)/2$ and so Theorem 5 tells us that for this G the number of G-congruence classes in G_2 is a divisor of $2^{(p-3)/2}$. However, it is known (this is unpublished; see [1]) that for all $p \leqq 100$, with a single exception, the actual number of G_2 classes is one. Thus our bound is much too large in these cases.

In some cases, however, our bound 2^r is the precise number of G-congruence classes in G_2. This is so when G_2 is the direct product of cyclic groups of orders 2 and/or 4 and also when G_2 is the direct product of cyclic groups of orders 2 and/or 3, since in these cases $r = 0$, i.e., there is only one G class. Thus our estimate is exact, but in a trivial way.

In all examples heretofore known the number of G-congruence classes in G_2 is one or two. In view of this evidence it is natural to ask whether this class number can ever become larger than two.

We now give an example of a class of groups G for which the number of G-congruence classes in G_2 is exactly 2^r, and for which this number can be made arbitrarily large by selecting an appropriate group from the class.

Let H be a cyclic group of order eight and let K be an elementary abelian 2-group of order 2^t. Set $G = H \times K$. Then we claim, for this group G, that $r = 2^t$ and that the number of G-congruence classes in G_2 is

$$2^r = 2^{2^t}\,.$$

Proof. Let h, k denote the typical elements of H, K respectively. Let ψ, ρ be the typical characters on H, K respectively, and prolong them to characters on G by setting $\psi(k) = \rho(h) = 1$. Then the typical character χ on G has the form $\chi = \psi\rho$ and the typical element of G is $g = hk$. Let

$$A = \sum_{g \in G} a_g P(g) = \sum_{h \in H} \sum_{k \in K} a_{hk} P(hk)$$

belong to G_0. The matrix A is symmetric if and only if $a_g = a_{g^{-1}}$; this is equivalent to

$$a_{h^{-1}k} = a_{hk}$$

for all $h \in H$, $k \in K$. The eigenvalues of A are

$$\begin{aligned}\lambda_{\psi\rho}(A) &= \sum_h \sum_k a_{hk}\psi(h)\rho(k) \\ &= \sum_{\substack{h \\ h^2=e}} \psi(h) \sum_k a_{hk}\rho(k) + \sum_{\substack{h \\ h^2\neq e}} (\psi(h) + \psi(h^{-1})) \sum_k a_{hk}\rho(k) \,.\end{aligned} \tag{11}$$

The first $\sum_h$ denotes the sum over all h such that $h^2 = e$, the second $\sum_h$ denotes the sum over all pairs (h, h^{-1}) for which $h \neq h^{-1}$. Let

$$A_{h\rho} = \sum_k a_{hk}\rho(k) \,. \tag{12}$$

Then

$$\lambda_{\psi\rho}(A) = \sum_{\substack{h \\ h^2=e}} \psi(h)A_{h\rho} + \sum_{\substack{h \\ h^2\neq e}} (\psi(h) + \psi(h^{-1}))A_{h\rho} \,. \tag{13}$$

For fixed h, by letting ρ range over $\hat{K}$, we may view (12) as a system of linear equations in the a_{hk} for which the coefficient matrix $(\rho(k))_{\rho\in\hat{K},k\in K}$ is a nonsingular matrix with entries ± 1. $\left(\text{In fact the matrix is the Kronecker product of } t \text{ copies of } \begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}.\right)$ Thus assigning arbitrary values to the $A_{h\rho}$ yields unique a_{hk}, lying in the same field as the $A_{h\rho}$.

Let h_0 be the generator of H and ψ_0 the generator of $\hat{H}$ for which $\psi_0(h_0) = (1 + i)2^{-1/2}$. Then from (13) we obtain

$$\begin{aligned}\lambda_\rho &= A_\rho + A_{h_0^4\rho} + 2A_{h_0^2\rho} + 2A_{h_0\rho} + 2A_{h_0^3\rho} \,, \\ \lambda_{\psi_0^4\rho} &= A_\rho + A_{h_0^4\rho} + 2A_{h_0^2\rho} - 2A_{h_0\rho} - 2A_{h_0^3\rho} \,.\end{aligned}$$

Here $\lambda_\rho = \pm 1$, $\lambda_{\psi_0^4\rho} = \pm 1$ (since these numbers are units and rational). Subtracting, we find

$$\lambda_\rho - \lambda_{\psi_0^4\rho} \equiv 0 \pmod 4 \,.$$

Hence

$$\lambda_\rho = \lambda_{\psi_0^4\rho} \,, \quad A_{h_0\rho} + A_{h_0^3\rho} = 0 \,.$$

Thus also

$$\lambda_\rho = A_\rho + A_{h_0^4\rho} + 2A_{h_0^2\rho} \,. \tag{14}$$

From (13) we next get

$$\lambda_{\psi_0^2\rho} = A_\rho + A_{h_0^4\rho} - 2A_{h_0^2\rho} \tag{15}$$

and therefore (since the right-hand side of (15) is rational), we get

$$\lambda_{\psi_0^2\rho} = \pm 1 .$$

Subtracting (15) from (14) we obtain

$$\lambda_\rho - \lambda_{\psi_0^2\rho} = 4A_{h_0^2\rho} ,$$

and therefore

$$\lambda_\rho = \lambda_{\psi_0^2\rho} , \quad A_{h_0^2\rho} = 0 .$$

Define $\varepsilon_\rho = \lambda_\rho$, so that $\varepsilon_\rho = \pm 1$. We now have

$$\varepsilon_\rho = \lambda_\rho = \lambda_{\psi_0^2\rho} = \lambda_{\psi_0^4\rho} = \lambda_{\psi_0^6\rho} = A_\rho + A_{h_0^4\rho} , \tag{16}$$

$$A_{h_0^2\rho} = 0 = A_{h_0^6\rho} , \quad A_{h_0^3\rho} = -A_{h_0\rho} . \tag{17}$$

Returning to (13) we also have

$$\begin{aligned} \lambda_{\psi_0\rho} &= A_\rho - A_{h_0^4\rho} + 2^{1/2}(A_{h_0\rho} - A_{h_0^3\rho}) \\ &= (2A_\rho - \varepsilon_\rho) + 2A_{h_0\rho}\cdot 2^{1/2} . \end{aligned} \tag{18}$$

Thus $\lambda_{\psi_0\rho}$ is a unit in $Z[2^{1/2}]$ and hence has the form $\pm(1 + 2^{1/2})^\tau$. But $(1 + 2^{1/2})^\tau = \alpha + \beta\cdot 2^{1/2}$ has $\beta \equiv 0 \pmod 2$ if and only if τ is even. Therefore we must have

$$\lambda_{\psi_0\rho} = (2A_\rho - \varepsilon_\rho) + 2\cdot 2^{1/2}\cdot A_{h_0\rho} = \delta_\rho(3 + 2\cdot 2^{1/2})^{\tau_\rho} = u_\rho + 2^{1/2}v_\rho$$

where $\delta_\rho = \pm 1$, $u_\rho \in Z$, $v_\rho \in Z$. Then also

$$\lambda_{\psi_0^3\rho} = u_\rho - 2^{1/2}v_\rho = \lambda_{\psi_0^5\rho} , \quad \lambda_{\psi_0^7\rho} = u_\rho + 2^{1/2}v_\rho .$$

Next, observe (by (16)) that

$$\varepsilon_\rho = \sum_k a_k \rho(k) + \sum_k a_{h_0^4k}\rho(k) .$$

Let ρ' be a fixed character on k. Then

$$\begin{aligned} \varepsilon_\rho + \varepsilon_{\rho\rho'} &= \sum_k a_k\rho(k) + \sum_k a_{h_0^4k}\rho(k) + \sum_k a_k\rho(k)\rho'(k) + \sum_k a_{h_0^4k}\rho(k)\rho'(k) \\ &= 2\sum_{\substack{k \\ \rho'(k)=1}} a_k\rho(k) + 2\sum_{\substack{k \\ \rho'(k)=1}} a_{h_0^4k}\rho(k) . \end{aligned}$$

The last two sums here are over all k for which $\rho'(k) = 1$. Hence

$$(\varepsilon_\rho + \varepsilon_{\rho\rho'})/2 = \sum_{\substack{k \\ \rho'(k)=1}} a_k\rho(k) + \sum_{\substack{k \\ \rho'(k)=1}} a^4_{h_0k}\rho(k) .$$

Thus

$$(\varepsilon_\rho + \varepsilon_{\rho\rho'})/2 \equiv \sum_{\substack{k \\ \rho'(k)=1}} a_k + \sum_{\substack{k \\ \rho'(k)=1}} a_{h_0^4k} \pmod 2 .$$

On the right-hand side here no character other than ρ' appears. Therefore, for any character ρ and ρ_1 we have

$$(\varepsilon_\rho + \varepsilon_{\rho\rho'})/2 \equiv (\varepsilon_{\rho_1} + \varepsilon_{\rho_1\rho'})/2 \pmod 2 ,$$

and this implies that

$$\varepsilon_\rho + \varepsilon_{\rho\rho'} \equiv \varepsilon_{\rho_1} + \varepsilon_{\rho_1\rho'} \pmod 4 .$$

Consequently $\varepsilon_\rho = s(\rho')\varepsilon_{\rho\rho'}$, for all ρ, where $s(\rho') = \pm 1$ and $s(\rho')$ depends only on ρ'. Changing notation, we get

$$\varepsilon_{\rho_1\rho_2} = s(\rho_1)\varepsilon_{\rho_2} . \tag{19}$$

LEMMA 5.
(i) *$\tau_\rho \equiv \tau_{\rho'}$ (mod 2) for every $\rho, \rho' \in \hat{K}$.*
(ii) *If $\varepsilon_\rho = \varepsilon_{\rho'}$ then $\lambda_{\psi_0\rho}$ and $\lambda_{\psi_0\rho'}$ have the same sign.*

Proof.
(i) We have

$$A_{h_0\rho} = v_\rho/2 .$$

Now $A_{h_0\rho} \equiv A_{h_0\rho'}$ (mod 2) since

$$A_{h_0\rho} \equiv \sum_k a_{h_0k} \pmod 2 .$$

Therefore $v_\rho \equiv v_{\rho'}$ (mod 4). But

$$(3 + 2\cdot 2^{1/2})^\tau \equiv (-1)^\tau + (1 - (-1)^\tau)2^{1/2} \pmod 4$$

for any integer exponent τ. Thus

$$v_\rho \equiv \delta_\rho(1 - (-1)\tau_\rho) \equiv \begin{cases} 0 \pmod 4 & \text{if } \tau_\rho \equiv 0 \pmod 2 , \\ 2 \pmod 4 & \text{if } \tau_\rho \equiv 1 \pmod 2 . \end{cases}$$

Therefore (i) is proved.

We also have $2A_\rho - \varepsilon_\rho = u_\rho \equiv \delta_\rho(-1)^{\tau_\rho}$ (mod 4). Thus, if $\varepsilon_\rho = \varepsilon_{\rho'}$ then

$$\delta_\rho - \delta_{\rho'} \equiv (-1)^{\tau_\rho}2(A_\rho - A_{\rho'}) \pmod 4 .$$

Since $A_\rho \equiv A_{\rho'}$ (mod 2) we get $\delta_\rho \equiv \delta_{\rho'}$ (mod 4) and this implies $\delta_\rho = \delta_{\rho'}$. That is, (ii) holds.

Notice that, if $k \in K$, then $\lambda_{\psi\rho}(P(k)) = \rho(k)$.

Let $k_1, k_2, \cdots, k_t$ be basis elements of K and let $\rho_1, \rho_2, \cdots, \rho_t$ be the associated dual characters (that is, $\rho_i(k_j) = 1$ if $i \neq j$, $= -1$ if $i = j$). Let

$$\rho = \rho_1^{e_1} \cdots \rho_t^{e_t}, \quad e_1, \cdots, e_t = 0 \quad \text{or} \quad 1 .$$

Then from (19) we see that

$$\begin{aligned}\varepsilon_\rho &= s(\rho_1)^{e_1} \cdots s(\rho^t)^{e_t}\varepsilon \\ &= (-1)^{\sigma_1 e_1} \cdots (-1)^{\sigma_t e_t}\varepsilon\end{aligned}$$

where $\varepsilon = \pm 1$, and depends on A but not on ρ, and where $\sigma_1, \cdots, \sigma_k$ are defined by $(-1)^{\sigma_1} = s(\rho_1), \cdots, (-1)^{\sigma_t} = s(\rho_t)$. Let $A_1 = P(k_1^{\sigma_1} \cdots k_t^{\sigma_t})A$. Then

$$\begin{aligned}\varepsilon_\rho(A_1) &= \lambda_\rho(A_1) = \lambda_\rho(P(k_1^{\sigma_1} \cdots))\lambda_\rho(A) \\ &= (-1)^{e_1\sigma_1 + \cdots + e_t\sigma_t}\varepsilon_\rho(A) = \varepsilon \,.\end{aligned}$$

That is, for A_1, all ε_ρ are the same, and hence, denoting A_1 by A, we have in A that $\varepsilon_\rho = \varepsilon$, independent of ρ. Multiplying A by ε, we can assume all $\varepsilon_\rho = +1$. Thus in A we have all $\lambda_\rho = \lambda_{\psi_0^2\rho} = \lambda_{\psi_0^4\rho} = \lambda_{\psi_0^6\rho} = +1$, and all $\lambda_{\psi_C\rho}$ have the sign δ (independent of ρ) (by Lemma 5).

Next observe that $\lambda_{\psi\rho}(P(h_0^4)) = \psi(h_0^4)$. Thus

$$\lambda_\rho(P(h_0^4)) = \lambda_{\psi_C^2\rho}(P(h_0^4)) = \lambda_{\psi_0^4\rho}(P(h_0^4)) = \lambda_{\psi_0^6\rho}(P(h_0^4)) = 1 \,.$$

If $\delta = +1$ then all $\lambda_{\psi\rho}$ of A are positive. If $\delta = -1$, then in $P(h_0^4)A$ all $\lambda_\rho = \lambda_{\psi_0^2\rho} = \lambda_{\psi_0^4\rho} = \lambda_{\psi_0^6\rho} = +1$ and $\lambda_{\psi_0\rho}(P(h_0^4)A)$ has the sign of $-\delta > 0$, so that in $P(h_0^4)A$ each eigenvalue is positive. The outcome of this discussion is the following: starting with our original $A \in G_1$, we have found $\pm P(g)$, with $g^2 = e$, such that $\pm P(g)A$ has each eigenvalue positive. That is, $\pm P(g)A \in G^2$ for some g with $g^2 = e$. We summarize this as Lemma 6.

LEMMA 6. *If $A \in G_1$ then $\pm P(g)$ exists, $g \in G$ with $g^2 = e$, such that $\pm P(g)A \in G_2$.*

Since $(\pm P(g)A)B(\pm P(g)A)^{\mathscr{T}} = ABA^{\mathscr{T}}$, in computing the matrices $ABA^{\mathscr{T}}$ of the G-congruence class of a positive definite $B \in G_2$, we may do our computation using only A in G_2. Thus the number of G-congruence classes in G_2 is $[G_2 \colon G_2^2]$. Since G_2 is the direct product of r infinite cyclic groups, we easily see that $[G_2 \colon G_2^2] = 2^r$. It is easy to compute from (6) that for the group G in question we have $r = 2^t$. We have completed the proof of Theorem 7.

THEOREM 7. *If G is the direct product of a cylic group of order eight and t cyclic groups of order two, then the number of G-congruence classes in G_2 is*

$$2^r = 2^{2^t} \,.$$

6. Skew circulants. Let P be the companion matrix of the polynomial $\lambda^n + 1$. Let $C = \sum_{t=0}^{n-1} a_t P^t$ where $a_t \in Z$. The matrix C is an integral skew circulant. It may be symmetric and even positive definite symmetric. Let S_0 be the group of integral unimodular skew circulants, S_1 the group of symmetric integral unimodular skew circulants, S_2 the group of positive definite symmetric integral unimodular skew circulants. By using the techniques above, with some minor modifications, the following facts may be proved.

(i) $\operatorname{rank} S_0 = \operatorname{rank} S_1 = \operatorname{rank} S_2 = r$, where

$$r = \sum_{\substack{d \mid n \\ d \text{ odd} \\ d < n}}' \left(\frac{1}{2} \varphi(2n/d) - 1 \right). \tag{20}$$

(ii) For $A \in S_0$ the map $\sigma: A \to A^{-1}A^{\mathscr{T}}$ is a homomorphism from S_0 onto the group P^{2t}, $t = 0, 1, \cdots, n$, with kernel S_1.

(iii) Given $A \in S_0$, there exists $t \in Z$ and $B \in S_1$ such that $A = P^t B$.

Let K be either S_1 or S_2. On K define the equivalence relation of skew circulant congruence by $A \sim B$ if and only if $A = CBC^{\mathscr{T}}$ for some $C \in G_0$. Here $A, B \in K$. Then:

(iv) Two members of K congruent by an element of S_0 are also congruent by an element of S_1.

(v) When K is S_1, the number of skew circulant congruence classses is 2^{1+r} where r is given by (20).

(vi) When K is S_2, the number of skew circulant congruence classes is a divisor of 2^r, where r is given by (20).

For calculation of the number of skew circulant classes in S_2 for some values of n, see [3].

REFERENCES

1. R. Austing, *Groups of unimodular circulants*, J. Research Nat. Bur. Standards, **65B**, (1965), 313-318.
2. Daniel Lee Davis, *On the distribution of the signs of the conjugates of the cyclotomic units in the maximal real subfield of the* q^{th} *cyclotomic field, q a prime.* Thesis, California Institute of Technology. 1969.
3. D. Garbanati and R. C. Thompson, *Skew circulant quadratic forms*, J. Number Theory, to appear.
4. G. Higman, *The units of group rings*, Proc. London Math. Soc., **46** (1940), 231-248.
5. M. Newman, *Circulant quadratic forms*, Report of the Institute in the Theory of Numbers, Boulder, Colorado, 1959, 189-192.
6. M. Newman and O. Taussky, *Classes of positive definite circulants*, Canad. J. Math., **9** (1957), 71-73.
7. ———, *On a generalization of the normal basis in abelian algebraic number fields*, Comm. Pure and Appl. Math., **19** (1956), 89-91.
8. R. C. Thompson, *Classes of definite group matrices*, Pacific J. Math., **17** (1966), 175-190.
9. O. Taussky, *Unimodular integral circulants*, Math. Z., **63** (1955), 286-289.
10. E. Weiss, *Algebraic Number Theory*, McGraw Hill, 1963.

Received June 1, 1971. The preparation of this paper was supported in part by the U. S. Air Force Office of Scientific Research, under Grant 698-67.

UNIVERSITY OF CALIFORNIA, SANTA BARBARA