CLASSES OF UNIMODULAR ABELIAN GROUP MATRICES

Dennis Garbanati and Robert Charles 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 $A = CBC^\tau$, where $\tau$ 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 $g \rightarrow P(g)$ be the regular representation of $G$ into the group of $n$-square permutation matrices. Let $\mathcal{A}$ denote the enveloping algebra over the complex numbers $\mathbb{C}$ of the permutation matrices $P(g)$, that is,

$$\mathcal{A} = \left\{ \sum_{g \in G} a_g P(g) \mid a_g \in \mathbb{C} \right\}.$$

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

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 $G_0,$
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 $\chi$ denote the typical character. Of course, $\hat{G}$ is isomorphic to $G$. Let

$$A = \sum_{g \in G} a_g P(g) \in \mathbb{C}.$$  

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 $\Omega$ denote the matrix

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

Here the rows of $\Omega$ 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 $\lambda_\chi$ defined by

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

We may write this relation as

$$(\cdots, \lambda_\chi(A), \cdots)^T = \Omega(\cdots, a_g, \cdots)^T$$  

where the vector on the left-hand side has the $\lambda_\chi$ as entries and the vector on the right-hand side has the $a_g$ as entries.

Notice that each character $\chi$ determines and is completely determined by the entries in a particular row of $\Omega$.

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 \( \chi_t \) by
\[
\chi_t(g_i) = \exp\left(\frac{2\pi i}{n_t}\right), \quad \chi_t(g_j) = 1 \quad \text{for} \quad j \neq t;
\]
t = 1, \ldots, k. The typical character \( \chi \in \hat{G} \) is then uniquely representable as
\[
\chi = \chi_1^{e_1} \cdots \chi_k^{e_k}
\]
where \( e_1, \ldots, e_k \) are integers with \( 0 \leq e_i < n_t \), \( t = 1, \ldots, k \). Analogously the typical element \( g \) of \( G \) has the form
\[
g = g_1^{e_1} \cdots g_k^{e_k}
\]
where again \( 0 \leq e_i < n_t \), for \( t = 1, \ldots, k \).

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.** \( \text{Rank } G_0 = \text{rank } G_1 = \text{rank } G_2 < \infty \).

**Proof.** If \( A \in G_0 \) then each eigenvalue of \( A \) is a unit in a cyclotomic number field, hence \( G_0 \) is contained in the direct product of a number of groups of finite rank, hence rank \( G_0 < \infty \). (See [5].) We clearly have \( G_0 \supseteq G_1 \supseteq G_2 \). It will suffice to find an exponent \( m \) such that \( G_2 \supseteq G_0^m \). Let \( A \in G_0 \). Then each eigenvalue \( \lambda_x(A) \) of \( A \) is a unit in the algebraic integer ring of the cyclotomic field \( \mathbb{Q}(\zeta_n) \). Here \( \zeta_n = \exp\left(\frac{2\pi i}{n}\right) \). It is known [10] that an exponent \( m \) exists such that for any unit \( u \) in \( \mathbb{Q}(\zeta_n) \), 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 \( \lambda_x(A) \) is a unit in \( \mathbb{Q}(\zeta_n) \). But these eigenvalues are not independent of one another, since any conjugate of \( \lambda_x(A) \) under an automorphism of \( \mathbb{Q}(\zeta_n) \) will also be an eigenvalue of \( A \). We wish to identify the conjugacy classes of the eigenvalues of \( \lambda_x(A) \) of \( A \). For this we use formula (2).

First we observe that if character \( \chi \) has order \( d \) (as a member of the group \( \hat{G} \)) then for each \( g \in G \), the complex 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 \( \chi \), as group in this field, is a cyclic group. Let \( g_0 \in G \) be such that \( \chi(g_0) \) generates the range of \( \chi \). Then the order of \( \chi \) in \( \hat{G} \) is the order of \( \chi(g_0) \) in the multiplicative group of \( \mathbb{C} \). 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 \(\Omega\)) 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 \(\chi\) 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 \(\chi\) 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 \(\varrho(d)\) denote the number of elements of order \(d\) in \(\hat{G}\). The elements of order \(d\) in \(\hat{G}\) thus produce exactly \(\varrho(d)/\varphi(d)\) independent characters. We may make this calculation for each \(d | n\). It is a simple matter to see that \(\varrho(d)/\varphi(d) = N(d)\), 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 \(\lambda_\chi\) an arbitrary value from the field \(Q(\zeta_d)\) (where \(d\) is the order of \(\chi\)) and use the conjugacy relations to determine from these independent eigenvalues values to be assigned to the nonindependent eigenvalues. Rewriting (3) as

\[
(\cdots, a_g, \cdots)^T = n^{-1}\Omega^*(\cdots, \lambda_\chi, \cdots)^T
\]

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

\[
a_g = n^{-1} \sum_{\chi \in \hat{G}} \overline{\chi}(g)\lambda_\chi = n^{-1} \sum_i \sum_{\chi} \overline{\chi}(g)\lambda_\chi
\]

where, for a fixed independent character \(\chi\), the sum \(\sum_{\chi}\) is over all characters conjugate to it, and \(\sum_i\) is the sum over the different independent characters. Since the \(\lambda_\chi\) take conjugate values in exactly the same manner as the \(\chi\) do, the sum \(\sum_{\chi}\) 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 $\chi$ let $\lambda_{\chi}$ 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 $\chi$. Use the conjugacy relations to obtain values to assign to the remaining $\lambda_{\chi}$. 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 $\lambda_{\chi}$ has rank

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

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

$$
r = \sum_{d|n} \left( \frac{1}{2} \varphi(d) - 1 \right) N(d).
$$

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 $G_{-1} \subseteq G_0$ 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 $\lambda_{\chi}$, 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 $i_{\chi}$ is an algebraic integer. For the matrix $A^m$ the associated eigenvalues are the $\lambda_{\chi}^m$, and if we apply formula (4) to find the entries of $A^m$, we find that they take the form

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

Here $\sum_{\chi} i_{\chi} \overline{\chi}$ 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 $G_{m-1} \subseteq G_0$, 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

\[ A = \sum_{g \in G} a_g P(g), \quad a_g \in \mathbb{Z}. \tag{7} \]

Define a map $\sigma : G_0 \to G_0$ by $\sigma(A) = A^{-1}A^\varphi$. Clearly $\sigma$ is a homomorphism since $G_0$ is abelian. Because $\lambda_\chi(AB) = \lambda_\chi(A)\lambda_\chi(B)$ and $\lambda_\chi(A^\varphi) = \lambda_\chi(A^*) = \overline{\lambda_\chi(A)}$, 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 $Q(\zeta_m)$. 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,

\[ \text{trace } C = nc_0 = |\sum_\chi \lambda_\chi(C)| \leq \sum_\chi |\lambda_\chi(C)| = n. \]

Thus $0 < c_0 < 1$, 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 $A^\varphi = -P(h)A$ 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

(8)
\[ a_g = -a_{g^{-1}h^{-1}}, \text{ all } g \in G, \]

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

Let \( f \) denote the permutation on \( G \) defined by \( f: g \rightarrow g^{-1}h^{-1} \). 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

(9.1)
\[ a_g = 0 \]

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

(9.2)
\[ a_g + a_{f(g)} = 0. \]

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 \( A^\sigma = P(h)A \) we obtain (in place of (8)) the formula

(10)
\[ a_g = a_{f(g)}, \text{ and } g \neq f(g). \]

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 \( \det A = 0 \) (mod 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 \( \sigma \) is a homomorphism from \( G_o \) onto the group of all \( P(g^2), g \in G \). What is kernel of \( \sigma \)? A short calculation shows it to be \( G \). Thus \( G_o/G_1 \cong \text{the group of all } P(g^2) \text{ for } g \in G \). This completes the proof of Theorem 2.

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

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

Proof. Let \( \sigma(A) = P(g^{-2}) \). Then \( A^\sigma = P(g^{-2})A \), hence \( (P(g^{-1})A)^\sigma = P(g^{-1})A \). 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 $[K: G_1^r]$.

*Proof.* If $A, B \in K$ and are $G$-congruent then $B = CAC^{-\sigma}$ where $C \in G_1$. By Theorem 3, $C = P(g)C$, where $C \in G_1$. Hence $B = C_1AC_1^{-\sigma} = C_1A$. Thus $B$ and $A$ are in the same residue class of $A$ modulo $G_1^r$. Conversely, if $A \equiv B \mod G_1^r$ then $A = BC_1^r$ for $C_1 \in G_1$, hence $A = C_1BC_1^{-\sigma}$ and so $A$ and $B$ are $G$-congruent. Thus the number of $G$-congruence classes is exactly $[K: G_1^r]$.

**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 $[G_1: G_1^r]$. 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 $\{ -I_n \}$. The only finite order element in $G_1^r$ is $I_n$. Hence the finite order part of $G_1$ contributes $2^{t+1}$ to $[G_1: G_1^r]$. The infinite order generators contribute $2^r$ to $[G_1: G_1^r]$. 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 $[G_2: G_2^r]$. Now $G_1/G_2 \cong (G_1/G_1^r)/(G_2/G_2^r)$ and hence

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

By the proof of Theorem 5, $[G_1: G_1^r] = 2^{r+t+1}$, and thus $[G_2: G_1^r]$ is a divisor of $2^{r+t+1}$. Thus $[G_2: G_1^r]$ 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 $G_1 \mod G_2$. 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 \( \pm P(g g_0^{-1}) = I_n = P(e) \). 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 \( G_2 \), we see that \( 2^{t+1} | [G_1: G_2] \). Thus \( [G_2: G_1] \) 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 \( p \leq 100 \), 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 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 \( \psi, \rho \) 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 \( \chi \) 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
for all \( h \in H, k \in K \). The eigenvalues of \( A \) are

\[
\lambda_{\psi}(A) = \sum_h \sum_k a_{hk} \psi(h) \rho(k)
\]

(11)

\[
= \sum_{h^2 = e} \psi(h) \sum_k a_{hk} \rho(k) + \sum_{h^2 \neq e} (\psi(h) + \psi(h^{-1})) \sum_k a_{hk} \rho(k) .
\]

The first \( \sum_a \) 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

\[
A_{h, \rho} = \sum_k a_{hk} \rho(k) .
\]

Then

\[
\lambda_{\psi}(A) = \sum_{h^2 = e} \psi(h) A_{h, \rho} + \sum_{h^2 \neq e} (\psi(h) + \psi(h^{-1})) A_{h, \rho} .
\]

(13)

For fixed \( h \), by letting \( \rho \) 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 \( \pm 1 \). (In fact the matrix is the Kronecker product of \( t \) copies of \( \begin{bmatrix} 1 & 1 \\ -1 & -1 \end{bmatrix} \).) 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 \( \psi_0 \) the generator of \( \hat{H} \) for which \( \psi_0(h_0) = (1 + i)2^{-1/2} \). Then from (13) we obtain

\[
\lambda_{\rho} = A_{\rho} + A_{h_0, \rho} + 2A_{h_0^2, \rho} + 2A_{h_0^2, \rho} + 2A_{h_0, \rho} ,
\]

\[
\lambda_{\psi_0}(\rho) = A_{\rho} + A_{h_0^2, \rho} + 2A_{h_0^2, \rho} - 2A_{h_0, \rho} - 2A_{h_0^2, \rho} .
\]

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

\[
\lambda_{\rho} - \lambda_{\psi_0}(\rho) \equiv 0 \pmod{4} .
\]

Hence

\[
\lambda_{\rho} = \lambda_{\psi_0}(\rho) , \quad A_{h, \rho} + A_{h_0^2, \rho} = 0 .
\]

Thus also

\[
\lambda_{\rho} = A_{\rho} + A_{h_0^2, \rho} + 2A_{h_0^2, \rho} .
\]

(14)

From (13) we next get

\[
\lambda_{\psi_0}(\rho) = A_{\rho} + A_{h_0^2, \rho} - 2A_{h_0^2, \rho}
\]

(15)

and therefore (since the right-hand side of (15) is rational), we get
\[ \lambda_{\psi^2 \rho} = \pm 1. \]

Subtracting (15) from (14) we obtain
\[ \lambda_{\rho} - \lambda_{\psi^2 \rho} = 4A_{h^2 \rho}, \]
and therefore
\[ \lambda_{\rho} = \lambda_{\psi^2 \rho}, \quad A_{h^2 \rho} = 0. \]

Define \( \varepsilon_{\rho} = \lambda_{\rho} \), so that \( \varepsilon_{\rho} = \pm 1. \) We now have

(16) \[ \varepsilon_{\rho} = \lambda_{\rho} = \lambda_{\psi^2 \rho} = \lambda_{\psi^2 \rho} = A_{\rho} + A_{h^2 \rho}, \]
(17) \[ A_{h^2 \rho} = 0 = A_{h^2 \rho}, \quad A_{h^2 \rho} = -A_{h^2 \rho}. \]

Returning to (13) we also have
\[ \lambda_{\psi^2 \rho} = A_{\rho} - A_{h^2 \rho} + 2^{1/2}(A_{h^2 \rho} - A_{h^2 \rho}) \]
\[ = (2A_{\rho} - \varepsilon_{\rho}) + 2A_{h^2 \rho} \cdot 2^{1/2}. \]

Thus \( \lambda_{\psi^2 \rho} \) 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 \( \tau \) is even.

Therefore we must have
\[ \lambda_{\psi^2 \rho} = (2A_{\rho} - \varepsilon_{\rho}) + 2 \cdot 2^{1/2} \cdot A_{h^2 \rho} = \delta_{\rho}(3 + 2 \cdot 2^{1/2})_{\rho} = u_{\rho} + 2^{1/2}v_{\rho} \]
where \( \delta_{\rho} = \pm 1, u_{\rho} \in Z, v_{\rho} \in Z. \) Then also
\[ \lambda_{\psi^3 \rho} = u_{\rho} - 2^{1/2}v_{\rho} = \lambda_{\psi^3 \rho}, \quad \lambda_{\psi^7 \rho} = u_{\rho} + 2^{1/2}v_{\rho}. \]

Next, observe (by (16)) that
\[ \varepsilon_{\rho} = \sum_k a_{k1} o(k) + \sum_k a_{h^2 k1} o(k). \]

Let \( \rho' \) be a fixed character on \( k. \) Then
\[ \varepsilon_{\rho} + \varepsilon_{\rho,\rho'} = \sum_k a_{k} o(k) + \sum_k a_{h^2 k1} o(k) + \sum_k a_{k} o(k) \rho'(k) + \sum_k a_{h^2 k1} o(k) \rho'(k) \]
\[ = 2 \sum_{\rho'(k)=1} a_{k} o(k) + 2 \sum_{\rho'(k)=1} a_{h^2 k1} o(k). \]

The last two sums here are over all \( k \) for which \( \rho'(k) = 1. \) Hence
\[ (\varepsilon_{\rho} + \varepsilon_{\rho,\rho'})/2 = \sum_{\rho'(k)=1} a_{k} o(k) + \sum_{\rho'(k)=1} a_{h^2 k1} o(k). \]

Thus
\[ (\varepsilon_{\rho} + \varepsilon_{\rho,\rho'})/2 \equiv \sum_{\rho'(k)=1} a_{k} + \sum_{\rho'(k)=1} a_{h^2 k1} \pmod{2}. \]

On the right-hand side here no character other than \( \rho' \) appears. There-
fore, for any character $\rho$ and $\rho_i$ we have

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

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 $\rho$, where $s(\rho') = \pm 1$ and $s(\rho')$ depends only on $\rho'$. Changing notation, we get

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

**Lemma 5.**

(i) $\tau_\rho \equiv \tau_{\rho'} \pmod{2}$ for every $\rho, \rho' \in \hat{K}$.

(ii) If $\varepsilon_\rho = \varepsilon_{\rho'}$ then $\lambda_{\psi_\rho}$ and $\lambda_{\psi_{\rho'}}$ have the same sign.

_**Proof.**_

(i) We have

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

Now $A_{h_0 \rho} \equiv A_{h_0 \rho'} \pmod{2}$ since

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

Therefore $v_\rho \equiv v_{\rho'} \pmod{4}$. But

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

for any integer exponent $\tau$. Thus

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

Therefore (i) is proved.

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

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

Since $A_\rho \equiv A_{\rho'} \pmod{2}$ we get $\delta_\rho \equiv \delta_{\rho'} \pmod{4}$ 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 $k_1, k_2, \ldots, k_t$ be basis elements of $K$ and let $\rho_1, \rho_2, \ldots, \rho_t$ be the associated dual characters (that is, $\rho_i(k_j) = 1$ if $i \neq j$, $-1$ if $i = j$). Let

$$\rho = \rho_{i_1} \cdots \rho_{i_t}, \quad e_i, \ldots, e_t = 0 \text{ or } 1 .$$

Then from (19) we see that
\[ \varepsilon_\rho = s(\rho_1)\varepsilon_1 \cdots s(\rho_t)\varepsilon_t \]
\[ = (-1)^{\varepsilon_1 \cdots \varepsilon_t} (-1)^{\varepsilon_1 \cdots \varepsilon_t} \]
where \( \varepsilon = \pm 1 \), and depends on \( A \) but not on \( \rho \), and where \( \sigma_1, \ldots, \sigma_k \)
are defined by \(( -1 )^{\varepsilon_1} = s(\rho_1), \ldots, (-1)^{\varepsilon_t} = s(\rho_t)\). Let \( A_1 = P(k_{i_1}^\rho \cdots k_{i_j}^\rho)A \).
Then
\[ \varepsilon_\rho(A_1) = \lambda_\rho(A_1) = \lambda_\rho(P(k_{i_1}^\rho \cdots ))\lambda_\rho(A) \]
\[ = (-1)^{\varepsilon_1 + \cdots + \varepsilon_j}\varepsilon_\rho(A) = \varepsilon . \]

That is, for \( A_1 \), all \( \varepsilon_\rho \) are the same, and hence, denoting \( A_1 \) by \( A \),
we have in \( A \) that \( \varepsilon_\rho = \varepsilon \), independent of \( \rho \). Multiplying \( A \) by \( \varepsilon \),
we can assume all \( \varepsilon_\rho = +1 \). Thus in \( A \) we have all \( \lambda_\rho = \lambda_\rho^\varepsilon = \lambda_\rho^\varepsilon = \lambda_\rho \),
and all \( \lambda_\rho \) have the sign \( \delta \) (independent of \( \rho \)) (by Lemma 5).

Next observe that \( \lambda_\rho(P(h_0^\rho)) = \psi(h_0^\rho) \). Thus
\[ \lambda_\rho(P(h_0^\rho)) = \lambda_\rho^\varepsilon = \lambda_\rho^\varepsilon = \lambda_\rho^\varepsilon = 1 . \]
If \( \delta = +1 \) then all \( \lambda_\rho \) of \( A \) are positive. If \( \delta = -1 \), then in \( P(h_0^\rho)A \)
all \( \lambda_\rho = \lambda_\rho^\varepsilon = \lambda_\rho^\varepsilon = \lambda_\rho^\varepsilon = +1 \) and \( \lambda_\rho(P(h_0^\rho)A) \) has the sign of \( -\delta > 0 \),
so that in \( P(h_0^\rho)A \) each eigenvalue is positive. The outcome of this discussion is the following:
starting with our original \( A \in C_1 \), 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 \( A \in C_1 \) then \( \pm P(g) \) exists, \( g \in G \) with \( g^2 = e \), such
that \( \pm P(g)A \in G^2 \).

Since \(( \pm P(g)A )B( \pm P(g)A )^\varepsilon = ABA^\varepsilon \), in computing the matrices
\( ABA^\varepsilon \) of the \( G \)-congruence class of a positive definite \( B \in G^2 \), we may
do our computation using only \( A \) in \( G \). Thus the number of \( G \)-congruence
classes in \( G^2 \) is \( [G^2 : G^2] \). Since \( G \) is the direct product of \( r \)
infinite cyclic groups, we easily see that \([G^2 : G^2] = 2^r \). 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 cyclic 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 \( x^n + 1 \). Let \( C = \sum_{i=0}^{n-2} a_i P^i \) where \( a_i \in Z \). 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) $\text{rank } S_0 = \text{rank } S_1 = \text{rank } S_2 = r$, where

$$r = \sum_{\substack{d | n \atop d \text{ odd}}} \left( \frac{1}{2} \varphi(2n/d) - 1 \right).$$

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

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

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 $A = CBC^\sigma$ 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 classes 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


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
Max K. Agoston, *An obstruction to finding a fixed point free map on a manifold* . . . 543
Nadim A. Assad and William A. Kirk, *Fixed point theorems for set-valued mappings of contractive type* ................................................................. 553
John Winston Bunce, *Characterizations of amenable and strongly amenable C*-algebras* ................................................................. 563
Erik Maurice Ellentuck and Alfred Berry Manaster, *The decidability of a class of AE sentence in the isols* ................................................................. 573
U. Haussmann, *The inversion theorem and Plancherel’s theorem in a Banach space* ................................................................. 585
Peter Lawrence Falb and U. Haussmann, *Bochner’s theorem in infinite dimensions* ................................................................. 601
Peter Fletcher and William Lindgren, *Quasi-uniformities with a transitive base* . . . 619
Dennis Garbanati and Robert Charles Thompson, *Classes of unimodular abelian group matrices* ................................................................. 633
Kenneth Hardy and R. Grant Woods, *On c-realcompact spaces and locally bounded normal functions* ................................................................. 647
Manfred Knebusch, Alex I. Rosenberg and Roger P. Ware, *Grothendieck and Witt rings of hermitian forms over Dedekind rings* ................................................................. 657
George M. Lewis, *Cut loci of points at infinity* ................................................................. 675
Jerome Irving Malitz and William Nelson Reinhardt, *A complete countable L^0_{\omega_1} theory with maximal models of many cardinalities* ................................................................. 691
Wilfred Dennis Pepe and William P. Ziemer, *Slices, multiplicity, and Lebesgue area* ................................................................. 701
Keith Pierce, *Amalgamating abelian ordered groups* ................................................................. 711
Stephen James Pride, *Residual properties of free groups* ................................................................. 725
Roy Martin Rakestraw, *The convex cone of n-monotone functions* ................................................................. 735
T. Schwartzbauer, *Entropy and approximation of measure preserving transformations* ................................................................. 753
Peter F. Stebe, *Invariant functions of an iterative process for maximization of a polynomial* ................................................................. 765
Kondagunta Sundaresan and Wojbor Woyczynski, *L-orthogonally scattered measures* ................................................................. 785
Kyle David Wallace, *C_\omega-groups and \lambda-basic subgroups* ................................................................. 799
Barnet Mordecai Weinstock, *Approximation by holomorphic functions on certain product sets in C^n* ................................................................. 811
Donald Steven Passman, *Corrections to: “Isomorphic groups and group rings”* . . . 823
Don David Porter, *Correction to: “Symplectic bordism, Stiefel-Whitney numbers, and a Novikov resolution”* ................................................................. 825
John Ben Butler, Jr., *Correction to: “Almost smooth perturbations of self-adjoint operators”* ................................................................. 825
Constantine G. Lascarides, *Correction to: “A study of certain sequence spaces of Maddox and a generalization of a theorem of Iyer”* ................................................................. 826
George A. Elliott, *Correction to: “An extension of some results of Takesaki in the reduction theory of von Neumann algebras”* ................................................................. 826
James Daniel Halpern, *Correction to: “On a question of Tarski and a maximal theorem of Kurepa”* ................................................................. 827