Pacific Journal of Mathematics

CLASSES OF DEFINITE GROUP MATRICES

ROBERT CHARLES THOMPSON

Vol. 17, No. 1 January 1966

PACIFIC JOURNAL OF MATHEMATICS
Vol. 17, No. 1, 1966

CLASSES OF DEFINITE GROUP MATRICES

R. C. THOMPSON

Two positive definite symmetric $n \times n$ matrices A, B with integer elements and determinant one are said to be congruent if there exists an integral C such that $B = CAC^T$ (C^T is the transpose of C). This is an equivalence relation. The number of equivalence classes, C-classes, is finite and is known for all $n \leqq 16$. Let G be a finite group of order n and let Y, Z be two positive definite symmetric group matrices for G with integral elements and determinant one. If an integral group matrix X for G exists such that $Z = XYX^T$ then Z, Y are said to be G-congruent. G congruence is an equivalence relation. In this paper the interlinking of the G-classes with the C-classes is determined for all groups of order $n \leqq 13$. The principal result is that the G-class number is two for certain groups of orders eight or twelve and is one for all other groups of order $n \leqq 13$.

Let G be a finite group with elements $g_1, g_2, \cdots, g_n$. Let $x_1, x_2, \cdots, x_n$ be variables and let X be an $n \times n$ matrix whose (i, j) element is x_k where k is determined by $g_k = g_i g_j^{-1}$. We say X is a group matrix for G. In this paper we study group matrices which have rational integers as elements. We call a matrix M integral if its elements are rational integers, unimodular if the determinant of $M = \det M = \pm 1$, symmetric if $M = M^T$ where M^T is the transpose of M. We let M^* denote the complex conjugate of M^T. The words positive, definite, symmetric, integral, unimodular are abbreviated as p, d, s, i, u, respectively. We say $pdsiu$ matrices M and M_1 are congruent if $M_1 = UMU^T$ for some iuU. Congruence is an equivalence relation on the set of $n \times n$ $pdsiu$ matrices. The number of equivalence classes (briefly: C-classes) is finite and in fact [2] is one for $1 \leqq n \leqq 7$, two for $8 \leqq n \leqq 11$, and three for $n = 12, 13$. If G is a finite group we say $pdsiu$ group matrices M and M_1 are G-congruent if $M_1 = UMU^T$ for some iu group matrix U for G. Since sums, products, inverses, and transposes of group matrices for G are still group matrices for G, G congruence is an equivalence relation on the set of $pdsiu$ group matrices for G. Not much is known about the equivalence classes (briefly: G-classes). In this paper we find all G-classes and determine their relationship with the C-classes for all groups of order $n \leqq 13$; we also get a little information for $n > 13$. Our interest in this problem stems from the following Theorem 1, proved in [8].

Received November 9, 1964.

THEOREM 1. *If a pdsiu group matrix M for G is in the principal C-class then M is in the principal G-class, when G is solvable.*

The principal class is, of course, the class containing I_n, the $n \times n$ identity matrix.

One may ask: are there any *pdsiu* group matrices for G, other than the identity?

THEOREM 2. *There exist pdsiu group matrices for G in addition to the identity precisely when G is not any of the following types of groups:*

(i) *the direct product of cyclic groups of orders two and/or four;*

(ii) *the direct product of cyclic groups of orders two and/or three;*

(iii) *the quaternion group or the direct product of the quaternion group with cyclic groups of order two.*

Proof. Combining the discussion on p. 340 of [6] with Theorem 11 of [1] shows that an *iu* group matrix for G exists which is not a permutation matrix or the negative of a permutation matrix precisely when G is not any of the groups (i), (ii), (iii). If M is an *iu* group matrix for G, not a permutation matrix or the negative of a permutation matrix, then MM^T is a *pdsiu* group matrix for G and not the identity since the (i, i) element of MM^T is the sum of squares of the integers in row i of M.

Concerning the finiteness of the G-class number, only the following fact is known.

THEOREM 3. *The G class number is finite if G is abelian.*

Proof. This follows from the argument of [3], making use of Lemma 2 of [7].

2. Two lemmas. Let $P = P_n$ be the $n \times n$ companion matrix of the polynomial $\lambda^n - 1$. Let $v = v_n = (1, 1, \cdots, 1)$ be the row n-tuple in which each entry is one.

LEMMA 1. *Let p be an odd prime and let t be an integer prime to p. Then $\lambda = 1$ is a simple eigenvalue of P_p^t, $\lambda = -1$ is not an eigenvalue, and v_p spans the eigenspace of P_p^t belonging to $\lambda = 1$.*

Proof. The eigenvalues of P_p are 1 and the $p - 1$ primitive pth roots of unity. Hence this is also true of P_p^t since ω^t is a primitive pth root of unity if ω is and $(t, p) = 1$. Thus 1 is a simple eigenvalue of P_p^t and -1 is not an eigenvalue. Since $v_pP_p = v_p$, the last assertion is immediate.

Let $\bar{\alpha}$ denote the complex conjugate of α.

LEMMA 2. *Let*

$$\begin{pmatrix}\alpha & \bar{\beta}\\ \beta & \bar{\alpha}\end{pmatrix}\begin{pmatrix}x & \bar{y}\\ y & x\end{pmatrix}\begin{pmatrix}\bar{\alpha} & \bar{\beta}\\ \beta & \alpha\end{pmatrix} = \begin{pmatrix}x_1 & \bar{y}_1\\ y_1 & x_1\end{pmatrix}$$

where α, β, y are complex numbers and x is a positive real number. Let $x^2 - |y|^2 = 1$. If $|\alpha|^2 - |\beta|^2 = 1$ then $x_1 < x$ implies $|\beta| < |y|$ and $x_1 \leqq x$ implies $|\beta| \leqq |y|$. If $|\alpha|^2 - |\beta|^2 = -1$ then $x_1 < x$ implies $|\alpha| < |y|$ and $x_1 \leqq x$ implies $|\alpha| \leqq |y|$.

Proof. The cases $\alpha = 0$ or $\beta = 0$ are easy. Let $\alpha \neq 0, \beta \neq 0$, $|\alpha|^2 - |\beta|^2 = 1$. Now $|\alpha|^2 + |\beta|^2 = 1 + 2|\beta|^2$, hence $x_1 - x = 2x|\beta|^2 + y\bar{\alpha}\bar{\beta} + \bar{y}\alpha\beta < 0$ if $x_1 < x$. Hence $0 < 2x|\beta|^2 < -y\bar{\alpha}\bar{\beta} - \bar{y}\alpha\beta$. By the triangle inequality we get $2x|\beta|^2 < 2|y||\alpha||\beta|$, hence $x^2|\beta|^2 < |y|^2|\alpha|^2 = |y|^2(1 + |\beta|^2)$, therefore $(x^2 - |y|^2)|\beta|^2 < |y|^2$, or $|\beta| < |y|$ as required. A similar computation holds when $x_1 \leqq x$ or when $|\alpha|^2 - |\beta|^2 = -1$.

An $n \times n$ circulant is, by definition, a polynomial in P_n. It is also a group matrix for the cyclic group of order n. Since P_n is unitarily diagonable, given a circulant

$$X = \sum_{i=0}^{n-1} x_i P_n^i ,$$

there exists a unitary V, independent of X, such that $VXV^* = \operatorname{diag}(\xi_0, \xi_1, \cdots, \xi_{n-1})$ where

$$\xi_i = \sum_{j=0}^{n-1} x_j \omega^{ij} , \qquad 0 \leqq j \leqq n-1 . \tag{1}$$

Here ω is a primitive nth root of unity. We make frequent use of this fact. If $Y = (Y_{ij})$ is partitioned into blocks Y_{ij} each of which is a circulant and if $W = V \dotplus V \dotplus \cdots \dotplus V$ ($\dotplus$ denotes direct sum) then each of the blocks in WYW^* is diagonalized. One may find a permutation matrix Q for which $QWYW^*Q^*$ splits into a direct sum. In the computations of §§ 4–9 some of the direct summands will again be circulants and so may themselves be unitarily diagonalized. In this manner we obtain the unitary U and the irreducible constituents of the group matrices of §§ 4–9. We also use the fact that a circulant equation like $Z = XY$ holds if and only if $\xi_i(Z) = \xi_i(X)\xi_i(Y)$ for all i.

3. The C-classes $\Phi_r \dotplus I_j$, where Φ_r does not represent one. Let Φ_r be an $r \times r$ *pdsiu* matrix (not necessarily a group matrix) such that $x\Phi_r x^T \neq 1$ for any integral vector x.

THEOREM 4. *The C-class of $\Phi_r \dotplus I_j$ does not contain any group matrix if there exists an odd prime divisor p of $r+j$ which does not divide r.*

Proof. Let $n = r + j$. Since Φ_r does not represent one, it is easy to find all integral n-tuples x for which $x(\Phi_r \dotplus I_j)x^T = 1$. The number of such x is exactly $2j$. Suppose X is a group matrix for some group G, with X in the C-class of $\Phi_r \dotplus I_j$. Then G contains an element a of order p. Let H be the cyclic subgroup of G generated by a and let $g_1H, g_2H, \cdots, g_kH$, $(k = n/p)$, be the cosets of H in G. If we take the elements of G in the order $g_1, g_1a, g_1a^2, \cdots, g_1a^{p-1}, g_2, g_2a, g_2a^2, \cdots, g_2a^{p-1}, \cdots, g_k, g_ka, g_ka^2, \cdots, g_ka^{p-1}$, then the group matrix X partitions as $X = (X_{ij})_{1 \leqq i, j \leqq k}$, where each X_{ij} is a $p \times p$ circulant. If $Q = P_p \dotplus P_p \dotplus \cdots \dotplus P_p$ then $QXQ^T = X$. Let $x = (x_1, x_2, \cdots, x_k)$ be a row n-tuple, where each x_i is a row p-tuple. If x is integral and $xXx^T = 1$ then $(xQ^\alpha)X(xQ^\alpha)^T = 1$ for $\alpha = 0, 1, 2, \cdots, p-1$. If $xQ^\alpha = xQ^\beta$ for a pair α, β with $0 \leqq \beta < \alpha < p$ then $xQ^{\alpha-\beta} = x$. This implies $x_iP_p^{\alpha-\beta} = x_i$ for $1 \leqq i \leqq k$, and by Lemma 1, $x_i = \lambda_i v_p$, $1 \leqq i \leqq k$. Since x_i is integral, λ_i is an integer. Moreover, v_p is an eigenvector of P_p, hence of any $p \times p$ circulant, hence $v_pX_{ij} = r_{ij}v_p$. Here r_{ij} is an integer (in fact the sum down any column of X_{ij}). Now

$$\begin{aligned} xXx^T &= \sum_{i,j=1}^{k} x_iX_{ij}x_j^T \\ &= \sum_{i,j=1}^{k} \lambda_i\lambda_j r_{ij} p \\ &\equiv 0 (\operatorname{mod} p) \end{aligned}$$

because $v_pv_p^T = p$. This contradicts $xXx^T = 1$, hence $xQ^\alpha = xQ^\beta$ is impossible. If $xQ^\alpha = -xQ^\beta$ then $xQ^{\alpha-\beta} = -x$, so $x_iP_p^{\alpha-\beta} = -x_i$, $1 \leqq i \leqq k$. By Lemma 1 this implies $x_i = 0$. Hence $x = 0$, a clear falsehood. Thus $\pm xQ^\alpha$ for $0 \leqq \alpha < p$ are $2p$ distinct integral solutions of $yXy^T = 1$. If y is further solution then $\pm yQ^\alpha$, $0 \leqq \alpha < p$ are also all different. If $\pm yQ^\alpha = \pm xQ^\beta$ then $y = \pm xQ^\gamma$, for some γ, $0 \leqq \gamma < p$, and this contradicts the choice of y. Thus the integral vectors representing one come in nonoverlapping sets of $2p$. We thus have $j \equiv 0 \ (\operatorname{mod} p)$. Since $r + j \equiv 0 \ (\operatorname{mod} p)$, we get $r \equiv 0 \ (\operatorname{mod} p)$, a contradiction.

Now let Φ_n (for $n \equiv 0 \ (\operatorname{mod} 4)$, $n > 4$) be the matrix on p. 331 of [5]. Then it is known that Φ_n is pdsiu and Φ_n does not represent one. Representatives of the nonprincipal C-classes up to $n = 13$ are Φ_8, $\Phi_8 \dotplus I_j$ for $1 \leqq j \leqq 5$, Φ_{12}, $\Phi_{12} \dotplus I_1$.

COROLLARY. *The only non principal $n \times n$ C-classes for $n \leqq 13$ that can contain a group matrix are the C-classes of Φ_8 and Φ_{12}.*

4. The dihedral group of order eight. The dihedral group of order $2n$ is generated by two elements a, b with $a^n = b^2 = 1, b^{-1}ab = a^{-1}$. If we take the elements in the order $1, a, a^2, \cdots, a^{n-1}, b, ba, ba^2, \cdots, ba^{n-1}$, then the group matrix X has the form

$$X = \begin{pmatrix} A & C \\ B & D \end{pmatrix} \tag{2}$$

where A, B, C, D are $n \times n$ circulants and $C = B^T, D = A^T$. If $n = 4$ and $A = x_0 I + x_1 P + x_2 P^2 + x_3 P^3, B = x_4 I + x_5 P + x_6 P^2 + x_7 P^3$, then there exists a unitary U such that $UXU^* = (\varepsilon_1) \dotplus (\varepsilon_2) \dotplus (\varepsilon_3) \dotplus (\varepsilon_4) \dotplus X_1 \dotplus X_1$ where:

$$\frac{1}{2}\begin{bmatrix} \varepsilon_1 \\ \varepsilon_2 \\ \varepsilon_3 \\ \varepsilon_4 \end{bmatrix} = \begin{bmatrix} \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & -\frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & \frac{1}{2} \end{bmatrix} \begin{bmatrix} \eta_1 \\ \eta_2 \\ \eta_3 \\ \eta_4 \end{bmatrix} \tag{3}$$

$$\eta_1 = x_0 + x_2, \eta_2 = x_1 + x_3, \eta_3 = x_4 + x_6, \eta_4 = x_5 + x_7 , \tag{4}$$

$$X_1 = \begin{bmatrix} A_X + iB_X & C_X - iD_X \\ C_X + iD_X & A_X - iB_X \end{bmatrix}, \tag{5}$$

$$A_X = 2x_0 - \eta_1, B_X = 2x_1 - \eta_2, C_X = 2x_4 - \eta_3, D_X = 2x_5 - \eta_4 . \tag{6}$$

For X to be *iu* each of $\varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4$, $\det X_1$ must be ± 1 since each of these is a rational integer. Since the matrix in (3) is unitary,

$$\eta_1^2 + \eta_2^2 + \eta_3^2 + \eta_4^2 = (|\varepsilon_1|^2 + |\varepsilon_2|^2 + |\varepsilon_3|^2 + |\varepsilon_4|^2)/4 = 1 . \tag{7}$$

Consequently as $\eta_1, \eta_2, \eta_3, \eta_4$ are rational integers, exactly one of $\eta_1 \eta_2, \eta_3, \eta_4$ is ± 1, and the other three are zero. Thus exactly one of A_X, B_X, C_X, D_X is odd, the other three are even. From $\det X_1 = \pm 1$ we get $\det X_1 = 1$ if A_X or B_X is even, $\det X_1 = -1$ if C_X or D_X is even. (Consider $A_X^2 + B_X^2 - C_X^2 - D_X^2 = \pm 1$ modulo 4.) Conversely if A_X, B_X, C_X, D_X are integers, one even, three odd, with $A_X^2 + B_X^2 - C_X^2 - D_X^2 = \pm 1$ we can use (3), (4), (5), (6) to construct an *iu* group matrix X. The *pdsiu* group matrices arise when $\varepsilon_1 = \varepsilon_2 = \varepsilon_3 = \varepsilon_4 = \eta_1 = 1, A_X > 0$.

Now let Y, Z be *pdsiu* group matrices. Then $Z = XYX^T$ holds if and only if $UZU^* = (UXU^*)(UYU^*)(UXU^*)^*$; and this holds if and only if $Z_1 = X_1Y_1X_1^*$, and $\varepsilon_i(Z) = \varepsilon_i(X)\varepsilon_i(Y)\overline{\varepsilon_i(X)}$, for $i = 1, 2, 3, 4$. This last condition is satisfied since the $\varepsilon_i(X)$ are ± 1. Here, and henceforth, let $\rho_1, \rho_2, \rho_3, \rho_4$ stand for integers which may independently be ± 1. We now use a descent argument. We attempt to choose A_X, B_X, C_X, D_X so that $A_Z < A_Y$. As in the proof of Lemma 2, we have

$$(8)\qquad \begin{aligned}(A_Z - A_Y)/2 &= A_Y(C_X^2 + D_X^2)\\ &\quad + C_Y(A_XC_X - B_XD_X) + D_Y(A_XD_X + B_XC_X)\,.\end{aligned}$$

Put $A_X = \rho_1, B_X = 2\rho_2, C_X = 2\rho_3, D_X = 0$. Then X is *iu* and by (8) we can choose the signs ρ_1, ρ_2, ρ_3 so that $A_Z < A_Y$ if

$$(9)\qquad 2A_Y - |C_Y| - 2|D_Y| < 0\,.$$

Next take $A_X = \rho_1, B_X = 2\rho_2, C_X = 0, D_X = 2\rho_4$. Then X is *iu* and by (8) we may choose the signs ρ_1, ρ_2, ρ_4 so that $A_Z < A_Y$ if

$$(10)\qquad 2A_Y - 2|C_Y| - |D_Y| < 0\,.$$

Since $A_Y^2 = 1 + C_Y^2 + D_Y^2, A_Y > 0$, (9) holds

$$\begin{aligned}&\iff 2A_Y < |C_Y| + 2|D_Y|\,,\\ &\iff 4A_Y^2 < C_Y^2 + 4|C_YD_Y| + 4D_Y^2\,,\\ &\iff 4(1 + C_Y^2 + D_Y^2) < C_Y^2 + 4|C_YD_Y| + 4D_Y^2\,,\\ (11)\qquad &\iff 4 + 3C_Y^2 - 4|C_Y||D_Y| < 0\,.\end{aligned}$$

Similarly (10) holds if and only if

$$(12)\qquad 4 + 3D_Y^2 - 4|C_Y||D_Y| < 0\,.$$

Now the region in the positive quadrant of the C_Y, D_Y plane not satisfying either (11) or (12) is a region of infinite extent with a portion of two hyperbolas as part of the boundary. The only points in this region with even integral coordinates have either $C_Y = 0$ or $D_Y = 0$, or else $|C_Y| = |D_Y| = 2$. Now if $C_Y = 0$ we get from $A_Y^2 = 1 + C_Y^2 + D_Y^2$ that $(A_Y - D_Y)(A_Y + D_Y) = 1$, so $A_Y + C_Y = A_Y - C_Y = \pm 1$, hence $A_Y = 1$, $D_Y = 0$. Now $A_Y = 1, C_Y = D_Y = 0$ gives $Y = I_8$. Thus any *pdsiu* group matrix Y is in the same G-class as I_8 or else in the G-class of a Y for which $C_Y = \pm 2, D_Y = \pm 2, A_Y = 3$. That these last four possible Y are in the same G-class is seen as follows. Let T denote the *pdsiu* group matrix with $A_T = 3, C_T = 2, D_T = 2$. If $A_X = 3, B_X = 0, C_X = -2, D_X = -2$ then $Z = XTX^T$ has $A_Z = 3$, $B_Z = 0, C_Z = -2, D_Z = -2$. If $A_X = -2, B_X = -2, C_X = 3, D_X = 0$ then $Z = XTX^T$ has $A_Z = 3, B_Z = 0, C_Z = -2, D_Z = 2$. If $A_X = 2$,

$B_X = -2$, $C_X = 0$, $D_X = -3$ then $Z = XTX^T$ has $A_Z = 3$, $B_Z = 0$, $C_Z = 2$, $D_Z = -2$. Thus the G-class number is ≤ 2. If it were one there would be an X such that $X_1 T_1 X_1^* = I_2$. Lemma 2 then shows that if $\det X_1 = 1$ we have $C_X^2 + D_X^2 < C_T^2 + D_T^2 = 8$ and if $\det X_1 = -1$ then $A_X^2 + B_X^2 < 8$. All possible A_X, B_X, C_X, D_X are easily found and none work.

5. **The other groups of order eight.** The cyclic group of order eight is completely worked out in [4]. The G class number is two. The only *pdsiu* group matrix belonging to any of the remaining groups of order eight is I_8.

6. **The cyclic group of order twelve.** Let $X = x_0 I_{12} + x_1 P_{12} + \cdots + x_{11} P_{12}$. Take $\omega = (3^{1/2} + i)/2$ for the primitive root of unity of order twelve. Then for a unitary U, $UXU^* = \operatorname{diag}(\xi_0, \xi_1, \cdots, \xi_{11})$ where (see (1)):

$$\begin{bmatrix} 1/2 & 1/2 & 1/2 & 1/2 \\ 1/2 & i/2 & -1/2 & -i/2 \\ 1/2 & -1/2 & 1/2 & -1/2 \\ 1/2 & -i/2 & -1/2 & i/2 \end{bmatrix} \begin{bmatrix} \eta_0 \\ \eta_3 \\ \eta_6 \\ \eta_9 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} \xi_0 \\ \xi_3 \\ \xi_6 \\ \xi_9 \end{bmatrix} \tag{13}$$

$$\begin{gathered} \eta_0 = x_0 + x_4 + x_8,\ \eta_3 = x_1 + x_5 + x_9,\ \eta_6 = x_2 + x_6 + x_{10}, \\ \eta_9 = x_3 + x_7 + x_{11}\ , \end{gathered} \tag{14}$$

$$\begin{aligned} \xi_1 = [&2x_0 + x_2 - x_4 - 2x_6 - x_8 + x_{10} \\ &+ i(x_1 + 2x_3 + x_5 - x_7 - 2x_9 - x_{11}) \\ &+ 3^{1/2}(x_1 - x_5 - x_7 + x_{11}) + (-3)^{1/2}(x_2 + x_4 - x_8 - x_{10})]/2\ , \end{aligned} \tag{15}$$

$$\begin{aligned} \xi_2 = [&2x_0 + x_1 - x_2 - 2x_3 - x_4 + x_5 + 2x_6 + x_7 - x_8 - 2x_9 \\ &- x_{10} + x_{11} + (-3)^{1/2}(x_1 + x_2 - x_4 - x_5 + x_7 + x_8 - x_{10} - x_{11})]/2\ , \end{aligned} \tag{16}$$

$$\begin{aligned} \xi_4 = [&2x_0 - x_1 - x_2 + 2x_3 - x_4 - x_5 + 2x_6 - x_7 - x_8 + 2x_9 \\ &- x_{10} - x_{11} + (-3)^{1/2}(x_1 - x_2 + x_4 - x_5 + x_7 - x_8 + x_{10} - x_{11})]/2\ . \end{aligned} \tag{17}$$

The remaining ξ_i are conjugate to one of ξ_1, ξ_2, ξ_4 in the field $R(\omega)$ of the 12th root of unity. As $\xi_0, \cdots, \xi_{11}$ are algebraic integers, X is unimodular if and only if $\xi_0, \cdots, \xi_{11}$ are units. Since the matrix in (13) is unitary, $\eta_0^2 + \eta_3^2 + \eta_6^2 + \eta_9^2 = (|\xi_0|^2 + |\xi_3|^2 + |\xi_6|^2 + |\xi_9|^2)/4 = 1$ since $\xi_0, \xi_3, \xi_6, \xi_9$ are units in the Gaussian integers, hence roots of unity. As $\eta_0, \eta_3, \eta_6, \eta_9$ are rational integers, exactly one of $\eta_0, \eta_3, \eta_6, \eta_9$ is ± 1, the other three are zero. We now show that we can find a circulant W of the form $\pm P_{12}^{\alpha}$ so that in XW we have

$$\eta_0 = 1 = \xi_0 = \xi_3 = \xi_6 = \xi_9 \tag{18}$$

and $\xi_2 = \pm 1$. If, for X, $\eta_0 = \pm 1$ then by (13), $\xi_0 = \xi_3 = \xi_6 = \xi_9 = \eta_0$ and for $X(\eta_0 I_{12})$, (18) is satisfied. If, for X, $\eta_3 = \pm 1$, then by (13), $\xi_0 = \eta_3$, $\xi_3 = i\eta_3$, $\xi_6 = -\eta_3$, $\xi_9 = -i\eta_3$. Then, for $X(\eta_3 P_{12}^3)$, (18) is satisfied. If, for X, $\eta_6 = \pm 1$, then by (13), $\xi_0 = \eta_6$, $\xi_3 = -\eta_6$, $\xi_6 = \eta_6$, $\xi_9 = -\eta_6$. Then, for $X(\eta_6 P_{12}^2)$, (18) is satisfied. If, for X, $\eta_9 = \pm 1$, then by (13), $\xi_0 = \eta_9$, $\xi_3 = -i\eta_9$, $\xi_6 = -\eta_9$, $\xi_9 = i\eta_9$, and for $X(\eta_9 P_{12})$, (18) is satisfied. So now let X satisfy (18). For X, ξ_2 is a unit in the field $R((-3)^{1/2})$, hence ξ_2 is a power of $\omega^2 = (1 + (-3)^{1/2})/2$. We can choose λ to be $-1, 0$, or 1, such that for $XP_{12}^{4\lambda}$ we still have (18) and, moreover, $XP_{12}^{4\lambda}$ has ξ_2 equal to ω^0 or ω^6; that is $\xi_2 = \pm 1$. Thus we have achieved our claim. Note that ξ_4 is also a unit in $R((-3)^{1/2})$ and that the rational part of the numerator of ξ_4 is congruent (mod 2) to the rational part of the numerator of ξ_2. Since the only units in $R((-3)^{1/2})$ are $(\pm 1 \pm (-3)^{1/2})/2$ or $\pm 2/2$, $\xi_2 = \pm 1$ forces $\xi_4 = \pm 1$.

We now construct the *pdsiu* circulants X. These have all ξ_i real and positive, whence (18) holds. Symmetry implies $x_{11-j} = x_{1+j}$ for $0 \leqq j \leqq 4$. Then for the ξ_i to be positive units we require $\xi_0 = \xi_2 = \xi_3 = \xi_4 = \xi_6 = 1$, hence:

$$\begin{aligned} x_0 + 2x_1 + 2x_2 + 2x_3 + 2x_4 + 2x_5 + x_6 &= 1\ , \\ x_0 + x_1 - x_2 - 2x_3 - x_4 + x_5 + x_6 &= 1\ , \\ x_0 - 2x_2 + 2x_4 - x_6 &= 1\ , \\ x_0 - x_1 - x_2 + 2x_3 - x_4 - x_5 + x_6 &= 1\ , \\ x_0 - 2x_1 + 2x_2 - 2x_3 + 2x_4 - 2x_5 + x_6 &= 1\ . \end{aligned}$$

Solving these simultaneously we get $x_0 = 1 - 2x_4$, $x_5 = -x_1$, $x_3 = 0$, $x_2 = -x_4$, $x_6 = 2x_4$. Then $\xi_1 = 1 - 6x_4 + (3)^{1/2}(2x_1)$, and $\xi_1\xi_5 = (1 - 6x_4)^2 - 3(2x_1)^2 = 1$ if ξ_1, ξ_5 are to be positive units. Hence ξ_1 satisfies a Pell's equation, the fundamental solution of which is $2 - 3^{1/2}$. Now by induction one easily checks that all odd powers of $2 - 3^{1/2}$ have even rational part and all even powers have rational part $\equiv 1 \pmod 6$ and even irrational part. Consequently all *pdsiu* circulants are powers of the circulant M for which $\eta_0 = 1 = \xi_0 = \xi_3 = \xi_6 = \xi_9 = \xi_2 = \xi_4$, $\xi_1 = (2 - 3^{1/2})^2 = 7 - 4 \cdot 3^{1/2}$. Now $M^{2\alpha} = M^\alpha(M^\alpha)^T$ is in the principal G-class and $M^{2\alpha+1} = M^\alpha \cdot M \cdot (M^\alpha)^T$ is in the G-class of M. To show that the G-class number is two, we need only show that M is not in the principal G-class. If $M = XX^T$ for X an *iu* circulant, then for any W of the form $W = \pm P_{12}^\alpha$ we have $M = (XW)(XW)^T$. Then by the remarks of the previous paragraph, we may, after changing XW to X, assume that $M = XX^T$ where, for X, (18) holds and $\xi_2 = \pm 1$, $\xi_4 = \pm 1$. From (14) and (18) we get

$$
\begin{cases} x_0 + x_4 + x_8 = 1 \,, \\ x_1 + x_5 + x_9 = 0 \,, \\ x_2 + x_6 + x_{10} = 0 \,, \\ x_3 + x_7 + x_{11} = 0 \,. \end{cases} \tag{19}
$$

From $\xi_2 = \pm 1$ we get

$$
\begin{cases} 2x_0 + x_1 - x_2 - 2x_3 - x_4 + x_5 + 2x_6 + x_7 - x_8 \\ \qquad\qquad\qquad\qquad - 2x_9 - x_{10} + x_{11} = 2\rho_1 \,, \\ x_1 + x_2 - x_4 - x_5 + x_7 + x_8 - x_{10} - x_{11} = 0 \,, \end{cases} \tag{20}
$$

and from $\xi_4 = \pm 1$:

$$
\begin{cases} 2x_0 - x_1 - x_2 + 2x_3 - x_4 - x_5 + 2x_6 - x_7 - x_8 \\ \qquad\qquad\qquad\qquad + 2x_9 - x_{10} - x_{11} = 2\rho_2 \,, \\ x_1 - x_2 + x_4 - x_5 + x_7 - x_8 + x_{10} - x_{11} = 0 \,. \end{cases} \tag{21}
$$

Solving (19), (20), (21) simultaneously and remembering that the variables are integers, we get $\rho_1 = \rho_2 = 1$, $x_1 = -x_7$, $x_2 = x_0 + x_4 - 1$, $x_3 = x_5 - x_7$, $x_6 = 1 - x_0$, $x_8 = 1 - x_0 - x_4$, $x_9 = x_7 - x_5$, $x_{10} = -x_4$, $x_{11} = -x_5$. Then for $M = XX^T$ we must have $7 - 4.3^{1/2} = \xi_1\bar{\xi}_1$. Using (15) this becomes

$$
(3x_0 - 2)^2 + 3(x_5 + x_7)^2 + 9(x_5 - x_7)^2 + 3(x_0 + 2x_4 - 1)^2 = 7 \,, \tag{22}
$$

$$
-2(x_5 + x_7)(3x_0 - 2) + 6(x_5 - x_7)(x_0 + 2x_4 - 1) = -4 \,. \tag{23}
$$

From (22) we first obtain $x_5 = x_7$, then $x_5 = x_7 = 0$. But then we contradict (23). Hence the G-class number is two.

7. The alternating group of order twelve. This group is generated by elements a, b, c with $a^2 = b^2 = c^3 = 1$, $ab = ba$, $ac = cab$, $bc = ca$. The irreducible constituents of the group matrix X are most easily computed if we take the group elements in the order, $1, a, b, ab, c, ca, cb, cab, c^2, c^2a, c^2b, c^2ab$. Then the group matrix partitions into 4×4 blocks each of which has the structure of

$$
N = \begin{bmatrix} \alpha & \beta & \gamma & \delta \\ \beta & \alpha & \delta & \gamma \\ \gamma & \delta & \alpha & \beta \\ \delta & \gamma & \beta & \alpha \end{bmatrix}
$$

If V denotes the unitary matrix of (3), then $VNV^* = \operatorname{diag}(\alpha + \beta + \gamma + \delta, \alpha + \beta - \gamma - \delta, \alpha - \beta + \gamma - \delta, \alpha - \beta - \gamma + \delta)$. Thus each block in X can be diagonalized. After the same permutation of rows and columns, the group matrix splits up into a direct sum of four 3×3 blocks, of which one is a circulant and may be diagonalized. Let $(x_0, x_1, \cdots, x_{11})^T$ be the first column of X.

Let $\eta_1 = x_0 + x_1 + x_2 + x_3$, $\eta_2 = x_4 + x_5 + x_6 + x_7$, $\eta_3 = x_8 + x_9 + x_{10} + x_{11}$, $a_{11} = x_2 + x_3$, $a_{22} = x_1 + x_3$, $a_{33} = x_1 + x_2$, $a_{12} = x_9 + x_{11}$, $a_{23} = x_9 + x_{10}$, $a_{31} = x_{10} + x_{11}$, $a_{13} = x_5 + x_6$, $a_{21} = x_6 + x_7$, $a_{32} = x_5 + x_7$. Also now let $\omega = (-1 + (-3)^{1/2})/2$. Define $\varepsilon_1, \varepsilon_2, \varepsilon_3, A_X$ by:

$$\begin{bmatrix} 3^{-1/2} & 3^{-1/2} & 3^{-1/2} \\ 3^{-1/2} & \omega 3^{-1/2} & \omega^2 3^{-1/2} \\ 3^{-1/2} & \omega^2 3^{-1/2} & \omega 3^{-1/2} \end{bmatrix} \begin{bmatrix} \eta_1 \\ \eta_2 \\ \eta_3 \end{bmatrix} = 3^{-1/2} \begin{bmatrix} \varepsilon_1 \\ \varepsilon_2 \\ \varepsilon_3 \end{bmatrix}, \tag{24}$$

$$A_X = \begin{bmatrix} \eta_1 - 2a_{11} & \eta_3 - 2a_{12} & \eta_2 - 2a_{13} \\ \eta_2 - 2a_{21} & \eta_1 - 2a_{22} & \eta_3 - 2a_{23} \\ \eta_3 - 2a_{31} & \eta_2 - 2a_{32} & \eta_1 - 2a_{33} \end{bmatrix}.$$

Then there exists a unitary U such that $UXU^* = (\varepsilon_1) \dotplus (\varepsilon_2) \dotplus (\varepsilon_3) \dotplus A_X \dotplus A_X \dotplus A_X$. Moreover X is unimodular if and only if $\det A_X = \pm 1$ and $\varepsilon_1, \varepsilon_2, \varepsilon_3$ are units in $R(\omega)$. Thus $\varepsilon_1, \varepsilon_2, \varepsilon_3$ have to be roots of unity and since the matrix in (24) is unitary, this forces $\eta_1^2 + \eta_2^2 + \eta_3^2 = (|\varepsilon_1|^2 + |\varepsilon_2|^2 + |\varepsilon_3|^2)/3 = 1$. Thus exactly one of η_1, η_2, η_3 is ± 1, the other two are zero. Note that $a_{11} = x_2 + x_3$, $a_{22} = x_1 + x_3$, $a_{33} = x_1 + x_2$, possess an integral solution x_1, x_2, x_3 if and only if $a_{11} + a_{22} + a_{33} \equiv 0 \pmod 2$; a similar remark holds for a_{12}, a_{23}, a_{31}; and for a_{13}, a_{21}, a_{32}. Thus X is *iu* if and only if A_X is *iu* and exactly two of η_1, η_2, η_3 are zero and one is ± 1, and $a_{11} + a_{22} + a_{33} \equiv a_{12} + a_{23} + a_{31} \equiv a_{13} + a_{21} + a_{32} \equiv 0 \pmod 2$. The *pdsiu* X arise when $\varepsilon_1 = \varepsilon_2 = \varepsilon_3 = 1$, $\eta_1 = 1$, $\eta_2 = \eta_3 = 0$, A_X is pdsiu.

Now if Y, Z are *pdsiu* group matrices we have $Z = XYX^T$ if and only if $A_Z = A_X A_Y A_X^T$ and $\varepsilon_i(z) = \varepsilon_i(X)\varepsilon_i(Y)\overline{\varepsilon_i(X)}$, $i = 1, 2, 3$. This last condition is met since $\varepsilon_i(X)\overline{\varepsilon_i(X)} = 1$ because $\varepsilon_i(X)$ is a root of unity. The fact that A_Y is *pdsiu* and the fact that the C-class number is one at $n = 3$ implies that $A_Y = WW^T$ for some *iu* W. Here W need not be an A_X. Consider W mod 2. Since mod 2, $A_Y \equiv I_3$, $W \pmod 2$ is orthogonal. Hence, mod 2, W is a permutation matrix. We may find a 3×3 permutation matrix Q such that, mod 2, $WQ \equiv I_3$. We can do more. If we permit Q to be a generalized permutation matrix (nonzero entries are ± 1) we can force $WQ \equiv I_3 \pmod 2$ and each diagonal element of WQ is $\equiv 1 \pmod 4$. Changing notation and letting WQ be W, we have $A_Y = WW^T$ where now W is *iu* and (mod 4) has 1 in each diagonal position and (mod 4) has 0 or 2 in each off-diagonal position. Now one can write down all 64 matrices W (mod 4) of this type and determine those for which WW^T has the structure (mod 4) of an A_Y. It turns out that the W matrices (mod 4) with this property are precisely the W matrices with an even number of twos (mod 4) off the main diagonal. Certain of these acceptable W already have the structure (mod 4) of an A_Y. When this is so, Y is in the principal G-class. For all those acceptable W not (mod 4) of the form of an A_X, it turns out that WT, where

$$T = \begin{bmatrix} 1 & 2 & 2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

is an A_X. Let $H = T^{-1}(T^{-1})^T$. Then $A_Y = (WT)H(WT)^T = A_X H A_X^T$ where $A_X = WT$. Moreover, H is an A_Z. Thus Y is in the same G-class as Z, where $A_Z = H$. Is Z in the principal G-class? If so $H = A_X A_X^T$ for some X. But it is easy to find all integral B for which $H = BB^T$; none is (mod 4) an A_X. Hence the G-class number is two.

8. The dihedral group of order twelve. As is § 4 the group matrix may be taken to have the form (2) with $C = B^T, D = A^T$. Let $A = x_0 I_6 + x_1 P_6 + \cdots + x_5 P_6^5$, $B = x_6 I_6 + x_7 P_6 + \cdots + x_{11} P_6^5$. There exists a unitary U such that $UXU^* = (\varepsilon_1) \dotplus (\varepsilon_2) \dotplus (\varepsilon_3) \dotplus (\varepsilon_4) \dotplus X_1 \dotplus X_1 \dotplus X_2 \dotplus X_2$ where: if $\eta_1 = x_0 + x_2 + x_4$, $\eta_2 = x_1 + x_3 + x_5$, $\eta_3 = x_6 + x_8 + x_{10}$, $\eta_4 = x_7 + x_9 + x_{11}$, and if $a = x_0 + x_3$, $b = x_1 + x_4$, $\alpha = x_0 - x_3$, $\beta = x_4 - x_1$, $c = x_6 + x_9$, $d = x_7 + x_{10}$, $\gamma = x_6 - x_9$, $\delta = x_{10} - x_7$, then (3) holds, and, in addition,

$$X_1 = \begin{bmatrix} X_{1,1} & \bar{X}_{1,2} \\ X_{1,1} & \bar{X}_{1,2} \end{bmatrix}, \qquad X_2 = \begin{bmatrix} X_{2,1} & \bar{X}_{2,2} \\ X_{2,2} & \bar{X}_{2,1} \end{bmatrix} \tag{25}$$

where

$$\begin{cases} X_{1,1} = (3a - \eta_1 - \eta_2 + (-3)^{1/2}(a + 2b - \eta_1 - \eta_2))/2 \,, \\ X_{1,2} = (3c - \eta_3 - \eta_4 + (-3)^{1/2}(c + 2d - \eta_3 - \eta_4))/2 \,, \\ X_{2,1} = (3\alpha - \eta_1 + \eta_2 + (-3)^{1/2}(\eta_1 - \eta_2 - \alpha - 2\beta))/2 \,, \\ X_{2,2} = (3\gamma - \eta_3 + \eta_4 + (-3)^{1/2}(\eta_3 - \eta_4 - \gamma - 2\delta))/2 \,. \end{cases} \tag{26}$$

Note that $x_0, \cdots, x_{11}$ are integers if and only if $a \equiv \alpha, b \equiv \beta, c \equiv \gamma, d \equiv \delta \pmod 2$. As $\varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4$, det X_1, det X_2 are rational integers, X is unimodular if and only if $\varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4$, det X_1, det X_2 are each ± 1. Hence, as with the dihedral group of order eight, exactly one of $\eta_1, \eta_2, \eta_3, \eta_4$ is ± 1 and the other three are zero. By considering the formulas for det X_1 and det X_2 (mod 3), we find det $X_1 =$ det $X_2 = 1$ if η_1 or η_2 is ± 1, and det $X_1 =$ det $X_2 = -1$ if η_3 or η_4 is ± 1. The *pdsiu* group matrices arise when $\eta_1 = 1$ and $X_{1,1}$ and $X_{2,1}$ are real and positive. If η_1 or η_2 is ± 1 we let $X_{1,1} = (A_X + (-3)^{1/2} B_X)/2$, $X_{1,2} = (C_X + (-3)^{1/2} D_X)/2$,

$X_{2,1} = (\mathfrak{A}_X + (-3)^{1/2}\mathfrak{B}_X)/2$, $X_{2,2} = (\mathfrak{C}_X + (-3)^{1/2}\mathfrak{D}_X)/2$; and if η_3 or η_4 is ± 1 we let $X_{1,1} = (C_X + (-3)^{1/2}D_X)/2$, $X_{1,2} = (A_X + (-3)^{1/2}B_X)/2$, $X_{2,1} = (\mathfrak{C}_X + (-3)^{1/2}\mathfrak{D}_X)/2$, $X_{2,2} = (\mathfrak{A}_X + (-3)^{1/2}\mathfrak{B}_X)/2$.

Now let Z, Y are *pdsiu* group matrices; then $Z = XYX^T$ holds if and only if $\varepsilon_i(Z) = \varepsilon_i(X)\varepsilon_i(Y)\overline{\varepsilon_i(X)}$ for $i = 1, 2, 3, 4$, $Z_1 = X_1Y_1X_1^*$, $Z_2 = X_2Y_2X_2^*$. The first of these conditions need not concern us as $\varepsilon_i(X)$ is always to be ± 1. We proceed to show that, given Y, we can choose Xiu such that $Z_2 = I_2$. If $Y_2 = I_2$ we have nothing to do. Otherwise we compute as in Lemma 2 that

$$\begin{aligned} 2(A_Z - A_Y) &= A_Y(C_X^2 + 3D_X^2) \\ &\quad + C_Y(A_XC_X - 3B_XD_X) + 3D_Y(A_XD_X + B_XC_X) , \end{aligned} \tag{27}$$

$$\begin{aligned} 2(\mathfrak{A}_Z - \mathfrak{A}_Y) &= \mathfrak{A}_Y(\mathfrak{C}_X^2 + 3\mathfrak{D}_X^2) \\ &\quad + \mathfrak{C}_Y(\mathfrak{A}_X\mathfrak{C}_X - 3\mathfrak{B}_X\mathfrak{D}_X) + 3\mathfrak{D}_Y(\mathfrak{A}_X\mathfrak{D}_X + \mathfrak{B}_X\mathfrak{C}_X) . \end{aligned} \tag{28}$$

We now assign special values to the quantities entering into X. If we put $\eta_1 = -\rho_1$, $\eta_2 = \eta_3 = \eta_4 = 0$, $a = \alpha = \rho_1$, $b = \beta = -\rho_1$, $c = \gamma = \rho_2$, $d = \delta = -\rho_2$ then we get $A_X = \mathfrak{A}_X = 4\rho_1$, $B_X = \mathfrak{B}_X = 0$, $C_X = \mathfrak{C}_X = 3\rho_2$ $D_X = -\rho_2$, $\mathfrak{D}_X = \rho_2$. For this iuX, $\mathfrak{A}_Z - \mathfrak{A}_Y < 0$ will hold if

$$\mathfrak{A}_Y + \rho_1\rho_2\mathfrak{C}_Y + \rho_1\rho_2\mathfrak{D}_Y < 0 . \tag{29}$$

Next we put $\eta_1 = \rho_1$, $\eta_2 = \eta_3 = \eta_4 = 0$, $a = \alpha = \rho_1$, $b = \beta = \rho_2$, $c = \gamma = \rho_3$, $d = \delta = -\rho_3$. Then $A_X = \mathfrak{A}_X = 2\rho_1$, $B_X = 2\rho_2$, $\mathfrak{B}_X = -2\rho_2$, $C_X = \mathfrak{C}_X = 3\rho_3$, $D_x = -\rho_2$, $D_X = -\rho_3$, $\mathfrak{D}_X = \rho_3$. For this iuX, $\mathfrak{A}_Z - \mathfrak{A}_Y < 0$ will hold if

$$12\mathfrak{A}_Y + \mathfrak{C}_Y(6\rho_1\rho_3 + 6\rho_2\rho_3) + 3\mathfrak{D}_Y(2\rho_1\rho_3 - 6\rho_2\rho_3) < 0 .$$

If $\rho_1 = \rho_2$ this becomes

$$\mathfrak{A}_Y + \rho_1\rho_3\mathfrak{C}_Y - \rho_1\rho_3\mathfrak{D}_Y < 0 , \tag{30}$$

and if $\rho_1 = -\rho_2$ this becomes

$$\mathfrak{A}_Y + 2\rho_1\rho_3\mathfrak{D}_Y < 0 . \tag{31}$$

Choosing the signs ρ_1, ρ_2, ρ_3 suitably, (29) and (30) becomes

$$\mathfrak{A}_Y - |\mathfrak{C}_Y| - |\mathfrak{D}_Y| < 0 , \tag{32}$$

and (31) becomes

$$\mathfrak{A}_Y - 2|\mathfrak{D}_Y| < 0 . \tag{33}$$

So we can make $\mathfrak{A}_Z < \mathfrak{A}_Y$ if $\mathfrak{A}_Y, \mathfrak{C}_Y, \mathfrak{D}_Y$ satisfy either (32) or (33). As in § 4, the facts that $\mathfrak{A}_Y > 0$ and $\mathfrak{A}_Y^2 = 4 + \mathfrak{C}_Y^2 + 3\mathfrak{D}_Y^2$ show that (32) and (33) are equivalent to

$$2 + |\mathfrak{D}_Y|^2 - |\mathfrak{C}_Y||\mathfrak{D}_Y| < 0 , \tag{34}$$

(35) $$4 + |\mathfrak{C}_Y|^2 - |\mathfrak{D}_Y|^2 < 0 ,$$

respectively.

Now the region in the positive quadrant of the $\mathfrak{C}_Y, \mathfrak{D}_Y$ plane satisfying neither (34) nor (35) is a region of infinite extent with hyperbolas as part of the boundary. Remembering that $\mathfrak{C}_Y \equiv 0 \pmod 3$, we find several points $(|\mathfrak{C}_Y|, |\mathfrak{D}_Y|)$ in our region: $(|\mathfrak{C}_Y|, |\mathfrak{D}_Y|) = (0, 2)$, $(3, 1)$, $(3, 2)$ and points with $|\mathfrak{C}_Y| = |\mathfrak{D}_Y|$ and points with $\mathfrak{D}_Y = 0$. The points $(0, 2)$, $(3, 1)$, $(3, 2)$ give $\mathfrak{A}_Y = 4$ or 5 and this can be rejected on the grounds that a *pdsiu* Y has $\mathfrak{B}_Y = 0$, $\eta_1 = 1$ and then $A_Y = 4$ or 5 give a nonintegral α, β. The cases in which $\mathfrak{D}_Y = 0$ or $|\mathfrak{C}_Y| = |\mathfrak{D}_Y|$ are rejected by showing that $\mathfrak{A}_Y^2 = 4 + \mathfrak{C}_Y^2 + 3\mathfrak{D}_Y^2$ does not give a positive integral $\mathfrak{A}_Y$, except if $\mathfrak{C}_Y = \mathfrak{D}_Y = 0$, $\mathfrak{A}_Y = 2$. When $\mathfrak{C}_Y = \mathfrak{D}_Y = 0$, $A_Y = 2$, we have $Y_2 = I_2$. Thus we have shown that if $Y_2 \neq I_2$ then we can find an *iu* X so that $\mathfrak{A}_Z < \mathfrak{A}_Y$. Since $\mathfrak{A}_Z > 0$, eventually this descent halts and then $Z_2 = I_2$.

Thus assume $Y_2 = I_2$. Our next goal is, using only X for which $X_2X_2^* = I_2$, to make $A_Z < A_Y$. Notice that $Y_2 = I_2$ and $\eta_1 = 1$ implies that the parameters $\alpha, \beta, \gamma, \delta$ of Y_2 are $\alpha = 1, \beta = \gamma = \delta = 0$. Thus the parameters a, b, c, d of Y satisfy $a \equiv 1, b \equiv c \equiv d \equiv 0 \pmod 2$. Hence $C_Y \equiv 0 \pmod 6$ and $D_Y \equiv c \equiv -c \equiv C_Y \pmod 4$. We next determine those X for which $X_2X_2^* = I_2$. By Lemma 2 these X must have $\mathfrak{C}_X = \mathfrak{D}_X = 0$, so that $\mathfrak{A}_X^2 + 3\mathfrak{B}_X^2 = 4$, $\mathfrak{A}_X = \pm 2$, $\mathfrak{B}_X = 0$, or $\mathfrak{A}_X = \pm 1$, $\mathfrak{B}_X = \pm 1$. It is then easy to determine the parameters $\alpha, \beta, \gamma, \delta$ of X. We find that if η_1 or η_2 is ± 1 then $\gamma = \delta = 0$ and not both α, β are odd; and if η_3 or η_4 is ± 1 then $\alpha = \beta = 0$ and not both γ, δ are odd. So in X the parameters a, b, c, d are restricted by: both c, d are even and not both a, b are odd in the cases when η_1 or η_2 is ± 1; and both a, b are even and not both c, d are odd in the cases when η_3 or η_4 is ± 1. In particular if we put $\eta_1 = -\rho_1$, $\alpha = 0$, $\beta = -(\rho_1 + \rho_2)/2$, $\gamma = 0$, $\delta = 0$, or if we put $\eta_1 = \rho_1$, $\alpha = \rho_1$, $\beta = \gamma = \delta = 0$, then $X_2X_2^* = I_2$.

We now seek X for which $A_Z < A_Y$ and $X_2X_2^* = I_2$. To this end we give special values to the parameters in X. Put $\eta_1 = \rho_1$, $\eta_2 = \eta_3 = \eta_4 = 0$, $a = \rho_1$, $\alpha = \rho_1$, $b = -2\rho_2$, $\beta = 0$, $\gamma = c = 0$, $d = 2\rho_4$, $\delta = 0$. Then $A_X = 2\rho_1$, $B_X = -4\rho_2$, $C_X = 0$, $D_X = 4\rho_4$, X is *iu* and $X_2X_2^* = I_2$. From (27) we find that the signs ρ_1, ρ_2, ρ_4 can be chosen to make $A_Z < A_Y$ if

(36) $$2A_Y - 2|C_Y| - |D_Y| < 0 .$$

Next set $\eta_1 = -\rho_1$, $a = -2\rho_1$, $\alpha = 0$, $b = (\rho_1 - 3\rho_2)/2$, $\beta = -(\rho_1 + \rho_2)/2$, $\gamma = c = 0$, $d = 2\rho_4$, $\delta = 0$. Then $A_X = -5\rho_1$, $B_X = -3\rho_2$, $C_X = 0$, $D_X = 4\rho_4$, X is *iu* and $X_2X_2^* = I_2$. Then from (27) we can choose the signs ρ_1, ρ_2, ρ_4 so that $A_Z < A_Y$ if

$$(37)\qquad 4A_Y - 3\,|\,C_Y\,| - 5\,|\,D_Y\,| < 0\,.$$

Finally we set $\eta_1 = -\rho_1$, $a = 2\rho_1$, $\alpha = 0$, $b = (\rho_2 - 3\rho_1)/2$, $\beta = -(\rho_1 + \rho_2)/2$, $c = \gamma = 0$, $d = 2\rho_4$, $\delta = 0$. Then $A_X = 7\rho_1$, $B_X = \rho_2$, $C_X = 0$, $D_X = 4\rho_4$. We can, using (27), choose the signs ρ_1, ρ_2, ρ_4 so that $A_Z < A_Y$ if

$$(38)\qquad 4A_Y - |\,C_Y\,| - 7\,|\,D_Y\,| < 0\,.$$

Using $A_Y > 0$, $A_Y^2 = 4 + C_Y^2 + 3D_Y^2$, we find that (36), (37), (38) are equivalent to

$$(39)\qquad 16 + 11D_Y^2 - 4\,|\,C_Y\,|\,|\,D_Y\,| < 0\,,$$

$$(40)\qquad 64 + 7C_Y^2 + 23D_Y^2 - 30\,|\,C_Y\,|\,|\,D_Y\,| < 0\,,$$

$$(41)\qquad 64 + 15C_Y^2 - D_Y^2 - 14\,|\,C_Y\,|\,|\,D_Y\,| < 0\,,$$

respectively.

Now the region in the positive quadrant of the C_Y, D_Y plane not satisfying any of (39), (40), (41) is a region of infinite extent with a portion of three hyperbolas as part of the boundary. In this region the only points $(|\,C_Y\,|, |\,D_Y\,|)$ with $C_Y \equiv 0 \pmod 6$, $C_Y \equiv D_Y \pmod 4$ are $(0, 4)$, $(6, 2)$, $(0, 8)$, $(12, 4)$, together with points for which $|\,C_Y\,| = |\,D_Y\,|$ or for which $D_Y = 0$. We can reject $(0, 4)$ and $(6, 2)$ since, using $A_Y^2 = 4 + C_Y^2 + 3D_Y^2$, they give nonintegral A_Y. Now $|\,C_Y\,| = |\,D_Y\,|$ gives $A_Y^2 = 4 + 4D_Y^2$, so $(A_Y - 2D_Y)(A_Y + 2D_Y) = 4$. This gives a finite number of possibilities of which only $C_Y = D_Y = 0$, $A_Y = 2$ is acceptable. Similarly $D_Y = 0$ leads only to $C_Y = D_Y = 0$, $A_Y = 2$. Now $A_Y = 2$, $C_Y = D_Y = 0$ gives $Y_1 = I_2$. Thus, subject to the constraint that $Z_2 = Y_2 = I_2$ we have found *iu* X so that in $Z = XYX^T$ we have $A_Z < A_Y$. Since this descent must eventually stop, we have shown that any *pdsiu* group matrix is in the G class of I_{12} or the G-class of a group matrix Y for which $Y_2 = I_2$, $A_Y = 14$, $(C_Y, D_Y) = (0, \pm 8)$ or $(\pm 12, \pm 4)$. Let now Y be the *pdsiu* group matrix for which $Y_2 = I_2$, $A_Y = 14$, $C_Y = 0$, $D_Y = 8$. We now exhibit *iu* X for which $Z = XYX^T$ has $Z_2 = I_2$, $A_Z = 14$, $(C_Z, D_Z) = (0, -8)$ or $(\pm 12, \pm 4)$.

First put $\eta_1 = -\rho_1$, $a = 0$, $\alpha = 0$, $b = -(\rho_1 + \rho_2)/2$, $\beta = -(\rho_1 + \rho_2)/2$, $c = \gamma = 0$, $d = \delta = 0$. Then $A_X = \rho_1$, $B_X = -\rho_2$, $C_X = D_X = 0$, $X_2X_2^* = I_2$, and $A_Z = 14$, $C_Z = -12\rho_1\rho_2$, $D_Z = -4$. Next put $\eta_1 = -\rho_1$, $a = 2\rho_1$, $\alpha = 0$, $b = (\rho_2 - 3\rho_1)/2$, $\beta = -(\rho_1 + \rho_2)/2$, $c = 0$, $\gamma = 0$, $d = -2\rho_1$, $\delta = 0$. Then $A_X = 7\rho_1$, $B_X = \rho_2$, $C_X = 0$, $D_X = -4\rho_1$, $X_2X_2^* = I_2$, $A_Z = 14$, $C_Z = 0$, $D_Z = -8$. Finally put $\eta_3 = -\rho_1$, $a = \alpha = b = \beta = c = \gamma = 0$, $d = \delta = -(\rho_1 + \rho_2)/2$. Then $A_X = \rho_1$, $B_X = -\rho_2$, $C_X = D_X = 0$, $\mathfrak{A}_X = \rho_1$, $\mathfrak{B}_X = \rho_2$, $\mathfrak{C}_X = \mathfrak{D}_X = 0$. Moreover $X_2X_2^* = I_2$ and $Z_1 = X_1Y_1X_1^*$ has $A_Z = 14$, $C_Z = -12\rho_1\rho_2$, $D_Z = 4$.

We have thus established that the G-class number is at most two. If it were one there would be an X for which $X_1Y_1X_1^* = I_2$ and $X_2X_2^* = I_2$. The second condition forces (as previously noted): $\gamma = \delta = 0$ or $\alpha = \beta = 0$. In turn these as before, $C_X \equiv 0 \pmod 6$, $C_X \equiv D_X \pmod 4$. Then Lemma 2 shows that $C_X^2 + 3D_X^2 < C_Y^2 + 3D_Y^2 = 192$. Using $A_X^2 + 3B_X^2 = 4 + C_X^2 + 3D_X^2$, all possible values of A_X, B_X, C_X, D_X are easily found and tested in (27). In all cases $A_Z - A_Y \geqq 0$. Thus we have proved that the G-class number is precisely two.

9. The group $a^4 = 1, b^3 = 1, a^{-1}ba = b^2$, of order twelve. If we take the group elements in the order $1, b, b^2, a, ab, ab^2, a^2, a^2b, a^2b^2, a^3, a^3b, a^3b^2$, then the group matrix X partitions into blocks which are 3×3 circulants. Let $(x_0, x_1, \cdots, x_{11})^T$ be the first column of X. We compute the irreducible representations as indicated in § 2. At one point it is necessary to make use of the following fact:

$$2^{-1/2}\begin{bmatrix} I_2 & I_2 \\ I_2 & -I_2 \end{bmatrix}\begin{bmatrix} A & B \\ B & A \end{bmatrix} 2^{-1/2}\begin{bmatrix} I_2 & I_2 \\ I_2 & -I_2 \end{bmatrix} = \begin{bmatrix} A+B & 0 \\ 0 & A-B \end{bmatrix}$$

if A, B are 2×2 matrices. Thus we find a unitary U such that $UXU^* = (\varepsilon_1) \dotplus (\varepsilon_4) \dotplus (\varepsilon_2) \dotplus (\varepsilon_3) \dotplus X_1 \dotplus X_1 \dotplus X_2 \dotplus X_2$. Here, if $\eta_1 = x_0 + x_1 + x_2$, $\eta_2 = x_6 + x_7, + x_8$, $\eta_3 = x_3 + x_4 + x_5$, $\eta_4 = x_9 + x_{10} + x_{11}$, then:

$$\begin{bmatrix} 1/2 & 1/2 & 1/2 & 1/2 \\ 1/2 & i/2 & -1/2 & -i/2 \\ 1/2 & -1/2 & 1/2 & -1/2 \\ 1/2 & -i/2 & -1/2 & i/2 \end{bmatrix}\begin{bmatrix} \eta_0 \\ \eta_4 \\ \eta_2 \\ \eta_3 \end{bmatrix} = \frac{1}{2}\begin{bmatrix} \varepsilon_1 \\ \varepsilon_4 \\ \varepsilon_2 \\ \varepsilon_3 \end{bmatrix}. \tag{42}$$

The matrix X_1 is described by (25) and (26) where $a = x_0 + x_6$, $b = x_2 + x_8$, $c = x_3 + x_9$, $d = x_5 + x_{11}$. X_2 is described by

$$X_2 = \begin{bmatrix} X_{2,1} & -\bar{X}_{2,2} \\ X_{2,2} & \bar{X}_{2,1} \end{bmatrix}$$

with $X_{2,1}, X_{2,2}$ given by (26); $\alpha = x_0 - x_6$, $\beta = x_2 - x_8$, $\gamma = x_3 - x_9$, $\delta = x_5 - x_{11}$.

As before, for integral $x_0, x_1, \cdots, x_{11}$ we must have $a \equiv \alpha$, $b \equiv \beta$, $c \equiv \gamma$, $d \equiv \delta \pmod 2$. Here $\varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4$, $\det X_1$, $\det X_2$ are algebraic integers and must be units if X is to be iu. Since the ε_i are Gaussian integers, this forces the ε_i to be roots of unity. Because the matrix in (42) is unitary, this forces exactly one η_i to be ± 1, the others to be zero. Now in fact $\det X_1$, $\det X_2$ are rational integers and $\det X_2 > 0$. Thus $\det X_1 = \pm 1$ ($+1$ if η_1 or η_2 is ± 1, -1 if η_3 or η_4 is ± 1) and $\det X_2 = 1$. The *pdsiu* X arise when $\eta_1 = 1$, $\varepsilon_1 = \varepsilon_2 = \varepsilon_3 = \varepsilon_4 = 1$, $\det X_1 = 1$, $X_{1,1} > 0$, $X_{2,1} > 0$. From $\det X_2 = 1$ we get $|X_{2,1}|^2 + |X_{2,2}|^2 = 1$.

Each of $|X_{2,1}|^2$, $|X_{2,2}|^2$ is a rational integer so either $X_{2,1} = 0$ or $X_{2,2} = 0$. When X is *pdsiu*, $X_{2,1}$ is thus a positive unit in the field of $R((-3)^{1/2})$, hence $X_{2,1} = 1$ and hence $X_2 = I_2$. But always if X is just *iu* we have $X_2X_2^* = I_2$. We show $X_{2,2} = 0$ when η_1 or η_2 is ± 1; and $X_{2,1} = 0$ when η_3 or η_4 is ± 1. If we had η_1 or η_2 equal to ± 1 and $X_{2,1} = 0$ we would have $3\alpha - \eta_1 + \eta_2 = 0$, which is not true for any integer α. Similarly if η_3 or η_4 is ± 1 then $X_{2,2} = 0$ is absurd. From this point on the discussion is almost word for word the same as the discussion in § 8. We introduce $A_X, B_X, C_X, D_X, \mathfrak{A}_X, \mathfrak{B}_X, \mathfrak{C}_X, \mathfrak{D}_X$ as in § 8. We have just established that $\mathfrak{C}_X = \mathfrak{D}_X = 0$ and that $Y_2 = I_2$ if Y is *pdsiu*. We now carry on from the point in § 8 at which we assumed $Y_2 = I_2$. The conclusion we reach is that the G-class number is two.

10. The noncyclic abelian group of order twelve. By Theorem 2 the only *pdsiu* group matrix for this group is I_{12}.

11. Summary. Let Φ_n be the matrix on p. 331 of [5].

THEOREM 5. *For all groups G of order $n \leqq 13$, the G-class number is one, except for the cyclic groups of orders 8 and 12, the dihedral groups of orders 8 and 12, the alternating group A_4, and the remaining nonabelian group of order twelve. In each of these exceptional cases the G-class number is two and the nonprincipal G-class is contained in the C-class of Φ_n.*

Acknowledgement. I have benefited from discussions of this problem with Dr. O. Taussky. In particular, through Dr. Taussky, I was aware of prior unpublished work of M. Kneser and E. C. Dade who computed the G-class number for the cyclic group of order nine (Kneser) and for a number of cyclic groups of prime order (Dade).

REFERENCES

1. G. Higman, *The units of group rings*, Proc. London Math. Soc. **46** (1940), 231-248.
2. M. Kneser, *Klassenzahlen definiter Quadratischer Formen*, Archiv der Math. **8** (1957), 241-250.
3. M. Newman, *Circulant quadratic forms*, Report of the Institute in the theory of numbers, Boulder, Colorado (1959), 189-193.
4. M. Newman and O. Taussky, *Classes of definite unimodular circulants*, Canad. Math. J. **9** (1956), 71-73.
5. O. T. O'Meara, *Introduction to quadratic forms*, Academic Press, New York, 1963.
6. O. Taussky, *Matrices of rational integers*, Bull. Amer. Math. Soc. **66** (1960), 327-345.
7. R. C. Thompson, *Normal matrices and the normal basis in abelian number fields*, Pacific J. Math. **12** (1962), 1115-1124.
8. R. C. Thompson *Unimodular group matrices with rational integers as elements*, Pacific J. Math. **14** (1964), 719-726.

THE UNIVERSITY OF CALIFORNIA, SANTA BARBARA

Printed in Japan by International Academic Printing Co., Ltd., Tokyo Japan

Pacific Journal of Mathematics
Vol. 17, No. 1 January, 1966