

# Pacific Journal of Mathematics

**CLASSES OF CIRCULANTS OVER THE  $p$ -ADIC AND  
RATIONAL INTEGERS**

DENNIS GARBANATI

# CLASSES OF CIRCULANTS OVER THE $p$ -ADIC AND RATIONAL INTEGERS

DENNIS A. GARBANATI

Let  $G = \{g^0, g, g^2, \dots, g^{q-1}\}$  be a finite abelian group of order  $q$  where  $q$  is a prime. Let  $Z_p$  and  $Z$  denote the  $p$ -adic and rational integers respectively. A circulant for  $G$  over  $Z_p$  (or  $Z$ ) is a  $q$ -square matrix  $A$  of the form  $A = \sum_{i=0}^{q-1} a_i P(g^i)$  where  $a_i \in Z_p$  (or  $Z$ ) and  $P$  is the left regular representation of  $G$ , i.e.,  $P(g^i)$  is a  $q$ -square permutation matrix and  $P(g^i g^j) = P(g^i)P(g^j)$ . Let  $M$  and  $L$  be symmetric unimodular circulants for  $G$  over  $Z_p$  (or  $Z$ ). The circulants  $M$  and  $L$  are said to be in the same  $G$ -class if there exists a circulant  $A$  for  $G$  over  $Z_p$  (or  $Z$ , respectively) such that  $M = A^\top L A$  where  $^\top$  denotes transposition. The central object of this paper is: (i) to give computable criteria for determining whether or not two circulants for  $G$  over  $Z_p$  are in the same  $G$ -class, (ii) to give a computable upper bound (which seems to be frequently equal to 1) for the number of  $G$ -classes among the positive definite symmetric unimodular circulants, and (iii) to introduce a group matrix concept (called  $G$ -genus) corresponding to the concept of genus.

This paper advances the work done by M. Newman, O. Taussky, R. C. Thompson, and the author in [3, 4, 5, 7, 8, 9, 13, 14]. The methods in (i) and (iii) involve generalizing a result of O. Taussky [13] and then applying a local theorem from [4]. The methods in (ii) involve a slight elaboration of the methods found in D. Davis' thesis [1].

2. Notation. Let  $q$  be an odd prime. Let  $F$  be a field whose characteristic does not divide  $2q$ . Let  $\zeta$  be a primitive  $q$ th root of 1, i.e., a  $q$ -order generator of the roots of  $x^q - 1 \in F[x]$ . Let  $K = F(\zeta)$  and  $k = F(\zeta + \zeta^{-1})$ . Let  $N(\cdot) = N_{K/k}(\cdot)$  be the norm function from  $K$  into  $k$ . Let  $S(\cdot) = S_{K/F}(\cdot)$  be the trace function from  $K$  into  $F$ . Let  $\mathcal{G}(K/F)$  denote the Galois group of  $K$  over  $F$ . Let  $G$  be a group of order  $q$ , that is,

$$G = \{1 = g^0, g, g^2, \dots, g^{q-1}\}$$

where  $g$  generates  $G$ . Let  $R'$  be a ring in  $F$ .

DEFINITION. A  $q$ -square matrix  $A$  is called a *circulant* for  $G$  over  $R'$  (or simply a *circulant*) if  $A$  has the form  $A = \sum_{i=0}^{q-1} a_i P(g^i)$  where  $a_i \in R'$  and  $P$  is the left regular representation of  $G$ . Thus the  $(i, j)$  entry of  $P(g^k)$  is 1 if  $g^k g^{j-1} = g^{i-1}$  and zero if  $g^k g^{j-1} \neq g^{i-1}$ .

The term circulant in this paper shall always refer to a circulant for  $G$  and hence shall always be a  $q$ -square matrix.

Let

$$H = \{\chi' = \chi^0, \chi, \chi^2, \dots, \chi^{q-1}\}$$

be the character group on  $G$ , i.e., the homomorphisms of  $G$  into  $K$  where  $\chi'$  is the principal character and  $\chi$  generates  $H$ . We may assume  $\chi(g) = \zeta$ .

If  $A = \sum_{i=0}^{q-1} a_i P(g^i)$  is a circulant, for  $0 \leq j \leq q-1$  define

$$(1) \quad \lambda_{\chi^j}(A) = \sum_{i=0}^{q-1} a_i \chi^j(g^i).$$

By § 2 of [3], there is a matrix  $U$  such that for any circulant  $A$  over  $R'$  we have

$$(2) \quad UAU^{-1} = \text{diag}(\dots, \lambda_{\chi^j}(A), \dots)$$

where  $\lambda_{\chi^j}(A)$  is the  $j+1$ th entry.

Let  $^{\top}$  denote transposition.

**3. Preliminary material.** We start with a generalization of O. Taussky's result [13]. Although it might look unnecessarily abstract, Lemma 1 has the advantage of being able to produce both the local theorem (Theorem 1) and O. Taussky's global theorem (Theorem 5). In anticipation of Lemma 1, note that if  $R'$  is a ring in  $F$  with 1 and  $M$  is a matrix over  $R'$  then  $M$  is unimodular if the determinant of  $M$  is a unit in  $R'$ .

**LEMMA 1.** *Let  $R'$  be a ring in  $F$  with 1 such that  $R'/qR'$  is a field whose characteristic is not 2. Let  $R = R' + R'\zeta + \dots + R'\zeta^{q-1}$ , a ring in  $K$ . Let  $U'$  and  $U$  be the groups of units of  $R'$  and  $R$  respectively. Suppose  $[K:F] = q-1$ . Let  $M$  and  $L$  be unimodular (not necessarily symmetric) circulants over  $R'$ . Then the following are equivalent:*

- (i) *There exists a circulant  $A$  over  $R'$  such that  $M = A^{\top}LA$ .*
- (ii)  *$\lambda_{\chi'}(ML^{-1}) \in R'^2$  and  $\lambda_{\chi}(ML^{-1}) \in N(R)$ .*
- (iii)  *$\lambda_{\chi'}(ML^{-1}) \in U'^2$  and  $\lambda_{\chi}(ML^{-1}) \in N(U)$ .*

*Proof.* (i)  $\Rightarrow$  (ii) By Lemma 5 of [3] and (2),  $\lambda_{\chi'}(ML^{-1}) = \lambda_{\chi'}(M)/\lambda_{\chi'}(L) = \lambda_{\chi'}(A^{\top})\lambda_{\chi'}(A) = [\lambda_{\chi'}(A)]^2 \in R'^2$ . Since  $[K:F] = q-1$  we see by Lemma 4 of [3] that  $[K:k] = 2$ . Hence again by Lemma 5 of [3] and by (2),  $\lambda_{\chi}(ML^{-1}) = \lambda_{\chi}(M)/\lambda_{\chi}(L) = \lambda_{\chi}(A^{\top})\lambda_{\chi}(A) = N(\lambda_{\chi}(A))$ . Since  $\lambda_{\chi}(A) \in R$  the result follows.

(ii)  $\Rightarrow$  (i) By (2)

$$\lambda_{\chi'}(ML^{-1}) = \lambda_{\chi'}(M)/\lambda_{\chi'}(L) = a = \alpha^2$$

where  $\alpha \in R'$ , and

$$\lambda_{\chi}(ML^{-1}) = \lambda_{\chi}(M)/\lambda_{\chi}(L) = b = N(\beta)$$

where  $\beta \in R$ . From  $[K:k] = 2$  it follows that  $N(\beta) = \beta\sigma(\beta)$  where  $\sigma: \zeta \rightarrow \zeta^{-1} \in \mathcal{S}(K/F)$ . Since  $L$  is unimodular,  $ML^{-1} = \sum_{i=0}^{q-1} c_i P(g^i)$  where  $c_i \in R'$ . From  $[K:F] = q - 1$  and (4) of [3], it follows that

$$\begin{aligned} c_0 &= q^{-1} \sum_{i=0}^{q-1} \lambda_{\chi^i}(ML^{-1}) = q^{-1} [\lambda_{\chi}(ML^{-1}) + S(\lambda_{\chi}(ML^{-1}))] \\ &= q^{-1}(a + S(b)). \end{aligned}$$

Since  $L$  is unimodular,  $a \in R'$ . Since  $S(\zeta^i) = -1$  for  $1 \leq i \leq q - 1$ ,  $S(b) \in R'$ . Also  $q \in R'$  because  $1 \in R'$ . Let  $c$  and  $d$  be elements of  $R'$ . Write  $c \equiv d$  if there exists an  $e \in R'$  such that  $c - d = qe$ . Then  $0 \equiv \alpha^2 + S(N(\beta))$ . Since  $\beta \in R$ , write  $\beta = b_0 + b_1\zeta + \cdots + b_{q-1}\zeta^{q-1}$  where  $b_i \in R'$ . Then

$$\begin{aligned} 0 &\equiv \alpha^2 + S[(b_0 + b_1\zeta + \cdots + b_{q-1}\zeta^{q-1})(b_0 + b_1\zeta^{-1} + b_2\zeta^{-2} + \cdots + b_{q-1}\zeta)] \\ &\equiv \alpha^2 + (q - 1)(b_0^2 + b_1^2 + \cdots + b_{q-1}^2) + S\left(\sum_{\substack{i \neq j \\ 0 \leq i, j \leq q-1}} b_i b_j \zeta^{i-j}\right) \\ &\equiv \alpha^2 - (b_0^2 + \cdots + b_{q-1}^2) - \sum_{\substack{i \neq j \\ 0 \leq i, j \leq q-1}} b_i b_j \equiv \alpha^2 - (b_0 + b_1 + \cdots + b_{q-1})^2. \end{aligned}$$

But we also have for any  $k$ ,  $0 \leq k \leq q - 1$ ,

$$\begin{aligned} (3) \quad S(\chi(g^{-k})\beta) &= S[\zeta^{-k}(b_0 + b_1\zeta + \cdots + b_{q-1}\zeta^{q-1})] \\ &= S(b_0\zeta^{-k} + b_1\zeta^{1-k} + \cdots + b_{q-1}\zeta^{q-1-k}) \\ &\equiv -(b_0 + \cdots + b_{q-1}). \end{aligned}$$

Therefore,  $[S(\chi(g^{-k})\beta)]^2 \equiv (b_0 + \cdots + b_{q-1})^2$  and hence  $0 \equiv \alpha^2 - [S(\chi(g^{-k})\beta)]^2$ . Since  $R'/qR'$  is a field, we see, using (3), that  $\alpha \equiv 0$  if and only if  $S(\chi(g^{-k})\beta) \equiv 0$  for all  $k$ ,  $0 \leq k \leq q - 1$ . If for all  $k$ ,  $0 \leq k \leq q - 1$ , we have  $\alpha \equiv 0$  and  $S(\chi(g^{-k})\beta) \equiv 0$  then let  $\lambda_{\chi'} = \alpha$  and  $\lambda_{\chi} = \beta$ . Suppose for all  $k$ ,  $0 \leq k \leq q - 1$ , we have  $\alpha \not\equiv 0$  and  $S(\chi(g^{-k})\beta) \not\equiv 0$ . Then since  $R'/qR'$  is a field of characteristic not equal to 2 it follows by (3) that either (i)  $0 \equiv \alpha - S(\chi(g^{-k})\beta)$  for all  $k$ ,  $0 \leq k \leq q - 1$ , or (ii)  $0 \equiv \alpha + S(\chi(g^{-k})\beta)$  for all  $k$ ,  $0 \leq k \leq q - 1$ . If (i) holds, let  $\lambda_{\chi'} = -\alpha$  and  $\lambda_{\chi} = \beta$ . If (ii) holds, let  $\lambda_{\chi'} = \alpha$  and  $\lambda_{\chi} = \beta$ . For  $1 \leq i \leq q - 1$  let  $\sigma_i: \zeta \rightarrow \zeta^i \in \mathcal{S}(K/F)$ . For  $1 \leq i \leq q - 1$  let  $\lambda_{\chi^i} = \sigma_i(\lambda_{\chi})$ . By Lemma 2 of [3], the  $q$  relations

$$a_k = q^{-1} \sum_{i=0}^{q-1} \chi^i(g^{-k}) \lambda_{\chi^i}$$

define a  $q$ -square circulant  $A$  over  $F$  such that  $A = \sum_{k=0}^{q-1} a_k P(g^k)$  where  $\lambda_{\chi'}(A) = \lambda_{\chi'}$  and  $\lambda_{\chi}(A) = \lambda_{\chi}$ . By choosing  $\lambda_{\chi'}$  and  $\lambda_{\chi}$  as above  $a_k \in R'$  for all  $k$ . Then for any  $1 \leq i \leq q - 1$  we have, using Lemma 5 of [3],

that  $\lambda_{\chi^i}(M)/\lambda_{\chi^i}(L) = \sigma_i(b) = \sigma_i(N(\beta)) = N(\sigma_i\beta) = N(\sigma_i(\lambda_{\chi}(A))) = N(\lambda_{\chi^i}(A)) = \lambda_{\chi^i}(A^\top)\lambda_{\chi^i}(A)$ . Also by Lemma 5 of [3],  $\lambda_{\chi'}(M)/\lambda_{\chi'}(L) = \alpha^2 = [\lambda_{\chi'}(A)]^2 = \lambda_{\chi'}(A^\top)\lambda_{\chi'}(A)$ . Therefore, by (2) we have  $M = A^\top LA$ .

It remains to show that (ii)  $\Rightarrow$  (iii). Since  $\lambda_{\chi'}(ML^{-1}) = \alpha^2$  and  $\lambda_{\chi}(ML^{-1}) = N(\beta)$  where  $\alpha \in R'$  and  $\beta \in R$  we have that  $\det ML^{-1} = \alpha^2 N_{K/F}(N(\beta))$ . Since  $M$  and  $L$  are unimodular,  $\det ML^{-1}$  is a unit in  $R'$ , and hence  $\beta$  is a unit in  $R$ . We shall show  $N_{K/F}(N(\beta)) \in R'$ . Then  $\alpha$  will be a unit in  $R'$ . The irreducible polynomial of  $\zeta$  over  $F$  is  $x^{q-1} + \cdots + x + 1$ . Therefore, each element of  $R$  can be written uniquely in the form  $a_1\zeta + a_2\zeta^2 + \cdots + a_{q-1}\zeta^{q-1}$  where  $a_i \in R'$ . Therefore,  $N_{K/F}(N(\beta)) = a_1\zeta + \cdots + a_{q-1}\zeta^{q-1} \in F$  where  $a_i \in R'$ . Since this expression is unique and since it is invariant under each  $\tau \in \mathcal{G}(K/F)$  it follows that  $a_1 = a_2 = \cdots = a_{q-1}$ . Hence  $N_{K/F}(N(\beta)) \in R'$ .

Now let us expand our considerations to discuss group matrices for an arbitrary abelian group  $G$  of order  $n$ . Let  $\mathfrak{o}$  denote the ring of integers of a local field  $F$ . A group matrix  $A$  for  $G$  over  $\mathfrak{o}$  is an  $n$ -square matrix of the form  $A = \sum_{g \in G} a_g P(g)$  where  $a_g \in \mathfrak{o}$  and  $P$  is the left regular representation of  $G$  so that using the elements of  $G$  to index the rows and columns of  $P(g)$  it follows that the  $(k, h)$  entry of  $P(g)$  is 1 if  $gh = k$  and zero if  $gh \neq k$ . As in [3], for each character  $\chi$  on  $G$ , we define  $\lambda_{\chi}(A) = \sum_{g \in G} a_g \chi(g)$ .

**LEMMA 2.** *Let  $G$  be an arbitrary abelian group of order  $n$ . Let  $F$  be a local field whose characteristic does not divide  $2n$ . Suppose  $n$  is a unit in  $\mathfrak{o}$  of  $F$ . Let  $M$  and  $L$  be symmetric unimodular group matrices for  $G$  over  $\mathfrak{o}$ , the ring of integers of  $F$ . Then there exists a group matrix  $A$  over  $\mathfrak{o}$  such that  $M = A^\top LA$  if and only if  $\lambda_{\chi}(ML^{-1})$  is the square of a unit in  $\mathfrak{o}$  for each  $\chi$  of order 1 or 2.*

*Proof.* ( $\Rightarrow$ ) Since  $M$  and  $L$  are unimodular  $\lambda_{\chi}(ML^{-1}) = \lambda_{\chi}(M)/\lambda_{\chi}(L)$  is a unit in  $\mathfrak{o}$  for each  $\chi$  of order 1 or 2. The result now follows from Theorem 1 of [3].

( $\Leftarrow$ ) Let  $\{\chi_*\}$  be an independent set of characters. (See definition in § 2 of [3].) If the order of  $\chi_*$  is 1 or 2 and  $\lambda_{\chi_*}(ML^{-1}) = \lambda_{\chi_*}(M)/\lambda_{\chi_*}(L) = \alpha_{\chi_*}^2$  where  $\alpha_{\chi_*}$  is a unit in  $\mathfrak{o}$ , let  $\lambda_{\chi_*} = \alpha_{\chi_*}$ . Suppose the order of  $\chi_*$  is  $d > 2$ . Let  $K = F(\zeta_d)$  and  $k = F(\zeta_d + \zeta_d^{-1})$ . If  $K = k$  then by Lemma 6 of [3] we can assume that the  $d$ -order independent characters occur in independent inverse pairs  $(\chi_*, \chi_*^{-1})$  no two of which have a character in common. For the pair  $(\chi_*, \chi_*^{-1})$  let  $\lambda_{\chi_*} = \lambda_{\chi_*}(M)/\lambda_{\chi_*}(L)$  and  $\lambda_{\chi_*^{-1}} = 1$ . Now suppose  $[K:k] = 2$ . Then, from 32:6a of [10],  $K$  is a quadratic unramified extension of  $k$ . So, since  $M$  and  $L$  are unimodular, it follows from 63:16 of [10] that  $\lambda_{\chi_*}(M)/\lambda_{\chi_*}(L) \in N_{K/k}(U)$  where  $U$  is the group of units of the local field  $K$ . Suppose  $\lambda_{\chi_*}(M)/\lambda_{\chi_*}(L) = N_{K/k}(\alpha_{\chi_*})$  where  $\alpha_{\chi_*} \in U$ . Then let  $\lambda_{\chi_*} = \alpha_{\chi_*}$ . Now use

Lemma 2 of [3] along with the fact that  $n$  is a unit in  $F$  and that  $\lambda_{\chi_*}$  is a unit in  $F(\zeta_d + \zeta_d^{-1})$  where  $d$  is the order of  $\chi_*$  to define a group matrix  $A$  over  $\mathfrak{o}$ . Proceed as in the proof of Theorem 1 of [3] to show that  $M = A^\top LA$ .

4. **Local theory.** Let the notation be that described in §2 with the following additions. Let  $p$  denote an arbitrary prime. Let  $\mathbb{Q}_p$  be the  $p$ -adic numbers. Let the  $F$  of §2 be  $\mathbb{Q}_p$ . Let  $\mathfrak{O}$  be the ring of integers of  $K$ . Let  $R' = \mathbb{Z}_p$  denote the  $p$ -adic integers and  $U'$  the group of units of  $\mathbb{Z}_p$ . If  $F$  is a field let  $F^\times$  denote the multiplicative group  $F \setminus \{0\}$ .

LEMMA 3. *If  $p = q$  then  $\mathfrak{O} = \mathbb{Z}_p + \mathbb{Z}_p\zeta + \cdots + \mathbb{Z}_p\zeta^{q-2}$ .*

*Proof.* Let  $\mathfrak{p}$  be the spot on  $\mathbb{Q}_p$  and  $\mathfrak{P}$  the spot on  $K$ . Let  $|\cdot|_{\mathfrak{p}}$  the normalized valuation on  $K$ . Let  $\Pi = \zeta - 1$ . Since  $K = \mathbb{Q}_p + \mathbb{Q}_p\zeta + \cdots + \mathbb{Q}_p\zeta^{q-2}$  it follows that  $K = \mathbb{Q}_p + \mathbb{Q}_p\Pi + \cdots + \mathbb{Q}_p\Pi^{q-2}$ . So if  $\alpha \in \mathfrak{O}$  then  $\alpha = a_0 + a_1\Pi + \cdots + a_{q-2}\Pi^{q-2}$  where  $a_i \in \mathbb{Q}_p$ . By Lemma 2(ii) of [4],  $K$  is a totally ramified extension of  $\mathbb{Q}_p$  of degree  $q - 1$  and  $\Pi$  is a prime in  $K$ . Hence if  $a_i \in \mathbb{Q}_p$  then  $|a_i|_{\mathfrak{p}} = p^{-c(q-1)}$  where  $c = \text{ord}_{\mathfrak{p}} a_i$ . Therefore, if  $0 \leq j < i \leq q - 2$  and  $a_i, a_j \in \mathbb{Q}_p$  then  $|a_i\Pi^i|_{\mathfrak{p}} \neq |a_j\Pi^j|_{\mathfrak{p}}$ . By the Principle of Domination for any  $a_j \in \mathbb{Q}_p$  where  $0 \leq j \leq q - 2$  we have

$$1 \geq |\alpha|_{\mathfrak{p}} = \max \{|a_i\Pi^i|_{\mathfrak{p}} : 0 \leq i \leq q - 2\} \geq |a_j\Pi^j|_{\mathfrak{p}} = p^{-c(q-1)-j}$$

where  $c = \text{ord}_{\mathfrak{p}} a_j$ . Hence  $c \geq 0$  and so  $|a_j|_{\mathfrak{p}} \leq 1$ .

THEOREM 1. *Let  $M$  and  $L$  be symmetric unimodular  $q$ -square circulants over  $\mathbb{Z}_p$ . Then there exists a  $q$ -square circulant  $A$  over  $\mathbb{Z}_p$  such that  $M = A^\top LA$  if and only if  $\lambda_{\chi}(ML^{-1}) \in U'^2$ .*

*Proof.* ( $\Rightarrow$ ) Since  $M$  and  $L$  are unimodular,  $\lambda_{\chi}(M)/\lambda_{\chi}(L) \in U'$ . Now use Theorem 1 of [4].

( $\Leftarrow$ ) By Theorem 1 of [4] there exists a circulant  $B$  over  $\mathbb{Q}_p$  such that  $M = B^\top LB$ . Hence by Theorem 1 of [3],  $\lambda_{\chi}(ML^{-1}) = \lambda_{\chi}(M)/\lambda_{\chi}(L) \in N(K)$ . Since  $M$  and  $L$  are unimodular, by 32:3 of [10],  $\lambda_{\chi}(ML^{-1}) = \lambda_{\chi}(M)/\lambda_{\chi}(L) \in N(U)$  where  $U$  is the group of units in  $\mathfrak{O}$  of  $K$ .

If  $p = q$  the conclusion follows from Lemma 2(ii) of [4] and Lemmas 1 and 3 where  $F = \mathbb{Q}_p$ ,  $R' = \mathbb{Z}_p$  and  $R = \mathfrak{O}$ . If  $p \neq q$  use Lemma 2 with  $F = \mathbb{Q}_p$  and  $\mathfrak{o} = \mathbb{Z}_p$ .

COROLLARY 1.1. *Let  $M$  and  $L$  be symmetric unimodular circulants over  $\mathbb{Z}_p$ . There exists a circulant  $B$  over  $\mathbb{Q}_p$  such that  $M = B^\top LB$  if and only if there exists a circulant  $A$  over  $\mathbb{Z}_p$  such that  $M = A^\top LA$ .*

*Proof.* ( $\Rightarrow$ ) By Theorem 1 of [4],  $\lambda_{\chi}(ML^{-1}) \in \dot{Q}_p^2$ . Hence  $\lambda_{\chi}(ML^{-1}) \in U'^2$ . The result now follows by Theorem 1.

**THEOREM 2.** *Let  $\{\varepsilon_1, \varepsilon_2\}$  or  $\{\varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4\}$  be representative of the 2 (if  $p \neq 2$ ) or 4 (if  $p = 2$ ) square classes,  $U'/U'^2$ , of units of  $Z_p$ . For a given symmetric unimodular circulant  $M$  over  $Z_p$  there exists a unique  $\varepsilon_i$  such that  $M = A^{\top}(\varepsilon_i I)A$  for some circulant  $A$  over  $Z_p$  (where  $I$  is the identity matrix).*

*Proof.* Pick the  $\varepsilon_i$  which is in the same square class as  $\lambda_{\chi}(M)$  and use Theorem 1.

**DEFINITION.** Let  $S$  denote the set of symmetric unimodular circulants over  $Z_p$ . Let  $M, L \in S$ . We say  $M$  is  $G$ -congruent to  $L$  if there exists a circulant  $A$  over  $Z_p$  such that  $M = A^{\top}LA$ . The equivalence relation of  $G$ -congruence partitions  $S$  into equivalence classes called  $G$ -classes of  $S$ .

**COROLLARY 2.1.** *If  $p \neq 2$  there are two  $G$ -classes of  $S$ . If  $p = 2$  there are four  $G$ -classes of  $S$ .*

**DEFINITION.** Let  $M$  be a symmetric unimodular circulant over  $Z_p$ . Define the discriminant of  $M$ , denoted  $dM$ , to be the square class of the determinant of  $M$ , i.e.,  $dM = (\det M)/U'^2$ .

**THEOREM 3.** *Let  $M$  and  $L$  be symmetric unimodular circulants over  $Z_p$ . Then  $M$  and  $L$  are  $G$ -congruent if and only if  $dM = dL$ .*

*Proof.* Use Theorem 2 and the fact that  $q$  is odd.

5. Global theory. Let the notation be that of §2 except that now  $F = Q$ , the rationals, and  $R' = Z$  the rational integers. Let  $R$  denote the ring of algebraic integers of  $K$  and  $U$  its group of units.

**DEFINITION.** Let  $G$  be an arbitrary abelian group. Let  $G_1$  denote the group of all symmetric unimodular group matrices for  $G$  over  $Z$ . Let  $G_2$  denote the subgroup of  $G_1$  consisting of all the positive definite group matrices. Let  $M, L \in G_1$ . Consider the following two equivalence relations on  $G_1$ .

(i) We say  $M$  and  $L$  are  $G$ -congruent if there exists a group matrix  $A$  over  $Z$  such that  $M = A^{\top}LA$ . The equivalence relation of  $G$ -congruence partitions  $G_1$  into subsets which we call  $G$ -classes. A typical  $G$ -class is denoted as follows

$$\text{cls } M = \{L \in G_1 \mid M \text{ and } L \text{ are } G\text{-congruent}\}.$$

Let  $n_1(G)$ , respectively  $n_2(G)$ , denote the number of subsets into which  $G$ -congruence partitions  $G_1$ , respectively  $G_2$ .

(ii) We say  $M$  and  $L$  are in the same inertia class if  $ML$  is positive definite. We denote an inertia class as follows

$$\text{int } M = \{L \in G_1 \mid M \text{ and } L \text{ are in the same inertia class}\}.$$

Let  $i(G)$  denote the number of inertia classes into which  $G_1$  is partitioned.

**PROPOSITION.** *Let  $M$  and  $L$  be symmetric unimodular group matrices over  $Z$ . The following are equivalent:*

- (i)  $ML$  is positive definite.
- (ii)  $\lambda_\chi(M)\lambda_\chi(L) > 0$  for each  $\chi$ .
- (iii)  $ML^{-1}$  is positive definite.
- (iv) There exists a group matrix  $A_\infty$  over the reals such that  $M = A_\infty^\top L A_\infty$ .
- (v) There exists a group matrix  $A$  over  $Q$  such that  $M = A^\top L A$ .

*Proof.* It is clear from § 2 of [3], (i)  $\Leftrightarrow$  (ii)  $\Leftrightarrow$  (iii). To show (iii)  $\Leftrightarrow$  (iv) use Corollary 1.2 of [3]. That (v)  $\Rightarrow$  (iv) is immediate. If (iv) holds then  $ML^{-1}$  is positive definite. Now apply Corollary 2.1 of [4] to get (v).

**THEOREM 4.** *Let  $M$  and  $L$  be symmetric unimodular group matrices over  $Z$ . If  $\text{cls } M = \text{cls } L$  then  $\text{int } M = \text{int } L$ . Furthermore, given any two inertia classes the number of  $G$ -classes lying inside each of them is the same.*

*Proof.* The first assertion is immediate. To establish the second assertion let  $\text{int } M$  be an arbitrary inertia class. Let  $G_1^2$  denote the group of all squares in  $G_1$ . Consider  $G_2/G_1^2$  which is a subgroup of  $G_1/G_1^2$  and  $(\text{int } M)/G_1^2$  which is a subset of  $G_1/G_1^2$ . By Theorem 4 and Corollary 1 of [5] it suffices to show there is a one-to-one correspondence between the cosets of  $(\text{int } M)/G_1^2$  and the cosets of  $G_2/G_1^2$ . Let  $G_2/G_1^2 = \{M_1G_1^2, \dots, M_sG_1^2\}$ , where  $M_i \in G_2$  ( $1 \leq i \leq s$ ). Let

$$\tau: G_2/G_1^2 \longrightarrow (\text{int } M)/G_1^2$$

via

$$\tau(M_iG_1^2) = MM_iG_1^2$$

for  $1 \leq i \leq s$ . It is easy to show that  $\tau$  is one-to-one. To show  $\tau$  is onto let  $L \in \text{int } M$ . Show  $MM_iG_1^2 = LG_1^2$  for some  $i$ . Since  $M^{-1}L \in G_2$  we have that  $M^{-1}L \in M_iG_1^2$  for some  $i$ . Therefore,  $M^{-1}LG_1^2 = M_iG_1^2$  and hence  $MM_iG_1^2 = M(M^{-1}LG_1^2) = LG_1^2$ .



**COROLLARY 4.1.** *Let  $G$  be an arbitrary abelian group. Then  $i(G)n_2(G) = n_1(G)$ . (A formula for  $n_1(G)$  can be found in [5].)*

Let us once again restrict our discussion to  $q$ -square circulants. Even in this restricted setting the converse of the first assertion of Theorem 4 does not hold. The example at the end of this paper shows that  $\text{int } M = \text{int } L$  does not necessarily imply that  $\text{cls } M = \text{cls } L$ .

The following question is central. If  $M$  and  $L$  are symmetric unimodular circulants then when does there exist a circulant  $A$  such that  $M = A^\top LA$ , i.e., when is it that  $\text{cls } M = \text{cls } L$ ? If  $ML^{-1}$  is not positive definite (i.e.,  $\text{int } M \neq \text{int } L$ ) (and this is easily checked by computation) then  $\text{cls } M \neq \text{cls } L$ . So we may assume  $ML^{-1}$  is positive definite. The question thus reduces itself to the following question. When is a positive definite circulant  $G$ -congruent to the identity matrix  $I$ ? (Since  $G$  is abelian  $M = A^\top LA$  if and only if  $ML^{-1} = A^\top A$ .) Conversely, if criteria can be produced which will establish when two indefinite circulants are  $G$ -congruent then the question of whether or not two positive definite circulants are  $G$ -congruent can be answered. For if  $M$  and  $L$  are positive definite circulants and  $N$  is an arbitrary indefinite circulant then  $NM$  and  $NL$  are indefinite and  $NM$  and  $NL$  are  $G$ -congruent if and only if  $M$  and  $L$  are  $G$ -congruent. This interdependence of the definite and indefinite case (also see Theorem 4) is the most striking way (as far as the author can see to date) in which the theory of  $G$ -classes differs from the ordinary theory of classes of quadratic forms as found in say O'Meara's book [10]. In the ordinary theory of classes of quadratic forms if  $M$  and  $L$  are symmetric unimodular indefinite matrices over  $Z$ , computable criteria exist for determining whether or not there exists a matrix  $A$  over  $Z$  such that  $M = A^\top LA$  [12, Theorem 4 and 5, pp. 92-93]. Whereas if  $M$  and  $L$  are positive definite the situation is quite different and the theory is by no means as definitive.

As an aid to answering the above-mentioned central question we shall give a proof of O. Taussky's result [13] using Lemma 1.

**THEOREM 5.** *Let  $M$  and  $L$  be symmetric unimodular  $q$ -square circulants over  $Z$ . Let  $V$  denote the group of units in the ring of algebraic integers of  $k$ . The following are equivalent:*

- (i) *There exists a circulant  $A$  over  $Z$  such that  $M = A^\top LA$ .*
- (ii)  *$\lambda_x(ML^{-1}) = 1$  and  $\lambda_x(ML^{-1}) \in N(R)$ .*
- (iii)  *$\lambda_x(ML^{-1}) = 1$  and  $\lambda_x(ML^{-1}) \in N(U)$ .*
- (iv)  *$\lambda_x(ML^{-1}) = 1$  and  $\lambda_x(ML^{-1}) \in V^2$ .*

*Proof.* From Lemma 1 and 7-5-4 of [15] it follows that (i)  $\Leftrightarrow$  (ii)  $\Leftrightarrow$  (iii). The equivalence (iii)  $\Leftrightarrow$  (iv) follows from Lemma 10.11 on page 119 of [11].

According to tradition E. C. Dade has shown that for all primes  $q < 100$  except for  $q = 29$  every positive definite symmetric unimodular  $q$ -square circulant over  $Z$  is in the same  $G$ -class. Since this result is not in the literature we will prove Theorem 6 which most likely repeats much of what he did.

Let  $k = Q(\zeta + \zeta^{-1})$ , the maximal real subfield of  $Q(\zeta)$  where  $\zeta$  is a primitive  $q$ th root of 1. Let  $V$  denote the group of units in the ring of algebraic integers of  $k$ . Let  $V^2$  denote the group obtained by squaring all the elements in  $V$ . Let  $T$  be the group of totally positive units in  $V$ . Let  $v_1, \dots, v_p$  denote the cyclotomic units, i.e.,  $v_1 = -1$  and  $v_i = (\zeta^i - \zeta^{-i})/(\zeta - \zeta^{-1})$  for  $i = 2, 3, \dots, p$  where  $p = (q - 1)/2$ . (See page 7 of D. Davis' thesis [1].) Let  $W$  denote the subgroup of  $V$  generated by the cyclotomic units. Consider the Galois group  $\mathcal{S}(k/Q) = \{\sigma_1, \dots, \sigma_p\}$  where  $p = (q - 1)/2$ . If  $\alpha \in k$  let

$$\tau(\alpha) = (\dots, \rho(\sigma_j(\alpha)/|\sigma_j(\alpha)|), \dots)$$

where  $\rho(\sigma_j(\alpha)/|\sigma_j(\alpha)|)$  is in the  $j$ th position and where  $|\cdot|$  denotes the ordinary absolute value function and  $\rho: \{1, -1\} \rightarrow GF(2)$  via  $\rho(1) = 0$  and  $\rho(-1) = 1$ . Let  $M_q$  be the matrix of cyclotomic signatures [1, p. 8] i.e., the  $p$ -square matrix whose  $i$ th row is  $\tau(v_i)$ . Consider the vector space [1, p. 10]

$$GF(2)\mathcal{S}(k/Q) = \{a_1\sigma_1 + \dots + a_p\sigma_p \mid a_i = 0 \text{ or } 1\}.$$

Let

$$\text{sgn}: V \rightarrow GF(2)\mathcal{S}(k/Q)$$

via

$$\text{sgn}(\alpha) = \sum_{j=1}^p \rho(\sigma_j(\alpha)/|\sigma_j(\alpha)|)\sigma_j.$$

The map  $\text{sgn}$  is a homomorphism from the multiplicative group  $V$  into the additive group of  $GF(2)\mathcal{S}(k/Q)$  [1, Lemma 2.4, p. 10]. The kernel of  $\text{sgn}$  is  $T$ . Thus  $V/T$  as a multiplicative group is isomorphic to the additive group  $\text{sgn } V$ . Now thinking of  $\text{sgn } V$  as a vector space over  $GF(2)$  we see that  $(V: T) = 2^a$  where  $a$  is the dimension of  $\text{sgn } V$ .

**THEOREM 6.** *Let  $G$  be a group of prime order  $q$ . Then  $n_2(G)$  divides  $2^{p-s}$  where  $s$  denotes the rank of  $M_q$  and  $p = (q - 1)/2$ .*

*Proof.* Let  $b$  be the dimension of  $\text{sgn } W$ . Then  $b \leq a$  where  $a$  is the dimension of  $\text{sgn } V$ . Thus by Theorem 2.6 on page 11 of [1]  $2^s = 2^b \leq 2^a = (V: T)$ . Since  $(V: V^2) = 2^p$  [1, Theorem 2.3, p.9] we have that  $(T: V^2) = (V: V^2)/(V: T) \leq 2^{p-s}$ . Let  $M$  and  $L$  be elements of  $G_2$ . If  $\lambda_x(M)$  and  $\lambda_x(L)$  are in the same coset of  $T/V^2$  then by Theorem 5 there exists a circulant  $A$  over  $Z$  such that  $M = A^T L A$ .

Hence  $n_2(G) \leq (T:V^2) \leq 2^{p-s}$ . By Theorem 6 of [5],  $n_2(G)$  divides  $2^{p-s}$ .

The tables in the back of D. Davis' thesis [1] inform us that for all primes  $q < 100$  except  $q = 29$  the rank of  $M_q$  is  $p$ . In fact, the tables reveal that for all but 24 of the 156 primes  $q < 1000$  the rank of  $M_q$  is  $p$ . By Theorem 6 if  $q$  is not one of the exceptional 24 primes,  $n_2(G) = 1$ . The example at the end of the paper shows that in the case  $q = 29$  we have that  $n_2(G) \geq 2$ .

**THEOREM 7.** *Let  $q$  be an odd prime. Let the order of  $G$  be  $q$ . If  $p = (q - 1)/2$  is prime and if 2 is a primitive root mod  $p$  then  $n_2(G) = 1$ .*

*Proof.* Use Theorem 3.5 of [1, p. 32] and Theorem 6.

**THEOREM 8.** *Let  $q$  be an odd prime  $\geq 7$ . Let the order of  $G$  be  $q$ . If  $p = (q - 1)/2$  is a prime and  $p \equiv 3 \pmod{8}$  and if  $(p - 1)/2$  is prime then  $n_2(G) = 1$ .*

*Proof.* Use Corollary 3.5.1 of [1, p. 33] and Theorem 6.

## 6. The $G$ -genus.

**DEFINITION.** Let  $M$  and  $L$  be symmetric unimodular group matrices over  $Z$ . We say  $M$  and  $L$  are in the same  $G$ -genus if for each prime  $p$  there exists a group matrix  $A_p$  over  $Z_p$  such that  $M = A_p^\top L A_p$  and there exists a group matrix  $A_\infty$  over the reals such that  $M = A_\infty^\top L A_\infty$ .

**THEOREM 9.** *Let  $M$  and  $L$  be symmetric unimodular circulants over  $Z$ . Then  $M$  and  $L$  are in the same  $G$ -genus if and only if  $M$  and  $L$  are in the same inertia class.*

*Proof.*  $(\Rightarrow)$  This is immediate.

$(\Leftarrow)$  This follows from Theorem 1.

Thus the class number question as translated into the group matrix setting (i.e., how many  $G$ -classes lie in a  $G$ -genus) because of Theorem 4 can be resolved for  $q$ -square circulants if  $n_2(G)$  can be computed.

**7. An example.** The following example will show that if  $G$  is a group of order 29 then  $n_2(G) \geq 2$ .

Let  $p$  be a prime integer. Let  $A = Z/p^n Z$  where  $n \geq 1$ . Let  $\varphi_n: A_n \rightarrow A_{n-1}$  via  $\varphi_n(x + p^n Z) = x + p^{n-1} Z$ . The inverse limit

$$\begin{aligned} Z_p &= \varprojlim (A_n, \varphi_n) \\ &= \left\{ (x_1 + pZ, x_2 + p^2Z, \dots) \in \prod_{n=1}^{\infty} A_n \mid \varphi_n(x_n + p^n Z) \right. \\ &\quad \left. = x_{n-1} + p^{n-1}Z \text{ for } n \geq 2 \right\} \end{aligned}$$

is the ring of  $p$ -adic integers [12, p. 23] where addition and multiplication are coordinatewise. Let  $Q_p$  denote the  $p$ -adic numbers, i.e., the quotient field of  $Z_p$  [12, p. 26]. Let  $\dot{A}_n$  denote the multiplicative subgroup of  $A_n$ .

From now on  $p$  shall denote the prime 59. Since the order of  $\dot{A}_n$  is  $p^{n-1}(p-1)$  it follows from the corollary on page 53 of [6] that there exists a unique multiplicative subgroup of  $\dot{A}_n$  of order 29. Denote this subgroup by  $W_n$ . Let  $\varphi_n$  restricted to  $W_n$  be denoted by  $\varphi'_n$ .

**PROPOSITION.** *For  $n \geq 2$  the map  $\varphi'_n$  is an isomorphism from the multiplicative group  $W_n$  onto the multiplicative group  $W_{n-1}$ . The inverse limit  $W_{\infty} = \varprojlim (W_n, \varphi'_n)$  is the multiplicative group of all the 29th roots of 1 in  $Z_p$ .*

*Proof.* Let  $o(\cdot)$  denote “the order of.” Since  $o(\dot{A}_n) = p^{n-1}(p-1)$ , by the Fundamental Theorem of Finite Abelian Groups we can express  $\dot{A}_n$  as the following internal direct product,  $\dot{A}_n = W_n \times B_n$  where  $o(B_n) = 2p^{n-1}$ . Likewise  $\dot{A}_{n-1} = W_{n-1} \times B_{n-1}$  where  $o(B_{n-1}) = 2p^{n-2}$ . We want to show that  $\varphi_n(W_n) \subseteq W_{n-1}$ . The map  $\varphi_n$  is a multiplicative homomorphism of  $\dot{A}_n$  onto  $\dot{A}_{n-1}$ . Suppose  $z \in W_n$  and  $\varphi_n(z) = x \cdot y$  where  $x \in W_{n-1}$  and  $y \in B_{n-1}$ . Since  $z^{29} = 1$  and  $x^{29} = 1$ , we get  $y^{29} = 1$ . Therefore,  $o(y)$  divides 29. But  $o(y)$  divides  $o(B_{n-1})$ . Hence  $o(y) = 1$ . Similarly  $\varphi_n(B_n) \subseteq B_{n-1}$ . Since  $\varphi$  maps  $\dot{A}_n$  onto  $\dot{A}_{n-1}$ , the above results establish that  $\varphi'_n(W_n) = W_{n-1}$ . Also if  $x \in Z_p$  then  $x^{29} = 1$  if and only if  $x \in W_{\infty}$ .

Now to construct a number  $u \in Z_p$  which among other things is not a square in  $Q_p$ . First note that  $3 + pZ \neq 1 + pZ$ , but  $(3 + pZ)^{29} = 1 + pZ$ . By the preceding proposition there exists one and only one  $\alpha = (x_1 + pZ, \dots) \in W_{\infty}$  such that  $x_i + pZ = 3 + pZ$ . For  $i = 2, 3, \dots, 14$  let

$$(4) \quad u_i = (\alpha^i - \alpha^{-1})/(\alpha - \alpha^{-1}).$$

Let

$$u = (u_2 u_3 u_5 u_7 u_8 u_9 u_{11} u_{13})(u_4 u_{10} u_{12})^4.$$

For  $j = 1, \dots, 14$ , let  $\omega_j = \alpha^j + \alpha^{-j}$ . If  $i$  is even ( $2 \leq i \leq 14$ ), then

$$(5) \quad u_i = \omega_1 + \omega_3 + \omega_5 + \cdots + \omega_{i-1}.$$

If  $i$  is odd ( $2 \leq i \leq 14$ ), then

$$(6) \quad u_i = 1 + \omega_2 + \omega_4 + \omega_6 + \cdots + \omega_{i-1}.$$

Hence for  $2 \leq i \leq 14$ ,  $u_i \in Z_p$ . To show  $u$  is not a square in  $Q_p$  it suffices to show  $w = u_2 u_3 u_5 u_7 u_8 u_9 u_{11} u_{13}$  is not a square in  $Q_p$ . Using (4), (5), and (6) one can deduce that  $w = (y_1 + pZ, \cdots)$  is a unit in  $Z_p$ . By Theorem 3 on page 34 of [12],  $w$  is a square in  $\dot{Q}_p$  if and only if  $y_1 + pZ$  is a square in  $\dot{A}_1$ . Calculation using (5) and (6) will show that  $y_1 + pZ = 33 + pZ$ . Let  $(\div)$  denote the Legendre symbol. Since  $(33/59) = -1$ , it follows that  $33 + pZ$  is not a square in  $\dot{A}_1$  and hence  $u$  is not a square in  $Q_p$ .

Let  $\zeta$  be the following complex number  $\zeta = e^{2\pi i/29}$ . Let  $K = Q(\zeta)$  and  $k = Q(\zeta + \zeta^{-1})$ . For  $i = 2, 3, \cdots, 14$ , let

$$v_i = (\zeta^i - \zeta^{-i})/(\zeta - \zeta^{-1})$$

and let

$$v = (v_2 v_3 v_5 v_7 v_8 v_9 v_{11} v_{13})(v_4 v_{10} v_{12})^4.$$

Let  $Q(\alpha)$  be the smallest field in  $Q_p$  containing  $Q$  and  $\alpha$ . Let  $\varphi(x) = 1 + x + x^2 + \cdots + x^{28}$ . Then both  $Q(\zeta)$  and  $Q(\alpha)$  are splitting fields of  $\varphi(x)$  over  $Q$ . By the corollary and Theorem 5.J. on page 184 of [6] there is an isomorphism  $\sigma$  from  $Q(\zeta)$  onto  $Q(\alpha)$  fixing  $Q$  such that  $\sigma(\zeta) = \alpha$ . Now  $v \in k$  [1, p. 7]. If  $v$  were a square in  $k$  then  $\sigma(v) = u$  would be a square in  $Q(\alpha) \subseteq Q_p$ , a contradiction. Hence  $v$  is not a square in  $k$ . Furthermore, it can be shown that  $v$  is a totally positive unit in the ring of algebraic integers of  $k$ . This can be done directly or by using the more rapid methods of Chapter II of [1].

For  $j = 1, 2, \cdots, 14$ , let  $y_j = x^j + x^{29-j}$ . If  $i$  is even ( $2 \leq i \leq 14$ ), let

$$v_i(x) = y_1 + y_3 + y_5 + \cdots + y_{i-1}.$$

If  $i$  is odd ( $2 \leq i \leq 14$ ), let

$$v_i(x) = 1 + y_2 + y_4 + y_6 + \cdots + y_{i-1}.$$

Then  $v_i(\zeta) = v_i$  and  $v_i(1) = i$ . Let

$$v(x) = (v_2(x)v_3(x)v_5(x)v_7(x)v_8(x)v_9(x)v_{11}(x)v_{13}(x))(v_4(x)v_{10}(x)v_{12}(x))^4.$$

Then  $v(\zeta) = v$  and  $v(1) \equiv 1 \pmod{29}$ .

If  $a(x) \in Z[x]$  and if  $b(x) = a(x) + t\varphi(x)$  where  $t \in Z$  then  $a(\zeta) = b(\zeta)$  but  $b(1) = a(1) + 29t$ . Hence there exists  $m(x) \in Z[x]$  of degree at most 28 such that  $m(\zeta) = v$  and yet  $0 \leq m(1) \leq 28$ . Since  $v(\zeta) -$

$m(\zeta) = 0$ , we see by using the corollary on page 269 of [2] that  $v(x) - m(x) = c(x)\mathcal{P}(x)$  where  $c(x) \in Z[x]$ . Since  $v(1) \equiv 1 \pmod{29}$  and  $\mathcal{P}(1) = 29$  we get  $m(1) = 1$ . If  $m(x) = m_0 + m_1x + \cdots + m_{28}x^{28}$  then let  $M = \sum_{i=0}^{28} m_i P(g^i)$ . This  $M$  is a positive definite, symmetric, unimodular, 29-square circulant over  $Z$  such that  $\lambda_\chi(M)$  is not the square of a unit and hence by Theorem 5,  $M$  and  $I$  are not  $G$ -congruent. Thus  $n_2(G) \geq 2$ .

## REFERENCES

1. D. Davis, *On the distribution of the signs of the conjugates of the cyclotomic units in the maximal real subfield of the  $q^{\text{th}}$  cyclotomic field*,  $q$  a prime, Thesis, California Institute of Technology, 1969.
2. J. Fraleigh, *A First Course in Abstract Algebra*, Addison-Wesley, 1967.
3. D. Garbanati, *Classes of nonsingular abelian group matrices over fields*, J. Algebra, to appear.
4. ———, *Abelian group matrices over the  $p$ -adic and rational integers*, J. Number Theory, to appear.
5. D. Garbanati and R. C. Thompson, *Classes of unimodular abelian group matrices*, Pacific J. Math., to appear.
6. I. Herstein, *Topics in Algebra*, Blaisdell Publishing Company, 1964.
7. M. Newman, *Circulant quadratic forms*, Report of the Institute in the Theory of Numbers, Boulder, Colorado, (1959), 189–192.
8. M. Newman and O. Taussky, *Classes of positive definite circulants*, Canad. J. Math., **9** (1957), 71–73.
9. ———, *On a generalization of the normal basis in abelian algebraic number fields*, Comm. Pure and Appl. Math., **19** (1956), 85–91.
10. O. T. O'Meara, *Introduction to Quadratic Forms*, Springer-Verlag, 1971.
11. H. Pollard, *The Theory of Algebraic Numbers*, The Mathematical Association of America, 1950.
12. J.-P. Serre, *Cours d'arithmétique*, Presses Universitaires de France, Paris, 1970.
13. O. Taussky, *Unimodular integral circulants*, Math. Z., **63** (1955), 286–289.
14. R. C. Thompson, *Classes of definite group matrices*, Pacific J. Math., **17** (1966), 175–190.
15. E. Weiss, *Algebraic Number Theory*, McGraw-Hill, 1963.

Received October 11, 1972. The preparation of this paper was supported in part by U. S. Air Force Office of Scientific Research Grant AFOSR-72-2164.

UNIVERSITY OF CALIFORNIA, SANTA BARBARA  
AND  
UNIVERSITY OF NOTRE DAME



# PACIFIC JOURNAL OF MATHEMATICS

## EDITORS

RICHARD ARENS (Managing Editor)  
University of California  
Los Angeles, California 90024

J. DUGUNDJI\*  
Department of Mathematics  
University of Southern California  
Los Angeles, California 90007

R. A. BEAUMONT  
University of Washington  
Seattle, Washington 98105

D. GILBARG AND J. MILGRAM  
Stanford University  
Stanford, California 94305

## ASSOCIATE EDITORS

E. F. BECKENBACH

B. H. NEUMANN

F. WOLF

K. YOSHIDA

## SUPPORTING INSTITUTIONS

UNIVERSITY OF BRITISH COLUMBIA  
CALIFORNIA INSTITUTE OF TECHNOLOGY  
UNIVERSITY OF CALIFORNIA  
MONTANA STATE UNIVERSITY  
UNIVERSITY OF NEVADA  
NEW MEXICO STATE UNIVERSITY  
OREGON STATE UNIVERSITY  
UNIVERSITY OF OREGON  
OSAKA UNIVERSITY

UNIVERSITY OF SOUTHERN CALIFORNIA  
STANFORD UNIVERSITY  
UNIVERSITY OF TOKYO  
UNIVERSITY OF UTAH  
WASHINGTON STATE UNIVERSITY  
UNIVERSITY OF WASHINGTON  
\* \* \*  
AMERICAN MATHEMATICAL SOCIETY  
NAVAL WEAPONS CENTER

---

The Supporting Institutions listed above contribute to the cost of publication of this Journal, but they are not owners or publishers and have no responsibility for its content or policies.

---

Mathematical papers intended for publication in the *Pacific Journal of Mathematics* should be in typed form or offset-reproduced, (not dittoed), double spaced with large margins. Underline Greek letters in red, German in green, and script in blue. The first paragraph or two must be capable of being used separately as a synopsis of the entire paper. Items of the bibliography should not be cited there unless absolutely necessary, in which case they must be identified by author and Journal, rather than by item number. Manuscripts, in duplicate if possible, may be sent to any one of the four editors. Please classify according to the scheme of Math. Rev. Index to Vol. 39. All other communications to the editors should be addressed to the managing editor, or Elaine Barth, University of California, Los Angeles, California, 90024.

100 reprints are provided free for each article, only if page charges have been substantially paid. Additional copies may be obtained at cost in multiples of 50.

---

The *Pacific Journal of Mathematics* is issued monthly as of January 1966. Regular subscription rate: \$60.00 a year (6 Vols., 12 issues). Special rate: \$30.00 a year to individual members of supporting institutions.

Subscriptions, orders for back numbers, and changes of address should be sent to Pacific Journal of Mathematics, 103 Highland Boulevard, Berkeley, California, 94708.

PUBLISHED BY PACIFIC JOURNAL OF MATHEMATICS, A NON-PROFIT CORPORATION

Printed at Kokusai Bunken Insatsusha (International Academic Printing Co., Ltd.), 270, 3-chome Totsuka-cho, Shinjuku-ku, Tokyo 160, Japan

\* C. R. DePrima California Institute of Technology, Pasadena, CA 91109, will replace J. Dugundji until August 1974.

Copyright © 1973 by Pacific Journal of Mathematics  
Manufactured and first issued in Japan



Mustafa Agah Akcoglu, John Philip Huneke and Hermann Rost, <i>A counter example to the Blum Hanson theorem in general spaces</i> .....	305
Huzihiro Araki, <i>Some properties of modular conjugation operator of von Neumann algebras and a non-commutative Radon-Nikodym theorem with a chain rule</i> .....	309
E. F. Beckenbach, Fook H. Eng and Richard Edward Tafel, <i>Global properties of rational and logarithmico-rational minimal surfaces</i> .....	355
David W. Boyd, <i>A new class of infinite sphere packings</i> .....	383
K. G. Choo, <i>Whitehead Groups of twisted free associative algebras</i> .....	399
Charles Kam-Tai Chui and Milton N. Parnes, <i>Limit sets of power series outside the circles of convergence</i> .....	403
Allan Clark and John Harwood Ewing, <i>The realization of polynomial algebras as cohomology rings</i> .....	425
Dennis Garbanati, <i>Classes of circulants over the p-adic and rational integers</i> .....	435
Arjun K. Gupta, <i>On a "square" functional equation</i> .....	449
David James Hallenbeck and Thomas Harold MacGregor, <i>Subordination and extreme-point theory</i> .....	455
Douglas Harris, <i>The local compactness of <math>vX</math></i> .....	469
William Emery Haver, <i>Monotone mappings of a two-disk onto itself which fix the disk's boundary can be canonically approximated by homeomorphisms</i> .....	477
Norman Peter Herzberg, <i>On a problem of Hurwitz</i> .....	485
Chin-Shui Hsu, <i>A class of Abelian groups closed under direct limits and subgroups formation</i> .....	495
Bjarni Jónsson and Thomas Paul Whaley, <i>Congruence relations and multiplicity types of algebras</i> .....	505
Lowell Duane Loveland, <i>Vertically countable spheres and their wild sets</i> .....	521
Nimrod Megiddo, <i>Kernels of compound games with simple components</i> .....	531
Russell L. Merris, <i>An identity for matrix functions</i> .....	557
E. O. Milton, <i>Fourier transforms of odd and even tempered distributions</i> .....	563
Dix Hayes Pettey, <i>One-one-mappings onto locally connected generalized continua</i> .....	573
Mark Bernard Ramras, <i>Orders with finite global dimension</i> .....	583
Doron Ravdin, <i>Various types of local homogeneity</i> .....	589
George Michael Reed, <i>On metrizability of complete Moore spaces</i> .....	595
Charles Small, <i>Normal bases for quadratic extensions</i> .....	601
Philip C. Tonne, <i>Polynomials and Hausdorff matrices</i> .....	613
Robert Earl Weber, <i>The range of a derivation and ideals</i> .....	617