Diagonalizations of Circulant Matrices and Analogous Reductions for Group Matrices

Roger Chalkley

April 26, 2002

1. INTRODUCTION. The main purpose of this completely expository paper is to help numerous persons acquire a better historical perspective about the subject of circulant matrices and its most natural generalizations.

Of the many rediscoveries of old results about circulant matrices, we are particularly aware of the ones in the recent article [21] titled "Polynomial Equations and Circulant Matrices." That paper deals with an interesting subject but fails to mention that its main results were clearly presented with complete detail in the easily accessible papers [4, 5, 6] that were published 27 years earlier by the MAA. While the key reference [13] in [21, page 840] does list the title "Circulant Matrices and Algebraic Equations" of [5] along with acknowledgment of [4, 5, 7] on [13, page 237], the basic idea of using circulant matrices to solve polynomial equations is much older.

Our translation of the summary by Emil Lampe in [22] for [20] of 1904 states that: Question 15319 is the problem of finding a, b, c in terms of p, q, r so that the equation $X^4 + p\,X^2 + q\,X + r = 0$ can be rewritten and solved as

$$\begin{vmatrix} X & a & b & c \\ c & X & a & b \\ b & c & X & a \\ a & b & c & X \end{vmatrix} = 0. \tag{1}$$

We are to interpret p, q, r, a, b, c, and $\boldsymbol{i}$ as complex numbers such that $\boldsymbol{i}^2 = -1$. Then, the linear factors $X+a+b+c$, $X+\boldsymbol{i}\,a-b-\boldsymbol{i}\,c$, $X-a+b-c$, $X-\boldsymbol{i}\,a-b+\boldsymbol{i}\,c$ for the left member of (1) yield the solutions of $X^4+p\,X^2+q\,X+r=0$. This had been done twenty-four years earlier by L. Clariana y Ricart in [29] of 1880. In [3] of 1882, Arthur Cayley used a primitive 5th root of unity and the corresponding linear factors for the determinant of a 5×5 circulant matrix to study the roots of a fifth-degree polynomial. In [24] of 1883, Alphonse Legoux showed in detail how a root ω of $X^2 + X + 1 = 0$ and the identity

$$\begin{vmatrix} X & a_1 & a_2 \\ a_2 & X & a_1 \\ a_1 & a_2 & X \end{vmatrix} = (X + a_1 + a_2)(X + \omega a_1 + \omega^2 a_2)(X + \omega^2 a_1 + \omega a_2)$$

can be used to obtain the roots of $X^3 + pX + q = 0$. Legoux also presents the technique described for (1); and he explains how the linear factors for the determinant of an $n \times n$ circulant matrix allow the procedures to be generalized. In [26] of 1883, Arthur Lodge provided more detail for the case $n = 4$ considered in [24]; in particular, he examined questions about the reality of the roots when the coefficients of the 4th degree polynomial are real numbers. Thomas Muir reports in [27, Vol. 4, page 370] that he withdrew from publication in 1882 a paper of his on this general subject when he learned about [3] of 1882; he then discovered [29] of 1880 much later.

These investigations were suggested by a basic result that Richard Balzer published in [1, page 92] of 1864; namely, from [27, Vol. 3, pages 374–375], we learned that: for any complex numbers a_0, a_1, ..., a_{n-1}, Balzer showed that the n solutions of

$$\begin{vmatrix} a_0 - X & a_1 & a_2 & \dots & a_{n-1} \\ a_{n-1} & a_0 - X & a_1 & \dots & a_{n-2} \\ a_{n-2} & a_{n-1} & a_0 - X & \dots & a_{n-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_1 & a_2 & a_3 & \dots & a_0 - X \end{vmatrix} = 0 \tag{2}$$

are given in terms of a primitive nth root ρ of unity by

$$x_i = \sum_{j=0}^{n-1} a_j \, \rho^{(i-1)j}, \quad \text{for } 1 \le i \le n.$$

When X is replaced with 0, the left member of (2) is the determinant $det(A)$ of a circulant matrix A. The factorization $(x_1 - X)(x_2 - X) \cdots (x_n - X)$ for the left member of (2) shows that the substitution $X = 0$ yields

$$det(A) = \prod_{i=1}^{n} \left[\sum_{j=0}^{n-1} a_j \, \rho^{(i-1)j} \right]. \tag{3}$$

Muir's publications [27, Vol.2, Ch. 14; Vol. 3, Ch. 15] give information about the work of three contributors to the earlier discovery of (3). His four volumes are particularly useful for references before the appearance in 1868 of the first volume of the *Jahrbuch über die Fortschritte der Mathematik*. For instance, in [27, Vol. 2, page 401], he credits the earliest introduction of a circulant (i.e., determinant of a circulant matrix) to Eugène Catalan in [2] of 1846.

For the class of $n \times n$ circulant matrices over the field $\mathbb{C}$ of complex numbers, we present basic results in Section 2. With the usual operations of matrix addition, multiplication, and scalar multiplication, that class forms an algebra over $\mathbb{C}$ that is isomorphic to the algebra of $n \times n$ diagonal matrices over $\mathbb{C}$. Group matrices are introduced in Definition 4 of Section 3 and some of their numerous classes are considered in Sections 3–5. The $n \times n$ circulant matrices form the most familiar class of group matrices. The group characters developed for finite

abelian groups in Section 7 are applied in Section 8 to show that: each class of group matrices for a finite abelian group G of order n forms an algebra over $\mathbb{C}$ that is isomorphic to the commutative algebra of $n \times n$ diagonal matrices over $\mathbb{C}$. The arguments needed for these results are all simple ones that can be traced to the 1880's and 1890's through [32, pages 38–53]. In contrast, each class of group matrices for a finite noncommutative group is isomorphic to a noncommutative algebra of block diagonal matrices specified by the much more difficult research of Georg Frobenius in [15, 16, 17]. Thus, of the various group matrices, it is the ones for abelian groups to which current interests in circulant matrices can be easily extended. In Section 9, we shall merely mention several key results about the much deeper investigation of Frobenius. Fortunately, there are several excellent historical surveys about his research. Both [9] by Keith Conrad and [11] by Charles Curtis are clearly written and very interesting. For one who may wish to read the original papers [15, 16, 17], the context of [32] and the brief summary in [32, pages 193–218] can also be helpful.

2. GENERALIZABLE RESULTS FOR CIRCULANT MATRICES. An $n \times n$ matrix A over the field $\mathbb{C}$ of complex numbers is a circulant matrix when there are elements $a_0, a_1, \ldots, a_{n-1}$ in $\mathbb{C}$ such that

$$A = \begin{bmatrix} a_0 & a_1 & a_2 & \ldots & a_{n-1} \\ a_{n-1} & a_0 & a_1 & \ldots & a_{n-2} \\ a_{n-2} & a_{n-1} & a_0 & \ldots & a_{n-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_1 & a_2 & a_3 & \ldots & a_0 \end{bmatrix}. \tag{4}$$

For the list $S = (e, \alpha, \alpha^2, \ldots, \alpha^{n-1})$ of the n distinct elements in a cyclic group C_n of order n in which e (for German *Einheit*) is the unit element and $\alpha^n = e$, we set $g_1 = e$, $g_2 = \alpha$, $g_3 = \alpha^2$, $\ldots$, $g_n = \alpha^{n-1}$ and obtain

	g_1	g_2	g_3	$\ldots$	g_n
g_1^{-1}	e	α	α^2	$\ldots$	α^{n-1}
g_2^{-1}	α^{n-1}	e	α	$\ldots$	α^{n-2}
g_3^{-1}	α^{n-2}	α^{n-1}	e	$\ldots$	α^{n-3}
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
g_n^{-1}	α	α^2	α^3	$\ldots$	e

(5)

as the multiplication table for C_n in terms of S. Thus, an $n \times n$ matrix A over $\mathbb{C}$ is a circulant matrix if and only if there are elements $a_0, a_1, \ldots, a_{n-1}$ in $\mathbb{C}$ such that the function σ on C_n to $\mathbb{C}$ defined by $\sigma(\alpha^k) = a_k$, for $0 \le k \le n-1$, specifies the (r, s)-component $[A]_{r,s}$ of A as

$$[A]_{r,s} = \sigma(g_r^{-1} g_s) = \sigma\big(\alpha^{n+1-r}\alpha^{s-1}\big) = \sigma\big(\alpha^{s-r}\big), \quad \text{for } 1 \le r, s \le n. \tag{6}$$

The first equality in (6) motivates Definition 4 of a group matrix.

For $n \geq 2$, various tables differing from (5) could be used as our starting point. For instance, in place of (5), we could begin with

	g_1^{-1}	g_2^{-1}	g_3^{-1}	$\dots$	g_n^{-1}
g_1	e	α^{n-1}	α^{n-2}	$\dots$	α
g_2	α	e	α^{n-1}	$\dots$	α^2
g_3	α^2	α	e	$\dots$	α^3
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
g_n	α^{n-1}	α^{n-2}	α^{n-3}	$\dots$	e

(7)

as the multiplication table for C_n. Thus, an $n \times n$ matrix A over $\mathbb{C}$ is a circulant matrix if and only if there are elements a_0, a_1, $\dots$, a_{n-1} in $\mathbb{C}$ such that the function τ on C_n to $\mathbb{C}$ defined by $\tau(\alpha^k) = a_{n-k}$, for $1 \leq k \leq n$, specifies the (r, s)-component $[A]_{r,s}$ of A by means of

$$[A]_{r,s} = \tau\big(g_r\, g_s^{-1}\big) = \tau\big(\alpha^{r-1}\alpha^{1-s}\big) = \tau\big(\alpha^{r-s}\big), \quad \text{for } 1 \leq r, s \leq n.$$

The interiors of both multiplication tables (5) and (7) preserve their form when cyclic permutations are performed on g_1, g_2, $\dots$, g_n as column labels for (5) or as row labels for (7). Our preference for (5) rather than (7) was the reason we introduced in [7] of 1976 the standardly adopted notation $\sigma(g_r^{-1}g_s)$ in (16) of Definition 4 rather than notation like $\tau(g_r g_s^{-1})$.

In the spirit of matrices as place holders for the arguments of determinants, Luigi Cremona introduced, in [10] of 1856, the $n \times n$ matrix M over $\mathbb{C}$ that is specified in terms of a primitive n-th root ρ of unity in $\mathbb{C}$ by

$$[M]_{r,s} = \rho^{(r-1)(s-1)}, \quad \text{for } 1 \leq r, s \leq n. \tag{8}$$

For a particular matrix B obtainable from A in (4) by a permutation of its last $n-1$ rows, Cremona used the determinant of M to express the determinant of B as a product of linear combinations of its components. He credited the idea to Francesco Brioschi. It was soon found that the simpler formula (3) results when A is used in place of B. After addition, multiplication, and scalar multiplication for matrices became available, various arguments could be simplified. In particular, it is easily shown that the $n \times n$ matrix L defined in terms of ρ by

$$[L]_{r,s} = \frac{1}{n}\, \rho^{-(r-1)(s-1)}, \quad \text{for } 1 \leq r, s \leq n, \tag{9}$$

is such that LM is the $n \times n$ identity matrix. Thus, M is a nonsingular matrix and its inverse is L. Additional contributions gave the following result.

Theorem 1. (Fundamental Theorem about Circulant Matrices) *An $n \times n$ matrix A over $\mathbb{C}$ is a circulant matrix if and only if the matrix $M^{-1}AM$ is a diagonal matrix. Moreover, when A is the $n \times n$ circulant matrix in (4), the (r, r)-component of the diagonal matrix $D = M^{-1}AM$ is given by*

$$[D]_{r,r} = \sum_{j=0}^{n-1} a_j\, \rho^{(r-1)j}, \quad \textit{for } 1 \leq r \leq n. \tag{10}$$

A clear proof of Theorem 1 was presented in [5, pages 73–75]. That it is a consequence of Theorem 17 will be noted in Example 21.

Proposition 2. *The set $\mathcal{A}_n$ of $n \times n$ circulant matrices over $\mathbb{C}$ and the set $\mathcal{D}_n$ of $n \times n$ diagonal matrices over $\mathbb{C}$ form isomorphic commutative algebras over $\mathbb{C}$ with respect to the matrix operations of addition, multiplication, and scalar multiplication.*

Proof. Let ψ be the function on $\mathcal{D}_n$ to $\mathcal{A}_n$ that is defined according to Theorem 1 by $\psi(D) = MDM^{-1}$, for each D in $\mathcal{D}_n$. For A in $\mathcal{A}_n$, the matrix $D = M^{-1}AM$ belongs to $\mathcal{D}_n$; and it yields $\psi(D) = A$. Moreover, if D_1 and D_2 in $\mathcal{D}_n$ give $\psi(D_1) = \psi(D_2)$, then $D_1 = D_2$. Thus, ψ establishes a one-to-one correspondence between the elements of $\mathcal{D}_n$ and $\mathcal{A}_n$. For D_1, D_2 in $\mathcal{D}_n$ and c in $\mathbb{C}$, the matrices $D_1 + D_2$, $D_1 D_2$, and cD_1 belong to $\mathcal{D}_n$ and satisfy $D_1 D_2 = D_2 D_1$; thus, $\mathcal{D}_n$ forms a commutative algebra over $\mathbb{C}$. Those matrices yield

$$\psi(D_1 + D_2) = \psi(D_1) + \psi(D_2), \quad \psi(D_1 D_2) = \psi(D_1)\,\psi(D_2),$$

and $\psi(cD_1) = c\psi(D_1)$. We use $\mathcal{A}_n = \psi(\mathcal{D}_n)$ and the properties of ψ to conclude that $\mathcal{A}_n$ forms an algebra over $\mathbb{C}$ that is isomorphic to $\mathcal{D}_n$. As subalgebras of the algebra of all $n \times n$ matrices over $\mathbb{C}$, they are associative. ■

For any $n \times n$ circulant matrix A over $\mathbb{C}$ and its corresponding diagonal matrix $D = M^{-1}AM$, the relation $AM = MD$ yields the following conclusion. *The columns of M constitute n linearly independent eigenvectors over $\mathbb{C}$ for A; and the corresponding eigenvalues for A are the diagonal elements of D.* Due to $det(A) = detD$, we see that (3) expresses $det(A)$ as the product of its eigenvalues given by (10).

The inverse A^{-1} of a nonsingular circulant matrix A is a circulant matrix. Namely, the diagonal matrix $D = M^{-1}AM$ is nonsingular, its inverse D^{-1} is a diagonal matrix given by $D^{-1} = M^{-1}A^{-1}M$, and therefore A^{-1} is the circulant matrix given by $A^{-1} = MD^{-1}M^{-1}$. This result was presented in [18].

The transpose of a circulant matrix is a circulant matrix. By looking at (4), we can convince ourselves that this is true. However, we seek a proof that can be generalized later to show the less obvious result that the transpose of any group matrix is a group matrix of the same type. For this purpose, suppose that A is an $n \times n$ circulant matrix whose components are given by (6); let υ be the function on C_n to C_n defined by $\upsilon(x) = x^{-1}$, for each x in C_n; and let τ be the function $\tau = \sigma \circ \upsilon$ on C_n to $\mathbb{C}$. Then, for $1 \le r,\, s \le n$, we have

$$[A^T]_{r,s} = [A]_{s,r} = \sigma\big(g_s^{-1} g_r\big) = \sigma\big(\upsilon(g_r^{-1} g_s)\big) = \tau(g_r^{-1} g_s). \tag{11}$$

Thus, A^T is a circulant matrix. For an interesting alternative argument having less generality, we can specialize Proposition 16 to our present context.

As motivation for old results about group characters in Theorem 13, we note that: in terms of the list S used in (5) for the elements of the cyclic group C_n, the $(r,\, s)$-component of M in (8) is also specified by

$$[M]_{r,s} = \left(\rho^{r-1}\right)^{s-1} = \chi_r(g_s), \quad \text{for } 1 \le r,\, s \le n,$$

where, for each fixed integer r satisfying $1 \le r \le n$, χ_r is the function on C_n to $\mathbb{C}$ defined by

$$\chi_r(\alpha^{s-1}) = \left(\rho^{r-1}\right)^{s-1}, \quad \text{for } 1 \le s \le n. \tag{12}$$

We introduce $Char(C_n)$ as the set consisting of $\chi_1,\, \chi_2,\, \ldots,\, \chi_n$ and we recall that: for any two functions $\phi,\, \psi$ on C_n to $\mathbb{C}$, a product function $\phi\,\psi$ on C_n to $\mathbb{C}$ is defined by $(\phi\,\psi)(x) = \phi(x)\;\psi(x)$, for each x in C_n.

Proposition 3. *The functions $\chi_1,\, \chi_2,\, \ldots,\, \chi_n$ satisfy*

$$\chi_r(x\,y) = \chi_r(x)\;\chi_r(y), \quad \textit{for } 1 \le r \le n \textit{ and any } x,\, y \textit{ in } C_n, \tag{13}$$

and, with respect to $S = (g_1,\ g_2,\, \ldots,\, g_n) = (e,\, \alpha,\, \ldots,\, \alpha^{n-1})$,

$$\chi_r(g_s) = \chi_s(g_r), \quad \textit{for } 1 \le r,\, s \le n. \tag{14}$$

Moreover, in terms of multiplication of functions, $Char(C_n)$ forms a cyclic group of order n.

Proof. By expressing any integer i in the form $i = q\,n + (s-1)$, with $1 \le s \le n$, and using $\alpha^n = e$ as well as $\rho^n = 1$, we find that

$$\chi_r(\alpha^i) = \chi_r(\alpha^{s-1}) = \left(\rho^{r-1}\right)^{s-1} = \left(\rho^{r-1}\right)^{i}, \quad \text{for } 1 \le r \le n. \tag{15}$$

In terms of $x = \alpha^i$ and $y = \alpha^j$, for some integers $i,\, j$, we apply (15) to obtain

$$\chi_r(x\,y) = \chi_r(\alpha^{i+j}) = \left(\rho^{r-1}\right)^{i+j} = \left(\rho^{r-1}\right)^{i}\left(\rho^{r-1}\right)^{j} = \chi_r(x)\;\chi_r(y),$$

for $1 \le r \le n$. Thus, (13) is valid. Moreover, (12) yields (14) immediately. To show that $Char(C_n)$ is closed under multiplication, let $i,\, r,\, s$ denote any integers that satisfy $1 \le i,\, r,\, s \le n$. Then, there is a unique integer t such that $1 \le t \le n$ and $g_r\, g_s = g_t$. We combine this with (14) and (13) to deduce that

$$(\chi_r\,\chi_s)(g_i) = \chi_r(g_i)\;\chi_s(g_i) = \chi_i(g_r)\;\chi_i(g_s) = \chi_i(g_r\,g_s) = \chi_i(g_t) = \chi_t(g_i).$$

Since g_i can be any element of C_n, we have $\chi_r\,\chi_s = \chi_t$. Thus, $Char(G)$ is closed under multiplication. Moreover, the one-to-one correspondence between G and $Char(C_n)$ specified by $g_r \mapsto \chi_r$, for $1 \le r \le n$, shows that $Char(C_n)$ has a group structure that makes it isomorphic to C_n. ∎

Up to this point, each result in this section remains valid when the field $\mathbb{C}$ of complex numbers is replaced by any field F in which the polynomial $X^n - 1$ has a root ρ such that no two of the elements ρ, ρ^2, $\ldots$ ρ^n are equal. In particular, for $f(X) = X^n - 1$, we then have $n\rho^{n-1} = f'(\rho) \neq 0$ as well as $n \cdot 1 \neq 0$. Then, the expression $(1/n)\,\rho^{-(r-1)(s-1)}$ in (9) is well defined as an element of F. Other generalizations are possible at the expense of an awkward context.

For the situation $F = \mathbb{C}$, we can replace M in Theorem 1 with a unitary matrix. To do this, we first note that the complex conjugate $\overline{\rho}$ of the primitive nth root ρ of unity introduced for M in (8) yields $\rho\,\overline{\rho} = |\rho|^2 = |\rho^n|^{2/n} = 1$ and $\overline{\rho} = \rho^{-1}$. The complex conjugate $\overline{N}$ of any matrix N over $\mathbb{C}$ is the matrix obtained from N by replacing each component with its complex conjugate. Thus, for M and L in (8) and (9), we find that $\overline{M} = nL = nM^{-1}$. The *hermitian transpose* N^H of any matrix N over $\mathbb{C}$ is the transpose $(\overline{N})^T$ of the conjugate $\overline{N}$ of N. Since M in (8) is symmetric, we have $M^H = nL = nM^{-1}$. Consequently, the matrix $U = \dfrac{1}{\sqrt{n}}M$ yields

$$U^H U = \frac{1}{\sqrt{n}} M^H \frac{1}{\sqrt{n}} M = M^{-1}M = I_n,$$

where I_n is the $n \times n$ identity matrix. Thus, we obtain $U^{-1} = U^H$ and U is therefore a unitary matrix. In terms of it, Theorem 1 can be restated as follows. *An $n \times n$ matrix A over $\mathbb{C}$ is a circulant matrix if and only if the matrix $U^H AU$ is a diagonal matrix.*

3. CLASSES OF GROUP MATRICES. Each group matrix for a finite group G is associated with some list for the elements in G (as a total ordering). Because a multiplication table of the form (5) exhibits the list more naturally than one of the type (7), we use (5) as a model for the following definition.

Definition 4. Let G be a finite group of order n, let $S = (g_1, g_2, \ldots, g_n)$ be a list of the elements in G, and let F be a field. Then, an $n \times n$ matrix A over F is a *group matrix* for G relative to S when there is a function σ on G to F such that the (r, s)-component of A is given by

$$[A]_{r,s} = \sigma(g_r^{-1} g_s), \quad \text{for } 1 \leq r, s \leq n. \tag{16}$$

Before [7] of 1976, the terminology *group matrix* referred to a somewhat different concept used by Frobenius in [15, 16, 17] and presented in Context 28. To avoid confusion, we used the term *G-matrix* in place of *group matrix* for the concept of Definition 4 when it was introduced in [7]. Because nearly all the papers on group matrices after [7] have adopted the definition of a G-matrix in [7] as the standard definition of a group matrix, we have continued that practice in Definition 4. We shall show in Formulation 29 of Section 9 that the original type of group matrix as employed by Frobenius can be obtained by specializing Definition 4.

Notation 5. For a field F, a given finite group G of order n, and a list $S = (g_1, g_2, \ldots, g_n)$ for G, the symbol $F[G, S]$ denotes the class (i.e., set) of those $n \times n$ matrices over F that are group matrices for G with respect to S.

Example 6. Suppose that G is the cyclic group C_4 of order 4 with elements e, α, α^2, α^3. Then, the three multiplication tables

	e	α	α^2	α^3
e	e	α	α^2	α^3
α^3	α^3	e	α	α^2
α^2	α^2	α^3	e	α
α	α	α^2	α^3	e

	e	α^2	α^3	α
e	e	α^2	α^3	α
α^2	α^2	e	α	α^3
α^3	α^3	α	e	α^2
α	α	α^3	α^2	e

	e	α	α^3	α^2
e	e	α	α^3	α^2
α^3	α^3	e	α^2	α
α	α	α^2	e	α^3
α^2	α^2	α^3	α	e

for C_4 correspond respectively to the three lists

$$S_1 = (e, \alpha, \alpha^2, \alpha^3), \quad S_2 = (e, \alpha^2, \alpha^3, \alpha), \quad S_3 = (e, \alpha, \alpha^3, \alpha^2)$$

of its elements. With respect to a, b, c, d in F and suitable functions on G to F, the three multiplication tables yield the respective matrices

$$A_1 = \begin{bmatrix} a & b & c & d \\ d & a & b & c \\ c & d & a & b \\ b & c & d & a \end{bmatrix}, \; A_2 = \begin{bmatrix} a & b & c & d \\ b & a & d & c \\ d & c & a & b \\ c & d & b & a \end{bmatrix}, \; A_3 = \begin{bmatrix} a & b & c & d \\ c & a & d & b \\ b & d & a & c \\ d & c & b & a \end{bmatrix}. \tag{17}$$

The class $\mathbb{C}[C_4, S_1]$ of group matrices for $F = \mathbb{C}$, $G = C_4$, and $S = S_1$ consists of the matrices having the form of A_1 as a, b, c, d range through $\mathbb{C}$. Similarly, $\mathbb{C}[C_4, S_2]$ and $\mathbb{C}[C_4, S_3]$ consist of matrices having the respective forms of A_2 and A_3. As sets of elements, no two of $\mathbb{C}[C_4, S_1]$, $\mathbb{C}[C_4, S_2]$, and $\mathbb{C}[C_4, S_3]$ are equal. Of the 24 lists for the elements of C_4, 8 yield matrices of the form A_1, another 8 give matrices of the form A_2, and the remaining 8 provide matrices of the form A_3. Thus, when $F = \mathbb{C}$, there are precisely three classes of group matrices for a cyclic group of order 4. For perspective, see Example 10.

Definition 4 and Notation 5 merely involve F as a set of elements. One will notice other situations where the assumption that F is a field is not essential.

Proposition 7. *Suppose that S and T are any two lists for the elements of a finite group G of order n. Then, there is an $n \times n$ permutation matrix P over F such that the matrices in $F[G, T]$ are given by PAP^T as A ranges through the matrices in $F[G, S]$.*

Proof. With $S = (g_1, g_2, \ldots, g_n)$, let π be the permutation of $(1, 2, \ldots, n)$ such that $T = (g_{\pi(1)}, g_{\pi(2)}, \ldots, g_{\pi(n)})$. For $1 \leq r, s \leq n$, we set $\delta(r, s) = 1$, when $r = s$, and $\delta(r, s) = 0$, when $r \neq s$. Let P be the $n \times n$ permutation matrix over F given by $[P]_{r,s} = \delta(\pi(r), s)$, for $1 \leq r, s \leq n$. It is the matrix

obtained from the $n \times n$ identity matrix by permuting the rows according to π. Then, for any function σ on G to F, the $n \times n$ matrices A and B specified by

$$[A]_{r,s} = \sigma(g_r^{-1} g_s) \quad \text{and} \quad [B]_{r,s} = \sigma(g_{\pi(r)}^{-1}\, g_{\pi(s)}), \quad \text{for } 1 \le r,\, s \le n,$$

belong respectively to $F[G, S]$ and $F[G, T]$. They yield

$$[PAP^T]_{r,s} = \sum_{i=1}^{n} \sum_{j=1}^{n} \delta(\pi(r),\, i)\; \sigma(g_i^{-1} g_j)\; \delta(\pi(s),\, j) = \sigma(g_{\pi(r)}^{-1}\, g_{\pi(s)}) = [B]_{r,s},$$

for $1 \le r,\, s \le n$, and therefore $PAP^T = B$. Thus, as A ranges over $F[G, S]$, the matrices in $F[G, T]$ are given by PAP^T. ■

4. THE NUMBER OF CLASSES FOR A GIVEN FINITE GROUP. Definition 4 and Notation 5 both have meaning when F is replaced by any set containing at least two elements. In particular, when a, b, c, d range through such a set, that is sufficient for the matrices of the respective forms A_1, A_2, A_3 in (17) to specify three distinct classes. Consequently, as a combinatorial problem, *the number $N(G)$ of classes of group matrices for a finite group G is the same for each F that contains at least two elements.*

To present a formula for $N(G)$, we recall that: for any group G, a function θ on G to G is an *automorphism of G* when it is one-to-one, onto, and satisfies

$$\theta(x\, y) = \theta(x)\, \theta(y), \quad \text{for each } x,\, y \text{ in } G.$$

The set $Aut(G)$ of automorphisms of a group G contains the identity function on G defined by $x \mapsto x$, for each x in G. Also, if θ_1 and θ_2 are automorphisms of G, then their composite function $\theta_1 \circ \theta_2$ is an automorphisms of G. Moreover, each automorphism of G has an inverse function that is an automorphism of G. Thus, *$Aut(G)$ is a group under composition of functions.*

Theorem 8. *For a finite group G of order n, the number m of automorphisms of G divides $(n-1)!$ and the number $N(G)$ of classes of group matrices that G specifies is given by*

$$N(G) = \frac{(n-1)!}{m}. \tag{18}$$

A clear proof for this result of ours was presented in [8, pages 122–124].

By employing $|H|$ to indicate the order of any finite group H, the dependence of the right member for (18) on G alone is made more explicit as

$$N(G) = \frac{(|G|-1)!}{|Aut(G)|}.$$

Corollary 9. *The number $N(C_n)$ of classes of group matrices for a cyclic group C_n of order n is given by*

$$N(C_n) = \frac{(n-1)!}{\phi(n)}, \tag{19}$$

where $\phi(n)$ is the number of positive integers $\leq n$ that are relatively prime to n.

Proof. Let α be an element of period n in a cyclic group C_n of order n. For any automorphism θ of G, the period of $\theta(\alpha)$ is n. Also, if β is any element of period n in G and θ is defined by $\theta(\alpha^k) = \beta^k$, for $1 \leq k \leq n$, then it is easily checked that θ is an automorphism of C_n. Thus, the number of automorphisms for C_n is equal to the number of elements of period n in C_n. Representing the elements of C_n by α^k for $1 \leq k \leq n$, we find that the period of α^k is n if and only if k is relatively prime to n. Thus, the number m of automorphisms of C_n is given by $m = \phi(n)$. Now, (18) yields (19). ∎

Euler's ϕ-function in (19) is given by $\phi(1) = 1$ and

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right), \quad \text{for } n \geq 2,$$

where $p_1, p_2, \ldots p_k$ are the distinct prime integers that divide n; for instance, see [28, pages 51, 69].

Example 10. For the cyclic group C_4 in Example 6, we have $n = 2^2$ and $\phi(4) = 2$ so that (19) yields $N(C_4) = 3!/2 = 3$. Similarly, for C_6, we have $n = 2 \cdot 3$, $\phi(n) = 2$, and $N(C_6) = 5!/2 = 60$. Thus, for a cyclic group of order 6, there are 59 other classes of group matrices in addition to the class of 6×6 circulant matrices.

5. MACHINE COMPUTATIONS TO EXHIBIT THE CLASSES. Typical personal computers of current capability can be employed to exhibit the form for each of the $N(G)$ classes of group matrices for a finite group G of order n when $n \leq 8$ or slightly larger. Since $N(G)$ is independent of F so long as F has at least two elements, we assume that F contains a polynomial ring $K[X_1, X_2, \ldots, X_n]$ in n algebraically independent variables over a field K. Then, each class of group matrices for G over F contains one and only one group matrix having $X_1, X_2, \ldots, X_n$ as the respective components of its first row. In particular, if $S = (g_1, g_2, \ldots, g_n)$ is a list for G that specifies a particular class, then the (r, s)-component of the unique matrix just mentioned in that class is given in terms of $\sigma(g_j) = X_j$, for $1 \leq j \leq n$, by $\sigma(g_r^{-1} g_s)$, for $1 \leq r, s \leq n$.

With respect to a system of computer algebra such as MATHEMATICA, we can proceed as follows before making important modifications to reduce storage requirements. For a given finite group G whose order n is limited as previously described, use a suitable multiplication table to specify a particular

group matrix A_0 for G that has $X_1, X_2, \ldots, X_n$ as the respective components of its first row. Represent each of the $n \times n$ permutation matrices by symbols that correspond to $P_1, P_2, \ldots, P_{n!}$. For $1 \le i \le n!$, introduce $A_i = P_i A_0 P_i^T$. For $1 \le i \le n!$, define $Y_{i,1}, Y_{i,2}, \ldots, Y_{i,n}$ as the respective components of the first row of A_i. For $1 \le i \le n!$, let B_i denote the matrix obtained from A_i by replacing each occurrence of the variables $Y_{i,1}, Y_{i,2}, \ldots, Y_{i,n}$ in A_i with the corresponding variables $X_1, X_2, \ldots, X_n$. Proposition 7 shows that the sequence $B_1, B_2, \ldots, B_{n!}$ contains all of the group matrices for G that have the respective components of their first row given by $X_1, X_2, \ldots, X_n$; and it contains only matrices of that type. Moreover, for $n \ge 2$, each matrix it contains is repeated. By eliminating the repetitions, we obtain $N(G)$ distinct matrices of which each represents one and only one of the $N(G)$ distinct classes of group matrices.

To greatly reduce the memory requirements, we give an improved procedure. Enter A_0 and the $n!$ permutation matrices $P_1, P_2, \ldots, P_{n!}$ as before. Introduce a counter k initialized as $k = 1$, set $A_1 = P_1 A_0 P_1^T$, obtain B_1 as previously described, set $H_1 = B_1$, print H_1, erase the computation of B_1, and then proceed step by step from $i = 2$ to $i = n!$ as follows. At step i, set $A_i = P_i A_0 P_i^T$, introduce B_i as previously described, and compare B_i with each of $H_1, \ldots, H_k$. If B_i is equal to one of $H_1, \ldots, H_k$, then: erase from memory the computation used to compare B_i with $H_1, \ldots, H_k$; erase the computation of B_i; and continue to $i+1$ only when $i+1 \le n!$. If B_i is unequal to each of $H_1, \ldots, H_k$, increase k by 1, set $H_k = B_i$, print H_k, erase from memory the computation used to compare B_i with the previous H_j's, erase the computation of B_i, and continue to the next $i+1$ only when $i+1 \le n!$.

When the procedure just described is applied to each of the cyclic groups C_n of order $n \le 9$, it yields $N(C_n)$ in agreement with (19) of Corollary 9. When G is the symmetric group $\mathfrak{S}_3$ of order 6 consisting of the permutations on three objects, it gives $N(\mathfrak{S}_3) = 20$. Consequently, (18) of Theorem 8 shows that the group $\mathfrak{S}_3$ has $(6-1)!/20 = 6$ automorphisms. When G is the quaternion group $\mathcal{Q}$ of order 8 consisting of the eight elements $\mathbf{1}$, $-\mathbf{1}$, $\boldsymbol{i}$, $-\boldsymbol{i}$, $\boldsymbol{j}$, $-\boldsymbol{j}$, $\boldsymbol{k}$, $-\boldsymbol{k}$ under multiplication of quaternions (where $\boldsymbol{i}^2 = -1$, $\boldsymbol{i} \cdot \boldsymbol{j} = \boldsymbol{k}$, $\boldsymbol{j} \cdot \boldsymbol{i} = -\boldsymbol{k}$, etc.), we obtain $N(\mathcal{Q}) = 210$. Thus, (18) of Theorem 8 shows that the quaternion group $\mathcal{Q}$ has $(8-1)!/210 = 24$ automorphisms. In each situation, fewer than 12 MB of random access memory was used. For $n \le 7$, the computations are completed in minutes. For $n \ge 8$, one or more hours may be needed.

6. THE GROUP ALGEBRA $F[G]$. For any finite group G of order n and any field F, let $F[G]$ denote the set of functions on G to F. Let addition, multiplication, and scalar multiplication be defined for $F[G]$ with respect to σ_1, σ_2 in $F[G]$ and c in F by $(\sigma_1 + \sigma_2)(x) = \sigma_1(x) + \sigma_2(x)$, for each x in G,

$$(\sigma_1 * \sigma_2)(x) = \sum_{y \in G} \sigma_1(y)\, \sigma_2(y^{-1}x), \quad \text{for each } x \text{ in } G, \tag{20}$$

and $(c\,\sigma_1)(x) = c\,\sigma_1(x)$, for each x in G.

Given any list $S = (g_1, g_2, \ldots, g_n)$ for G, there is a corresponding class $F[G, S]$ of group matrices and there is a one-to-one function Ψ_S of $F[G, S]$ onto $F[G]$ that is defined for each group matrix A in $F[G, S]$ by $\Psi_S(A) = \sigma$, where σ in $F[G]$ is such that $[A]_{r,s} = \sigma(g_r^{-1} g_s)$, for $1 \leq r, s \leq n$. In his context, the following result was known to Frobenius in [17] of 1897.

Proposition 11. *With the matrix operations of addition, multiplication, and scalar multiplication, $F[G, S]$ forms an associative algebra over F. Moreover, with the addition, multiplication, and scalar multiplication introduced for it, $F[G]$ forms an algebra over F that is isomorphic to $F[G, S]$.*

Proof. For A_1, A_2 in $F[G, S]$, set $\sigma_1 = \Psi_S(A_1)$ and $\sigma_2 = \Psi_S(A_2)$. Then, we have

$$\begin{aligned}[A_1 + A_2]_{r,s} &= [A_1]_{r,s} + [A_2]_{r,s} = \sigma_1(g_r^{-1} g_s) + \sigma_2(g_r^{-1} g_s) \\ &= (\sigma_1 + \sigma_2)(g_r^{-1} g_s), \quad \text{for } 1 \leq r, s \leq n.\end{aligned}$$

This shows that $A_1 + A_2$ belongs to $F[G, S]$ and $\Psi_S(A_1 + A_2) = \Psi_S(A_1) + \Psi_S(A_2)$. We find that

$$\begin{aligned}[A_1 A_2]_{r,s} &= \sum_{j=1}^{n} [A_1]_{r,j} \, [A_2]_{j,s} = \sum_{j=1}^{n} \sigma_1(g_r^{-1} g_j) \, \sigma_2\big((g_j^{-1} g_r)(g_r^{-1} g_s)\big) \\ &= (\sigma_1 * \sigma_2)(g_r^{-1} g_s), \quad \text{for } 1 \leq r, s \leq n.\end{aligned}$$

Thus, $A_1 A_2$ belongs to $F[G, S]$ and $\Psi_S(A_1 A_2) = \sigma_1 * \sigma_2 = \Psi_S(A_1) * \Psi_S(A_2)$. We note that $[cA_1]_{r,s} = c[A_1]_{r,s} = c\,\sigma_1(g_r^{-1} g_s) = (c\,\sigma_1)(g_r^{-1} g_s)$, for $1 \leq r, s \leq n$, and $\Psi_S(cA_1) = c\Psi_S(A_1)$. Hence, $F[G, S]$ is a subalgebra of the algebra of all $n \times n$ matrices over F. Since Ψ_S is a one-to-one correspondence between $F[G, S]$ and $F[G]$ that preserves the operations of addition, multiplication, and scalar multiplication, we see that $F[G]$ forms an algebra over F that is isomorphic to $F[G, S]$. Moreover, because matrix multiplication is associative, both of these algebras are associative. ■

The argument for (11) shows that *an $n \times n$ matrix A over F belongs to $F[G, S]$ if and only if A^T belongs to $F[G, S]$.*

The standard expression for multiplication in $F[G]$ (as given, for instance, in [19, pages 255–256]) can be obtained by introducing notation for special functions in $F[G]$. Thus, for each c in F and g in G, we define $c \cdot g$ as the function in $F[G]$ such that, for any x in G: $(c \cdot g)(x) = c$, if $x = g$; and $(c \cdot g)(x) = 0$, if $x \neq g$. For a, b in F and u, v, x in G, we use (20) to obtain

$$\big((a \cdot u) * (b \cdot v)\big)(x) = \sum_{y \in G} \big[(a \cdot u)(y)\big] \big[(b \cdot v)(y^{-1} x)\big] = \big((a\,b) \cdot u\,v\big)(x) \qquad (21)$$

and therefore $(a \cdot u) * (b \cdot v) = (ab) \cdot u\,v$. Thus, multiplication is given by

$$\sigma_1 * \sigma_2 = \left[\sum_{p=1}^{n} \sigma_1(g_p) \cdot g_p\right] * \left[\sum_{q=1}^{n} \sigma_2(g_q) \cdot g_q\right] = \sum_{1 \leq p,q \leq n} \big(\sigma_1(g_p)\,\sigma_2(g_q)\big) \cdot g_p\, g_q.$$

This shows clearly that *multiplication for $F[G]$ is commutative if and only if G is abelian.* The isomorphism of $F[G, S]$ and $F[G]$ yields the following assertion.

Proposition 12. *The multiplication for $F[G, S]$ is commutative if and only if G is abelian.*

7. GROUP CHARACTERS FOR FINITE ABELIAN GROUPS. In [15, page 985] of 1896, Georg Frobenius defined a *group character* for a finite abelian group G as a function χ on G to $\mathbb{C}$ that satisfies $\chi(x\,y) = \chi(x)\,\chi(y) \neq 0$, for each x, y in G; and he indicated where special cases of the concept had been previously used. For instance, Lejeune Dirichlet employed particular characters in defining L-series for his 1837 proof that: whenever b and m are relatively prime positive integers, infinitely many terms of the sequence

$$b,\, b+m,\, b+2m,\, b+3m,\, \ldots$$

are prime integers; e.g., see [14]. More information about the early use of group characters is given in [11, pages 1–34] and [9]. We need group characters in order to construct a matrix M for Proposition 14 that will serve in Theorem 17 to diagonalize abelian-group matrices in a manner similar to the diagonalization of circulant matrices in Theorem 1.

For the unit element e of G, we must have $\chi(e) = \chi(e)\,\chi(e) \neq 0$ and $\chi(e) = 1$. When $|G| = n$, each element x in G yields $\big(\chi(x)\big)^n = \chi(x^n) = \chi(e) = 1$. Thus, $\chi(x)$ is an n-th root of unity for each x in G. In view of this, various old results that parallel the development in [32, pages 49–53] of 1899 can be easily presented in a more general context.

Throughout this section and the next, we suppose that *G is a finite abelian group of order n and $S = (g_1,\, g_2,\, \ldots,\, g_n)$ is a list of its elements.* In addition, we merely assume that *F is a field that contains a primitive nth root ρ of unity* in the usual sense that $\rho^n = 1$ and the n elements $1,\, \rho,\, \rho^2,\, \ldots \rho^{n-1}$ are distinct. In this context, a *group character for G* is a function χ on G to F such that

$$\chi(x\,y) = \chi(x)\,\chi(y) \neq 0, \quad \text{for each } x,\, y \text{ in } G. \tag{22}$$

A *direct product* of cyclic groups will provide the structure for G that enables all of its characters to be specified explicitly. To explain, suppose that q is a positive integer and, for $1 \leq j \leq q$, C_{n_j} is a cyclic group of order n_j with unit element e_j. Then, the Cartesian product $H = C_{n_1} \times C_{n_2} \times \cdots \times C_{n_p}$ has elements

$$x = (\xi_1,\, \xi_2,\, \ldots,\, \xi_q) \quad \text{and} \quad y = (\eta_1,\, \eta_2,\, \ldots,\, \eta_q), \tag{23}$$

where ξ_j and η_j belong to C_{n_j}, for $1 \leq j \leq q$. The set H becomes an abelian group when the product $x\,y$ of any two such elements x and y in H is defined by means of $x\,y = (\xi_1\,\eta_1,\, \xi_2\,\eta_2,\, \ldots,\, \xi_q\,\eta_q)$. The element $(e_1,\, e_2,\, \ldots,\, e_q)$ in H is its unit element; and $x^{-1} = (\xi_1^{-1},\, \xi_2^{-1},\, \ldots,\, \xi_q^{-1})$ in H is the inverse for x of (23). As a group, H is called the *direct product* of the groups $C_{n_1},\, C_{n_2},\, \ldots,\, C_{n_q}$ and its order is equal to $n_1\,n_2\,\cdots\,n_q$.

For some positive integer p and each j satisfying $1 \le j \le p$, there are cyclic groups C_{n_j} of order n_j such that the finite abelian group G is isomorphic to the direct product $C_{n_1} \times C_{n_2} \times \cdots \times C_{n_p}$; e.g., see [19, page 40, Theorem 3.3.1]. Thus, elements $\alpha_1, \alpha_2, \ldots, \alpha_p$ in G of respective periods $n_1, n_2, \ldots, n_p$ exist such that: for each x in G, there are unique integers $x_1, x_2, \ldots, x_p$ that satisfy

$$x = \alpha_1^{x_1}\, \alpha_2^{x_2} \cdots \alpha_p^{x_p} \quad \text{and} \quad 0 \le x_j \le n_j - 1, \text{ for } 1 \le j \le p. \tag{24}$$

We have $n = n_1\, n_2 \cdots n_p$. If χ is a character for G, then (22) and (24) yield

$$\chi(x) = \big(\chi(\alpha_1)\big)^{x_1} \big(\chi(\alpha_2)\big)^{x_2} \cdots \big(\chi(\alpha_p)\big)^{x_p}.$$

For $j = 1, 2, \ldots, p$, we see that $\alpha_j^{n_j} = e$ and $\big(\chi(\alpha_j)\big)^{n_j} = 1$. Since there are at most n_j possible values for $\chi(\alpha_j)$, *G has at most n group characters.*

To specify n group characters for G with respect to $S = (g_1, g_2, \ldots, g_n)$, we proceed as follows. For $1 \le i \le n$, let $\nu_{i,1}, \nu_{i,2}, \ldots, \nu_{i,p}$ denote the unique integers such that

$$g_i = \alpha_1^{\nu_{i,1}}\, \alpha_2^{\nu_{i,2}} \cdots \alpha_p^{\nu_{i,p}} \quad \text{and} \quad 0 \le \nu_{i,j} \le n_j - 1, \text{ for } 1 \le j \le p. \tag{25}$$

In terms of (24) as a unique representation for each x in G, a function χ_i on G to F is defined in terms of $\rho_j = \rho^{n/n_j}$, for $1 \le j \le p$, and the $\nu_{i,j}$ for (25) by

$$\chi_i(x) = \big(\rho_1^{\nu_{i,1}}\big)^{x_1} \big(\rho_2^{\nu_{i,2}}\big)^{x_2} \cdots \big(\rho_p^{\nu_{i,p}}\big)^{x_p}, \quad \text{for } i = 1, 2, \ldots, n. \tag{26}$$

Theorem 13. *Under multiplication of functions, the set $Char(G)$ of group characters for a finite abelian group G of order n forms an abelian group of order n that is isomorphic to G. Moreover, the functions $\chi_1, \chi_2, \ldots, \chi_n$ on G to F defined by* (24)–(26) *are the elements of $Char(G)$; and, in terms of the unit element e of G, they satisfy*

$$\chi_r(g_s) = \chi_s(g_r) \quad \textit{and} \quad \chi_r(g_s^{-1}) = \chi_s(g_r^{-1}), \quad \textit{for } 1 \le r, s \le n, \tag{27}$$

as well as

$$\sum_{i=1}^{n} \chi_i(x) = \begin{cases} n, & \textit{if } x = e, \\ 0, & \textit{for } x \textit{ in } G \textit{ and } x \ne e. \end{cases} \tag{28}$$

Proof. For any integers $s_1, \ldots, s_p$, let $q_1, \ldots, q_p$ and $r_1, \ldots, r_p$ be integers such that $s_j = q_j\, n_j + r_j$ and $0 \le r_j \le n_j - 1$, for $1 \le j \le p$. Then, for $1 \le i \le n$ and $1 \le j \le p$, we employ $\alpha_j^{n_j} = e$ and $\rho_j^{n_j} = (\rho^{n/n_j})^{n_j} = 1$ to see that

$$\chi_i(\alpha_1^{s_1} \cdots \alpha_p^{s_p}) = \chi_i(\alpha_1^{r_1} \cdots \alpha_p^{r_p}) = \big(\rho_1^{\nu_{i,1}}\big)^{r_1} \cdots \big(\rho_p^{\nu_{i,p}}\big)^{r_p} = \big(\rho_1^{\nu_{i,1}}\big)^{s_1} \cdots \big(\rho_p^{\nu_{i,p}}\big)^{s_p}.$$

Hence, for any elements x and y in G, we can represent x as in (24) and y by $y = \alpha_1^{y_1} \cdots \alpha_p^{y_p}$, with $0 \le y_j \le n_j - 1$ for $1 \le j \le p$, to deduce that

$$\chi_i(x\,y) = \chi_i(\alpha_1^{x_1+y_1} \cdots \alpha_p^{x_p+y_p}) = \big(\rho_1^{\nu_{i,1}}\big)^{x_1+y_1} \cdots \big(\rho_p^{\nu_{i,p}}\big)^{x_p+y_p} = \chi_i(x)\, \chi_i(y).$$

Thus, each of $\chi_1, \chi_2, \ldots, \chi_n$ is a group character for G; and they constitute all the elements of $Char(G)$ because G can have at most n group characters. We apply (24)–(26) to verify that

$$\chi_r(g_s) = \left(\rho_1^{\nu_{r,1}}\right)^{\nu_{s,1}} \cdots \left(\rho_p^{\nu_{r,p}}\right)^{\nu_{s,p}} = \left(\rho_1^{\nu_{s,1}}\right)^{\nu_{r,1}} \cdots \left(\rho_p^{\nu_{s,p}}\right)^{\nu_{r,p}} = \chi_s(g_r)$$

and $\chi_r(g_s^{-1}) = \left(\chi_r(g_s)\right)^{-1} = \left(\chi_s(g_r)\right)^{-1} = \chi_s(g_r^{-1})$, for $1 \le r, s \le n$. Hence, (27) is valid. For any χ_r, χ_s in $Char(G)$ and any x, y in G, we use the property of group characters in (22) to obtain

$$\begin{aligned}(\chi_r\,\chi_s)(x\,y) &= \chi_r(x\,y)\,\chi_s(x\,y) = \chi_r(x)\,\chi_r(y)\,\chi_s(x)\,\chi_s(y) \\ &= (\chi_r\,\chi_s)(x)\,(\chi_r\,\chi_s)(y)\end{aligned}$$

and conclude that $\chi_r\chi_s$ is a group character for G. This shows that $Char(G)$ is closed under multiplication of functions. Let μ be the integer such that $1 \le \mu \le n$ and g_μ is the unit element e in G. With $i = \mu$ and $\nu_{\mu,j} = 0$, for $1 \le j \le p$, we apply (25) and (26) to deduce that $\chi_\mu(x) = 1$, for each x in G. Hence, $Char(G)$ has χ_μ as a unit element. For any χ_κ in $Char(G)$, let g_λ be the inverse element for g_κ in G. Then, for any g_i in G, we find that

$$(\chi_\kappa\,\chi_\lambda)(g_i) = \chi_\kappa(g_i)\,\chi_\lambda(g_i) = \chi_i(g_\kappa)\,\chi_i(g_\lambda) = \chi_i(g_\mu) = \chi_\mu(g_i)$$

and $\chi_\kappa\,\chi_\lambda = \chi_\mu$. Thus, each element in $Char(G)$ has an inverse in $Char(G)$. Also, multiplication of functions is associative. Hence, $Char(G)$ forms a group. Let Φ be the function on G to $Char(C)$ such that $\Phi(g_i) = \chi_i$, for $1 \le i \le n$. Given g_r and g_s in G, we let g_t denote the unique element in G for which $g_r\,g_s = g_t$. Then, for any g_i in G, we have

$$\chi_t(g_i) = \chi_i(g_t) = \chi_i(g_r)\,\chi_i(g_s) = \chi_r(g_i)\,\chi_s(g_i) = (\chi_r\,\chi_s)(g_i)$$

and therefore $\chi_t = \chi_r\,\chi_s$. Rewriting the latter as $\Phi(g_r\,g_s) = \Phi(g_r)\,\Phi(g_s)$, we see that Φ is an isomorphism of G onto $Char(G)$.

Let S denote the left member of (28). If $x = e$, then $\chi_i(x) = 1$, for $1 \le i \le n$, and $S = n$. In any case, as i ranges through $1, 2, \ldots, n$, the corresponding p-tuples $(\nu_{i,1}, \nu_{i,2}, \ldots, \nu_{i,p})$ for (26) range over the p-tuples $(\tau_1, \tau_2, \ldots, \tau_p)$ of integers having $0 \le \tau_j \le n_j - 1$, for $1 \le j \le p$. Thus, (28), (24), and (26) yield

$$S = \left[\sum_{\tau=0}^{n_1-1} \left(\rho_1^{x_1}\right)^\tau\right]\left[\sum_{\tau=0}^{n_2-1} \left(\rho_2^{x_2}\right)^\tau\right] \cdots \left[\sum_{\tau=0}^{n_p-1} \left(\rho_p^{x_p}\right)^\tau\right]. \tag{29}$$

For x in G given by (24), suppose that $x \ne e$. Then, there is an integer j such that $1 \le j \le p$, $0 < x_j \le n_j - 1$, and $\rho_j^{x_j} \ne 1$. Setting $r = \rho_j^{x_j}$, we use $r \ne 1$ and $r^{n_j} = \rho_j^{n_j\,x_j} = (\rho^n)^{x_j} = 1$ to see that the factor

$$\sum_{\tau=0}^{n_j-1} r^\tau = \frac{r^{n_j} - 1}{r - 1} = 0$$

of S in (29) yields $S = 0$. This completes the proof. ■

8. A DIAGONALIZATION FOR ABELIAN-GROUP MATRICES. In this section we retain the context introduced for (22) where S is a list of the elements for a finite abelian group G of order n and F is a field that contains a primitive nth root of unity. The n distinct characters $\chi_1, \chi_2, \ldots, \chi_n$ for G defined by (25)–(26) enable us to introduce an $n \times n$ matrix over F by means of

$$[M]_{r,s} = \chi_r(g_s), \quad \text{for } 1 \le r, s \le n. \tag{30}$$

Since the roots of $f(X) = X^n - 1 = (X-\rho)(X-\rho^2)\cdots(X-\rho^n)$ are distinct, we obtain $n\rho^{n-1} = (\rho-\rho^2)\cdots(\rho-\rho^n) \neq 0$ by a formal differentiation of $f(X)$ and a substitution of ρ for X. Thus, $1/n$ can be interpreted as an element of F; and an $n \times n$ matrix L is well defined over F by

$$[L]_{r,s} = \frac{1}{n}\,\chi_r(g_s^{-1}), \quad \text{for } 1 \le r, s \le n. \tag{31}$$

In view of (27), *M and L are symmetric matrices.*

Proposition 14. *The matrix M is nonsingular and L is its inverse.*

Proof. We apply (31), (30), (27), and (22) to obtain

$$\begin{aligned}[LM]_{r,s} &= \sum_{i=1}^{n} [L]_{r,i}\,[M]_{i,s} = \frac{1}{n}\sum_{i=1}^{n} \chi_r(g_i^{-1})\,\chi_i(g_s) \\ &= \frac{1}{n}\sum_{i=1}^{n} \chi_i(g_r^{-1})\,\chi_i(g_s) = \frac{1}{n}\sum_{i=1}^{n} \chi_i(g_r^{-1}\,g_s), \quad \text{for } 1 \le r, s \le n.\end{aligned}$$

We compare this with (28) to see that $[LM]_{r,s}$ equals 1 when $r = s$ and it equals 0 when $r \neq s$. Consequently, M is nonsingular and its inverse is L. ∎

Observation 15. We note that each group character is a particular element of the algebra F_G of functions on G to F in which addition, multiplication, and scalar multiplication are defined for σ, τ in F_G and c in F by

$$(\sigma+\tau)(x) = \sigma(x) + \tau(x), \quad (\sigma\,\tau)(x) = \sigma(x)\,\tau(x), \quad \text{and} \quad (c\,\sigma)(x) = c\,\sigma(x),$$

for each x in G. (The algebra $F[G]$ of Section 6 has a different multiplication.)

In view of $det(M) \neq 0$, we find that $Char(G)$, as a subset of F_G, is linearly independent over F. Since the dimension of F_G as a vector space over F is n, we conclude that $Char(G)$ provides a basis for the algebra F_G over F.

Proposition 16. *The matrix $N = (1/n)M^2$ is a symmetric $n \times n$ permutation matrix over F with inverse $N^{-1} = N$. Moreover, for any $n \times n$ matrix A over F, A belongs to $F[G,S]$ if and only if NAN belongs to $F[G,S]$; and, when A belongs to $F[G,S]$, $NAN = A^T$.*

Proof. Since M is symmetric, N is symmetric. We use $N = (1/n)M^2$, (30), (27), (22), and (28) to obtain

$$[N]_{r,s} = \frac{1}{n}\sum_{i=1}^{n} [M]_{r,i}\,[M]_{i,s} = \frac{1}{n}\sum_{i=1}^{n} \chi_r(g_i)\chi_i(g_s) = \frac{1}{n}\sum_{i=1}^{n} \chi_i(g_r)\chi_i(g_s)$$
$$= \frac{1}{n}\sum_{i=1}^{n} \chi_i(g_r g_s) = \begin{cases} 1, & \text{if } g_r\, g_s = e, \\ 0, & \text{if } g_r\, g_s \neq e, \end{cases} \quad \text{when } 1 \leq r,\, s \leq n. \tag{32}$$

For each fixed integer r satisfying $1 \leq r \leq n$, we apply (32) to see that there is precisely one value of s in the range $1 \leq s \leq n$ such that $[N]_{r,s}$ is nonzero and that it is then equal to 1. Thus, the nonsingular matrix N is an $n \times n$ permutation matrix over F. Because any permutation matrix is an orthogonal matrix and N is symmetric, we therefore have $N^{-1} = N^T = N$.

Suppose that A belongs to $F[G, S]$ and is given by $[A]_{r,s} = \sigma(g_r^{-1} g_s)$, for $1 \leq r,\, s \leq n$. Let υ be the function on G to G such that $\upsilon(x) = x^{-1}$, for each x in G, and set $\tau = \sigma \circ \upsilon$. We note that

$$[NAN]_{r,s} = \sum_{i=1}^{n}\sum_{j=1}^{n} [N]_{r,i}\,\sigma(g_i^{-1} g_j)\,[N]_{j,s}, \quad \text{for } 1 \leq r,\, s \leq n. \tag{33}$$

Since we have $[N]_{r,i}\,[N]_{j,s} = 0$ unless $g_r\, g_i = e = g_j\, g_s$, we find that (33), (32), and the commutativity of multiplication in G yield

$$[NAN]_{r,s} = \sigma\big((g_r^{-1})^{-1}\, g_s^{-1}\big) = \sigma(g_s^{-1}\, g_r) = [A]_{s,r} = [A^T]_{r,s} = \tau(g_r^{-1} g_s),$$

for $1 \leq r,\, s \leq n$. Thus, we have $NAN = A^T$ and NAN belongs to $F[G, S]$.

Finally, if an $n \times n$ matrix A over F is such that NAN belongs to $F[G, S]$, then the matrix $A = N(NAN)N$ belongs to $F[G, S]$. ∎

Theorem 17. (Fundamental Theorem about Abelian-Group Matrices) *Suppose that $n \times n$ matrices A and D over F are related by $AM = MD$. Then, A belongs to $F[G, S]$ if and only if D is a diagonal matrix; and, A is a diagonal matrix if and only if D belongs to $F[G, S]$. Moreover, when A belongs to $F[G, S]$ and is given by $[A]_{r,s} = \sigma(g_r^{-1} g_s)$, the n diagonal components of the diagonal matrix $D = M^{-1}AM$ are specified in terms of $\chi_1, \ldots, \chi_n$ for* Theorem 13 *by*

$$[D]_{r,r} = \sum_{j=1}^{n} \sigma(g_j)\,\chi_r(g_j), \quad \textit{with } 1 \leq r \leq n. \tag{34}$$

Proof. (i) Suppose A belongs to $F[G, S]$ and $[A]_{r,s} = \sigma(g_r^{-1} g_s)$, for $1 \leq r,\, s \leq n$. We use $D = M^{-1}AM$, (31), (27), and (30) to obtain

$$[D]_{r,s} = \sum_{i=1}^{n} [L]_{r,i} \sum_{j=1}^{n} [A]_{i,j}\,[M]_{j,s} = \frac{1}{n}\sum_{i=1}^{n} \chi_i(g_r^{-1}) \sum_{j=1}^{n} \sigma(g_i^{-1} g_j)\,\chi_j(g_s).$$

As g_j ranges through G while i is fixed, $g_i^{-1}g_j$ ranges through G. This gives

$$\sum_{j=1}^{n} \sigma(g_i^{-1}g_j)\ \chi_j(g_s) = \sum_{j=1}^{n} \sigma(g_i^{-1}g_j)\ \chi_s(g_j) = \sum_{j=1}^{n} \sigma(g_i^{-1}g_j)\ \chi_s(g_i^{-1}g_j)\ \chi_s(g_i)$$
$$= \chi_i(g_s) \sum_{j=1}^{n} \sigma(g_j)\ \chi_s(g_j).$$

We combine the two preceding formulas and use (28) to deduce that

$$[D]_{r,s} = \frac{1}{n} \sum_{i=1}^{n} \chi_i(g_r^{-1}g_s) \sum_{j=1}^{n} \sigma(g_j)\ \chi_s(g_j) = \delta(r,\, s) \sum_{j=1}^{n} \sigma(g_j)\ \chi_s(g_j),$$

where $\delta(r,\, s)$ equals 0 when $r \neq s$ and it equals 1 when $r = s$. This yields (34) and shows that D is a diagonal matrix.

(ii) Suppose that D is a diagonal matrix and set $A = MDM^{-1}$. Then, for $1 \leq r,\, s \leq n$, we have $[D]_{r,s} = [D]_{r,r}\, \delta(r,\, s)$ and

$$[A]_{r,s} = \sum_{i=1}^{n} \sum_{j=1}^{n} [M]_{r,i}\ [D]_{i,i}\ \delta(i,\, j)\ [L]_{j,s} = \sum_{i=1}^{n} [M]_{r,i}\ [D]_{i,i}\ [L]_{i,s}$$
$$= \frac{1}{n} \sum_{i=1}^{n} \chi_i(g_r)\ [D]_{i,i}\ \chi_i(g_s^{-1}) = \frac{1}{n} \sum_{i=1}^{n} [D]_{i,i}\ \chi_i\big((g_r^{-1}g_s)^{-1}\big).$$

Hence, the function σ on G to F defined by

$$\sigma(x) = \frac{1}{n} \sum_{i=1}^{n} [D]_{i,i}\ \chi_i(x^{-1}), \quad \text{for each } x \text{ in } G,$$

gives $[A]_{r,s} = \sigma(g_r^{-1}g_s)$, when $1 \leq r,\, s \leq n$. Thus, A belongs to $F[G, S]$.

(iii) Suppose that D belongs to $F[G, S]$. Proposition 16 shows that NDN belongs to $F[G, S]$. By (i) of this proof, $M^{-1}(NDN)M$ is a diagonal matrix. We use $N = (1/n)M^2$ and $N = N^{-1} = n(M^{-1})^2$ to obtain

$$M^{-1}(NDN)M = M^{-1}M^2D(M^{-1})^2M = MDM^{-1} = A$$

and conclude that A is a diagonal matrix.

(iv) Suppose that A is a diagonal matrix. Then, $NAN = NAN^T$ is a diagonal matrix and (ii) of this proof shows that $M(NAN)M^{-1}$ belongs to $F[G, S]$. With $N = (1/n)M^2$ and $N = N^{-1} = n(M^{-1})^2$, we find that

$$M(NAN)M^{-1} = M(M^{-1})^2AM^2M^{-1} = M^{-1}AM = D.$$

Thus, D belongs to $F[G, S]$. This completes the proof. ■

Theorem 17 was implicit in the work of Richard Dedekind, Georg Frobenius, and Heinrich Weber before 1900. Our proof is a slight modification of that in [7, page 123, Theorem 1]. An expression for $[D]_{r,r}$ of (34) directly in terms of $\sigma(g_1)$, $\sigma(g_2)$, ..., $\sigma(g_n)$, and ρ is provided by [7, page 127, Theorem 3].

Proposition 18. *Let S be any list of the elements in a finite abelian group G. Then, the algebras $F[G, S]$ and $F[G]$ over F are isomorphic to the commutative algebra $\mathcal{D}_n$ of $n \times n$ diagonal matrices over F.*

Proof. With Theorem 17 in place of Theorem 1, minor changes of wording in the proof of Proposition 2 show that $F[G, S]$ is isomorphic to $\mathcal{D}_n$. The isomorphism of $F[G, S]$ and $F[G]$ in Proposition 11 completes the proof. ■

Corollary 19. *Suppose that G_1 and G_2 are finite abelian groups having the same order n. Then, in terms of any lists S_1 for G_1 and S_2 for G_2, the algebras $F[G_1, S_1]$, $F[G]$, $F[G_2, S_2]$, and $F[G]$ are isomorphic over F.*

The preceding is valid because each of the those algebras is isomorphic to the algebra $\mathcal{D}_n$ of $n \times n$ diagonal matrices over F. Also, each of them is isomorphic to the algebra of $n \times n$ circulant matrices over F.

The observations about eigenvectors, eigenvalues, and inverses in Section 2 are also valid for our present context.

Observation 20. Let F be the field $\mathbb{C}$ of complex numbers. Then, the matrix M for Theorem 17 can be replaced with $U = (1/\sqrt{n})M$. Because each $\chi_r(g_s)$ for M in (30) is a root of unity, we have $\chi_r(g_s^{-1}) = \big(\chi_r(g_s)\big)^{-1} = \overline{\chi_r(g_s)}$. In view of (30)–(31) and the symmetry of M, this yields

$$[U^{-1}]_{r,s} = [\sqrt{n}\, L]_{r,s} = \frac{1}{\sqrt{n}}\, \chi_r(g_s^{-1}) = \frac{1}{\sqrt{n}}\, \overline{\chi_r(g_s)} = [\overline{U}]_{r,s} = [\overline{U}^T]_{r,s} = [U^H]_{r,s}$$

and $U^{-1} = U^H$. Thus, *U is a unitary matrix.*

Example 21. Let G be the cyclic group C_n with $S = (e, \alpha, \alpha^2, \ldots, \alpha^{n-1})$ and suppose that $F = \mathbb{C}$. Then, the corresponding characters χ_1, χ_2, ..., χ_n of Theorem 13 can be identified with the functions defined in (12) for Proposition 3. Given $a_0, a_1, \ldots, a_{n-1}$ in $\mathbb{C}$ and $\sigma(\alpha^{j-1}) = a_{j-1}$, for $1 \le j \le n$, we use (34) to obtain

$$\begin{aligned}[D]_{r,r} &= \sum_{j=1}^{n} \sigma(g_j)\, \chi_r(g_j) = \sum_{j=1}^{n} \sigma(g_j)\, \chi_j(g_r) = \sum_{j=1}^{n} \sigma(\alpha^{j-1})\, \chi_j(\alpha^{r-1}) \\ &= \sum_{j=1}^{n} a_{j-1}\, \rho^{(j-1)(r-1)} = \sum_{j=0}^{n-1} a_j\, \rho^{(r-1)j}, \quad \text{for } 1 \le r \le n.\end{aligned}$$

This yields (10). Thus, Theorem 1 *is the special case of* Theorem 17 *having $G = C_n$, $S = (e, \alpha, \alpha^2, \ldots, \alpha^{n-1})$, and $F = \mathbb{C}$.*

In particular, suppose that $n = 4$, $F = \mathbb{C}$, $G = C_4$, $S = (e, \alpha, \alpha^2, \alpha^3)$, $\boldsymbol{i}$ in $\mathbb{C}$ satisfies $\boldsymbol{i}^2 = -1$, and ρ is the principal 4th root of unity $\boldsymbol{i}$. Then, we see that

$$A = \begin{bmatrix} a & b & c & d \\ d & a & b & c \\ c & d & a & b \\ b & c & d & a \end{bmatrix} \quad \text{and} \quad M_1 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & \boldsymbol{i} & -1 & -\boldsymbol{i} \\ 1 & -1 & 1 & -1 \\ 1 & -\boldsymbol{i} & -1 & \boldsymbol{i} \end{bmatrix} \tag{35}$$

specify a typical matrix A in $F[C_4, S]$ and a matrix M_1 for M in Theorem 17. Here, $M_1^{-1}AM_1$ is a diagonal matrix and $(1/2)M_1$ is a unitary matrix.

Example 22. Let G be the direct product $C_2 \times C_2$ of two cyclic groups of order 2. Select $T = (e, \alpha_1, \alpha_2, \alpha_1\alpha_2)$, where e is the unit element while α_1 and α_2 are any two of the three elements of period 2. The remaining element of period 2 is therefore $\alpha_1\alpha_2$. In terms of T and the function on $C_2 \times C_2$ to $\mathbb{C}$ specified by $e \mapsto a$, $\alpha_1 \mapsto b$, $\alpha_2 \mapsto c$, and $\alpha_1\alpha_2 \mapsto d$, we see that the corresponding multiplication table and group matrix have the respective forms

	e	α_1	α_1	$\alpha_1\,\alpha_2$
e	e	α_1	α_2	$\alpha_1\alpha_2$
α_1	α_1	e	$\alpha_1\alpha_2$	α_2
α_2	α_2	$\alpha_1\,\alpha_2$	e	α_1
$\alpha_1\alpha_2$	$\alpha_1\alpha_2$	α_2	α_1	e

and $$B = \begin{bmatrix} a & b & c & d \\ b & a & d & c \\ c & d & a & b \\ d & c & b & a \end{bmatrix}. \tag{36}$$

In terms of $n = 4$, $F = \mathbb{C}$, $\boldsymbol{i}$ in $\mathbb{C}$ with $\boldsymbol{i}^2 = -1$, $\rho = \boldsymbol{i}$, $n_1 = 2$ as the period of α_1, $n_2 = 2$ as the period of α_2, $\rho_1 = \boldsymbol{i}^{n/n_1} = -1$, $\rho_2 = \boldsymbol{i}^{n/n_2} = -1$, and $x = \alpha_1^{x_1}\alpha_2^{x_2}$, for any x in $C_2 \times C_2$, the characters for $C_2 \times C_2$ are

$$\chi_1(x) = 1, \quad \chi_2(x) = (-1)^{x_1}, \quad \chi_3(x) = (-1)^{x_2}, \quad \chi_4(x) = (-1)^{x_1+x_2}.$$

The corresponding character table and matrix M for Theorem 17 are

	e	α_1	α_2	$\alpha_1\alpha_2$
χ_1	1	1	1	1
χ_2	1	-1	1	-1
χ_3	1	1	-1	-1
χ_4	1	-1	-1	1

and $$M_2 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}. \tag{37}$$

In particular, $M_2^{-1}BM_2$ is a diagonal matrix and $(1/2)M_2$ is a unitary matrix.

The determinant of B equals the product of the diagonal components of $M_2^{-1}BM_2$. In [25] of 1884, Constantin-Jerome Le Paige used this result in a manner analogous to the technique for (1) to derive formulas for the roots of a biquadratic equation.

We note that $C_2 \times C_2$ has 6 automorphisms. They correspond to the $3! = 6$ permutations of α_1, α_2, and $\beta = \alpha_1\alpha_2$. Consequently, the number $N(C_2 \times C_2)$ of classes of group matrices for $C_2 \times C_2$ is given by (18) as $3!/6 = 1$. Thus, $C_2 \times C_2$ has just one class of group matrices and B in (36) provides the pattern.

Example 23. According to Corollary 19, the algebra $\mathbb{C}[C_4, S]$ of matrices having the form of A in (35) and the algebra $\mathbb{C}[C_2 \times C_2, T]$ of matrices having the form of B in (36) are isomorphic over $\mathbb{C}$. The matrix M_1 in (35) provides the isomorphism $A \mapsto D = M_1^{-1} A M_1$ of $\mathbb{C}[C_4, S]$ onto the algebra $\mathcal{D}_4$ of 4×4 diagonal matrices over $\mathbb{C}$. Also, M_2 in (37) yields the isomorphism $D \mapsto M_2 D M_2^{-1}$ of $\mathcal{D}_4$ onto $\mathbb{C}[C_2 \times C_2, T]$. Thus, the assignment $A \mapsto \Phi(A) = (M_2 M_1^{-1}) A (M_1 M_2^{-1})$ is an isomorphism of $\mathbb{C}[C_4, S]$ onto $\mathbb{C}[C_2 \times C_2, T]$. We find that

$$A = \begin{bmatrix} a & b & c & d \\ d & a & b & c \\ c & d & a & b \\ b & c & d & a \end{bmatrix} \quad \text{yields} \quad \Phi(A) = \begin{bmatrix} a & c & \kappa & \lambda \\ c & a & \lambda & \kappa \\ \kappa & \lambda & a & c \\ \lambda & \kappa & c & a \end{bmatrix},$$

where $\kappa = \frac{1}{2}(1+\boldsymbol{i})\, b + \frac{1}{2}(1-\boldsymbol{i})\, d$ and $\lambda = \frac{1}{2}(1-\boldsymbol{i})\, b + \frac{1}{2}(1+\boldsymbol{i})\, d$. Under this and our previous isomorphisms, the element $1 \cdot \alpha$ of period 4 in $\mathbb{C}[C_4]$ corresponds to the element $\frac{1}{2}(1+\boldsymbol{i}) \cdot \alpha_2 + \frac{1}{2}(1-\boldsymbol{i}) \cdot \alpha_1 \alpha_2$ of period 4 in $\mathbb{C}[C_2 \times C_2]$.

Proposition 24. *Let S be a list for a finite group G of order n. In order for the isomorphic algebras $\mathbb{C}[G, S]$ and $\mathbb{C}[G]$ over $\mathbb{C}$ to be isomorphic to the algebra of $n \times n$ diagonal matrices over $\mathbb{C}$, it is necessary and sufficient that G be abelian.*

Proof. Suppose that G is abelian. Then, Proposition 18 shows that $\mathbb{C}[G, S]$ and $\mathbb{C}[G]$ are isomorphic to the algebra of $n \times n$ diagonal matrices over $\mathbb{C}$.

Suppose that $\mathbb{C}[G, S]$ is isomorphic to the algebra of $n \times n$ diagonal matrices over $\mathbb{C}$. Then, $\mathbb{C}[G, S]$ is commutative and G is abelian by Proposition 12. ■

Observation 25. For the conclusion of Theorem 17, it is sufficient for G to be a finite abelian group of some order n and for F to contain a primitive nth root of unity. Since the conclusion of Theorem 17 requires $F[G, S]$ to be commutative, it is also necessary for G to be abelian. However, for some finite abelian groups G of order n, it is not necessary for F to contain a primitive nth root of unity. For instance, consider $G = C_2 \times C_2$ in Example 22 with the list T of its elements and select F as the field $\mathbb{Q}$ of rational numbers. Then, for M_2 over $\mathbb{Q}$ in (37) and any 4×4 matrix B over $\mathbb{Q}$, $M_2^{-1} B M_2$ is a diagonal matrix if and only if B belongs to $\mathbb{Q}[C_2 \times C_2, T]$. However, $\mathbb{Q}$ does not contain a primitive 4th root of unity.

Example 26. The two 6×6 matrices

$$B_1 = \begin{bmatrix} a & b & c & d & e & f \\ b & a & d & c & f & e \\ e & f & a & b & c & d \\ f & e & b & a & d & c \\ c & d & e & f & a & b \\ d & c & f & e & b & a \end{bmatrix} \quad \text{and} \quad B_2 = \begin{bmatrix} a & b & c & d & e & f \\ c & a & b & f & d & e \\ b & c & a & e & f & d \\ d & e & f & a & b & c \\ f & d & e & c & a & b \\ e & f & d & b & c & a \end{bmatrix}$$

specify two of the 60 classes of group matrices for a cyclic group C_6 of order 6. The matrix B_1 can be obtained with the list $(e, \alpha, \beta, \alpha\beta, \beta^2, \alpha\beta^2)$ where the periods of e, α, and β are respectively 1, 2, and 3. It can be interpreted as a 3×3 block-circulant matrix in which the blocks are 2×2 circulant matrices. Similarly, B_2 can be associated with the list $(e, \beta, \beta^2, \alpha, \alpha\beta, \alpha\beta^2)$ and interpreted as a 2×2 block-circulant matrix in which the blocks are 3×3 circulant matrices. For any finite abelian group that is expressed as a direct product of two or more cyclic groups of orders ≥ 2, there are particular lists that produce matrices with block structures analogous to B_1 and B_2; e.g., see [7, pages 126–129].

9. EXTENSIONS TO ANY FINITE GROUP. Henceforth, G denotes a finite group of order n. The particular group matrices employed by Dedekind and Frobenius are defined in Context 28 with respect to (38) of the next result.

Proposition 27. *Let $T = (h_1, h_2, \ldots, h_n)$ be a list of the elements in G and let $\mathcal{A}$ be the set of those $n \times n$ matrices A over a field F for which there is a function τ on G to F such that*

$$[A]_{r,s} = \tau(h_r\, h_s^{-1}), \quad \textit{for } 1 \leq r,\, s \leq n. \tag{38}$$

Then, in terms of $S = (g_1, g_2, \ldots, g_n)$ defined by $g_s = h_s^{-1}$, for $1 \leq s \leq n$, the set $\mathcal{A}$ is the class $F[G, S]$ of group matrices. Moreover the classes $F[G, S]$ and $F[G, T]$ are the same if and only if G is abelian.

Proof. In (38), we have $[A]_{r,s} = \tau(g_r^{-1} g_s)$, for $1 \leq r,\, s \leq n$. Thus, $\mathcal{A} = F[G, S]$.

Let υ be the function on G to G such that $\upsilon(x) = x^{-1}$, for each x in G.

(i) Suppose that G is abelian. For each function τ on G to F, we have

$$\tau(h_r^{-1}\, h_s) = \tau(g_s^{-1} g_r) = \tau\big(\upsilon(g_r^{-1} g_s)\big) = \sigma(g_r^{-1} g_s), \tag{39}$$

where $\sigma = \tau \circ \upsilon$. And, for each function σ on G to F, the function $\tau = \sigma \circ \upsilon$ yields $\tau \circ \upsilon = \sigma$ and (39). Thus, we obtain $F[G, T] = F[G, S]$.

(ii) Suppose that $F[G, S] = F[G, T]$. Then, for each function σ on G to F, there is a function τ on G to F such that $\sigma(g_r^{-1} g_s) = \tau(h_r^{-1} h_s) = \tau(g_r\, g_s^{-1})$, for $1 \leq r,\, s \leq n$. We find that $\sigma(g_s) = \tau(g_s^{-1}) = (\tau \circ \upsilon)(g_s)$, for $1 \leq s \leq n$, and therefore $\sigma = \tau \circ \upsilon$ as well as $\tau = \sigma \circ \upsilon$. Thus, for each σ on G to F and for $1 \leq r,\, s \leq n$, we have $\sigma(g_r^{-1} g_s) = \sigma(g_s\, g_r^{-1})$, $g_r^{-1} g_s = g_s\, g_r^{-1}$, and $g_s\, g_r = g_r\, g_s$. Consequently, G is abelian. This completes the proof. ∎

Context 28. Let $x_1, x_2, \ldots, x_n$ denote algebraically independent variables over the field $\mathbb{C}$ of complex numbers and let $\mathbb{C}[x_1, x_2, \ldots, x_n]$ denote the ring of polynomials over $\mathbb{C}$ in those variables. In terms of $T = (h_1, h_2, \ldots, h_n)$ as a list for the elements of G, let τ be the function on G to $\mathbb{C}[x_1, x_2, \ldots, x_n]$ such that $\tau(h_i) = x_i$, for $1 \leq i \leq n$. For Dedekind and Frobenius, a matrix $\mathfrak{A}$ is a group matrix for G with respect to T and $x_1, x_2, \ldots, x_n$ when $\mathfrak{A}$ is the unique $n \times n$ matrix such that

$$[\mathfrak{A}]_{r,s} = \tau(h_r\, h_s^{-1}), \quad \text{for } 1 \leq r,\, s \leq n. \tag{40}$$

Formulation 29. With respect to Context 28, set $g_i = h_i^{-1}$, for $1 \leq i \leq n$; introduce the list $S = (g_1, g_2, \ldots, g_n)$ for G; let $X_1, \ldots, X_n$ be the permutation of $x_1, \ldots, x_n$ given by $X_i = \tau(h_i^{-1})$, for $1 \leq i \leq n$; let F be any field that contains $\mathbb{C}[X_1, X_2, \ldots, X_n]$; and let σ be the function on G to F defined by $\sigma(g_i) = X_i$, for $1 \leq i \leq n$. Then, $\sigma = \tau$ and the matrix $\mathfrak{A}$ for (40) satisfies

$$[\mathfrak{A}]_{r,s} = \sigma(g_r^{-1} g_s), \quad \text{for } 1 \leq r, s \leq n. \tag{41}$$

Thus, $\mathfrak{A}$ is a group matrix for G relative to S in the sense of Definition 4.

The determinant of the matrix $\mathfrak{A}$ given by (41) is a nonconstant polynomial in $\mathbb{C}[X_1, X_2, \ldots, X_n]$. Thus, $det(\mathfrak{A})$ is expressible as a product of irreducible polynomials in $\mathbb{C}[X_1, X_2, \ldots, X_n]$ that are unique apart from nonzero factors from $\mathbb{C}$; e.g., see [23, page 183, Corollary 2.4].

Definition 30. For any two elements u, v in a group G, to say that u *is conjugate to* v means that there is an element t in G such that $u = t^{-1} v\, t$. Conjugacy is an equivalence relation. (The unit element e of G yields $u = e^{-1} u\, e$, for each u in G. If $u = t^{-1} v\, t$, then $v = (t^{-1})^{-1} u\, (t^{-1})$. If $u = t_1^{-1} v\, t_1$ and $v = t_2^{-1} w\, t_2$, then $u = (t_2\, t_1)^{-1} w\, (t_2\, t_1)$.) This equivalence relation partitions G into equivalence classes whose number $k(G)$ is called the *class number of* G.

When G is abelian, each equivalence class contains a single element and $k(G) = n$. When G is not commutative, there are elements u, v in G such that $v\, u \neq u\, v$ and $u \neq v^{-1} u\, v$; then, the equivalence class to which the unequal conjugates u and $v^{-1} u\, v$ belong contains more than one element and $k(G) < n$.

Theorem 31. (Frobenius, Part 1) *Let $S = (g_1, g_2, \ldots, g_n)$ be a list for a finite group G of order n and let $k = k(G)$ be the class number for G. Then, there are k irreducible polynomials $P_1, P_2, \ldots, P_k$ in $\mathbb{C}[X_1, X_2, \ldots, X_n]$ such that the determinant of the group matrix $\mathfrak{A}$ defined by* (41) *has the factorization*

$$det(\mathfrak{A}) = (P_1)^{m_1} (P_2)^{m_2} \cdots (P_k)^{m_k}, \tag{42}$$

where, for $1 \leq i \leq k$, m_i is equal to the total degree of the polynomial P_i in the variables $X_1, X_2, \ldots, X_n$ over $\mathbb{C}$ and where P_i and P_j are relatively prime whenever $i \neq j$. Moreover, $m_1, m_2, \ldots, m_k$ satisfy

$$m_1^2 + m_2^2 + \cdots + m_k^2 = n \tag{43}$$

and each of $m_1, m_2, \ldots, m_k$ divides n.

Frobenius proved in [16, pages 1362–1363] of 1896 that: when $det(\mathfrak{A})$ is expressed as a product of irreducible factors in $\mathbb{C}[X_1, X_2, \ldots, X_n]$, there are k and no more than k pairwise relatively prime factors among them. Frobenius showed in [16, pages 1368–1372] that the multiplicity of each irreducible factor of $det(\mathfrak{A})$ over $\mathbb{C}$ is equal to its total degree. That each of $m_1, m_2, \ldots, m_k$ divides n is concluded in [16, page 1382]. Finally, (43) is obtained by equating the total degrees of the polynomials in the left and right members of (42).

Definition 32. Let $m_1, m_2, \ldots, m_k$ and n denote positive integers subject to $m_1^2+m_2^2+\cdots+m_k^2 = n$ and let B be an $n \times n$ matrix. For each pair (μ, ν) of integers that satisfy $1 \le \mu \le k$ and $1 \le \nu \le m_\mu$, let $B_{\mu,\nu}$ be the principal submatrix of B defined in terms of $\lambda = \sum_{p=1}^{\mu-1} m_p^2 + (\nu-1)m_\mu$ by $[B_{\mu,\nu}]_{r,s} = [B]_{\lambda+r,\lambda+s}$, for $1 \le r, s \le m_\mu$. Then, the principal submatrices

$$B_{1,1}, \ldots, B_{1,m_1};\ B_{2,1}, \ldots, B_{2,m_2};\ \ldots;\ B_{k,1}, \ldots, B_{k,m_k} \tag{44}$$

of B are such that their successive diagonal components are the n diagonal components of B. We say that B is an $m_1, m_2, \ldots, m_k$-*block-diagonal matrix* when all of its components outside the submatrices of (44) are zero and

$$B_{\mu,\nu} = B_{\mu,1}, \quad \text{for } 1 \le \mu \le k \text{ and } 1 \le \nu \le m_\mu.$$

Theorem 33. (Frobenius, Part 2) *For* Theorem 31 *and its conclusions about* $\mathfrak{A}$ *of* (41)*, there is a nonsingular* $n \times n$ *matrix* M *over* $\mathbb{C}$ *such that the matrix* $\mathfrak{B} = M^{-1}\mathfrak{A}M$ *is an* $m_1, m_2, \ldots, m_k$*-block-diagonal matrix whose blocks*

$$\mathfrak{B}_{1,1}, \ldots, \mathfrak{B}_{1,1};\ \ \mathfrak{B}_{2,1}, \ldots, \mathfrak{B}_{2,1};\ \ \ldots;\ \ \mathfrak{B}_{k,1}, \ldots \mathfrak{B}_{k,1} \tag{45}$$

yield the factorization (42) *with* $P_\mu = det(\mathfrak{B}_{\mu,1})$*, for* $1 \le \mu \le k$*. Moreover, for* $1 \le \mu \le k$*, each component of* $\mathfrak{B}_{\mu,1}$ *is a linear polynomial in* $X_1, X_2, \ldots, X_n$ *over* $\mathbb{C}$*; and* $det(\mathfrak{B}_{\mu,1})$ *is an irreducible polynomial over* $\mathbb{C}$*.*

Frobenius presented the preceding result in [17, page 1007]. An explicit construction of a suitable matrix M for Theorem 33 is given in Theorem 34.

10. MATRIX REPRESENTATIONS RELATED TO THEOREM 33. With reference to Theorem 33 and $S = (g_1, g_2, \ldots, g_n)$ for G, let

$$A(g_j),\ B(g_j),\ B_{1,1}(g_j),\ B_{2,1}(g_j), \ldots,\ B_{k,1}(g_j),\ \text{for } 1 \le j \le n,$$

denote the matrices over $\mathbb{C}$ obtained from $\mathcal{A}$, $\mathfrak{B}$, $\mathfrak{B}_{1,1}$, $\mathfrak{B}_{2,1}$, $\ldots$, $\mathfrak{B}_{k,1}$ by substituting 1 for X_j and 0 for each X_i having $1 \le i \le n$ and $i \ne j$. We use (41) and the notation for (21) to deduce that: for $1 \le j \le n$,

$$[A(g_j)]_{r,s} = \sigma_j(g_r^{-1}g_s) = (1 \cdot g_j)(g_r^{-1}g_s), \quad \text{when } 1 \le r, s \le n,$$

where $\sigma_j = 1 \cdot g_j$ on G to $\mathbb{C}$ has $(1 \cdot g_j)(g_i) = \delta(i, j)$, for $1 \le i \le n$. Since (21) yields $1 \cdot x\,y = (1 \cdot x) * (1 \cdot y)$, for each x, y in G, the isomorphism of $\mathbb{C}[G]$ and $\mathbb{C}[G, S]$ given by Proposition 11 establishes that $A(x\,y) = A(x)\,A(y)$, for each x, y in G. In view of $B(x) = M^{-1}A(x)M$, for each x in G, we also have $B(x\,y) = B(x)\,B(y)$ and $B_{\mu,1}(x\,y) = B_{\mu,1}(x)\,B_{\mu,1}(y)$, for any x, y in G and $1 \le \mu \le k$. Thus, the assignments $x \mapsto A(x)$ and $x \mapsto B(x)$, for each x in G, are *representations of* G *by matrices over* $\mathbb{C}$ *of size* $n \times n$; and, for $1 \le i \le k$, the

assignment $x \mapsto B_{i,1}(x)$, for each x in G, is a *representation of G by matrices over $\mathbb{C}$ of size $m_i \times m_i$*. For $1 \le i < j \le k$, $det(\mathfrak{B}_{i,1})$ and $det(\mathfrak{B}_{j,1})$ are relatively prime; and each of $det(\mathfrak{B}_{1,1})$, ..., $det(\mathfrak{B}_{k,1})$ is irreducible over $\mathbb{C}$. Thus, the k representations

$$x \mapsto B_{1,1}(x), \quad x \mapsto B_{2,1}(x), \quad \ldots, \quad x \mapsto B_{k,1}(x), \quad \text{for each } x \text{ in } G, \tag{46}$$

are *pairwise inequivalent* and *irreducible*. Here, *pairwise inequivalent* means that: for any distinct integers i, j satisfying $1 \le i, j \le k$ and any nonsingular $m_i \times m_i$ matrix M_i over $\mathbb{C}$, there is an x in G such that $M_i^{-1} B_{i,1}(x) M_i \ne B_{j,1}(x)$. A representation $x \mapsto B_{i,1}(x)$ is *irreducible* when there is no nonsingular $m_i \times m_i$ matrix M_i over $\mathbb{C}$ such that all of the n matrices $M_i^{-1} B_{i,1}(x) M_i$, for x in G, have a nontrivial block-diagonal reduction of the same type.

The study of group representations by matrices was approached directly through the simplifications of Issai Schur in [30] and later researchers. Details about the transition to this extensive subject are interestingly presented in [11]. A set $\mathfrak{R}$ of k pairwise inequivalent and irreducible matrix representations over $\mathbb{C}$ for G is referred to as a *complete set of matrix representations for G*. The terminology arose because, for any such $\mathfrak{R}$, each matrix representation over $\mathbb{C}$ for G is isomorphic to a direct sum of representations in $\mathfrak{R}$ (with repetitions permitted); e.g., see [19, page 267, Theorem 16.5.5]. Thus, if (46) and

$$x \mapsto R_1(x), \quad x \mapsto R_2(x), \quad \ldots, \quad x \mapsto R_k(x), \quad \text{for each } x \text{ in } G, \tag{47}$$

are the elements of any two complete sets of matrix representations over $\mathbb{C}$ for G, then there is a permutation π of (1, 2, ..., k) and, for $1 \le i \le k$, there are nonsingular matrices N_i over $\mathbb{C}$ such that $B_{i,1}(x) = N_i^{-1} R_{\pi(i)}(x) N_i$, for $1 \le i \le k$ and each x in G.

11. A MATRIX M FOR THEOREM 33. Let $S = (g_1, g_2, \ldots, g_n)$ be a list of the elements for a finite group G of order n and class number k; and suppose that a complete set of representations for G by matrices over $\mathbb{C}$ is given by (47). For $1 \le i \le k$ and x in G, let the matrix $R_i(x)$ have size $m_i \times m_i$. Then, we have $m_1^2 + m_2^2 + \cdots + m_k^2 = n$. In terms of the ring $\mathbb{Z}$ of integers and

$$\mathcal{T} = \big\{ (u, v, w) \mid \quad u, v, w \in \mathbb{Z};\ 1 \le u \le k; \text{ and } 1 \le v, w \le m_u \big\},$$

the function $s = \psi(u, v, w)$ defined on T by

$$s = \sum_{i=1}^{u-1} m_i^2 + (v-1) m_u + w \tag{48}$$

is easily shown to give a one-to-one correspondence between $\mathcal{T}$ and the set $\mathcal{N} = \big\{1, 2, \ldots, n\big\}$. For each s in $\mathcal{N}$, we let $u(s)$, $v(s)$, $w(s)$ denote the unique integers such that $\big(u(s), v(s), w(s)\big) \in \mathcal{T}$ and $\psi\big(u(s), v(s), w(s)\big) = s$. Writing $m(i) = m_i$, for $1 \le i \le k$, we define $n \times n$ matrices L and M over $\mathbb{C}$ by

$$[L]_{r,s} = \tfrac{m(u(r))}{n} \big[R_{u(r)}(g_s^{-1})\big]_{w(r),v(r)} \quad \text{and} \quad [M]_{r,s} = \big[R_{u(s)}(g_r)\big]_{v(s),w(s)},$$

for $1 \le r, s \le n$.

Theorem 34. *The matrix M is nonsingular and L is its inverse. Moreover, for any extension field F of $\mathbb{C}$ and any two $n \times n$ matrices A and B over F related by $AM = MB$, B is an $m_1, m_2, \ldots, m_k$-block-diagonal matrix if and only if A belongs to $F[G, S]$.*

A slight change of notation in the proof of [8, page 127, Theorem 2] yields the preceding result.

The proof of [8, page 127, Theorem 2] shows directly that the statement of Theorem 34 remains valid when the matrices L and M are replaced with the $n \times n$ matrices $\mathcal{L}$ and $\mathcal{M}$ defined over $\mathbb{C}$ by

$$[\mathcal{L}]_{r,s} = \sqrt{\tfrac{m(u(r))}{n}}\big[R_{u(r)}(g_s^{-1})\big]_{w(r),v(r)}\,, \quad [\mathcal{M}]_{r,s} = \sqrt{\tfrac{m(u(s))}{n}}\big[R_{u(s)}(g_r)\big]_{v(s),w(s)}\,,$$

for $1 \le r,\, s \le n$. The matrix $\mathcal{M}$ was emphasized in [8] because it is a unitary matrix whenever, for $1 \le i \le k$ and $1 \le j \le n$, $R_i(g_j)$ is a unitary matrix.

Proposition 35. *The inverse of a nonsingular group matrix is a group matrix of the same class.*

Proof. Suppose that A is a nonsingular matrix in $F[G, S]$ and set $B = M^{-1}AM$. Then, B is a nonsingular $m_1, m_2, \ldots, m_k$-block-diagonal matrix and B^{-1} is therefore a block-diagonal matrix of the same type. Consequently, the matrix $A^{-1} = MB^{-1}M^{-1}$ belongs to $F[G, S]$. ∎

Machine Computation 36. A program for a system of computer algebra can be written so that: when a complete set of matrix representations for a given finite group is entered, the corresponding matrix M in Theorem 34 is produced. For any given positive integers m_1, m_2, …, m_k, this requires explicit formulas to compute $u(s)$, $v(s)$, and $w(s)$ whenever $1 \le s \le m_1^2 + m_2^2 + \cdots + m_k^2$. We use (48) to see that $u(s)$ can be computed as the unique integer that satisfies

$$1 + \sum_{i=1}^{u(s)-1} m_i^2 \le s \le \sum_{i=1}^{u(s)} m_i^2.$$

In terms of s and $u(s)$, (48) shows that $v(s) - 1$ is the greatest integer that is strictly less than the rational number

$$\frac{1}{m\big(u(s)\big)}\left(s - \sum_{i=1}^{u(s)-1} m_i^2\right).$$

When $Floor(r)$ designates the greatest integer that is less than or equal to r, we note that $-Floor(1 - r)$ is equal to the greatest integer that is strictly less than r. With respect to s, $u(s)$, and $v(s)$, we obtain $w(s)$ by solving (48) for w.

Example 37. Part 1. For the symmetric group $\mathfrak{S}_3$ of permutations on three objects symbolized as 1, 2, and 3, let $S = (g_1, g_2, \ldots, g_6)$ be given by the cycles

$$g_1 = (1),\ \ g_2 = (1\ 2\ 3),\ \ g_3 = (1\ 3\ 2),\ \ g_4 = (2\ 3),\ \ g_5 = (1\ 3),\ \ g_6 = (1\ 2). \quad (49)$$

For instance, g_2 denotes the permutation that replaces 1 with 2, 2 with 3, and 3 with 1. We read composition of cycles from left to right; for example, $g_2\, g_4 = g_5$. The conjugacy classes are $\{g_1\}$, $\{g_2, g_3\}$, and $\{g_4, g_5, g_6\}$ so that $k = k(\mathfrak{S}_3) = 3$. Let $X_1, \ldots, X_6$ be algebraically independent variables over $\mathbb{C}$ and let F be any field extension of the polynomial ring $\mathbb{C}[X_1, \ldots, X_6]$. The multiplication table for $\mathfrak{S}_3$ with respect to the list S yields

$$\mathfrak{A} = \begin{bmatrix} X_1 & X_2 & X_3 & X_4 & X_5 & X_6 \\ X_3 & X_1 & X_2 & X_6 & X_4 & X_5 \\ X_2 & X_3 & X_1 & X_5 & X_6 & X_4 \\ X_4 & X_6 & X_5 & X_1 & X_3 & X_2 \\ X_5 & X_4 & X_6 & X_2 & X_1 & X_3 \\ X_6 & X_5 & X_4 & X_3 & X_2 & X_1 \end{bmatrix} \quad (50)$$

as the corresponding group matrix of Formulation 29. When the computer algebra system MATHEMATICA is employed to factor $\mathfrak{A}$ in (50), it yields two relatively prime linear factors and one quadratic factor of multiplicity 2. Each is a polynomial in the variables $X_1, \ldots, X_6$ over the ring $\mathbb{Z}$ of integers. Due to $k(\mathfrak{S}_3) = 3$, Theorem 31 shows that the quadratic factor is also irreducible over $\mathbb{C}$. We may select $m_1 = m_2 = 1$ and $m_3 = 2$. (For most other situations where an irreducible factorization (42) over $\mathbb{C}$ for $det(\mathfrak{A})$ can be obtained by applying MATHEMATICA directly to $\mathfrak{A}$ in (41), it is generally necessary to adjoin an algebraic number to the ring $\mathbb{Z}$ of integers when the Factor command is used. For $n \times n$ circulant matrices, a primitive nth root of unity suffices.)

Part 2. For $1 \le i \le 6$, let P_i denote the 3×3 permutation matrix obtained from the 3×3 identity matrix by permuting its rows according to g_i in (49). Then, for $1 \le i, j, q \le 6$, a product $g_i\, g_j$ equals g_q if and only if $P_i P_j = P_q$. Consequently, the assignment $g_i \mapsto P_i$, for $1 \le i \le 6$, is a group representation of $\mathfrak{S}_3$. To see that it is reducible, we introduce Q as the 3×3 Brioschi-Cremona matrix (8) having $[Q]_{r,s} = \omega^{(r-1)(s-1)}$, for $1 \le r, s \le 3$, where ω is a primitive cube root of unity. Computer algebra enables us to easily verify the observation in [5, page 78] that

$$Q^{-1} P_i Q = \begin{bmatrix} 1 & Z \\ Z^T & R_3(g_i) \end{bmatrix}, \quad \text{for } 1 \le i \le 6 \text{ and } Z = [\ 0 \quad 0\ ],$$

where $R_3(g_1)$, $R_3(g_2)$, $\ldots$, $R_3(g_6)$ are respectively the six 2×2 matrices

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} \omega & 0 \\ 0 & \omega^2 \end{bmatrix}, \begin{bmatrix} \omega^2 & 0 \\ 0 & \omega \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & \omega \\ \omega^2 & 0 \end{bmatrix}, \begin{bmatrix} 0 & \omega^2 \\ \omega & 0 \end{bmatrix}.$$

This yields the representations $g_i \mapsto R_1(g_i) = [1]$ and $g_i \mapsto R_3(g_i)$ for $\mathfrak{S}_3$. Clearly, $g_i \mapsto R_1(g_i)$ is irreducible. Also, $g_i \mapsto R_3(g_i)$ is irreducible because

a reducible 2×2 representation is equivalent to a representation by diagonal matrices for which multiplication is commutative. A third representation is given by $g_i \mapsto R_2(g_i) = [det(R_3(g_i)]$. It has $R_2(g_i) = [1]$, for $1 \le i \le 3$, and $R_2(g_i) = [-1]$, for $4 \le i \le 6$. These three pairwise inequivalent and irreducible representations yield the matrices M and $M^{-1}\mathfrak{A}M$ respectively as

$$\begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & \omega & 0 & 0 & \omega^2 \\ 1 & 1 & \omega^2 & 0 & 0 & \omega \\ 1 & -1 & 0 & 1 & 1 & 0 \\ 1 & -1 & 0 & \omega & \omega^2 & 0 \\ 1 & -1 & 0 & \omega^2 & \omega & 0 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} Y_1 & 0 & 0 & 0 & 0 & 0 \\ 0 & Y_2 & 0 & 0 & 0 & 0 \\ 0 & 0 & Y_3 & Y_4 & 0 & 0 \\ 0 & 0 & Y_5 & Y_6 & 0 & 0 \\ 0 & 0 & 0 & 0 & Y_3 & Y_4 \\ 0 & 0 & 0 & 0 & Y_5 & Y_6 \end{bmatrix},$$

where

$$\begin{aligned} Y_1 &= X_1 + X_2 + X_3 + X_4 + X_5 + X_6, & Y_2 &= X_1 + X_2 + X_3 - X_4 - X_5 - X_6, \\ Y_3 &= X_1 + \omega\, X_2 + \omega^2 X_3, & Y_4 &= X_4 + \omega\, X_5 + \omega^2 X_6, \\ Y_5 &= X_4 + \omega^2 X_5 + \omega\, X_6, & Y_6 &= X_1 + \omega^2 X_2 + \omega\, X_3. \end{aligned}$$

Thus, we find that

$$det(\mathfrak{A}) = det(M^{-1}\mathfrak{A}M) = Y_1\, Y_2 (Y_3\, Y_6 - Y_4\, Y_5)^2 \tag{51}$$

and $Y_3\, Y_6 - Y_4\, Y_5$ is an irreducible quadratic polynomial in $X_1, \ldots, X_6$ over $\mathbb{C}$ each of whose coefficients is ± 1. By interchanging X_2 with X_3 and ω with ω^2 throughout, we obtain the group matrix of [17, page 1007] and its block-diagonal reduction of [17, page 1008]. Frobenius indicated there that the example was discovered by Richard Dedekind in 1886 and communicated to him in April of 1896. It motivated his research for [15, 16, 17]. The matrix they used for M differs from the one above and rules for its formation were not made explicit.

Alternative Procedure. The representation $g_i \mapsto R_3(g_i)$ is equivalent to precisely two that have integral components; e.g., see [12, page 505, Example 1]. After introducing

$$D_1 = \begin{bmatrix} 1 & \omega \\ \omega & 1 \end{bmatrix} \quad \text{and} \quad D_2 = \begin{bmatrix} 1 & \omega^2 \\ \omega^2 & 1 \end{bmatrix},$$

we set $\widehat{R}_3(g_i) = D_1^{-1} R_3(g_i)\, D_1$ and $\widetilde{R}_3(g_i) = D_2^{-1} R_3(g_i)\, D_2$, for $1 \le i \le 6$. The matrices $\widehat{R}_3(g_1)$, $\widehat{R}_3(g_2)$, $\ldots$, $\widehat{R}_3(g_6)$ are respectively given by

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix}, \begin{bmatrix} -1 & 1 \\ -1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ -1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & -1 \\ 0 & -1 \end{bmatrix}.$$

When the representations $g_i \mapsto R_1(g_i)$, $g_i \mapsto R_2(g_i)$, and $g_i \mapsto \widehat{R}_3(g_i)$ are used

in Theorem 34, the corresponding matrices $\widehat{M}$ and $\widehat{M}^{-1}\mathfrak{A}\widehat{M}$ are

$$\begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & -1 & 1 & -1 \\ 1 & 1 & -1 & 1 & -1 & 0 \\ 1 & -1 & 0 & 1 & 1 & 0 \\ 1 & -1 & -1 & 0 & -1 & 1 \\ 1 & -1 & 0 & -1 & 0 & -1 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} Z_1 & 0 & 0 & 0 & 0 & 0 \\ 0 & Z_2 & 0 & 0 & 0 & 0 \\ 0 & 0 & Z_3 & Z_4 & 0 & 0 \\ 0 & 0 & Z_5 & Z_6 & 0 & 0 \\ 0 & 0 & 0 & 0 & Z_3 & Z_4 \\ 0 & 0 & 0 & 0 & Z_5 & Z_6 \end{bmatrix},$$

where $Z_1 = Y_1$ and $Z_2 = Y_2$ for (51) while

$$Z_3 = X_1 - X_3 - X_5 + X_6, \qquad Z_4 = -X_2 + X_3 + X_4 - X_6,$$
$$Z_5 = X_2 - X_3 + X_4 - X_5, \qquad Z_6 = X_1 - X_2 + X_5 - X_6.$$

In view of $Z_3 Z_6 - Z_4 Z_5 \equiv Y_3 Y_6 - Y_4 Y_5$, this also yields (51) for $det(\mathfrak{A})$.

The matrices $\widetilde{R}_3(g_1)$, $\widetilde{R}_3(g_2)$, ..., $\widetilde{R}_3(g_6)$, are respectively given by

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} -1 & 1 \\ -1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & -1 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ -1 & 1 \end{bmatrix}.$$

Thus, the representation $g_i \mapsto \widetilde{R}_3(g_i)$ of $\mathcal{S}_3$ is the second of the two that are equivalent to $g_i \mapsto R_3(g_i)$ and have integral components. When it is used in place of $g_i \mapsto \widehat{R}_3(g_i)$ for Theorem 34, the corresponding matrix $\widetilde{M}$ yields $\widetilde{M}^{-1}\mathfrak{A}\widetilde{M} = \widehat{M}^{-1}\mathfrak{A}\widehat{M}$ and the same expression for $det(\mathfrak{A})$.

For each integer $q \geq 3$, there is a corresponding dihedral group of order $2q$ whose elements can be identified with the symmetries of a regular polygon having q vertices that are consecutively numbered 1, 2, ..., q. Thus, $\mathfrak{S}_3$ can be identified with the group of symmetries for an equilateral triangle. Each dihedral group of order $2q$ has a cyclic subgroup of order q; and each finite abelian group of order q is a subgroup of a generalized dihedral group of order $2q$. Kai Wang showed in [31] how results analogous to those of Example 37 can be explicitly obtained for any generalized dihedral group of order $2q$. His technique depends on an application of Theorem 17 to the abelian subgroup of order q. Interesting exercises for students can be based on checking his results with computer algebra and using them to obtain explicit constructions analogous to those for $\mathfrak{S}_3$.

Example 38. An abelian group G of order n has $k = k(G) = n$ and $m_i = 1$, for $1 \leq i \leq k = n$, as well as $u(s) = s$ and $v(s) = w(s) = 1$, for $1 \leq s \leq n$. For $F = \mathbb{C}$, the n group characters χ_1, χ_2, ..., χ_n specified for G by (24)–(26) in Section 7 can be regarded as n pairwise inequivalent and irreducible group representations for G by matrices of size 1×1. Selecting $R_i(x)$ as the 1×1 matrix $[\chi_i(x)]$, for each x in G and $1 \leq i \leq n$, we see that the corresponding matrix M for Theorem 34 coincides with the matrix M constructed in (30) for Theorem 17. These group representations are unitary and the matrix $\mathcal{M}$ following Theorem 34 coincides with U in Observation 20. When G is a cyclic group of order n and S is the list used for (5), the characters are given by (12) and yield Theorem 1 for circulant matrices.

References

[1] Heinrich Richard Baltzer, *Theorie und Anwendung der Determinanten*, 2nd edition, Leipzig, 1864.

[2] Eugène Charles Catalan, *Recherches sur les déterminants*, Bull. de l'Acad. royal de Belgique **13** (1846) 534–555.

[3] Arthur Cayley, *A solvible case of the quintic equation*, Quart. J. Pure Appl. Math. **18** (1882) 154–157.

[4] Roger Chalkley, *Cardan's formulas and biquadratic equations*, Math. Mag. **47** (1974) 8–14.

[5] Roger Chalkley, *Circulant matrices and algebraic equations*, Math. Mag. **48** (1975) 73–80.

[6] Roger Chalkley, *Quartic equations and tetrahedral symmetries*, Math. Mag. **48** (1975) 211–215.

[7] Roger Chalkley, *Matrices derived from finite abelian groups*, Math. Mag. **49** (1976) 121-129.

[8] Roger Chalkley, *Information about group matrices*, Linear Algebra Appl. **38** (1981) 121-133.

[9] Keith Conrad, *The origin of representation theory*, Enseign. Math. (2) **44** (1998) 361-392.

[10] Luigi Cremona, *Intorno ad un theorema di Abel*, Annali di Sci. mat. e fis., **7** (1856) 99-105.

[11] Charles W. Curtis, *Pioneers of Representation Theory: Frobenius, Burnside, Schur, and Brauer*, Amer. Math. Soc., Providence, 1999.

[12] Charles W. Curtis and Irving Reiner, *Representation Theory of Finite Groups and Associative Algebras*, Wiley-Interscience, New York, 1962.

[13] Philip J. Davis, *Circulant Matrices*, Wiley-Interscience, New York, 1979.

[14] Peter Gustav Lejeune Dirichlet and Julius Wilhelm Richard Dedekind, *Vorlesungen über Zahlentheorie*, 4th edition, Braunschweig 1893. (Translated from the German by John Stillwell as *Lectures on Number Theory*, Amer. Math. Soc., Providence, 1999.)

[15] Ferdinand Georg Frobenius, *Über Gruppencharacter*, Sitzungsberichte Akad. Wiss. Berlin (1896), 985–1021; Gesammelte Abhandlungen III, Springer-Verlag, Berlin, 1968, pp. 1–37.

[16] Ferdinand Georg Frobenius, *Über die Primfactoren der Gruppendeterminante*, Sitzungsberichte Akad. Wiss. Berlin (1896), 1343–1382; Gesammelte Abhandlungen III, Springer-Verlag, Berlin, 1968, 38–77.

[17] Ferdinand Georg Frobenius, *Über die Darstellung der endlichen Gruppen durch lineare Substitutionen*, Sitzungsberichte Akad. Wiss. Berlin (1897), 944–1015; Ges. Abh. III, Springer-Verlag, Berlin, 1968, pp. 82–103.

[18] Irving John Good, *On the inversion of circulant matrices*, Biometrika **37** (1950) 185–186.

[19] Marshall Hall, *The Theory of Groups*, Macmillan, New York, 1959.

[20] J. L. S. Hatton and A. M. Nesbitt, *Question 15319*, Mathematical questions and solutions from the "Educational Times" (C. J. Marks, Editor; Published by Francis Hodgson, London) (2) **5** (1904) 106-107.

[21] Dan Kalman and James E. White, *Polynomial equations and circulant matrices*, Amer. Math. Monthly **108** (2001) 821-840.

[22] Karl Otto Emil Lampe, Summary for *Question 15319 by J. L. S. Hatton and A. M. Nesbitt*, Jahrbuch über die Fortschritte der Mathematik, **35** (1904) 116.

[23] Serge Lang, *Algebra,* Revised Third edition, Springer, New York, 2002.

[24] Edme Alphonse Legoux, *Sur une application d'un déterminant*, Quar. J. Pure Appl. Math. **19** (1983) 41–43.

[25] Constantin-Jerome Le Paige, *Sur l'équation du quatrième degré*, Časopis pro pěstování math. a fys., **14** (1884) 26–28.

[26] Alfred Lodge, *On the solution of the general equation of the fourth degree*, Quar. J. Pure Appl. Math. **19** (1883) 257–262.

[27] Thomas Muir, *The Theory of Determinants in the Historical Order of Development*, Vol. 1 (1906), Vol. 2 (1911), Vol. 3 (1920), Vol. 4 (1923), Macmillan, London. (Reprinted by Dover, New York.)

[28] Ivan Morton Niven, Herbert S. Zuckerman, and Hugh L. Montgomery, *An Introduction to the Theory of Numbers,* 5th edition, Wiley, New York, 1991.

[29] L. Clariana y Ricart, *Aplicación de las determinantes a la resolución de las ecuaciones de cuarto grado*, Crónica Científica Revista Internacional de Ciencias (Barcelona) **3** (1880) 425–429.

[30] Issai Schur, *Neue Begründung der Theorie der Gruppencharaktere*, Sitzungsberichte Akad. Wiss. Berlin (1905) 406-432; Gesammelte Abhandlungen I, Springer-Verlag, Berlin, 1973, pp. 143–169.

[31] Kai Wang, *On the group matrices for a generalized dihedral group*, Linear Algebra Appl. **39** (1981) 83-89.

[32] Heinrich Weber, *Lehrbuch der Algebra*, Vol. 2, 2nd edition, Friedrich Vieweg und Sohn, Braunschweig, 1899. (Reprinted by Chelsea, New York; and then reprinted by the American Mathematical Society, Providence, 1979.)