ijgt.ui.ac.ir

International Journal of Group Theory
ISSN (print): 2251-7650, ISSN (on-line): 2251-7669
Vol. x No. x (201x), pp. xx-xx.

www.ui.ac.ir

REPRESENTATIONS OF GROUP RINGS AND GROUPS

TED HURLEY
NATIONAL UNIVERSITY OF IRELAND GALWAY

Communicated by Patrizia Longobardi

Abstract. An isomorphism between the group ring of a finite group and a ring of certain block diagonal matrices is established. The group ring RG of a finite group G is isomorphic to the set of *group ring matrices* over R. It is shown that for any group ring matrix A of $\mathbb{C}G$ there exists a matrix U (independent of A) such that $U^{-1}AU = \mathrm{diag}(T_1, T_2, \ldots, T_r)$ for block matrices T_i of fixed size $s_i \times s_i$ where r is the number of conjugacy classes of G and s_i are the ranks of the group ring matrices of the primitive idempotents.

Using the isomorphism of the group ring to the ring of group ring matrices followed by the mapping $A \mapsto P^{-1}AP$ (fixed P) gives an isomorphism from the group ring to the ring of such block matrices. Specialising to the group elements gives a faithful representation of the group. Other representations of G may be derived using the blocks in the images of the group elements.

For a finite abelian group Q an explicit matrix P is given which diagonalises any group ring matrix of $\mathbb{C}Q$. The characters of Q and the character table of Q may be read off directly from the rows of the diagonalising matrix P. This is a special case of the general block diagonalisation process but is arrived at independently. The case for cyclic groups is well-known: Circulant matrices are the group ring matrices of the cyclic group and the Fourier matrix diagonalises any circulant matrix.

This has applications to signal processing.

1. Introduction

For basic information on groups and group rings, including information on conjugacy classes and representation theory, see [7], and for background on group ring matrices see [4]. For further information on representation theory and character theory see [3] and/or [6]. Results are given over the complex numbers $\mathbb{C}$ but many of the results hold over other suitably chosen fields.

MSC(2010): Primary: 16S34; Secondary: 20C05.

Keywords: Group, Ring, Representations.

Received: 07 December 2016, Accepted: 11 March 2017.

A matrix A is said to be *diagonalised by* P if $P^{-1}AP = D$ where D is a diagonal matrix. A circulant matrix can be diagonalised by the Fourier matrix of the same size. The diagonalising Fourier matrix is independent of the particular circulant matrix; this is the basis for the finite Fourier transform and the convolution theorem, see for example [2]. The Fourier $n \times n$ matrix satisfies $FF^* = nI_n$, (and is thus a complex Hadamard matrix) and when the rows are labelled by $\{1, g, g^2, \ldots, g^{n-1}\}$, it gives the characters and character table of the cyclic group C_n generated by g. The ring of circulant matrices over R is isomorphic to the ring of *group ring matrices* over R of the cyclic group.

The group ring of a finite group is isomorphic to the ring of group ring matrices as determined for example in [4]. The group ring matrices are types of matrices determined by their first rows; see section 2 below for precise formulation. For example circulant matrices are the group ring matrices of the cyclic group and matrices of the form $\begin{pmatrix} A & B \\ B^{\mathrm{T}} & A^{\mathrm{T}} \end{pmatrix}$, where A, B are circulant matrices, are determined by their first rows and correspond to the group ring matrices of the dihedral group. See Sections 2,4 and 5 below for further examples.

An isomorphism from the ring of group ring matrices of a finite group G into certain block diagonal matrices is established. More precisely it is shown that for any matrix A in the group ring matrix of a finite group G there exists a matrix U such that $U^{-1}AU = \mathrm{diag}(T_1, T_2, \ldots, T_r)$ for block matrices T_i of fixed size $s_i \times s_i$ where r is the number of conjugacy classes of G and the s_i are the ranks of the group ring matrices of the primitive idempotents. Thus the group ring $\mathbb{C}G$ is isomorphic to matrices of the type $\mathrm{diag}(T_1, T_2, \ldots, T_r)$. A faithful representation of the group itself may be given by taking images of the group elements. Other (linear) representations of G may be obtained by mapping elements of G to a block or a (direct) sum of a subset of the blocks which occur in their images in the isomorphism. See Sections 4 and 5 below for some applications and examples.

For a given finite abelian group H there exists a matrix P such that $P^{-1}BP$ is diagonal where B is any group ring matrix of H. The matrix P may be chosen so that $PP^* = nI_n$ and when the rows of P are labelled appropriately to the structure of the group as a product of cyclic group, then the rows of P gives the characters and character table of H. The diagonal entries are given precisely in terms of the entries of the first row of B. The abelian group case may be considered as a special case of the general case but the results are given directly and show explicitly how the characters and character tables of the abelian group may be obtained from the diagonalising matrix. Thus Section 5 (the abelian group case) is independent of the general case of Section 3.

The results for circulant $n \times n$ matrices hold over any field F which contains a primitive n^{th} root of unity. Similarly the general case holds over other such fields but this is not dealt with here.

The idea of using complete orthogonal sets of idempotents originated in [5] where these are used in the study and construction of types of multidimensional paraunitary matrices.

2. **Group ring matrices**

Certain classes of matrices are determined by their first row or column. A particular type of such matrices are those corresponding to group rings. It is shown in [4] that the group ring RG where $|G| = n$

may be embedded in the ring of $n \times n$ matrices over R in a precise manner. Let $\{g_1, g_2, \ldots, g_n\}$ be a fixed listing of the elements of G. Consider the following matrix:

$$\begin{pmatrix} g_1^{-1}g_1 & g_1^{-1}g_2 & g_1^{-1}g_3 & \cdots & g_1^{-1}g_n \\ g_2^{-1}g_1 & g_2^{-1}g_2 & g_2^{-1}g_3 & \cdots & g_2^{-1}g_n \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ g_n^{-1}g_1 & g_n^{-1}g_2 & g_n^{-1}g_3 & \cdots & g_n^{-1}g_n \end{pmatrix}$$

Call this the *matrix of* G (relative to this listing) and denote it by $M(G)$.

2.1. ***RG*-matrix.** Given a listing of the elements of G, form the matrix $M(G)$ of G relative to this listing. An *RG-matrix* over a ring R is a matrix obtained by substituting elements of R for the elements of G in $M(G)$. If $w \in RG$ and $w = \sum_{i=1}^{n} \alpha_i g_i$ then $\sigma(w)$ is the $n \times n$ RG-matrix obtained by substituting each α_i for g_i in the group matrix.

$$\text{Precisely } \sigma(w) = \begin{pmatrix} \alpha_{g_1^{-1}g_1} & \alpha_{g_1^{-1}g_2} & \alpha_{g_1^{-1}g_3} & \cdots & \alpha_{g_1^{-1}g_n} \\ \alpha_{g_2^{-1}g_1} & \alpha_{g_2^{-1}g_2} & \alpha_{g_2^{-1}g_3} & \cdots & \alpha_{g_2^{-1}g_n} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \alpha_{g_n^{-1}g_1} & \alpha_{g_n^{-1}g_2} & \alpha_{g_n^{-1}g_3} & \cdots & \alpha_{g_n^{-1}g_n} \end{pmatrix}$$

It is shown in [4] that $w \mapsto \sigma(w)$ gives a monomorphism of the group ring RG into the ring of $n \times n$ matrices over R.

Given the entries of the first row of an RG-matrix the entries of the other rows are determined from the matrix $M(G)$ of G.

An RG-matrix is a matrix corresponding to a group ring element in the isomorphism from the group ring into the ring of $R_{n\times n}$ matrices. The isomorphism depends on the listing of the elements of G. For example if G is cyclic, an RG-matrix is a circulant matrix relevant to the natural listing $G = \{1, g, g^2, \cdots, g^{n-1}\}$ where G is generated by g. When G is dihedral an RG-matrix is one of the form $\begin{pmatrix} A & B \\ B & A \end{pmatrix}$ where A is circulant and B is reverse circulant but also one of the form $\begin{pmatrix} A & B \\ B^{\mathrm{T}} & A^{\mathrm{T}} \end{pmatrix}$ where both A, B are circulant, in a different listing of G. Other examples are given within [4].

In general given a group ring element w, and a fixed listing of the elements of the group, the corresponding capital letter W is often used to denote the image of w, $\sigma(w)$, in the ring of RG-matrices.

Listing. Changing the listing of the elements of the group gives an equivalent RG-matrix and one is obtained from the other by a sequence of processes consisting of interchanging two rows and then interchanging the corresponding two columns.

3. **Block diagonal**

Matrices, when diagonalisable, may be simultaneously diagonalised if and only if they commute. However a set of matrices may be simultaneously block diagonalisable in the sense that there exist a matrix U such that $U^{-1}AU$ has the form $\text{diag}(T_1, T_2, \ldots, T_r)$, where each T_i is of fixed $r_i \times r_i$ size, for every matrix A in the set – and for U independent of A. This is the case for group ring matrices.

Idempotents will naturally play an important part. (See [5] where these are used for paraunitary matrices.) Recall that e is an idempotent in a ring R if $e^2 = e$ and $\{e, f\}$ are orthogonal if $ef = 0 = fe$. Say $\{e_1, e_2, \ldots, e_k\}$ is a complete orthogonal set of idempotents in a ring R if $e_i^2 = e_i, e_ie_j = 0$ for $i \neq j$ and $e_1 + e_2 + \cdots + e_k = 1$ where 1 is the identity of R. Moreover $\text{tr}A$ denotes the trace of a matrix A.

Proposition 3.1. *Suppose that $e_1, e_2, \ldots, e_k$ is a complete orthogonal set of idempotents in an associative algebra over a field F. Let $w = \alpha_1e_1 + \alpha_2e_2 + \cdots + \alpha_ke_k$ with $\alpha_i \in F$. Then w is invertible if and only if each $\alpha_i \neq 0$ and in this case $w^{-1} = {\alpha_1}^{-1}e_1 + {\alpha_2}^{-1}e_2 + \cdots + {\alpha_k}^{-1}e_k$.*

Proof. The proof is straightforward and is left to the reader.

□

Lemma 3.2. *Let $\{E_1, E_2, \ldots, E_s\}$ be a set of orthogonal idempotents in a ring of matrices. Then* $\text{rank}(E_1 + E_2 + \cdots + E_s) = tr(E_1 + E_2 + \cdots + E_s) = trE_1 + trE_2 + \cdots + trE_s = \text{rank}\, E_1 + \text{rank}\, E_2 + \cdots + \text{rank}\, E_s$.

Proof. It is known that $\text{rank}\, A = \text{tr}A$ for an idempotent matrix, see for example [1], and so $\text{rank}\, E_i = \text{tr}E_i$ for each i. If $\{E, F, G\}$ is a set of orthogonal idempotent matrices so is $\{E + F, G\}$. From this it follows that $\text{rank}(E_1 + E_2 + \cdots + E_s) = \text{tr}(E_1 + E_2 + \cdots E_s) = \text{tr}E_1 + \text{tr}E_2 + \cdots + \text{tr}E_s = \text{rank}\, E_1 + \text{rank}\, E_2 + \cdots + \text{rank}\, E_s$. □

Let $A = a_1E_1 + a_2E_2 + \cdots + a_kE_k$ for a complete set of idempotent orthogonal matrices E_i. Then A is invertible if and only if each a_i is non-zero and in this case $A^{-1} = a_1^{-1}E_1 + {a_2}^{-1}E_2 + \cdots + {a_k}^{-1}E_k$. This is a special case of the following.

Proposition 3.3. *Suppose that $E_1, E_2, \ldots, E_k$ is a complete symmetric orthogonal set of idempotents in ${}_{n\times n}$. Let $= a_1E_1 + a_2E_2 + \cdots + a_kE_k$. Then the determinant of Q is $|Q| = a_1^{\text{rank}\, E_1}a_2^{\text{rank}\, E_2} \cdots a_k^{\text{rank}\, E_k}$.*

Let RG be the group ring of a finite group G over the ring R. Let $\{e_1, e_2, \ldots, e_k\}$ be a complete orthogonal set of idempotents in RG and $\{E_1, E_2, \ldots, E_k\}$ the corresponding RG-matrices (relevant to some listing of the elements of G). Such a set of idempotents is known to exist when $R = \mathbb{C}$ (the complex number field), and also over other fields, see for example [3] or [7]. We will confine ourselves here to $\mathbb{C}$ but many of the results hold over these other fields. In the group ring $\mathbb{C}G$ the involution * is defined by $(\sum a_gg)^* = \sum a_g^*g^{-1}$ where * is the involution in $\mathbb{C}$. It follows from [4] that the matrix representation (the $\mathbb{C}G$-matrix) of $(\sum a_gg)^*$ is the complex conjugate transposed of the matrix representation ($\mathbb{C}G$-matrix) of $\sum a_gg$ as required.

The idempotent elements from the group ring over $\mathbb{C}$ satisfy $e^* = e$ and so the idempotent matrices are symmetric, that is $E^* = E$, and satisfy $E^2 = EE^* = E$.

We now specialise the E_i to be $n \times n$ matrices corresponding to the group ring idempotents e_i, that is $\sigma e_i = E_i$. Define the rank of e_i to be that of E_i.

Consider now the group ring FG where $F = \mathbb{C}$ (the complex number field) and G is a finite group. As already mentioned, FG contains a complete orthogonal set of idempotents $\{e_1, e_2, \ldots, e_k\}$ which may be taken to be primitive, see [7].

Theorem 3.4. *Let A be a FG-matrix with $F = \mathbb{C}$. Then there exists a non-singular matrix P independent of A such that $P^{-1}AP = T$ where T is a block diagonal matrix with blocks of size $r_i \times r_i$ for $i = 1, 2, \ldots, k$ and r_i are the ranks of the e_i.*

Proof. Let $\{e_1, e_2, \ldots, e_k\}$ be the orthogonal idempotents and $S = \{E_1, E_2, \ldots, E_k\}$ the group ring matrices corresponding to these, that is, $\sigma(e_i) = E_i$ in the embedding of the group ring into the $\mathbb{C}G$-matrices. Any column of E_i is orthogonal to any column of E_j for $i \neq j$ as $E_i E_j^* = 0$. Now let $\operatorname{rank} E_i = r_i$. Then $\sum_{i=1}^{k} r_i = n$. Let $S_i = \{v_{i,1}, v_{i,2}, \ldots, v_{i,r_i}\}$ be a basis for the column space of E_i consisting of a subset of the columns of E_i; do this for each i. Then each element of S_i is orthogonal to each element of S_j for $i \neq j$. Since $\sum_{i=1}^{k} r_i = n$ it follows that $S = \{S_1, S_2, \ldots, S_k\}$ is a basis for F^n.

Let $V_{i,j}$ denote the FG-matrix determined by the column vector $v_{i,j}$, let $S_i(G)$ denote the set of FG-matrices obtained by substituting $V_{i,j}$ for $v_{i,j}$ in S_i and let $S(G)$ denote the set of FG-matrices obtained by substituting $S_i(G)$ for S_i in S.

As S is a basis for F^n the first column of AE_i is a linear combination of elements from S. The first column of AE_i determines AE_i, as AE_i is an FG-matrix, and hence AE_i is a linear combination of elements of $S(G)$. By multiplying AE_i through on the right by E_i, and orthogonality, it follows that AE_i is a linear combination of $S_i(G) = \{V_{i,1}, V_{i,2}, \ldots, V_{i,r_i}\}$. Now each $V_{i,j}$ consists of columns which are a permutation of the columns of E_i. Also E_i contains the columns S_i. Thus equating AE_i to the linear combination of $S_i(G)$ implies that each $AV_{i,j}$ is a linear combination of S_i.

Let P be the matrix with columns consisting of the first columns S_i for $i = 1, 2, \ldots, k$. Then $AP = PA$ where T is a matrix of blocks of size $r_i \times r_i$ arranged diagonally for $i = 1, 2, \ldots, k$. Since P is invertible it follows that $P^{-1}AP = T$. □

The proof is constructive in the sense that the matrix P is constructed from the complete orthogonal set of idempotents. These are the steps:

(1) Find complete orthogonal set of idempotents $\{e_1, e_2, \ldots, e_k\}$ for FG.
(2) Construct the corresponding FG-matrices $\{E_1, E_2, \ldots, E_k\}$.
(3) Find a basis S_i for the column space of E_i for $1 \leq 1 \leq k$.
(4) Let P be the matrix made up of columns of the union of the S_i.
(5) Then $P^{-1}AP$ is a block diagonal matrix consisting of blocks of size $r_i \times r_i$ where r_i is the rank of E_i.

However this algorithm requires being able to construct a complete orthogonal set of idempotents. If the matrix P could be obtained directly then indeed this would be a way for the construction of the idempotents.

Corollary 3.5. *The group ring FG is isomorphic to a subring of such block diagonal matrices. The isomorphism is given by $w \mapsto \sigma(w) = W \mapsto P^{-1}WP$.*

The isomorphism includes an isomorphic embedding of the group G itself into the set of such block diagonal matrices. Other linear representations of G may be obtained by using the block images of the group elements.

Theorem 3.6. *Suppose that A is an FG-matrix where $F = \mathbb{C}$. Then there exists a unitary matrix P such that $P^TAP = T$ where T is a block diagonal matrix with blocks of size $r_i \times r_i$ for $i = 1, 2, \ldots, k$ along the diagonal.*

Proof. The diagonalising matrix in the proof of Theorem 3.4 may be made unitary by constructing an orthonormal basis for the space generated by $\{V_{i,1}, V_{i,2}, \ldots, V_{i,r_i}\}$ for each $i = 1, 2, \ldots, k$. Let $S_i = \{W_{i,1}, W_{i,2}, \ldots, W_{i,r_i}\}$ be an orthonormal basis for the space spanned by $\{V_{i,1}, V_{i,2}, \ldots, V_{i,r_i}\}$. Then $\hat{S} = \{S_1, S_2, \ldots, S_k\}$ is an orthonormal basis for F^n. Set P to be the matrix with elements of $\hat{S}$ as columns. Then P is unitary and $P^{\mathrm{T}}AP = T$ as required. □

The group ring is isomorphic to the ring of RG-matrices, see [4], and the ring of RG matrices is isomorphic to the ring of such block diagonal matrices under the mapping $w \mapsto \sigma(w) = W \mapsto P^{-1}WP$ for this fixed P.

4. Cases, applications

4.1. **Abelian.** When $G = C_n$, the cyclic group of order n, the matrix P of Theorem 3.4 is the Fourier matrix and T is a diagonal matrix. The case when G is any abelian group is fully dealt with in section 5.

4.2. **Dihedral.** The dihedral group D_{2n} is generated by two elements a and b with presentation:
$\langle a, b \mid a^n = 1,\ b^2 = 1,\ bab = a^{-1}\rangle$
It has order $2n$, and a natural listing of the elements is $\{1, a, a^2, \ldots, a^{n-1}, b, ab, a^2b, \ldots, a^{n-1}b\}$.

As every element in D_{2n} is conjugate to its inverse, the complex characters of D_{2n} are real. The characters D_{2n} are contained in an extension of $\mathbb{Q}$ of degree $\phi(n)/2$ and this is $\mathbb{Q}$ only for $2n \leq 6$. Here ϕ is the Euler phi function.

Let S_n denote the symmetric group of order n. Representations and orthogonal idempotents of the symmetric group are well known; see for example [3]. The characters of S_n are rational.

4.2.1. $S_3 = D_6$**.** Consider D_6. Note that $D_6 = S_3$. The conjugacy classes are $\{1\}, \{a, a^2\}, \{b, ab, a^2b\}$. The central (primitive, symmetric) idempotents are $e_0 = 1/6(1 + a + a^2 + b + ab + a^2b), e_1 = 1/6(1 + a + a^2 - b - ab - a^2b), e_3 = 1/3(2 - a - a^2)$.

This gives the corresponding group ring matrices:

$$E_0 = \frac{1}{6}\begin{pmatrix} 1&1&1&1&1&1\\ 1&1&1&1&1&1\\ 1&1&1&1&1&1\\ 1&1&1&1&1&1\\ 1&1&1&1&1&1\\ 1&1&1&1&1&1 \end{pmatrix}, E_1 = \frac{1}{6}\begin{pmatrix} 1&1&1&-1&-1&-1\\ 1&1&1&-1&-1&-1\\ 1&1&1&-1&-1&-1\\ -1&-1&-1&1&1&1\\ -1&-1&-1&1&1&1\\ -1&-1&-1&1&1&1 \end{pmatrix}, E_2 = \frac{1}{3}\begin{pmatrix} 2&-1&-1&0&0&0\\ -1&2&-1&0&0&0\\ -1&-1&2&0&0&0\\ 0&0&0&2&-1&-1\\ 0&0&0&-1&2&-1\\ 0&0&0&-1&-1&2 \end{pmatrix}.$$

Now E_0, E_1 have rank 1 and E_2 has rank 4 from general theory.

Thus we need a set consisting of one column from each of E_0, E_1 and 4 linearly independent columns from E_2 to form a set of 6 linearly independent vectors. It is easy to see that
$v_1 = (1,1,1,1,1,1)^{\mathrm{T}}, v_2 = (1,1,1,-1,-1,-1)^{\mathrm{T}}, v_3 = (2,-1,-1,0,0,0)^{\mathrm{T}},$
$v_4 = (-1,2,-1,0,0,0)^{\mathrm{T}}, v_5 = (0,0,0,2,-1,-1)^{\mathrm{T}}, v_6 = (0,0,0,-1,2,-1)^{\mathrm{T}}$
is such a set.

Now let $P = (v_1, v_2, v_3, v_4, v_5, v_6)$. Then for any $\mathbb{C}D_6$ matrix A, $P^{-1}AP = \mathrm{diag}(a, b, D)$ where D is a 4×4 matrix.

As noted, the group ring is isomorphic to the ring of RG-matrices, and the ring of RG matrices is isomorphic to the ring of such block diagonal matrices under the mapping $A \mapsto P^{-1}AP$ for this fixed P.

Now consider the image of D_6 itself under this isomorphism. The matrix A of $a \in S_3 = D_6$ in this isomorphism is mapped to $P^{-1}AP$. Here $A = \left(\begin{array}{ccc|ccc} 0&1&0&0&0&0\\ 0&0&1&0&0&0\\ 1&0&0&0&0&0\\ \hline 0&0&0&0&0&1\\ 0&0&0&1&0&0\\ 0&0&0&0&1&0 \end{array}\right)$

and $P^{-1}AP = \left(\begin{array}{cc|cccc} 1&0&0&0&0&0\\ 0&1&0&0&0&0\\ \hline 0&0&-1&1&0&0\\ 0&0&-1&0&0&0\\ 0&0&0&0&0&-1\\ 0&0&0&0&1&-1 \end{array}\right)$.

(In some cases it is easier to work out AP and then solve for D in PD where D is of the correct block diagonal type.)

Similarly the image of b is obtained; B is the RG-matrix of b and $P^{-1}BP = \left(\begin{array}{cc|cccc} 1&0&0&0&0&0\\ 0&-1&0&0&0&0\\ \hline 0&0&0&0&1&0\\ 0&0&0&0&0&1\\ 0&0&1&0&0&0\\ 0&0&0&1&0&0 \end{array}\right)$.

Representations of $S_3 = D_6$ may be obtained using the block matrices of the images of the group elements. For example $a \mapsto \begin{pmatrix} -1 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & -1 \end{pmatrix}, b \mapsto \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$ gives a representation of $D_6 = S_3$.

It may be shown directly from the structure of P and of A corresponding to a group element a that the 4×4 part in $P^{-1}AP$ has the form $T = \begin{pmatrix} X & 0 \\ 0 & Y \end{pmatrix}$ or of the form $S = \begin{pmatrix} 0 & X \\ Y & 0 \end{pmatrix}$ where X, Y are 2×2 blocks.

Say a matrix is in $\mathbb{T}$ if it has the form T as above and say a matrix is in $\mathbb{S}$ if it has the form S as above. Interestingly then generally $TS \in \mathbb{S}, ST \in \mathbb{S}, T_1T_2 \in \mathbb{T}, S_1S_2 \in \mathbb{T}$, for $S, S_1, S_2 \in \mathbb{S}, T, T_1, T_2 \in \mathbb{T}$. Such structures and their generalisations will be dealt with in a later paper.

4.2.2. **Unitary simultaneous block diagonalisation.** Now P may be made orthogonal by finding an orthogonal basis for the 4 linearly independent columns of E_2 and then dividing each of the resulting set of 6 vectors by their lengths.

An orthogonal basis for the columns of E_2 is

$\{(2,-1,-1,0,0,0)^{\mathrm{T}}, (0,1,-1,0,0,0)^{\mathrm{T}}, (0,0,0,2,-1,-1)^{\mathrm{T}}, (0,0,0,0,1,-1)^{\mathrm{T}}\}$.

Construct an orthonormal basis:

$v_1 = \sqrt{\frac{1}{6}}(1,1,1,1,1,1)^{\mathrm{T}}, v_2 = \sqrt{\frac{1}{6}}(1,1,1,-1,-1,-1)^{\mathrm{T}}, v_3 = \sqrt{\frac{1}{6}}(2,-1,-1,0,0,0)^{\mathrm{T}},$

$v_4 = \sqrt{\frac{1}{2}}(0,1,-1,0,0,0)^{\mathrm{T}}, v_5 = \sqrt{\frac{1}{6}}(0,0,0,2,-1,-1)^{\mathrm{T}}, v_6 = \sqrt{\frac{1}{2}}(0,0,0,0,1,-1)^{\mathrm{T}}.$

Now construct the unitary (orthogonal in this case) matrix $P = (v_1, v_2, v_3, v_4, v_5, v_6)$. Then for any $\mathbb{C}D_6$ matrix A, $P^*AP = \mathrm{diag}(a, b, D)$ where D is a 4×4 matrix.

When P is unitary, = orthogonal in this case, then $P^{\mathrm{T}}AP$ and $P^{\mathrm{T}}BP$ are unitary as A, B are orthogonal. The diagonal 4×4 matrix must then be orthogonal. For example:

$$P^{\mathrm{T}}AP = P^*AP = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1/2 & \sqrt{3}/2 & 0 & 0 \\ 0 & 0 & -\sqrt{3}/2 & -1/2 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1/2 & -\sqrt{3}/2 \\ 0 & 0 & 0 & 0 & \sqrt{3}/2 & -1/2 \end{pmatrix}$$

The 4×4 block matrix is easily checked to be unitary/orthogonal as expected from the theory.

4.3. **Further dihedral groups.** The character tables for D_{2n} may be found in [6]. We outline how the results may be applied in the case of D_{10}.

The character table of D_{10} is the following: $\left(\begin{array}{cccc} 1 & b & a & a^2 \\ 1 & 5 & 2 & 2 \\ \hline 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ 2 & 0 & 2\cos(2\pi/5) & 2\cos(4\pi/5) \\ 2 & 0 & 2\cos(4\pi/5) & 2\cos(8\pi/5) \end{array}\right)$.

This gives the following complete (symmetric) orthogonal set of idempotents in the group ring: $e_0 = \frac{1}{10}(1+a+a^2+a^3+a^4+b+ba+ba^2+ba^3+ba^4), e_1 = \frac{1}{10}(1+a+a^2+a^3+a^4-b-ba-ba^2-ba^3-ba^4), e_2 = \frac{4}{10}(1+\cos(2\pi/5)a+\cos(4\pi/5)a^2+\cos(4\pi/5)a^3+\cos(2\pi/5)a^4), e_3 = \frac{4}{10}(1+\cos(4\pi/5)a+\cos(8\pi/5)a^2+\cos(8\pi/5)a^3+\cos(4\pi/5)a^4)$.

Let $\sigma(e_i) = E_i$ – this is the image of the group ring element e_i in the group ring matrix. Each of E_0, E_1 has rank 1 and each of E_2, E_3 has rank 4. Four linearly independent columns in each of E_2, E_3 are easy to obtain and indeed four orthogonal such may be derived if required. The matrix P is formed using the first columns of E_1, E_2 and 4 linearly independent columns of each of E_3 and E_4. Then $P^{-1}AP = \text{diag}(\alpha_1, \alpha_2, T_1, T_2)$ for any group ring matrix A of D_{10} where T_1, T_2 are 4×4 block matrices. Then the composition of mappings $w \mapsto \sigma(w) = W \mapsto P^{-1}WP$ is an isomorphism. Representations of the group may be obtained by specialising to blocks of the images of the group elements.

The form of P is $\begin{pmatrix} A & C & 0 & D & 0 \\ B & 0 & C_1 & 0 & D_1 \end{pmatrix}$ for suitable 5×2 blocks $A, 0, C, D, C_1, D_1$. Then it may be shown that in $P^{-1}AP$ the two 4×4 blocks have the form $\begin{pmatrix} X & 0 \\ 0 & Y \end{pmatrix}$ or else the form $\begin{pmatrix} 0 & X \\ Y & 0 \end{pmatrix}$ for 2×2 blocks X, Y when A corresponds to a group element a.

4.4. **Quaternion group of order** 8**.** The five primitive central idempotents $\{e_1, e_2, e_3, e_4, e_5\}$ of $\mathbb{C}K_8$ where K_8 is the quaternion group of order 8 is given in [7] page 186. $K_8 = \langle a, b \,|\, a^4 = 1, a^2 = b^2, bab^{-1} = a^{-1} \rangle$ and is listed as $\{1, a, a^2, a^3, b, ab, a^2b, a^3b\}$.

$$\begin{aligned} e_1 &= 1/8(1 + a + a^2 + a^3 + b + ab + a^2b + a^3b) \\ e_2 &= 1/8(1 + a + a^2 + a^3 - b - ab - a^2b - a^3b) \\ e_3 &= 1/8(1 - a + a^2 - a^3 + b - ab + a^2b - a^3b) \\ e_4 &= 1/8(1 - a + a^2 - a^3 - b + ab - a^2b + a^3b) \\ e_5 &= 1/2(1 - a^2) \end{aligned}$$

([7] has $-ab$ in e_4 which should be $+ab$ as above.)

The group ring matrices $\{E_1, E_2, E_3, E_4\}$ corresponding to $\{e_1, e_2, e_3, e_4\}$ respectively have rank 1 and the group ring matrix E_5 corresponding to e_5 has rank 4, which can be seen from theory. Thus take the first columns of E_1, E_2, E_3, E_4 and 4 linearly independent columns of E_5 to form a matrix P. Then $P^{-1}AP = \text{diag}(T_1, T_2, T_3, T_4, T_5)$ where T_1, T_2, T_3, T_4 are scalars and T_4 is a 4×4 matrix, for any group ring matrix A of K_8.

Precisely we may take:

$$P=\left(\begin{array}{c|c|c|c|cccc}
1 & 1 & 1 & 1 & 1 & 0 & 0 & 0\\
1 & 1 & -1 & -1 & 0 & 1 & 0 & 0\\
1 & 1 & 1 & 1 & -1 & 0 & 0 & 0\\
1 & 1 & -1 & -1 & 0 & -1 & 0 & 0\\
1 & -1 & 1 & -1 & 0 & 0 & 1 & 0\\
1 & -1 & -1 & 1 & 0 & 0 & 0 & 1\\
1 & -1 & 1 & -1 & 0 & 0 & -1 & 0\\
1 & -1 & -1 & 1 & 0 & 0 & 0 & -1
\end{array}\right)$$

and then $P^{-1}AP = \mathrm{diag}(\alpha_1, \alpha_2, \alpha_3, \alpha_4, T)$ for any group ring matrix A of K_8 where T is a 4×4 matrix.

This gives an isomorphism from the group ring of K_8 to these block matrices given by $w \mapsto \sigma(w) = W \mapsto P^{-1}WP$. Representations of K_8 may be obtained by specialising to the group elements.

The following then gives an embedding of K_8:

$$a \mapsto \left(\begin{array}{cccc|cccc}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & -1 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & -1 & 0 & 0 & 0 & 0\\
\hline
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0\\
0 & 0 & 0 & 0 & -1 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & -1\\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0
\end{array}\right), b \mapsto \left(\begin{array}{cccc|cccc}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & -1 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & -1 & 0 & 0 & 0 & 0\\
\hline
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1\\
0 & 0 & 0 & 0 & -1 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & -1 & 0 & 0
\end{array}\right)$$

Using the blocks gives other representations. For example

$$a \mapsto \left(\begin{array}{cc|cc}
0 & 1 & 0 & 0\\
-1 & 0 & 0 & 0\\
\hline
0 & 0 & 0 & -1\\
0 & 0 & 1 & 0
\end{array}\right), b \mapsto \left(\begin{array}{cc|cc}
0 & 0 & 1 & 0\\
0 & 0 & 0 & 1\\
\hline
-1 & 0 & 0 & 0\\
0 & -1 & 0 & 0
\end{array}\right)$$

gives a representation of K_8.

It may be shown directly from the block form of P that the image of a group element has the 4×4 block of the form $\begin{pmatrix} X & 0 \\ 0 & Y \end{pmatrix}$ or else the form $\begin{pmatrix} 0 & X \\ Y & 0 \end{pmatrix}$ for 2×2 blocks X, Y.

5. **Abelian groups**

The abelian group case follows from the general case, Section 3, but may be tackled directly and more illuminatingly as follows.

Let $\{A_1, A_2, \ldots, A_k\}$ be an ordered set of matrices of the same size. Then the *block circulant matrix* formed from the set is $A = \text{circ}(A_1, A_2, \ldots, A_k) = \begin{pmatrix} A_1 & A_2 & \cdots & A_k \\ A_k & A_1 & \cdots & A_{k-1} \\ \vdots & \vdots & \vdots & \vdots \\ A_2 & A_3 & \cdots & A_1 \end{pmatrix}$

If the A_i have size $m \times t$ then A has size $km \times kt$. The block circulant formed depends on the order of the elements in $\{A_1, A_2, \ldots, A_k\}$.

Let P be an $n \times n$ matrix. Then the *block Fourier matrix* P_f corresponding to P is $P \otimes F$, the tensor product of P and F where F is the Fourier $n \times n$ matrix.

Thus $P_f = P \otimes F = \begin{pmatrix} P & P & P & \cdots & P \\ P & \omega P & \omega^2 P & \cdots & \omega^{n-1} P \\ \vdots & \vdots & \vdots & \vdots & \\ P & \omega^{n-1} P & \omega^{2(n-1)} & \cdots & \omega^{(n-1)(n-1)} P \end{pmatrix}$

It is clear then that:

Proposition 5.1. *P_f is invertible if and only if P is invertible and the inverse when it exists is $P^{-1} \otimes F^*$.*

Here F^* denotes the inverse of the Fourier matrix. If the Fourier matrix is normalised in $\mathbb{C}$, then F^* is the complex conjugate transposed of F.

The following theorem may be proved in a manner similar to the proof that the Fourier matrix diagonalises a circulant matrix.

Theorem 5.2. *Suppose that $\{A_1, A_2, \ldots, A_k\}$ are matrices of the same size and can be simultaneously diagonalised by P with $P^{-1} A_i P = D_i$ where each D_i is diagonal. Then the block circulant matrix A formed from these matrices can be diagonalised by*

$$P_f = P \otimes F = \begin{pmatrix} P & P & P & \cdots & P \\ P & \omega P & \omega^2 P & \cdots & \omega^{k-1} P \\ P & \omega^2 P & \omega^4 P & \cdots & \omega^{2(k-1)} P \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ P & \omega^{k-1} P & \omega^{2(k-1)} P & \cdots & \omega^{(k-1)(k-1)} P \end{pmatrix}$$ *where ω is a primitive k-th root of unity.*

Moreover $P_f^{-1} A P_f = D$ where D is diagonal and

$D = \text{diag}(D_1 + D_2 + \cdots + D_k, D_1 + \omega D_2 + \cdots + \omega^{k-1} D_k, D_1 + \omega^2 D_2 + \omega^4 D_3 + \cdots + \omega^{2(k-1)} D_k, \ldots, D_1 + \omega^{k-1} D_2 + \omega^{2(k-1)} D_3 + \cdots + \omega^{(k-1)(k-1)} D_k)$

Proof. The proof of this is direct, involving working out AP_f and showing it is $P_f D$, with D as given. Since P_f is invertible by Proposition 5.1 the result will follow. This is similar to a proof that the Fourier matrix diagonalises a circulant matrix. □

The simultaneous diagonalisation process of Theorem 5.2 may then be repeated.

Suppose now $G = K \times H$, the direct product of K, H, and H is cyclic. Then a group ring matrix of G is of the form $M = \text{circ}(K_1, K_2, \ldots, K_h)$ where K_i are group ring matrices of K and $|H| = h$. If the

K_i can be diagonalised by P then M can be diagonalised by the Fourier block matrix formed from P by Theorem 5.2. A finite abelian group is the direct product of cyclic groups and thus repeating the process enables the simultaneous diagonalisation of the group ring matrices of a finite abelian group. The characters and character table of the finite abelian group may be read off from the diagonalising matrix. The examples below illustrate the method.

5.1. **Examples.**

- Consider $G = C_3 \times C_3$. Now $P = \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{pmatrix}$ where ω is a primitive third root of unity diagonalises any circulant 3×3 matrix which is the group ring matrix of C_3. Then $P_f = \begin{pmatrix} P & P & P \\ P & \omega P & \omega^2 P \\ P & \omega^2 P & \omega P \end{pmatrix}$ diagonalises any group ring matrix of $C_3 \times C_3$.

  Written out in full: $P_f =$

$$\left(\begin{array}{ccc|ccc|ccc} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^2 & 1 & \omega & \omega^2 & 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega & 1 & \omega^2 & \omega & 1 & \omega^2 & \omega \\ \hline 1 & 1 & 1 & \omega & \omega & \omega & \omega^2 & \omega^2 & \omega^2 \\ 1 & \omega & \omega^2 & \omega & \omega^2 & 1 & \omega^2 & 1 & \omega \\ 1 & \omega^2 & \omega & \omega & 1 & \omega^2 & \omega^2 & \omega & 1 \\ \hline 1 & 1 & 1 & \omega^2 & \omega^2 & \omega^2 & \omega & \omega & \omega \\ 1 & \omega & \omega^2 & \omega^2 & 1 & \omega & \omega & \omega^2 & 1 \\ 1 & \omega^2 & \omega & \omega^2 & \omega & 1 & \omega & 1 & \omega^2 \end{array}\right)$$

  The characters and character table of $C_3 \times C_3$ may be read off from the rows of P_f by labelling the rows of P_f appropriate to the listing of the elements of $C_3 \times C_3$ when forming the group ring matrices. The listing here is $\{1, g, g^2, h, hg, hg^2, h^2, h^2g, h^2g^2\}$ where the C_3 are generated by $\{g, h\}$ respectively. Thus the character table of $C_3 \times C_3$ is

$$\left(\begin{array}{ccccccccc} 1 & g & g^2 & h & hg & hg^2 & h^2 & hg^2 & h^2g^2 \\ \hline\hline 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^2 & 1 & \omega & \omega^2 & 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega & 1 & \omega^2 & \omega & 1 & \omega^2 & \omega \\ 1 & 1 & 1 & \omega & \omega & \omega & \omega^2 & \omega^2 & \omega^2 \\ 1 & \omega & \omega^2 & \omega & \omega^2 & 1 & \omega^2 & 1 & \omega \\ 1 & \omega^2 & \omega & \omega & 1 & \omega^2 & \omega^2 & \omega & 1 \\ 1 & 1 & 1 & \omega^2 & \omega^2 & \omega^2 & \omega & \omega & \omega \\ 1 & \omega & \omega^2 & \omega^2 & 1 & \omega & \omega & \omega^2 & 1 \\ 1 & \omega^2 & \omega & \omega^2 & \omega & 1 & \omega & 1 & \omega^2 \end{array}\right)$$

  Note that $\frac{1}{\sqrt{9}}P_f$ is unitary and that P_f is a Hadamard complex matrix.

- For $C_2 \times C_4$ consider $P = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ and note that a primitive fourth root of 1 is $i = \sqrt{-1}$. Then $i^2 = -1, i^3 = -i, i^4 = 1$. Now form $Q = \begin{pmatrix} P & P & P & P \\ P & iP & -P & -iP \\ P & -P & P & -P \\ P & -iP & -P & iP \end{pmatrix}$. The characters of $C_2 \times C_4$ can be read off from Q, Q is a Hadamard complex matrix and $\frac{1}{\sqrt{8}}Q$ is unitary.
- For $C_3 \times C_4$ consider that $C_3 \times C_4 \cong C_{12}$. Then the diagonalising matrix obtained using the natural ordering in $C_3 \times C_4$ is equivalent to the diagonalising matrix using the natural ordering in C_{12}.
- Consider C_2^n. Let $P_1 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ and inductively define for $n \geq 2$, $P_n = \begin{pmatrix} P_{n-1} & P_{n-1} \\ P_{n-1} & -P_{n-1} \end{pmatrix}$. Then P_n diagonalises any $\mathbb{C}C_2^n$-matrix and the characters of C_2^n may be read off from the rows of P_n. Note that P_n is a Hadamard (real) matrix.

References

[1] O. M. Baksalary, D. S. Bernstein and G. Trenkler, On the equality between rank and trace of an idempotent matrix, *Appl. Math. Comput.*, **217** 2010 4076–4080.

[2] R. E. Blahut, *Algebraic Codes for Data Transmission*, CUP, 2003.

[3] C. Curtis and I. Reiner, Representation Theory of Finite Groups and Associative Algebras, *Amer. Math. Soc.*, Chelsea, 1966.

[4] T. Hurley, Group rings and rings of matrices, *Inter. J. Pure & Appl. Math.*, **31** (2006) 319–335.

[5] B. Hurley and T. Hurley, Paraunitary matrices and group rings, *Int. J. of Group Theory*, **3** (2014) 31-56. (See also arXiv:1205.0703v1.)

[6] I. Martin Isaacs, *Character Theory of Finite Groups*, Dover, 2011.

[7] C. Polcino Milies and S. Sehgal, *An introduction to Group Rings*, Klumer, 2002.