International Journal of Pure and Applied Mathematics

Volume 31 No. 3 2006, 319-335

GROUP RINGS AND RINGS OF MATRICES

Ted Hurley

Department of Mathematics
National University of Ireland
Galway, IRELAND
e-mail: ted.hurley@nuigalway.ie

Abstract: It is shown that the group ring RG of a group G of order n over a ring R is isomorphic to a certain ring of $n \times n$ matrices over R. When the ring R has an identity element and no zero-divisors, this representation enables us to describe the units and zero-divisors of the group ring in terms of properties of these matrices and where appropriate in terms of the determinant of the matrices.

The isomorphism extends to group rings of infinite groups when the elements of the group can be listed.

The rings of matrices which turn up as isomorphic to certain group rings include circulant matrices, Toeplitz matrices, Walsh-Toeplitz matrices, circulant or Toeplitz combined with Hankel matrices and block-type circulant matrices. Group rings thus can be considered to be a generalisation of these rings of matrices, which occur in communications, signal processes, time series analysis and elsewhere.

When G is finite and R is a field, it follows from the representation that $U(RG)$, the group of units of RG, satisfies the Tits' alternative and consequently the generalised Burnside problem has a positive answer for $U(RG)$.

AMS Subject Classification: 20C05, 20C07, 16S34, 15A30
Key Words: group ring, rings of matrices

1. Introduction

Let RG denote the group ring of the group G over the ring R.

A non-zero element z in a ring W is said to be a *zero-divisor* in W if and

Received: July 19, 2006

only if there exists a non-zero element $r \in W$ with $z * r = 0$. When W has an identity 1_W say u is a *unit* in W if and only if there exists an element $w \in W$ with $u * w = 1_W$. The group of units of W is denoted by $U(W)$. We shall be particularly interested in zero-divisors and units in RG. In many cases we will assume that R itself has no zero divisors.

$R_{n\times n}$ denotes the ring of $n \times n$ matrices with coefficients from R.

For further details and background see Milies and Sehgal [2] and Sehgal [4].

Group rings and their units appear in many branches of mathematics. The book [2] also contains excellent historical background, notes and applications.

We establish an isomorphism between the group ring RG and a ring of certain $n \times n$ matrices over R and these are described explicitly below.

The representation is used to give a number of results on units and zero-divisors in group rings. A matrix method/algorithm for deciding whether or not an element in RG is a unit or a zero-divisor and a description of the units and zero-divisors as units and zero-divisors in a matrix ring are given. It is shown for example that over a field every element is either a unit or a zero-divisor; this was known for finite fields.

Using this representation it follows that $U(RG)$, the group of units of RG, satisfies the Tits' alternative when R is a field and consequently the generalised Burnside problem has a positive answer for $U(RG)$.

1.1. Some Rings of Matrices which Occur as Group Rings

When G is the cyclic group of order n these RG-matrices turn out to be the *circulant* $n \times n$ matrices over R.[1] In the case of an elementary Abelian 2-group of rank n and order 2^n, where the matrix size is $2^n \times 2^n$, the RG-matrices turn out to be what are termed *Walsh-Toeblitz* matrices over R - see for example [3]. In the case of the dihedral group the RG-matrices turn out to be matrices of the form $\begin{pmatrix} A & B \\ B & A \end{pmatrix}$, where A is a (general) circulant matrix and B is a reverse circulant matrix very similar to a Hankel matrix. The ring of such matrices in this case is, when R is an integral domain not of characteristic 2, isomorphic to the ring of matrices of the form $\begin{pmatrix} A+B & 0 \\ 0 & A-B \end{pmatrix}$.

In the general finite Abelian group case, RG is isomorphic to certain block

[1] When $R = F$, a field, particularly for $\mathbb{C}$ the complex numbers, this is known and used although not always explicitly stated in terms of group rings; it is used in signal processing especially when considering the convolution of vectors or signals. The circulant matrix is diagonalised by the Fourier matrix – see for example [1]

circulant matrices. It is an easy consequence that these block circulant matrices commute and are normal. Some special classes of these block circulant matrices have been studied previously for their applications.

A Toeplitz matrix is one that is constant along any diagonal running from upper left to lower right. Circulant matrices are special types of Toeplitz matrices. It is known that a Toeplitz $n \times n$ matrix can be embedded in a $2n \times 2n$ circulant matrix (see for example [1]), and this has proved useful in the study of Toeplitz matrices and their applications.

1.1.1. Infinite

The set of infinite[2] Toeplitz matrices over R is isomorphic to the group ring RG of the infinite cyclic group G. The set of Walsh-Toeplitz infinite matrices over R is isomorphic to RG, where G is the direct product of an infinite number of copies of $\mathbb{Z}_2$. When G is the infinite dihedral group then RG is isomorphic to the set (ring) of infinite matrices of the form $\begin{pmatrix} A & B \\ B & A \end{pmatrix}$, where A is the infinite Toeplitz matrix and B is the infinite Hankel matrix (with no restriction); as for the finite case the ring of matrices of the form $\begin{pmatrix} A & B \\ B & A \end{pmatrix}$ is isomorphic to the ring of matrices of the form $\begin{pmatrix} A+B & 0 \\ 0 & A-B \end{pmatrix}$, when R is an integral domain not of characteristic 2.

1.1.2. Possible Applications

For each group ring RG the set of RG-matrices can be considered as a ring of matrices of a special type some of which have already been studied for their applications in communications, signal processing, time series analysis and other areas. There are structure theorems for group rings which could also prove to be useful in the study of these rings of matrices.

2. The Matrix of G

Let $\{g_1, g_2, \ldots, g_n\}$ be a fixed listing of the elements of G.

[2]In the infinite case we naturally assume that the infinite matrices have only a finite number of entries in any row or column.

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 $M(G)$. Its entries are elements of G and it has some interesting properties. Every row and every column contains the elements of G in some order.

2.1. The Matrix Corresponding to a Group Ring Element

Suppose then $w = \sum_{i=1}^{n} \alpha_{g_i} g_i \in RG$. We now form the RG-matrix of w denoted by $M(RG, w)$ and defined as follows:

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

Thus $M(RG, w)$ is in $R_{n\times n}$. Consider the first column of $M(RG, w)$ as being *labelled* by g_1, the second column by g_2, etc. The importance of this matrix is that if $b = \sum_{i=1}^{n} \beta_{g_i} g_i$ is in RG then the coefficient of g_i in the product $b * w$ is $(\beta_{g_1}, \beta_{g_2}, \ldots, \beta_{g_n})$ times the i-th column of $M(RG, w)$.

Given then a listing of the elements of G, form the matrix $M(G)$ of G relative to this listing. Then an *RG-matrix over R* is a matrix obtained by substituting elements of R for elements of $M(G)$, so that if two entries in $M(G)$ are equal as group elements then the corresponding entries in the RG-matrix are equal.[3]

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; each row and each column is a permutation of the first row determined by the matrix of G.

Theorem 1 below is the main theorem.

Theorem 1. *Given a listing of the elements of a group G of order n there is a bijective ring homomorphism between RG and the $n \times n$ G-matrices over R. This bijective ring homomorphism is given by $\sigma : w \mapsto M(RG, w)$.*

[3]The matrix $M(G)$ of G is not its multiplication table.

Proof. Let $G = \{g_1, g_2, \ldots, g_n\}$ be the listing of the elements of G and let M denote the set of G-matrices relative to this listing. Now define mapping $\sigma : RG \to M$ as follows. Suppose $w = \sum_{i=1}^{n} \alpha_{g_i} g_i$. Then

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

This mapping is obviously additive, surjective and injective. It is thus sufficient to show that σ is multiplicative. Consider $t = \sum_{i=1}^{n} \beta_{g_i} g_i$ and

$$\sigma(t) = \begin{pmatrix} \beta_{g_1^{-1}g_1} & \beta_{g_1^{-1}g_2} & \beta_{g_1^{-1}g_3} & \ldots & \beta_{g_1^{-1}g_n} \\ \beta_{g_2^{-1}g_1} & \beta_{g_2^{-1}g_2} & \beta_{g_2^{-1}g_3} & \ldots & \beta_{g_2^{-1}g_n} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \beta_{g_n^{-1}g_1} & \beta_{g_n^{-1}g_2} & \beta_{g_n^{-1}g_3} & \ldots & \beta_{g_n^{-1}g_n} \end{pmatrix}.$$

Suppose $t * w = c$, where $c = \sum_{i=1}^{n} \gamma_{g_i} g_i$. Then

$$\sigma(t) * \sigma(w) = \begin{pmatrix} \gamma_{g_1^{-1}g_1} & \gamma_{g_1^{-1}g_2} & \gamma_{g_1^{-1}g_3} & \ldots & \gamma_{g_1^{-1}g_n} \\ \gamma_{g_2^{-1}g_1} & \gamma_{g_2^{-1}g_2} & \gamma_{g_2^{-1}g_3} & \ldots & \gamma_{g_2^{-1}g_n} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \gamma_{g_n^{-1}g_1} & \gamma_{g_n^{-1}g_2} & \gamma_{g_n^{-1}g_3} & \ldots & \gamma_{g_n^{-1}g_n} \end{pmatrix},$$

and this of course is $M(RG, c) = \sigma(t * w)$ as required. □

From now on σ denotes the mapping σ as in Theorem 1.

Theorem 2. *Suppose R has an identity. Then $w \in RG$ is a unit in RG if and only if $\sigma(w)$ is a unit in $R_{n\times n}$.*

Proof. Suppose w is a unit in RG and that u is its inverse. Then $u * w = 1_{RG}$ and hence $\sigma(u * w) = \sigma(1_{RG}) = I_n$, the identity matrix in $R_{n\times n}$. Thus $\sigma(u) * \sigma(w) = I_n$. Similarly $\sigma(w) * \sigma(u) = I_n$ and so $\sigma(w)$ is invertible in $R_{n\times n}$.

Suppose now $\sigma(w)$ is a unit in $R_{n\times n}$ and let B denote its inverse. Let

$w = \alpha_{g_1} g_1 + \alpha_{g_2} g_2 + \ldots \alpha_{g_n} g_n$. Then

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

We do not know a priori that B is a RG-matrix. Let $b = (\beta_1, \beta_2, \ldots, \beta_n)$ be the first row of B. Then:

$$\begin{array}{ccccccccccc} \beta_1\alpha_{g_1^{-1}g_1} & + & \beta_2\alpha_{g_2^{-1}g_1} & + & \ldots & + & \beta_n\alpha_{g_n^{-1}g_1} & = & 1\,, \\ \beta_1\alpha_{g_1^{-1}g_2} & + & \beta_2\alpha_{g_2^{-1}g_2} & + & \ldots & + & \beta_n\alpha_{g_n^{-1}g_2} & = & 0\,, \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \beta_1\alpha_{g_1^{-1}g_n} & + & \beta_2\alpha_{g_2^{-1}g_n} & + & \ldots & + & \beta_n\alpha_{g_n^{-1}g_n} & = & 0\,. \end{array} \tag{1}$$

Now $w = \alpha_{g_1} g_1 + \alpha_{g_2} g_2 + \ldots \alpha_{g_n} g_n = \alpha_{g_i^{-1}g_1} g_i^{-1} g_1 + \alpha_{g_i g_2} g_i^{-1} g_2 + \ldots + \alpha_{g_i^{-1}g_n} g_i^{-1} g_n$, for each $i, 1 \le i \le n$.

Define $u = \beta_1 g_1 + \beta_2 g_2 + \ldots + \beta_n g_n$. Then:

$$\beta_i g_i(\alpha_{g_1} g_1 + \alpha_{g_2} g_2 + \ldots \alpha_{g_n} g_n) = \beta_i g_i \alpha_{g_i^{-1}g_1} g_i^{-1} g_1 + \beta_i g_i \alpha_{g_i^{-1}g_2} g_i^{-1} g_2$$
$$+ \ldots + \beta_i g_i \alpha_{g_i^{-1}g_n} g_i^{-1} g_n = \beta_i \alpha_{g_i^{-1}g_1} g_1 + \beta_i \alpha_{g_i^{-1}g_2} g_2 + \ldots + \beta_i \alpha_{g_i^{-1}g_n} g_n\,.$$

Hence: $u * w = (\beta_1 g_1 + \beta_2 g_2 + \ldots + \beta_n g_n)(\alpha_{g_1} g_1 + \alpha_{g_2} g_2 + \ldots \alpha_{g_n} g_n)$ is equal to:

$$\begin{array}{ccccccccccc} & \beta_1 g_1 \alpha_{g_1^{-1}g_1} g_1^{-1} g_1 & + & \beta_2 g_2 \alpha_{g_2^{-1}g_1} g_2^{-1} g_1 & + & \ldots & + & \beta_n g_n \alpha_{g_n^{-1}g_1} g_n^{-1} g_1 \\ + & \beta_1 g_1 \alpha_{g_1^{-1}g_2} g_1^{-1} g_2 & + & \beta_2 g_2 \alpha_{g_2^{-1}g_2} g_2^{-1} g_2 & + & \ldots & + & \beta_n g_n \alpha_{g_n^{-1}g_2} g_n^{-1} g_2 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ + & \beta_1 g_1 \alpha_{g_1^{-1}g_n} g_1^{-1} g_n & + & \beta_2 g_2 \alpha_{g_2^{-1}g_n} g_2^{-1} g_n & + & \ldots & + & \beta_n g_n \alpha_{g_n^{-1}g_1} g_n^{-1} g_n \end{array}$$

which is:

$$\begin{array}{ccccccccccc} & \beta_1 \alpha_{g_1^{-1}g_1} g_1 & + & \beta_2 \alpha_{g_2^{-1}g_1} g_1 & + & \ldots & + & \beta_n \alpha_{g_n^{-1}g_1} g_1 \\ + & \beta_1 \alpha_{g_1^{-1}g_2} g_2 & + & \beta_2 \alpha_{g_2^{-1}g_2} g_2 & + & \ldots & + & \beta_n \alpha_{g_n^{-1}g_2} g_2 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ + & \beta_1 \alpha_{g_1^{-1}g_n} g_n & + & \beta_2 \alpha_{g_2^{-1}g_n} g_n & + & \ldots & + & \beta_n \alpha_{g_n^{-1}g_1} g_n \end{array}$$

and this is g_1 from the above. Thus $g_1^{-1} * u$ is the inverse of w and w is a unit in RG. □

Corollary 1. *If the inverse of an RG-matrix exists then this inverse is also an RG-matrix.*

Corollary 2. *When R is commutative, w is a unit in RG if and only if $\sigma(w)$ is a unit in $R_{n\times n}$ if and only if $\det(\sigma(w))$ is a unit in R.*

Corollary 3. *w is a zero divisor in RG if and only if $\sigma(w)$ is a zero divisor in $R_{n\times n}$.*

Proof. The proof of this is similar to the proof of Theorem 2. The only significant difference is that in equation (1) above, 0 should appear on the right hand side of the first row. In constructing our element u as in Theorem 2 note that if $B * \sigma(w) = 0$ for non-zero B then some row of B, which *a priori* is not necessarily the first row, is non-zero. Then b should be taken as this non-zero row and u is constructed from b.

Corollary 1. *When R is commutative and has no zero-divisors, w is a zero divisor in RG if and only if $\sigma(w)$ is a zero divisor in $R_{n\times n}$ if and only if $\det(\sigma(w)) = 0$.* □

Theorem 3. *When R is a field, $w \neq 0$ in RG is either a unit or else is a zero divisor, depending on whether $\det(\sigma(w)) \neq 0$ or $\det(\sigma(w)) = 0$.*

Proof. The proof of this is a direct result of Theorem 1 and Corollary 2 of Theorem 2. □

Theorem 4. *Let R be a field and G a finite group. Then $W = U(RG)$ satisfies the Tits' alternative, i.e. W is either soluble-by-finite or else contains a non-cyclic free group.*

Proof. From Theorem 1 and Theorem 2, W is a linear group, a subgroup of $GL(n, R)$, and hence satisfies the Tits' alternative by Tits' Original Theorem [5]. □

A corollary to this is the following theorem.

Theorem 5. *Let G be a locally finite group and R a field, then any finitely generated torsion group of $U(RG)$ is finite, i.e. the generalised Burnside problem has a positive answer for $U(RG)$.*

Note that if $R = \mathbb{Z}$, the integers, then $\det(\sigma(w)) = \pm 1, 0, \text{or } n$ where $|n| > 1$ so that three situations can occur here, the first corresponding to a unit, the second to a zero-divisor and in the third case w is neither a unit nor a zero-divisor.

3. Types

We now look at some types which occur for particular classes of groups. To work out the G-matrix proceed to list the elements of G, which form a listing for the columns, then write, or list, the inverses of these elements in order along a column outside the matrix and proceed to make the calculations in the matrix as indicated in the following:

	g_1	g_2	$\cdots$	g_n
g_1^{-1}	$g_1^{-1}g_1$	$g_1^{-1}g_2$	$\cdots$	$g_1^{-1}g_n$
g_2^{-1}	$g_2^{-1}g_1$	$g_2^{-1}g_2$	$\cdots$	$g_2^{-1}g_n$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
g_n^{-1}	$g_n^{-1}g_1$	$g_n^{-1}g_2$	$\cdots$	$g_n^{-1}g_n$

Once the G-matrix has been calculated an RG-matrix is obtained by substituting elements of R for the elements of G in the G-matrix.

3.1. Cyclic Case

Suppose $G = \{1, g, \ldots, g^{n-1}\}$ is the cyclic group of order n with n the least power such that $g^n = 1$. Then the matrix of G relative to this listing corresponds to a *circulant* matrix; if $w = \sum_{i=0}^{n-1} \alpha_i g^i \in RG$ then $M(RG, w)$ is the circulant matrix

$$\begin{pmatrix} \alpha_0 & \alpha_1 & \alpha_2 & \ldots & \alpha_{n-1} \\ \alpha_{n-1} & \alpha_0 & \alpha_1 & \ldots & \alpha_{n-2} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \alpha_1 & \alpha_2 & \alpha_3 & \ldots & \alpha_0 \end{pmatrix}.$$

Circulant matrices over fields, particularly over $\mathbb{C}$, have been studied in great detail and have applications in many areas. The Fourier matrix will diagonalise a circulant matrix and there is a formula for calculating its eigenvalues. The eigenvalues are given, as one might expect, in terms of n-th roots of unity. Circulant matrices are then again special types of *Toeplitz matrices*.

It is also known that Toeplitz matrices may be embedded in circulant matrices.

Generally when G is finite the G-matrix of a group G is a Toeplitz matrix if and only if G is cyclic and thus the matrix is circulant; see however the infinite case below.

The rich structure theory of group rings should prove useful.

3.2. Symmetric Case

It is easily checked that the matrix $M(G)$ of a group G is symmetric if and only if G has exponent 2 which happens if and only if G is elementary Abelian of exponent 2. G is then isomorphic to the vector space $\mathbb{Z}_2^n$ over the field $\mathbb{Z}_2$. Here it may be verified that the RG-matrices when G has order 2^n and rank n, are the *Walsh-Toeblitz matrices* - see [3] for example. Thus we have the next result.

Theorem 6. *The set of $2^n \times 2^n$ Walsh-Toeblitz matrices over R is isomorphic to the group ring RG of the elementary Abelian 2-group of rank n. The isomorphism is given as in Theorem 1.*

To see this we need a listing of the elements of the elementary Abelian 2-group G of rank n. Suppose G is generated by $\{a_1, a_2, \ldots, a_n\}$. Then list the elements of G by:

$$1, a_1, a_2, a_1 * a_2, a_3, a_1 * a_3, a_2 * a_3, a_1 * a_2 * a_3, a_4, a_1 * a_4, \ldots, a_1 * a_2 * \ldots * a_n.$$

In other words, list the elements of the elementary Abelian 2-group of rank $n-1$, call this list $L(n-1)$, introduce a new symbol a_n and add on (in order) $L(n-1) * a_n$ to the end of $L(n-1)$ to get $L(n)$.

Relative to this ordering we get the isomorphism between Walsh-Toeplitz $2^n \times 2^n$ matrices over R and RG. Walsh-Toeplitz matrices of size $2^n \times 2^n$ are defined as follows: Suppose A, B are $2^{n-1} \times 2^{n-1}$ Walsh-Toeplitz matrices. Then a $2^n \times 2^n$ Walsh-Toeplitz matrix is one of the form $\begin{pmatrix} A & B \\ B & A \end{pmatrix}$. The initial element a_0 appears on the diagonal. So for example an 8×8 Walsh-Toeplitz matrix is

$$\left(\begin{array}{cccc|cccc} a_0 & a_1 & a_2 & a_3 & b_0 & b_1 & b_2 & b_3 \\ a_1 & a_0 & a_3 & a_2 & b_1 & b_0 & b_3 & b_2 \\ a_2 & a_3 & a_0 & a_1 & b_2 & b_3 & b_0 & b_1 \\ a_3 & a_2 & a_1 & a_0 & b_3 & b_2 & b_1 & b_0 \\ \hline b_0 & b_1 & b_2 & b_3 & a_0 & a_1 & a_2 & a_3 \\ b_1 & b_0 & b_3 & b_2 & a_1 & a_0 & a_3 & a_2 \\ b_2 & b_3 & b_0 & b_1 & a_2 & a_3 & a_0 & a_1 \\ b_3 & b_2 & b_1 & b_0 & a_3 & a_2 & a_1 & a_0 \end{array}\right).$$

3.2.1. General p

When G is an elementary Abelian p-group we will also get an interesting isomorphism between RG and a set (ring) of $p^n \times p^n$ matrices over R. Thus define

an *elementary* $p^n \times p^n$*-matrix* as follows: An elementary $p \times p$-matrix is a $p \times p$ circulant matrix and an elementary $p^n \times p^n$-matrix, for $n \geq 2$, is one of the form $\begin{pmatrix} A & B \\ B & A \end{pmatrix}$, where A, B are elementary $p^{n-1} \times p^{n-1}$-matrices.

Thus:

Theorem 7. *The group ring over R of the elementary Abelian p-group of order p^n is isomorphic to the set of (and hence ring of) elementary $p^n \times p^n$-matrices.*

Proof. Apply Theorem 1 to the listing of G which is similar to the listing in the Walsh-Toeplitz case given above. Suppose $L(n-1)$ is the listing of the elementary p^{n-1} group. Introduce a new symbol a_n and then the listing of the elementary Abelian p^n group is $\{L(n-1)*a_n, L(n-1)*a_n^2, \ldots, L(n-1)*a_n^{p-1}\}$. Then it is easily checked that the RG-matrices corresponding to this listing are the elementary $p^n \times p^n$ matrices over R. □

Thus these elementary $p^n \times p^n$-matrices over R generalise Walsh-Toeplitz matrices, which is the case $p = 2$.

Notice also (see below) that the ring of matrices of the form $\begin{pmatrix} A & B \\ B & A \end{pmatrix}$ is isomorphic as a ring to the set of matrices of the form $\begin{pmatrix} A+B & 0 \\ 0 & A-B \end{pmatrix}$ when R is an integral domain not of characteristic 2.

3.3. Dihedral

The dihedral group D_{2n} of order $2n$ is given by $D_{2n} =< a, b : a^2, b^n, a*b = b^{-1}*a >$. There are a number of listings of the elements of D_{2n} but the following listing is the most convenient:

$D_{2n} = \{1, b, b^2, \ldots, b^{n-1}, a, ab, ab^2, \ldots, ab^{n-1}\}$. The inverse of ab^i is itself. Then the matrix of D_{2n} relative to this listing is:

$$\left[\begin{array}{ccccc|ccccc} 1 & b & b^2 & \ldots & b^{n-1} & a & ab & ab^2 & \ldots & ab^{n-1} \\ b^{n-1} & 1 & b & \ldots & b^{n-2} & ab & ab^2 & ab^3 & \ldots & a \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ b & b^2 & b^3 & \ldots & 1 & ab^{n-1} & a & ab & \ldots & ab^{n-2} \\ \hline a & ab & ab^2 & \ldots & ab^{n-1} & 1 & b & b^2 & \ldots & b^{n-1} \\ ab & ab^2 & ab^3 & \ldots & a & b^{n-1} & 1 & b & \ldots & b^{n-2} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ ab^{n-1} & a & ab & \ldots & ab^{n-2} & b & b^2 & b^3 & \ldots & 1 \end{array}\right].$$

Thus the set of matrices of the following form is isomorphic to the group ring of D_{2n}:

$$\left(\begin{array}{ccccc|ccccc} \alpha_0 & \alpha_1 & \alpha_2 & \dots & \alpha_{n-1} & \beta_0 & \beta_1 & \beta_2 & \dots & \beta_{n-1} \\ \alpha_{n-1} & \alpha_0 & \alpha_1 & \dots & \alpha_{n-2} & \beta_1 & \beta_2 & \beta_3 & \dots & \beta_0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \alpha_1 & \alpha_2 & \alpha_3 & \dots & \alpha_0 & \beta_{n-1} & \beta_0 & \beta_1 & \dots & \beta_{n-2} \\ \hline \beta_0 & \beta_1 & \beta_2 & \dots & \beta_{n-1} & \alpha_0 & \alpha_1 & \alpha_2 & \dots & \alpha_{n-1} \\ \beta_1 & \beta_2 & \beta_3 & \dots & \beta_{n-1} & \alpha_{n-1} & \alpha_0 & \alpha_1 & \dots & \alpha_{n-2} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \beta_{n-1} & \beta_0 & \beta_1 & \dots & \beta_{n-2} & \alpha_1 & \alpha_2 & \alpha_3 & \dots & \alpha_0 \end{array}\right).$$

These matrices have the form $\begin{pmatrix} A & B \\ B & A \end{pmatrix}$, where A is a *circulant matrix* and B is a *Hankel* matrix of a special form. A (general) Hankel matrix is one which is constant on any diagonal from upper right to lower left. These Hankel-type matrices have n parameters as opposed to the usual $2n-1$ parameters; the same parameters appear below the main diagonal as above in the same order. Call such a matrix B a *Hankel-type* or *reverse circulant* matrix.

Suppose R is an integral domain not of characteristic 2. If we let $P = \begin{pmatrix} I_n & I_n \\ I_n & -I_n \end{pmatrix}$ then clearly P is invertible in R or in the field of fractions of R and

$$\begin{pmatrix} I_n & I_n \\ I_n & -I_n \end{pmatrix} * \begin{pmatrix} A & B \\ B & A \end{pmatrix} = \begin{pmatrix} A+B & 0 \\ 0 & A-B \end{pmatrix} * \begin{pmatrix} I_n & I_n \\ I_n & -I_n \end{pmatrix},$$

and hence

$$P * \begin{pmatrix} A & B \\ B & A \end{pmatrix} * P^{-1} = \begin{pmatrix} A+B & 0 \\ 0 & A-B \end{pmatrix}.$$

This matrix P is independent of A and B. Thus the following theorem holds true.

Theorem 8. *The group ring of the dihedral group of order $2n$ is isomorphic to the ring of matrices of the form $\begin{pmatrix} A & B \\ B & A \end{pmatrix}$, where A is a circulant $n \times n$ matrix and B is an $n \times n$ Hankel-type-matrix.*

When R is an integral domain not of characteristic 2, this ring of matrices is isomorphic to the ring of matrices of the form $\begin{pmatrix} A+B & 0 \\ 0 & A-B \end{pmatrix}$ with A, B as stated above.

A matrix of this form is invertible if and only if $A+B$ and $A-B$ are invertible and this gives a classification of the units of the group ring of the dihedral group of order $2n$. Similarly we can classify the zero-divisors of the dihedral group.

Corollary. *If A is an $n \times n$ circulant matrix and B, B' are $n \times n$ Hankel-type then: (i) $B * B'$ is a circulant matrix, (ii) $A * B$ and $A * B'$ are Hankel-type matrices.*

Proof. Suppose A, A' are circulant matrices and B, B' are Hankel-type matrices. Then:

$$\begin{pmatrix} A & B \\ B & A \end{pmatrix} * \begin{pmatrix} A' & B' \\ B' & A' \end{pmatrix} = \begin{pmatrix} A*A'+B*B' & A*B'+B*A' \\ B*A'+A*B' & B*B'+A*A' \end{pmatrix}.$$

Since $A * A'$ is circulant it follows that $B * B'$ is circulant. By taking $A = I_n$ we get that $B * A'$ is Hankel-type and by taking $A' = I_n$ we get that $A * B'$ is Hankel-type. □

Hankel-type or reverse circulant matrices have similar relationship to Hankel matrices as circulant matrices have to Toeplitz matrices. In particular a Hankel $n \times n$ matrix may be embedded in a Hankel-type $(2n-1) \times (2n-1)$ matrix similar to the embedding of a Toeplitz $n \times n$ matrix into a $(2n-1) \times (2n-1)$ circulant matrices; this embedding does not seem to have appeared in the literature but a proof is similar to the Toeplitz matrix embedding into a circulant matrix.

Problems involving Toeplitz matrices have been tackled and solved using circulant matrices. This suggests that problems involving Hankel matrices should be tackled using Hankel-type matrices.

3.4. Abelian Groups

We have seen that the ring of circulant matrices is isomorphic to the group ring of a cyclic group. For finitely generated Abelian groups, the matrices which turn up are certain block-circulant matrices.

A finitely generated Abelian group is the direct product of cyclic groups. Given a sequence $S = (d_1, d_2, \ldots, d_r)$ of positive integers define a *S-block circulant matrix over R* as follows. If $S = (d_1)$ then an S-block circulant matrix is a circulant $d_1 \times d_1$ matrix over R. Suppose $r > 1$ and S-block circulant matrices have been defined for positive integers less than r. If then $S = (d_1, d_2, \ldots, d_r)$ an S-circulant block matrix over R is a $d_r \times d_r$ circulant matrix, A, say where each entry in A is a $(d_1, d_2, \ldots, d_{r-1})$-block circulant matrix.

Theorem 9. *The group ring over R of the direct product of cyclic groups of orders $d_1, d_2, \ldots, d_r$ is isomorphic to the set of S-block circulant matrices*

over R.

Proof. The proof is omitted but follows directly from Theorem 1. □

So for example the group ring RG of the group $C_2 \times C_4$ is isomorphic to the ring of matrices over R of the form:

$$\begin{pmatrix} A & B & C & D \\ D & A & B & C \\ C & D & A & B \\ B & C & D & A \end{pmatrix},$$

where A, B, C, D are 2×2 circulant matrices. This is also isomorphic, by a relisting of the elements of the group using $C_2 \times C_4 = C_4 \times C_2$, to the ring of matrices over R of the following form:

$$\begin{pmatrix} P & Q \\ Q & P \end{pmatrix},$$

where P, Q are 4×4 circulant matrices.

Since S-block circulant matrices over R are isomorphic to the group ring of an Abelian group over R, this immediately implies that the S-block circulant matrices commute when R is commutative.

Theorem 10. *The S-block circulant matrices over R commute and are normal when R is commutative.*

S-block circulant matrices have been studied in the literature for their applications when $r = 2$.

There are a number of ways of presenting an Abelian group as the direct product of cyclic groups, one of which is unique. Different isomorphic forms of the S-block circulant matrices may be obtained in this manner.

3.5. Applications

Toeblitz matrices, circulant matrices, Walsh-Toeblitz matrices, block circulant matrices all have been shown to have powerful applications in communications systems, signal processing, time series analysis and elsewhere. These occur as RG-matrices for cyclic, elementary Abelian 2-groups and Abelian groups. Hankel matrices turn up in the study of the group ring of the dihedral group and these also have many applications.

As already mentioned a Toeplitz $n \times n$ matrix may be embedded in a circulant $2n \times 2n$ matrix and the circulant matrices may be diagonalised by the

Fourier matrix. The method of embedding Toeplitz block matrices in block circulant matrices has also been used very effectively.

Thus RG-matrices are a generalisation of all these useful types of matrices and are worthy of some investigation for possible applications in the communications and other areas. Structure theorems for group rings should also prove useful.

3.6. Change the Listing

If A, B are RG-matrices and are obtained from the same group ring element of RG but possibly different listings then the the relationship between A and B is easy to obtain. Say two $n \times n$ matrices are *permutation equivalent* if and only if there exists an $n \times n$ permutation matrix P such that $PAP^t = B$. Then A and B are the RG-matrix of the same element $w \in RG$ relative to possibly different listings if and only if A is permutation equivalent to B. Notice that $P^t = P^{-1}$ for a permutation matrix. It is only necessary to show this is true for an interchange of two elements in the listing; this can be shown directly from the definition of RG-matrix.

4. Infinite

Let $G = \{g_1, g_2, \ldots, \}$ be a listing of the infinite group G. Then the infinite matrix $M(G)$ may be formed as follows:

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

Given a group ring element $w = \sum_{i=1}^{\infty} \alpha_{g_i} g_i \in RG$, where only a finite number of the coefficients are non-zero, consider the infinite RG-matrix of w denoted by $M(RG, w)$ and defined as follows:

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

This is an infinite matrix but only a finite number of the entries are non-zero in any row or column and it has a special form. As for the finite case an

isomorphism exists between a group ring of an infinite group G whose elements can be listed and the set of such infinite RG-matrices.

Theorem 11. *The group ring RG of an infinite group G whose elements can be listed is isomorphic to the RG-matrices over R.*

An RG-matrix here has only a finite number of elements in each row and column. Note that in any case multiplication is defined on infinite matrices with only a finite number of entries in each row and column.

Thus for example the infinite circulant matrices with only a finite number of entries in any row or column is isomorphic to the group ring of the direct product of an infinite number of copies of $\mathbb{Z}_2$.

A study of such matrices should give information on the units and zero divisors of group rings of infinite groups.

Infinite groups could be listed like $\{\ldots, g_{-2}, g_{-1}, g_0, g_1, g_2, g_3, \ldots\}$ and this can be a useful way for considering the corresponding group ring as rings of infinite matrices.

4.1. Infinite and Cyclic

Consider then the G-matrix of the infinite cyclic group G generated by g, where the listing of is given by $\{1, g, g^2, \ldots, g^{-1}, g^{-2}, \ldots\}$:

$$\begin{pmatrix} 1 & g & g^2 & g^3 & \ldots \\ g^{-1} & 1 & g & g^2 & \ldots \\ g^{-2} & g^{-1} & 1 & g & \ldots \\ \vdots & \vdots & \vdots & \vdots & \vdots \end{pmatrix}.$$

If we now consider the matrix corresponding the the group ring element $w = \sum_{i=0}^{\infty} \alpha_i g^i + \sum_{i=1}^{\infty} \alpha_{-i} g^{-i}$, where of course only a finite number of the coefficients are non-zero, we get the following matrix:

$$\begin{pmatrix} \alpha_0 & \alpha_1 & \alpha_2 & \alpha_3 & \ldots \\ \alpha_{-1} & \alpha_0 & \alpha_1 & \alpha_2 & \ldots \\ \alpha_{-2} & \alpha_{-1} & \alpha_0 & \alpha_1 & \ldots \\ \vdots & \vdots & \vdots & \vdots & \vdots \end{pmatrix}.$$

This gives an infinite Toeplitz matrix with only a finite number of entries on any row or column which corresponds to the group ring element w.

List the infinite cyclic group as $\{\ldots, g^{-3}, g^{-2}, g^{-1}, 1, g, g^2, g^3, \ldots\}$ and then it is seen that the its group ring is isomorphic to the infinite matrices of the following form, where only a finite number of non-zero entries occur in any row or column:

$$\begin{pmatrix} \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots \\ \ddots & \alpha_{-3} & \alpha_{-2} & \alpha_{-1} & \alpha_0 & \alpha_1 & \alpha_2 & \alpha_3 & \ddots & \ddots & \ddots \\ \ddots & \ddots & \alpha_{-3} & \alpha_{-2} & \alpha_{-1} & \alpha_0 & \alpha_1 & \alpha_2 & \alpha_3 & \ddots & \ddots \\ \ddots & \ddots & \ddots & \alpha_{-3} & \alpha_{-2} & \alpha_{-1} & \alpha_0 & \alpha_1 & \alpha_2 & \alpha_3 & \ddots \\ \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots \end{pmatrix}.$$

This is the infinite Toeplitz matrix as seen in signal processing.

4.2. Infinite Dihedral

We have seen that the group ring of a finite dihedral group is isomorphic to matrices of the form $\begin{pmatrix} A & B \\ B & A \end{pmatrix}$, where A is a circulant matrix and B is Hankel matrix of a special form. It can be verified that the group ring of the infinite dihedral group D_∞ is isomorphic to the set of infinite matrices of the form $\begin{pmatrix} A & B \\ B & A \end{pmatrix}$, where now A is an infinite Toeplitz matrix and B is an infinite Hankel matrix. Thus the group ring over R of the infinite dihedral group is isomorphic to the set of matrices over R of this form where only a finite number of elements appear in any row or column. When R is an integral domain not of characteristic 2 then, as with the finite, case given a matrix of the form $\begin{pmatrix} A & B \\ B & A \end{pmatrix}$ there exist an invertible matrix P independent of A, B so that:

$$P * \begin{pmatrix} A & B \\ B & A \end{pmatrix} * P^{-1} = \begin{pmatrix} A+B & 0 \\ 0 & A-B \end{pmatrix}.$$

Thus we have the next result.

Theorem 12. *The group ring of the infinite dihedral group is isomorphic to the ring of matrices of the form* $\begin{pmatrix} A & B \\ B & A \end{pmatrix}$, *where A is an infinite Toeplitz matrix and B is an infinite Hankel matrix (where it is assumed that only a finite number of entries in any row or column of the matrices are non-zero). When R is an integral domain not of characteristic 2 this ring of matrices is*

isomorphic to the ring of matrices of the form $\begin{pmatrix} A+B & 0 \\ 0 & A-B \end{pmatrix}$, *with* A, B *as stated.*

To get the isomorphism, use the following listing of D_∞:

$$\{\ldots, b^{-2}, b^{-1}, 1, b, b^2, \ldots \quad \ldots ab^{-2}, ab^{-1}, a, ab, ab^2, \ldots\}.$$

Note that $(ab^i)^{-1} = ab^i$. Now form the G-matrix and apply Theorem 9 to get the result.

References

[1] P.J. Davis, *Circulant Matrices*, Chelsea, New York, N.Y. (1994).

[2] César P. Milies, Sudarsan K. Sehgal, *An Introduction to Group Rings*, Kluver, Dordrecht-Boston-London (2002).

[3] Kent E. Morrison, Spectral approximation of multiplication operators, *New York J. Math.*, **1** (1995), 75-96.

[4] S.K. Sehgal, *Units in Integral Group Rings*, Longman, Essex (1993).

[5] J. Tits, Free subgroups in linear groups, *J. Algebra*, **20** (1972), 250-270.