JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

RELATION BETWEEN GROUP RINGS $R[G]$ AND RINGS OF MATRICES $M(R[G], w)$, $w \in R[G]$

Dr. Hiteshwar Singh
Ret. Assistant Professor
Dept. of Mathematics, M.L.S.M. College, Darbhanga

Dhananjay Kumar Mishra
Univ. Dept. of Mathematics, L.N.M.U. Darbhanga

Abstract

It is shown that the group ring $R[G]$ 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 as well as 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 is 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 $R[G]$ thus can be considered to be a generalization of these rings of matrices. These generalizations are used in communications, signal processes, time series analysis and elsewhere. When G is finite and R is a field, it follows from the representation that $U(R[G])$, the group of units of $R[G]$, satisfies the Tits' alternative and consequently the generalized Burnside problem has a positive answer for $U(R[G])$.

Keywords: group ring, rings of matrices, circulant matrices, Toeptitize matrices, Walsh-Toeplitz matrices, Hankel matrices, Tits alternative.

1. Introduction:

Let $R[G]$ 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 only if there exists a non-zero element $r \in W$ with $z \,.\, r = 0$. When W has an identity 1_W and 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 $R[G]$. In many cases we will assume that $R[G]$ itself has no zero divisors. Let $R_{n\times n}$ denoted the ring of $n \times n$ matrices with coefficients from R. Group rings and their units appear in many branches of mathematics. In this paper we establish an isomorphism between the group ring $R[G]$ and a ring of certain $n \times n$ matrices over R.

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 $R[G]$ 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 that over a finite field every element is either a unit or a zero-divisor. Using

this representation we can say that $U(R[G])$, the group of units of $R[G]$, satisfies the Tits alternative when R is a field and consequently the generalized Burnside problem has a positive answer for $U(R[G])$.

2. Some Rings of Matrices which Occur as Group Rings:

When G is the cyclic group of order n then $R[G]$-matrices turn out to be the circulant $n \times n$ matrices over R. (is a field of the complex numbers). 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 $R[G]$-matrices turn out to be what are termed Walsh-Toeblitz matrices over R [3]. In the case of the dihedral group the $R[G]$-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, $R[G]$ is isomorphic to certain block 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 [1], and this has proved useful in the study of Toeplitz matrices and their applications.

3. Infinite groups and matrices:

The set of infinite (infinite matrices have only a finite number of entries in any row or column). Toeplitz matrices over R is isomorphic to the group ring $R[G]$ of the infinite cyclic group G. The set of Walsh-Toeplitz infinite matrices over R is isomorphic to $R[G]$, where G is the direct product of an infinite number of copies of Z_2. When G is the infinite dihedral group then $R[G]$ 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.

4. Possible Applications of ring of matrices:

For each group ring $R[G]$ the set of $R[G]$-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.

5. How do we write a matrix of group *G* ?

Let us suppose that $\{g_1, g_2, \ldots, g_n\}$ be a fixed listing of the elements of group G. Now let us consider the following matrix:

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

We call this is the matrix of group G relative to this listing and we 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.

6. The Matrix Corresponding to a Group Ring Element:

Let us suppose that $w = \sum_{i=1}^{n} \alpha_{g_i} g_i \in R[G]$. We now form the $R[G]$-matrix of w which is denoted by $M(R[G], w)$ 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 $M(R[G], w)$ is in $R_{n\times n}$. Here we observe that the first column of $M(R[G], w)$ is 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 $R[G]$ then the coefficient of g_i in the product $b \,.\, w$ is (β_{g1}, β_{g2}, …, β_{gn}) times the i-th column of $M(R[G],w)$. It is given that a listing of the elements of G, form the matrix $M(G)$ of G relative to this listing. Then an $R[G]$-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 $R[G]$-matrix are equal (The matrix $M[G]$ of G is not the multiplication table of group G). We have given the entries of the first row of an $R[G]$-matrix, the entries of the other rows are determined from the matrix $M(G)$ of G; here each row and each column is a permutation of the first row determined by the matrix of G.

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

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

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

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

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

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

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

and this of course is $M(R[G], c) = \sigma\ (t \,.\, w)$ as required.

8. Theorem: Let us suppose that R has an identity. Then $w \in R[G]$ is a unit in $R[G]$ if and only if $\sigma(w)$ is a unit in $R_{n\times n}$.

Proof. We suppose that w is a unit in $R[G]$ and u is its inverse. Then $u \,.w =$

$1_{R[G]}$ and hence $\sigma\ (u \,.\, w) = \sigma\ (1_{R[G]}) = I_n$, 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 $R_{n\times n}$.

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

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

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

We do not know theoretically that B is a $R[G]$-matrix. Let us suppose that $b = (\beta_1, \beta_2, \ldots\ \beta_n)$ be the first row of B. Then:

$$\begin{array}{ccccccccc} \beta_1\alpha_{g_1}^{-1}g_1 & + & \beta_2\alpha_{g_{21}}^{-1}g_1 & + & \cdots & + & \beta_n\alpha_{g_{n1}}^{-1}g_1 & = & 1 \\ \beta_1\alpha_{g_2}^{-1}g_2 & + & \beta_2\alpha_{g_2}^{-1}g_2 & + & \cdots & + & \beta_n\alpha_{g_n}^{-1}g_2 & = & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \beta_1\alpha_{g_n}^{-1}g_n & + & \beta_2\alpha_{g_2}^{-1}g_n & + & \cdots & + & \beta_n\alpha_{g_n}^{-1}g_n & = & 0 \end{array} \qquad (1)$$

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

We choose which $u = \beta_1 g_1 + \beta_2 g_2 + \ldots + \beta_n g_n$. Then:

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

$$+ \beta_i\, \alpha_{g_i}^{-1} g_2 g_2 + \ldots + \beta_i\, \alpha_{g_i}^{-1} g_n g_n$$

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:

$$
\begin{array}{ccccccccc}
+ & \beta_1 g_1 \alpha^{-1}_{g_1 g_1} g_1^{-1} g_1 & + & \beta_2 g_2 \alpha^{-1}_{g_2 g_1} g_2^{-1} g_1 & + & \cdots & + & \beta_n g_n \alpha^{-1}_{g_n g_1} g_n^{-1} g_1 \\
+ & \beta_1 g_1 \alpha^{-1}_{g_1 g_2} g_1^{-1} g_2 & + & \beta_2 g_2 \alpha^{-1}_{g_2 g_2} g_2^{-1} g_2 & + & \cdots & + & \beta_n g_n \alpha^{-1}_{g_n g_2} g_n^{-1} g_2 \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
+ & \beta_1 g_1 \alpha^{-1}_{g_1 g_n} g_1^{-1} g_n & + & \beta_2 g_2 \alpha^{-1}_{g_2 g_n} g_2^{-1} g_n & + & \cdots & + & \beta_n g_n \alpha^{-1}_{g_n g_n} g_n^{-1} g_n
\end{array}
$$

Which is:

$$
\begin{array}{ccccccccc}
+ & \beta_1 \alpha^{-1}_{g_1 g_1} g_1 & + & \beta_2 \alpha^{-1}_{g_2 g_1} g_1 & + & \cdots & + & \beta_n \alpha^{-1}_{g_n g_1} g_1 \\
+ & \beta_1 \alpha^{-1}_{g_1 g_2} g_2 & + & \beta_2 \alpha^{-1}_{g_2 g_2} g_2 & + & \cdots & + & \beta_n \alpha^{-1}_{g_n g_2} g_2 \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
+ & \beta_1 \alpha^{-1}_{g_1 g_n} g_n & + & \beta_2 \alpha^{-1}_{g_2 g_n} g_n & + & \cdots & + & \beta_n \alpha^{-1}_{g_n g_n} g_n
\end{array}
$$

and this is g_1 from the above. Thus g_1^{-1}. u is the inverse of w and w is a unit in $R[G]$.

9. Corollary: If the inverse of an $R[G]$-matrix exists then this inverse is also an $R[G]$-matrix.

10. Corollary: When R is commutative, w is a unit in $R[G]$ 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.

11. Corollary: w is a zero divisor in $R[G]$ 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 8. 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 8 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.

12. Corollary: When R is commutative and has no zero-divisors, w is a zero- divisor in $R[G]$ if and only if $\sigma(w)$ is a zero-divisor in $R_{n\times n}$ if and only if det ($\sigma(w)$) = 0.

13. Theorem: When R is a field, $w \neq 0$ in $R[G]$ 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 theorem will be obtained from the result of theorem 7 and Corollary 10 of theorem 8.

14. Theorem: Let us suppose that R be a field and G be a finite group. Then $W = U(R[G])$ satisfies the Tits alternative, i.e. W is either soluble-by-finite or else contains a non-cyclic free group.

Proof. From Theorem 7 and Theorem 8, 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.

15.Theorem: Let G be a locally finite group and R a field, then any finitely generated torsion group of $U(R[G])$ is finite, i.e. the generalized Burnside problem has a positive answer for $U(R[G])$. Note that if $R = Z$, the integers, then det($\sigma(w)$) = ±1, 0, 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.

References

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

[2] C´esar 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.

[6] D.S. Passman, The Algebraic Structure of Group Rings. Dover Publication, Inc., Mineola, New York, 2011.