BULL. AUSTRAL. MATH. SOC. 16A20, 20C05
VOL. 12 (1975), 293-299.

A primitive group ring

Warren Brisley and R. Groenhout

An explicit construction is given for a primitive group ring, together with an explicit construction of a faithful irreducible module for it.

Until Formanek and Snider established sufficient conditions [1] for a group to generate a primitive group ring, there were some doubts about the existence of such objects. Their proof of primitivity uses the "internal" characterisation of primitivity in terms of the existence of a certain maximal one-sided ideal. By contrast, it seems worthwhile to construct a particularly easily-described group ring, together with an explicit faithful irreducible module for it; this provides an actual example, in which the primitivity is displayed in its "external" characterisation.

1. The group

Let Σ be the group of permutations, on the non-negative integers N, generated by $\{\sigma_0, \sigma_1, \sigma_2, \ldots\}$, where σ_i is defined by:

$(n\sigma_i)$ is the number obtained from n by changing the digit for 2^i in the binary representation of n.

(Thus, σ_0 interchanges each even integer with its successor, σ_1 permutes N to $2, 3, 0, 1, 6, 7, 4, 5, \ldots$, and in general, σ_k interchanges (rigidly) blocks of length 2^k.) Clearly Σ is singly transitive, any element of Σ is specified completely by its action on

Received 6 December 1974. The authors thank R.W. Robinson for the encouragement to believe that a set like S could be chosen in an easily-described manner.

https://doi.org/10.1017/S0004972700023893 Published online by Cambridge University Press

0 , and Σ is isomorphic to $C_2 \times C_2 \times C_2 \times \ldots$.

Let A be another copy of $C_2 \times C_2 \times C_2 \times \ldots$ generated by commuting involutions $\{a_0, a_1, a_2, \ldots\}$ and split-extend A by Σ using the automorphisms $\sigma_j : a_i \rightsquigarrow a_k$ where $k = (i\sigma_j)$. The result is the group $G = \langle \{a_0, a_1, a_2, \ldots\} \cup \{x_0, x_1, x_2, \ldots\} \rangle$ with the relations

(i) all x_i are of order 2 and commute pairwise,

(ii) all a_i are of order 2 and commute pairwise,

(iii) for each i, j pair, $x_j a_i x_j = a_k$ where $k = (i\sigma_j)$.

By the transitivity of Σ , G is generated by $\{a_0\} \cup \{x_0, x_1, x_2, \ldots\}$. Further, by the block action of elements of Σ , G is locally finite; and by the transitivity of Σ , any normal subgroup of G must be infinite. (As an aid to calculation, note that any element of G can be written as ax , with $a \in A$, $x \in X$, where X is generated by $\{x_0, x_1, x_2, \ldots\}$.)

2. The group ring

Let F be any field: the group ring $F(G)$ consists of elements (formal sums) of the form $\left(\sum_i \alpha_i g_i\right)$ with $\alpha_i \in F$, $g_i \in G$; addition and multiplication are defined in the natural way, using the multiplication in G and collecting terms.

In this particular case, we require that F not have characteristic 2 . We note that for this particular group ring, any element r of $F(G)$ can be written

$$r = A_1X_1 + A_2X_2 + \ldots + A_kX_k$$

where

(i) each X_i is an element of X , and all the X_i are different,

(ii) each A_i is an element of $F(A)$, and so it can be written (with e the unit element of G):

$$A_i = \beta e + \beta_0 a_0 + \beta_1 a_1 + \beta_{01} a_0 a_1 + \ldots + \beta_{01\ldots n} a_0 a_1 \ldots a_n$$

where there are 2^{n+1} terms for some n . (Some, but not all, of the β's may well be zero: each β is in F .)

3. The module

Let V be the vector space over F with basis (independent) elements $\{b_0, b_1, b_2, \ldots\}$: that is, V consists of finite formal sums $\sum \alpha_i b_i$, with the α_i in F . We need only define the action of G on V (in fact, on the basis elements) in such a way as to make V into a G-module, and then V will be an $F(G)$-module in the natural way.

Assuming the existence of a certain set

$$S = \{2, 5, 6, 7, 12, \ldots\}$$

(whose existence, construction and use we will deal with later), we specify:

$$b_i x_j = b_k \quad \text{where} \quad k = (i\sigma_j) \ ,$$

$$b_i a_0 = \varepsilon_i b_i \quad \text{where} \quad \varepsilon_i = -1 \ \text{ if } \ i \in S \ ,$$

$$\varepsilon_i = +1 \ \text{ if } \ i \notin S \ .$$

This specification extends associatively to words in the generators of G , and we obtain V as a G-module if the relations in G are satisfied. Clearly the requirements of order and commutativity are satisfied: for the other relations, we note that elements of Σ are uniquely specified by their action on 0 , so if x_j interchanges r and n , and X_r interchanges 0 and r then $x_j X_r$ is precisely the element which interchanges 0 and n . Thus $b_i(x_j a_r x_j)$ is $b_i(x_j X_r a_0 X_r x_j)$, which is $b_i((x_j X_r) a_0 (x_j X_r))$, which is $b_i a_n$. In either case, the result is $\varepsilon_t b_i$, where $x_j X_r$ interchanges i and t .

V is now an $F(G)$-module in the natural way.

4. Faithfulness and irreducibility

The set S is selected using the following array:

$$\begin{array}{cccccccccccc} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & \ldots \\ 1 & 0 & 3 & 2 & 5 & 4 & 7 & 6 & 9 & 8 & \ldots \\ 2 & 3 & 0 & 1 & 6 & 7 & 4 & 5 & 10 & 11 & \ldots \\ 3 & 2 & 1 & 0 & 7 & 6 & 5 & 4 & 11 & 10 & \ldots . \\ . & . & . & . & . & . & . & . & . & . & \\ . & . & . & . & . & . & . & . & . & . & \end{array}$$

where the entry e_{ij} in row i, column j is $j\sigma$, where σ is that unique element of Σ which interchanges 0 and i. (The rows and columns are numbered from zero.) Clearly, if $e_{ij} = n$, then the action of a_i on b_j is given by:

$b_j a_i = -b_j$ if and only if $b_n a_0 = (-b_n)$, that is if $n \in S$,

$b_j a_i = +b_j$ if and only if n is not in S.

The array is symmetric, since by the definition of Σ, e_{ij} is calculated from j using the difference between the binary expression of zero and that of i; this is equivalent to using the non-zero binary digits of j to mark which of the binary digits of i to change; thus $e_{ij} = e_{ji}$.

We now need a lemma:

LEMMA. *The set* S *can be chosen in such a way that, given* $n \geq 0$, *the set of part-columns of length* $n + 1$ *:*

$$\left\{ \begin{bmatrix} e_{0j} \\ e_{1j} \\ \vdots \\ e_{nj} \end{bmatrix}, \; j = 0, 1, 2, \ldots \right\}$$

contains at least one of each of the 2^{n+1} *possible patterns of* $+, -$ *produced by the* ε_k, *where* $k = e_{ij}$.

(Thus, with S as mentioned in the previous section, and with

$n = 1$, we have the pattern

$$\left.\begin{aligned} b_0a_0 &= +b_0 \\ b_0a_1 &= +b_1 \end{aligned}\right\} \quad \left.\begin{aligned} b_2a_0 &= -b_2 \\ b_2a_1 &= +b_2 \end{aligned}\right\} \quad \left.\begin{aligned} b_4a_0 &= +b_4 \\ b_4a_1 &= -b_4 \end{aligned}\right\} \quad \left.\begin{aligned} b_6a_0 &= -b_6 \\ b_6a_1 &= -b_6 \end{aligned}\right\}$$

corresponding to columns $j = 0, 2, 4, 6$, and rows 0 and 1 for a_0 and a_1 acting on those b_j : for example, $b_4a_1 = -b_4$ since $e_{14} \in S$.)

Leaving the algorithm to produce S until later, we now have:

(i) V is a faithful $F(G)$-module.

Proof. Take any r in $F(G)$, and assume $Vr = 0$. Write r as in Section 2. Then

$$b_jr = b_jA_1X_1 + b_jA_2X_2 + \ldots + b_jA_kX_k = 0 \text{ for each } j .$$

This reads:

$$\alpha_{1,j}b_jX_1 + \alpha_{2,j}b_jX_2 + \ldots + \alpha_{k,j}b_jX_k = 0 ,$$

where the $\alpha_{i,j}$ are in F . Since the $X_1, \ldots, X_k$ are all different, so too are the $b_jX_1, \ldots, b_jX_k$, by the properties of Σ . Hence each $\alpha_{i,j}$ is zero. Now any $\alpha_{i,j}$ is produced from A_i $(b_jA_i = \alpha_{i,j}b_j)$ by

$$A_i = \beta e + \beta_0a_0 + \beta_1a_1 + \ldots + \beta_{01\ldots n}a_0a_1 \ldots a_n$$

for some n . Then

$$\alpha_{i,j} = \beta \pm \beta_0 \pm \beta_1 \pm \ldots \pm \beta_{01\ldots n}$$

where the $\pm$ signs depend on the allotment of the ε_k . Since *each* of the 2^{n+1} patterns of $\pm$ which could be produced by the action of the a_i , may be achieved by the use of *some* b_j , by the lemma, we have the 2^{n+1} equations

https://doi.org/10.1017/S0004972700023893 Published online by Cambridge University Press

$$M\begin{bmatrix} \beta \\ \beta_0 \\ \vdots \\ \beta_{01\ldots n} \end{bmatrix} = 0$$

where the coefficient matrix M has mutually orthogonal rows. (Indeed, this production of possible $\pm$ patterns - setting $a_0 = \pm 1$, $a_1 = \pm 1$, ... in the monic words built from $1, a_0, a_1, \ldots, a_n$, is one of the standard ways of producing a Hadamard matrix of side 2^{n+1}.) Thus, each of the β's is zero, and A_i is the zero of $F(A)$ for each i. Hence r is zero. The module is faithful.

(ii) V is an irreducible $F(G)$-module.

Proof. Take any element $v = \sum_{i=0}^{n} \alpha_i b_i$ in V, in which not all the α_i are zero - say $\alpha_k \neq 0$. Then, by the lemma, and the symmetry of the array, there is an a_r such that

$$b_j a_r = \begin{cases} -b_k & \text{for } j = k , \\ +b_j & \text{for } 0 \le j \le n \text{ but } j \neq k . \end{cases}$$

So $v\{e-a_r\} = 2\alpha_k b_k$, so $vF(G)$ contains b_k, and since by the action of Σ, $b_k F(G)$ contains all basic elements of V, we have $vF(G) = V$ and hence V is irreducible.

It only remains to describe the algorithm to produce S and hence establish the lemma. We note first that if $q = 2^k$, $k > 0$, and $2^m > q$, then the blocks along the top row of the array

$$(2^m, \ldots, 2^m+q-1), \ (2^m+q, \ldots, 2^m+2q-1), \ (2^m+2q, \ldots), \ldots$$

are "reflected", in the sense that the first q elements in the *columns* headed 2^m; 2^m+q; 2^m+2q; ... are just these blocks, in the same internal order. This follows since the permutations sending

https://doi.org/10.1017/S0004972700023893 Published online by Cambridge University Press

0 to 1, 0 to 2, ..., 0 to 2^k-1 cannot change the binary digits past the $2^{(k-1)}$-digit. We start by flagging 2, 4, 5, 6, 7 as members of S : this deals with $n = 0, 1$ and we have reached 7 as last flagged integer.

Assume we have flagged sufficient to justify the lemma for $n = 0, 1, 2, \ldots, 2^{k-1}-1$, and that the last flag was placed at r . Set $q = 2^k$. (To start, $k = 2$, $r = 7$.)

(*) Find the next power of 2 , say 2^m , such that $2^m > r$ and $2^m > q$. Then allot flags within the next 2^q blocks of length q ,

$$\left(2^m, 2^m+1, \ldots, 2^m+q-1\right), \left(2^m+q, \ldots, 2^m+2q-1\right), \ldots$$

to produce one of each of the possible 2^q patterns of flagging. This could be done in "dictionary" order, the first block totally unflagged, the last one totally flagged. We have now provided the ε_n for $n = 0, 1, 2, \ldots, 2^k-1$. Set r to the last integer flagged, set $q = 2^{k+1}$, and return to (*). As noted in Section 3, this produces the set:

$$S = \{2, 5, 6, 7, 12, 17, 22, 27, 28, 29, \ldots\} ,$$

and, in fact, the algorithm produces a plethora of columns of each required type for each n , and so the lemma is justified.

Consequently the irreducibility and fidelity of the module is established.

Reference

[1] Edward Formanek and Robert L. Snider, "Primitive group rings", *Proc. Amer. Math. Soc.* 36 (1972), 357-360.

Department of Mathematics,
University of Newcastle,
Newcastle, New South Wales.