

THE CHARACTERS AND STRUCTURE OF A CLASS OF MODULAR REPRESENTATION ALGEBRAS OF CYCLIC p -GROUPS

J. C. RENAUD

(Received 28 July 1977; revised 28 February 1978)

Communicated by M. F. Newman

Abstract

Let $\mathcal{A}_{p,m}^*$ be the modular representation algebra of the cyclic group of order p^m over the prime field Z_p . The characters of $\mathcal{A}_{p,m}^*$ are derived. For $p = 2$, this provides an alternative proof of a result due to Carlson (1975), that $\mathcal{A}_{2,m}^*$ is a local ring. It is shown that for $p > 2$, $\mathcal{A}_{p,m}^*$ is a direct sum of 2^m local rings. Their dimensions and primitive idempotents are derived.

Subject classification (Amer. Math. Soc. (MOS) 1970): 20 C 20, 12 C 05, 12 C 30, 33 A 65.

1. Introduction

Let G be a cyclic group of order p^m , where p is a prime. Let Z_p be the residue field of integers modulo p . Let V_i be the isomorphism class of indecomposable (Z_p, G) -modules of dimension i .

For $0 \leq k \leq m$, the elements of the set $\{V_i, i = 1, \dots, p^k\}$ form a basis for an algebra $\mathcal{A}_{p,k}^*$ over Z_p . Products in the algebra are defined by

$$V_i \times V_j = \sum_{l=1}^{p^k} a_{ijl} V_l,$$

where a_{ijl} is the number (reduced modulo p) of terms of Z_p -dimension l in the decomposition of $M_i \otimes_{Z_p} M_j$ into the direct sum of indecomposable modules, M_i and M_j being modules in V_i and V_j respectively.

A character of $\mathcal{A}_{p,k}^*$ is a non-trivial algebra homomorphism from $\mathcal{A}_{p,k}^*$ to Z_p . By examining these characters in the case $p = 2$ it is shown that $\mathcal{A}_{2,m}^*$ is a local ring, proved by Carlson (1975). For $p > 2$ it is shown that $\mathcal{A}_{p,m}^*$ has 2^m distinct characters and hence is isomorphic to a direct sum of 2^m local rings. Their idempotents and dimensions are derived.

A major part of this work is based on formulae due to Green (1962), extended by the author (1977). The technique of using Chebyshev polynomials to derive the characters can be used as an alternative method to that of Green in Section 2 of his paper.

NOTATION. When a product decomposition formula is used, the expression $(\text{mod } p)$ means the coefficients are to be regarded as elements of Z_p . Similarly, the expression $\text{res}_p(r)$ means the residue of r , modulo p .

2. The structure of $\mathcal{A}_{2,m}^*$

THEOREM 1. *There exists exactly one character of $\mathcal{A}_{2,m}^*$, and this is defined by*

$$\varphi^m(V_r) = \text{res}_2(r), \quad 1 \leq r \leq 2^m.$$

PROOF. (All references are to Green, 1962.) $V_1 \times V_1 = V_1$, and by (2.7d), $V_2 \times V_2 = 0$. Hence there exists only one character of $\mathcal{A}_{2,1}^*$, defined by

$$\varphi^1(V_1) = 1, \quad \varphi^1(V_2) = 0.$$

Let θ be any character of $\mathcal{A}_{2,k}^*$, $1 < k \leq m$. Let $q = 2^{k-1}$. By (2.7d),

$$V_q \times V_q = V_{2q} \times V_{2q} = 0.$$

Hence $\theta(V_q) = \theta(V_{2q}) = 0$. By (2.8e), $V_{q+1} \times V_{q+1} = V_1$, and hence $\theta(V_{q+1}) = 1$. By (2.8c), for $1 \leq r_1 \leq q$,

$$V_{r_1} \times V_{q+1} \equiv V_{q+r_1} + (r_1 - 1)V_q \pmod{2}$$

and hence $\theta(V_{q+r_1}) = \theta(V_{r_1})$.

Now any character of $\mathcal{A}_{2,k}^*$ is entirely defined by a character of $\mathcal{A}_{2,k-1}^*$: the theorem follows by induction on k .

COROLLARY. (Carlson, 1975.) $\mathcal{A}_{2,m}^*$ is a local ring.

3. Preliminary formulae

The Chebyshev polynomial S_n , with integral coefficients, is as defined in Abramovitz and Stegun (1972), Section 22.7: for x indeterminate,

$$S_0(x) = 1, \quad S_1(x) = x, \quad S_n(x) = xS_{n-1}(x) - S_{n-2}(x).$$

The polynomials A_n and F_n are defined by

$$A_0(x) = 1, \quad A_1(x) = x - 1, \quad A_n(x) = (x - 1)A_{n-1}(x) - A_{n-2}(x),$$

$$F_0(x) = 1, \quad F_1(x) = x, \quad F_n(x) = (x - 1)F_{n-1}(x) - F_{n-2}(x).$$

These definitions may be extended to

$$S_{-1}(x) = A_{-1}(x) = 0.$$

Induction on n now gives

- (1) $A_n(x) = S_n(x_{-1})$ ($n \geq -1$),
- (2) $F_n(x) = A_n(x) + A_{n-1}(x)$ ($n \geq 0$).

Using the results in (2) and (8) of the formulae section of Snyder (1966) it is easy to show that

- (3) $F_n(x) = S_{2n}((x+1)^{\frac{1}{2}})$ ($n \geq 0$).

By Section 22.7 in Abramovitz and Stegun and the above sections in Snyder, together with equations (1)–(3) above, the following factorizations are straightforward exercises:

- (4) $F_{2n}(x) + 1 = F_n(x) [F_n(x) - F_{n-1}(x)]$ ($n \geq 1$),
- (5) $F_{2n-1}(x) + x = F_n(x) [F_{n-1}(x) - F_{n-2}(x)]$ ($n \geq 2$),
- (6) $F_{2n}(x) - 1 = A_{n-1}(x) [F_{n+1}(x) - F_{n-1}(x)]$ ($n \geq 1$),
- (7) $F_{2n-1}(x) - x = A_{n-2}(x) [F_{n+1}(x) - F_{n-1}(x)]$ ($n \geq 1$).

A further factorization is possible:

- (8) $F_{n+1}(x) - F_{n-1}(x) = (-1)^n(x+1)F_n(2-x)$ ($n \geq 1$).

(Direct calculation shows (8) holds at $n = 1, n = 2$: induction on n yields the general result.)

Let $x \in \mathbb{Z}_p, p > 2$. Henceforth all polynomials have their coefficients in \mathbb{Z}_p . In Section 4, the solutions (over \mathbb{Z}_p) of the following pairs of simultaneous equations are required:

- (a) $F_{p-1}(x) + 1 = 0, F_{p-2}(x) + x = 0,$
- (b) $F_{p-1}(x) - 1 = 0, F_{p-2}(x) - x = 0.$

For $p = 3$, equations (a) have the solution $x = 0$, while for (b), $x = 2$. For $p > 3$, on setting $p = 2n + 1$ and applying equations (4)–(8) above, the equations reduce to

- (a') $F_n(x) = 0,$
- (b') $(x+1)F_n(2-x) = 0$

provided only that:

- (i) $[F_n(x) - F_{n-1}(x)]$ and $[F_{n-1}(x) - F_{n-2}(x)]$ cannot be simultaneously zero, and
- (ii) $A_{n-1}(x)$ and $A_{n-2}(x)$ cannot be simultaneously zero. These provisos are immediate from the definitions of F_n and A_n , using descending induction on the subscripts to reach a contradiction.

It remains to find the solutions to equations (a') and (b') above. Two lemmas are required:

LEMMA 1

$$S_{p-1}(x) \equiv (x^2 - 4)^n \pmod{p} \quad (p = 2n + 1).$$

PROOF. Snyder (1966) gives the result

$$S_{2n}(x) = \sum_{r=0}^n (-1)^r \binom{2n-r}{r} x^{2n-2r}$$

Hence on expansion of $(x^2 - 4)^n$ it is sufficient to show that

$$4^r \binom{n}{r} \equiv \binom{2n-2r}{r} \pmod{p}, \quad 0 \leq r \leq n, \quad \text{where } p = 2n + 1.$$

This is an elementary though tedious exercise and is omitted here.

LEMMA 2

$$F_n(x) \equiv (x-3)^n \pmod{p} \quad (p = 2n + 1).$$

PROOF. Apply equations (1) and (3) and Lemma 1.

COROLLARIES.

- (i) $S_{p-1}(x) = 0$ implies $x = 2$ or $x \equiv -2 \pmod{p}$.
- (ii) The solution to (a') is $x \equiv 3 \pmod{p}$.
- (iii) The solution to (b') is $x \equiv -1 \pmod{p}$.

Three further results are required in Section 4:

LEMMA 3. For $r \geq -1$, $S_r(2) \equiv r + 1 \pmod{p}$.

PROOF. Apply induction on r using the definition of S_r .

LEMMA 4. For $a \geq 0$, $F_a(-1) \equiv (-1)^a \pmod{p}$.

PROOF. Apply 22.4.5 in Abramovitz and Stegun to equation (3) above.

LEMMA 5. For $a \geq 0$, $F_a(3) \equiv 2a + 1 \pmod{p}$.

PROOF. Apply equations (1) and (3) and Lemma 3.

4. The characters of $\mathcal{A}_{p,m}^*$

In this section, we assume that $p > 2$. It is shown that $\mathcal{A}_{p,m}^*$ has exactly 2^m distinct characters: these are expressed in terms of the 2^{m-1} characters of $\mathcal{A}_{p,m-1}^*$, $m \geq 2$.

We first derive the characters of $\mathcal{A}_{p,1}^*$:

THEOREM 2. There exist exactly two characters of $\mathcal{A}_{p,1}^*$, and these are defined by

$$\varphi_0^1(V_r) = \text{res}_p((-1)^{r-1} r),$$

$$\varphi_1^1(V_r) = \text{res}_p(r)$$

for $1 \leq r \leq p$.

PROOF. By Green (1962) or Renaud (1977), products in $\mathcal{A}_{p,1}^*$ are determined by

$$V_1 \times V_r = V_r \quad (1 \leq r \leq p),$$

$$V_2 \times V_r = V_{r-1} + V_{r+1} \quad (1 \leq r < p)$$

and

$$V_r \times V_p \equiv rV_p \pmod{p} \quad (1 \leq r \leq p).$$

Let θ be any character of $\mathcal{A}_{p,1}^*$. Now $\theta(V_1) = 1$, and since $V_p \times V_p = 0$, $\theta(V_p) = 0$. Let $\theta(V_2) = x$. Then for $2 \leq r \leq p$, $\theta(V_r) = x\theta(V_{r-1}) - \theta(V_{r-2})$: that is,

$$\theta(V_r) = S_{r-1}(x), S_n$$

as defined in Section 3 above.

The permissible values of x are now the solutions of $S_{p-1}(x) = 0$: by Lemma 1, these are $x = 2$ or $x \equiv -2 \pmod{p}$. By Lemma 3, the first value gives ϕ_1^1 , while since $S_n(-x) = (-1)^n S_n(x)$ by 22.4.5 in Abramovitz and Stegun, the second value gives ϕ_0^1 .

For $k > 1$, we now derive the characters of $\mathcal{A}_{p,k}^*$ in terms of those of $\mathcal{A}_{p,k-1}^*$. Let $r = r_0q + r_1$, $1 \leq r < p^k$, $q = p^{k-1}$, $0 \leq r_1 < q$. Let ϕ_i^{k-1} , $i = 0, \dots, 2^{k-1} - 1$, be the characters of $\mathcal{A}_{p,k-1}^*$.

THEOREM 3. *The characters of $\mathcal{A}_{p,k}^*$ are defined by*

$$\phi_i^k(V_r) = (-1)^{r_0} \phi_i^{k-1}(V_{r_1}) \quad (0 \leq i < 2^{k-2}),$$

$$\phi_i^k(V_r) = (-1)^{r_0} (2r_0 + 1) \phi_i^{k-1}(V_{r_1}) \quad (2^{k-2} \leq i < 2^{k-1}),$$

$$\phi_i^k(V_r) = (2r_0 + 1) \phi_{i-2^{k-1}}^{k-1}(V_{r_1}) \quad (2^{k-1} \leq i < 2^{k-1} + 2^{k-2})$$

and

$$\phi_i^k(V_r) = \phi_{i-2^k-1}^{k-1}(V_{r_1}) \quad (2^{k-1} + 2^{k-2} \leq i < 2^k).$$

PROOF. (References are to Green, 1962.) Let θ be any character of $\mathcal{A}_{p,k}^*$. By (2.7d), $\theta(V_q) = \theta(V_{pq}) = 0$. By (2.5b), $V_{q-1} \times V_{q-1} \equiv V_1 + (q-2)V_q \pmod{p}$ and hence $\theta(V_{q-1}) = 1$ or -1 . Let $\theta(V_{q+1}) = x$. By (2.9c), for $1 < a \leq p$,

$$V_{q-1} \times V_{(a-1)q+1} \equiv V_{aq-1} + (q-2)V_{(a-1)q} \pmod{p}.$$

By (2.8d), for $2 \leq a < p$,

$$V_{q+1} \times V_{(a-1)q+1} \equiv V_{(a-2)q+1} + (q-2)V_{(a-1)q} + V_{aq-1} + V_{aq+1} \pmod{p}.$$

CASE 1. $\theta(V_{q-1}) = 1$.

Now $\theta(V_{aq-1}) = \theta(V_{(a-1)q+1})$, $1 \leq a \leq p$. Hence

$$\theta(V_{aq+1}) = (x-1)\theta(V_{(a-1)q+1}) - \theta(V_{(a-2)q+1}), \quad 2 \leq a < p,$$

and so $\theta(V_{aq+1}) = F_a(x)$, $0 \leq a < p$.

CASE 2. $\theta(V_{q-1}) = -1$.

The same reasoning as in Case 1 gives

$$\theta(V_{aq+1}) = -F_a(-x), \quad 0 \leq a < p.$$

By (2.5b), $V_{pq-1} \times V_{pq-1} \equiv V_1 - 2V_{pq} \pmod{p}$, and hence $\theta(V_{pq-1}) = 1$ or -1 . Combining all possibilities, four situations arise:

- (i) $\theta(V_{q-1}) = 1, F_{p-1}(x) = 1, F_{p-2}(x) = x,$
- (ii) $\theta(V_{q-1}) = 1, F_{p-1}(x) = -1, F_{p-2}(x) = -x,$
- (iii) $\theta(V_{q-1}) = -1, F_{p-1}(-x) = -1, F_{p-2}(-x) = x$

and

- (iv) $\theta(V_{q-1}) = -1, F_{p-1}(-x) = 1, F_{p-2}(-x) = -x.$

By the results obtained in Section 3, the permissible values for x in these cases are:

- (i) $x = -1,$
- (ii) $x \equiv 3 \pmod{p},$
- (iii) $x \equiv -3 \pmod{p}$

and

- (iv) $x = 1.$

By Lemma 2.3 in Renaud (1977), an extension of Green's formulae, for $1 \leq r < pq,$

$$V_r \equiv V_{r_1} \times V_{r_0q+1} - (r_1 - 1)V_{r_0q} \pmod{p}.$$

Hence $\theta(V_r) = \theta(V_{r_1}) \times \theta(V_{r_0q+1})$. Induction up to $k-1$ on the characters in the theorem shows that $\phi_i^{k-1}(V_{q-1}) = 1$ for $0 \leq i < 2^{k-2},$ while $\phi_i^{k-1}(V_{q-1}) = -1$ for $2^{k-2} \leq i < 2^{k-1}.$

Now result (i) above gives rise to the first set of characters, (ii) to the third set, (iii) to the second set and (iv) to the fourth set, on applying Lemmas 4 and 5 in Section 3.

COROLLARY. $\mathcal{A}_{p,m}^*$ has exactly 2^m distinct characters. Hence $\mathcal{A}_{p,m}^*$ is isomorphic to a direct sum of 2^m local rings.

5. The structure of $\mathcal{A}_{p,m}^* (p > 2)$

For $k = 1, \dots, m,$ let

$$e_{k,0} = \frac{1}{2}(V_1 + V_{p^{k-1}} - V_{p^k})$$

and

$$e_{k,1} = \frac{1}{2}(V_1 - V_{p^{k-1}} + V_{p^k}),$$

where $\frac{1}{2}$ denotes the inverse of 2 in $Z_p.$ Application of the appropriate product formulae in Green shows $e_{k,0}$ and $e_{k,1}$ are orthogonal idempotents.

For any integer j such that $0 \leq j < 2^m,$ express j as its 2-adic expansion

$$j = j_0 + j_1 2 + \dots + j_{m-1} 2^{m-1}.$$

Define $f_j = e_{1,j_0} e_{2,j_1} \dots e_{m,j_{m-1}}.$ Now clearly $f_j f_{j'} = \delta_{j,j'} f_j:$ that is, the set of $2^m f_j$ terms forms a set of primitive orthogonal idempotents in $\mathcal{A}_{p,m}^*,$ provided none of these are zero.

Consider the action of the characters φ_j^m on f_j . Using Theorem 3, it is elementary to show that

$$\varphi_j(V_{p^{i-1}}) = (-1)^{j_{i-1}}, \quad 1 \leq i \leq m.$$

Now

$$\begin{aligned} \varphi_j^m(f_j) &= \varphi_j(e_{1,j_0} e_{2,j_1}, \dots, e_{m,j_{m-1}}) \\ &= \frac{1}{2^m} \prod_{i=1}^m (1 + (-1)^{j_{i-1}} \varphi_j^m(V_{p^{i-1}})) \\ &= \frac{1}{2^m} \prod_{i=1}^m (1 + (-1)^{j_{i-1}} (-1)^{j_{i-1}}) \\ &= \delta_{j,j}. \end{aligned}$$

Hence the f_j terms, being distinct and non-zero, form the set of primitive idempotents of $\mathcal{A}_{p,m}^*$.

Let $I_j = f_j \mathcal{A}_{p,m}^*$, $j = 0, 1, \dots, 2^m - 1$. Now $\mathcal{A}_{p,m}^* = I_0 \oplus \dots \oplus I_{2^m-1}$. We wish to develop a method of calculating the Z_p -dimension of these principal ideals, by examining the effect of f_j on the basis elements in $\mathcal{A}_{p,m}^*$.

Consider a heirarchy of blocks of basis elements of $\mathcal{A}_{p,m}^*$, the blocks on the lowest level being of type

$$\{V_{ap+1}, \dots, V_{(a+1)p}\} \quad \text{for } 0 \leq a \leq p^{m-1} - 1,$$

those on the next level being of type

$$\{V_{bp^2+1}, \dots, V_{(b+1)p^2}\} \quad \text{for } 0 \leq b \leq p^{m-2} - 1,$$

and so forth. Each block is composed of p blocks from the next lower level, except for the lowest blocks, each of which has one element of type $V_{(a+1)p}$ and $(p-1)$ elements of type V_{ap+r} , $r = 1, \dots, p-1$.

Applying Green's product formulae (1962):

$$\begin{aligned} e_{1,0} V_{ap+r} &= e_{1,0} V_{(a+1)p-r}, \\ e_{1,0} V_{(a+1)p} &= 0 \end{aligned}$$

and

$$\begin{aligned} e_{1,1} V_{ap+r} &= V_{ap} + V_{(a+1)p} - e_{1,1} V_{(a+1)p-r}, \\ e_{1,1} V_{(a+1)p} &= V_{(a+1)p} \end{aligned}$$

for a, r as above. Hence if $e_{1,0}$ appears as a factor of f_j , each block at the lowest level can contribute only $\frac{1}{2}(p-1)$ basis elements to I_j , while if $e_{1,1}$ appears, such blocks can contribute only $\frac{1}{2}(p+1)$ elements. It is shown below that not all blocks contribute to I_j .

Consider a higher level, whose blocks are of type

$$\{V_{cp^k+1}, \dots, V_{(c+1)p^k}\}.$$

Each such block is composed of a central smaller block of type

$$\{V_{c p^k + \frac{1}{2}(p-1)p^{k-1} + r}, r = 1, \dots, p^{k-1}\}$$

and $(p - 1)$ other blocks belonging to that level.

Applying Green's formulae:

$$e_{k,0} V_{c p^k + s} = e_{k,0} V_{(c+1) p^k - s},$$

$$e_{k,0} V_{(c+1) p^k} = 0$$

and

$$e_{k,1} V_{c p^k + s} = V_{c p^k} + V_{(c+1) p^k} - e_{k,1} V_{(c+1) p^k - s}$$

$$e_{k,1} V_{(c+1) p^k} = V_{(c+1) p^k}$$

for $0 \leq c \leq p^{m-k} - 1, 0 < s < p^k$. Hence if $e_{k,0}$ is a factor in f_j , the $(k-1)$ th level contributes only $\frac{1}{2}(p-1)$ blocks to I_j in each block of the k th level, apart from the central block (discussed below). Similarly, if $e_{k,1}$ is a factor in f_j , the $(k-1)$ th level again contributes $\frac{1}{2}(p-1)$ non-central blocks to I_j .

The central blocks may or may not contribute basis elements to I_j . Assume $e_{k,0} e_{k+1,0}$ is a factor in f_j . The centre block at the k th level in each block of the $(k+1)$ th level is halved by $e_{k,0}$ and is then unaffected by $e_{k+1,0}$. Hence I_j has $1 + \frac{1}{2}(p-1) = \frac{1}{2}(p+1)$ k th level blocks in each $(k+1)$ th level block.

Assume instead that $e_{k,1} e_{k+1,0}$ is a factor in f_j . The central block now vanishes in each $(k+1)$ th level block in I_j , and there exist only $\frac{1}{2}(p-1)$ k th level blocks in each such block. This also holds if $e_{k,0} e_{k+1,1}$ is a factor, while if $e_{k,1} e_{k+1,1}$ is a factor the central block does not vanish.

To summarize: the dimension of I_j is the product of m factors, each being $\frac{1}{2}(p+1)$ or $\frac{1}{2}(p-1)$, where:

- (i) the first factor is $\frac{1}{2}(p-1)$ if $e_{1,0}$ is a factor of f_j , $\frac{1}{2}(p+1)$ otherwise,
- (ii) the $(k+1)$ th factor is $\frac{1}{2}(p-1)$ if $e_{k,0} e_{k+1,1}$ or $e_{k,1} e_{k+1,0}$ is a factor, $\frac{1}{2}(p+1)$ otherwise.

EXAMPLE. In $\mathcal{A}_{p,4}^*$, $f_3 = e_{1,1} e_{2,1} e_{3,0} e_{4,0}$, and hence I_3 has dimension

$$\frac{1}{2}(p+1) \frac{1}{2}(p+1) \frac{1}{2}(p-1) \frac{1}{2}(p+1) = \frac{1}{2^4} (p-1)(p+1)^3.$$

The dimension of each summand is calculable by this method.

REMARK. Elementary number theory shows that there exist $\binom{m}{r}$ summands of dimension $(1/2^m)(p-1)^{m-r}(p+1)^r$, for $r = 0, 1, \dots, m$.

References

- M. Abramovitz and I. Stegun (1972), *Handbook of mathematical functions* (Dover, New York).
- J. F. Carlson (1975), 'The modular representation ring of a cyclic 2-group', *J. London Math. Soc.* (2), **11**, 91–92.
- J. A. Green (1962), 'The modular representation algebra of a finite group', *Illinois J. Math.* **6**, 607–619.
- J. C. Renaud (1977), *The decomposition of products in the modular representation ring of a cyclic p -group* (M.Sc. Thesis, University of Papua New Guinea).
- M. A. Snyder (1966), *Chebyshev methods in numerical approximation* (Prentice-Hall, New Jersey).

Department of Mathematics
University of Papua New Guinea
Box 4820 University P.O.
Papua New Guinea