

# The Burnside Ring Modulo a Prime

ELIOT JACOBSON

*Department of Mathematics, Ohio University, Athens, Ohio 45701*

*Communicated by Nathan Jacobson*

Received August 15, 1983

## 1. INTRODUCTION

Let  $G$  be a finite group, and let  $B(G)$  denote the Burnside ring of  $G$ , that is, the Grothendieck ring constructed on the category of finite  $G$ -sets under disjoint union and cartesian product (see [2] for a more complete description). As Solomon [9] pointed out, the structure of  $B(G)$  becomes trivial upon scalar extension to  $\mathbb{Q}$ ; indeed,  $\mathbb{Q} \otimes_{\mathbb{Z}} B(G)$  is isomorphic with a finite product of copies of  $\mathbb{Q}$ . It is natural to ask for a similar result when  $\mathbb{Q}$  is replaced by the prime field  $\mathbb{Z}_p$  of integers modulo  $p$ . The purpose of the present paper is to determine the structure of the ring  $B_p(G) = \mathbb{Z}_p \otimes_{\mathbb{Z}} B(G)$ . As we shall see, if  $p \mid |G|$ , then the structure of  $B_p(G)$  is quite complex.

We begin with some notational conventions. Let  $P = P(G)$  denote the set of all conjugacy classes of subgroups of  $G$ . For each  $b \in P$ , pick a representative  $H_b$  of  $b$ , and let  $S_b$  denote the transitive  $G$ -set of cosets modulo  $H_b$ . Let  $\iota$  denote the class of the trivial subgroup, so that  $S_\iota = G/\{1\}$ . The set  $P$  has a natural partial ordering, where we write  $a \leq b$  whenever  $H_a$  is subconjugate to  $H_b$  (denoted  $H_a \leq H_b$ ). Then  $\iota$  is the unique minimal element of  $P$ . For  $a, b, c \in P$ , let  $V_{abc}$  be the number of orbits in  $S_a \times S_b$ , under the diagonal action of  $G$ , which are isomorphic with  $S_c$  as  $G$ -sets. Equivalently, write  $G = \cup_{i=1}^r H_a \sigma_i H_b$ , then  $V_{abc} = |\{i: H_a \cap \sigma_i H_b \sim H_c\}|$ , where  $\sim$  denotes  $G$ -conjugacy. For brevity, denote  $V_{abb} = V_{ab}$  and  $V_{bbb} = V_b$ . For a  $G$ -set  $S$ , we let  $[S]$  denote its image in  $B(G)$ . The following proposition collects some well-known properties of  $B(G)$  (see [3]).

1.1. PROPOSITION. (a) *Additively,  $B(G)$  is free on the set  $\{[S_a]: a \in P\}$ , that is,  $\{S_a: a \in P\}$  is a complete set of representatives of isomorphism classes of transitive  $G$ -sets.*

(b) *For any  $a, b \in P$ ,  $[S_a][S_b] = \sum_{c \in P} V_{abc}[S_c]$ , that is, the  $V_{abc}$  are structure constants for  $B(G)$ .*

- (c) For any  $a, b, c \in P$ ,  $V_{abc} = 0$  unless both  $c \leq a$  and  $c \leq b$ .
- (d) For any  $a \in P$ ,  $V_a = (N_G(H_a) : H_a)$ .

For the remainder of this paper, assume we have a fixed finite group  $G$ . For brevity, we denote  $B_p = B_p(G)$ , and  $B = B(G)$ . Even though  $B$  does not embed faithfully in  $B_p$ , the natural isomorphism  $B_p \simeq B/pB$  implies that we may consider  $B_p = \bigoplus_{a \in P} \mathbb{Z}_p[S_a]$ , where multiplication is given by 1.1(b) by reducing the  $V_{abc}$  modulo  $p$ .

## 2. THE RADICAL OF $B_p$

If  $S$  is a  $G$ -set, and  $H \leq G$ , then  $S^H$  denotes the set of  $H$  fixed points in  $S$ . For any  $a \in P$ , there is a ring homomorphism  $\phi_a : B \rightarrow \mathbb{Z}$  given by  $\phi_a([S]) = |S^{H_a}|$  (see [2]), in particular,  $\phi_a([S_b]) = V_{ba}$ . The product map  $\phi = (\phi_a) : B \rightarrow \prod_{a \in P} \mathbb{Z}$  is injective. By reducing modulo  $p$ , there are induced ring homomorphisms  $\psi_a : B_p \rightarrow \mathbb{Z}_p$  and  $\psi = (\psi_a) : B_p \rightarrow \prod_{a \in P} \mathbb{Z}_p$ , where  $\psi_a([S_b]) = V_{ba} \in \mathbb{Z}_p$ . However,  $\psi$  need not be injective.

2.1. LEMMA.  $\psi$  is injective if and only if  $p \nmid |G|$ . In this case,  $\psi$  is an isomorphism.

*Proof.*  $\Rightarrow$  If  $p \mid |G|$ , then  $\psi_i([S_i]) = V_{ii} = |G| = 0$ , and for any other  $a \in P$ ,  $\psi_a([S_i]) = V_{ia} = 0$  by 1.1(c), since  $a \not\leq i$ . Thus,  $[S_i] \in \ker \psi$ .

$\Leftarrow$  Suppose  $0 \neq x = \sum_b r_b [S_b] \in \ker \psi$ , and choose  $g \in P$  maximal with  $r_g \neq 0$ . For any other  $c \in P$ ,  $r_c \neq 0$  implies  $g \leq c$ , so that  $V_{cg} = 0$ . Then,  $0 = \psi_g(x) = \sum_b r_b V_{bg} = r_g V_g$ , so that  $p \mid V_g$ . It follows that  $p \mid |G|$ . By counting  $\mathbb{Z}_p$ -dimensions,  $\psi$  is injective if and only if it is an isomorphism. ■

We let  $J_p = J(B_p)$  denote the Jacobson radical of  $B_p$ .

2.2. PROPOSITION.  $J_p = \ker \psi$ .

*Proof.*  $\subseteq$  Recall that  $J_p$  is the intersection of the annihilators of all simple  $B_p$ -modules. For any  $a \in P$ ,  $\mathbb{Z}_p$  becomes a simple  $B_p$ -module via  $\psi_a$ . Thus, if  $x \in J_p$ , then  $\psi_a(x) \cdot \mathbb{Z}_p = 0$ , so that  $\psi_a(x) = 0$ , all  $a \in P$ . It follows that  $x \in \ker \psi$ .

$\supseteq$  If  $p \nmid |G|$ , then  $\ker \psi = 0$  by 2.1, and the inclusion is clear. Thus we may assume  $p \mid |G|$ . Let  $0 \neq x = \sum_b r_b [S_b] \in \ker \psi$ . It is sufficient to show that  $x$  is nilpotent, and this we accomplish by induction on  $n(x) = \max\{|H_b| : r_b \neq 0\}$ . If  $n(x) = 1$ , then  $x = r_i [S_i]$ , so that  $x^2 = r_i^2 |G| [S_i] = 0$  since  $p \mid |G|$ . Assume  $n(x) > 1$ . It is enough to show

that  $n(x^2) < n(x)$ , since induction then implies  $x^2$  (hence  $x$  also) is nilpotent. Since  $x \in \ker \psi$ , we have the equations:

$$\sum_b r_b V_{ba} = 0 \quad \text{all } a \in P. \quad (1)$$

Therefore,

$$\begin{aligned} x^2 &= \sum_{b,c,d} r_b r_c V_{bcd} [S_d] \\ &= \sum_c r_c \left( \sum_b r_b V_{bc} \right) [S_c] + \sum_{\substack{b,c \\ d < c}} r_b r_c V_{bcd} [S_d] \\ &= \sum_{\substack{b,c \\ d < c}} r_b r_c V_{bcd} [S_d] \quad (\text{by (1)}); \end{aligned}$$

thus

$$x^2 = \sum_d \left( \sum_{c > d} r_c \left( \sum_b r_b V_{bcd} \right) \right) [S_d] = \sum_d t_d [S_d]. \quad (2)$$

Fix  $g \in P$  with  $r_g \neq 0$  and  $n(x) = |H_g|$ . It is sufficient to show that  $t_d \neq 0$  implies  $|H_d| < |H_g|$ . By (2), if  $t_d \neq 0$ , then there exists  $c > d$  with  $r_c \neq 0$ . Then  $|H_d| < |H_c| \leq |H_g|$ . ■

2.3. COROLLARY.  $B_p$  is semisimple if and only if  $P \nmid |G|$ . In fact, if  $p \mid |G|$ , then  $B_p \simeq \mathbb{Z}_p \dot{+} \cdots \dot{+} \mathbb{Z}_p$ ,  $|P|$ -times.

### 3. THE DIMENSION OF THE RADICAL

Fix any  $a, b \in P$ , and assume that  $a \leq b$ . Define  $T = \{\sigma \in G: H_a^\sigma \subseteq H_b\}$ . If  $\sigma \in T$ , then  $H_a \sigma N_G(H_b) \subseteq T$ , so that  $T$  is a union of  $H_a - N_G(H_b)$  double cosets. Fix a double coset decomposition  $T = \bigcup_{i=1}^k H_a \tau_i N_G(H_b)$  (possibly  $k=0$ ), and write  $G = T \cup \bigcup_{i=1}^s H_a \sigma_i H_b$ , where  $H_a^\sigma \not\subseteq H_b$  for  $1 \leq i \leq s$ . Let  $t = V_b = (N_G(H_b): H_b)$ , and write  $N_G(H_b) = \rho_1 H_b \cup \cdots \cup \rho_l H_b$ .

3.1. LEMMA. If  $H_a \tau_i \rho_j H_b = H_a \tau_i \rho_k H_b$ , then  $j = k$ .

*Proof.* Write  $\tau_i \rho_j = h_1 \tau_i \rho_k h_2$ , for some  $h_1 \in H_a$ ,  $h_2 \in H_b$ . Then  $\rho_k^{-1} \rho_j = \rho_k^{-1} \tau_i^{-1} \tau_i \rho_j = \rho_k^{-1} \tau_i^{-1} h_1 \tau_i \rho_k h_2 \in H_b$ , since  $\tau_i^{-1} h_1 \tau_i \in H_b$ , and  $\rho_k \in N_G(H_b)$ . Thus  $\rho_j H_b = \rho_k H_b$ , so that  $j = k$ . ■

3.2. PROPOSITION. For any  $a, b \in P$ ,  $V_b \mid V_{ba}$ .

*Proof.* If  $a \not\leq b$ , then  $V_{ba} = 0$  and the result is clear. Assume  $a \leq b$ . Then by 3.1, we have (with the above notation) the *disjoint* double coset decomposition:

$$G = \bigcup_{i=1}^k \bigcup_{j=1}^t H_a \tau_i \rho_j H_b \cup \bigcup_{i=1}^s H_a \sigma_i H_b.$$

Therefore,

$$\begin{aligned} S_a \times S_b &= G/H_a \times G/H_b \\ &\simeq \bigcup_{i=1}^k \bigcup_{j=1}^t G/H_b \cap H_a^{\tau_i \rho_j} \cup \bigcup_{i=1}^s G/H_b \cap H_a^{\sigma_i} \\ &\simeq \bigcup_{i=1}^k \bigcup_{j=1}^t G/H_a \cup \bigcup_{i=1}^s G/H_{a_i} \quad \text{where } a_i < a, \text{ all } i \\ &= (kt) \cdot S_a \cup \bigcup_{i=1}^s S_{a_i}. \end{aligned}$$

We conclude that  $V_{ba} = kt = kV_b$ , so  $V_b \mid V_{ba}$ . ■

For the remainder of this paper, “dimension” will mean dimension as a  $\mathbb{Z}_p$ -space.

3.3. PROPOSITION.  $\dim(J_p) = |\{a: p \mid V_a\}|$ .

*Proof.* If  $p \nmid |G|$  the result is clear, so assume that  $p \mid |G|$ . Extend the partial ordering  $\leq$  on  $P$  to a total ordering so that  $H_a \leq H_b$  implies  $a \leq b$  (but not necessarily the converse). Set  $n = |P|$ , and define a map  $B_p \rightarrow \mathbb{Z}_p^{(n)} = \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p$  ( $n$ -times) by sending  $x = \sum_b r_b [S_b]$  to the vector  $\bar{x} = (\dots, r_b, \dots)$ , ordered by  $\leq$ . Then  $x \rightarrow \bar{x}$  defines a  $\mathbb{Z}_p$ -space isomorphism. Let  $M$  be the matrix  $(V_{ba})$ , considered as a linear transformation by right multiplication on  $\mathbb{Z}_p^{(n)}$ . Note that  $x = \sum_b r_b [S_b] \in J_p$  iff  $x \in \ker \psi$  iff  $\sum_b r_b V_{ba} = 0$  all  $a \in P$  iff  $\bar{x} \cdot M = 0$  iff  $\bar{x} \in \ker M$ . Hence the map  $x \rightarrow \bar{x}$  restricts to a  $\mathbb{Z}_p$ -space isomorphism  $J_p \rightarrow \ker M$ . In particular, we conclude that  $\dim(J_p) + \text{rank}(M) = |P|$ . Since  $M$  is lower triangular, and since a zero diagonal entry occurs if and only if the entire row is zero (by 3.2), it follows that  $\text{rank}(M) = |\{a: p \nmid V_a\}|$ , giving our result. ■

4. IDEMPOTENTS IN  $B_p$

In this section we use the map  $\psi$  to construct the primitive idempotents of  $B_p$ . Fix a prime  $p \in \mathbb{Z}$ , then define  $P^* = P^*(G) = \{a: p \nmid V_a\}$ . Let  $n(p) = |P^*|$ . By 3.3,  $B_p/J_p \simeq \text{im}(\psi)$  is a semisimple subalgebra of  $\prod_{a \in P} \mathbb{Z}_p$

of dimension  $n(p)$ . By Wedderburn's theorem,  $\text{im}(\psi)$  is isomorphic with an algebra product of field extensions of  $\mathbb{Z}_p$ . By noting that no element in  $\text{im}(\psi)$  has multiplicative order larger than  $p-1$ , it follows that there is an algebra isomorphism  $\sigma: \text{im}(\psi) \rightarrow \prod_{i=1}^{n(p)} \mathbb{Z}_p$ . Let  $\delta_i \in \prod_{i=1}^{n(p)} \mathbb{Z}_p$  be the primitive idempotent corresponding to projection onto the  $i$ th coordinate. For each  $i$ , choose  $x_i \in B_p$  with  $\sigma\psi(x_i) = \delta_i$ . Then  $\sigma\psi(x_i^2 - x_i) = 0$ , so that  $x_i^2 - x_i \in \ker \psi = J_p$ , that is,  $x_i$  is idempotent modulo  $J_p$ . By a standard lifting theorem [7, p. 97], there are idempotents  $e_i \in B_p$  such that  $e_i \equiv x_i \pmod{J_p}$ ,  $i = 1, \dots, n(p)$ . We now establish some properties of the idempotents  $\{e_i: i = 1, \dots, n(p)\}$ .

4.1. LEMMA. *The idempotents  $\{e_i: i = 1, \dots, n(p)\}$  are distinct, pairwise orthogonal, and sum to 1. Moreover, each  $e_i$  is primitive.*

*Proof.* If  $e_i = e_j$  then  $\delta_i = \psi(e_i) = \psi(e_j) = \delta_j$ , so  $i = j$ . For orthogonality, if  $i \neq j$  then  $\sigma\psi(e_i e_j) = \delta_i \delta_j = 0$ , hence  $e_i e_j \in \ker \psi = J_p$ . Since  $e_i e_j$  is idempotent, and  $J_p$  is nilpotent,  $e_i e_j = 0$ . To see that  $\sum_i e_i = 1$ , note that  $\sigma\psi(\sum_i e_i) = \sum_i \delta_i = 1 = \sigma\psi(1)$ , so that  $1 - \sum_i e_i \in J_p$ . As above, this implies  $1 - \sum_i e_i = 0$ .

To see that each  $e_i$  is primitive, let  $f \in B_p$  be idempotent with  $f e_i \neq 0$ . We must show  $f e_i = e_i$ . Write  $\sigma\psi(f) = \sum_{j \in S} \delta_j$ , for some  $S \subseteq \{1, \dots, n(p)\}$ . If  $i \notin S$  then  $0 = \sigma\psi(f) \delta_i = \sigma\psi(f e_i)$  implies  $f e_i \in J_p$ , so that  $f e_i = 0$  contrary to assumption. Hence  $i \in S$ . Since  $f \equiv \sum_{j \in S} e_j \pmod{J_p}$ , we have  $f e_i \equiv e_i \pmod{J_p}$ . As in the preceding paragraph, this implies  $f e_i = e_i$ . ■

To aid in the statement of the next lemma, we (temporarily) write  $e_i = \sum_a c_{ia} [S_a]$ , some  $c_{ia} \in \mathbb{Z}_p$ ,  $i = 1, \dots, n(p)$ .

4.2. LEMMA. (a) *For any  $i$ , if  $a \in P$  is maximal with  $c_{ia} \neq 0$ , then  $a \in P^*$  and  $c_{ia} = V_a^{-1}$ .*

(b) *Suppose  $i \neq j$ , and choose  $a, b$  maximal with  $c_{ia}, c_{jb} \neq 0$ , respectively. Then  $a \neq b$ .*

(c) *Each idempotent  $e_i$  contains a unique maximal  $a \in P^*$  with  $c_{ia} \neq 0$ . If  $i \neq j$ , then these maximal elements are distinct.*

*Proof.* A simple computation using  $e_i^2 = e_i$  and maximality of  $a$  yields  $e_i \equiv c_{ia}^2 V_a [S_a] \pmod{\bigoplus_{b \neq a} \mathbb{Z}_p [S_b]}$ . Thus  $c_{ia} = c_{ia}^2 V_a \neq 0$ , so  $a \in P^*$  and  $c_{ia} = V_a^{-1}$ , proving (a).

(b) If  $a = b$ , then  $0 = e_i e_j \equiv c_{ia} c_{ja} [S_a]^2 \pmod{\bigoplus_{b \neq a} \mathbb{Z}_p [S_b]} \equiv c_{ia} c_{ja} V_a [S_a] \pmod{\bigoplus_{b \neq a} \mathbb{Z}_p [S_b]}$ . This implies  $c_{ia} c_{ja} V_a = 0$ , contrary to (a).

(c) Let  $n_i$  be the number of maximal elements occurring in  $e_i$ . Then by (b),  $|P^*| \geq \sum_i n_i \geq \sum_i 1 = |P^*|$ , forcing  $n_i = 1$ , all  $i$ . The second statement restates part (b). ■

For each  $a \in P^*$  let  $e_a = \sum_b \lambda_{ab} [S_b]$  be the primitive idempotent of  $B_p$  with  $\lambda_{aa} = V_a^{-1}$  and  $\lambda_{ab} = 0$  if  $b \not\leq a$ . By 4.2 the idempotents  $\{e_a : a \in P^*\}$  are just the idempotents  $\{e_i : i = 1, \dots, n(p)\}$  relabeled. Relabel the  $x_i$ 's and  $\delta_i$ 's accordingly, so that  $\sigma\psi(x_a) = \delta_a$  and  $e_a \equiv x_a \pmod{J_p}$ . For  $b \in P^*$ , let  $\pi_b : \prod_{a \in P^*} \mathbb{Z}_p \rightarrow \mathbb{Z}_p$  be projection onto the  $b$ -th coordinate.

4.3. THEOREM. *Let  $G$  be a finite group, and  $p \in \mathbb{Z}$  be a prime. Then  $B_p(G) \simeq \prod_{a \in P^*} L_a$ , where for  $b \in P^*$ ,  $L_b = B_p(G)e_b$  is a local ring with residue field  $\mathbb{Z}_p$ .*

*Proof.* For each  $b \in P^*$ , define  $\tau_b : B_p e_b \rightarrow \mathbb{Z}_p$  by  $\tau_b = \pi_b \sigma\psi$ . We claim that  $J(B_p e_b) = \ker \tau_b$ . To see this suppose first that  $xe_b \in J(B_p e_b)$ . Then  $xe_b \in B_p$  is nilpotent, so that  $xe_b \in J(B_p) = \ker \psi \subseteq \ker \tau_b$ . Conversely, let  $xe_b \in \ker \tau_b$ . Note that  $\sigma\psi(xe_b) = \sigma\psi(xe_b e_b) = \sigma\psi(xe_b) \delta_b$ . Since  $\pi_b : (\prod_{a \in P^*} \mathbb{Z}_p) \delta_b \rightarrow \mathbb{Z}_p$  is an isomorphism, it follows that  $\sigma\psi(xe_b) = 0$ , that is,  $xe_b \in \ker \psi = J(B_p)$ . Then  $xe_b \in J(B_p)e_b = J(B_p e_b)$ , finishing the claim. By the first homomorphism theorem we conclude  $B_p e_b / J(B_p e_b) \simeq \mathbb{Z}_p$ , so  $B_p e_b$  is a local ring with residue field  $\mathbb{Z}_p$ . The remainder of the theorem is clear, since by 4.1,  $B_p = B_p(\sum_a e_a) \simeq \prod_a (B_p e_a)$ . ■

4.4. COROLLARY.  *$G$  is a  $p$ -group if and only if  $B_p(G)$  is a local ring.*

*Proof.*  $\Rightarrow$  If  $G$  is a  $p$ -group and  $H \subset G$ , then  $H \subset N_G(H)$ . Thus,  $|P^*| = 1$ , and the result follows from 4.3.

$\Leftarrow$  Let  $H$  be  $p$ -Sylow in  $G$ . Then  $p \nmid (N_G(H) : H)$ , so  $H$  represents a class in  $P^*$ . However, if  $B_p(G)$  is local, then by 4.3,  $|P^*| = 1$ . Thus  $H$  and  $G$  are conjugate, that is,  $H = G$ . ■

### 5. DIMENSION OF THE LOCAL DIRECT FACTORS

Fixed throughout this section is a prime  $p \in \mathbb{Z}$ . For any  $a \in P^*$  and  $b \in P$ ,  $\psi_b(e_a)$  is an idempotent in  $\mathbb{Z}_p$ , hence  $\psi_b(e_a) \in \{0, 1\}$ . We define the “support of  $a$  modulo  $p$ ” to be  $\text{supp}(a) = \{b \in P : \psi_b(e_a) = 1\}$ . Thus,  $|\text{supp}(a)| = 1$  iff  $\psi(e_a)$  is a primitive idempotent of  $\prod_{b \in P} \mathbb{Z}_p$ . Our first objective is to establish the identity:  $\sum_{a \in P^*} |\text{supp}(a)| = |P|$ .

5.1. LEMMA. (a) *If  $a \neq b$ , then  $\text{supp}(a) \cap \text{supp}(b) = \emptyset$ .*

(b) For any  $b \in P$ , there exists  $a \in P^*$  (unique by part (a)) such that  $b \in \text{supp}(a)$ .

(c) For any  $a \in P^*$ ,  $\text{supp}(a) \cap P^* = \{a\}$ .

*Proof.* (a) Suppose  $d \in \text{supp}(a) \cap \text{supp}(b)$ , so that  $\psi_d(e_a) = \psi_d(e_b) = 1$ . Then  $1 = \psi_d(e_a) \psi_d(e_b) = \psi_d(e_a e_b) = \psi_d(0) = 0$ , a contradiction.

(b) If  $b \notin \text{supp}(a)$  for all  $a \in P^*$ , then  $1 = \psi_b(1) = \psi_b(\sum_a e_a) = \sum_a \psi_b(e_a) = 0$ , contradiction.

(c) Since  $\psi_a(e_a) = \psi_a(\sum_{b \leq a} \lambda_{ab} [S_b]) = \sum_{b \leq a} \lambda_{ab} V_{ba} = \lambda_{aa} V_a = 1$ ,  $a \in \text{supp}(a)$ . If also  $b \in \text{supp}(a) \cap P^*$ , then  $b \in \text{supp}(a) \cap \text{supp}(b) = \emptyset$ . ■

5.2. COROLLARY.  $\sum_{a \in P^*} |\text{supp}(a)| = |P|$ .

*Proof.* By 5.1,  $P = \bigcup_{a \in P^*} \text{supp}(a)$ . ■

5.3. LEMMA. If  $a \in P^*$  then the set  $\{[S_b] e_a : b \in \text{supp}(a)\}$  is a linearly independent subset of  $B_p e_a$ .

*Proof.* For brevity denote  $S = \text{supp}(a)$ . If  $b \in S$ , then  $\psi_b(e_a) = 1$  implies  $\sum_c \lambda_{ac} V_{cb} = 1$ . Thus  $[S_b] e_a = \sum_{c,d} \lambda_{ac} \lambda_{cb} [S_d] e_a \equiv [S_b] \pmod{\bigoplus_{c < b} \mathbb{Z}_p [S_c]}$ . Suppose there is a dependence relation  $\sum_{b \in S} r_b [S_b] e_a = 0$ , for some  $r_b \in \mathbb{Z}_p$ , and fix  $g \in S$  maximal with  $r_g \neq 0$ . Thus  $r_b \neq 0$  implies  $g \leq b$  if  $b \neq g$ , so that  $[S_g] \notin \bigoplus_{c \leq b} \mathbb{Z}_p [S_c]$ . Let  $S' = \{b \in S : b \neq g, r_b \neq 0\}$ , and let  $I$  be the ideal:  $I = (\sum_{b \in S'} \sum_{c \leq b} \mathbb{Z}_p [S_c]) + (\sum_{d < g} \mathbb{Z}_p [S_d])$ . By the computation above,  $0 = \sum_{b \in S} r_b [S_b] e_a \equiv r_g [S_g] e_a \not\equiv 0 \pmod{I}$ , a contradiction. ■

5.4. THEOREM. Let  $a \in P^*$ . Then  $\dim(B_p e_a) = |\text{supp}(a)|$ . Moreover,  $\{[S_b] e_a : b \in \text{supp}(a)\}$  is a  $\mathbb{Z}_p$ -basis of  $B_p e_a$ , and  $\{[S_b] e_a : b \in \text{supp}(a), b \neq a\}$  is a  $\mathbb{Z}_p$ -basis of  $J(B_p e_a)$ . In particular,  $J_p = \bigoplus_{a \in P^*} \bigoplus_{b \in \text{supp}(a), b \neq a} \mathbb{Z}_p [S_b] e_a$ .

*Proof.* By 5.2 and 5.3 we have  $\dim(B_p) = \sum_{a \in P^*} \dim(B_p e_a) \geq \sum_{a \in P^*} |\text{supp}(a)| = |P| = \dim(B_p)$ , and equality must hold throughout. Thus,  $\dim(B_p e_a) = |\text{supp}(a)|$ , and the second statement follows from 5.3. Next, note that if  $b \in \text{supp}(a)$  and  $b \neq a$ , then by 5.1(c),  $b \notin P^*$ . Thus by 3.2,  $[S_b] \in \ker \psi = J_p$ , so that  $[S_b] e_a \in J(B_p e_a)$ . Since  $B_p e_a$  local, a dimension count now implies the third result. ■

Because of 5.4, it would be helpful to have a formula for the “modular” idempotents of  $B_p$ . The techniques used by Gluck [4] fail to work in our situation; however, there is another approach which gives a formula for these idempotents modulo the radical  $J_p$ . It is convenient to extend the ordering  $\leq$  on  $P$  to a total ordering, so that  $H_a \lesssim H_b$  implies  $a \leq b$ , but not

necessarily conversely. We introduce some auxiliary matrices. Define  $M = (V_{ab})_{a,b \in P}$ ,  $M_p = (V_{ab})_{a,b \in P^*}$ , and  $M_p^* = (V_{ab})_{a \in P^*, b \in P}$ . We consider  $M_p, M_p^*$  to have entries in  $\mathbb{Z}_p$ , so that their arithmetic is modulo  $p$ . In particular,  $M_p$  is nonsingular since it is lower triangular with nonzero diagonal entries. Define  $N_p$  to be the matrix product:  $N_p = M_p^{-1}M_p^* = (W_{ab})_{a \in P^*, b \in P}$ .

5.5. PROPOSITION. (a)  $M_p^{-1} = (\lambda_{ab})_{a,b \in P^*}$ .

(b) For any  $a \in P^*$ ,  $\psi(e_a) = (\dots, W_{ab}, \dots)$ . Thus the  $a$ th row of  $N_p$  corresponds to the image under  $\psi$  of  $e_a$ .

(c)  $\text{Supp}(a) = \{b: W_{ab} = 1\}$ . In particular,  $\dim(B_p e_a) = \sum_{b \in P} W_{ab}$ .

*Proof.* Let  $c \in P^*$ . Then by 5.1(c),  $\delta_{ac} = \psi_c(e_a) = \sum_{b \in P} \lambda_{ab} V_{bc}$ . However, if  $b \notin P^*$ , then  $V_b = 0$ , whence  $V_{bc} = 0$ , by 3.2. Thus the sum is over  $P^*$ , so that  $\sum_{b \in P^*} \lambda_{ab} V_{bc} = \delta_{ac}$ . Statement (a) follows.

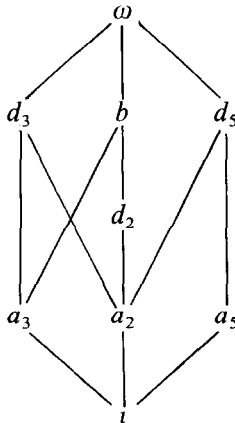
(b) It suffices to show that  $\psi_b(e_a) = W_{ab}$ . By part (a) we have:  $\psi_b(e_a) = \psi_b(\sum_{c \in P} \lambda_{ac} [S_c]) = \sum_{c \in P} \lambda_{ac} V_{cb} = \sum_{c \in P^*} \lambda_{ac} V_{cb} = W_{ab}$ , since  $V_{cb} = 0$  if  $c \notin P^*$ .

(c) Immediate from part (b). ■

Thus, modulo  $J_p$ , we can find the idempotents of  $B_p$  by inverting the matrix  $M_p$ . The following example illustrates the techniques involved.

6. EXAMPLE:  $G = A_5$

The purpose of this section is to compute  $B_2(A_5)$ . The conjugacy classes of subgroups of  $A_5$  are  $1 = (\{1\})$ ,  $a_p = (\mathbb{Z}_p) p = 2, 3, 5$ ,  $d_p = (D_p) p = 2, 3, 5$ ,  $b = (A_4)$ , and  $\omega = (A_5)$ . The lattice of  $P(A_5)$  is given by the diagram:





We extend the ordering  $\leq$  to a total ordering by setting  $1 < a_2 < a_3 < a_5 < d_2 < d_3 < d_5 < b < \omega$ . It is a simple but tedious task to compute the double coset decompositions for pairs of subgroups of  $A_5$ , and then to compute the constants  $V_{ac}$  for all  $a, c \in P(A_5)$ . This information is given by the matrix

$$M = \begin{pmatrix} 60 \\ 30 & 2 \\ 20 & 0 & 2 & \circlearrowleft \\ 12 & 0 & 0 & 2 \\ 15 & 3 & 0 & 0 & 3 \\ 10 & 2 & 1 & 0 & 0 & 1 \\ 6 & 2 & 0 & 1 & 0 & 0 & 1 \\ 5 & 1 & 2 & 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

We now consider the prime  $p=2$ . Then  $P^* = \{d_2, d_3, d_5, b, \omega\}$ ,

$$M_2 = \begin{pmatrix} 1 \\ 0 & 1 & \circlearrowleft \\ 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 \end{pmatrix} \quad \text{and} \quad M_2^{-1} = \begin{pmatrix} 1 \\ 0 & 1 & \circlearrowleft \\ 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

Therefore,

$$N_2 = \begin{pmatrix} 1 \\ 0 & 1 & \circlearrowleft \\ 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & \circlearrowleft \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & \circlearrowleft \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

From 5.5(c) we have  $\text{supp}(d_2) = \{1, a_2, d_2\}$ ,  $\text{supp}(d_3) = \{a_3, d_3\}$ ,  $\text{supp}(d_5) = \{a_5, d_5\}$ ,  $\text{supp}(b) = \{b\}$ , and  $\text{supp}(\omega) = \{\omega\}$ . Also, from 5.5(a), the primitive idempotents of  $B_2(A_5) \pmod{J_2(A_5)}$  are  $e_{d_p} \equiv [S_{d_p}]$   $p=2, 3, 5$ ,  $e_b \equiv [S_b] + [s_{d_2}]$ , and  $e_\omega \equiv [S_\omega] + [S_b] + [S_{d_5}] + [S_{d_3}]$ .

From 5.5(c), the dimensions of the local direct factors are 3, 2, 2, 1, 1, respectively. Moreover,  $B_2(A_5) \cdot e_{d_2}$  has 2-nilpotent radical. This follows from direct computation, using the fact [6, Lemma 3] that

$J(B_2(A_5) \cdot e_{a_2}) = \mathbb{Z}_p[S_1] \oplus \mathbb{Z}_p[S_{a_2}]$  (since  $D_2$  is 2-Sylow in  $A_5$ ). Algebras over finite fields of dimension 2 or 3 have been completely classified by Raghavendran [8, Theorems 10, 11]. In particular, a local ring of dimension 2 over  $\mathbb{Z}_p$  is isomorphic with the ring of matrices  $R_p(2) = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} : a, b \in \mathbb{Z}_p \right\}$ , while a local ring of dimension 3 with 2-nilpotent radical is isomorphic with the ring of matrices

$$R_p(3) = \left\{ \begin{pmatrix} a & b & c \\ 0 & a & 0 \\ 0 & 0 & a \end{pmatrix} : a, b, c \in \mathbb{Z}_p \right\}.$$

From this discussion it follows that:  $B_2(A_5) \simeq \mathbb{Z}_2 \dot{+} \mathbb{Z}_2 \dot{+} R_2(2) \dot{+} R_2(2) \dot{+} R_2(3)$ . In a similar fashion, the rings  $B_3(A_5)$  and  $B_5(A_5)$  can be computed. They are

$$B_3(A_5) \simeq \mathbb{Z}_3 \dot{+} \mathbb{Z}_3 \dot{+} \mathbb{Z}_3 \dot{+} \mathbb{Z}_3 \dot{+} \mathbb{Z}_3 \dot{+} R_3(2) \dot{+} R_3(2), \quad \text{and}$$

$$B_5(A_5) \simeq \mathbb{Z}_5 \dot{+} \mathbb{Z}_5 \dot{+} \mathbb{Z}_5 \dot{+} \mathbb{Z}_5 \dot{+} \mathbb{Z}_5 \dot{+} \mathbb{Z}_5 \dot{+} R_5(2).$$

### 7. THE STRUCTURE OF THE SUPPORT

This section is devoted to the problem of giving a non-combinatorial description of  $\text{supp}(a)$ , for any  $a \in P^*$ . At the heart of this work, and what follows in Section 8, is the following lemma.

7.1. LEMMA. *Suppose  $c, d \in P$  are such that  $H_d$  is  $G$ -conjugate to a normal subgroup of  $H_c$  (notation:  $H_d \trianglelefteq H_c$ ) of  $p$ -power index. Then for all  $a \in P$ ,  $V_{ad} \equiv V_{ac} \pmod{p}$ .*

*Proof.* We may assume  $H_d \subseteq H_c$ . Take  $H_c - H_a$  and  $H_d - H_a$  double coset decompositions:

$$G = \bigcup_{i=1}^{V_{ac}} H_c \tau_i H_a \cup \bigcup_{i=1}^k H_c \alpha_i H_a$$

and

$$G = \bigcup_{i=1}^{V_{ad}} H_d \sigma_i H_a \cup \bigcup_{i=1}^m H_d \beta_i H_a,$$

where for all  $i$ ,  $H_c^{\tau_i} \subseteq H_a$ ,  $H_d^{\sigma_i} \subseteq H_a$ ,  $H_c^{\alpha_i} \not\subseteq H_a$ , and  $H_d^{\beta_i} \not\subseteq H_a$ . Denote  $S_i = H_d \sigma_i H_a$  and let  $S = \{S_i : 1 \leq i \leq V_{ad}\}$ . Since  $H_d$  is normal in  $H_c$ , there is a well-defined  $H_c$  action on  $S$  given by  $\sigma S_i = S_j$  if and only if  $\sigma \sigma_i \in S_j$ , all

$\sigma \in H_c$ . Evidently,  $H_d \subseteq \text{Stab}_{H_c}(S_i)$  and  $\text{Stab}_{H_c}(S_i) = H_c \cap {}^{\sigma_i}H_a$ . Thus by hypothesis,  $|\text{Orb}_{H_c}(S_i)| = (H_c : \text{Stab}_{H_c}(S_i))$  is  $p$ -power for all  $i$ , with  $|\text{Orb}_{H_c}(S_i)| = 1$  if and only if  $H_c^{\sigma_i} \subseteq H_a$ .

Now observe that  $V_{ac} = |\{\sigma_i : H_c^{\sigma_i} \subseteq H_a\}|$ . To see this, define a map from  $\{\sigma_i : H_c^{\sigma_i} \subseteq H_a\}$  to  $\{\tau_j : 1 \leq j \leq V_{ac}\}$  by  $\sigma_i \rightarrow \tau_j$  if and only if  $\sigma_i \in H_c \tau_j H_a$ . Note that  $H_c \tau_i H_a = \tau_i H_a$  for  $1 \leq i \leq V_{ac}$ , and if  $H_c^{\sigma_i} \subseteq H_a$ , then  $H_d \sigma_i H_a = \sigma_i H_a = \tau_j H_a$  for some  $j$ ,  $1 \leq j \leq V_{ac}$ . Thus  $\sigma_i \rightarrow \tau_j$  defines a bijection. Since  $S$  is a disjoint union of  $H_c$  orbits,  $V_{ad} = |S| \equiv \sum_{H_c^{\sigma_i} \subseteq H_a} 1 = |\{\sigma_i : H_c^{\sigma_i} \subseteq H_a\}| = V_{ac} \pmod{p}$ . ■

7.2. COROLLARY. (Sylow) *If  $p \mid |G|$ , then the number of  $p$ -Sylow subgroups of  $G$  is congruent to one modulo  $p$ .*

*Proof.* Let  $c$  denote the class of the  $p$ -Sylow subgroups. Take  $d = i$  and  $a = c$  in 7.1. ■

For any subgroup  $H \leq G$  we let  $O^p(H)$  denote the (unique) smallest normal subgroup of  $H$  of  $p$ -power index.

7.3. THEOREM. *Let  $a \in P^*$  and  $d \in P$ . The following are equivalent.*

- (a)  $d \in \text{supp}(a)$ .
- (b) *There is a normal chain  $H_d = H_0 \triangleleft H_1 \triangleleft \dots \triangleleft H_n \sim H_a$  with each quotient a  $p$ -group.*
- (c)  $O^p(H_a) \lesssim H_d \lesssim H_a$ .

*Proof.* (b)  $\Rightarrow$  (a) Induce on  $n$ . The case  $n = 0$  being clear, assume that  $n \geq 1$ . Choose  $c \in P$  with  $H_1 \sim H_c$ . By induction,  $c \in \text{supp}(a)$ . Applying 7.1 we then have  $\psi_d(e_a) = \sum_b \lambda_{ab} V_{bd} = \sum_b \lambda_{ab} V_{bc} = \psi_c(e_a) = 1$ . Therefore,  $d \in \text{supp}(a)$ .

(a)  $\Rightarrow$  (b) We define the chain inductively. Let  $H_0 = H_d$ , and assume we have constructed  $H_0 \triangleleft H_1 \triangleleft \dots \triangleleft H_k$  with each quotient a  $p$ -group. Choose  $c \in P$  with  $H_k \sim H_c$ . Note that if  $c \in P^*$  then by the implication (b)  $\Rightarrow$  (a) we have  $d \in \text{supp}(c) \cap \text{supp}(a)$ , thus  $c = a$  and the chain is complete. If  $c \notin P^*$  then  $p \mid (N_G(H_c) : H_c)$ , so let  $H \leq G$  be such that  $H/H_c$  is  $p$ -Sylow in  $N_G(H_c)/H_c$ . Then  $H_k \cong H$ , so there is a subgroup  $H_{k+1} \sim H$  with  $H_k \triangleleft H_{k+1}$  and the quotient a  $p$ -group.

(b)  $\Leftrightarrow$  (c) is standard, and we omit the proof. ■

This Theorem has two interesting corollaries.

7.4. COROLLARY. *If  $p$  exactly divides  $|G|$ , then the local direct factors of  $B_p$  have  $\mathbb{Z}_p$ -dimension either one or two.*

*Proof.* By 4.3 and 5.4 it suffices to show that for any  $a \in P^*$ ,  $\text{supp}(a) = 1$  or  $2$ . If  $p$  exactly divides  $|H_a|$ , then there can be at most one normal subgroup of  $H_a$  of index  $p$ , while there can be no such subgroups if  $p$  does not divide  $|H_a|$ . Apply 7.3. ■

In fact, this Corollary is precise in the sense that if  $p^2 \mid |G|$ , then the local direct factor corresponding to a  $p$ -Sylow has dimension at least 3 (see [6]).

Using the characterization of dimension 2 algebras over  $\mathbb{Z}_p$  as in Section 6 we find that if  $|G|$  is square free, then for any prime  $p$ ,  $B_p(G) \simeq \mathbb{Z}_p^{(r)} \dot{+} R_p(2)^{(s)}$ , for some nonnegative integers  $r, s$ , depending on  $p$ , with  $s > 0$  if and only if  $p \mid |G|$ . Since  $R_p(2)$  has a unique proper ideal, it is trivial to check that  $R_p(2)$  is self-injective. Since it is also Artinian,  $R_p(2)$  is quasi-Frobenius. Moreover, the property of being quasi-Frobenius is invariant under finite direct products and scalar extensions. Hence we obtain in a more concrete fashion Corollary 2 of [6].

7.5. COROLLARY. *If  $G$  has square free order then for any field  $F$ ,  $F \otimes_{\mathbb{Z}} B(G)$  is a quasi-Frobenius  $F$ -algebra.*

### 8. APPLICATIONS TO MODULAR REPRESENTATIONS

We now discuss  $\mathbb{Z}_p$ -representations of the group  $G$ , where we fix a prime  $p$  dividing  $|G|$ . For any  $G$ -set  $S$ , the permutation representation of  $S$  is integral, so by reducing modulo  $p$  we obtain a  $\mathbb{Z}_p$ -representation whose character will be denoted by  $\xi_S$ . In particular if  $S = S_a$  we denote by  $\xi_a$  the permutation character  $1_{H_a}^G$  reduced modulo  $p$ . This correspondence yields a ring homomorphism  $B(G) \rightarrow X(G, p)$ , where  $X(G, p)$  is the ring of  $\mathbb{Z}_p$ -characters. Since  $pB(G)$  is contained in the kernel of this map, there is a ring homomorphism  $\theta: B_p(G) \rightarrow X(G, p)$ , where  $\theta$  satisfies  $\theta([S]) = \xi_S$  for any  $G$ -set  $S$ . For each  $\sigma \in G$ , we let  $a_\sigma \in P$  denote the class of the cyclic subgroup  $\langle \sigma \rangle$  of  $G$ .

8.1. PROPOSITION. (a) *Let  $b \in P$  and  $\sigma \in G$ . Then  $\xi_b(\sigma) = V_{ba_\sigma}$  (considered in  $\mathbb{Z}_p$ ). In particular, if  $b \notin P^*$ , then  $[S_b] \in \ker \theta$ .*

(b) *Let  $a \in P^*$  and denote  $\mathcal{U}_a = \{\sigma \in G: O^p(H_a) \lesssim \langle \sigma \rangle \lesssim H_a\}$ . Then  $\theta(e_a)$  is the indicator function of the set  $\mathcal{U}_a$ . In particular,  $e_a \notin \ker \theta$  if and only if  $H_a$  is  $p$ -hypercyclic.*

*Proof.* (a) Let  $m = (1/|H_b|) |\{\tau \in G: \sigma\tau H_b = \tau H_b\}|$ , then by definition  $\xi_b(\sigma)$  equals  $m$  reduced modulo  $p$ . But  $\sigma\tau H_b = \tau H_b$  if and only if  $\langle \sigma \rangle^\tau \leq H_b$ , so that  $m = V_{ba_\sigma}$ , which is the first statement. The second statement now follows from 3.2.

(b) Let  $\sigma \in G$ , then by 5.5 we have  $\theta(e_a)(\sigma) = \theta(\sum_b \lambda_{ab}[S_b])(\sigma) = \sum_b \lambda_{ab} V_{ba_\sigma} = W_{aa_\sigma}$ . Apply 5.5(c) and 7.3 to get the first statement. Finally,  $e_a \notin \ker \theta$  if and only if  $\mathcal{U}_a$  is nonempty if and only if  $O^p(H_a)$  is cyclic if and only if  $H_a$  is  $p$ -hyperelementary. ■

It will be helpful to have another description of the sets  $\mathcal{U}_a$ . Towards this we define, for any  $p$ -regular element  $x$  of  $G$ , the set  $\mathcal{L}_x = \{\sigma \in G: \langle \sigma' \rangle \sim \langle x \rangle\}$ , where  $\sigma'$  denotes the  $p$ -prime part of  $\sigma$  (see [5]).

8.2. PROPOSITION. (a) *Let  $a \in P^*$  be such that  $e_a \notin \ker \theta$ , and let  $x \in G$  be any generator of the cyclic  $p'$ -group  $O^p(H_a)$ . Then  $\mathcal{U}_a = \mathcal{L}_x$ .*

(b) *Conversely, for any  $p$ -regular  $x \in G$ , there exists a unique  $a \in P^*$  such that  $\langle x \rangle \sim O^p(H_a)$ , and for this  $a$ ,  $\mathcal{U}_a = \mathcal{L}_x$ .*

*Proof.* (a) Choose  $b \in P$  with  $H_b \sim O^p(H_a)$ . If  $\sigma \in \mathcal{U}_a$ , then  $H_b \lesssim \langle \sigma \rangle$ , hence  $\langle \sigma' \rangle \sim H_b \sim \langle x \rangle$  implies  $\sigma \in \mathcal{L}_x$ . Conversely, if  $\sigma \in \mathcal{L}_x$  then  $H_b \sim \langle \sigma' \rangle \leq \langle \sigma \rangle$ . Choose  $c \in P^*$  with  $a_\sigma \in \text{supp}(c)$ . Then by 7.3,  $b \in \text{supp}(c) \cap \text{supp}(a)$ , whence  $c = a$  by 5.1. Thus  $a_\sigma \leq a$ , so  $\langle \sigma \rangle \lesssim H_a$ . By definition,  $\sigma \in \mathcal{U}_a$ .

(b) Say  $\langle x \rangle \sim H_b$ , some  $b \in P$ , and choose  $a \in P^*$  with  $b \in \text{supp}(a)$ . Obviously,  $H_b \sim O^p(H_a)$ , and by part (a),  $\mathcal{U}_a = \mathcal{L}_x$ . Uniqueness follows directly from 5.1. ■

This proposition has a consequence the following modular version of the main theorem of Gluck [5].

8.3. THEOREM. *Let  $p$  be a prime dividing  $|G|$ . Then for any  $p$ -regular  $x \in G$ , the indicator function  $I_{\mathcal{L}_x}$  is in the image of  $\theta$ . In particular we may write  $I_{\mathcal{L}_x} = \sum_H u_H 1_H^G$ ,  $u_H \in \mathbb{Z}_p$ , where the sum ranges over  $p$ -hyperelementary subgroups  $H$  satisfying  $p \nmid (N_G(H): H)$  and  $H \lesssim H_a$ , where  $a \in P^*$  is such that  $\mathcal{U}_a = \mathcal{L}_x$ .*

*Proof.* Let  $a \in P^*$  be as in 8.2(b). Since  $\mathcal{U}_a = \mathcal{L}_x$  is nonempty,  $H_a$  and all subconjugate subgroups are  $p$ -hyperelementary. Then,  $I_{\mathcal{L}_x} = I_{\mathcal{U}_a} = \theta(e_a) = \theta(\sum_{b \leq a} \lambda_{ab}[S_b]) = \sum_{b \leq a, b \in P^*} \lambda_{ab} \xi_b$ . A change of notation gives the result. ■

We now describe the image of  $\theta$ . Call a character  $\chi: G \rightarrow \mathbb{Z}_p$   $p$ -constant if whenever  $\sigma, \tau \in G$  with  $\langle \sigma' \rangle \sim \langle \tau' \rangle$ , then  $\chi(\sigma) = \chi(\tau)$ . The essence of the Artin induction theorem is that the corresponding property holds for rational characters [1, Lemma 39.4], however, it is easy to discover  $\mathbb{Z}_p$ -characters that are not  $p$ -constant. Nevertheless, it is clear that sums and products of  $p$ -constant characters are again  $p$ -constant, and we obtain

8.4. THEOREM. *The image of  $\theta$  is the subring of  $X(G, p)$  consisting of the  $p$ -constant characters.*

*Proof.*  $\subseteq$  By 5.4 and 8.1(a), it suffices to show that  $\theta([S_a] e_a)$  is  $p$ -constant for any  $a \in P^*$ . Choose  $x \in G$  as in 8.2, and let  $\sigma, \tau \in G$  be such that  $\langle \sigma' \rangle \sim \langle \tau' \rangle$ . If  $\sigma \notin \mathcal{L}_x$  then plainly  $\tau \notin \mathcal{L}_x$ , hence  $\theta([S_a] e_a)(\sigma) = \theta([S_a] e_a)(\tau) = 0$  in this case. Assume  $\sigma, \tau \in \mathcal{L}_x$ . Then by 7.1,  $\theta([S_a] e_a)(\sigma) = \xi_a(\sigma) = V_{aa_\sigma} = V_{aa_{\sigma'}} = V_{aa_{\tau'}} = V_{aa_\tau} = \xi_a(\tau) = \theta([S_a] e_a)(\tau)$ .

$\supseteq$  If  $\chi$  is a  $p$ -constant character of  $G$ , then by definition  $\chi$  is constant on each of the sets  $\mathcal{L}_x$  for  $p$ -regular  $x \in G$ , hence on each of the sets  $\mathcal{U}_a$ ,  $a \in P^*$ . Say  $\chi(\mathcal{U}_a) = n_a \in \mathbb{Z}_p$  ( $n_a := 0$  if  $\mathcal{U}_a$  is empty). Then  $\chi = \chi \cdot 1 = \chi \cdot \theta(\sum_{a \in P^*} e_a) = \sum_{a \in P^*} \chi \cdot I_{\mathcal{U}_a} = \sum_{a \in P^*} n_a I_{\mathcal{U}_a} = \theta(\sum_{a \in P^*} n_a e_a) \in$  image of  $\theta$ .  $\blacksquare$

Finally, as a corollary of this result and 8.3, we obtain the following modular version of the Artin induction theorem.

8.5. THEOREM. *Any  $p$ -constant character  $\chi: G \rightarrow \mathbb{Z}_p$  is a  $\mathbb{Z}_p$ -linear combination  $\chi = \sum_H u_H 1_H^G$ , where  $H$  ranges over those  $p$ -hyerelementary subgroups of  $G$  such that  $p \nmid (N_G(H): H)$ .*

#### REFERENCES

1. C. W. CURTIS AND I. REINER, "Representation Theory of Finite Groups and Associative Algebras," Pure and Appl. Math., Vol. 11, Interscience, New York, 1962.
2. A. DRESS, A characterization of solvable groups, *Math. Z.* **110** (1969), 213–217.
3. A. DRESS, "Notes on the Theory of Representations of Finite Groups. Part I. The Burnside Ring of a Finite Group and some AGN-Applications," multicopied notes, Universität Bielefeld, 1971.
4. D. GLUCK, Idempotent formula for the Burnside algebra with applications to the  $p$ -subgroup simplicial complex, *Illinois J. Math.* **25** (1981), 63–67.
5. D. GLUCK, A character table bound for the Schur index, *Illinois J. Math.* **25** (1981), 649–653.
6. W. H. GUSTAFSON, Burnside rings which are Gorenstein, *Comm. Algebra* **5** (1977), 1–15.
7. R. S. PIERCE, "Associative Algebras," Graduate Texts in Mathematics, Vol: 88, Springer-Verlag, Berlin/Heidelberg/New York, 1982.
8. R. RAGHAVENDRAN, Finite associative rings, *Compositio Math.* **21** (1969), 195–229.
9. L. SOLOMON, The Burnside algebra of a finite group, *J. Combin. Theory* **2** (1967), 603–615.