The Burnside Algebra of a Finite Group

LOUIS SOLOMON

New Mexico State University,
University Park, New Mexico 88070

Communicated by Gian - Carlo Rota

ABSTRACT

Let $G$ be a finite group. The isomorphism classes of $G$-sets generate a commutative ring $B[G]$ which we call the Burnside ring of $G$. We prove that $B[G] \otimes \mathbb{Q}$ is a semisimple algebra over $\mathbb{Q}$ and that formulas for certain primitive idempotents of this algebra yield the theorem of Artin on rational characters in an explicit form due to Brauer. The proof uses an isomorphism between $B[G] \otimes \mathbb{Q}$ and an algebra defined by the Möbius function of the partially ordered set of conjugacy classes of subgroups of $G$.

1. INTRODUCTION

Let $G$ be a finite group. A finite set $X$ is a $G$-set if there is given a mapping $(\sigma, x) \rightarrow \sigma x$ from $G \times X$ into $X$ such that $\sigma(\tau x) = (\sigma \tau)x$ and $1x = x$, for all $\sigma, \tau \in G$ and $x \in X$. Thus a $G$-set amounts to a finite set $X$ together with a representation of $G$ in the group of permutations of $X$. Each subgroup $H$ of $G$ defines a $G$-set $X_H$ whose elements are the left cosets mod $H$. The isomorphism classes of $G$-sets may be added and multiplied in natural fashion and generate a commutative ring $B[G]$ which, since it seems to have been defined for the first time in Burnside’s book [3, Secs. 184–5], we call the Burnside ring of $G$.

Every $G$-set $X$ defines a representation of $G$ in $G L (n, \mathbb{Q})$ and hence

---

1 This work was supported in part by the National Science Foundation under grant GP 6080. The author would also like to thank the Warwick Algebra Symposium for its hospitality.
defines a rational character of $G$. Isomorphic $G$-sets define the same character and the mapping which assigns to each isomorphism class its character, defines a ring homomorphism

$$\text{char}: \mathcal{B}[G] \rightarrow \mathcal{Z}[G]$$

of $\mathcal{B}[G]$ into the ring $\mathcal{Z}[G]$ of rational characters of $G$. It is no easy matter to describe the image of this homomorphism and very little is known about it. On the other hand if one is willing to consider the algebras $\mathcal{B}_Q[G] = \mathcal{B}[G] \otimes \mathbb{Q}$ and $\mathcal{Z}_Q[G] = \mathcal{Z}[G] \otimes \mathbb{Q}$ over the rational field $\mathbb{Q}$, then the problem is a tractable one and one knows that the mapping $\text{char} : \mathcal{B}_Q[G] \rightarrow \mathcal{Z}_Q[G]$, is an epimorphism. In fact, a theorem of Artin [1, 4] states that $\mathcal{Z}_Q[G]$ is the image, under char, of the subalgebra of $\mathcal{B}_Q[G]$ spanned over $\mathbb{Q}$ by those isomorphism classes of $G$-sets which are defined by cyclic subgroups $H$ of $G$. Alternatively, every rational character of $G$ is a linear combination with rational coefficients, of permutation characters defined by cyclic subgroups.

In this paper we stick to the easy case and show Artin's theorem is a consequence of general facts about $\mathcal{B}_Q[G]$. We prove that $\mathcal{B}_K[G] = \mathcal{B}[G] \otimes K$ is a semisimple algebra for any field $K$ of characteristic zero or prime to the order $|G|$ of $G$. If $K = \mathbb{Q}$, the argument yields a description of the kernel (and image) of char as well as a formula for certain primitive idempotents in $\mathcal{B}_Q[G]$. This formula passes, under char, into a formula of Brauer [2] which refines Artin's theorem by expressing any rational character as an explicit linear combination of permutation characters defined by cyclic subgroups.

The proofs hinge on definition of a semisimple algebra $\mathcal{M}_K[P]$ which we associate with any finite partially ordered set $P$ and field $K$, and which, for reason apparent in its definition, we call the Möbius algebra of $P$ over $K$. In case $P$ is the set of conjugacy classes of subgroups of $G$, partially ordered in natural fashion, it turns out that there is a canonical isomorphism $\mathcal{B}_K[G] \simeq \mathcal{M}_K[P]$, whenever the characteristic of $K$ is zero or prime to $|G|$, and this determines the structure of $\mathcal{B}_K[G]$.

2. The Möbius Algebra

Let $P$ be a finite partially ordered set. The Möbius function $\mu$ of $P$ is a function from $P \times P$ to the ring $\mathbb{Z}$ of integers defined [5] recursively as follows: $\mu(a, b) = 0$ unless $a \leq b$, while for $a \leq b$, $\mu(a, b)$ is defined...
THE BURNSIDE ALGEBRA OF A FINITE GROUP

recursively by either of the two equivalent [5] formulas

\[ \sum_{a \leq c \leq b} \mu(a, c) = \delta_{a,b}, \]
\[ \sum_{a \leq c \leq b} \mu(c, b) = \delta_{a,b}. \]

Let \( \mathcal{M}[P] \) be the free \( \mathbb{Z} \)-module which has the elements of \( P \) for basis. If \( P \) is a lattice, we may define a product \( ab \) of elements of \( P \) by \( ab = a \cap b \), and then extending the definition of multiplication to \( \mathcal{M}[P] \) by linearity we see that \( \mathcal{M}[P] \) has an invariantly defined structure of commutative ring. The following theorem asserts that an analogous ring structure exists in \( \mathcal{M}[P] \) whether \( P \) is a lattice or not.

**Theorem 1.** Let \( P \) be a finite partially ordered set. Let \( \mu \) be the Möbius function of \( P \). For each pair \((a, b)\) of elements of \( P \), define a function \( \varphi_{a,b} : P \to \mathbb{Z} \) by

\[ \varphi_{a,b}(p) = \sum_{q \in P_{a,b}} \mu(p, q), \quad p \in P, \]

where \( P_{a,b} \) is the set of all elements \( q \in P \) such that \( q \leq a \) and \( q \leq b \). Define

\[ ab = \sum_{p \in P} \varphi_{a,b}(p)p, \]

and extend the definition of product to \( \mathcal{M}[P] \) by linearity. Then \( \mathcal{M}[P] \) is a commutative ring isomorphic to a direct sum of copies of \( \mathbb{Z} \) which we call the Möbius ring of \( P \). If \( K \) is a field, then the Möbius algebra \( \mathcal{M}_K[P] = \mathcal{M}[P] \otimes K \) is a semisimple algebra over \( K \), and its primitive idempotents are \( e_a \otimes 1 \) where

\[ e_a = \sum_{b \in P} \mu(b, a)b, \quad a \in P. \]

**Proof:** Certainly the multiplication is commutative since \( P_{a,b} = P_{b,a} \). The associativity of the multiplication will follow from properties of the \( e_a \).

The zeta function of \( P \) [5] is a function \( \zeta : P \times P \to \mathbb{Z} \) defined by \( \zeta(a, b) = 1 \) if \( a \leq b \) and \( \zeta(a, b) = 0 \) otherwise. Define for each \( c \in P \), a \( \mathbb{Z} \)-linear mapping

\[ \zeta_c : \mathcal{M}[P] \to \mathbb{Z} \]
by

$$\eta_e(a) = \zeta(c, a), \quad a \in P.$$ 

Then for $a, b \in P$

$$\eta_e(ab) = \sum_{p \in P} \eta_{a,b}(p) \zeta(c, p)$$
$$= \sum_{q \in P} \sum_{p \in P} \zeta(c, p) \mu(p, q)$$
$$= \sum_{q \in P} \delta_{c,q} = \zeta_e(a) \zeta_e(b),$$

so that $\zeta_e$ is a homomorphism of $\mathcal{M}[P]$ into $\mathbb{Z}$. Suppose all $\zeta_e$ annihilate some $x \in \mathcal{M}[P]$. Then $x = \sum_{a \in P} \psi(a) a$ for suitable $\psi(a) \in \mathbb{Z}$, where $0 = \sum_{a \in P} \psi(a)$ for all $c \in P$. Since $P$ is finite it has maximal elements $c$ and for any such $c$ we conclude $\psi(c) = 0$. It follows by descending induction on $a$, that $\psi(a) = 0$ for all $a \in P$ and hence $x = 0$. Thus if $x, y \in \mathcal{M}[P]$ and $\zeta_e(x) = \zeta_e(y)$ for all $c \in P$, we have $x = y$. Now define $e_a \in \mathcal{M}[P]$ as in the statement of the theorem. Then for $a, c \in P$ and $x \in \mathcal{M}[P]$

$$\eta_e(xe_a) = \zeta_e(x) \zeta_e(e_a) = \zeta_e(x) \delta_{a,c} = \zeta_e(\zeta_a(x)e_a),$$

so that by our previous remark

$$xe_a = \zeta_a(x)e_a, \quad a \in P, \ x \in \mathcal{M}[P].$$

Thus $e_b a = \zeta_a(e_b) e_a = \delta_{a,b} e_a$, so that the $e_a$ are pairwise orthogonal idempotents of $\mathcal{M}[P]$. Let $e = \sum_{a \in P} e_a$. Then $\zeta_e(b e) = \zeta_e(b) \zeta_e(e) = \zeta_e(b)$ for all $c \in P$ so that $b e = b$ and $e$ is thus an identity element for $\mathcal{M}[P]$. Thus given $x \in \mathcal{M}[P]$ we may write

$$x = xe = \sum_{a \in P} \zeta_a(x) e_a.$$

Now the orthogonality of the idempotents shows for any $x, y, z \in \mathcal{M}[P]$ that

$$(xy)z = \sum_{a \in P} \zeta_a(x) \zeta_a(y) \zeta_a(z) e_a = x(yz),$$

so the multiplication is associative and $\mathcal{M}[P]$ is indeed a commutative ring isomorphic to the direct sum of the $\mathbb{Z} e_a$. If $K$ is a field then

$$\mathcal{M}_K[P] = \sum_{a \in P} K(e_a \otimes 1)$$

is certainly semisimple and the proof is complete.
Note that if \( a \cap b \) exists for a particular pair \((a, b)\) then

\[
\varphi_{a,b}(p) = \sum_{p \leq q \leq a \cap b} \mu(p, q) = \begin{cases} 1 & \text{if } p = a \cap b, \\ 0 & \text{otherwise,} \end{cases}
\]

so that \( ab = a \cap b \). Thus if \( P \) has a unique maximal element \( m \), then \( ma = m \cap a = a \) for all \( a \in P \) so that \( m \) is the identity of \( \mathcal{A}[P] \).

3. The Burnside Algebra

Let \( G \) be a finite group. Two \( G \)-sets \( X, Y \) are isomorphic if there exists a one-to-one map \( \theta \) from \( X \) onto \( Y \) such that \( \theta(\sigma x) = \sigma(\theta x) \) for all \( x \in X \) and \( \sigma \in G \). The product \( X \times Y \) becomes a \( G \)-set if we define \( \sigma(x, y) = (\sigma x, \sigma y) \). We say that \( X \) is transitive if \( X = Gx \) for some \( x \in X \). Any \( G \)-set \( X \) may be written as a disjoint union of uniquely determined transitive \( G \)-sets, the orbits of \( X \) under \( G \). Any subgroup \( H \) of \( G \) defines a transitive \( G \)-set \( X_H \) whose elements are the left cosets mod \( H \), with \( \sigma(\tau H) \) defined as \( (\sigma \tau)H \). Conversely, if \( X \) is a transitive \( G \)-set and \( x \) is any element of \( X \), then \( X \) is isomorphic to \( X_H \), where \( H \), the stabilizer of \( x \), consists of the elements of \( G \) which fix \( x \). Two subgroups define isomorphic \( G \)-sets if and only if they are conjugate in \( G \).

Let \( P \) be the set of all conjugacy classes of subgroups of \( G \). Let \( \mathcal{B}[G] = \sum_{a \in P} \mathbb{Z}x_a \) be the free Abelian group generated by symbols \( x_a \) in one-to-one correspondence with the elements \( a \) of \( P \). For each \( a \in P \) choose a subgroup \( H_a \) in the class \( a \). Let \( X_a \) be the corresponding \( G \)-set and for \( a, b, c \in P \) let \( \nu_{a,b,c} \) be the number of orbits of \( X_a \times X_b \) under \( G \) which are isomorphic to \( X_c \). This number depends only on \( a, b, c \) and not on the subgroups \( H_a, H_b, H_c \). Then defining products

\[
x_a x_b = \sum_{c \in P} \nu_{a,b,c} x_c
\]

of the basis elements, and extending the definition to \( \mathcal{B}[G] \) by linearity, gives \( \mathcal{B}[G] \) the structure of commutative ring, which we call the Burnside ring of \( G \). The elements \( \sum_{a \in P} \kappa_a x_a, \kappa_a \geq 0 \), correspond to the isomorphism classes of \( G \)-sets and one may thus view the \( x_a \) as the isomorphism classes of transitive \( G \)-sets. These are elementary facts about permutation groups, and proofs are in Burnside's book [3]. If \( K \) is a field, we call \( \mathcal{B}_K[G] = \mathcal{B}[G] \otimes K \) the Burnside algebra of \( G \) over \( K \).

Define a partial ordering in \( P \) as follows. Write \( b \preceq a \) if \( H_b \) is conjugate
in $G$ to a subgroup of $H_a$. This ordering depends only on $P$ and not on the chosen subgroups $H_a$. For $a, b \in P$ let 

$$P_a = \{p \in P | p \leq a\},$$

let 

$$Q_a = \{p \in P | p < a\}$$

and let 

$$P_{a,b} = \{p \in P | p \leq a \text{ and } p \leq b\}.$$ 

**Lemma 1.** 

$$x_a x_b \equiv 0 \pmod{\sum_{p \in P_{a,b}} ZX_p}.$$ 

**Proof:** It follows from the definition that $v_{a,b,c}$ is $|G:H_c|^{-1}$ times the number of elements in $X_a \times X_b$ with stabilizer conjugate to $H_c$. The stabilizer of an element $(\alpha H_a, \beta H_b) \in X_a \times X_b$ is $\alpha H_a \alpha^{-1} \cap \beta H_b \beta^{-1}$. This group can be conjugate to $H_p$ only if $p \leq a$ and $p \leq b$. The lemma is proved.

We write $v_{a,b} = v_{a,b,b}$ and $v_a = v_{a,a,a}$.

**Lemma 2.** If $b \leq a$ then 

$$x_a x_b \equiv v_{a,b} x_b \pmod{\sum_{p \in Q_b} ZX_p},$$

where $v_{a,b}$ is a positive integral divisor of $|G|$. If $N_a$ is the normalizer of $H_a$ in $G$ then $v_a = |N_a : H_a|$.

**Proof:** We may replace $H_b$ by a conjugate if necessary, so it is no restriction to assume $H_b \leq H_a$. Since $b \leq a$, Lemma 1 implies 

$$x_a x_b \equiv v_{a,b} x_b \pmod{\sum_{p \in Q_b} ZX_p}$$

where $v_{a,b}$ is $|G:H_b|^{-1}$ times the number of elements $(\alpha H_a, \beta H_b) \in X_a \times X_b$ such that $\alpha H_a \alpha^{-1} \cap \beta H_b \beta^{-1}$ is conjugate to $H_b$. Such conjugacy occurs if and only if $\beta H_b \beta^{-1} \leq \alpha H_a \alpha^{-1}$, or, in other words, if and only if $\alpha^{-1} \beta \in N_{b,a}$, where $N_{b,a} \supseteq H_a$ is the subgroup of all $\sigma \in G$ such that $\sigma H_0 \sigma^{-1} \subseteq H_a$. Let $q_1, ..., q_r$ represent the left cosets of $G$ mod $N_{b,a}$, let $\sigma_1, ..., \sigma_s$ represent the left cosets of $N_{b,a}$ mod $H_a$, and let $\tau_1, ..., \tau_t$ represent the left cosets of $H_a$ mod $H_b$. Then 

$$G = \bigcup q_i \sigma_j H_a \quad G = \bigcup q_k \sigma_l H_b$$

where $i, k = 1, ..., r$; $j, l = 1, ..., s$; and $m = 1, ..., t$. Now
so that $v_{a,b} = rs^at/rst = |N_{b,a}:H_a|$ is a positive integral divisor of $|G|$. In case $b = a$, $N_{b,a}$ is the normalizer of $H_a$, and this completes the proof.

**Theorem 2.** Let $G$ be a finite group and let $K$ be a field of characteristic zero or prime to $|G|$. Let $P$ be the set of conjugacy classes of subgroups of $G$, partially ordered in the natural way. Then there is a canonical isomorphism of the Burnside algebra $B_K[G]$ with the Möbius algebra $\mathbb{M}_K[P]$.

**Proof:** Let $y_a = x_a \otimes 1$. Then the $y_a$ are a $K$-basis for $\mathbb{K}[G]$. Let

$$U_a = \sum_{p \in P_a} Ky_p \quad \text{and} \quad V_a = \sum_{p \in Q_a} Ky_p.$$ 

By Lemma 1, multiplication by $y_a$ defines a $K$-linear mapping $\lambda_a$ of $U_a$ into $U_a$. Number the elements of $P_a$ as $a_1, ..., a_r$ in such a way that $a_i < a_j$ implies $i < j$. Such numbering is clearly possible in any finite partially ordered set. Then, by Lemma 2, the matrix for $\lambda_a$ in the basis $y_{a_1}, ..., y_{a_r}$ is triangular, with diagonal entries either $v_{a_i}, ..., v_{a_r}$, or $v_{a_1}, ..., v_{a_r}$ reduced modulo the prime characteristic of $K$. In view of our assumption on the characteristic, it follows that $\lambda_a$ is a non-singular linear transformation of $U_a$. Thus there exists a unique element $u_a \in U_a$ such that $y_au_a = y_a$.

Let $b \leq a$ and suppose we have shown that $y_cu_a = y_c$ for all $c < b \leq a$. Then the congruence $y_au_b \equiv v_{a,b}y_b \mod V_b$, of Lemma 2, shows that $(y_au_b - v_{a,b}y_b)u_a = y_au_b - v_{a,b}y_b$ whence, by our assumption on the characteristic, it follows that $y_au_b = y_b$. Thus we conclude by ascending induction on $b$ that $y_bu_a = y_b$ for all $b \leq a$. Thus $u_a$ is an identity element for $U_a$ and in particular, $u_bu_a = u_b$ for all $b \leq a$.

Since $y_au_a = y_a \not\in V_a$, it follows from Lemma 1 that $u_a \not\in V_a$ whence by ascending induction on $a$ we see that the $u_b$ with $b \leq a$ span $u_a$, and hence that the $u_a$ span $B_K[G]$. Since their number is equal to the dimension of $B_K[G]$ over $K$, the $u_a$ are a basis for $B_K[G]$ over $K$.

Thus we may write, for any $a, b \in P$

$$u_au_b = \sum_{p \in P} \psi_{a,b}(p)u_p,$$

where the $\psi_{a,b}$ are well-defined functions from $P$ into $K$ which we proceed to determine. By Lemma 1, $\psi_{a,b}(p) = 0$ if $p \not\in P_{a,b}$. Let $q \in P$ and suppose first that $q \in P_{a,b}$. Then $u_au_bu_q = u_q$ so
\[ u_q = \sum_{p \in P} \psi_{a,b}(p)u_pq. \]

Now we may write
\[ u_pq = \sum_{r \in P} \psi_{p,q}(r)u_r. \]

If \( \psi_{p,q}(q) \neq 0 \) we must have \( q \in P_{p,q} \) whence \( q \leq p \) so \( u_pq = u_q \). Thus, comparing coefficients of \( u_q \) in our formula for \( u_q \) above, we have
\[ 1 = \sum_{q \leq p} \psi_{a,b}(p) \quad \text{if} \quad q \in P_{a,b}. \]

On the other hand, if \( q \notin P_{a,b} \) and \( p \geq q \) then \( p \notin P_{a,b} \) so
\[ 0 = \sum_{q \leq p} \psi_{a,b}(p) \quad \text{if} \quad q \notin P_{a,b}. \]

Thus, if we define a function \( \theta_{a,b} : P \to K \) by \( \theta_{a,b}(q) = 1 \) if \( q \in P_{a,b} \) and \( \theta_{a,b}(q) = 0 \) otherwise, we have
\[ \theta_{a,b}(q) = \sum_{q \leq p} \psi_{a,b}(p). \]

\[ \phi_{a,b}(q) = \sum_{q \leq p} \mu(q, p)\theta_{a,b}(p) = \phi_{a,b}(q) \]

where \( \phi_{a,b} \) is the function which defines the multiplication in the Möbius algebra. Thus the mapping \( u_a \to a \otimes 1, \ a \in P \), defines an isomorphism of \( \mathbb{P}_K[G] \) onto \( \mathcal{M}_K[P] \) which certainly merits the adjective "canonical," since \( u_a \) is invariably defined by \( x_a \). The proof is complete.

**Corollary.** Let \( G \) be a finite group and let \( K \) be a field of characteristic zero or prime to \( |G| \). Then the Burnside algebra \( \mathbb{P}_K[G] \) is semisimple.

### 4. Rational Characters

A rational character of \( G \) is the character of a representation of \( G \) in \( \text{GL}(n, \mathbb{Q}) \).\(^2\) Beyond the bare definition we require only one fact [4, Lemma 39.4], which is a direct consequence of the definition and an ele-

\(^2\) For Artin, a rational character is a rational valued character of a representation in \( \text{GL}(n, \mathbb{C}) \). This distinction is important for some purposes but is irrelevant here.
mentary field theoretic argument: if $\chi$ is a rational character and $\sigma \in G$, then $\chi(\sigma^k) = \chi(\sigma)$ for any integer $k$ prime to the order of $\sigma$. The ring $\mathcal{Z}[G]$ is by definition the ring of all $\mathbb{Z}$-linear combinations of rational characters. We identify $\mathcal{Z}_Q[G] = \mathcal{Z}[G] \otimes Q$ with the algebra of all $Q$-linear combinations of rational characters, so that $\mathcal{Z}[G]$ is a subring of $\mathcal{Z}_Q[G]$. We also view $\mathcal{Z}[G]$ as a subring of $\mathcal{Z}_Q[G]$ so that $x_a = y_a$. Our aim is to study the homomorphism $\text{char}$ by computing its effect on the primitive idempotents of $\mathcal{Z}_Q[G]$.

Let $u_a$ be the element defined in the proof of Theorem 2 and write

$$u_a = \sum_{b \leq a} \lambda_{b, a} x_b$$

for suitable $\lambda_{b, a} \in Q$. Since $x_a = x_a u_a$, Lemma 1 implies

$$x_a \equiv \lambda_{a, a} x_a^2 \mod V_a.$$  

But Lemma 2 says

$$x_a^2 \equiv |N_a : H_a| x_a \mod V_a$$

so that $\lambda_{a, a} = |N_a : H_a|^{-1}$ and thus

$$u_a \equiv |N_a : H_a|^{-1} x_a \mod V_a.$$  

Let $e_a = \sum_{b \leq a} \mu(b, a) u_b$ be the primitive idempotent of $\mathcal{Z}_Q[G]$ defined by the construction of Theorem 1 and the isomorphism of Theorem 2. Since $\mu(a, a) = 1$ our formula for $u_a$ implies

$$e_a = |N_a : H_a|^{-1} x_a + \sum_{b < a} \lambda_{b, a} x_b$$

for suitable $\lambda_{b, a} \in Q$. Thus

$$\text{char } e_a = |N_a : H_a|^{-1} \xi_b + \sum_{b < a} \lambda_{b, a} \xi_b,$$

where $\xi_b$ is the character defined by the $G$-set consisting of cosets mod $H_b$. Since $\xi_b(\sigma)$ is the number of cosets fixed by $\sigma$, $\xi_b(\sigma) = |H_b|^{-1} \sum_{\tau} 1$, $\sigma \in G$, where the sum is over all $\tau \in G$ such that $\tau^{-1} \sigma \tau \in H_b$.

Let $Z$ be the subset of all $a \in P$ such that $H_a$ is cyclic. Choose, for each $a \in Z$, a generator $\sigma_a$ of $H_a$. Since $\tau^{-1} \sigma_a \tau \in H_b$ is impossible for
b < a we have \( \xi_b(\sigma_a) = 0 \) in that case, while \( \tau^{-1}\sigma_a\tau \in H_a \) if and only if \( \tau \in N_a \), so that \( \xi_a(\sigma_a) = |N_a : H_a| \). Thus

\[
(\text{char } e_a)(\sigma_a) = 1 \quad \text{if } a \in Z.
\]

Since char is a homomorphism, the elements char \( e_a \) are idempotents of \( \mathcal{F}_Q[G] \) and thus, being functions on \( G \), assume only the values 0, 1. Let

\[
e = \sum_{a \in Z} \text{char } e_a.
\]

Then, since \( e \) is also an idempotent, we have

\[
1 \geq e(\sigma_b) = \sum_{a \in Z} (\text{char } e_a)(\sigma_b) \geq (\text{char } e_b)(\sigma_b) = 1
\]

for any \( b \in Z \), whence \( (\text{char } e_a)(\sigma_b) = \delta_{a,b} \) for any \( a, b \in Z \).

Let \( K_a, a \in Z \), be the collection of all elements \( \sigma \in G \) such that \( \sigma \) generates a group conjugate to \( H_a \). Then

\[
G = \bigcup_{a \in Z} K_a
\]

is a disjoint union. Let \( \varepsilon_a \) be the function on \( G \) which is 0 on \( K_a \) and 1 elsewhere. By the aforementioned lemma of [4], char \( e_a \) is constant on the sets \( K_a \), whence we conclude from \( (\text{char } e_a)(\sigma_b) = \delta_{a,b} \) that char \( e_a = \varepsilon_a \), and that \( e \) is the function everywhere equal to 1. In particular, \( \varepsilon_a \in \mathcal{F}_Q[G] \) and the lemma of [4] implies now that the \( e_a, a \in Z \), are a \( Q \)-basis for \( \mathcal{F}_Q[G] \). Thus

\[
\text{char}: \mathcal{F}_Q[G] \to \mathcal{F}_Q[G]
\]

is an epimorphism. This much is Artin's theorem. Now \( \sum_{a \in P} e_a \) is the identity of \( \mathcal{P}_Q[G] \) and must map under the epimorphism char into the identity \( \varepsilon = \sum_{a \in Z} \text{char } e_a \) of \( \mathcal{F}_Q[G] \). Thus

\[
0 = e - \varepsilon = \sum_{a \notin Z} \text{char } e_a.
\]

But again, the char \( e_a \) assume only the values 0, 1 so char \( e_a = 0 \) for \( a \notin Z \). We summarize the results, as

**Theorem 3.** Let \( G \) be a finite group. Let \( P \) be the set of all conjugacy classes of subgroups of \( G \). Choose for each \( a \in P \), a subgroup \( H_a \) in the class \( a \). Let \( e_a \) be the primitive idempotent of \( \mathcal{P}_Q[G] \) which our construction
assigns to a. Let Z be the set of all a ∈ P for which H_a is cyclic. For each a ∈ Z let K_a be the set of elements of G which generate a subgroup conjugate to H_a, and let ε_a : G → Z be the function equal to 1 on K_a and 0 elsewhere. Then

\[ \text{char } e_a = \begin{cases} 
\epsilon_a, & \text{if } H_a \text{ is cyclic,} \\
0, & \text{otherwise.} 
\end{cases} \]

Thus char defines an isomorphism of algebras

\[ \sum_{a \in Z} Qx_a \simeq \mathcal{D} Q[G], \]

where x_a is the isomorphism class of G-sets defined by H_a, and the kernel of char is \( \sum_{a \in Z} Qe_a \).

**THEOREM 4.** If H_a is cyclic, then

\[ e_a = \frac{1}{N_a |} \sum_{c \leq a} \mu(c, a) | H_c | x_c. \]

**PROOF:** Following [2], let the right-hand side be denoted \( e'_a \). For c ∈ Z direct computation gives

\[ \xi_c(\sigma_b) = \frac{1}{|H_c|} \sum_{r^{-1} \in H_c} 1 = \begin{cases} 
N_b : H_c & \text{if } b \leq c \\
0 & \text{otherwise} 
\end{cases} \]

Thus

\[ (\text{char } e'_a)(\sigma_b) = \frac{1}{N_a |} \sum_{c \leq a} \mu(c, a) | H_c | \xi_c(\sigma_b) \]

\[ = \frac{|N_b|}{|N_a|} \sum_{b \leq c} \mu(c, a) = \delta_{a,b} = (\text{char } e_a)(\sigma_b) \]

Since both \( e_a \) and \( e'_a \) are in \( \sum_{a \in Z} Qx_a \) we conclude from Theorem 3 that \( e'_a = e_a \) and the proof is complete.

Note then that for any \( \chi \in \mathcal{D} Q[G] \) we may write

\[ \chi = \sum_{a \in Z} \chi(\sigma_a)e_a = \sum_{a \in Z} \frac{\chi(\sigma_a)}{N_a} \sum_{c \leq a} \mu(c, a) | H_c | \xi_c \]

as an explicit linear combination of the permutation characters \( \xi_c \). To see that this is the formula Brauer has given in [2], one must remark
that, for a cyclic group \( H_a \), the partially ordered set \( P_a \) is isomorphic to the lattice of divisors of the integer \( |H_a| \) and that \( \mu(c, a) = \mu(|H_a: H_c|) \) where \( \mu \) on the right is the Möbius function of elementary number theory.

**Theorem 5.** Let \( G \) be a finite group. Let \( A \supseteq B \supseteq C \) be cyclic subgroups of \( G \). Then

\[
\frac{|C|}{|A||B|} \sum_{\emptyset \neq D \supseteq B} \mu(|D : C|) |N(D)|
\]

is a non-negative integer, where \( \mu \) is the Möbius function of elementary number theory, \( N(D) \) is the normalizer of \( D \) in \( G \), and the sum is over all subgroups \( D \) which lie between \( C \) and \( B \).

**Proof:** The argument succeeds because we may compute the constants \( v_{a,b,c} \) when \( H_a \) is cyclic and \( b \leq a \). So let \( H_a \) be cyclic and define \( \omega_c \in \mathfrak{X}_Q[G] \) for \( c \leq a \) by

\[
\omega_c = \sum_{c \leq d \leq a} \mu(c, d) |K_d|^{-1} N_d|^{-1} \varepsilon_d.
\]

For \( \xi, \eta \in \mathfrak{X}_Q[G] \), put

\[
(\xi, \eta) = \sum_{\sigma \in G} \xi(\sigma)\eta(\sigma).
\]

Since \( \xi_q(\sigma_d) = |N_d : H_q| \) whenever \( d \leq q \) and is zero otherwise,

\[
(\xi_q, \omega_c) = \sum_{\sigma \in \widehat{G}} \xi_q(\sigma) \sum_{c \leq d \leq a} \mu(c, d) |K_d|^{-1} N_d|^{-1} \varepsilon_d(\sigma)
\]

\[
= \sum_{c \leq d \leq a} \mu(c, d) |K_d|^{-1} N_d|^{-1} \sum_{\sigma \in \widehat{G}} \xi_q(\sigma) \varepsilon_d(\sigma)
\]

\[
= \sum_{c \leq d \leq a} \mu(c, d) |K_d|^{-1} N_d|^{-1} |K_d| |N_d : H_q|
\]

\[
= |H_q|^{-1} \delta_{c,d}.
\]

Since \( \operatorname{char} \) is a homomorphism,

\[
\xi_{a^*b} = \sum_{q \in P} v_{a,b,q} \xi_q = \sum_{q \leq a} v_{a,b,q} \xi_q.
\]

Then

\[
(\xi_{a^*b}, \omega_c) = \sum_{q \leq a} v_{a,b,q}(\xi_q, \omega_c) = |H_c|^{-1} v_{a,b,c}
\]

so that
\[ v_{b,c} = \left| H_e \right| \left( \xi_{a,b} \xi_{c,d} \right) \]
\[ = \left| H_e \right| \sum_{\sigma \in G} \xi_{a}(\sigma) \xi_{b}(\sigma) \sum_{e \leq d \leq a} \mu(c, d) \mid K_{d} \mid^{-1} \mid N_{d} \mid^{-1} \epsilon_{d}(\sigma) \]
\[ = \left| H_e \right| \sum_{e \leq d \leq a} \mu(c, d) \mid K_{d} \mid^{-1} \mid N_{d} \mid^{-1} \sum_{\sigma \in K_{d}} \xi_{a}(\sigma) \xi_{b}(\sigma) \]
\[ = \left| H_e \right| \sum_{e \leq d \leq b} \mu(c, d) \mid K_{d} \mid^{-1} \mid N_{d} \mid^{-1} \mid K_{d} \mid \mid N_{d} : H_{a} \mid \mid N_{d} : H_{b} \mid \]
\[ = \frac{\left| H_e \right|}{\left| H_{a} \right| \left| H_{b} \right|} \sum_{e \leq d \leq b} \mu(c, d) \mid N_{d} \mid . \]

Since \( v_{a,b,c} \) is, by its definition, a non-negative integer, this is, except for notation, the statement of the theorem.

Theorem 5 has the following curious corollary.

**Corollary.** Let \( G \) be a finite group. Let \( A \) be a cyclic subgroup of prime power order \( p^k \). Let \( D \) be the subgroup of order \( p \) in \( A \). If \( \mid G \mid < p^k(p^k + 1) \) then \( D \) is normal in \( G \).

**Proof:** This follows at once on taking \( A = B \) and \( C = 1 \), since
\[ \mid G \mid - \mid N(D) \mid \equiv 0 \text{ mod } p^{2k} \quad \text{ and } \quad \mid N(D) \mid \geq \mid A \mid = p^k. \]

**References**