# THE MODULAR REPRESENTATION ALGEBRA OF A FINITE GROUP

BY

J. A. GREEN[1]

## 1. Representation algebras

1.1. *Notation and terminology.*

$G$ is a finite group, with unit element $e$.

$k$ is a field of characteristic $p$.

By a *G-module* $M$ is meant a $(k, G)$-module. Elements of $G$ act as right operators on $M$, and $me = m$ $(m \in M)$. The $k$-dimension $\dim M$ of $M$ is assumed finite. For example,

$\Gamma = \Gamma(k, G)$ is the *regular G-module*, i.e., the group algebra of $G$ over $k$, regarded as $G$-module, and

$k_G$ is the *unit G-module*, i.e., the field $k$, made into a "trivial" $G$-module, i.e., $\kappa x = \kappa$ $(\kappa \in k, x \in G)$. For any $G$-module $M$,

$\{M\}$ is the class of all $G$-modules isomorphic to $M$.

$V_i$ ($i$ runs over a suitable index set $I$) is a set of representatives of the classes $\{V_i\}$ of indecomposable $G$-modules. The number of these indecomposable classes is finite if and only if either $p = 0$, or $p$ is a finite prime such that the Sylow $p$-subgroups of $G$ are cyclic (D. G. Higman [5]).

$F_j$ $(j = 1, \cdots, n)$ is a set of representatives of the classes $\{F_j\}$ of irreducible $G$-modules. The number $n$ of these is always finite. If $k$ is algebraically closed, $n$ is equal to the number of $p$-regular classes of $G$ (R. Brauer, see [1], [2]).

If $M'$, $M''$ are $G$-modules, $M' + M''$ denotes their *direct* sum. If $M$ is a $G$-module, and $s$ a nonnegative integer, $sM$ denotes the direct sum of $s$ isomorphic copies of $M$.

1.2. Let $\mathfrak{c}$ be an arbitrary commutative ring with identity element. Then the *representation algebra* $A_{\mathfrak{c}}(k, G)$ of the pair $(k, G)$, with coefficients in $\mathfrak{c}$, is defined as follows. It is the $\mathfrak{c}$-module generated by the set of all isomorphism classes $\{M\}$ of $G$-modules, subject to relations $\{M\} = \{M'\} + \{M''\}$ for all $M, M', M''$ such that $M \cong M' + M''$, and equipped with the bilinear multiplication given by $\{M\}\{M'\} = \{M \otimes M'\}$. Here $M \otimes M' = M \otimes_k M'$ is made $G$-module by $(m \otimes m')x = mx \otimes m'x$ $(m \in M, m' \in M', x \in G)$. By the Krull-Schmidt theorem for $G$-modules, $A_{\mathfrak{c}}(k, G)$ is free as $\mathfrak{c}$-module, and the $\{V_i\}$ $(i \in I)$ form a $\mathfrak{c}$-basis. $A_{\mathfrak{c}}(k, G)$ is a commutative, associative algebra over $\mathfrak{c}$, and has identity element $1 = \{k_G\}$.

The *Grothendieck algebra* $A_{\mathfrak{c}}^*(k, G)$ is the quotient of $A_{\mathfrak{c}}(k, G)$ by the ideal $J$

Received August 3, 1961.

[1] This work was done while the author was supported by a grant from the National Science Foundation at the Institute for Advanced Study, and under an Army contract at Cornell University.

generated by all elements $\{M'\} - \{M\} + \{M''\}$ such that there exists an exact sequence (of $G$-modules and $G$-module homomorphisms)

$$0 \to M' \to M \to M'' \to 0. \tag{1.2a}$$

By the Jordan-Hölder theorem for $G$-modules, the elements $\{F_j\} + J$ $(j = 1, \cdots, n)$ form a c-basis of $A_{\mathfrak{c}}^*(k, G)$, which is therefore always finite-dimensional.

If $p = 0$, or if $p$ is a finite prime not dividing the order of $G$, then every exact sequence (1.2a) splits, i.e., $J = 0$ and $A_{\mathfrak{c}}(k, G) \cong A_{\mathfrak{c}}^*(k, G)$.

1.3. Returning to the general case, let now $k'$ be an extension field of $k$. Each $(k, G)$-module $M$ gives rise to a $(k', G)$-module $M_{k'} = k' \otimes_k M$ ("extension of coefficient field"). The mapping $\{M\} \to \{M_{k'}\}$ gives a natural homomorphism

$$A_{\mathfrak{c}}(k, G) \to A_{\mathfrak{c}}(k', G), \tag{1.3a}$$

and by a theorem of E. Noether (see e.g. Deuring [3]), which says that two $(k, G)$-modules $M$, $M'$ are isomorphic if $M_{k'} \cong M'_{k'}$, it follows that (1.3a) is a monomorphism. Clearly (1.3a) also induces a map

$$A_{\mathfrak{c}}^*(k, G) \to A_{\mathfrak{c}}^*(k', G), \tag{1.3b}$$

and it is readily shown that this, again, is a monomorphism.[2]

1.4. From now on we shall take $\mathfrak{c}$ to be the field of complex numbers, and write $A(k, G)$, $A^*(k, G)$ for $A_{\mathfrak{c}}(k, G)$, $A_{\mathfrak{c}}^*(k, G)$, respectively. We prove in §1.5, as an immediate consequence of R. Brauer's representation theory,

THEOREM 1. *For any field $k$, and any finite group $G$, the algebra $A^*(k, G)$ is semisimple.*

If $p = 0$ or if $p$ is a finite prime not dividing the order of $G$, then $A(k, G)$ coincides with $A^*(k, G)$, and so is semisimple by Theorem 1. If $p$ is a finite prime dividing the order of $G$, very little is known about $A(k, G)$, even in the case where this is a finite-dimensional algebra, i.e., when the Sylow $p$-subgroups of $G$ are cyclic. The greater part of this paper (§2) is devoted to the proof of

THEOREM 2. *If $k$ has finite prime characteristic $p$, and if $G$ is a cyclic group of order a power of $p$, then $A(k, G)$ is semisimple.*

*Corollary. $A(k, G)$ is semisimple, for any finite cyclic group $G$.*

For the proof of this corollary, see §2.11.

---

[2] Let $k' \otimes F_j = F_{j1} + F_{j2} + \cdots$, where $F_{j1}, F_{j2}, \cdots$ are irreducible $(k', G)$-modules. If $\{F_h\}$, $\{F_j\}$ are distinct classes of irreducible $(k, G)$-modules, then no one of $F_{h1}$, $F_{h2}, \cdots$ can be isomorphic to any one of $F_{j1}, F_{j2}, \cdots$, by Schur's lemma. Therefore the basis elements $\{F_j\} + J$ $(j = 1, \cdots, n)$ of $A^*(k, G)$, are mapped into linearly independent elements of $A^*(k', G)$.

1.5. If $A$ is any commutative complex algebra with identity element 1, define a *character* of $A$ to be a nonzero algebra homomorphism $\phi : A \rightarrow \mathfrak{c}$. By definition, $A$ is semisimple if and only if, given any nonzero element $a \in A$, there exists some character $\phi$ of $A$ such that $\phi(a) \neq 0$. If $A$ has finite dimension $s$, say, then this condition is equivalent to the condition that $A$ should have $s$ distinct characters.

*Proof of Theorem* 1. Let $k'$ be the algebraic closure of $k$. If $A^*(k', G)$ is semisimple, then so is $A^*(k, G)$, because, by (1.3b), $A^*(k, G)$ is isomorphic to a subalgebra of $A^*(k', G)$. So we may assume $k$ is algebraically closed. By Brauer's theorem (see §1.1), $A^*(k, G)$ has dimension $n$ = number of $p$-regular classes of $G$. For each $p$-regular class $K_\nu$, $\nu = 1, \cdots, n$, we may define a function $\beta_\nu$ on $A^*(k, G)$, as follows: Each class $\{M\}$ of $G$-modules determines a class of equivalent matrix representations of $G$ over $k$; let M be one of these matrix representations. Define $\beta_\nu(\{M\} + J)$ to be the value, at an element of the conjugacy class $K_\nu$, of the *Brauer character* of M (see [1]). For example, taking $K_1 = \{e\}$, we have $\beta_1(\{M\} + J) = \dim M$. Well-known properties of the Brauer character ensure that $\beta_\nu$ is well-defined and is a character of $A^*(k, G)$. Moreover $\beta_1, \cdots, \beta_n$ are distinct,[3] so $A^*(k, G)$ has as many characters as its dimension, which proves the theorem.

1.6. We collect here some general facts which will be used in §2. Let $G, H$ be two groups, and $\theta : H \rightarrow G$ a homomorphism. If $M$ is a $G$-module, let $M\theta^*$ denote the *restricted* $H$-module, i.e., $M\theta^*$ has the same underlying $k$-space as $M$, and $y \in H$ operates by $my = m(y\theta)$ $(m \in M)$. If $L$ is an $H$-module, let $L\theta_*$ denote the *induced* $G$-module, i.e., $L\theta_*$ is generated, as $k$-space, by symbols $l \otimes \gamma$ $(l \in L, \gamma \in \Gamma = \Gamma(k, G))$ subject to the relations which make $\otimes$ bilinear over $k$, and also

$$ly \otimes \gamma = l \otimes (y\theta)\gamma \qquad (l \in L, \gamma \in \Gamma, y \in H).$$

An element $x \in G$ acts on $L\theta_*$ by the rule $(l \otimes \gamma)x = l \otimes \gamma x$. If $\theta$ is monomorphic, we have

$$\dim L\theta_* = (G : H\theta) \dim L. \tag{1.6a}$$

The maps $\{M\} \rightarrow \{M\theta^*\}$ and $\{L\} \rightarrow \{L\theta_*\}$ induce linear mappings

$$\theta^* : A(k, G) \rightarrow A(k, H) \quad \text{and} \quad \theta_* : A(k, H) \rightarrow A(k, G),$$

respectively. $\theta^*$ is clearly an algebra homomorphism; for $\theta_*$ we have the identity

$$L\theta_* \otimes M \cong (L \otimes M\theta^*)\theta_* \tag{1.6b}$$

(see e.g. Swan [7]).

[3] Any character $\beta$ of $A^*(k, G)$ is determined by the values $\beta^j = \beta(\{F_j\} + J)$ $(j = 1, \cdots, n)$. The $n \times n$ matrix $(\beta_\nu^j)$ ($\nu$ row, $j$ column affix) is just the transpose of Brauer's matrix of modular characters (called $\Phi$ in [2]), and hence is nonsingular.

In particular, if $\theta$ is the inclusion map of the subgroup $H = \{e\}$ in $G$, and if $L = k_{\{e\}}$, we find $L\theta_* \cong \Gamma$; hence (1.6b) gives

(1.6c) $$\Gamma \otimes M \cong (\dim M)\Gamma, \qquad \text{for any } G\text{-module } M.$$

Let $\phi$ be any character of $A(k, G)$. We write $\phi(M)$ in place of $\phi(\{M\})$ for convenience. Then (1.6c) shows that $\phi(\Gamma)\phi(M) = (\dim M)\phi(\Gamma)$; hence if $\phi(\Gamma) \neq 0$, we have $\phi(M) = \dim M$ for all $M$.

(1.6d) *The only character $\phi$ of $A(k, G)$, for which $\phi(\Gamma) \neq 0$, is the "dimension character" $\phi(M) = \dim M$.*

Finally we note the following theorem of Schanuel (see e.g. Swan [8]).

(1.6e) *If $0 \to A \to P \to B \to 0$ and $0 \to A' \to P' \to B' \to 0$ are two exact sequences of G-modules, with $P$, $P'$ both projective, and if $B \cong B'$, then*

$$A + P' \cong A' + P.$$

We shall use (1.6e) only in the case where $P$, $P'$ are both *free* $G$-modules, $P = s\Gamma$, $P' = s'\Gamma$, say. If $s \geqq s'$, the theorem gives

$$A \cong A' + (s - s')\Gamma.$$

## 2. The representation algebra of a finite cyclic group

2.1. Throughout §2 we make the following conventions.

$k$ is a field of finite prime characteristic $p$.
$\alpha$ is a nonnegative integer, $q = p^\alpha$.
$G_\alpha$ is a cyclic group of order $q = p^\alpha$, and $\Gamma_\alpha = \Gamma(k, G_\alpha)$.
$A_\alpha = A(k, G_\alpha)$.

Any $G_\alpha$-module can be regarded as a $\Gamma_\alpha$-module, and conversely. If $x_\alpha$ is a generator of $G_\alpha$, and if $\omega_\alpha = x_\alpha - e$, then $\omega_\alpha^q = 0$, and

$$V_{r\alpha} = \Gamma_\alpha/\omega_\alpha^r\,\Gamma_\alpha \qquad (r = 1, \cdots, p^\alpha)$$

form a set of representatives of the classes of indecomposable $G$-modules. We write also $V_{0\alpha} = \{0\}$, the zero $G_\alpha$-module.

If $a$ is a module generator of $V_{r\alpha}$, then the elements $a\omega_\alpha^i$ $(i = 0, 1, \cdots, r - 1)$ form a $k$-basis of $V_{r\alpha}$. With respect to this basis, $x_\alpha$ is represented by the $r \times r$ matrix

$$X_r = \begin{pmatrix} 1 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 1 & \cdots & 0 & 0 \\ \cdot & \cdot & \cdot & \cdots & \cdot & \cdot \\ 0 & 0 & 0 & \cdots & 1 & 1 \\ 0 & 0 & 0 & \cdots & 0 & 1 \end{pmatrix}.$$

The only submodules of $V_{r\alpha}$ are $V_{r\alpha}\,\omega^i$ $(i = 0, 1, \cdots, r)$. If $r$, $s$ are integers such that $0 \leqq r \leqq s \leqq q = p^\alpha$, then there is an obvious exact sequence

(2.1a) $$0 \to V_{r\alpha} \to V_{s\alpha} \to V_{s-r,\alpha} \to 0.$$

2.2. If $\alpha$, $\beta$ are integers such that $\beta \geqq \alpha \geqq 0$, there is a homomorphism $\theta : G_\beta \to G_\alpha$ which takes $x_\beta$ onto $x_\alpha$. It is clear that $V_{r\alpha}\theta^* \cong V_{r\beta}\,(1 \leqq r \leqq p^\alpha)$, and in most contexts we write simply $V_r$ for $V_{r\alpha}$. The mapping $\theta^* : A_\alpha \to A_\beta$ is a monomorphism, and we shall identify $A_\alpha$ with the appropriate part of $A_\beta$ according to $\theta^*$, and write $v_r = \{V_{r\alpha}\} = \{V_{r\beta}\}$. Thus $A_0, A_1, A_2, \cdots$ are subalgebras of a commutative algebra $A = \bigcup_{\alpha=0}^{\infty} A_\alpha$. $A$ has basis $v_1, v_2, \cdots$, and identity element $v_1 = 1$. $A_\alpha$ has basis $v_1, \cdots, v_{p^\alpha}$. We shall write[4] $v_0 = 0$.

2.3. Take a fixed $\alpha \geqq 0$, $q = p^\alpha$. The next theorem gives relations which describe $A_{\alpha+1}$ as an extension of $A_\alpha$.

THEOREM 3. *Let* $w = v_{q+1} - v_{q-1}$. *Then*

(2.3a) $$v_r w = v_{r+q} - v_{q-r} \qquad (1 \leqq r \leqq q),$$

(2.3b) $$v_r w = v_{r+q} + v_{r-q} \qquad (q < r < (p-1)q),$$

(2.3c) $$v_r w = v_{r-q} + 2v_{pq} - v_{2pq-(r+q)} \qquad ((p-1)q \leqq r \leqq pq).$$

These formulae show that $A_{\alpha+1} = A_\alpha[w]$. However we prefer to regard $A_{\alpha+1}$ as the ring generated over $A_\alpha$ by the $p^{\alpha+1} - p^\alpha$ elements $v_r$ $(q+1 \leqq r \leqq pq)$, and then

(2.3d) *Relations* (2.3a), (2.3b), (2.3c) *are defining relations for this extension.*

For let $B = A_\alpha[v_{q+1}, \cdots, v_{pq}]$ be the commutative ring obtained by adjoining to $A_\alpha$ symbols $v_{q+1}, \cdots, v_{pq}$ which satisfy these relations, and let $\pi: B \to A_{\alpha+1}$ be the natural epimorphism of $B$ onto $A_{\alpha+1}$. The given relations obviously imply that $B$ is spanned linearly by $v_1, \cdots, v_{pq}$; hence by comparison of dimensions of $B$ and $A_{\alpha+1}$, $\pi$ must be an isomorphism.

2.4. In this paragraph, $\alpha$ is again fixed, all modules are $G_\alpha$-modules, and we write $V_r = V_{r\alpha}$, $\Gamma = \Gamma_\alpha$, $\omega = \omega_\alpha = x_\alpha - e$. By a *partition* $\lambda$ we understand a sequence $(\lambda_1, \lambda_2, \cdots)$ whose terms are nonnegative integers, almost all zero, and such that $\lambda_1 \geqq \lambda_2 \geqq \cdots$. Those terms which are positive are called *parts* of $\lambda$. For each integer $i \geqq 1$, write $n_i(\lambda)$ for the number of parts equal to $i$, and $b_i(\lambda)$ for the number of parts $\geqq i$. Either of the sequences

[4] The multiplication in $A$ is that determined by the Kronecker product of the matrices $X_r$, i.e., if $X_r \times X_s$ has Jordan form $\sum a_{rst} X_t$, then $v_r v_s = \sum a_{rst} v_t$. For matrices over a field of characteristic zero, Littlewood [6, p. 195] has calculated these coefficients $a_{rst}$ explicitly. We have not been able to find such an explicit description of this product in the modular case.

$(n_1, n_2, \cdots)$ or $(b_1, b_2, \cdots)$ determines $\lambda$ uniquely, and

$$n_i(\lambda) = b_i(\lambda) - b_{i+1}(\lambda).$$

$b_1(\lambda)$ is the number of parts of $\lambda$.

Let $V$ be any $G_\alpha$-module. There is a unique expansion

$$V \cong V_{\lambda_1} + \cdots + V_{\lambda_b} \qquad (\lambda_1 \geqq \cdots \geqq \lambda_b > 0), \tag{2.4a}$$

and we write $\lambda(V)$ for the partition $(\lambda_1, \cdots, \lambda_b, 0, 0, \cdots)$. All the parts of $\lambda(V)$ lie between 1 and $q = p^\alpha$, and $\sum \lambda_i = \dim V$. Moreover $\lambda(V)$ can be invariantly described by the well-known formulae

$$b_i(\lambda(V)) = \dim (V\omega^{i-1}/V\omega^i) \qquad (i = 1, 2, \cdots). \tag{2.4b}$$

It will be useful to have the particular notations

$l(V) = \lambda_1 =$ least integer $l$ such that $V\omega^l = 0$, and
$b(V) = b_1(\lambda(V)) = \dim (V/V\omega) =$ number of summands in (2.4a).

We observe that if $V'$ is a homomorphic image of $V$, then $b(V) \geqq b(V')$.

2.5.

(2.5a) *If* $1 \leqq r, s \leqq q$, *and if*

$$V_r \otimes V_s \cong V_{\lambda_1} + \cdots + V_{\lambda_b} \quad (\lambda_1 \geqq \cdots \geqq \lambda_b > 0),$$

*then* $s \geqq b$, *and*

$$V_{q-r} \otimes V_s \cong V_{q-\lambda_1} + \cdots + V_{q-\lambda_b} + (s - b) V_q .$$

*Proof.* Since $\Gamma = V_q$, there is an exact sequence

$$0 \to V_{q-r} \to \Gamma \to V_r \to 0,$$

from which, taking tensor products with $V_s$ and using (1.6c), we get an exact sequence

$$0 \to V_{q-r} \otimes V_s \to s\Gamma \to V_r \otimes V_s \to 0.$$

It is clear that $b(s\Gamma) = s$; hence by the remark at the end of §2.4, $s \geqq b(V_r \otimes V_s) = b$. But we can also present $\sum V_{\lambda_i}$ by an exact sequence

$$0 \to \sum V_{q-\lambda_i} \to b\Gamma \to \sum V_{\lambda_i} \to 0.$$

Then Schanuel's theorem (1.6e) gives the result.

Take the special case $r = 1$. We have $V_1 \otimes V_s \cong V_s$; hence

$$V_{q-1} \otimes V_s \cong V_{q-s} + (s - 1) V_q \qquad (1 \leqq s \leqq q). \tag{2.5b}$$

From this we deduce

(2.5c) *If* $\phi : A_\alpha \to \mathfrak{c}$ *is any character of* $A_\alpha$, *there exists an integer* $T(\phi) = \pm 1$ *such that* $\phi(v_{q-s}) + T(\phi)\phi(v_s) = \phi(v_q)$ $(0 \leqq s \leqq q)$.

*Proof.* If $\phi$ is the dimension character (see (1.6d)), $\phi(v_s) = s$, so we may take $T(\phi) = 1$. If $\phi$ is not the dimension, then by (1.6d), $\phi(V_q) = 0$. By (2.5b), $\phi(v_{q-s}) + T(\phi)\phi(v_s) = 0$, where $T(\phi) = -\phi(V_{q-1})$. Again, if we put $s = q - 1$ in (2.5b), we find $(\phi(V_{q-1}))^2 = \phi(V_1) = 1$; hence $T(\phi) = \pm 1$, and this completes the proof.

2.6. Any partition $\lambda$ can be associated with a *graph* (see e.g. Littlewood [6, Ch. V]) consisting of rows of symbols called *nodes*, $\lambda_1$ in the first row, $\lambda_2$ in the second, and so on.

A partition $\mu$ is said to be obtained from $\lambda$ by *regular adjunction of $r$ nodes* if there is a sequence of partitions

$$\lambda = \lambda^0, \quad \lambda^1, \quad \cdots, \quad \lambda^r = \mu \tag{2.6a}$$

such that for each $h = 1, \cdots, r$, the graph of $\lambda^h$ is obtained from that of $\lambda^{h-1}$ by adding one new node $a_h$, in such a way that no two of the $r$ added nodes $a_1, \cdots, a_r$ appear in the same column. For example, the diagram

$$\begin{array}{cccc} \cdot & \cdot & \cdot & a_4 \\ \cdot & \cdot & \cdot & \\ \cdot & \cdot & a_3 & \\ a_1 & a_2 & & \end{array}$$

shows how $(4, 3, 3, 2, 0, \cdots)$ can be obtained from $(3, 3, 2, 0, \cdots)$ by regular adjunction of 4 nodes.

(2.6b) *Let $\lambda$, $\mu$ be two partitions. Then $\mu$ can be obtained from $\lambda$ by regular adjunction of $r$ nodes, if and only if there exist $r$ distinct positive integers $i_1, \cdots, i_r$ such that*

$$\begin{aligned} b_i(\mu) - b_i(\lambda) &= 1 \quad \textit{if} \quad i \in \{i_1, \cdots, i_r\}, \quad \textit{and} \\ &= 0 \quad \textit{if} \quad i \notin \{i_1, \cdots, i_r\}. \end{aligned} \tag{2.6c}$$

*Proof.*[5] We observe that, for any partition $\lambda$, $b_i(\lambda)$ is the number of nodes in the $i^{\text{th}}$ column of the diagram of $\lambda$. Thus (2.6b) follows at once from the definition of regular adjunction, because (2.6c) is simply the condition that $\mu$ be obtainable from $\lambda$ by adding new nodes to the distinct columns $i_1, \cdots, i_r$.

We are now in a position to prove the following lemma, which is a very special case of a theorem (proof unpublished) of P. Hall (see [4, Theorem 2]).

(2.6d) *Let $V_r = V_{r\alpha}$ $(0 \leqq r \leqq q)$, and let $V$, $W$ be any $G_\alpha$-modules. If there exists an exact sequence*

$$0 \to V_r \xrightarrow{\iota} V \xrightarrow{\varepsilon} W \to 0,$$

*then $\lambda(V)$ can be obtained from $\lambda(W)$ by regular adjunction of $r$ nodes.*

[5] The author is much indebted to the referee for simplifying the original proofs of (2.6b) and (2.6d).

*Proof.* Since $\dim V = \dim W + r$, the graph of $\lambda(V)$ has $r$ more nodes than that of $\mu(W)$. We have to prove that we can obtain $\lambda(V)$ from $\lambda(W)$ by regular adjunction.

We may assume that $V_r$ is a submodule of $V$, and that $\iota$ is the inclusion map. For each $i = 1, 2, \cdots,$ $\varepsilon$ induces an epimorphism

$$V\omega^{i-1}/V\omega^{i} \to W\omega^{i-1}/W\omega^{i},$$

whose kernel is annihilated by $\omega$, and is also a cyclic module, being an image of $V_r \cap V\omega^{i-1}$. Therefore this kernel is either $V_0$ or $V_1$, so that

$$b_i(\lambda(V)) - b_i(\lambda(W)) = 0 \text{ or } 1,$$

by (2.4b). The conclusion now follows from (2.6b).

2.7. Let $\iota : G_1 \to G_{\alpha+1}$ be the monomorphism which takes $x_1$ to $x_{\alpha+1}^q$ ($q = p^\alpha$ as before). If $V_r$ ($1 \leqq r \leqq pq = p^{\alpha+1}$) is the $G_{\alpha+1}$-module $V_{r,\alpha+1}$, we obtain the $G_1$-module $V_r\,\iota^*$ by defining $vx_1 = vx_{\alpha+1}^q$ ($v \in V_r$), from which it follows (using $\omega_{\alpha+1}^q = x_{\alpha+1}^q - e$)

$$(V_r\,\iota^*)\omega_1^i = V_r\,\omega_{\alpha+1}^{iq} \qquad (i = 0, 1, \cdots).$$

Hence if $\lambda = \lambda(V_r\,\iota^*)$, we have by (2.4b)

$$b_i(\lambda) = \dim V_r\,\omega_{\alpha+1}^{(i-1)q} - \dim V_r\,\omega_{\alpha+1}^{iq} \qquad (i = 1, 2, \cdots).$$

Now $\dim V_r\,\omega_{\alpha+1}^j = r - j$ ($0 \leqq j \leqq r$) or $0$ ($j > r$). Writing

$$r = r_0\,q + r_1 \qquad (0 \leqq r_1 < q), \tag{2.7a}$$

we have then

$$b_i(\lambda) = q \quad (1 \leqq i \leqq r_0), \qquad b_{r_0+1}(\lambda) = r_1, \qquad b_i(\lambda) = 0 \quad (i > r_0 + 1).$$

Thus $n_i(\lambda) = 0$ if $1 \leqq i \leqq r_0$ or if $i > r_0 + 1$, while $n_{r_0}(\lambda) = q - r_1$ and $n_{r_0+1}(\lambda) = r_1$. Therefore

(2.7b) *If $1 \leqq r \leqq pq$, and $r$ is given by* (2.7a), *we have*

$$V_{r,\alpha+1}\,\iota^* \cong (q - r_1)V_{r_0,1} + r_1\,V_{r_0+1,1}\,.$$

It is easy to compute the induced map $\iota_*$. If $1 \leqq s \leqq p$, we find that $V_{s,1}\,\iota_*$ is indecomposable; and since its dimension is $qs$, we have

$$V_{s,1}\,\iota_* \cong V_{qs,\alpha+1} \qquad (1 \leqq s \leqq p). \tag{2.7c}$$

In particular, $V_{1,1}\,\iota_* \cong V_{q,\alpha+1}$. Then from (1.6b), with $\theta = \iota$, $L = V_{1,1}$, and $M = V_{r,\alpha+1}$, (2.7b) and (2.7c) give

(2.7d) *If $r$ is given by* (2.7a), $1 \leqq r \leqq pq$, *and all modules are $G_{\alpha+1}$-modules, then*

$$V_r \otimes V_q \cong (q - r_1)V_{qr_0} + r_1\,V_{q(r_0+1)}\,.$$

In particular, the graph of $\lambda(V_r \otimes V_q)$ consists of $r_1$ rows of length $q(r_0 + 1)$, and $(q - r_1)$ rows of length $qr_0$.

2.8. In this and the next paragraph, all modules are $G_{\alpha+1}$-modules, $q = p^{\alpha}$, $x = x_{\alpha+1}$, $\omega = \omega_{\alpha+1}$, and $r$ is an integer such that $1 \leqq r \leqq pq = p^{\alpha+1}$, $r = r_0 q + r_1$ $(0 \leqq r_1 < q)$.

By taking the tensor product of the exact sequence

$$0 \to V_1 \to V_{q+1} \to V_q \to 0$$

with $V_r$, we obtain the exact sequence

$$0 \to V_r \to V_r \otimes V_{q+1} \to V_r \otimes V_q \to 0.$$

Hence by (2.6d)

(2.8a) *$\lambda(V_r \otimes V_{q+1})$ is obtained from $\lambda(V_r \otimes V_q)$ by regular adjunction of $r$ nodes.*

Next we prove

(2.8b) *If $1 \leqq r < (p-1)q$, then $l(V_r \otimes V_{q+1}) = q + r$.*

*Proof.* Let $a$, $b$ be any elements of $V_r$, $V_{q+1}$ respectively. Then

$$\begin{aligned}(a \otimes b)\omega = (a \otimes b)(x - e) = ax \otimes bx - a \otimes b &= a\omega \otimes bx + a \otimes b\omega \\ &= (a \otimes b)(\omega \otimes x + e \otimes \omega),\end{aligned}$$

where $\omega \otimes x + e \otimes \omega$ is an element of the product algebra $\Gamma_{\alpha+1} \otimes \Gamma_{\alpha+1}$, which operates naturally on $V_r \otimes V_{q+1}$. Since $\omega \otimes x$ and $e \otimes \omega$ commute, and since $a\omega^r = b\omega^{q+1} = 0$, we find by the binomial theorem that for any integer $\xi \geqq 0$,

$$(a \otimes b)\omega^{q(r_0+1)+\xi} = (r_0 + 1)(a \otimes b)(\omega^{qr_0+\xi} \otimes x^{qr_0+\xi}\omega^q).$$

Now $r_0 + 1 \neq 0$, because $r_0 \leqq p - 2$. Hence $(V_r \otimes V_{q+1})\omega^{q(r_0+1)+\xi}$ is zero for $\xi = r_1$, but not zero for $\xi = r_1 - 1$. So $l(V_r \otimes V_{q+1}) = q(r_0 + 1) + r_1 = q + r$.

(2.8c) *If $1 \leqq r \leqq q$, then $V_r \otimes V_{q+1} \cong V_{r+q} + (r-1)V_q$.*

*Proof.* $\lambda(V_r \otimes V_q)$ consists of $r$ rows of $q$ nodes. The only way to make a graph by regular adjunction of $r$ nodes, in such a way that the first part should be $q + r$, is to adjoin all nodes to the first row. Thus the graph of $\lambda(V_r \otimes V_{q+1})$ has one part $q + r$, and $r - 1$ parts $q$.

(2.8d) *If $q < r < (p-1)q$, then*

$$\begin{aligned}V_r \otimes V_{q+1} \cong V_{r-q} + (q - r_1 - 1)V_{r_0 q} &+ V_{(r_0+1)q-r_1} \\ &+ (r_1 - 1)V_{(r_0+1)q} + V_{r+q}.\end{aligned}$$

*Proof.* Since $l(V_r \otimes V_{q+1}) = q + r$, the module $V_r \otimes V_{q+1}$ must have a component $V_{q+r}$. Applying (2.8b) to $V_{pq-r}$, we see that $V_{pq-r} \otimes V_{q+1}$ has a component $V_{pq-r+q} = V_{pq-(r-q)}$. Then (2.5a) shows that $V_r \otimes V_{q+1}$ has a component $V_{r-q}$. Hence $\lambda(V_r \otimes V_{q+1})$ has a part $r + q$, and a part $r - q$. It is easy to verify, that the only partition which has a part $r + q$, a part $r - q$, and can be obtained from $\lambda(V_r \otimes V_q)$ by regular adjunction of $r$ nodes, is the partition of the module on the right of (2.8d).

By another application of (2.5a) we deduce from (2.8c)

(2.8e) *If* $(p - 1)q \leqq r < pq$, *then*

$$V_r \otimes V_{q+1} \cong V_{r-q} + (q - r_1 - 1)V_{(p-1)q} + (r_1 + 1)V_{pq}.$$

2.9. We consider next the module $V_r \otimes V_{q-1}$. From the exact sequence

$$0 \to V_1 \to V_q \to V_{q-1} \to 0,$$

we get the exact sequence

$$0 \to V_r \to V_r \otimes V_q \to V_r \otimes V_{q-1} \to 0;$$

therefore

(2.9a) $\lambda(V_r \otimes V_q)$ *can be obtained from* $\lambda(V_r \otimes V_{q-1})$ *by regular adjunction of* $r$ *nodes.*

(2.9b)
$$\begin{aligned} b(V_r \otimes V_{q-1}) &= r \qquad &&\text{if} \quad r \leqq q - 1, \\ &= q - 1 &&\text{if} \quad r \geqq q - 1. \end{aligned}$$

*Proof.* Put $V = V_r \otimes V_{q-1}$; then $b(V) = \dim(V/V\omega)$ (see §2.4). Let $a, b$ be module generators for $V_r$, $V_{q-1}$ respectively. The elements

$$u_{ij} = a\omega^i x^j \otimes b\omega^j \qquad (0 \leqq i \leqq r - 1, 0 \leqq j \leqq q - 2)$$

form a basis of $V$. We write $u_{ij} = 0$ if $i \geqq r$ or if $j \geqq q - 1$. Then

$$u_{ij}\,\omega = u_{i+1,j} + u_{i,j+1} \qquad \text{for all} \quad i, j \geqq 0;$$

hence if $\bar{u}_{ij} = u_{ij} + V\omega$, then $\bar{u}_{i+1,j} = -\bar{u}_{i,j+1}$. It follows that $V/V\omega$ has a $k$-basis either

$$\bar{u}_{i,0} \quad (0 \leqq i \leqq r - 1) \quad \text{if} \quad r \leqq q - 1, \quad \text{or}$$

$$\bar{u}_{0,j} \quad (0 \leqq j \leqq q - 2) \quad \text{if} \quad r \geqq q - 1.$$

(2.9c) *If* $q \leqq r \leqq pq$, *then*

$$V_r \otimes V_{q-1} \cong (r_1 - 1)V_{q(r_0+1)} + V_{q(r_0+1)-r_1} + (q - r_1 - 1)V_{qr_0}.$$

*Proof.* $b(V_r \otimes V_q) = q$, by (2.7d), and $b(V_r \otimes V_{q-1}) = q - 1$ by (2.9b). Therefore the whole of the last row of the graph of $\lambda(V_r \otimes V_q)$ (considered to be obtained from $\lambda(V_r \otimes V_{q-1})$ by regular adjunction of $r$ nodes) must consist of added nodes. This means that $\lambda(V_r \otimes V_{q-1})$ must be the partition of the module on the right of (2.9c).

By applying a similar argument, or else by using (2.5a) on this last formula, we find also

(2.9d) *If* $1 \leqq r \leqq q$, *then* $V_r \otimes V_{q-1} \cong V_{q-r} + (r-1)V_q$.

The formulae in §§2.8 and 2.9 yield immediately the proof of Theorem 3.

2.10. *Proof of Theorem* 2. We wish to show that, for any $\alpha \geqq 0$, the algebra $A_\alpha$ has $p^\alpha$ characters. For $\alpha = 0$ this is clear; now suppose $\alpha \geqq 0$ is such that $A_\alpha$ does have $p^\alpha = q$ characters; we complete the induction by showing that $A_{\alpha+1}$ has $p^{\alpha+1}$ characters. This will be achieved when we prove

(2.10a) *If* $\phi : A_\alpha \to \mathfrak{c}$ *is any character of* $A_\alpha$, *then there are* $p$ *distinct characters of* $A_{\alpha+1}$ *which extend* $\phi$.

Put $z_i = \phi(v_i)$ $(0 \leqq i \leqq q)$. Finding an extension $\phi^*$ of $\phi$ to $A_{\alpha+1}$ is equivalent to finding $pq - q$ complex numbers $z_r$ $(q+1 \leqq r \leqq pq)$ such that

(2.10b) $$z_r y = z_{r+q} - z_{q-r} \qquad (1 \leqq r \leqq q),$$

(2.10c) $$z_r y = z_{r+q} + z_{r-q} \qquad (q < r < (p-1)q),$$

(2.10d) $$z_r y = z_{r-q} + 2z_{pq} - z_{2pq-(r+q)} \qquad ((p-1)q \leqq r \leqq pq),$$

where $y = z_{q+1} - z_{q-1}$. For if $\phi^*$ is such an extension, then by Theorem 3, $z_r = \phi^*(v_r)$ will satisfy these relations; conversely given such $z_r$ we define $\phi^*$ by $\phi^*(v_r) = z_r$, and then by (2.3d), $\phi^*$ is a character of $A_{\alpha+1}$.

Let $t$ be an indeterminate over $\mathfrak{c}$, and define for each $s \geqq -1$ the function (polynomial in $t, t^{-1}$)

$$L_s(t) = \sum_{i=0}^{s-1} t^{-s+2i+1} = (t^s - t^{-s})/(t - t^{-1}),$$

so that $L_{-1}(t) = -1$, $L_0(t) = 0$, $L_1(t) = 1$, $L_2(t) = t^{-1} + t$, etc. Notice $L_s(t) = L_s(t^{-1})$. We find also

(2.10e) $$L_s(t)L_2(t) = L_{s+1}(t) + L_{s-1}(t) \qquad (s \geqq 0).$$

Now let $z_r = \phi(v_r)$ $(0 \leqq r \leqq q)$ as before, and let $\varepsilon$ be a nonzero complex number. Define $z_r = \phi(v_r)$ $(0 \leqq r \leqq pq)$ by putting $r = r_0 q + r_1$ $(0 \leqq r_1 < q)$ and

(2.10f) $$z_r = z_{r_1} L_{r_0+1}(\varepsilon) + z_{q-r_1} L_{r_0}(\varepsilon).$$

Then $y = z_{q+1} - z_{q-1} = L_2(\varepsilon)$. We find, using (2.10e), that (2.10b) and (2.10c) are satisfied by these $z_r$, for any $\varepsilon \neq 0$. Also for $r = (p-1)q + r_1$ $(0 \leqq r_1 \leqq q)$ we have

(2.10g) $$\begin{aligned} &z_r y - \{z_{r-q} + 2z_{pq} - z_{2pq-(r+q)}\} \\ &\qquad = z_{r_1}(L_{p+1} + L_{p-1}) + 2z_{q-r_1} L_p - 2z_q L_p, \end{aligned}$$

where we have written $L_s$ in place of $L_s(\varepsilon)$, for short. The right-hand side of (2.10g) is zero, and hence (2.10d) is satisfied in the following cases:

(i) If $\varepsilon^2$ is a primitive $p^{\text{th}}$ root of unity (i.e., $\varepsilon = \exp(\pi i w/p)$, $1 \leqq w \leqq (p-1)$). For then $L_p(\varepsilon) = 0$; hence $L_{p+1}(\varepsilon) + L_{p-1}(\varepsilon) = 0$ by (2.10e). We have in this way $(p-1)$ distinct extensions of $\phi$, with $z_{q+1} - z_{q-1} = L_2(\varepsilon) = 2\cos(\pi w/p), w = 1, \cdots, p-1$.

(ii) If $\varepsilon = T(\phi)$ (see (2.5c)). For then $\varepsilon = \pm 1$, so that $L_s(\varepsilon) = s\varepsilon^{s-1}$, and the right-hand side of (2.10g) becomes

$$2p\varepsilon^{p-1}(\varepsilon z_{r_1} + z_{q-r_1} - z_q),$$

and this is zero by (2.5c). Thus there are $p$ distinct extensions of $\phi$. This proves (2.10a) and hence Theorem 2.

*Remarks.* If we take $\alpha = 0$, our argument shows that $A_1$ has $p$ characters

$$\phi_0 : v_r \to r, \quad \text{and}$$

$$\phi_w : v_r \to L_r(\varepsilon) = \frac{\sin(\pi r w/p)}{\sin(\pi w/p)} \qquad (r = 1, \cdots, p),$$

$w = 1, \cdots, p-1$. The field generated by the values $\phi(v_r)$, for all characters $\phi$ of $A_\alpha$, and $r = 1, \cdots, p^\alpha$, is independent of $\alpha$ (provided $\alpha \geqq 1$), and is the maximal real subfield of the field of $(2p)^{\text{th}}$ roots of unity.

2.11. We conclude with a proof of the Corollary to Theorem 2, that $A(k, G)$ is semisimple for any finite cyclic group $G$. $G$ can be written $G = H_1 \times H_2$, where $H_1$, $H_2$ are cyclic groups, respectively of order prime to $p$, and of order a power of $p$. As in the proof of Theorem 1, we may assume $k$ is algebraically closed. Then it is easy to see that any indecomposable $G$-module $V$ has the form $V_1 \otimes V_2$, where $V_1$ is an irreducible $H_1$-module (hence $\dim V_1 = 1$), and $V_2$ is an indecomposable $H_2$-module, and $V_1 \otimes V_2$ is an $H_1 \times H_2$-module by the rule

$$(v_1 \otimes v_2)(h_1, h_2) = v_1 h_1 \otimes v_2 h_2 \qquad (v_i \in V_i, h_i \varepsilon H_i, i = 1, 2).$$

The map

$$\{V\} \to \{V_1\} \otimes \{V_2\}$$

defines an isomorphism from $A(k, G)$ onto $A(k, H_1) \otimes A(k, H_2)$. Both factors are semisimple; therefore so is $A(k, G)$.

## REFERENCES

1. R. BRAUER AND C. NESBITT, *On the modular representations of groups of finite order. I*, University of Toronto Studies, Mathematical Series, no. 4, 1937.
2. ———, *On the modular characters of groups*, Ann. of Math. (2), vol. 42 (1941), pp. 556–590.
3. M. DEURING, *Galoissche Theorie und Darstellungstheorie*, Math. Ann., vol. 107 (1932), pp. 140–144.
4. J. A. GREEN, *Les polynômes de Hall et les caractères des groupes GL(n, q)*, Colloque

d'Algèbre Supérieure, Bruxelles, 1956, Centre Belge de Recherches Mathématiques, 1957, pp. 207–215.
5. D. G. HIGMAN, *Modules with a group of operators*, Duke Math. J., vol. 21 (1954), pp. 369–376.
6. D. E. LITTLEWOOD, *The theory of group characters and matrix representations of groups*, Oxford, 1940.
7. R. G. SWAN, *Induced representations and projective modules*, Ann. of Math. (2), vol. 71 (1960), pp. 552–578.
8. ———, *Periodic resolutions for finite groups*, Ann. of Math. (2), vol. 72 (1960), pp. 267–291.

THE INSTITUTE FOR ADVANCED STUDY
PRINCETON, NEW JERSEY
CORNELL UNIVERSITY
ITHACA, NEW YORK