

## MODULAR PERMUTATION REPRESENTATIONS<sup>(1)</sup>

BY

L. L. SCOTT

**ABSTRACT.** A modular theory for permutation representations and their centralizer rings is presented, analogous in several respects to the classical work of Brauer on group algebras.

Some principal ingredients of the theory are characters of indecomposable components of the permutation module over a  $p$ -adic ring, modular characters of the centralizer ring, and the action of normalizers of  $p$ -subgroups  $P$  on the fixed points of  $P$ . A detailed summary appears in [15].

A main consequence of the theory is simplification of the problem of computing the ordinary character table of a given centralizer ring. Also, some previously unsuspected properties of permutation characters emerge. Finally, the theory provides new insight into the relation of Brauer's theory of blocks to Green's work on indecomposable modules.

The purpose of this article is to present proofs of the results announced in [15]. Statements of these results have been included here, though a number of explanatory remarks and general background references have not been repeated.

With the exception of §0, the sections of this paper have been named according to the features of the classical modular theory with which they are most closely related.

**0. The centralizer ring.** Throughout this paper  $G$  is a finite group acting on a finite set  $\Omega$  (perhaps not transitively or faithfully) and  $p$  is a fixed prime.

If  $S$  is any commutative ring with identity, we define the  $S$ -centralizer ring  $V_S(G) = V_S(G, \Omega)$  to be the collection of all matrices with entries from  $S$  that commute with the permutation matrices determined (with respect to some fixed ordering of  $\Omega$ ) by elements of  $G$ . In case  $S$  is the ring of rational integers, we write only  $V(G)$  for  $V_S(G)$  and refer to  $V(G)$  as the *centralizer ring*. The *standard basis matrices*  $\{A_i\}_{i=1}^r$  are obtained from the full set  $\{O_i\}_{i=1}^r$  of orbits of  $G$  on  $\Omega \times \Omega$  by setting the  $\alpha, \beta$  entry of  $A_i$  equal to 1 for  $(\alpha, \beta) \in O_i$  and 0 otherwise. These matrices always form an  $S$ -basis for  $V_S(G)$ . In particular,  $V_S(G)$  is isomorphic to the tensor product  $SV(G)$ .

---

Received by the editors August 27, 1971.

AMS (MOS) subject classifications (1970). Primary 20C20; Secondary 16A26, 20C05.

Key words and phrases. Indecomposable module, vertex, centralizer ring, decomposition numbers, Brauer homomorphism, Brauer's first fundamental theorem, Green correspondence, Brauer's second fundamental theorem, defect group, defect 0 and 1, splitting field.

<sup>(1)</sup> Manuscript preparation supported by NSF-GP-9572.

The notation  $S\Omega$  refers to the usual  $S$ -free  $SG$  module obtained from the action of  $G$  on  $\Omega$ ; we regard  $S\Omega$  also as a  $V_S(G)$  module in the obvious way. (2)

In this paper  $S$  will usually be  $K$ ,  $R$ , or  $F$  where  $K$  is a  $p$ -adic number field,  $R$  is the ring of local integers in  $K$ , and  $F$  is the residue class field  $R/\pi R$ .  $\pi$  is a generator of the maximal ideal of  $R$ . We use the notation  $\bar{x}$  for the image of  $x$  under some (hopefully obvious) map  $X \rightarrow X/\pi X$  of an  $R$ -module  $X$  containing  $x$ .

$$(0.1) \quad \overline{V_R(G)} \cong V_F(G).$$

**Proof.** This is an immediate consequence of the isomorphism mentioned in the first paragraph.

(0.2) **Proposition 1.** *Let  $M, N$  be  $RG$ -indecomposable components of  $R\Omega$ . Then*

- (a)  $\overline{\text{Hom}_{RG}(M, N)} \cong \text{Hom}_{FG}(\bar{M}, \bar{N})$ .
- (b)  $\bar{M}$  is indecomposable and has the same vertex as  $M$ .

**Proof.** Of course the natural map  $\overline{\text{Hom}_{RG}(M, N)} \rightarrow \text{Hom}_{FG}(\bar{M}, \bar{N})$  is a monomorphism. Since the functor  $\text{Hom}$  is additive and  $\overline{V_R(G)} \cong V_F(G)$ , the map must be an isomorphism.

Now  $\text{Hom}_{RG}(M, M)$  is a completely primary ring, as is well known. Obviously, the isomorphism of  $\overline{\text{Hom}_{RG}(M, M)}$  with  $\text{Hom}_{FG}(\bar{M}, \bar{M})$  is a ring homomorphism; therefore  $\text{Hom}_{FG}(\bar{M}, \bar{M})$  contains only one idempotent—that is,  $\bar{M}$  is indecomposable.

If  $P$  is a subgroup of  $G$ , then we deduce easily from the above ring isomorphism and D. Higman's criterion [10, Theorem 1] that  $M$  is  $P$ -projective if and only if  $\bar{M}$  is  $P$ -projective. So by definition (see Green [7, 1.2])  $M$  has vertex  $P$  if and only if  $\bar{M}$  has vertex  $P$ .

Because of Proposition 1, many results we obtain for  $V_F(G)$  contain implicit analogues for  $V_R(G)$ .

**1. Decomposition numbers.** Let  $A$  be an  $R$  algebra (finitely generated as an  $R$  module) and  $M$  an  $R$ -free  $A$  module such that  $KM$  is completely reducible. Let  $B$  be an  $R$  algebra acting faithfully on  $M$  and inducing  $\text{End}_A(M)$  by its action.

We are interested in the case  $A = RG$ ,  $M = R\Omega$ ,  $B = V_R(G, \Omega)$ . However, the results in this section are purely formal and are accordingly given a more general treatment.

The following result is well known. The notation  $X|Y$  means  $X$  is isomorphic to a direct summand of  $Y$ .

(2) All "modules" are, by convention, finitely generated and acted upon on the right, with the exception that the action of a base ring such as  $S$  is written on the left.

(1.1) Let  $e, f$  be idempotents in  $B$ . Then the following statements are equivalent:

- (a)  $e = xfy$  for some  $x, y \in B$ .
- (b)  $Me \mid Mf$  (considered as  $A$  modules).
- (c)  $eB \mid fB$  (considered as  $B$  modules).

Accordingly we say that  $e$  and  $f$  are *equivalent* ( $e \sim f$ ) if  $e = xfy$  and  $f = zew$  for some  $x, y, z, w \in B$ . When  $e, f$  are primitive then  $e \sim f$  whenever one of the conditions (a), (b), (c) is satisfied.

Of course the preceding discussion is valid also for  $KA, KM, KB$  (and  $\bar{A}, \bar{M}, \bar{B}$  if  $\bar{B}$  induces  $\text{End}_{\bar{A}}(\bar{M})$ ).

By using equivalence classes of primitive idempotents as intermediaries we establish 1-1 correspondences  $[M_j] \leftrightarrow [U_j]$  and  $[X_s] \leftrightarrow [Z_s]$  between isomorphism classes of  $A$ -indecomposable components of  $M$  and projective indecomposable  $B$  modules, and between isomorphism classes of irreducible  $KA$  submodules of  $KM$  and irreducible  $KB$  modules.

Also there is a well-known 1-1 correspondence  $[U_j] \leftrightarrow [L_j]$  between isomorphism classes of projective indecomposable  $B$  modules and irreducible  $\bar{B}$  modules ( $L_j$  is the unique irreducible quotient module of  $\bar{U}_j$ ).

In view of these correspondences there are three kinds of "decomposition numbers" we can define:

(1) Let  $Z_s^0$  be an  $R$ -free  $B$  module with  $KZ_s^0 \approx Z_s$ . Then we list the composition factors of  $\bar{Z}_s^0$ , writing  $\bar{Z}_s^0 \leftrightarrow \sum_j \tilde{d}_{sj} L_j$ .

(2) Set  $KU_j \approx \sum_s d_{sj} Z_s$ .

(3) Set  $KM_j \approx \sum_s d_{sj}^M X_s$ .

(1.2) **Theorem 1.** Assume  $K, F$  are splitting fields for  $KB, \bar{B}$  respectively. Then  $\tilde{d}_{sj} = d_{sj} = d_{sj}^M$  for all  $s, j$ . Also  $M \approx \bigoplus_j (\dim_F L_j) M_j$ .

Note that the last assertion is a modular-theoretic version of the familiar  $KM \approx \sum_s (\dim_K Z_s) X_s$ .

**Proof.** The equality  $\tilde{d}_{sj} = d_{sj}$  is well known [2, IX, 8]. Let  $u \in B$  be a primitive idempotent with  $Mu \approx M_j$ . Now the following two assertions are easily verified:

(i) For each nonnegative integer  $d$ ,  $dZ_s \mid uKB$  if and only if there exists a set of  $d$  orthogonal primitive idempotents in  $uKBu$  each equivalent to an idempotent  $f$  with  $fKB \approx Z_s$ .

(ii) For each nonnegative integer  $d$ ,  $dX_s \mid KM_u$  if and only if there exists a set of  $d$  orthogonal primitive idempotents in  $uKBu$  each equivalent to an idempotent  $f$  with  $KMf \approx X_s$ . By definition  $fKB \approx Z_s$  if and only if  $KMf \approx X_s$ . Thus  $d_{sj} = d_{sj}^M$ .

To finish the proof we make two further observations:

(iii) For each nonnegative integer  $l$ ,  $lM_j | M$  if and only if there exists a set of  $l$  orthogonal primitive idempotents in  $B$  each equivalent to  $u$ .

(iv) The multiplicity of  $\bar{U}_j$  as a component of  $\bar{B}$  is  $\dim_F L_j$  (see the argument on p. 419 of [4]).

The final assertion of the theorem is an obvious consequence.

The following proposition clarifies the hypothesis of Theorem 1.

(1.3)  $\text{End}_{KB}(Z_s)$ ,  $\text{End}_{\bar{B}}(L_j)$  are anti-isomorphic to  $\text{End}_{KA}(X_s)$ ,  $\text{End}_A(M_j)/\text{Rad}(\text{End}_A(M_j))$  respectively.

In particular  $K$  is a splitting field for  $KB$  if and only if each  $X_s$  is absolutely irreducible, and  $F$  is a splitting field for  $\bar{B}$  if and only if each  $M_j$  is absolutely indecomposable.

**Proof.** Let  $e \in B$  be a primitive idempotent. Then of course  $eBe \approx \text{End}_A(Me)$ . But also the left multiplications by members of  $eBe$  form  $\text{End}_B(eB)$ . Hence  $\text{End}_A(Me)$  is anti-isomorphic to  $\text{End}_B(eB)$ .

Since  $eB$  is projective,  $\text{End}_B(eB/e \text{ Rad}(B))$  is a homomorphic image of  $\text{End}_B(eB)$ . Since the latter is completely primary,

$$\text{End}_B(eB)/\text{Rad}(\text{End}_B(eB)) \approx \text{End}_B(eB/e \text{ Rad}(B)).$$

This proves the assertion regarding  $\text{End}_{\bar{B}}(L_j)$ ; the statement regarding  $\text{End}_{KB}(Z_s)$  is established by the first paragraph of the same argument.

**2. Defect groups.** Let  $A_i$  be a standard basis matrix. We define "the" defect group  $D_i$  of  $A_i$  to be a Sylow  $p$ -subgroup of  $G_{\alpha\beta}$  where  $(\alpha, \beta) \in O_i$ . (Defect groups are well defined only up to conjugation by elements of  $G$ .)

Set  $A_i A_j = \sum_k a_{ijk} A_k$  (in  $V(G)$ ). The quantities  $a_{ijk}$  are the "intersection numbers" defined by D. Higman [11]. We have

$$(2.1) \quad a_{ijk} = |O_i(\alpha) \cap O_j^*(\beta)| \quad \text{where } (\alpha, \beta) \in O_k.$$

Here  $O_i(\alpha) = \{\beta \mid (\alpha, \beta) \in O_i\}$  and  $O_j^* = O_{j*} = \{(\beta, \alpha) \mid (\alpha, \beta) \in O_j\}$ . The proof of (2.1) is a direct matrix calculation from the definition of the  $A_i$ 's.

(2.2) If  $a_{ijk} \neq 0(p)$  then  $D_k \leq_G D_i$  and  $D_k \leq_G D_j$ . (The notation " $\leq_G$ " means " $\leq$  a  $G$ -conjugate of.")

**Proof.**  $G_{\alpha\beta}$  acts on  $O_i(\alpha) \cap O_j^*(\beta)$  and hence so does (a suitable)  $D_k$ . If  $|O_i(\alpha) \cap O_j^*(\beta)| \neq 0(p)$  then  $D_k$  must fix a letter  $\gamma \in O_i(\alpha) \cap O_j^*(\beta)$ . Thus  $D_k$  fixes  $(\alpha, \gamma) \in O_i$  and  $(\gamma, \beta) \in O_j$ . The result now follows from Sylow's theorem.

For any  $p$ -subgroup  $P$  of  $G$  we define  $I_F(P) = I_F(P; G, \Omega)$  to be the set of  $F$ -linear combinations of  $A_i$ 's satisfying  $D_i \leq_G P$ .

**Lemma 1.** For  $P, Q$ ,  $p$ -subgroups of  $G$ ,

$$(2.3) \quad I_F(P)I_F(Q) \leq \sum_{D_i \leq_G P; D_i \leq_G Q} I_F(D_i).$$

**Proof.** Immediate from (2.2).

Now, given a primitive idempotent  $e \in V_F$ , there is an index  $i$  such that  $e \in I_F(D_i)$  and  $D_i \leq_G P$  whenever  $e \in I_F(P)$ . We set  $D(e) = {}_G D_i$  and call  $D(e)$  "the" defect group of  $e$ . (See Green's proof [7, 3.3b] for a discussion of how Lemma 1 guarantees the legitimacy of our definition of defect group.)

$D(e)$  is also the defect group of any idempotent equivalent to  $e$ . This is easily verified directly, or may be seen as a consequence of the next result.

**Proposition 2.**  $D(e)$  is the vertex of  $F\Omega e$ .

To prove Proposition 2 we need an alternate description of the ideals  $I_F(P)$ . Define  $N_{G,H}(x)$ , for  $H \leq G$  and  $x \in V_F(H, \Omega)$ , to be  $\sum x^g$  where  $g$  ranges over a set of right coset representatives of  $H$  in  $G$  (here  $x^g \in V_F(H^g, \Omega)$  is defined in the obvious way).<sup>(3)</sup> Clearly  $N_{G,H}(x) \in V_F(G, \Omega)$ .

$$(2.4) \quad I_F(P; G, \Omega) = N_{G,P}(V_F(P, \Omega)).$$

**Proof.** For  $\alpha, \beta \in \Omega$  let  $e_{\alpha, \beta}$  denote the  $|\Omega| \times |\Omega|$  matrix with 1 in the  $\alpha, \beta$  position and 0 everywhere else. Obviously,  $e_{\alpha, \beta} \in V_F(H, \Omega)$  whenever  $H \leq G_{\alpha\beta}$ . It is easy to calculate that, for  $(\alpha, \beta) \in O_i$  and  $D_i \leq G_{\alpha\beta}$ ,  $A_i = N_{G, D_i}(x)$  where  $x = [G_{\alpha\beta} : D_i]^{-1} e_{\alpha, \beta}$ . Thus if  $D_i \leq P$  we have  $A_i = N_{G, P}(N_{P, D_i}(x)) \in N_{G, P}(V_F(P, \Omega))$ . Consequently  $I_F(P; G, \Omega) \subseteq N_{G, P}(V_F(P, \Omega))$ .

Next let  $a \in V_F(P, \Omega)$  be a standard basis matrix. As above we calculate  $a = N_{P, d}(e_{\alpha\beta})$  where  $(\alpha, \beta)$  belongs to the orbit of  $P$  on  $\Omega \times \Omega$  corresponding to  $a$  and  $d = P_{\alpha\beta}$ . Now

$$N_{G, P}(a) = N_{G, d}(e_{\alpha\beta}) = N_{G, G_{\alpha\beta}}(N_{G_{\alpha\beta}, d}(e_{\alpha\beta})) = N_{G, G_{\alpha\beta}}([G_{\alpha\beta} : d]e_{\alpha\beta}).$$

Thus  $N_{G, P}(a) = 0$  if  $d$  is not a Sylow subgroup of  $G_{\alpha\beta}$ , and  $N_{G, P}(a)$  is a multiple of the standard basis matrix in  $V_F(G, \Omega)$  corresponding to  $(\alpha, \beta)^G$  if  $d$  is a Sylow subgroup of  $G_{\alpha\beta}$ . In either case  $N_{G, P}(a) \in I_F(P; G, \Omega)$  and so  $N_{G, P}(V_F(P, \Omega)) \subseteq I_F(P; G, \Omega)$ .

(2.5) **Proof of Proposition 2.** This follows from (2.4) and the definition of  $D(e)$  because of D. Higman's criterion [10, Theorem 1]. See also Green [9, p. 143].

(2.6) **Remarks.** (a) Note that if  $e_0 \in V_R(G, \Omega)$  is a primitive idempotent with  $\bar{e}_0 = e$ , then  $D(e)$  is also a vertex of  $R\Omega e_0$  by Proposition 1.

(b) An alternate proof of Lemma 1 can be given by (2.4) and Green's formula [9, 4.11].

If  $F$  is a splitting field for  $V_F$  and  $e \in V_F$  is a primitive idempotent, then there is a unique irreducible modular character<sup>(4)</sup>  $\lambda$  of  $V_F$  satisfying  $\lambda(e) = 1$ .

<sup>(3)</sup> We follow Feit's notation [5]. The analogous notation in Green [7] is  $T_{G:H}(x)$ , and  $T_{H,G}(x)$  in Green [9].

<sup>(4)</sup> Throughout this paper the term "character" refers to the trace function obtained from a module.

This leads to a second characterization of defect groups.

**Proposition 3.** *Assume  $F$  is a splitting field for  $V_F$ . Let  $e, e' \in V_F$  be primitive idempotents, and let  $\lambda, \lambda'$  be the associated modular characters. Then*

- (1)  $\lambda(xA_i) = 0$  for all  $x \in V_F$  unless  $D_i \geq_G D(e)$ .
- (2)  $\lambda(A_i) \neq 0$  for some  $i$  with  $D_i =_G D(e)$ .
- (3)  $e$  is equivalent to  $e'$  if and only if  $D(e) =_G D(e')$ , and  $\lambda(A_i) = \lambda'(A_i)$  for all  $i$  with  $D_i =_G D(e)$ .

Before giving the proof we establish a general fact which will be used again in §6.

(2.7) Suppose  $\lambda$  is the character afforded by an absolutely irreducible representation of a finite dimensional  $F$ -algebra  $A$ , and  $e \in A$  is a primitive idempotent with  $\lambda(e) \neq 0$ . Then the restriction of  $\lambda$  to  $eAe$  is an algebra homomorphism.

**Proof.** Let  $\mathfrak{L}$  be a matrix representation affording  $\lambda$ . Then  $\mathfrak{L}(e)$  is still a primitive idempotent in  $\mathfrak{L}(A)$ , as is well known. Thus by suitably choosing  $\mathfrak{L}$  we may assume that  $\mathfrak{L}(e)$  has a 1 in the upper left-hand corner and 0's everywhere else. Hence for  $x \in eAe$ ,  $\lambda(x)$  is the upper left-hand corner entry of  $\mathfrak{L}(x)$ , and all other entries are 0. The result is now obvious.

(2.8) **Proof of Proposition 3.** (1) If  $D_i \not\leq_G D(e)$  then  $e \notin I_F(D_i; G, \Omega)$  by definition of  $D(e)$ . Thus  $I_F(D_i; G, \Omega) \cap eV_F e$  is contained in the kernel of  $\lambda|_{eV_F e}$ . So  $\lambda(exA_i) = \lambda(exA_i e) = 0$  for all  $x \in V_F$ . Clearly the same equation holds if  $e$  is replaced by an equivalent idempotent. But an idempotent not equivalent to  $e$  is in the kernel of any representation affording  $\lambda$ . Since  $\lambda(xA_i) = \lambda(1xA_i)$  and 1 is a sum of primitive idempotents, the proof of (1) is complete.

(2) By definition  $e$  is an  $F$ -linear combination of standard basis matrices  $A_i$  with  $D_i \leq_G D(e)$ . Since  $\lambda(e) \neq 0$ , and  $\lambda(A_i) = 0$  whenever  $D_i <_G D(e)$  by (1), we must have  $\lambda(A_i) \neq 0$  for some  $i$  with  $D_i =_G D(e)$ .

(3) Suppose  $D(e) =_G D(e')$  and  $\lambda(A_i) = \lambda'(A_i)$  for all  $i$  with  $D_i =_G D(e)$ . Since  $\lambda$  and  $\lambda'$  vanish on matrices  $A_i$  with  $D_i <_G D(e)$ , and  $e$  is an  $F$ -linear combination of matrices  $A_i$  with  $D_i \leq_G D(e)$ , we have  $\lambda'(e) = \lambda(e) = 1$ . Thus  $e'$  must be equivalent to  $e$ . The converse is almost trivial.

The following theorem depends on Theorem 3 in §4.

(2.9) **Theorem 2.** *A necessary condition that  $D$  be the vertex of an indecomposable component of  $F\Omega$  is that there exists  $\alpha \in \Omega$  and  $y \in N_G(D)$  such that  $D$  is a Sylow  $p$ -subgroup of  $G_{\alpha y}$ .*

**Proof** (assuming Theorem 3 (and Proposition 5)). By Theorem 3 and the remark following its proof we can assume  $G = N_G(P)$ . Since any indecomposable component of  $F\Omega$  is a component of  $F\Gamma$  for some orbit  $\Gamma$  of  $G$  on  $\Omega$ , we can assume  $G$  is transitive. By Proposition 2 and the definition of defect group,  $P$  is a Sylow subgroup of  $G_{\alpha\beta}$  for some  $\alpha, \beta \in \Omega$ .

**3 The Brauer homomorphism.** Suppose  $P \leq H \leq N_G(P)$  where  $P$  is a  $p$ -group, and let  $\Omega_P$  denote the set of fixed points of  $P$  in  $\Omega$ . Then there is a natural homomorphism  $f = f_{(G, \Omega, P, H)}$  mapping  $V_F(G, \Omega)$  into  $V_F(H, \Omega_P)$ : First define  $f$  in the special case  $G = H$ —if  $O_i \subseteq \Omega_P \times \Omega_P$  define  $f(A_i)$  to be the standard basis matrix for  $(H, \Omega_P)$  corresponding to  $O_i$ , and otherwise set  $f(A_i) = 0$ ; then extend the definition of  $f$  to  $V_F(H, \Omega)$  by linearity.  $f$  is now defined in the general case as the composite of the natural inclusion  $V_F(G, \Omega) \rightarrow V_F(H, \Omega)$  and  $f_{(H, \Omega, P, H)}$ .

We give the verification that  $f_{(H, \Omega, P, H)}$  is a homomorphism: Note that  $O_i \subseteq \Omega_P \times \Omega_P$  if and only if  $P \leq D_i$ . Set  $J = \sum_{P \leq D_i} I_F(D_i; H, \Omega)$  and let  $B$  denote the set of all  $F$ -linear combinations of standard basis matrices  $A_i$  in  $V_F(H, \Omega)$  satisfying  $O_i \subseteq \Omega_P \times \Omega_P$ . Then  $B$  is an algebra isomorphic to  $V_F(H, \Omega_P)$  in an obvious way, and  $J$  is an ideal in  $V_F(H, \Omega)$  by Lemma 1. Trivially,  $V_F(H, \Omega) = J + B$  and  $J \cap B = 0$ . The map  $f$  is clearly the composite of the natural projection  $V_F(H, \Omega) \rightarrow B$  and the obvious isomorphism  $B \rightarrow V_F(H, \Omega_P)$ . Thus  $f$  is a homomorphism.

If  $A \in V_F(G)$  then the restriction  $V_F(G) \rightarrow V_F(H)$  carries  $A$  into  $J$  if and only if  $A = \sum_{i=1}^r c_i A_i$  where  $O_i \cap \Omega_P \times \Omega_P = \emptyset$ —that is,  $P \not\leq D_i$ —whenever  $c_i \neq 0$ . Now the above proof gives

(3.1) *The kernel of  $f_{(G, \Omega, P, H)}$  is  $\sum_{P \not\leq D_i} I_F(P; G, \Omega)$ .*

The relationship between  $f$  and the classical Brauer homomorphism is described below. (See also [15, footnote 8].)

**Proposition 4.** *Assume  $C_G(P) \leq H$  and let  $s: Z(FG) \rightarrow Z(FH)$  be the standard Brauer homomorphism. Then the following diagram is commutative:*

$$\begin{array}{ccc} Z(FG) & \longrightarrow & V_F(G, \Omega) \\ s \downarrow & & \downarrow f \\ Z(FH) & \longrightarrow & V_F(H, \Omega_P) \end{array}$$

If  $C \subseteq G$  we write  $\underline{C}$  for the  $R$ -sum of all permutation matrices corresponding to members of  $C$ . Thus, if  $C$  is a conjugacy class of  $G$ ,  $\underline{C}$  is the image of the class sum  $\hat{C} \in Z(RG)$  under the map  $Z(RG) \rightarrow V_R(G)$ . To prove Proposition 4 we need to calculate  $\underline{C}$  in terms of standard basis matrices. This has essentially been done by Tamaschke (for the transitive case, in the formalism of  $S$ -rings [16]). We give an alternate approach more suitable to the present formalism by using the "orbital character" notation.

For  $i = 1, \dots, r$  we define  $\theta_i(g) = |\{\alpha \in \Omega \mid (\alpha, \alpha^g) \in O_i\}|$  for each  $g \in G$  (as in Scott [14]). Of course  $\theta_i$  is identically 0 unless  $O_i \subseteq \alpha^G \times \alpha^G$  for some  $\alpha \in \Omega$ .

(3.2) (Scott [13, 2.2])  $\theta_i(g)$  is the trace of  $g A_i^*$  acting on  $R\Omega$ .

The proof is a direct calculation from the definition of  $A_i^*$ .

(3.3)  $\underline{C} = \sum_i (|O_i|^{-1} \sum_{x \in C} \theta_i(x)) A_i$ , whenever  $C$  is a union of  $G$ -conjugacy classes.

**Proof.** Certainly we can express  $\underline{C} = \sum_i c_i A_i$  for some coefficients  $c_i \in R$ . A particular coefficient  $c_i$  is computed by multiplying  $\underline{C}$  by  $A_i^*$  and taking the trace (the trace of  $A_j A_i^*$  on  $R\Omega$  is easily calculated to be  $\delta_{ij} |O_i|$ ; see Wielandt [18, V]).

(3.4) (Scott [13, 2.7.9]) Suppose  $C$  is a union of  $G$ -conjugacy classes. Fix  $\alpha, \beta \in O_i$ . Then  $|O_i|^{-1} \sum_{x \in C} \theta_i(x) = |\{x \in C \mid \alpha^x = \beta\}|$ .

**Proof.** Count the number of triples  $(\gamma, \delta, x)$  with  $(\gamma, \delta) \in O_i$ ,  $x \in C$ , and  $\gamma^x = \delta$ . Counting in terms of  $x$  gives a total  $\sum_{x \in C} \theta_i(x)$ . Counting in terms of  $(\gamma, \delta)$  gives  $|O_i| |\{x \in C \mid \alpha^x = \beta\}|$ .

(3.5) **Proof of Proposition 4.** Fix a conjugacy class  $C$  of  $G$  and a standard basis matrix  $a \in V_F(H, \Omega_P)$ . Let  $\alpha, \beta \in \Omega_P$  be such that  $(\alpha, \beta)^H$  corresponds to  $a$ .

Then the  $a$ -coefficient of  $f(\underline{C})$  is  $|\{x \in C \mid \alpha^x = \beta\}|$  by (3.3) and (3.4). Now  $s(\underline{C})$  is by definition  $\underline{C} \cap C_G(P)$ . The  $a$ -coefficient of  $\underline{C} \cap C_G(P)$  is  $|\{x \in C \cap C_G(P) \mid \alpha^x = \beta\}|$ , again by (3.3) and (3.4). Since  $P$  fixes  $\alpha, \beta$  and centralizes no member of  $C - C \cap C_G(P)$ , we deduce

$$|\{x \in C \mid \alpha^x = \beta\}| \equiv |\{x \in C \cap C_G(P) \mid \alpha^x = \beta\}| \quad (p).$$

Thus the two  $a$ -coefficients are equal. Since  $C$  and  $a$  were arbitrary, the commutativity of the diagram is established.

The following two propositions describe elementary properties of  $f_{(G, \Omega, P, H)}$ .

(3.6) **Proposition 5.** Let  $e \in V_F(G)$  be a primitive idempotent. Then  $f(e) \neq 0$  if and only if  $D(e) \geq_G P$ .

**Proof.** If  $f(e) = 0$  then  $e \in \sum_{P \not\leq_G D_i} I_F(D_i; G, \Omega)$  by (3.1). Hence  $e \in I_F(D_i; G, \Omega)$ —consequently  $D(e) \leq_G D_i$ —for some  $i$  with  $D_i \not\leq_G P$  by Green [7, 3.3a]. Since  $P \not\leq_G D_i$  we have  $P \not\leq_G D(e)$ .

If  $f(e) \neq 0$  then  $f(I_F(D(e); G, \Omega)) \neq 0$ , since  $e \in I_F(D(e); G, \Omega)$ , and so  $P \leq_G D_i$  by (3.1).

(3.7) **Proposition 6.** Let  $e \in V_F(G)$  be a primitive idempotent with  $f(e) \neq 0$ . If  $N$  is an indecomposable component of  $F\Omega_P f(e)$ , then some  $D(e)$  contains a vertex of  $N$ . If  $C_G(P) \leq H$  then  $N$  lies in a block  $b$  of  $H$  such that  $F\Omega e$  is in  $b^G$ .<sup>(5)</sup>

**Proof.** It is easy to check that, for any  $i$ ,  $f(A_i)$  is a sum of standard basis matrices with defect group contained in a  $G$ -conjugate of  $D_i$ . Thus  $f(e) \in \sum_{Q \leq_G D(e)} I_F(Q; H, \Omega_P)$ .

<sup>(5)</sup> See Brauer [3, §2] for a definition of  $b^G$ .



Set  $f(e) = \sum_j e_j$  where the  $e_j$ 's are primitive orthogonal idempotents. Then  $N \approx F\Omega_P e_j$  for some  $j$  by the Krull-Schmidt theorem, and the vertex of  $N$  is  $D(e_j)$  by Proposition 2. Since  $f(e)e_j = e_j$  we have  $e_j \in \sum_{Q \leq_G D(e)} I_F(Q; H, \Omega_P)$ . So  $e_j \in I_F(Q; H, \Omega_P)$  for some  $Q \leq_G D(e)$  by Green [7, 3.3a]. Hence  $D(e_j) \leq_H Q \leq_G D(e)$ .

Now suppose  $C_G(P) \leq H$  so that the standard Brauer homomorphism  $s: Z(FG) \rightarrow Z(FH)$  is defined. Let  $c \in Z(FG)$  be a primitive idempotent whose image  $\underline{c}$  under the map  $Z(FG) \rightarrow V_F(G)$  satisfies  $e_{\underline{c}} = e$  (thus  $(F\Omega e)c = F\Omega e$  and so  $F\Omega e$  belongs to the block associated with  $\underline{c}$ ). Then  $f(e) = f(e_{\underline{c}}) = f(e)f(\underline{c}) = f(e)\underline{s(c)}$  by Proposition 4. Hence  $e_j = e_j f(e) = e_j f(e)\underline{s(c)} = e_j \underline{s(c)}$ ; consequently  $(F\Omega_P e_j)s(c) = F\Omega_P e_j$ . By [3, paragraph following 4.16], the proof is complete.

The following fact is also worth noting.

(3.8) Any indecomposable component of  $F\Omega_P$  is isomorphic to a component of  $F\Omega_P f(e)$  for some primitive idempotent  $e \in V_F(G)$ .

**Proof.** Since  $f(1) = 1$ , a decomposition  $1 = \sum_k e_k$  into primitive orthogonal idempotents in  $V_F(G)$  leads to a decomposition  $1 = \sum_{f(e_k) \neq 0} f(e_k)$  into orthogonal idempotents in  $V_F(H, \Omega_P)$ . The result now follows from the Krull-Schmidt theorem.

At this stage of our development we sacrifice a little simplicity for the sake of obtaining more detailed information.

**The 1-1 condition.** A  $p$ -group  $Q \geq_G P$  satisfies the 1-1 condition with respect to  $(G, \Omega, P, H)$  if  $P \leq_G D_i$  whenever  $D_i \leq_G Q$ .

**The onto condition.** A  $p$ -group  $Q \geq_G P$  satisfies the onto condition with respect to  $(G, \Omega, P, H)$  if  $o^G \cap \Omega_P \times \Omega_P = o$  whenever  $o$  is an orbit of  $H$  on  $\Omega_P \times \Omega_P$  whose associated defect group  $d$  satisfies  $d \leq_G Q$ .

If  $P$  contains no proper subgroup conjugate to any  $D_i$ , then  $P$  satisfies the 1-1 condition with respect to  $(G, \Omega, P, H)$ .

If  $H = N_G(P)$ , and if  $P = Q$  (or more generally, if  $P$  is weakly closed in  $Q$  with respect to  $G$ ), then  $Q$  satisfies the onto condition with respect to  $(G, \Omega, P, H)$ .

(3.9) We insert here a proof that  $Q$  satisfies the onto condition with respect to  $(G, \Omega, P, H)$  when  $H = N_G(P)$  and  $P$  is weakly closed in  $Q$  with respect to  $G$ . Let  $o$  be an orbit of  $H$  on  $\Omega_P \times \Omega_P$  whose associated defect group  $d$  is contained in a conjugate of  $Q$ . Then a straightforward argument shows  $P$  is weakly closed in  $d$ . In particular  $N_G(d) \leq H$ , so  $d$  is a full Sylow subgroup of  $G_{\alpha\beta}$  for  $(\alpha, \beta) \in o$ . We now easily deduce that any  $G$ -conjugate of  $P$  contained in  $G_{\alpha\beta}$  is  $G_{\alpha\beta}$ -conjugate to  $P$ . By the Jordan-Frattini argument (see [18, proof of 3.5])  $H$  is transitive on the fixed points of  $P$  in  $o^G$ . That is,  $o^G \cap \Omega_P \times \Omega_P = o$ .

If  $e$  is any idempotent in  $V_F(G)$ , we let  $\Psi_e$  denote the character of  $G$  afforded by  $K\Omega e_0$  where  $e_0$  is an idempotent in  $V_R(G)$  satisfying  $\bar{e}_0 = e$ . In addition we define  $\Psi_e = 0$  for  $e = 0$ .

**Proposition 7.** Suppose  $Q$  satisfies the 1-1 condition with respect to  $(G, \Omega, P, H)$ . Let  $e, e'$  be idempotents in  $V_F(G)$ , and assume that  $e$  is primitive with  $D(e) =_G Q$ . Then

$$(\Psi_e, \Psi_{e'})_G \leq (\Psi_{f(e)}, \Psi_{f(e')})_H.$$

**Proposition 8.** Suppose  $Q$  satisfies the onto condition with respect to  $(G, \Omega, P, H)$ . Let  $e, e'$  be idempotents in  $V_F(G)$ , and assume that  $e$  is primitive with  $D(e) =_G Q$ . Then

$$(\Psi_e, \Psi_{e'})_G \geq (\Psi_{f(e)}, \Psi_{f(e')})_H.$$

The following standard fact is needed for the proofs of Propositions 7 and 8.

(3.10) Suppose  $e, e' \in V_F(G)$ , and  $e^2 = e, (e')^2 = e'$ . Then  $(\Psi_e, \Psi_{e'}) = \dim_F eV_F(G)e'$ .

**Proof.** The assertion is trivial in case  $e$  or  $e'$  is 0; consequently, we may assume  $e, e'$  are idempotents. Let  $u, u'$  be idempotents in  $V_R(G)$  with  $\bar{u} = e, \bar{u}' = e'$ . Let  $\tilde{K}$  be a splitting field for  $V_{\tilde{K}}(G)$ . Then obviously  $(\Psi_e, \Psi_{e'}) = \dim_{\tilde{K}} (\text{Hom}_{\tilde{K}G}(\tilde{K}\Omega u, \tilde{K}\Omega u'))$ , and  $\text{Hom}_{\tilde{K}G}(\tilde{K}\Omega u, \tilde{K}\Omega u') \cong uV_{\tilde{K}}u'$ . Since  $V_{\tilde{K}} \cong K \otimes_R V_R$  and  $uV_Ru'$  is an  $R$ -direct summand of  $V_R$ , we have

$$\dim_{\tilde{K}} uV_{\tilde{K}}u' = \text{rank}_R uV_Ru' = \dim_F \overline{uV_Ru'} = \dim_F eV_Fe'.$$

(3.11) **Proof of Proposition 7.** By (3.1) and our hypothesis, the kernel of  $f$  intersects the ideal  $I_F(Q; G, \Omega)$  trivially. Since  $e \in I_F(Q; G, \Omega)$  we have  $eV_Fe' \subseteq I_F(Q; G, \Omega)$ . Thus  $eV_Fe' \approx f(eV_Fe') \subseteq f(e)V_F(H, \Omega_P)f(e')$ . Application of (3.10) now finishes the proof.

(3.12) **Proof of Proposition 8.** Set  $J = \sum_{d \leq GQ} I_F(d; H, \Omega_P)$ . Then  $J$  is an ideal in  $V_F(H, \Omega_P)$ , and  $J \subseteq f(V_F(G))$  by hypothesis. By Proposition 6 (or direct calculation) we have  $f(e) \in J$ . Thus

$$f(e)V_F(H, \Omega_P)f(e') \subseteq f(e)f(V_F(G))f(e') \subseteq f(e)V_F(H, \Omega_P)f(e').$$

Therefore  $f(e)V_F(H, \Omega_P)f(e') = f(e)f(V_F(G))f(e') = f(eV_F(G)e')$ . Again application of (3.10) completes the proof.

The next section is devoted to further consequences of the onto condition.

**4. Brauer's first fundamental theorem.** We assume throughout this section that  $Q$  satisfies the onto condition with respect to  $(G, \Omega, P, H)$ .  $P \leq H \leq N_G(P)$  and  $f = f_{(G, \Omega, P, H)}$  as in §3.

(4.1) **Theorem 3.** (a) Let  $e, e'$  be idempotents in  $V_F(G, \Omega)$  with  $e$  primitive and  $D(e) =_G Q$ . Then  $f(e)$  is primitive, and  $F\Omega e | F\Omega e'$  if and only if  $F\Omega_P f(e) | F\Omega_P f(e')$ .

(b) In case  $H = N_G(P)$  and  $\tilde{e} \in V_F(H, \Omega_P)$  is a primitive idempotent with  $D(\tilde{e}) = P$ , then  $\tilde{e}$  is equivalent to  $f(e)$  for some primitive  $e \in V_F(G)$  with  $D(e) =_G P$ .

**Proof.** (a) We shall use the fact established in (3.12) that  $f(eV_F(G)e') = f(e)V_F(H, \Omega_P)f(e')$ . Of course we also have  $f(e'V_F(G)e) = f(e')V_F(H, \Omega_P)f(e)$ .

Since  $eV_F(G)e$  is completely primary, so is  $f(eV_F(G)e) = f(e)V_F(H, \Omega_P)f(e)$ . Hence  $f(e)$  is a primitive idempotent. ( $f(e) \neq 0$  by Proposition 5.)

If  $F\Omega f(e)|F\Omega f(e')$  we have  $f(e) = zf(e')w$  where  $z \in f(e)V_F(H, \Omega_P)f(e')$  and  $w \in f(e')V_F(H, \Omega_P)f(e)$ . Choose  $x \in eV_F(G)e'$  and  $y \in e'V_F(G)e$  with  $f(x) = z$  and  $f(y) = w$ . Then  $xe'y \in eV_F(G)e$ , and no power of  $xe'y$  is 0 since  $f(xe'y) = zf(e')e = f(e)$ . Thus  $xe'y$  is a unit in  $eV_F(G)e$ . Consequently  $F\Omega e|F\Omega e'$ .

Conversely if  $F\Omega e|F\Omega e'$ , then  $e = ue'v$  for some  $u, v \in V_F(G)$ . Hence  $f(e) = f(u)f(e')f(v)$  and so  $F\Omega f(e)|F\Omega f(e')$ .

(b) By the remark following Proposition 6 we have  $\tilde{e} = zf(e)w$  for some  $z \in \tilde{e}V_F(H, \Omega_P)$ ,  $w \in V_F(H, \Omega_P)\tilde{e}$  and a primitive idempotent  $e \in V_F(G)$ . Since  $\tilde{e}$  belongs to the ideal  $I_F(P; H, \Omega_P)$  by hypothesis, we have  $z, w \in I_F(P; H, \Omega_P)$ .

By Sylow's theorem  $P$  is a Sylow  $p$ -subgroup of  $G_{\alpha\beta}$  if and only if  $P$  is a Sylow  $p$ -subgroup of  $H_{\alpha\beta}$ ; when this occurs  $H$  is transitive on the nonempty set  $(\alpha, \beta)^G \cap \Omega_P \times \Omega_P$ . Now we easily deduce that  $f(I_F(P; G, \Omega)) = I_F(P; H, \Omega)$ . Hence we can choose  $x, y \in I_F(P; G, \Omega)$  such that  $z = f(x)$  and  $w = f(y)$ .

Thus  $eyxe \in eV_F(G)e \cap I_F(P; G, \Omega)$ . Since  $f(xey) = zf(e)w = \tilde{e}$  we see that no power of  $eyxe$  is 0. Consequently  $eyxe$  is a unit in the completely primary ring  $eV_F(G)e$ . Therefore  $eV_F(G)e = eV_F(G)e \cap I_F(P; G, \Omega)$ , and we conclude that  $e \in I_F(P; G, \Omega)$ .

By part (a),  $f(e)$  is a primitive idempotent. Clearly  $f(e)$  is equivalent to  $\tilde{e}$ .

Since  $e \in I_F(P; G, \Omega)$  we have  $D(e) \leq_G P$ . But  $f(e) \neq 0$  so  $D(e) \geq_G P$  by Proposition 5. Thus  $D(e) =_G P$  and the proof is complete.

The previous theorem and Proposition 5 show that  $f$  establishes a 1-1 correspondence between equivalence classes of primitive idempotents in  $V_F(G, \Omega)$  and  $V_F(N_G(P), \Omega_P)$  with defect group  $P$ . This correspondence will now be identified with the help of a lemma in the next section.

**Proposition 9.** Suppose  $H = N_G(P)$  and  $e \in V_F(G)$  is a primitive idempotent with  $D(e) =_G P$ . Then  $F\Omega_P f(e)$  is the Green correspondent<sup>(6)</sup> of  $F\Omega e$ . In particular

$$\Psi_e(1) \equiv [G : H]\Psi_{f(e)}(1) \quad (p^{\nu_p([G : P]) + 1}).$$

The following preliminary result is an easy application of Proposition 1; the details are left to the reader.

(4.2) Suppose the  $RG$  modules  $X, Y$  are direct summands of  $R\Omega$ . Then  $X$  is isomorphic to a direct summand of  $Y$  if and only if  $\bar{X}$  is isomorphic to a direct summand of  $\bar{Y}$ .

(6) See [8, Theorem 2].

Now we use (4.2) to prepare for the proof of Proposition 9.

(4.3) Let  $X$  be an  $N_G(P)$ -indecomposable component of  $R\Omega_{N_G(P)}$ , and  $Y$  a  $G$ -indecomposable component of  $R\Omega$  with vertex  $P$ . Then  $X$  is the Green correspondent of  $Y$  if and only if  $\bar{X}$  is the Green correspondent of  $\bar{Y}$ .

**Proof.** Of course  $\bar{Y}$  is indecomposable with vertex  $P$  by Proposition 1.

If  $X$  is the Green correspondent of  $Y$ , then  $X|Y_{N_G(P)}$  and  $X$  has vertex  $P$ . Thus  $\bar{X}|Y_{N_G(P)}$  and  $\bar{X}$  is indecomposable with vertex  $P$  by Proposition 1, and so  $\bar{X}$  is the Green correspondent of  $\bar{Y}$ .

Conversely if  $\bar{X}$  is the Green correspondent of  $\bar{Y}$ , then  $\bar{X}|Y_{N_G(P)}$  and  $\bar{X}$  has vertex  $P$ . Therefore  $X$  has vertex  $P$  by Proposition 1, and  $X|Y_{N_G(P)}$  by (4.2) applied to  $N_G(P)$ . Hence  $X$  is the Green correspondent of  $Y$ .

(4.4) **Proof of Proposition 9 (assuming Lemma 2).** Lemma 2 gives  $F\Omega f(e)|(F\Omega e)_H$ .

Trivially  $P \leq D(f(e))$ , and  $D(f(e)) \leq_G P$  by Proposition 6. Thus  $D(f(e)) =_G P$ , and so  $F\Omega_p f(e)$  is the Green correspondent of  $F\Omega e$ .

Now choose primitive idempotents  $u, v$  in  $V_R(G)$ ,  $V_R(H, \Omega_P)$  respectively, with  $\bar{u} = e$  and  $\bar{v} = f(e)$ . Thus  $\overline{R\Omega u} \cong F\Omega e$  and  $\overline{R\Omega_P v} \cong F\Omega_P f(e)$ . By Proposition 1,  $R\Omega u$  has vertex  $P$ , and by (4.3)  $R\Omega_P v$  is the Green correspondent of  $R\Omega u$ . Thus  $(R\Omega_P v)^G$  is the direct sum of  $R\Omega u$  and indecomposable modules with vertex conjugate to a proper subgroup of  $P$ . The stated congruence on character degrees now follows from Green [7, Theorem 3].

(4.5) **Theorem 4.** Assume  $F$  is a splitting field for  $V_F(G, \Omega)$  and  $V_F(H, \Omega_P)$ . Suppose  $e \in V_F(G)$  is a primitive idempotent with  $D(e) =_G Q$  and let  $\lambda, \tilde{\lambda}$  be the modular characters associated with  $e, f(e)$  respectively. Then  $\lambda = \tilde{\lambda} \circ f$ .

**Proof.** Let  $\mathcal{L}$  and  $\tilde{\mathcal{L}}$  denote matrix representations affording  $\lambda, \tilde{\lambda}$  respectively. These representations have the same degree by Theorems 1 and 3. Thus  $\mathcal{L}$  and  $\mathcal{L} \circ f$  are representations of  $V_F(G)$  of the same degree. Since  $\tilde{\lambda}(f(e)) = 1$ ,  $\mathcal{L}$  is a constituent of  $\mathcal{L} \circ f$ . Thus  $\mathcal{L}$  is equivalent to  $\mathcal{L} \circ f$ .

5. **Brauer's second fundamental theorem.** Again,  $P \leq H \leq N_G(P)$  where  $P$  is a  $p$ -subgroup of  $G$ , and  $f$  denotes  $f_{(G, \Omega_P, H)}$ .  $\theta$  is the permutation character of  $G$ , and if  $B$  is a  $p$ -block of  $G$ , we set  $\theta_B = \sum_{\chi \in B} (\theta, \chi) \chi$  (where the  $\chi$ 's are absolutely irreducible characters of  $G$ ).

**Lemma 2.** Let  $e \in V_F(G)$  be an idempotent. Then  $(F\Omega e)_H \approx F\Omega_P f(e) \oplus T$  where  $T$  is a summand of  $f(\Omega - \Omega_P)$ .

(5.1) Before the proof, we clarify the condition on  $T$ . Suppose  $P \triangleleft G$ . Let  $M$  be an indecomposable component of  $F\Omega$ . Then  $M|F\Omega_P$  if and only if  $P$  is contained in the vertex of  $M$ .

**Proof.** Obviously  $P$  is contained in the defect group of every standard basis matrix of  $(G, \Omega_P)$  and is contained in the defect group of no standard basis matrix of  $(G, \Omega - \Omega_P)$ . So the result follows from Proposition 2, the Krull-Schmidt theorem, and the way defect groups for idempotents were defined.

(5.2) **Proof of Lemma 2.** Obviously we may assume that  $G = H$  and  $e$  is primitive. By (5.1) and Proposition 5 we have  $f(e) = 0$  if and only if  $F\Omega e | F(\Omega - \Omega_P)$ . Thus it remains to show  $F\Omega_P f(e) \approx F\Omega e$  in case  $f(e) \neq 0$ .

Observe that  $f(e)$  is a primitive idempotent since  $f$  is onto  $(f(e)V_F(H, \Omega_P)/f(e) = f(eV_F(H, \Omega)e)$  is completely primary).

To complete the proof we identify  $V_F(H, \Omega_P)$  with the algebra  $B$  described in the first paragraph of §3. The map  $f$  is now just the projection  $V_H(H) \rightarrow B$ . In particular  $f(f(e)) = f(e)$  and so  $f(ef(e)e) = f(e) \neq 0$ . Consequently  $ef(e)e$  is a unit in  $eV_F(H, \Omega)e$ . Therefore  $e$  is equivalent to  $f(e)$  and the proof is complete.

(5.3) **Theorem 5.** Suppose  $x \in G$  and a power  $x^n = z$  is a  $p$ -element. Let  $e \in V_F(G)$  be an idempotent, and take  $P = \langle z \rangle$ ,  $x \in H$ . Then  $\Psi_e(x) = \Psi_{f(e)}(x)$ . In particular  $\Psi_e(z)$  is a nonnegative rational integer, and  $|\Psi_e(x)| \leq \Psi_e(z) \leq \theta(z)$ .

If  $e$  is primitive, then  $\Psi_e(z) > 0$  if and only if  $z$  is conjugate in  $G$  to an element of  $D(e)$ .

**Proof.** First we show  $\Psi_e(x) = \Psi_{f(e)}(x)$ . Again we may assume that  $G = H$  and  $e$  is primitive. By Lemma 2 we need only show  $\Psi_e(x) = \Psi_{f(e)}(x) = 0$  when  $F\Omega e | F(\Omega - \Omega_P)$ . Let  $e_0 \in V_R(H)$  be a primitive idempotent with  $\bar{e}_0 = e$ . Then  $P$  is not contained in the vertex of  $R\Omega e_0$  by Proposition 1 and (5.1). Therefore, the  $p$ -part of  $x$  is not conjugate to an element of the vertex of  $R\Omega e_0$ , and so  $\Psi_e(x) = 0$  by Green [7, Theorem 3]. Of course  $\Psi_{f(e)}(x) = 0$  since  $f(e) = 0$  by Proposition 5.

Since  $P$  acts trivially on  $\Omega_P$ ,  $\Psi_{f(e)}(z) = \Psi_{f(e)}(1) \geq |\Psi_{f(e)}(x)|$ .

$\Psi_e(z) \neq 0$  precisely when  $\Psi_{f(e)} \neq 0$ —that is,  $f(e) \neq 0$ . By Proposition 5 this occurs if and only if  $P$  is conjugate in  $G$  to a subgroup of  $D(e)$ . This completes the proof.

As an immediate consequence of the above theorem (3.8) and Proposition 6, we have

(5.4) **Corollary A.** Suppose  $x \in G$  and a power  $x^n$  is a  $p$ -element. Let  $\tilde{\theta}$  be the permutation character for the action of  $C_G(x^n)$  on the set of fixed points of  $x^n$  in  $\Omega$ . Then

$$\theta_B(x) = \sum_{b \in G=B} \tilde{\theta}_b(x).$$

In particular,  $\theta_B(x^n)$  is a nonnegative rational integer, and  $|\theta_B(x)| \leq \theta_B(x^n) \leq \theta(x^n)$ .

6. Defect 0 and 1. We state all the main results of this section before attempting any proofs.

Assume  $K, F$  are splitting fields for  $V_K, V_F$ , and let  $\chi_s, \Psi_j$  denote the characters of  $G$  afforded by  $X_s, KM_j$  respectively (see §1 for notation). Let the symbol  $\sum_p \chi_s^\sigma$  denote the sum of all distinct  $p$ -conjugates of  $\chi_s$  and write  $s \sim t$  if  $\chi_s$  is  $p$ -conjugate to  $\chi_t$ .

Set  $a = \nu_p(|G|)$ , and define  $\nu_s = \nu_p(\chi_s(1))$ . Put  $e = \max\{\nu_p(|O_i|)\}_{i=1}^r$ .

By a theorem of Wielandt (see Keller [12]), we have  $\nu_s \leq e$  for all  $s$ . We are interested here in the cases  $\nu_s = e$  and  $\nu_s = e - 1$ .

**Lemma 3.** Suppose the number of  $p$ -conjugates of  $\chi_s$  is divisible by  $p^y$ . Then

- (a)  $y \leq e - \nu_s$ .
- (b) If  $y = e - \nu_s$  then  $\chi_s$  has exactly  $p^y$   $p$ -conjugates, and  $\sum_p \chi_s^\sigma = \Psi_j$  for some  $j$ . If  $\chi_s \subseteq \Psi_k$  then  $k = j$ . The vertex of  $M_j$  has order  $p^{a-e}$ .

**Theorem 6.** Suppose  $\nu_s = e$ .

Then  $\chi_s = \Psi_j$  for some  $j$ . If  $\chi_s \subseteq \Psi_k$  then  $k = j$ . The vertex of  $M_j$  has order  $p^{a-e}$ .

Also,  $\chi_s$  is  $p$ -rational.

**Theorem 7.** Suppose  $\nu_s = e - 1$ . Then we have either A or B below:

(A)  $\chi_s$  has exactly  $p$   $p$ -conjugates.  $\sum_p \chi_s^\sigma = \Psi_j$  for some  $j$ , and if  $\chi_s \subseteq \Psi_k$ , then  $k = j$ . The vertex of  $M_j$  has order  $p^{a-e}$ .

(B) The number of  $p$ -conjugates of  $\chi_s$  divides  $p - 1$ . If  $\chi_s \subseteq \Psi_j$  then one of the following occurs:

- (i)  $\Psi_j = \sum_p \chi_s^\sigma$ . The vertex of  $M_j$  has order  $p^{a-e+1}$ .
- (ii)  $\Psi_j = \sum_p \chi_s^\sigma + \sum_p \chi_t^\sigma$  where  $t \not\sim s$ ,  $\nu_t = e - 1$ , and the number of  $p$ -conjugates of  $\chi_t$  divides  $p - 1$ . The vertex of  $M_j$  has order  $p^{a-e}$ . If  $\Psi_j = \Psi_k$ , then  $k = j$ .

(iii)  $\Psi_j = \sum_p \chi_s^\sigma + \mathbf{T}$  where  $\mathbf{T} \neq 0$  is a character such that, whenever  $\chi_t \subseteq \mathbf{T}$ , the number of  $p$ -conjugates of  $\chi_t$  is divisible by  $p$ ,  $\nu_t \leq e - 2$ , and each  $p$ -conjugate of  $\chi_t$  appears in  $\mathbf{T}$  with the same multiplicity as  $\chi_t$ . The vertex of  $M_j$  has order  $p^{a-e}$ . If  $\Psi_j = \Psi_k$ , then  $k = j$ .

(iv)  $p = 2$  and  $\Psi_j = 2\chi_s$ . The vertex of  $M_j$  has order  $p^{a-e}$ . If  $\Psi_j = \Psi_k$ , then  $k = j$ .

**Corollary B.** Suppose the block  $B$  has defect 1. Let  $\langle x \rangle$  be a defect group of  $B$ , and let  $b$  be the block of  $N_G(\langle x \rangle)$  satisfying  $b^G = B$ . Let  $\tilde{\theta}$  be the permutation character of  $N_G(\langle x \rangle)$  on the fixed points of  $x$  in  $\Omega$ , and set  $\tilde{\theta}_b = \sum_k l_k \tilde{\chi}_k$ , where  $\tilde{\chi}_k$  is absolutely irreducible and appears in  $\tilde{\theta}_b$  with multiplicity  $l_k$ .

Then we may find distinct indices  $j_k$  such that  $\theta_B = \sum_k l_k \Psi_{j_k} + \Phi$  where

- (1)  $\Phi$  is the sum (with multiplicities) of characters  $\Psi_j$  whose affording module  $M_j$  is projective and lies in  $B$ .  
 (2)  $\Psi_{j_k}(x) > 0$  for each  $k$ , and  $\Psi_{j_k}$  is either a nonexceptional character of  $B$  or the sum of all exceptional characters of  $B$ .

Now we prepare to give the proofs. Several arithmetic preliminaries are required.

(6.1) *There exists a  $p$ -adic number field  $K$  with the following properties:*

- (i)  $K$  is obtained by adjoining an  $m$ th root of unity, where  $p \nmid m$ , to the  $p$ -adic completion of the rational field.  
 (ii)  $K$  contains a primitive  $l$ th root of unity, where  $l$  is the  $p'$ -part of the group order  $|G|$ .  
 (iii) Each character  $\chi_s$  is afforded by a  $K(\chi_s)$  representation.  
 (iv) Each indecomposable component of  $R\Omega$  is absolutely indecomposable (where  $R$  denotes the ring of local integers in  $K$ ).

**Proof.** By Fong's result<sup>(7)</sup> (see [6, 16.5]) a field  $K_0$  satisfying the first three conditions is obtained by adjoining an  $l$ th root of unity (or  $(3l)$ th root of unity if  $p = 2$  and  $3 \nmid l$ ) to the  $p$ -adic completion of the rational field. Let  $F_0$  denote the residue class field of  $K_0$ , and select a finite field  $GF(q)$  which is a splitting field for  $V_{F_0}(G, \Omega)$ . Now let  $K$  be the field obtained by adjoining a primitive  $(q-1)$ th root of unity to  $K_0$ . Then the field  $K$  satisfies condition (iv) by (1.3). Obviously  $K$  satisfies the other three conditions.

(6.2) **Notation.** Note that it suffices to prove Lemma 3, Theorems 6 and 7 and Corollary B for any particular  $p$ -adic field satisfying condition (iv) above. Consequently we shall assume throughout the rest of this section that  $K$  is a field satisfying all the conditions of (6.1).

We let  $\mathcal{G}_s$  denote the Galois group of  $K(\chi_s)/K$ , and let  $\mathcal{G}_s^0$  denote the Sylow  $p$ -subgroup of  $\mathcal{G}_s$ . Set  $p^{ws} = |\mathcal{G}_s^0|$ .

- (6.3) (i)  $\Psi_s^\sigma$  ranges over all the distinct  $p$ -conjugates of  $\chi_s$  as  $\sigma$  ranges over  $\mathcal{G}_s$ .  
 (ii)  $\sum_{\sigma \in \mathcal{G}_s^0} y^\sigma \equiv 0 \pmod{p^{ws}}$  for any local integer  $y$  of  $K(\chi_s)$ .

**Proof.** By (6.1ii)  $\tilde{Q} \subseteq K$ , where  $\tilde{Q}$  is the field of  $l$ th roots of unity. Then  $K(\chi_s) \subseteq K(\omega)$  where  $\omega$  is a primitive  $p^a$ th root of unity.  $K(\omega)/K$  is a fully ramified abelian extension of degree  $(p-1)p^{a-1}$  (see [17, proof of 7-4-1]). The  $p$ -conjugates of  $\chi_s$  are by definition the characters  $\chi_s^\sigma$ ,  $\sigma$  ranging over the Galois group of  $\tilde{Q}(\chi_s)/\tilde{Q}$ . Since  $\tilde{Q}(\omega)/\tilde{Q} = (p-1)p^{a-1}$ , it follows from our description of

---

<sup>(7)</sup> Quoting this result to prove (6.1) is, in a historical sense, putting the cart before the horse. The reader familiar with algebras over local fields (see Albert [1, IX, Theorem 23]) can easily prove (6.1) directly.

$K(\omega)/K$  that  $K(\chi_s)/K$  is a fully ramified extension of degree  $[\tilde{Q}(\chi_s):\tilde{Q}]$ , and  $\mathcal{G}_s$  is naturally isomorphic to the Galois group of  $\tilde{Q}(\chi_s)/\tilde{Q}$ . In particular (i) has now been proved.

Let  $\omega_s$  be a primitive  $p^{w_s+1}$ th root of unity.  $K(\omega_s) \subseteq K(\omega)$  since

$$p^{w_s} = |\mathcal{G}_s^0| | [K(\chi_s):K] | [K(\omega):K] = (p-1)p^{a-1}$$

We claim  $K(\chi_s) \subseteq K(\omega)$ .<sup>(8)</sup>

Let  $\mathcal{E}$  denote the Galois group of  $K(\omega)/K$ , and let  $\mathcal{E}_\chi, \mathcal{E}_\omega$  be the subgroups of  $\mathcal{E}$  which Galois correspond to  $K(\chi_s), K(\omega_s)$  respectively. Since  $\mathcal{G}_s^0$  is a Sylow subgroup of  $\mathcal{G}_s$  and  $\mathcal{G}_s \cong \mathcal{E}/\mathcal{E}_\chi$ , the power of  $p$  in  $|\mathcal{E}_\chi|$  is  $p^{a-1-w_s}$ . Since  $\mathcal{E}/\mathcal{E}_\omega$  is isomorphic to the Galois group of  $K(\omega_s)/K$  and  $[K(\omega_s):K] = (p-1)p^{w_s}$ , we have  $|\mathcal{E}_\omega| = p^{a-1-w_s}$ . Thus  $\mathcal{E}_\omega \subseteq \mathcal{E}_\chi$  and so  $K(\omega_s) \supseteq K(\chi_s)$ .

Now let  $\mathcal{G}_s^1$  denote the group of all automorphisms  $\sigma$  of  $K(\omega_s)/K$  such that  $\omega_s^\sigma = \omega_s^n$  for some integer  $n \equiv 1 \pmod{p}$ . We claim  $\mathcal{G}_s^1$  is isomorphic to  $\mathcal{G}_s^0$  by restriction to  $K(\chi_s)$ .

Let  $\mathcal{G}_s^2$  denote the Galois group of  $K(\omega_s)/K$ . From the definition of  $\mathcal{G}_s^0$  we have  $[\mathcal{G}_s^2:\mathcal{G}_s^1] = p-1$  and so  $\mathcal{G}_s^1$  is a Sylow  $p$ -subgroup of  $\mathcal{G}_s^2$ . The natural restriction map  $\mathcal{G}_s^2 \rightarrow \mathcal{G}_s$  is an epimorphism and consequently sends  $\mathcal{G}_s^1$  onto  $\mathcal{G}_s^0$ . But  $|\mathcal{G}_s^1| = p^{w_s} = |\mathcal{G}_s^0|$  and so  $\mathcal{G}_s^1$  is isomorphic to  $\mathcal{G}_s^0$  by restriction as claimed.

Thus to prove (ii) it is enough to show  $\sum_{\sigma \in \mathcal{G}_s^1} y^\sigma \equiv 0 \pmod{p^{w_s}}$  for any local integer  $y$  of  $K(\omega_s)$ .

Now the powers of  $\omega_s$  contain an integral basis for  $K(\omega_s)/K$  [17, proof 7-5-3]. Thus we need only verify the congruence in case  $y = \omega_s^k$  for some integer  $k$ . Then

$$\sum_{\sigma \in \mathcal{G}_s^1} y^\sigma = \sum_{z=0}^{p^{w_s}-1} \omega_s^{(1+zp)k} = \omega_s^k \sum_{z=0}^{p^{w_s}-1} (\omega_s^{pk})^z.$$

The final sum is  $p^{w_s}$  if  $\omega_s^{pk} = 1$  and  $(\omega_s^{pk})p^{w_s} - 1/\omega_s^{pk} - 1 = 0$  otherwise. This proves (ii).

(6.4) If  $s \sim t$  then  $d_{sj} = d_{tj}$  for all  $j$ .

**Proof.** By (6.1 iv) each character  $\Psi_j$  is afforded by an  $RG$  representation. Hence  $(\Psi_j, \chi_s^\sigma) = (\Psi_j, \chi_s^\tau)$  for each  $\sigma \in \mathcal{G}_s$  and each  $j$ . The result now follows from (6.3 i).

(6.5) If  $\Psi_j = \Psi_k$  and  $M_j, M_k$  both have a vertex of order  $p^{a-e}$ , then  $j = k$ .

**Proof.** Let  $P$  be a vertex of  $M_j$ . Then  $P$  satisfies both the 1-1 condition and the onto condition with respect to  $(G, \Omega, P, N_G(P))$ . Let  $e_j, e_k \in V_F(G, \Omega)$

---

<sup>(8)</sup> This argument fails if  $p = 2$ . But in this case the sum in (ii) is just  $[\tilde{Q}(\omega):\tilde{Q}(\chi_s)]^{-1} \text{tr}_{\tilde{Q}(\omega)/\tilde{Q}}(\gamma)$ .



be primitive idempotents with  $\bar{M}_j \approx F\Omega e_j$ ,  $\bar{M}_k \approx F\Omega e_k$ . Then Propositions 7 and 8 give

$$\begin{aligned}(\Psi_{f(e_j)}, \Psi_{f(e_k)}) &= (\Psi_{e_j}, \Psi_{e_k}) = (\Psi_j, \Psi_k) \\ &= (\Psi_j, \Psi_j) \quad (\neq 0) \\ &= (\Psi_{f(e_j)}, \Psi_{f(e_j)}).\end{aligned}$$

Since the inner product is not zero, we have  $D(e_k) \geq_G P$  by Proposition 5. By hypothesis  $|D(e_k)| = |P|$ . Hence  $D(e_k) =_G P$ . By symmetry we now have a second equality

$$(\Psi_{f(e_j)}, \Psi_{f(e_k)}) = (\Psi_{f(e_k)}, \Psi_{f(e_k)}).$$

It follows that  $\Psi_{f(e_j)} = \Psi_{f(e_k)}$ . Since  $F\Omega_P f(e_j)$  and  $F\Omega_P f(e_k)$  are projective indecomposable  $F(N_G(P)/P)$  modules (Theorem 3), we deduce that  $F\Omega_P f(e_j) \approx F\Omega_P f(e_k)$  (from Proposition 1 and [4, 7-14 or 8.4.11]). Thus  $e_j$  is equivalent to  $e_k$  by Theorem 3 (or Proposition 9) and so  $j = k$ .

(6.6) **Proof of Lemma 3.** Select an index  $j$  such that  $\chi_s \subseteq \Psi_j$ , and choose a primitive idempotent  $u \in V_R$  with  $M_j \approx R\Omega u$ .

Let  $\tilde{R}$  denote the ring of local integers in  $K(\chi_s) = \tilde{K}$ . By (6.1 iii) there exists a primitive idempotent  $f_s \in uV_{\tilde{K}}u$  such that  $\tilde{K}\Omega f_s$  affords  $\chi_s$ . By a suitable choice we can insure that  $f_s$  belongs to an  $\tilde{R}$  order of  $uV_{\tilde{K}}u$  containing  $uV_Ru$ .

Let  $\zeta_s$  denote the absolutely irreducible character of  $V_{\tilde{K}}$  associated with  $f_s$  (that is,  $\zeta_s(f_s) = 1$ ). Then  $\zeta_s(f_s x) = \zeta_s(u f_s u x) = \zeta_s(f_s u x u) \in \tilde{R}$  for all  $x \in V_{\tilde{R}}$ , and  $\zeta(f_s x) = 0$  for any character  $\zeta$  of  $V_{\tilde{K}}$  which does not contain  $\zeta_s$ .

We let  $\mathcal{G}_s$  act on  $V_{\tilde{K}}$  in the obvious way. For  $\sigma \in \mathcal{G}_s$  let  $\zeta_s^\sigma$  denote the character associated with  $f_s^\sigma$ . Thus  $\zeta_s^\sigma(x^\sigma) = \zeta_s(x)^\sigma$  for all  $x \in V_{\tilde{K}}$ .

Since the characters  $\chi_s^\sigma$ ,  $\sigma \in \mathcal{G}_s$ , are distinct, the idempotents  $f_s^\sigma$  are orthogonal. In particular  $\sum_{\sigma \in \mathcal{G}_s^0} f_s^\sigma = f$  is an idempotent in  $uV_{\tilde{K}}u$ .

Now set  $f = \sum t_i A_i$ . We compute the coefficients  $t_i$  as follows: Let  $\tau$  denote the character of  $V_{\tilde{K}}$  afforded by  $\tilde{K}\Omega$ . Then  $\tau = \sum_t \chi_t(1)\zeta_t$ , and  $\tau(A_j A_i^*) = \delta_{ij} |O_i|$  (as in the proof of (3.3)). Thus  $|O_i| t_i = \tau(f A_i^*) = \chi_s(1) \sum_{\sigma \in \mathcal{G}_s^0} \zeta_s^\sigma(f A_i^*)^\sigma$  for each  $i$ .

Hence

$$\begin{aligned}\nu_p(t_i) &= \nu_s + \nu_p \left( \sum_{\sigma \in \mathcal{G}_s^0} \zeta_s^\sigma(f A_i^*)^\sigma \right) - \nu_p(|O_i|) \\ &\geq \nu_s + w_s - \nu_p(|O_i|) \quad \text{by (6.3ii)} \\ &\geq \nu_s + w_s - e.\end{aligned}$$

Since  $f$  is an idempotent,  $\nu_p(t_i) \leq 0$  for some  $i$ . This proves part (a) of Lemma 3.

Now suppose  $w_s = e - v_s$ .

Then  $\nu_p(t_i) \geq 0$  for all  $i$  and so  $f \in uV_R^{\sim}u$ . Hence  $f = u$ . In particular  $\Psi_j = \sum_{\sigma \in \mathcal{G}_s^0} \chi_s^\sigma$ . By (6.4)  $\mathcal{G}_s^0 = \mathcal{G}_s$ —that is,  $\chi_s$  has exactly  $p^{w_s}$   $p$ -conjugates.

If  $\nu_p(t_i) = 0$  then  $0 \geq v_s + w_s - \nu_p(|O_i|) \geq 0$  and so  $\nu_p(|O_i|) = v_s + w_s = e$ . So by definition  $|D(\bar{u})| = p^{a-e}$ .  $D(\bar{u})$  is the vertex of  $M_j$  by Propositions 1 and 2.

Since the choice of  $j$  was arbitrary except for  $\chi_s \subseteq \Psi_j$ , we have  $\Psi_j = \Psi_k = \sum_p \chi_s^\sigma$  whenever  $\chi_s \subseteq \Psi_k$ . Also the vertex of  $M_k$  has order  $p^{a-e}$ ; thus  $\chi_s \subseteq \Psi_k$  implies  $k = j$  because of (6.5). This completes the proof of part (b) and the lemma.

(6.7) **Proof of Theorem 6.** Immediate from Lemma 3.

The next result is a technical preliminary to the proof of Theorem 7. Its assertions are almost trivial in case  $V_K$  is commutative.

(6.8) Suppose  $\chi_s + \chi_t \subseteq \Psi_j$  where either  $s = t$  or  $s \not\sim t$ . Let  $u \in V_R$  be a primitive idempotent with  $R\Omega u \approx M_j$ , and let  $\tilde{K}$  be a  $p$ -adic field containing  $K(\chi_s)$ ,  $K(\chi_t)$ . Denote the ring of local integers in  $\tilde{K}$  by  $\tilde{R}$ .

Then there exist primitive idempotents  $f_s, f_t \in V_K^{\sim}$  such that  $\tilde{K}\Omega f_s$  affords  $\chi_s$ ,  $\tilde{K}\Omega f_t$  affords  $\chi_t$ , and

- (i)  $f_s \in uV_{K(\chi_s)}u$  and  $f_t \in uV_{K(\chi_t)}u$ ;
- (ii)  $f_s^\sigma$  is orthogonal to  $f_t^\tau$  for each  $\sigma \in \mathcal{G}_s$  and  $\tau \in \mathcal{G}_t$ ;
- (iii)  $\zeta_s(f_s w) \in \tilde{R}$  and  $\zeta_t(f_t w) \in \tilde{R}$  for all  $w \in V_R^{\sim}$ , where  $\zeta_s, \zeta_t$  are the absolutely irreducible characters of  $V_K^{\sim}$  satisfying  $\zeta_s(f_s) = \zeta_t(f_t) = 1$ . Furthermore,  $\overline{\zeta_s(f_s w)} = \overline{\zeta_t(f_t w)} = \lambda(\overline{uwu})$  where  $\lambda$  is the absolutely irreducible character of  $\overline{V_R^{\sim}}$  (with values in  $\tilde{R}$ ) satisfying  $\lambda(\bar{u}) = 1$ .

**Proof.** From (the proof of) Theorem 1 we know that  $uV_{K(\chi_s)}u$  has an absolutely irreducible representation module  $Y_s$  of degree  $d_{s_j}$  such that  $K(\chi_s)\Omega/$  affords  $\chi_s$  for any primitive idempotent  $f \in uV_{K(\chi_s)}u$  with  $Y_s f \neq 0$ . If  $\zeta_s$  is the character of  $V_{K(\chi_s)}$  associated with  $f$  then  $\zeta_s(fw)$  is easily seen to be the trace of the action of  $fuwu$  on  $Y_s$  ( $w \in V_{K(\chi_s)}$ ). Moreover, if  $f_1, f_2, \dots$  are a full set of  $d_{s_j}$  orthogonal primitive idempotents in  $uV_{K(\chi_s)}u$  which do not annihilate  $Y_s$ , then we may view the quantities  $\zeta_s(f_1 w), \zeta_s(f_2 w), \dots$  as diagonal coefficients for  $uwu$  in a matrix representation associated with  $Y_s$ .

Let  $R_s$  denote the ring of local integers in  $K(\chi_s)$ . Now the algebra  $\overline{uV_{R_s}u}$  has a unique irreducible representation, which is linear and may be realized as the restriction to  $\overline{uV_{R_s}u}$  of the irreducible character  $\lambda$  of  $\overline{V_{R_s}}$  associated with  $\bar{u}$  (see (2.7)). Thus we may choose a matrix representation associated with  $Y_s$  so that any  $x \in uV_{R_s}u$  is represented integrally with all diagonal coefficients having residue class  $\lambda(x)$ . Let  $f_1, f_2, \dots \in uV_{K(\chi_s)}u$  be primitive idempotents which give rise to such a matrix representation.

In case  $s = t$  we take  $f_s = f_1$ ,  $f_t = f_2$  and it is clear from the preceding discussion that (i) and (iii) are satisfied. (ii) is a consequence of the mutual orthogonality of the idempotents  $(f_1 + f_2)^\sigma$ ,  $\sigma \in \mathcal{G}_s$ .

In case  $s \neq t$  we take  $f_s = f_1$  and repeat the whole procedure (with  $\chi_t$  instead of  $\chi_s$ ) to obtain  $f_t$ . Here (ii) is automatic, while (i) and (iii) are satisfied as before.

(6.9) **Proof of Theorem 7.** If the number of  $p$ -conjugates of  $\chi_s$  is divisible by  $p$ , then we have (A) by Lemma 3. Hence we may assume the number of  $p$ -conjugates of  $\chi_s$  is prime to  $p$ —that is, divides  $p - 1$ .

Suppose  $\chi_s \subseteq \Psi_j$  and let  $u \in V_R$  be a primitive idempotent with  $R\Omega u \approx M_j$ . We distinguish two main cases.

Case 1.  $\Psi_j = \sum_p \chi_s^\sigma$ .

Then  $\Psi_j(1) \neq 0 \pmod{p}$ . Hence by Green [7, Theorem 3] (or Theorem 3) the vertex of  $M_j$  does not have order  $p^{a-e}$ . We calculate  $u = \sum_i t_i A_i$  where  $|O_i| t_i = \chi_s(1) \sum_{\sigma \in \mathcal{G}_s} \zeta_s(u A_i^*)^\sigma$ . Hence  $\nu_p(t_i) > 0$  if  $|D_i| > p^{a-e+1}$ . So by definition  $|D(\bar{u})| \leq p^{a-e+1}$ . Thus  $D(\bar{u})$  (= vertex of  $M_j$ ) has order exactly  $p^{a-e+1}$ .

Case 2.  $\Psi_j \neq \sum_p \chi_s^\sigma$ .

Here we must show that we get one of the types B (ii), (iii), or (iv). Note that  $\sum_p \chi_s^\sigma \subseteq \Psi_j$  by hypothesis and (6.4). Let  $\sum_p \chi_s^\sigma + \chi_t \subseteq \Psi_j$  where  $s = t$  or  $s \neq t$ .

Set  $x_s = \chi_s(1)$ ,  $x_t = \chi_t(1)$ .

Let  $\tilde{K}$  be a  $p$ -adic field containing  $K(\chi_s)$ ,  $K(\chi_t)$ , and choose  $f_s, f_t$  as in (6.8). Then we calculate

$$(p^e/x_s)f_s = \sum_i (p^e/|O_i|)\zeta_s(f_s A_i^*)A_i \in uV_R u$$

and

$$(p^e/x_t)f_t = \sum_i (p^e/|O_i|)\zeta_t(f_t A_i^*)A_i \in uV_R u.$$

Thus

$$\overline{(p^e/x_s)f_s} = \overline{(p^e/x_t)f_t} = \sum_i \overline{(p^e/|O_i|)\lambda(u A_i^* u)A_i} \in \overline{uV_R u}.$$

We show  $\overline{(p^e/x_s)f_s} \neq 0$ : If not, then  $(p^{e-1}/x_s) \sum_{\sigma \in \mathcal{G}_s} f_s^\sigma \in uV_R u$  and so  $\sum_{\sigma \in \mathcal{G}_s} f_s^\sigma \in uV_R u$ . Therefore  $\sum_{\sigma \in \mathcal{G}_s} f_s^\sigma = u$ . But this implies  $\Psi_j = \sum_p \chi_s^\sigma$ , a contradiction.

In particular  $\lambda(u A_i^* u) \neq 0$  for some  $i$  with  $|D_i| = p^{a-e}$ . By Proposition 3 the vertex of  $M_j$  has order  $p^{a-e}$ . Note also that this gives  $k = j$  whenever  $\Psi_j = \Psi_k$  because of (6.5).

Suppose now that the number of  $p$ -conjugates of  $\chi_t$  divides  $p - 1$ . We will show that this leads to type (ii) or (iv).

Here we may assume that  $\tilde{K}$  is obtained from  $K$  by the adjunction of a primitive  $p$ th root of unity (this may be seen directly or from the proof of (6.3)). Set  $\mathcal{G} = \mathcal{G}(\tilde{K}/K)$  and let  $r_s = |\mathcal{G}_s|$ ,  $r_t = |\mathcal{G}_t|$ . Write  $\hat{f}_s$  for  $\sum_{\sigma \in \mathcal{G}_s} f_s^\sigma$  and  $\hat{f}_t$  for  $\sum_{\sigma \in \mathcal{G}_t} f_t^\sigma$ . Then

$$(p - 1/r_s)(p^e/x_s)\hat{f}_s - (p - 1/r_t)(p^e/x_t)\hat{f}_t = \sum_{\sigma \in \mathcal{G}} ((p^e/x_s)f_s - (p^e/x_t)f_t)^\sigma \equiv 0 \pmod{p}.$$

Hence  $\hat{f}_s + c\hat{f}_t \in uV_R u$  where  $c = -r_s x_s / r_t x_t$ . Now  $v_p(x_t) = v_t \leq e - 1$  by Theorem 6, and so  $c \in R$ .

Set  $v = \hat{f}_s + c\hat{f}_t$ . Then  $\lambda(\bar{v}) = \overline{\zeta_s(f_s v)} = \overline{\zeta_s(f_s)} = 1$ ; also  $\lambda(\bar{v}) = \overline{\zeta_t(f_t v)} = \overline{\zeta_t(c f_t)} = \bar{c}$ . Therefore  $\bar{c} = 1$ . In particular,  $v_t = v_p(x_t) = e - 1$ , and  $c = 1 + (p^e/x_t)k$  for some  $k \in R$ . Now  $\hat{f}_s + \hat{f}_t = v - k(p^e/x_t)\hat{f}_t \in uV_R u$ . By (6.8)  $\hat{f}_s + \hat{f}_t$  is an idempotent, and so  $\hat{f}_s + \hat{f}_t = u$ . Consequently  $\Psi_j = \sum_p \chi_s^\sigma + \sum_p \chi_t^\sigma$ . If  $s \neq t$  we have type (ii). If  $s = t$  then  $p = 2$ , since  $\bar{c} = 1$  and  $c = -1$ ; so we have type (iv).

Finally, we are reduced to the case where the number of  $p$ -conjugates of  $\chi_t$  is divisible by  $p$  whenever  $\sum_p \chi_s^\sigma + \chi_t \subseteq \Psi_j$ . By Lemma 3,  $v_t \leq e - 2$ . By (6.4) all  $p$ -conjugates of  $\chi_t$  appear in  $\Psi_j$  with the same multiplicity. Thus we have type (iii), and the proof is complete.

(6.10) **Proof of Corollary B.** Suppose  $M_j$  is a nonprojective indecomposable component of  $R\Omega$  which lies in  $B$ . Thus the vertex of  $M_j$  is  $\langle x \rangle$  by Green [7, Corollary to Lemma 4.1a]. In particular  $\Psi_j(x) > 0$  by Theorem 5.

Let  $\chi_s \subseteq \Psi_j$ . Then  $v_s = a - 1 \geq e - 1$ . If  $v_s = e$  then  $\chi_s = \Psi_j$  is  $p$ -rational by Theorem 6. If  $v_s = e - 1$ , then  $a - e = 0$  and so we have type B(ii), since  $M_j$  is not projective. Hence  $\Psi_j = \sum_p \chi_s^\sigma$ .

Note that the latter case does not occur when  $\langle x \rangle$  acts trivially on  $\Omega$ , because  $e$  is obviously less than  $a$ . So by Theorem 6 the  $l_k$ 's are the multiplicities of the various indecomposable components of  $R\Omega_x$  which lie in  $b$  ( $R$  suitably large). Application of Theorem 3 now finishes the proof.

#### REFERENCES

1. A. A. Albert, *Structure of algebras*, Amer. Math. Soc. Colloq. Publ., vol. 24, Amer. Math. Soc., Providence, R. I., 1939. MR 1, 99.
2. E. Artin, C. J. Nesbitt and R. M. Thrall, *Rings with minimum condition*, Univ. of Michigan Publ. in Math., no. 1, Univ. of Michigan Press, Ann Arbor, Mich., 1944. MR 6, 33.
3. R. Brauer, *Zur Darstellungstheorie der Gruppen endlicher Ordnung*, II, Math. Z. 72 (1959/60), 25-46. MR 21 #7258.
4. C. W. Curtis and I. Reiner, *Representation theory of finite groups and associative algebras*, Pure and Appl. Math., vol. 11, Interscience, New York, 1962. MR 26 #2519.
5. W. Feit, *Some properties of the Green correspondence*, Theory of Finite Groups (Sympos., Harvard Univ., Cambridge, Mass., 1968), Benjamin, New York, 1969, pp. 139-148. MR 39 #4295.

6. W. Feit, *Characters of finite groups*, Benjamin, New York, 1967. MR 36 #2715.
7. J. A. Green, *Blocks of modular representations*, Math. Z. 79 (1962), 100–115.  
MR 25 #5114.
8. ———, *A transfer theorem for modular representations*, J. Algebra 1 (1964), 73–84.  
MR 29 #147.
9. ———, *Some remarks on defect groups*, Math. Z. 107 (1968), 133–150. MR 38 #2222.
10. D. G. Higman, *Modules with a group of operators*, Duke Math. J 21 (1954), 369–376. MR 16, 794.
11. ———, *Intersection matrices for finite permutation groups*, J. Algebra 6 (1967), 22–42. MR 35 #244.
12. G. Keller, *Concerning the degrees of irreducible characters*, Math. Z. 107 (1968), 221–224. MR 38 #3362.
13. L. L. Scott, *Uniprimitive groups of degree  $kp$* , Ph. D. Thesis, Yale University, New Haven, Conn., 1968.
14. ———, *Uniprimitive permutation groups*, Theory of Finite Groups, (Sympos., Harvard Univ., Cambridge, Mass., 1968), Benjamin, New York, 1969), pp. 55–62.
15. ———, *The modular theory of permutation representations*, Proc. Sympos. Pure Math., vol. 21, Amer. Math. Soc., Providence, R. I. 1971, pp. 137–144.
16. O. Tamaschke, *A generalized character theory on finite groups*, Proc. Internat. Conf. Theory of Groups, Austral. Nat. U. Canberra, August 1965, New York, 1967, pp. 347–355.
17. E. Weiss, *Algebraic number theory*, McGraw-Hill, New York, 1963. MR 28 #3021.
18. H. Wielandt, *Finite permutation groups*, Lectures, University of Tübingen, 1954/55; English transl., Academic Press, New York, 1964. MR 32 #1252.

DEPARTMENT OF MATHEMATICS, YALE UNIVERSITY, NEW HAVEN CONNECTICUT 06520

*Current address:* Department of Mathematics, University of Virginia, Charlottesville, Virginia 22904