CHAPTER VIII

Character Theory Pertaining to Finite Simple Groups

E. C. DADE

1. Introduction

The original idea behind these lectures was to prove directly, starting from "first principals", some beautiful, but deep, result about finite simple groups, whose proof would illustrate the "practical" uses of character theory in group theory. The advantages of this idea were evident. Since the number (twelve) of lectures was quite limited, it would be necessary to concentrate on those parts of representation theory which are really used to prove the theorem —essentially those parts dealing with the values of the ordinary irreducible characters and their relations with the structure of the group and its subgroups—and to use the minimum of ring-theoretic machinery. This would avoid the usual trap in which one spends so much time developing this machinery that none is left over for the groups. The main disadvantage was also evident—namely, this machinery is used currently in the literature. So a student attending this course would perhaps learn the proof of this one theorem, plus many auxiliary results, but would by no means be prepared to read published proofs.

A minor disadvantage was less evident at the time, but became serious during the lectures themselves. The result chosen as a goal—Glauberman's

theorem about weakly closed involutions in 2-Sylow subgroups (Theorem 15.1 below)—has a very elegant proof, given the character-theoretic tools which were developed in the course. But it depends essentially upon the theorem of Brauer and Suzuki that groups with quaternion 2-Sylow subgroups are not simple (Theorem 14.11 below), whose proof is rather messy no matter how you do it, and which requires more machinery—in particular, Brauer's characterization of characters (Theorem 7.1 below)—than is needed for Glauberman's proof. In fact, due to the pressure of time, it was impossible to prove either of the last two theorems during the lectures. So part of the written account below—Sections 7 and 14, and the last part of Section 12, starting at (12.16)—were not actually given verbally.

The rest of this account represents more or less closely the lectures as given, although there are a large number of minor modifications and a few major ones. These will be evident to those who were present during the course, and of no interest to anyone else. So there is no need to list them here.

As mentioned above, the reader really needs more preparation than this before tackling articles in the literature. For example, he should read the chapter on modular representation (Chapter XII) in the book by Curtis and Reiner (1962), or the excellent lecture notes of Feit (1969) on the subject. Even in the theory of ordinary characters, he should be familiar with much more than there was time to mention here. A reading of Chapter V of the book by Huppert (1967) would be very profitable in this regard.

2. Characters

Let V be a finite-dimensional vector space over a (commutative) field F. We denote by $GL(V)$ the group of all non-singular linear transformations of V. A *(linear) representation* of a finite group G on V is a homomorphism R of G into $GL(V)$. The *character* χ_R of such a representation R is the function from G to F sending each $\sigma \in G$ into the trace $\mathrm{tr}\,(R(\sigma))$ of the corresponding linear transformation $R(\sigma)$ of V:

$$\chi_R(\sigma) = \mathrm{tr}\,(R(\sigma)), \quad \textit{for all } \sigma \in G. \tag{2.1}$$

We are interested in the characters as invariants of the group G, and in their relations with the algebraic structure of G. For example, we have

PROPOSITION 2.2. $\chi_R(\sigma^\tau) = \chi_R(\sigma)$, *for all* $\sigma, \tau \in G$.

Proof. Of course, σ^τ is the conjugate $\tau^{-1}\sigma\tau$ of σ by τ. Since R is a homomorphism, we have $R(\sigma^\tau) = R(\tau)^{-1}R(\sigma)R(\tau)$. So the linear transformations $R(\sigma^\tau)$ and $R(\sigma)$ are similar. Therefore they have the same trace, which is the proposition.

The (finite) dimension of V is called the *degree* $\deg(R)$ of the representation R. Since the homomorphism R sends the identity $1 = 1_G$ of G into the

identity linear transformation $1_{V\to V}$ of V, we have

$$\chi_R(1_G) = \deg(R)\cdot 1_F = \overbrace{1_F + \ldots + 1_F}^{\deg(R)}. \tag{2.3}$$

In particular, if F has characteristic zero, and if we identify the ordinary integers with their images in F, then $\chi_R(1) = \deg(R)$ is always a non-negative integer.

If $\deg(R) = \dim(V) = 1$, then χ_R is called a *linear character* of G. In this case the trace function is an isomorphism of $GL(V)$ onto the multiplicative group $F^\times$ of F. It follows that

The linear characters of G are just the homomorphisms from G into $F^\times$. (2.4)

Of course, the linear characters are all equal to 1_F on the derived group G' of G (since F is commutative). So there aren't very many of them. In fact, the only linear character present for all finite groups G is the *trivial character* $1 = 1_{G\to F} : \sigma \to 1_F$, for all $\sigma \in G$.

We should note that any function R satisfying the following conditions is a representation of the group G on the finite-dimensional vector space V:

$$R(\sigma) \in \mathrm{Hom}_F(V, V), \quad \textit{for all } \sigma \in G, \tag{2.5a}$$

$$R(\sigma)R(\tau) = R(\sigma\tau), \quad \textit{for all } \sigma, \tau \in G, \tag{2.5b}$$

$$R(1_G) = 1_{V\to V}. \tag{2.5c}$$

Indeed, (1.5b, c) imply that $R(\sigma^{-1})$ is a two-sided inverse to $R(\sigma)$, for al $\sigma \in G$. So R is in fact a homomorphism of G into $GL(V)$.

Any permutation representation of G determines a linear representation, and hence a character, of G. Let G act as permutations of a finite set S, with any $\sigma \in G$ taking each $s \in S$ into $s\sigma \in S$. Form the finite-dimensional vector space FS having S as a basis (the elements of FS are just the formal linear combinations $\sum_{s\in S} f_s s$ with unique coefficients $f_s \in F$, and the operations are "coefficientwise"). Then any $\sigma \in G$ determines a unique linear transformation $R_S(\sigma)$ of FS satisfying

$$sR_S(\sigma) = s\sigma, \quad \textit{for all } s \in S. \tag{2.6}$$

One verifies immediately that R_S satisfies (2.5) and hence is a linear representation of G on FS. Using the matrix of the linear transformation $R_S(\sigma)$ with respect to the basis S of FS, we easily compute the character of this representation:

$$\chi_{R_S}(\sigma) = \big|\{s \in S : s\sigma = s\}\big| \cdot 1_F, \quad \textit{for all } \sigma \in G. \tag{2.7}$$

An important special case is the *regular representation* in which $S = G$ and $s\sigma$, for $s \in S = G$ and $\sigma \in G$, is the product in the group G. We then denote R_S by Reg. In this case $s\sigma = s$ if and only if $\sigma = 1_G$. So the *regular*

character χ_{Reg} has the values:

$$\chi_{\mathrm{Reg}}(\sigma) = \begin{cases} |G| \cdot 1_F, & \text{if } \sigma = 1_G, \\ 0, & \text{if } \sigma \neq 1_G. \end{cases} \tag{2.8}$$

Any natural method for making new vector spaces from old ones can be used to construct new linear representations or characters from old ones. For example, let $R_1, R_2, \ldots, R_n$ be a finite number of representations of G on finite-dimensional vector spaces $V_1, V_2, \ldots, V_n$, respectively, over F. The direct sum $V_1 \oplus \ldots \oplus V_n$ is again a finite-dimensional vector space over F, on which we have the representation $R_1 \oplus \ldots \oplus R_n$ of G defined by

$$[R_1 \oplus \ldots \oplus R_n](\sigma) = R_1(\sigma) \oplus \ldots \oplus R_n(\sigma):$$
$$v_1 \oplus \ldots \oplus v_n \to v_1 R_1(\sigma) \oplus v_2 R_2(\sigma) \oplus \ldots \oplus v_n R_n(\sigma),$$
$$\text{for all } \sigma \in G,\ v_1 \in V_1, \ldots, v_n \in V_n. \tag{2.9}$$

An elementary calculation gives

$$\chi_{R_1 \oplus \ldots \oplus R_n}(\sigma) = \chi_{R_1}(\sigma) + \ldots + \chi_{R_n}(\sigma), \quad \text{for all } \sigma \in G. \tag{2.10}$$

In particular, *the sum of two characters of G is again a character of G.*

Suppose that Q, R are representations of finite groups H, G on finite-dimensional vector spaces U, V, all respectively, over F. Then the tensor product $U \otimes V$ (over F) is again a finite-dimensional vector space on which we have the representation $Q \otimes R$ of the direct product group $H \times G$ determined by

$$[Q \otimes R](\sigma \times \tau) = Q(\sigma) \otimes R(\tau) : u \otimes v \to uQ(\sigma) \otimes vR(\tau),$$
$$\text{for all } \sigma \in H,\ \tau \in G,\ u \in U,\ v \in V. \tag{2.11}$$

The character $\chi_{Q \otimes R}$ can easily be computed:

$$\chi_{Q \otimes R}(\sigma \times \tau) = \chi_Q(\sigma)\chi_R(\tau), \quad \text{for all } \sigma \in H,\ \tau \in G. \tag{2.12}$$

If $H = G$ in the preceding case, then the diagonal map $\sigma \to \sigma \times \sigma$ is a natural monomorphism of G into $G \times G$ whose composition with $Q \otimes R$ gives the *inner Kronecker product* $Q*R$ of the two representations Q and R of G:

$$[Q*R](\sigma) = Q(\sigma) \otimes R(\sigma) : u \otimes v \to uQ(\sigma) \otimes vR(\sigma),$$
$$\text{for all } \sigma \in G,\ u \in U,\ v \in V. \tag{2.13}$$

Of course $Q*R$ is a representation of G on $U \otimes V$ whose character is given by

$$\chi_{Q*R}(\sigma) = \chi_Q(\sigma)\chi_R(\sigma), \quad \text{for all } \sigma \in G. \tag{2.14}$$

In particular, *the product of two characters of G is again a character of G.*

Returning to the case of representations Q, R of two groups H, G on U, V, respectively, we can define a representation $\mathrm{Hom}\,(R^{-1}, Q)$ of $G \times H$ on the finite-dimensional vector space $\mathrm{Hom}_F(V, U)$ by:

$$[\mathrm{Hom}\,(R^{-1}, Q)](\sigma \times \tau) = \mathrm{Hom}\,(R(\sigma^{-1}), Q(\tau)) : T \to R(\sigma^{-1})TQ(\tau),$$
$$\text{for all } \sigma \in G,\ \tau \in H,\ T \in \mathrm{Hom}_F(V, U). \tag{2.15}$$

Its character is given by:

$$\chi_{\mathrm{Hom}(R^{-1},Q)}(\sigma\times\tau)=\chi_R(\sigma^{-1})\chi_Q(\tau),\quad \textit{for all } \sigma\in G,\ \tau\in H. \tag{2.16}$$

As a special case, let $H=\langle 1\rangle$ be the trivial group, U be F, and $Q(1)=1_{F\to F}$. Then $\mathrm{Hom}_F(V,F)$ is the dual vector space V^* to V and $[\mathrm{Hom}(R^{-1},Q)](\sigma\times 1)$, for $\sigma\in G$, is the dual linear transformation $R(\sigma^{-1})^*$ to the linear transformation $R(\sigma^{-1})$ of V. Hence the *dual representation* R^{-*} to R, the representation on V^* defined by

$$T[R^{-*}(\sigma)]=R(\sigma^{-1})T,\quad \textit{for all } \sigma\in G,\ T\in V^*, \tag{2.17}$$

has the character

$$\chi_{R^{-*}}(\sigma)=\chi_R(\sigma^{-1}),\quad \textit{for all } \sigma\in G. \tag{2.18}$$

3. Group Algebras

The deeper properties of the characters of a finite group G come from a study of the group algebra FG of G over the field F, and of modules over this algebra. Those parts of the theory of algebras needed to carry out this study (essentially the theory of Wedderburn) are quite well known. A very concise account of them can be found in Chapter V of the book by Huppert (1967). So we shall just state the necessary definitions and results here, and refer the reader to that book for the proofs.

By an *algebra* A over our field F, we understand a finite-dimensional vector space A over F together with an F-bilinear associative product $(a,a')\to aa'$ from $A\times A$ to A. We assume, unless otherwise noted, that A has a two-sided identity $1=1_A$ for this product. Then algebra multiplication and vector space addition make A into a ring with identity, while scalar multiplication gives us a natural, identity-preserving homomorphism $f\to f1_A$ of the field F into the center of the ring A.

Let $a_1,\ldots,a_n$ be a basis of A (as a finite-dimensional vector space over F). Then there are unique *multiplication coefficients* $f_{ijk}\in F$, for $i,j,k=1,\ldots,n$, such that:

$$a_ia_j=\sum_{k=1}^{n}f_{ijk}a_k,\quad \textit{for all } i,j=1,\ldots,n. \tag{3.1}$$

Since the product in A is F-bilinear, it is determined by the n^2 products a_ia_j $(i,j=1,\ldots,n)$. These products themselves are computed via (3.1) from the coefficients f_{ijk}. Hence the multiplication coefficients determine the algebra A to within isomorphism.

The *group algebra* FG of a finite group G over F has the elements of G as a basis. The corresponding multiplication coefficients are determined by the rule that the algebra product of two basis elements $\sigma,\tau\in G$ be their product $\sigma\tau$ in the group G. Using F-bilinearity, we see that the product of two arbitrary

elements of FG is given by:

$$\left(\sum_{\sigma\in G} f_\sigma\sigma\right)\left(\sum_{\tau\in G} g_\tau\tau\right) = \sum_{\rho\in G}\left(\sum_{\sigma,\,\tau\in G,\sigma\tau=\rho} f_\sigma g_\tau\right)\rho, \tag{3.2}$$

for any coefficients f_σ, $g_\tau \in F$. The associativity in G easily implies that of multiplication in FG, and the identity 1_G of G is also the identity for FG. So FG is an algebra over F in the sense in which we use the term.

By a *module* M over an F-algebra A we mean a right module over the ring A, which is unitary, in the sense that $m1_A = m$, for all $m\in M$, and finite-dimensional as a vector space over F. Of course, the vector space structure of M comes from the A-module structure via the natural homomorphism of F into the center of A, so that scalar multiplication is defined by:

$$fm = m(f1_A), \quad \textit{for all } f\in F,\ m\in M. \tag{3.3}$$

We note that the module product $(m, a) \to ma$ is an F-bilinear map of $M\times A$ into M, and that any A-homomorphism of modules is also an F-linear map.

If M is an FG-module, then each $\sigma \in G$ defines a linear transformation $R(\sigma)$ of the finite-dimensional vector space M by

$$mR(\sigma) = m\sigma, \quad \textit{for all } m\in M. \tag{3.4}$$

The module identities $m(\sigma\tau) = (m\sigma)\tau$, for all $\sigma, \tau \in G$, $m \in M$, and $m1_G = m$, for all $m \in M$, imply that R satisfies (2.5), i.e. that R is a representation of G on M.

Conversely, let R be a representation of G on a finite-dimensional vector space M over F. Then there is a unique FG-module structure for M which is consistent with both (3.4) and the vector space structure of M. Indeed, the module product must be given by

$$m\left(\sum_{\sigma\in G} f_\sigma\sigma\right) = \sum_{\sigma\in G} f_\sigma mR(\sigma), \quad \textit{for all } m\in M \textit{ and any } f_\sigma\textit{'s}\in F. \tag{3.5}$$

Thus there is a complete identity between FG-modules and representations of G on finite-dimensional vector spaces over F.

A module M over an algebra A is *irreducible* if $M \neq \{0\}$, and if M and $\{0\}$ are the only A-submodules of M. The (Jacobson) *radical* $J(A)$ of the algebra A is the two-sided ideal of A defined by

$$J(A) = \{a\in A : Ma = 0, \quad \textit{for all irreducible } A\textit{-modules } M\}. \tag{3.6}$$

The algebra A is called semi-simple if $J(A) = 0$. In the case of group algebras FG we have

PROPOSITION 3.7. *The group algebra FG of a finite group G over a field F is semi-simple if and only if the characteristic of F does not divide the order $|G|$ of G.*

Proof. See Satz V.2.7 in Huppert (1967). Notice that the condition of Proposition 3.7 is always satisfied when F has characteristic zero.

An irreducible module M over an algebra A satisfies $MJ(A) = 0$. So M can naturally be regarded as a module over the factor algebra $A/J(A)$. Obviously M is also irreducible as an $A/J(A)$-module. Evidently $\{0\} = J(A)/J(A)$ is the ideal $J(A/J(A))$ of all elements in $A/J(A)$ annihilating all such irreducible $A/J(A)$-modules M. Hence, we have

the factor algebra $A/J(A)$ is always semi-simple. (3.8)

An algebra A is *simple* if $A \neq \{0\}$ and if A and $\{0\}$ are the only two-sided ideals of A. A *semi-simple* algebra can be decomposed into a direct sum of simple ones.

PROPOSITION 3.9. *A semi-simple algebra A has only a finite number $k \geq 0$ of minimal two-sided ideals $A_1, \ldots, A_k$. Each such ideal A_i is a simple subalgebra of A, and*

$$A = \oplus \sum_{i=1}^{k} A_i. \tag{3.10}$$

Any two-sided ideal of A is a direct sum of a subset of the A_i's. Finally, $A_i A_j = \{0\}$, for all $i, j = 1, \ldots, k$ with $i \neq j$.

Proof. See Satz V.3.8 in Huppert (1967).

Notice that the condition $A_i A_j = \{0\}$, for $i \neq j$, implies that algebra multiplication, as well as addition and scalar multiplication, is componentwise in (3.10):

$$(a_1 \oplus \ldots \oplus a_k)(a_1' \oplus \ldots \oplus a_k') = (a_1 a_1') \oplus (a_2 a_2') \oplus \ldots \oplus (a_k a_k'),$$
$$\text{if } a_i, a_i' \in A_i \quad (i = 1, \ldots, k). \tag{3.11}$$

We indicate this by saying that (3.10) is a *direct sum of algebras* (as well as of vector spaces).

It remains to consider the structure of a simple algebra.

PROPOSITION 3.12. *A simple algebra A has, up to isomorphism, exactly one irreducible module I. The commuting ring $D = \mathrm{Hom}_A(I, I)$ is a division algebra over F. The natural map of A into* Hom (I, I) *is an algebra isomorphism of A onto the commuting ring* $\mathrm{Hom}_D(I, I)$.

Proof. This follows from lemma I.10.5 and Section V.4 in Huppert (1967).

Of course, a *division algebra* is an algebra in which the non-zero elements form a multiplicative group. Notice that our hypotheses of finite-dimensionality for algebras and modules force D to be finite-dimensional over F and I to be finite-dimensional as a vector space over the skew-field D.

The field F is called a *splitting field* for a simple algebra A if the above division algebra D is just $F \cdot 1_D$. Notice that:

PROPOSITION 3.13. *If F is algebraically closed, then it is a splitting field for any simple F-algebra.*

Proof. See Lemma V.4.3 in Huppert (1967).

If A is a semi-simple algebra over F, and $A_1, \ldots, A_k$ are the simple subalgebras of Proposition 3.9, then F is a *splitting field* for A if and only if it is a splitting field for each A_i $(i = 1, \ldots, k)$.

Fix a semi-simple algebra A over F (which may or may not be a splitting field for A). Then A is the direct sum (3.10) of its minimal two-sided ideals $A_1, \ldots, A_k$. There is a corresponding decomposition of A-modules as direct sums of A_i-modules.

PROPOSITION 3.14. *If M is an A-module, then each MA_i $(i = 1 \ldots, k)$, is an A-submodule of M. The A-module MA_i is "really" an A_i-module, in the sense that:*

$$m(a_1 \oplus \ldots \oplus a_t) = ma_i, \quad \text{for all } m \in MA_i,\ a_1 \in A_1, \ldots, a_k \in A_k. \tag{3.15}$$

Furthermore,

$$M = \oplus \sum_{i=1}^{k} MA_i. \tag{3.16}$$

Proof. Since A_i is a two-sided ideal of A, the product MA_i is an A-submodule of M. Equation (3.15) comes from the fact that $A_iA_j = \{0\}$, for all $j \neq i$ (see Proposition 3.9). By (3.10) we have

$$M = MA = \sum_{i=1}^{k} MA_i. \tag{3.17}$$

The intersection $L = MA_i \cap \left(\sum_{j \neq i} MA_i\right)$ is "really" an A_i-submodule of MA_i. Hence it satisfies $L = LA = LA_i$. On the other hand, $LA_i \subseteq \sum_{j \neq i} MA_jA_i = \{0\}$. So $L = \{0\}$ and the sum (3.17) is direct, which finishes the proof of the proposition.

The unique submodule MA_i is called the *A_i-primary* (or *A_i-homogeneous*) *component* of M.

Let I_i be an irreducible A_i-module, for each $i = 1, \ldots, k$ (such a module exists by Proposition 3.12). Using (3.15) in reverse, we regard I_i as an obviously irreducible) A-module.

PROPOSITION 3.18. *Let M be an A-module. For each $i = 1, \ldots, k$, there is a unique integer $m_i \geq 0$ such that*

$$MA_i \cong m_i \times I_i = \overbrace{I_i \oplus \ldots \oplus I_i}^{m_i\text{-times}} \quad (\text{as } A\text{- (or as } A_i\text{-) modules}). \tag{3.19}$$

Proof. It follows from Proposition 3.12 that the simple algebra A_i is semi-simple. So Satz (V.3.4 of Huppert, 1967) tells us that MA_i is a direct sum of

irreducible A_i-modules. But I_i is, to within isomorphism, the only irreducible A_i-module (by Proposition 3.12). Hence (3.19) holds for some integer $m_i \geq 0$. Clearly $m_i = \dim_F(MA_i)/\dim_F(I_i)$ is unique. So the proposition is proved.

The unique integer m_i of Proposition 3.18 is called the *multiplicity* $m(I_i$ in $M)$ of the irreducible A-module I_i in M. Combining the preceding propositions, we get:

$$M \cong (m(I_1 \text{ in } M) \times I_1) \oplus \ldots \oplus (m(I_k \text{ in } M) \times I_k)$$
$$(\textit{as } A\textit{-modules}), \textit{ for all } A\textit{-modules } M. \qquad (3.20)$$

An immediate consequence of this is:

Any irreducible A-module is isomorphic to exactly one of the modules
$$I_1, \ldots, I_k. \qquad (3.21)$$

4. Character Identities

Let G be a finite group. Proposition 3.7 says that the group algebra FG of G over any field F of characteristic zero is semi-simple. If F is algebraically closed, then Proposition 3.13 gives

F is a splitting field for the group algebra FH of any
subgroup H of G. (4.1)

We assume, from now on, that F is any field of characteristic zero satisfying (4.1). As usual, we identify the ordinary integers with their images in F.

It is convenient to extend the definitions of "representation" and "character" from group elements to arbitrary elements of FG. Let M be an FG-module. Then any element y of FG defines an F-linear transformation $R_M(y)$ of the vector space M by

$$mR_M(y) = my, \quad \textit{for all } m \in M. \qquad (4.2)$$

The module identities tell us that the map R_M is an algebra homomorphism of FG into $\mathrm{Hom}_F(M, M)$. It is called the *representation* of FG on M corresponding to the module structure of M. It is related to the representation R of G on M given in (3.4) by

$$R_M\Big(\sum_{\sigma \in G} f_\sigma \sigma\Big) = \sum_{\sigma \in G} f_\sigma R(\sigma), \quad \textit{for any } f_\sigma\textit{'s in } F. \qquad (4.3)$$

The *character* χ_M of the module M is the function from FG to F defined by

$$\chi_M(y) = \mathrm{tr}\,(R_M(y)), \quad \textit{for all } y \in FG. \qquad (4.4)$$

Since both tr and R_M are F-linear, so is χ_M. Evidently, it is related to the character χ_R of the representation R, given in (2.1), by

$$\chi_M\Big(\sum_{\sigma \in G} f_\sigma \sigma\Big) = \sum_{\sigma \in G} f_\sigma \chi_R(\sigma), \quad \textit{for any } f_\sigma\textit{'s in } F. \qquad (4.5)$$

Thus the representation R_M and character χ_M are just the extensions to FG of

the representation R and character χ_R, respectively, by use of F-linearity. From now on we shall use these extended definitions of "representation" and "character".

Proposition 3.9 tells us that the semi-simple algebra FG has the unique decomposition

$$FG = A_1 \oplus \ldots \oplus A_k \quad (\textit{as algebras}), \tag{4.6}$$

where the simple subalgebras $A_1, \ldots, A_k$ are the minimal two-sided ideals of FG. By Proposition 3.12, each A_i $(i = 1, \ldots, k)$ has, up to isomorphism, a unique irreducible module I_i. We regard I_i, as usual, as an irreducible A-module, and denote the corresponding representation R_{I_i} and character χ_{I_i} by R_i and χ_i, respectively. The characters $\chi_1, \ldots, \chi_k$ are called the *irreducible characters* of G (or of FG).

The definition of the FG-module structure of I_i gives

$$R_i(A_j) = \{0\}, \quad \textit{and hence } \chi_i(A_j) = \{0\}, \quad \textit{for all } i, j = 1, \ldots, k \textit{ with } i \neq j. \tag{4.7}$$

Condition (4.1) says that F is a splitting field for each simple algebra A_i. This and Proposition 3.12 imply that

$$R_i \textit{ sends the algebra } A_i \textit{ isomorphically onto } \mathrm{Hom}_F(I_i, I_i), \textit{ for all } i = 1, \ldots, k. \tag{4.8}$$

In particular, there exists an element $a_i \in A_i$ such that $\chi_i(a_i) = \mathrm{tr}\,(R_i(a_i)) = 1$, for any $i = 1, \ldots, k$. Since $\chi_j(a_i) = 0$, for $j \neq i$, (by (4.7)), we conclude that

$$\chi_1, \ldots, \chi_k \textit{ are } F\textit{-linearly independent functions from } FG \textit{ to } F. \tag{4.9}$$

Let M be any FG-module. From (2.10), (3.20) and (4.5) we get

$$\chi_M = m(I_1 \text{ in } M)\chi_1 + \ldots + m(I_k \text{ in } M)\chi_k. \tag{4.10}$$

By (4.9) the multiplicities $m(I_1 \text{ in } M), \ldots, m(I_k \text{ in } M)$ are uniquely determined by the character χ_M via this equation. So (3.20) gives

$$\textit{An } FG\textit{-module } M \textit{ is determined to within isomorphism by its character } \chi_M. \tag{4.11}$$

The algebra FG is itself an FG-module in which the module product my of an element m of the module FG with an element y of the algebra FG is the algebra product of m and y in FG. It is clear from (2.6) and the definition of FG that the corresponding representation of G on FG is the regular representation Reg. So (2.8), (4.5) and the identification of arbitrary integers with their images in F give

$$\chi_{FG}(\sigma) = \begin{cases} |G|, & \textit{if } \sigma = 1_G, \\ 0, & \textit{if } \sigma \in G - \{1_G\}. \end{cases} \tag{4.12}$$

We can compute χ_{FG} another way using (4.10). Clearly $A_i = (FG)A_i$ is the A_i-primary component of the module FG. So $A_i \simeq \mathrm{m}(I_i \text{ in } FG) \times I_i$ as

an A-module. The dimension of I_i is $\chi_i(1)$ by (2.3) and (4.5). The dimension of $A_i \simeq \mathrm{Hom}_F(I_i, I_i)$ (by (4.8)) is $(\dim I_i)^2 = \chi_i(1)^2$. Hence,

$$m(I_i \text{ in } FG) = \dim A_i/\dim I_i = \chi_i(1), \quad \textit{for all } i = 1, \ldots, k. \tag{4.13}$$

This and (4.10) give

$$\chi_{FG} = \chi_1(1)\chi_1 + \ldots + \chi_k(1)\chi_k. \tag{4.14}$$

For each $i = 1, \ldots, k$, the simple algebra A_i has an identity element 1_{A_i}. Let y be a general element of FG. By (4.6) there are unique elements $y_i \in A_i$ $(i = 1, \ldots, k)$ such that $y = y_1 + \ldots + y_k$. From (3.11) we see that $y_i = y1_{A_i}$ $(i = 1, \ldots, k)$. Hence (4.7) implies

$$\begin{aligned} \chi_j(y1_{A_i}) = \chi_j(y_i) &= 0, \quad \textit{if } j = 1, \ldots, k \textit{ and } j \neq i, \\ &= \chi_i(y), \quad \textit{if } j = i. \end{aligned} \tag{4.15}$$

In view of (4.14), this gives

$$\chi_{FG}(y1_{A_i}) = \chi_i(1)\chi_i(y), \quad \textit{for all } y \in FG,\ i = 1, \ldots, k. \tag{4.16}$$

We apply this equation and the other formula (4.12) for χ_{FG} to compute 1_{A_i}. As an element of FG, the identity 1_{A_i} has the form $\sum_{\sigma \in G} f_\sigma \sigma$, for some unique coefficients $f_\sigma \in F$. Evidently f_σ is the coefficient of 1_G when $\sigma^{-1}1_{A_i}$ is written as a linear combination of elements of G:

$$\sigma^{-1}1_{A_i} = f_\sigma 1_G + \ldots$$

Applying χ_{FG} and using (4.12) we obtain

$$\chi_{FG}(\sigma^{-1}1_{A_i}) = |G| f_\sigma, \quad \textit{for all } \sigma \in G.$$

This and (4.16) give us a formula for 1_{A_i} as a function $e(\chi_i)$ of the character χ_i:

$$1_{A_i} = e(\chi_i) = \sum_{\sigma \in G} \frac{\chi_i(1)\chi_i(\sigma^{-1})}{|G|}\sigma, \quad \textit{for } i = 1, \ldots, k. \tag{4.17}$$

We know from (3.11) that $1_{A_i}1_{A_j} = 0$, if $i \neq j$. So (4.15) implies that $\chi_j(1_{A_i}) = 0$, for $i \neq j$. On the other hand, (4.15) also implies that $\chi_i(1_{A_i}) = \chi_i(1)$, for all i. Substituting the expression (4.17) for 1_{A_i} in these equations and using the linearity of the characters χ_j, we obtain

$$\begin{aligned} \frac{\chi_i(1)}{|G|} \sum_{\sigma \in G} \chi_i(\sigma^{-1})\chi_j(\sigma) &= 0, \quad \textit{if } i, j = 1, \ldots, k \textit{ and } i \neq j, \\ &= \chi_i(1), \quad \textit{if } i = j = 1, \ldots, k. \end{aligned}$$

By (2.3) the integer $\chi_i(1)$ is strictly positive. So we can divide by it to get:

$$\begin{aligned} \frac{1}{|G|} \sum_{\sigma \in G} \chi_i(\sigma^{-1})\chi_j(\sigma) &= 0, \quad \textit{if } i, j = 1, \ldots, k \textit{ and } i \neq j, \\ &= 1, \quad \textit{if } i = j = 1, \ldots, k. \end{aligned} \tag{4.18}$$

The identities (4.18) are usually expressed by means of an *inner product*

$(\phi, \psi)_G$ defined for any two linear functions ϕ, ψ from FG to F by

$$(\phi, \psi)_G = \frac{1}{|G|} \sum_{\sigma \in G} \phi(\sigma^{-1})\psi(\sigma). \tag{4.19}$$

Since we can replace σ by σ^{-1} in this summation, $(\cdot, \cdot)_G$ is a symmetric, F-bilinear form on the space $(FG)^* = \mathrm{Hom}_F(FG, F)$. Equations (4.18) just say that

The irreducible characters $\chi_1, \ldots, \chi_k$ are orthonormal with respect to the form $(\cdot, \cdot)_G$. (4.20)

So far we have no close connections between the irreducible characters $\chi_1, \ldots, \chi_k$ and the structure of the group G. One way of forming such connections uses the center $Z(FG)$ of the group algebra FG. The center $Z(\mathrm{Hom}_F(I_i, I_i))$ of the algebra of all F-linear transformations of I_i is clearly the set $F \cdot 1_{I_i \to I_i}$ of F-multiples of the identity transformation. By (4.8) this implies that

$$Z(A_i) = F \cdot 1_{A_i}, \quad (i = 1, \ldots, k). \tag{4.21}$$

This and (4.6) give immediately

$$Z(FG) = Z(A_1) \oplus \ldots \oplus Z(A_k) = F \cdot 1_{A_1} \oplus \ldots \oplus F \cdot 1_{A_k} \quad (\textit{as algebras}). \tag{4.22}$$

There is another way of looking at the center $Z(FG)$. Let $K_1, \ldots, K_c$ be the conjugacy classes of the finite group G, and $\tilde{K}_i$ be the *class sum*

$$\tilde{K}_i = \sum_{\sigma \in K_i} \sigma \tag{4.23}$$

in FG, for $i = 1, \ldots, c$). Then we have

PROPOSITION 4.24. *The class sums $\tilde{K}_1, \ldots, \tilde{K}_c$ form a basis for the algebra $Z(FG)$.*

Proof. Let $y = \sum_{\sigma \in G} f_\sigma \sigma$ be any element of FG, where the f_σ's all lie in F. Evidently y lies in $Z(FG)$ if and only if $y\tau = \tau y$, for all τ in the basis G of FG, i.e. if and only if $\tau^{-1} y \tau = y$, for all $\tau \in G$. Since $\tau^{-1} y \tau = \sum_{\sigma \in G} f_\sigma \sigma^\tau$, this occurs if and only if $f_\sigma = f_{\sigma^\tau}$ for all $\sigma, \tau \in G$, i.e. if and only if y is a linear combination of the class sums $\tilde{K}_1, \ldots, \tilde{K}_c$. Therefore $\tilde{K}_1, \ldots, \tilde{K}_c$ span $Z(FG)$. They are linearly independent, since $K_1, \ldots, K_c$ are pairwise disjoint, non-empty subsets of G. So the proposition holds.

Combining this proposition with (4.22) we obtain

PROPOSITION 4.25. *The number k of irreducible characters of G equals the number c of conjugacy classes of G.*

Proof. By (4.22), $k = \dim_F Z(FG)$. By Proposition 4.24, the latter number is c. So the proposition holds.

There is another way to regard Proposition 4.25. A *class function* on the group G is a linear function $\phi : FG \to F$ which is constant on each conjugacy class K_i of G. Evidently these functions form an F-subspace $CF(G)$ of $(FG)^*$ and $\dim_F(CF(G)) = c$. By Proposition 2.2, each character χ_M of G is a class function. In view of (4.9) and (4.20), Proposition 4.25 is equivalent to

The irreducible characters $\chi_1, \ldots, \chi_k$ form an orthonormal basis for $CF(G)$ with respect to the form $(\cdot, \cdot)_G$. (4.26)

Since $Z(FG)$ is a subalgebra of FG, there are unique multiplication coefficients a_{hij}, $(h, i, j = 1, \ldots, c)$, such that

$$\tilde{K}_h \tilde{K}_i = \sum_{j=1}^{c} a_{hij} \tilde{K}_j, \quad (h, i = 1, \ldots, c). \tag{4.27}$$

These coefficients have a simple, but important, relationship with multiplication in the group G.

PROPOSITION 4.28. *Let $h, i, j = 1, \ldots, c$. If $\rho \in K_j$, then a_{hij} is the number of ordered pairs (σ, τ) of elements of G such that $\sigma \in K_h$, $\tau \in K_i$ and $\sigma\tau = \rho$.*

Proof. By (4.27), a_{hij} is the coefficient of ρ in $\tilde{K}_h \tilde{K}_i = \sum_{\sigma \in K_h, \tau \in K_i} \sigma\tau$. This coefficient is obviously the number of the above ordered pairs (σ, τ).

Evidently the decomposition (4.22) gives us k distinct epimorphisms $\theta_1, \ldots, \theta_k$ of the algebra $Z(FG)$ onto F defined by

$$\theta_i(f_1 \cdot 1_{A_1} \oplus \ldots \oplus f_k \cdot 1_{A_k}) = f_i, \quad \textit{for all } i = 1, \ldots, k \textit{ and any } f_j\text{'s in } F. \tag{4.29}$$

These epimorphisms θ_i can easily be computed in terms of the irreducible characters χ_i.

If $y \in Z(FG)$, then evidently $R_i(y) = \theta_i(y) \cdot 1_{I_i \to I_i} \in \mathrm{Hom}_F(I_i, I_i)$. Since the trace of the identity transformation $1_{I_i \to I_i}$ is $\dim_F I_i$, which equals $\chi_i(1)$ by (2.3), we have

$$\chi_i(y) = \mathrm{tr}\,(R_i(y)) = \theta_i(y)\,\mathrm{tr}\,(1_{I_i \to I_i}) = \theta_i(y)\chi_i(1).$$

Therefore,

$$\theta_i(y) = \frac{\chi_i(y)}{\chi_i(1)}, \quad \textit{for all } y \in Z(FG) \textit{ and all } i = 1, \ldots, k. \tag{4.30}$$

If we substitute (4.30) in the formula $\theta_i(yz) = \theta_i(y)\theta_i(z)$ (which is valid for all $y, z \in Z(FG)$ since θ_i is a homomorphism) and then multiply by $\chi_i(1)^2$, we obtain the useful formula:

$$\chi_i(y)\chi_i(z) = \chi_i(1)\chi_i(yz), \quad \textit{for all } y, z \in Z(FG), \text{ and } i = 1, \ldots, k. \tag{4.31}$$

We can use the formulas (4.18) and (4.30) to compute the values of the irreducible characters χ_i starting from the multiplication table of the group G. By Proposition 4.28, we can compute the multiplication coefficients a_{hij} in

(4.27). Since any θ_g is a homomorphism of $Z(FG)$ into F, its value $\theta_g(\tilde{K}_h)$ at a class sum $\tilde{K}_h$ satisfies:

$$\theta_g(\tilde{K}_h)\theta_g(\tilde{K}_i) = \sum_{j=1}^{c} a_{hij}\theta_g(\tilde{K}_j), \quad \textit{for all } i = 1, \ldots, c.$$

Because θ_g is an epimorphism, not all the $\theta_g(\tilde{K}_i)$ $(i = 1, \ldots, c)$, can be zero. We conclude that $\theta_g(\tilde{K}_h)$ is an eigenvalue of the $c \times c$ matrix $(a_{hij})_{i,j=1,\ldots,c}$, and that $(\theta_g(\tilde{K}_1), \ldots, \theta_g(\tilde{K})_c)^T$ is a corresponding eigenvector. With this observation one can theoretically (and even practically on a computer) compute the values $\theta_g(\tilde{K}_h)$ of the k distinct epimorphisms $\theta_1, \ldots, \theta_k$ of $Z(FG)$ onto F at the class sums $\tilde{K}_h$, $(h = 1, \ldots, c)$. Applying Proposition 2.2, and (4.30), we get

$$\frac{\chi_g(\sigma)}{\chi_g(1)} = \frac{\theta_g(\tilde{K}_h)}{|K_h|}, \quad \textit{for all } g = 1, \ldots, k \textit{ and } \sigma \in G, \tag{4.32}$$

where K_h is the class σ^G of σ. Using (4.18) we find that

$$\frac{1}{\chi_g(1)^2} = \frac{1}{|G|} \sum_{\sigma \in G} \frac{\chi_g(\sigma^{-1})}{\chi_g(1)} \frac{\chi_g(\sigma)}{\chi_g(1)}, \quad \textit{for all } g = 1, \ldots, k.$$

Therefore $\chi_g(1)^2$ is computable. But $\chi_g(1)$ is a positive integer by (2.3). Hence it is computable. This, together with (4.32), determines the character values $\chi_g(\sigma)$ for all $\sigma \in G$ and all $g = 1, \ldots, k$.

Of course the above program is a bit difficult because of the eigenvalue computation needed in the middle. But it does imply one important fact: *the multiplication coefficients a_{hij} of* (4.27) *determine the irreducible characters $\chi_1, \ldots, \chi_k$ of G; in particular, any information about these coefficients should be reflected in properties of the group characters.*

We illustrate the last principle, which is vital in many proofs, by considering the coefficients of 1_G in (4.27). Evidently $\{1_G\}$ is a class, say K_1, and 1_G is its class sum $\tilde{K}_1$. For any class K_i, let K_i^{-1} be the class $\{\sigma^{-1} : \sigma \in K_i\}$ and $\widetilde{K_i^{-1}}$ be its class sum. Using Proposition 4.28 with $\rho = 1_G$, we compute to obtain

$$\begin{aligned} \tilde{K}_i\widetilde{K_j^{-1}} &= 0 \cdot 1_G + \ldots, && \textit{if } i, j = 1, \ldots, c \textit{ and } i \neq j, \\ &= |K_i| \cdot 1_G + \ldots, && \textit{if } i = j = 1, \ldots, c, \end{aligned}$$

where the three dots refer to linear combinations of the other sums $\tilde{K}_h$ $(h > 1)$.

Applying χ_{FG} to these equations and using (4.12), we obtain

$$\chi_{FG}(\tilde{K}_i\widetilde{K_j^{-1}}) = \begin{cases} 0, & \textit{if } i, j = 1, \ldots, c \textit{ and } i \neq j, \\ |G||K_i|, & \textit{if } i = j = 1, \ldots, c. \end{cases}$$

Next we use (4.14) and (4.31) to get

$$\chi_{FG}(\widetilde{K_i K_j^{-1}}) = \sum_{h=1}^{k} \chi_h(1)\chi_h(\tilde{K}_i K_j^{-1}) = \sum_{h=1}^{k} \chi_h(\tilde{K}_i)\chi_h(\widetilde{K_j^{-1}}).$$

Choose any elements $\sigma \in K_i$, $\tau \in K_j$. Then Proposition 2.2 implies that $\chi_h(\tilde{K}_i) = |K_i|\chi_h(\sigma)$, and $\chi_h(\widetilde{K_j^{-1}}) = |K_j|\chi_h(\tau^{-1})$, for all $h = 1, \ldots, k$. Hence the above equations become:

$$|K_i||K_j| \sum_{h=1}^{k} \chi_h(\sigma)\chi_h(\tau^{-1}) = \begin{cases} 0, & \text{if } \sigma \underset{G}{\nsim} \tau, \\ |G||K_i|, & \text{if } \sigma \underset{G}{\sim} \tau, \end{cases}$$

where, of course, $\sigma \underset{G}{\sim} \tau$ means "σ is G-conjugate to τ", and $\chi \underset{G}{\nsim} \tau$ means "σ is not G-conjugate to τ". Dividing by $|K_i||K_j|$, and using the fact that $|G|/|K_j| = |C_G(\tau)|$, we obtain the following identities:

$$\sum_{h=1}^{k} \chi_h(\sigma)\chi_h(\tau^{-1}) = \begin{cases} |C_G(\tau)|, & \text{if } \sigma, \tau \in G \text{ and } \sigma \underset{G}{\sim} \tau, \\ 0, & \text{if } \sigma, \tau \in G \text{ and } \sigma \underset{G}{\nsim} \tau. \end{cases} \tag{4.33}$$

Besides their relations with the conjugacy classes and the multiplication coefficients a_{hij}, the irreducible characters of G are also connected with certain normal subgroups of G. To explain this connection, we start with two lemmas.

LEMMA 4.34. *Let M be any FG-module and σ be any element of G. Then there exists a basis $m_1, \ldots, m_n$ for M satisfying:*

$$m_i\sigma = \zeta_i m_i \quad (i = 1, \ldots, n), \tag{4.35}$$

where $\zeta_1, \ldots, \zeta_n \in F$ are $|G|$th roots of unity (they are even eth roots of unity, where e is the exponent of G).

Proof. The cyclic subgroup $\langle\sigma\rangle$ generated by σ is abelian, and F is a splitting field for its group algebra $F\langle\sigma\rangle$ by (4.1). It follows from (4.6) and (4.8) that each irreducible $F\langle\sigma\rangle$-module is one-dimensional. Because $F\langle\sigma\rangle$ is semi-simple, (3.20) tells us that M, considered as an $F\langle\sigma\rangle$-module, is a direct sum of irreducible $F\langle\sigma\rangle$-submodules $J_1 \oplus \ldots \oplus J_n$. If m_i is a basis element for the one-dimensional module J_i ($i = 1, \ldots, n$), then $m_1, \ldots, m_n$ is a basis for M satisfying (4.35), for some $\zeta_1, \ldots, \zeta_n \in F$. Evidently $\sigma^e = 1$ implies that each ζ_i is an eth root of unity and hence a $|G|$th root of unity. So the lemma holds.

LEMMA 4.36. *Let* $\zeta_1, \ldots, \zeta_n$ $(n \geq 1)$ *be* $|G|$th *roots of unity in* F. *If* $\zeta_1 + \ldots + \zeta_n = n\zeta$, *where* ζ *is also a* $|G|$th *root of unity, then* $\zeta_1 = \ldots = \zeta_n = \zeta$.

Proof. The $|G|$th roots of unity in F generate a subfield E which is finite-dimensional over the rational subfield Q. Evidently it suffices to prove the lemma for E in place of F. But E can be isomorphically embedded in the complex numbers C. Therefore it suffices to prove the lemma for $F = C$.

In C, the absolute value $|\zeta|$ of any $|G|$th root of unity is 1. So, we have

$$|\zeta_1 + \ldots + \zeta_n| = |n\zeta| = n = |\zeta_1| + \ldots + |\zeta_n|.$$

This implies that $\zeta_1, \ldots, \zeta_n$ are all positive multiples of each other. Since they all have absolute value 1, they must be equal $\zeta_1 = \ldots = \zeta_n$. Evidently their common value is $(\zeta_1 + \ldots + \zeta_n)/n = \zeta$. So the lemma holds.

The normal subgroups associated with the irreducible character χ_i $(i = 1, \ldots, k)$ are

$$\text{Ker}\,(\chi_i) = \{\sigma \in G : y\sigma = y, \quad \textit{for all } y \in I_i\} \tag{4.37a}$$

$$Z(G \bmod \text{Ker}\,(\chi_i)) = \{\sigma \in G : \sigma \text{ Ker}\,(\chi_i) \in Z(G/\text{Ker}\,(\chi_i))\}. \tag{4.37b}$$

Their relations with the values of χ_i are given by

PROPOSITION 4.38. *Fix* $i = 1, \ldots, k$. *If* $\sigma \in G$, *then*

(a) $\sigma \in \text{Ker}\,(\chi_i)$ *if and only if* $\chi_i(\sigma) = \chi_i(1)$,

(b) $\sigma \in Z(G \bmod \text{Ker}\,(\chi_i))$ *if and only if* $\chi_i(\sigma) = \zeta\chi_i(1)$, *for some* $|G|$th *root of unity* $\zeta \in F$.

Proof. If $\sigma \in Z(G \bmod \text{Ker}\,(\chi_i))$, then the linear transformation $R_i(\sigma)$ evidently commutes with every $R_i(\tau)$ $(\tau \in G)$. In view of (4.8), $R_i(\sigma)$ must lie in the center of $\text{Hom}_F(I_i, I_i)$. So it has the form $R_i(\sigma) = \zeta \cdot 1_{I_i \to I_i}$, where $\zeta \in F$. This implies that $\chi_i(\sigma) = \zeta \dim_F(I_i) = \zeta\chi_i(1)$, by (2.3). Since $\sigma^{|G|} = 1$, the element $\zeta \in F$ is a $|G|$th root of unity. Obviously $\zeta = 1$ if and only if $\sigma \in \text{Ker}\,(\chi_i)$. So we have proved the "only if" parts of both (a) and (b).

Now suppose that σ satisfies $\chi_i(\sigma) = \zeta\chi_i(1)$, for some $|G|$th root of unity $\zeta \in F$ (in the case (a), we take $\zeta = 1$). Lemma 4.34 gives us a basis $m_1, \ldots, m_n$ for I_i and $|G|$th roots of unity $\zeta_1, \ldots, \zeta_n$ satisfying (4.35). The trace $\chi_i(\sigma)$ of $R_i(\sigma)$ is then clearly $\zeta_1 + \ldots + \zeta_n = n\zeta$, which implies $\zeta_1 = \ldots = \zeta_n = \zeta$ by Lemma 4.36. So $R_i(\sigma) = \zeta 1_{I_i \to I_i}$ commutes with $R_i(\tau)$, for all $\tau \in G$, which is equivalent to saying that $\sigma \in Z(G \bmod \text{Ker}\,(\chi_i))$. When $\zeta = 1$, we even have $\sigma \in \text{Ker}\,(\chi_i)$. Therefore the proposition is true.

5. Induced Characters

We continue to use the notation and hypotheses of Section 4. If $\sigma \in G$ and $\chi \in (FG)^* = \text{Hom}_F(FG, F)$, then the *conjugate function* $\chi^\sigma \in (FG)^*$ is given by:

$$\chi^\sigma(y) = \chi(y^{\sigma^{-1}}) = \chi(\sigma y \sigma^{-1}), \quad \textit{for all } y \in FG. \tag{5.1}$$

This is a linear action of G on $(FG)^*$ contragradient to the conjugation action of G on FG. Notice that the form $(\cdot, \cdot)_G$ of (4.19) is invariant under this action:

$$(\xi^\sigma, \chi^\sigma)_G = (\xi, \chi)_G, \quad \textit{for all } \sigma \in G,\ \xi, \chi \in (FG)^*. \tag{5.2}$$

The subspace $CF(G)$ of all class functions on G is evidently given by

$$CF(G) = \{\chi \in (FG)^* : \chi^\sigma = \chi, \quad \textit{for all } \sigma \in G\}. \tag{5.3}$$

Let H be any subgroup of G. We extend any function $\phi \in CF(H)$ to a linear function $\hat{\phi} \in (FG)^*$ by setting $\hat{\phi}(\sigma) = 0$, for all $\sigma \in G \backslash H$. So $\hat{\phi}$ is defined by:

$$\hat{\phi}\Big(\sum_{\sigma \in G} f_\sigma \sigma\Big) = \phi\Big(\sum_{\sigma \in H} f_\sigma \sigma\Big), \quad \textit{for any } f_\sigma\textit{'s in } F. \tag{5.4}$$

Since ϕ is a class function on H, its extension $\hat{\phi}$ satisfies $\hat{\phi}^\sigma = \hat{\phi}$ for all $\sigma \in H$. Hence we can define the *induced function* $\phi^G \in (FG)^*$ to be the "trace from H to G" of $\hat{\phi}$:

$$\phi^G = \sum_{\sigma \in \operatorname{rep}(G/H)} \hat{\phi}^\sigma, \tag{5.5}$$

where rep (G/H) is any family of representatives for the left cosets $H\sigma$ of H in G. Evidently ϕ^G is independent of the choice of these representatives, and is fixed under conjugation by any element of G. So (5.3) implies

$$\textit{Induction: } \phi \to \phi^G \textit{ is an } F\textit{-linear map of } CF(H) \textit{ into } CF(G). \tag{5.6}$$

The restriction χ_H to FH of a class function χ of G is clearly a class function of H. The F-linear map $\chi \to \chi_H$ of $CF(G)$ into $CF(H)$ is, in fact, contragradient to induction.

PROPOSITION 5.7 (Frobenius reciprocity law). *If $\chi \in CF(G)$ and $\phi \in CF(H)$, then*

$$(\chi, \phi^G)_G = (\chi_H, \phi)_H.$$

Proof. We know from (5.3) that $\chi = \chi^\sigma$, for all $\sigma \in G$. So (5.5) and (5.2) give:

$$\begin{aligned}(\chi, \phi^G)_G &= \Big(\chi, \sum_{\sigma \in \operatorname{rep}(G/H)} \hat{\phi}^\sigma\Big)_G \\ &= \sum_{\sigma \in \operatorname{rep}(G/H)} (\chi^\sigma, \hat{\phi}^\sigma)_G = [G : H](\chi, \hat{\phi})_G.\end{aligned}$$

By (4.19) and (5.4), we have:

$$\begin{aligned}(\chi, \hat{\phi})_G &= \frac{1}{|G|} \sum_{\sigma \in G} \chi(\sigma)\hat{\phi}(\sigma^{-1}) = \frac{1}{|G|} \sum_{\sigma \in H} \chi(\sigma)\phi(\sigma^{-1}) \\ &= \frac{1}{[G : H]} (\chi_H, \phi)_H.\end{aligned}$$

The result follows from this and the preceding equation.

The Frobenius reciprocity law has the following important consequence.

PROPOSITION 5.8. *If ϕ is a character of H, then ϕ^G is a character of G.*

Proof. By (4.26) the class function ϕ^G is a unique linear combination $\phi^G = f_1\chi_1 + \ldots + f_k\chi_k$, with coefficients $f_1, \ldots, f_k \in F$, of the irreducible characters $\chi_1, \ldots, \chi_k$ of G. In view of (4.10), ϕ^G is a character of G if and only if each f_i is a non-negative integer. Using (4.20) and the Frobenius reciprocity law, we have:

$$f_i = (\chi_i, \phi^G)_G = ((\chi_i)_H, \phi)_H.$$

Evidently the restriction $(\chi_i)_H$ is a character of H (the corresponding representation is that of FH on the FG-module I_i). By definition, ϕ is a character of H. If $\lambda_1, \ldots, \lambda_l$ are the irreducible characters of H, equation (4.10) gives us non-negative integers $n_1, \ldots, n_l, m_1, \ldots, m_l$ such that

$$(\chi_i)_H = n_1\lambda_1 + \ldots + n_l\lambda_l, \qquad \phi = m_1\lambda_1 + \ldots + m_l\lambda_l.$$

But then (4.20) for H implies:

$$f_i = ((\chi_i)_H, \phi)_H = \sum_{i=1}^{l} n_i m_i.$$

The last expression is a non-negative integer, since each n_i or m_i is. This completes the proof of the proposition.

Another consequence of the Frobenius reciprocity law is used often enough to deserve special mention.

PROPOSITION 5.9. *Let $\chi_1, \ldots, \chi_k$ be the irreducible characters of G, and $\lambda_1, \ldots, \lambda_l$ be the irreducible characters of H, where χ_1, λ_1 are the trivial characters of G, H, respectively. If $\phi = \sum_{i=1}^{l} f_i\lambda_i$, with each $f_i \in F$, is any class function on H, and $\phi^G = \sum_{j=1}^{k} e_j\chi_j$, with each $e_j \in F$, then $e_1 = f_1$.*

Proof. This is shorter to prove than to state. Obviously $(\chi_1)_H = \lambda_1$. So the Frobenius reciprocity law and (4.26) give:

$$e_1 = (\lambda_1, \phi)_H = ((\chi_1)_H, \phi)_H = (\chi_1, \phi^G) = f_1,$$

which proves the result.

A *trivial intersection set* (or *t.i. set*) with H as its normalizer is a non-empty subset S of H satisfying:

$$S^\sigma = S, \quad \textit{for all } \sigma \in H, \tag{5.10a}$$

$$S^\sigma \cap S \textit{ is empty}, \quad \textit{for all } \sigma \in G \backslash H, \tag{5.10b}$$

$$S = S^{-1} = \{\sigma^{-1} : \sigma \in S\}. \tag{5.10c}$$

As an example of a t.i. set, we define a subset $\sqrt{\sigma}$, for any $\sigma \in G$, by:

$$\sqrt{\sigma} = \{\tau \in G : \sigma \in \langle\tau\rangle\}. \tag{5.11}$$

Then we have:

PROPOSITION 5.12. *For any $\sigma \in G$, the set $\sqrt{\sigma}$ is a t.i. set with $N_G(\langle\sigma\rangle)$ as its normalizer.*

Proof. Clearly $\sqrt{\sigma}$ is a non-empty subset of $N_G(\langle\sigma\rangle)$. Since $\sigma \in \langle\tau\rangle$ if and only if $\langle\sigma\rangle \leq \langle\tau\rangle$, the subset $\sqrt{\sigma}$ is invariant under conjugation by elements of $N_G(\langle\sigma\rangle)$. If $\rho \in G\backslash N_G(\langle\sigma\rangle)$ and $\tau \in S^\rho \cap S$, then $\langle\tau\rangle$ contains both $\langle\sigma\rangle$ and $\langle\sigma^\rho\rangle = \langle\sigma\rangle^\rho \neq \langle\sigma\rangle$. This is impossible, since the cyclic group $\langle\tau\rangle$ contains only one subgroup of order $|\langle\sigma\rangle| = |\langle\sigma\rangle^\rho|$. Hence $S^\rho \cap S$ is empty. Finally $\langle\tau\rangle = \langle\tau^{-1}\rangle$ implies that $(\sqrt{\sigma})^{-1} = \sqrt{\sigma}$. So the proposition holds.

Let S be any t.i. set with H as its normalizer. We define an F-subspace $CF(H|S)$ of $CF(H)$ by

$$CF(H|S) = \{\phi \in CF(H) : \phi(\sigma) = 0, \quad \text{for all } \sigma \in H\backslash S\}. \tag{5.13}$$

The functions in $CF(H|S)$ behave very well under induction.

PROPOSITION 5.14. *If $\phi \in CF(H|S)$ and $\sigma \in G$, then*

$$\phi^G(\sigma) = \begin{cases} 0, & \text{unless } \sigma \underset{G}{\sim} \tau, \text{ for some } \tau \in S, \\ \phi(\tau), & \text{if } \sigma \underset{G}{\sim} \tau, \text{ for some } \tau \in S. \end{cases}$$

Proof. By (5.4) the extension $\hat{\phi}$ is zero on $G\backslash S$. For any $\rho \in \text{rep}\,(G/H)$, the conjugate $\hat{\phi}^\rho$ is zero on $G\backslash S^\rho$. From (5.5) we conclude that ϕ^G is zero on $G\backslash \bigcup_\rho S^\rho$, which gives the first of the above equations. For the second, we may assume that $\sigma = \tau \in S$, since ϕ^G is a class function on G. Then (5.10) implies that $\sigma \notin S^\rho$ for all $\rho \in \text{rep}\,(G/H)$ except the single representative $\rho_0 \in H$. So $\hat{\phi}^\rho(\sigma) = 0$, for all $\rho \neq \rho_0$ in rep (G/H). This and (5.5) imply that $\phi^G(\sigma) = \hat{\phi}^{\rho_0}(\sigma) = \hat{\phi}(\sigma^{\rho_0 \rho_0^{-1}}) = \phi(\sigma^{\rho_0 \rho_0^{-1}}) = \phi(\sigma)$, which completes the proof of the proposition.

From this proposition and the Frobenius reciprocity law, we deduce

PROPOSITION 5.15. *The map $\phi \to \phi^G$ is an isometry of $CF(H|S)$ into $CF(G|S^G)$ $\left(\text{where } S^G = \bigcup_{\sigma \in G} S^\sigma\right)$, i.e.*

$$(\phi^G, \xi^G)_G = (\phi, \xi)_H, \quad \text{for all } \phi, \xi \in CF(H|S). \tag{5.16}$$

Proof. By (5.6) and Proposition 5.14 the map $\phi \to \phi^G$ sends $CF(H|S)$ linearly into $CF(G|S^G)$. So we only need to prove (5.16). The Frobenius reciprocity law gives

$$(\phi^G, \xi^G)_G = ((\phi^G)_H, \xi)_H = \frac{1}{|H|} \sum_{\sigma \in H} \phi^G(\sigma)\xi(\sigma^{-1}).$$

Since $\xi \in CF(H|S)$, the value $\xi(\sigma^{-1})$ is zero unless $\sigma^{-1} \in S$. By (5.10c) this

occurs if and only if $\sigma \in S$. But then $\phi^G(\sigma) = \phi(\sigma)$ by Proposition 5.14. So we have

$$(\phi^G, \xi^G)_G = \frac{1}{|H|} \sum_{\sigma \in S} \phi^G(\sigma)\xi(\sigma^{-1}) = \frac{1}{|H|} \sum_{\sigma \in S} \phi(\sigma)\xi(\sigma^{-1})$$
$$= \frac{1}{|H|} \sum_{\sigma \in H} \phi(\sigma)\xi(\sigma^{-1}) = (\sigma, \xi)_H,$$

which proves the proposition.

Obviously the identity 1_G can lie in S only if $H = G$, which is not a very interesting case. So (2.3) implies that the only character in $CF(H|S)$ is 0, whenever $H < G$. Nevertheless, one can very well have generalized characters of H in $CF(H|S)$. A *generalized character* χ of the group G is a class function of the form

$$\chi = n_1\chi_1 + \ldots + n_k\chi_k, \quad (n_1, \ldots, n_k \in \mathbf{Z}) \tag{5.17}$$

where, as usual, $\chi_1, \ldots, \chi_k$ are the irreducible characters of G. By (4.10) the generalized character χ is an actual character if and only if each of the coefficients $n_1, \ldots, n_k$ is non-negative. Clearly the generalized characters form the additive subgroup $X(G)$ of $CF(G)$ generated by the characters. From this description and Proposition 5.8 we immediately obtain

Induction $\phi \to \phi^G$ is an additive homorphism of $X(H)$ into $X(G)$. (5.18)

We denote by $X(H|S)$ the intersection $X(H) \cap CF(H|S)$, consisting of all generalized characters ϕ of H vanishing on $H \setminus S$. Then (5.18) and Proposition 5.15 give

Induction $\phi \to \phi^G$ is an additive isometry of the subgroup $X(H|S)$ into $X(G|S^G)$. (5.19)

To obtain the full force of trivial intersection sets, we use them in conjunction with involutions of the group G. An *involution* is just an element of order 2. Their most important property is

PROPOSITION 5.20. *If ι, ι' are involutions in G, then $\sigma = \iota\iota'$ is inverted by both ι and ι':*

$$\sigma^{\iota} = \sigma^{\iota'} = \sigma^{-1}. \tag{5.21}$$

It follows that $\langle \iota, \iota' \rangle = \langle \iota, \sigma \rangle$ is a dihedral subgroup of G, with $\langle \sigma \rangle$ as a normal cyclic subgroup of index 2.

Proof. Since $\iota = \iota^{-1}$ and $\iota' = \iota'^{-1}$, we have:

$$\sigma^{-1} = (\iota')^{-1}\iota^{-1} = \iota'\iota = \iota^{-1}(\iota\iota')\iota = \sigma^{\iota}$$

Similarly we have $\sigma^{-1} = \sigma^{\iota'}$. So (5.21) holds. The rest of the proposition follows easily from this.

COROLLARY 5.22. *If $\sigma \in S$, then $\iota, \iota' \in H$.*

Proof. By (5.21) and (5.10c), the intersection $S^\iota \cap S$ contains $\sigma^\iota = \sigma^{-1}$. So $\iota \in H$ by (5.10b). Similarly $\iota' \in H$.

As a result of the above corollary, we obtain the very useful

PROPOSITION 5.23. *Let I, I' be conjugacy classes of involutions in G. Denote by $\tilde{I}$, $\tilde{I'}$, $\widetilde{(I \cap H)}$, $\widetilde{(I' \cap H)}$ the sums in FG of the elements of the corresponding sets I, I', $I \cap H$, $I' \cap H$, respectively. If $\phi \in CF(H|S)$, then we have*

$$\phi^G(\tilde{I}\tilde{I'}) = [G : H]\phi(\widetilde{(I \cap H)}\,\widetilde{(I' \cap H)}). \tag{5.24}$$

Proof. Let $\tilde{I}\tilde{I'} = \sum_{\sigma \in G} f_\sigma \sigma$, for non-negative integers f_σ. If $\sigma \notin S^G$, then $\phi^G(\sigma) = 0$ by Proposition 5.14. Hence,

$$\phi^G(\tilde{I}\tilde{I'}) = \sum_{\sigma \in S^G} f_\sigma \phi^G(\sigma).$$

The conditions (5.10) say that S^G is the disjoint union of its conjugate subsets S^ρ, for $\rho \in \text{rep}\,(G|H)$. Since $\tilde{I}\tilde{I'} \in Z(FG)$, the constant f_σ^ρ equals f_σ, for all $\sigma \in S$, $\rho \in \text{rep}\,(G|H)$. Applying Proposition 5.14 again, we get

$$\begin{aligned}\phi^G(\tilde{I}\tilde{I'}) &= \sum_{\rho \in \text{rep}\,(G/H)} f_\sigma \phi^G(\sigma^\rho) \\ &= [G : H] \sum_{\sigma \in S} f_\sigma \phi(\sigma).\end{aligned}$$

If $\sigma \in S$, the coefficient f_σ of σ in $\tilde{I}\tilde{I'}$ is just the number of ordered pairs of involutions (ι, ι') such that $\iota \in I$, $\iota' \in I'$ and $\iota\iota' = \sigma$. In view of Corollary 5.22, this is just the number e_σ of ordered pairs (ι, ι'), where $\iota \in I \cap H$, $\iota' \in I' \cap H$ and $\iota\iota' = \sigma$. But e_σ in turn is the coefficient of σ in $\widetilde{(I \cap H)}\,\widetilde{(I' \cap H)} = \sum_{\sigma \in H} e_\sigma \sigma$. Since $\phi(\sigma) = 0$ for $\sigma \in H \backslash S$, the previous equation becomes

$$\begin{aligned}\phi^G(\tilde{I}\tilde{I'}) &= [G : H] \sum_{\sigma \in S} e_\sigma \phi(\sigma) = [G : H]\phi\left(\sum_{\sigma \in H} e_\sigma \sigma\right) \\ &= [G : H]\phi(\widetilde{(I \cap H)}\,\widetilde{(I' \cap H)}),\end{aligned}$$

and this proves the proposition.

6. Generalized Quaternion Sylow Groups

We apply the ideas of the last section to study the finite groups having generalized quaternion groups as 2-Sylow subgroups.

To construct a generalized quaternion group, we start with a cyclic group

$\langle\tau\rangle$ of order 2^n, where $n \geq 2$. The automorphism $\sigma \to \sigma^{-1}$ of $\langle\tau\rangle$ then has order 2 and leaves fixed the involution $\iota = \tau^{2^{n-1}}$. It follows that there is a unique group Q containing $\langle\tau\rangle$ as a normal subgroup of index 2, in which some element $\rho \in Q\backslash\langle\tau\rangle$ satisfies

$$\tau^\rho = \tau^{-1}, \qquad \rho^2 = \iota = \tau^{2^{n-1}}. \tag{6.1}$$

This group Q is called the generalized quaternion group of order 2^{n+1}. If $n = 2$, it is, of course, the ordinary quaternion group.

PROPOSITION 6.2. *Each element $\rho \in Q\backslash\langle\tau\rangle$ satisfies* (6.1). *Hence ι is the only involution in Q.*

Proof. Fix an element $\rho_0 \in Q\backslash\langle\tau\rangle$ satisfying (6.1). Since $[Q : \langle\tau\rangle] = 2$, any element $\rho \in Q\backslash\langle\tau\rangle$ has the form $\tau^i\rho_0$, for some integer i. From (6.1) for ρ_0 we compute that

$$\tau^\rho = \tau^{\tau^i\rho_0} = \tau^{\rho_0} = \tau^{-1},$$
$$\rho^2 = \tau^i\rho_0\tau^i\rho_0 = \tau^i\rho_0^2(\rho_0^{-1}\tau^i\rho_0) = \tau^i\iota\tau^{-i} = \iota.$$

Therefore ρ also satisfies (6.1). In particular, ρ has order 4. So any involution in Q must lie in $\langle\tau\rangle$ and therefore equal ι, which finishes the proof.

We must compute some irreducible characters of Q in a field F of characteristic zero satisfying (4.1) for the group Q. Certainly we have the trivial character $1 = 1_{Q \to F}$. Since $Q/\langle\tau\rangle$ is cyclic of order 2, we have a linear character λ satisfying

$$\chi = \begin{cases} -1 & \text{on } Q\backslash\langle\tau\rangle, \\ 1 & \text{on } \langle\tau\rangle. \end{cases} \tag{6.3}$$

Because $n \geq 2$, there is a linear character μ of $\langle\tau\rangle$ sending τ into a primitive fourth root of unity $\sqrt{-1}$. We can find such a root in F by (4.1). So we have two linear characters μ, μ^{-1} of $\langle\tau\rangle$ given by

$$\mu(\tau^i) = (\sqrt{-1})^i, \qquad \mu^{-1}(\tau^i) = (\sqrt{-1})^{-i} = (-\sqrt{-1})^i, \quad \textit{for all integers } i. \tag{6.4}$$

By (5.5) and (6.1), the induced character $\theta = \mu^Q$ satisfies

$$\theta = \begin{cases} 0 & \text{on } Q\backslash\langle\tau\rangle, \\ \mu + \mu^{-1} & \text{on } \langle\tau\rangle. \end{cases} \tag{6.5}$$

Since μ and μ^{-1} are distinct irreducible characters of $\langle\tau\rangle$, the Frobenius reciprocity law implies that $(\theta, \theta)_Q = (\theta_{\langle\tau\rangle}, \mu)_{\langle\tau\rangle} = (\mu + \mu^{-1}, \mu)_{\langle\tau\rangle} = 1$. But the character θ is a linear contribution of the irreducible characters of Q with non-negative integral coefficients. From this and (4.20) we conclude that θ is an irreducible character of Q. Since $\theta(1) = 2 \neq 1 = 1(1) = \lambda(1)$, we have

$$1, \lambda, \theta \textit{ are distinct irreducible characters of } Q. \tag{6.6}$$

From (6.3), (6.4) and (6.5), we compute:

$$1+\lambda-\theta=\begin{cases}0 & \text{on } Q\backslash\langle\tau\rangle,\\ 2 & \text{on } \langle\tau\rangle\backslash\langle\tau^2\rangle,\\ 4 & \text{on } \langle\tau^2\rangle\backslash\langle\tau^4\rangle,\\ 0 & \text{on } \langle\tau^4\rangle.\end{cases} \tag{6.7}$$

With this we are ready to prove

THEOREM 6.8 (Brauer–Suzuki). *If $n \geq 3$ and the above generalized quaternion group Q of order 2^{n+1} is a 2-Sylow subgroup of a finite group G, then G has a proper normal subgroup N containing the involution ι.*

Proof. Let $\sigma = \tau^2$. Proposition 5.12 tells us that $\sqrt{\sigma}$ is a t.i. set with $H = N_G(\langle\tau\rangle)$ as its normalizer. We first prove

LEMMA 6.9. *The group H is the semi-direct product QK of Q with a normal subgroup K of odd order centralizing σ.*

Proof. Evidently the characteristic subgroup $\langle\sigma\rangle$ of $\langle\tau\rangle$ is itself normal in Q. So $Q \leq H$. Since Q is a 2-Sylow subgroup of G, it must also be one of H.

Because $n \geq 3$, the element σ of order 2^{n-1} is not its own inverse. It follows from this and Proposition 6.2 that $Q \cap C_G(\sigma) = \langle\tau\rangle$. Since $C_G(\sigma)$ is normal in $N_G(\langle\sigma\rangle) = H$, this intersection is a 2-Sylow subgroup of $C_G(\sigma)$. It is well known and elementary (see Section I.6 of Huppert, 1967) that the finite group $C_G(\sigma)$ with a cyclic 2-Sylow group $\langle\tau\rangle$ has a unique normal 2-complement K, i.e., a normal subgroup K of odd order such that $C_G(\sigma) = \langle\tau\rangle K$.

The factor group $H/C_G(\sigma) = N_G(\langle\sigma\rangle)/C_G(\sigma)$ is isomorphic to a subgroup of the automorphism group of $\langle\sigma\rangle$, and hence is a 2-group. It follows that $[H : K] = [H : C_G(\sigma)]\,[C_G(\sigma) : K]$ is a power of 2. Since K is characteristic in $C_G(\sigma)$, it is normal in H. Therefore it is a normal 2-complement in H. and the lemma is proved.

Next we must compute the t.i. set $\sqrt{\sigma} \subseteq H$.

LEMMA 6.10. $\sqrt{\sigma} = \langle\tau\rangle K\backslash\langle\tau^4\rangle K$.

Proof. Suppose that $\rho\pi \in \sqrt{\sigma}$, for $\rho \in Q$, $\pi \in K$. Passing to the factor group $H/K = QK/K \simeq Q$, we see that $\sigma \in \langle\rho\rangle$. Since $n \geq 3$, the element σ is not in $\langle\iota\rangle$. So Proposition 5.2 implies that $\rho \in \langle\tau\rangle$. Obviously $\rho \notin \langle\tau^4\rangle$ since $\sigma = \tau^2 \notin \langle\tau^4\rangle$. Hence $\sqrt{\sigma} \subseteq \langle\tau\rangle K\backslash\langle\tau^4\rangle K$.

Suppose that $\rho \in \langle\tau\rangle\backslash\langle\tau^4\rangle$ and $\pi \in K$. Then either $\langle\rho\rangle = \langle\tau^2\rangle = \langle\sigma\rangle$ or $\langle\rho\rangle = \langle\tau\rangle$. In the first case π is an element of odd order commuting with

the element ρ of order 2^{n-1}, by Lemma 6.9. So $\langle\rho\pi\rangle = \langle\rho\rangle \times \langle\pi\rangle \geq \langle\rho\rangle = \langle\sigma\rangle$. In the second case $(\rho\pi)^2 \in \langle\tau^2\rangle K \backslash \langle\tau^4\rangle K$. So $\sigma \in \langle(\rho\pi)^2\rangle \leq \langle\rho\pi\rangle$, by the first case. Hence $\rho\pi \in \sqrt{\sigma}$ in both cases, which completes the proof of the lemma.

Let ϕ be the natural epimorphism of $H = QK$ onto Q. Then (6.6) implies that the compositions $1_\circ\phi$, $\lambda_\circ\phi$, $\theta_\circ\phi$ are distinct irreducible characters of H. From (6.7) and Lemma 6.10 we see that $1_\circ\phi + \lambda_\circ\phi - \theta_\circ\phi = (1+\lambda-\theta)_\circ\phi$ is a generalized character of H vanishing outside $\sqrt{\sigma}$, i.e. a member of $X(H|\sqrt{\sigma})$. Since $\sqrt{\sigma}$ is a t.i. set with H as its normalizer, we can apply (5.19) and deduce that $(1_\circ\phi + \lambda_\circ\phi - \theta_\circ\phi)^G \in X(G|(\sqrt{\sigma})^G)$. In view of (5.17) and Proposition 5.9 we have

$$(1_\circ\phi + \lambda_\circ\phi - \theta_\circ\phi)^G = 1 + n_2\chi_2 + \ldots + n_k\chi_k,$$

where 1 is the trivial character, and $\chi_2, \ldots, \chi_k$ are the other irreducible characters of G, and where $n_2, \ldots, n_k$ are arbitrary integers. Using (4.20) and (5.16), we get

$$\begin{aligned} 1^2 + n_2^2 + \ldots + n_k^2 &= ((1_\circ\phi + \lambda_\circ\phi - \theta_\circ\phi)^G, \quad (1_\circ\phi + \lambda_\circ\phi - \theta_\circ\phi)^G)_G \\ &= (1_\circ\phi + \lambda_\circ\phi - \theta_\circ\phi, \quad 1_\circ\phi + \lambda_\circ\phi - \theta_\circ\phi)_H \\ &= 3. \end{aligned}$$

Hence exactly two of the n_i are non-zero, and they are both ± 1. Therefore, we have

There exist distinct non-trivial irreducible characters Λ, Θ *of* G *and integers* $\varepsilon_1, \varepsilon_2 = 1$ *such that*: $(1_\circ\phi + \lambda_\circ\phi - \theta_\circ\phi)^G = 1 + \varepsilon_1\Lambda - \varepsilon_2\Theta$. (6.11)

Since $\langle\iota\rangle \leq \langle\tau^4\rangle$, it follows from Lemma 6.10 and Proposition 6.2 that $\sqrt{\sigma}$ contains no involution. Hence $(\sqrt{\sigma})^G$ contains neither ι nor 1_G. Since $(1_\circ\phi + \lambda_\circ\phi - \theta_\circ\phi)^G$ is zero outside $(\sqrt{\sigma})^G$, this and (6.11) imply that

$$1 + \varepsilon_1\Lambda(1) - \varepsilon_2\Theta(1) = 0, \qquad 1 + \varepsilon_1\Lambda(\iota) - \varepsilon_2\Theta(\iota) = 0. \tag{6.12}$$

Let I be the conjugacy class of ι in G. From Proposition 6.2 and Lemma 6.9, the intersection $I \cap H$ is contained in ιK. So $(I \cap H)^2 \subseteq (\iota K)^2 = K$. It follows from this and Lemma 6.10 that $(I \cap H)^2 \cap \sqrt{\sigma}$ is empty. Since $1_\circ\phi + \lambda_\circ\phi - \theta_\circ\phi$ is zero on $H \backslash \sqrt{\sigma}$, we conclude that (in the notation of Proposition 5.23)

$$(1_\circ\phi + \lambda_\circ\phi - \theta_\circ\lambda)(\widetilde{(I \cap H)^2}) = 0.$$

Applying (5.24) and (6.11), we get

$$\begin{aligned} 0 &= [G : H](1_\circ\phi + \lambda_\circ\phi - \theta_\circ\phi)(\widetilde{(I \cap H)^2}) \\ &= (1 + \varepsilon_1\Lambda - \varepsilon_2\Theta)(\tilde{I}^2). \end{aligned}$$

In view of (4.31) and Proposition 2.2, this gives

$$0 = \frac{1(\tilde{I})^2}{1} + \varepsilon_1 \frac{\Lambda(\tilde{I})^2}{\Lambda(1)} - \varepsilon_2 \frac{\Theta(\tilde{I})^2}{\Theta(1)}$$
$$= |I|^2 \left(1 + \frac{(\varepsilon_1 \Lambda(\iota))^2}{\varepsilon_1 \Lambda(1)} - \frac{(\varepsilon_2 \Theta(\iota))^2}{\varepsilon_2 \Theta(1)}\right).$$

We can remove the non-zero factor $|I|^2$. Substituting the values of $\varepsilon_2\Theta(\iota)$, $\varepsilon_2\Theta(1)$ obtained from (6.12), we have:

$$0 = 1 + \frac{(\varepsilon_1 \Lambda(\iota))^2}{\varepsilon_1 \Lambda(1)} - \frac{(1+\varepsilon_1 \Lambda(\iota))^2}{1+\varepsilon_1 \Lambda(1)}$$
$$= \frac{(\varepsilon_1 \Lambda(\iota) - \varepsilon_1 \Lambda(1))^2}{\varepsilon_1 \Lambda(1)(1+\varepsilon_1 \Lambda(1))}.$$

Therefore $\Lambda(\iota) = \Lambda(1)$. By Proposition 4.38, the involution ι lies in $N = \mathrm{Ker}\,(\Lambda)$, which is a proper normal subgroup of G, since $\Lambda \neq 1$. This proves the theorem.

7. Brauer's Characterization of Generalized Characters

As usual, let G be a finite group and F be a field of characteristic zero satisfying (4.1). A subgroup E of G is called *Brauer elementary* if it is the direct product of a cyclic group and a p-group, for some prime p. The following theorem, due to Brauer (but whose present proof is due to Brauer and Tate jointly) is difficult but extremely useful for constructing group characters.

THEOREM 7.1. *A class function ϕ on G is a generalized character if and only if its restriction ϕ_E to each Brauer elementary subgroup E of G is a generalized character of E.*

Proof. The "only if" part is trivial, so we need only prove the "if" part. We shall do it in a series of lemmas. First we pass to a different (but actually equivalent) form of the theorem. Let $\mathscr{E}$ be the family of all Brauer elementary subgroups of G. For each $E \in \mathscr{E}$, induction maps the additive group $X(E)$ of all generalized characters of E onto a subgroup $X(E)^G$ of $X(G)$ (by (5.18)).

LEMMA 7.2. *Theorem* 7.1 *is implied by the equality:*

$$X(G) = \sum_{E \in \mathscr{E}} X(E)^G. \tag{7.3}$$

Proof. Suppose that (7.3) holds. Let ϕ be any class function on G whose restriction ϕ_E lies in $X(E)$, for any $E \in \mathscr{E}$. Then the Frobenius reciprocity law implies that $(\phi, \xi^G)_G = (\phi_E, \xi)_E \in \mathbf{Z}$, for all $\xi \in X(E)$ and any $E \in \mathscr{E}$. It follows that $(\phi, \psi)_G \in \mathbf{Z}$, for any ψ in the right side of (7.3), i.e., for any $\psi \in X(G)$. If $\chi_1, \ldots, \chi_k \in X(G)$ are the irreducible characters of G, we con-

clude from this, (4.26), and (5.17) that $\phi = (\phi, \chi_1)\chi_1 + \ldots + (\phi, \chi_k)\chi_k$ is a generalized character of G. This proves the lemma.

For the rest of this section we regard characters, generalized characters, and class functions as functions from G to F, rather than as linear functions from FG to F, i.e., we adopt the viewpoint of Section 2 instead of that of Section 4. It follows from (2.14) that the additive group $X(G)$ is closed under multiplication of functions, and hence is a ring of functions from G to F. The identity element of this *character ring* $X(G)$ is clearly the trivial character $1 = 1_{G \to F}$ of G.

Let $Y \subseteq X(G)$ denote the right side of (7.3).

LEMMA 7.4. *Y is an ideal in the character ring $X(G)$.*

Proof. Clearly Y is an additive subgroup of $X(G)$. So we need only show that it is closed under multiplication by an arbitrary element $\psi \in X(G)$. Clearly it suffices to show that $\psi\xi^G \in X(E)^G \subseteq Y$, for any $E \in \mathscr{E}$ and any $\xi \in X(E)$.

As in (5.4), let $\hat{\xi}$ be the extension of ξ to a function from G to F which is zero outside E. Then, clearly, we have

$$\psi\hat{\xi} = \widehat{(\psi_E\xi)}$$

Since the restriction ψ_E lies in the ring $X(E)$, so does the product $\psi_E\xi$. Hence $(\psi_E\xi)^G$ lies in $X(E)^G$. Because ψ is a class function on G, it equals ψ^σ, for all $\sigma \in G$. So the above equality and (5.5) imply that

$$\begin{aligned}(\psi_E\xi)^G &= \sum_{\sigma \in \mathrm{rep}(G/E)} \widehat{(\psi_E\xi)}^\sigma = \sum_{\sigma \in \mathrm{rep}(G/E)} (\psi\hat{\xi})^\sigma \\ &= \sum_{\sigma \in \mathrm{rep}(G/E)} \psi^\sigma\hat{\xi}^\sigma = \psi \sum_{\sigma \in \mathrm{rep}(G/E)} \hat{\xi}^\sigma \\ &= \psi\xi^G.\end{aligned}$$

Therefore $\psi\xi^G \in X(E)^G$, which proves the lemma.

The importance of Lemma 7.4 is that any ideal $Y \neq X(G)$ is contained in a maximal ideal of $X(G)$, and that we can say something about these maximal ideals. Before we do so, however, we must make a "ground ring extension".

It follows from (4.1) that F contains a primitive $|\langle\sigma\rangle|$th root of unity (the value $\lambda(\sigma)$ of a suitable linear character λ of $\langle\sigma\rangle$), for each $\sigma \in G$. If e denotes the exponent of G, we conclude that F contains a primitive eth root of unity ω. Let $\mathfrak{O} = \mathbf{Z}[\omega]$ be the subring of F generated by ω.

Lemma 4.34 implies that $\chi(\sigma) \in \mathfrak{O}$, for all $\chi \in X(G)$, $\sigma \in G$. So $X(G)$ is a ring of functions from G to $\mathfrak{O}$. Therefore, so is the family $\mathfrak{O}X(G)$ of all $\mathfrak{O}$-linear combinations of members of $X(G)$:

$$\mathfrak{O}X(G) \text{ is a ring of functions from } G \text{ to } \mathfrak{O}. \tag{7.5}$$

Lemma 7.4 and the F-linearity of induction imply that the corresponding family $\mathfrak{O}Y$ satisfies

$$\mathfrak{O}Y = \sum_{E \in \mathcal{E}} [\mathfrak{O}X(E)]^G \quad \textit{is an ideal of } \mathfrak{O}X(G). \tag{7.6}$$

We must show that nothing is lost by passing from $\mathbf{Z}$ to $\mathfrak{O}$.

LEMMA 7.7. *If we have*

$$\mathfrak{O}Y = \mathfrak{O}X(G), \tag{7.8}$$

then (7.3) *holds.*

Proof. By (4.9) and (5.17) the additive group $X(G)$ is a free $\mathbf{Z}$-module with the irreducible characters $\chi_1, \ldots, \chi_k$ of G as a basis. Since $Y \subseteq X(G)$, the elementary divisor theorem gives us a $\mathbf{Z}$-basis $\phi_1, \ldots, \phi_k$ of $X(G)$ and non-negative integers $n_1, \ldots, n_k$ such that $Y = \mathbf{Z}n_1\phi_1 + \ldots + \mathbf{Z}n_k\phi_k$.

Because the $\mathbf{Z}$-basis $\chi_1, \ldots, \chi_k$ of $X(G)$ is F-linearly independent (by (4.9)), so is the $\mathbf{Z}$-basis $\phi_1, \ldots, \phi_k$. It follows that $\mathfrak{O}X(G) = \mathfrak{O}\phi_1 \oplus \ldots \oplus \mathfrak{O}\phi_k$ is a free $\mathfrak{O}$-module with $\phi_1, \ldots, \phi_k$ as a basis. If (7.8) holds, then $\mathfrak{O}n_1\phi_1 \oplus \ldots \oplus \mathfrak{O}n_k\phi_k = \mathfrak{O}Y = \mathfrak{O}X(G) = \mathfrak{O}\phi_1 \oplus \ldots \oplus \mathfrak{O}\phi_k$. So,

$$\mathfrak{O}n_i = \mathfrak{O}, \quad (i = 1, \ldots, k).$$

Fix $i = 1, \ldots, k$. The above equation implies that the non-negative integer n_i is positive, and that $\mathfrak{O}$ contains $1/n_i$. So $\mathfrak{O}$ contains the subring $\mathbf{Z}[1/n_i]$ of rational numbers generated by $1/n_i$. Since $\mathfrak{O} = \mathbf{Z}[\omega] = \mathbf{Z}\cdot 1 + \mathbf{Z}\omega + \mathbf{Z}\omega^2 + \ldots + \mathbf{Z}\omega^{e-1}$ is a finitely generated $\mathbf{Z}$-module, so is its submodule $\mathbf{Z}[1/n_i]$. This is only possible if $n_i = 1$

From $n_i = 1$ $(i = 1, \ldots, k)$, we get

$$Y = \mathbf{Z}n_1\phi_1 + \ldots + \mathbf{Z}n_k\phi_k = \mathbf{Z}\phi_1 + \ldots + \mathbf{Z}\phi_k = X(G).$$

This proves the lemma.

Each element $\sigma \in G$ defines an "evaluation" homomorphism η_σ of the function ring $\mathfrak{O}X(G)$ into $\mathfrak{O}$ given by

$$\eta_\sigma(\psi) = \psi(\sigma), \quad \textit{for all } \psi \in \mathfrak{O}X(G). \tag{7.9}$$

Since $\eta_\sigma(y\cdot 1) = y1(\sigma) = y$, for all $y \in \mathfrak{O}$, we have

For each $\sigma \in G$, the map η_σ is an epimorphism of the ring

$$\mathfrak{O}X(G) \textit{ onto } \mathfrak{O}. \tag{7.10}$$

Now we fix a maximal ideal M in $\mathfrak{O}X(G)$. We shall construct an element of Y not lying in M. First we must analyze M.

LEMMA 7.11. *There exists an element $\sigma \in G$ and a maximal ideal P of $\mathfrak{O}$ such that M is the inverse image $\eta_\sigma^{-1}(P)$ of P by η_σ.*

Proof. The intersection of the kernels $\operatorname{Ker}(\eta_\sigma)$ of the epimorphisms η_σ, $\sigma \in G$, is the set of all functions $\psi \in X(G)$ which vanish at all $\sigma \in G$, i.e., it is

$\{0\}$. Since there are only a finite number of $\sigma \in G$, and the product

$$\prod_{\sigma \in G} \mathrm{Ker}\,(\eta_\sigma) \subseteq \bigcap_{\sigma \in G} \mathrm{Ker}\,(\eta_\sigma) = \{0\}$$

is contained in the maximal ideal M of the ring $\mathfrak{O}X(G)$ with identity, there is some $\sigma \in G$ such that $\mathrm{Ker}\,(\eta_\sigma) \subseteq M$. Evidently this and (7.10) force M to be the inverse image $\eta_\sigma^{-1}(P)$ of a maximal ideal P of $\mathfrak{O}$. So the lemma is true.

We fix σ and P satisfying the conditions of Lemma 7.11. Since P is a maximal ideal of $\mathfrak{O}$, the quotient ring $\mathfrak{O}/P$ is a field.

LEMMA 7.12. *The field $\mathfrak{O}/P$ has prime characteristic p.*

Proof. Suppose not. Then it has characteristic zero. But its additive group is a finitely-generalized **Z**-module, since $\mathfrak{O}$ is. This is impossible, since it contains the additive group of the rationals, which is not finitely-generated. So the lemma holds.

We write the exponent e as a product $e = p^n f$, where $n \geq 0$ and p does not divide the positive integer f. Then there exist integers a, b such that:

$$ap^n + bf = 1. \tag{7.13}$$

It follows that $\sigma = \sigma^{ap^n}\sigma^{bf}$, where the order of σ^{ap^n} divides f and that of σ^{bf} is a power of p.

LEMMA 7.14. $\psi(\sigma) \equiv \psi(\sigma^{ap^n}) \pmod{P}$, *for all* $\psi \in \mathfrak{O}X(G)$.

Proof. Since both sides of this congruence are $\mathfrak{O}$-linear in ψ, it suffices to prove it when ψ is an irreducible character of G. Let I be a corresponding irreducible FG-module. By Lemma 4.34 there are a basis $y_1, \ldots, y_t$ for I over F and eth roots of unity $\zeta_1, \ldots, \zeta_t$ such that $y_i\sigma = \zeta_i y_i$, for all $i = 1, \ldots, t$. This implies that $y_i\sigma^{ap^n} = \zeta_t^{ap^n} y_i$ $(i = 1, \ldots, t)$. Hence,

$$\begin{aligned}\psi(\sigma) - \psi(\sigma^{ap^n}) &= (\zeta_1 + \ldots + \zeta_t) - (\zeta_1^{ap^n} + \ldots + \zeta_t^{ap^n}) \\ &= \zeta_1^{ap^n}(\zeta_1^{bf} - 1) + \ldots + \zeta_t^{ap^n}(\zeta_t^{bf} - 1)\end{aligned}$$

by (7.13). So it suffices to prove that $\zeta_i^{bf} - 1 \in P$, $(i = 1, \ldots, t)$.

Since ζ_i is an eth root of unity, its power $\delta = \zeta_i^{bf}$ is a p^n-th root of unity. The image $\bar{\delta}$ of δ in $\mathfrak{O}/P$ is also a p^n-th root of unity. But 1 is the only p^n-th root of unity in the field $\mathfrak{O}/P$ of characteristic p. Hence $\bar{\delta} = 1$, and $\zeta_i^{bf} - 1 = \delta - 1 \in P$, which finishes the proof of the lemma.

COROLLARY 7.15. *We can assume that the order of σ is relatively prime to p.*

Proof. If not, let $\tau = \sigma^{ap^n}$. The lemma implies that $M = \eta_\sigma^{-1}(P) = \eta_\tau^{-1}(P)$. So we can replace σ by τ, whose order divides f and hence is relatively prime to p.

Of course, from now on we do assume that $|\langle\sigma\rangle|$ is relatively prime to p. Let S be a p-Sylow subgroup of $C_G(\sigma)$. Then $E = \langle\sigma\rangle \times S$ is a Brauer

elementary subgroup of G. Since $\langle\sigma\rangle$ is abelian, each of its irreducible characters λ is linear. Using the projection of E on $\langle\sigma\rangle$ (or (2.12)), we obtain a corresponding linear character $\lambda\times 1$ of E satisfying

$$\lambda\times 1(\rho\tau)=\lambda(\rho),\quad \textit{for all } \rho\in\langle\sigma\rangle,\ \tau\in S.$$

Let $\lambda_1,\ldots,\lambda_l$ ($l=|\langle\sigma\rangle|$) be the irreducible characters of $\langle\sigma\rangle$. Then

$$\Lambda=\sum_{i=1}^{l}\lambda_i(\sigma^{-1})(\lambda_i\times 1)\in\mathfrak{D}X(E).$$

Using (4.33) we compute:

$$\Lambda(\rho\tau)=\begin{cases}0, & \text{if } \rho\neq\sigma,\\ |\langle\sigma\rangle|, & \text{if } \rho=\sigma,\end{cases}\quad(\rho\in\langle\sigma\rangle,\ \tau\in S).\tag{7.16}$$

By (7.6) the induced character Λ^G lies in $\mathfrak{D}Y$. It satisfies

LEMMA 7.17. $\Lambda^G(\sigma)=[C_G(\sigma):S]\not\equiv 0\pmod P$.

Proof. As in (5.4), we extend Λ to a function $\hat{\Lambda}$ from G to F which is zero outside E.

Suppose that $\hat{\Lambda}^\tau(\sigma)\neq 0$, for some $\tau\in G$. Then $\sigma^{\tau^{-1}}\in E$ and $\Lambda(\sigma^{\tau^{-1}})\neq 0$. The order of $\sigma^{\tau^{-1}}$ equals that of σ. Evidently $\langle\sigma\rangle$ is the set of all elements of $E=\langle\sigma\rangle\times S$ whose orders are not divisible by p. Hence $\sigma^{\tau^{-1}}\in\langle\sigma\rangle$. But then $\Lambda(\sigma^{\tau^{-1}})\neq 0$ implies $\sigma^{\tau^{-1}}=\sigma$, by (7.16). Therefore $\tau\in C_G(\sigma)$.

On the other hand, if $\tau\in C_G(\sigma)$, then (7.16) gives $\hat{\Lambda}^\tau(\sigma)=\hat{\Lambda}(\sigma^{\tau^{-1}})=\Lambda(\sigma)=|\langle\sigma\rangle|\neq 0$. It follows from this and (5.5) that

$$\Lambda^G(\sigma)=\sum_{\tau\in\operatorname{rep}(G/E)}\hat{\Lambda}^\tau(\sigma)=\sum_{\tau\in\operatorname{rep}(C_G(\sigma)/E)}|\langle\sigma\rangle|=[C_G(\sigma):\langle\sigma\rangle\times S]|\langle\sigma\rangle|$$
$$=[C_G(\sigma):S].$$

This is not divisible by p, since S is a p-Sylow subgroup of $C_G(\sigma)$. So it does not lie in P by Lemma 7.12. This completes the proof of the lemma.

Now we can finish the proof of the theorem. By Lemmas 7.2 and 7.7, we need only show that (7.8) holds. If that is false then $\mathfrak{D}Y$ is an ideal properly contained in $\mathfrak{D}X(G)$, by (7.6). So we can choose our maximal ideal M to contain $\mathfrak{D}Y$. But the above character Λ^G lies in $\mathfrak{D}Y$ and not in $M=\eta_\sigma^{-1}(P)$, by (7.9) and Lemmas 7.11 and 7.17. The contradiction proves the theorem.

8. *p*-adic Algebras

Fix a prime p in the ring $\mathbf{Z}$ of ordinary integers. From the descending chain $p\mathbf{Z}\supset p^2\mathbf{Z}\supset p^3\mathbf{Z}\supset\ldots$ of ideals of $\mathbf{Z}$ we obtain an infinite chain of natural ring epimorphisms

$$\ldots\to\mathbf{Z}/p^3\mathbf{Z}\to\mathbf{Z}/p^2\mathbf{Z}\to\mathbf{Z}/p\mathbf{Z}.\tag{8.1}$$

The corresponding inverse limit ring $\mathbf{Z}_p=\varprojlim_{n\to\infty}\mathbf{Z}/p^n\mathbf{Z}$ is called the *ring of p-adic integers.*

From its definition $\mathbf{Z}_p$ is provided with a family of natural ring epimorphisms $\mathbf{Z}_p \to \mathbf{Z}/p^n\mathbf{Z}$, for all $n > 0$, commuting with the epimorphisms in (8.1). If $m > n$, then the kernel of the epimorphism $\mathbf{Z}/p^m\mathbf{Z} \to \mathbf{Z}/p^n\mathbf{Z}$ in (8.1) is $p^n\mathbf{Z}/p^m\mathbf{Z}$, which is $p^n(\mathbf{Z}/p^m\mathbf{Z})$ as an additive subgroup of $\mathbf{Z}/p^m\mathbf{Z}$. It follows that the kernel of $\mathbf{Z}_p \to \mathbf{Z}/p^n\mathbf{Z}$ is $p^n\mathbf{Z}_p = \varprojlim_{m\to\infty} p^n(\mathbf{Z}/p^m\mathbf{Z})$. So we have a natural identification of rings:

$$\mathbf{Z}_p/p^n\mathbf{Z}_p = \mathbf{Z}/p^n\mathbf{Z}, \quad \textit{for all } n > 0. \tag{8.2}$$

Under this identification, the chain (8.1) becomes the corresponding chain for $\mathbf{Z}_p$:

$$\ldots \to \mathbf{Z}_p/p^3\mathbf{Z}_p \to \mathbf{Z}_p/p^2\mathbf{Z}_p \to \mathbf{Z}_p/p\mathbf{Z}_p.$$

We conclude that the natural homomorphism of $\mathbf{Z}_p$ into $\varprojlim_{n\to\infty} \mathbf{Z}_p/p^n\mathbf{Z}_p$ is an identity of rings:

$$\mathbf{Z}_p = \varprojlim_{n\to\infty} \mathbf{Z}_p/p^n\mathbf{Z}_p. \tag{8.3}$$

The rings $\mathbf{Z}/p^n\mathbf{Z}$ have identities $1_{\mathbf{Z}/p^n\mathbf{Z}}$ which map onto each other in (8.1). It follows that their inverse $1_{\mathbf{Z}_p} = \varprojlim_{n\to\infty} 1_{\mathbf{Z}/p^n\mathbf{Z}}$ is the identity for $\mathbf{Z}_p$. The unit group $U(\mathbf{Z}_p)$ is easily seen to be the inverse limit

$$U(\mathbf{Z}_p) = \varprojlim_{n\to\infty} U(\mathbf{Z}/p^n\mathbf{Z}),$$

of the unit groups $U(\mathbf{Z}/p^n\mathbf{Z})$ of the rings $\mathbf{Z}/p^n\mathbf{Z}$. But $U(\mathbf{Z}/p^n\mathbf{Z}) = (\mathbf{Z}/p^n\mathbf{Z})\backslash(p\mathbf{Z}/p^n\mathbf{Z})$, for all $n > 0$. Hence, we have

$$U(\mathbf{Z}_p) = \varprojlim_{n\to\infty} ((\mathbf{Z}/p^n\mathbf{Z})\backslash p(\mathbf{Z}/p^n\mathbf{Z})) = \mathbf{Z}_p\backslash p\mathbf{Z}_p. \tag{8.4}$$

From the above information we can deduce the entire ideal structure of $\mathbf{Z}_p$.

PROPOSITION 8.5. *The distinct ideals of* $\mathbf{Z}_p$ *are* $\{0\}$ *and* $p^n\mathbf{Z}_p$ ($n = 0, 1, 2, 3, \ldots$).

Proof. By (8.2) we have $\mathbf{Z}_p = p^0\mathbf{Z}_p \supset p\mathbf{Z}_p \supset p^2\mathbf{Z}_p \supset \ldots$. So the ideals $p^n\mathbf{Z}_p$ ($n = 0, 1, 2, \ldots$), are distinct from each other and from $\{0\}$.

Let I be any non-zero ideal of $\mathbf{Z}_p$. By (8.3) the intersection $\bigcap_{n=0}^{\infty} p^n\mathbf{Z}_p = \{0\}$. So I is not contained in every ideal $p^n\mathbf{Z}_p$. On the other hand, $I \subseteq p^0\mathbf{Z}_p = \mathbf{Z}_p$. Hence there exists an integer $n \geq 0$ such that $I \subseteq p^n\mathbf{Z}_p$ but $I \nsubseteq p^{n+1}\mathbf{Z}_p$. Let y be any element of I not in $p^{n+1}\mathbf{Z}_p$. Since $y \in p^n\mathbf{Z}_p$, there is an element $\mu \in \mathbf{Z}_p$ such that $y = p^n\mu$. Since $y \notin p^{n+1}\mathbf{Z}_p$, the element μ does not lie in $p\mathbf{Z}_p$. By (8.4) μ is a unit of $\mathbf{Z}_p$. Therefore $I \supseteq y\mathbf{Z}_p = p^n\mu\mathbf{Z}_p = p^n\mathbf{Z}_p$. So $I = p^n\mathbf{Z}_p$, and the proposition is proved.

COROLLARY 8.6. *The ring* $\mathbf{Z}_p$ *is a principal ideal domain of characteristic zero, and* $p\mathbf{Z}_p$ *is its only maximal ideal.*

Proof. By the proposition, $\mathbf{Z}_p$ is a commutative ring with identity in which every ideal is principal. The product $p^n\mathbf{Z}_p p^m\mathbf{Z}_p = p^{n+m}\mathbf{Z}_p$ of any two non-zero ideals $p^n\mathbf{Z}_p$, $p^m\mathbf{Z}_p$ of $\mathbf{Z}_p$ is again non-zero. It follows that the product of any two non-zero elements of $\mathbf{Z}_p$ is non-zero. So $\mathbf{Z}_p$ is a principal ideal domain.

The characteristic of the domain $\mathbf{Z}_p$ is either zero or a prime. But $\mathbf{Z}_p$ has a quotient ring $\mathbf{Z}_p/p^2\mathbf{Z}_p$ of characteristic p^2, by (8.2). So its characteristic cannot be a prime. Hence it is zero.

The final conclusion of the corollary, that $p\mathbf{Z}_p$ is the only maximal ideal of $\mathbf{Z}_p$, comes directly from the proposition.

We should note that the field of fractions Q_p of the integral domain $\mathbf{Z}_p$ is called the *p-adic number field.*

A *p-adic module* M will be a finitely-generated unitary module over $\mathbf{Z}_p$. Since $\mathbf{Z}_p$ is a principal ideal domain, we can apply the structure theory of finitely-generated modules over such domains (see Section I.13 of Huppert, 1967). In view of Proposition 8.5, we obtain

$$M \simeq \overbrace{\mathbf{Z}_p \oplus \ldots \oplus \mathbf{Z}_p}^{r \text{ terms}} \oplus (\mathbf{Z}_p/p^{n_1}\mathbf{Z}_p) \oplus \ldots \oplus (\mathbf{Z}_p/p^{n_s}\mathbf{Z}_p) \quad (\text{as } \mathbf{Z}_p\text{-modules}), \tag{8.7}$$

for some unique integers $r, s \geq 0$ and $n_1, \ldots, n_s \geq 1$. This has two important consequences.

In the first place, the factor module M/pM is clearly the direct sum of $r+s$ copies of $\mathbf{Z}_p/p\mathbf{Z}_p$, which is isomorphic to $\mathbf{Z}/p\mathbf{Z}$ by (8.2). Regarding M/pM as a vector space over the field $\mathbf{Z}/p\mathbf{Z}$, we obtain

$$\dim_{\mathbf{Z}/p\mathbf{Z}} (M/pM) = r+s, \textit{ for all p-adic modules } M. \textit{ Furthermore, this dimension is zero if and only if } M = \{0\}. \tag{8.8}$$

The second immediate consequence of (8.7) and (8.3) is that

$$M = \varprojlim_{n\to\infty} M/p^nM, \quad \textit{for all p-adic modules } M, \tag{8.9}$$

in the usual sense that the natural map of the left side into the right is a module isomorphism.

By a *p-adic algebra* we understand a p-adic module A together with a $\mathbf{Z}_p$-bilinear, associative product $(a, a') \to aa'$ from $A \times A$ to A. Unless otherwise noted we assume that A has an identity $1 = 1_A$ for this multiplication. So A is a ring with identity, and $z \to z1_A$ is an identity-preserving ring homomorphism of $\mathbf{Z}_p$ into the center of A.

Obviously the additive subgroup pA is a two-sided ideal of A. By (8.8) the factor ring A/pA is finite-dimensional over $\mathbf{Z}/p\mathbf{Z}$. Hence, we have

$$A/pA \quad \textit{is an algebra over } \mathbf{Z}/p\mathbf{Z}. \tag{8.10}$$

We define the *radical* $J(A)$ to be the inverse image in A of the radical $J(A/pA)$

of the algebra A/pA. (In fact, one can easily see that $J(A)$ is the Jacobson radical of A). Then $J(A)$ is a two-sided ideal of A containing pA and, by (3.8)

$$A/J(A) \simeq [A/pA]/J(A/pA) \text{ is a semi-simple algebra over } \mathbf{Z}/p\mathbf{Z}. \tag{8.11}$$

By Satz V.2.4 of Huppert (1967), the radical $J(A/pA)$ is a nilpotent ideal in the algebra A/pA. It follows that

$$J(A)^d \subseteq pA \subseteq J(A), \quad \text{for some integer } d > 0. \tag{8.12}$$

This implies that $J(A)^{dn} \subseteq (pA)^n = p^nA \subseteq J(A)^n$, for all integers $n \geq 0$. Hence we have natural ring epimorphisms

$$\varprojlim_{n\to\infty} A/J(A)^{dn} \to \varprojlim_{n\to\infty} A/p^nA \to \varprojlim_{n\to\infty} A/J(A)^n.$$

But the natural epimorphism of the left ring onto the right is clearly an isomorphism. So they are both isomorphic to the center ring. From this and (8.9) we conclude that

$$A = \varprojlim_{n\to\infty} A/p^nA = \varprojlim_{n\to\infty} A/J(A)^n \tag{8.13}$$

in the usual sense that the natural maps among these objects are isomorphisms.

9. The Krull–Schmidt Theorem

Let M be a module over a ring R. Consider a decomposition

$$M = M_1 \oplus \ldots \oplus M_m, \tag{9.1}$$

where $M_1, \ldots, M_m$ are R-submodules of M. The corresponding projections $e_i : M \to M_i$ $(i = 1, \ldots, m)$ all lie in the ring $\mathrm{Hom}_R(M, M)$ of R-endomorphisms of M, and satisfy

$$e_i^2 = e_i \quad (i = 1, \ldots, m), \tag{9.2a}$$

$$e_ie_j = 0 \quad (i, j = 1, \ldots, m \quad \text{with } i \neq j), \tag{9.2b}$$

$$1 = e_1 + \ldots + e_m. \tag{9.2c}$$

Furthermore, these projections determine (9.1) since $M_i = Me_i$, for $i = 1, \ldots, m$. (Notice that we regard the R-endomorphisms as right operators on M.)

On the other hand, if $e_1, \ldots, e_m$ are elements of $\mathrm{Hom}_R(M, M)$ satisfying (9.2), then one easily verifies that $M_1 = Me_1, \ldots, M_m = Me_m$ are R-submodules of M satisfying (9.1), and that e_i is the corresponding projection of M onto M_i $(i = 1, \ldots, m)$. So there is a natural one to one correspondence between decompositions (9.1) of the R-module M and decompositions (9.2c) of the identity into elements $e_1, \ldots, e_m$ of the ring $\mathrm{Hom}_R(M, M)$ satisfying (9.2a, b).

The R-module M is *indecomposable* if it is non-zero and cannot be written as the direct sum of two proper R-submodules. The former condition is equivalent to $1 \neq 0$ in the ring $\mathrm{Hom}_R(M, M)$. The latter says that there is

no decomposition $1 = e_1 + e_2$ in the ring $\mathrm{Hom}_R(M, M)$ satisfying (9.2a, b) for $m = 2$. Since any idempotent $e \neq 0, 1$ in $\mathrm{Hom}_R(M, M)$ gives such a decomposition $1 = e + (1-e)$, we see that

M is indecomposable if and only if 1 is the unique non-zero idempotent in $\mathrm{Hom}_R(M, M)$. (9.3)

In the case when R is a p-adic algebra A (with identity), we can give another condition for the indecomposability of certain A-modules. By a *module M over the p-adic algebra A* we understand a finitely-generated unitary right A-module. Since A is itself a finitely-generated unitary module over $\mathbf{Z}_p$, so is M. Hence M is a p-adic module in the sense of Section 8.

PROPOSITION 9.4. *For any module M (in the above sense) over the p-adic algebra A, the ring* $\mathrm{Hom}_A(M, M)$ *is naturally a p-adic algebra.*

Proof. Since all multiplications involving A or M are $\mathbf{Z}_p$-bilinear, the ring $\mathrm{Hom}_A(M, M)$ is naturally a unitary $\mathbf{Z}_p$-module, and its multiplication is $\mathbf{Z}_p$-bilinear. So the only problem is to show that $\mathrm{Hom}_A(M, M)$ is a finitely-generated $\mathbf{Z}_p$-module. But it is a $\mathbf{Z}_p$-submodule of $\mathrm{Hom}_{\mathbf{Z}_p}(M, M)$, which is a finitely-generated $\mathbf{Z}_p$-module since M is and since $\mathbf{Z}_p$ is a principal ideal domain. It follows that $\mathrm{Hom}_A(M, M)$ is finitely-generated over $\mathbf{Z}_p$, which proves the proposition.

In view of (9.3) and the above proposition, we must study the p-adic algebras for which 1 is the unique non-zero idempotent. To do so, we use

LEMMA 9.5 (Idempotent refinement lemma). *Let A be a p-adic algebra and f be an idempotent in $A/J(A)$. Then there exists an idempotent e in A such that $f = e + J(A)$.*

Proof. By (8.13) the ring A is the inverse limit of the family of rings and epimorphisms

$$\ldots \to A/J(A)^3 \to A/J(A)^2 \to A/J(A).$$

We shall construct, by induction, idempotents $e_n \in A/J(A)^n$, for $n \geq 1$, satisfying:

$$\ldots \to e_3 \to e_2 \to e_1 = f.$$

Evidently $e = \varprojlim e_n$ will be the desired idempotent of A.

We start with $e_1 = f$. Suppose that idempotents $e_1 \in A/J(A)$, $e_2 \in A/J(A)^2$, $\ldots$, $e_n \in A/J(A)^n$ have been constructed so that $e_n \to e_{n-1} \to \ldots \to e_1 = f$. Let g be any element of $A/J(A)^{n+1}$ having e_n as image in $A/J(A)^n$. From $e_n^2 = e_n$ we obtain

$$g^2 = g + y,$$

where y lies in the kernel $Y = J(A)^n/J(A)^{n+1}$ of $A/J(A)^{n+1} \to A/J(A)^n$.

Evidently $y = g^2 - g$ commutes with g. Furthermore $y^2 \in Y^2 = \{0\}$ (since $n \geq 1$). It follows that $e_{n+1} = g + (1-2g)y$ satisfies

$$\begin{aligned} e_{n+1}^2 &= g^2 + 2g(1-2g)y + (1-2g)^2 y^2 \\ &= g + y + (2g - 4g^2)y + 0 \\ &= g + (1-2g)y + (4g - 4g^2)y \\ &= e_{n+1} - 4y^2 = e_{n+1}. \end{aligned}$$

Since $e_{n+1} \equiv g \pmod{Y}$, we have found an idempotent $e_{n+1} \in A/J(A)^{n+1}$ satisfying $e_{n+1} \to e_n$. This completes the inductive construction of the e_n and finishes the proof of the lemma.

It is convenient to know the structure of the unit group of A.

LEMMA 9.6. *Let A be a p-adic algebra. An element u is a unit in A if and only if its image $u + J(A)$ is a unit in $A/J(A)$.*

Proof. If u is a unit in A, then $u + J(A)$ is clearly a unit in $A/J(A)$. Suppose, conversely, that $u + J(A)$ is a unit in $A/J(A)$. Then there exists an element $v \in A$ such that $uv \equiv vu \equiv 1 \pmod{J(A)}$. Let $y = 1 - uv \in J(A)$. Then $y^n \in J(A)^n$, for all $n \geq 1$. It follows from (8.13) that the sum $1 + y + y^2 + y^3 + \ldots$ "converges" in $\varprojlim A/J(A)^n = A$ to a two-sided inverse to $1 - y = uv$. Therefore u has the right inverse $v(1-y)^{-1}$. Similarly u has a left inverse. So u is a unit in A and the lemma holds.

As a result of these lemmas, we have:

PROPOSITION 9.7. *The following properties are equivalent for a p-adic algebra A:*

(a) *1 is the unique non-zero idempotent in A,*
(b) *1 is the unique non-zero idempotent in $A/J(A)$,*
(c) *$A/J(A)$ is a division algebra over $\mathbf{Z}/p\mathbf{Z}$,*
(d) *$A \backslash J(A)$ is the unit group of A.*

Proof. (a) $\Leftrightarrow$ (b). First notice that 0 is the only idempotent in $J(A)$. Indeed, any such idempotent e satisfies $e = e^n \in J(A)^n$, for all $n \geq 1$, and hence $e \in \bigcap_{n \geq 1} J(A)^n = \{0\}$ by (8.13).

Now suppose that (a) holds. Since $1 \neq 0$ in A, the idempotent 1 does not lie in $J(A)$. Hence its image 1 is $\neq 0$ in $A/J(A)$. If f is an idempotent of $A/J(A)$ different from 0 and 1, then Lemma 9.5 gives us an idempotent $e \in A$ having f as its image in $A/J(A)$. Clearly $e \neq 0, 1$ in A, which is impossible by (a). Therefore (a) implies (b).

Suppose that (b) holds. Then $1 \neq 0$ in $A/J(A)$, which implies $1 \neq 0$ in A. If e is an idempotent of A other than 1 or 0, then so is $1 - e$ (since $(1-e)^2 = 1 - 2e + e^2 = 1 - 2e + e = 1 - e$). Both e and $1 - e$ must have the

image 1 in $A/J(A)$, by (b) and the first paragraph of this proof. That is impossible since their sum 1 also has the image 1 and $1 \neq 0$ in $A/J(A)$. Therefore (b) implies (a).

(b) $\Leftrightarrow$ (c). Suppose that (b) holds. By (8.11), the ring $A/J(A)$ is a semi-simple algebra over $\mathbf{Z}/p\mathbf{Z}$. Proposition 3.9 gives us simple subalgebras $A_1, \ldots, A_k$ such that $A/J(A) = A_1 \oplus \ldots \oplus A_k$. If $k > 1$, then 1_{A_1} is an idempotent of A different from 0 and 1, contradicting (b). If $k = 0$, then $1 = 0$ in $A/J(A)$, also contradicting (b). So $k = 1$ and $A/J(A)$ is a simple algebra over $\mathbf{Z}/p\mathbf{Z}$.

Now Proposition 3.12 tells us that $A/J(A) \simeq \mathrm{Hom}_D(I, I)$, where D is a division algebra over $\mathbf{Z}/p\mathbf{Z}$ and I is a finite-dimensional vector space over D. Applying (9.3) with D, I in place of R, M, we see from (b) that I is an indecomposable D-module. So $I \simeq D$ is one-dimensional over D. It follows easily that $A/J(A) \simeq \mathrm{Hom}_D(D, D)$ is a division algebra anti-isomorphic to D. So (b) implies (c).

Suppose that (c) holds. Then $1 \neq 0$ in $A/J(A)$. If f is an idempotent in $A/J(A)$ different from 1 and 0, then $f \neq 0$, $1-f \neq 0$, and $f(1-f) = f-f^2 = f-f = 0$, which is impossible in a division algebra. Hence (c) implies (b).

(c) $\Leftrightarrow$ (d). Evidently (c) holds if and only if $[A/J(A)]\backslash\{0\}$ is the unit group of $A/J(A)$. By Lemma 9.6 this is equivalent to (d). So the proposition is proved.

COROLLARY 9.8 (Fitting's Lemma). *The following conditions are equivalent for a module M over a p-adic algebra A:*

(a) *M is indecomposable,*

(b) *$\mathrm{Hom}_A(M, M)/J(\mathrm{Hom}_A(M, M))$ is a division algebra over $\mathbf{Z}/p\mathbf{Z}$,*

(c) *$\mathrm{Hom}_A(M, M)\backslash J(\mathrm{Hom}_A(M, M))$ is the group of A-automorphisms of M.*

Proof. In view of Proposition 9.4, this follows directly from the above proposition and (9.3).

Since any module over a p-adic algebra is, in particular, a p-adic module, it satisfies (8.8). This implies immediately that

A module M over a p-adic algebra A has at least one decomposition $M = M_1 \oplus \ldots \oplus M_m$, where $m \geq 0$ and each M_i is an indecomposable A-submodule of M. (9.9)

The point of the Krull–Schmidt theorem is that this decomposition is as unique as it can be.

THEOREM 9.10 (Krull–Schmidt Theorem). *Let M be a module over a p-adic algebra A. Suppose that $M = M_1 \oplus \ldots \oplus M_m = N_1 \oplus \ldots \oplus N_n$, where $m, n \geq 0$ and each M_i or N_j is an indecomposable A-submodule of M. Then $n = m$ and, after renumbering, $M_i \simeq N_i$ (as A-modules), for $i = 1, \ldots, m$.*

Proof. We use induction on m. If $m = 0$, then $M = \{0\}$ and the theorem is trivial. So we can assume that $m > 0$, and that the result is true for all smaller values of m. Obviously this implies that $M \neq \{0\}$, and hence that $n > 0$.

The decomposition $M = M_1 \oplus \ldots \oplus M_m$ defines projections e_i of M onto M_i $(i = 1, \ldots, m)$. Similarly, the decomposition $M = N_1 \oplus \ldots \oplus N_n$ defines projections f_j of M onto N_j $(j = 1, \ldots, n)$. From (9.2c) we obtain

$$f_1 = 1f_1 = e_1f_1 + e_2f_1 + \ldots + e_mf_1.$$

Let $e_{1i} \in \mathrm{Hom}_A(N_1, M_i)$ be the restriction of e_i to N_1, and $f_{i1} \in \mathrm{Hom}_A(M_i, N_1)$ be the restriction of f_1 to M_i $(i = 1, \ldots, m)$. Then $e_{1i}f_{i1} \in \mathrm{Hom}_A(N_1, N_1)$ $(i = 1, \ldots, m)$. Since f_1 is identity on N_1, the above equation implies that

$$1 = e_{11}f_{11} + e_{12}f_{21} + \ldots + e_{1m}f_{m1} \quad \textit{in } \mathrm{Hom}_A(N_1, N_1).$$

Because N_1 is an indecomposable A-module, we may apply Corollary 9.8 to it. It is impossible that every $e_{1i}f_{i1}$ lies in $J(\mathrm{Hom}_A(N_1, N_1))$, $(i = 1, \ldots, m)$, since their sum 1 does not lie in this ideal. After renumbering, we can assume that $e_{11}f_{11} \notin J(\mathrm{Hom}_A(N_1, N_1))$. By Corollary 9.8(c), the product $e_{11}f_{11}$ is an A-automorphism of N_1. Let $(e_{11}f_{11})^{-1}$ be its inverse in $\mathrm{Hom}_A(N_1, N_1)$. Then $e_{11} \in \mathrm{Hom}_A(N_1, M_1)$ and $f_{11}(e_{11}f_{11})^{-1} \in \mathrm{Hom}_A(M_1, N_1)$ satisfy $e_{11}f_{11}(e_{11}f_{11})^{-1} = 1_{N_1 \to N_1}$. It follows that e_{11} is a monomorphism, and that $M_1 = N_1e_{11} \oplus \mathrm{Ker}\,(f_{11}(e_{11}f_{11})^{-1})$ (as A-modules). Since M is indecomposable and $N_1 \neq \{0\}$, we conclude that $\mathrm{Ker}\,(f_{11}(e_{11}f_{11})^{-1}) = \{0\}$, and that e_{11} is an isomorphism of N_1 onto M_1.

We now know that the restriction of e_1 is an isomorphism of N_1 onto M_1. It follows that $M = M_1 \oplus M_2 \oplus \ldots \oplus M_m = N_1 \oplus M_2 \oplus \ldots \oplus M_m$. Therefore $M_2 \oplus \ldots \oplus M_m \simeq M/N_1 \simeq N_2 \oplus \ldots \oplus N_n$, (as A-modules). By induction $m = n$ and, after renumbering, $M_i \simeq N_i$ (as A-modules), for $i = 2, \ldots, m$. Since $M_1 \simeq N_1$ already, this proves the theorem.

Let R be a commutative ring with identity. Then any idempotent $e \in R$ is the identity of the subring $eR = Re$. If $e_1, \ldots, e_m \in R$ satisfy (9.2), then R is the ring direct sum of its subrings $Re_1, \ldots, Re_m$. Conversely, if $R = R_1 \oplus \ldots \oplus R_m$ (as rings), then the identities $e_1, \ldots, e_m$ of $R_1, \ldots, R_m$, respectively, satisfy (9.2) and $R_i = Re_i$ $(i = 1, \ldots, m)$. So our "standard" condition that 1 be the unique non-zero idempotent in R is equivalent to the condition that R be idecomposable as a ring.

We say that an idempotent $e \in R$ is *primitive* if it is the unique non-zero idempotent in the subring eR, i.e., if eR is an indecomposable subring of R. The importance of decompositions (9.2) in which each e_i is primitive is explained by the

PROPOSITION 9.11. *Let $e_1, \ldots, e_m$ be primitive idempotents satisfying* (9.2)

in a commutative ring R. Then the elements $e_S = \sum_{i \in S} e_i$, for $S \subseteq \{1, \ldots, m\}$, are precisely the distinct idempotents in R. In particular, $e_1, \ldots, e_m$ are the only primitive idempotents in R.

Proof. An elementary calculation shows that e_s is an idempotent, for any $S \subseteq \{1, \ldots, m\}$. Since $e_i e_S = e_i$, if $i \in S$, and is zero if $i \notin S$, $(i = 1, \ldots, m)$, the idempotent e_S determines the set S. Therefore distinct subsets S of $\{1, \ldots, m\}$ yield distinct idempotents e_S.

Let f be any idempotent of R. For $i = 1, \ldots, m$, $fe_i = e_i f$ is an idempotent in $e_i R$. Since e_i is primitive, fe_i is either 0 or e_i. Letting S be the set of all $i = 1, \ldots, m$ such that $fe_i = e_i$, we obtain

$$f = f1 = fe_1 + fe_2 + \ldots + fe_m = \sum_{i \in S} e_i = e_S.$$

This proves that the e_S are the only idempotents in R.

Since Re_S contains $e_i e_S = e_i$, for all $i \in S$ and any $S \subseteq \{1, \ldots, m\}$, we see immediately that e_S is primitive if and only if S contains exactly one element. So the proposition is proved.

We shall apply the above result to a commutative p-adic algebra A. In any decomposition $A = A_1 \oplus \ldots \oplus A_m$ (as rings), the subrings A_i are ideals and hence p-adic subalgebras of A. As in the case of (9.9), statement (8.8) implies that A has such a decomposition in which $m \geq 0$ and each A_i is an indecomposable ring. The equivalence between these decompositions and the decompositions (9.2) in A, together with Proposition 9.11, imply that

A commutative p-adic algebra A has a finite number of primitive idempotents $e_1, \ldots, e_m$ $(m \geq 0)$. These idempotents satisfy (9.2) *and the elements $e_S = \sum_{i \in S} e_i$, for $S \subseteq \{1, \ldots, m\}$ are precisely the distinct idempotents in A.* (9.12)

The Idempotent Refinement Lemma 9.5 can be used to give a close connection between idempotents of A and those of $A/J(A)$.

PROPOSITION 9.13. *Let A be a commutative p-adic algebra. The map $e \to e+J(A)$ sends the family of all idempotents e of A one to one onto the family of all idempotents of $A/J(A)$. Furthermore e is primitive in A if and only if $e+J(A)$ is primitive in $A/J(A)$.*

Proof. Evidently $e \to e+J(A)$ sends the first family into the second. By Lemma 9.5 the map is onto. So we must prove it to be one to one.

Suppose that e, f are idempotents of A such that $e \equiv f (\mathrm{mod}\ J(A))$. Then $e \equiv e^2 \equiv ef (\mathrm{mod}\ J(A))$. Hence $e - ef = e(1-f)$ is an idempotent in $J(A)$. As in the first paragraph of the proof of Proposition 9.7, this implies that $e - ef = 0$, or $e = ef$. Similarly, $ef = f$. Therefore $e \to e+J(A)$ is one to one and the first statement of the proposition is proved.

We know that an idempotent e is non-zero in A if and only if $e+J(A)$ is non-zero in $A/J(A)$. If f is an idempotent in eA different from e and 0, then $f+J(A)$ is an idempotent in $(e+J(A))\,(A/J(A))$ different from $e+J(A)$ and 0. Conversely, if $(e+J(A))\,(A/J(A))$ contains an idempotent $g \neq e+J(A)$, 0, then Lemma 9.5 gives us an idempotent f in A such that $g = f+J(A)$. The product ef is an idempotent in eA whose image in $A/J(A)$ is $(e+J(A))g = g$ (since $g \in (e+J(A))\,(A/J(A))$). Hence $ef \neq 0, e$. This proves the second statement and finishes the proof of the proposition.

10. Orders

We fix a prime p. Recall from Section 8 that the p-adic number field Q_p is the field of fractions of the integral domain $\mathbf{Z}_p$ of p-adic integers. Let A be an algebra (in the sense of Section 3) over Q_p. An *order* (or, more strictly, a $\mathbf{Z}_p$-*order*) in A is a subset $\mathfrak{O}$ satisfying:

$$\mathfrak{O} \text{ is a subring of } A, \tag{10.1a}$$

$$1_A \in \mathfrak{O}, \tag{10.1b}$$

$$\mathfrak{O} \text{ is a finitely-generated } \mathbf{Z}_p\text{-submodule of } A. \tag{10.1c}$$

$$\text{For each } a \in A, \text{ there exists } z \neq 0 \text{ in } \mathbf{Z}_p \text{ such that } za \in \mathfrak{O}. \tag{10.1d}$$

Evidently (10.1a, b, c) imply that

$$\mathfrak{O} \text{ is a } p\text{-adic algebra.} \tag{10.2}$$

Since $\mathfrak{O}$ is a $\mathbf{Z}_p$-submodule of the vector space A over Q_p, it is a torsion-free $\mathbf{Z}_p$-module. Because $\mathbf{Z}_p$ is a principal ideal domain, this and (10.1c) imply that $\mathfrak{O}$ is a free $\mathbf{Z}_p$-module of finite rank n. Hence there is a $\mathbf{Z}_p$-basis $a_1, \ldots, a_n$ of $\mathfrak{O}$ such that

$$\mathfrak{O} = \mathbf{Z}_p a_1 \oplus \ldots \oplus \mathbf{Z}_p a_n \cong \overbrace{\mathbf{Z}_p \oplus \ldots \oplus \mathbf{Z}_p}^{n \text{ times}} \quad (\text{as } \mathbf{Z}_p\text{-modules}). \tag{10.3}$$

From (10.1d) it is clear that $a_1, \ldots, a_n$ is also a Q_p-basis for the algebra A. Therefore, we have

$$\dim_{Q_p} A = n = \operatorname{rank}_{\mathbf{Z}_p} \mathfrak{O}. \tag{10.4}$$

The order $\mathfrak{O}$ determines the algebra A to within isomorphism, since the multiplication coefficients for the basis $a_1, \ldots, a_n$ can be computed in $\mathfrak{O}$.

Of course, orders always exist.

PROPOSITION 10.5. *Any algebra A over Q_p contains at least one order $\mathfrak{O}$.*

Proof. Let $b_1, \ldots, b_n$ be any basis for A over Q_p. Then there are unique multiplication coefficients $f_{ijk} \in Q_p$, for $i, j, k = 1, \ldots, n$, such that

$$b_i b_j = \sum_{k=1}^{n} f_{ijk} b_k \quad (i, j = 1, \ldots, n).$$

Since Q_p is the field of fractions of $\mathbf{Z}_p$, there is a $z \neq 0$ in $\mathbf{Z}_p$ such that $zf_{ijk} \in \mathbf{Z}_p$ $(i, j, k = 1, \ldots, n)$. The basis $zb_1, \ldots, zb_n$ for A over Q_p then satisfies

$$(zb_i)(zb_j) = \sum_{k=1}^{n} (zf_{ijk})(zb_k) \in \mathbf{Z}_p(zb_1) + \ldots + \mathbf{Z}_p(zb_n) \quad (i, j = 1, \ldots, n).$$

So the $\mathbf{Z}_p$-submodule $\mathfrak{M} = \mathbf{Z}_p(zb_1) + \ldots + \mathbf{Z}_p(zb_n)$ of A is closed under multiplication. It follows that $\mathfrak{O} = \mathbf{Z}_p \cdot 1_A + \mathfrak{M}$ is also closed under multiplication. Therefore $\mathfrak{O}$ satisfies (10.1a). By its construction it satisfies (10.1b, c). It satisfies (10.1d), since $\mathfrak{M}$ does. Hence it is the order we seek.

A general algebra A contains many orders, and it is impossible to single out one of them in any reasonable fashion. However, there is one important exception to this rule when the algebra A is a finite algebraic extension field F of Q_p.

PROPOSITION 10.6. *There is a unique maximum order $\mathfrak{O}$ containing all the other orders in F.*

Proof. Let $\mathfrak{O}_1$ and $\mathfrak{O}_2$ be two orders in F. Since F is commutative and $1 \in \mathfrak{O}_1 \cap \mathfrak{O}_2$, the subring generated by $\mathfrak{O}_1$ and $\mathfrak{O}_2$ is their product $\mathfrak{O}_1\mathfrak{O}_2$, the additive subgroup generated by all products xy, with $x \in \mathfrak{O}_1$, $y \in \mathfrak{O}_2$. If $a_1, \ldots, a_n$ is a $\mathbf{Z}_p$-basis of $\mathfrak{O}_1$ and $b_1, \ldots, b_n$ is a $\mathbf{Z}_p$-basis of $\mathfrak{O}_2$, then clearly the products a_ib_j $(i, j = 1, \ldots, n)$ generate $\mathfrak{O}_1\mathfrak{O}_2$ as a $\mathbf{Z}_p$-module. Therefore $\mathfrak{O}_1\mathfrak{O}_2$ is an order of F containing both $\mathfrak{O}_1$ and $\mathfrak{O}_2$.

In view of Proposition 10.5, the above argument implies that the union $\mathfrak{O}$ of all the orders in F satisfies (10.1a, b, d). To complete the proof of the proposition, we therefore need only show that $\mathfrak{O}$ is a finitely-generated $\mathbf{Z}_p$-module.

If $f \in F$, then its field trace $\operatorname{tr}(f) \in Q_p$ is the trace of the Q_p-linear transformation $L_f : y \to fy$ of F. We must prove that

$$\operatorname{tr}(f) \in \mathbf{Z}_p, \quad \textit{for all } f \in \mathfrak{O}. \tag{10.7}$$

Indeed, an element $f \in \mathfrak{O}$ is, by definition, contained in an order $\mathfrak{O}_1$ in F. A $\mathbf{Z}_p$-basis $a_1, \ldots, a_n$ for $\mathfrak{O}_1$ is also a Q_p-basis for F. Since $\mathfrak{O}_1$ is closed under multiplication, there are elements $z_{ij} \in \mathbf{Z}_p$ $(i, j = 1, \ldots, n)$ such that $fa_i = \sum_{j=1}^{n} z_{ij}a_j$, $(i = 1, \ldots, n)$. But, then,

$$\operatorname{tr}(f) = \operatorname{tr}(L_f) = \operatorname{tr}((z_{ij})) = z_{11} + z_{22} + \ldots + z_{nn} \in \mathbf{Z}_p.$$

So (10.7) holds.

Since $\mathbf{Z}_p$ has characteristic zero (by Corollary 8.6), the trace $\operatorname{tr}(1_F) = \dim_{Q_p}(F)$ is non-zero. If $f \neq 0$ in F, then $\operatorname{tr}(ff^{-1}) = \operatorname{tr}(1) \neq 0$. It follows that $f, g \to \operatorname{tr}(fg)$ is a non-singular Q_p-bilinear form from $F \times F$ into Q_p. If $\mathfrak{O}_1$ is an order of F with a $\mathbf{Z}_p$-basis $a_1, \ldots, a_n$, then there exists a dual

basis $c_1, \ldots, c_n$ for F over Q_p such that tr $(a_i c_j)$ is the Kronecker δ-function δ_{ij} $(i, j = 1, \ldots, n)$. It follows easily that

$$\{f \in F : \text{tr}\,(fx) \in \mathbf{Z}_p, \quad \textit{for all } x \in \mathfrak{O}_1\} = \mathbf{Z}_p c_1 \oplus \ldots \oplus \mathbf{Z}_p c_n.$$

In view of (10.7), the ring $\mathfrak{O}$ is contained in the left side of this equation. So $\mathfrak{O}$ is a $\mathbf{Z}_p$-submodule of the finitely-generated $\mathbf{Z}_p$-module on the right side. Since $\mathbf{Z}_p$ is a principal ideal domain, this implies that $\mathfrak{O}$ is a finitely-generated $\mathbf{Z}_p$-module, which completes the proof of the proposition.

The above maximum order $\mathfrak{O}$ is usually described differently in the literature. We don't really need the other description, but we put it here anyway out of respect for tradition.

An element $f \in F$ is *integral* over $\mathbf{Z}_p$ if it satisfies an equation of the form:

$$f^m + z_1 f^{m-1} + \ldots + z_m = 0, \quad \textit{for some } m \geq 1 \text{ and } z_1, \ldots, z_m \in \mathbf{Z}_p. \quad (10.8)$$

The set of all such elements f is called the *integral closure* of $\mathbf{Z}_p$ in F. In fact, it is simply the maximum order $\mathfrak{O}$.

PROPOSITION 10.9. *The maximum order $\mathfrak{O}$ is the integral closure of $\mathbf{Z}_p$ in F.*

Proof. Obviously condition (10.8) for an element $f \in F$ implies that $1, f, f^2, \ldots, f^{m-1}$ alone generate the $\mathbf{Z}_p$-module $\mathbf{Z}_p[f]$ generated by all the powers $1, f, f^2, \ldots$ of f. On the other hand, if $\mathbf{Z}_p[f]$ is a finitely-generated $\mathbf{Z}_p$-module, then we can find a finite subset $1, f, f^2, \ldots, f^{m-1}$ generating $\mathbf{Z}_p[f]$ in the infinite family $1, f, f^2, \ldots$ of generators. Clearly this implies that (10.8) holds. Hence f is integral over $\mathbf{Z}_p$ if and only if $\mathbf{Z}_p[f]$ is a finitely-generated $\mathbf{Z}_p$-module.

If $f \in \mathfrak{O}$, then $\mathbf{Z}_p[f]$ is a submodule of the finitely-generated $\mathbf{Z}_p$-module $\mathfrak{O}$, and hence is finitely-generated. If $\mathbf{Z}_p[f]$ is a finitely-generated $\mathbf{Z}_p$-module, then $\mathbf{Z}_p[f] \cdot \mathfrak{O}$ is also a finitely-generated $\mathbf{Z}_p$-module. But $\mathbf{Z}_p[f]\mathfrak{O}$ is a subring of F containing $\mathfrak{O}$, and hence is an order in F. By Proposition 10.6, $f = f \cdot 1 \in \mathbf{Z}_p[f] \cdot \mathfrak{O} \subseteq \mathfrak{O}$. Therefore $f \in \mathfrak{O}$ if and only if $\mathbf{Z}_p[f]$ is a finitely-generated $\mathbf{Z}_p$-module. Together with the first paragraph, this proves the proposition.

That the order $\mathfrak{O}$ is a local ring is given by

PROPOSITION 10.10. *The radical $J(\mathfrak{O})$ is the unique maximal ideal in the maximum order $\mathfrak{O}$ of F.*

Proof. Since F is a field, the only idempotents in F are 0 and $1 \neq 0$. It follows that 1 is the unique non-zero idempotent in the p-adic algebra $\mathfrak{O}$. By Proposition 9.7 and the commutativity of $\mathfrak{O}$, the factor ring $\mathfrak{O}/J(\mathfrak{O})$ is a field. Hence $J(\mathfrak{O})$ is a maximal ideal in $\mathfrak{O}$. Furthermore, Proposition 9.7 also says that every element of $\mathfrak{O} \setminus J(\mathfrak{O})$ is a unit in $\mathfrak{O}$. Therefore every ideal $\neq \mathfrak{O}$ of $\mathfrak{O}$ is contained in $J(\mathfrak{O})$. So the proposition is true.

We return to an arbitrary algebra A over Q_p and an arbitrary order $\mathfrak{O}$ in A. Let M be a module over A in the sense of Section 3. By an *$\mathfrak{O}$-lattice L in M* we understand a subset satisfying:

$$L \text{ is a finitely-generated } \mathfrak{O}\text{-submodule of } M, \tag{10.11a}$$

$$\text{For each } y \in M, \text{ there exists } z \neq 0 \text{ in } \mathbf{Z}_p \text{ such that } zy \in L. \tag{10.11b}$$

Evidently L is a module over the p-adic algebra $\mathfrak{O}$ in the sense of Section 9, and hence is a p-adic module in the sense of Section 8 (see the remarks preceding Proposition 9.4). As in the case of (10.3), this implies that L is a free $\mathbf{Z}_p$-module of finite rank m. From (10.11b) we see that any $\mathbf{Z}_p$-basis for L is also a Q_p-basis for M. Hence,

$$\dim_{Q_p} M = m = \operatorname{rank}_{\mathbf{Z}_p} L. \tag{10.12}$$

As usual, this implies that the $\mathfrak{O}$-module L determines the A-module M to within isomorphism.

As in the case of Proposition 10.5, lattices always exist.

PROPOSITION 10.13. *If $\mathfrak{O}$ is an order in an algebra A over Q_p, and M is a module over A, then there exists at least one $\mathfrak{O}$-lattice in M.*

Proof. Let $y_1, \ldots, y_m$ be a Q_p-basis for M. Then $L = \mathfrak{O}y_1 + \ldots + \mathfrak{O}y_m$ is evidently a finitely-generated $\mathfrak{O}$-submodule of M satisfying (10.11b). This is the lattice we are seeking.

11. Blocks

Before we can define the blocks of a finite group G, we must find a good splitting field.

PROPOSITION 11.1. *If E is a field of characteristic zero, then there is a finite algebraic extension F of E which is a splitting field for the group algebra FG.*

Proof. In view of Propositions 3.9 and 3.12, an extension F of E is a splitting field for FG if and only if there exist integers $n_1, \ldots, n_k \geq 1$ (for some $k \geq 1$) such that:

$$FG \simeq [F]_{n_1} \oplus \ldots \oplus [F]_{n_k} \quad (\textit{as algebras}),$$

where $[F]_{n_i}$ is the algebra of all $n_i \times n_i$ matrices with entries in F. Choosing the usual basis for the matrix algebra $[F]_{n_i}$ (consisting of those matrices with all but one entry equal to zero, and that entry equal to one), we see that this occurs if and only if FG has a basis over F consisting of elements $e_{ij}^{(l)}$, for $l = 1, \ldots, k$ and $i, j = 1, \ldots, n_l$, satisfying

$$e_{ij}^{(l)} e_{i'j'}^{(l')} = \begin{cases} e_{ij'}^{(l)}, & \text{if } l = l' \text{ and } j = i', \\ 0, & \text{otherwise}, \end{cases} \tag{11.2}$$

for all $l, l' = 1, \ldots, k$, all $i, j = 1, \ldots, n_l$ and all $i', j' = 1, \ldots, n_{l'}$.

By Proposition 3.13 the algebraic closure $\hat{E}$ of E is a splitting field for $\hat{E}G$. So $\hat{E}G$ has a basis $\{e_{ij}^{(l)}\}$ of the above form. Since both bases are finite, there are only a finite number of coefficients in the matrix transforming the basis G into the basis $\{e_{ij}^{(l)}\}$. Hence these coefficients generate a finite algebraic extension $F \subseteq \hat{E}$ of E such that $e_{ij}^{(l)}$ lies in $FG \subseteq \hat{E}G$. Evidently the $e_{ij}^{(l)}$ form a basis of FG satisfying (11.2). Hence F is a splitting field for FG, and the proposition is proved.

Now let p be any prime. Since the finite group G has only a finite number of subgroups, the above proposition implies the existence of a field F satisfying

F is a finite algebraic extension of the p-adic number field Q_p, (11.3a)

F is a splitting field for the group algebra FH of any subgroup H of G. (11.3b)

We fix such a field F, and denote by $\mathfrak{O}$ the maximum order in F given by Proposition 10.6.

Because of (11.3a), the group algebra FG is finite-dimensional as a vector space over $Q_p \subseteq F$. Hence it is an algebra over Q_p in the sense of Section 3. Evidently the *group ring* $\mathfrak{O}G$ of G over $\mathfrak{O}$, defined by

$$\mathfrak{O}G = \left\{ \sum_{\sigma \in G} y_\sigma \sigma \in FG : y_\sigma \in \mathfrak{O}, \quad \textit{for all } \sigma \in G \right\}, \tag{11.4}$$

is an order in FG.

As in (4.23), let $K_1, \ldots, K_c$ be the conjugacy classes of G and $\tilde{K}_1, \ldots, \tilde{K}_c$ be the corresponding class sums. We can repeat the proof of Proposition 4.24 almost word for word to show that the center $Z(\mathfrak{O}G)$ of the ring $\mathfrak{O}G$ is given by

$$Z(\mathfrak{O}G) = \left\{ \sum_{i=1}^{c} y_i \tilde{K}_i : y_i \in \mathfrak{O} \quad (i = 1, \ldots, c) \right\}. \tag{11.5}$$

In view of that proposition, this implies that $Z(\mathfrak{O}G)$ is an order in the center $Z(FG)$ of the group algebra FG. In particular, $Z(\mathfrak{O}G)$ is a commutative p-adic algebra. So (9.12) says that the primitive idempotents $e_1, \ldots, e_b \in Z(\mathfrak{O}G)$ satisfy

$$1 = e_1 + \ldots + e_b \textit{ and } e_i e_j = 0, \quad \textit{for all } i, j = 1, \ldots, b \textit{ with } i \neq j. \tag{11.6}$$

The group G has b *blocks* $B_1, \ldots, B_b$ (for the prime p) corresponding to the primitive idempotents $e_1, \ldots, e_b$, respectively. The concept "block" is open and not closed. That is, we do not define it once and for all (e.g., by calling e_i, which determines B_i, *the* block B_i). Rather, any time a collection C of objects attached to the group G decomposes naturally into a disjoint union of subsets $C_1, \ldots, C_b$ attached to the idempotents $e_1, \ldots, e_b$, respectively, we put the objects of C_i in the block B_i, for each $i = 1, \ldots, b$.

For example, we can put e_i in the block B_i, for each $i = 1, \ldots, b$. It is then the unique primitive idempotent of $Z(\mathfrak{O}G)$ lying in B_i.

As in (4.6), let $A_1, \ldots, A_k$ be the minimal two-sided ideals of FG. From (4.22) we see that their identities $1_{A_1}, \ldots, 1_{A_k}$ are idempotents in $Z(FG)$ satisfying $1 = 1_{A_1} + \ldots + 1_{A_k}$ and $1_{A_i} 1_{A_j} = 0$ if $i, j = 1, \ldots, k$ with $i \neq j$. Since $1_{A_i} Z(FG) 1_{A_i} = F \cdot 1_{A_i} \simeq F$ is a field, the idempotent 1_{A_i} is primitive in $Z(FG)$ $(i = 1, \ldots, k)$. Applying Proposition 9.11 to the ring $Z(FG)$, the decomposition $1 = 1_{A_1} + \ldots + 1_{A_k}$, and the idempotents $e_1, \ldots, e_b$ of the subring $Z(\mathfrak{O}G)$, we obtain unique subsets $S_1, \ldots, S_b$ of $\{1, \ldots, k\}$ such that

$$e_i = \sum_{l \in S_i} 1_{A_l} \quad (i = 1, \ldots, b). \tag{11.7}$$

Evidently the condition $e_i e_j = 0$, for $i \neq j$, says that $S_i \cap S_j$ is empty, while the condition $1 = e_1 + \ldots + e_b$ says that $S_1 \cup \ldots \cup S_b = \{1, \ldots, k\}$. Therefore $\{1, \ldots, k\}$ is the disjoint union of its subsets $S_1, \ldots, S_b$. If $l \in S_i$, for some $i = 1, \ldots, b$, we can now put the minimal two-sided ideal A_l, its identity 1_{A_l}, and the corresponding irreducible character χ_l of G in B_i. In view of (4.17), the equation (11.7) becomes

$$e_i = \sum_{\chi_l \in B_i} e(\chi_l) \quad (i = 1, \ldots, b). \tag{11.8}$$

Hence *the block B_i is uniquely determined by its irreducible characters.*

Some blocks only contain one irreducible character.

PROPOSITION 11.9. *Let p^a be the largest power of the prime p dividing $|G|$. If p^a divides $\chi_l(1)$, for some irreducible character χ_l of G, then χ_l is the only irreducible character in its block.*

Proof. In this case (4.17) implies that $e(\chi_l) \in Z(\mathfrak{O}G)$. Since $e(\chi_l)$ is primitive in $Z(FG)$, it is primitive in $Z(\mathfrak{O}G)$. Hence $e(\chi_l) = e_i$, for some $i = 1, \ldots, b$. In view of (11.8), this implies the proposition.

COROLLARY 11.10. *If p does not divide $|G|$, then there is a one to one correspondence between blocks and irreducible characters of G, in which each block corresponds to the unique character it contains. After renumbering we then have $e_i = e(\chi_i)$, $(i = 1, \ldots, b)$.*

Proof. In this case $p^a = 1$ divides $\chi_l(1)$, for all $l = 1, \ldots, k$. So the proposition gives the corollary.

The blocks of the type described in Proposition 11.9 are called *blocks of defect* 0.

Proposition 9.13 says that the images $\bar{e}_1, \ldots, \bar{e}_b$ of $e_1, \ldots, e_b$, respectively, are precisely the primitive idempotents in $Z(\mathfrak{O}G)/J(Z(\mathfrak{O}G))$. Hence we can distribute them among the blocks so that $\bar{e}_i$ is the primitive idempotent of $Z(\mathfrak{O}G)/J(Z(\mathfrak{O}G))$ in B_i $(i = 1, \ldots, b)$. Notice that the idempotent $\bar{e}_i$ also determines B_i since, by Proposition 9.13, e_i is the only idempotent of $Z(\mathfrak{O}G)$ having $\bar{e}_i$ as its image in $Z(\mathfrak{O}G)/J(Z(\mathfrak{O}G))$.

Since $Z(\mathfrak{O}G)$ is a commutative p-adic algebra, (8.11) and Propositions 3.9 and 3.12 imply that $Z(\mathfrak{O}G)/J(Z(\mathfrak{O}G))$ has a unique decomposition

$$Z(\mathfrak{O}G)/J(Z(\mathfrak{O}G)) = E_1 \oplus \ldots \oplus E_b \quad (\textit{as } \mathbf{Z}/p\mathbf{Z}\textit{-algebras}), \tag{11.11}$$

where $E_1, \ldots, E_b$ are finite-dimensional extension fields of $\mathbf{Z}/p\mathbf{Z}$. Incidentally, we have not made an error in counting the E_i's. Evidently $1_{E_1}, \ldots, 1_{E_b}$ are precisely the primitive idempotents of $Z(\mathfrak{O}G)/J(Z(\mathfrak{O}G))$. So the number of direct summands E_i in (11.11) is in fact the number b of primitive idempotents $\bar{e}_i$, and hence the number of blocks of G. We choose the notation so that

$$1_{E_i} = \bar{e}_i, \quad \textit{for } i = 1, \ldots, b. \tag{11.12}$$

Of course we put each E_i in the corresponding block B_i.

The natural homomorphism $y \to y1$ of the ring $\mathfrak{O}$ into $Z(\mathfrak{O}G)$ makes the latter ring an algebra (with identity) over the former.

LEMMA 11.13. *For each $l = 1, \ldots, k$, the restriction of the epimorphism $\theta_l : Z(FG) \to F$ of* (4.29) *is an epimorphism of $Z(\mathfrak{O}G)$ onto $\mathfrak{O}$ as $\mathfrak{O}$-algebras.*

Proof. Since θ_l is a homomorphism of F-algebras, its restriction is an $\mathfrak{O}$-algebra epimorphism of $Z(\mathfrak{O}G)$ onto an $\mathfrak{O}$-subalgebra $\theta_l(Z(\mathfrak{O}G))$ of F. Evidently $\theta_l(Z(\mathfrak{O}G))$ contains $\mathfrak{O}\theta_l(1) = \mathfrak{O} \cdot 1 = \mathfrak{O}$. On the other hand, the image $\theta_l(Z(\mathfrak{O}G))$ of the order $Z(\mathfrak{O}G)$ of $Z(FG)$ must be an order in $\theta_l(Z(FG)) = F$ (just verify (10.1)!). So $\theta_l(Z(\mathfrak{O}G)) \subseteq \mathfrak{O}$ by Proposition 10.6. That proves the lemma.

We know from (4.29) that $\chi_l(1_{A_j})$ is 1, if $l = j$, and is 0, if $l \neq j$ $(j, l = 1, \ldots, k)$. This and (11.8) imply that

$$\theta_l(e_i) = \begin{cases} 1, & \textit{if } \chi_l \in B_i, \\ 0, & \textit{if } \chi_l \notin B_i, \end{cases} \tag{11.14}$$

for all $l = 1, \ldots, k$ and $i = 1, \ldots, b$.

We denote by $\bar{\theta}_l$ the $\mathfrak{O}$-algebra epimorphism of $Z(\mathfrak{O}G)$ onto $\bar{F} = \mathfrak{O}/J(\mathfrak{O})$ obtained by composing θ_l with the natural epimorphism of $\mathfrak{O}$ onto $\mathfrak{O}/J(\mathfrak{O})$.

PROPOSITION 11.15. *There are precisely b epimorphisms $\eta_1, \ldots, \eta_b$ of $Z(\mathfrak{O}G)$ onto $\bar{F}$ as $\mathfrak{O}$-algebras. For any $i = 1, \ldots, b$, the epimorphism η_i is zero on $J(Z(\mathfrak{O}G))$, and the induced epimorphism $\bar{\eta}_i$ on $Z(\mathfrak{O}G)/J(Z(\mathfrak{O}G))$ is zero on each E_h $(h \neq i)$ and an isomorphism of E_i onto $\bar{F}$. An irreducible character χ_l of G lies in a block B_i if and only if $\bar{\theta}_l = \eta_i$.*

Proof. Let η be any $\mathfrak{O}$-algebra epimorphism of $Z(\mathfrak{O}G)$ onto $\bar{F}$. Since $\bar{F}$ is a field of characteristic p, the ideal $pZ(\mathfrak{O}G)$ is contained in the kernel $\mathrm{Ker}(\eta)$ of η. In view of (8.12), the image $\eta(J(Z(\mathfrak{O}G)))$ is nilpotent. Because $\bar{F}$ is a field, this image is zero. Therefore η induces an $\mathfrak{O}$-algebra epimorphism $\bar{\eta}$ of $Z(\mathfrak{O}G)/J(Z(\mathfrak{O}G))$ onto $\bar{F}$.

Since $\bar{F}$ is a field, and each field E_i ($i = 1,\ldots, b$) is an $\mathfrak{O}$-subalgebra of $Z(\mathfrak{O}G)/J(Z(\mathfrak{O}G))$, it is clear from (11.11) that the epimorphism $\bar{\eta}$ must be zero on all but one of the E_i and an isomorphism on that one. Because $\bar{F} = \mathfrak{O}\cdot 1_F$, the exceptional E_i satisfies $E_i = \mathfrak{O}\cdot 1_{E_i}$. Hence it has exactly one $\mathfrak{O}$-isomorphism onto $\bar{F}$. Therefore $\eta = \eta_i$ is uniquely determined by this value of i.

Now let i be any of the integers $1,\ldots, b$ and χ_l be any irreducible character of G in the block B_i. Then $\bar{\theta}_l$ is an $\mathfrak{O}$-algebra epimorphism of $Z(\mathfrak{O}G)$ onto $\bar{F}$. By the above argument, $\bar{\theta}_l$ induces an $\mathfrak{O}$-algebra epimorphism $\bar{\bar{\theta}}_l$ of $Z(\mathfrak{O}G)/J(Z(\mathfrak{O}G))$ onto $\bar{F}$. From (11.14) we see that $\bar{\bar{\theta}}_l(\bar{e}_i) = \bar{\theta}_l(e_i) = 1$. Hence $\bar{\bar{\theta}}_l$ is not zero on E_i. The above argument implies that $\bar{\theta}_l$ is the unique $\mathfrak{O}$-epimorphism η_i associated with this value of i. This completes the proof of the proposition.

COROLLARY 11.16. *Two irreducible characters χ_j, χ_l of G belong to the same block if and only if*

$$\frac{\chi_j(\tilde{K}_i)}{\chi_j(1)} \equiv \frac{\chi_l(\tilde{K}_i)}{\chi_l(1)} \pmod{J(\mathfrak{O})}, \tag{11.17}$$

for each class sum $\tilde{K}_i$ ($i = 1,\ldots, c$) of G.

Proof. This follows from the proposition, (11.5), and (4.30).

As usual, we put η_i in the block B_i, for each $i = 1,\ldots, b$. Evidently η_i determines e_i (and hence B_i) by the condition

$$\eta_i(e_h) = \begin{cases} 1_F, & \text{if } i = h, \\ 0, & \text{if } i \neq h, \end{cases} \quad (i, h = 1,\ldots, b). \tag{11.18}$$

As a final example of objects which can be put in blocks, we consider the indecomposable $\mathfrak{O}G$-modules. If L is any $\mathfrak{O}G$-module (in the sense of Section 9) then conditions (11.6) and the fact that the idempotents e_i all belong to the center of $\mathfrak{O}G$ imply that

$$L = Le_1 \oplus \ldots \oplus Le_b \quad (\textit{as } \mathfrak{O}G\textit{-modules}). \tag{11.19}$$

In particular, if L is indecomposable, then exactly one of the $\mathfrak{O}G$-submodules Le_i is non-zero, and that one equals L. Obviously we put L in the corresponding block. Hence,

An indecomposable $\mathfrak{O}G$-module L lies in the block B_i (where $i = 1,\ldots, b$) if and only if $L = Le_i$. (11.20)

One relation between indecomposable lattices and irreducible characters in a block is very useful.

PROPOSITION 11.21. *Let M be an FG-module (in the sense of Section 3) and L be an $\mathfrak{O}G$-lattice in M. If L is indecomposable and lies in a block B_i of G,*

then the character χ_M of M (defined by (4.4)) *has the form*

$$\chi_M = \sum_{\chi_l \in B_i} c_l \chi_l, \tag{11.22}$$

for some integers $c_l \geq 0$.

Proof. By (11.20) multiplication by e_i is identity on L. It follows that e_i also acts as identity on M. In view of (11.8) this implies that

$$M = \oplus \sum_{\chi_l \in B_i} Me(\chi_l) \quad (\textit{as } FG\textit{-modules})$$

From Proposition 3.18 we see that each $Me(\chi_l) = M1_{A_l} = MA_l$ is a direct sum of c_l copies of the irreducible FG-module I_l corresponding to the character χ_l, for some integer $c_l \geq 0$. The proposition results directly from this, the preceding equation, and (2.10).

We close this section with a useful example of groups for which the blocks are highly non-trivial.

PROPOSITION 11.23. *Suppose that G is a p-group. Then we have*

$$J(\mathfrak{O}G) = J(\mathfrak{O})1 + \sum_{\sigma \in G,\, \sigma \neq 1} \mathfrak{O}(\sigma - 1). \tag{11.24}$$

Therefore:

$$\mathfrak{O}G/J(\mathfrak{O}G) \simeq \mathfrak{O}/J(\mathfrak{O}) \simeq \bar{F}. \tag{11.25}$$

Proof. By definition $J(\mathfrak{O}G)$ is the inverse image in $\mathfrak{O}G$ of $J(\mathfrak{O}G/p\mathfrak{O}G)$. Let I be an irreducible $\mathfrak{O}G/p\mathfrak{O}G$-module. Since I has finite dimension over $\mathbf{Z}_p$, its additive group is a finite p-group. Using the operation of G on I, we form the semi-direct product GI, which is also a finite p-group having I as a non-trivial normal subgroup. It follows (see Satz III.7.2 in Huppert, 1967) that $I \cap Z(GI)$ is non-trivial. Hence there is an element $y \neq 0$ in I such that $y\sigma = y$, for all $\sigma \in G$. Because I is irreducible, we must have $I = z(\mathfrak{O}/p\mathfrak{O})$ Furthermore, I must be irreducible as an $\mathfrak{O}/p\mathfrak{O}$-module. Hence $yJ(\mathfrak{O}/p\mathfrak{O}) = 0$. It follows that *the only irreducible $\mathfrak{O}G/p\mathfrak{O}G$-module is $\bar{F} = \mathfrak{O}/J(\mathfrak{O})$ with trivial action of G.* Equation (11.24) follows directly from this and (3.6), while (11.25) follows from (11.24).

COROLLARY 11.26. *The p-group G has just one block containing every irreducible character of G.*

Proof. The proposition and Proposition 9.7 imply that 1 is the unique non-zero idempotent in $\mathfrak{O}G$. Hence 1 is also the unique non-zero idempotent in the subring $Z(\mathfrak{O}G)$. This implies the corollary.

12. Orthogonality Relations

We continue to use the notation and hypotheses of the last section.

Let L be an $\mathfrak{O}G$-module, and K be an $\mathfrak{O}H$-submodule of L, for some

su bgroup H of G. We say that L is *induced* from K (and write $L = K^G$) if

$$L = \oplus \sum_{\sigma \in \text{rep}(G/H)} K\sigma \quad (\textit{as } \mathfrak{O}\textit{-modules}) \tag{12.1}$$

where rep (G/H) is, as in (5.5), a family of representatives for the left cosets $H\sigma$ of H in G. For each $\sigma \in \text{rep}\,(G/H)$ and $\tau \in G$, there are unique $\sigma' \in \text{rep}\,(G/H)$ and $\rho \in H$ such that $\sigma\tau = \rho\sigma'$. Since K is an $\mathfrak{O}H$-submodule of L, it follows that:

$$(k\sigma)\tau = (k\rho)\sigma' \in K\sigma', \quad \textit{for all } k \in K. \tag{12.2}$$

Evidently $k \to k\sigma$ is an $\mathfrak{O}$-isomorphism of K on to $K\sigma$. So this and (12.1) imply that the $\mathfrak{O}G$-module structure of L is completely determined by the $\mathfrak{O}H$-module structure of K. Furthermore it is evident that we can start with an arbitrary $\mathfrak{O}H$-module K and construct via (12.1) and (12.2) an $\mathfrak{O}G$-module L satisfying $L = K^G$ (to get K to be a submodule of L, pick rep (G/H) to contain 1 and identify K with the summand $K1$ in (12.1)).

There is a simple connection between induced modules and the induced characters of Section 5. To express it, it is convenient to write χ_L for the character χ_M of an FG-module M having L as an $\mathfrak{O}G$-lattice.

PROPOSITION 12.3. *Let M be an FG-module, L be an $\mathfrak{O}G$-lattice in M, and K be an $\mathfrak{O}H$-submodule such that $L = K^G$. Then K is an $\mathfrak{O}H$-lattice in the F-subspace N of M which it spans. Furthermore,*

$$\chi_L = \chi_{K^G} = (\chi_K)^G, \tag{12.4}$$

where χ_K is the H-character of K.

Proof. Clearly N is an FH-submodule of M. A glance at (10.11) shows that K is an $\mathfrak{O}H$-lattice in N. From (12.1) we easily obtain the equation

$$M = \oplus \sum_{\sigma \in \text{rep}(G/H)} N\sigma \quad (\textit{as } F\textit{-spaces})$$

Let τ be any element of G and T be the linear transformation $m \to m\tau$ of M. The above decomposition gives us unique F-linear maps $T_{\sigma,\pi} : N\sigma \to N\pi$, for $\sigma, \pi \in \text{rep}\,(G/H)$, such that

$$T(m) = \oplus \sum_{\pi \in \text{rep}(G/H)} T_{\sigma,\pi}(m), \quad \textit{for all } \sigma \in \text{rep}\,(G/H),\ m \in N\sigma.$$

Furthermore,

$$\chi_L(\tau) = \chi_M(\tau) = \text{tr}\,(T) = \sum_{\sigma \in \text{rep}(G/H)} \text{tr}\,(T_{\sigma,\sigma}).$$

Let σ be any element of rep (G/H), and $\sigma' \in \text{rep}\,(G/H)$, $\rho \in H$ be the unique elements such that $\sigma\tau = \rho\sigma'$. Then $T(N\sigma) = N\sigma\tau = N\rho\sigma' = N\sigma'$. Hence $T_{\sigma,\pi} = 0$ for $\pi \neq \sigma'$. In particular $T_{\sigma,\sigma} = 0$ unless $\sigma = \sigma'$, which occurs if and only if $\tau^{\sigma^{-1}} = \rho \in H$. In that case the F-isomorphism $n \to n\sigma$ of N onto $N\sigma$ defines an equivalence between $T_{\sigma,\sigma}$ and the linear transformation $n \to n\tau^{\sigma^{-1}}$ of N. Therefore tr $(T_{\sigma,\sigma})$ equals the trace $\chi_N(\tau^{\sigma^{-1}})$ of this last

transformation. Using (5.1), (5.4) and (5.5), we conclude that

$$\chi_L(\tau) = \sum_{\sigma \in \mathrm{rep}\,(G/H),\ \tau^{\sigma^{-1}} \in H} \chi\ (\tau^{\sigma^{-1}}) = (\chi_N)^G(\tau) = (\chi_K)^G(\tau).$$

So the proposition holds.

We shall need some lemmas to aid us to compute endomorphism rings of induced modules.

LEMMA 12.5. *Let L be an $\mathfrak{O}G$-module and K be an $\mathfrak{O}H$-submodule such that $L = K^G$. If $\phi \in \mathrm{Hom}_{\mathfrak{O}G}(L, L)$ then the restriction ϕ_K to K lies in $\mathrm{Hom}_{\mathfrak{O}H}(K, L)$. Furthermore the map $\phi \to \phi_K$ is an $\mathfrak{O}$-isomorphism of $\mathrm{Hom}_{\mathfrak{O}G}(L, L)$ onto $\mathrm{Hom}_{\mathfrak{O}H}(K, L)$.*

Proof. Clearly $\phi_K \in \mathrm{Hom}_{\mathfrak{O}H}(K, L)$, for all $\phi \in \mathrm{Hom}_{\mathfrak{O}G}(L, L)$. Furthermore ϕ_K determines ϕ because of (12.1) and the equation

$$\phi(k\sigma) = \phi(k)\sigma = \phi_K(k)\sigma, \quad \textit{for all } k \in K,\ \sigma \in \mathrm{rep}\,(G/H). \tag{12.6}$$

Hence the map $\phi \to \phi_K$ is an $\mathfrak{O}$-monomorphism of $\mathrm{Hom}_{\mathfrak{O}G}(L, L)$ into $\mathrm{Hom}_{\mathfrak{O}H}(K, L)$.

Suppose we are given $\phi_K \in \mathrm{Hom}_{\mathfrak{O}H}(K, L)$. By (12.1) there is a unique $\mathfrak{O}$-linear map ϕ of L into L satisfying (12.6). Choosing $\sigma \in H$, we see that ϕ_K is indeed the restriction of ϕ to K. From (12.2) we compute easily that $\phi \in \mathrm{Hom}_{\mathfrak{O}G}(L, L)$. So $\phi \to \phi_K$ is an epimorphism, and the lemma is proved.

COROLLARY 12.7. *The inverse of the above isomorphism $\phi \to \phi_K$ sends $\mathrm{Hom}_{\mathfrak{O}H}(K, K) \subseteq \mathrm{Hom}_{\mathfrak{O}H}(K, L)$ monomorphically into $\mathrm{Hom}_{\mathfrak{O}G}(L, L)$ as $\mathfrak{O}$-algebras. This monomorphism carries the identity $1_{K \to K}$ of the first algebra into the identity $1_{L \to L}$ of the second.*

Proof. If $\phi, \psi \in \mathrm{Hom}_{\mathfrak{O}G}(L, L)$ satisfy $\phi_K, \psi_K \in \mathrm{Hom}_{\mathfrak{O}H}(K, K)$, then clearly $(\phi\psi)_K = \phi_K\chi_K$. The first statement of the corollary follows from this and the lemma. The second comes from the remark that $1_{K \to K}$ is obviously the restriction to K of $1_{L \to L}$.

We shall use the above lemma in a very special case. Let $\langle \pi \rangle$ be a cyclic p-group of order $p^d > 1$. We consider an $\mathfrak{O}\langle \pi \rangle$-module L and an $\mathfrak{O}\langle \pi^p \rangle$-submodule K such that $L = K^{\langle \pi \rangle}$. Since $\langle \pi \rangle$ is commutative, the map $\Pi : l \to l\pi$ is a central element of $\mathrm{Hom}_{\mathfrak{O}\langle \pi \rangle}(L, L)$. We identify $\mathrm{Hom}_{\mathfrak{O}\langle \pi^p \rangle}(K, K)$ with its image in $\mathrm{Hom}_{\mathfrak{O}\langle \pi \rangle}(L, L)$ via the algebra monomorphism of Corollary 12.7. Then we have

LEMMA 12.8. *The power Π^p is the central unit $\psi : k \to k\pi^p$ of $\mathrm{Hom}_{\mathfrak{O}\langle \pi^p \rangle}(K, K)$. Furthermore,*

$$\mathrm{Hom}_{\mathfrak{O}\langle \pi \rangle}(L, L) = \mathrm{Hom}_{\mathfrak{O}\langle \pi^p \rangle}(K, K) \oplus \mathrm{Hom}_{\mathfrak{O}\langle \pi^p \rangle}(K, K)\Pi \oplus \ldots \oplus \mathrm{Hom}_{\mathfrak{O}\langle \pi^p \rangle}(K, K)\Pi^{p-1}$$

(as $\mathfrak{O}$-modules) (12.9)

Proof. The first statement is clear from the definition of Π and Lemma 12.5. For the second, notice that $\Pi^i : k \to k\pi^i$ is an $\mathfrak{O}\langle\pi^p\rangle$-isomorphism of K onto $K\pi^i$ $(i = 0, 1, \ldots, p-1)$. Hence $\mathrm{Hom}_{\mathfrak{O}\langle\pi^p\rangle}(K, K)\Pi^i$ is isomorphic to $\mathrm{Hom}_{\mathfrak{O}\langle\pi^p\rangle}(K, K\pi^i)$ $(i = 0, 1, \ldots, p-1)$. Since $L = K \oplus K \oplus \ldots \oplus K\pi^{p-1}$ (as $\mathfrak{O}\langle\pi^p\rangle$-modules), this and Lemma 12.5 prove (12.9). So the lemma holds.

From this knowledge of the structure of $\mathrm{Hom}_{\mathfrak{O}\langle\pi\rangle}(L, L)$ we easily prove

PROPOSITION 12.10 (Green). *If, in the situation of Lemma* 12.8, *the* $\mathfrak{O}\langle\pi^p\rangle$-*submodule* K *is indecomposable, then so is the* $\mathfrak{O}\langle\pi\rangle$-*module* L.

Proof. Let $A = \mathrm{Hom}_{\mathfrak{O}\langle\pi\rangle}(L, L)$ and B be its subalgebra $\mathrm{Hom}_{\mathfrak{O}\langle\pi^p\rangle}(K, K)$. By Lemma 12.8, A is obtained from B by adjoining the central element $\Pi : A = B[\Pi]$. If I is an irreducible A/pA-module, we conclude that $IJ(B)$ is an A/pA-submodule of I. By (8.12), the ideal $J(B)$ is nilpotent modulo $pB \subseteq pA$. So $IJ(B) = I$ would imply that $I = IJ(B) = IJ(B)^2 = \ldots = 0$, which is impossible. Therefore $IJ(B) = 0$, and I is really an irreducible module over the ring $\bar{A} = A/J(B)A$. It follows that $J(A)$ is the inverse image in A of $J(\bar{A})$.

The ring $\bar{A}$ is generated over its subring $\bar{B} = B/(B \cap J(B)A)$ by the image $\bar{\Pi}$ of Π. From the definition of Π it is clear that $\Pi^{p^d} = 1$ in A. Hence $\bar{\Pi}^{p^d} = 1$ in $\bar{A}$. But $\bar{A}$ is a ring of characteristic p. Therefore $0 = \bar{\Pi}^{p^d} - 1 = (\bar{\Pi} - 1)^{p^d}$. It follows that the central element $\bar{\Pi} - 1$ generates a nilpotent two-sided ideal of $\bar{A}$. As usual, this ideal is contained in $J(\bar{A})$. Hence $J(A)$ is the inverse image in A of the radical of $\bar{A}/(\bar{\Pi} - 1)\bar{A} \simeq \bar{B}/(\bar{B} \cap (\bar{\Pi} - 1)\bar{A})$.

The indecomposability of K and Corollary 9.8 tell us that $B/J(B)$ is a division algebra over $\mathbf{Z}/p\mathbf{Z}$. Since $B \cap J(B)A \supseteq J(B)$, we conclude that $\bar{B} = B/(B \cap J(B)A) \neq 0$ is also a division algebra over $\mathbf{Z}/p\mathbf{Z}$. Hence so is its epimorphic image $\bar{B}/(\bar{B} \cap (\bar{\Pi} - 1)\bar{A}) \simeq \bar{A}/(\bar{\Pi} - 1)\bar{A}$. We conclude that $A/J(A) \simeq \bar{A}/(\bar{\Pi} - 1)\bar{A}$ is a division algebra over $\mathbf{Z}/p\mathbf{Z}$. By Corollary 9.8 again, this implies that L is indecomposable. So the proposition is proved.

We combine Propositions 12.3 and 12.10 to obtain an extremely useful criterion for the vanishing of certain characters.

PROPOSITION 12.11. *Let* $\langle\sigma\rangle$ *be a cyclic group whose order is divisible by* p, *and* $\langle\pi\rangle$ *be the* p-*Sylow subgroup of* $\langle\sigma\rangle$. *Suppose that* M *is an* $F\langle\sigma\rangle$-*module,* L *is an* $\mathfrak{O}\langle\sigma\rangle$-*lattice in* M, *and* K *is an* $\mathfrak{O}\langle\pi^p\rangle$-*submodule of* L *such that* $L = K^{\langle\pi\rangle}$ *as an* $\mathfrak{O}\langle\pi\rangle$-*module. If* L' *is any* $\mathfrak{O}\langle\sigma\rangle$-*direct summand of* L, *then* L' *is an* $\mathfrak{O}\langle\sigma\rangle$-*lattice and*

$$\chi_{L'}(\tau) = 0, \quad \textit{for all } \tau \in \langle\sigma\rangle \backslash \langle\sigma^p\rangle. \tag{12.12}$$

Proof. Of course, we assume implicitly that the conditions of Section 11, in particular (11.3), are satisfied by the group $\langle\sigma\rangle$ and field F. Obviously L' is an $\mathfrak{O}\langle\sigma\rangle$-lattice in the F-subspace of M which it generates. So the problem is

to prove (12.12). In doing so, we can assume that L' is an indecomposable $\mathfrak{O}\langle\sigma\rangle$-module, since a decomposition $L' = L'_1 \oplus L'_2$ (as $\mathfrak{O}\langle\sigma\rangle$-modules) implies that $\chi_{L'} = \chi_{L'_1} + \chi_{L'_2}$.

We can find a subgroup $\langle\rho\rangle$ of the cyclic group such that p does not divide the order of $\langle\rho\rangle$ and $\langle\sigma\rangle = \langle\rho\rangle \times \langle\pi\rangle$. Let $\lambda_1, \ldots, \lambda_k$ be the irreducible, and hence linear, characters of $\langle\rho\rangle$. By Corollary 11.10 the corresponding idempotents $e(\lambda_1), \ldots, e(\lambda_k)$ of $F\langle\rho\rangle$ all lie in $\mathfrak{O}\langle\rho\rangle \subseteq \mathfrak{O}\langle\sigma\rangle$. Since $\mathfrak{O}\langle\sigma\rangle$ is abelian, this implies that

$$L' = L'e(\lambda_1) \oplus \ldots \oplus L'e(\lambda_k) \quad (\textit{as } \mathfrak{O}\langle\sigma\rangle\textit{-modules}).$$

Because L' is an indecomposable $\mathfrak{O}\langle\sigma\rangle$-module, we conclude that $L' = L'e(\lambda_i)$, for some $i = 1, \ldots, k$. It follows that $l'\rho^j = \lambda_i(\rho^j)l'$, for all $l' \in L'$ and $\rho^j \in \langle\rho\rangle$. Since all the values of the linear character λ_i lie in $\mathfrak{O}$ (by (11.3)), this implies that any $\mathfrak{O}$-submodule of L' is an $\mathfrak{O}\langle\rho\rangle$-submodule of L'. Hence any $\mathfrak{O}\langle\pi\rangle$-submodule of L' is an $\mathfrak{O}(\langle\rho\rangle \times \langle\pi\rangle) = \mathfrak{O}\langle\sigma\rangle$-submodule. In particular, L' is indecomposable as an $\mathfrak{O}\langle\pi\rangle$-module.

Choose indecomposable $\mathfrak{O}\langle\pi^p\rangle$-submodules $K_1, \ldots, K_t$ of K so that $K = K_1 \oplus \ldots \oplus K_t$. From (12.1) it is clear that

$$L = K^{\langle\pi\rangle} = K_1^{\langle\pi\rangle} \oplus \ldots \oplus K_t^{\langle\pi\rangle} \quad (\textit{as } \mathfrak{O}\langle\pi\rangle\textit{-modules}).$$

Proposition 12.10 tells us that each $K_j^{\langle\pi\rangle}$ is an indecomposable $\mathfrak{O}\langle\pi\rangle$-submodule of L. Since L' is an indecomposable $\mathfrak{O}\langle\pi\rangle$-direct summand of L, the Krull–Schmidt Theorem 9.10 implies that $L' \simeq K_j^{\pi}$ (as $\mathfrak{O}\langle\pi\rangle$-modules), for some $j = 1, \ldots, t$. Hence there is an $\mathfrak{O}\langle\pi^p\rangle$-submodule K' of L' such that $L' = (K')^{\langle\pi\rangle}$ (as $\mathfrak{O}\langle\pi\rangle$-modules). The $\mathfrak{O}$-submodule K' is invariant under $\langle\rho\rangle$, and hence is an $\mathfrak{O}(\langle\rho\rangle \times \langle\pi^p\rangle) = \mathfrak{O}\langle\sigma^p\rangle$-submodule of L'. From this and (12.1) we see easily that $L' = (K')^{\langle\sigma\rangle}$ (as $\mathfrak{O}\langle\sigma\rangle$-modules). Now Proposition 12.3 tells us that $\chi_{L'}$ is induced from the character $\chi_{K'}$ on $\langle\sigma^p\rangle$. Using (5.1), (5.4) and (5.5) we compute directly that

$$\chi_{L'}(\tau) = (\chi_{K'})^{\langle\sigma\rangle}(\tau) = \begin{cases} 0, & \text{if } \tau \in \langle\sigma\rangle \setminus \langle\sigma^p\rangle, \\ p\chi_{K'}(\tau), & \text{if } \tau \in \langle\sigma^p\rangle. \end{cases}$$

In particular, (12.12) holds. This proves the proposition.

As an application of the above proposition, we prove an orthogonality relation for the characters in a single block which should be compared with the identity (4.33) for all the characters.

For any element σ of a finite group G, we define the *p-part* σ_p and the *p'-part* $\sigma_{p'}$ of σ to be the unique elements of $\langle\sigma\rangle$ whose orders are, respectively, a power of p and relatively prime to p, and which satisfy $\sigma = \sigma_p\sigma_{p'} = \sigma_{p'}\sigma_p$.

THEOREM 12.13. *Let B_i be any block of the finite group G, and σ, τ be any two elements of G whose p-parts σ_p, τ_p are not G-conjugate. Then*

$$\sum_{\chi_j \in B_i} \chi_j(\sigma)\chi_j(\tau^{-1}) = 0. \tag{12.14}$$

Proof. The cyclic subgroup $\langle \tau \times \sigma \rangle$ of $G \times G$ acts naturally on the set G so that

$$\rho(\tau \times \sigma) = \tau^{-1} \rho \sigma \quad (\textit{for all } \rho \in G). \tag{12.15}$$

Evidently this operation makes $\mathfrak{O}G$ an $\mathfrak{O}\langle \tau \times \sigma \rangle$-lattice in the $F\langle \tau \times \sigma \rangle$-module FG.

Suppose that $\pi = (\tau \times \sigma)_p = \tau_p \times \sigma_p$ fixes an element $\rho \in G$. Then $\tau_p^{-1} \rho \sigma_p = \rho$, which implies that $\sigma_p = \rho^{-1} \tau_p \rho$. This is impossible since σ_p and τ_p are not G-conjugate. Therefore each $\langle \pi \rangle$-orbit R of G has length $p^d > 1$. It follows that R is the disjoint union of $\langle \pi^p \rangle$-orbits of the form $R = S \cup S\pi \cup \ldots \cup S\pi^{p-1}$. Hence the submodules $\mathfrak{O}R$, $\mathfrak{O}S$ generated by R, S, respectively, in $\mathfrak{O}G$, satisfy

$$\mathfrak{O}R = \mathfrak{O}S \oplus \mathfrak{O}S\pi \oplus \ldots \oplus \mathfrak{O}S\pi^{p-1} \quad (\textit{as } \mathfrak{O}\textit{-modules}).$$

Comparing with (12.1), we see that the $\mathfrak{O}\langle \pi \rangle$-module $\mathfrak{O}R$ is induced from its $\mathfrak{O}\langle \pi^p \rangle$-submodule $\mathfrak{O}S$. Since $\mathfrak{O}G$ is the direct sum of the $\mathfrak{O}R$ (as $\mathfrak{O}\langle \pi \rangle$-modules), where R runs over all the $\langle \pi \rangle$-orbits of G, we conclude that $\mathfrak{O}G$ is induced, as an $\mathfrak{O}\langle \pi \rangle$-module, from an $\mathfrak{O}\langle \pi^p \rangle$-submodule.

Because the primitive idempotents $e_1, \ldots, e_b$ all lie in the center of $Z(\mathfrak{O}G)$, we have

$$\mathfrak{O}G = e_1 \mathfrak{O}G \oplus \ldots \oplus e_b \mathfrak{O}G \quad (\textit{as two-sided } \mathfrak{O}G\textit{-modules}).$$

From (12.15) it is clear that this is also a decomposition as $\mathfrak{O}\langle \tau \times \sigma \rangle$-modules. Now all the conditions of Proposition 12.11 are satisfied with $\langle \tau \times \sigma \rangle$ as the cyclic group, $\langle \pi \rangle$ as its p-Sylow subgroup, $\mathfrak{O}G$ as the $\mathfrak{O}\langle \tau \times \sigma \rangle$-lattice L, and $e_i \mathfrak{O}G$ as its $\mathfrak{O}\langle \tau \times \sigma \rangle$-direct summand L'. Since $\tau \times \sigma \notin \langle \tau^p \times \sigma^p \rangle$, equation (12.12) implies that

$$\chi_{e_i \mathfrak{O}G}(\tau \times \sigma) = 0.$$

Evidently $e_i \mathfrak{O}G$ is an $\mathfrak{O}\langle \tau \times \sigma \rangle$-lattice in $e_i FG$. Using (11.8), (4.6) and (4.7) we see that

$$e_i FG = \bigoplus_{\chi_j \in B_i} e(\chi_j) FG = \bigoplus_{\chi_j \in B_i} A_j \quad (\textit{as two-sided } FG\textit{-modules}).$$

It follows that

$$0 = \chi_{e_i \mathfrak{O}G}(\tau \times \sigma) = \chi_{e_i FG}(\tau \times \sigma) = \sum_{\chi_j \in B_i} \chi_{A_j}(\tau \times \sigma).$$

Fix $j = 1, \ldots, k$ so that $\chi_j \in B_i$. From (4.8) and (12.15) we see that the representation of $\langle \tau \times \sigma \rangle$ on $A_j \simeq \mathrm{Hom}_F(I_j, I_j)$ is obtained by restriction from the representation $\mathrm{Hom}\,(R_j^{-1}, R_j)$ of $G \times G$ on $\mathrm{Hom}_F(I_j, I_j)$ defined by (2.15). So (2.16) tells us that $\chi_{A_j}(\tau \times \sigma) = \chi_j(\tau^{-1}) \chi_j(\sigma)$. Substituting this in the preceding equation, we obtain (12.14). Hence the theorem is proved.

Let T be any family of p-elements of G closed under inverses, i.e., $T^{-1} = T$. The *p-section* $S_p(T)$ is defined by

$$S_p(T) = \{\sigma \in G : (\sigma_p)^\tau \in T, \ \textit{for some } \tau \in G\}. \tag{12.16}$$

Clearly $S_p(T)$ is a union of conjugacy classes of G which is also closed under inverses.

As in (5.13), we denote by $CF(G|S_p(T))$ the F-vector space of all class functions from G to F which vanish outside $S_p(T)$. For each block B_i of G, let $CF(G|S_p(T), B_i)$ be the subspace of all F-linear combinations ϕ of the irreducible characters $\chi_j \in B_i$ such that $\phi = 0$ on $G\backslash S_p(T)$.

PROPOSITION 12.17. *The inner product* $(\cdot, \cdot)_G$ *of* (4.19) *is non-singular on the subspace* $CF(G|S_p(T))$ *of* $CF(G)$. *With respect to this inner product,* $CF(G|S_p(T))$ *is the perpendicular direct sum of its subspaces* $CF(G|S_p(T), B_i)$, *i.e.*

$$CF(G|S_p(T)) = \sum_{i=1}^{b} CF(G|S_p(T), B_i). \tag{12.18}$$

Proof. Let $K_1, \ldots, K_l$ be the conjugacy classes of G contained in $S_p(T)$. Since $S_p(T)$ is closed under inverses, there is an involutory permutation π of $1, \ldots, l$ such that $K_i^{-1} = K_{\pi(i)}$, for each $i = 1, \ldots, l$. The characteristic functions $\phi_1, \ldots, \phi_l$ of the classes $K_1, \ldots, K_l$, respectively, form a basis for $CF(G|S_p(T))$. In view of (4.19) we have

$$(\phi_i, \phi_{\pi(j)})_G = \begin{cases} \dfrac{|K_i|}{|G|} & \text{if } i = j, \\ 0 & \text{if } i \neq j, \end{cases}$$

for all $i, j = 1, \ldots, l$. It follows that $(\cdot, \cdot)_G$ is non-singular on $CF(G|S_p(T))$.

For any $\rho \in S_p(T)$ and any block B_i of G, we define a class function ψ_{ρ, B_i} by

$$\psi_{\rho, B_i} = \sum_{\chi_j \in B_i} \chi_j(\rho^{-1})\chi_j.$$

From (12.16), we see that ρ_p is not conjugate to τ_p, for any $\tau \in G\backslash S_p(T)$. Therefore ψ_{ρ, B_i} vanishes at all such τ by Theorem 12.13. Hence $\psi_{\rho, B_i} \in CF(G|S_p(T), B_i)$. By (4.33) the sum

$$\sum_{i=1}^{b} \psi_{\rho, B_i} = \sum_{j=1}^{k} \chi_j(\rho^{-1})\chi_j$$

is $|C_G(\rho)|$ times the characteristic function ϕ_h of the class K_h containing ρ. Since every ϕ_h can be obtained in this fashion, this proves that

$$CF(G|S_p(T)) = \sum_{i=1}^{b} CF(G|S_p(T), B_i).$$

Suppose that $\theta \in CF(G|S_p(T), B_i)$ and $\theta' \in CF(G|S_p(T), B_{i'})$, for two distinct blocks $B_i, B_{i'}$ of G. Then θ is a linear combination of the $\chi_j \in B_i$ and θ' is a linear combination of the $\chi_{j'} \in B_{i'}$. Hence $(\theta, \theta')_G$ is a linear combination of the $(\chi_j, \chi_{j'})_G$, for $\chi_j \in B_i$, $\chi_{j'} \in B_{i'}$. But all these $(\chi_j, \chi_{j'})_G$ are zero by (4.20) since $B_i \neq B_{i'}$. Therefore $CF(G|S_p(T), B_i)$ is perpendicular to

$CF(G|S_p(T), B_{i'})$, for all $i, i' = 1, \ldots, b$ with $i \neq i'$. Since $(\cdot, \cdot)_G$ is non-singular on $CF(G|S_p(T)) = \sum_{i=1}^{b} CF(G|S_p(T), B_i)$, this is enough to prove the proposition.

We use the above result to prove another orthogonality relation similar to (4.18). For any class function ϕ on G, we denote by $\phi|_{S_p(T)}$ the class function which equals ϕ on $S_p(T)$ and is zero on $G \backslash S_p(T)$.

THEOREM 12.19. *If the irreducible character χ_j belongs to the block B_i of G, then $\chi_j|_{S_p(T)} \in CF(G|S_p(T), B_i)$. If $\chi_{j'}$ is another irreducible character belonging to a different block $B_{i'}$ of G, then*

$$0 = (\chi_j|_{S_p(T)}, \chi_{j'}|_{S_p(T)})_G = \frac{1}{|G|} \sum_{\sigma \in S_p(T)} \chi_j(\sigma^{-1})\chi_{j'}(\sigma). \tag{12.20}$$

Proof. Clearly $\chi_j|_{S_p(T)} \in CF(G|S_p(T))$. If $B_{i'}$ is any block of G different from B_i, and $\theta \in CF(G|S_p(T), B_{i'})$, then $(\chi_j, \theta)_G = 0$ by (4.20), since θ is a linear combination of the irreducible characters $\chi_{j'} \in B_{i'}$, all of which are different from χ_j. Since $\theta = 0$ on $G \backslash S_p(T)$, this and (4.19) give

$$\begin{aligned} 0 = (\chi_j, \theta)_G &= \frac{1}{|G|} \sum_{\sigma \in S_p(G)} \chi_j(\sigma^{-1})\theta(\sigma) \\ &= (\chi_j|_{S_p(T)}, \theta)_G. \end{aligned}$$

Therefore $\chi_j|_{S_p(T)}$ is perpendicular to $CF(G|S_p(T), B_{i'})$, for every $i' \neq i$. In view of (12.18), this implies that $\chi_j|_{S_p(T)} \in CF(G|S_p(T), B_i)$. The rest of the theorem follows directly from this and (12.18).

13. Some Brauer Main Theorems

As in the last section, we continue to use the hypotheses and notations of Section 11.

Let P be a p-subgroup of G. We define an $\mathfrak{O}$-linear map $S = S_{1 \to P}$ of $Z(\mathfrak{O}G)$ into $\mathfrak{O}G$ by

$$S(\tilde{K}_i) = \sum_{\sigma \in K_i \cap C_G(P)} \sigma, \text{ for each class sum } \tilde{K}_i \ (i = 1, \ldots, c) \text{ of } G, \tag{13.1}$$

where an empty sum is understood to be zero.

PROPOSITION 13.2. *If H is a subgroup of G satisfying $C_G(P) \leq H \leq N_G(P)$, then $S(Z(\mathfrak{O}G)) \subseteq Z(\mathfrak{O}H)$. Furthermore,*

$$S(\tilde{K}_i)S(\tilde{K}_j) \equiv S(\tilde{K}_i\tilde{K}_j) \pmod{pZ(\mathfrak{O}H)} \quad (i, j = 1, \ldots, c). \tag{13.3}$$

Proof. Since $C_G(P)$ is a normal subgroup of H and K_i is invariant under H-conjugation, the intersection $K_i \cap C_G(P)$ is H-invariant, $(i = 1, \ldots, c)$.

Hence its sum $S(\tilde{K}_i)$ lies in $Z(\mathfrak{O}H)$. This proves the first statement of the proposition.

For the second, let ρ be any element of H. We must prove that the coefficient x of ρ in the product $S(\tilde{K}_i)S(\tilde{K}_j)$ is congruent to the coefficient y of ρ in $S(\tilde{K}_i\tilde{K}_j)$ modulo p when both products are written as linear combinations of elements of H. Since $S(\tilde{K}_i)$ and $S(\tilde{K}_j)$ both lie in $\mathfrak{O}C_G(P)$, so does $S(\tilde{K}_i)S(\tilde{K}_j)$. Therefore $x = 0$ for $\rho \notin C_G(P)$. In that case y is also zero by (13.1). Hence the result is true for $\rho \notin C_G(P)$.

Now suppose that $\rho \in C_G(P)$. From Proposition 4.28 and (13.1) it is clear that y is the number of elements in the set T of all ordered pairs (σ, τ) such that $\sigma \in K_i$, $\tau \in K_j$ and $\sigma\tau = \rho$. Because P centralizes ρ, it operates naturally on T by conjugation

$$(\sigma, \tau) \in T,\ \pi \in P \to (\sigma, \tau)^\pi = (\sigma^\pi, \tau^\pi) \in T.$$

Let T_1 be the subset of all elements of T fixed by P. Evidently $(\sigma, \tau) \in T_1$ if and only if $\sigma \in K_i \cap C_G(P)$, $\tau \in K_j \cap C_G(P)$ and $\sigma\tau = \rho$. In view of (13.1), the coefficient x of ρ in $S(\tilde{K}_i)S(\tilde{K}_j)$ is precisely the order of T_1. But every P-orbit of $T \backslash T_1$ has length divisible by p, since P is a p-group. Therefore $x = |T_1| \equiv |T| = y \pmod{p}$, and the proposition is proved.

COROLLARY 13.4. *The map S induces an identity-preserving $\mathfrak{O}$-algebra homomorphism of $Z(\mathfrak{O}G)/pZ(\mathfrak{O}G)$ into $Z(\mathfrak{O}H)/pZ(\mathfrak{O}H)$.*

Proof. This follows directly from the proposition and the observation that $S(1_G) = 1_H$.

Let $\hat{B}$ be a block of H. By Proposition 11.15 there is a unique $\mathfrak{O}$-algebra epimorphism $\eta_{\hat{B}} : Z(\mathfrak{O}H) \to \bar{F}$ lying in B. Clearly $\eta_{\hat{B}}$ is zero on $pZ(\mathfrak{O}H)$. So Corollary 13.4 implies that the composition $\eta_{\hat{B}} \circ S$ is an $\mathfrak{O}$-algebra epimorphism of $Z(\mathfrak{O}G)$ onto $\bar{F} = \mathfrak{O} \cdot 1_F$. We denote by $\hat{B}^G$ the unique block of G having $\eta_{\hat{B}} \circ S$ as its $\mathfrak{O}$-algebra epimorphism $Z(\mathfrak{O}G) \to \bar{F}$, i.e., satisfying

$$\eta_{\hat{B}^G} = \eta_{\hat{B}} \circ S. \tag{13.5}$$

There is another way of considering the relation between $\hat{B}$ and $\hat{B}^G$. For any block $\hat{B}$ of H, let $e_{\hat{B}}$ be the corresponding primitive idempotent of $Z(\mathfrak{O}H)$. Define $e_B \in Z(\mathfrak{O}G)$ similarly, for any block B of G. Then we have

PROPOSITION 13.6. *If H is any subgroup of G satisfying $C_G(P) \leq H \leq N_G(P)$ and if B is any block of G, then*

$$S(e_B) \equiv \sum e_{\hat{B}} \pmod{pZ(\mathfrak{O}H)}, \tag{13.7}$$

summed over all blocks $\hat{B}$ of H such that $\hat{B}^G = B$.

Proof. Since (8.11) holds for $Z(\mathfrak{O}H)$, Proposition 9.13 implies that the primitive idempotents of $Z(\mathfrak{O}H)/pZ(\mathfrak{O}H)$ are precisely the images of the primitive idempotents $e_{\hat{B}}$ of $Z(\mathfrak{O}H)$. By Corollary 13.4 the image of $S(e_B)$ is

an idempotent in $Z(\mathfrak{O}H)/pZ(\mathfrak{O}H)$. So Proposition 9.11 gives us a unique set T of blocks of H such that

$$S(e_B) \equiv \sum_{\hat{B} \in T} e_{\hat{B}} \pmod{pZ(\mathfrak{O}H)}.$$

Suppose that $\hat{B} \in T$. From (11.8) for H we see that $\eta_{\hat{B}} \circ S(e_B) = 1_F$. Hence $\eta_{\hat{B}} \circ S = \eta_B$, by (11.18) for G, and $B = \hat{B}^G$. If $\hat{B}$ is a block of H not in T, then $\eta_{\hat{B}} \circ S(e_B) = 0$ by (11.18) for H. Therefore $\eta_{\hat{B}} \circ S \neq \eta_B$, by (11.18) for G. So T is precisely the set of all blocks $\hat{B}$ of H such that $B = \hat{B}^G$, and the proposition is proved.

For Brauer's second main theorem we need a simple criterion (due to D. Higman) telling us when we can apply Proposition 12.11.

LEMMA 13.8. *Let $\langle\pi\rangle$ be a non-trivial cyclic p-group, and L be an $\mathfrak{O}\langle\pi\rangle$-module. Suppose there is an $\mathfrak{O}\langle\pi^p\rangle$-endomorphism $\phi : l \to l\phi$ of L satisfying*

$$1_{L \to L} = \phi + \pi^{-1}\phi\pi + \ldots + \pi^{-(p-1)}\phi\pi^{(p-1)}. \tag{13.9}$$

Then there is an $\mathfrak{O}\langle\pi^p\rangle$-submodule K such that $L = K^{\langle\pi\rangle}$.

Proof. Form an $\mathfrak{O}\langle\pi\rangle$-module L^* having L as an $\mathfrak{O}\langle\pi^p\rangle$- (but *not* $\mathfrak{O}\langle\pi\rangle$-) submodule so that $L^* = L^{\langle\pi\rangle}$. We write the module product in L^* with * to distinguish it from that in L. Then (12.1) gives

$$L^* = L \oplus L*\pi \oplus \ldots \oplus L*\pi^{p-1} \quad (\textit{as } \mathfrak{O}\textit{-modules}).$$

Let $\psi : L \to L^*$ be the map:

$$l \to l\psi = l\phi \oplus l\pi^{-1}\phi*\pi \oplus \ldots \oplus l\pi^{-(p-1)}\phi*\pi^{p-1}.$$

Using (12.2), we easily compute that ψ is an $\mathfrak{O}\langle\pi\rangle$-homomorphism of L into L^*. Similarly the map $\xi : L^* \to L$ defined by

$$l_0 \oplus l_1*\pi \oplus \ldots \oplus l_{p-1}*\pi^{p-1} \to l_0 + l_1\pi + \ldots + l_{p-1}\pi^{p-1},$$
$$\textit{for all } l_0, l_1, \ldots, l_{p-1} \in L,$$

is an $\mathfrak{O}\langle\pi\rangle$-homomorphism of L^* into L. Condition (13.9) says that $\psi\xi$ is the identity on L. Hence ψ is an $\mathfrak{O}\langle\pi\rangle$-monomorphism and $L^* = \psi(L) \oplus \operatorname{Ker}\xi$ (as $\mathfrak{O}\langle\pi\rangle$-modules).

Because the $\mathfrak{O}\langle\pi\rangle$-module L^* is induced from its $\mathfrak{O}\langle\pi^p\rangle$-submodule L, Proposition 12.10 and the Krull–Schmidt Theorem 9.10 imply that every $\mathfrak{O}\langle\pi\rangle$-direct summand of L is induced from one of its $\mathfrak{O}\langle\pi^p\rangle$-submodules. We have just seen that L is $\mathfrak{O}\langle\pi\rangle$-isomorphic to such an $\mathfrak{O}\langle\pi\rangle$-direct summand $\psi(L)$. Therefore the lemma holds.

To state the following theorem, we choose P to be a non-trivial cyclic p-subgroup $\langle\pi\rangle$ of G. If χ_j is any irreducible character of G, then its restriction $(\chi_j)_{C_G(\pi)}$ is a character of $C_G(\pi) = C_G(P)$, and hence a linear combination of the irreducible characters of that group. Since these are partitioned

among the blocks $\hat{B}$ of $C_G(\pi)$, we have a unique decomposition

$$(\chi_j)_{C_G(\pi)} = \sum_{\hat{B}} \chi_{j,\hat{B}}, \tag{13.10}$$

where each $\chi_{j,\hat{B}}$ is a linear combination of the irreducible characters in the block $\hat{B}$ of $C_G(\pi)$.

With this notation we have

THEOREM 13.11 (Brauer's second main theorem). *Let the irreducible character χ_j lie in the block B of G. If ρ is a p'-element of $C_G(\pi)$, then:*

$$\chi_j(\pi\rho) = \sum_{\hat{B}^G = B} \chi_{j,\hat{B}}(\pi\rho). \tag{13.12}$$

Proof. (Nagao). As in Proposition 13.6, let e_B be the primitive central idempotent of $Z(\mathfrak{O}G)$ lying in B. Let e be the idempotent $\sum_{\hat{B}^G = B} e_{\hat{B}}$ of $Z(\mathfrak{O}C_G(\pi))$. Choose any $\mathfrak{O}G$-lattice L in the irreducible FG-module I_j corresponding to χ_j. Then $L = L(1-e) \oplus Le$ (as $\mathfrak{O}C_G(\pi)$-modules). Evidently $\sum_{\hat{B}^G = B} \chi_{j,\hat{B}}$ is the character χ_{Le} of Le. So (13.10) implies that (13.12) is equivalent to

$$\chi_{L(1-e)}(\pi\rho) = 0. \tag{13.13}$$

Let K_i be any class of G. Then $K_i \backslash (K_i \cap C_G(\pi))$ is a union of $\langle\pi\rangle$-orbits, each of which has length p^n, for some $n > 0$. It follows that there is a $\langle\pi^p\rangle$-invariant subset H_i of $K_i \backslash (K_i \cap C_G(\pi))$, such that the latter set is the disjoint union of the conjugates $H_i, H_i^{\pi}, \ldots, H_i^{\pi^{p-1}}$ of H_i. Writing $\tilde{H}_i$ for the sum of the elements of H_i, we obtain

$$\tilde{K}_i - S(\tilde{K}_i) = \tilde{H}_i + \pi^{-1}\tilde{H}_i\pi + \ldots + \pi^{-(p-1)}\tilde{H}_i\pi^{p-1} \quad (i = 1, \ldots, c).$$

Write $e_B = \sum_{i=1}^{c} a_i K_i$, with coefficients $a_i \in \mathfrak{O}$. Then $S(e_B) = \sum_{i=1}^{c} a_i S(\tilde{K}_i)$. By (13.7) the difference $S(e_B) - e$ has the form

$$S(e_B) - e = px = x + \pi^{-1}x\pi + \ldots + \pi^{-(p-1)}x\pi^{p-1},$$

for some $x \in Z(\mathfrak{O}C_G(\pi))$. We conclude that

$$\begin{aligned} e_B &= (e_B - S(e_B)) + (S(e_B) - e) + e \\ &= \sum_{i=1}^{c} a_i(\tilde{K}_i - S(\tilde{K}_i)) + px + e \\ &= y + \pi^{-1}y\pi + \ldots + \pi^{-(p-1)}y\pi^{p-1} + e, \end{aligned}$$

where

$$y = \left(\sum_{i=1}^{c} a_i \tilde{H}_i\right) + x$$

is an element of $\mathfrak{O}G$ commuting with π^p. Since e is an idempotent commuting with π, this implies that

$$e_B(1-e) = y(1-e) + \pi^{-1}y(1-e)\pi + \ldots + \pi^{-(p-1)}y(1-e)\pi^{p-1}.$$

Because χ_j lies in the block B, the idempotent e_B acts as identity on I_j. It follows that $e_B(1-e)$ acts as identity on $L(1-e)$. Since L is an $\mathfrak{O}G$-module and $y(1-e) \in \mathfrak{O}G$ commutes with π^p, the map $\phi : l \to \phi = ly(1-e)$ is an $\mathfrak{O}\langle\pi^p\rangle$-endomorphism of $L(1-e)$. The above equation now tells us that $\langle\pi\rangle$, $L(1-e)$, and ϕ satisfy the hypotheses of Lemma 13.8. Hence there is an $\mathfrak{O}\langle\pi^p\rangle$-submodule K such that $L(1-e) = K^{\langle\pi\rangle}$.

Since ρ is a p'-element centralizing π, the group $\langle\pi\rangle$ is a p-Sylow subgroup of the cyclic group $\langle\pi\rho\rangle$. Now we can apply Proposition 12.11 to $\langle\pi\rho\rangle$, $\langle\pi\rangle$, $I_j(1-e)$, $L(1-e)$ and K, with $L(1-e)$ in the role of both L and L'. From (12.12) we conclude that (13.13) holds. So the theorem is proved.

To make the most effective use of Brauer's second main theorem we need Brauer's "third main theorem" which tells us that prinicipal blocks correspond only to principal blocks in the relation $\hat{B}^G = B$. The *principal block* of a group G is the block containing the trivial character 1 of G. We shall denote this block by $B_0(G)$. In view of Proposition 11.15 and equation (4.30), the corresponding $\mathfrak{O}$-epimorphism $\eta_{B_0(G)}$ of $Z(\mathfrak{O}G)$ onto $\bar{F}$ is given by

$$\eta_{B_0(G)}(\tilde{K}_i) = |K_i| \cdot 1_F, \quad \textit{for all classes } K_i \textit{ of } G. \tag{13.14}$$

As you might expect, we have

PROPOSITION 13.15. *If P is a p-subgroup of G and $C_G(P) \leq H \leq N_G(P)$ then $B_0(H)^G = B_0(G)$.*

Proof. Let K_i be any class of G. Letting P operate by conjugation on K_i, we see that the non-trivial P-orbits form the subset $K_i \backslash (K_i \cap C_G(P))$, whose order is divisible by p. From (13.1), (13.5) and (13.14) we obtain

$$\begin{aligned} \eta_{B_0(H)^G}(\tilde{K}_i) &= \eta_{B_0(H)}(S(\tilde{K}_i)) = |K_i \cap C_G(P)| \cdot 1_F \\ &= |K_i| \cdot 1_F = \eta_{B_0(G)}(\tilde{K}_i) \quad (i = 1 \ldots, c), \end{aligned}$$

since $\bar{F}$ has characteristic p. This proves the proposition.

The difficult thing is to show that the converse to Proposition 13.15 holds whenever H contains $PC_G(P)$. In that case any block $\hat{B}$ of H satisfying $\hat{B}^G = B_0(G)$ must be equal to $B_0(H)$. The proof of this, which is Brauer's third main theorem, is rather roundabout.

We start with the study of defect groups. A *defect group* $D(K_i) = D_G(K_i)$ of a conjugacy class K_i of G is any p-Sylow subgroup of the centralizer $C_G(\sigma)$ of any element $\sigma \in K_i$. Evidently $D(K_i)$ is a p-subgroup of G determined up to G-conjugation by the class K_i.

In order to talk about conjugacy classes of subgroups of G, we adopt the notation $D_1 \lesssim D_2$ (or $D_1 \lesssim_G D_2$) to mean that D_1 and D_2 are subgroups of G and that D_1 is G-conjugate to a subgroup of D_2. Evidently $\lesssim$ is a partial ordering on the subgroups of G. Two subgroups D_1, D_2 are equivalent for

this partial ordering if and only if they are conjugate in G, in which case we write $D_1 \sim D_2$ (or $D_1 \sim_G D_2$).

LEMMA 13.16. *Let a_{ijh} be the integers satisfying*

$$\tilde{K}_i\tilde{K}_j = \sum_{h=1}^{c} a_{ijh}\tilde{K}_h, \quad \text{for all } i, j = 1, \ldots, c.$$

If $a_{ijh} \not\equiv 0 \pmod{p}$, for some i, j, h, then $D(K_h) \lesssim D(K_i)$ and $D(K_h) \lesssim D(K_j)$.

Proof. Pick $\rho \in K_h$. We know from Proposition 4.28 that a_{ijh} is the number of elements in the set $T = \{(\sigma, \tau) : \sigma \in K_i, \ \tau \in K_j, \ \sigma\tau = \rho\}$. Choose the defect group $D(K_h)$ to be a p-Sylow subgroup of $C_G(\rho)$. Then $D(K_h)$ operates by conjugation on the set T of ordered pairs (σ, τ). If $a_{ijh} = |T| \not\equiv 0 \pmod{p}$, then there must be a $(\sigma, \tau) \in T$ fixed by the p-group $D(K_h)$. Then $D(K_h)$ is a p-subgroup of both $C_G(\sigma)$ and $C_G(\tau)$, and hence is contained in p-Sylow subgroups of these two groups, which we may take to be $D(K_i)$ and $D(K_j)$, respectively. So the lemma holds.

With the aid of the above lemma we can define defect groups of blocks.

PROPOSITION 13.17. *Let B be a block of G, and η be the corresponding $\mathfrak{O}$-algebra epimorphism of $Z(\mathfrak{O}G)$ onto $\bar{F}$. Then there is a unique G-conjugacy class of p-subgroups $D(B)$ of G satisfying*

There exists a conjugacy class K_i such that $D(B) \sim D(K_i)$ and

$$\eta_B(\tilde{K}_i) \neq 0. \tag{13.18a}$$

If K_j is any conjugacy class of G such that $\eta_B(\tilde{K}_j) \neq 0$,

$$\text{then } D(B) \lesssim D(K_j). \tag{13.18b}$$

Proof. Choose $D(B)$ among the minimal elements for the partial ordering $\lesssim$ on the set of all defect groups of all classes K_j such $\eta_B(\tilde{K}_j) \neq 0$. Then there exists a class K_i such that $D(B) \sim D(K_i)$ and $\eta_B(\tilde{K}_i) \neq 0$. If K_j is any class of G such that $\eta_B(\tilde{K}_j) \neq 0$, then $\eta_B(\tilde{K}_i\tilde{K}_j) = \eta_B(\tilde{K}_i)\eta_B(\tilde{K}_j) \neq 0$ in the field $\bar{F}$. In the notation of Lemma 13.16 we have

$$0 \neq \eta_B(\tilde{K}_i\tilde{K}_j) = \sum_{h=1}^{c} a_{ijh}\eta_B(\tilde{K}_h).$$

So there must exist an $h = 1, \ldots, c$ such that $\eta_B(\tilde{K}_h) \neq 0$ and $a_{ijh} \not\equiv 0 \pmod{p}$. From Lemma 13.16 we obtain $D(K_h) \lesssim D(K_i) \sim D(B)$. The minimality of $D(B)$ forces $D(K_h) \sim D(B)$. But then Lemma 13.16 again tells us that $D(B) \sim D(K_h) \lesssim D(K_j)$. Therefore $D(B)$ satisfies (13.18). Evidently the properties (13.18) determine $D(B)$ to within conjugation. So the proposition is proved.

The groups $D(B)$ are called the *defect groups* of the block B. When η_B is known, they are, of course, very easy to calculate. For example, (13.14) implies that $\eta_{B_0(G)}(\tilde{K}_i) \neq 0$ if and only if p does not divide $|K_i|$, i.e., if and

only if $D(K_i)$ is a p-Sylow subgroup of G. Hence,

$$D(B_0(G)) \text{ is a } p\text{-Sylow subgroup of } G. \tag{13.19}$$

To obtain a different characterization of the defect groups of a block we shall use

LEMMA 13.20. *Let A be an $\mathfrak{O}$-sub algebra (with or without identity) of $Z(\mathfrak{O}G)$, and λ be an $\mathfrak{O}$-algebra epimorphism of A onto $\bar{F}$. Then there is an $\mathfrak{O}$-algebra epimorphism η of $Z(\mathfrak{O}G)$ onto $\bar{F}$ whose restriction to A is λ.*

Proof. By Proposition 11.15 and (11.11) the $\mathfrak{O}$-algebra epimorphisms $\eta_1, \ldots, \eta_b$ of $Z(\mathfrak{O}G)$ onto $\bar{F}$ satisfy $\operatorname{Ker}\eta_1 \cap \ldots \cap \operatorname{Ker}\eta_b = J(Z(\mathfrak{O}G))$. By (8.12) there is an integer $t > 0$ such that $J(Z(\mathfrak{O}G))^t \subseteq pZ(\mathfrak{O}G)$. Since A is a $\mathbf{Z}_p$-submodule of the finitely-generated $\mathbf{Z}_p$-module $Z(\mathfrak{O}G)$, there is an integer $s > 0$ such that $p^sZ(\mathfrak{O}G) \cap A \subseteq pA \subseteq \operatorname{Ker}\lambda$. It follows that $A \cap \operatorname{Ker}\eta_1, \ldots, A \cap \operatorname{Ker}\eta_b$ are ideals of A satisfying

$$\begin{aligned}[(A \cap \operatorname{Ker}\eta_1)\ldots(A \cap \operatorname{Ker}\eta_b)]^{st} &\subseteq A \cap [(\operatorname{Ker}\eta_1)\ldots(\operatorname{Ker}\eta_b)]^{st} \\ &\subseteq A \cap [(\operatorname{Ker}\eta_1 \cap \ldots \cap \operatorname{Ker}\eta_b)]^{st} \\ &= A \cap J(Z(\mathfrak{O}G))^{st} \\ &\subseteq A \cap p^sZ(\mathfrak{O}G) \subseteq pA \subseteq \operatorname{Ker}\lambda.\end{aligned}$$

Since λ is an epimorphism of A onto a field $\bar{F}$, we conclude that $A \cap \operatorname{Ker}\eta_i \subseteq \operatorname{Ker}\lambda$, for some $i = 1, \ldots, b$. But then λ is the restriction to A of an $\mathfrak{O}$-algebra epimorphism η of $A + \operatorname{Ker}\eta_i$ onto $\bar{F}$ such that $\operatorname{Ker}\eta_i \subseteq \operatorname{Ker}\eta$. Since

$$\operatorname{Ker}\eta_i \subseteq \operatorname{Ker}\eta \subset A + \operatorname{Ker}\eta_i \subseteq Z(\mathfrak{O}G),$$

and $Z(\mathfrak{O}G)/\operatorname{Ker}\eta_i \simeq \bar{F}$ (as $\mathfrak{O}$-algebras), we must have $\operatorname{Ker}\eta = \operatorname{Ker}\eta_i$, $A + \operatorname{Ker}\eta_i = Z(\mathfrak{O}G)$, and $\eta = \eta_i$. Therefore the lemma holds.

The other characterization of the defect groups of a block B is as the largest groups P, in the partial ordering $\lesssim$, from which B can be obtained via (13.5).

PROPOSITION 13.21. *Let P be a p-subgroup of G, H be any subgroup satisfying $C_G(P) \leq H \leq N_G(P)$, and B be a block of G. Then there exists a block $\hat{B}$ of H such that $\hat{B}^G = B$ if and only if $P \lesssim D(B)$.*

Proof. Suppose such a block $\hat{B}$ exists. Then the $\mathfrak{O}$-algebra epimorphism $\eta_{\hat{B}}$ of $Z(\mathfrak{O}H)$ onto $\bar{F}$ lying in $\hat{B}$ defines the corresponding epimorphism $\eta_B : Z(\mathfrak{O}G) \to \bar{F}$ by (13.5). From (13.1) it is clear that $S(\tilde{K}_i) = 0$, for all classes K_i of G such that $P \not\lesssim D(K_i)$. Hence $\eta_B(\tilde{K}_i) = \eta_B(S(\tilde{K}_i)) = 0$, for all such K_i. In view of (13.18*a*), this implies that $P \lesssim D(B)$.

Now suppose that $P \lesssim D(B)$. From (13.18*b*) we see that $\eta_B(K_i) = 0$, for all classes K_i of G such that $P \not\lesssim D(K_i)$. But the kernel of $S : Z(\mathfrak{O}G) \to Z(\mathfrak{O}H)$

is precisely the $\mathfrak{O}$-linear span of the sums $\tilde{K}_i$ of these classes (by 13.1). Hence there is a unique $\mathfrak{O}$-linear map λ_1 of the image $S(Z(\mathfrak{O}G))$ into $\bar{F}$ such that $\eta_B = \lambda_1 \circ S$. It is clear from (13.1) that $S(pZ(\mathfrak{O}G)) = pS(Z(\mathfrak{O}G)) = pZ(\mathfrak{O}H) \cap S(Z(\mathfrak{O}G))$. Since η_B is zero on $pZ(\mathfrak{O}G)$, the map λ_1 is zero on $pS(Z(\mathfrak{O}G))$. So it has a unique extension to an $\mathfrak{O}$-linear map λ of $A = pZ(\mathfrak{O}H) + S(Z(\mathfrak{O}G))$ onto $\bar{F}$ such that $\lambda(pZ(\mathfrak{O}H)) = 0$. In view of Corollary 13.4, A is an $\mathfrak{O}$-subalgebra of $Z(\mathfrak{O}H)$ and λ is an $\mathfrak{O}$-algebra epimorphism. Lemma 13.20 now gives us an $\mathfrak{O}$-algebra epimorphism $\eta : Z(\mathfrak{O}H) \to \bar{F}$ whose restriction to A is λ. Then $\eta \circ S = \lambda \circ S = \lambda_1 \circ S = \eta_B$, and $\hat{B}^G = B$, where $\hat{B}$ is the block of H corresponding to η in Proposition 11.15. This proves the proposition.

We need some information about the blocks of a group H having a normal p-subgroup P. Let ϕ be the $\mathfrak{O}$-algebra epimorphism of $\mathfrak{O}H$ onto $\mathfrak{O}(H/P)$ induced by the natural group epimorphism $H \to H/P$. Then the restriction of ϕ is an $\mathfrak{O}$-algebra homomorphism of $Z(\mathfrak{O}H)$ into $Z(\mathfrak{O}(H/P))$.

LEMMA 13.22. *If $\hat{B}$ is a block of H, then there exists a block B of H/P such that $\eta_B = \eta_{\hat{B}} \circ \phi$.*

Proof. Let Aug $(\mathfrak{O}P)$ be the *augmentation ideal* of $\mathfrak{O}P$, having the elements $\sigma - 1$, for $\sigma \in P - \{1\}$, as $\mathfrak{O}$-basis. Proposition 11.23 implies that Aug $(\mathfrak{O}P) \subseteq J(\mathfrak{O}P)$. So (8.12) gives us an integer $d > 0$ such that $[\text{Aug}\,(\mathfrak{O}P)]^d \subseteq p\mathfrak{O}P$. Evidently the kernel of ϕ is Ker $\phi = \text{Aug}\,(\mathfrak{O}P)\cdot\mathfrak{O}H = \mathfrak{O}H\cdot\text{Aug}\,(\mathfrak{O}P)$. Hence,

$$(\text{Ker}\,\phi)^d = [\text{Aug}\,(\mathfrak{O}P)]^d \cdot \mathfrak{O}H \subseteq p\mathfrak{O}H.$$

It follows that Ker $\phi \cap Z(\mathfrak{O}H)$, the kernel of the restriction of ϕ to $Z(\mathfrak{O}H)$, is an ideal of $Z(\mathfrak{O}H)$ which is nilpotent modulo $pZ(\mathfrak{O}H)$. This implies that Ker $\phi \cap Z(\mathfrak{O}H) \subseteq$ Ker $\eta_{\hat{B}}$. So there is a unique $\mathfrak{O}$-algebra epimorphism λ of $A = \phi(Z(\mathfrak{O}H))$ onto $\bar{F}$ such that $\eta_{\hat{B}} = \lambda \circ \phi$. Applying Lemma 13.20, we obtain an $\mathfrak{O}$-algebra epimorphism η of $Z(\mathfrak{O}(H/P))$ onto $\bar{F}$ whose restriction to A is λ. By Proposition 11.15, $\eta = \eta_B$, for a block B of H/P. We have proved the lemma.

COROLLARY 13.23. *If K is a conjugacy class of H lying in $H \setminus C_H(P)$ then $\eta_{\hat{B}}$ vanishes on the corresponding class sum $\tilde{K}$. Hence $P \leq D(\hat{B})$.*

Proof. Let σ be an element of K, and $C_H(\phi(\sigma))$ be the inverse image in H of $C_{H/P}(\phi(\sigma))$. Then the image in H/P of the class K of σ is the class L of $\phi(\sigma)$. But the corresponding class sums $\tilde{K}$ and $\tilde{L}$ are related by

$$\phi(\tilde{K}) = [C_H(\phi(\sigma)) : C_H(\sigma)]\tilde{L},$$

since $[C_H(\phi(\sigma)) : C_H(\sigma)]$ members of K map onto each member of L. Evidently $C_H(\phi(\sigma))$ contains $PC_H(\sigma)$. Therefore $[C_H(\phi(\sigma)) : C_H(\sigma)]$ is

divisible by $[PC_H(\sigma) : C_H(\sigma)] = [P : C_P(\sigma)] = p^s$, for some $s \geq 1$, since P does not centralize σ. It follows that $\phi(\tilde{K}) \in pZ(\mathfrak{O}(H/P))$, and hence that $\eta_{\hat{B}}(\tilde{K}) = \eta_B \circ \phi(\tilde{K}) = 0$ in $\bar{F}$, which is the first conclusion of the corollary. The second conclusion comes from the first and the definition (13.18) of $D(\hat{B})$.

Since P is a normal subgroup of H, so is $C_H(P)$. Hence H acts by conjugation as $\mathfrak{O}$-algebra automorphisms of $Z(\mathfrak{O}C_H(P))$. It follows that H permutes the $\mathfrak{O}$-algebra epimorphisms $\eta : Z(\mathfrak{O}C_H(P)) \to \bar{F}$ among themselves by conjugation:

$$\eta^\sigma(y) = \eta(y^{\sigma^{-1}}), \quad \textit{for all } \sigma \in H,\ y \in Z(\mathfrak{O}C_H(P)). \tag{13.24}$$

Applying Proposition 11.15, we obtain a natural action of H on the corresponding blocks of $C_H(P)$.

PROPOSITION 13.25. *There is a one-to-one correspondence between blocks $\hat{B}$ of H and H-conjugacy classes of blocks $\bar{B}$ of $C_H(P)$. The block $\hat{B}$ corresponds to the class of $\bar{B}$ if and only if the corresponding $\mathfrak{O}$-algebra epimorphisms $\eta_B : Z(\mathfrak{O}H) \to \bar{F}$ and $\eta_{\bar{B}} : Z(\mathfrak{O}C_H(P)) \to \bar{F}$ have the same restriction to $Z(\mathfrak{O}H) \cap Z(\mathfrak{O}C_H(P))$.*

Proof. For each block $\hat{B}$ of H, let $T(\hat{B})$ be the family of all blocks $\bar{B}$ of $C_H(P)$ such that $\eta_{\hat{B}}$ and $\eta_{\bar{B}}$ have the same restriction to $A = Z(\mathfrak{O}H) \cap Z(\mathfrak{O}C_H(P))$. Since $1 \in A$, the restriction λ of $\eta_{\hat{B}}$ is an $\mathfrak{O}$-algebra epimorphism of A onto $\bar{F}$. So Lemma 13.20 and Proposition 11.15 imply that $T(\hat{B})$ is not empty. Because each element of A is fixed under conjugation by elements of H, it follows from (13.24) that $T(\hat{B})$ is an H-invariant set of blocks of $C_H(P)$.

Let $\bar{B}_1, \ldots, \bar{B}_s$ be an H-orbit in $T(\hat{B})$, and $e_1, \ldots, e_s$ be the corresponding primitive idempotents of $Z(\mathfrak{O}C_H(P))$. Evidently $e_1, \ldots, e_s$ is an H-conjugacy class of primitive idempotents of $Z(\mathfrak{O}C_H(P))$. So $e_1 + \ldots + e_s$ is invariant under H, and hence lies in A. From (11.18) we see that $\lambda(e_1 + \ldots + e_s) = \eta_{\bar{B}_1}(e_1 + \ldots + e_s) = 1$. If $\bar{B}$ is any other block of $C_H(P)$, then (11.18) gives $\eta_{\bar{B}}(e_1 + \ldots + e_s) = 0 \neq \lambda(e_1 + \ldots + e_s)$. Therefore $\bar{B}$ does not lie in $T(\hat{B})$. Hence $T(\hat{B}) = \{\bar{B}_1 \ldots, \bar{B}_s\}$ is an H-conjugacy class of blocks of $C_H(P)$.

If $\bar{B}$ is any block of $C_H(P)$, then the restriction λ of $\eta_{\bar{B}}$ to A is an $\mathfrak{O}$-algebra epimorphism of A onto $\bar{F}$, and hence is the restriction to A of $\eta_{\hat{B}}$, for some block $\hat{B}$ of H, by Lemma 13.20 and Proposition 11.15. Therefore $\bar{B} \in T(\hat{B})$, for some block $\hat{B}$ of H.

Corollary 13.23 implies that $\eta_{\hat{B}}$ is determined by its restriction to $Z(\mathfrak{O}H) \cap \mathfrak{O}C_H(P) = A$, for any block $\hat{B}$ of H. Hence $\hat{B}$ is determined by $T(\hat{B})$. We have shown that $\hat{B} \leftrightarrow T(\hat{B})$ is a one to one correspondence between blocks of H and H-conjugacy classes of blocks of $C_H(P)$. That is the proposition.

We need one more lemma.

LEMMA 13.26. *Let P be a p-subgroup of the group G. Then the map $K_i \to K_i \cap C_G(P)$ sends the family of all conjugacy classes K_i of G such that $P \sim D_G(K_i)$ one to one onto the family of all conjugacy classes L_j of $N_G(P)$ such that $P = D_{N_G(P)}(L_j)$.*

Proof. If P is a defect group of a conjugacy class K_i of G, then K_i contains some element σ having P as a Sylow subgroup of its centralizer $C_G(\sigma)$. Hence $\sigma \in K_i \cap C_G(P)$. Therefore $K_i \cap C_G(P)$ is not empty.

If τ is another element of $K_i \cap C_G(P)$, then $\tau = \sigma^\rho$, for some $\rho \in G$. Evidently both P and P^ρ are p-Sylow subgroups of $C_G(\tau)$. Hence there exists $\pi \in C_G(\tau)$ such that $P^{\rho\pi} = P$. Now $\rho\pi$ is an element of $N_G(P)$ satisfying $\sigma^{\rho\pi} = \tau^\pi = \tau$. We conclude that $K_i \cap C_G(P)$ is a conjugacy class of $N_G(P)$. Because P is a p-Sylow subgroup of $C_{N_G(P)}(\sigma)$, the defect group $D_{N_G(P)}(K_i \cap C_G(P))$ is precisely P.

Now let L_j be any conjugacy class of $N_G(P)$ such that $P = D_{N_G(P)}(L_j)$, and let K_i be the conjugacy class of G containing L_j. Evidently $L_j \subseteq K_i \cap C_G(P)$. Pick an element $\sigma \in L_j$. Let D be a p-Sylow subgroup of $C_G(\sigma)$ containing P. If $P < D$, then $P < N_D(P) \leq C_{N_G(P)}(\sigma)$, which is impossible since P is a p-Sylow subgroup of $C_{N_G(P)}(\sigma)$. Hence $P = D \sim D(K_i)$. Because $K_i \cap C_G(P)$ is a class of $N_G(P)$, we have $L_j = K_i \cap C_G(P)$. The map $K_i \to K_i \cap C_G(P)$ being clearly one-to-one, this is enough to prove the lemma.

At last we have

THEOREM 13.27 (Brauer's third main theorem). *Suppose that P is a p-subgroup of G, and that H is a subgroup satisfying $PC_G(P) \leq H \leq N_G(P)$. If $\hat{B}$ is a block of H, then $\hat{B}^G = B_0(G)$, if and only if $\hat{B} = B_0(H)$.*

Proof. We already know that $\hat{B} = B_0(H)$ implies $\hat{B}^G = B_0(G)$, by Proposition 13.15. So it is only necessary to prove the converse. Choose a counterexample P, H, $\hat{B}$ with $|P|$ maximal. We must first show that we can assume $H = N_G(P)$.

Since P is a normal subgroup of H and $C_G(P) = C_H(P)$, Proposition 13.25 tells us that $\hat{B}$ and $B_0(H) \neq \hat{B}$ correspond to distinct H-conjugacy classes of blocks of $C_G(P)$. It is evident from (13.14) that $B_0(H)$ corresponds to the H-conjugacy class containing $B_0(C_G(P))$. Let $\bar{B} \neq B_0(C_G(P))$ be a block of $C_G(P)$ in the H-conjugacy class corresponding to $\hat{B}$. It follows from (13.14) that $B_0(C_G(P))$ is $N_G(P)$-invariant. So the block $\hat{B}_1$ of $N_G(P)$ corresponding to the $N_G(P)$-class of $\bar{B}$ in Proposition 13.25 is different from $B_0(N_G(P))$. But $\eta_{\hat{B}_1}$, $\eta_{\bar{B}}$ and $\eta_{\hat{B}}$ have the same restriction to

$$S(Z(\mathfrak{O}G)) \subseteq Z(\mathfrak{O}C_G(P)) \cap Z(\mathfrak{O}N_G(P)) \subseteq Z(\mathfrak{O}C_G(P)) \cap Z(\mathfrak{O}H).$$

Therefore $\eta_{\hat{B}_1} \circ S = \eta_{\hat{B}} \circ S$. Hence $\hat{B}_1^G = \hat{B}^G = B_0(G)$, and P, $N_G(P)$, $\hat{B}_1$ is a counterexample to the theorem.

Now assume that $H = N_G(P)$. By Corollary 13.23, the defect group $D(\hat{B})$ contains P. Suppose that $D(\hat{B}) = P$. Then $\eta_{\hat{B}}(\tilde{L}_j) \neq 0$, for some sum $\tilde{L}_j$ of some class L_j of $N_G(P)$ having $D(L_j) = P$. Lemma 13.26 gives us a conjugacy class K_i of G satisfying $D(K_i) \sim P$ and $K_i \cap C_G(P) = L_j$. By (13.1), $S(\tilde{K}_i) = \tilde{L}_j$. Therefore $\eta_{B_0(G)}(\tilde{K}_i) = \eta_{\hat{B}} \circ S(\tilde{K}_i) = \eta_{\hat{B}}(\tilde{L}_j) \neq 0$. From (13.18b) and (13.19) we conclude that P is a p-Sylow subgroup of G. Now every class L_j of $N_G(P)$ contained in $C_G(P)$ has P as its defect group. Since $\hat{B} \neq B_0(N_G(B))$, Corollary 13.23 implies the existence of such a class L_j such that $\eta_{\hat{B}}(\tilde{L}_j) \neq \eta_{B_0}(\tilde{L}_j)$. But then the corresponding class K_i of G satisfies

$$\eta_{\hat{B}} \circ S(\tilde{K}_i) = \eta_{\hat{B}}(\tilde{L}_j) \neq \eta_{B_0}(\tilde{L}_j) = \eta_{B_0} \circ S(\tilde{K}_v),$$

which is impossible, since $\hat{B}^G = B_0^G = B_0(G)$ (by Proposition 13.15). We conclude that $D(\hat{B})$ strictly contains P.

From $P < D(\hat{B})$ we obtain $C_G(D(\hat{B})) \leq C_G(P) \leq N_G(P)$. Therefore $D(\hat{B})C_G(D(\hat{B})) \leq N_G(P)$. Proposition 13.21 gives us a block $\hat{\hat{B}}$ of $D(\hat{B})C_G(D(\hat{B}))$ such that $\hat{\hat{B}}_{N_G(P)} = \hat{B}$. Since $\hat{B} \neq B_0(N_G(P))$, Proposition 13.15 implies that $\hat{\hat{B}}$ is not $B_0(D(\hat{B})C_G(D(\hat{B})))$. From (13.1) we compute immediately that $\hat{\hat{B}}^G$ (defined with respect to the p-group $D(\hat{B})$) is $(\hat{\hat{B}}^{N_G(P)})^G = \hat{B}^G = B_0(G)$. Therefore $D(\hat{B})$, $D(\hat{B})C_G(D(\hat{B}))$, $\hat{\hat{B}}$ is a counterexample with $|D(\hat{B})| > |P|$. This contradicts the maximality of $|P|$. The final contradiction proves the theorem.

We denote by $O_{p'}(G)$ the largest normal p'-subgroup of G, i.e., the largest normal subgroup whose order is not divisible by p. The following relation between $O_{p'}(G)$ and $B_0(G)$ is very useful in applications.

PROPOSITION 13.28. $O_{p'}(G) = \bigcap_{\chi_j \in B_0(G)} \operatorname{Ker}(\chi_j)$.

Proof. Let $f = |O_{p'}(G)|^{-1} \sum_{\sigma \in O_{p'}(G)} \sigma$ be the primitive idempotent of $ZFO_{p'}(G))$ corresponding to the trivial character of $O_{p'}(G)$. By Corollary 11.10, f is an idempotent in $\mathfrak{O}G$. Clearly it lies in $Z(\mathfrak{O}G)$. So Proposition 9.11 gives a unique decomposition $f = e_1 + \ldots + e_t$, where $e_1, \ldots, e_t$ are primitive idempotents of $Z(\mathfrak{O}G)$ corresponding to blocks $B_1, \ldots, B_t$, respectively, of G. Using (11.8), we see that the unique decomposition of f as a sum of primitive idempotents in $Z(FG)$ is

$$f = \sum_{i=1}^{t} \sum_{\chi_j \in B_i} e(\chi_j) \tag{13.29}$$

Evidently the idempotent $e(1) = |G|^{-1} \sum_{\sigma \in G} \sigma$ of $Z(FG)$ corresponding to the trivial character of G satisfies $fe(1) = e(1)$. So it appears in the decomposition (13.29) of f. Hence the block $B_0(G)$ containing $e(1)$ appears in the list $B_1, \ldots, B_t$, say as B_1. If χ_j is any character in $B_0(G)$, then (13.29) implies that $e(\chi_j)f = e(\chi_j)$. If I_j is any irreducible FG-module with character χ_j,

then $I_j = I_j e(\chi_j)$ and $e(\chi_j)f = e(\chi_j)$ imply that f acts as identity on I_j. Since $f\sigma = f$, for all $\sigma \in O_{p'}(G)$, we conclude that $O_{p'}(G)$ acts trivially on I_j. Therefore $O_{p'}(G) \leq \operatorname{Ker}(\chi_j)$, by (4.37a). This proves that

$$O_{p'}(G) \subseteq \bigcap_{\chi_j \in B_0(G)} \operatorname{Ker}(\chi_j).$$

Evidently $N = \bigcap_{\chi_j \in B_0(G)} \operatorname{Ker}(\chi_j)$ is a normal subgroup of G. Suppose that $N \not\subseteq O_{p'}(G)$. Then p must divide $|N|$. So there is a p-element $\pi \neq 1$ in N. Applying Theorem 12.13, we obtain

$$0 = \sum_{\chi_j \in B_0(G)} \chi_j(\pi)\chi_j(1).$$

But this sum is

$$\sum_{\chi_j \in B_0(G)} \chi_j(1)^2 > 0,$$

since $\pi \in \operatorname{Ker}(\chi_j)$, for all $\chi_j \in B_0(G)$ (see Proposition 4.38(a)). The contradiction shows that $N \leq O_{p'}(G)$, and finishes the proof of the proposition.

14. Quaternion Sylow Groups

In addition to the hypotheses of the last three sections, we suppose that G has a t.i. set S satisfying

An element $\sigma \in G$ lies in S if and only if $\sigma_p \in S$. (14.1)

We denote by H the normalizer of S in G.

Let T be the subset of all p-elements in S. By (5.10a, c), the subset T is closed under inverses and invariant under H-conjugation. From (14.1) it is clear that S is the p-section of H defined by T via (12.16). We write this section as $S_p(T \text{ in } H)$, instead of $S_p(T)$, to indicate the group H. Then S^G is the p-section $S_p(T \text{ in } G)$.

We use the notation of Proposition 12.17 and Theorem 12.19 with respect to $CF(H|S, \hat{B})$, or $CF(G|S^G, B)$, for blocks $\hat{B}$, B of H, G respectively.

PROPOSITION 14.2. *Induction: $\phi \to \phi^G$ is an isometry of $CF(H|S, B_0(H))$ on to $CF(G|S^G, B_0(G))$.*

Proof. Proposition 5.15 says that $\phi \to \phi^G$ is an isometry of $CF(H|S)$ into $CF(G|S^G)$. If ψ is any class function on G, let $\psi|_S$ be the class function on H which equals ψ on S and is zero on $H \backslash S$. From Proposition 5.14 it is clear that $(\psi|_S)^G$ equals ψ on S^G and is zero on $G \backslash S^G$. It follows that $\phi \to \phi^G$ is an isometry of $CF(H|S)$ onto $CF(G|S^G)$, with $\psi \to \psi|_S$ as its inverse.

Let π be any p-element of S. Since S is a t.i. set, the centralizer $C = C_G(\pi)$ is contained in H, and hence equals $C_H(\pi)$. Let $R = R(\pi) = S_p(\{\pi, \pi^{-1}\} \text{ in } C)$. Evidently R is the set of all $\sigma \in C$ such that $\sigma_p = \pi$ or π^{-1}. By (14.1), S is the union of its subsets $R(\pi)$, where π runs over all elements of T.

Suppose that ψ is a class function on some group containing C. For each

block $\bar{B}$ of C we denote by $\psi_{\bar{B}}$ the unique F-linear combination of the irreducible characters in $\bar{B}$ such that the restriction ψ_C of ψ to C satisfies

$$\psi_C = \sum_{\bar{B}} \psi_{\bar{B}}.$$

As usual, we denote by $\psi|_R$ the class function on C which equals ψ on R and is zero on $C\backslash R$. Theorem 12.19 implies that $\psi_{\bar{B}}|_R \in CF(C|R, \bar{B})$, for all blocks $\bar{B}$ of C. Hence,

$$\psi|_R = \psi_C|_R = \sum_{\bar{B}} \psi_{\bar{B}}|_R \tag{14.3}$$

is the unique decomposition of $\psi|_R \in CF(C|R)$ as a sum of elements $\psi_{\bar{B}}|_R \in CF(C|R, \bar{B})$, given by (12.18).

Now let ψ be an element of $CF(G|S^G, B)$, for some block B of G. Brauer's second main theorem, applied to both π and π^{-1}, tells us that

$$\psi|_R = \sum_{\bar{B}^G = B} \psi_{\bar{B}}|_R.$$

Since the decomposition (14.3) is unique, we conclude that

$$\psi_{\bar{B}}|_R = 0, \quad \textit{for all } \bar{B} \textit{ such that } \bar{B}^G \neq B. \tag{14.4}$$

We decompose $\psi|_S$ in the form

$$\psi|_S = \sum_{\hat{B}} \psi_{\hat{B}},$$

where $\psi^{\hat{B}} \in CF(H|S, \hat{B})$, for each block $\hat{B}$ of H. As in (14.4), we have

$$(\psi_{\hat{B}})_{\bar{B}}|_R = 0, \quad \textit{for all } \bar{B}, \hat{B} \textit{ such that } \bar{B}^H \neq \hat{B}. \tag{14.5}$$

Evidently $R \subseteq S$ implies that

$$\psi|_R = (\psi|_S)|_R = \sum_{\hat{B}} \psi_{\hat{B}}|_R = \sum_{\hat{B}, \bar{B}} (\psi_{\hat{B}})_{\bar{B}}|_R.$$

The unicity of (14.3) and (14.5) give

$$\psi_{\bar{B}}|_R = \sum_{\hat{B}} (\psi_{\hat{B}})_{\bar{B}}|_R = (\psi_{\bar{B}^H})_{\bar{B}}|_R, \quad \textit{for all } \bar{B}. \tag{14.6}$$

Suppose that $B = B_0(G)$. Brauer's third main theorem and (14.4) tell us that $\psi_{\bar{B}}|_R = 0$, for all $\bar{B} \neq B_0(C)$. If $\hat{B} \neq B_0(H)$, then (14.5), (14.6) and Brauer's third main theorem now imply that $(\psi_{\hat{B}})_{\bar{B}}|_R = 0$, for all $\bar{B}$. Hence $\psi_{\hat{B}}|_R = 0$ by (14.3). Since π is an arbitrary element of T, this says that $\psi_{\hat{B}}$ vanishes on the union S of the $R(\pi)$, $\pi \in T$. Therefore $\psi_{\hat{B}} = 0$. We conclude that $\psi|_S = \psi_{B_0(H)}$. So $\psi \to \psi|_S$ maps $CF(G|S^G, B_0(G))$ into $CF(H|S, B_0(H))$.

Suppose that $B \neq B_0(G)$. Brauer's third main theorem and (14.4) tell us that $\psi_{B_0(C)}|_R = 0$. So (14.6), (14.5), and Brauer's third main theorem imply that $(\psi_{B_0(H)})_{\bar{B}}|_R = 0$, for all $\bar{B}$. Therefore $\psi_{B_0(H)}|_R = 0$. As above, we conclude that $\psi_{B_0(H)} = 0$. So $\psi \to \psi|_S$ maps $\sum_{B \neq B_0(G)} CF(G|S^G, B)$ into $\sum_{\hat{B} \neq B_0(H)} CF(H|S, \hat{B})$. Since $\psi \to \psi|_S$ sends $CF(G|S^G)$ onto $CF(H|S)$, this and (12.18) are enough to prove the proposition.

COROLLARY 14.7. *The inverse map to* $\phi \to \phi^G$ *sends* $\psi \in CF(G|S^G, B_0(G))$ *into* $\psi|_S \in CF(H|S, B_0(H))$.

Proof. This was shown in the first paragraph of the above proof.

The above proposition gives us a "method" for finding those irreducible characters $\chi_j \in B_0(G)$ which do not vanish on S^G. By Theorem 12.19 and (12.18), an irreducible character χ_j of G satisfies these conditions if and only if $\chi_j|_{SG}$ is a non-zero element of $CF(G|S^G, B_0(G))$, hence if and only if there exists $\psi \in CF(G|S^G, B_0(G))$ such that $(\psi, \chi_j)_G = (\psi, \chi_j|_{SG})_G \neq 0$. By the proposition this occurs if and only if $(\phi^G, \chi_j)_G \neq 0$, for some $\phi \in CF(H|S, B_0(H))$. Therefore we can find all these χ_j by taking all the characters $\phi \in CF(H|S, B_0(H))$ (actually, a basis will do), inducing them to G, writing the resulting characters ϕ^G as linear combinations of irreducible characters χ_j of G, and taking all the χ_j having a non-zero coefficient in one of these decompositions. This doesn't *sound* too practical, but, as we shall see later, it can be made to work in certain cases.

The best of all cases is the *coherent case.* To define this, let $\phi_1, \ldots, \phi_c$ be the irreducible characters in $B_0(H)$ which do not vanish on S. The coherent case occurs when we can find irreducible characters $\chi_1, \ldots, \chi_c$ of G and signs $\varepsilon_1, \ldots, \varepsilon_c = \pm 1$ satisfying

$$\text{If } f_1, \ldots, f_c \in F \text{ and } f_1\phi_1 + \ldots + f_c\phi_c \in CF(H|S, B_0(H)), \quad \text{then}$$
$$(f_1\phi_1 + \ldots + f_c\phi_c)^G = f_1\varepsilon_1\chi_1 + \ldots + f_c\varepsilon_c\chi_c. \tag{14.8}$$

In the coherent case we have

PROPOSITION 14.9. *The characters* $\chi_1, \ldots, \chi_c$ *are precisely the irreducible characters in* $B_0(G)$ *which do not vanish on* S^G. *Furthermore, they satisfy:*

$$\chi_i|_S = \varepsilon_i\phi_i|_S \quad (i = 1, \ldots, c). \tag{14.10}$$

Proof. Evidently every $\phi \in CF(H|S, B_0(H))$ has the form $f_1\phi_1 + \ldots + f_c\phi_c$, for some $f_1, \ldots, f_c \in F$. We have seen in the above discussion that the irreducible characters in $B_0(G)$ which do not vanish on S^G are precisely those which occur with a non-zero coefficient in some such ϕ^G. So these characters are among $\chi_1, \ldots, \chi_c$ by (14.8).

Fix $i = 1, \ldots, c$. By Theorem 12.19, the class function $\phi_i|_S$ is a non-zero member of $CF(H|S, B_0(H))$. So Proposition 12.17 gives us an element $\phi \in CF(H|S, B_0(H))$ such that $(\phi_i|_S, \phi)_H \neq 0$. Evidently $\phi = f_1\phi_1 + \ldots + f_c\phi_c$, for some $f_1, \ldots, f_c \in F$, and

$$f_i = (\phi_i, \phi)_H = (\phi_i|_S, \phi)_G \neq 0.$$

From (14.8) we see that χ_i has a non-zero coefficient $f_i\varepsilon_i$ in ϕ^G. Therefore $\chi_i \in B_0(G)$ and $\chi_i|_{SG} \neq 0$. This proves the first statement of the proposition.

For the second statement, notice that condition (14.8) implies that

$$(\chi_i, \phi^G)_G = (\varepsilon_i\phi_i, \phi)_H, \quad \textit{for all } \phi \in CF(H|S, B_0(H)).$$

Using the Frobenius reciprocity law, this becomes

$$(\chi_i|_S, \phi)_H = ((\chi_i)_H, \phi)_H = (\chi_i, \phi^G)_G = (\varepsilon_i\phi_i|_S, \phi)_H,$$
$$\text{for all } \phi \in CF(H|S, B_0(H)).$$

By Corollary 14.7 and Theorem 12.19, both $\chi_i|_S$ and $\varepsilon_i\phi_i|_S$ lie in $CF(H|S, B_0(H))$. So Proposition 12.17 and the above equation imply (14.10), which finishes the proof of the proposition.

We shall apply the above ideas in the case $p = 2$ to prove

THEOREM 14.11 (Brauer–Suzuki). *Let G have a quaternion group Q (of order 8) as a 2-Sylow subgroup. Then G has a normal subgroup $N \neq G$ containing the involution ι of Q.*

To show this we shall prove a series of lemmas, all based on the hypothesis that G is a counterexample. We begin with

LEMMA 14.12. *All the elements of $Q\backslash\langle\iota\rangle$ are conjugate to each other in G.*

Proof. Let ρ, τ be two elements of $Q\backslash\langle\iota\rangle$ which are not G-conjugate to each other. Since ρ is Q-conjugate to ρ^{-1}, the cosets $\rho\langle\iota\rangle$, $\tau\langle\iota\rangle$, $\rho\tau\langle\iota\rangle$ are the three involutions in the four-group $Q/\langle\iota\rangle$. One of ρ and τ, say ρ, is not G-conjugate to $\rho\tau$. Then the two cosets $\langle\rho\rangle = \{1, \rho, \iota, \rho^{-1}\}$ and $\tau\langle\rho\rangle = \{\tau, \rho\tau, \tau^{-1}, (\rho\tau)^{-1}\}$ of $\langle\rho\rangle$ in Q have the property that no element in one is G-conjugate to any element in the other.

We define a function $\lambda : G \to F$ by

$$\lambda(\sigma) = \begin{cases} +1, & \text{if } \sigma_2 \text{ is } G\text{-conjugate to an element of } \langle\rho\rangle, \\ -1, & \text{if } \sigma_2 \text{ is } G\text{-conjugate to an element of } \tau\langle\rho\rangle \end{cases}$$

for any $\sigma \in G$. Evidently λ is a well-defined class-function on G whose restriction to Q is a linear character. If E is any nilpotent subgroup of G, and $E = D \times A$, where $D \leq Q$ and A is a subgroup of odd order, then the restriction of λ to E is clearly a linear character. Since every nilpotent subgroup of G is conjugate to such an E, we conclude from Theorem 7.1 that λ is a generalized character of G.

By definition $\lambda(\sigma) = \pm 1$, for all $\sigma \in G$. Furthermore, $\lambda(\sigma^{-1}) = \lambda(\sigma)$. Hence,

$$(\lambda, \lambda)_G = \frac{1}{|G|} \sum_{\sigma \in G} \lambda(\sigma^{-1})\lambda(\sigma) = \frac{1}{|G|} \sum_{\sigma \in G} (\pm 1)^2 = 1.$$

But $\lambda = \sum_{j=1}^{k} a_j\chi_j$, where $a_1, \ldots, a_k \in \mathbf{Z}$ and $\chi_1, \ldots, \chi_k$ are the irreducible characters of G. From (4.20) we get $1 = (\lambda, \lambda)_G = \sum_{j=1}^{k} a_j^2$, which implies that all the a_j except one are zero and that that one is ± 1. Hence $\pm\lambda$ is an

irreducible character of G. Since $\lambda(1) = 1 > 0$, we conclude that λ is a linear character of G. Now $N = \operatorname{Ker} \lambda$ is a normal subgroup of G containing ι and not containing ρ. This contradicts the fact that G is a counterexample to Theorem 14.11. The contradiction proves the lemma.

Fix an element $\rho \in Q\backslash\langle\iota\rangle$. The above lemma implies immediately that

COROLLARY 14.13. *The elements* 1, ι, ρ *are representatives for the distinct conjugacy classes of* 2*-elements of* G.

In fact, we can say more. Let H be the normalizer in G of $\langle\iota\rangle$. Of course, $H = C_G(\iota)$, and Q is a 2-Sylow subgroup of H.

LEMMA 14.14. *The elements* 1, ι, ρ *are representatives for the distinct conjugacy classes of* 2*-elements of* H.

Proof. Let τ be any element of $Q\backslash\langle\iota\rangle$. By Lemma 14.12 there exists $\pi \in G$ such that $\rho^\pi = \tau$. But then $\iota^\pi = (\rho^2)^\pi = \tau^2 = \iota$. Hence $\pi \in H = C_G(\iota)$. Therefore all elements of $Q\backslash\langle\iota\rangle$ are H-conjugate to ρ. The lemma follows from this.

Evidently H contains the group $L = N_G(\langle\rho\rangle)$. Hence $L = N_H(\langle\rho\rangle)$. The structure of L is quite simple.

LEMMA 14.15. *The group* L *is the semi-direct product* QK *of* Q *with an odd normal subgroup* K *centralizing* ρ.

Proof. Since $\langle\rho\rangle$ is normal in Q, and Q is a 2-Sylow subgroup of G, the group Q is a 2-Sylow subgroup of L. Inversion $\rho \to \rho^{-1}$, is the only non-trivial automorphism of the cyclic group $\langle\rho\rangle$ of order 4, and any element of $Q\backslash\langle\rho\rangle$ inverts $\langle\rho\rangle$. It follows that $L = QC$, where $C = C_G(\rho)$, and that $\langle\rho\rangle = Q \cap C$ is a cyclic 2-Sylow subgroup of C. This implies that $C = \langle\rho\rangle K$, where $K = 0_{2'}(C)$ (see Section I.6 of Huppert, 1967). Since K is characteristic in C, it is normal in L, and $L = QK$ is the semi-direct product of Q and K. This proves the lemma.

The group Q has four linear characters 1, λ_1, λ_2, λ_3, coming from the four-group $Q/\langle\iota\rangle$, and the irreducible character θ defined by (6.5). If $\tau \in Q\backslash\langle\rho\rangle$, then 1, ι, ρ, τ, $\rho\tau$ are representatives for the five Q-conjugacy classes of Q, and we have (after renumbering) the character table:

	1	ι	ρ	τ	$\rho\tau$
1	1	1	1	1	1
λ_1	1	1	1	−1	−1
λ_2	1	1	−1	1	−1
λ_3	1	1	−1	−1	1
θ	2	−2	0	0	0

(14.16)

By Proposition 4.25, $1, \lambda_1\ \lambda_2, \lambda_3, \theta$ are all the irreducible characters of Q. We denote by $\tilde{1}, \tilde{\lambda}_1, \tilde{\lambda}_2, \tilde{\lambda}_3, \tilde{\theta}$ the corresponding characters of $L = QK$ obtained from $1, \lambda_1, \lambda_2, \lambda_3, \theta$, respectively, by composition with the natural epimorphism of QK onto $Q = QK/K$.

LEMMA 14.17. *The characters* $\tilde{1}, \tilde{\lambda}_1, \tilde{\lambda}_2, \tilde{\lambda}_3, \tilde{\theta}$ *are precisely the irreducible characters in* $B_0(L)$.

Proof. By Proposition 13.28 any irreducible character in $B_0(L)$ has $K = 0_{2'}(L)$ in its kernel. Therefore it must be among the characters $\tilde{1}, \tilde{\lambda}_1, \tilde{\lambda}_2, \tilde{\lambda}_3, \tilde{\theta}$ which come from those of $Q = L/K$. On the other hand, one verifies easily from (4.30), (13.14) and Proposition 11.15 that each character on our list lies in $B_0(K)$. This proves the lemma.

By Proposition 5.12, the set $\sqrt{\rho}$ is a t.i. set in both H and G with L as its normalizer. Since ρ is a 2-element, this t.i. set clearly satisfies (14.1) (for both H and G). From Lemma 14.15 it is evident that $\sqrt{\rho} = \rho K \cup \rho^{-1}K$. Now the table (14.16) and Lemma 14.17 imply that

$$CF(L|\sqrt{\rho}, B_0(L)) = F(\tilde{1}+\tilde{\lambda}_1-\tilde{\lambda}_2-\tilde{\lambda}_3). \tag{14.18}$$

In view of (5.19), the induced character $(\tilde{1}+\tilde{\lambda}_1-\tilde{\lambda}_2-\tilde{\lambda}_3)^H = \Phi$ is a generalized character of H satisfying:

$$(\Phi, \Phi)_H = (\tilde{1}+\tilde{\lambda}_1-\tilde{\lambda}_2-\tilde{\lambda}_3, \tilde{1}+\tilde{\lambda}_1-\tilde{\lambda}_2-\tilde{\lambda}_3)_L = 4.$$

Proposition 5.9 implies that $\Phi = 1 + \sum_{j=1}^{d} a_j\phi_j$, where 1 is the trivial character and $\phi_1, \ldots, \phi_d$ are the non-trivial irreducible characters of H, and where $a_1, \ldots, a_d$ are integers. Since $4 = 1^2 + \sum_{j=1}^{d} a_j^2$, all the a_j but three must be zero, and those three must be ± 1. Hence there are three distinct non-trivial irreducible characters, say ϕ_1, ϕ_2, ϕ_3 of H, and three signs $a_1, a_2, a_3 = \pm 1$ such that

$$(\tilde{1}+\tilde{\lambda}_1-\tilde{\lambda}_2-\tilde{\lambda}_3)^H = 1 + a_1\phi_1 + a_2\phi_2 + a_3\phi_3.$$

By (14.18) and (14.8) we are in the coherent case. So Proposition 14.9 tells us that

$$1, \phi_1, \phi_2, \phi_3 \text{ *are precisely the irreducible characters in* } B_0(H) \text{ *which do not vanish on* } (\sqrt{\rho})^H. \tag{14.19}$$

Furthermore, (14.10) and (14.16) give

$$a_1\phi_1 = a_2\phi_2 = a_3\phi_3 = 1 \quad \text{on } (\sqrt{\rho})^H. \tag{14.20}$$

To compute the rest of the characters in $B_0(H)$ we shall use a process of modification of generalized characters based on Theorem 7.1. Let $H_{2'}$ be the subset of all elements of odd order in H. Since ι is central in H, it is clear

that $\langle\iota\rangle H_{2'} = H_{2'} \cup \iota H_{2'}$ is the 2-section of all $\sigma \in H$ such that $\sigma_2 = 1$ or ι. We define $X(H|\langle\iota\rangle H_{2'}, B_0(H))$ to be the intersection $X(H) \cap CF(H|\langle\iota\rangle H_{2'}, B_0(H))$, i.e., the additive group of all $\mathbf{Z}$-linear combinations ϕ of the irreducible characters $\phi_j \in B_0(H)$ such that $\phi = 0$ on $H\backslash\langle\iota\rangle H_{2'}$.

Let X_+, X_- be the two additive subgroups of $X(H|\langle\iota\rangle H_{2'}, B_0(H))$ defined by

$$X_+ = \{\phi \in X(H|\langle\iota\rangle H_{2'}, B_0(H)) : \phi(\sigma\iota) = \phi(\sigma), \quad \textit{for all } \sigma \in H\}, \tag{14.21a}$$

$$X_- = \{\phi \in X(H|\langle\iota\rangle H_{2'}, B_0(H)) : \phi(\sigma\iota) = \phi(\sigma), \quad \textit{for all } \sigma \in H\}. \tag{14.21b}$$

For any $\phi \in X_+ \cup X_-$ we define a class function ϕ^* on H by

$$\phi^*(\sigma) = \begin{cases} \phi(\sigma), & \textit{for } \sigma \in H_{2'}, \\ -\phi(\sigma), & \textit{for } \sigma \in \iota H_{2'}, \\ 0, & \textit{for } \sigma \in H\backslash\langle\iota\rangle H_{2'}. \end{cases} \tag{14.22}$$

Then we have

LEMMA 14.23. *The map $\phi \to \phi^*$ sends X_+ isometrically into X_- and $2X_-$ isometrically into X_+.*

Proof. Let ϕ be any element of $X_+ \cup 2X_-$. We first show that $\phi^* \in X(H)$. By Theorem 7.1 it suffices to prove that the restriction ϕ_E^* lies in $X(E)$, for any nilpotent subgroup E of H. Since we can pass to any H-conjugate of E, Lemma 14.14 implies that we can assume E to have one of the four forms T, $\langle\iota\rangle \times T$, $\langle\rho\rangle \times T$, or $Q \times T$, where $|T|$ is odd.

If $E = T$, then $\phi_E^* \in X(E)$, by (14.22). If $E = \langle\iota\rangle \times T$, then (14.21) implies that $\phi_E = \lambda \times \psi$, where $\psi \in X(T)$ and λ is one of the two linear characters of $\langle\iota\rangle$. Evidently ϕ_E^* is then $\lambda' \times \psi$, where λ' is the other linear character of $\langle\iota\rangle$. So $\phi_E^* \in X(E)$.

If $E = \langle\rho\rangle \times T$, then the fact that ϕ is zero on $(\langle\rho\rangle\backslash\langle\iota\rangle) \times T \subseteq H\backslash\langle\iota\rangle H_{2'}$, together with (14.21), implies that $\phi_E = \lambda^{\langle\rho\rangle} \times \psi$, where $\psi \in X(T)$ and λ is one of the linear characters of $\langle\iota\rangle$. Then $\phi_E^* = (\lambda')^{\langle\rho\rangle} \times \psi \in X(E)$, where λ' is the other linear character of $\langle\iota\rangle$.

There remains the case in which $E = Q \times T$. Suppose that $\phi \in X_+$. Since $\phi = 0$ on $(Q\backslash\langle\iota\rangle) \times T$, it follows from (14.16) and (14.21a) that $\phi_E = (1 + \lambda_1 + \lambda_2 + \lambda_3) \times \psi$, for some $\psi \in X(T)$. But then $\phi_E^* = 2\theta \times \psi \in X(E)$. On the other hand, if $\phi \in 2X_-$, we see from (14.16) and (14.21b) that $(\frac{1}{2}\phi)_E = \theta \times \psi$, for some $\psi \in X(T)$. Hence $\phi_E = 2\theta \times \psi$ and $\phi_E^* = (1 + \lambda_1 + \lambda_2 + \lambda_3) \times \psi \in X(E)$. Therefore $\phi_E^* \in X(E)$ in all cases, which proves that $\phi^* \in X(H)$.

It is evident from (14.22) that ϕ^* lies in $X(H|\langle\iota\rangle H_{2'})$. We must show that it lies in $X(H|\langle\iota\rangle H_{2'}, B_0(H))$. Let ϕ_j be an irreducible character of H such that $(\phi^*, \phi_j)_H \neq 0$. It suffices to prove that $\phi_j \in B_0(H)$.

Since ϕ is a linear combination of the irreducible characters in $B_0(H)$,

Theorem 12.19 implies that $\phi|_{H_{2'}} \in CF(H|H_{2'}, B_0(H))$ and $\phi|_{\iota H_{2'}} \in CF(H|\iota H_{2'}, B_0(H))$. From (14.22) we get

$$0 \neq (\phi^*, \phi_j)_H = (\phi|_{H_{2'}} - \phi|_{\iota H_{2'}}, \phi_j)_H = (\phi|_{H_{2'}}, \phi_j|_{H_{2'}})_H - (\phi|_{\iota H_{2'}}, \phi_j|_{\iota H_{2'}})_H$$

So one of $(\phi|_{H_{2'}}, \phi_j|_{H_{2'}})_H$, $(\phi|_{\iota H_{2'}}, \phi_j|_{\iota H_{2'}})_H$ is non-zero. In view of Theorem 12.19 and (12.18), this implies that $\phi_j \in B_0(H)$.

We now know that $\phi^* \in X(H|\langle\iota\rangle H_{2'}, B_0(H))$. It is clear from (14.21) and (14.22) that $\phi^* \in X_-$ if $\phi \in X_+$ and $\phi^* \in X_+$ if $\phi \in 2X_-$. Since the map $\phi \to \phi^*$ is obviously an isometry (with respect to $(\cdot, \cdot)_H$), this proves the lemma.

Because the involution ι lies in the center of H, it acts on any irreducible FH-module I either as multiplication by 1 or as multiplication by -1. So the corresponding irreducible character ϕ_j of H satisfies either

$$\phi_j(\sigma\iota) = \phi_j(\sigma), \quad \textit{for all } \sigma \in H, \textit{ or} \tag{14.24a}$$

$$\phi_j(\sigma\iota) = -\phi_j(\sigma), \quad \textit{for all } \sigma \in H, \tag{14.24b}$$

respectively.

LEMMA 14.25. *The characters* 1, ϕ_1, ϕ_2, ϕ_3 *are precisely the irreducible characters* ϕ_j *in* $B_0(H)$ *satisfying* (14.24a).

Proof. Since ρ is conjugate to $\rho\iota = \rho^{-1}$, any irreducible character ϕ_j satisfying (14.24b) is zero on ρ. This and (14.20) imply that each of 1, ϕ_1, ϕ_2, ϕ_3 satisfies (14.24a).

Now let ϕ_j be any irreducible character in $B_0(H)$ satisfying (14.24a). Assume that ϕ_j is not 1, ϕ_1, ϕ_2, or ϕ_3. Then $\phi_j = 0$ on $(\sqrt{\rho})^H$ by (14.19). Lemma 14.14 implies that $(\sqrt{\rho})^H = H\backslash\langle\iota\rangle H_{2'}$. Hence $\phi_j \in X_+$. Applying Lemma 14.23, we see that $\phi_j^* \in X_-$ and $(\phi_j^*, \phi_j^*)_H = (\phi_j, \phi_j)_H = 1$. Therefore $\pm\phi_j^*$ is an irreducible character of H. Since $\phi_j^*(1) = \phi_j(1) > 0$, we conclude that ϕ_j, ϕ_j^* are (obviously distinct) irreducible characters in $B_0(H)$.

Because ϕ_j is zero on $Q\backslash\langle\iota\rangle$ and satisfies (14.24a), its restriction to Q is an integral multiple of $(1+\lambda_j+\lambda_2+\lambda_3)$. Hence 4 divides $\phi_j(1)$. Now (4.17) and (14.22) imply that the primitive idempotents f_j, f_j^* of $Z(FH)$ corresponding to ϕ_j, ϕ_j^*, respectively, satisfy

$$\begin{aligned} f_j + f_j^* &= \sum_{\sigma \in H} \frac{\phi_j(1)[\phi_j(\sigma^{-1}) + \phi_j^*(\sigma^{-1})]\sigma}{|H|} \\ &= \sum_{\sigma \in H_{2'}} \frac{2\phi_j(1)\phi_j(\sigma^{-1})\sigma}{|H_1|} \end{aligned}$$

Since 8, which is the highest power of 2 dividing $|H|$, divides $2\phi_j(1)$, we conclude that $f_j + f_j^* \in Z(\mathfrak{O}H)$. This is impossible by (11.8), since $B_0(H)$ contains other characters besides ϕ_j and ϕ_j^*. Therefore ϕ_j does not exist and the lemma is proved.

COROLLARY 14.26. $X_+ = \{c_0 1 + c_1 a_1 \phi_1 + c_2 a_2 \phi_2 + c_3 a_3 \phi_3 :$
$c_0, c_1, c_2, c_3 \in \mathbf{Z}, c_0 + c_1 + c_2 + c_3 = 0\}$

Proof. It is evident from (14.21a) and (14.24) that any $\phi \in X_+$ is a $\mathbf{Z}$-linear combination of those irreducible characters $\phi_j \in B_0(H)$ satisfying 14.24a, i.e., of $1, \phi_1, \phi_2, \phi_3$. So X_+ consists precisely of all $\phi = c_0 1 + c_1 a_1 \phi_1 + c_2 a_2 \phi_2 + c_3 a_3 \phi_3$, with $c_0, c_1, c_2, c_3 \in \mathbf{Z}$, such that $\phi = 0$ on $H \backslash \langle \iota \rangle H_{2'}$. But $H \backslash \langle \iota \rangle H_{2'} = (\sqrt{\rho})^H$ by Lemma 14.14. By (14.20), $\phi = 0$ on $(\sqrt{\rho})^H$ if and only if $c_0 + c_1 + c_2 + c_3 = 0$. This proves the corollary.

COROLLARY 14.27. *$B_0(H)$ contains precisely three irreducible characters ϕ_4, ϕ_5, ϕ_6 satisfying* (14.24b). *Furthermore* $X_- = \{c_4 \phi_4 + c_5 \phi_5 + c_6 \phi_6 :$ $c_4, c_5, c_6 \in \mathbf{Z}\}$.

Proof. Any irreducible character $\phi_j \in B_0(H)$ satisfying (14.24b) is certainly not one of $1, \phi_1, \phi_2, \phi_3$. So $\phi_j = 0$ on $(\sqrt{\rho})^H = H \backslash \langle \iota \rangle H_{2'}$ by (14.9). Hence $\phi_j \in X_-$. It follows that these ϕ_j form a $\mathbf{Z}$-basis for X_-. Since Lemma 14.23 implies that the $\mathbf{Z}$-rank of X_- is the same as that of X_+, which is 3 by Corollary 14.26, this completes the proof of the corollary.

Actually, we can compute ϕ_4, ϕ_5, ϕ_6 quite explicitly.

LEMMA 14.28. *There exist signs $a_4, a_5, a_6 = \pm 1$, such that (after renumbering)*

$$\left.\begin{aligned} 2a_4\phi_4^* &= 1 + a_1\phi_1 - a_2\phi_2 - a_3\phi_3 \\ 2a_5\phi_5^* &= 1 - a_1\phi_1 + a_2\phi_2 - a_3\phi_3 \\ 2a_6\phi_6^* &= 1 - a_1\phi_1 - a_2\phi_2 + a_3\phi_3 \end{aligned}\right\} \tag{14.29}$$

Proof. If $j = 4$, 5 or 6, then Lemma 14.23 implies that $(2\phi_j)^*$ is an element of X_+ satisfying $((2\phi_j)^*, (2\phi_j)^*)_H = 4$. From the description of X_+ in Corollary 14.26 it is clear that $(2\phi_j)^*$ has the form $\pm 1 \pm a_1\phi_1 \pm a_2\phi_2 \pm a_3\phi_3$ where the sum of the four $\pm$'s is zero. So, with a suitable choice of $a_j = \pm 1$, the character $2a_j\phi_j^*$ has one of the three forms on the right of (14.29). Since there are three distinct ϕ_j, they must exhaust these three forms. This proves the lemma.

Now we can compute the module $X(H|\sqrt{\iota}, B_0(H))$ of all $\mathbf{Z}$-linear combinations ϕ of irreducible characters in $B_0(H)$ such that $\phi = 0$ on $H \backslash \sqrt{\iota} = H_{2'}$.

LEMMA 14.30. *The $\mathbf{Z}$-module $X(H|\sqrt{\iota}, B_0(H))$ has the $\mathbf{Z}$-basis*

$$1 + a_1\phi_1 + a_2\phi_2 + a_3\phi_3, \quad a_2\phi_2 + a_3\phi_3 + a_4\phi_4, \quad a_1\phi_1 + a_3\phi_3 + a_5\phi_5,$$
$$a_1\phi_1 + a_2\phi_2 + a_6\phi_6. \tag{14.31}$$

Proof. We know from its definition that $1 + a_1\phi_1 + a_2\phi_2 + a_3\phi_3$ vanishes outside $(\sqrt{\rho})^H$. In particular, it is zero on $H_{2'}$. So $1 + a_1\phi_1 + a_2\phi_2 + a_3\phi_3$

$\in X(H|\sqrt{\iota}, B_0(H))$. From this, (14.22) and (14.29) we see that

$$2a_4\phi_4|_{H_2'} = 1+a_1\phi_1|_{H_2'}-a_2\phi_2|_{H_2'}-a_3\phi_3|_{H_2'}$$
$$= -2(a_2\phi_2|_{H_2'}+a_3\phi_3|_{H_2'}).$$

It follows that $a_2\phi_2+a_3\phi_3+a_4\phi_4 \in X(H|\sqrt{\iota}, B_0(H))$. Similarly $a_1\phi_1+a_3\phi_3$ $+a_5\phi_5$, $a_1\phi_1+a_2\phi_2+a_6\phi_6 \in X(H|\sqrt{\iota}, B_0(H))$.

Since ϕ_4, ϕ_5, ϕ_6 are F-linearly independent on H, vanish on $(\sqrt{\rho})^H$ $= H\backslash\langle\iota\rangle H_2'$, and satisfy (14.24b), their restrictions to $H_{2'}$ are F-linearly independent. It follows that the module $X(H|B_0(H))$ of all $\mathbf{Z}$-linear combinations of $1, \phi_1, \ldots, \phi_6$ maps by restriction to $H_{2'}$ onto a $\mathbf{Z}$-module isomorphic to $X(H|B_0(H))/X(H|\sqrt{\iota}, B_0(H))$ of rank at least 3. But the elements (14.31) generate a submodule M of rank 4 in $X(H|\sqrt{\iota}, B_0(H))$. Hence $X(H|\sqrt{\iota}, B_0(H))$ has rank 4. Since $X(H|B_0(H))/L$ is clearly $\mathbf{Z}$-torsion free, M equals $X(H|\sqrt{\iota}, B_0(H))$, and the lemma is proved.

By Proposition 5.12 the set $\sqrt{\iota}$ is a t.i. set in G with normalizer H.

LEMMA 14.32. *There exist distinct non-trivial irreducible characters* $\chi_1, \ldots, \chi_6$ *of* G *and signs* $\varepsilon_1, \ldots, \varepsilon_6 = \pm 1$ *such that*

$$(1+a_1\phi_1+a_2\phi_2+a_3\phi_3)^G = 1+\varepsilon_1\chi_1+\varepsilon_2\chi_2+\varepsilon_3\chi_3. \tag{14.33a}$$
$$(a_2\phi_2+a_3\phi_3+a_4\phi_4)^G = \varepsilon_2\chi_2+\varepsilon_3\chi_3+\varepsilon_4\chi_4 \tag{14.33b}$$
$$(a_1\phi_1+a_3\phi_3+a_5\phi_5)^G = \varepsilon_1\chi_1+\varepsilon_3\chi_3+\varepsilon_5\chi_5 \tag{14.33c}$$
$$(a_1\phi_1+a_2\phi_2+a_6\phi_6)^G = \varepsilon_1\chi_1+\varepsilon_2\chi_2+\varepsilon_6\chi_6 \tag{14.33d}$$

Proof. It follows as usual from Lemma 14.30, Proposition 5.9 and (5.19) that there exist three distinct non-trivial irreducible characters χ_1, χ_2, χ_3 of G and three signs $\varepsilon_1, \varepsilon_2, \varepsilon_3 = \pm 1$ such that (14.33a) holds. (Compare the argument preceding (14.19)). Since (5.19) and Lemma 14.30 imply that $\Psi = (a_2\phi_2+a_3\phi_3+a_4\phi_4)^G$ is a generalized character of G satisfying $(\Psi, \Psi)_G = a_2^2+a_3^2+a_4^2 = 3$, there exist three distinct irreducible characters ψ_1, ψ_2, ψ_3 of G and three signs $d_1, d_2, d_3 = \pm 1$ such that $\Psi = d_1\psi_1+d_2\psi_2$ $+d_3\psi_3$. By Proposition 5.9, none of ψ_1, ψ_2, ψ_3 is 1. We also know from (5.19) that

$$(1+\varepsilon_1\chi_1+\varepsilon_2\chi_2+\varepsilon_3\chi_3, d_1\psi_1+d_2\psi_2+d_3\psi_3)_G = a_2^2+a_3^2 = 2.$$

It follows that two of the ψ_i are equal to two of the χ_j, say $\psi_1 = \chi_2, \psi_2 = \chi_3$ that $d_1 = \varepsilon_2$, $d_2 = \varepsilon_3$, and that ψ_3 is distinct from $1, \chi_1, \chi_2, \chi_3$. Hence (14.33b) holds with $\chi_4 = \psi_3$ and $\varepsilon_4 = d_3$.

Similarly $(a_1\phi_1+a_3\phi_3+a_5\phi_5)^G = \varepsilon_i\chi_i+\varepsilon_j\chi_j+\varepsilon_5\chi_5$, where $i, j = 1, 2, 3$, $i \neq j$, $\varepsilon_5 = \pm 1$ and χ_5 is an irreducible character of G distinct from $1, \chi_1, \chi_2$, χ_3. If $i, j = 2, 3$, then (5.19) gives

$$1 = a_3^2 = (\varepsilon_2\chi_2+\varepsilon_3\chi_3+\varepsilon_4\chi_4, \varepsilon_2\chi_2+\varepsilon_3\chi_3+\varepsilon_5\chi_5)_G = 2+\varepsilon_4\varepsilon_5(\chi_4, \chi_5)_G.$$

Hence $\chi_4 = \chi_5$ and $\varepsilon_4 = -\varepsilon_5$. But both $\varepsilon_2\chi_2+\varepsilon_3\chi_3+\varepsilon_4\chi_4 = (a_2\phi_2+a_3\phi_3 a_4\phi_4)^G$ and $\varepsilon_2\chi_2+\varepsilon_3\chi_3-\varepsilon_4\chi_4 = (a_1\phi_1+a_3\phi_3+a_5\phi_5)^G$ vanish at 1. Hence $\chi_4(1) = 0$, which is impossible. Therefore one of i, j is equal to 1 and the other is equal to 2 or 3, say 3. Now (14.33c) holds. Since

$$1 = (\varepsilon_2\chi_2+\varepsilon_3\chi_3+\varepsilon_4\chi_4, \varepsilon_1\chi_1+\varepsilon_3\chi_3+\varepsilon_5\chi_5)_G = 1+\varepsilon_1\varepsilon_5(\chi_4, \chi_5)_G,$$

the characters $1, \chi_1, \chi_2, \chi_3, \chi_4, \chi_5$ are all distinct.

A similar argument shows that (14.33d) holds for an irreducible character χ_6 distinct from $1, \chi_1, \ldots, \chi_5$ and for an $\varepsilon_6 = \pm 1$. So the lemma is proved.

COROLLARY 14.34. $\varepsilon_i\chi_i|\sqrt{\iota} = a_i\phi_i|\sqrt{\iota}$ $(i = 1, \ldots, 6)$.

Proof. This follows directly from the lemma, Proposition 14.9, and Lemma 14.30.

At last we can prove Theorem 14.11. Let I be the conjugacy class of ι in G. Evidently ι is the only involution in H, and $\iota^2 = 1 \notin \sqrt{\iota}$. So Corollary 5.22 implies that $I^2 \cap \sqrt{\iota}$ is empty. It follows from this and Proposition 5.23 that $\phi^G(\tilde{I}^2) = 0$, for any $\phi \in X(H|\sqrt{\iota})$. Applying this to $\phi = a_2\phi_2+a_3\phi_3+a_4\phi_4$, and using (14.33b), we get

$$\begin{aligned} 0 &= \varepsilon_2\chi_2(\tilde{I}^2)+\varepsilon_3\chi_3(\tilde{I}^2)+\varepsilon_4\chi_4(\tilde{I}^2) \\ &= \frac{[\varepsilon_2\chi_2(\tilde{I})]^2}{\varepsilon_2\chi_2(1)} + \frac{[\varepsilon_3\chi_3(\tilde{I})]^2}{\varepsilon_3\chi_3(1)} + \frac{[\varepsilon_4\chi_4(\tilde{I})]^2}{\varepsilon_4\chi_4(1)} \quad (by\ (4.31)) \\ &= |I|^2 \left\{ \frac{[\varepsilon_2\chi_2(\iota)]^2}{\varepsilon_2\chi_2(1)} + \frac{[\varepsilon_3\chi_3(\iota)]^2}{\varepsilon_3\chi_3(1)} + \frac{[\varepsilon_4\chi_4(\iota)]^2}{\varepsilon_4\chi_4(1)} \right\} \quad (\text{by Proposition 2.2}) \end{aligned}$$

Since $1+a_1\phi_1+a_2\phi_2+a_3\phi_3 = (1+\lambda_1-\lambda_2-\lambda_3)^H$ vanishes at ι, we compute from (14.29) and (14.22) that

$$2a_4\phi_4(\iota) = -1-a_1\phi_1(\iota)+a_2\phi_2(\iota)+a_3\phi_3(\iota) = 2a_2\phi_2(\iota)+2a_3\phi_3(\iota)$$

Using Corollary 14.34, we see that this implies

$$\varepsilon_4\chi_4(\iota) = \varepsilon_2\chi_2(\iota)+\varepsilon_3\chi_3(\iota).$$

Because $\phi^G = \varepsilon_2\chi_2+\varepsilon_3\chi_3+\varepsilon_4\chi_4$ vanishes at 1, we have

$$\varepsilon_4\chi_4(1) = -\varepsilon_2\chi_2(1)-\varepsilon_3\chi_3(1).$$

Substituting these in the previous equation we obtain:

$$\begin{aligned} 0 &= \frac{[\varepsilon_2\chi_2(\iota)]^2}{\varepsilon_2\chi_2(1)} + \frac{[\varepsilon_3\chi_3(\iota)]^2}{\varepsilon_3\chi_3(1)} - \frac{[\varepsilon_2\chi_2(\iota)+\varepsilon_3\chi_3(\iota)]^2}{\varepsilon_2\chi_2(1)+\varepsilon_3\chi_3(1)} \\ &= \frac{[\varepsilon_2\chi_2(\iota)\varepsilon_3\chi_3(1)-\varepsilon_3\chi_3(\iota)\varepsilon_2\chi_2(1)]^2}{\varepsilon_2\chi_2(1)\varepsilon_3\chi_3(1)(\varepsilon_2\chi_2(1)+\varepsilon_3\chi_3(1)} \end{aligned}$$

Hence,

$$\chi_2(\iota)\chi_3(1)-\chi_3(\iota)\chi_2(1) = 0.$$

or

$$\frac{\chi_2(\iota)}{\chi_2(1)} = \frac{\chi_3(\iota)}{\chi_3(1)}.$$

By symmetry we also have $\dfrac{\chi_2(\iota)}{\chi_2(1)} = \dfrac{\chi_1(\iota)}{\chi_3(1)}$. So there is a constant d such that $\chi_i(\iota) = d\chi_i(1)$, for $i = 1, 2, 3$. Since $1+\varepsilon_1\chi_1+\varepsilon_2\chi_2+\varepsilon_3\chi_3 = (1+a_1\phi_1 + a_2\phi_2+a_3\phi_3)^G = (1+\lambda_1-\lambda_2-\lambda_3)^G$ vanishes outside $(\sqrt{\rho})^G$, it is zero at 1 and at ι. This gives

$$\begin{aligned} 0 &= 1+\varepsilon_1\chi_1(1)+\varepsilon_2\chi_2(1)+\varepsilon_3\chi_3(1) \\ 0 &= 1+\varepsilon_1\chi_1(\iota)+\varepsilon_2\chi_2(\iota)+\varepsilon_3\chi_3(\iota) \\ &= 1+d(\varepsilon_1\chi_1(1)+\varepsilon_2\chi_2(1)+\varepsilon_3\chi_3(1)). \end{aligned}$$

Therefore $d = 1$, and $\chi_i(\iota) = \chi_i(1)$, for $i = 1, 2, 3$. Proposition 4.38 now tells us that $N = \mathrm{Ker}(\chi_1)$ is a normal subgroup of G containing ι. Since $\chi_1 \neq 1$, its kernel N is not the whole of G. Therefore G is not a counter-example to the theorem. This contradiction proves the theorem.

15. Glauberman's Theorem

We have now reached the goal of these lectures, which is the proof of

THEOREM 15.1 (Glauberman). *Let G be a finite group, and T be a 2-Sylow subgroup of G. Suppose that T contains an involution ι satisfying*

$$\text{if } \iota^\sigma \in T, \quad \text{for some } \sigma \in G, \quad \text{then } \iota^\sigma = \iota. \tag{15.2}$$

Then ι lies in $Z(G \bmod O_{2'}(G))$. In particular, if G is simple, then $G = \langle \iota \rangle$.

Proof. We use induction on the order of G. The result is obvious if $|G| = 2$, so we can assume it to be true for all groups of smaller order than $|G|$.

Assume that G contains a normal subgroup N with $\iota \in N < G$. Then $T \cap N$ is a 2-Sylow subgroup of N containing ι, and N, $T \cap N$, ι satisfy the hypotheses of the theorem. So the image of ι is central in $N/O_{2'}(N)$ by induction. Since $O_{2'}(N)$ is characteristic in N, it is normal in G. It follows that $O_{2'}(N) = N \cap O_{2'}(G)$. Therefore the image $\bar{\iota}$ of ι in $\bar{G} = G/O_{2'}(G)$ is central in the image $\bar{N}$ of N.

Suppose that $\bar{\iota}$ is not central in $\bar{G}$. Then there exists some element $\sigma \in G$ such that $\bar{\iota}$ is different from the image $\overline{(\iota^\sigma)}$ of ι^σ. Both ι and its $\bar{G}$-conjugate $\overline{(\iota^\sigma)}$ lie in the 2-Sylow subgroup of $Z(\bar{N})$, which is characteristic in $\bar{N}$ and hence normal in $\bar{G}$. So they both lie in the image $\bar{T}$ of T. Regarding things in the inverse image $TO_{2'}(G)$ of $\bar{T}$, we see that $\iota^{\sigma\tau} \in T$, for some $\tau \in O_{2'}(G)$. By (15.2), this implies that $\iota^{\sigma\tau} = \iota$. But then the image $\overline{(\iota^{\sigma\tau})} = \overline{(\iota^\sigma)}$ of $\iota^{\sigma\tau}$ equals $\bar{\iota}$. This contradiction forces $\bar{\iota}$ to be central in $\bar{G}$, which is the theorem in this case. Therefore we can assume from now on that

The only normal subgroup of G containing ι is G itself (15.3)

One case in which (15.2) is satisfied is that in which ι is the only involution in T. To handle this case, we shall use the following old result about 2-groups.

LEMMA 15.4. *Let T be a finite 2-group containing exactly one involution ι. Then T is either generalized quaternion of order 2^{n+1}, for some $n \geq 2$, or else cyclic.*

Proof. Choose A maximal among the normal abelian subgroups of T. We must show that

$$A = C_T(A). \tag{15.5}$$

Because A is an abelian normal subgroup of T, its centralizer $C_T(A)$ is a normal subgroup containing A. If $C_T(A) > A$, let B be minimal among all the normal subgroups of T satisfying $A < B \leq C_T(A)$. Then $[B : A] = 2$, and $B = \langle \beta, A \rangle$, for any $\beta \in B \backslash A$. Since A is abelian and $\beta \in C_T(A)$ centralizes A, the normal subgroup B of T is also abelian. This contradicts the maximality of A. Therefore (15.5) holds.

Evidently ι is the only involution in the abelian subgroup A. So $A = \langle \tau \rangle$ is cyclic of some order $2^n > 1$. In view of (15.5), conjugation in T defines an isomorphism of T/A onto a subgroup $\overline{T}$ of the automorphism group of A. If $\overline{T} = 1$, then $T = A$ is cyclic, and the proof is finished. So we can assume that $\overline{T} \neq 1$. Then there exists an element $\rho \in T$ whose image $\bar{\rho}$ is an involution in $\overline{T}$. Let k be an integer such that $\tau^\rho = \tau^k$. Because τ^ρ also generates $A = \langle \tau \rangle$, the integer k is a unit modulo 2^n. This, $\bar{\rho} \neq 1$, and $\bar{\rho}^2 = 1$, imply that

$$k \equiv 1 \pmod 2, \qquad k \not\equiv 1 \pmod{2^n}, \qquad k^2 \equiv 1 \pmod{2^n}. \tag{15.6}$$

Obviously $n \geq 2$. If $n = 2$, the only solution to (15.6) is $k \equiv -1 \pmod{2^n}$. If $n > 2$, there are two other solutions: $k \equiv 1 + 2^{n-1}$ and $k \equiv -1 + 2^{n-1} \pmod{2^n}$ which we must eliminate.

Suppose that $n > 2$ and that $k \equiv 1 + 2^{n-1} \pmod{2^n}$. Since $\bar{\rho}^2 = 1$, the element ρ^2 lies in A. Hence it lies in $C_A(\rho) = \langle \tau^2 \rangle$. So $\rho^2 = \tau^{2l}$, for some integer l. If h is any integer, then

$$(\rho\tau^h)^2 = \rho\tau^h\rho\tau^h = \rho^2(\rho^{-1}\tau^h\rho)\tau^h = \tau^{2l}\tau^{(1+2^{n-1})h}\tau^h = \tau^{2(l+(1+2^{n-2})h)}.$$

Since $n > 2$, the integer $1 + 2^{n-2}$ is a unit modulo 2^n. Hence we can choose h so that $(1 + 2^{n-2})h \equiv -l \pmod{2^n}$. Then $(\rho\tau^h)^2 = 1$. So $\rho\tau^h$ is an involution in T, which is impossible since $\rho\tau^h \notin A$ and the only involution ι lies in A.

Suppose that $n > 2$ and that $k \equiv -1 + 2^{n-1} \pmod{2^n}$. Then $\rho^2 \in C_A(\rho) = \langle \tau^{2^{n-1}} \rangle = \langle \iota \rangle$. Since ρ is not an involution, we must have $\rho^2 = \tau^{2^{n-1}}$. But then

$$(\rho\tau)^2 = \rho\tau\rho\tau = \rho^2(\rho^{-1}\tau\rho)\tau = \tau^{2^{n-1}}\tau^{-1+2^{n-1}}\tau = \tau^{2^n} = 1.$$

So $\rho\tau$ is an involution not in A, which is impossible.

In view of the above arguments, we must have $n \geq 2$ and $k \equiv -1 \pmod{2^n}$. Since $\rho^2 \in C_A(\rho) = \langle \tau^{2^{n-1}} \rangle$ and $\rho^2 \neq 1$, we have $\rho^2 = \tau^{2^{n-1}} = \iota$. Therefore $\langle \rho, A \rangle = \langle \rho, \tau \rangle$ is a generalized quaternion group of order 2^{n+1} (by (6.1)).

If $\langle \rho, A \rangle < T$, then $\langle \bar{\rho} \rangle < \bar{T}$. The above arguments show that $\bar{\rho}$ is the only involution in $\bar{T}$. So there must exist a $\sigma \in T$ whose image $\bar{\sigma} \in \bar{T}$ satisfies $\bar{\sigma}^2 = \bar{\rho}$. Then $\tau^\sigma = \tau^m$ for some integer m satisfying $m^2 \equiv -1 \pmod{2^n}$. Since $n \geq 2$, this implies $m^2 \equiv -1 \pmod 4$, which is impossible. Therefore $\langle \rho, A \rangle = T$, and the lemma is proved.

Now assume that ι is the only involution in T (our Sylow subgroup). By the above lemma, T is either cyclic or generalized quaternion. If T is cyclic, then $G = TO_{2'}(G)$ (see Section I.6 of Huppert, 1967). So the image of ι is central in $G/O_{2'}(G) \simeq T$, which is the theorem in this case. If T is generalized quaternion of order 2^{n+1}, for $n \geq 2$, then Theorem 6.8 (for $n \geq 3$) or Theorem 14.11 (for $n = 2$) give us a normal subgroup $N < G$ containing ι. This contradicts (15.3). Therefore we can assume from now on that

$$T \text{ contains an involution other than } \iota. \tag{15.7}$$

Another "trivial case" is that in which some involution ι_1 is central in G. If $\iota_1 = \iota$, the theorem is clearly true. If $\iota_1 \neq \iota$, then the image $\bar{\iota}$ of ι in $\bar{G} = G/\langle \iota_1 \rangle$ satisfies (15.2) with respect to the image $\bar{T}$ of T, which is a 2-Sylow subgroup of $\bar{G}$. Indeed, if $\bar{\iota}^{\bar{\sigma}} \in \bar{T}$, for some $\bar{\sigma} \in \bar{G}$, and $\sigma \in G$ has $\bar{\sigma}$ as its image in $\bar{G}$, then ι^σ lies in the inverse image T of $\bar{T}$. So $\iota^\sigma = \iota$ (by (15.2)) and $\bar{\iota}^{\bar{\sigma}} = \bar{\iota}$. Since $|\bar{G}| < |G|$, induction tells us that $\bar{\iota} \in Z(\bar{G} \bmod O_{2'}(\bar{G}))$. It follows that the inverse image in G of $\langle \iota \rangle O_{2'}(\bar{G})$ is a normal subgroup containing ι. By (15.3), it must be G itself. The inverse image N of $O_{2'}(\bar{G})$ is then a normal subgroup of G with $G = \langle \iota \rangle N$. The 2-Sylow subgroup $\langle \iota_1 \rangle$ of N is cyclic and centralizes N. We conclude that $N = \langle \iota_1 \rangle \times O_{2'}(N)$. Now $O_{2'}(N) = O_{2'}(G)$. Since $G/O_{2'}(G)$ has order 4, it is abelian. So the theorem is true in this case. Therefore we can assume from now on that

$$C_G(\iota_1) < G, \quad \textit{for all involutions } \iota_1 \in G. \tag{15.8}$$

One almost obvious remark is

LEMMA 15.9. *If two G-conjugates ι^σ, ι^τ of ι lie in the same 2-subgroup P of G, then $\iota^\sigma = \iota^\tau$.*

Proof. The 2-subgroup P is contained in a conjugate T^π of the 2-Sylow subgroup T. So $\iota^{\sigma\pi^{-1}}, \iota^{\tau\pi^{-1}}$ both lie in T. By (15.2), $\iota^{\sigma\pi^{-1}} = \iota = \iota^{\tau\pi^{-1}}$. Hence $\iota^\sigma = \iota^\tau$.

COROLLARY 15.10. *If H is a subgroup of G such that $\iota \in H < G$, then $\iota \in Z(H \bmod O_{2'}(H))$.*

Proof. Applying the lemma to a 2-Sylow subgroup P of H containing ι,

we conclude that H, P and ι satisfy the hypotheses of the theorem. Since $|H| < |G|$, induction gives this corollary.

Now we come to the heart of the matter.

LEMMA 15.11. *Let ι_2 be any involution in T other than ι. If χ is an irreducible character in $B_0(G)$ and $\sigma \in G$, then $\chi(\iota\iota_2^\sigma) = \chi(\iota\iota_2)$.*

Proof. First assume that $\iota\iota_2^\sigma$ is an involution. Then ι centralizes ι_2^σ. We can therefore find an element $\pi \in C_G(\iota_2^\sigma)$ such that ι and $\iota^{\sigma\pi}$ lie in the same 2-Sylow subgroup P of $C_G(\iota_2^\sigma)$. By Lemma 15.9 we have $\iota = \iota^{\sigma\pi}$. Hence $\iota\iota_2^\sigma = \iota^{\sigma\pi}\iota_2^{\sigma\pi}$ is G-conjugate to $\iota\iota_2$. Therefore $\chi(\iota\iota_2^\sigma) = \chi(\iota\iota_2)$ in this case.

Now let $\tau = \iota\iota_2^\sigma$ be arbitrary. By Proposition 5.20, the group $D = \langle \iota, \iota_2^\sigma \rangle$ is dihedral, with $\langle \tau \rangle$ as a cyclic normal subgroup of index 2 inverted by both ι and ι_2^σ. For any integer i we have

$$(\iota_2^\sigma)^{\tau^i} = \tau^{-i}\iota_2^\sigma\tau^i = \tau^{-i}(\iota_2^\sigma)^{-1}\tau^i(\iota_2^\sigma)(\iota_2^\sigma) = \tau^{-2i}\iota_2^\sigma, \tag{15.12}$$

since ι_2^σ is an involution. If $|\langle \tau \rangle|$ is odd, we can choose i so that $\tau^{-2i}\iota_2^\sigma = \tau\iota_2^\sigma = \iota$. This is impossible, since ι_2 is not G-conjugate to ι (by (15.2)). Therefore $|\langle \tau \rangle|$ is even, and $\langle \tau \rangle$ contains an involution ι_1 centralized by all of D.

In view of (15.8) the group $H = C_G(\iota_1)$ is properly contained in G. This group contains D and hence ι. By Corollary 15.10, ι lies in $Z(H \bmod O_{2'}(H))$. Therefore $\tau = \iota\iota_2^\sigma \equiv \iota_2^\sigma\iota \pmod{O_{2'}(H)}$. It follows that $\tau^2 \in O_{2'}(H)$. Hence $\langle \tau^2 \rangle$ has odd order, and we are in the following situation:

$$\langle \tau \rangle = \langle \iota_1 \rangle \times \langle \tau^2 \rangle, \qquad \langle \tau^2 \rangle = \langle \tau \rangle \cap O_{2'}(H). \tag{15.13}$$

The Brauer second and third main theorems tell us that there exist integers a_j, one for each irreducible character $\phi_j \in B_0(H)$, such that

$$\chi(\iota_1\rho) = \sum_{\phi_j \in B_0(H)} a_j\phi_j(\iota_1\rho),$$

for all elements ρ of odd order in H. From (15.13) we see that $\tau = \iota_1\rho$, where $\rho \in \langle \tau^2 \rangle \leq O_{2'}(H)$ has odd order. Proposition 13.28 then implies that $\phi_j(\iota_1\rho) = \phi_j(\iota_1)$, for all $\phi_j \in B_0(H)$. So, we have

$$\chi(\iota\iota_2^\sigma) = \chi(\tau) = \chi(\iota_1\rho) = \sum_{\phi_j \in B_0(H)} a_j\phi_j(\iota_1\rho) = \sum_{\phi_j \in B_0(H)} a_j\phi_j(\iota_1) = \chi(\iota_1).$$

But (12.12) and (13.13) imply that $\iota_1 = \iota(\iota_2^\sigma)^{\tau^i}$, for some integer i. Since ι_1 is an involution, we have already seen that this implies $\chi(\iota_1) = \chi(\iota\iota_2)$. Therefore $\chi(\iota\iota_2^\sigma) = \chi(\iota_1) = \chi(\iota\iota_2)$, and the lemma is proved.

Let I be the conjugacy class of ι in G, and $\tilde{I}$ be the corresponding class sum. Define I_2, $_2$ similarly for any involution $\iota_2 \neq \iota$ in T. If χ is any irreducible character in $B_0(G)$, then (4.31) gives

$$\chi(\tilde{I})\chi(\tilde{I}_2) = \chi(1)\chi(\tilde{I}\tilde{I}_2).$$

Evidently $\tilde{I}\tilde{I}_2$ is a sum of $|I||I_2|$ elements of the form $\iota^\sigma \iota_2^\tau = (\iota \iota_2^{\tau\sigma^{-1}})^\sigma$, for $\sigma, \tau \in G$. By Lemma 15.11, the value of χ at any such element is $\chi(\iota\iota_2)$. Therefore the above equation becomes

$$|I|\chi(\iota)|I_2|\chi(\iota_2) = \chi(1)|I||I_2|\chi(\iota\iota_2)$$

or

$$\chi(\iota)\chi(\iota_2) = \chi(1)\chi(\iota\iota_2).$$

Since ι is central in T (by (15.2)), the product $_2$ $\iota\iota$is also an involution different from ι in T. Applying the above equation to $\iota\iota_2$ in place of ι_2, we obtain

$$\chi(\iota)\chi(\iota\iota_2) = \chi(1)\chi(\iota_2).$$

Hence,

$$\chi(\iota)^2\chi(\iota_2) = \chi(\iota)\chi(1)\chi(\iota\iota_2) = \chi(1)^2\chi(\iota_2).$$

If $\chi(\iota_2) \neq 0$, we conclude that $\chi(\iota) = \pm\chi(1)$, and hence that $\iota \in Z(G \bmod \text{Ker}(\chi))$ (by Proposition 4.38(b)). So we have

If χ is any irreducible character in $B_0(G)$ such that $\chi(\iota_2) \neq 0$, for some involution $\iota_2 \in T\backslash\langle\iota\rangle$, then $\iota \in Z(G \bmod \text{Ker}(\chi))$. (15.14)

Let N be the intersection of the kernels, $\text{Ker}(\chi)$, of all the irreducible characters χ of G satisfying the hypotheses of (15.14). Then N is a normal subgroup of G and $\iota \in Z(G \bmod N)$. From Proposition 13.28 we see that $N \geq O_{2'}(G)$. To show that $N \leq O_{2'}(G)$, which will finish the proof of the theorem, it suffices to prove that no involution of T lies in N.

Suppose that N contains an involution ι_2 of T other than ι. Then the definition of N and Proposition 4.38(a) imply that the value $\chi(\iota_2)$ is either 0 or $\chi(1)$, for any irreducible character $\chi \in B_0(G)$. Now Theorem 12.13 tells us that

$$0 = \sum_{\chi \in B_0(G)} \chi(\iota_2)\chi(1) = \sum_{\chi \in B_0(G),\ \chi(\iota_2) \neq 0} \chi(1)^2$$

Since at least one χ, the trivial character, satisfies $\chi(\iota_2) \neq 0$, and since each $\chi(1)$ is a positive integer, this is impossible. So $\iota_2 \notin N$.

Suppose that $\iota \in N$. Then $N = G$ by (15.3). So N contains an involution $\iota_2 \in T$ other than ι, by (15.7). We have just seen that this is impossible. Therefore N contains no involutions, $N = O_{2'}(G)$, and the theorem is proved.

BIBLIOGRAPHY

Curtis, C. W. and Reiner, I. (1962). "Representation Theory of Finite Groups and Associative Algebras". Interscience. New York.

Feit, W. (1969). "Representations of Finite Groups". Department of Mathematics, Yale University.

Huppert, B. (1967). "Endliche Gruppen I". Springer–Verlag, Heidelberg.