Invent. math. 109, 187–210 (1992)

Inventiones mathematicae

Counting characters in blocks, I *

Everett C. Dade

University of Illinois at Urbana-Champaign, Department of Mathematics, 1409 W. Green St., Urbana, IL 61801, USA

Oblatum 2-I-1992

We're going to present a conjecture expressing the number of complex irreducible characters with a fixed height h in a p-block B of a finite group G in terms of the numbers of complex irreducible characters of related heights h' in related blocks B' of certain p-local subgroups of G. The present paper treats only the simplest form of this conjecture, that for ordinary characters. Later papers in this series will consider the same conjecture for projective characters, for projective characters invariant under a given automorphism group of G and, finally, for invariant projective characters having a fixed Clifford extension and fixed homomorphism relating that extension to the Clifford extension for the block B. Each of these forms of the conjecture implies all the preceding ones, but is harder to state or verify than they are. In particular, the final form is quite complicated and delicate. However, it has one vital property that the others lack – it holds for arbitrary finite groups G if it holds for all non-abelian simple G. So its proof can be reduced to a long computation for each of the finite simple groups.

It is quite easy to look for a counterexample to these conjectures. You merely take your favorite simple group G, one whose local subgroup structure you know intimately. You compute the numbers of characters of various heights in the blocks of certain subgroups of G, including G itself. Finally, you calculate an alternating sum with these numbers, as in (6.4) or (6.6) below. If that sum is not zero you have found a counterexample. In that case please check your calculations and then inform the author, who will be *very* interested to learn of your discovery. If, on the other hand, that sum turns out to be zero, then you have verified a form of the conjecture for G. If that form is equivalent to the final form for G, then you have contributed one step towards the ultimate proof of all these conjectures. Thus your effort to compute this sum for G will be worthwhile whatever the outcome may be.

When are the weaker conjectures equivalent to the final one? The ordinary conjecture studied in this paper has this property if G has both trivial Schur multiplier Mult(G) and trivial outer automorphism group Out(G). These conditions are satisfied by 11 of the 26 sporadic simple groups (see [3, Table 1]).

* This research was partially supported by a grant from the National Science Foundation

In § 10 and § 11 below we verify the ordinary conjecture (and hence the final conjecture) for two of these eleven groups, namely J_1 and M_{11}. Someone should take a look at the other nine groups, even though the largest ones, such as the monster M, will have to be handled by computers.

The projective form of the conjecture is equivalent to the final one for all groups G with $\mathrm{Out}(G)=1$. The invariant projective form is equivalent to the final one for all G such that $\mathrm{Out}(G)$ has only cyclic Sylow q-subgroups for each prime q. From the tables in [3] it follows that the only finite simple groups not satisfying this last condition are of Lie type. So the final and most delicate form of the conjecture only has to be verified explicitly for simple groups of Lie type. Since a number of deep algebraic constructions are available to help us study representations of those groups, we can at least hope that the conjecture will be settled for them by general arguments without treating each case separately.

The alternating sums used to state our conjectures are over representatives for the G-conjugacy classes in various familes $\mathscr{X}$ of increasing chains C of p-subgroups of G. The local subgroups involved are the normalizers $N_G(C)$ of these chains. The idea that conjectures about numbers of characters in blocks can best be expressed as the vanishing of such alternating sums is due to G. Robinson, who pointed out several years ago in [10] that Alperin's Weight Conjecture can be written in this form. Thanks to his work [9] with Knörr, it is easy to show in § 8 below that this conjecture of Alperin is a consequence of the ordinary form of our conjecture. We shall see in the next paper that the Alperin-McKay Conjecture follows from the projective form of our conjecture. By [9, 5.6] these two Alperin conjectures imply half of the Brauer Height Conjecture.

The first three sections of the present paper give a quick survey of properties of p-subgroups, families of p-chains and alternating sums. The next two sections review block theory over a valuation ring $\mathfrak{R}$ whose field of fractions $\mathfrak{F}$ is a splitting field of characteristic zero for every subgroup H of G. It should be remarked that our conjectures are actually stated using irreducible $\mathfrak{F}$-characters instead of the equivalent complex irreducible characters. Furthermore, their statements refer to the defect $d(\chi)$ of a character χ instead of the height $h(\chi)$ of χ. The two numbers $d(\chi)$ and $h(\chi)$ are related by (5.7).

The ordinary conjecture itself is given in several forms in § 6. One of the disadvantages of alternating sums over chains of p-subgroups is that they don't work right when $O_p(G)>1$. For this reason the conjecture is restricted to the situation where $O_p(G)=1$. Indeed, Example 7.3 shows that it can be invalid without this restriction. Another condition in the conjecture is that B must have positive defect. These case where $d(B)=0$ is handled by Proposition 7.1.

We have already mentioned that Alperin's Weight Conjecture is derived from the ordinary conjecture in § 8. It is a simple matter in § 9 to verify that the ordinary conjecture holds for blocks with cyclic defect groups (in fact, all our conjectures do). This avoids a lot of computations when we look at actual examples in § 10 and § 11.

As of this writing (December 18, 1991), the author has verified the final conjecture for all primes when G is one of the simple groups M_{11}, M_{12}, J_1, $L_2(q)$ or $Sz(q)$ (in the notation of [3]). J. Huang has verified the ordinary conjecture for $G=M_{22}$. This is not a long list of examples. Additions to it would be more than welcome.

1. Radical p-subgroups

Let G be any finite multiplicative group. We denote the identity element of G by $1 = 1_G$, and the center of G by $Z(G)$. As usual, we write $H \leqq G$ to indicate that H is a subgroup of G, and $H \trianglelefteq G$ to indicate that H is a normal subgroup of G. To say that H is also properly contained in G we write $H < G$ or $H \lhd G$, respectively.

Conjugation in G is written exponentially, so that

$$\sigma^\tau = \tau^{-1} \sigma \tau \in G \quad \text{and} \quad H^\tau = \tau^{-1} H \tau \leqq G,$$

for any $\sigma, \tau \in G$ and any $H \leqq G$. If $H, K \leqq G$, then $N_K(H)$ and $C_K(H)$ denote the normalizer and centralizer, respectively, of H in K. We often replace $N_K(H)$ and $C_K(H)$ by $N(H \text{ in } K)$ and $C(H \text{ in } K)$, respectively, when the expression for K is complicated. For example, we would write $C(H \text{ in } N_G(K))$ rather than $C_{N_G(K)}(H)$.

Throughout these papers we fix a prime p. We use the usual symbol $O_p(G)$ to denote the largest normal p-subgroup of G. We write $\mathrm{Syl}_p(G)$ for the family of all Sylow p-subgroups of G. If P is a p-group, then $\Omega(P)$ will denote its subgroup generated by all $\sigma \in P$ satisfying $\sigma^p = 1$. The product of operators such as Z, O_p, N_G, etc. is defined to be their composition. Thus ZO_p is the operator sending G to $ZO_p(G) = Z(O_p(G))$, while $O_p N_G \Omega Z$ would send any p-subgroup P of G to the p-subgroup

$$O_p N_G \Omega Z(P) = O_p(N_G(\Omega(Z(P)))).$$

Alperin and Fong [2] have defined a *radical p-subgroup* of G to be any p-subgroup P of G satisfying

$$(1.1) \qquad P = O_p N_G(P).$$

Evidently any Sylow p-subgroup of G is a radical p-subgroup of G. More generally, we have

(1.2) *Any defect group D of any p-block B of G is a radical p-subgroup of G.*

This follows immediately from [4, III.8.15].

Further properties of radical p-subgroups are consequences of

Lemma 1.3 *Let P be any radical p-subgroup of G, and Q be any p-subgroup of G normalized by $N_G(P)$. Then $Q \leqq P$.*

Proof. Since P normalizes Q, the product PQ is also a p-subgroup of G normalized by $N_G(P)$. It follows that $N_{PQ}(P)$ is a normal p-subgroup of $N_G(P)$ containing P. In view of (1.1) we have

$$P \leqq N_{PQ}(P) \leqq O_p N_G(P) = P.$$

So $P = N_{PQ}(P)$. Because the p-group PQ is nilpotent, this forces it to equal its subgroup P. Therefore $Q \leqq PQ = P$, and the lemma is proved.

The subgroup $O_p(G)$ is a very special radical p-subgroup of G.

Proposition 1.4 *Any radical p-subgroup of G contains $O_p(G)$. Furthermore, $O_p(G)$ is a radical p-subgroup of G. Hence $O_p(G)$ is the unique minimal radical p-subgroup of G.*

Proof. The first statement follows from Lemma 1.3 applied to $Q=O_p(G)$. Since this Q is a normal subgroup of G, it satisfies

$$O_p N_G(Q)=O_p(G)=Q.$$

By (1.1) this proves the second statement of the proposition. The rest of the proposition follows immediately from this.

Corollary 1.5 *The only radical p-subgroup P of G satisfying $P \trianglelefteq G$ is $P=O_p(G)$.*

Proof. The proposition tells us that $O_p(G)$ is a normal radical p-subgroup of G. Conversely, any normal radical p-subgroup P must satisfy

$$P=O_p N_G(P)=O_p(G)$$

by (1.1). So the corollary holds.

If we apply the operator $O_p N_G$ to any p-subgroup Q of G, we obtain a new p-subgroup $O_p N_G(Q)$. Since Q is a normal p-subgroup of $N_G(Q)$, it satisfies

$$Q \leqq O_p N_G(Q).$$

Repeating this process, we obtain an increasing chain

$$Q \leqq O_p N_G(Q) \leqq (O_p N_G)^2(Q) \leqq (O_p N_G)^3(Q) \leqq \dots$$

of p-subgroups of G. Since G is finite, this chain must break off with

$$(1.6) \qquad (O_p N_G)^i(Q)=(O_p N_G)^{i+1}(Q)=\dots=(O_p N_G)^\infty(Q)$$

for some $i \geqq 0$. We call $P=(O_p N_G)^\infty(Q)$ the *radical p-closure of Q* in G. It is evident that P is a radical p-subgroup of G containing Q such that

$$(1.7) \qquad N_G(Q) \leqq N_G(P).$$

This implies that the normalizers of radical p-subgroups control the fusion of p-elements und p-subgroups in G (see [7, §X.4]).

2. Radical p-chains

A *p-chain* C of G is any non-empty, strictly increasing chain

$$(2.1) \qquad C\colon P_0 < P_1 < \dots < P_n$$

of p-subgroups P_i of G. Its *length* $|C|$ is the number $n \geqq 0$ of its inclusions. So C consists of $|C|+1$ subgroups P_i, starting with its *initial* subgroup P_0 and ending with its *final* subgroup P_n. For each $i=0, 1, \dots, n$ we denote by C_i the *initial subchain*

$$(2.2\text{a}) \qquad C_i\colon P_0 < P_1 < \dots < P_i$$

of C with length i, and by C^i the *final subchain*

(2.2b) $$C^i\colon P_i < P_{i+1} < \dots < P_n$$

of C with length $n-i$. Thus C_n and C^0 are both C itself, while C_0 and C^n just consist of P_0 and P_n, respectively.

The group G acts by conjugation on the family $\mathscr{C}=\mathscr{C}(G)$ of all p-chains of G. Under this action any $\sigma \in G$ sends the p-chain C of (2.1) to the p-chain

(2.3) $$C^\sigma\colon P_0^\sigma < P_1^\sigma < \dots < P_n^\sigma.$$

The stabilizer of C in any subgroup $K \leqq G$ is then the *normalizer*

(2.4) $$N_G(C) = N(C \text{ in } K) = N_K(P_1) \cap N_K(P_2) \cap \dots \cap N_K(P_n)$$

of C in K. It is clear from this and (2.2a) that

(2.5a) $$N_K(C) = N_K(C_{n-1}) \cap N_K(P_n) = N(P_n \text{ in } N_K(C_{n-1}))$$

whenever $n > 0$. We also have

(2.5b) $$N_K(C) = N_K(C_i) \cap N_K(C^i) = N(C^i \text{ in } N_K(C_i))$$

for any $i = 0, 1, \dots, n$.

By a *radical p-chain* of G we mean any p-chain $C\colon P_0 < P_1 < \dots < P_n$ of G satisfying

(2.6a) $$P_0 = O_p(G)$$

and

(2.6b) $$P_i \text{ is a radical } p\text{-subgroup of } N_G(C_{i-1}),$$

for each $i = 1, 2, \dots, n$. In view of (1.1) and (2.5a) the condition (2.6b) is equivalent to

(2.6c) $$P_i = O_p N_G(C_i)$$

for all $i = 1, 2, \dots, n$. Under this form radical p-chains were briefly mentioned in the remarks following [9, 3.4], although Robinson had already used them in several earlier, privately circulated preprints such as [10]. We denote by $\mathscr{R}=\mathscr{R}(G)$ the family of all radical p-chains of G. Clearly $\mathscr{R}$ is a G-invariant subfamily of $\mathscr{C}$ under the conjugation action (2.3).

We collect several elementary properties of radical p-chains in

Proposition 2.7 *If $C\colon P_0 < P_1 < \dots < P_n$ is a radical p-chain of G, then*
(a) $P_n = O_p N_G(C)$.
(b) *Each P_i, for $i = 0, 1, \dots, n$, is a normal p-subgroup of both $N_G(C)$ and P_n.*
(c) *$N_G(C) = G$ if and only if C is the unique radical p-chain $C\colon O_p(G)$ of length* 0.
(d) *For each $i = 0, 1, \dots, n$, the initial subchain C_i is a radical p-chain of G, and the final subchain C^i is a radical p-chain of $N_G(C_i)$.*

Proofs. (a) If $n=0$, then C consists only of $P_0=O_p(G)$ by (2.6a). In this case $N_G(C)=G$ and (a) holds trivially. If $n>0$, then (a) follows from (2.6c) for $i=n$.

(b) Since $N_G(C)$ normalizes each P_i by (2.4), statement (b) follows from (a) and the inclusions (2.1).

(c) If $|C|=0$, then the only member of C is $O_p(G)$. Hence $N_G(C)=G$ in this case.

If $|C|>0$, then P_1 is a radical p-subgroup of $G=N_G(P_0)=N_G(C_0)$ by (2.6b, a). Since $P_1>P_0=O_p(G)$, Corollary 1.5 implies that $N_G(C)\leqq N_G(P_1)<G$ in this case. So (c) holds.

(d) The fact that C_i lies in $\mathscr{R}(G)$ follows immediately from (2.6). In view of (2.5b), so does the statement that $C^i\in\mathscr{R}(N_G(C_i))$.

We should remark that the converse to Proposition 2.7(d) holds, i.e. that

(2.8) *If C is any p-chain of G starting with a radical p-chain C_i of G and continuing with a radical p-chain C^i of $N_G(C_i)$, then C is a radical p-chain of G.*

This follows immediately from (2.5b) and (2.6).

3. Alternating sums

In order to treat alternating sums with a generality sufficient for the later papers in this series, we introduce two new groups E and H satisfying

(3.1) $$E \text{ is a finite group with } G\trianglelefteq E \quad\text{and}\quad H\leqq E.$$

Then E acts by conjugation (2.3) on the family $\mathscr{C}$ of all p-chains of G. Hence so does its subgroup H. If $\mathscr{X}$ is any H-invariant subfamily of $\mathscr{C}$, then $\mathscr{X}/H$ will denote an arbitrary set of representatives for the H-orbits in $\mathscr{X}$. We only use this notation in situations where the actual choice of the representatives in $\mathscr{X}/H$ is irrelevant.

We fix an additive group A and a function $f\colon \mathscr{C}\to A$. We assume that

(3.2a) $$f(C)=f(C') \text{ whenever } C, C'\in\mathscr{C} \text{ satisfy } N_E(C)=N_E(C'),$$

and

(3.2b) $$f(C^\sigma)=f(C) \quad\text{for all } C\in\mathscr{C} \quad\text{and}\quad \sigma\in H.$$

Then the *alternating sum*

(3.3) $$S(f,\mathscr{X}/H)=\sum_{C\in\mathscr{X}/H}(-1)^{|C|}f(C)$$

is a well-defined element of A for any H-invariant subfamily $\mathscr{X}$ of $\mathscr{C}$.

Alternating sums of the above type have been studied by several mathematicians, starting with Quillen (see [9] and the papers cited there). The result of their work is that the sum $S(f,\mathscr{X}/H)$ has the same value for many natural subfamilies $\mathscr{X}$ of $\mathscr{C}$, and that this value is zero when $O_p(G)>1$. The idea behind the proofs of their theorems is quite simple. To some chain $C\in\mathscr{X}$ we associate another chain $C'\in\mathscr{X}$ having the same normalizer $N_E(C')=N_E(C)$ in E but length of opposite parity, so that $(-1)^{|C'|}=-(-1)^{|C|}$. Then (3.2a) implies that the terms for the orbits of C and C' cancel in the sum (3.3). So $S(f, \mathscr{X}/H)=S(f, \mathscr{X}'/H)$, where $\mathscr{X}'$ is the subfamily obtained by removing the H-orbits of C and C' from $\mathscr{X}$. After repeatedly removing the orbits of such pairs C, C' from $\mathscr{X}$, we are left with a smaller H-invariant subfamily $\mathscr{Y}$ having the same alternating sum $S(f, \mathscr{Y}/H)=S(f, \mathscr{X}/H)$. Sometimes we can even remove all the orbits from $\mathscr{X}$ in this way, in which case $\mathscr{Y}$ is empty and $S(f, \mathscr{X}/H)=S(f, \mathscr{Y}/H)=0$.

We illustrate this with the case where $\mathscr{X}$ is the family $\mathscr{C}$ of all p-chains of G. To each p-chain C: $P_0<P_1<\ldots<P_n$ with initial group $P_0>1$ we associate the p-chain C': $1<P_0<P_1<\ldots<P_n$, with initial group 1. Clearly $N_E(C')=N_E(C)$, while the lengths of C' and C have opposite parities. So we may remove the H-orbits of all such C and their associated C' from $\mathscr{C}$ without changing the sum $S(f, \mathscr{C}/H)$. After we do so the only remaining orbit in $\mathscr{C}$ just consists of the single p-chain C_0: 1 whose only member is the trivial subgroup 1 of G. We conclude that

$$S(f, \mathscr{C}/H)=S(f, \{C_0\}/H)=f(C_0). \tag{3.4}$$

So alternating sums over $\mathscr{C}/H$ are rather trivial.

To avoid situations of the above sort we stick to subfamilies $\mathscr{X}$ of $\mathscr{C}$ which are "anchored" by some fixed H-invariant subgroup K of G, in the sense that each chain $C\in\mathscr{X}$ has K as its initial subgroup P_0. By (2.6a) the family $\mathscr{R}=\mathscr{R}(G)$ of all radical p-chains of G is anchored in this way by $O_p(G)$. In [9] Knörr and Robinson choose 1 as the anchor for all their families. Thus their basic family $\mathscr{P}$ consists of all p-chains C of G starting with

$$P_0=1. \tag{3.5a}$$

They also use the family $\mathscr{N}=\mathscr{N}(G)$ of all p-chains C: $P_0<P_1<\ldots<P_n$ of G satisfying both (3.5a) and

$$P_i \trianglelefteq P_n, \tag{3.5b}$$

for all $i=0, 1, \ldots, n$. In addition they discuss the family $\mathscr{E}=\mathscr{E}(G)$ of all $C\in\mathscr{P}$ consisting only of elementary abelian p-subgroups P_i of G, and the family $\mathscr{U}=\mathscr{U}(G)$ of all $C\in\mathscr{P}$ consisting only of radical p-subgroups P_i of G. Since we shall use the families $\mathscr{N}$ and $\mathscr{E}$ extensively, we call their members the *normal* and the *elementary* p-chains, respectively, of G. The family $\mathscr{R}$ is much more useful than $\mathscr{U}$. So its members have the honor of being called the radical p-chains of G.

In the special case where $E=G=H$ Knörr and Robinson showed that

$$S(f, \mathscr{P}/H)=S(f, \mathscr{N}/H)=S(f, \mathscr{E}/H)=S(f, \mathscr{U}/H) \tag{3.6}$$

(see [9, 3.3]). Their arguments work equally well for any E and H satisfying (3.1). So we shall treat (3.6) as a known fact. However, the equality between the sums (3.6) and $S(f, \mathscr{R}/H)$ when $O_p(G)=1$ is left as an exercise for the reader in the remarks following [9, 3.4]. Since we shall need that equality, we give its proof in detail.

Proposition 3.7 *The alternating sum $S(f, \mathscr{N}/H)$ is equal to $S(f, \mathscr{R}/H)$ if $O_p(G)=1$, and is equal to 0 if $O_p(G)>1$.*

Proof. Let $\mathcal{M}$ be the H-invariant subfamily $\mathcal{N}-\mathcal{R}$ of $\mathcal{N}$. Every chain $C\in\mathcal{R}$ begins with $P_0=O_p(G)$ by (2.6a), while all the chains in $\mathcal{N}$ begin with 1 by definition. It follows that $\mathcal{M}=\mathcal{N}$ if $O_p(G)>1$. On the other hand, (2.6a) and Proposition 2.7(b) imply that $\mathcal{R}\subseteq\mathcal{N}$ if $O_p(G)=1$. We conclude that the present proposition is equivalent to the single equation

$$S(f, \mathcal{M}/H)=0, \tag{3.8}$$

whatever the value of $O_p(G)$ may be.

Let C: $P_0=1<P_1<\ldots<P_n$ be any p-chain in $\mathcal{N}$, and C_i: $P_0<P_1<\ldots<P_i$ be its initial subchain of length i for any $i=0, 1, \ldots, n$. It follows from (3.5b) that

$$P_j\leqq P_n\leqq N_G(C_i) \tag{3.9}$$

for all $i, j=0, 1, \ldots, n$. In particular P_i is a normal p-subgroup of $N_G(C_i)$. So we have

$$P_i\leqq O_p N_G(C_i) \tag{3.10}$$

for any $i=0, 1, \ldots, n$.

If C lies in $\mathcal{R}$ then equality always holds in (3.10) by (2.6a, c). On the other hand, if equality always holds in (3.10), then

$$1=P_0=O_p N_G(C_0)=O_pN_G(1)=O_p(G).$$

So $C\in\mathcal{R}$ by (2.6a, c). Thus $\mathcal{M}$ consists of all $C\in\mathcal{N}$ for which the inclusion (3.10) is strict for some i. In particular, if $C\in\mathcal{M}$, then the set of all $i=0, 1, \ldots, n$ for which (3.10) is a strict inclusion has a unique largest member $k=k(C)$.

Suppose that the above chain C lies in $\mathcal{M}$ with $k<n$. Then P_{k+1} is a p-subgroup of $N_G(C_k)$ by (3.9). The maximality of k implies that

$$P_{k+1}=O_p N_G(C_{k+1})=O_p N(P_{k+1} \text{ in } N_G(C_k)).$$

Therefore P_{k+1} is a radical p-subgroup of $N_G(C_k)$. So Proposition 1.4 tells us that

$$O_p N_G(C_k)\leqq P_{k+1}. \tag{3.11}$$

We denote by $\mathcal{M}_0$ the subfamily of all $C\in\mathcal{M}$ such that $k<n$ and (3.11) is equality. Clearly $\mathcal{M}_0$ is an H-invariant subfamily of $\mathcal{M}$, as is the complementary subfamily $\mathcal{M}_1=\mathcal{M}-\mathcal{M}_0$. If $C\in\mathcal{M}_0$, we define C' to be the p-chain

$$C'\colon P_0<P_1<\ldots<P_k<P_{k+2}<\ldots<P_n$$

obtained by omitting the subgroup $P_{k+1}=O_p N_G(C_k)$ from C. (Notice that C' is just C_k if $n=k+1$.) Clearly C' is also a normal p-chain of G with $N_E(C')=N_E(C)$ and $(-1)^{|C'|}=-(-1)^{|C|}$. Furthermore, $C'\notin\mathcal{R}$ since $C'_k=C_k\notin\mathcal{R}$. Therefore $C'\in\mathcal{M}$.

Because $P_{k+1}=O_p N_G(C_k)$ is normalized by $N_G(C_k)$, we have

$$\begin{aligned} N_G(C'_i)&=N_G(C_i) && \text{if } i=0, 1, \ldots, k,\\ &=N_G(C_{i+1}) && \text{if } i=k+1, \ldots, n-1.\end{aligned}$$

It follows that $k(C')=k\ (C)=k$ and that either $k=n-1=|C'|$, or $k<n-1$ and the $(k+1)$st subgroup P_{k+2} in C' properly contains $O_p N_G(C'_k)=P_{k+1}$. In either case C' belongs to $\mathcal{M}_1$. Of course C can be recovered from C' by reinserting the missing subgroup P_{k+1}, which only depends on C' since

$$P_{k+1}=O_p N_G(C_k)=O_p N_G(C'_k).$$

So the correspondence $C \leftrightarrow C'$ is one-to-one between all $C \in \mathcal{M}_0$ and some $C' \in \mathcal{M}_1$.

In fact, every chain C': $Q_0<Q_1<\ldots<Q_{n-1}$ in $\mathcal{M}_1$ corresponds in the avove fashion to a unique chain $C \in \mathcal{M}_0$. If $k=k(C')$ is equal to $n-1$, then C is given by

$$C\colon Q_0<Q_1<\ldots<Q_{n-1}<O_p N_G(C'),$$

which exists by the definition of $k(C')$. If $k<n-1$, then C is the chain

$$C\colon Q_0<Q_1<\ldots<Q_k<O_p N_G(C'_k)<Q_{k+1}<\ldots<Q_n,$$

which exists by (3.11) for C' and the definition of $\mathcal{M}_1$. Hence $C \leftrightarrow C'$ is a one-to-one, H-invariant correspondence between all $C \in \mathcal{M}_0$ and all $C' \in \mathcal{M}_1=\mathcal{M}-\mathcal{M}_0$. So the removal from $\mathcal{M}$ of all the H-orbits corresponding to such pairs C, C' leaves only the empty family. Since this removal does not change $S(f, \mathcal{M}/H)$, we conclude that (3.8) holds. Thus the proposition is proved.

Corollary 3.12 *The alternating sums $S(f, \mathcal{P}/H)$, $S(f, \mathcal{N}/H)$, $S(f, \mathcal{E}/H)$, and $S(f, \mathcal{U}/H)$ all vanish when $O_p(G)>1$.*

Proof. This follows immediately from the proposition and (3.6).

The only reason $S(f, \mathcal{R}/H)$ does not appear among the sums in Corollary 3.12 is that the chains in $\mathcal{R}$ are anchored by $O_p(G)$ and not by 1.

4. Rings, algebras and orders

When we speak of a *ring* $\mathfrak{A}$ we mean an associative ring with identity element $1=1_{\mathfrak{A}}$. We denote by $Z(\mathfrak{A})$, $U(\mathfrak{A})$ and $J(\mathfrak{A})$ the center, unit group and Jacobson radical, respectively, of $\mathfrak{A}$. Any $\mathfrak{A}$-*module* $\mathfrak{M}$, whether right or left, is understood to be unitary in the sense that multiplication by $1_{\mathfrak{A}}$ is the identity map of $\mathfrak{M}$ onto itself. As usual, we write $\mathbb{Z}$ for the ring of all ordinary integers $0, \pm 1, \pm 2, \ldots$.

The above conventions and notation also apply when $\mathfrak{A}$ is an *algebra* over a commutative ring $\mathfrak{S}$. In particular, $\mathfrak{A}$ is then a unitary $\mathfrak{S}$-module. Furthermore, any $\mathfrak{A}$-module $\mathfrak{M}$ is automatically an $\mathfrak{S}$-module, with multiplication by any $s \in \mathfrak{S}$ being multiplication by $s1_{\mathfrak{A}} \in \mathfrak{A}$. When we speak of an $\mathfrak{S}$-*subalgebra* $\mathfrak{B}$ of $\mathfrak{A}$, we do not assume that its identity element $1_{\mathfrak{B}}$ is equal to $1_{\mathfrak{A}}$. If $1_{\mathfrak{B}}=1_{\mathfrak{A}}$ we say that $\mathfrak{B}$ is a *unitary* subalgebra of $\mathfrak{A}$. Similarly an arbitrary *homomorphism* $\gamma\colon \mathfrak{B} \to \mathfrak{A}$ of $\mathfrak{S}$-algebras need not send $1_{\mathfrak{B}}$ to $1_{\mathfrak{A}}$. We say that γ is *unitary* or *identity-preserving* if it does send $1_{\mathfrak{B}}$ to $1_{\mathfrak{A}}$.

There are plenty of valuation rings whose value groups are discrete, yet different from the additive group of $\mathbb{Z}$. To construct them, just compose together discrete, rank-one valuation rings as in [11, §VI.10]. So we prefer to speak of a "local principal ideal domain" rather than use the expression "discrete valuation ring" familiar to group theorists. Accordingly we fix $\mathfrak{R}$, $\mathfrak{F}$, and $\bar{\mathfrak{F}}$ satisfying

(4.1) *$\mathfrak{R}$ is a local principal ideal domain whose field of fraction $\mathfrak{F}$ has characteristic 0, and whose residue class field $\bar{\mathfrak{F}}=\mathfrak{R}/J(\mathfrak{R})$ has the prime characteristic p.*

We shall denote the unique maximal ideal $J(\mathfrak{R})$ of $\mathfrak{R}$ by $\mathfrak{p}$.

As usual, an $\mathfrak{R}$-*lattice* is any finitely-generated, torsion-free (and hence free) $\mathfrak{R}$-module, an $\mathfrak{R}$-*order* $\mathfrak{D}$ is any $\mathfrak{R}$-algebra which is a lattice as an $\mathfrak{R}$-module, and a $\mathfrak{D}$-*lattice* $\mathfrak{L}$ is any (right or left) $\mathfrak{D}$-module which is a lattice as an $\mathfrak{R}$-module. In that case the $\mathfrak{R}$-algebra $\mathrm{End}_{\mathfrak{D}}(\mathfrak{L})$ of all $\mathfrak{D}$-endomorphisms of $\mathfrak{L}$ is itself an $\mathfrak{R}$-order. Of course $\mathfrak{D}$ can be embedded naturally in the finite-dimensional $\mathfrak{F}$-algebra $\mathfrak{A}=\mathfrak{F}\otimes_{\mathfrak{R}}\mathfrak{D}$, and $\mathfrak{L}$ in the finitely-generated $\mathfrak{A}$-module $\mathfrak{M}=\mathfrak{F}\otimes_{\mathfrak{R}}\mathfrak{L}$, in such a way that $\mathfrak{R}$-bases of $\mathfrak{D}$ and $\mathfrak{L}$ become $\mathfrak{F}$-bases of $\mathfrak{A}$ and $\mathfrak{M}$, respectively. Then $\mathrm{End}_{\mathfrak{D}}(\mathfrak{L})$ can be identified with the $\mathfrak{R}$-suborder of $\mathrm{End}_{\mathfrak{A}}(\mathfrak{M})$ consisting of all $\mathfrak{A}$-endomorphisms of $\mathfrak{M}$ sending $\mathfrak{L}$ into itself. After this identification any $\mathfrak{R}$-basis of $\mathrm{End}_{\mathfrak{D}}(\mathfrak{L})$ is an $\mathfrak{F}$-basis of $\mathrm{End}_{\mathfrak{A}}(\mathfrak{M})$.

The Jacobson radical $J(\mathfrak{D})$ of any $\mathfrak{R}$-order $\mathfrak{D}$ contains $\mathfrak{p}\mathfrak{D}$ by Nakayama's Lemma for the $\mathfrak{R}$-lattice $\mathfrak{D}$. So the factor $\mathfrak{R}$-algebra $\mathfrak{D}/J(\mathfrak{D})$ is a finite-dimensional semi-simple algebra over the residue class field $\bar{\mathfrak{F}}=\mathfrak{R}/\mathfrak{p}$. The order $\mathfrak{D}$ is *local* if the factor $\bar{\mathfrak{F}}$-algebra $\mathfrak{D}/J(\mathfrak{D})$ is a division algebra. This happens if and only if $\mathfrak{D}$ is non-zero with $U(\mathfrak{D})=\mathfrak{D}-J(\mathfrak{D})$.

We are especially interested in the case where $\mathfrak{D}$ satisfies

(4.2) *$\mathfrak{D}$ is an $\mathfrak{R}$-order whose associated finite-dimensional $\mathfrak{F}$-algebra $\mathfrak{A}=\mathfrak{F}\otimes_{\mathfrak{R}}\mathfrak{D}$ is split and semi-simple.*

A well-known theorem of Heller [5, 2.5] implies that

(4.3) *If $\mathfrak{D}$ satisfies (4.2), then any idempotent $\bar{e}$ of the factor $\bar{\mathfrak{F}}$-algebra $\mathfrak{D}/J(\mathfrak{D})$ is the image $e+J(\mathfrak{D})$ of some idempotent e of $\mathfrak{D}$.*

This ability to lift idempotents is all that we need for block theory.

Suppose that $\mathfrak{D}$ satisfies (4.2). The blocks of $\mathfrak{D}$ correspond one-to-one to the primitive central idempotents of $\mathfrak{D}$, and hence to the primitive direct summands of $\mathfrak{D}$ as an $\mathfrak{R}$-order. We denote by $\mathrm{Blk}(\mathfrak{D})$ the set of all blocks of $\mathfrak{D}$. If $B\in\mathrm{Blk}(\mathfrak{D})$, then 1_B will be the corresponding primitive central idempotent of $\mathfrak{D}$, and $1_B\mathfrak{D}$ the corresponding primitive direct summand of $\mathfrak{D}$. Our hypothesis (4.2) implies that $\mathfrak{F}\otimes_{\mathfrak{R}}Z(\mathfrak{D})\simeq Z(\mathfrak{A})$ is isomorphic as an $\mathfrak{F}$-algebra to a direct sum

(4.4) $$\mathfrak{F}\otimes_{\mathfrak{R}}Z(\mathfrak{D})\simeq\mathfrak{F}\oplus\ldots\oplus\mathfrak{F}$$

of copies of $\mathfrak{F}$. In particular, $Z(\mathfrak{D})$ also satisfies (4.2). Because $Z(\mathfrak{D})$ is commutative, Heller's Theorem (4.3) implies that the natural map is a bijection of the primitive idempotents of $Z(\mathfrak{D})$ onto those of $Z(\mathfrak{D})/JZ(\mathfrak{D})$ (where, of course, $JZ(\mathfrak{D})$ is $J(Z(\mathfrak{D}))$). It follows easily from (4.4) and (4.1) that the $\bar{\mathfrak{F}}$-algebra $Z(\mathfrak{D})/JZ(\mathfrak{D})$ is isomorphic to a direct sum

$$Z(\mathfrak{D})/JZ(\mathfrak{D})\simeq\bar{\mathfrak{F}}\oplus\ldots\oplus\bar{\mathfrak{F}}$$

of copies of $\bar{\mathfrak{F}}$. So its primitive idempotents correspond one-to-one to its algebra epimorphisms onto $\bar{\mathfrak{F}}$, which, in turn, correspond to the $\mathfrak{R}$-algebra epimorphisms of $Z(\mathfrak{D})$ onto $\bar{\mathfrak{F}}$. Thus any block $B \in \mathrm{Blk}(\mathfrak{D})$ determines a unique epimorphism

(4.5a) $$\omega_B\colon Z(\mathfrak{D}) \twoheadrightarrow \bar{\mathfrak{F}}$$

of $\mathfrak{R}$-algebras such that

(4.5b) $$\begin{aligned} \omega_B(1_{B'}) &= 1_{\bar{\mathfrak{F}}} \quad \text{if } B' = B, \\ &= 0 \quad \text{if } B' \neq B, \end{aligned}$$

for any $B' \in \mathrm{Blk}(\mathfrak{D})$. Furthermore, the map $B \mapsto \omega_B$ is a bijection of $\mathrm{Blk}(\mathfrak{D})$ onto the set of all epimorphisms of the $\mathfrak{R}$-algebra $Z(\mathfrak{D})$ onto $\bar{\mathfrak{F}}$. As usual, ω_B is called the *central character* for B.

In the above paragraph we have been careful not to say just what a block B of $\mathfrak{D}$ is. Authors differ on this point. In [4] Feit defines B to be the category of all $\mathfrak{D}$-modules on which 1_B acts as the identity. A more customary definition is that used in [9], where B is the direct summand $1_B\mathfrak{D}$ of $\mathfrak{D}$. Still others identify B with the idempotent 1_B. For our purposes it really doesn't matter which definition is used. All we need to know is that two blocks are equal if they are defined for the same $\mathfrak{R}$-order $\mathfrak{D}$ and correspond to the same primitive central idempotent of $\mathfrak{D}$.

The other tool necessary for representation theory, namely the Krull-Schmidt Theorem, also holds for lattices $\mathfrak{L}$ over orders $\mathfrak{D}$ satisfying (4.2). Evidently the endomorphism algebra $\mathrm{End}_{\mathfrak{A}}(\mathfrak{M})$ of the finitely-generated $\mathfrak{A}$-module $\mathfrak{M} = \mathfrak{F} \otimes_{\mathfrak{R}} \mathfrak{L}$ is also a finite-dimensional, split, semi-simple $\mathfrak{F}$-algebra. So the $\mathfrak{R}$-order $\mathrm{End}_{\mathfrak{D}}(\mathfrak{L})$ satisfies (4.2). Hence Heller's Theorem (4.3) tells us that any idempotent of $\mathrm{End}_{\mathfrak{D}}(\mathfrak{L})/J(\mathrm{End}_{\mathfrak{D}}(\mathfrak{L}))$ is the image of one of $\mathrm{End}_{\mathfrak{D}}(\mathfrak{L})$. Since $\mathfrak{L}$ is indecomposable if and only if the identity element is the unique non-zero idempotent of $\mathrm{End}_{\mathfrak{D}}(\mathfrak{L})$, this implies Fitting's Lemma that

(4.6) *An $\mathfrak{D}$-lattice $\mathfrak{L}$ is indecomposable if and only if $\mathrm{End}_{\mathfrak{D}}(\mathfrak{L})$ is a local order.*

As a consequence (see [4, I.11.1]) we have the Krull-Schmidt Theorem that

(4.7) *If a $\mathfrak{D}$-lattice $\mathfrak{L}$ has two decompositions*

$$\mathfrak{L} = \mathfrak{L}_1 \dotplus \mathfrak{L}_2 \dotplus \dots \dotplus \mathfrak{L}_n = \mathfrak{K}_1 \dotplus \mathfrak{K}_2 \dotplus \dots \dotplus \mathfrak{K}_m$$

as direct sums of $\mathfrak{D}$-sublattices $\mathfrak{L}_i$ and $\mathfrak{K}_j$, then $n = m$ and the $\mathfrak{K}_j$ can be renumbered so that $\mathfrak{L}_i \simeq \mathfrak{K}_i$ (as $\mathfrak{D}$-lattices) for each $i = 1, 2, \dots, n$.

5. Blocks of characters

We write $\mathfrak{S}G$ for the group algebra of our finite group G over any commutative ring $\mathfrak{S}$. Then $\mathfrak{R}G$ is an order whose associated $\mathfrak{F}$-algebra $\mathfrak{F} \otimes_{\mathfrak{R}} \mathfrak{R}G$ is the group algebra $\mathfrak{F}G$. Of course $\mathfrak{F}G$ is semi-simple since the field $\mathfrak{F}$ has characteristic 0 by (4.1). In order to obtain all the benefits of Heller's Theorem, we assume that

(5.1) *$\mathfrak{F}$ is a splitting field for any subgroup H of G.*

By one of Brauer's theorems [6, V.19.11] this just says that $\mathfrak{F}$ contains a primitive exp(G)th root of unity, where exp(G) is the exponent of G. Since the orders $\mathfrak{R}H$ now satisfy (4.2) for every $H \leqq G$, the arguments of the preceding paragraphs give us all the tools needed for block theory as developed in [4]. So we shall use the results of that theory as required, without worrying about the fact that the ground rings in [4] are different from our present $\mathfrak{R}$.

We denote by $\mathrm{Irr}(\mathfrak{F}G)$ the set of all irreducible $\mathfrak{F}$-characters of the group G. If $\chi \in \mathrm{Irr}(\mathfrak{F}G)$, then 1_χ will be the corresponding primitive central idempotent

(5.2) $$1_\chi = \frac{\chi(1)}{|G|} \sum_{\sigma \in G} \chi(\sigma^{-1})\,\sigma$$

of $\mathfrak{F}G$.

We often call the members of $\mathrm{Blk}(\mathfrak{R}G)$ the *p-blocks* of G. If B is a p-block of G, then $\mathrm{Irr}(B)$ denotes the family of all $\chi \in \mathrm{Irr}(\mathfrak{F}G)$ which *belong* to B in the sense that 1_B acts as the identity on any simple $\mathfrak{F}G$-module affording χ. The set $\mathrm{Irr}(B)$ determines the block B, since

(5.3) $$1_B = \sum_{\chi \in \mathrm{Irr}(B)} 1_\chi .$$

Of course, any $\chi \in \mathrm{Irr}(\mathfrak{F}G)$ belongs to a unique block of $\mathfrak{R}G$, a block which we denote by $B(\chi)$.

If n is any positive integer, then $a(n)$ will denote the unique non-negative integer such that

(5.4) $$n = p^{a(n)} m,$$

where m is an integer not divisible by p. Since the degree $\chi(1)$ of any $\chi \in \mathrm{Irr}(\mathfrak{F}G)$ divides $|G|$ by [6, V.12.6], there is a unique integer $d(\chi) \geqq 0$ such that

(5.5) $$a(\chi(1)) = a(|G|) - d(\chi).$$

We call $d(\chi)$ the *defect* of χ. By [4, IV.4.5] the defect $d(B)$ of a block $B \in \mathrm{Blk}(\mathfrak{R}G)$ is the maximum

(5.6) $$d(B) = \max\{d(\chi) \mid \chi \in \mathrm{Irr}(B)\}$$

of the defects of its irreducible $\mathfrak{F}$-characters. The defect of any $\chi \in \mathrm{Irr}(B)$ is related to the height $h(\chi)$ of χ (as defined in [4, § IV.4]) by

(5.7) $$d(\chi) + h(\chi) = d(B).$$

In particular, χ has height zero if and only if $d(\chi) = d(B)$.

Let $\mathfrak{S}$ be any commutative ring and H be any subgroup of G. We denote by pr_H^G the unique $\mathfrak{S}$-linear map from $\mathfrak{S}G$ to $\mathfrak{S}H$ such that

(5.8) $$\begin{aligned} pr_H^G(\sigma) &= \sigma \quad \text{if } \sigma \in H, \\ &= 0 \quad \text{if } \sigma \notin H, \end{aligned}$$

for any $\sigma \in G$. Then pr_H^G sends $Z(\mathfrak{S}G)$ into $Z(\mathfrak{S}H)$ whenever $\mathfrak{S}$ is an integral domain. If B is a p-block of H, then the *induced block* $B^G \in \mathrm{Blk}(\mathfrak{R}G)$ is defined if and only if the composite map $\omega_B \circ pr_H^G: Z(\Re G) \to \bar{\mathfrak{F}}$ is an epimorphism of $\Re$-algebras. In that case B^G is the unique p-block of G satisfying

(5.9) $$\omega_{B^G} = \omega_B \circ pr_H^G: Z(\Re G) \twoheadrightarrow \bar{\mathfrak{F}}.$$

One case in which B^G is known to be defined is that in which

$$PC_G(P) \leqq H \leqq N_G(P),$$

for some p-subgroup P of G (see [4, III.9.4]). In [9, 3.2] Knörr and Robinson used this to show that

(5.10) *The induced block B^G is defined whenever $B \in Blk(\Re N_G(C))$ for some p-chain C of G.*

6. The ordinary conjecture

We fix a block B of $\Re G$ and an integer $d \geqq 0$. If C is any p-chain of G, then $\mathrm{Irr}(\mathfrak{F} N_G(C), B, d)$ will denote the set of all characters $\psi \in \mathrm{Irr}(\mathfrak{F} N_G(C))$ such that

(6.1 a) $$B(\psi)^G = B \quad \text{and} \quad d(\psi) = d.$$

(Notice that $B(\psi)^G$ is defined by (5.10).) We then set

(6.1 b) $$k(\mathfrak{F} N_G(C), B, d) = |\mathrm{Irr}(\mathfrak{F} N_G(C), B, d)|.$$

It is evident from (2.3) and (2.4) that conjugation by any $\tau \in G$ sends $N_G(C)$ to $N_G(C^\tau) = N_G(C)^\tau$. Hence it sends $\mathrm{Irr}(\mathfrak{F} N_G(C))$ one-to-one onto $\mathrm{Irr}(\mathfrak{F} N_G(C^\tau))$. Fix a character $\psi \in \mathrm{Irr}(\mathfrak{F} N_G(C))$. Then $B(\psi^\tau) = B(\psi)^\tau$ induces B if and only if $B(\psi)$ does (see (5.9) and (5.8)). Furthermore, $\psi^\tau(1) = \psi(1)$ and $d(\psi^\tau) = d(\psi)$ by (5.5). We conclude that conjugation by τ is a bijection of $\mathrm{Irr}(\mathfrak{F} N_G(C), B, d)$ onto $\mathrm{Irr}(\mathfrak{F} N_G(C^\tau), B, d)$, and hence that

(6.2) $$k(\mathfrak{F} N_G(C^\tau), B, d) = k(\mathfrak{F} N_G(C), B, d)$$

for any $C \in \mathscr{C}$ and $\tau \in G$.

The ordinary form of our conjecture is

Conjecture 6.3 *If G is any finite group with $O_p(G) = 1$, if B is any p-block of G with defect $d(B) > 0$, and if d is any non-negative integer, then*

(6.4) $$\sum_{C \in \mathscr{R}/G} (-1)^{|C|} k(\mathfrak{F} N_G(C), B, d) = 0.$$

Of course (6.2) implies that the alternating sum in (6.4) is well-defined.

We have stated the conclusion (6.4) of our conjecture using an alternating sum over the family $\mathscr{R}$ of all radical p-chains of G. We could just as easily have used any of the families of p-chains in [9].

Proposition 6.5 *Under the hypotheses of Conjecture 6.3 the equation (6.4) is equivalent to*

$$(6.6)\qquad \sum_{C\in\mathscr{X}/G}(-1)^{|C|}k(\mathfrak{F}N_G(C),B,d)=0,$$

where $\mathscr{X}$ is any of the families $\mathscr{P}$, $\mathscr{N}$, $\mathscr{E}$ or $\mathscr{U}$ of p-chains of G.

Proof. We shall apply the results of § 3 with

$$E=H=G \quad\text{and}\quad A=\mathbb{Z}.$$

For any p-chain C of G, let $f(C)$ be the element $k(\mathfrak{F}N_G(C), B, d)$ of $\mathbb{Z}$. Clearly f satisfies (3.2a), while (6.2) implies (3.2b). The left side of (6.6) is the alternating sum $S(f, \mathscr{X}/G)$ of (3.3), and the left side of (6.4) is $S(f, \mathscr{R}/G)$. Since $O_p(G)=1$, Proposition 3.7 and the equations (3.6) tell us that the left sides of (6.4) and (6.6) are equal to each other for $\mathscr{X}=\mathscr{P}, \mathscr{N}, \mathscr{E}$ or $\mathscr{U}$. The proposition follows immediately from this.

By (2.6a) there is only one radical p-chain C of G with length $|C|=0$. This C consists only of $O_p(G)$, and has G as its normalizer $N_G(C)$. By (3.5a) there is only one p-chain C' of length $|C'|=0$ in each of the families $\mathscr{P}$, $\mathscr{N}$, $\mathscr{E}$ or $\mathscr{U}$. This C' consists only of 1, and has G as its normalizer. It follows that

(6.7) *The conclusions (6.4) and (6.6) of Conjecture 6.3 are equivalent to*

$$(6.8)\qquad k(\mathfrak{F}G,B,d)=\sum_{\substack{C\in\mathscr{X}/G\\ |C|>0}}(-1)^{|C|+1}k(\mathfrak{F}N_G(C),B,d),$$

where $\mathscr{X}$ is any of the families $\mathscr{R}$, $\mathscr{P}$, $\mathscr{N}$, $\mathscr{E}$ or $\mathscr{U}$.

Since the hypothesis $O_p(G)=1$ of Conjecture 6.3 implies that $N_G(C)<G$ for any p-chain C of G with $|C|>0$, the formula (6.8) expresses the number $k(\mathfrak{F}G, B, d)$ of characters $\chi\in\mathrm{Irr}(B)$ with a given defect $d(\chi)=d$ in terms of similar numbers for blocks of *proper* subgroups $N_G(C)$ of G.

The following observation can often be used to eliminate terms from the sums in (6.4) or (6.6).

Lemma 6.9 *Let G be any finite group, B be a p-block of G and d be a non-negative integer. If $k(\mathfrak{F}N_G(C), B, d)>0$ for some p-chain C in $\mathscr{R}$, $\mathscr{N}$ or $\mathscr{E}$, then the final subgroup P_n of C is contained in some defect group D of B.*

Proof. Our hypotheses imply that P_n is a normal p-subgroup of $N_G(C)$, and hence that $P_n\leqq O_pN_G(C)$. (If $C\in\mathscr{R}$ this comes from Proposition 2.7(b). If $C\in\mathscr{N}$ or $C\in\mathscr{E}$ this follows from (3.5b).) Since $k(\mathfrak{F}N_G(C), B, d)>0$, there is some character $\psi\in\mathrm{Irr}(\mathfrak{F}N_G(C), B, d)$. Then the p-block $B(\psi)$ of $N_G(C)$ induces the p-block B of G. Hence any defect group D' of $B(\psi)$ must be contained in some defect group D of B (see [4, III.9.6]). But D' must also contain $O_pN_G(C)$ by [4, III.6.9]. Therefore

$$P_n\leqq O_pN_G(C)\leqq D'\leqq D,$$

and the lemma is proved.

As an example of the simplification afforded by the above lemma, consider the case where a defect group D of B is a *trivial intersection* subgroup of G, i..e. where

$$D^{\sigma} \cap D = 1$$

for any $\sigma \in G - N_G(D)$.

Proposition 6.10 *Suppose that the hypotheses of Conjecture* 6.3 *hold for some block B with a trivial intersection defect group D. Let B' be the unique p-block of $G' = N_G(D)$ inducing B in Brauer's first Main Theorem* [4, III.9.7]. *Then the conclusion* (6.4) *of Conjecture* 6.3 *is equivalent to the statement that*

(6.11) *B and B' have the same number of irreducible $\mathfrak{F}$-characters of defect d.*

Proof. In view of Lemma 6.9 we may restrict the sum in (6.4) to those radical p-chains C: $1 = P_0 < P_1 < \ldots < P_n$ which also satisfy

$$P_n \leqq D.$$

Suppose that $n > 0$. Then P_1 is a non-trivial radical p-subgroup of G contained in D (see (2.6 b)). Because D is a trivial intersection subgroup of G, this implies that

$$N_G(P_1) \leqq N_G(D).$$

Hence $N_D(P_1) = D \cap N_G(P_1)$ is a normal p-subgroup of $N_G(P_1)$. So

$$P_1 \leqq N_D(P_1) \leqq O_p N_G(P_1) = P_1 .$$

Since the p-group D is nilpotent, this is only possible when $P_1 = D$. In that case $n = 1$ and C is $1 < D$.

The above discussion tells us that there are only two possible non-zero terms in the sum (6.4), those corresponding to the trivial chain 1 and to the chain $1 < D$. The normalizers of these two chains are G and G', respectively. Since B' is the only p-block of G' inducing B, it is now obvious that (6.4) is equivalent to (6.11). So the proposition holds.

7. Limits of validity

The conclusion (6.4) of Conjecture 6.3 can be false when B has defect zero. What happens in this case is explained in

Proposition 7.1 *Let G be any finite group and B be any p-block of G with defect $d(B) = 0$. Then $O_p(G) = 1$ and*

(7.2)
$$\sum_{C \in \mathscr{X}/G} (-1)^{|C|} k(\mathfrak{F} N_G(C), B, d) = 1 \quad \text{if } d = 0,$$
$$= 0 \quad \text{if } d > 0,$$

whenever $\mathscr{X}$ is one of the families $\mathscr{R}$, $\mathscr{P}$, $\mathscr{N}$, $\mathscr{E}$ or $\mathscr{U}$.

Proof. The defect group 1 of B must contain $O_p(G)$ by [4, III.6.9]. Hence $O_p(G) = 1$. So (3.6) and Proposition 3.7 tell us that the value of the alternating sum on the left side of (7.2) is independent of the choice of $\mathscr{X}$ among $\mathscr{R}$, $\mathscr{P}$, $\mathscr{N}$, $\mathscr{E}$ and $\mathscr{U}$. Thus we may assume that

$$\mathscr{X} = \mathscr{R}.$$

Suppose that $C \in \mathscr{R}$ satisfies $k(\mathfrak{F}N_G(C), B, d) > 0$. Then Lemma 6.9 tells us that the final subgroup P_n of C is contained in the trivial defect group 1 of B. So C must be the trivial p-chain consisting only of $P_0 = 1$. We conclude that the left side of (7.2) is just the number $k(\mathfrak{F}G, B, d)$ of characters of defect d in $\mathrm{Irr}(B)$. But the block B of defect zero contains exactly one ordinary irreducible character χ, and the defect $d(\chi)$ of this character is zero (see [4, IV.4.19] and (5.6)). This implies the proposition.

The following example shows that the conclusion (6.4) of Conjecture 6.3 can also be false when $O_p(G) > 1$.

Example 7.3 Multiplication in the field $GF(p^p)$ of p^p elements gives an action of the multiplicative group M of $GF(p^p)$ as automorphisms of the additive group A of $GF(p^p)$. So we may form the semidirect product $MA = M \rtimes A$ of M with A. The (absolute) Galois group Γ of $GF(p^p)$ acts as automorphisms of both M and A, while preserving the action of M on A. So it acts as automorphisms of MA, and we may form the semidirect product

$$G = \Gamma MA = \Gamma \rtimes (MA).$$

The elementary abelian group A of order p^p is clearly $O_p(G)$. The groups M and Γ are both cyclic, with orders $p^p - 1$ and p, respectively. Hence ΓA is a p-Sylow subgroup of G. It follows that there are exactly two G-conjugacy classes of radical p-chains in G, represented by the chains

$$C_0 \colon A \quad \text{and} \quad C_1 \colon A < \Gamma A$$

of lengths 0 and 1, respectively. The normalizers of these chains are

$$N_G(C_0) = G \quad \text{and} \quad N_G(C_1) = N_G(\Gamma A) = \Gamma M_1 A = (\Gamma \times M_1) A,$$

where M_1 is the multiplicative group of the fixed subfield $GF(p)$ of Γ.

The normal p-subgroup A is its own centralizer $C_G(A)$ in G. Therefore the only p-block of G is the principal block $B = B_0(G)$ (see [4, V.3.11]). Using Clifford theory for the normal subgroups A and MA of G, it is straightforward to compute that $\mathrm{Irr}(B) = \mathrm{Irr}(\mathfrak{F}G)$ has

$$\begin{aligned} p(p-1) &\quad \text{characters of degree } 1, \\ \frac{(p^p-1)-(p-1)}{p} = p^{p-1} - 1 &\quad \text{characters of degree } p, \text{ and} \\ p &\quad \text{characters of degree } p^p - 1. \end{aligned}$$

Since $a(|G|) = p + 1$ (see (5.4)), this and (5.5) imply that

$$\begin{aligned} k(\mathfrak{F}G, B, d) &= p(p-1) + p = p^2 && \text{if } d = p+1, \\ &= p^{p-1} - 1 && \text{if } d = p, \\ &= 0 && \text{otherwise.} \end{aligned}$$

A similar computation shows that the only p-block of $\Gamma M_1 A$ is the principal block $B' = B_0(\Gamma M_1 A)$, which has

$$\begin{array}{rl} p(p-1) & \text{characters of degree } 1, \\ p & \text{characters of degree } p-1, \text{ and} \\ \dfrac{p^p - p}{p(p-1)} = \dfrac{p^{p-1}-1}{p-1} & \text{characters of degree } p(p-1). \end{array}$$

Since $a(|\Gamma M_1 A|)$ is also $p+1$, this and (5.5) imply that

$$\begin{aligned} k(\mathfrak{F}\Gamma M_1 A, B, d) &= p(p-1)+p = p^2 && \text{if } d=p+1, \\ &= (p^{p-1}-1)/(p-1) && \text{if } d=p, \\ &= 0 && \text{otherwise.} \end{aligned}$$

The left side of (6.4) for $d=p$ is now

$$k(\mathfrak{F}G, B, p) - k(\mathfrak{F}\Gamma M_1 A, B, p) = (p^{p-1}-1)\left(1-\frac{1}{p-1}\right),$$

which is non-zero if $p>2$. So (6.4) fails in this case, even though $d(B) = p+1 > 0$.

8. Alperin's weight conjecture

In its original form [1] the Alperin Weight Conjecture for a block B of a finite group G said that the number of modular irreducible characters in B should equal the number of G-conjugacy classes of weights in B. Here a *weight* of B is any modular irreducible character ϕ of the normalizer $N_G(P)$ of some p-subgroup $P \leqq G$ such that P is a vertex of any simple $N_G(P)$-module affording ϕ, and ϕ belongs to some block $B(\phi)$ of $N_G(P)$ inducing B. So Alperin's conjecture only dealt with modular characters of subgroups of G.

In [9] Knörr and Robinson translated that conjecture into one involving only ordinary irreducible characters. For any $H \leqq G$ let $\operatorname{Irr}(\mathfrak{F}H, B)$ be the set of all characters $\psi \in \operatorname{Irr}(\mathfrak{F}H)$ belonging to blocks $B(\psi)$ inducing B. We denote by $k(\mathfrak{F}H, B)$ the order $|\operatorname{Irr}(\mathfrak{F}H, B)|$ of this set. Then [9, 4.6] tells us that Alperin's Weight Conjecture is equivalent to

Conjecture 8.1 *If G is any finite group and B is any p-block of G such that $d(B)>0$, then*

$$\sum_{C \in \mathcal{N}/G} (-1)^{|C|} k(N_G(C), B) = 0. \tag{8.2}$$

Alperin's conjecture in the Knörr-Robinson form is an easy consequence of ours.

Theorem 8.3 *If Conjecture* 6.3 *holds, then Alperin's Weight Conjecture holds.*

Proof. We only need derive Conjecture 8.1 from Conjecture 6.3. So we assume that B is a block of a finite group G such that $d(B)>0$, and must prove that (8.2) holds.

We apply the results of § 3 with $E=H=G$ and $A=\mathbb{Z}$. For f we take the function sending any p-chain C of G to $k(N_G(C), B)$. Evidently f satisfies (3.2a, b). Furthermore, the left side of (8.2) is the alternating sum $S(f, \mathcal{N}/G)$ of (3.3). So Proposition 3.7 tells us that (8.2) holds if $O_p(G)>1$.

Now assume that $O_p(G)=1$. From the definition of $\mathrm{Irr}(\mathfrak{F}N_G(C), B, d)$ in § 6 it is clear that $\mathrm{Irr}(\mathfrak{F}N_G(C), B)$ is the disjoint union of its subsets $\mathrm{Irr}(\mathfrak{F}N_G(C), B, d)$ for $d \geqq 0$. Hence

$$(8.4) \qquad k(\mathfrak{F}N_G(C), B)=\sum_{d \geqq 0} k(\mathfrak{F}N_G(C), B, d)$$

for any $C \in \mathscr{C}$, where all but a finite number of terms in this infinite sum are zero. Because $O_p(G)=1$, Conjecture 6.3 and Proposition 6.5 tell us that

$$\sum_{C \in \mathcal{N}/G} (-1)^{|C|} k(\mathfrak{F}N_G(C), B, d)=0$$

for all $d \geqq 0$. Summing these equations over d and using (8.4), we obtain (8.2). So the theorem is proved.

9. Cyclic defect groups

The only blocks whose structure in known in detail are those with cyclic defect groups. For them our conjecture is a routine calculation.

Theorem 9.1 *Conjecture* 6.3 *holds for blocks with cyclic defect groups.*

Proof. Assume that G, B and d satisfy the hypotheses of Conjecture 6.3, and that B has a cyclic defect group D. In view of Proposition 6.5 it will suffice to prove that

$$(9.2) \qquad \sum_{C \in \mathscr{E}/G} (-1)^{|C|} k(\mathfrak{F}N_G(C), B, d)=0.$$

Let $C: P_0=1<P_1<\ldots<P_n$ be an elementary p-chain of G. Then each P_i is an elementary abelian p-subgroup of G. If P_n is not contained in a defect group of B, i.e. in a G-conjugate D^σ of D, then $k(\mathfrak{F}N_G(C), B, d)=0$ by Lemma 6.9. If $P_n \leqq D^\sigma$ and $n>0$, then the elementary group P_n must be the unique cyclic subgroup $\Omega(D)^\sigma$ of order p in D^σ. Since $d(B)>0$, the subgroup D has order $p^{d(B)}>1$. We conclude that the alternating sum in (9.2) has at most two non-zero terms, corresponding to the G-orbits of the trivial chain $C_0: 1$ and the chain $C_1: 1<\Omega(D)$. So (9.2) reduces to

$$(9.3) \qquad k(\mathfrak{F}G, B, d)-k(\mathfrak{F}N_G\,\Omega(D), B, d)=0.$$

We're going to use the results in Chapter VII of Feit's book [4]. Feit's field K is our $\mathfrak{F}$. Our hypothesis (5.1) that $\mathfrak{F}$ splits every subgroup of G implies that Feit's field $\hat{K}$ is also $\mathfrak{F}=K$. Hence Feit's inertial indices e and $\hat{e}$ are equal to each other. Our $\Omega(D)$ and $N_G\,\Omega(D)$ are Feit's D_{a-1} and N_{a-1}, respectively. We know from page 270 of [4] that there is a unique p-block B' (which Feit calls B_{a-1}) of $N_G\,\Omega(D)$ inducing B. Furthermore, B' has the same defect group D and the same index of inertia e as B. From [4, VII.2.12] we know that $\mathrm{Irr}(B)$

and $\mathrm{Irr}(B')$ have the same number $e+(|D|-1)/e$ of characters, all of which have height zero by [4, VII.2.16]. Since $d(B)=d(B')$, we conclude from this and (5.7) that all these characters have the same defect $d(B)$. Thus

$$\begin{aligned} k(\mathfrak{F}G, B, d) &= e+\frac{|D|-1}{e} && \text{if } d=d(B), \\ &= 0 && \text{if } d\neq d(B), \end{aligned}$$

and

$$\begin{aligned} k(\mathfrak{F}N_G\,\Omega(D), B, d) = k(\mathfrak{F}N_G\,\Omega(D), B', d) &= e+\frac{|D|-1}{e} && \text{if } d=d(B), \\ &= 0 && \text{if } d\neq d(B). \end{aligned}$$

Therefore (9.3) holds and the theorem is proved.

10. The first Janko group

Following the conventions of [3] we denote by J_1 the simple group described by Janko in [8].

Theorem 10.1 *Conjecture* 6.3 *holds if* G *is* J_1.

Proof. Let B be any p-block of $G=J_1$ with $d(B)>0$, and d be any non-negative integer. By [8, § I] all odd order Sylow subgroups of G are cyclic of prime order. So Theorem 9.1 implies the present theorem if $p>2$. Thus we may assume that $p=2$. In this case we shall prove the theorem by showing directly that (6.4) holds.

A Sylow 2-subgroup S of G is elementary abelian of order 8 by [8, § VI]. Hence we have

$$a(|G|)=a(|S|)=3.$$

We follow the notation of the table in [8, § I] for the irreducible $\mathfrak{F}$-characters of G. There are fifteen such characters, denoted by ψ_i for $i=1, 2, \ldots, 15$. By [8, 5.1] the first eight characters $\psi_1, \ldots, \psi_8$ are those in the principal 2-block $B_0(G)$ of $\mathfrak{R}G$. The next two, ψ_9 and ψ_{10}, both have degree $76=2^2\cdot 19$, and thus have defect 1 by (5.5). The remaining characters $\psi_{11}, \ldots, \psi_{15}$ all have degrees divisible by 8, and hence have defect 0. We conclude that G has seven 2-blocks, the principal block $B_0(G)$ of defect 3, a block $B_1(G)$ of defect 1 with $\mathrm{Irr}(B_1(G))=\{\psi_9, \psi_{10}\}$, and five blocks of defect 0, one for each of the characters $\psi_{11}, \ldots, \psi_{15}$. Since B has defect $d(B)>0$, it must be either $B_0(G)$ or $B_1(G)$. In the latter case a defect group of B is cyclic of order 2, and the present theorem holds by Theorem 9.1. So we may assume from now on that

$$B=B_0(G).$$

The normalizer $N_G(S)$ is described in [8, § VI]. It is a double semi-direct product

$$N_G(S)=\Gamma MS=\Gamma\ltimes M\ltimes S. \tag{10.2}$$

If we identify S with the additive group of the field $GF(8)$ of eight elements, then M can be identified with the multiplicative group of $GF(8)$ acting on S via multiplication in $GF(8)$. In particular, M is cyclic of order 7. The group Γ can be identified with the absolute Galois group of $GF(8)$ acting naturally on both the additive group S and the multiplicative group M. So Γ is cyclic of order 3.

The above description of $N_G(S)$ implies that any involution in G is conjugate to the unique involution $\tau \in S$ fixed by Γ. One of the defining properties of J_1 (see the theorem on the first page of [8]) is that

$$(10.3) \qquad N_G(\langle\tau\rangle) = C_G(\tau) = \langle\tau\rangle \times F,$$

where F is isomorphic to the alternating group A_5 on five letters.

As Janko remarks in [8, §VI], it follows from (10.2) and (10.3) that any four-subgroup of G is conjugate to the unique Γ-invariant complement $V = [S, \Gamma]$ to $\langle\tau\rangle$ in S. Furthermore, we have

$$(10.4) \qquad N_G(V) = \Gamma \ltimes S = \langle\tau\rangle \times (\Gamma V),$$

where ΓV is isomorphic to the alternating group A_4 of degree 4.

The above arguments tell us that any 2-subgroup P of G is conjugate to exactly one of 1, $\langle\tau\rangle$, V or S. From the description of the normalizers in (10.2)–(10.4), and the definition (2.1) of radical p-subgroups, we conclude that

(10.5) *The radical 2-subgroups of G are the conjugates of 1, $\langle\tau\rangle$ and S.*

In view of (2.6) any radical 2-chain of G with length at least one must begin with either $1 < \langle\tau\rangle$ or $1 < S$. The latter chain cannot be extended any farther, since S is a Sylow 2-subgroup of G. The former can be extended by adjoining a radical 2-subgroup of its normalizer $\langle\tau\rangle \times F$ (see (10.3)). Since $F \simeq A_5$ has Sylow 2-subgroups with trivial intersections, the only possible such extension is $1 < \langle\tau\rangle < S$, which cannot be extended any farther. Thus

(10.6) *The radical 2-chains of G are the conjugates of the four chains*

$$1, \quad 1 < \langle\tau\rangle, \quad 1 < S, \quad \text{and} \quad 1 < \langle\tau\rangle < S.$$

Let $C\colon 1$ be the trivial radical 2-chain of G. Then $N_G(C) = G$. So $\operatorname{Irr}(\mathfrak{F}N_G(C), B, d)$ consists of those characters in $\operatorname{Irr}(B)$ having defect d. Since B is the principal block $B_0(G)$, the set $\operatorname{Irr}(B)$ consists of $\psi_1, \ldots, \psi_8$. By the character table in [8, §I] each of these characters has odd degree, and hence has defect 3. Thus

$$(10.7) \qquad \begin{aligned} k(\mathfrak{F}N_G(1), B, d) &= 8 \quad \text{if } d = 3, \\ &= 0 \quad \text{if } d \neq 3. \end{aligned}$$

Now let C be the 2-chain $1 < \langle\tau\rangle$ of G. From (10.3) it follows that $N_G(C) = \langle\tau\rangle \times F$. The principal 2-block of $F \simeq A_5$ has four irreducible $\mathfrak{F}$-characters ϕ_1, ϕ_2, ϕ_3 and ϕ_4 with degrees 1, 3, 3 and 5, respectively (see the character table in [8, §IV]). It follows that the principal 2-block $B_0(\langle\tau\rangle \times F)$ of $\langle\tau\rangle \times F$ has eight irreducible $\mathfrak{F}$-characters $\lambda^i \times \phi_j$, for $i = 0, 1$ and $j = 1, 2, 3, 4$, where λ is the faithful linear $\mathfrak{F}$-character of $\langle\tau\rangle$. Each of these characters has odd degree, and hence defect 3. By a theorem of Brauer [4, V.6.2] no non-principal 2-block of $\langle\tau\rangle \times F$ can induce the principal block B of G. Therefore

(10.8) $$k(\mathfrak{F}N_G(1<\langle\tau\rangle), B, d)=8 \quad \text{if } d=3,$$
$$=0 \quad \text{if } d\neq 3.$$

Next we let C be the 2-chain $1<S$ with normalizer $N_G(C)=N_G(S)=\Gamma MS$ (see (10.2)). Since ΓMS has a self-centralizing Sylow 2-subgroup S, all its irreducible $\mathfrak{F}$-characters belong to its principal 2-block $B_0(\Gamma MS)$. Using the description of ΓMS following (10.2), and Clifford theory for its normal subgroups MS and S, we easily compute that $\mathrm{Irr}(\mathfrak{F}\Gamma MS)$ has eight members with degrees 1, 1, 1, 3, 3, 7, 7 and 7. Since all these degrees are odd, these characters all have defect 3. Hence

(10.9) $$k(\mathfrak{F}N_G(1<S), B, d)=8 \quad \text{if } d=3,$$
$$=0 \quad \text{if } d\neq 3.$$

Finally we let C be the 1-chain $2<\langle\tau\rangle<S$ of G. Its normalizer is that of $\langle\tau\rangle$ in $N_G(S)$, and hence is

$$N_G(C)=\Gamma S\simeq\langle\tau\rangle\times A_4.$$

All the characters in $\mathrm{Irr}(\mathfrak{F}\Gamma S)$ belong to the principal 2-block $B_0(\Gamma S)$. There are eight such characters, six of degree 1 and two of degree 3. They all have defect 3. Thus

(10.10) $$k(N_G(1<\langle\tau\rangle<S), B, d)=8 \quad \text{if } d=3,$$
$$=0 \quad \text{if } d\neq 3.$$

The equation (6.4) for any value of d follows directly from (10.6)–(10.10). So the theorem is proved.

11. The smallest Mathieu group

We denote by M_{11} the Mathieu group on 11 letters as described in [7, §XII.1].

Theorem 11.1 *Conjecture* 6.3 *is true if* G *is* M_{11}.

Proof. We fix a p-block B of G with $d(B)>0$, and a non-negative integer d. By [7, XII.1.3] the group $G=M_{11}$ is a sharply quadruply transitive permutation group on a set $\Delta=\{1, 2, \ldots, 11\}$ of 11 points. So its order is

(11.2) $$|G|=11\cdot 10\cdot 9\cdot 8=2^4\cdot 3^2\cdot 5\cdot 11.$$

In particular, all Sylow p-subgroups of G are cyclic if $p>3$. In that case our theorem holds by Theorem 9.1. So we may assume that p is either 3 or 2.

We first treat the case where $p=3$. Since G is sharply quadruply transitive on Δ, the stabilizer $G_{11,10}$ in G of two points $11, 10\in\Delta$ is a Frobenius group of order $9\cdot 8$ on the set $\Delta_9=\{1, 2, \ldots, 9\}$ of the remaining nine points. Its Frobenius kernel F is a normal subgroup of order 9 acting regularly on Δ_9. Its stabilizer $Q=G_{11,10,9}$ of the point $9\in\Delta_9$ has order 8 and acts regularly on both $F-\{1\}$

(by conjugation) and $\Delta_8=\{1, 2, \dots, 8\}$. This forces F to be elementary abelian. Of course $F\in \mathrm{Syl}_3(G)$ by (11.2).

Because G is doubly transitive on Δ, its stabilizer $G_{\{11,10\}}$ of the subset $\{11, 10\}\subseteq\Delta$ has $G_{11,10}$ as a normal subgroup of index 2. So the characteristic subgroup F of $G_{11,10}$ is a normal subgroup of index $8\cdot 2=16$ in $G_{\{11,10\}}$. Any $\sigma\in N_G(F)$ must leave invariant the set $\{11,10\}$ of all fixed points of F, and hence lie in $G_{\{11,10\}}$. Therefore $G_{\{11,10\}}$ is precisely the normalizer $N_G(F)$.

Of course $G_{\{11,10\}}$ acts faithfully on Δ_9, and hence is the semi-direct product of its regular normal subgroup F on that set and its stabilizer $S=G_{\{11,10\},9}$ of the point $9\in\Delta_9$. Since S has order 16, it is a Sylow 2-subgroup of G by (11.2). Because S acts faithfully on F by conjugation, it is isomorphic to a 2-subgroup of the automorphism group $\mathrm{Aut}(F)\simeq GL_2(3)$. But a Sylow 2-subgroup of $GL_2(3)$ is semi-dihedral of order $16=|S|$. We conclude that

(11.3) *The Frobenius kernel F of $G_{11,10}$ is an elementary abelian Sylow 3-subgroup of G with order 9, acting regularly on $\Delta_9=\Delta-\{11, 10\}$. Its normalizer $N_G(F)$ is the stabilizer $G_{\{11,10\}}$, and is a semi-direct product $S\rtimes F$, where $S=G_{\{11,10\}}\cap G_9$ is a semi-dihedral Sylow 2-subgroup of G acting faithfully on F (under conjugation) like a Sylow 2-subgroup of $\mathrm{Aut}(F)\simeq GL_2(3)$.*

Any element $\sigma\neq 1$ of F fixes only the points 11 and 10 of Δ. So $N_G(\langle\sigma\rangle)$ is a subgroup of $G_{\{11,10\}}=N_G(F)$. It follows that F is a trivial intersection subgroup of G. This implies that B has F as a defect group, and corresponds in Brauer's First Main Theorem [4, III.9.7] to a unique 3-block B' of $N_G(F)=SF$. Because SF has a self-centralizing normal 3-subgroup F, its only 3-block is the principal one $B_0(SF)$ (see [4, V.3.11]). Therefore $B=B_0(SF)^G$ is the principal 3-block $B_0(G)$ of G, and all other 3-blocks of G must have defect zero.

We use the notation of [3] for the ten characters $\chi_1, \chi_2, \dots, \chi_{10}$ in $\mathrm{Irr}(\mathfrak{F}G)$. By the character table of $G=M_{11}$ in [3], the character χ_9 has degree 45 divisible by 9, and hence lies in a 3-block of defect zero. All the other nine characters have degrees not divisible by 3. So they all have defect 2 (see (5.5)) and lie in $\mathrm{Irr}(B)$. Therefore

(11.4) $\mathrm{Irr}(B)$ *has nine characters, all of defect 2.*

From the description of $N_G(F)=SF$ given in (11.3), it follows that $\mathrm{Irr}(\mathfrak{F}SF)$ consists of nine characters with degrees 1, 1, 1, 1, 2, 2, 2, 8 and 8. These characters all lie in B' and have defect 2. Therefore $\mathrm{Irr}(B')$ also has nine characters, all of defect 2. In view of Proposition 6.10, this and (11.4) imply our theorem when $p=3$.

Finally, we assume that $p=2$. Proposition 6.5 tells us that we can prove the theorem by showing that

(11.5) $$\sum_{C\in\mathscr{E}/G}(-1)^{|C|}k(\mathfrak{F}N_G(C), B, d)=0.$$

We may choose a four-subgroup V in the semi-dihedral Sylow 2-subgroup S of G. Any elementary abelian subgroup of S is S-conjugate to one of V. Hence any elementary abelian 2-subgroup of G is G-conjugate to one of V. It follows from (11.3) that V has exactly one orbit Γ of length 4 on Δ, the remaining orbits being of lengths 2, 2, 2 and 1. Because G is sharply quadruply transitive, the normalizer $N_G(V)$ must act faithfully on Γ. So $N_G(V)$ is isomorphic to a subgroup of the symmetric group S_4 on four letters.

If $N_G(V)$ is not isomorphic to S_4, then it must be the dihedral group $N_S(V)$ of order 8. This would imply that the central involution τ of S (which lies in V) could not be G-conjugate to any other involution $\rho \in V$. But (11.3) implies that τ is the unique involution in $G_{11,10,9}$, and that ρ fixes 3 elements in Δ_9. Because G is triply transitive on Δ, this forces ρ to be G-conjugate to τ. Therefore

(11.6) $$N_G(V) \simeq S_4.$$

Incidently, this says that V is a radical 2-subgroup of G.

We know from [7, XII.5.1] that

(11.7) $$N_G(\langle\tau\rangle) = C_G(\tau) \simeq GL_2(3).$$

So both $N_G(\langle\tau\rangle)$ and $N_G(V)$ have normal 2-subgroups whose centralizers are their centers. It follows that the only 2-blocks of these normalizers are their principal blocks (see [4, V.3.11]). Since any 2-block of G with positive defect must be induced from a 2-block of the normalizer of some non-trivial elementary abelian 2-subgroup of G, we conclude that B is the principal 2-block $B_0(G)$, of G, and is the unique 2-block of G with positive defect.

Because any elementary abelian 2-subgroup of G is conjugate to a subgroup of the four-group V, it follows from (11.6) that

(11.8) *The members of $\mathscr{E}$ are the G-conjugates of the four 2-chains*

$$1, \quad 1 < \langle\tau\rangle, \quad 1 < V \quad \text{and} \quad 1 < \langle\tau\rangle < V.$$

Of the ten characters $\chi_1, \chi_2, \ldots, \chi_{10}$ in $\mathrm{Irr}(\mathfrak{F}G)$, only χ_6 and χ_7 have degrees divisible by 16 (see the character table of M_{11} in [3]). So these two lie in 2-blocks of defect zero, while the remaining eight characters $\chi_1, \ldots, \chi_5$ and $\chi_8, \chi_9, \chi_{10}$ form $\mathrm{Irr}(B)$. The degrees of these eight characters are 1, 10, 10, 10, 11 and 44, 45, 55. Since $a(|G|) = 4$, we conclude that

(11.9) $$\begin{aligned} k(\mathfrak{F}N_G(1), B, d) &= 4 && \text{if } d = 4, \\ &= 3 && \text{if } d = 3, \\ &= 1 && \text{if } d = 2, \\ &= 0 && \text{otherwise}. \end{aligned}$$

In view of (11.7) there are eight characters in $\mathrm{Irr}(\mathfrak{F}C_G(\tau))$, with degrees 1, 1, 2, 3, 3, 2, 2 and 4. They all belong to the principal 2-block $B_0(C_G(\tau))$, which induces $B = B_0(G)$. Since $a(|C_G(\tau)|) = 4$, we conclude that

(11.10) $$\begin{aligned} k(\mathfrak{F}N_G(1 < \langle\tau\rangle), B, d) &= 4 && \text{if } d = 4, \\ &= 3 && \text{if } d = 3, \\ &= 1 && \text{if } d = 2, \\ &= 0 && \text{otherwise}. \end{aligned}$$

It follows from (11.6) that there are five characters in $\mathrm{Irr}(\mathfrak{F}N_G(V))$, with degrees 1, 1, 2, 3 and 3. They all lie in the principal 2-block $B_0(N_G(V))$, which induces $B=B_0(G)$. Since $a(|S_4|)=3$, this implies that

(11.11) $$k(\mathfrak{F}N_G(1<V), B, d)=4 \quad \text{if } d=3, \qquad =1 \quad \text{if } d=2, \qquad =0 \quad \text{otherwise}.$$

The normalizer $N_G(1<\langle\tau\rangle<V)$ is the centralizer of τ in the above group $N_G(V)$. This is the Sylow 2-subgroup $N_S(V)$ of that group, and so is dihedral of order 8. All its irreducible $\mathfrak{F}$-characters belong to its principal 2-block, which induces B. Since these characters have degrees 1, 1, 1, 1 and 2, while $a(|N_S(V)|)=3$, we conclude that

(11.12) $$k(\mathfrak{F}N_G(1<\langle\tau\rangle<V), B, d)=4 \quad \text{if } d=3, \qquad =1 \quad \text{if } d=2, \qquad =0 \quad \text{otherwise}.$$

The equation (11.5) for any value of d follows directly from (11.8)–(11.12). So the theorem is proved.

References

1. Alperin, J.: Weights for finite groups. Proc. Symp. Pure Maths. **47**, 369–379 (1987)
2. Alperin, J., Fong, P.: Weights for symmetric and general linear groups. J. Algebra **131**, 2–22 (1990)
3. Conway, J., Curtis, R., Norton, S., Parker, R., Wilson, R.: Atlas of finite simple groups. Oxford New York: Oxford University Press 1985
4. Feit, W.: The representation theory of finite groups. Amsterdam New York Oxford: North Holland Publishing Co., 1982
5. Heller, A.: On group representations over a valuation ring. Proc. Nat. Acad. Sci. USA **47**, 1194–1197 (1961)
6. Huppert, B.: Endliche Gruppen I. Berlin Heidelberg New York: Springer 1967
7. Huppert, B., Blackburn, N.: Finite groups III. Berlin Heidelberg New York: Springer 1982
8. Janko, Z.: A new finite simple group with abelian Sylow 2-subgroups and its characterization. J. Algebra **3**, 147–186 (1966)
9. Knörr, R., Robinson, G.: Some remarks on a conjecture of Alperin. J. London Math. Soc. (2) **39**, 48–60 (1989)
10. Robinson, G.: A remark on a conjecture of Alperin, preprint (1986)
11. Zariski, O., Samuel, P.: Commutative algebra II. Princeton New York: D. van Nostrand Co. Inc., 1960