ILLINOIS JOURNAL OF MATHEMATICS
Volume 28, Number 2, Summer 1984

ON THE NUMBER OF CHARACTERS IN A p-BLOCK OF A p-SOLVABLE GROUP

BY

REINHARD KNÖRR

In [3], R. Brauer conjectured that the number $k(B)$ of ordinary irreducible characters of a finite group G in a p-block B is bounded by the order $|D|$ of a defect group D of B. It is fairly easy to show that $k(B) \leqslant |D|^2$, even better, Brauer and Feit [4] showed $k(B) \leqslant \frac{1}{4}|D|^2 + 1$.

The conjecture has been proved under some very specific assumptions on D. If D is cyclic, it follows from Brauer-Dade theory [2], [6].

If D is elementary abelian of order 8, it is true as shown by Landrock in [12], which also contains a review of what little is known in general.

In case of p-solvable groups, Nagao [14] used the method of Fong [8] to reduce the problem to the following question:

Let V be an elementary abelian p-group on which a p'-group G acts faithfully and irreducibly. Is it then true that the number of conjugacy classes of the semidirect product GV is bounded by the order of V?

This sounds very innocent; however, an affirmative answer would give information on all faithful (and irreducible) representations of all finite groups over nearly all finite fields—excluding only those with a characteristic dividing the group order.

The aim of this paper is to develop some ideas how to tackle the problem (§§ 1–4). A key role is played by a generalized character δ of G which measures how far an element $g \in G$ is from acting trivially on V. It turns out that we need information on δ only for a—possibly very small—subgroup of G, namely the centraliser of an arbitrary element $v \in V$.

As an application, it is shown that the answer to the above question is yes, if G is a supersolvable group (§§ 6–7). Also, some consequences for more general classes of finite groups (not just semidirect products) are given. More specifically, Brauer's conjecture holds for p-blocks of solvable groups with a supersolvable p'-Hall group (Theorem 7.4).

The result of § 5 gives a fairly general criterion for an irreducible module to stay irreducible when restricted to the centraliser of an abelian normal subgroup.

The main part of this work was done during a stay at the University of Illinois in Urbana and Chicago. I would like to thank the mathematicians

Received June 16, 1981.

there, in particular E. C. Dade and Paul Fong for their hospitality. My thanks go to the Deutsche Forschungsgemeinschaft as well, whose support made this work possible.

1. Two Results on Characters

1.1 Proposition *Let χ be a generalized character of G and let $z = \Sigma_{i=1}^{n} \chi(g_i)$ where the g_i run over a set of representatives of the conjugacy classes of G:*

(i) *z is rational integer.*
(ii) *If $z \neq 0$, then $z\chi^{-1}$ is a generalized character of G.*
(iii) *Assume $0 \neq z$ is relatively prime to $|G|$. If ψ is a generalized character of G such that $\chi(g)^{-1}\psi(g)$ is an algebraic integer for all $g \in G$, then $\chi^{-1}\psi$ is a generalized character.*

Proof. (i) Consider the vector space of class functions on G. Multiplication with χ is an endomorphism χ^* of this space and $z = \det \chi^*$ as is seen by taking the characteristic function of the conjugacy classes as a basis. On the other hand, we may take the irreducible characters of G as a basis. Let M be the matrix of χ^* with respect to this basis, so $M = (m_{\sigma\tau})$ where $m_{\sigma\tau} = (\sigma\chi, \tau) \in \mathbf{Z}$ for all $\sigma, \tau \in \operatorname{Irr} G$. Hence $z = \det \chi^* = \det M \in \mathbf{Z}$.

(ii) Let $\varphi = z\chi^{-1}$; clearly this is a well defined class function. Set $N = (n_{\sigma\tau})$ where $n_{\sigma\tau} = (\sigma\varphi, \tau)$. Clearly $NM = zE$, so $N = zM^{-1} = \operatorname{adj} M$ has entries in $\mathbf{Z}$. Hence $(\varphi, \tau) \in \mathbf{Z}$ for all $\tau \in \operatorname{Irr} G$ and φ is a generalized character.

(iii) Again $\chi^{-1}\psi$ is a well defined class function, so we have to show $(\chi^{-1}\psi, \tau) \in \mathbf{Z}$ for all $\tau \in \operatorname{Irr} G$. Pick $a, b \in \mathbf{Z}$ such that $1 = az + b\,|G|$. Then

$$\begin{aligned}(\chi^{-1}\psi, \tau) &= a(z\chi^{-1}\psi, \tau) + b|G|(\chi^{-1}\psi, \tau)\\ &= a(z\chi^{-1}\psi, \tau) + b\sum_{g} \chi^{-1}(g)\psi(g)\overline{\tau(g)}\end{aligned}$$

is an algebraic integer: $\chi^{-1}(g)\psi(g)$ is integral by assumption, $\tau(g)$ is integral as character value and $(z\chi^{-1}\psi, \tau) \in \mathbf{Z}$ by (ii). At the same time $(\chi^{-1}\psi, \tau) = z^{-1}(z\chi^{-1}\psi, \tau) \in \mathbf{Q}$, hence $(\chi^{-1}\psi, \tau) \in \mathbf{Z}$.

1.2 *Remark.* In (iii), the condition $(z, |G|) = 1$ is essential: Let 1 and λ be the irreducible characters of C_2. Let $\chi = 2 \cdot 1$ and $\psi = 3 \cdot 1 + \lambda$. Then $\chi^{-1}(g)\psi(g) \in \mathbf{Z}$ for $g \in C_2$, but $\chi^{-1}\psi$ is not a generalized character. The condition that $\chi^{-1}(g)\psi(g)$ is an algebraic integer is clearly necessary.

1.3 Definition. Let $H \leq G$ and χ a class function of H. For $g \in G$, let $G = \dot{\bigcup} Hx_i\langle g\rangle$ an H-$\langle g\rangle$ double coset decomposition. For each i, let

$$\begin{aligned} n_i &= |H|^{-1}|Hx_i\langle g\rangle| \\ &= \min\{n \mid x_ig^nx_i^{-1} \in H\} \\ &= |\langle x_igx_i^{-1}\rangle : \langle x_igx_i^{-1}\rangle \cap H| \end{aligned}$$

and define $\chi^{\otimes G}(g) = \Pi_i\, \chi(x_ig^{n_i}x_i^{-1})$.

By the next lemma, $\chi \mapsto \chi^{\otimes G}$ is a map from the class functions of H into the class functions of G. This map is called *tensor induction.*

1.4 LEMMA *$\chi^{\otimes G}$ is a well defined class function of G.*

Proof. Let $\{y_i\}$ be another set of double coset representatives. Then $y_i = h_ix_ia_i$ for $h_i \in H$ and $a_i \in \langle g\rangle$, so

$$y_ig^{n_i}y_i^{-1} = h_ix_ia_ig^{n_i}a_i^{-1}x_i^{-1}h_i^{-1} = Hx_ig^{n_i}x_i^{-1}.$$

Since χ is a class function on H, the value of $\chi^{\otimes G}(g)$ does not depend on the choice of the x_i's.

Now let $g_1 \in G$ be conjugate to g, say $g_1 = g^y$ for $y \in G$. Then

$$G = Gy = \dot{\cup}\, Hx_i\langle g\rangle y = \dot{\cup}\, Hx_iyy^{-1}\langle g\rangle y = \dot{\cup}\, Hx_iy\langle g_1\rangle,$$

so $\{x_iy\rangle$ is a set of H-$\langle g_1\rangle$ double coset representatives. Since

$$|Hx_iy\langle g_1\rangle| = |Hx_i\langle g\rangle|,$$

the n_i's are the same for g_1 and g. Now $x_iyg_1^{n_i}(x_iy)^{-1} = x_ig^{n_i}x_i^{-1}$ for all i, so $\chi^{\otimes G}(g_1) = \chi^{\otimes G}(g)$ and $\chi^{\otimes G}$ is a class function.

The next result shows what one might expect:

1.5 LEMMA. *Let U, $H \leqslant G$ and χ, ψ be class functions on H.*

(i) *(Transitivity) If $H \leqslant U \leqslant G$, then $(\chi^{\otimes U})^{\otimes G} = \chi^{\otimes G}$.*
(ii) *(Mackey Decomposition) Let $G = \dot{\cup}\, Hg_iU$ be a double coset decomposition. Then $(\chi^{\otimes G})_U = \Pi_i\, (\chi^{g_i}_{H^{g_i}\cap U}) \otimes U$.*
(iii) *(Multiplicativity) $(\chi\psi)^{\otimes G} = \chi^{\otimes G}\psi^{\otimes G}$.*

Proof. (i) Let $G = \dot{\cup}_i\, Uy_i\langle g\rangle$ be a U-$\langle g\rangle$ double coset decomposition; let $n_i = |U|^{-1}|Uy_i\langle g\rangle|$ and $u_i = y_ig^{n_i}y_i^{-1}$. Now let $U = \dot{\cup}_j\, Hv_{ij}\langle u_i\rangle$ be an H-$\langle u_i\rangle$ double coset decomposition, and set $m_{ij} = |H|^{-1}|Hv_{ij}\langle u_i\rangle|$. It is straightforward to check that $G = \dot{\cup}_{i,j}\, Hv_{ij}y_i\langle g\rangle$ is an H-$\langle g\rangle$ double coset decomposition. Moreover,

$$|H|^{-1}|Hv_{ij}y_i\langle g\rangle| = n_im_{ij}$$

and

$$v_{ij}y_ig^{n_im_{ij}}(v_{ij}y_i)^{-1} = v_{ij}u_i^{m_{ij}}v_{ij}^{-1}.$$

The assertion follows.

(ii) Take $u \in U$ and let $U = \dot{\bigcup}_j (H^{g_i} \cap U)y_{ij}\langle u\rangle$ be an $(H^{g_i} \cap U)$-$\langle u\rangle$ double coset decomposition. Then $G = \dot{\bigcup}_{i,j} Hg_iy_{ij}\langle u\rangle$ is a double coset decomposition,

$$|H|^{-1}|Hg_iy_{ij}\langle u\rangle| = |H^{g_i} \cap U|^{-1}|(H^{g_i} \cap U)y_{ij}\langle u\rangle| =: n_{ij}$$

and

$$\chi^{g_i}(y_{ij}u^{n_{ij}}y_{ij}^{-1}) = \chi(g_iy_{ij}u^{n_{ij}}y_{ij}^{-1}g_i^{-1}).$$

Hence the assertion.

(iii) Trivial.

Addition and tensor induction are far from being nicely connected. The next lemma studies the simplest non-trivial case. We need some notation: Let $H \lhd G$ be a normal subgroup of prime index r. Then G acts on $\Omega = \{Hg \mid g \in G\}$ and therefore also on the power set $\mathcal{P}\Omega$. Since G is transitive on Ω, there are precisely two fixed points in $\mathcal{P}\Omega$ (namely $\emptyset$ and Ω), so the $2^r - 2$ non-trivial subsets form orbits of length r under G. Let $I_j \subseteq \Omega$ be representatives for these orbits, i.e., $\dot{\bigcup}_j I_j^G = \mathcal{P}\Omega \backslash \{\emptyset, \Omega\}$. Now let χ and ψ be class functions of H. For each $I \subseteq \Omega$, define

$$\varphi_I = \prod_{\omega \in I} \chi^\omega \prod\nolimits_{\omega \notin I} \psi^\omega,$$

where $\chi^\omega = \chi^g$ if $\omega = Hg$. Let $\varphi_j = \varphi_{I_j}$. With this notation:

1.6 Lemma. *Let $H \lhd G$ and $|G:H| = r$ a prime.*

(i) $(\chi + \psi)^{\otimes G} = \chi^{\otimes G} + \psi^{\otimes G} + \Sigma_j \varphi_j^G$ *for class functions* χ, ψ *of* H.
(ii) $(\alpha 1_H)^{\otimes G} = \alpha 1_G + \mathrm{r}^{-1}(\alpha_r - \alpha)1_H^G$ *for* $\alpha \in \mathbf{C}$ *a constant.*

Proof. (i) Let $g \in G \backslash H$. Then $G = H\langle g\rangle$ and $|\langle g\rangle : \langle g\rangle \cap H| = r$, so

$$(\chi + \psi)^{\otimes G}(g) = (\chi + \psi)(g^r) = \chi(g^r) + \psi(g^r) = \chi^{\otimes G}(g) + \psi^{\otimes G}(g).$$

Since $\varphi_j^G(g) = 0$ for all j, the equality holds on $G\backslash H$. Since H is normal in G, it follows from Lemma 1.5 (ii) that

$$[(\chi + \psi)^{\otimes G}]_H = \prod_{\omega \in \Omega} (\chi + \psi)^\omega = \sum_{I \in P\Omega} \varphi_I = \varphi_\Omega + \varphi_\emptyset + \sum_j \sum_{I \in I_j^G} \varphi_I.$$

Since

$$(\varphi_j^G)_H = \sum_{g \in [G:H]} \varphi_{I_j}^g = \sum_{g \in [G:H]} \varphi_{I_j}^g = \sum_{I \in I_j^G} \varphi_I$$

and

$$\varphi_\Omega = \prod_{\omega \in \Omega} \chi^\omega = (\chi^{\otimes G})_H, \qquad \varphi_\emptyset = (\psi^{\otimes G})_H,$$

the equality also holds on H.

(ii) We have

$$(\alpha 1_H)^{\otimes G}(g) = \begin{cases} \alpha & \text{if } g \in G\setminus H \\ \alpha^r & \text{if } g \in H \end{cases}$$

and

$$1_H^G(g) = \begin{cases} 0 & \text{if } g \in G\setminus H \\ r & \text{if } g \in H. \end{cases}$$

Hence the assertion.

1.7 *Remark.* If R is a subring of $\mathbf{C}$ and $\alpha \in R$, then, in general, $r^{-1}(\alpha^r - \alpha)$ will not belong to R. Therefore tensor induction of an R-generalized character does not always yield an R-generalized character. For $R = \mathbf{Z}$, however, we have:

1.8 PROPOSITION. *Let H be a subgroup of G.*

(i) *If χ is a character of H, then $\chi^{\otimes G}$ is a character of G.*
(ii) *If γ is a generalized character of H, then $\gamma^{\otimes G}$ is a generalized character of G.*

Proof. (i) This is well known (see [1] for instance).

(ii) By Brauer's characterization of characters, it is enough to show $(\gamma^{\otimes G})_E$ is a generalized character for each elementary subgroup E of G. Since, by Lemma 1.5 (ii),

$$(\gamma^{\otimes G})_E = \prod_i (\gamma^{g_i}_{H^{g_i}\cap E})^{\otimes E} \quad \text{for } G = \dot{\bigcup_i} Hg_iE,$$

it is enough to show that $\gamma^{\otimes E}$ is a generalized character if γ is a generalized character of a subgroup U of the elementary group E. We proceed by induction on $|E:U|$. If $E = U$, there is nothing to show. If $U < U_1 < E$, then U_1 is elementary and $|U_1 : U|$, $|E : U_1| < |E : U|$, so by induction $\gamma^{\otimes U_1}$ and then also $(\gamma^{\otimes U_1})^{\otimes E}$ are generalized characters. In view of Lemma 1.5 (i), this is what we want.

We may therefore assume that U is maximal in E. Since E is nilpotent, this means $U \lhd E$ and $|E:U| = r$ is a prime. Let χ, ψ be characters of U such that $\chi - \psi = \gamma$. Then Lemma 1.6 (i) tells us that

$$\gamma^{\otimes E} = [\chi + (-\psi)]^{\otimes E} = \chi^{\otimes E} + (-\psi)^{\otimes E} + \sum_j \varphi_j^E$$

where, of course, in the definition of the φ_j's, we have to replace ψ by $-\psi$. In any case, the φ_j are—up to a sign—products of characters of U, so $\Sigma_j \varphi_j^E$ is a generalized character of E. By (i), $\chi^{\otimes E}$ and $\psi^{\otimes E}$ are characters, and

$$\begin{aligned}(-\psi)^{\otimes E} &= [(-1_U)\psi]^{\otimes E}\\ &= (-1_U)^{\otimes E}\psi^{\otimes E} \quad \text{(by Lemma 1.5 (iii))}\\ &= \{-1_E + r^{-1}[(-1)^r + 1]1_U^E\}\psi^{\otimes E} \quad \text{(by Lemma 1.6 (ii))}\end{aligned}$$

is a generalized character of E since $r \mid (-1)^r + 1$.

1.9 *Remark/Definition.* (i) If γ and δ are class functions of a group G, we say $\gamma \leqslant \delta$ if for all $g \in G$, the values $\gamma(g)$, $\delta(g)$ and $\delta(g) - \gamma(g)$ are non-negative real numbers. If $\gamma \leqslant \delta$ are class functions of $H \leqslant G$, then $\gamma^{\otimes G} \leqslant \delta^{\otimes G}$.

(ii) For γ and δ as above and $\mathscr{A}$ an ideal of the ring I of algebraic integers in $\mathbf{C}$, we say $\gamma \equiv \delta \bmod \mathscr{A}$ if $\gamma(g) \equiv \delta(g) \bmod \mathscr{A}$ for all $g \in G$. If $\gamma \equiv \delta \bmod \mathscr{A}$ are class functions of $H \leqslant G$ whose values are algebraic integers, then $\gamma^{\otimes G} \equiv \delta^{\otimes G} \bmod \mathscr{A}$ (and the values of $\gamma^{\otimes G}$, $\delta^{\otimes G}$ are algebraic integers).

2. Reduction to $C_G(v)$

2.1 *Notation.* We fix a prime p and denote by F a finite field of characteristic p, by F_0 its prime field $GF(p)$ and by G a finite group with order prime to p. If V is a finite-dimensional FG-module, then $\pi = \pi(G, V)$ denotes the permutation character of G on V, i.e., $\pi(g) = |C_V(g)|$. Observe that $\pi(g) \neq 0$ for all $g \in G$; in fact, $\pi(g)$ is always a power of p which divides $|V|$. Therefore $\pi^{-1}|V|$ is a generalized character of G by Proposition 1.1. We call this generalized character—which plays a central role in the rest of this paper—$\delta = \delta(G, V)$. Obviously $\delta(g) = 1$ iff $\pi(g) = |V|$ iff $g \in \operatorname{Ker}(G \text{ on } V)$; otherwise, $\delta(g) = p^n$ for some $n = n(g) > 0$. Since G acts on V, we may form the semidirect product GV which is a finite group. We try to bound $k(GV)$, where $k(H)$ is the number of conjugacy classes of the group H. The reason why δ is important is the following result.

2.2 THEOREM. *Assume* 2.1 *and suppose there is a* $v \in V$ *such that* $C = C_G(v)$ *satisfies:*

(*) *if* γ *is a generalized character of* C *such that* $\gamma(1) \not\equiv 0 \bmod p$, *then* $(\gamma\delta, \gamma)_C \geqslant k(C)$.

Then $k(GV) \leqslant |V|$.

Proof. We distinguish two cases: (i) $v = 1$ and (ii) $v \neq 1$. We first treat the easier case, $v = 1$.

(i) Here $C = G$. If $g \in G$ and $u \in V$, then $G \ni g^u = u^{-1}gu = g(u^{-1})^g u$ iff $(u^{-1})^g u = 1$ iff $u \in C_V(g)$, since G and V intersect trivially. This implies $g^{GV} \cap G = g^G$ so there are precisely $k(G)$ conjugacy classes of GV which intersect G non-trivially. $\delta^{GV} = 0$ on all other conjugacy classes, whereas

$$\begin{aligned}\delta^{GV}(g) &= \frac{1}{|G|}\sum_{x\in GV}\dot{\delta}(g^x)\\ &= \frac{1}{|G|}\sum_{\substack{h\in G\\ u\in V}}\dot{\delta}(g^{hu})\\ &= \frac{1}{|G|}\sum_{\substack{h\in G\\ u\in C_V(g^h)}}\delta(g^h)\\ &= \frac{1}{|G|}\sum_{h\in G}\delta(g^h)\pi(g^h)\\ &= |V|.\end{aligned}$$

Thus, if $\{x_i\}$ is a set of representatives of the conjugacy classes of GV, then

$$\begin{aligned}k(G)|V| &= \sum_i \delta^{GV}(x_i)\\ &= \sum_{\tau\in\mathrm{Irr}\ GV}(\tau\delta^{GV},\tau)_{GV}\quad\text{(by the orthogonality relations)}\\ &= \sum_{\tau\in\mathrm{Irr}\ GV}(\tau\delta,\tau)_G\quad\text{(by Frobenius reciprocity)}\\ &\geqslant \sum_{\tau\in\mathrm{Irr}\ GV}k(G)\quad\text{(by (*), since }\tau(1)\mid |G|\text{ by Itô's theorem)}\\ &= k(GV)k(G)\end{aligned}$$

Dividing by $k(G)$ gives the desired result.

(ii) Now assume $v \neq 1$. Let A be the subgroup of V generated by v. Then $|A| = p$ and $C_G(a) = C$ for all $1 \neq a \in A$. Put $N = N_G(A)$; then $C \lhd N$ and N/C operates fixpoint freely on A, in particular $|N:C| \mid p - 1$. The direct product $C \times A$ is a subgroup of GV. We will define a generalized character η on $C \times A$ and imitate the proof given in case (i) using η instead of δ. We first prove the following result.

Let $\{c_i \mid i = 1, \ldots, k(C)\}$ be a set of representatives for the C-conjugacy classes of C and let $\{a_j \mid j = 1, \ldots, |N:C|^{-1}(p - 1)\}$ be a set of representatives for the N-conjugacy classes of $A\setminus 1$. Then $\{c_i a_j\}$ is a set of representatives for the conjugacy classes of GV which intersect $C \times (A\setminus 1)$ non-trivially. In particular, there are $k(C)|N:C|^{-1}(p - 1)$ such classes.

Proof. Let $ca \in CA$, $a \neq 1$. Then there is $n \in N$ and j such that $a^n = a_j$. Since $c^n \in C$, there exist $d \in C$ and i such that $c^{nd} = c_i$. Then $(ca)^{nd} = c_i a_j^d = c_i a_j$. On the other hand, if $(c_i a_j)^{gu} = c_r a_s$ for some $g \in G$, $u \in V$, then $c_i^{gu} = c_r$ and $a_j^{gu} = a_s$ since C and A are relatively prime and commute with each other.

Now $A \ni a_s = a_j^{gu} = a_j^g$ implies $g \in N$ since $\langle a_j \rangle = A$. But then $j = s$ and $g \in C$. Since $c_i^{gu} \in G$ implies $u \in C_V(c_i^g)$, this means $c_r = c_i^g \in c_i^C$, so $r = i$.

From this proof, we also see that for $c \in C$, $1 \neq a \in A$, $g \in G$ and $u \in V$ the following holds: $(ca)^{gu} \in C \times A$ iff $g \in N$ and $u \in C_V(c^g)$.
Now define η on $C \times A$ by $\eta = \delta_C \times (p1_A - \rho_A)$, where ρ_A is the regular character of A.

So

$$\eta(ca) = \begin{cases} p\delta(c) & \text{if } a \neq 1 \\ 0 & \text{if } a = 1. \end{cases}$$

Therefore η^{GV} vanishes on all conjugacy classes of GV which intersect $C \times (A \setminus 1)$ trivially, whereas for $c \in C$, $1 \neq a \in A$,

$$\begin{aligned} \eta^{GV}(ca) &= \frac{1}{|C \times A|} \sum_{\substack{g \in G \\ u \in V}} \dot{\eta}[(ca)^{gu}] \\ &= \frac{1}{|C|p} \sum_{\substack{g \in N \\ u \in C_V(c^g)}} \eta(c^g a^g) \\ &= \frac{1}{|C|p} \sum_{g \in N} p\delta(c^g)\pi(c^g) \\ &= \frac{1}{|C|} \sum_{g \in N} |V| \\ &= |N:C||V|. \end{aligned}$$

Thus, if $\{x_i\}$ is again a set of representatives for the conjugacy classes of GV, then

$$\begin{aligned} (p-1)k(C)|V| &= [k(C)|N:C|^{-1}(p-1)][|N:C||V|] \\ &= \sum_i \eta^{GV}(x_i) \\ &= \sum_{\tau \in \mathrm{Irr}\, GV} (\tau\eta^{GV}, \tau)_{GV} \\ &= \sum_{\tau \in \mathrm{Irr}\, GV} (\tau\eta, \tau)_{C \times A} \\ &\geqslant \sum_{\tau \in \mathrm{Irr}\, GV} (p-1)k(C) \quad \text{(see below!)} \\ &= k(GV)(p-1)k(C) \end{aligned}$$

and, cancelling $(p - 1)k(C)$, the assertion follows.
So it remains to show $(\tau\eta, \tau)_{C \times A} \geqslant (p - 1)k(C)$ for each irreducible character τ of GV. Since $C \times A$ is a direct product, we can write

$$\tau|_{C\times A} = \sum_{\lambda} \tau_\lambda \times \lambda$$

where λ runs through $\Lambda = \operatorname{Irr} A$ (observe $|\Lambda| = p$) and τ_λ is a character of C or $\tau_\lambda = 0$, so

$$\begin{aligned}(\tau\eta, \tau)_{C\times A} &= \frac{1}{|C \times A|} \sum_{\substack{c\in C\\ a\in A}} \tau(ca)\eta(ca)\overline{\tau(ca)} \\ &= \frac{1}{|C|} \sum_{\substack{c\in C\\ 1\neq a\in A}} \tau(ca)\delta(c)\overline{\tau(ca)} \\ &= \frac{1}{|C|} \sum_{\substack{\lambda,\mu\in\Lambda\\ \mathrm{c}\in\mathrm{C}}} \tau_\lambda(c)\delta(c)\overline{\tau_\mu(c)} \sum_{1\neq a\in A} \lambda(a)\overline{\mu(a)}\end{aligned}$$

Since

$$\sum_{1\neq a\in A} \lambda(a)\overline{\mu(a)} = \begin{cases} p - 1 & \text{if } \lambda = \mu \\ -1 & \text{if } \lambda \neq \mu, \end{cases}$$

we have

$$\begin{aligned}(\tau\eta, \tau)_{C\times A} &= p \sum_{\lambda\in\Lambda} (\tau_\lambda\delta, \tau_\lambda)_C - \sum_{\lambda,\mu\in\Lambda} (\tau_\lambda\delta, \tau_\mu)_C \\ &= \sum_{\lambda<\mu} ((\tau_\lambda - \tau_\mu)\delta, (\tau_\lambda - \tau_\mu))_C\end{aligned}$$

for some arbitrary ordering $\leqslant$ on Λ. By (*), we are done if there are at least $p - 1$ pairs $\lambda < \mu$ with $(\tau_\lambda - \tau_\mu)(1) \not\equiv 0 \bmod p$. If

$$\tau_\lambda(1) \equiv \tau_\mu(1) \bmod p \quad \text{for all } \lambda, \mu,$$

then

$$\tau(1) = \sum_{\lambda} \tau_\lambda(1) \equiv 0 \bmod p,$$

contradicting Itô's theorem.

So let $\Lambda_1 = \{\lambda \mid \tau_\lambda(1) \equiv \tau_1(1) \bmod p\}$ and $\Lambda_2 = \Lambda\setminus\Lambda_1$. Then $\Lambda_1, \Lambda_2 \neq \emptyset$ and $|\Lambda_1| + |\Lambda_2| = p$. Moreover, we may choose the ordering such that $\lambda \in \Lambda_1$, and $\mu \in \Lambda_2$ implies $\lambda < \mu$. Hence there are at least $|\Lambda_1||\Lambda_2|$ pairs $\lambda < \mu$ with $(\tau_\lambda - \tau_\mu)(1) \not\equiv 0 \bmod p$.

Now

$$\begin{aligned}0 &\leqslant (|\Lambda_1| - 1)(|\Lambda_2| - 1) \\ &= |\Lambda_1|\,|\Lambda_2| - |\Lambda_1| - |\Lambda_2| + 1 \\ &= |\Lambda_1|\,\Lambda_2| - (p - 1),\end{aligned}$$

so $|\Lambda_1||\Lambda_2| \geqslant p - 1$ and we are done.

In the next two sections, we seek conditions which guarantee (*).

3. $\delta(G, V)$ for abelian G

The following will be used throughout this paragraph except for the last result:

3.1 *Notation.* G is a finite abelian group and U_i, $i \in N = \{1, \dots, n\}$ are subgroups of G. Let Λ be the group of irreducible characters of G and $\Lambda_i = \mathrm{Irr}(G/U_i)$, regarded as characters of G, so Λ_i is a subgroup of Λ for each $i \in N$. If $I \subseteq N$, then we set

$$U_I = \bigcap_{i\in I} U_i \leqslant G \quad \text{and} \quad \Lambda_I = \prod_{i\in I} \Lambda_i \leqslant \Lambda.$$

We form $A_I = \Pi_{i\in I} \times \Lambda_i$, the direct product. If $J \subseteq I$ and $\alpha \in A_I$, we set $\alpha_J = \Pi_{j\in J}\, \alpha(j)$, so $\alpha_J \in \Lambda_J$, and $\alpha \mapsto \alpha_I$ is an epimorphism from A_I onto Λ_I. Again, for $\alpha \in A_I$ and $J \subseteq I$, we define $\alpha^J \in A_I$ by

$$\alpha^J(i) = \begin{cases} \alpha(i) & \text{for } i \in I \setminus J \\ \alpha(i)^{-1} & \text{for } i \in J. \end{cases}$$

Finally, we define two kinds of generalized characters of G: For $\alpha \in A_I$, let $\gamma_\alpha = \Pi_{i\in I}\,(1_G - \alpha(i))$. For each $i \in N$, set

$$\eta_i = (|G:U_i| + 1)1_G - 1_{U_i}^G \quad \text{and} \quad \eta = \prod_{i\in N} \eta_i.$$

3.2 LEMMA. *Fix $\lambda \in \Lambda$ and $I \subseteq N$. Then the Boolean group $B = \mathcal{P}(I)$ operates on $\lambda\Lambda_I \times A_I$ by $[\mu, \alpha]^J = [\mu\alpha_J, \alpha^J]$. Furthermore:*

(i) *If $[\mu, \beta] \in [\lambda, \alpha]^B$, then $\mu\gamma_\beta \in \{\pm\lambda\gamma_\alpha\}$.*

(ii) *$|C_B[\lambda, \alpha]|^{-1}\lambda\gamma_\alpha$ is a generalized character of G for all $\alpha \in A_I$.*

(iii) *Let χ be a generalized character of G and $\alpha \in A_I$. Then*

$$2^{-|I|} \sum_{[\mu,\beta]\in[\lambda,\alpha]^B} (\chi, \mu\gamma_\beta)^2$$

is a non-negative integer. It is positive if $(\chi, \lambda\gamma_\alpha) \neq 0$.

Proof. Clearly $\alpha_J \in \Lambda_I$ and $\alpha^J \in A_I$ for any $J \subseteq I$, $\alpha \in A_I$, so

$$[\mu, \alpha]^J \in \lambda\Lambda_I \times A_I \quad \text{if} \quad [\mu, \alpha] \in \lambda\Lambda_I \times A_I.$$

For $J, K \in B$, let $J \dotplus K = (J \cup K)\setminus(J \cap K)$. It is well-known that $(B, \dotplus)$ is an elementary abelian 2-group. Moreover

$$(\alpha^J)^K = \alpha^{J\dotplus K} \quad \text{and} \quad \alpha_J(\alpha^J)_K = \alpha_{J\dotplus K},$$

so $[\mu, \alpha] \mapsto [\mu, \alpha]^J$ defines an action of B.

(i) Suppose $[\mu, \beta] = [\lambda, \alpha]^J = [\lambda\alpha_J, \alpha^J]$. Then

$$\begin{aligned}\mu\gamma_\beta &= \lambda\alpha_J \prod_{i\in I}(1-\alpha^J(i))\\ &= \lambda\prod_{j\in J}\alpha(j)\prod_{j\in J}(1-\alpha(j)^{-1})\prod_{i\in I\setminus J}(1-\alpha(i))\\ &= \lambda\prod_{j\in J}(\alpha(j)-1)\prod_{i\in I\setminus J}(1-\alpha(j))\\ &= (-1)^{|J|}\lambda\prod_{j\in J}(1-\alpha(j))\prod_{i\in I\setminus J}(1-\alpha(i))\\ &= (-1)^{|J|}\lambda\gamma_\alpha.\end{aligned}$$

(ii) Let $C = C_B[\lambda, \alpha]$. If $K \in C$, then $[\lambda, \alpha] = [\lambda, \alpha]^K = [\lambda\alpha_K, \alpha^K]$, so $\alpha_K = 1$ and $\alpha^K = \alpha$. For any $J \in B$, therefore $\alpha_{K\dotplus J} = \alpha_K(\alpha^K)_J = \alpha_J$. Now, let $B = \bigcup_s C \dotplus J_s$ be a coset decomposition. Then

$$\begin{aligned}\gamma_\alpha &= \prod_{i\in I}(1-\alpha(i))\\ &= \sum_{J\subseteq I}(-1)^{|J|}\alpha_J\\ &= \sum_s\sum_{K\in C}(-1)^{|K\dotplus J_s|}\alpha_{K\dotplus J_s}\\ &= \sum_s(-1)^{|J_s|}\alpha_{J_s}\sum_{K\in C}(-1)^{|K|},\end{aligned}$$

since $|K \dotplus J_s| \equiv |K| + |J_s| \bmod 2$.
If $|K| \equiv 0 \bmod 2$ for all $K \in C$, then $\Sigma_{K\in C}(-1)^{|K|} = |C|$. If there is $K \in C$ such that $|K| \equiv 1 \bmod 2$, then the K's of even cardinality form a subgroup of index 2 in C, so $\Sigma_{K\in C}(-1)^{|K|} = 0$. In either case, $|C|^{-1}\gamma_\alpha$ is a generalized character and so is $|C|^{-1}\lambda\gamma_\alpha$.

(iii) By (i), $\mu\gamma_\beta = \pm\lambda\gamma_\alpha$ for $[\mu, \beta] \in [\lambda, \alpha]^B$, so all summands in the sum are equal. If $C = C_B[\lambda, \alpha]$, then there are $|B:C| = 2^{|I|}|C|^{-1}$ summands, hence

$$2^{-|I|}\sum_{[\mu,\beta]\in[\lambda,\alpha]^{\mathrm{B}}}(\chi, \mu\gamma_\beta)^2 = |C|^{-1}(\chi, \lambda\gamma_\alpha)^2 = (\chi, \lambda\gamma_\alpha)(\chi, |C|^{-1}\lambda\gamma_\alpha)$$

which is an integer by (ii). The other assertions are obvious.

3.3 LEMMA. $\eta = \Sigma_{I\subseteq N}\, 2^{-|I|}\, \Sigma_{\alpha\in A_I}\, \gamma_\alpha\bar{\gamma}_\alpha$.

Proof. Induction on n. If $n = 0$, then the left hand side is 1_G as product over the empty set, whereas oı the right, there is only one I, namely $I = \emptyset$, $A_\emptyset$ contains precisely one element, namely the empty map $\alpha_\emptyset$, and $\gamma_{\alpha_\emptyset} = 1_G$, again as product over the empty index set.
Now let $n > 0$, $N' = N\setminus\{n\}$ and $\eta' = \Pi_{i\in N'}\,\eta_i$, so $\eta = \eta'\eta_n$ and we have the result for η' by induction. We rewrite η_n:

$$\sum_{\lambda\in\Lambda_n}(1_G-\lambda)(1_G-\bar{\lambda}) = 2\left[|\Lambda_n|1_G - \sum_{\lambda\in\Lambda_n}\lambda\right]$$
$$= 2[|G:U_n|1_G - 1_{U_n}^G]$$
$$= 2\eta_n - 2\,1_G,$$

so $\eta_n = 1_G + \frac{1}{2}\Sigma_{\lambda\in\Lambda_n}(1_G-\lambda)(1_G-\bar{\lambda})$. Therefore

$$\eta = \eta'\eta_n = \sum_{I\subseteq N'} 2^{-|I|}\sum_{\alpha\in A_I}\gamma_\alpha\bar{\gamma}_\alpha$$
$$+\frac{1}{2}\sum_{I\subseteq N'} 2^{-|I|}\sum_{\alpha\in A_I}\gamma_\alpha\bar{\gamma}_\alpha\sum_{\lambda\in\Lambda_n}(1_G-\lambda)(1_G-\bar{\lambda})$$
$$= \sum_{I\subseteq N'} 2^{-|I|}\sum_{\alpha\in A_I}\gamma_\alpha\bar{\gamma}_\alpha + \sum_{I\subseteq N'} 2^{-|I\cup\{n\}|}\sum_{\alpha\in A_{I\cup\{n\}}}\gamma_\alpha\bar{\gamma}_\alpha$$

since $\{\gamma_\alpha(1_G - \lambda) \mid \alpha\in A_I, \lambda\in\Lambda_n\} = \{\gamma_\beta \mid \beta\in A_{I\cup\{n\}}\}$. This proves the lemma.

3.4 Corollary. *Let χ be a virtual character of G. Then*

$$(\chi\eta, \chi) = \sum_{I\subseteq N} 2^{-|I|}\sum_{[\lambda,\alpha]\in\Lambda\times A_I}(\chi, \lambda\gamma_\alpha)^2.$$

Proof. Clearly $(\chi\gamma_\alpha\bar{\gamma}_\alpha, \chi) = \Sigma_{\lambda\in\Lambda}(\chi, \lambda\gamma_\alpha)^2$, so the result follows from the preceding lemma.

3.5 Proposition. *Let the notation be as before and assume in addition that $U_N = 1$. Then $(\chi\eta, \chi) \geqslant |G|$ for every virtual character $\chi \neq 0$ of G.*

Proof. For each $\lambda\in\Lambda$, let

$$\mathcal{M}_\lambda = \{I\subseteq N \mid \text{there exists } \mu\in\Lambda_I \text{ such that } (\chi, \lambda\mu)\neq 0\}.$$

Since $\chi\neq 0$, there is $\nu\in\Lambda$ such that

$$0\neq(\chi,\nu) = (\chi, \lambda[\lambda^{-1}\nu]) \quad\text{and}\quad \lambda^{-1}\nu\in\Lambda = \Lambda_N$$

Since Ker $\Lambda_N = \cap$ Ker $\Lambda_i = U_N = 1$), which shows that $N\in\mathcal{M}_\lambda$, so, in particular, $\mathcal{M}_\lambda\neq\emptyset$. Now, in each $\mathcal{M}_\lambda$ choose an element of minimal cardinality; call this element $m(\lambda)$. So we have a map $m:\Lambda\to\mathcal{P}(N)$ such that, for all $\lambda\in\Lambda$,

(i) there exists $\mu\in\Lambda_{m(\lambda)}$ with $(\chi, \lambda\mu)\neq 0$, and
(ii) If $J\subset_{\neq} m(\lambda)$, then $(\chi, \lambda\mu) = 0$ for all $\mu\in\Lambda_J$.

We partition $\Lambda = \dot{\cup}_{I\subseteq N}\, m^{-1}(I)$ where $m^{-1}(I) = \{\lambda\in\Lambda \mid m(\lambda) = I\}$ is the inverse image of I under m.

Fix $I \subseteq N$ and a coset $\varphi\Lambda_I \subseteq \Lambda$.

Claim. $|m^{-1}(I) \cap \varphi\Lambda_I| \leq 2^{-|I|} \sum_{[\mu,\alpha]\in\varphi\Lambda_I\times A_I} (\chi, \mu\gamma_\alpha)^2$

Proof of claim. There is nothing to show if $m^{-1}(I) \cap \varphi\Lambda_I = \emptyset$, so assume $m^{-1}(I) \cap \varphi\Lambda_I = \{\varphi\sigma_1, \ldots, \varphi\sigma_t\}$, the $\sigma_s \in \Lambda_I$ all different. By construction, $m(\varphi\sigma_s) = I$, so if $J \subset_{\neq} I$ and $\beta \in \Lambda_J$, then $(\chi, \varphi\sigma_s\beta) = 0$. For $\alpha \in A_I$, we have $\gamma_\alpha = \sum_{J\subseteq I} (-1)^{|J|}\alpha_J$, so

$$(\chi, \varphi\sigma_s\gamma_\alpha) = \sum_{J\subseteq I} (-1)^{|J|}(\chi, \varphi\sigma_s\alpha_J) = (-1)^{|I|}(\chi, \varphi\sigma_s\alpha_I).$$

Now, $\alpha \mapsto \alpha_I$ is an epimorphism $A_I \to \Lambda_I$ and by definition of I, there is a $\beta \in A_I$ such that $(\chi, \varphi\sigma_1\beta_I) \neq 0$. Moreover, we can choose $\alpha_s \in A_I$ such that $(\alpha_s)_I = \sigma_s^{-1}\sigma_1 \in \Lambda_I$. Let $\beta_s = \alpha_s\beta \in A_I$; then $[\varphi\sigma_s, \beta_s] \in \varphi\Lambda_I \times A_I$ for $s = 1, \ldots, t$. We will show that (i) $(\chi, \varphi\sigma_s\gamma_{\beta_s}) \neq 0$ for all s and (ii) the $[\varphi\sigma_s, \beta_s]$'s belong to different orbits under the action of $B = \mathcal{P}(I)$ (see Lemma 3.2). The claim will then follow from (iii) of the lemma.

(i) As we have seen before,

$$\begin{aligned}(\chi, \varphi\sigma_s\gamma_{\beta_s}) &= (-1)^{|I|}(\chi, \varphi\sigma_s(\beta_s)_I)\\ &= (-1)^{|I|}(\chi, \varphi\sigma_s(\alpha_s)_I\beta_I)\\ &= (-1)^{|I|}(\chi, \varphi\sigma_1\beta_I)\\ &\neq 0.\end{aligned}$$

(ii) Let $J \subseteq I$ such that for $1 \leq s, k \leq t$,

$$[\varphi\sigma_s, \beta_s] = [\varphi\sigma_k, \beta_k]^J = [\varphi\sigma_k(\beta_k)_J, (\beta_k)^J].$$

Then

(1) $\alpha_s\beta = \beta_s = (\beta_k)^J = \alpha_k^J\beta^J$,
(2) $\sigma_s = \sigma_k(\beta_k)_J = \sigma_k(\alpha_k)_J\beta_J$.

From (1), we get

$$\begin{aligned}\sigma_s^{-1}\sigma_1\beta_I &= (\alpha_s)_I\beta_I\\ &= (\alpha_s\beta)_I\\ &= (\alpha_k^J\beta^J)_I\\ &= (\alpha_k^J)_I(\beta^J)_I\\ &= (\alpha_k)_I[(\alpha_k)_J]^{-2}\beta_I(\beta_J)^{-2}\\ &= \sigma_k^{-1}\sigma_1[(\alpha_k)_J]^{-2}\beta_I(\beta_J)^{-2},\end{aligned}$$

so $\sigma_s = \sigma_k[(\alpha_k)_J]^2(\beta_J)^2$.

Comparing with (2), we get $(\alpha_k)_J\beta_I = 1$, so $\sigma_s = \sigma_k$ and $s = k$. Now it is easy to prove the proposition:

$$\begin{aligned}(\chi\eta, \chi) &= \sum_{I\subseteq N} 2^{-|I|} \sum_{[\lambda,\alpha]\in\Lambda\times A_I} (\chi, \lambda\gamma_\alpha)^2 \quad \text{(by Corollary 3.4)}\\ &= \sum_{I\subseteq N} \sum_{\varphi\in[\Lambda:\Lambda_I]} 2^{-|I|} \sum_{[\mu,\alpha]\in\varphi\Lambda_I\times A_I} (\chi, \mu\gamma_\alpha)^2\\ &\geqslant \sum_{I\subseteq N} \sum_{\varphi\in[\Lambda:\Lambda_I]} |m^{-1}(I) \cap \varphi\Lambda_I| \quad \text{(by the claim)}\\ &= \sum_{I\subseteq N} \left| \dot{\bigcup_{\varphi\in[\Lambda:\Lambda_I]}} m^{-1}(I) \cap \varphi\Lambda_I \right|\\ &= \sum_{I\subseteq N} |m^{-1}(I)|\\ &= |\Lambda|\\ &= |G|.\end{aligned}$$

The application to the problem of bounding the class number is contained in the next two results. We use again the notation introduced in § 2.

3.6 Proposition. *Let G be an abelian p'-group and V a faithful FG-module. Then $(\chi\delta, \chi) \geqslant |G|$ for each virtual character $\chi \neq 0$ of G (of course $\delta = \delta(G, V)$).*

Proof. Let $V = \Sigma_{i=1}^n \oplus W_i$ be a decomposition into irreducible FG-modules and put $\delta_i = \delta(G, W_i)$. Since $\pi(g) = |C_V(g)| = \Pi_i |C_{W_i}(g)|$ for all $g \in G$ *and* $|V| = \Pi_i |W_i|$, we have $\delta = \Pi_i \delta_i$. Now $C_{W_i}(g)$ is an FG-submodule of W_i since G is abelian, so by the irreducibility of W_i either $C_{W_i}(g) = W_i$ which means $g \in \mathrm{Ker}(G \text{ on } W_i)$ ($= U_i$ for short) or $C_{W_i}(g) = 0$. This implies

$$\delta_i(g) = \begin{cases} 1 & \text{if } g \in U_i \\ |W_i| & \text{if } g \notin U_i, \end{cases}$$

so

$$\delta_i = |W_i| 1_G - \frac{|W_i| - 1}{|G:U_i|} 1_{U_i}^G.$$

Since δ_i is a generalized character and $(1_{U_i}^G, 1_G) = 1$, this implies in particular $|G:U_i| \mid |W_i| - 1$, say $|W_i| = t_i|G:U_i| + 1$. Therefore

$$\begin{aligned}\delta_i &= (t_i|G:U_i| + 1)1_G - t_i 1_{U_i}^G\\ &= (|G:U_i| + 1)1_G - 1_{U_i}^G + (t_i - 1)[|G:U_i|1_G - 1_{U_i}^G]\\ &\geqslant (|G:U_i| + 1)1_G - 1_{U_i}^G\\ &= \eta_i\end{aligned}$$

since $t_i \geqslant 1$ and $|G:U_i|1_G - 1_{U_i}^G$ only takes non-negative real values. This implies $\delta = \Pi_i\delta_i \geqslant \Pi_i\eta_i = \eta$, so $(\chi\delta, \chi) \geqslant (\chi\eta, \chi) \geqslant |G|$ by Proposition 3.5 since $U_N = \cap_{i\in N}U_i = \mathrm{Ker}(G \text{ on } V) = 1$.

We now drop the assumption that G is abelian.

3.7 THEOREM. *Let G be a p'-group and V a faithful FG-module. If there exists $v \in V$ such that $C_G(v)$ is abelian, then $k(GV) \leqslant |V|$.*

Proof. Immediate from Theorem 2.2 and Proposition 3.6.

4. δ Contains a Square

4.1 DEFINITION. Let $\mathscr{L}$ be a $\mathbf{Z}$-lattice in $\mathbf{C}$ and $\mathscr{A}$ an ideal of I (the ring of algebraic integers in $\mathbf{C}$). Assume η to be a generalized character of G with non-negative real values. We say that η *contains an $\mathscr{L}$-square with respect to $\mathscr{A}$*, if there is an $\mathscr{L}$-generalized character ν of G such that

(i) $\eta \geqslant \nu\bar{\nu}$ and
(ii) $\eta \equiv \nu \bmod \mathscr{A}$

(see Remark 1.9).

4.2 *Notation.* In our applications, $\mathscr{A}$ will always be the same ideal, namely $\mathscr{A} = \sqrt{pI}$. We therefore drop the reference to $\mathscr{A}$ and say simply that η contains an $\mathscr{L}$-square. The most important case is $\mathscr{L} = \mathbf{Z}$; we then shorten notation further and say that η contains a square. If convenient, we will also say that η contains the square of ν. The assumption on $\mathscr{L}$ in the next proposition is certainly satisfied for $\mathscr{L} = \mathbf{Z}$.

4.3 PROPOSITION. *Let η be a generalized character of G with $\eta(1) \not\equiv 0 \bmod p$ but $\eta(g) \in \mathscr{A}$ for all $1 \neq g \in G$. Let $\mathscr{L}$ be a $\mathbf{Z}$-lattice in $\mathbf{C}$ such that $|x| \geqslant 1$ for all $0 \neq x \in \mathscr{L}$. If η contains an $\mathscr{L}$-square, then $(\gamma\eta, \gamma) \geqslant k(G)$ for each generalized character γ of G with $\gamma(1) \not\equiv 0 \bmod p$.*

Proof. First, observe that the assumption on the values of η forces G to be a p'-group:

$$(\eta, 1) \in \mathbf{Z} \quad \text{and} \quad |G|(\eta, 1) = \sum_g \eta(g) \equiv \eta(1) \not\equiv 0 \bmod \mathscr{A},$$

so $p \nmid |G|$.

Now let γ be as in the assumption and ν as in Definition 4.1. Then

$$(\gamma\eta, \gamma) \geqslant (\gamma\nu\bar{\nu}, \gamma) = (\gamma\nu, \gamma\nu) = \sum_{\tau\in\mathrm{Irr}\, G} |(\gamma\nu, \tau)|^2.$$

Since ν is an $\mathscr{L}$-generalized character and $\mathscr{L}$ is a $\mathbf{Z}$-lattice, $\gamma\nu$ is an $\mathscr{L}$-

generalized character, so $(\gamma\nu, \tau) \in \mathscr{L}$. In view of the assumption on $\mathscr{L}$, it is therefore enough to show that $(\gamma\nu, \tau) \neq 0$ for all $\tau \in \operatorname{Irr} G$. We have

$$\begin{aligned}|G|(\gamma\nu, \tau) &= \sum_{g\in G} \gamma(g)\nu(g)\overline{\tau(g)}\\ &\equiv \sum_{g\in G} \gamma(g)\eta(g)\overline{\tau(g)} \mod \mathscr{A}\\ &\equiv \gamma(1)\eta(1)\tau(1) \mod \mathscr{A}\\ &\not\equiv 0 \mod \mathscr{A},\end{aligned}$$

since $\gamma(1)\eta(1)\tau(1) \in \mathbf{Z}$ is not divisible by p (recall $\tau(1) \mid |G|$).

In view of Theorem 2.2 and the last proposition, it is of interest to give sufficient conditions for the existence of an element $v \in V$ (an FG-module) such that $\delta(C_G(v), V)$ contains a square. It is fairly easy to show that it is usually enough to consider a primitive module V. The induction step will be provided by Proposition 4.6.

4.4 *Notation.* Let $H \leqslant G$ be a subgroup, G a p'-group. Then we write

$$\pi(G{:}H) = \pi(G, F_0 \otimes_{F_0H} F_0G) \quad \text{and} \quad \delta(G{:}H) = \delta(G, F_0 \otimes_{F_0H} F_0G),$$

F_0 the trivial F_0H-module; i.e., we consider the permutation module (over the prime field) of G on the cosets of H in G.

4.5 PROPOSITION. *Let H be a subgroup of the p'-group G and let W be an FH-module. Then*

$$\delta(G, W \otimes_{FH} FG) = \delta(H, W)^{\otimes G}\, \delta(G{:}H)^t \quad \textit{where } t = \dim_{F_0} W.$$

Proof. Take $x \in G$ and write $X = \langle x \rangle$. Let $G = \dot{\bigcup}_{i=1,\ldots,s} Hg_iX$ be a double coset decomposition, $n_i = |H|^{-1}|Hg_iX|$ and put $V = W \otimes_{FH} FG$. By Mackey Decomposition and Frobenius Reciprocity,

$$\begin{aligned}\dim_F C_V(x) &= \dim_F \operatorname{Hom}_{FX}(F, V_{FX})\\ &= \dim_F \operatorname{Hom}_{FX}\Big(F, \sum_i \oplus\, W^{g_i} \otimes_{F\langle x^{n_i}\rangle} FX\Big)\\ &= \sum_i \dim_F \operatorname{Hom}_{F\langle x^{n_i}\rangle}(F, W^{g_i})\\ &= \sum_i \dim_F C_W(g_ix^{n_i}g_i^{-1}),\end{aligned}$$

so

$$\pi(G, V)(x) = \prod_i \pi(H, W)(g_ix^{n_i}g_i^{-1}) = \pi(H, W)^{\otimes G}(x),$$

i.e., $\pi(G, V) = \pi(H, W)^{\otimes G}$. On the other hand,

$$[\pi(H, W)\,\delta(H, W)]^{\otimes G}(x) = |W|^{\otimes G}(x) = |W|^s = p^{st} = [\pi(G{:}H)(x)]^t,$$

i.e., $[\pi(H, W)\,\delta(H, W)]^{\otimes G} = \pi(G{:}H)^t$. Therefore

$$\begin{aligned}\pi(G, V)\,\delta(H, W)^{\otimes G}\,\delta(G{:}H)^t &= [\pi(H, W)\,\delta\,(H, W)]^{\otimes G}\,\delta(G{:}H)^t\\ &= [\pi(G{:}H)\,\delta(G{:}H)]^t\\ &= p^{|G:H|t}\\ &= |W|^{|G:H|}\\ &= |V|\\ &= \pi(G, V)\,\delta(G, V).\end{aligned}$$

The assertion follows.

4.6 Proposition. *Let W be an FH-module, H a subgroup of the p'-group G and put $V = W \otimes_{FH} FG$. Assume $\dim_{F_0}(W) > 1$. If there exists $w \in W$ such that $\delta(C_H(w), W)$ contains a square, then there exists $v \in V$ such that $\delta(C_G(v), V)$ contains a square.*

Proof. Let $G = \dot{\bigcup}_{i\in I} Hg_i$ be a coset decomposition and $v = \Sigma_i w \otimes g_i$. Let $C = C_H(w)$ and $D = C_G(v)$; let $\delta = \delta(G, V)$, $\eta = \delta(H, W)$ and $\gamma = \delta(G{:}H)$. By the previous proposition, $\delta = \eta^{\otimes G}\gamma^t$, where $t = \dim_{F_0} W > 1$. Moreover, by assumption there exists a generalized character ν of C such that $\eta|_C \geqslant \nu\bar{\nu}$ and $\eta|_C \equiv \nu \bmod \mathscr{A}$. Let $G = \dot{\bigcup}_{j\in J} Hg_jD$ be a double coset decomposition, $J \subseteq I$. Take $x \in H^{g_j} \cap D$, say $x = h^{g_j}$. Looking at *j-th* component of $\Sigma_i w \otimes g_i = v = vx = \Sigma_i w \otimes g_i h^{g_j}$, we see that $wh = w$, so $h \in C$ and $x \in C^{g_j}$; hence $H^{g_j} \cap D \leqslant C^{g_j}$. Now let $\nu_j = \nu^{g_j}_{H^{g_j}\cap D}$ and $\zeta = \Pi_{j\in J}\nu_j^{\otimes D}$. By Proposition 1.8 (ii), ζ is a generalized character of D. Moreover

$$\begin{aligned}\zeta\bar{\zeta} &= \prod_j \nu_j^{\otimes D}\overline{\nu_j^{\otimes D}}\\ &= \prod_j (\nu_j\bar{\nu}_j)^{\otimes D} \quad \text{(since tensor induction is multiplicative and commutes with taking the complex conjugate)}\\ &\leqslant \prod_j (\eta^{g_j}|_{H^{g_j}\cap D})^{\otimes D} \quad \text{(by Remark 1.9 (i))}\\ &= \eta^{\otimes G}|_D \quad \text{(by Lemma 1.5 (ii))},\end{aligned}$$

and $\nu_j \equiv \eta^{g_j}|_{H^{g_j}\cap D} \bmod \mathscr{A}$, so

$$\nu_j^{\otimes D} \equiv (\eta^{g_j}|_{H^{g_j}\cap D})^{\otimes D} \quad \bmod \mathscr{A} \quad \text{(by Remark 1.9 (ii))}$$

and

$$\zeta \equiv \eta^{\otimes G}|_D \bmod \mathscr{A}.$$

This means that $\eta^{\otimes G}|_D$ contains the square of ζ. Clearly γ^t contains the square of γ, so $\delta(D, V) = \eta^{\otimes G}|_D(\gamma|_D)^t$ contains the square of $\zeta\gamma|_D$.

4.7 Corollary. *Let W be an FH-module, H a subgroup of the p'-group G. Assume that $\delta(H, W)$ contains a square and that* $\dim_{F_0} W > 1$. *Then $\delta(G, W \otimes_{FH} FG)$ contains a square.*

Proof. This follows from the proof of the preceding proposition, putting $v = w = 0$.

The last two results are used as induction steps. We also need "absolute" results for two special modules. The first one is the group algebra itself (G a p'-group):

4.8 Lemma. *Either $\delta(G, FG)$ contains a square or $|G| = 2$ and $F = F_0$.*

Proof. If $F > F_0$, then $\delta(G, FG)$ contains the square of $\delta(G, F_0G)$, so we assume $F = F_0$.
By Corollary 4.7, it is enough to find a subgroup H such that $\delta = \delta(H, FH)$ contains a square, since $FG = FH \otimes_{FH} FG$. The case $G = 1$ being trivial, we may choose a subgroup H of order r, where r is either an odd prime or $r = 4$. Let

$$k = \begin{cases} \frac{1}{2}(r - 1) & \text{if } r \text{ is odd} \\ 1 & \text{if } r = 4, \end{cases}$$

and observe that $(p^k)^2 \equiv 1 \bmod r$ since p and r are relatively prime. Therefore $p^k \equiv \varepsilon = \pm 1 \bmod r$.
Define $\nu = \varepsilon p^k 1_H - r^{-1}(\varepsilon p^k - 1)\rho_H$ where ρ_H denotes the regular character of H. Then ν is a generalized character of H and if $h \in H$, then

$$\nu(h) = \begin{cases} 1 & \text{if } h = 1 \\ \varepsilon p^k & \text{if } h \neq 1. \end{cases}$$

Since $\delta(h) = p^{r[1 - o(h)^{-1}]}$, it is obvious that $\nu \equiv \delta \bmod \mathscr{A}$ and easy to check that $\nu\bar{\nu} = \nu^2 \leqslant \delta$ (in fact, we have equality unless $H = C_4$). Therefore δ contains the square of ν.

The second result in this context concerns permutation modules of 2-groups. Let p be an odd prime, $\alpha = \frac{1}{2}(1 + i\sqrt{p}) \in \mathbf{C}$ and $\mathscr{L} = \mathbf{Z} \oplus \mathbf{Z}\alpha$. With this notation:

4.9 Proposition. *Let G be a 2-group acting on a finite set Ω. Then $\delta(G, F\Omega)$ contains an $\mathscr{L}$-square.*

Proof. It is enough to consider the cases $|\Omega| = 2^n$ ($n = 0, 1, \ldots$) and G a Sylow-2-subgroup of S_Ω, since the assertion will then hold for any subgroup as well (observe that $\delta = \delta(G, F\Omega) = \delta(G, F\Omega')$ if $\Omega' \supseteq \Omega$ and G acts trivially on $\Omega' \setminus \Omega$).

We set σ = sign, so σ is a linear character of G, and proceed by induction on n to produce a generalized character χ such that $\nu = \chi[1_G + \alpha(\sigma - 1_G)]$ has the following two properties:

(i) $\nu\bar{\nu} = \delta$

(ii) $\nu \equiv \delta \bmod \mathscr{A}$

(the induction will show that χ takes values in $\mathbf{Z}$). Since ν is clearly an $\mathscr{L}$-generalized character, this will prove the proposition.

It is easy to check that $\chi = 1_G$ will do for $n = 0, 1$.

So assume $n > 1$. The structure of G is then easily described: say

$$\Omega = \{1, \ldots, 2^n\},$$

and let $\Omega_1 = \{1, \ldots, 2^{n-1}\}$ and $\Omega_2 = \{2^{n-1} + 1, \ldots, 2^n\}$, so $\Omega = \Omega_1 \dot{\cup} \Omega_2$. Let H_1 be a Sylow-2-subgroup of S_{Ω_1} and s the product of the transpositions $(i, i + 2^{n-1})$ for $i = 1, \ldots, 2^{n-1}$. Then $H_2 = H_1^s$ is a Sylow-2-subgroup of S_{Ω_2} and a look at the orders shows that G is—up to conjugation in S_Ω—the semidirect product $(H_1 \times H_2)\langle s\rangle$. We put $H = H_1 \times H_2$, so

$$F\Omega \simeq F\Omega_1 \otimes_{FH} FG,$$

where of course H acts on Ω_1 with kernel H_2. By induction, there is a (integral-valued) generalized character χ_1 of H_1—and therefore of H—such that

$$\nu_1 = \chi_1[1_H + \alpha(\sigma_1 - 1_H)]$$

satisfies (i) and (ii) with δ replaced by $\delta_1 = \delta(H, F\Omega_1)$. It should be noted that σ_1 is the signum function of H not on Ω but on Ω_1, i.e., $\sigma_1(h_1h_2) = \text{sign}_{\Omega_1}(h_1)$ for $h_i \in H_i$.

We need some notation: let φ be the linear character of G with $\text{Ker}\varphi = H$, i.e., $1_H^G = 1_G + \varphi$, and let $\mu = \sigma_1^G$; then clearly $\varphi\mu = \mu$. Since $n > 1$, the element s belongs to the alternating group; using this and the definition of tensor induction, it is straightforward to check $\sigma = \sigma_1^{\otimes G}$. Observe that $\sigma \neq \varphi$ since H contains transpositions. Furthermore, $\sigma_H = \sigma_1\sigma_1^s$, so $\sigma\mu = (\sigma|_H\sigma_1)^G = (\sigma_1^s)^G = \mu$. This implies that $(\mu^2, \sigma) = (\mu, \mu\sigma) = (\mu, \mu)$, and we may replace σ in the last equations by 1_G, φ or $\varphi\sigma$. Since $\mu^2(1) = 4$, it follows that $\mu^2 = \rho = 1_G + \varphi + \sigma + \varphi\sigma$. Finally $\rho^2 = 4\rho$, $\mu\rho = 4\mu$ and $\rho = \rho\varphi = \rho\sigma$. All characters introduced here are integral-valued. Write $t = \dim(F\Omega_1) = 2^{n-1}$ and $q = p^t$; observe that $a = \frac{1}{2}(1 + \sqrt{q})$ is an integer. We define three small integers b_1, b_2, b_3 depending on the congruency class of p mod 8:

$$(b_1, b_2, b_3) = \begin{cases} (1, 1, 1) & \text{if } p \equiv 1 \bmod 8 \\ (-1, 2, 0) & \text{if } p \equiv 3 \bmod 8 \\ (-1, 1, -1) & \text{if } p \equiv 5 \bmod 8 \\ (1, 0, 0) & \text{if } p \equiv 7 \bmod 8. \end{cases}$$

Set $b_4 = -\frac{1}{2}(p + 1)(b_2 + b_3 - 1) \in \mathbf{Z}$. Then one checks that

$$b_2 + b_4 \equiv 0 \mod 4 \quad \text{and} \quad b_3 + b_4 \equiv 0 \mod 2.$$

Therefore

$$\psi = b_1\left[1_G + a(\varphi - 1_G) - \frac{1}{4}(b_2 + b_4)\rho + \frac{1}{2}(b_3 + b_4)\mu\right]$$

is a generalized character with values in **Z**.

We claim that $\chi = \chi_1^{\otimes G}\psi$ has the desired properties.

(i) Put $\nu = \chi[1_G + \alpha(\sigma - 1_G)]$. We have to show that $\nu\bar{\nu} = \delta$. Define

$$\psi_1 = 1_G - \frac{1}{8}(p + 1)\rho + \alpha(\sigma - 1_G) + \frac{1}{4}(p + 1)\mu,$$

$$\eta = b_1\left[1_G + a(\varphi - 1_G) - \frac{1}{4}b_2\rho + \frac{1}{2}b_3\mu\right].$$

Then $\eta(1) = b_1(1 - b_2 + b_3) = 1$, by choice of the b_i's.

An application of Lemma 1.6 together with $\frac{1}{2}(\alpha^2 - \alpha) = -\frac{1}{8}(p + 1)$ will show that $\psi_1 = [1_H + \alpha(\sigma_1 - 1_H)]^{\otimes G}$, and by easy calculations one finds $\psi_1\eta = \psi[1_G + \alpha(\sigma - 1_G)]$ and

$$\begin{aligned} \eta\bar{\eta} = \eta^2 &= 1_G + 2(a^2 - a)(1_G - \varphi) + \frac{1}{4}(b_2^2 + b_3^2 - 2b_2)\rho + b_3(1 - b_2)\mu \\ &= \frac{q+1}{2}1_G - \frac{q-1}{2}\varphi \quad \text{(by choice of } a \text{ and } b_1, b_2, b_3) \\ &= \left(\frac{p+1}{2}1_G - \frac{p-1}{2}\varphi\right)^t \quad (\text{since } p^t = q) \\ &= \delta(G : H)^t. \end{aligned}$$

To summarize,

$$\begin{aligned} \nu &= \chi[1_G + \alpha(\sigma - 1_G)] \\ &= \chi_1^{\otimes G}\psi[1_G + \alpha(\sigma - 1_G)] \\ &= \chi_1^{\otimes G}\psi_1\eta \\ &= \chi_1^{\otimes G}[1_H + \alpha(\sigma_1 - 1_H)]^{\otimes G}\eta \\ &= \nu_1^{\otimes G}\eta \quad \text{(by Lemma 1.5 (iii))}, \end{aligned}$$

so

$$\begin{aligned} \nu\bar{\nu} &= \nu_1^{\otimes G}\eta\overline{\nu_1^{\otimes G}\eta} \\ &= (\nu_1\bar{\nu}_1)^{\otimes G}\eta\bar{\eta} \quad \text{(again by Lemma 1.5 (iii) and since tensor induction commutes with complex conjugation)} \\ &= \delta_1^{\otimes G}\delta(G:H)^t \quad \text{(by induction)} \\ &= \delta \quad \text{(by Proposition 4.5)} \end{aligned}$$

(ii) Since $\nu_1(1) = \chi_1(1) \in \mathbf{Z}$ and $\nu_1(1)^2 = \delta_1(1) \equiv \nu_1(1) \bmod \mathscr{A}$, necessarily $\nu_1(1) = 1$. This implies

$$\nu(1) = \nu_1^{\otimes G}(1)\eta(1) = 1 = \delta(1).$$

If $1 \neq g \in G$, then $\delta(g) \in \mathscr{A}$, so it is enough to show that $\nu(g) \in \mathscr{A}$. If $\sigma(g) = 1$, then $\nu(g) = \chi(g) \in \mathbf{Z}$, so $\nu(g)^2 = \delta(g) \in \mathscr{A}$ implies that $\nu(g) \in \mathscr{A}$. If $\sigma(g) = -1$, then $\nu(g) = -i\sqrt{p}\chi(g) \in \mathscr{A}$, since $i\sqrt{p} \in \mathscr{A}$.

5. A Result Which Does Not Belong Here

The next result and its corollary are true for any field F with char $F = p > 0$ and any finite group G. The present proof is due to the referee.

5.1 Proposition. *Let V be an irreducible FG-module, A an abelian normal subgroup of G and $C = C_G(A)$. Assume that*

(i) $A \cap \operatorname{Ker}(G \text{ on } V) = 1$ *and*
(ii) *all irreducible constituents of $V_{|FC}$ are isomorphic.*

Then $V|_{FC}$ is irreducible.

Proof. In view of (ii), it is enough to show that $V|_{FC}$ is multiplicity-free. This in turn will follow if $(V \otimes K)|_{KC}$ is multiplicity-free for K being the algebraic closure of F. Let V_i be the irreducible constituents of the KG-module V. Then the V_i's are all different and algebraically conjugate (see [16, Theorem 9.21]). If S is an irreducible constituent of $V_i|_{KA}$, then S is a faithful KA-module since $V|_{FA}$ is faithful and homogeneous by (i), (ii) and Clifford theory. Therefore the inertia group of S in G is C and $V_i = W_i \otimes_{KC} KG$ for any irreducible $W_i \mid V_i|_{KC}$. Now

$$\dim_K\operatorname{Hom}_{KC}(W_i, (V \otimes K)|_{KC}) = \dim_K\operatorname{Hom}_{KG}(V_i, V \otimes K) = 1$$

by Frobenius reciprocity, and the assertion follows.

5.2 Corollary. *Let V be a faithful primitive FG-module, A an abelian normal subgroup of G and $C = C_G(A)$. Then $V|_{FC}$ is irreducible.*

Proof. Use the proposition: (i) is satisfied since Ker(G on V) $= 1$ and (ii) is a consequence of Clifford theory since V is primitive.

The title of this section also covers the next remark. Although it will only partly be used in the sequel, it explains where some of the complications in the next two paragraphs come from.

5.3 *Remark.* Let p, r be primes and $0 < n, m \in \mathbf{N}$ such that $p^n - 1 = r^m$. Then one of the following holds:

(i) $p = 2$, $m = 1$ and r is a Mersenne prime;
(ii) $r = 2$, $n = 1$ and p is a Fermat prime;
(iii) $r = n = 2$ and $p = m = 3$.

Proof. Well known.

6. Lemmas on Supersolvable Groups

6.1 Lemma. *Let G be a supersolvable group.*

(i) *If $H < G$ is a proper subgroup and s is the largest prime dividing $|G{:}H|$, then there exists a subgroup G_1 such that $H \leqslant G_1 \leqslant G$ and $|G_1{:}H| = s$.*

(ii) *If A is a maximal abelian normal subgroup of G, then $C_G(A) = A$.*

Proof. (i) It is well known (see [10, Satz 9.1, p. 716]) that G has a Sylow tower

$$1 = N_0 < N_1 < \dots < N_m = G$$

where $N_i \lhd G$ and $|N_i{:}N_{i-1}| = p_i^{k_i}$ for $i = 1, \dots, m$ with primes p_i such that $p_1 > p_2 > \dots > p_m$. Refining this series to a principal series gives

$$1 = K_0 < K_1 < \dots < K_n = G,$$

where the K_i are normal in G and $|K_i{:}K_{i-1}| \geqslant |K_{i+1}{:}\, K_i|$ are primes. Multiply this series with H to obtain

$$H = K_0H \leqslant K_1H \leqslant \dots \leqslant K_nH = G.$$

The first term K_jH bigger than H has the desired property.

(ii) Clearly $A \leqslant C = C_G(A) \lhd G$. Suppose $C >_{\neq} A$; then, refining the normal series $1 \leqslant A < C \leqslant G$, we find a normal subgroup N of G with $A < N \leqslant C$ and $|N{:}A|$ a prime, so in particular N/A cyclic. Since $A \leqslant Z(N)$, this implies N abelian, contradicting the maximality of A.

6.2 Lemma. *Let W be an FH-module, H a subgroup of the supersolvable group G. Let $K =$ Ker(H on W) and let s be the largest prime dividing $|G|$. If $V = W \otimes_{FH} FG$ is faithful and irreducible, then $s \mid |H{:}K|$.*

Proof. The Sylow-s-subgroup S of G is normal [10, Satz 9.1, p. 716]. If $s \nmid |G{:}K|$, then $S \leqslant K$, so

$$S \leqslant \bigcap_{g \in G} K^g = \mathrm{Ker}(G \text{ on } V) = 1,$$

a contradiction.

So $s \mid |G{:}K| = |G{:}H||H{:}K|$. If $s \nmid |H{:}K|$, then there exists a subgroup U such that $H \leqslant U$ and $|U{:}H| = s$ by Lemma 6.1 (i). Set $N = \cap_{u \in U} H^u$, so N is the kernel of the permutation action of U on $\{Hu \mid u \in U\}$. By a result of Galois (see [10, Satz 3.6, p. 163]), the structure of U/N is known; in particular $s \mid |U{:}N|$ but $s^2 \nmid |U{:}N|$.

Let $M = \cap_{u \in U} K^u$, so $M \lhd U$, in fact $M = \mathrm{Ker}(U \text{ on } W \otimes_{FH} FU)$. Since we have an embedding $N/M \hookrightarrow \Pi_{u \in U} \times H^u/K^u$ and $s \nmid |H{:}K|$, it follows that $s \nmid |N{:}M|$, so $s \mid |U{:}M|$ and $s^2 \nmid |U{:}M|$.

Therefore there is a normal subgroup T of U such that $|T{:}M| = s$ (again by [10, Satz 9.1], used for U/M); clearly $T \nleqslant H$.

Now consider $V_1 = W \otimes_{FH} FU$. Choose $0 \neq w \in W$ and $t \in T \setminus M$. Then

$$0 \neq \sum_{i=1}^{s} w \otimes t^i \in C_{V_1}(T) \quad \text{and} \quad w \otimes 1 \notin C_{V_1}(T).$$

Therefore $0 <_{\neq} C_{V_1}(T) <_{\neq} V_1$. But $C_{V_1}(T)$ is an FU-submodule of V_1, since $T \lhd U$. Therefore V_1 is not irreducible, hence $V = V_1 \otimes_{FU} FG$ is not irreducible, the desired contradiction.

6.3 LEMMA. *Let W be an FH-module, H a subgroup of the nilpotent group G, and assume $|F^*|$ is not a prime power. Let $V = W \otimes_{FH} FG$. If there exists an element $w \in W$ such that $C_H(w) = \mathrm{Ker}(H$ on $W)$, then there exists an element $v \in V$ such that $C_G(v) = \mathrm{Ker}(G$ on $V)$.*

Proof. Proceeding by induction on $|G{:}H|$, we may assume H normal and of prime index s in G, since G is nilpotent. Let S be the Sylow-s-subgroup of G. Then $G = HS$, so we may choose $1 = x_1, x_2, \ldots, x_s \in S$ such that $G = \dot{\bigcup}_i Hx_i$. Pick an element $1 \neq f \in F^*$ of order prime to s; such element exists since F^* is not an s-group. Let $V \ni v = w \otimes x_1 + \Sigma_{i>1} wf \otimes x_i$ for w given by the hypothesis. If $g \in C_G(v)$, then the s-part g_s of g also belongs to $C_G(v)$ since g_s is a power of g. Now $x_i g_s = h_i x_{j(i)}$ for suitable $h_i \in H$ since the x_i's are coset representatives. In fact, the $h_i \in H \cap S$ since x_i, $x_{j(i)}$ and g_s belong to S. Now assume $g_s \notin H$. Then $(w \otimes x_1)g_s = wh_1 \otimes x_{j(1)}$ with $j(1) \neq 1$. Since $g_s \in C_G(v)$, this implies $wh_1 = wf$, a contradiction, since $o(h_1)$ is a power of s, whereas $1 \neq o(f)$ is prime to s.

Therefore $g_s \in H$; but the s'-part $g_{s'}$ of g also belongs to H since $|G{:}H| = s$ and $H \lhd G$. Therefore $g \in H$, so

$$\begin{aligned} w \otimes x_1 + \sum_{i>1} wf \otimes x_i &= v \\ &= vg \\ &= wg \otimes x_1 + \sum_{i>1} wfx_i g x_i^{-1} \otimes x_i, \end{aligned}$$

which implies $x_i g x_i^{-1} \in C_H(w)$ for all i. Hence

$$g \in \bigcap_i C_H(w)^{x_i} = \bigcap_i \operatorname{Ker}(H \text{ on } W)^{x_i} = \operatorname{Ker}(G \text{ on } V).$$

We have shown that $C_G(v) \leq \operatorname{Ker}(G$ on $V)$. The converse is trivial.

6.4 *Remark/Notation.* Let E be a finite field extension of F and $\Gamma = \operatorname{Gal}(E/F)$ the Galois group. There is a natural action of Γ on E^*, and the semidirect product ΓE^* acts on E *by* $e(\gamma e_1) = e^\gamma e_1(\gamma \in \Gamma$, e, $e_1 \in E$ and $e_1 \neq 0)$ This action is F-linear, making E into an $F(\Gamma E^*)$-module.

6.5 Proposition [10, 3.11, p. 166]. *Let W be a primitive FH-module, H a supersolvable group. Then there exists a field extension E of F and a homomorphism $\sigma : H \to \Gamma E^*$ such that $W \simeq E$ as FH-modules, where of course the action of H on E is defined via σ.*

Proof. Passing from H to $H/\operatorname{Ker}(H$ on $W)$, we may assume that W is faithful. Let A be a maximal normal subgroup of H. Then $A = C_G(A)$ by Lemma 6.1 (ii), so $W|_{FA}$ is irreducible by Corollary 5.2. Therefore there exists an FA-linear epimorphism $\varepsilon : FA \to W$. Since FA is commutative, ker ε is a maximal ideal and $E = FA/\operatorname{Ker} \varepsilon$ is a field extension of F. We have an FA-isomorphism $\varphi : E \to W$ induced by ε, which we use to impose an FH-structure on E, i.e. for $e \in E$, $h \in H$ we define $eh = e\varphi h \varphi^{-1}$. This of course makes φ an FH-isomorphism. Therefore it is enough to define a homomorphism $\sigma : H \to \Gamma E^*$ such that $eh = e\sigma(h)$ for all $e \in E$ and $h \in H$. We first define a homomorphism $\tau : H \to \Gamma$: The conjugation action of H on A extends to an action as F-algebra automorphisms of H on FA. Because W is an FH-module, $\mathcal{M} = \operatorname{ann}_{FA}(W)$ is invariant, so we have the induced action of H on E. Since F is fixed, H acts as a group of F-automorphisms on E. This gives τ as desired. Observe that writing $E \ni e = x + \mathcal{M}$ for some $x \in FA$, we have $e^{\tau(h)} = x^h + \mathcal{M}$. Now it is easy to define σ : if $h \in H$, then $1_E h \in E^*$, so $\sigma(h) = (\tau(h), 1_E h) \in \Gamma E^*$. We show that $eh = e\sigma(h)$ for all $e \in E$, $h \in H$.
Any $e = x + \mathcal{M}$ for some $x \in FA$, and for each $y \in FA$, we have $ey = xy + \mathcal{M} = e(y + \mathcal{M})$ since ε is FA-linear, so in particular $e = 1_E x$. Therefore

$$\begin{aligned} eh &= (1_E x)h \\ &= (1_E h)x^h \quad (\text{since } E \text{ is an } FH\text{-module}) \\ &= (1_E h)(x^h + \mathcal{M}) \\ &= (1_E h)e^{\tau(h)} \\ &= e\sigma(h). \end{aligned}$$

Since E is faithful as an ΓE^*-module, this also implies that σ is an homomorphism (in fact a monomorphism).

6.6 COROLLARY. *Let W be a primitive FH-module, H a supersolvable p'-group. Let K =* Ker(H on W)*. Then one of the following holds:*

(I) $\dim_{F_0}(W) \geq 2$ *and there exists a $w \in W$ such that $\delta(C_H(w), W)$ contains a square.*
(II) $\dim_{F_0}(W) = 1$ *(and H/K acts by multiplication on $W \simeq F_0$).*
(III) $\dim_{F_0}(W) = 2$ *and $H/K \simeq \Gamma A$ for a subgroup A of E^*, acting on $W \simeq E = GF(p^2)$ as described in Remark 6.4. Furthermore* $(p + 1) \mid |A|$.

Proof. By Proposition 6.5, we may assume $\overline{H} = H/K \leq \Gamma E^*$ for a suitable field extension E of F and $\Gamma = \mathrm{Gal}(E/F)$. If $0 \neq e \in E$, then $C = C_{\overline{H}}(e) \leq C_{\Gamma E^*}(e) =_{\Gamma E^*} C_{\Gamma E^*}(1) = \Gamma$. The existence of a normal basis for E (see [13]) implies $E \simeq F\Gamma$ as $F\Gamma$-module, so $E \simeq (FC)^t$ as FC-module where $t = |C|^{-1}|\Gamma|$; therefore $\delta(C, E) = \delta(C, FC)^t$ which contains a square by Lemma 4.8 unless $t = 1$, $F = F_0$ and $|C| = 2$.
So if $\dim_{F_0} W \geq 2$ but (I) does not hold, then $\overline{H}$ is a subgroup of ΓE^* for $E = GF(p^2)$, satisfying $|C_{\overline{H}}(e)| = 2$ for all $0 \neq e \in E$; so in particular $\Gamma = C_{\Gamma E^*}(1) = C_{\overline{H}}(1) \leq \overline{H}$, which implies that $\overline{H} = \Gamma(\overline{H} \cap E^*)$ is indeed a semidirect product. To show (III), it remains to prove the assertion on the order of $A = \overline{H} \cap E^*$.
Let $\varphi : E^* \to E^*$ by defined by $\varphi(e) = e^{1-p}$. Clearly φ is a group endomorphism and Ker $\varphi = F^*$, so $|\mathrm{Im}\ \varphi| = p + 1$. But Im $\varphi \leq A$: Take $e \in E^*$, then $|C_{\overline{H}}(e)| = 2$, so there exists $a \in A$ with $(\gamma, a) \in C_{\overline{H}}(e)$, where $1 \neq \gamma \in \Gamma$. This means $e = e(\gamma, a) = e^p a$, i.e. $\varphi(e) = e^{1-p} = a \in A$.
If $\dim_{F_0} W = 1$, then clearly (II) holds.

7. Results

7.1 *Remark.* We are now in a position to study irreducible modules over supersolvable p'-groups, taking Corollary 6.6—which covers the primitive case—as a starting point. The proofs are not difficult, but there are far too many different cases to consider to call the approach satisfactory, let alone esthetic. The gentle and patient reader is likely to feel growing exasperation before he or she is halfway through that lengthy struggle, a feeling warmly shared by the author. It will turn out that the trouble is caused by the "small" cases and the small primes dividing the group order, in particular by 2-groups. Some indication why these cases are difficult is given by the exceptions which appear in Lemma 4.7, Lemma 4.8 and Corollary 6.6, and also by the number theoretic Remark 5.3. But it seems that the difficulties are not only caused by the technicalities of the proof. Examples show that the inequality we are trying to establish actually becomes an equality (or is at least not far from it) for some of these small cases.

7.2 Lemma. *Let W be an FH-module, H a subgroup of the supersolvable group G such that $|G{:}H|$ is a power of* 2. *Assume there is a $w \in W$ such that D/K is a* 2-*group and $W|_{FD}$ is a permutation module, where $D = C_H(w)$ and $K = \operatorname{Ker}(H \text{ on } W)$. Then there is $v \in V = W^G$ such that $C/\operatorname{Ker}(G \text{ on } V)$ is a* 2-*group and $V|_{FC}$ is a permutation module for $C = C_G(v)$.*

Proof. There is no loss in assuming $\operatorname{Ker}(G \text{ on } V) = 1$. Let $\{g_i \mid i \in I\}$ be a set of coset representatives of H in G and put $v = \Sigma_i w \otimes g_i$. Then $H^{g_i} \cap C \leqslant D^{g_i}$ as is easily seen. By Mackey decomposition,

$$V|_{FC} = \sum_{i\in J} \oplus\, W^{g_i} \otimes_{F(H^{g_i}\cap C)} FC \quad \text{for some } J \subseteq I.$$

By assumption, $W|_{FD} = \Sigma_r \oplus F \otimes_{FU_r} FD$ for suitable subgroups $U_r \leqslant D$ acting trivially on F. Together, this implies $V|_{FC} = \Sigma_s F \otimes_{FX_s} FC$, the $X_s \leqslant C$ acting trivially on F, so $V|_{FC}$ is a permutation group.
It remains to show that C is a 2-group. Since, by assumption, H contains the normal $2'$-Hall subgroup of G (see [10, p. 716 Satz 9.1]), the same is true for $N = \bigcap_{g\in G} H^g$. Therefore G/N and in particular $C/C \cap N$ are 2-groups. If $n \in C \cap N$, then

$$\sum_i w \otimes g_i = v = vn = \sum_i w g_i n g_i^{-1} \otimes g_i,$$

so $n \in \bigcap_i D^{g_i}$. Hence there is a homomorphism

$$\alpha : C \cap N \to \prod_i \times\, D^{g_i}/K^{g_i}.$$

Since $\operatorname{Ker} \alpha = \bigcap_i K^{g_i} = \operatorname{Ker}(G \text{ on } V) = 1$, this implies that $C \cap N$—hence C—is a 2-group.

7.3 Proposition. *Let V be a faithful irreducible FG-module, G a supersolvable p'-group. Then (at least) one of the following holds:*

(i) *There exists $v \in V$ such that $\delta(C_G(v), V)$ contains a square.*
(ii) *There exists $v \in V$ such that $C_G(v)$ is abelian.*
(iii) *There exists $v \in V$ such that $C = C_G(v)$ is a* 2-*group and $V|_{FC}$ is a permutation module.*

Proof. There exists a subgroup H of G and a primitive FH-module W such that $V = W \otimes_{FH} FG$. We treat the cases (I)–(III) given by Corollary 6.6 separately and keep the notation introduced there.

(I) By Proposition 4.6, (i) holds.
(II) If $p = 2$, then $H/K = 1$, so $G = 1$ by Lemma 6.2 and (i) holds.

Assume next p odd but not a Fermat prime; so $|F^*|$ is not a prime power. As usual, denote by G' the commutator subgroup of G. Since G is supersolvable, G' is nilpotent [10, p. 716 Satz 9.1]. By Mackey decomposition,

$$V|_{G'} = \sum_i \oplus\, W^{g_i} \otimes_{F(H^{g_i}\cup G')} FG', \quad \text{where } G = \dot{\bigcup} Hg_iG'.$$

Since W^{g_i} is a one-dimensional $F(H^{g_i} \cap G')$-module, there exists an element $w_i \in W^{g_i}$ such that $C_{H^{g_i} \cap G'}(w_i) = \operatorname{Ker}(H^{g_i} \cap G' \text{ on } W^{g_i})$—in fact, every element $\neq 0$ will do. By Lemma 6.3 then, there exists an element

$$v_i \in V_i = W^{g_i} \otimes_{F(H^{g_i} \cap G')} FG'$$

such that $C_{G'}(v_i) = \operatorname{Ker}(G' \text{ on } V_i)$. Setting $v = \Sigma v_i$, it follows that

$$\begin{aligned} C_{G'}(v) &= \bigcap_i C_{G'}(v_i) \\ &= \bigcap_i \operatorname{Ker}(G' \text{ on } V_i) \quad (\text{since } V = \sum_i \oplus V_i) \\ &= \operatorname{Ker}(G' \text{ on } V) \\ &= 1 \quad (\text{since } V \text{ is faithful}) \end{aligned}$$

Therefore $C_G(v) \cap G' = 1$, i.e., there exists an embedding $C_G(v) \hookrightarrow G/G'$, which is an abelian group. Hence (ii) holds. Now assume p a Fermat prime. Then $|F^*|$ is a power of 2, so H/K is a 2-group; by Lemma 6.2, G is a 2-group. Therefore the conditions of Lemma 7.2 are satisfied (with $D = K$) and (iii) follows.

(III) Identify W with E and H/K with ΓA. If $|G:H|$ is a power of 2, then (iii) follows again from Lemma 7.2, since $C_H(1_E)/K = \Gamma$ is a 2-group and E is a permutation module over $F\Gamma$ by the normal basis theorem.

So assume that $|G:H|$ is not a power of 2. Since $2 = |\Gamma| \mid |G|$, p must be an odd prime. If $p = 3$, then $|E^*| = 8$, so $|H/K| \mid 16$, and G is a 2-group by Lemma 6.2. But this contradicts the assumption on $|G:H|$. Hence $p > 3$. Let G' be as before and put $U = H \cap G'$; so UK/K is a subgroup of ΓA. We distinguish two cases:

(α) $UK/K \leqslant A$

(β) $UK/K \not\leqslant A$.

(α) This means that U acts on E by multiplication, so E is an EU-module. Since $p > 3$, it follows from Remark 5.3 that $|E^*|$ is not a prime power, so we use the same argument as in case (II) to show that (ii) holds. In doing so, observe that

$$E \otimes_{FU} FG' \simeq E \otimes_{EU} EG'|_{FG'}$$

and similarly for the conjugate modules in the Mackey decomposition of $V|_{FG'}$.

(β) It is easy to check that $(\Gamma A)' = \operatorname{Im} \varphi$, where $\varphi : A \to A$ is defined by $\varphi(a) = a^{1-p}$. By (III), $|A| = d(p + 1)$ for some $d \mid p - 1$. Hence $|\operatorname{Ker} \varphi| = \text{g.c.d.}\ (|A|, p - 1) \mid 2d$, so there is a subgroup $B \leqslant (\Gamma A)'$ of order $\frac{1}{2}(p + 1)$. Now $H' \leqslant H \cap G' = U$, so $B \leqslant (\Gamma A)' = (H/K)' = H'K/K \leqslant UK/K \simeq U/U \cap K$ which is nilpotent, since U is nilpotent.
Let $b \in B$ by an element of prime order r. By assumption (β), there is an element $\gamma a \in UK/K$, where $1 \neq \gamma \in \Gamma$. Conjugation with γa is an inner automorphism of order 2 in UK/K, and $b^{\gamma a} = b^p$. If $b^p = b$, then $r \mid p -$

1. Since r also divides $|B| = \frac{1}{2}(p + 1)$, this forces $r = 2$. On the other hand, if $b^p \neq b$, then the nilpotency of UK/K implies $r = 2$, since γa acts trivially on all Sylow-subgroups of UK/K except (possibly) the Sylow-2-subgroup.

Thus we have shown that B is a 2-group. This of course implies that $p = 2|B| - 1$ is a Mersenne prime, and that E^*/F^* is a 2-group.

Now let s be the largest prime dividing $|G{:}H|$. By assumption, $s > 2$, and by Lemma 6.1 (i), there is a subgroup G_1 of G such that $|G_1{:}H| = s$. Put $V_1 = E \otimes_{FH} FG_1$. We will show that $\delta(C_{G_1}(v_1), V_1)$ contains a square for a suitable element $v_1 \in V_1$. Once this is done, (i) will follow from Proposition 4.6. Therefore, there is no loss in assuming $G = G_1$ and $V = V_1$, so we drop the subscript.

Since Γ acts trivially on F^* and E^*/F^* is a 2-group, it is clear that H/K is nilpotent. Put $N = \bigcap_{g\in G} H^g$; then $N \lhd G$ and there is a homomorphism $\alpha : N \to \Pi_{g\in G} \times H^g/K^g$. Since

$$\operatorname{Ker}\alpha = \bigcap_{g\in G} K^g = \operatorname{Ker}(G \text{ on } V) = 1,$$

this implies that N is nilpotent, so the Sylow-2-subgroup M of N is characteristic in N, hence $M \lhd G$. The $2'$-Hall group G_2, is normal in G since G is supersolvable [10, Satz 9.1] and $M \cap G_2, = 1$, so $m \in M$ commutes with any element $g \in G$ of odd order.

Let S be a Sylow-s-subgroup of G and choose $x \in S\setminus H$. Then

$$\{x^i \mid i = 0, \ldots, s - 1\}$$

is a set of H-coset representatives in G, so any element in V can be written as $\Sigma_i e_i \otimes x^i$ for suitable $e_i \in E$. Let $\{1_E, e\}$ be an F-basis of E and let $v = 1_E \otimes 1 + \Sigma_{i=1}^{s-1} e \otimes x^i$ and $C = C_G(v)$.

We claim that $C \cap N = 1$. Let us first show that it is a 2-group: if $n \in C \cap N$, then

$$\begin{aligned} 1_E \otimes 1 + \sum_{i\neq 0} e \otimes x^i &= v \\ &= vn \\ &= 1_E n \otimes 1 + \sum_{i\neq 0} ex^i n x^{-i} \otimes x^i, \end{aligned}$$

so $1_E n = 1_E$ and $ex^i n x^{-i} = e$ for $i \neq 0$. Since $|C_H(1_E)/K| = |C_H(e)/K| = 2$, this forces $x^i n^2 x^{-i} \in K$ for all i. Therefore

$$\left(\sum_i e_i \otimes x^i\right) n^2 = \sum_i e_i x^i n^2 x^{-i} \otimes x^i = \sum_i e_i \otimes x^i$$

for all $e_i \in E$. This means $n^2 \in \operatorname{Ker}(G \text{ on } V) = 1$ and shows $C \cap N \leqslant M$.

But then any $n \in C \cap N$ commutes with x (which is of odd order), so $1_E n = 1_E$ and $e = ex^i n x^{-i} = en$ implies $n \in K$, since $\{1_E, e\}$ is an F-basis of E. The argument used above then shows $n = 1$, thereby proving the claim.

Now it is easy to see that $\delta(C, V)$ contains a square: by Proposition 4.5,

$$\delta = \delta(G, V) = \delta(H, E)^{\otimes G}\, \delta(G{:}H)^2 \geqslant \delta(G{:}H)^2,$$

since $\delta(H, E)^{\otimes G} \geqslant 1_G$. So certainly $\delta|_C \geqslant \delta(G{:}H)^2|_C$ and it is enough to check that $\delta(c) \equiv \delta(G{:}H)(c) \bmod p$ for all $c \in C$. For $c = 1$, both characters have value 1. In general, $\delta(G{:}H)(c) \mid \delta(c)$, and if $c \neq 1$, then $c \notin N$, the kernel of the permutation action of G on $[G{:}H]$, so $\delta(G{:}H)(c) \equiv 0 \bmod p$.

This finishes the proof.

7.4 Theorem. *Let G be a p-solvable group such that a p'-Hall-group of G is supersolvable. If B is a p-block of G with defect d, then $k(B) \leqslant p^d$.*

Proof. We use Fong-Nagao reduction (see [8] and [14]) as presented by Gow in [9, Theorem 1.3]. Therefore, it is enough to consider the situation described in Proposition 7.3. In case (ii) of 7.3, we are done by Theorem 3.7. In case (iii), we know from Proposition 4.9 that $\delta|_C$ contains an $\mathscr{L}$-square, where $\mathscr{L} = \mathbf{Z} \oplus \mathbf{Z}\,\alpha$ with $\alpha = \frac{1}{2}(1 + i\sqrt{p})$ and p an odd prime. If $0 \neq x = a + b\alpha \in \mathscr{L}$, then

$$|x|^2 = a^2 + b^2 + ab + \frac{1}{4}(p - 3) \geqslant a^2 + b^2 + ab \geqslant 1.$$

Therefore, Proposition 4.3 applies in case (iii) and clearly also in case (i); it follows that $(\gamma\delta, \gamma)_C \geqslant k(C)$ for any generalized character γ of C with $\gamma(1) \not\equiv 0 \bmod p$. So the condition of Theorem 2.2 is satisfied and the assertion follows.

References

1. T. R. Berger, *Hall-Higman type theorems V*, Pacific J. Math., vol. 73 (1977), pp. 1–62.
2. R. Brauer, *On groups whose order contains a prime number to the first power I, II*, Amer. J. Math., vol. 64 (1942), pp. 401–420, 421–440.
3. ———, *Number theoretical investigations on groups of finite order*, Proceedings of the International Symposium on Algebraic Number Theory, Tokyo, 1956, pp. 55–62.
4. R. Brauer and W. Feit, *On the number of the irreducible characters of finite groups in a given block*, Proc. Nat. Acad. Sci USA, vol. 45 (1959), pp. 361–365.
5. C. W. Curtis and I. Reiner, *Representation theory of finite groups and associative algebras*, Wiley, New York, 1962.
6. E. C. Dade, *Blocks with cyclic defect groups*, Ann. of Math. (2), vol. 84 (1966), pp. 20–48.
7. ———, *Compounding Clifford's theory*, Ann. of Math. (2), vol. 91 (1970), pp. 236–290.
8. P. Fong, *On the characters of p-solvable groups*, Trans. Amer. Math. Soc., vol. 98 (1961), pp. 263–284.
9. R. Gow, *On the number of characters in a p-block of a p-solvable group*, J. Algebra, vol. 65 (1980), pp. 421–426.
10. B. Huppert, *Endliche Gruppen I*. Springer-Verlag, Berlin, 1967.

11. N. Itô, *On the degrees of irreducible representations of a finite group,* Nagoya Math. J., vol. 3 (1951), pp. 5–6.

12. P. Landrock, *On the number of irreducible characters in a 2-block,* J. Algebra, vol. 68 (1981), pp. 426–442.

13. S. Lang, *Algebra,* Addison Wesley, Reading, Mass., 1965.

14. H. Nagao, *On a conjecture of Brauer for p-solvable groups,* J. Math. Osaka City University, vol. 13 (1962), pp. 35–38.

15. J. P. Serre, *Représentations linéaires des groupes finis,* Hermann, Paris, 1967.

16. I. M. Isaacs, *Character theory of finite groups,* Academic Press, New York, 1976.

Universität Essen
Essen, West Germany