ON A CONJECTURE OF ALPERIN AND MCKAY

G. I. LEHRER

For any finite group \( G \) and rational prime \( p \), denote by \( m_p(G) \) the number of irreducible complex characters (henceforth referred to as "characters") whose degree is prime to \( p \). Such characters will be referred to as \( p' \)-characters. Alperin has conjectured (see [1] for details and background) that for any \( G \):

\[
(1) \quad m_p(G) = m_p(N_G(S)), \text{ where } N_G(S) \text{ is the normalizer of a } p\text{-Sylow subgroup } S \text{ of } G.
\]

Alperin (loc. cit.) proves (1) when \( G = \text{GL} \ (n, q) \) and \( q = p^e \). Since then, (1) has been proved for \( G = \text{GL} \ (n, q) \) or \( G = \Sigma_n \) (the symmetric group on \( n \) symbols) and \( p \) any prime by Olsson [7]. The purpose of this note is twofold: firstly, we show that the results of [2] and [3] imply (1) for almost all finite Lie groups of "conformal type" over \( F_q \) (e.g. the general symplectic group rather than \( \text{Sp} \ (2n, q) \)) and \( q = p^e \). Secondly, we prove (1) for \( G = \text{SL} \ (n, q) \) and \( q = p^e \), with the aid of the results of [5] and [6]. The former result follows very easily from those of [2] and [3] by Alperin's method. In contrast, to prove the result for \( \text{SL} \ (n, q) \) one needs much more detailed information about the \( p' \)-characters of \( \text{GL} \ (n, q) \) and their restriction to \( \text{SL} \ (n, q) \). The way in which distinct arithmetical paths lead to the same result here lends support to the conjecture.

For an abelian group \( A \), \( (A)^\circ \) will denote its complex character group.

1. The case of an algebraic group over a finite field.

Our notation is as follows: \( G \) is a connected, reductive group defined over \( F_q \); it is assumed that \( G \) has connected centre \( Z \), and that the characteristic \( p \) is good for \( G \) (see [3]; only a few small characteristics are excluded in some cases). \( G \) will denote the group \( F_q \)-rational points of \( G \), and \( l \) the \( F_q \)-rank of \( G/Z \).

Let \( B, T \) and \( U \) be as in § 5 of [3]. Then \( U \) is a Sylow \( p \)-subgroup of \( G \), \( B = N_G(U) \) and \( B \) is the semidirect product \( B = T \cdot U \).

We shall prove:

Received October 19, 1977.
THEOREM 1. With notation as above,

\[ m_p(G) = m_p(B) = |Z|q^l \]

where \( Z \) is the group of rational points of the centre \( Z \) of \( G \).

PROOF. Theorem 3 of [2] asserts, inter alia, that \( m_p(G) = |Z|q^l \). Hence one needs only to show that \( m_p(B) = |Z|q^l \). For this, following Alperin, one notes the following facts:

(3) \( m_p(B) \) is the number of irreducible complex characters of \( B/U' \).

The proof is the same as Alperin's for the case \( GL(n,q) \).

Now there is a canonical isomorphism \( \eta: U/U' \rightarrow X_1 \times \ldots \times X_S \) where \( X_i = \text{GF}(q^n)^+ \) and \( n_1 + \ldots + n_s = l \) (see [3, p. 258]). Thus for any linear (i.e. 1-dimensional) character \( \lambda \) of \( U \), one defines its support by

\[ \text{supp} (\lambda) = \{ i \mid \lambda|_{X_i} \neq 1 \} . \]

As in [1], one then has

(4) Two linear characters of \( U \) are conjugate under the action of \( B \) (or, equivalently, \( T \)) if and only if they have the same support.

This is clear from the arguments used to establish Theorem B' in [3]. The proof of the theorem is now completed by showing

(5) The number of irreducible complex characters of \( B/U' \) is \( |Z| \cdot q^l \).

We have a canonical isomorphism: \( B/U' \rightarrow T \cdot U/U' \). Since \( T \) is abelian and has \( p' \)-order, all the irreducible characters of \( B/U' \) are constructed as follows: one takes an irreducible (linear) character \( \mu \) of \( U/U' \), extends to its centralizer \( T(\mu).U/U' \) and induces to \( B/U' \). The set of \( |T(\mu)| \) characters \( \{(\varphi \mu)^{B/U'} \mid \varphi \in (T(\mu))^\wedge \} \) depends only on the \( T \)-orbit \( \Omega(\mu) \). Hence the number of irreducible characters of \( B/U' \) is

(6)

\[ m(B/U') = \sum_{\Omega} |T(\Omega)| \]

the sum being over the \( T \)-orbits \( \Omega \) of characters of \( U/U' \), and \( T(\Omega) \) denoting the stabilizer of any element of \( \Omega \). But by (4), the orbits corresponds to subsets \( I \subset \{1, \ldots, l\} \). Moreover by the arguments in § 5 of [2], it is easy to see that

\[ |T(I)| = |T|/\prod_{i \in I} (q^n - 1) \]

Thus

\[ |T(I)| = |Z| \cdot \prod_{i \in I} (q^n - 1) . \]
\[ m(B/U) = m_p(B) = \sum_{l=1}^{l-1} |Z| \prod_{i \neq l} (q^n - 1) = |Z| \prod_{i} (q^n - 1 + 1) = |Z|q^\Sigma n_i = |Z|q^l. \]

This completes the proof of Theorem 1.

2. The case \( G = \text{SL}(n, q) \).

For this section, notation will be as follows: \( G = \text{GL}(n, q) \), \( B \) is the group of upper triangular matrices in \( G \), \( T \) is the group of diagonal matrices in \( G \), \( U \) \((< B)\) is the \((p\text{-group})\) of upper unitriangular matrices. For any subgroup \( H \leq G \), \( H_1 \) will denote \( H \cap \text{SL}(n, q) \). Thus \( G_1 = \text{SL}(n, q) \), \( U_1 = U \) and \( B_1 = N_{G_1}(U_1) \). We shall prove, (for \( p = \text{characteristic of } \mathbb{F}_q \)):

**Theorem 2.** \( m_p(G_1) = m_p(B_1) \).

To prove this, it will be necessary to go into more detail concerning the \( p' \)-characters of \( G \) and \( B \). In fact we shall in effect set up an explicit bijection between the two sets, something which was not necessary for the proof of theorem 1. We first note the following elementary facts:

**Lemma 3.** Let \( H, K \) be finite groups, \( K \leq H \) with \( H/K \) cyclic, of \( p' \)-order. Then

(i) For any irreducible character \( \chi \) of \( H \), \( \chi|_K = \mu_1 + \ldots + \mu_e \) where the sum is precisely over one \( H \)-orbit \( \{\mu_1, \ldots, \mu_e\} \) of characters of \( K \).

(ii) If \( \chi_1 \) and \( \chi_2 \) are characters of \( H \) then their restrictions to \( K \) either coincide or are disjoint, and \( \chi_1|_K = \chi_2|_K \Leftrightarrow \chi_2 = \theta \chi_1 \) with \( \theta \in (H/K)^{\ast} \).

(iii) The \( p' \)-characters of \( K \) are precisely the irreducible constituents of the restrictions of the \( p' \)-characters of \( H \).

(iv) For any character \( \chi \) of \( H \), let \( f(\chi) \) be the number of characters \( \chi' \) of \( H \) such that \( \chi' = \theta \chi \) for some \( \theta \in (H/K)^{\ast} \), and let \( e(\chi) \) be the number of irreducible components of \( \chi|_K \). Then \( e(\chi) \cdot f(\chi) = |H/K| \).

Putting these facts together, we obtain

\[ m_p(K) = \sum \frac{e(\chi)}{f(\chi)} = \sum \frac{e(\chi)^2}{|H/K|} = \frac{|K|}{|H|} \sum e(\chi)^2. \]
where the sum is over the $p'$-characters $\chi$ of $H$. Notice also that in the action of $(H/K)$ on the characters of $H$, the stabilizer $S(\chi)$ of $\chi$ has order $|H/K|/f(\chi) = e(\chi)$. Hence (7) can be rewritten

$$m_p(K) = \frac{|K|}{|H|} \sum |S(\chi)|^2.$$  

Here $S(\chi)$ is the stabilizer in $(H/K)$ of $\chi$, and the sum is over the $p'$-characters of $H$.

We now set up a bijection between the $p'$-characters of $G$ and $B$, such that $|S(\chi)|$ is the same for corresponding characters. This will prove Theorem.

$p'$ characters of $G$. The $p'$-characters of GL $(n,q)$ are precisely the characters $\langle \psi_1 \rangle \circ \ldots \circ \langle \psi_k \rangle$, in the notation of [5]. Here $\langle \psi_i \rangle$ is an $n_i$-simplex, $\{r_i\}$ is the partition of $r_i$ consisting of one part, and $\sum_{i=1}^k n_i r_i = n$. Now $\langle \psi_i \rangle$ corresponds ([6]) to an irreducible monic polynomial $f_i$ of degree $n_i$ over $F_q (\{\psi_i, \psi_i', \ldots\})$ is regarded as the set of roots of $f_i$. Thus the character $\chi$ above may be written

$$\chi = f_1^{\alpha_1} f_2^{\alpha_2} \ldots f_k^{\alpha_k}$$

$$= f = t^n + a_1 t^{n-1} + \ldots + a_n$$

$$= [a_1, \ldots, a_n] \quad (a_n \neq 0).$$

This identification of the $p'$-characters with polynomials of degree $n$ immediately gives $m_p(G) = q^n - 1$, as this is the number of monic polynomials of degree $n$ over $F_q$, with non-zero constant term.

In view of (8), we describe how $(G/G_1)$ acts on $\chi$ above: we have $(G/G_1) \cong F_q^*$, and by Corollary 5.23 in [5], the latter acts on $\chi$ by multiplicatively translating the roots of $f$. If we denote $\chi$ above (cf. (9)) by

$$\chi = [a_1, a_2, \ldots, a_n]$$

(recall $a_i \in F_q, i = 1, \ldots, n-1, a_n \in F_q^*$), then for $a \in (G/G_1) \cong F_q^*$ it is easily seen that

$$\chi^a = [aa_1, a^2 a_2, a^3 a_3, \ldots, a^n a_n].$$

For the same $\chi$, define

$$\text{supp} (\chi) = I = \{ i \mid a_i = 0 \} \subset \{1, \ldots, n-1\}.$$ 

Then for the stabilizer $S(\chi)$ of $\chi$ in $F_q^*$, we have (from (10)).

$$|S(\chi)| = |\{ a \in F_q^* \mid a^i = 1 \text{ for } i \notin I \}|.$$
$p'$-characters of $B$. From the discussion preceding formula (6) it is apparent that for each $p'$-character $\chi$ of $B$ there is a subset $I \subset \{1, \ldots, n-1\}$ such that $\chi$ corresponds to a character $\varphi$ of $T(I)$. Moreover $I$ and $\varphi$ are uniquely determined by $\chi$. We write

$$\chi = (I, \varphi).$$

(12)

To identify $T(I)$, consider the isomorphism $\alpha: T \to F_q^* \times \cdots \times F_q^*$ (n times) given by

$$\alpha(\text{diag} \ (a_1, \ldots, a_n)) = (a_1a_2^{-1}, \ldots, a_{n-1}a_n^{-1}, a_n).$$

(13)

Identifying $T$ with $F_q^* \times \cdots \times F_q^*$ using $\alpha$, we have

$$T(I) = \{(t_1, \ldots, t_n) \mid t_i \in F_q^*, \ t_i = 1 \text{ for } i \in I\}.$$  

(14)

In this way we identify $\chi$ with a symbol

$$\chi = [\varphi_j]_{j \notin I}, \quad \varphi_j \in (F_q^*)^\times, \ j \in \{1, 2, \ldots, n\}.$$  

(15)

The character $\varphi$ of $\chi = (I, \varphi)$ is defined by

$$\varphi(t_1, \ldots, t_n) = \prod_{i \notin I} \varphi_i(t_i).$$  

(16)

We now describe the action of $(B/B_1)^\times$ on $\chi$. Using the notation of the discussion preceding (6) above, we have, for $\theta \in (B/B_1)^\times$

$$\theta \cdot (\varphi \mu)^{B/U'} = ((\theta \varphi) \cdot \mu)^{B/U'}.$$  

(17)

where $\theta \varphi$ denotes the product of $\varphi$ and the restriction of $\theta$ to $T(I)$, and $\mu$ is the linear character of $U$ in (6). Since $B/B_1$ may be canonically identified with $T/T_1$ (and hence similarly for their character groups), we therefore have in the notation of (12), for $\theta \in (T/T_1)^\times = (B/B_1)^\times$

$$\chi^\theta = \theta \cdot (I, \varphi) = (I, \theta \varphi).$$  

(18)

Any character $\theta$ of $T$ which is trivial on $T_1$ is of the form

$$\theta(\text{diag} \ (a_1, \ldots, a_n)) = \psi(a_1a_2 \ldots a_n), \quad \text{for some } \psi \in (F_q^*)^\times$$

$$= \psi(a_1a_2^{-1})\psi(a_2a_3^{-1})^2 \ldots \psi(a_{n-1}a_n^{-1})^{n-1}\psi(a_n)^n,$$

that is,

$$\theta(t_1, \ldots, t_n) = \psi(t_1)\psi^2(t_2) \cdots \psi^n(t_n)$$

(19)

(here $\psi \in (F_q^*)^\times$).

Thus from (15) and (18) we have, for $\theta \in (T/T_1)^\times$

$$\chi^\theta = [\psi^i \varphi_j]_{j \notin I} \quad (\psi \in (F_q^*)^\times).$$  

(20)
It follows that the order of the stabilizer $S(\chi)$ of $\chi$ in $(B/B')^\wedge (=(T/T_1)^\wedge)$ has order given by

\begin{equation}
|S(\chi)| = |\{\psi \in (\mathbb{F}_q^\ast)^\wedge \mid \psi^j = 1 \text{ for } j \notin I\}|.
\end{equation}

Thus in both (11) and (21), $|S(\chi)|$ depends only on $I \subset \{1, \ldots, n-1\}$, and has the same value in each case. Since the number of $\chi$ corresponding to a given $I$ is the same in both cases ($=(q-1)^{n-|I|}$), Theorem 2 now follows from (8) applied to the pairs $G, G_1$ and $B, B_1$.

\textbf{REFERENCES}