ON CERTAIN FINITE LINEAR GROUPS
OF PRIME DEGREE

Thesis by

David Alan Sibley

In Partial Fulfillment of the Requirements

For the Degree of

Doctor of Philosophy

California Institute of Technology

Pasadena, California

1972

(Submitted April 3, 1972)

ACKNOWLEDGMENTS

I am particularly indebted to my adviser, D.B. Wales, for his advice and encouragement. I also wish to thank Walter Feit for his helpful discussion with me.

I am grateful to the National Science Foundation and the Ford Foundation for their support, and to the California Institute of Technology for providing me with several teaching assistantships and research assistantships.

ABSTRACT

In studying finite linear groups of fixed degree over the complex field, it is convenient to restrict attention to irreducible, unimodular, and quasiprimitive groups. If one assumes the degree to be an odd prime p, there is a natural division into cases, according to the order of a Sylow p-group of such a group. When the order is p^4 or larger, all such groups are known (by W. Feit and J. Lindsey, independently).

THEOREM 1. Suppose G is a finite group with a faithful, irreducible, unimodular, and quasiprimitive complex representation of prime degree $p \geq 5$. If a Sylow p-group P of G has order p^3, then P is normal in G.

As is well known, Theorem 1 is false for p = 2 or 3. Combining Theorem 1 with known results, we have immediately the following conjecture of Feit.

THEOREM 2. Suppose G is a finite group with a faithful, irreducible, and unimodular complex representation of prime degree $p \geq 5$. Then p^2 does not divide the order of $G/O_p(G)$.

The following result, which is of independent interest, is used in the proof of Theorem 1.

THEOREM 3. Suppose G is a finite group with a Sylow p-group P of order larger than 3, which satisfies

$$C_G(x) = P, \quad \text{for all } x \neq 1 \text{ in } P.$$

If G has a faithful complex representation of degree less than $(|P| - 1)^{2/3}$, then P is normal in G.

CHAPTER I

INTRODUCTION

In studying finite linear groups of fixed degree over the complex field, it is convenient to restrict attention to irreducible, unimodular, and quasiprimitive groups. (For example, see [3], [9], and [12].) As is well-known, any representation is projectively equivalent to a unimodular one. Also, a representation which is not quasiprimitive is induced from a representation of a proper subgroup. (A quasiprimitive representation is one whose restriction to any normal subgroup is homogeneous, i.e., a multiple of one irreducible representation of the subgroup.) Hence, these assumptions are not too restrictive. If one assumes also that the degree is an odd prime p, there is a natural division into cases, according to the order of a Sylow p-group P of such a group G. The following is known.

1. $|P| = p$. G is known for small values of p. See below.
2. $|P| = p^2$. Here G is $G_1 \times Z$, where Z is the group of order p and G_1 is a group from case 1. [3].
3. $|P| = p^3$. G is known only for small values of p.
4. $|P| = p^4$. Here P contains a subgroup Q of index p which is normal in G, and G/Q is isomorphic to a subgroup of SL(2,p). [7] and [10], independently.
5. $|P| \geq p^5$. No such G exists. [7] and [10].

Our main theorem concerns the third case above.

<u>THEOREM 1</u>. Suppose G is a finite group with a faithful, irreducible, unimodular and quasiprimitive representation of prime degree $p \geq 5$. If a Sylow p-group P of G has order p^3, then P is normal in G and G/P is isomorphic to a subgroup of SL(2,p).

It is well-known that this Theorem is false for p = 2 or 3. Counterexamples are provided by groups projectively equivalent to the alternating groups A_5 and A_6, respectively. Combining Theorem 1 with the other results in the five cases cited above, we have the following conjecture of Feit [6].

THEOREM 2. Suppose G is a finite group with a faithful, irreducible and unimodular complex representation of prime degree $p \geq 5$. Then p^2 does not divide the order of $G/O_p(G)$.

Note that the quasiprimitivity condition is dropped in Theorem 2. Representations of prime degree which are not quasi-primitive are monomial, and for monomial representations, the Theorem is trivial.

It is likely that Brauer conjectured all of the above when he wrote [3], although he was able to get full results only when $|P| = p^2$. Partial results in the other cases allowed him to classify all groups where $p = 5$. (The cases $p = 2$ or 3 are classical, as are groups of degree 4. [1].) Using Brauer's general approach, Wales was able to handle the case $p = 7$ in three papers, [12], [13], and [14]. It is clear from the amount of work involved in these that full results for primes ≥ 11 will be very difficult without further techniques. Lindsey [9] has used some of these same ideas in his classification of groups of degree 6. Using entirely different special methods, Feit has settled the case $p = 11$ when the character of degree 11 is rational-valued, [7].

The general method for the cases $|P| \geq p^3$ used by both Brauer and Wales was to show P was not too large, and then handle each case arithmetically. Feit and Lindsey have now settled the case $|P| \geq p^4$ in general. With Theorem 1, only the case $|P| = p$ remains unsolved.

The following result, which is used in the proof of Theorem 1, is of independent interest.

THEOREM 3. Suppose G is a finite group with a Sylow p-group P satisfying

$$C_G(x) = P, \quad \text{all } x \neq 1 \text{ in } P.$$

If $|P| > 3$ and G has a faithful complex representation of degree d with

$$d \leq (|P| - 1)^{2/3},$$

then P is normal in G.

Leonard [8] has proved a theorem like Theorem 3 under a considerably stronger bound on d. Brauer and Leonard have shown [4] that under the weaker hypothesis

$$C_G(x) = C_G(P), \quad \text{all } x \neq 1 \text{ in } P,$$

the bound

$$d < (|P| - 1)^{1/2}$$

forces P normal in G. Both this result and Theorem 3 are sharp, in the sense that if we replace d by d-1 in the inequalities, the results are false. Counterexamples are SL(2,5) and PSL(2,5) with p = 5. However, a more reasonable bound in both cases might be

$$d < \frac{1}{2}(|P| - 1),$$

which would be sharp infinitely often. The techniques used to prove Theorem 3 can be refined to yield bounds of the form

$$d < \frac{1}{3m}(|P| - 1),$$

where m is a certain integer depending only on $|P|$, but this result is not needed here.

Our notation is fairly standard. If G is a finite group with a subgroup H, then $N_G(H)$, $C_G(H)$ and $Z(G)$ denote, respectively, the normalizer in G of H, the centralizer in G of H, and the center of G. If p is a prime number, $O^{p'}(G)$ denotes the smallest normal subgroup of G whose quotient has order prime to p. Equivalently, it is the subgroup of G generated by all elements of G whose order is a power of p. If $x \in G$ has order a power of p, we call x a p-element, while if x has order prime to p, we say x is a p'-element, or call x p-regular. $|G|$ denotes the order of G.

We will use the term character only for characters of complex representations, while the term generalized character will be used for the difference of two characters. If θ_1 and θ_2 are two class functions on G, we have the usual inner product

$$(\theta_1,\theta_2) = \frac{1}{|G|}\sum_{x\in G} \theta_1(x)\theta_2(x^{-1}).$$

CHAPTER II

PROOF OF THEOREM 3

Brauer and Leonard [4] have considered the character theory of finite groups G with a Sylow p-group P which satisfies

$$C_G(x) = C_G(P), \quad \text{all } x \neq 1 \text{ in } P.$$

Throughout this thesis, we will be interested in a special case of these results; namely, when P satisfies the stronger condition

$$(1) \qquad C_G(x) = P, \quad \text{all } x \neq 1 \text{ in } P.$$

In this case, P is an abelian group and $N = N_G(P)$ is a Frobenius group with Frobenius kernel P.

The character theory for N itself is well-known. Let $s = |N/P|$ and $ts = |P| - 1$, so that t is an integer. There are s_1 irreducible characters, $s_1 \leq s$,

$$1_N = \theta_1, \ldots, \theta_{s_1}$$

whose kernels all contain P, and t irreducible characters

$$\lambda_1, \ldots, \lambda_t$$

which are faithful on N. These faithful characters are induced from non-principal linear characters of P. In particular, their degrees are all $|N/P| = s$, and if $g \in N-P$, then

$$0 = \lambda_1(g) = \ldots = \lambda_t(g).$$

If $x \in P$, then

$$\sum_{i=1}^{t} \lambda_i(x) = -1,$$

and

$$\sum_{i=1}^{s_1} \theta_i^2(1) = \sum_{i=1}^{s_1} \theta_i^2(x) = |N/P| = s.$$

The results of Brauer and Leonard show that G has a similar character theory. The integers s and t are as above: $s = |N/P|$, and $ts = |P| - 1$. There are l irreducible characters, $l \leq s$,

$$1_G = \varphi_1, \ldots, \varphi_l$$

called ordinary characters of G, and t irreducible characters

$$\Lambda_1, \ldots, \Lambda_t$$

called exceptional characters of G. These two sets of characters constitute exactly those characters of G which do not vanish on the non-identity elements of P, and exactly those whose degrees are not divisible by $|P|$. There are non-zero integers $b_1, \ldots, b_l$, an integer r, and a sign $\delta = \pm 1$, such that, for $x \neq 1$ in P,

$$\varphi_m(x) = b_m \equiv \varphi_m(1) \pmod{|P|}, \text{ for } 1 \leq m \leq l,$$

$$\Lambda_k(x) = r + \delta\lambda_k(x),$$

$$\Lambda_k(1) \equiv r + \delta s \pmod{|P|}, \text{ for } 1 \leq k \leq t.$$

If $g \in G$ has order prime to p, then

$$\Lambda_1(g) = \ldots = \Lambda_t(g),$$

and this common value is an integer. We have

$$\sum_{m=1}^{l} b_m^2 + r^2(t-1) + (r-\delta)^2 = s + 1.$$

In particular, each $|b_m| \leq p$.

When $t = 1$, the exceptional character is indistinguishable from the ordinary characters, so all mention of exceptional characters is omitted in this case.

We are now ready to begin the proof of Theorem 3, which we restate as

<u>Proposition 1</u>. Suppose G is a finite group containing a Sylow p-group which satisfies

$$C_G(x) = P, \text{ all } x \neq 1 \text{ in } P.$$

Suppose also that G has a faithful representation of degree d with

$$d \leq \frac{1}{2}(|P| - 1).$$

Then one of the following holds.

(i) P is normal in G.

(ii) $t^2 < s$, where $s = |N_G(P)/P|$ and $st = |P| - 1$.

It is easy to show that Proposition 1 implies Theorem 3. If G satisfies the hypotheses of Theorem 3, then G satisfies the hypotheses of Proposition 1, and as $|P| > 3$, the degree d given for G by Theorem 3 is less than $\frac{1}{2}(|P| - 1)$. Let φ_m be any non-exceptional constituent of the character χ of degree d. Since $\varphi_m(1) < \frac{1}{2}(|P| - 1)$ and $\varphi_m(1) = e_m|P| + b_m$, for integer e_m and $|b_m| < p$, we must have $e_m = 0$, so P is contained in the kernel of φ_m. Thus, as χ is faithful, it must have some exceptional constituent Λ. We have

$$s \leq \Lambda(1) \leq \chi(1) = d \leq (|P| - 1)^{2/3} = (st)^{2/3}.$$

That is, $s^3 \leq s^2t^2$, so $s \leq t^2$, contrary to (ii). Hence, (i) holds, proving Theorem 3 from Proposition 1.

Before proving Proposition 1, we need two lemmas concerning class multiplication in N.

<u>LEMMA 1</u>. Suppose that G satisfies the hypotheses of Proposition 1, and that P is not contained in any proper normal subgroup of G. If there are three (not necessarily distinct) classes K_i, K_j, K_k of $N = N_G(P)$ consisting of non-identity p-elements of N whose associated class multiplication constant a_{ijk} for N satisfies

$$a_{ijk} \leq (s - n)/t,$$

for some positive integer n, then $((n - 1)t)^2 < s$.

Proof. The given faithful representation of G must have an exceptional character as a constituent. By a theorem of Leonard [8], it has degree s, and the restriction of any exceptional character of G to N remains irreducible. Let g_i, g_j, g_k be elements of K_i, K_j, K_k, respectively, and define

$$L_{ijk} = \Sigma' \Lambda(g_i)\Lambda(g_j)\Lambda(g_k^{-1}),$$

where the sum Σ' is over all exceptional characters Λ of G, or, equivalently, of N. We have

$$a_{ijk} = \frac{|N|}{|P|^2}\left(\sum{}'' \frac{\theta(g_i)\theta(g_j)\theta(g_k^{-1})}{\theta(1)} + \frac{1}{s} L_{ijk}\right),$$

$$= \frac{s}{|P|}(\Sigma'' \theta(1)^2 + \frac{1}{s} L_{ijk}),$$

$$= \frac{s}{|P|}(s + \frac{1}{s} L_{ijk}),$$

where the sum Σ'' is over all non-exceptional irreducible characters θ of N. As $a_{ijk} \leq (s-n)/t$, we get

$$s - \frac{|P|}{st}(s-n) \leq -\frac{1}{s} L_{ijk}.$$

Now N controls fusion of its p-elements with respect to G, so there is a class multiplication constant α_{ijk} for G associated with a_{ijk}. Here we find

$$0 \leq \alpha_{ijk} = \frac{|G|}{|P|^2}\left(\sum_m \frac{b_m^3}{\varphi_m(1)} + \frac{1}{s} L_{ijk}\right).$$

Hence,

$$s - \frac{|P|}{st}(s-n) \leq -\frac{1}{s} L_{ijk} \leq \sum_m \frac{b_m^3}{\varphi_m(1)}.$$

Since P is contained in no proper normal subgroup of G, we see that $b_m = \varphi_m(1)$ holds only for $m = 1$, i.e., only for the principal character φ_1. Thus, if $m \neq 1$, $\varphi_m(1) \geq |P| - 1 = st$. Note that as $r = 0$, we have $\Sigma b_m^2 = s$. Let B denote the maximum positive value among all the b_m. Then

$$s - \frac{|P|}{st}(s-n) \leq \frac{1}{st}\sum_{m\neq 1} b_m^3 + 1,$$

$$s^2t - (st+1)(s-n) \leq \sum_{m\neq 1} b_m^3 + st,$$

$$s^2t - s^2t - s + nst + n \leq sB + st,$$

$$(n-1)t - 1 + \frac{n}{s} \leq B.$$

As B is an integer, and $0 < n \leq s$, $(n-1)t \leq B$. But $\Sigma\, b_m^2 = s$, and B is some b_m, so $((n-1)t)^2 \leq s$. It is easy to see that this last inequality is strict.

COROLLARY. With the above notation, some $b_m \geq (n-1)t$.

LEMMA 2. The integer n in Lemma 1 may be taken to be at least 2.

Proof. Let $K_1, \ldots, K_t$ be the classes of non-identity p-elements of N, and K_0 the class of the identity. For each $i = 1, \ldots, t$, let i' be the subscript of the class consisting of elements which are the inverses of elements in K_i. Then for fixed $i \neq 0$,

$$s^2 = |K_i|^2 = \sum_{k=1}^{t} a_{ii'k}|K_k| + a_{ii'0}|K_0|$$
$$= \sum_{k=1}^{t} a_{ii'k}\, s + s$$

so that

$$s^2 - s = \sum_{k=1}^{t} a_{ii'k}\, s,$$
$$s - 1 = \sum_{k=1}^{t} a_{ii'k}.$$

Thus, some $a_{ii'k} \leq (s-1)/t$. If $i' \neq j$, then

$$s^2 = |K_i||K_j| = \sum_{k=1}^{t} a_{ijk}|K_k|$$
$$= \sum_{k=1}^{t} a_{ijk}\, s.$$

Hence, some such $a_{ijk} \leq s$.

Now suppose by way of contradiction, that all $a_{ijk} \geq (s-1)/t$, for all $i, j, k = 1, 2, \ldots, t$. By the above calculations, we must have

$$a_{ii'k} = (s-1)/t, \qquad \text{all } i, k = 1, \ldots, t,$$

$$a_{ijk} = (s-1)/t \quad \text{for } t-1 \text{ values of } k,$$
$$= (s-1+t)/t \quad \text{for 1 value of } k, \qquad \text{if } i' \neq j.$$

Note t divides $s-1$ here, as $a_{ii'k}$ is an integer. We will show that this situation can occur only when t is 1 or 2, contrary to $s \leq d < \frac{1}{2}(|P| - 1)$.

Let λ be a faithful character of N, and ω the corresponding representation of the center of the group algebra of N:

$$\omega(K_i) = |K_i| \frac{\lambda(g_i)}{\lambda(1)} = \frac{s}{s}\lambda(g_i) = \lambda(g_i).$$

As $t \neq 1$, there is some $j \neq i'$, so we may write

(2) $$\lambda(g_i)\lambda(g_j) = \omega(K_i)\omega(K_j) = \sum_{k=1}^{t} a_{ijk}\,\omega(K_k)$$
$$= \frac{s-1}{t}\sum_{k=1}^{t}\lambda(g_k) + \lambda(g_{ij})$$
$$= -\frac{s-1}{t} + \lambda(g_{ij}).$$

Here we have chosen $g_k \in K_k$, all k, and g_{ij} in the unique class for which a_{ijk} has the distinguished value. We also have

$$(3) \qquad \lambda(g_i)\overline{\lambda(g_i)} = \omega(K_i)\omega(K_{i'}) = \sum_{k=1}^{t} a_{ii'k}\,\omega(K_k) + s\omega(1)$$

$$= \frac{s-1}{t} \sum_{k=1}^{t} \lambda(g_k) + s$$

$$= s - \frac{s-1}{t} .$$

Combining (2) and (3) for $i' \neq j$, we find

$$\left(s - \frac{s-1}{t}\right)^2 = \lambda(g_i)\overline{\lambda(g_i)}\,\lambda(g_j)\overline{\lambda(g_j)}$$

$$= \left(- \frac{s-1}{t} + \lambda(g_{ij})\right)\left(- \frac{s-1}{t} + \overline{\lambda(g_{ij})}\right)$$

Setting $x = \lambda(g_{ij})$, this is

$$\left(s - \frac{s-1}{t}\right)^2 = \left(x - \frac{s-1}{t}\right)\left(\bar{x} - \frac{s-1}{t}\right)$$

$$s^2 - 2s\,\frac{s-1}{t} + \left(\frac{s-1}{t}\right)^2 = x\bar{x} - (x+\bar{x})\,\frac{s-1}{t} + \left(\frac{s-1}{t}\right)^2$$

$$= s - \frac{s-1}{t} - (x+\bar{x})\,\frac{s-1}{t} + \left(\frac{s-1}{t}\right)^2.$$

Thus,

$$s^2 - s = \frac{s-1}{t}\,(-1-(x+\bar{x}) +2s).$$

As $s \neq 1$ (otherwise $G = P$ follows trivially),

$$s = \frac{1}{t}\,(-1-(x+\bar{x})+2s),$$

$$ts - 2s + 1 = -(x+\bar{x}).$$

Now $t > 2$, so this is positive. Since $|x+\bar{x}| \leq 2|x|$, we have

$$(t-2)s + 1 = ts - 2s + 1 \leq 2\left(s - \frac{s-1}{t}\right)^{1/2} < 2s^{1/2}.$$

But $t-2 > 1$, so

$$s < 2s^{1/2},$$

$$s < 4.$$

Thus, $s = 1$, 2, or 3, and since t divides $s-1$, we have $t = 1$ or 2, or else $s = 1$, none of which are allowed. This completes the proof of Lemma 2.

Finally, we prove Proposition 1. Suppose G is a counterexample of minimal order. By Lemmas 1 and 2 together, we have $t^2 < s$ unless P is contained in a proper normal subgroup of G. As G is a counterexample, the latter is true. But the given faithful character of G is still faithful when restricted to the normal subgroup H, so H satisfies the hypotheses of the Proposition. As $|H| < |G|$, we have P normal in H, and so characteristic in H, whence P is normal in G. Proposition 1 is proved.

Brauer [3] has shown that the situation described in Proposition 1 arises naturally in the study of finite linear groups of prime degree. In particular, suppose G is a group satisfying the hypotheses of Theorem 1. Then $Z(G) = Z(P)$ is cyclic of order p, and a Sylow p-group $\bar{P}$ of $\bar{G} = G/Z(G)$ satisfies (1). Hence, all of the character theory described at the beginning of this chapter applies to $\bar{G}$, and so to G. Furthermore, if χ is the given character of degree p, then we have one of only two cases:

<u>CASE I</u>: $\chi\bar{\chi}$ has norm 2. That is, $\chi\bar{\chi} = \varphi_1 + \varphi_2$, where φ_1 is the principal character of G, and φ_2 is some ordinary irreducible character of $\bar{G}$, and so of G.

<u>CASE II</u>: $\chi\bar{\chi}$ has norm $1+t$. Here we have

$$\chi\bar{\chi} = \varphi_1 + \Sigma' \Lambda,$$

where Σ' denotes the sum over all exceptional characters Λ of $\bar{G}$.

Notice that when $t = 1$, the two cases are indistinguishable. Also, if $t \neq 1,2$, then in Case II, $\bar{G}/\ker \Lambda$ satisfies the hypotheses of Proposition 1. Now suppose that G is a counterexample to the Theorem of minimal order. From Wales [12], we have that $\bar{G}$ is simple, so $\ker \Lambda$ is the trivial group. Hence, in Case II, we must have $t^2 < s$ or $t = 1$ or 2. In fact, the former always holds except for $p = 2$, a case we are not discussing. In Chapter III we will prove a similar result (Lemma 14) for a minimal counterexample in Case I, namely

PROPOSITION 2. Suppose G is a counterexample to Theorem 1 of minimal order, and suppose Case I holds for G. If $p \geq 7$, then $(t-1)^2 \leq s$.

Groups satisfying the hypotheses of Theorem 1 are all known for $p \leq 7$, and Theorem 1 is true here. We may assume, then, that in all cases $(t-1)^2 \leq s$. We now show that this severely limits the possibilities for p, s and t.

As usual, we let $N = N_G(P)$, so $\bar{N} = N_{\bar{G}}(\bar{P})$. Here $\bar{P}$ is the elementary abelian group of order p^2, and so we have $\bar{N}/\bar{P}$ being isomorphic to a subgroup of $GL(2,p)$. However, since $\bar{N}/\bar{P}$ is N/P, and $Z(P)$ is in the center of N, this is actually a subgroup of $SL(2,p)$. The subgroups of $SL(2,p)$ of order prime to p are easily described. For each of these, we get information about s, and so about t, as $(t-1)^2 \leq s$. From this we then find information about p. These results are summarized in the following table.

$\overline{N}/P$	s	t	p
(a) Has a cyclic subgroup of index at most 2.	$s \leq 2p+2$	$t \geq \frac{1}{2}(p-1)$	$p \leq 13$
(b) SL(2,3)	$s = 24$	$t \leq 5$	$p \leq 11$
(c) Projective cover of S_4	$s = 48$	$t \leq 7$	$p \leq 17$
(d) SL(2,5)	$s = 120$	$t \leq 11$	$p \leq 31$

Case (a) is computed as follows. Since $s \leq 2p+2$ and $st = |\overline{P}| - 1 = p^2 - 1$, we must have $t \geq \frac{1}{2}(p-1)$. Now as $(t-1)^2 < s$, we have

$$\left(\frac{p-3}{2}\right)^2 \leq 2p + 2,$$

or

$$p^2 - 14p + 1 \leq 0,$$

so $p < 14$. As p is an integer, $p \leq 13$.

The remaining cases are all computed by the same method. We do case (d) as an example. As $s = 120$ and $(t-1)^2 \leq s$, we get $t \leq 11$. Thus, $p^2 - 1 = st \leq 120 \times 11 = 1320$. Hence, $p^2 < 37^2 = 1369$. Since p is a prime, $p \leq 31$.

The values of p, s, and t occurring in the above list will be considered in the last chapter, where we will show that they do not occur for the group G. That is, no minimal counterexample to Theorem 1 exists, so Theorem 1 is true.

CHAPTER III

CHARACTER THEORY FOR A COUNTEREXAMPLE TO THEOREM 1

Throughout this chapter, we will assume G is a counterexample to Theorem 1 of minimal order. In particular, as was mentioned in Chapter II, we have $\overline{G} = G/Z(G)$ a simple group, and the character theory described at the beginning of Chapter II applies to $\overline{G}$. We will use the notation introduced there, and will sometimes consider characters of $\overline{G}$ as characters of G, without changing this notation. We begin by investigating the characters of $N = N_G(P)$ more thoroughly. Let ξ denote the sum of the distinct faithful irreducible characters of $\overline{N}$. We will let $Z = Z(G) = Z(P)$.

The class function ζ defined by

$$\begin{aligned} \zeta(x) &= p^2 \quad \text{if } x \text{ is a non-central } p\text{-element,} \\ &= 0 \quad \text{otherwise,} \end{aligned}$$

is a generalized character of $\overline{G}$, and, in fact,

$$\zeta = \sum_{m=1}^{l} b_m t\varphi_m + (rt-\delta) \sum_{k=1}^{t} \Lambda_k.$$

(Brauer and Leonard [4]).

<u>LEMMA 3</u>. Let θ be a character of $\overline{N}$ such that

$$\theta(1) = np^2 - n, \quad \text{some positive integer } n,$$

$$\theta(x) = -n, \quad \text{all } x \neq \overline{1} \text{ in } \overline{P}.$$

Then $\theta = n\xi$. In particular, $\theta(g) = 0$ if $g \in \overline{N}-\overline{P}$.

Proof. Clearly, $\theta|\overline{P}$ is n times the sum of all non-principal irreducible characters of $\bar{P}$. Hence, θ is a sum of faithful characters of $\bar{N}$. Since θ is constant on non-identity elements of $\bar{P}$, the result follows.

LEMMA 4. $\chi\bar{\chi}|N = \theta_1 + \xi$. In particular, $|\chi(x)| = 1$, if $x \in N-P$.

Proof. $\chi\bar{\chi}|N = (\chi|N)(\bar{\chi}|N)$, so θ_1 is a constituent. Define the character Φ by

$$\chi\bar{\chi}|N = \theta_1 + \Phi.$$

We note that $Z \subseteq \ker \chi\bar{\chi}$, so $\chi\bar{\chi}$ can be considered a character of $\bar{N}$. Since $\chi(x) = 0$ for $x \in P-Z$, we have

$$\Phi(1) = p^2 - 1,$$

$$\Phi(x) = -1, \qquad \text{for } x \neq \bar{1} \text{ in } \bar{P}.$$

By Lemma 3, $\Phi = \xi$.

LEMMA 5. Let θ be an irreducible character of N such that $Z \not\subseteq \ker \theta$. Then there is a conjugate χ^ρ of χ such that $\chi = \chi^\rho$ on p-regular elements of N, and an irreducible character θ_i of N/P such that $\theta = \theta_i(\chi^\rho|N)$.

Proof. We enumerate the characters of N. First, we show that if χ^ρ is a conjugate of χ, and θ_i is irreducible for N/P, then $\theta_i(\chi^\rho|N)$ is irreducible. We have

$$(\theta_i(\chi^\rho|N), \theta_i(\chi^\rho|N))_N = (\theta_i\bar{\theta}_i, \chi^\rho\bar{\chi}^\rho|N)_N$$

$$= (\theta_i\bar{\theta}_i, \theta_1 + \xi).$$

Now $(\theta_i\bar{\theta}_i, \theta_1) = 1$, and since $\theta_i\bar{\theta}_i$ has P in its kernel, but no constituent of ξ does, $(\theta_i\bar{\theta}_i, \xi) = 0$. Hence, $\theta_i(\chi^\rho|N)$ has norm 1 and so is irreducible.

Now χ has p-1 distinct conjugates χ^ρ which agree with χ on all p-regular elements of G. Thus, our contribution to the sum of the squares of the irreducible degrees so far is

$$\sum_{i=1}^{s_1} \theta_i(1)^2 + \sum_{k=1}^{t} \lambda_k(1)^2 + (p-1)\sum_{i=1}^{s_1} (\theta(1)\chi(1))^2$$

$$= s + ts^2 + (p-1)sp^2$$

$$= s + (p^2-1)s + (p-1)sp^2$$

$$= s(p^2 + p^3 - p^2) = sp^3 = |N|.$$

Hence, we have all the irreducible characters of N in this way. The Lemma is proved.

Let χ' and χ'' denote the symmetric and skew-symmetric tensor constituents of χ^2.

$$\chi'(g) = \frac{1}{2}(\chi(g)^2 + \chi(g^2)),$$

$$\chi''(g) = \frac{1}{2}(\chi(g)^2 - \chi(g^2)), \quad \text{all } g \in G.$$

These are characters of G. Since χ' and χ'' have no constituents with Z in their kernels, there are characters θ' and θ'' of N/P such that

$$\chi'|N = \theta'(\chi^\rho|N),$$

$$\chi''|N = \theta''(\chi^\rho|N),$$

for an appropriate conjugate χ^ρ of χ. Note that θ' and θ'' need not be irreducible. Also, $\theta'(1) = \frac{1}{2}(p+1)$ and $\theta''(1) = \frac{1}{2}(p-1)$.

LEMMA 6. If s is even, θ' and θ'' have no common constituents.
Proof. Let $x \in N$, $x^2 = 1$, $x \neq 1$. Then

$$p = \chi(1) = \chi(x^2) = (\chi' - \chi'')(x)$$

$$= (\theta' - \theta'')(x)\ (\chi^\rho(x))$$

$$= \pm(\theta' - \theta'')(x),$$

so

$$p = |\theta'(x) - \theta''(x)| \leq |\theta'(x)| + |\theta''(x)|$$

$$\leq \frac{p+1}{2} + \frac{p-1}{2} = p.$$

This forces representations affording θ' and θ'' to represent x as I in one case and -I in the other (of appropriate sizes). They can have no common constituents.

We will next construct a generalized character of $\overline{G}$ and apply the character theory so far developed. Suppose η is any generalized character of G. Define a class function η_0 by

$$\eta_0(x) = \eta(x_0), \qquad \text{all } x \in G,$$

where x_0 denotes the p-regular part of x. It follows from Brauer's characterization of characters that η_0 is again a generalized character of G, and in fact, of $\overline{G}$. We will be interested in χ_0, χ_0', χ_0'', and χ_0^2. Note that we have that

$$\chi_0^2 = \chi\overline{\chi} + \zeta,$$

as χ is real on p-regular elements (Wales [12]).

LEMMA 7. Suppose η and μ are generalized characters of G, and λ is a non-principal linear character of Z. Assume that for all irreducible characters X of G, whenever $(\eta, X) \neq 0$ or $(\mu, X) \neq 0$ we have $X|Z = X(1)\lambda$. Then

$$(\eta_0, \mu_0) = (\eta, \mu) + \frac{1}{p^2}\eta(1)\mu(1)t.$$

Proof. Let R denote the set of p-regular elements of G, and S the set of non-central p-elements of G. We put $1 \in R$. Let λ be an irreducible constituent of $\eta|Z$. Note that η and μ vanish on P-Z. Write

$$\begin{aligned}
(\eta_0, \mu_0) &= \frac{1}{|G|}\sum_{x\in G}\eta(x_0)\,\overline{\mu(x_0)} \\
&= \frac{1}{|G|}\sum_{x\in R}\sum_{z\in Z}\eta((xz)_0)\,\overline{\mu((xz)_0)} \\
&\qquad + \frac{1}{|G|}\sum_{x\in S}\eta(x_0)\,\overline{\mu(x_0)} \\
&= \frac{1}{|G|}\sum_{x\in R}\sum_{z\in Z}\eta(x)\,\lambda(z)\,\overline{\lambda(z)}\,\overline{\mu(x)} \\
&\qquad + \frac{1}{|G|}\sum_{x\in S}\eta(1)\,\mu(1) \\
&= \frac{1}{|G|}\sum_{x\in R}\sum_{z\in Z}\eta(xz)\,\overline{\mu(xz)} \\
&\qquad + \frac{1}{|G|}\sum_{x\in G}\frac{1}{p^2}\eta(1)\,\mu(1)\,\zeta(x) \\
&= \frac{1}{|G|}\sum_{x\in G}\eta(x)\,\overline{\mu(x)} \\
&\qquad + \frac{1}{|G|}\sum_{x\in G}\frac{1}{p^2}\eta(1)\,\mu(1)\,\zeta(x).
\end{aligned}$$

But this is just

$$(\eta_0, \mu_0) = (\eta, \mu) + \frac{1}{p^2}\eta(1)\mu(1)(\varphi_1, \zeta)$$

$$= (\eta, \mu) + \frac{1}{p^2}\eta(1)\mu(1)\,t,$$

as required.

We will denote $\chi_0' - \chi_0''$ by χ_2. Note that $\chi_2 - \chi_0$ has degree 0.

LEMMA 8. χ_0 has norm $1+t$. If $\chi\bar{\chi}$ has norm 2, then $\chi_2 - \chi_0$ has norm 3.

Proof. Apply Lemma 7. Note that χ' and χ'' are irreducible when $\chi\bar{\chi}$ has norm 2, and χ is not conjugate to either of them, as $p > 3$.

When $\chi\bar{\chi}$ has norm 2, we will choose our notation so that $\chi\bar{\chi} = \varphi_1 + \varphi_2$. Choose a conjugate χ^σ of χ such that $\chi_0^\sigma = \chi_0$ and $\chi^\sigma\chi^2$ has Z in its kernel.

LEMMA 9. Suppose s is even and η is an irreducible character of G such that

$$(\eta, \chi^\sigma\chi'), \ (\eta, \chi^\sigma\chi'') \geq 1.$$

Then $\eta | N$ has only exceptional characters as constituents.

Proof. Note first that

$$\chi^\sigma\chi' | N = \theta'\chi^\sigma\chi^\rho | N = \theta'(\chi^\sigma\chi^{-\sigma} | N) = \theta'(\theta_1 + \xi)$$

$$= \theta' + \frac{p+1}{2}\xi.$$

Similarly, $\chi^\sigma\chi'' = \theta'' + \frac{p-1}{2}\xi$. By Lemma 6, θ' and θ'' have no common constituents.

LEMMA 10. We have $t \neq 1$.

Proof. If $t = 1$, $s = p^2 - 1$, and so s is even. Since $\bar{G}$ is simple, it has no non-principal characters of degree $< p$, for such a character would have P in its kernel. Thus, $\chi_0 = \alpha_1 - \alpha_2$, for irreducibles α_i of $\bar{G}$. Now $(\chi^\sigma \chi', \chi_0) = 1$, as

$$(\chi^\sigma \chi', \chi_0) = (\chi', \bar{\chi}^\sigma \chi_0) = (\chi', \chi^2) = 1,$$

and, similarly, $(\chi^\sigma \chi'', \chi_0) = 1$. It follows that

$$(\chi^\sigma \chi', \alpha_1), (\chi^\sigma \chi'', \alpha_1) \geq 1.$$

By Lemma 9, $\alpha_1 | N = n\xi$, for some integer n. Note that ξ is irreducible here. That is, $\alpha_1(1) = np^2-n$, and $\alpha_1(x) = -n$, for $x \in P-Z$. Hence, $\alpha_2(1) = np^2-n-p$ and $\alpha_2(x) = -n-p$, for $x \in P-Z$. This is contrary to $|\alpha_2(x)| < p$, proving the Lemma.

LEMMA 11. φ_1 is not a constituent of $\chi_2 - \chi_0$ if $\chi\bar{\chi}$ has norm 2.

Proof. Assume the contrary. $(\chi_2 - \chi_0, \chi_0^2) = 0$ by Lemma 5. However,

$$(\chi_2 - \chi_0, \chi_0^2) = (\chi_2 - \chi_0, \chi\bar{\chi} + \zeta) = (\chi_2 - \chi_0, \chi\bar{\chi})$$

$$= (\chi_2 - \chi_0, \varphi_1 + \varphi_2).$$

Thus, $(\chi_2 - \chi_0, \varphi_2) = (\chi_2 - \chi_0, -\varphi_1)$. Hence, $(\chi_2 - \chi_0, \varphi_1) = \pm 1$, and $(\chi_2 - \chi_0, \varphi_2)$ is its negative. Since we have three constituents in $\chi_2 - \chi_0$, there is only one left, say φ. Then $\varphi(1) = p^2 - 2$, and $\varphi(x) = -2$, for $x \in P-Z$. By Lemma 3, $(\varphi + \varphi_1)|N$ has only exceptional constituents. This is a contradiction, since θ_1 is obviously a constituent, and is not exceptional.

LEMMA 12. χ_0 has no exceptional constituents if $\chi\overline{\chi}$ has norm 2.

Proof. Suppose the contrary. As χ_0 is constant on P-Z, all t exceptionals Λ_k have the same multiplicity in χ_0. As χ_0 has norm 1+t, we must have

$$\pm\chi_0 = \sum_{k=1}^{t} \Lambda_k \pm \varphi,$$

for some irreducible φ for $\overline{G}$. Note $\varphi \neq \varphi_1$.

Suppose first that s is odd. Then t is even, so

$$1 + t = (\varphi_1 , \chi\overline{\chi} + \zeta) = (\varphi_1 , \chi_0^2)$$

$$= (\varphi_1 , \chi_0' + \chi_0'')$$

is odd. Hence, $(\varphi_1 , \chi_2) = (\varphi_1 , \chi_0' - \chi_0'')$ is also odd. Since $(\varphi_1 , \chi_0) = 0$, we have $(\varphi_1 , \chi_2 - \chi_0)$ odd, and so not zero. This contradicts Lemma 11.

Hence, we may assume s is even. In this case, each exceptional Λ_k is real-valued. For any character η of G, let $\nu(\eta) = (\varphi_1 , \widetilde{\eta})$, where $\widetilde{\eta}(x) = \eta(x^2)$. (For the properties of the function ν, see Feit [5], for instance.) Observe that $\widetilde{\chi}_0 = \chi_2$. If η is real and irreducible, then $\nu(\eta) = \pm 1$. Otherwise $\nu(\eta) = 0$ for irreducible η. Now, from Lemma 11

$$0 = (\varphi_1 , \chi_2 - \chi_0) = (\varphi_1 , \chi_2)$$

$$= \pm(\sum_{k=1}^{t} \nu(\Lambda_k) \pm \nu(\varphi)).$$

Since $\nu(\Lambda_k)$ is non-zero and independent of k, we have

$$0 = t\, \nu(\Lambda_1) \pm \nu(\varphi).$$

This shows that $t = 1$, contrary to Lemma 10. The Lemma is proved.

LEMMA 13. If $\chi\bar{\chi}$ has norm 2, either

(i) $rt - \delta$ is even. In particular, t is odd and s is even, and r is not zero.

(ii) $t = 2$ and $p \leq 5$.

Proof. Suppose $rt - \delta$ is odd and $\chi_2 - \chi_0$ has no exceptional constituents. Then for any k, $1 \leq k \leq t$,

$$rt - \delta = (\Lambda_k , \zeta) = (\Lambda_k , \chi\bar{\chi} + \zeta)$$

$$= (\Lambda_k , \chi_0^2) = (\Lambda_k , \chi_0' + \chi_0'')$$

is odd. Hence, $(\Lambda_k , \chi_0' - \chi_0'')$ is odd, and so not zero. Since $(\Lambda_k , \chi_2 - \chi_0) = 0$, we have Λ_k a constituent of χ_0, contrary to Lemma 12.

Now suppose $\chi_2 - \chi_0$ has some exceptional constituent. Since $\chi_2 - \chi_0$ is constant on P-Z, all exceptionals have equal multiplicity in $\chi_2 - \chi_0$. As this character has norm 3 and degree 0, there are at most 2 exceptionals. That is, $t = 2$. Since $3 = 1 + t = (\varphi_1 , \chi_0^2)$ is odd, we can show in the usual way that $(\varphi_1 , \chi_0) \neq 0$. For an appropriate conjugate χ^σ of χ, Lemma 7 shows

$$(\chi_0 , \chi_0^2) = (\chi, (\chi^\sigma)^2) + pt = pt = (\chi_0 , \zeta).$$

Hence, $(\chi_0 , \chi\bar{\chi}) = (\chi_0 , \chi_0^2 - \zeta) = 0$, so that φ_2 is a constituent of χ_0, and its multiplicity is the negative of the multiplicity of φ_1 in χ_0. As χ_0 has norm $1+t = 3$, there is only one other constituent of χ_0. It has degree $p^2 \pm p-2$, but p^2-p-2 would be an ordinary degree with corresponding $b_m = -p-2$, contrary to $|b_m| < p$. Hence, we have a character of $\bar{G}$ of degree p^2+p-2. This must be an ordinary degree with corresponding value of b_m

being p-2. Now

$$\frac{1}{2}(p^2-1) = s \geq \sum_m b_m^2 > (p-2)^2.$$

Thus, $p < 7$, so $p \leq 5$, as required.

LEMMA 14. We have

$$(\varphi_m, \chi_0) = \left[\frac{b_m t}{p}\right] \text{ or } \left[\frac{b_m t}{p}\right] + 1,$$

where square brackets denote the "greatest integer" function. If $\chi\bar{\chi}$ has norm 2 and $p \geq 7$, then $(\varphi_1, \chi_0) = 0$ and $(t-1)^2 \leq s$.

Proof. A calculation similar to that of Lemma 7 shows

$$(p\chi_0 - \zeta, p\chi_0 - \zeta) = (p\chi, p\chi) = p^2.$$

Thus,

$$(\varphi_m, p\chi_0 - \zeta)^2 \leq p^2,$$

and equality holds only if $p\chi_0 - \zeta = p\varphi_m$. However, equality would then imply $\varphi_m(1) = p$, which is not the case. Hence,

$$p > |(\varphi_m, p\chi_0 - \zeta)| = |p(\varphi_m, \chi_0) - b_m t|,$$

so that

$$1 > |(\varphi_m, \chi_0) - \frac{b_m t}{p}|,$$

proving the first statement.

To prove the last statement, consider

$$\sum_{k=1}^{t} (\Lambda_k, p\chi_0 - \zeta)^2 \leq p^2.$$

As above, equality cannot hold. Note that

$$(\Lambda_k , p\chi_0 - \zeta) = - (\Lambda_k , \zeta) = -rt+\delta,$$

by Lemma 12. As $r \neq 0$, we have $|rt-\delta| \geq t-1$, whence $t(t-1)^2$ is less than p^2. This implies $(t-1)^2 \leq s$.

To prove the remaining statement, note that $(t-1)^2 < s$ forces $t < p$, and we know $b_1 = 1$. Hence, $(\varphi_1 , \chi_0) = 0$ or 1. Say it is 1. By Lemma 11, $(\varphi_1 , \chi_2 - \chi_0) = 0$, so $(\varphi_1 , \chi_2) = -1$. However, $(\varphi_1 , \chi_0^2) = 1+t$ is an even integer, so $-1 = (\varphi_1 , \chi_2)$ must be even, a contradiction.

This Lemma immediately implies Proposition 2 of ChapterII.

<u>LEMMA 15</u>. χ is rational-valued on p-regular elements of G.

Proof. Suppose not. By a theorem of Wales [12], χ is real-valued on p-regular elements, and we have Case I. As χ is not rational on p'-elements, there is a Galois automorphism τ of the field of $|G|$-th roots of 1 such that

$$\chi^\tau \neq \chi,$$

$$\chi^\tau | P = \chi | P.$$

Again by the results of Wales [12], $\chi\overline{\chi}^\tau$ is irreducible, and real-valued. We choose our notation so that $\chi\overline{\chi} = \varphi_1 + \varphi_2$, as usual. Note that χ' and χ'' are irreducible, and

$$(\chi^2, (\chi^\tau)^2) = (\chi\overline{\chi}^\tau, \overline{\chi}\chi^\tau) = (\chi\overline{\chi}^\tau, \chi\overline{\chi}^\tau) = 1.$$

Thus, exactly one of χ' or χ'' is fixed by τ.

It is trivial to show $\chi_0 - \chi_0^\tau$ has norm 2. Say

$$\chi_0 - \chi_0^\tau = \alpha_1 - \alpha_2,$$

where α_1 and α_2 are irreducible. Now

$$(\chi^\sigma\chi', \chi_0) = (\chi', \bar{\chi}^\sigma\chi_0) = (\chi', \chi^2) = 1,$$

and similarly, $(\chi^\sigma\chi'', \chi_0) = 1$ also. We have

$$(\chi^\sigma\chi', \chi_0^\tau) = (\chi', \bar{\chi}^\sigma\chi_0^\tau) = (\chi', \chi\chi^\tau) = 0,$$

as χ' and $\chi\chi^\tau$ are irreducible. Similarly, $(\chi^\sigma\chi'', \chi_0^\tau) = 0$. Thus,

$$(\chi^\sigma\chi', \chi_0 - \chi_0^\tau) = (\chi^\sigma\chi'', \chi_0 - \chi_0^\tau) = 1.$$

In particular, both $(\chi^\sigma\chi', \alpha_1)$ and $(\chi^\sigma\chi'', \alpha_1)$ are at least 1. Hence, $\alpha_1|N$ consists of faithful characters of $\bar{N}$ by Lemma 9, for s is even by Lemma 13. From Lemma 12, α_1 is not an exceptional character, so it is constant on P-Z. Thus, $\alpha_1|N = n\xi$, for some positive integer n. We have $\alpha_1(1) = np^2-n$ and $\alpha_1(x) = -n$, for all $x \in$ P-Z. As $\chi_0 - \chi_0^\tau$ vanishes on P, $\alpha_2(1) = np^2-n$ and $\alpha_2(x) = -n$, for all $x \in$ P-Z, also. Thus, $\alpha_2|N = n\xi$, by Lemma 3. In particular, $(\alpha_1 - \alpha_2)|N = (\chi_0 - \chi_0^\tau)|N = 0$.

Now $(\chi_2 - \chi_0, \chi_0 - \chi_0^\tau) = 1$ from Lemma 7, so either α_1 or α_2 occurs in $\chi_2 - \chi_0$. Furthermore,

$$\begin{aligned}(\chi_2 - \chi_0, \chi^\tau\bar{\chi}^\tau) &= (\chi_2 - \chi_0, \chi^\tau\bar{\chi}^\tau + \zeta) \\ &= (\chi_2 - \chi_0, (\chi_0^\tau)^2) \\ &= (\chi' - \chi'' - \chi^\sigma, (\chi^\tau)^2) = \pm 1\end{aligned}$$

as exactly one of χ', χ'' is fixed by τ. Since α_1 is not a constituent of $\chi_2 - \chi_0$, we must have that α_2^τ is.

We show next that neither of α_1, α_2 is φ_2^{τ}. In fact, if one is, then χ_0 has a conjugate φ_2^{ρ} of φ_2 as a constituent. Now, as $p > 3$,

$$(\chi_0 , \chi^{\rho}\overline{\chi}^{\rho}) = (\chi^{\sigma}, (\chi^{\rho})^2) = 0,$$

by a calculation similar to that of Lemma 7. This forces φ_1 also to be a constituent of χ_0, contrary to Lemma 14.

Hence, $\chi_2 - \chi_0$ has two distinct constituents whose restrictions to N are multiples of ξ. It follows from Lemma 3 that the third constituent is also a multiple of ξ when restricted to N. Thus, $(\chi_2 - \chi_0)|N = 0$. But as s is even, N contains an involution x not in the kernel of χ. Thus,

$$0 = (\chi_2 - \chi_0)(x) = \chi(x^2) - \chi(x) = \chi(1) - \chi(x),$$

a contradiction. This completes the proof.

Lemma 15 limits the prime divisors of G, by a theorem of Schur [11]. The following consequence will be very helpful in Chapter IV.

<u>LEMMA 16</u>. Suppose q is a prime, $q \geq \frac{1}{2}(p+3)$, $p \neq q$. If q divides the order of G, then there is an integer m, $1 \leq m \leq \frac{1}{2}(p+1)$ such that $mp \equiv 1 \pmod{q}$. In particular, if either $q > p$ or Case I holds, then q does not divide the order of G.

Proof. By Lemma 15, χ is rational on p-regular elements. In particular, if Q is a Sylow q-group of G, then $\chi|Q$ is rational. Setting $|Q| = q^a$, a theorem of Schur [11] tells us

$$a \leq \left[\frac{p}{q-1}\right] + \left[\frac{p}{q(q-1)}\right] + \left[\frac{p}{q^2(q-1)}\right] + \dots ,$$

where square brackets denote the greatest integer function. In particular, if $q > p$, then q does not divide the order of G. If $q < p$, we see that q divides the order of G at most to the first power. Thus, Brauer's theory [2] applies. Let

$$C_G(Q) = Q \times V \times Z.$$

To each q-block β of G of full q-defect, there corresponds a character α of V and a positive integer τ, where α has τ distinct conjugates $\alpha = \alpha_1, \ldots, \alpha_\tau$, under the action of $N_G(Q)$. Let λ_i, $i = 1, \ldots, q-1$, denote the distinct non-principal linear characters of Q, and ρ the regular representation of Q. Each irreducible character in β has one of the following forms,

$$\text{(a)}\quad 1_Q \sum_{i=1}^{\tau} \alpha_i + \rho\,\eta,$$

$$\text{(b)}\quad \sum_{i=1}^{q-1} \lambda_i \sum_{j=1}^{\tau} \alpha_j + \rho\,\eta,$$

$$\text{(c)}\quad \Sigma'\,\lambda_i \sum_{j=1}^{\tau} \alpha_j + \rho\,\eta,$$

when restricted to $Q \times V$. Here η is some character of V which may be different for each character in β, and may be 0. Also, Σ' is a certain Gauss sum. Characters of type (c) are called exceptional, and are similar to the exceptional characters introduced in Chapter II. Only characters which are irrational on Q are considered to be exceptional, for the rational case must correspond to either type (a) or (b).

We first consider $\chi|(Q \times V)$. Since χ is rational on p-regular elements, $\chi|Q$ is rational, so we have case (a) or (b). A character of type (b) has degree

$$(q-1)\tau\alpha(1) + q\eta(1),$$

which cannot equal p, according to our assumptions on q. Hence, χ is of type (a), and η has degree 1. Let

$$\Gamma = \sum_{i=1}^{\tau} \alpha_i .$$

We have shown

$$\chi | (Q \times V) = 1_Q \Gamma + \rho\eta .$$

Note that Γ is rational valued, as χ is.

Now consider the symmetric and skew-symmetric tensor constituents of χ^2. Since, for any $g \in G$,

$$\chi'(g) = \frac{1}{2} (\chi^2(g) + \chi(g^2)),$$

$$\chi''(g) = \frac{1}{2} (\chi^2(g) - \chi(g^2)),$$

we calculate that, for $g \in Q \times V$,

$$\chi'(g) = 1_Q \Gamma'(g) + \frac{1}{2} (q-1) \rho\eta^2(g) + \rho\eta'(g) + \rho\eta\Gamma(g),$$

$$\chi''(g) = 1_Q \Gamma''(g) + \frac{1}{2} (q-1) \rho\eta^2(g) + \rho\eta''(g) + \rho\eta\Gamma(g).$$

Since Γ is rational-valued, either Γ' or Γ'' has 1_V as a constituent. Hence, either χ' or χ'' has a term $1_Q 1_V$ which does not come from a character of G of zero q-defect. The character φ of G corresponding to this term must then be of type (a). It cannot be the principal character of G, for χ is not rational-valued on P. That is, φ is a faithful character of G whose degree satisfies

$$\varphi(1) \equiv 1 \pmod{q}, \qquad p | \varphi(1),$$

$$\varphi(1) \leq \frac{1}{2} (p^2 + p).$$

This proves the first statement.

Now suppose $\chi\bar{\chi}$ has norm 2. As we have seen, χ' and χ'' must be irreducible in this case, so φ is one of them. In particular, φ has degree $\frac{1}{2}(p^2 \pm p)$, and either Γ' or Γ'' is $\tau 1_V$. This forces α to have degree 1. Since $\varphi(1) \equiv 1 \pmod{q}$, we must also have $\tau = 1$. Hence, χ has degree

$$p = \chi(1) = (q-1)\tau\alpha(1) + q\eta(1) = 2q - 1,$$

so that $q = \frac{1}{2}(p+1)$, contrary to assumption. This shows that q does not divide the order of G.

LEMMA 17. In either Case I or Case II, χ_0 has no exceptional characters as constituents.

Proof. If Case I holds, this is just Lemma 12. Suppose Case II holds. Since χ_0 is constant on P-Z, all exceptional characters have the same multiplicity in χ_0. By Lemma 8, χ_0 has norm 1+t, so we must have

$$\pm\chi_0 = \sum_{k=1}^{t} \Lambda_k - \varphi_n,$$

for some n. The Λ_k all have degree s, so equating degrees,

$$\pm p = st - \varphi_n(1) = p^2 - 1 - \varphi_n(1).$$

That is,

$$\varphi_n(1) = p^2 - 1 \pm p,$$

and

$$b_n = \pm p - 1.$$

But $b_n = -p - 1$ is contrary to $|b_n| < p$, so we have $b_n = p - 1$. Now $t \neq 1$ by Lemma 10, so $t \geq 2$, whence

$$\frac{1}{2}(p^2 - 1) \geq s \geq \sum_m b_m^2 \geq b_n^2 = (p - 1)^2$$
$$= p^2 - 2p + 1.$$

From this it follows that $p \leq 3$, contrary to hypothesis. This proves the Lemma.

Let η denote a generalized character of $\overline{G}$ whose degree is divisible by p, and let λ be a non-principal linear character of Z. Define the class function η^λ by

$$\eta^\lambda(x) = \eta(x_0)\,\lambda(x_p) \quad \text{unless } x \text{ a non-central p-element,}$$
$$= 0 \qquad\qquad x \text{ a non-central p-element,}$$

where x_0 denotes the p-regular part of x, and x_p the p-part. Note that if $(\chi | Z, \lambda)_Z \neq 0$, then $(\chi_0)^\lambda = \chi$. Brauer's characterization of characters shows that, in general, η^λ is a generalized character of G.

LEMMA 18. Suppose η is an irreducible character of $\overline{G}$ of zero p-defect (i.e., degree divisible by p^2), and η_1 is a generalized character of $\overline{G}$ whose degree is divisible by p. Let λ be a non-principal character of Z. Then

(i) η^λ is an irreducible character of G,

(ii) $(\eta^\lambda, \eta_1^\lambda) = (\eta, \eta_1)$.

Proof. Both parts follow from a calculation similar to the one used to prove Lemma 7. Note that both η and η^λ vanish on non-central p-elements.

LEMMA 19. χ_0 has no constituents of zero defect for $\bar{G}$.

Proof. Suppose, by way of contradiction, that η is an irreducible constituent of χ_0 of zero defect. Write

$$\chi_0 = n\eta + \eta_1 ,$$

where $(\eta, \eta_1) = 0$. Choose a character λ of Z so that $(\chi_0)^\lambda = \chi$. Now

$$\chi = (\chi_0)^\lambda = (n\eta + \eta_1)^\lambda = n\eta^\lambda + \eta_1^\lambda.$$

As χ is irreducible and has degree p, $(\chi, \eta^\lambda) = 0$. Thus, we have $(\eta^\lambda, \eta_1^\lambda) \neq 0$, contrary to Lemma 20.

LEMMA 20. All constituents of χ_0 are ordinary characters of $\bar{G}$.

Proof. This is an immediate consequence of Lemmas 17 and 19.

In view of this Lemma, we may define the integers a_m by

$$\chi_0 = \sum_m a_m \varphi_m.$$

LEMMA 21. We have

(i) $a_m = \frac{b_m t}{p}$ or $\frac{b_m t}{p} + 1$, for each m. In particular, each term $a_m b_m$ is non-negative.

(ii) $\sum_m a_m^2 = 1 + t.$

(iii) $\sum_m a_m b_m = p.$

Proof. Part (i) is Lemma 14. Part (ii) follows from $(\chi_0, \chi_0) = 1 + t$, which is Lemma 8. Part (iii) may be proved by observing that , as ζ vanishes off P-Z,

$$(\chi_0, \zeta) = (p\varphi_1, \zeta) = pt,$$

on the one hand, while

$$(\chi_0, \zeta) = \sum_m a_m(\varphi_m, \zeta) = \sum_m a_m b_m t,$$

on the other.

CHAPTER IV

NUMERICAL RESULTS

In this Chapter, we use the results of Chapter III to investigate the minimal counterexample G to Theorem 1. From Chapter II, we see that $p \leq 31$, and the values of s and t are quite restricted. We treat the possibilities for p individually. First note that Theorem 1 is proved for p = 5 and 7 in [3] and [12], [13], and [14]. We may assume $p \geq 11$.

LEMMA 22. We have $p \neq 11$.

Proof. First say Case I holds. By Lemma 13, t is odd, and by Lemma 10, $t \neq 1$. As t divides $p^2 - 1 = 120$, we must have t = 3 or 5. If t = 3, then s = 40, but SL(2,11) has no subgroup of this order. Hence, t = 5, and s = 24.

From the proof of Lemma 14, we have

$$121 = p^2 \geq t(rt-\delta)^2 = 5(5r-\delta)^2,$$

whence $|5r-\delta| \leq 4$. As $r \neq 0$, we have $r = \delta$. Furthermore,

$$25 = s + 1 = \sum_m b_m^2 + (t-1)r^2 + (r-\delta)^2$$

$$= \sum_m b_m^2 + 4,$$

so that

$$\sum_m b_m^2 = 21$$

and

$$\sum_{a_m \neq 0} b_m^2 \leq 21.$$

Now, Lemma 21 shows

$$\sum_m a_m^2 = 1 + t = 6,$$

$$\sum_m a_m b_m = p = 11,$$

with each term $a_m b_m \geq 0$.

An easy analysis of cases yields only the following two solutions for the set of $|a_m|$ and the set of $|b_m|$ such that $a_m \neq 0$.

$\|a_m\|$	$\|b_m\|$	$\|a_m\|$	$\|b_m\|$
1	2	2	4
1	2	1	2
1	2	1	1
1	2		
1	2		
1	1		

Both of these have

$$\sum_{a_m \neq 0} b_m^2 = 21,$$

so the values of $|b_m|$ above are the only ones which occur. However, recall that $b_1 = 1$ and $b_2 = -1$. There must be two values $|b_m|$ which are 1. This contradiction proves the Lemma in Case I.

For Case II, we have $t^2 \leq s$, $t \neq 1$, and $t | (p^2-1)$. There are no solutions, so Case II cannot occur either, as s must be the order of a subgroup of SL(2,11).

LEMMA 23. We have $p \neq 17$.

Proof. Case I is eliminated by observing that $t \mid (p^2-1)$, $t \neq 1$, $t(t-1)^2 \leq p^2$, and t odd leave only $t = 3$, so $s = 96$, while SL(2,17) has no subgroup of order 96.

Applying the argument of Lemma 22 for Case II, we now find possible values for t and s, namely, $t = 6$ and $s = 48$, for N/P the proper covering of S_4. From Leonard [8], we see that each positive b_m is less than or equal to some irreducible degree of this while the Corollary to Lemma 1 shows that some b_m is at least 6. This is a contradiction.

For $p = 13$, we may eliminate Case I as in Lemma 23, and Case II as in Lemma 24.

The table given in Chapter II shows that we have now eliminated all possibilities for N/P except SL(2,5). In all remaining cases, $s = 120$ and t is uniquely determined by p, for $120s = p^2-1$. In particular, 5 divides either $p+1$ Or $p-1$. This eliminates $p = 23$, so it remains only to consider $p = 19$, 29, and 31.

LEMMA 24. If Case II holds, we have $p = 19$. If Case I holds, $p \neq 31$.

Proof. Suppose $p = 31$, so $t = 8$. As t is odd in Case I, this possibility is eliminated. Thus, say Case II holds. By Lemma 1, there is an integer $a_{ijk} \leq (s-n)/t$, and by Lemma 2, we may choose $n \geq 2$. Hence, we may actually choose $n = 8$. Now Lemma 1 shows $49 \times 64 \leq s = 120$, a contradiction. The Case $p = 29$ is handled similarly in Case II.

LEMMA 25. We have $p \neq 19$.

Proof. Choose a conjugate χ^σ of χ such that $\chi^\sigma \chi^2$ has Z in its kernel. Write

$$(\chi^\sigma \chi'', \chi_0) = (\chi'', \bar{\chi}^\sigma \chi_0) = (\chi'', \chi^2) > 0.$$

Thus, $\chi^\sigma \chi''$ has an irreducible constituent ω_n in common with χ_0, and $(\varphi_n, \chi_0) > 0$. This character is an ordinary character by Lemma 20, and has positive b_n by Lemma 14. We will show that there is no possibility for $\varphi_n(1) = ep^2 + b_n$. Note that $b_n \leq 10$, as $b_n^2 \leq s = 120$, and that $e \leq 8$, as $\varphi_n(1) < \chi^\sigma(1)\chi''(1) = 9 \times 19^2$.

Since χ is rational on 19-regular elements, it must be that the order of G is divisible only by primes less than or equal to 19. In fact, if q is a prime other than 19, a theorem of Schur tells us that the power to which q occurs in $|G|$ is at most

$$\left[\frac{19}{q-1}\right] + \left[\frac{19}{q(q-1)}\right] + \left[\frac{19}{q^2(q-1)}\right] + \cdots,$$

where square brackets denote the greatest integer function. Furthermore, Lemma 16 shows that neither 13 nor 17 divide the order of G.

Calculation shows that no integer of the form $19^2e + b_n$, with e and b_n as above, divides $|G|$ as described. As there is no possible value for $\varphi_n(1)$, we have proved the Lemma.

LEMMA 26. We have $p \neq 29$.

Proof. Note that if p = 29, we must have Case I. We apply the technique of Lemma 27 to find the common constituent of $\chi^\sigma\chi''$ and χ_0. Here $b \leq 10$ and $e \leq 13$. Further, we look for a common constituent of $\chi^\sigma\chi'$ and χ_0, with $b \leq 10$ again, and $e \leq 14$. Only the following six degrees occur.

$$\begin{aligned}
29^2 + 4 &= 845 \\
29^2 + 6 &= 847 \\
2 \times 29^2 + 8 &= 1690 \\
11 \times 29^2 + 1 &= 9252 \\
11 \times 29^2 + 10 &= 9261 \\
13 \times 29^2 + 2 &= 10935.
\end{aligned}$$

We claim that 9261 cannot be the degree of an irreducible constituent φ of $\chi^{\sigma}\chi'$ or $\chi^{\sigma}\chi''$. The restriction $\varphi|N$ is of the form $a\xi + \theta$, for some positive integer a and some character θ with no faithful constituents for $\overline{N}$. Here θ has degree at least 21, but we know that $\chi^{\sigma}\chi'|N = \theta' + 15\xi$, where θ' has degree 15. We get a similar contradiction for $\chi^{\sigma}\chi''$. The same sort of argument shows 10935 does not occur for $\chi^{\sigma}\chi''$.

Now observe that

$$(25\chi_0 - \zeta,\ 25\chi_0 - \zeta) = 625\times 8 - 50\times 29\times 7 + 29^2\times 8$$
$$= 737.$$

We know that for any exceptional Λ, we have $(\Lambda, \chi_0) = 0$, and $(\Lambda, \zeta) = rt-\delta$. Thus, since there are t exceptional characters,

$$t(rt-\delta)^2 = 7(7r-\delta)^2 \leq 737,$$

$$(7r-\delta)^2 \leq 106.$$

This forces $|7r-\delta| = 8$ or 6, as $r \neq 0$. We can now account for at least $7\times 6^2 = 252$ out of the norm of $25\chi_0 - \zeta$. Also, φ_1 and φ_2 do not occur in χ_0, and so each account for 49 towards this norm. Hence, we must still account for at most 737 - 340 = 387. This will be useful several times in the argument.

Except for exactly five values of m, a_m and b_m have the same parity. Two of these are, of course, m = 1 and 2. The other three are the constituents of $\chi_2 - \chi_0$. Indeed, the multiplicity of φ_m in χ_2 is of the same parity as in χ_0^2, and this is $b_m t$ if $m \neq 1,2$. Thus, a_m and b_m have different parity exactly when $(\varphi_m, \chi_2 - \chi_0) \neq 0$, or m = 1 or 2. We will use this fact often.

Our third tool is a consequence of the Cauchy-Schwarz inequality. Write

$$841 = 29^2 = \Big(\sum_{a_m \neq 0} a_m b_m \Big)^2$$

$$\leq \Big(\sum_{a_m \neq 0} a_m^2 \Big) \Big(\sum_{a_m \neq 0} b_m^2 \Big)$$

$$= 8 \sum_{a_m \neq 0} b_m^2 ,$$

so that

$$105 < \sum_{a_m \neq 0} b_m^2 .$$

We use the above to help show there is no m such that $a_m b_m = 1$. Such an m would imply a contribution of another $(25\ a_m - tb_m)^2 = (25 - 7)^2 = 18^2 = 324$, leaving only 387 - 324 = 63 unaccounted for. For all other m, we must have

$$(25a_m - 7b_m)^2 \leq 63,$$

so

$$|25a_m - 7b_m| < 8.$$

For given $|a_m|$, the value of $|b_m|$ must lie in the range indicated.

$\lvert a_m \rvert$	$\lvert b_m \rvert$
0	1
1	3 or 4
2	7 or 8

Suppose first that no $|a_m| = 2$. Let a be the number of constituents of χ_0 with $|b_m| = 4$, and b the number with $|b_m| = 3$. We have from Lemma 21 that

$$4a + 3b = 28,$$
$$16a + 9b \geq 105,$$
$$a + b = 7.$$

We find $a > 5$, but we have seen above that there are at most three values m other than 1 and 2 for which a_m and b_m have different parity. This provides a contradiction.

Now suppose some $|a_m| = 2$. All other $|a_m|$ are 1. Here we have

$$4a + 3b \geq 12,$$
$$a + b = 3,$$

forcing $a = 3$, $b = 0$. Now we find all constituents of $\chi_2 - \chi_0$ have $b_m = \pm 4$. As this character has degree 0, this cannot happen. This final contradiction shows that in no case do we have $a_m b_m = 1$. Hence, by Lemma 14, if $b_m = \pm 1$, we have $a_m = 0$. In particular, this eliminates 9252 as an irreducible degree in χ_0.

We now consider each of the possible pairs of degrees from our list of four remaining which can arise from $\chi^\sigma \chi'$ or $\chi^\sigma \chi''$. Note that these two characters have no common constituents by Lemma 9, except possibly some exceptionals. The object is to try to extend the pair into lists of $|a_m|$ and $|b_m|$, subject to the above, and Lemma 21. The arguments here are similar to those used to show no $a_m b_m = 1$, and to those used for Case I of Lemma 22. In only two cases do these arguments not suffice. These can both be eliminated in essentially the same way, so we do the harder one.

The set to consider is

$$8, 5, 4, 2, 2, 1, 1,$$

which satisfies all the above conditions. In this case we have $rt-\delta = \pm 6$. The table below allows us to compute certain inner products. For each of the above values of b_m, we list the absolute values of the multiplicities in the indicated generalized characters. Note that although we do not know the signs of these multiplicities, they are in each case of the same sign as b_m. That is , the entries of any row all have the same sign. For χ_0^2, we list the sum of the multiplicities in χ_0' and χ_0''. We know both of these values because we know their sum and difference, but, because of the ambiguity of signs, we do not know which is which. Our goal is to show that no possible choice of multiplicities for χ_0' is consistent.

b_m	χ_0	χ_2	χ_0^2
8	2	2	27+29
5	1	1	17+18
4	1	0 or 2	14+14 or 13+15
2	1	0 or 2	7+7 or 6+8
2	1	0 or 2	7+7 or 6+8
1	0	0	4+4
1	0	0	3+3

The inner products we will check are

$$(\chi_0', \chi_0') = 1 + \tfrac{1}{2}(p+1)^2 t = 1576,$$

$$(\chi_0', \chi_2) = 1 + \tfrac{1}{2}(p+1)\, t = 106,$$

according to Lemma 7. Note that the inner product with χ_2 is even, so the multiplicity in χ_0' of the character with $b_m = \pm 5$ must be 18. Suppose first that the character with $b_m = 8$ has multiplicity 27 in χ_0'. Then it is easy to see that none of the possible choices of multiplicities for the remaining three characters gives the correct inner product with χ_2. Thus, the character with $b_m = 8$ has multiplicity 29 in χ_0'. Now, checking the inner product with χ_2, we find only the two possibilities

b_m	χ_0'	or χ_0'
8	29	29
5	18	18
4	15	?
2	?	7
2	?	8
1	4	4
1	3	3

There are many ways to fill in the unknown entries, but none of these satisfies $(\chi_0', \chi_0') = 1576$, as is easily checked. Note that here we must also consider the contribution $7 \times 3^2 = 63$ from the exceptional characters.

The same method eliminates the set

$$8, 5, 3, 3, 2, 1, 1, 1, 1,$$

which also occurs. With these arguments, the proof of Theorem 1 is complete.

REFERENCES

[1] Blichfeldt, H. F., Finite Collineation Groups, University of Chicago Press, Chicago, 1917.

[2] Brauer, R., "On Groups whose Order Contains a Prime to the First Power I, II", Am. J. Math. 64(1942), 401-420, 421-440.

[3] Brauer, R., "Uber endliche lineare Gruppen von Primzahlgrad", Math. Annalen 169 (1967), 73-96.

[4] Brauer, R. and Leonard, H., "On finite groups with an abelian Sylow group", Canad. J. Math. 14 (1962), 436-450.

[5] Feit, W., Characters of Finite Groups, Benjamin, New York, 1967.

[6] Feit, W., The Current Situation In The Theory Of Finite Simple Groups, to appear.

[7] Feit, W., Unpublished work.

[8] Leonard, H. S., " Finite Linear Groups Having an Abelian Sylow Subgroup", J. Algebra 20 (1972), 57-69.

[9] Lindsey, J., "Finite Linear Groups of Prime Degree", Math. Annalen 189 (1970), 47-59.

[10] Lindsey, J., "Finite Linear Groups of Degree 6", to appear.

[11] Schur, I., "Uber eine Klasse von endlichen Gruppen linearer Substitutionen", Sitzber. Preuss. Akad. Wiss. Berlin (1905), 77-91.

[12] Wales, D., "Finite Linear Groups of Prime Degree", Canad. J. Math. 21 (1969), 1025-1041.

[13] Wales, D., "Finite Linear Groups of Degree Seven.I", Canad. J. Math. 21 (1969), 1042-1056.

[14] Wales, D., "Finite Linear Groups of Degree Seven.II", Pacific J. Math. 34 (1970), 207-235.