

FINITE GROUPS WITH PRIME p TO THE FIRST POWER

BY

ZON-I CHANG⁽¹⁾

ABSTRACT. Earlier D. G. Higman classified the finite groups of order n , such that n is divisible by 3 to the first power, with the assumption that the centralizer $C_G(X)$ of X , where X is a subgroup of order 3, is a cyclic trivial intersection set of even order $3s$. In this paper the theorem is generalized to include all prime numbers greater than 3. With an additional assumption: $|N_G(X) : C_G(X)| = 2$, we have proved that one of the following holds for these groups, hereafter designated as G :

- (A) G is isomorphic to $L_2(q)$, where $q = 2ps \pm 1$;
- (B) there exists a normal subgroup G_0 of odd index in G , and a normal subgroup N of G_0 of index 2 such that $G = N\langle\sigma\rangle$ where $C_G(X) = X \times \langle\sigma\rangle$.

1. Introduction. The problem of finite simple groups has been investigated by many workers. This paper is another effort in this general area. Earlier D. G. Higman proved that a nonabelian simple group having a Sylow subgroup of order 3 whose centralizer is a cyclic trivial intersection set of even order is isomorphic to $L_2(q)$ for suitable odd q . In this paper the theorem is generalized to include all prime numbers greater than 3. More precisely, we have proved the following theorem.

THEOREM. *Let G be a finite group and p be a prime number greater than 3 such that $p \nmid |G|$, and let X be a subgroup of order p . Assume that the centralizer $C_G(X)$ of X in G is a cyclic trivial intersection set of even order ps , and that $|N_G(X) : C_G(X)| = 2$. Then one of the following holds:*

- (A) G is isomorphic to $L_2(q)$, $q = 2ps \pm 1$;
- (B) *there exists a normal subgroup G_0 of odd index in G , and a normal subgroup N of G_0 of index 2 such that $G = N\langle\sigma\rangle$ where $C_G(X) = X \times \langle\sigma\rangle$.*

The main theorem of this paper reduces to the theorem of Higman when the prime p is three. We remark that if $p = 3$, the assumption $|N_G(X) : C_G(X)| = 2$ can be dropped. The only possibility for G other than (A) and (B) of the

Received by the editors July 10, 1974.

AMS (MOS) subject classifications (1970). Primary 20D05, 20G40; Secondary 20C15, 20C20.

Key words and phrases. Trivial intersection set, p -blocks of defect 1, irreducible characters of defect 0.

⁽¹⁾This work was completed at the University of Illinois at Urbana-Champaign, 1973–1974, and appeared as a part of the author's Ph.D. thesis, under the supervision of Michio Suzuki. The author wishes to express his deepest gratitude to Michio Suzuki, for his guidance, enormous patience and encouragement during the preparation of this work.

theorem is that G may have a normal 3-complement.

In the proof of the theorem we let $X = \langle x \rangle$, $C_G(X) = X \times \langle \sigma \rangle$, and $\pi = \sigma^{s/2}$. There are two cases:

Case (1). The element $x\sigma$ is a product of two conjugates of π .

In this case we show that G is isomorphic to $L_2(q)$, $q = 2ps \pm 1$, by an application of a theorem of Brauer, Suzuki, and Wall [2]. This is done in §2.

Case (2). The element $x\sigma$ cannot be written as a product of two conjugates of π .

To deal with this case, in §3, we use two theorems of Curtis and Reiner [7] to determine the characters of $N_G(X)$. In §4, by using Brauer's results [1] for groups with prime p to the first power, and the assumption that $C_G(X)$ is a trivial intersection set, we are able to determine the p -blocks of defect 1, and obtain two columns in the character table of interest. Finally, in §5, by applying Burnside's theorem, we prove the existence of a normal subgroup G_0 as described in (B) of the theorem, with the property that, replacing G by G_0 , it can be assumed that the fixed point group of $N_G(X)/C_G(X)$ acting on $\langle \sigma \rangle$ has 2-power order. The existence of the desired subgroup of index 2 is obtained by using the p -blocks of defect 1 which are determined in §4, and applying the well-known formula for the multiplication constants of the class algebra in terms of the characters.

Unfortunately, at this moment the classification of the finite groups which contain a self-centralizing subgroup of order p has not been determined, but the classification has been achieved in interesting special cases in Leo J. Alex's papers [8], [9], [10].

2. Proof of the theorem in Case (1). We now begin the proof of the theorem stated in the introduction. Assume the notations and hypotheses of the theorem.

Let $X = \langle x \rangle$, $x^p = 1$, $C_G(X) = X \times \langle \sigma \rangle = \langle x\sigma \rangle = \langle y \rangle$, $\sigma^s = 1$, and let $\pi = \sigma^{s/2}$.

Before we start to prove the theorem in Case (1), first we prove the following two general lemmas.

LEMMA 2.1. *The centralizer $C_G(\pi)$ is equal to the normalizer $N_G(X)$.*

PROOF. Since $C_G(X)$ is a trivial intersection set, we have $C_G(\pi) \subseteq N_G(C_G(X))$. Since $C_G(X) = X \times \langle \sigma \rangle$, it follows that $C_G(\pi) \subseteq N_G(X)$. Conversely, since $C_G(X)$ is cyclic, it has only one element of order 2. Hence, since $C_G(X)$ is a normal subgroup of $N_G(X)$, we see that $N_G(X) \subseteq C_G(\pi)$. It follows that $C_G(\pi) = N_G(X)$.

LEMMA 2.2. *Let q be an odd prime divisor of $|\langle y \rangle|$ and Q be a Sylow q -*

subgroup of $\langle y \rangle$. Then $N_G(Q) = N_G(\langle y \rangle) = C_G(\pi)$, and Q is a Sylow q -subgroup of G .

PROOF. Lemma 2.1 implies that $C_G(\pi) \subseteq N_G(\langle y \rangle) \subseteq N_G(Q)$. Since $\langle y \rangle$ is a trivial intersection set, we see that $N_G(Q) \subseteq N_G(\langle y \rangle) \subseteq N_G(X) = C_G(\pi)$. Hence $N_G(Q) = N_G(\langle y \rangle) = C_G(\pi)$. Furthermore, since Q is a Sylow subgroup of $N_G(Q)$, Q must be a Sylow subgroup of G .

Next, we are going to prove the theorem in Case (1).

In Case (1) we assume that $y = x\sigma$ is a product of two conjugates α and τ of π .

In the following lemmas, except Lemma 2.5, we are going to use all the above hypotheses and notations.

LEMMA 2.3. *The centralizer $C_G(\pi)$ is dihedral and $C_G(\pi) = N_G(X) = \langle y, \tau \rangle$, $y^\tau = y^{-1}$.*

PROOF. By Lemma 2.1, we have $C_G(\pi) = N_G(X)$. It is easy to see that $\langle y \rangle$ is a normal subgroup of $\langle \alpha, \tau \rangle$, $y^\tau = y^{-1}$, and $\pi^\tau = \pi^{-1} = \pi$. So $r \in C_G(\pi)$. Also it is clear that $\tau \notin C_G(X)$. This completes the proof of Lemma 2.3.

LEMMA 2.4. *The classes of involutions in $C_G(\pi)$ are represented by π , τ , and $y\tau$.*

PROOF. By Lemma 2.3, $C_G(\pi) = \langle y, \tau \rangle$, and $y^\tau = y^{-1}$. Hence every element of $C_G(\pi)$ can be expressed in the form $y^i \tau^j$ where i is a nonnegative integer, and $j = 0$ or 1 . If $j = 0$, it is easy to see that the only class of involutions which intersects $\langle y \rangle$ is $\{\pi\}$. If $j = 1$, then every element of the form $y^i \tau$ is an involution. Let m be a nonnegative integer, we see that $y^{2m} \tau$ and $y^{2m+1} \tau$ are conjugate to τ and $y\tau$, respectively. Therefore, there are two classes of involutions represented by τ and $y\tau$ in the case $j = 1$. Hence the classes of involutions in $C_G(\pi)$ are represented by π , τ , and $y\tau = \alpha\tau\tau = \alpha$. This completes the proof of Lemma 2.4.

LEMMA 2.5. *Assume in general that $C_G(\pi)$ is dihedral of order $2t$ for some involution π in a finite group G . Let $y \in C_G(\pi)$ be of order t with $\pi = y^{t/2}$. Then the following conditions are equivalent:*

- (1) *the element y is a product of two conjugates of π ;*
- (2) *the involutions in $C_G(\pi)$ are conjugate in G ;*
- (3) *G has just one class of involutions.*

If (1)–(3) hold, then G has dihedral Sylow 2-subgroups.

PROOF. First we show that condition (1) implies condition (2). Suppose that $y = \alpha\tau$ where α and τ are conjugates of π . By Lemma 2.4, we know that

the classes of involutions in $C_G(\pi)$ are represented by π , τ , and α . Hence the involutions in $C_G(\pi)$ are conjugate in G .

Secondly we show that condition (2) implies condition (3). If μ is an involution in G which is not conjugate to π , then there exists an involution ρ such that $\rho \in C_G(\pi) \cap C_G(\mu)$. Then by (2), ρ is conjugate to π and hence μ is conjugate to ρ . It follows that μ is conjugate to π . This is a contradiction.

Finally we show that condition (3) implies condition (1). Since $C_G(\pi)$ is dihedral, y is a product of two involutions. It follows that if there is only one class of involutions in G , then y is a product of two involutions which are conjugates of π . Therefore, the three conditions stated in the lemma are equivalent.

If G has only one class of involutions, then the dihedral group $C_G(\pi)$ contains a Sylow 2-subgroup of G . Hence G has dihedral Sylow 2-subgroups.

LEMMA 2.6. *In Case (1), G is isomorphic to $L_2(q)$ where $q = 2ps \pm 1$.*

PROOF. We show that G is simple. Assume on the contrary that G is not simple. Let M be a nontrivial minimal normal subgroup of G .

By Lemma 2.3, we know that $C_G(\pi)$ is dihedral, and $C_G(\pi) = \langle y, \tau \rangle$, $y^\tau = y^{-1}$.

Now we show that $M \cap C_G(\pi) \neq \{1\}$. If $M \cap C_G(\pi) = \{1\}$, then π acts fixed point free on M , hence so do τ and $\pi\tau$. It follows that π inverts every element of M , and hence τ and $\pi\tau$ invert every element of M . Then if $\mu \in M$, we have $\mu^{-1} = \mu^{\pi\tau} = (\mu^{-1})^\tau = \mu$. It follows that $\pi\tau$ fixes μ , which implies that $\mu = 1$. Therefore, $M = \{1\}$; this is a contradiction.

If $|M|$ is even, then there exists an involution in M . By Lemma 2.5, we see that τ and $y\tau = \alpha$ belong to M . From $C_G(\pi) = \langle y, \tau \rangle$ and $y = \alpha\tau$, we see that $C_G(\pi) \subseteq M$.

By assumption, we know that $|C_G(\pi)|$ is not a 2-power. It follows that there is an odd prime q dividing $|M \cap C_G(\pi)|$. Now let Q be a Sylow q -subgroup of $\langle y \rangle$. By Lemma 2.2, we have $N_G(Q) = N_G(\langle y \rangle) = C_G(\pi)$, and Q is a Sylow q -subgroup of G . It follows that $M \cap Q$ is a Sylow q -subgroup of M and M is simple. By the same argument as Lemma 2.2, we see that $N_G(M \cap Q) = C_G(\pi)$; and hence $G = MC_G(\pi)$. If $|M|$ is odd, then $N_M(M \cap Q) = M \cap C_G(\pi) = M \cap \langle y \rangle = C_M(M \cap Q)$. By Burnside's theorem, M has a normal q -complement. It follows that $M \subseteq Q \subseteq C_G(\pi)$ and thus $G = MC_G(\pi) = C_G(\pi)$, which is impossible since G has a single class of involutions. Thus $|M|$ is even, so $C_G(\pi) \subseteq M$, and hence $G = MC_G(\pi) = M$. Consequently, G is simple. By the theorem of Brauer, Suzuki, and Wall [2], we know that G is isomorphic to $L_2(q)$ where $q = 2ps \pm 1$.

3. The characters of $N_G(X)$. In this section, we begin the preparations for the proof in Case (2). Again G is to be a finite group such that $p \parallel |G|$ and X is

a subgroup of order p . We assume that $C_G(X)$ is a cyclic group of even order ps and that $|N_G(X) : C_G(X)| = 2$.

We have $C_G(X) = X \times \langle \sigma \rangle = \langle y \rangle$, $X = \langle x \rangle$, $y = x\sigma$, where x is of order p , and σ is of order s . Also we have $N_G(X) = \langle X, \sigma, \tau \rangle$ with $x^\tau = x^{-1}$, $\tau^2 \in \langle \sigma \rangle$, $\sigma^\tau = \sigma^t$, and $t^2 \equiv 1 \pmod{s}$.

We proceed by proving the following lemmas.

LEMMA 3.1. *Let e be the least positive integer such that σ^e is a generator of the fixed point of τ acting on $\langle \sigma \rangle$. Also let $f = (s, t - 1)$; here we use the convention that $(s, 0) = s$. Then $ef = s$.*

PROOF. Since $\langle \sigma^e \rangle$ is a subgroup of $\langle \sigma \rangle$, so $e|s$. By assumption, we have $(\sigma^e)^\tau = \sigma^e$. Since $\sigma^\tau = \sigma^t$, we have $\sigma^{et} = \sigma^e$ or $et \equiv e \pmod{s}$. This is equivalent to saying $e(s, t - 1)$ is divisible by s . That is, $e(s, t - 1) = sn$, for some positive integer n . Since we want e to be the least positive integer so that σ^e is a generator of the fixed point group of τ acting on $\langle \sigma \rangle$, hence $e(s, t - 1) = s$, that is, $ef = s$.

REMARK. By Lemma 3.1, we know that $\langle \sigma^e \rangle$ is of order f . Since τ fixes involutions in $\langle \sigma \rangle$, f is certainly even.

LEMMA 3.2. *The positive integer e is equal to $(s, (t + 1))/d$ where $d = 1$ if $t^2 - 1 \not\equiv 0 \pmod{2s}$, and $d = 2$ if $t^2 - 1 \equiv 0 \pmod{2s}$.*

PROOF. Clearly we have $s|(s, t + 1)(s, t - 1)$. It follows that $(s, t + 1)(s, t - 1) = sn$, where n is a positive integer. We want to show that $n = 1$ if $t^2 - 1 \not\equiv 0 \pmod{2s}$, and $n = 2$ if $t^2 - 1 \equiv 0 \pmod{2s}$.

First, if $t^2 - 1 \not\equiv 0 \pmod{2s}$, then n is odd. But clearly $(t + 1, t - 1) = 2$. Hence $n = 1$, since every prime divisor of n would be a divisor of s .

Next, if $t^2 - 1 \equiv 0 \pmod{2s}$, then n is even. By reasoning just as in the first case we find that $n = 2$. This completes the proof of the lemma.

Let ζ be a primitive s th root of unity so that $\phi_i(\sigma^j) = \zeta^{ij}$, $0 \leq i, j < s$, define s distinct linear characters of $\langle \sigma \rangle$.

Let ω be a primitive p th root of unity so that $\rho_m(x) = \omega^m$ and $\bar{\rho}_m(x) = \bar{\omega}^m$, $0 \leq m \leq (p - 1)/2$, define the p distinct linear characters of $X = \langle x \rangle$, where the bar denotes the complex conjugate.

Let ξ be a primitive ps th root of unity so that $\theta_k(y) = \xi^k$, $0 \leq k < ps$, define the ps distinct linear characters of $C_G(X) = \langle y \rangle$. We may choose ξ , ζ , and ω so that $\xi = \omega\zeta$ and $\theta_{pi} = \phi_i$, $0 \leq i < s$.

Now since $y^\tau = y^r$ for some positive integer r , we have $(x\sigma)^\tau = (x\sigma)^r$. It follows that $x^{-1}\sigma^t = x^r\sigma^r$; hence $r \equiv p - 1 \pmod{p}$ and $r \equiv t \pmod{s}$. Also, we know that for given i , $i \equiv it \pmod{s}$ if and only if $i(t - 1) \equiv 0 \pmod{s}$; this last

condition is equivalent to $e \nmid i$ because $s = ef$ and $f = (s, t - 1)$.

We will use \sim to denote induction to $N_G(X)$.

LEMMA 3.3. *The character $\tilde{\theta}_{pi} = \widetilde{1\phi_i}$, $0 \leq i < s$, is irreducible if and only if $e \nmid i$.*

PROOF. By [7, Theorem 47.8], we know that $\tilde{\theta}_{pi}$ is irreducible if and only if $r(pi) \not\equiv pi \pmod{ps}$, which leads to the equivalent conditions: $ri \not\equiv i \pmod{s}$, $ti \not\equiv i \pmod{s}$, and $i(t-1) \not\equiv 0 \pmod{s}$. The last condition then gives us the desired equivalent result, $e \nmid i$.

LEMMA 3.4. *The character $\tilde{\theta}_{pei} = \widetilde{1\phi_{ie}}$, $0 \leq i < f$, decomposes into $\lambda_{i1} + \lambda_{i2}$, where λ_{i1} and λ_{i2} are distinct linear characters of $N_G(X)$.*

PROOF. Lemma 3.3 implies that $\tilde{\theta}_{pei}$ is reducible; also since $|N_G(X) : C_G(X)| = 2$, we see that the degree of $\tilde{\theta}_{pei}$ is 2. It follows that $\tilde{\theta}_{pei} = \lambda_{i1} + \lambda_{i2}$, $0 \leq i < f$, where λ_{i1} and λ_{i2} are linear characters of $N_G(X)$. Furthermore, since $\tilde{\theta}_{pei}(\tau) = 0$, we see that λ_{i1} and λ_{i2} , $0 \leq i < f$, are distinct.

LEMMA 3.5. *The characters $\tilde{\theta}_{pei}$ and $\tilde{\theta}_{pei'}$ are orthogonal if $i \neq i'$ where $0 \leq i, i' < f$.*

PROOF. Since

$$(\tilde{\theta}_{pei}, \tilde{\theta}_{pei'})_{N_G(X)} = (\theta_{pei}, \tilde{\theta}_{pei'}|_{C_G(X)})_{C_G(X)} = 0,$$

$\tilde{\theta}_{pei}$ and $\tilde{\theta}_{pei'}$, $0 \leq i, i' < f$, are orthogonal if $i \neq i'$. This completes the proof of the lemma.

REMARK. From Lemma 3.4 and Lemma 3.5, we know that $\tilde{\theta}_{pei} = \widetilde{1\phi_{ie}} = \lambda_{i1} + \lambda_{i2}$, $0 \leq i < f$, give $2f$ distinct linear characters of $N_G(X)$.

LEMMA 3.6. *The character $\widetilde{1\phi_i}$, $0 < i < s$, is irreducible of degree 2 if $e \nmid i$. These give $(s-f)/2$ distinct irreducible characters.*

PROOF. By Lemma 3.3 and Lemma 3.4, we know that $\widetilde{1\phi_i}$, $0 < i < s$, $e \nmid i$, is irreducible of degree 2.

By [7, Theorem 47.9], we know that for $i \neq i'$, $0 < i, i' < s$, $\widetilde{1\phi_i}$ is inequivalent to $\widetilde{1\phi_{i'}}$ if and only if $r(pi) \not\equiv pi' \pmod{ps}$, which is equivalent to $ri \not\equiv i' \pmod{s}$, and then $ti \not\equiv i' \pmod{s}$.

If $\widetilde{1\phi_{i1}}$ is equivalent to $\widetilde{1\phi_{i2}}$, and $\widetilde{1\phi_{i2}}$ is equivalent to $\widetilde{1\phi_{i3}}$, then it is obvious that $ti_1 \equiv i_2 \pmod{s}$ and $ti_2 \equiv i_3 \pmod{s}$. It now follows that $i_1 \equiv t^2 i_1 \equiv ti_2 \equiv i_3 \pmod{s}$. Therefore, $\widetilde{1\phi_i}$, $0 < i < s$, $e \nmid i$, give $(s-f)/2$ distinct irreducible characters.

LEMMA 3.7. *The character $\widetilde{\rho_m \phi_i}$, $0 \leq i < s$, $1 \leq m \leq (p-1)/2$, is irreducible.*

ible of degree 2. These give the remaining $s(p-1)/2$ irreducible characters of $N_G(X)$.

PROOF. The linear characters $\rho_m \phi_i$ and $y^j \rightarrow \rho_m \phi_i(y^j)^\tau$ are distinct since $m \geq 1$. Hence, by [7, Corollary 45.5], $\widetilde{\rho_m \phi_i}$ is irreducible of degree 2 when $1 \leq m \leq (p-1)/2$, $0 \leq i < s$.

We have

$$\begin{aligned} 2ps = |N_G(X)| &= (2f)(1^2) + ((s-f)/2)(2^2) + (s(p-1)/2)(2^2) \\ &= 2f + 2(s-f) + 2s(p-1) = 2ps. \end{aligned}$$

So $\widetilde{\rho_m \phi_i}$, $1 \leq m \leq (p-1)/2$, $0 \leq i < s$, are the remaining $s(p-1)/2$ irreducible characters of $N_G(X)$.

LEMMA 3.8. The character $\widetilde{\rho_m \phi_i}$, $1 \leq m \leq (p-1)/2$, $0 \leq i < s$, is equivalent to $\widetilde{\rho_m \phi_{ti}}$.

PROOF. Both of the characters $\widetilde{\rho_m \phi_i}$ and $\widetilde{\rho_m \phi_{ti}}$ vanish on $N_G(X) - C_G(X)$. Furthermore, their restrictions to $C_G(X)$ have exactly the same constituents. Hence they are equal.

The $(s+f)/2$ p -blocks of $N_G(X)$ (all of defect 1) are

$$b_{ie} = \{\lambda_{i1}, \lambda_{i2}\} \cup \{\widetilde{\rho_m \phi_{ie}} \mid 1 \leq m \leq (p-1)/2\},$$

where $0 \leq i < f$, and

$$\begin{aligned} b_i = b_{ti} &= \{\widetilde{1\phi_i}\} \cup \{\widetilde{\rho_m \phi_i} \mid 1 \leq m \leq (p-1)/2\} \\ &\cup \{\widetilde{\rho_m \phi_i} \mid 1 \leq m \leq (p-1)/2\} \end{aligned}$$

where $e \nmid i$, $0 < i < s$.

Next we are going to compute some of the characters of $N_G(X)$ that will be needed later.

By Clifford's theorem, we have

$$\begin{aligned} \widetilde{1\phi_{ie}}|_{C_G(X)} &= 2\phi_{ie}; \\ \widetilde{\rho_m \phi_{ie}}|_{C_G(X)} &= \rho_m \phi_{ie} + \bar{\rho}_m \phi_{ie}; \\ \widetilde{1\phi_i}|_{C_G(X)} &= \phi_i + \phi_{it}; \\ \widetilde{\rho_m \phi_i}|_{C_G(X)} &= \rho_m \phi_i + \bar{\rho}_m \phi_{it}; \\ \widetilde{\bar{\rho}_m \phi_i}|_{C_G(X)} &= \widetilde{\rho_m \phi_{ti}}|_{C_G(X)} = \bar{\rho}_m \phi_i + \rho_m \phi_{it}. \end{aligned}$$

By using this information, the part of the character table of $N_G(X)$ that is of interest to us is obtained as follows:

TABLE I

	σ^j	$x\sigma^j$
λ_{i1}	ζ^{ije}	$\zeta^{ije} \quad 0 \leq i < f$
λ_{i2}	ζ^{ije}	$\zeta^{ije} \quad 1 \leq m \leq (p-1)/2$
$\widetilde{\rho_m \phi_{ie}}$	$2\zeta^{ije}$	$(\omega^m + \omega^{-m})\zeta^{ije}$
$\widetilde{1\phi_i}$	$\zeta^{ij} + \zeta^{ijt}$	$\zeta^{ij} + \zeta^{ijt} \quad e \nmid i$
$\widetilde{\rho_m \phi_i}$	$\zeta^{ij} + \zeta^{ijt}$	$\omega^m \zeta^{ij} + \omega^{-m} \zeta^{ijt} \quad 0 < i < s$
$\widetilde{\rho_m \phi_i}$	$\zeta^{ij} + \zeta^{ijt}$	$\omega^{-m} \zeta^{ij} + \omega^m \zeta^{ijt} \quad 1 \leq m \leq (p-1)/2$

4. The characters of G . In this section, we add to the assumption of §3 the condition that $C_G(X)$ is a trivial intersection set.

Let

$${}_m\alpha_{ij} = 1\phi_i - \rho_m\phi_j, \quad \text{and} \quad {}_m\beta_{ij} = 1\phi_i - \bar{\rho}_m\phi_j,$$

where $0 \leq i, j < s$, $1 \leq m \leq (p-1)/2$.

We will use $*$ to denote induction to G . Again, as in §3, we proceed by proving a series of lemmas.

LEMMA 4.1. For $0 \leq i < f$, $1 \leq m \leq (p-1)/2$, we have

$${}_m\alpha_{ie,ie}^* = \mu_i(\lambda_i + \tau_i\theta_i - \chi_i^m),$$

where λ_i , θ_i , and χ_i^m are distinct irreducible characters of G , and $\mu_i = \pm 1$, $\tau_i = \pm 1$.

PROOF. We have

$$\begin{aligned} ({}_m\alpha_{ie,ie}^*, {}_m\alpha_{ie,ie}^*) &= (\widetilde{{}_m\alpha_{ie,ie}}, \widetilde{{}_m\alpha_{ie,ie}}) \\ &= (\widetilde{1\phi_{ie} - \rho_m\phi_{ie}}, \widetilde{1\phi_{ie} - \rho_m\phi_{ie}}) \\ &= (\lambda_{i1} + \lambda_{i2} - \rho_m\phi_{ie}, \lambda_{i1} + \lambda_{i2} - \rho_m\phi_{ie}) \\ &= 3. \end{aligned}$$

Hence ${}_m\alpha_{ie,ie}^*$ is reducible, and

$${}_m\alpha_{ie,ie}^* = \epsilon_{i1}^m\lambda_i^m + \epsilon_{i2}^m\theta_i^m + \epsilon_{i3}^m\chi_i^m,$$

where $0 \leq i < f$, $1 \leq m \leq (p-1)/2$, and $\epsilon_{i_n}^m = \pm 1$, $1 \leq n \leq 3$, and λ_i^m , θ_i^m , and χ_i^m are distinct irreducible characters of G .

Let $m \neq m'$; then by the method used above we have $({}_m\alpha_{ie,ie}^*, {}_{m'}\alpha_{ie,ie}^*) = 2$. Hence we may assume that $\epsilon_{i_1}^m$, λ_i^m , $\epsilon_{i_2}^m$, θ_i^m are independent of m , i.e.,

$${}_m\alpha_{ie,ie}^* = \epsilon_{i_1}\lambda_i + \epsilon_{i_2}\theta_i + \epsilon_{i_3}^m\chi_i^m.$$

Also, since ${}_m\alpha_{ie,ie}^*(1) - {}_{m'}\alpha_{ie,ie}^*(1) = 0$, we may assume that $\epsilon_{i_3}^m$ is independent of m . Therefore,

$${}_m\alpha_{ie,ie}^* = \epsilon_{i_1}\lambda_i + \epsilon_{i_2}\theta_i + \epsilon_{i_3}\chi_i^m.$$

Now since ${}_m\alpha_{ie,ie}^*(1) = 0$, so ϵ_{i_1} , ϵ_{i_2} , and ϵ_{i_3} cannot be all positive and also cannot be all negative. Let us take $\epsilon_{i_1} = \mu_i$, $\epsilon_{i_2} = \mu_i\tau_i$, and $\epsilon_{i_3} = -\mu_i$ where $\mu_i = \pm 1$, and $\tau_i = \pm 1$. Therefore,

$${}_m\alpha_{ie,ie}^* = \mu_i(\lambda_i + \tau_i\theta_i - \chi_i^m).$$

This completes the proof of the lemma.

LEMMA 4.2. For $0 < i < s$, $e \nmid i$, $1 \leq m \leq (p-1)/2$, we have

$${}_m\alpha_{ii}^* = \epsilon_i(\psi_i - \xi_i^m), \quad \text{and} \quad {}_m\beta_{ii}^* = \epsilon_i(\psi_i - \eta_i^m),$$

where ψ_i , ξ_i^m , and η_i^m are distinct irreducible characters of G and $\epsilon_i = \pm 1$.

PROOF. By the same argument as Lemma 4.1, we get the desired conclusion.

By using the result of Brauer [1], we know that the $(s+f)/2$ p -blocks of G of defect 1 are seen to be

$$b_{ie}^G = B_{ie} = \{\lambda_i\} \cup \{\theta_i\} \cup \{\chi_i^m \mid 1 \leq m \leq (p-1)/2\},$$

where $0 \leq i < f$; and

$$b_i^G = B_i = B_{ii} = \{\psi_i\} \cup \{\xi_i^m \mid 1 \leq m \leq (p-1)/2\} \cup \{\eta_i^m \mid 1 \leq m \leq (p-1)/2\},$$

where $0 < i < s$, $e \nmid i$.

Since ${}_m\alpha_{ij}^*(\pi) = (\widetilde{1}\phi_j - \widetilde{\rho_m}\phi_j)(\pi) = 0$, for all $\pi \in \langle \sigma \rangle$, and for all j , $0 \leq j < s$, also for all m , $1 \leq m \leq (p-1)/2$, we have

$$(1) \quad \lambda_i(\pi) + \tau_i\theta_i(\pi) - \chi_i^m(\pi) = 0,$$

where $\pi \in \langle \sigma \rangle$, $0 \leq i < f$, $1 \leq m \leq (p-1)/2$; and

$$(2) \quad \psi_i(\pi) = \xi_i^m(\pi) = \eta_i^m(\pi),$$

where $\pi \in \langle \sigma \rangle$, $e \nmid i$, $0 < i < s$, $1 \leq m \leq (p-1)/2$.

Again by using the result of Brauer [1], we obtain the following table for

G in which the entries under the column under σ^j are intended to be modulo a prime divisor of the integer p in an appropriate algebraic number field.

TABLE II

	σ^j	$x\sigma^j$
λ_i	$\mu_i \zeta^{ije}$	$\mu_i \zeta^{ije} \quad 0 \leq i < f$
θ_i	$\mu_i \tau_i \zeta^{ije}$	$\mu_i \tau_i \zeta^{ije} \quad 1 < m < (p-1)/2$
χ_i^m	$2\mu_i \zeta^{ije}$	$\mu_i (\omega^m + \omega^{-m}) \zeta^{ije}$
ψ_i	$\epsilon_i (\zeta^{ij} + \zeta^{ijt})$	$\epsilon_i (\zeta^{ij} + \zeta^{ijt}) \quad 0 < i < s$
ξ_i^m	$\epsilon_i (\zeta^{ij} + \zeta^{ijt})$	$\epsilon_i (\omega^m \zeta^{ij} + \omega^{-m} \zeta^{ijt}) \quad 1 \leq m \leq (p-1)/2$
η_i^m	$\epsilon_i (\zeta^{ij} + \zeta^{ijt})$	$\epsilon_i (\omega^{-m} \zeta^{ij} + \omega^m \zeta^{ijt})$

Moreover, every irreducible character of defect 0 vanishes on $C_G(X) - \langle \sigma \rangle$. In fact, it can be seen from Corollaries 4.6, and 4.9 and Lemma 4.10 that characters of defect 0 vanish on $C_G(X) - \{1\}$.

Now we are going to determine the column under $\pi = \sigma^{s/2}$ by using the assumption that $C_G(X)$ is a trivial intersection set.

LEMMA 4.3. For $0 \leq i, j < s$, and $1 \leq m \leq (p-1)/2$, we have

$${}_m \widetilde{\alpha}_{ij} = {}_m \widetilde{\beta}_{i,jt} \quad \text{and} \quad {}_m \widetilde{\beta}_{ij} = {}_m \widetilde{\alpha}_{i,jt}.$$

PROOF. This is a direct consequence of Lemma 3.8.

LEMMA 4.4. For $0 \leq i, j, k, n < s$, and $1 \leq m, m' \leq (p-1)/2$, we have

$$({}_m \alpha_{ij}^*, {}_{m'} \alpha_{kn}^*) = \nu \delta_{ik} + \delta_{mm'} \delta_{jn},$$

$$({}_m \beta_{ij}^*, {}_{m'} \alpha_{kn}^*) = \nu \delta_{ik} + \delta_{mm'} \delta_{jt,n},$$

and

$$({}_m \alpha_{ij}^*, {}_{m'} \beta_{kn}^*) = \nu \delta_{ik} + \delta_{mm'} \delta_{j,nt};$$

here $\nu = 2$ if $i \equiv 0 \pmod{e}$, and $\nu = 1$ if $i \not\equiv 0 \pmod{e}$.

PROOF.

$$({}_m \alpha_{ij}^*, {}_{m'} \alpha_{kn}^*) = (\widetilde{1\phi_i} - \widetilde{\rho_m \phi_j}, \widetilde{1\phi_k} - \widetilde{\rho_{m'} \phi_n}) = \nu \delta_{ik} + \delta_{mm'} \delta_{jn},$$

where ν takes the values given in the lemma.

The second and third equations of the lemma are proved by the same method together with the use of Lemma 4.3.

LEMMA 4.5. *If $0 < i, j < s$, $i \not\equiv 0, j \not\equiv 0 \pmod{e}$, and $1 \leq m \leq (p-1)/2$, then ${}_m\alpha_{ij}^* = \epsilon_i\psi_i - \epsilon_j\xi_j^m$.*

PROOF. By Lemma 4.2, we may assume $i \neq j$. By Lemma 4.4, we have

$$({}_m\alpha_{ij}^*, {}_m\alpha_{ij}^*) = 2, \quad ({}_m\alpha_{ij}^*, {}_{m'}\alpha_{ii}^*) = 1,$$

$$({}_m\alpha_{ij}^*, {}_{m'}\beta_{ii}^*) = 1 + \delta_{mm'}\delta_{j,ii}, \quad \text{and} \quad ({}_m\alpha_{ij}^*, {}_{m'}\alpha_{jj}^*) = \delta_{mm'}.$$

From above we know that ${}_m\alpha_{ij}^*$ is a difference of two irreducible characters and has one common character with each of ${}_{m'}\alpha_{ii}^*$ and ${}_{m'}\beta_{ii}^*$. Since there are at least $2(p-1)/2 \geq 4$ characters to compare, ${}_m\alpha_{ij}^*$ contains $\epsilon_i\psi_i$. From $({}_m\alpha_{ij}^*, {}_m\alpha_{ij}^*) = 1$, it follows that ${}_m\alpha_{ij}^*$ contains $\epsilon_j\psi_j$ or $-\epsilon_j\xi_j^m$. If ${}_m\alpha_{ij}^*$ contains $\epsilon_j\psi_j$, then $({}_m\alpha_{ij}^*, {}_{m'}\alpha_{jj}^*) \geq 1$ for $m \neq m'$; this is not the case. Therefore, ${}_m\alpha_{ij}^* = \epsilon_i\psi_i - \epsilon_j\xi_j^m$.

COROLLARY 4.6. *If $0 < i, j < s$, $i \not\equiv 0, j \not\equiv 0 \pmod{e}$, and $1 \leq m \leq (p-1)/2$, then $\epsilon_i = \epsilon_j$ in the notation of Lemma 4.2. Set $\epsilon_i = \delta$ for all i , we have ${}_m\alpha_{ij}^* = \delta(\psi_i - \xi_j^m)$, where $\delta = \pm 1$.*

PROOF. By Table I, we have ${}_m\alpha_{ij}^*(1) = 0$. By Lemma 4.5, we have

$$0 = {}_m\alpha_{ij}^*(1) = \epsilon_i\psi_i(1) - \epsilon_j\xi_j^m(1).$$

It follows that $\epsilon_i = \epsilon_j$. This completes the proof of the lemma.

COROLLARY 4.7. *If $0 < i < s$, $i \not\equiv 0 \pmod{e}$, and $1 \leq m \leq (p-1)/2$, then ${}_m\alpha_{1i}^* = \delta(\psi_1 - \xi_i^m)$.*

PROOF. This is just a special case of Corollary 4.6.

LEMMA 4.8. *If $0 \leq i < f$, $0 < j < s$, $j \not\equiv 0 \pmod{e}$, and $1 \leq m \leq (p-1)/2$, then*

$${}_m\alpha_{ie,j}^* = \mu_i(\lambda_i + \tau_i\theta_i) - \delta\xi_j^m.$$

PROOF. By Lemma 4.4, we have $({}_m\alpha_{ie,j}^*, {}_m\alpha_{ie,j}^*) = 3$. Thus ${}_m\alpha_{ie,j}^*$ is a sum of three irreducible characters. From $({}_m\alpha_{ie,j}^*, {}_{m'}\alpha_{jj}^*) = \delta_{mm'}$, we know that ${}_m\alpha_{ie,j}^*$ contains $-\delta\xi_j^m$. Moreover, from $({}_m\alpha_{ie,j}^*, {}_{m'}\alpha_{ie,ie}^*) = 2$, we know that ${}_m\alpha_{ie,j}^*$ contains $\mu_i(\lambda_i + \tau_i\theta_i)$. Consequently,

$${}_m\alpha_{ie,j}^* = \mu_i(\lambda_i + \tau_i\theta_i) - \delta\xi_j^m.$$

COROLLARY 4.9. *For $0 \leq i < f$, we have $\mu_i = \delta$ in the notation of*

Lemma 4.1. So we see that ${}_m\alpha_{ie,j}^* = \delta(\lambda_i + \tau_i\theta_i - \xi_j^m)$, where $0 \leq i < f$, $0 < j < s$, $j \not\equiv 0 \pmod{e}$, $1 \leq m \leq (p-1)/2$.

PROOF. Since ${}_m\alpha_{ie,j}^*(1) = 0$, $\mu_i = \delta$.

LEMMA 4.10. If $0 \leq i, j < f$, and $1 \leq m \leq (p-1)/2$, then ${}_m\alpha_{ie,je}^* = \delta(\lambda_i + \tau_i\theta_i - \chi_j^m)$.

PROOF. By Lemma 4.1, we may assume that $i \neq j$. From $({}_m\alpha_{ie,je}^*, {}_m\alpha_{ie,je}^*) = 3$, it is known that ${}_m\alpha_{ie,je}^*$ is a sum of three irreducible characters. If $j' \not\equiv 0 \pmod{e}$, we have $({}_m\alpha_{ie,je}^*, {}_m\alpha_{ie,j'}^*) = 2$.

By Corollary 4.9, we know that ${}_m\alpha_{ie,je}^*$ contains $\delta(\lambda_i + \tau_i\theta_i)$. And $({}_m\alpha_{ie,je}^*, {}_m\alpha_{je,je}^*) = \delta_{mm'}$, yields that ${}_m\alpha_{ie,je}^*$ contains $-\delta\chi_j^m$. It follows that ${}_m\alpha_{ie,je}^* = \delta(\lambda_i + \tau_i\theta_i - \chi_j^m)$.

COROLLARY 4.11. If $i = 0$ in Lemma 4.1, then we have the following two cases:

Case (A): $\lambda_0 = 1, \mu_0 = 1, \tau_0 = 1$, i.e., ${}_m\alpha_{00}^* = 1 + \theta_0 - \chi_0^m$;

Case (B): $\theta_0 = 1, \mu_0 = -1, \tau_0 = -1$, i.e., ${}_m\alpha_{00}^* = 1 - \lambda_0 + \chi_0^m$.

PROOF. This is an immediate consequence of Lemma 4.1.

Combining Corollaries 4.7, 4.9, and 4.11 and Lemma 4.10, we obtain the following table.

TABLE III

	Case (A) $\mu_0 = \delta = 1, \lambda_0 = 1$ $\tau_0 = 1$	Case (B) $\mu_0 = \delta = -1, \theta_0 = 1$, $\tau_0 = -1$
${}_m\alpha_{1i}^*$ $i \not\equiv 0 \pmod{e}, 0 < i < s$ $1 \leq m \leq (p-1)/2$	$\psi_1 - \xi_i^m$	$-\psi_1 + \xi_i^m$
${}_m\alpha_{01}^*$ $1 \leq m \leq (p-1)/2$	$1 + \theta_0 - \xi_1^m$	$1 - \lambda_0 + \xi_1^m$
${}_m\alpha_{0,i}^*$ $0 \leq i < f$ $1 \leq m \leq (p-1)/2$	$1 + \theta_0 - \chi_i^m$	$1 - \lambda_0 + \chi_i^m$

LEMMA 4.12. If $\pi = \sigma^{s/2}$, and $0 \leq i, j < s$, and $1 \leq m \leq (p-1)/2$, then ${}_m\alpha_{ij}^*(\pi) = 2[(-1)^i - (-1)^j]$.

PROOF. Since $t^2 \equiv 1 \pmod{s}$, it follows that t is odd. From Table I, we have

$$\begin{aligned} {}_m\alpha_{ij}^*(\pi) &= {}_m\tilde{\alpha}_{ij}(\pi) \\ &= \widetilde{1\phi_i(\pi)} - \widetilde{\rho_m\phi_j(\pi)} \\ &= (\zeta^{is/2} + \zeta^{ist/2}) - (\zeta^{js/2} + \zeta^{jst/2}) \\ &= [(-1)^i + (-1)^{it}] - [(-1)^j + (-1)^{jt}] \\ &= 2[(-1)^i - (-1)^j]. \end{aligned}$$

We shall set $\pi = \sigma^{s/2}$ here. We now apply these results and proceed by considering Cases (A) and (B) separately.

Case (A) with $e > 1$:

LEMMA 4.13. For $0 < i < s$, $i \not\equiv 0 \pmod{e}$, we have

$$\psi_i(\pi) = \begin{cases} \psi_1(\pi), & \text{if } i \text{ is odd,} \\ \psi_1(\pi) + 4, & \text{if } i \text{ is even.} \end{cases}$$

In addition, for $0 \leq i < f$, and $1 \leq m \leq (p-1)/2$, we have

$$\chi_i^m(\pi) = \begin{cases} \psi_1(\pi), & \text{if } ie \text{ is odd,} \\ \psi_1(\pi) + 4, & \text{if } ie \text{ is even.} \end{cases}$$

PROOF. From Lemma 4.12, it is known that

$${}_m\alpha_{1i}^*(\pi) = \begin{cases} 0, & \text{if } i \text{ is odd,} \\ -4, & \text{if } i \text{ is even.} \end{cases}$$

If $0 < i < s$, $i \not\equiv 0 \pmod{e}$, by the first line of Table III and formula (2), we must have

$${}_m\alpha_{1i}^*(\pi) = \psi_1(\pi) - \xi_i^m(\pi) = \psi_1(\pi) - \psi_i(\pi).$$

Then

$$\psi_i(\pi) = \begin{cases} \psi_1(\pi), & \text{if } i \text{ is odd,} \\ \psi_1(\pi) + 4, & \text{if } i \text{ is even.} \end{cases}$$

By Lemma 4.12, we have ${}_m\alpha_{01}^*(\pi) = 4$. From the second line of Table III, we get

$${}_m\alpha_{01}^*(\pi) = 1 + \theta_0(\pi) - \xi_1^m(\pi) = 4.$$

Formula (1) gives us $1 + \theta_0(\pi) - \chi_0^m(\pi) = 0$. It follows that

$$\chi_0^m(\pi) = 1 + \theta_0(\pi) = 4 + \xi_1^m(\pi).$$

By formula (2), we obtain $\chi_0^m(\pi) = 4 + \psi_1(\pi)$. Again by Lemma 4.12, we see that

$${}_m\alpha_{0,ie}^*(\pi) = \begin{cases} 4, & \text{if } ie \text{ is odd,} \\ 0, & \text{if } ie \text{ is even.} \end{cases}$$

Now if $0 \leq i < f$ and $1 \leq m \leq (p-1)/2$, then by the last line of Table III, we have

$${}_m\alpha_{0,ie}^*(\pi) = 1 + \theta_0(\pi) - \chi_i^m(\pi).$$

It follows that

$$\chi_i^m(\pi) = 4 + \psi_1(\pi) - {}_m\alpha_{0,ie}^*(\pi).$$

Hence

$$\chi_i^m(\pi) = \begin{cases} \psi_1(\pi), & \text{if } ie \text{ is odd,} \\ \psi_1(\pi) + 4, & \text{if } ie \text{ is even.} \end{cases}$$

LEMMA 4.14. *We have*

$$\begin{aligned} 2ps = & \sum_{i=0}^{f-1} [\lambda_i(\pi)^2 + \theta_i(\pi)^2] + [(p-1)a/2] \psi_1(\pi)^2 \\ & + [(p-1)b/2] (\psi_1(\pi) + 4)^2 \\ & + (p/2)[c\psi_1(\pi)^2 + d(\psi_1(\pi) + 4)^2], \end{aligned}$$

where

$$\begin{aligned} a &= \#\{i \mid 0 \leq i < f, ie \text{ is odd}\} \\ &= \begin{cases} f/2, & \text{if } e \text{ is odd,} \\ 0, & \text{if } e \text{ is even;} \end{cases} \\ b &= \#\{i \mid 0 \leq i < f, ie \text{ is even}\} \\ &= \begin{cases} f/2, & \text{if } e \text{ is odd,} \\ f, & \text{if } e \text{ is even;} \end{cases} \\ c &= \#\{i \mid 0 < i < s, i \not\equiv 0 \pmod{e}, i \text{ is odd}\} \\ &= \begin{cases} (s-f)/2, & \text{if } e \text{ is odd,} \\ s/2, & \text{if } e \text{ is even;} \end{cases} \end{aligned}$$

and

$$d = \#\{i \mid 0 < i < s, i \not\equiv 0 \pmod{e}, i \text{ is even}\} \\ = \begin{cases} (s-f)/2, & \text{if } e \text{ is odd,} \\ (s/2) - f, & \text{if } e \text{ is even.} \end{cases}$$

PROOF. Since $C_G(\pi) = N_G(X)$, we have

$$\begin{aligned} 2ps &= \sum_{i=1}^{f-1} [\lambda_i(\pi)^2 + \theta_i(\pi)^2] + \sum_{i=0}^{f-1} \sum_{m=1}^{(p-1)/2} (\chi_i^m(\pi))^2 \\ &\quad + (1/2) \sum_{\substack{i \not\equiv 0 \pmod{e} \\ 0 < i < s}} \psi_i(\pi)^2 \\ &\quad + (1/2) \sum_{\substack{i \not\equiv 0 \pmod{e} \\ 0 < i < s}} \sum_{m=1}^{(p-1)/2} [(\xi_i^m(\pi))^2 + (\eta_i^m(\pi))^2] \\ &= \sum_{i=0}^{f-1} [\lambda_i(\pi)^2 + \theta_i(\pi)^2] + \sum_{i=0}^{f-1} \sum_{m=1}^{(p-1)/2} (\chi_i^m(\pi))^2 \\ &\quad + (p/2) \sum_{\substack{i \not\equiv 0 \pmod{e} \\ 0 < i < s}} \psi_i(\pi)^2 \\ &= \sum_{i=0}^{f-1} [\lambda_i(\pi)^2 + \theta_i(\pi)^2] + [(p-1)a/2] \psi_1(\pi)^2 \\ &\quad + [(p-1)b/2] (\psi_1(\pi) + 4)^2 \\ &\quad + (p/2) [c\psi_1(\pi)^2 + d(\psi_1(\pi) + 4)^2] \end{aligned}$$

where a, b, c , and d are the quantities stated in the lemma.

LEMMA 4.15. *If $0 < i < s, i \not\equiv 0 \pmod{e}$, then $\psi_i(\pi) = 2(-1)^i$; and if $0 \leq i < f, 1 \leq m \leq (p-1)/2$, then $\chi_i^m(\pi) = 2(-1)^{ie}$.*

PROOF. We prove this lemma by showing that $\psi_1(\pi) = -2$. If e is odd, by Lemma 4.14, we have

$$\begin{aligned} 2ps &= \sum_{i=0}^{f-1} [\lambda_i(\pi)^2 + \theta_i(\pi)^2] + [(p-1)/2] (f/2)(\psi_1(\pi))^2 \\ &\quad + [(p-1)/2] (f/2)(\psi_1(\pi) + 4)^2 \\ &\quad + (p/2) [\{(s-f)/2\} \psi_1(\pi)^2 + \{(s-f)/2\} (\psi_1(\pi) + 4)^2] \\ &= \sum_{i=0}^{f-1} [\lambda_i(\pi)^2 + \theta_i(\pi)^2] + [(ps-f)/2] \psi_1(\pi)^2 \\ &\quad + 2(ps-f)\psi_1(\pi) + 4ps - 4f. \end{aligned}$$

Then

$$[(ps-f)/2] \psi_1(\pi)^2 + 2(ps-f)\psi_1(\pi) \leq -2ps + 4f < 0;$$

and hence

$$\psi_1(\pi)[\{(ps-f)/2\}\psi_1(\pi) + 2(ps-f)] < 0.$$

It follows that $-4 < \psi_1(\pi) < 0$.

By Table II, we have

$$\begin{aligned}\psi_1(\pi) &\equiv \zeta^{s/2} + \zeta^{st/2} \pmod{p} \equiv (-1) + (-1) \pmod{p} \\ &\equiv -2 \pmod{p}.\end{aligned}$$

Hence $\psi_1(\pi) = -2$ as required.

In the second case where e is even, the same argument again shows that $-4 < \psi_1(\pi) < 0$; and hence $\psi_1(\pi) = -2$. Therefore, in both cases, $\psi_1(\pi) = -2$. Now an application of Lemma 4.13 completes the proof of Lemma 4.15.

LEMMA 4.16. For $0 \leq i < f$, we have $\lambda_i(\pi) = (-1)^{ie}$, and $\theta_i(\pi) = \tau_i(-1)^{ie}$.

PROOF. If e is odd, we have

$$\begin{aligned}2ps &= \sum_{i=0}^{f-1} [\lambda_i(\pi)^2 + \theta_i(\pi)^2 + [(p-1)/2](f/2)4 \\ &\quad + [(p-1)/2](f/2)4 \\ &\quad + (p/2)[\{(s-f)/2\}4 + \{(s-f)/2\}4] \\ &= \sum_{i=0}^{f-1} [\lambda_i(\pi)^2 + \theta_i(\pi)^2] + 2(p-1)f + 2p(s-f).\end{aligned}$$

Hence

$$\sum_{i=0}^{f-1} [\lambda_i(\pi)^2 + \theta_i(\pi)^2] = 2f.$$

In the second case where e is even, the same argument again shows that

$$\sum_{i=0}^{f-1} [\lambda_i(\pi)^2 + \theta_i(\pi)^2] = 2f.$$

Since

$$\lambda_i(\pi) \equiv \zeta^{ise/2} \equiv (-1)^{ie} \pmod{p},$$

and

$$\theta_i(\pi) \equiv \tau_i \zeta^{ise/2} \equiv \tau_i(-1)^{ie} \pmod{p},$$

hence $\lambda_i(\pi) = (-1)^{ie}$ and $\theta_i(\pi) = \tau_i(-1)^{ie}$ for $0 \leq i < f$. This completes the proof of Lemma 4.16.

Case (A) with $e = 1$:

LEMMA 4.17. For $0 \leq i < s$, and $1 \leq m \leq (p-1)/2$, we have

$$\chi_i^m(\pi) = \begin{cases} \chi_0^m(\pi) - 4, & \text{if } i \text{ is odd,} \\ \chi_0^m(\pi), & \text{if } i \text{ is even.} \end{cases}$$

PROOF. By Lemma 4.12, we have

$${}_m\alpha_{0i}^*(\pi) = \begin{cases} 4, & \text{if } i \text{ is odd,} \\ 0, & \text{if } i \text{ is even.} \end{cases}$$

By formula (1), we have $1 + \theta_0(\pi) - \chi_0^m(\pi) = 0$. Hence $\chi_0^m(\pi) = 1 + \theta_0(\pi)$. By the last line of Table III, we have

$${}_m\alpha_{0i}^*(\pi) = 1 + \theta_0(\pi) - \chi_i^m(\pi),$$

and hence ${}_m\alpha_{0i}^*(\pi) = \chi_0^m(\pi) - \chi_i^m(\pi)$. Therefore,

$$\chi_i^m(\pi) = \begin{cases} \chi_0^m(\pi) - 4, & \text{if } i \text{ is odd,} \\ \chi_0^m(\pi), & \text{if } i \text{ is even.} \end{cases}$$

LEMMA 4.18. For $0 \leq i < s$, and $1 \leq m \leq (p-1)/2$, we have $\chi_i^m(\pi) = 2(-1)^i$.

PROOF. Since $e = 1$, $c = d = 0$. Then we have

$$\begin{aligned} 2ps &= \sum_{i=0}^{s-1} [\lambda_i(\pi)^2 + \theta_i(\pi)^2] + [(p-1)/2](s/2)[\chi_0^m(\pi) - 4]^2 \\ &\quad + [(p-1)/2](s/2)\chi_0^m(\pi)^2 \\ &= \sum_{i=0}^{s-1} [\lambda_i(\pi)^2 + \theta_i(\pi)^2] + [(ps-s)/2]\chi_0^m(\pi)^2 \\ &\quad - 2(ps-s)\chi_0^m(\pi) + 4(ps-s). \end{aligned}$$

Then

$$[(ps-s)/2]\chi_0^m(\pi)^2 - 2(ps-s)\chi_0^m(\pi) \leq -2ps + 4s < 0;$$

and hence

$$\chi_0^m(\pi)[\{(ps-s)/2\}\chi_0^m(\pi) - 2(ps-s)] < 0.$$

It follows that $0 < \chi_0^m(\pi) < 4$.

Since $\chi_0^m(\pi) \equiv 2 \pmod{p}$, $\chi_0^m(\pi) = 2$. By Lemma 4.17, we get $\chi_i^m(\pi) = 2(-1)^i$.

LEMMA 4.19. For $0 \leq i < s$, $\lambda_i(\pi) = (-1)^i$ and $\theta_i(\pi) = \tau_i(-1)^i$.

PROOF. From Lemma 4.18, we have

$$\sum_{i=0}^{s-1} [\lambda_i(\pi)^2 + \theta_i(\pi)^2] = 2ps - [(p-1)s/4]4 - [(p-1)s/4]4 = 2s.$$

Since

$$\lambda_i(\pi) \equiv \zeta^{is/2} \equiv (-1)^i \pmod{p},$$

and

$$\theta_i(\pi) \equiv \tau_i \zeta^{is/2} \equiv \tau_i (-1)^i \pmod{p},$$

hence $\lambda_i(\pi) = (-1)^i$ and $\theta_i(\pi) = \tau_i (-1)^i$.

The above results combined yield the following table for Case (A).

TABLE IV

	$\pi = \sigma^{s/2}$	
λ_i	$(-1)^{ie}$	$0 \leq i < f$
θ_i	$\tau_i (-1)^{ie}$	$1 \leq m \leq (p-1)/2$
χ_i^m	$2(-1)^{ie}$	
ψ_i	$2(-1)^i$	$i \not\equiv 0 \pmod{e}$
ξ_i^m	$2(-1)^i$	$0 < i < s$
η_i^m	$2(-1)^i$	$1 \leq m \leq (p-1)/2$
ζ	0	

Here ζ denotes the characters of defect 0.

The computations used in Case (A) can be applied to Case (B) as well. The results can be tabulated as follows:

TABLE V

	$\pi = \sigma^{s/2}$	
λ_i	$(-1)^{ie+1}$	$0 \leq i < f$
θ_i	$\tau_i (-1)^{ie+1}$	$1 \leq m \leq (p-1)/2$
χ_i^m	$2(-1)^{ie+1}$	
ψ_i	$2(-1)^{i+1}$	$i \not\equiv 0 \pmod{e}$
ξ_i^m	$2(-1)^{i+1}$	$0 < i < s$
η_i^m	$2(-1)^{i+1}$	$1 \leq m \leq (p-1)/2$
ζ	0	

Here ζ denotes the characters of defect 0.

5. Completion of the proof of the theorem in Case (2). In this section, we assume that the hypotheses of the theorem and the notations of §4 hold.

LEMMA 5.1. *Assume the hypotheses of the theorem hold. Let $F = \langle \sigma^e \rangle$ be the fixed point group of τ acting on $\langle \sigma \rangle$. Write $F = F_0 \times F_1$ where $|F_0|$ is a 2-power and $|F_1|$ is odd. Then there is a normal complement G_0 for F_1 in G .*

PROOF. Let q be an odd prime divisor of $|C_G(X)|$, and Q be a Sylow q -subgroup of $C_G(X)$. By Lemma 2.2, we see that $N_G(Q) = N_G(\langle y \rangle) = C_G(\pi) = N_G(X)$, and Q is a Sylow q -subgroup of G .

Let q be a prime number such that $q \mid |F_1|$, and Q be a Sylow q -subgroup of F_1 . Now we show that Q is a Sylow q -subgroup of $\langle \sigma \rangle$. By Lemmas 3.1 and 3.2, we have $e = (s, t + 1)/d$ and $f = (s, t - 1)$. It follows that the greatest common divisor of e and f has no odd prime factors. Therefore, Q is a Sylow q -subgroup of $\langle \sigma \rangle$. It then follows that Q is a Sylow q -subgroup of G , and $N_G(Q) = N_G(X)$. Since Q is cyclic, and Q is fixed by τ , we have $Q \subseteq Z(N_G(X)) = Z(N_G(Q))$. By Burnside's theorem, Q has a normal q -complement M_q in G . Let

$$G_0 = \bigcap_{q \mid |F_1|} M_q.$$

It is clear that G_0 is a normal subgroup of G . Since each M_q is a normal q -complement of G , the order of G_0 is not divisible by each q dividing $|F_1|$. Hence $G_0 \cap F_1 = \{1\}$. On the other hand, the index $|G : G_0|$ divides $|F_1|$. Hence we have $G_0 F_1 = G$. Thus, G_0 is a normal complement of F_1 in G .

REMARK. In order to complete the proof of the main theorem in Case (2), By Lemma 5.1, we can replace G by G_0 for the rest of our discussion. This amounts merely to the introduction of the assumption that $f = |F|$ is a 2-power in Lemma 5.2. Moreover, the conclusion of the main theorem follows immediately from Lemmas 5.1 and 5.2.

LEMMA 5.2. *Assume the hypotheses of the theorem hold. Let $F = \langle \sigma^e \rangle$ be the fixed point group of τ acting on $\langle \sigma \rangle$. If $f = |F|$ is a 2-power and $x\sigma$ cannot be written as a product of two conjugates of $\pi = \sigma^{s/2}$, then G contains a normal subgroup of index 2.*

PROOF. Evaluating the appropriate multiplication constant for the class algebra of G , we get

$$\sum_{\xi} \frac{\xi(x\sigma)\xi(\pi)^2}{\xi(1)} = 0.$$

We have two cases.

Case (A). From Table IV and by block theory of modular representation, we have

$$\sum_{i=0}^{f-1} \frac{((-1)^{ie})^2 \zeta^{ie}}{\lambda_i(1)} + \sum_{i=0}^{f-1} \frac{(\tau_i(-1)^{ie})^2 \tau_i \zeta^{ie}}{\theta_i(1)} + \sum_{i=0}^{f-1} \sum_{m=1}^{(p-1)/2} \frac{(2(-1)^{ie})^2 (\omega^m + \omega^{-m}) \zeta^{ie}}{\chi_i^m(1)} = 0.$$

Since $\sum_{m=1}^{(p-1)/2} (\omega^m + \omega^{-m}) = -1$, we have

$$\sum_{i=0}^{f-1} \left(\frac{1}{\lambda_i(1)} + \frac{\tau_i}{\theta_i(1)} - \frac{4}{\chi_i^m(1)} \right) \zeta^{ie} = 0.$$

Since ζ^e is a primitive f th root of unity, and f is even,

$$\left(1 + \frac{1}{\theta_0(1)} - \frac{4}{\chi_0^m(1)} \right) - \left(\frac{1}{\lambda_{f/2}(1)} + \frac{\tau_{f/2}}{\theta_{f/2}(1)} - \frac{4}{\chi_{f/2}^m(1)} \right) = 0.$$

Since ${}_m\alpha_{0,ie}^*(1) = 0$, by Table III, we have $1 + \theta_0(1) - \chi_i^m(1) = 0$, $0 \leq i < f$, $1 \leq m \leq (p-1)/2$. Hence $\chi_0^m(1) = 1 + \theta_0(1) = \chi_{f/2}^m(1)$. It follows that

$$1 + \frac{1}{\theta_0(1)} - \frac{1}{\lambda_{f/2}(1)} - \frac{\tau_{f/2}}{\theta_{f/2}(1)} = 0.$$

Since $1 + \theta_0(1) - \chi_0^m(1) = 0$, $\theta_0(1) = \chi_0^m(1) - 1$. By formula (1) of §4, we have $\lambda_{f/2}(1) + \tau_{f/2}\theta_{f/2}(1) - \chi_{f/2}^m(1) = 0$. Hence $\lambda_{f/2}(1) = \chi_0^m(1) - \tau_{f/2}\theta_{f/2}(1)$. Then

$$1 + \frac{1}{\chi_0^m(1) - 1} = \frac{1}{\chi_0^m(1) - \tau_{f/2}\theta_{f/2}(1)} + \frac{\tau_{f/2}}{\theta_{f/2}(1)},$$

and hence

$$\frac{\chi_0^m(1)}{\chi_0^m(1) - 1} = \frac{\tau_{f/2}\chi_0^m(1)}{\theta_{f/2}\chi_0^m(1) - \tau_{f/2}\theta_{f/2}(1)^2}.$$

Since $\chi_0^m(1) \neq 0$, we have

$$\theta_{f/2}(1)\chi_0^m(1) - \tau_{f/2}\theta_{f/2}(1)^2 - \tau_{f/2}\chi_0^m(1) + \tau_{f/2} = 0.$$

By multiplying both sides by $\tau_{f/2}$, we have

$$\theta_{f/2}(1)^2 - \tau_{f/2}\chi_0^m(1)\theta_{f/2}(1) + \chi_0^m(1) - 1 = 0,$$

from which it follows that $\tau_{f/2} = 1$. Hence

$$\theta_{f/2}(1)^2 - \chi_0^m(1)\theta_{f/2}(1) + \chi_0^m(1) - 1 = 0,$$

and thus

$$[\theta_{f/2}(1) - 1][\theta_{f/2}(1) - (\chi_0^m(1) - 1)] = 0.$$

Therefore, $\theta_{f/2}(1) = 1$ or $\theta_{f/2}(1) = \chi_0^m(1) - 1$. If $\theta_{f/2}(1) = \chi_0^m(1) - 1$, then $\lambda_{f/2}(1) = \chi_0^m(1) - \theta_{f/2}(1) = \chi_0^m(1) - \chi_0^m(1) + 1 = 1$. Thus one of $\lambda_{f/2}$, $\theta_{f/2}$ is linear. Let N be its kernel. Since $\lambda_{f/2}(x) = \theta_{f/2}(x) = 1$, and $\lambda_{f/2}(\sigma) \equiv \theta_{f/2}(\sigma) \equiv -1 \pmod{p}$ which implies that $\lambda_{f/2}(\sigma) = \theta_{f/2}(\sigma) = -1$, we know that $x \in N$ and $\sigma \notin N$. Since $x \in N$, X is a Sylow p -subgroup of N . By Frattini's argument, we have $G = NN_G(X)$. It follows that $G = NN_G(X) = N\langle x, \sigma, \tau \rangle = N\langle \sigma, \tau \rangle$. If $N \cap \langle \sigma, \tau \rangle \subseteq \langle \sigma \rangle$, we see that $|G : N\langle \sigma \rangle| = 2$. Otherwise we can assume that $\tau \in N$. Next we show that $\sigma^f \in N$. We have $\lambda_{f/2}(\sigma^f) \equiv \zeta^{f^2e/2} \equiv 1 \pmod{p}$. Let $\omega = \lambda_{f/2}(\sigma^f)$. We know that ω is an n th root of unity where n is a positive integer and $(n, p) = 1$. If $\omega = 1$, then $\sigma^f \in N$. Assume on the contrary that $\omega \neq 1$. Let q be a prime number dividing n and let $\zeta = \omega^{n/q}$. Then ζ is a primitive q th root of unity, and $\zeta \neq 1$. From $\zeta^q = 1$, we have $(\zeta - 1)(\zeta^{q-1} + \zeta^{q-2} + \cdots + 1) = 0$. Since $\zeta \neq 1$, $\zeta^{q-1} + \zeta^{q-2} + \cdots + 1 = 0$. Taking module p on both sides, we get $q \equiv 0 \pmod{p}$. This is a contradiction. Hence $\sigma^f \in N$, and thus $G = N\langle \sigma^e \rangle$. By the isomorphism theorem, we have $|G : N| = |\langle \sigma^e \rangle : \langle \sigma^e \rangle \cap N|$. Since the order of $\langle \sigma^e \rangle$ is a 2-power by assumption, we conclude that the index of N is a power of 2. Since N is a proper subgroup, G contains a normal subgroup of index 2.

Case (B). From Table V, we have

$$\begin{aligned} \sum_{i=0}^{f-1} \frac{((-1)^{ie+1})^2(-\zeta^{ie})}{\lambda_i(1)} + \sum_{i=0}^{f-1} \frac{(\tau_i(-1)^{ie+1})^2(-\tau_i\zeta^{ie})}{\theta_i(1)} \\ + \sum_{i=0}^{f-1} \sum_{m=1}^{(p-1)/2} \frac{(2(-1)^{ie+1})^2(\omega^m + \omega^{-m})\zeta^{ie}}{\chi_i^m(1)} = 0. \end{aligned}$$

Procedures similar to Case (A) yield

$$\theta_{f/2}(1)^2 - \tau_{f/2}\chi_0^m(1)\theta_{f/2}(1) - \chi_0^m(1) - 1 = 0.$$

If $\tau_{f/2} = 1$, then

$$[\theta_{f/2}(1) + 1][\theta_{f/2}(1) - (1 + \chi_0^m(1))] = 0.$$

Since $\theta_{f/2}(1) + 1 \neq 0$, so $\theta_{f/2}(1) = 1 + \chi_0^m(1)$. It follows that $\lambda_{f/2}(1) = \chi_0^m(1) - \theta_{f/2}(1) = \chi_0^m(1) - 1 - \chi_0^m(1) = -1$; this is a contradiction. Therefore, $\tau_{f/2} = -1$. Then we have

$$[\theta_{f/2}(1) - 1][\theta_{f/2}(1) + 1 + \chi_0^m(1)] = 0.$$

Since $\theta_{f/2}(1) + 1 + \chi_0^m(1) \neq 0$, so $\theta_{f/2}(1) = 1$. Thus $\theta_{f/2}$ is a linear character. Now by the same argument as Case (A), we get the desired conclusion.

REFERENCES

1. Richard Brauer, *On groups whose order contains a prime number to the first power*. I, Amer. J. Math. **64** (1942), 401–420. MR 4, 1.
2. Richard Brauer, Michio Suzuki and G. E. Wall, *A characterization of the one-dimensional unimodular projective groups over finite fields*, Illinois J. Math. **2** (1958), 718–745. MR 21 #3487.
3. Richard Brauer and K. A. Fowler, *On groups of even order*, Ann. of Math. (2) **62** (1955), 565–583. MR 17, 580.
4. Larry Dornhoff, *Group representation theory*. Part A: *Ordinary representation theory*; Part B: *Modular representation theory*, Pure and Appl. Math., vol. 7, Dekker, New York, 1972. MR 50 #458a, b.
5. Daniel Gorenstein, *Finite groups*, Harper and Row, New York and London, 1968. MR 38 #229.
6. Donald G. Higman, *Finite groups with 3 to the first power*, Univ. of Michigan and Univ. of British Columbia (preprint).
7. Charles W. Curtis and Irving Reiner, *Representation theory of finite groups and associative algebras*, Pure and Appl. Math., vol. 11, Interscience, New York, 1962. MR 26 #2519.
8. Leo J. Alex, *Simple groups of order $2^a 3^b 5^c 7^d p$* , Trans. Amer. Math. Soc. **173** (1972), 389–399. MR 47 #6838.
9. ———, *On simple groups of order $2^a \cdot 3^b \cdot 7^c \cdot p$* , J. Algebra **25** (1973), 113–124. MR 47 #8675.
10. ———, *Index two simple groups*, J. Algebra **31** (1974), 262–275. MR 50 #7320.

DEPARTMENT OF APPLIED MATHEMATICS, NATIONAL CHUNG-HSING UNIVERSITY, TAICHUNG, TAIWAN, REPUBLIC OF CHINA