A CHARACTERIZATION OF THE GROUPS $LF(2, q)$

BY
KOICHIRO HARADA

1. Introduction

Let G be a finite group satisfying the following condition ($\#$):

G has a subgroup S such that

($\#$) (1) *the centralizer of any non-identity of element A is A,*

(2) *the order of the normalizer of A is* $2 \cdot |A|$, *where* $|A|$ *denotes the order of A.*

We call a finite group G satisfying the condition ($\#$) simply a ($\#$)-group. The letter A always denotes a subgroup of G which satisfies (1) and (2) of the condition ($\#$). We call A a *special* subgroup of G. We first remark that A is an abelian subgroup of G and its order is odd, since A has a fixed-point-free automorphism of order 2.

As is well known, the classical groups $LF(2, q)$ and the Suzuki groups $Sz(q)$ are ($\#$)-groups. In fact, if $q = 2^n > 2$, the cyclic subgroups of $LF(2, q)$ of order $q + 1$ and of order $q - 1$ satisfy the conditions (1) and (2). If $q \equiv \varepsilon \pmod 4$, where $\varepsilon = \pm 1$, then the cyclic subgroups of order $\frac{1}{2}(q + \varepsilon)$ of $LF(2, q)$ are special. The cyclic subgroups of order $q - 1$ of the Suzuki group of order $q^2(q - 1)(q^2 + 1)$ also have the property ($\#$). Besides examples mentioned above, the Sylow 5-groups of $LF(3, 4)$ are special. In any case their special subgroups are cyclic.

In this paper we shall first prove the following Theorem A and Theorem A$'$.

THEOREM A. *If G is a solvable ($\#$)-group, then there exists a nilpotent normal subgroup N of G such that G/N is isomorphic to a generalized dihedral group.*

Here a generalized dihedral group is defined as follows. Let H be an abelian group and τ be an automorphism of H such that if $h \in H$, $h^\tau = h^{-1}$, where h^τ denotes the image of h by τ. Under these conditions holomorph of H by τ is called a generalized dihedral group.

THEOREM A$'$. *If G is a non-solvable ($\#$)-group, then G has a nilpotent normal subgroup N such that G/N is a simple ($\#$)-group.*

In case of a non-solvable ($\#$)-group G we shall add another condition:

(i) *G has two non-conjugate special subgroups* A_1 *and* A_2 *or*

(ii) $|G| \leq 4(|A| + 1)^3$.

We remark here that $LF(2, 2^n)$ $(2^n > 2)$ have the property (i) and LF$(2, q)$ $(q > 3)$ have the property (ii). We shall prove

Received October 1, 1966.

THEOREM B. *Let G be a simple ($\#$)-group. If G satisfies the condition* (i), *then G is isomorphic to $LF(2, 2^n)$, where $2^n > 2$.*

THEOREM C. *Let G be a simple ($\#$)-group. If G satisfies the condition* (ii), *then G is isomorphic to $LF(2, q)$, where $q = p^n > 3$.*

Before proving our Theorem B and Theorem C, we shall prove Theorem 1 which will be stated in Section 3. Our idea to prove Theorem 1 is essentially the same as that of R. Brauer, M. Suzuki and G. E. Wall [1]. In their paper [3], W. Feit and J. G. Thompson have considered the simple groups satisfying the condition ($\#$) with $|A| = 3$, and they have proved that $LF(2, 5)$ and $LF(2, 7)$ are the only such groups. Therefore in this paper we assume $|A| \geq 5$, and this restriction is rather essential in our proof. The argument of this paper relies heavily on the theory of group characters. Most of the notation are standard. All groups considered are finite.

Finally, the author wishes to express his thanks to Prof. M. Suzuki for his kind encouragement and advice. Due to his suggestions the proof of Theorem B was made considerably shorter than the author's original one. Moreover the author expresses his thanks to Dr. T. Kondo for his helpful guidance throughout this work.

2. Proof of Theorem A and Theorem A′

LEMMA 1. *Let G be a ($\#$)-group and A a special subgroup of G. Then*

(a) *A is a T.I. set[1] in G,*

(b) *A is a Hall subgroup of G,*

(c) *$N_G(A)$ is a generalized dihedral group,*

(d) *$N_G(B) = N_G(A)$ holds for any subgroup $B \neq 1$ of A.*

Proof. If a conjugate subgroup $x^{-1}Ax$ of A contains an element $a \neq 1$ of A, then the centralizer $C_G(\langle a\rangle)$ of $\langle a\rangle$ contains both A and $x^{-1}Ax$. By the condition (1) of ($\#$), $x \in N_G(A)$. Hence A is a T.I. set in G. $N_G(A)$ is clearly a generalized dihedral group, since $a^\tau = a^{-1}$ for $a \in A$, $\tau \in N_G(A) - A$. The last statement of Lemma 1 is easy to prove, since A is a T.I. set in G. A is a Hall subgroup of G, since $N_G(P) = N_G(A)$ for any p-Sylow subgroup of A.

LEMMA 2. *There exists a nilpotent normal subgroup N of G such that the factor group G/N is isomorphic to*

(i) *a generalized dihedral group of order $2|A|$, or*

(ii) *a simple ($\#$)-group.*

Proof. Let M be a maximal normal subgroup of G.

Case (I) $(|M|, |A|) \neq 1$. Let p be a prime number dividing $(|M|, |A|)$, and P be a p-Sylow subgroup of M. Using Frattini argument we have $N(P)M = G$. Since A is a Hall subgroup of G by Lemma 1, we can suppose

[1] A subset H of G is called a T.I. set in G, when H satisfies the following condition:

if $x \in G$ and $H \cap H^x > \{1\}$ then $H^x = H$, (cf. [4]).

$P \subset A$. By Lemma 1, $N(P) = N(A)$. Hence $|G/M| = 2$ or p', where p' is a prime number dividing $|A|$. Let us assume $|G/M| = p'$. Then all the involutions in G are contained in M. In particular $\tau \in M$ for $\tau \in N(A) - A$. Hence $\tau^a = \tau a^2 \in M$ for $a \in A$, and $a^2 \in M$ holds. Since A is a group of odd order, we have $M \supset A$. This contradicts with $|G/M| = p'$. Therefore we have $|G/M| = 2$. Next we will show that $x \in M$ and $A \cap A^x \neq \{1\}$ imply $x \in A$. Since $|G/M| = 2$ and $G = M \cdot N(A)$, we have $N(A) \cap M = A$. Since A is a T.I. set, $A \cap A^x \neq \{1\}$ implies that $x \in N(A)$. Then $x \in N(A) \cap M = A$, as required. By Frobenius' famous theorem there exists a characteristic subgroup N of M which satisfies $M = A \cdot N$ and $A \cap N = \{1\}$. The nilpotency of N follows from a theorem of Thompson [10]. The normality of N in G is obvious. Since $G/N \cong N(A)$, we have proved the lemma in this case.

Case (II) $(|M|, |A|) = 1$. Since an element of $A - \{1\}$ induces on M a fixed-point-free automorphism, M is nilpotent (Thompson [10]). We shall show that the factor group $\bar{G} = G/M$ is a ($*$)-group. Put $N_G(A) = \langle \tau, A \rangle$. If $\tau \in M$, then $[\tau, A] \subset A \cap M = 1$. This is a contradiction. Hence $\tau \notin M$. Let a be an element of $A - \{1\}$ and $\bar{x}$ be an element of $C_{\bar{G}}(\bar{a})$. Since x normalizes the group $\langle a, M \rangle$ and $(|\langle a \rangle|, |M|) = 1$, we have $\langle a \rangle^x = \langle a \rangle^y$, $y \in M$ by Schur's splitting theorem. Hence $xy^{-1} \in N(\langle a \rangle) = N(A)$ and $x \in \langle \bar{\tau}, \bar{A} \rangle$ holds. However $\bar{\tau} \neq \bar{1}$ and $\bar{\tau}$ does not centralize $\bar{a}$. Hence $\bar{x} \in \bar{A}$. This proves the condition (1) of ($*$). As for the condition (2), using the same argument above, we can easily prove that $[N_{\bar{G}}(\bar{A}) : \bar{A}] = 2$. Changing the letter M into N in this case, we have proved the lemma.

Theorem A and Theorem A′ are easy consequences of this lemma.

3. Character theory

The theory of exceptional characters has been developed by R. Brauer, M. Suzuki (cf. [6], [7]) and others. In this section we apply it to compute the order of G. We summarize here their results which are necessary to our proof.

Let G be a finite group, and let G have a subgroup A satisfying the following condition:

A is the centralizer of every element $\neq 1$ of A. (In M. Suzuki's paper [7], the theory has been constructed under a more general condition.)

Let n denote the order of A, m the index $[N_G(A) : A]$ and put $w = n - 1/m$. If $w > 1$ then there exist exactly w irreducible characters (exceptional characters associated with A, or simply A-characters cf. [6]) such that X_i is not constant on $A - \{1\}$ for $i = 1, \cdots, w$. If an element x is not conjugate to any element of $A - \{1\}$, then we have $X_i(x) = X_1(x)$. If an irreducible character Y is non-exceptional, Y takes a constant value c on $A - \{1\}$ and degree $Y \equiv c \pmod{n}$. We have a linear combination

$$1 + \varepsilon X_i + a \sum_{j=1}^{w} X_j + \sum cY$$

which vanishes on elements not conjugate to an element of $A - \{1\}$. Here 1 is the principal character of G, $\varepsilon = \pm 1$, a is a certain integer and the second summation ranges over all the non-exceptional characters except 1. We have moreover

$$1 + (a+\varepsilon)^2 + (w-1)a^2 + \sum c^2 = m+1.$$

Now we apply the above results to our ($\#$)-group G. In this case

$$[N(A):A] = 2, \qquad |A| = n.$$

By the assumption $n \geq 5$ we have $w = (n - 1/2) \geq 2$. There are w exceptional characters associated with A, namely $X_1, \cdots, X_w$. We have a linear combination ψ of irreducible characters of weight 3, which vanishes on elements not conjugate to any element of $A - \{1\}$. ψ contains the principal character of G with multiplicity 1, and at least one exceptional character. Since $\psi(1) = 0$, we have

$$\psi = 1 - \varepsilon X_i + \varepsilon Y \qquad (\varepsilon = \pm 1),$$

where Y is an irreducible character of G.

Let $Dg(X)$ denote the degree of a character X of G. Since $\psi(1) = 0$, $Dg(X_i) \neq Dg(Y)$. Hence Y is non-exceptional. We have

$$Dg(Y) = kn + \varepsilon \quad \text{and} \quad Y(a) = \varepsilon \quad \text{if} \quad 1 \neq a \in A,$$

where k is a non-negative integer. Then $Dg(X_i) = kn + 2\varepsilon$. All the irreducible characters of G other than 1, $X_1, \cdots, X_w$ and Y have degrees divisible by n and vanish on $A - \{1\}$. We summarize the results in the following lemma.

LEMMA 3. *Let G be a ($\#$)-group and A a special subgroup of G. There is a generalized character*

$$\psi = 1 - \varepsilon X_i + \varepsilon Y \qquad (\varepsilon = \pm 1)$$

which vanishes on the set of all those elements which are not conjugate to any element of $A - \{1\}$. X_i is an A-character and Y is a non-principal, non-exceptional irreducible character. We have

$$Dg(X_i) = kn + 2\varepsilon \quad \textit{and} \quad Dg(Y) = kn + \varepsilon$$

for some non-negative integer k, and

$$Y(a) = \varepsilon \qquad \textit{if} \quad a \in A - \{1\}.$$

Moreover if Z is an irreducible character of G other than 1, $X_1, \cdots, X_w$ and Y, then

$$Dg(Z) = nz \quad \textit{and} \quad Z(a) = 0, \qquad a \in A - \{1\}.$$

Let G be a ($\#$)-group, and D the set of elements in G which are conjugate to an element $\neq 1$ of A.

LEMMA 4. *Under the same notation as above*

(i) $X_1(g) = \cdots = X_w(g)$, $Y(g) = X_1(g) - \epsilon$ *for* $g \in G - D$

(ii) $X_1(h) + \cdots + X_w(h) = -\varepsilon,$
$X_1(h)\cdot X_1(h^{-1}) + \cdots + X_w(h)\cdot X_w(h^{-1}) = n - 2$ *for* $h \in D$.

Proof. (i) is an immediate consequence of the theory exceptional characters and of Lemma 3. From the orthogonality relations of group characters follow two equalities

$$\sum \zeta_\mu(h)\cdot\zeta_\mu(1) = 0, \qquad h \in D,$$

and

$$\sum \zeta_\mu(h)\cdot\zeta_\mu(h^{-1}) = |C_G(h)| = n, \qquad h \in D,$$

where ζ_μ ranges over all the irreducible characters of G. (ii) is an easy consequence of these equalities.

The following argument on the group algebra is essentially due to Brauer and Fowler [2].

Let Γ be the group algebra of a ($\divideontimes$)-group G over the field of rational numbers. Let $\mathfrak{K}_0, \cdots, \mathfrak{K}_s$ denote the classes of conjugate elements of G such that $\mathfrak{K}_0 \ni 1$ and $\mathfrak{K}_1, \cdots, \mathfrak{K}_w$ contain at least one element of $A - \{1\}$. Let g_i denote a representative element of $\mathfrak{K}_i$. Let K_i denote the sum of the elements in $\mathfrak{K}_i$; then $K_0, \cdots, K_s$ form a basis of the center of Γ. In particular, we have an equation

$$K_i^2 = \sum_{j=0}^{s} c_j^i K_j \qquad \text{for } 0 \leq i \leq s. \tag{3}$$

It follows easily from the basic properties of the group characters that the coefficients c_j^i in (3) are given by the formula

$$c_j^i = \frac{|G|}{|C(g_i)|^2}\cdot\sum\frac{\zeta_\mu(g_i)^2\cdot\zeta_\mu(g_j^{-1})}{\zeta_\mu(1)}$$

where ζ_μ ranges over all the irreducible characters of G.

LEMMA 5. *Under the same notation as above we have*

$$c_i^j = \frac{|G|(kn + \varepsilon - Y(g_j))^2}{|C(g_j)|^2(kn + 2\varepsilon)(kn + \varepsilon)}$$

where $1 \leq i \leq w$, $w + 1 \leq j \leq s$, *and*

$$c_j^i = \frac{G}{n^2}\left[1 + \frac{n - 2}{kn + 2\varepsilon} X_1(g_j) + \frac{Y(g_j)}{kn + \varepsilon}\right]$$

where $1 \leq i \leq w$, $w + 1 \leq j \leq s$.

Proof. First, for $1 \leq i \leq w$, $w + 1 \leq j \leq s$, we have

$$c_i^j = \frac{|G|}{|C(g_j)|^2}\left[1 + \frac{X_1(g_j)^2}{kn + 2\varepsilon}\sum_{l=1}^{w} X_l(g_i) + \frac{Y(g_j)^2\varepsilon}{kn + \varepsilon}\right].$$

By Lemma 4

$$\sum_{l=1}^{w} X_l(g_i) = -\varepsilon \quad\text{and}\quad X_1(g_j)^2 = (Y(g_j) + \varepsilon)^2.$$

Hence

$$c_i^j = \frac{|G|}{|C(g_j)|^2}\left[1 + \frac{(Y(g_j)+\varepsilon)^2}{kn+2\varepsilon}(-\varepsilon) + \frac{(Y(g_j))^2\varepsilon}{kn+\varepsilon}\right]$$
$$= \frac{|G|}{|C(g_j)|^2}\frac{(kn+\varepsilon-(Y(g_j))^2}{(kn+2\varepsilon)(kn+\varepsilon)}.$$

Secondly for $1 \leq i \leq w$, $w+1 \leq j \leq s$, we have by Lemma 4,

$$c_j^i = \frac{|G|}{|C(g_j)|^2}\left[1 + \frac{n-2}{kn+2\varepsilon}X_1(g_j) + \frac{Y(g_j)}{kn+\varepsilon}\right].$$

The next corollary is due to M. Suzuki [8].

COROLLARY 1. *If G is a simple $(\#)$-group, then all the involutions in G are contained in a single conjugate class of G.*

Proof. We first remark that in a generalized dihedral group of order $2n$ (n odd) all the involutions are contained in a single class.

Let u be any involution of G. If we can prove that there exist $x, y \in G$ such that $u \cdot u^x = a^y$ for $a \in A - \{1\}$, then u is contained in $N(A)^y$. This follows from $a^{yu} = (a^y)^{-1}$. Hence u is conjugate to τ, where τ is an involution in $N(A)$. On the other hand, by Lemma 5 and the simplicity of G, we have $c_i^j \neq 0$ for $1 \leq i \leq w$, $w+1 \leq j \leq s$. Hence our corollary is proved.

LEMMA 6. *If G is a $(\#)$-group, then the order of G is written in the form*

$$|G| = n(kn+2\varepsilon)(kn+\varepsilon)\left[\frac{|C(\tau)|}{kn+\varepsilon-Y(\tau)}\right]^2,$$

where τ is an involution in $N(A)$.

Proof. Suppose $\tau \in \mathfrak{K}_{w+1}$. Then $c_i^{w+1} \neq 0$ for $1 \leq i \leq w$, since

$$\tau\cdot\tau^a = \tau\cdot\tau a^2 = a^2 \neq 1, \qquad \text{for} \quad a \in A - \{1\}.$$

From the theorem (4A) of R. Brauer and K. A. Fowler [2], the integer c_i^{w+1} is the number of elements of order 2 which satisfy the equation

$$\sigma^{-1}a_i\sigma = a_i^{-1}, \qquad a_i \in \mathfrak{K}_i \qquad \text{for} \quad 1 \leq i \leq w.$$

By Lemma 1, $N(A) = N(\langle a_i\rangle)$. Hence

$$c_i^{w+1} = n = |N(A) - A|.$$

From this follows the lemma.

Throughout the rest of this paper τ denotes a fixed involution of $N(A)$, and we put

$$m = \frac{|C(\tau)|}{|kn+\varepsilon-Y(\tau)|}.$$

LEMMA 7. *Under the same notation as in Lemma 6, m is an integer and*

$$m^2 \equiv 1 \pmod{n}.$$

Proof. From $Dg(Y) = kn + \varepsilon$, $Dg(X_i) = kn + 2\varepsilon$ and from the fact that n, $kn + 2\varepsilon$, $kn + \varepsilon$ are relatively prime to each other follows that $|G|$ is divisible by $n(kn + 2\varepsilon)(kn + \varepsilon)$. Hence m is an integer.

From the equality

$$|G| = \sum (Dg(\zeta_\mu))^2 \equiv 1 + (n - 1/2)(kn + 2\varepsilon)^2 + (kn + \varepsilon)^2 \pmod{n^2}$$

we get

$$2nm^2 \equiv 2n \pmod{n^2}.$$

Hence

$$m^2 \equiv 1 \pmod{n}.$$

Throughout the rest of this section, we assume that G is a non-solvable ($\divideontimes$)-group. In particular, we assume $k > 0$ in Lemmas 3–9.

We set

$$\pi_0 = \{p \mid \text{prime number such that } p \mid n\},$$

$$\pi_1 = \{q \mid \text{prime number such that } q \mid kn + 2\varepsilon\},$$

$$\pi_2 = \{r \mid \text{prime number such that } r \mid kn + \varepsilon\}.$$

LEMMA 8. *Let G be a non-solvable ($\divideontimes$)-group. Suppose $m = 1$; then G contains only π_0-, π_1-, π_2-elements, and the centralizer of a π_i-element is a π_i-subgroup of G for $i = 0, 1, 2$.*

Proof. Let p, q be primes such that $p \mid kn + 2\varepsilon$, $q \mid kn + \varepsilon$. If G has an element x of order pq, then x is both a p-singular element and a q-singular one. Since X_i belongs to a p-block of defect 0 and Y belongs to a q-block of defect 0, we have $X_i(x) = 0$ and $Y(x) = 0$. Hence $\psi(x) = 1 \neq 0$. This is a contradiction, because x is not conjugate to any element of $A - \{1\}$. By the condition (1) of ($\divideontimes$) and by the fact above, we have proved the lemma.

Throughout the rest of this section, we assume that $m = 1$.

Let $a_1, \cdots, a_w$; $b_1, \cdots, b_t$; $c_1, \cdots, c_u$ be representative of the conjugate classes of π_0-, π_1-, π_2-elements respectively. From the theory of modular characters we have

$$X_1(b_j) = \cdots = X_w(b_j) = 0, \qquad \text{for } 1 \leq j \leq t.$$

Using ψ we obtain

$$Y(b_j) = -\varepsilon, \qquad \text{for } 1 \leq j \leq t.$$

In the same way we obtain

$$X_1(c_l) = \cdots = X_w(c_l) = \varepsilon, \quad \text{and} \quad Y(c_l) = 0, \qquad \text{for } 1 \leq l \leq u.$$

By Lemma 1,

$$Y(a_i) = \varepsilon \quad \text{and} \quad Z(z_i) = 0, \qquad \text{for } 1 \leq i \leq w.$$

TABLE 1

	1	X_1	$\cdots$	X_w	Y	Z_1	$\cdots$	Z_r
1	1	$kn + 2\varepsilon$	$\cdots$	$kn + 2\varepsilon$	$kn + \varepsilon$	nz_1	$\cdots$	nz_r
a_1	1				ε	0	$\cdots$	0
$\vdots$	$\vdots$				$\vdots$	$\vdots$		
a_w	1				ε	0	$\cdots$	0
b_1	1	0	$\cdots$	0	$-\varepsilon$			
$\vdots$	$\vdots$				$\vdots$			
b_t	1	0	$\cdots$	0	$-\varepsilon$			
c_1	1	ε	$\cdots$	ε	0			
$\vdots$	$\vdots$				$\vdots$			
c_u	1	ε	$\cdots$	ε	0			

Let E be a subset of G which consists of all the π_2-elements in G.

LEMMA 9. *Under the same notation as above we have*

$$|E| = kn(kn + 2\varepsilon).$$

Proof. From the orthogonality relations of group characters we have

$$\textstyle\sum_{x\in G} X_1(x)\overline{Y(x)} = 0.$$

Hence we get

$$\textstyle\sum_{i=1}^{w} X_1(a_i) = -\varepsilon.$$

Therefore we conclude

$$0 = \textstyle\sum_{x\in G} X_1(x) = (kn + 2\varepsilon) - \varepsilon(kn + 2\varepsilon)(kn + \varepsilon) + \varepsilon|E|.$$

This proves the lemma.

THEOREM 1. *Let G be a non-solvable $(\divideontimes)$-group. If $m = 1$ and $k = 1$ or 2, then G is isomorphic to $LF(2, q)$ where $q = p^\alpha > 3$.*

Proof. *Case* (I) $k = 1$. In this case

$$|G| = n(n + 2\varepsilon)(n + \varepsilon).$$

Since $n + \varepsilon$ is even, $Y(\tau) = 0$. Hence

$$C(\tau) = |kn + \varepsilon - Y(\tau)| = n + \varepsilon.$$

By Lemma 9, $|E| = n(n + 2\varepsilon)$. Since the centralizer of a π_2-element is a π_2-subgroup of G, this implies that $C_G(\tau)$ has only one conjugate class in G. Therefore $C(\tau)$ is an elementary abelian 2-group. Let B be a cylcic subgroup of G of even order; then $|B| = 2$. Since G has no linear character other than the principal character, G coincides with its commutator subgroup. Hence all the conditions of the theorem of Brauer, Suzuki and Wall [1] are satisfied.

Since $C(\tau)$ is an elementary abelian 2-group, we conclude that $G \cong LF(2, 2^{\alpha})$ where $\alpha > 1$ is an integer.

Case (II) $k = 2$. In this case

$$G = n(2n + 2\varepsilon)(2n + \varepsilon).$$

By Lemma 9, we have $|E| = 2n(2n + 2\varepsilon)$. Since the centralizer of a π_2-element is a π_2-subgroup of G, we can conclude that $2n + \varepsilon$ is a power of odd prime p and there exist two conjugate classes of p-element. Put $2n + \varepsilon = p^{\beta}$. Let P be a Sylow p-subgroup of G. Next argument on the structure of P and $N_G(P)$ and on the conclusion of our theorem is due to Brauer, Suzuki and Wall [1]. For the reader's convenience sake, we quote their argument, modifying to our case.

First we shall prove that P is abelian. If P consists of the identity and two real classes, then from the theorem (4D) of Brauer and Fowler [2] we can conclude that P is abelian.

If P consists of the identity and two non-real classes, we apply the Lemma (II.0) of R. Brauer, M. Suzuki and G. E. Wall's paper [1], which we quote here.

LEMMA 10. *Let G be any finite group. Let p be a prime dividing the order of G. Let us assume the following properties;*

(a) *If σ is an element of prime order $q^{\gamma} > 1$ and $p \neq q$ then the order of $C(\sigma)$ is not divisible by p;*

(b) *A generalized quaternion group does not appear as a subgroup of G.*

Then either the p-Sylow group of G is normal in G or any two distinct p-Sylow groups have intersection 1.

In our group G, under the condition $m = 1$ and non-solvability, assumption (a) holds by Lemma 8. As for (b), if we can prove that for any p-subgroup $P_1 \neq 1$ of G, $|N(P_1)|$ is not divisible by 2, then the proof of Lemma 10 is available (cf. [1]). However a p-Sylow group P of G has no real element in G and an involution of G does not commute with any p-element, hence $|N(P_1)|$ is not divisible by 2. Clearly P is not a normal subgroup of G, so we have proved that p-Sylow groups of G is a T.I. set in G.

Let P be a Sylow p-subgroup of G, and ρ be any element $\neq 1$ of P. Since $|C(\rho)| = p^{\beta}$, we have $C(\rho) = P^x$, $x \in G$. Since $P^x \cap P \ni \rho$, we have $x \in N(P)$. Thus we have proved that P is abelian.

From Lemma 8, the centralizer of any element $\neq 1$ of P is P. Hence two elements of P are conjugate in G, if and only if they are conjugate in $N(P)$. Since P consists of the identity and two classes we have

$$[N(P):P] = (p^{\beta} - 1)/2 = (2n + \varepsilon - 1)/2.$$

It follows that G has a representation as a transitive group of permutations in $2n$ letters in case $\varepsilon = -1$ and $2n + 2$ letters in case $\varepsilon = 1$ respectively. Observing Table 1, we can conclude that the character of this permutation representation is $1 + Y$. Hence this representation Θ is doubly transitive and no element except the identity leaves three letters fixed, and the order of the subgroup of G leaving two letters fixed is $n - 1 = (p^\beta - 1)/2$ in case $\varepsilon = -1$, and $n = (p^\beta - 1)/2$ in case $\varepsilon = 1$ respectively.

We now apply Zassenhaus' theorem (cf. [11], [1]). Thus we can conclude that

$$G \cong LF(2, p^\beta) \qquad (p^\beta > 3).$$

4. Proof of the main theorem

In this section G denotes always a simple ($\divideontimes$)-group. We shall prove that the hypothesis of Theorem 1 is satisfied if G satisfies one of the following conditions:

(i) *G has two non-conjugate special subgroups A_1 and A_2*,

(ii) $|G| \leq 4(|A| + 1)^3$.

We first assume that G satisfies the condition (i). Put

$$A_1 = n_1 \quad \text{and} \quad A_2 = n_2 \qquad \text{where} \quad n_1 > n_2 \geq 5.$$

Let X_i^1 $(1 \leq i \leq w_1 = n_1 - \frac{1}{2})$ be A_1-characters and $Y^1 \neq 1$ be the non-exceptional irreducible character which does not vanish on $A_1 - \{1\}$. Let X_j^2 $(1 \leq j \leq w_2 = n_2 - \frac{1}{2})$ and Y^2 be defined for A_2 in the same way as in the case of A_1. Put

$$Dg(X_i^1) = k_1 n_1 + 2\varepsilon_1, \quad Dg(Y^1) = k_1 n_1 + \varepsilon_1, \quad \varepsilon_1 = \pm 1,$$
$$Dg(X_j^2) = k_2 n_2 + 2\varepsilon_2, \quad Dg(Y^2) = k_2 n_2 + \varepsilon_2, \quad \varepsilon_2 = \pm 1.$$

Since G has only one conjugate class of involutions (Corollary 1) we can set

$$m_1 = |C(\tau)|/|k_1 n_1 + \varepsilon_1 - Y(\tau)|, \qquad m_2 = |C(\tau)|/|k_2 n_2 + \varepsilon_2 - Y(\tau)|$$

where τ is an involution in $N(A_1)$.

By Lemma 6 we have two equalities

$$|G| = n_1(k_1 n_1 + 2\varepsilon_1)(k_1 n_1 + \varepsilon_1)m_1^2,$$

$$|G| = n_2(k_2 n_2 + 2\varepsilon_2)(k_2 n_2 + \varepsilon_2)m_2^2.$$

LEMMA 11. *Under the same notation as above we have*

(i) $Y^1 = Y^2, k_1 = k_2 = 1, \varepsilon_1 = -\varepsilon_2 = -1, m_1 = m_2, n_1 - n_2 = 2,$

(ii) $D_g(X_i^1) = n_1 - 2, Dg(Y_1) = n_1 - 1, Dg(X_j^2) = n_1,$

(iii) $Y^1(a_1) = -1$ *for* $a_1 \in A_1 - \{1\},$

$Y^1(a_2) = 1$ *for* $a_2 \in A_2 - \{1\},$

(iv) $|G| = n_1(n_1 - 1)(n_1 - 2)m_1^2.$

Proof. By Lemma 3 and $k > 0$ we first remark that if an irreducible character W of G has same degree as X_i^1 (or X_j^2), then W is an element of

$$\{X_i^1, 1 \leq i \leq w_1\}$$

(or $\{X_j^2, i \leq j \leq w_2\}$) and if W has same degree as Y^1 (or Y^2) then $W = Y^1$ (or Y^2).

Let 1, X_i^1 $(1 \leq i \leq w_1)$, Y^1, X_j^2 $(1 \leq j \leq w_2)$, $U_1, \cdots, U_t$ be all the irreducible characters of G. Assume $Y^1 \neq Y^2$. Since $Y^2 \neq X_i^1$ for $1 \leq i \leq w_1$, we have $Y^2 = U_l$. Hence by Lemma 3, $Dg(X_1^1)$ and $Dg(Y^1)$ are divisible by n_2. This is impossible, since $k_1 n_1 + 2\varepsilon_1$ and $k_1 n_1 + \varepsilon_1$ are relatively prime to each other. Thus $Y^1 = Y^2$ and so

$$k_1 n_1 + \varepsilon_1 = k_2 n_2 + \varepsilon_2 .$$

Therefore $m_1 = m_2$. Since

$$Dg(X_1^2) = k_2 n_2 + 2\varepsilon_2 = k_1 n_1 + \varepsilon_1 + \varepsilon_2 \equiv 0 \pmod{n_1},$$

we obtain

$$\varepsilon_1 = -\varepsilon_2 .$$

Since

$$k_1 n_1 + 2\varepsilon_1 = k_2 n_2 + \varepsilon_2 + \varepsilon_1 = k_2 n_2 , \tag{4}$$

we obtain

$$|G| = n_1 k_2 n_2 (k_1 n_1 + \varepsilon_1) m_1^2 . \tag{5}$$

Since $k_2 n_2 + 2\varepsilon_2 = k_1 n_1$, we get

$$\begin{aligned} |G| &= n_2 k_1 n_1 (k_2 n_2 + \varepsilon_1) m_2^2 \\ &= n_2 k_1 n_1 (k_1 n_1 + \varepsilon_1) m_1^2 . \end{aligned} \tag{6}$$

By (5) and (6) we have $k_1 = k_2$.

From (4) follows

$$k_1 n_1 - k_2 n_2 = k_1(n_1 - n_2) = -2\varepsilon_1 .$$

Hence we have

$$k_1 = 1, \qquad n_1 - n_2 = 2, \qquad \varepsilon_1 = -1,$$

and

$$|G| = n_1(n_1 - 1)(n_1 - 2)m_1^2 .$$

Thus the lemma is proved.

Now we take off the suffix 1 of A_1, n_1, m_1, X_i^1 $(1 \leq i \leq w_1)$ and Y^1. Let F *be a subset of* G which is consisted of elements which are conjugate no elements of $A - \{1\}$ or $A_2 - \{1\}$.

Next we shall prove

LEMMA 12.

(i) $0 \leq Y(g) < n - 1$ *for* $g \in F$,

(ii) $\sum_{g \in F} Y(g)^2 = (m^2 - 1)(n - 1)^2$,

(iii) $\sum_{g \in F} Y(g) = (m^2 - 1)(n - 1)$.

Proof. Use the same notation as in Section 3 and let $a \in \mathfrak{K}_1$ ($a \in A - \{1\}$) and $g \in \mathfrak{K}_v$ for $g \in F$. By Lemma 5 we have

$$c_v^1 = \frac{|G|}{n^2} \cdot \left[1 + \frac{n-2}{n-2} X_1(g) + \frac{Y(g)}{n-1}\right]$$
$$= (n-2)m^2 Y(g) \geq 0 \qquad \text{for } g \in F.$$

(i) follows from the fact above and the simplicity of G. (ii) follows from the orthogonality relation

$$\sum_{g \in F} Y(g)Y(g^{-1}) = \sum_{g \in F} Y(g)^2$$
$$= |G| - (n-1)^2 - \frac{|G|}{2n}(n-1) - \frac{|G|}{2(n-2)}(n-3)$$
$$= (m^2 - 1)(n-1)^2.$$

(iii) follows from

$$\sum_{g \in F} Y(g) = -(n-1) - \frac{G}{2n}(n-1)\varepsilon_1 - \frac{G}{2(n-2)}(n-3)\varepsilon_2$$
$$= (m^2 - 1)(n-1).$$

Now we shall show that $m = 1$. By (ii), (iii) of Lemma 12 we get

$$\sum_{g \in F} Y(g)(n - 1 - Y(g)) = 0.$$

By (i) of Lemma 12 we have $Y(g) = 0$ for $g \in F$. Hence $m = 1$. Thus we have proved that G is isomorphic to $LF(2, q)$ ($q = 2^\alpha > 2$).

Next we assume the condition (ii):

$$|G| \leqq 4(|A| + 1)^3.$$

By the assumption $|A| = n \geq 5$ and by Lemma 7 we have

$$m^2 = 1 \quad \text{or} \quad m^2 \geq 16.$$

Assume $m^2 \neq 1$. Then

$$|G| \geq 16n(kn + 2\varepsilon)(kn + \varepsilon).$$

By the condition (ii) above, we have

$$(n + 1)^3 - 4n(kn + 2\varepsilon)(kn + \varepsilon) \geq 0.$$

Since $k > 0$ we have $(n + 1)^3 - 4n(n - 2)(n - 1) \geq 0$, namely

$$-3n^2(n - 5) - 5n + 1 \geq 0.$$

This is a contradiction. Hence we have $m^2 = 1$.

Next we shall show $k = 1$ or 2. In fact, if $k \geq 3$ then

$$n(3n + 2\varepsilon)(3n + \varepsilon) \leq 4(n + 1)^3.$$

Hence

$$n(3n - 2)(3n - 1) \leq 4(n + 1)^3,$$

and we get

$$5n^2(n - 5) + 4n(n - 5) + 10n - 4 \leq 0.$$

This is a contradiction.

Thus we have proved, by Theorem 1, that G is isomorphic to $LF(2, q)$ $(q = p^\beta > 3)$.

Combining these results and Theorem A, Theorem A′, we have proved the theorems stated in the introduction.

References

1. R. Brauer, M. Suzuki and G. E. Wall, *A characterization of the one-dimensional unimodular projective groups over finite fields*, Illinois J. Math., vol. 2 (1958), pp. 718–745.
2. R. Brauer and K. A. Fowler, *On groups of even order*, Ann. of Math., vol. 62 (1955), pp. 565–583.
3. W. Feit and J. G. Thompson, *Finite groups which contain a self-centralizing subgroup of order 3*, Nagoya Math. J., vol. 21 (1962), pp. 185–197.
4. ———, *Solvability of groups of odd order*, Pacific J. Math., vol. 13 (1963), pp. 775–1029.
5. C. Curtis and I. Reiner, *Representation theory of finite groups and associative algebras*, New York, Interscience, 1962.
6. M. Suzuki, *The nonexistence of a certain type of simple group of odd order*, Proc. Amer. Math., Soc., vol. 8 (1957), pp. 686–695.
7. ———, *On finite groups with cyclic Sylow subgroups for all odd primes*, Amer. J. of Math., vol. 77 (1955), pp. 656–671.
8. ———, *Application of group characters*, Proc. Symposia in Pure Math., vol. 6, Amer. Math. Soc., Institute on Finite Groups, Pasadena, California, 1960.
9. W. Scott, *Group theory*, Englewood Cliffs, New Jersey, Prentice Hall, 1964.
10. J. G. Thompson, *Finite groups with fixed-point-free automorphisms of prime order*, Proc. Nat. Acad. Sci., vol. 45 (1959), pp. 578–581.
11. H. Zassenhaus, *Kennzeichnung endlicher linearer Gruppen als Permutationsgruppen*, Abh. Math. Sem. Univ. Hamburg, vol. 11 (1936), pp. 17–40.

University of Nagoya
Nagoya, Japan