

INVESTIGATIONS ON FINITE GROUPS
OF EVEN ORDER

by
Kenneth A. Fowler

A dissertation submitted in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy in the
University of Michigan
1951

Committee in charge:

Professor Richard D. Brauer, Chairman
Assistant Professor George Piranian
Professor Charles L. Stevenson
Assistant Professor Leonard Tornheim
Professor Raymond L. Wilder

CONTENTS

Section	Page
I Introduction	1
II On the Multiplication of Classes	4
III Proof of Theorem 1	7
IV On the Existence of Blocks of Highest Kind	10
V On Groups Containing No Element of Order 2p for p an Odd Prime	17
VI A Characterization of $LF(2, 2^a)$	24

I. Introduction

Let $\mathcal{G}$ be a group of even order g and let Λ denote the center of the group ring of $\mathcal{G}$ formed with regard to a field of characteristic 0. As is well known, the classes of conjugate elements $K_1, K_2, \dots, K_k$ of $\mathcal{G}$ form a basis of Λ , where each class is interpreted as the sum of its elements. We then have formulae

$$(1) \quad K_i K_j = \sum_t a_{ijt} K_t$$

where the a_{ijt} are rational integers ≥ 0 .

In section II we will obtain some information concerning the multiplication of classes of elements of order 2. These results will have frequent application throughout this paper. They lead easily to our first theorem, which states that $\mathcal{G}$ properly contains a normal subgroup of bounded index, the bound depending only on the ratio of the order of $\mathcal{G}$ to the number of elements of order 2 which are contained in $\mathcal{G}$.

When we speak of a representation or a character of $\mathcal{G}$ we mean a representation in the field of complex numbers and the corresponding character.

If p is a given prime dividing the order g of $\mathcal{G}$, then the irreducible characters of $\mathcal{G}$ are distributed into "blocks" such that every character belongs to one and only one block.¹

¹See R. Brauer and C. Nesbitt, "On the Modular Characters of Groups," Ann. of Math. 42, No. 2, 1941.

If p^a is the highest power of p dividing g , then a character of a degree divisible by p^a forms a block consisting of this one character alone. Such a block is said to have "defect" 0. More generally, a block B is said to have "defect" d if p^{a-d} is the highest power of p which divides all the degrees of the characters belonging to B .

R. Brauer has shown² that the question of finding the number of blocks of defect $d > 0$ can be reduced to the study of groups of order smaller than g . The methods employed do not give results of the same kind for blocks of defect 0, and in general very little is known concerning conditions sufficient for the existence of such blocks. We propose, in section IV, to obtain some information in this connection.

In sections V and VI we will investigate groups $\mathcal{G}$ of even order which contain no elements of order $2p$ for p an odd prime. Our main result will be a characterization of the linear fractional group $LF(2, 2^a)$ consisting of all matrices of degree 2 and determinant 1 with coefficients in the Galois field with 2^a elements. In this connection we have the following theorem:

Let $\mathcal{G}$ be a group of order $2^a g'$, g' odd. If $\mathcal{G}$ contains no element of order $2p$ for p an odd prime, and if the 2-Sylow subgroups $\mathcal{P}$ are Abelian, then one of the following cases must hold:

(a) $\mathcal{P}$ is a normal subgroup of $\mathcal{G}$.

²R. Brauer, "On the Arithmetic in a Group Ring," Nat. Ac. of Sciences, 30, No. 5, 1944, p. 112, Th. 4.

- (b) $\mathcal{P}$ is cyclic and $\mathcal{G}$ contains a normal subgroup of index 2^a .
- (c) $\mathcal{G}$ is isomorphic to $\text{LF}(2, 2^a)$.

II. On the Multiplication of Classes

We shall use the following notation:

G_t denotes an element of the class K_t .

$\mathcal{N}(G_t)$ is the normalizer of G_t .

g_t is the number of elements in K_t .

$n_t = \frac{g}{g_t}$ is the order of $\mathcal{N}(G_t)$.

T is the element of Λ which is the sum of all elements of order 2.

$$T^2 = \sum b_t K_t$$

where the b_t are rational integers ≥ 0 .

(A) For G_t not of order 2, b_t is equal to the number of elements of order 2 which transform G_t into G_t^{-1} . For G_t of order 2, b_t is one less than the number of elements of order 2 in $\mathcal{N}(G_t)$. For every t , $b_t \leq n_t$.

Proof: For G_t fixed, b_t is the number of solutions of the equation $PQ = G_t$ with P and Q elements of order 2. If (P, Q) is a solution, then $P^{-1}G_tP = G_t^{-1}$. Conversely, if $P^{-1}G_tP = G_t^{-1}$ for P of order 2, we set $Q = PG_t$. Then $PQ = G_t$ and Q will have order 2 provided that $G_t \neq P$.

The last statement in (A) follows from the fact that the total number of elements in $\mathcal{G}$ which transform G_t into G_t^{-1} is either 0 or n_t .

As an immediate consequence of (A), we have

(B) If K_i and K_j are classes of elements of order 2, then $a_{ij}t \leq n_t$, and $a_{ij}t = 0$ if G_t is not conjugate to G_t^{-1} .

It may be advantageous (for example, in applying theorem 3 on page 13) to know conditions under which b_t is actually equal to n_t . Our first result of this kind will be found useful in IV.

(C) If G_t is conjugate to G_t^{-1} and no element in $\mathcal{G}$ except the identity commutes with G_t and an element of order 2, then $b_t = n_t$. Moreover, there exists a class K_r of elements of order 2 such that $a_{rr}t = n_t$; and if K_i and K_j are two classes of elements of order 2, then $a_{ij}t = 0$ except when both i and j are equal to r .

Proof: Let $G = G_t$ and let A be any element such that $A^{-1}GA = G^{-1}$. Denote the order of A by $2^c v$, where v is odd. Then $c \neq 0$, since A^2 is in $\mathcal{N}(G)$ and A is not in $\mathcal{N}(G)$. The element A can be written in the form $A = PV = VP$, where P is of order 2^c and V is of order v . Moreover, V is an even power of A . The last remark implies that V is in $\mathcal{N}(G)$ and $P^{-1}GP = G^{-1}$. Since P^2 lies in $\mathcal{N}(G)$, P^2 must have odd order. Then P has order 2.

Under our assumption, the n_t elements $N^{-1}PN$ with N in $\mathcal{N}(G)$ are distinct. They are therefore the only elements which transform G into G^{-1} . Let $Q = PG$. Since Q transforms G into G^{-1} , Q is conjugate to P . Statement (C) then follows from the fact that $(N^{-1}PN)(N^{-1}QN) = G$ for every N in $\mathcal{N}(G)$.

(D) Assume that G_t is conjugate to G_t^{-1} and that the only elements of $\mathcal{N}(G_t)$ which commute with elements of order 2 are powers of G_t . Then either $b_t = n_t$ or $b_t = 0$. In the latter case, G_t has even order and generates $\mathcal{N}(G_t)$.

Proof: We again set $G = G_t$. If G has order 2, then $\mathcal{N}(G)$ has just two elements and $b_t = 0$ by (A). Therefore we may assume that $G^2 \neq 1$. Let A be any element such that $A^{-1}GA = G^{-1}$. As in the last proof, $A = PV = VP$, where P is of order 2^c , $c \geq 1$, and V is of odd order. Moreover, V lies in $\mathcal{N}(G)$ and $P^{-1}GP = G^{-1}$. By our hypothesis, V is a power of G . Hence $P^{-1}VP = V^{-1} = V$, $V^2 = 1$, $V = 1$, A has order 2^c . Since A^2 lies in $\mathcal{N}(G)$, A^2 is a power of G . This implies that $A^{-1}A^2A = A^{-2}$, and therefore A has order 2 or 4.

Suppose that A has order 4. Then G must have even order and a power of G has order 2. This means that $\mathcal{N}(G)$ is generated by G .

Now the most general element transforming G into G^{-1} is of the form AG^d . Such an element has order 4, since its square is equal to A^2 . We have thus shown that all the elements which transform G into G^{-1} have the same order, which is either 2 or 4. Since the number of such transforming elements is n_t , we obtain (D) by applying (A).

III. Proof of Theorem 1

In preparation for the proof of theorem 1, we establish two results, the first of which is:

(E) Let h equal the number of conjugate classes in $\mathcal{G}$ each of which is equal to its inverse class. Let m denote the total number of elements in $\mathcal{G}$ each of which is of order 2. Then

$$h - 1 \geq \frac{m^2 + m}{g}.$$

Proof: Let K_0 be the 1-class and let $K_1, K_2, \dots, K_s$ be the s classes containing elements of order 2. For any class K_i , let K_i^{-1} denote its inverse class. Then

$$T^2 = mK_0 + \sum_1^s b_i K_i + \sum' b_i K_i,$$

where the last sum is to be taken over the $(h - 1 - s)$ classes K_i with $K_i = K_i^{-1}$ and $i \neq 0, 1, 2, \dots, s$. Each side of the last equation is the sum of a certain number of elements of $\mathcal{G}$. If we count the number of elements we obtain

$$m^2 = m + \sum_1^s b_i g_i + \sum' b_i g_i.$$

By (A), $b_i \leq n_i$; and for $i = 1, \dots, s$, $b_i \leq n_i - 2$. Then

$$\sum_1^s b_i g_i \leq gs - 2m.$$

This gives

$$m^2 \leq m + gs - 2m + g(h - 1 - s),$$

$$h - 1 \geq \frac{m^2 + m}{g}.$$

(F) There exists a degree f of a real character distinct from the 1-character such that

$$f < \frac{g}{m}.$$

Proof: If we denote by f_i the degrees of irreducible representations, we have

$$1 + \sum f_i^2 \leq g,$$

where the sum $\sum$ is taken over the degrees of all the real characters distinct from the 1-character. There will be $h - 1$ terms in the sum $\sum$, since the number of real characters of a group is the same as the number of conjugate classes each of which is equal to its inverse class.³ If we denote by f the smallest of the degrees appearing in $\sum$, then

$$(h - 1)f^2 \leq g - 1,$$

$$f^2 \leq \frac{g - 1}{h - 1},$$

$$f^2 \leq \frac{g(g - 1)}{m(m + 1)},$$

by (E).

Theorem 1: Let $\mathcal{G}$ have even order g and let m be the number of elements in $\mathcal{G}$ of order 2. Then either $\mathcal{G}$ contains a normal subgroup of index 2 or $\mathcal{G}$ contains a normal subgroup

³G. Frobenius and I. Schur, "Über die reellen Darstellungen der Gruppen," S.-B. Preuss. Akad. Wiss. Berlin, 1906, p. 186.

α , distinct from $\mathcal{G}$, such that the index of α is not greater than

$$n! 5^{(n-1)[Z(n)+2]},$$

where n is the greatest integer not exceeding g/m and $Z(n)$ denotes the number of primes smaller than $n + 1$.

Proof: By (F), $\mathcal{G}$ has an irreducible representation $\mathcal{F}$ which is distinct from the 1-representation, has a real character, and is of degree $f \leq n$. If $\mathcal{F}$ is an imprimitive group of linear transformations, then there exists a homomorphism of $\mathcal{G}$ onto a transitive permutation group on k letters, where $2 \leq k \leq f$.⁴ Let α be the kernel of this homomorphism.

$\alpha \neq \mathcal{G}$ and the index of α in $\mathcal{G}$ is not greater than $n!$.

If $\mathcal{F}$ is a primitive group, let $\mathcal{K}$ be the kernel of the representation $\mathcal{F}$. Then $\mathcal{F}$ is a one-to-one irreducible representation of $\mathcal{G}/\mathcal{K}$. Denote by $\mathcal{O}/\mathcal{K}$ the center of $\mathcal{G}/\mathcal{K}$. Here α is a normal subgroup of $\mathcal{G}$. By a result of Blichfeldt,⁵ the index of α in $\mathcal{G}$ does not exceed

$$n! 5^{(n-1)[Z(n)+2]}.$$

Therefore theorem 1 is established provided α is not equal to $\mathcal{G}$. But if α is equal to $\mathcal{G}$, then f must be 1, since $\mathcal{O}/\mathcal{K}$ is Abelian. The character of $\mathcal{F}$ being real then implies that $\mathcal{F}(G) = \pm 1$ for all G in $\mathcal{G}$. Since $\mathcal{F}$ is not the 1-representation, the index of $\mathcal{K}$ in $\mathcal{G}$ is 2.

⁴H. F. Blichfeldt, Finite Collineation Groups, Univ. of Chicago Press, 1917, p. 77.

⁵Ibid., p. 103.

IV. On the Existence of Blocks of Defect 0

A block of defect 0 is sometimes referred to as a "block of highest kind"; one of defect a is often called a "block of lowest kind."

Our first result in this section, namely theorem 2, holds for any group $\mathcal{G}$, whether of odd or even order.

It is well known that the irreducible representations of $\mathcal{G}$ in the field of complex numbers can be so chosen that their coefficients lie in an algebraic number field Ω . We denote by Λ the center of the group ring of $\mathcal{G}$ formed with regard to Ω . Then every irreducible character χ_μ of $\mathcal{G}$ determines a linear character ω_μ of Λ ; ω_μ is given by

$$(2) \quad \omega_\mu(K_i) = \frac{g_i \chi_{\mu i}}{f_\mu}$$

where

$$\chi_{\mu i} = \chi_\mu(K_i)$$

and f_μ is the degree of χ_μ , and g_i is the number of elements in K_i . Applying ω_μ to both sides of (1) we obtain

$$\omega_\mu(K_r) \omega_\mu(K_s) = \sum_t a_{rst} \omega_\mu(K_t).$$

By (2), this can be written

$$\frac{\chi_{\mu r} \chi_{\mu s}}{f_{\mu}} = \sum \frac{a_{rst} g_t}{g_r g_s} \chi_{\mu t}$$

Multiplying both sides of the last equation by $\overline{\chi_{\mu h}}$, where the bar denotes "complex conjugate," next summing over all μ , and then applying the orthogonality relations for group characters, we obtain

$$(3) \quad g \sum_{\mu} \frac{\chi_{\mu r} \chi_{\mu s} \overline{\chi_{\mu h}}}{f_{\mu}} = a_{rsh} n_r n_s.$$

We shall use (3) to derive a result concerning the existence of blocks of defect 0.

Let $\mathcal{G}$ have order $g = p^a g'$ for p a prime and $(g', p) = 1$. Let $\mathcal{P}$ be a prime ideal divisor of p in Ω , and denote by the center of the group ring of $\mathcal{G}$ formed with regard to the residue class field of the integers of $\Omega \pmod{\mathcal{P}}$. We now prove:

Theorem 2: The classes K_r of $\mathcal{G}$ with n_r prime to p form the basis of an invariant subalgebra M of $\overline{\Lambda}$. There exist blocks of $\mathcal{G}$ of defect 0 if and only if $M^2 \neq 0$. If K_r is a class in M , then K_r will be nilpotent only if K_r^2 is already 0.

Proof: Let G_h be a fixed element of the class K_h . Then a_{rsh} is equal to the number of distinct solutions (A, B) , with A in K_r and B in K_s , of the equation $AB = G_h$. If (A, B) is a given solution let $\mathcal{N}_{\star}$ be the intersection of $\mathcal{N}(A)$ and $\mathcal{N}(B)$. It is easily seen that the number of distinct solutions of the form $(N^{-1}AN, N^{-1}BN)$ for N in $\mathcal{N}(G_h)$ is equal to the index of $\mathcal{N}_{\star}$ in $\mathcal{N}(G_h)$. This index will be divisible by p if n_h is divisible by p and n_r is prime to p . It follows that

$$a_{rsh} \equiv 0 \pmod{p}$$

for K_r in M and K_h not in M . This proves the first statement in theorem 2.

Now we let K_r and K_s be any two classes in M and set $f_\mu = p^{d_\mu} f'_\mu$ for $(f'_\mu, p) = 1$. Equation (3) then becomes

$$(4) \quad g' \sum_{\mu} \frac{p^{a-d_\mu} \chi_{\mu r} \chi_{\mu s} \overline{\chi_{\mu h}}}{f'_\mu} = a_{rsh} n_r n_s.$$

If $K_r K_s \not\equiv 0 \pmod{p}$, that is, if there exists an h such that $a_{rsh} \not\equiv 0 \pmod{p}$, we take this h in (4). Each side of (4) is then a p -integer $\not\equiv 0 \pmod{\mathcal{P}}$.⁶ Hence there exists some μ such that

$$\begin{aligned} f_\mu &\equiv 0 \pmod{p^a}, \\ \chi_{\mu r} &\not\equiv 0 \pmod{\mathcal{P}}, \\ \chi_{\mu s} &\not\equiv 0 \pmod{\mathcal{P}}. \end{aligned}$$

This means that if $\mathcal{G}$ has no p -blocks of defect 0, then $M^2 = 0$. The converse follows from a theorem of R. Brauer.⁷

To get the last statement in our theorem, we take $r = s$ in the above. Then $K_r^2 \not\equiv 0 \pmod{p}$ implies there exists an ω_μ such that $\omega_\mu(K_r) \not\equiv 0 \pmod{\mathcal{P}}$. Since ω_μ taken $\pmod{\mathcal{P}}$ is an irreducible representation of $\overline{\Lambda}$, K_r cannot be in the radical of $\overline{\Lambda}$. Then since $\overline{\Lambda}$ is a commutative algebra, K_r cannot be nilpotent. This completes the proof of theorem 2.

⁶A p -integer is a number which can be expressed in the form α/β where α and β are integers of Ω and β is prime to $\mathcal{P}$. $\alpha/\beta \equiv 0 \pmod{\mathcal{P}}$ means $\alpha \equiv 0 \pmod{\mathcal{P}}$.

⁷"On the Arithmetic in a Group Ring," National Academy of Sciences, Vol. 30, 1944, p. 112, Th. 3.

We return now to a group of even order. As before, we denote by T the sum of all elements of order 2 in $\mathcal{G}$,

$$T^2 = \sum b_t K_t.$$

Let 2^{a_0} be the highest power of 2 dividing g . Let p be a fixed odd prime dividing g ,

$$g = p^a g', \quad (g', p) = 1,$$

and let p^c be the highest power of p which divides any of the degrees f_μ not divisible by 2^{a_0} . We now prove:

Theorem 3: Assume $\mathcal{G}$ contains no element of order $2p$, for some fixed p . Then p^{a-c} divides b_t for every t . If for some t $(b_t, p) = 1$, then there exists a χ_μ such that

$$f_\mu \equiv 0 \pmod{p^a},$$

$$f_\mu \not\equiv 0 \pmod{2^{a_0}},$$

$$(5) \quad \begin{aligned} \chi_\mu(G_t) &\not\equiv 0 \pmod{\mathfrak{p}} \text{ where } \mathfrak{p} \text{ is a} \\ &\text{prime ideal divisor of } p, \\ \chi_\mu(A) &\not\equiv 0 \pmod{\mathfrak{p}} \text{ for some } A \text{ of} \\ &\text{order 2.} \end{aligned}$$

Proof: Let $K_1, K_2, \dots, K_s$ be the classes of elements of order 2, so that $T = \sum_1^s K_i$. Then

$$T^2 = \sum_{i,j=1}^s K_i K_j = \sum b_t K_t.$$

Using the same method applied in deriving (3) we obtain

$$g \sum_\mu \frac{\overline{\chi_{\mu t}}}{f_\mu} \sum_{i,j=1}^s \frac{\chi_{\mu i} \chi_{\mu j}}{n_i n_j} = b_t.$$

Here we need sum only over μ such that $f_\mu \not\equiv 0 \pmod{2^{a_0}}$, since if $f_\mu \equiv 0 \pmod{2^{a_0}}$, then χ_μ vanishes for all elements of order 2 in $\mathcal{G}$.⁸ Setting

$$\Omega_\mu = \sum_{i,j} \frac{\chi_{\mu i} \chi_{\mu j}}{n_i n_j},$$

$f_\mu = p^{d_\mu} f'_\mu$ for $(f'_\mu, p) = 1$, and $e_\mu = c - d_\mu \geq 0$, we then have

$$(6) \quad g' \sum_{\mu} \frac{p^{e_\mu} \overline{\chi_{\mu t}} \Omega_\mu}{f'_\mu} = \frac{b_t}{p^{a-c}}.$$

Since $\mathcal{G}$ contains no element of order $2p$, $(n_i, p) = 1$ for $i = 1, 2, \dots, s$. Then Ω_μ is a p -integer, each side of (6) is a p -integer, p^{a-c} divides b_t . If $(b_t, p) = 1$, then for some μ

$$p^{e_\mu} \overline{\chi_{\mu t}} \Omega_\mu \not\equiv 0 \pmod{\mathcal{G}},$$

and the theorem is proved.

For any element G , we denote by $n(G)$ the order of the normalizer $\mathcal{N}(G)$ of G .

Corollary 1: Let $g = p^a g'$, p an odd prime. If

- (a) $\mathcal{G}$ contains no element of order $2p$, and
- (b) $\mathcal{G}$ contains an element G not of order 2 such that $n(G)$ is prime to p , $\mathcal{N}(G)$ is Abelian, and there exists an element Q of order 2 transforming G into G^{-1} ,

⁸ See R. Brauer and C. Nesbitt, "On the Modular Characters of Groups," p. 565, Th. 1.

then there exists an irreducible character χ_μ such that (5) holds (with $G_t = G$).

Proof: We set $G = G_t$. By (A) b_t equals the number of elements of order 2 which transform G into G^{-1} . The most general element transforming G into G^{-1} is QN for N an element of $\mathcal{N}(G)$. If QN has order 2, then $QNQ = N^{-1}$. Conversely, if $QNQ = N^{-1}$ for N an element of $\mathcal{N}(G)$, then QN has order 2, since Q is not an element of $\mathcal{N}(G)$. Therefore b_t equals the number of solutions N , for N an element of $\mathcal{N}(G)$, of the equation $QNQ = N^{-1}$. Since $\mathcal{N}(G)$ is Abelian, these solutions form a group of order b_t . Hence b_t divides $n(G)$ and is therefore prime to p .

Remark: It is obvious that Corollary 1 remains valid if we replace (b) by the following assumption:

(b') There exists an element G not of order 2 such that G is conjugate to G^{-1} , all elements which transform G into G^{-1} have order 2, and $n(G)$ is prime to p .

As a special case of Corollary 1 we have the following result:

Corollary 2: Let $\mathcal{G}$ have even order g divisible by an odd prime p_1 . Assume that $\mathcal{G}$ contains no element of order $p_1 n$ for n prime to p_1 ($n \neq 1$), and that some element of order p_1^m , $m > 0$, is conjugate to its inverse. Let p be any other prime dividing g ($p \neq 2$ or p_1). Then if $\mathcal{G}$ contains no element of order $2p$, there will exist a χ_μ which forms a p -block of highest kind, which belongs to the p_1 -block of lowest kind, and which does not form a 2-block of highest kind.

Proof: For any prime q , a class K is called " q -regular" if its elements have an order not divisible by q . A class which is not q -regular is called " q -singular." R. Brauer has shown that the number of q -blocks of defect d is less than or equal to the number of q -regular classes K_t for which q^d is the highest power of q dividing n_t .⁹ Since $\mathcal{G}$ contains no element of order $p_1 n$ for n prime to p_1 , the only p_1 -regular class K_t with n_t divisible by p_1 is the 1-class. Hence there is exactly one p_1 -block of lowest kind and all other p_1 -blocks are of highest kind.

By hypothesis, there exists an element P of order p_1^m , $m > 0$ with P conjugate to P^{-1} . Since $\mathcal{G}$ contains no element of order $p_1 n$ for n prime to p_1 , it follows that $n(P)$ is a power of p_1 and that no element except the identity commutes with P and an element of order 2. We now apply (C) with G_t taken as P , and find that

$$b_t = n_t = n(P).$$

By theorem 3, there exists a χ_μ such that

$$f_\mu \equiv (\text{mod } p^a),$$

$$f_\mu \not\equiv (\text{mod } 2^{a_0}),$$

$$\chi_\mu(P) \neq 0.$$

χ_μ cannot form a p_1 -block of highest kind,¹⁰ and so must belong to the p_1 -block of lowest kind.

⁹R. Brauer, "On the Arithmetic in a Group Ring," p. 111, Cor. 1.

¹⁰See R. Brauer and C. Nesbitt, "On the Modular Characters of Groups," p. 565, Th. 1.

V. On Groups Containing No Element of Order $2p$
for p an Odd Prime

In this section we shall consider groups $\mathcal{G}$ satisfying the following assumption:

(★) $\mathcal{G}$ has even order and contains no element of order $2p$ for p an odd prime.

It follows easily that the order of an element of $\mathcal{G}$ is either odd or a power of 2, and that if P is an element of order 2^k , $k \geq 1$, then $n(P)$ is a power of 2.

If $\mathcal{G}$ has order $2^a g'$, for g' odd, then the number m of elements of order 2 in $\mathcal{G}$ is at least g' . Theorem 1 then yields:

(G) For a fixed integer a and an arbitrary odd integer g' , there exist only a finite number of simple groups of order $g = 2^a g'$ which satisfy (★). In fact,

$$g \leq 2^a! \cdot 5^{(2^a-1)} [2(2^a)-2]$$

(H) If $\mathcal{G}$ has order $g = 2^a g'$ (g' odd) and satisfies (★), then either $g \leq 2^{2a}(2^a - 1)$ or all elements of order 2 are conjugate.

Proof: A class K will be 2-singular if and only if the order of its elements is a power of 2. We will always denote the r 2-singular classes by $K_1, K_2, \dots, K_r$. Since every

element whose order is a power of 2 is conjugate to an element of a given fixed 2-Sylow subgroup, it follows that

$$r \leq 2^a - 1.$$

Suppose that K_1 and K_2 are two distinct classes containing elements of order 2.

$$K_1 K_2 = \sum a_{12t} K_t$$

Let G_t be an element of K_t . For G_t of odd order, $a_{12t} = 0$; this follows from (B) if G_t is not conjugate to G_t^{-1} , and from (★) and (C) if G_t is conjugate to G_t^{-1} . Hence

$$(7) \quad K_1 K_2 = \sum_1^r a_{12t} K_t.$$

This implies that

$$\frac{g^2}{n_1 n_2} = \sum_1^r a_{12t} \frac{g}{n_t}.$$

By (B)

$$\frac{g^2}{n_1 n_2} \leq gr,$$

$$g \leq n_1 n_2 r,$$

$$g \leq 2^{2a}(2^a - 1).$$

(I) Let $\mathcal{G}$ have order $g = 2^a g'$ (g' odd) and assume $\mathcal{G}$ satisfies (★). If a 2-Sylow subgroup contains more than one element of order 2, then

$$g \leq 2^{2a}(2^{2a} - 2^a - 1)2^{a-1}.$$

Remark: If a 2-Sylow subgroup $\mathcal{P}$ contains only one element of order 2, then either $\mathcal{P}$ is cyclic or $\mathcal{P}$ is the generalized

quaternion group.¹¹ It can be shown that in either case $\mathcal{G}$ contains a normal subgroup of index 2^a .

Proof of (I): Because of $(\star)$, $\mathcal{G}$ has exactly one block of lowest kind and all other blocks of $\mathcal{G}$ are of highest kind. Denote by x the number of degrees f_μ in the block of lowest kind and by y the number of blocks of highest kind. Then

$$\sum_1^x f_\mu^2 + 2^{2a}y \leq g = 2^a g'.$$

Let h be the number of classes of $\mathcal{G}$ each of which is equal to its inverse class, and let h' be the number of the remaining classes.

$$y = h + h' - x.$$

By (E),

$$h - 1 \geq \frac{g' + 1}{2^a}.$$

An easy calculation then yields

$$(8) \quad \sum_1^x f_\mu^2 \leq 2^{2a}x - 2^{2a} - 2^a.$$

We next show that $x \leq 2^a$. Let P be an invariant element of order 2 of a 2-Sylow subgroup $\mathcal{P}$. We consider the matrix of the generalized decomposition numbers of $\mathcal{G}$ for 2.¹² The submatrix which corresponds to the section P will have but one column (d_μ) , since $\mathcal{N}(P) = \mathcal{P}$. The d_μ are rational integers and $\sum_\mu d_\mu^2 = 2^a$.¹³ Moreover, d_μ , for $\mu = 1, \dots, x$

¹¹W. Burnside, Theory of Groups of Finite Order, Sec. Ed., Cambridge, 1911, p. 132.

¹²R. Brauer, "On the Connection between the Ordinary and the Modular Characters of Groups of Finite Order," Ann. of Math. 42, No. 4, 1941, pp. 927-929.

¹³Ibid., p. 930, Th. 4.

cannot be zero.¹⁴ Hence

$$x \leq 2^a.$$

Now let K_1 be the class containing P . Set $g = 2^a \prod p_i^{a_i}$, where the p_i are distinct odd primes, and let $p_i^{c_i}$ be the highest power of p_i dividing any of the f_μ in the 2-block of lowest kind. By theorem 3, $\prod p_i^{a_i - c_i}$ divides b_1 . Because of (A) and our assumption on $\mathcal{P}$, $b_1 \neq 0$. Hence

$$\prod p_i^{a_i - c_i} \leq b_1,$$

$$(8) \quad g' = \prod p_i^{a_i} \leq b_1 \prod p_i^{c_i} \leq 2^a \prod p_i^{c_i}$$

By a theorem on the geometric and arithmetic means,

$$\left(\prod_{\mu} f_{\mu}^2 \right)^{1/x} \leq \frac{1}{x} \sum_{\mu} f_{\mu}^2.$$

By (8) and the inequality $x \leq 2^a$, we obtain

$$\left(\prod_{\mu} f_{\mu}^2 \right)^{1/x} \leq 2^{2a} - 2^a - 1.$$

Since $\prod p_i^{c_i}$ divides $\prod_{\mu} f_{\mu}$,

$$\begin{aligned} \prod p_i^{c_i} &\leq (2^{2a} - 2^a - 1)^{x/2} \\ &\leq (2^{2a} - 2^a - 1)^{2^{a-1}}. \end{aligned}$$

This last inequality together with (8') establishes (I).

(J) Let $\mathcal{G}$ satisfy (*). If the 2-Sylow subgroups of $\mathcal{G}$ are

¹⁴R. Brauer, "On Blocks of Characters of Groups of Finite Order II," Nat. Ac. of Sciences 32, No. 8, 1946, p. 217, Th. 4.

Abelian, then the intersection of any two distinct ones is 1.

Proof: Let $\mathcal{P}_1$ and $\mathcal{P}_2$ be two distinct 2-Sylow subgroups. If $Q \neq 1$ is in $\mathcal{P}_i$, then $\mathcal{N}(Q) = \mathcal{P}_i$ because of ($\star$).

(K) If the 2-Sylow subgroups of $\mathcal{G}$ are Abelian and if A is any element of order 2^n , $n \geq 2$, then A is not conjugate to A^{-1} .

Proof: If $B^{-1}AB = A^{-1}$, we may assume that the order of B is a power of 2. Then the group $\mathcal{H}$ generated by A and B is a group whose order is a power of 2. Hence $\mathcal{H}$ is contained in a 2-Sylow subgroup. Since the latter is Abelian and $\mathcal{H}$ is non-Abelian, we have a contradiction.

(L) If $\mathcal{G}$ satisfies ($\star$) and if its 2-Sylow subgroups $\mathcal{P}$ are Abelian, then either $\mathcal{P}$ is a normal subgroup of $\mathcal{G}$ or all elements of order 2 are conjugate in $\mathcal{G}$. In the latter case, $\mathcal{P}$ must be of type $(2^m, 2^m, \dots, 2^m)$.

Proof: If not all elements of order 2 are conjugate, let K_1 and K_2 be two classes containing elements of order 2. By (K) and (B), (7) becomes

$$(9) \quad K_1 K_2 = \sum_1^s a_{12t} K_t,$$

where $K_1, K_2, \dots, K_s$ are the classes containing elements of order 2.

Let G_1 be an element of K_1 and denote by $\mathcal{P}_1$ the Sylow subgroup containing G_1 . Now let $\mathcal{P}$ be any 2-Sylow subgroup. We may assume G_2 is in $\mathcal{P}$. By (9), $G_1 G_2 = Q$ is an element

of order 2. Hence G_2 is an element of $\mathcal{N}(G_1) = \mathcal{P}_1$. But G_2 is in $\mathcal{P}$. By (J), $\mathcal{P} = \mathcal{P}_1$ and $\mathcal{G}$ contains only one 2-Sylow subgroup. Hence the normalizer of $\mathcal{P}$ is $\mathcal{G}$. This proves the first part of (L).

To prove the second part, we first show that if Q is any element of $\mathcal{P}$, then the normalizer $\mathcal{N}(\mathcal{P})$ of $\mathcal{P}$ has order $n = 2^a b$, where 2^a is the order of $\mathcal{P}$ and b is the number of elements in $\mathcal{P}$ which are conjugate to Q in $\mathcal{G}$. Denote these b elements by $Q = Q_1, Q_2, \dots, Q_b$. Since Q is conjugate to Q_1 in $\mathcal{N}(\mathcal{P})$, there exists an N_1 in $\mathcal{N}(\mathcal{P})$ such that $N_1^{-1} Q N_1 = Q_1$, for $i = 1, 2, \dots, b$. The N_1 represent b distinct cosets of $\mathcal{N}(\mathcal{P}) \bmod \mathcal{P}$. Since $\mathcal{N}(Q) = \mathcal{P}$, every N in $\mathcal{N}(\mathcal{P})$ is in one of these b cosets. Hence $n = 2^a b$.

Under our assumption that all elements of order 2 are conjugate, $n = 2^a b$, where b is the number of elements of order 2 in $\mathcal{P}$. By what we have just proved, the elements of $\mathcal{P}$ distinct from 1 are distributed into r families, two elements being in the same family if and only if they are conjugate in $\mathcal{G}$, and each family contains the same number b of elements. It follows that the number of elements in $\mathcal{P}$ of order 2^m , for any fixed m , is divisible by b .

Suppose now that $\mathcal{P}$ is of type

$$(\underbrace{2^m, 2^m, \dots, 2^m}_{s \text{ terms}}, \underbrace{2^{k_1}, 2^{k_2}, \dots, 2^{k_t}}_{c-s \text{ terms}}),$$

with $m > k_1 \geq k_2 > 0$. Then $b = 2^c - 1$ and the number of

elements in $\mathcal{P}$ of order 2^m is $2^{a-s}(2^s - 1)$. Since b divides $2^s - 1$, we must have $c \leq s$, $c = s$. This completes the proof of (L).

VI. A Characterization of $LF(2, 2^a)$

Lemma: Assume $\mathcal{G}$ has the following properties:

- (a) Its order is $g = 2^a g'$, g' odd, $a \geq 1$.
- (b) Its 2-Sylow subgroups $\mathcal{P}$ are Abelian.
- (c) It contains no element of order $2p$ for p an odd prime.

Then we must have one of the following cases:

- (a) $\mathcal{P}$ is a normal subgroup of $\mathcal{G}$.
- (β) $\mathcal{P}$ is cyclic and $\mathcal{G}$ contains a normal subgroup of index 2^a .
- (γ) $\mathcal{P}$ is of type $(2, 2, \dots, 2)$.

Proof: Because of property (c), $\mathcal{G}$ has exactly one 2-block of lowest kind and all other 2-blocks are of highest kind.

We shall adopt the following notation:

χ_μ is an irreducible character of $\mathcal{G}$ of degree f_μ .

x is the number of characters in the block of lowest kind. We take χ_μ , $\mu = 0, 1, \dots, x-1$, as these characters.

y is the number of blocks of highest kind.

$f_\mu = 2^a w_\mu$ for $\mu > x-1$ (w_μ is odd ≥ 1).

b equals the number of elements of order 2 in a 2-Sylow subgroup $\mathcal{P}$.

$P_1, P_2, \dots, P_r$ are elements of $\mathcal{P}$ which represent the r 2-singular classes; P_1 has order 2.

We assume that the case (a) does not hold. Then by (L) and its proof, all the elements of order 2 are conjugate; b is equal to the number of elements in $\mathcal{P}$ which are conjugate to P_1 in $\mathcal{G}$ ($i = 1, 2, \dots, r$); and the normalizer $N(\mathcal{P})$ of $\mathcal{P}$ has order

$$(10) \quad n = 2^a b.$$

We also have

$$(11) \quad br = 2^a - 1.$$

If we consider χ_μ as a character for $\mathcal{P}$ and denote by m_μ the multiplicity of the 1-character of $\mathcal{P}$ in χ_μ , we obtain

$$(12) \quad f_\mu = 2^a m_\mu - b \sum_{i=1}^r \chi_\mu(P_i).$$

By (11)

$$rf_\mu \equiv \sum_{i=1}^r \chi_\mu(P_i) \pmod{2^a},$$

$$(13) \quad rf_\mu = \sum_{i=1}^r \chi_\mu(P_i) + 2^a z_\mu, \quad z_\mu \geq 0.$$

That z_μ cannot be negative follows from the inequality $|\chi_\mu| \leq f_\mu$.

We denote by $\mathcal{F}_\mu$ the representation corresponding to the character χ_μ and by $\mathcal{K}_\mu$ the kernel of $\mathcal{F}_\mu$. We now prove that $\mathcal{P}$ is contained in $\mathcal{K}_\mu$ if and only if $z_\mu = 0$. The "only if" part is trivial. Assume then that $z_\mu = 0$, so that (13) becomes

$$(13') \quad rf_{\mu} = \sum_{i=1}^r \chi_{\mu}(P_i).$$

Then

$$rf_{\mu} \leq \sum_{i=1}^r |\chi_{\mu}(P_i)| \leq rf_{\mu}$$

implies that

$$|\chi_{\mu}(P_i)| = f_{\mu} \quad \text{for all } i.$$

If we express $\chi_{\mu}(P_i)$ as a sum of f_{μ} roots of unity, it follows easily that these roots of unity must all be equal.

$$\chi_{\mu}(P_i) = f_{\mu} \eta_{\mu i},$$

where $\eta_{\mu i}$ is a root of unity. We now have

$$rf_{\mu} = f_{\mu} \left| \sum_{i=1}^r \eta_{\mu i} \right|,$$

which shows us that all the $\eta_{\mu i}$ must be equal (for $i = 1, 2, \dots, r$). Denote their common value by η . It follows from (13') that η must be 1. Hence $\mathcal{P}$ is contained in $\mathcal{K}_{\mu}$ if and only if $z_{\mu} = 0$.

Since $\chi_{\mu}(P_i) = 0$ for $\mu > x - 1$,¹⁵ the orthogonality relations for characters give

$$(14) \quad \sum_{\mu=0}^{x-1} f_{\mu} \chi_{\mu}(P_i) = 0,$$

¹⁵R. Brauer and C. Nesbitt, op. cit., p. 565, Th. 1.

$$(15) \quad \sum_{\mu=0}^{x-1} \chi_{\mu}(P_i) \overline{\chi_{\mu}(P_j)} = 0 \quad \text{for } i \neq j, \\ = 2^a \quad \text{for } i = j.$$

Multiplying both sides of (13) by $\overline{\chi_{\mu}(P_j)}$ and summing over μ from 0 to $x - 1$ we obtain:

$$(16) \quad \sum_{\mu=0}^{x-1} z_{\mu} \chi_{\mu}(P_i) = -1.$$

Multiplying both sides of (13) by $r f_{\mu}$ and summing over μ from 0 to $x - 1$, we obtain:

$$\begin{aligned} r^2 \sum_{\mu=0}^{x-1} f_{\mu}^2 &= 2^a \sum_{\mu=0}^{x-1} z_{\mu} r f_{\mu}, \\ &= 2^a \sum_{\mu=0}^{x-1} \left[\sum_{i=1}^r z_{\mu} \chi_{\mu}(P_i) + 2^a z_{\mu}^2 \right], \\ &= -2^a r + 2^{2a} \sum_{\mu=0}^{x-1} z_{\mu}^2 \end{aligned}$$

because of (16). Since

$$g = \sum_0^{x-1} f_{\mu}^2 + 2^{2a} \sum_1^y w_{\nu}^2,$$

we have

$$(17) \quad r^2 g' = 2^a \sum_0^{x-1} z_{\mu}^2 - r + 2^a r^2 \sum_1^y w_{\nu}^2.$$

Denote by K the class of elements of order 2, and by K_0 the 1-class. It follows from (A), (C), and (K) that

$$K^2 = g' K_0 + (b - 1)K + \sum' n_t K_t.$$

where there are $h - 2$ terms in $\sum'$. This yields

$$(18) \quad g' = b + 2^a(h - 2).$$

Then (17), (18), and (11) give

$$(19) \quad r + r^2(h - 2) = \sum_{\mu=0}^{x-1} z_{\mu}^2 + r^2 \sum_{j=1}^y w_j^2.$$

It follows from (11), (12), and (13) that

$$z_{\mu} = m_{\mu}r - \sum_i \chi_{\mu}(P_i).$$

Multiplying both sides of the last equation by z_{μ} , and summing over μ from 0 to $x - 1$, and finally making use of (16) we obtain

$$(20) \quad \sum_{\mu=0}^{x-1} z_{\mu}^2 = r \sum_{\mu=0}^{x-1} m_{\mu} z_{\mu} + r.$$

If we let $2h'$ be the number of classes each of which is not equal to its inverse class, then

$$y = h + 2h' - x.$$

We put $\sum_{j=1}^y w_j^2 = 8t + y$, $t \geq 0$, so that (19) becomes

$$(21) \quad \sum_{\mu=0}^{x-1} z_{\mu}^2 + 8r^2t + 2r^2h' = r + r^2x - 2r^2.$$

We now turn our attention to $\mathcal{N} = \mathcal{N}(\mathcal{P})$. So far in this proof we have assumed, in addition to (a), (b), and (c), only that case (a) does not hold. Actually the only implication of this added assumption which we have used is that all elements of order 2 in $\mathcal{G}$ are conjugate. Since two elements of $\mathcal{P}$ are conjugate in $\mathcal{G}$ only if they are conjugate

in $\mathcal{N}$, it follows that all our above results hold for $\mathcal{N}$. For the next few pages we will not refer to $\mathcal{G}$, and will use the same notation for $\mathcal{N}$ as we used above for $\mathcal{G}$.

Suppose $\mathcal{N}$ has an irreducible representation of a degree $2^a w$. Since the order of $\mathcal{N}$ is $2^a b$,

$$2^{ab} = \sum_{\mu} f_{\mu}^2,$$

$$2^{ab} \geq 2^a.$$

But this is a contradiction. Hence

$$y = 0.$$

Now the irreducible representations of $\mathcal{N}/\mathcal{P}$ are just those of $\mathcal{N}$ for which $\mathcal{P}$ is contained in the kernel, i.e., for which $z_{\mu} = 0$. Since the order of $\mathcal{N}/\mathcal{P}$ is b , we have

$$(22) \quad b = \sum' f_{\mu}^2,$$

where the prime denotes that the sum is to be taken over all μ with $z_{\mu} = 0$.

By (18), $h = 2$. Then (19) and (20) become respectively

$$\sum_{\mu=0}^{x-1} z_{\mu}^2 = r$$

and

$$\sum_{\mu=0}^{x-1} m_{\mu} z_{\mu} = 0.$$

Since $m_{\mu} \geq 0$ and $z_{\mu} \geq 0$, the last equation implies that $m_{\mu} = 0$ for $z_{\mu} > 0$. It follows from (11), (12), and (13) that

$$f_{\mu} = bz_{\mu}, \quad \text{for } z_{\mu} > 0.$$

This means that f_μ , for $z_\mu > 0$, forms a p-block of highest kind for every odd prime p dividing $n = 2^a b$. Hence

$\chi_\mu(N) = 0$ for every element N of odd order (not equal to 1) and every μ with $z_\mu > 0$. The table of characters for $\mathcal{N}$ then has the following form:

1		$P_1 \ P_2 \cdots P_r$
1	$1 \cdots 1$	$1 \ 1 \cdots 1$
f_μ		$f_\mu \ f_\mu \cdots f_\mu$
bz_μ		

} $\ell =$ the number of $z_\mu > 0$.

$\underbrace{\hspace{10em}}_r$

Since the columns of the table are linearly independent, $r \leq \ell$. But by (17),

$$\ell \leq \sum_{\substack{\mu \\ z_\mu > 0}} z_\mu^2 = r.$$

Hence $\ell = r$ and every $z_\mu = 1$. Then by (13)

$$(22') \quad \sum_{i=1}^r \chi_\mu(P_i) = -1, \quad \text{for } f_\mu = b.$$

We now change our notation for $\mathcal{N}$. We denote the characters of $\mathcal{N}$ of degree b by $\theta_1, \theta_2, \dots, \theta_r$; the remaining ones by ψ_μ and their degrees by $f_\mu^\star$.

1		P_1	P_2	$\cdot$	$\cdot$	$\cdot$	P_r
$f_{\mu}^{\star}$		$f_{\mu}^{\star}$	$f_{\mu}^{\star}$	$\cdot$	$\cdot$	$\cdot$	$f_{\mu}^{\star}$
$\left. \begin{array}{c} b \\ b \\ \cdot \\ \cdot \\ \cdot \\ b \end{array} \right\} r$							

In our new notation, (22), (22'), and (16) become respectively

$$(23) \quad \sum f_{\mu}^{\star 2} = b,$$

$$(24) \quad \sum_{i=1}^r \theta_{\mu}(P_i) = -1,$$

$$(25) \quad \sum_{\mu=1}^r \theta_{\mu}(P_i) = -1.$$

We use (23) and the orthogonality relations (15) to obtain

$$(26) \quad \sum_{\mu=1}^r |\theta_{\mu}(P_i)|^2 = 2^a - b.$$

If σ is a subgroup of $\mathcal{G}$, then every character χ of $\mathcal{G}$ may be regarded as a character $\chi(\sigma)$ of σ . We now apply the following theorem:¹⁶

¹⁶The proof of this theorem will appear in a paper to be published by R. Brauer.

Let σ be a subgroup of $\mathcal{G}$, Σ a system of classes K_1 of $\mathcal{G}$, and $\theta_1, \theta_2, \dots, \theta_r$ ($r \geq 2$) a system of irreducible characters of σ . Let ψ_i denote the other irreducible characters of σ . Assume

- (1) Every K_1 in Σ contains one and only one class $\widetilde{K}_1$ of σ .
- (2) For suitable A in $\widetilde{K}_1$, $\mathcal{N}(A) \leq \sigma$.
- (3) $\theta_j = \theta_k$ for every class of σ which is not a $\widetilde{K}_1$.

Then exactly r characters $\chi_1, \dots, \chi_r$ of $\mathcal{G}$ are of the following type:

Type I: $\chi_j(\sigma) = s \sum_{i=1}^r \theta_i + \delta \theta_j + \sum d_i \psi_i$, where

$\delta = \pm 1$, s and d_i are rational integers ≥ 0 , $s + \delta \geq 0$, and δ , s , and the d_i are independent of $j = 1, \dots, r$.

Every other χ of $\mathcal{G}$ is of the following type:

Type II: $\chi_\lambda(\sigma) = b_\lambda \sum_{i=1}^r \theta_i + \sum_{\mu} a_{\lambda\mu} \psi_\mu$, where the b_λ ,

$a_{\lambda\mu}$ are rational integers ≥ 0 .

The assumptions of this theorem are satisfied if we take $\sigma = \mathcal{N}$ and Σ as the family of the 2-singular classes.¹⁷ We then have

$$\left. \begin{aligned} (27) \quad \chi_\lambda(P_1) &= \sum_{\mu} a_{\lambda\mu} f_{\mu}^* - b_{\lambda} \\ (28) \quad f_{\lambda} &= 2^a b_{\lambda} + \chi_{\lambda}(P_1) \end{aligned} \right\} \text{ for } \chi_{\lambda} \text{ of Type II.}$$

¹⁷ Strictly speaking, this is true only if $r \geq 2$. But if $r = 1$, then we have case (γ) of the lemma.

Now (27) shows that $\chi_{\lambda}(P_i)$ is independent of i . Then (13) and (28) give

$$(29) \quad rb_{\lambda} = z_{\lambda} \text{ for } \lambda \text{ of Type II.}$$

Setting $c = \sum d_i f_i^* - s$, we have

$$(30) \quad \chi_j(P_i) = c + \delta \theta_j(P_i) \left. \vphantom{\chi_j(P_i)} \right\} \text{ for } j \text{ of Type I}$$

$$(31) \quad f_j = 2^a s + c + b \delta$$

From the orthogonality relations (15) we have

$$\sum_{\text{all } \mu} |\chi_{\mu}(P_i)|^2 = 2^a,$$

which can be written

$$\sum_{\substack{j \text{ of} \\ \text{Type I}}} [c + \delta \theta_j(P_i)] [c + \delta \overline{\theta_j(P_i)}] + \sum_{\substack{\lambda \text{ of} \\ \text{Type II}}} |\chi_{\lambda}(P_i)|^2 = 2^a.$$

Because of (25) and (26), this becomes

$$\sum_{\substack{\lambda \text{ of} \\ \text{Type II}}} \chi_{\lambda}(P_i)^2 + rc^2 - 2c\delta = b.$$

We take χ_0 as the 1-character. Then

$$(32) \quad \sum_{\substack{\lambda \text{ of} \\ \text{Type II} \\ \text{but } \lambda \neq 0}} |\chi_{\lambda}(P_i)|^2 + (r-1)c^2 + (c-\delta)^2 = b.$$

We now show that we may assume $r-1 > b$, in which case (32) implies $c = 0$. Suppose on the contrary that $r-1 \leq b$. We know from (L) that $\mathcal{P}$ must be a direct product of u cyclic groups each of the same order 2^a . Then it follows easily

from the following relations

$$a = ua,$$

$$b = 2^u - 1,$$

$$br = 2^a - 1$$

that $a = 1$ and our lemma is proved. Thus we may assume $r - 1 > b$ and hence $c = 0$.

From (13), (30), and (24) we obtain

$$(33) \quad rf_j = 2^a z_j - \delta, \quad \text{for } j \text{ of Type I.}$$

This last result shows that the characters $\chi_1, \chi_2, \dots, \chi_r$ of Type I are in the 2-block of lowest kind. Moreover, (33) together with (31) yields

$$(34) \quad z_j = sr \pm 1 \quad \text{for } j \text{ of Type I.}$$

We now prove the lemma by an induction on the order of the group. Before doing so, however, let us remark that if b is 1, then we must have case (β) . Indeed, since b is the number of elements of order 2 in $\mathcal{P}$, and since $\mathcal{N}$ has order $2^a b$, we see that if b equals 1 then $\mathcal{P}$ is cyclic and $\mathcal{N}$ is equal to $\mathcal{P}$. The Burnside-Frobenius theorem¹⁸ implies that $\mathcal{G}$ contains a normal subgroup of index 2^a , and we have case (β) .

We make the induction hypothesis that the lemma is true for all groups $\mathcal{K}$ of order smaller than g . We propose to show that we may assume that

$$z_\mu \geq 1 \quad \text{for } \mu \neq 0.$$

¹⁸See, for instance, Burnside, op. cit., p. 327.

Suppose some $z_\mu = 0$ for $\mu \neq 0$. Then $\mathcal{P}$ is contained in the kernel $\mathcal{K}$ of F_μ . The group $\mathcal{K}$ satisfies the assumptions of the lemma and has order smaller than g . Hence by our induction hypothesis, $\mathcal{K}$ is of type (α) , (β) , or (γ) .

If $\mathcal{K}$ is of type (α) , then $\mathcal{P}$ is the only subgroup of order 2^a in $\mathcal{K}$. Since $\mathcal{K}$ is a normal subgroup of $\mathcal{G}$, every conjugate of $\mathcal{P}$ in $\mathcal{G}$ is contained in $\mathcal{K}$ and must then be $\mathcal{P}$ itself. Hence $\mathcal{K}$ of type (α) implies $\mathcal{G}$ is of type (α) .

If $\mathcal{K}$ is of type (β) , b equals 1. As we mentioned above, $\mathcal{G}$ is then of type (β) .

Suppose $\mathcal{K}$ is of type (γ) but not of type (α) . By (L), all elements of order 2 in $\mathcal{K}$ are conjugate in $\mathcal{K}$. Let Q be an element of order 2 in $\mathcal{P}$ and let G be any element of $\mathcal{G}$. Since Q lies in $\mathcal{K}$ and $\mathcal{K}$ is normal in $\mathcal{G}$, it follows that $G^{-1}QG = K^{-1}QK$ for some K in $\mathcal{K}$. This means that GK^{-1} lies in $\mathcal{N}(Q) = \mathcal{P}$, and therefore G is in $\mathcal{K}$. Hence $\mathcal{G} = \mathcal{K}$, and we have reached a contradiction.

We have thus shown that under our induction hypothesis, we may assume that

$$z_\mu \geq 1 \quad \text{for } \mu \neq 0.$$

Now since $c = 0$, $s = \sum d_i f_i^* \geq 0$. We consider two cases:

$$(1) \quad s > 0$$

Equation (29) shows that $z_\lambda \geq r$ for $\lambda \neq 0$ of Type II. On the other hand, (34) shows that $z_j \geq r - 1$ for j of Type I. It follows that

$$(x - 1 - r)r^2 + r(r - 1)^2 \leq \sum_{\mu=1}^{x-1} z_{\mu}^2.$$

By (21),

$$\sum_{\mu=1}^{x-1} z_{\mu}^2 \leq r + r^2x - 2r^2 - 2r^2h'.$$

Hence $2h' \leq 1$, $h' = 0$. But by (K), $2h' \geq r - 1$. Therefore $r = 1$, $b = 2^a - 1$, and we have case (γ).

(1i) $s = 0$

$\sum d_i f_i^{\star} = 0$ implies that every $d_i = 0$. Then (31) and (30) become respectively

$$f_j = b, \quad \text{for } j = 1, 2, \dots, r,$$

and

$$\chi_{j(P_i)} = \theta_{j(P_i)}, \quad \text{for } j = 1, 2, \dots, r.$$

Then the tables of characters of $\mathcal{N}$ and $\mathcal{G}$ will have the following forms:

For n :

1	P_1	
$f_\mu^\star$	$f_\mu^\star$	
b	d_1	
b	d_2	
$\vdots$	$\vdots$	
$\vdots$	$\vdots$	
b	d_r	

For g :

1	P_1	
1	1	
b	d_1	
b	d_2	
$\vdots$	$\vdots$	
$\vdots$	$\vdots$	
b	d_r	
f_{r+1}	c_{r+1}	
$\vdots$	$\vdots$	
$\vdots$	$\vdots$	
f_{x-1}	c_{x-1}	
$2^a w_1$	0	
$\vdots$	$\vdots$	
$\vdots$	$\vdots$	
$2^a w_c$	0	

The orthogonality relations and (23) give

$$b + \sum d_i^2 = 2^a$$

and

$$1 + \sum d_i^2 + \sum c_\lambda^2 = 2^a.$$

Hence

$$1 + \sum c_\lambda^2 = b,$$

$$|c_\lambda| < \sqrt{b}, \quad (\lambda = r+1, r+2, \dots, x-1).$$

By (28)

$$f_\lambda = 2^a b_\lambda + c_\lambda.$$

Since $z_\lambda \neq 0$, (29) shows that $b_\lambda \neq 0$. Hence

$$(35) \quad f_{\lambda} > 2^a - \sqrt{b}, \quad (\lambda = r+1, \dots, x-1).$$

Now (L) tells us that $\mathcal{P}$ is a direct product of u cyclic groups each of the same order 2^a , so that

$$a = au.$$

Since b is the number of elements of order 2 in $\mathcal{P}$,

$$b = 2^u - 1.$$

Since $br = 2^a - 1$, we find that

$$r = \frac{2^a - 1}{2^u - 1},$$

$$r = 1 + 2^u + \dots + 2^{(a-1)u},$$

$$r \geq 1 + 2^u \quad \text{if } a \neq 1,$$

$$r \geq b + 2.$$

Hence

$$(36) \quad 2^a - 1 \geq b^2 + 2b.$$

By (35) and (36),

$$(37) \quad f_{\lambda} > b^2.$$

Now let χ be any character of $\mathcal{G}$ of degree b . $\chi \bar{\chi}$ is a sum of irreducible characters of $\mathcal{G}$. In this sum, the 1-character χ_0 occurs exactly once. Since the character $\chi \bar{\chi}$ has degree b^2 , (36) and (37) imply that the only characters other than χ_0 which do occur in the sum are all of degree b . It follows that b must divide 1,

$$b = 1.$$

By the remark on page 34, $\mathcal{G}$ is of type (β) in this case.

We are now ready to prove the main result of this paper.

Theorem 4: Assume $\mathcal{G}$ has the following properties:

- (a) Its order is $g = 2^a g'$, g' odd, $a \geq 1$.
- (b) Its 2-Sylow subgroups $\mathcal{P}$ are Abelian.
- (c) It contains no element of order $2p$ for p an odd prime.

Then we must have one of the following cases:

- (a) $\mathcal{P}$ is a normal subgroup of $\mathcal{G}$.
- (b) $\mathcal{P}$ is cyclic and $\mathcal{G}$ contains a normal subgroup of index 2^a .
- (c) $\mathcal{G} \cong \text{LF}(2, 2^a)$.

Proof: We use the same notation as in the proof of the lemma.

Let us make the induction hypothesis that the theorem is true for all groups of order less than g . We may assume that $\mathcal{G}$ is not of type (a) or (b) and that¹⁹

$$z_\mu \geq 1 \quad \text{for } \mu \neq 0.$$

As the lemma shows, our assumptions imply that

$$b = 2^a - 1$$

and

$$r = 1.$$

As before, P_1 denotes an element of order 2. We set

$$\chi_\mu(P_1) = d_\mu.$$

The d_μ are rational integers different from 0 for $\mu = 0, 1, \dots, x-1$; and equal to 0 for $i \geq x$.²⁰

¹⁹See the proof beginning on p. 35.

²⁰See R. Brauer and C. Nesbitt, p. 565, Th. 1, and p. 585, Th. 10.

By the orthogonality relations,

$$(36) \quad \sum_0^{x-1} d_\mu^2 = 2^a.$$

Since the d_μ in the last sum are different from 0,

$$(37) \quad x \leq 2^a.$$

We see that (13), (16), (18), and (19) become respectively the following:

$$(38) \quad f_\mu = d_\mu + 2^a z_\mu, \quad z_\mu \geq 0,$$

$$(39) \quad \sum_{\mu=0}^{x-1} z_\mu d_\mu = -1,$$

$$(40) \quad \frac{g' + 1}{2^a} = h - 1,$$

$$(41) \quad \sum_0^{x-1} z_\mu^2 + \sum_1^y w_\nu^2 = h - 1.$$

Since $z_\mu \geq 1$ for $\mu \neq 0$, (41) gives $x + y \leq h$. Since $x + y$ is the total number of classes of $\mathcal{G}$, we must have $h = x + y$, all the characters of $\mathcal{G}$ are real, and $z_\mu = 1$ for all $\mu \neq 0$. Moreover, every $w_\nu = 1$. We now have

$$(42) \quad \begin{cases} f_0 = 1, \\ f_\mu = d_\mu + 2^a & \text{for } \mu = 1, 2, \dots, x-1, \\ f_\mu = 2^a & \text{for } \mu \geq x, \end{cases}$$

and (39) becomes

$$(43) \quad \sum_{\mu=0}^{x-1} d_\mu = 0.$$

If we consider χ_μ as a character for $\mathcal{P}$ and denote by m_μ the multiplicity of the 1-character of $\mathcal{P}$ in χ_μ , we find that $1 + d_\mu = m_\mu$ for $\mu \neq 0$. This gives

$$(44) \quad d_\mu \geq -1 \quad \text{for } \mu \neq 0.$$

We now turn our attention to $\mathcal{N} = \mathcal{N}(\mathcal{P})$. Recalling that $b = 2^a - 1$ and $r = 1$, we see from the table of characters on page 31 that $\mathcal{N}$ has one irreducible representation of degree $2^a - 1$ and that every other irreducible representation of $\mathcal{N}$ is a representation of $\mathcal{N}/\mathcal{P}$. We denote the characters of $\mathcal{N}$ by Ω_i , and let $\Omega_\star$ be the character of degree $2^a - 1$. We obtain immediately from (22') and the table on page 31 that

$$(45) \quad \begin{cases} \Omega_\star(P) = -1 & \text{for } P \text{ of order } 2, \\ \Omega_\star(N) = 0 & \text{for } N \text{ in } \mathcal{N} \text{ and } N^2 \neq 1. \end{cases}$$

Let χ_μ be an irreducible character of $\mathcal{G}$ distinct from χ_0 , and consider χ_μ as a character $\chi_\mu(\mathcal{N})$ of $\mathcal{N}$. Let m_μ be the multiplicity of $\Omega_\star$ in $\chi_\mu(\mathcal{N})$. Denote by n the order of $\mathcal{N}$, by $K_i^\star$ the classes of $\mathcal{N}$, and by $g_i^\star$ the number of elements in $K_i^\star$. Then

$$nm_\mu = \sum_i g_i^\star \chi_\mu(K_i^\star) \Omega_\star(K_i^{\star -1}).$$

It follows from (45) and (42) that the last equation becomes

$$2^a(2^a - 1)m_\mu = f_\mu(2^a - 1) - (2^a - 1)(f_\mu - 2^a),$$

which reduces to

$$m_\mu = 1.$$

Hence each character χ of $\mathcal{G}$ distinct from χ_0 , when regarded as a character of $\mathcal{N}$, contains $\Omega_{\star}$ with multiplicity equal to 1. For χ of degree 2^a , $\chi(\mathcal{N}) = \Omega_{\star} + \Omega$ for some real character Ω of degree 1. Since Ω is a character of $\mathcal{N}/\mathcal{P}$, a group of odd order, Ω must be the 1-character Ω_0 of $\mathcal{N}$.

We set

$$\chi_i(\mathcal{N}) = \sum_j a_{ij} \Omega_j,$$

where the a_{ij} are rational integers greater than or equal to 0. Then

$$\sum_i f_i \chi_i(\mathcal{N}) = \sum_j \sum_i f_i a_{ij} \Omega_j.$$

By the orthogonality relations for the χ_i , we obtain

$$\begin{aligned} \sum_j \sum_i f_i a_{ij} \Omega_j(N) &= g, \quad \text{for } N = 1, \\ &= 0, \quad \text{for } N \neq 1, \end{aligned}$$

where N denotes an element of $\mathcal{N}$. Denoting the degree of Ω_j by $f_j^{\star}$, we also have

$$\begin{aligned} \sum_j f_j^{\star} \Omega_j(N) &= n, \quad \text{for } N = 1, \\ &= 0, \quad \text{for } N \neq 1. \end{aligned}$$

It readily follows that

$$\sum_j \left(\sum_i f_i a_{ij} \right) \Omega_j = \frac{g}{n} \sum_j f_j^{\star} \Omega_j,$$

and hence

$$\sum_i f_i a_{ij} = \frac{g}{n} f_j^{\star}.$$

In particular, writing a_i for a_{i0} , we have

$$\sum_1 f_1 a_1 = \frac{g}{n}.$$

For $f_1 = 2^a + d_1$, we know that $\chi_1(n)$ contains the character $\Omega_{\star}$ with multiplicity equal to 1. Since the degree of $\Omega_{\star}$ is $2^a - 1$, we see that

$$2^a + d_1 \geq 2^a - 1 + a_1,$$

$$d_1 + 1 \geq a_1.$$

We now have:

$$\text{For } f_0, \quad a_0 = 1.$$

$$\text{For } f_1 = 2^a - 1, \quad a_1 = 0.$$

$$\text{For } f_1 = 2^a + d_1, \quad d_1 > 0, \quad 0 \leq a_1 \leq d_1 + 1.$$

$$\text{For } f_1 = 2^a, \quad a_1 = 1.$$

Hence

$$(46) \quad 1 + \sum' f_1 a_1 + 2^a y = \frac{g}{n},$$

where the sum $\sum'$ is taken over all f_1 with $d_1 > 0$, excluding f_0 . Because of (40) and the fact that $n = 2^a(2^a - 1)$,

$$\frac{g}{n} = 1 + 2^a u$$

for some u . Then (46) becomes

$$(46') \quad \sum' (2^a + d_1) a_1 + 2^a y = 2^a u,$$

from which we obtain

$$(47) \quad \sum' d_1 a_1 \equiv 0 \pmod{2^a}.$$

Since $a_1 \leq d_1 + 1$, we have

$$(48) \quad \sum' d_i a_i \leq \sum' (d_i^2 + d_i).$$

Now by (36) and (43),

$$\sum_0^{x-1} (d_i^2 + d_i) = 2^a,$$

$$\sum_{\substack{d_i > 0 \\ i \neq 0}}' (d_i^2 + d_i) + \sum_{\substack{\text{over} \\ d_0 \text{ and} \\ d_i = -1}}'' (d_i^2 + d_i) = 2^a.$$

But

$$\sum'' = 2,$$

$$\sum' (d_i^2 + d_i) < 2^a.$$

Then (47) and (48) imply that

$$\begin{aligned} \sum' d_i a_i &= 0, \\ a_i &= 0 \end{aligned}$$

for every i . By (46'),

$$u = y.$$

Since

$$g' = (2^a - 1)(1 + 2^a y),$$

we see from (40) that

$$h = 2 + 2^a y - y.$$

Now

$$h = x + y,$$

and from (37)

$$(2^a - 2)y = x - 2 \leq 2^a - 2.$$

Hence for $a \neq 1$,

$$y = 1,$$

$$g = 2^a(2^a - 1)(2^a + 1).$$

If we can show that $\mathcal{G}$ has a triply-transitive permutation representation of degree $2^a + 1$, then our theorem will be proved.²¹ To this end, let $m = 2^a + 1$ and denote by $\mathcal{P} = \mathcal{P}_1, \mathcal{P}_2, \dots, \mathcal{P}_m$ the 2-Sylow subgroups of $\mathcal{G}$. To every G in $\mathcal{G}$ we associate the permutation $F(G)$ of the $\mathcal{P}_i$ which sends $\mathcal{P}_i$ into $G^{-1}\mathcal{P}_iG$. The representation $F(G)$ is of course simply-transitive.

Let $\mathcal{M}$ be the subgroup of $\mathcal{N} = \mathcal{N}(\mathcal{P})$ consisting of those elements which transform $\mathcal{P}_2$ into itself. The number of distinct $\mathcal{P}_i$ into which elements of $\mathcal{N}$ can transform $\mathcal{P}_2$ is equal to the index $(\mathcal{N}:\mathcal{M})$ of $\mathcal{M}$ in $\mathcal{N}$. We see that

$$2^a = m - 1 \geq (\mathcal{N}:\mathcal{M}).$$

Now the order of $\mathcal{M}$ must be odd; this follows from the fact that the intersection of $\mathcal{P}$ and $\mathcal{P}_2$ is 1. This means that $(\mathcal{N}:\mathcal{M})$ is at least 2^a and hence exactly 2^a . Therefore $F(G)$ is doubly-transitive.

Now let $\mathcal{J}$ be the subgroup of $\mathcal{M}$ which leaves $\mathcal{P}_3$ fixed. All that remains for us to show is that the index of $\mathcal{J}$ in $\mathcal{M}$ is $2^a - 1$, i.e., that $\mathcal{J}$ consists of only the identity. Since $F(G)$ is doubly-transitive, it can be split up into the 1-representation and one other irreducible representation of $\mathcal{G}$ of

²¹H. Zassenhaus, Abhandlungen aus dem Math. Seminar der Hamburgischen Universität, vol. 11, p. 17, 1935.

of degree 2^a . Let χ be the character of the latter. For any T in $\mathcal{T}$, the trace of $F(T)$ is $1 + \chi(T) \geq 3$, $\chi(T) \geq 2$. Now χ , regarded as a character of $\mathcal{N}$, is the sum of $\Omega_{\star}$ and the 1-character of $\mathcal{N}$.

Then (45) implies that $T = 1$. This completes the proof of theorem 4.

BIBLIOGRAPHY

- Blichfeldt, H. F., Finite Collineation Groups, University of Chicago Press, 1917.
- Brauer, R., On the Arithmetic in a Group Ring, National Academy of Sciences, vol. 30, 1944, pp. 109-114.
- Brauer, R., On Blocks of Characters of Groups of Finite Order II, National Academy of Sciences, vol. 32, 1946, pp. 215-219.
- Brauer, R., On the Connection between the Ordinary and the Modular Characters of Groups of Finite Order, Annals of Mathematics, vol. 42, 1941, pp. 926-935.
- Brauer, R. and Nesbitt, C., On the Modular Characters of Groups, Annals of Mathematics, vol. 42, 1941, pp. 556-590.
- Burnside, W., Theory of Groups of Finite Order, 2nd edition, Cambridge, 1911.
- Zassenhaus, H., Kennzeichnung endlicher linearer Gruppen als Permutations Gruppen, Abhandlungen aus dem Math. Seminar der Hamburgischen Universität, vol. 11, 1935, pp. 17-24.