Annals of Mathematics
Vol. 62, No. 3, November, 1955
Printed in U.S.A.

ON GROUPS OF EVEN ORDER

By Richard Brauer and K. A. Fowler

(Received September 14, 1954)

I. Introduction

1. Let $\mathfrak{G}$ be a group of finite order g. We prove first that if $g > 2$ is even, then there exists a proper subgroup of order $v > \sqrt[3]{g}$. The proof is quite elementary but the method cannot be applied if g is odd, though it seems probable that a similar statement holds in that case too. Indeed, if $\mathfrak{G}$ is soluble of an order $g > 1$, g not a prime, it is very easy to see that $\mathfrak{G}$ has a proper subgroup of order $v \geqq \sqrt{g}$. It is a well known unproved conjecture that all groups of odd order are soluble.

We shall use the term *involution* for a group element of order 2. If m is the total number of involutions of $\mathfrak{G}$ and if we set $n = g/m$, the same method shows that $\mathfrak{G}$ contains a normal subgroup $\mathfrak{K}$ distinct from $\mathfrak{G}$ such that the index of $\mathfrak{K}$ is either 2 or is less than $[n(n + 2)/2]!$ (where $[x]$ denotes the largest integer not exceeding the real number x). If J is an involution in $\mathfrak{G}$ and if $n(J)$ is the order of its normalizer $\mathfrak{N}(J)$ in $\mathfrak{G}$, then $n \leqq n(J)$. It then follows that there exist only a finite number of simple groups in which the normalizer of an involution is isomorphic to a given group.

2. The following terminology will be useful. An element G of a group $\mathfrak{G}$ will be said to be *real in* $\mathfrak{G}$ if G and G^{-1} are conjugate in $\mathfrak{G}$.[1] Real elements different from the identity 1 occur only in groups of even order. With G, every conjugate element is real. We may therefore speak of real and non-real classes of conjugate elements in $\mathfrak{G}$.

Let $\mathfrak{G}^{\#}$ denote the set of elements different from 1 in $\mathfrak{G}$. We introduce a "distance" $d(G, H)$ for any two elements G, H of $\mathfrak{G}^{\#}$. If $G = H$, set $d(G, H) = 0$. If $G \neq H$ and if there exists a chain $G_0, G_1, \cdots, G_l$ of elements of $\mathfrak{G}^{\#}$ with $G_0 = G$, $G_l = H$ such that G_{i-1} and G_i commute, let $d(G, H)$ denote the length l of the shortest such chain connecting G and H. In particular, $d(G, H) = 1$ if and only if G and H commute and $G \neq H$. If there does not exist a chain connecting G and H, set $d(G, H) = \infty$. It is clear that this distance has all the usual properties except that it can be infinite.

If $\mathfrak{M}$ is a subset of $\mathfrak{G}^{\#}$ and $G \in \mathfrak{G}^{\#}$, we define the distance $d(G, \mathfrak{M})$ of G from $\mathfrak{M}$ to be the minimum of the distances $d(G, H)$ for $H \in \mathfrak{M}$.

3. In Section III, it is shown that if the group $\mathfrak{G}$ contains more than one class of involutions, then any two involutions have distance at most 3. This implies that if the two elements G and H both have normalizers of even order

[1] An element G is real in $\mathfrak{G}$ if and only if every character of $\mathfrak{G}$ has a real value for G. Note that if G is not real in $\mathfrak{G}$, it may be real in groups containing $\mathfrak{G}$ as a subgroup.

in a group of this kind, then $d(G, H) \leqq 5$. The values 3 and 5 given here cannot be replaced by smaller values.

4. Section IV deals with properties of real elements G different from 1. If G has distance at least 4 from the set $\mathfrak{M}$ of involutions, this distance is infinite. Actually, the normalizer $\mathfrak{H} = \mathfrak{N}(G)$ of G in $\mathfrak{G}$ is an abelian group which is the normalizer of each of its elements $H \neq 1$. This implies that $d(H, L) = \infty$ if H is an element of $\mathfrak{H}$, $H \neq 1$, and L is an element of $\mathfrak{G}$ not in $\mathfrak{H}$. Subgroups $\mathfrak{H}$ of this type occur fairly frequently in groups of even order. They have a number of interesting properties. In particular, the order h of $\mathfrak{H}$ is relatively prime to its index. There exist involutions J which transform every element of $\mathfrak{H}$ into its inverse. If $n(J)$ is the order of the normalizer $\mathfrak{N}(J)$ of J in $\mathfrak{G}$, then $h \leqq n(J) + 1$, unless $\mathfrak{H}$ is a normal subgroup of $\mathfrak{G}$; in the latter case, $\mathfrak{G}$ "splits" into $\mathfrak{H}$ and a subgroup $\mathfrak{W}$ of $\mathfrak{N}(J)$. There exist infinitely many simple groups $\mathfrak{G}$ each of which contains a subgroup $\mathfrak{H}$ of the type here discussed with $h = n(J) + 1$.

Our results concerning real elements $G \neq 1$ of distance at most 3 from the set $\mathfrak{M}$ of involutions are rather fragmentary. It can happen that the distance from G to $\mathfrak{M}$ is actually equal to 3. In this connection, we show that, under certain conditions, some of the Sylow subgroups of $\mathfrak{G}$ are abelian. It is, of course, very easy to construct groups in which no Sylow subgroup is abelian. However, a large number of "interesting" groups seem to possess some abelian Sylow subgroups. Perhaps, in view of this, our result deserves consideration.

5. The last section deals with properties of the characters of groups of even order. If n has the same significance as in **1**, there exists an irreducible real character, not the 1-character, of a degree less than n. On the basis of this remark, one can study the cases where n is small. If the results of C. Jordan and H. F. Blichfeldt on linear groups of a given degree could be improved materially, this would make it possible to improve the results mentioned above in **1**.

If p is a prime dividing g with the exact exponent a, it may be that $\mathfrak{G}$ does not possess irreducible characters of defect 0 for p, that is, characters whose degrees are divisible by p^a. On the other hand, many "interesting" groups do have such characters. In Section V we give some sufficient conditions for the existence of characters of defect 0.

Finally, if $\mathfrak{G}$ contains a subgroup $\mathfrak{H}$ of the type discussed in **4**, rather detailed information concerning the values of the irreducible characters of $\mathfrak{G}$ for the elements of $\mathfrak{H}$ can be given. This is of great help in constructing the characters of $\mathfrak{G}$.

6. Notation. The normalizer of an element G of $\mathfrak{G}$ will be denoted by $\mathfrak{N}(G)$ and its order by $n(G)$. The set of elements X of $\mathfrak{G}$ which transform G into G or G^{-1}, that is, for which

$$X^{-1}GX = G \quad \text{or} \quad X^{-1}GX = G^{-1}$$

forms a subgroup $\mathfrak{N}^*(G)$. If G is non-real or if G is an involution, $\mathfrak{N}^*(G) = \mathfrak{N}(G)$. If G is real and of order greater than 2, $\mathfrak{N}^*(G)$ has order $2n(G)$.

The classes of conjugate elements of $\mathfrak{G}$ will be denoted by $\mathfrak{K}_0, \mathfrak{K}_1, \cdots, \mathfrak{K}_{k-1}$. Here, $\mathfrak{K}_0$ will be the class containing 1. Then the classes containing involutions are taken, say these are the classes $\mathfrak{K}_1, \cdots, \mathfrak{K}_r$. Next we take the other real classes and finally the non-real classes. Usually, G_i will denote a representative element for $\mathfrak{K}_i$. If $n_i = n(G_i)$, then $\mathfrak{K}_i$ consists of g/n_i elements.

The group ring of $\mathfrak{G}$ formed over the field of rational numbers will be denoted by Γ. With each $\mathfrak{K}_i$ we associate an element K_i of Γ. Here, K_i is the sum of the g/n_i elements of $\mathfrak{K}_i$. As is well known, the elements $\mathrm{K}_0, \mathrm{K}_1, \cdots, \mathrm{K}_{k-1}$ form a basis for the center Λ of Γ, and hence we have formulae

$$\mathrm{K}_i\mathrm{K}_j = \sum_{\mu=0}^{k-1} a_{ij\mu}\mathrm{K}_\mu . \tag{0}$$

Here, the $a_{ij\mu}$ are non-negative rational integers.

If $\mathfrak{H}$ is a subgroup of $\mathfrak{G}$, the index of $\mathfrak{H}$ in $\mathfrak{G}$ will be denoted by $(\mathfrak{G}:\mathfrak{H})$.

II. Existence of large subgroups

7. Let $\mathfrak{M}$ be the set of involutions of the group $\mathfrak{G}$ of even order. Then $\mathfrak{M}$ is the union of $\mathfrak{K}_1, \mathfrak{K}_2, \cdots, \mathfrak{K}_r$. Set

$$\mathrm{M} = \mathrm{K}_1 + \mathrm{K}_2 + \cdots + \mathrm{K}_r . \tag{1}$$

Then M is that element of Λ which is the sum of all the involutions in $\mathfrak{G}$. It follows from (0) that we have formulae

$$\mathrm{M}^2 = \sum_{i=0}^{k-1} c_i\mathrm{K}_i . \tag{2}$$

Clearly, the coefficient c_i is equal to the number of ordered pairs (X, Y) of involutions X, Y such that

$$XY = G_i \qquad (X, Y \in \mathfrak{M}). \tag{3}$$

We show

LEMMA (2A). *If $G_i^2 \neq 1$, then c_i is the number of involutions of $\mathfrak{G}$ which transform G_i into G_i^{-1}. If G_i is an involution, then $c_i = \nu_i - 1$ where ν_i is the number of involutions in $\mathfrak{N}(G_i)$. Finally, for $G_i = 1$, $c_i = m$.*

PROOF. If X, Y satisfy the conditions (3), then

$$G_i^{-1} = Y^{-1}X^{-1} = YX = X^{-1}(XY)X = X^{-1}G_iX.$$

Conversely, if $X^{-1}G_iX = G_i^{-1}$ and $X \in \mathfrak{M}$, then the element $Y = XG_i$ satisfies the equation $Y^2 = 1$. Hence the conditions (3) are satisfied if $Y \neq 1$. We have $Y = 1$ if and only if $G_i = X$, and then G_i itself is an involution. All the statements of the lemma are now readily obtained.

COROLLARY (2B). *If G_i is non-real, $c_i = 0$. For any G_i, $c_i \leqq n(G_i)$. If G_i is an involution, $c_i \leqq n(G_i) - 2$.*

PROOF. If G_i is not real, the lemma shows that $c_i = 0$. If G_i is real, there are exactly $n(G_i)$ elements which transform G_i into G_i^{-1}, and hence $c_i \leqq n(G_i) = n_i$. Finally, if G_i is an involution, $\nu_i \leqq n_i - 1$ and hence $c_i \leqq n_i - 2$.

5. Counting the number of group elements occurring on both sides of (2), we obtain

$$m^2 = \sum_i c_i g/n_i ,$$

where m is the number of involutions in $\mathfrak{G}$. We now apply (2A) and (2B). For each real G_i, $c_i g/n_i \leqq g$. If k_1 is the number of real classes, we obtain

$$m^2 \leqq m + \sum_{i=1}^{r} (\nu_i - 1)g/n_i + (k_1 - r - 1)g \tag{4}$$

where the last term originates from the $k_1 - r - 1$ real classes $\mathfrak{K}_i$ of elements of order larger than 2.

The number of involutions is given by

$$m = \sum_{i=1}^{r} g/n_i . \tag{5}$$

If we set

$$\nu = \text{Max}\ \{\nu_1, \nu_2, \cdots, \nu_r\}$$

we obtain

$$m^2 \leqq \nu m + (k_1 - r - 1)g. \tag{4*}$$

On the other hand, since the total number of real elements is at most g, we have

$$1 + m + \sum_{i=r+1}^{k_1-1} g/n_i \leqq g. \tag{6}$$

Thus if we set

$$h = \text{Max}\ \{n_i\} \qquad \text{for } i = r + 1, r + 2, \cdots, k_1 - 1$$

we have

$$(k_1 - r - 1)g \leqq h(g - m - 1).$$

This is still true for $k_1 = r + 1$, if we set $h = 0$. If we substitute this in (4*) we obtain

(2C). *Let $\mathfrak{G}$ be a group of even order g which contains m involutions. If ν is the maximal number of involutions which can occur in the normalizer of an involution, then*

$$m^2 \leqq hg + (\nu - h)m - h$$

where h is either the order of the normalizer $\mathfrak{N}(H)$ of a real element H of order greater than 2 or $h = 0$.

We now prove

THEOREM (2D). *If $\mathfrak{G}$ is a group of even order $g > 2$, there exists a subgroup $\mathfrak{B} \neq \mathfrak{G}$ of order $v > \sqrt[3]{g}$.*

PROOF. If we set $m = g/n$, then (2C) yields

$$g \leqq hn^2 + (\nu - h)n = hn(n - 1) + \nu n.$$

One of the groups $\mathfrak{N}(G_i)$ with $1 \leqq i \leqq r$ contains ν involutions and hence $\nu \leqq n_i - 1$ for some such i. On the other hand, (5) yields

$$n^{-1} = n_1^{-1} + n_2^{-1} + \cdots + n_r^{-1} \tag{5*}$$

and hence $n \leqq n_i$. It now follows that

$$g \leqq hn_i(n_i - 1) + (n_i - 1)n_i = (h + 1)n_i(n_i - 1).$$

If $n_i \leqq h$, then $g < h^3$. Now h is the order of a subgroup $\mathfrak{N}(H)$ and, since H is conjugate to $H^{-1} \neq H$ in $\mathfrak{G}$, we have $\mathfrak{N}(H) \neq \mathfrak{G}$. Hence the theorem holds in this case.

If $h < n_i$, we have $g < n_i^3$. If $n_i \neq g$, the theorem is true with $\mathfrak{V} = \mathfrak{N}(G_i)$.

It remains to deal with the case $n_i = g$. Then $\mathfrak{G}$ contains an invariant involution G_i. We may assume that the theorem has been proved for groups of even order less than g. If $g/2$ is even and $g \neq 4$, we may apply the theorem to $\mathfrak{G}/\{G_i\}$. It follows that $\mathfrak{G}/\{G_i\}$ contains a subgroup $\mathfrak{V}^* \neq \mathfrak{G}/\{G_i\}$ of an order $v^* > \sqrt[3]{g/2}$. Since we may set $\mathfrak{V}^* = \mathfrak{V}/\{G_i\}$ where $\mathfrak{V}$ is a subgroup of order.$v = 2v^*$ of $\mathfrak{G}$, we have

$$g > v > \sqrt[3]{4g} > \sqrt[3]{g}.$$

Again the theorem holds. It is trivial for $g = 4$.

Finally, if $g/2$ is odd, it is well known[2] that $\mathfrak{G}$ contains a subgroup of order $g/2$ and $g/2 > \sqrt[3]{g}$. Hence the theorem holds in all cases.

(2E). *If $\mathfrak{G}$ does not contain invariant involutions, the group $\mathfrak{V}$ in* (2D) *can be chosen as the normalizer of a suitable real element of $\mathfrak{G}$.*

9. We use a method very similar to that in **8** in order to obtain a slightly stronger result.

Some of the classes $\mathfrak{K}_1, \mathfrak{K}_2, \cdots, \mathfrak{K}_r$ may consist of invariant involutions. Assume that the notation is chosen such that these are the classes $\mathfrak{K}_i$ with $i = 1, 2, \cdots, r'$. If there is no invariant involution, set $r' = 0$. Since we have $n_i = g$, $\mathfrak{N}(G_i) = \mathfrak{G}$ for $i = 1, 2, \cdots, r'$, we have $c_i = \nu_i - 1 = m - 1$ for $1 \leqq i \leqq r'$. Now (4) becomes

$$m^2 \leqq m + r'(m - 1) + \textstyle\sum_{i=r'+1}^{r} (n_i - 2)g/n_i + (k_1 - r - 1)g.$$

The formula (5) can be written in the form

$$m = r' + \textstyle\sum_{i=r'+1}^{r} g/n_i$$

and we obtain

$$m^2 \leqq m + r'(m - 1) + (r - r')g - 2(m - r') + (k_1 - r - 1)g$$

and hence

$$m^2 \leqq (r' - 1)m + r' + (r - r')g + (k_1 - r - 1)g. \tag{7}$$

[2] For instance, this is a simple consequence of a Theorem of Burnside. See [3], p. 133.

Let u denote the minimal index of all the subgroups of $\mathfrak{G}$ which are distinct from $\mathfrak{G}$, and assume that $u > 2$. Since $n_i < g$ for $i = r' + 1, \cdots, r$, we have $u \leqq g/n_i$ for these i, and (5*) yields

$$(r - r')u \leqq m - r'.$$

For $i = r + 1, r + 2, \cdots, k_1 - 1$, let $\mathfrak{N}^*(G_i)$ denote the group of order $2n_i$ introduced in **6**. Since $\mathfrak{N}^*(G_i)$ has a subgroup $\mathfrak{N}(G_i)$ of index 2 and we assumed $u > 2$, we must have $\mathfrak{N}^*(G_i) \neq \mathfrak{G}$. It follows that u cannot exceed the index $g/2n_i$ of $\mathfrak{N}^*(G_i)$ in $\mathfrak{G}$. Now (6) implies

$$2u(k_1 - r - 1) \leqq g - 1 - m.$$

If we combine the last two inequalities with (7), we obtain

$$m^2 \leqq (r' - 1)m + r' + (m - r')g/u + g(g - 1 - m)/2u.$$

Again set $m = g/n$. An easy computation yields

$$\text{(8)} \qquad \begin{gathered} g < (r' - 1)n + gn/2u + gn^2/2u, \\ g - gn(n + 1)/2u < (r' - 1)n. \end{gathered}$$

In particular, if $r' \leqq 1$ we must have $n(n + 1)/2u > 1$, that is, $u < n(n + 1)/2$.

Suppose that $r' > 1$ and assume that $u \geqq n(n + 2)/2$, $u \neq 2$. Then (8) yields

$$(r' - 1)n > gn/2u$$

and hence

$$g < 2u(r' - 1).$$

The r' invariant involutions together with 1 form a subgroup $\mathfrak{C}$ of order $r' + 1$ of the center of $\mathfrak{G}$. Since any subgroup of $\mathfrak{G}/\mathfrak{C}$ different from $\mathfrak{G}/\mathfrak{C}$ has an index at least u, the order of such a subgroup is not greater than $g/u(r' + 1)$, and

$$g/u(r' + 1) < g/u(r' - 1) < 2.$$

It follows that $\mathfrak{G}/\mathfrak{C}$ is certainly cyclic. Hence $\mathfrak{G}$ is generated by $\mathfrak{C}$ and at most one additional element. Since $\mathfrak{C}$ lies in the center of $\mathfrak{G}$, it follows that $\mathfrak{G}$ is abelian. But then $\mathfrak{G}$ has a subgroup of index 2, whereas we assumed $u > 2$. Thus the assumptions $u > 2$, $u \geqq n(n + 2)/2$ lead to a contradiction. This proves the theorem:

THEOREM (2F). *Let $\mathfrak{G}$ be a group of even order g which contains exactly m involutions. If $n = g/m$, then $\mathfrak{G}$ contains a subgroup of index u such that either $u = 2$ or*

$$1 < u < n(n + 2)/2.$$

If $\mathfrak{G}$ contains at most one invariant involution, the number $n(n + 2)/2$ can be replaced by $n(n + 1)/2$.

We now are able to obtain a slight improvement of (2D). We state:

COROLLARY (2G). *If $\mathfrak{G}$ is a group of even order $g > 2$, there exists a subgroup $\mathfrak{V} \neq \mathfrak{G}$ of order $v > \sqrt[3]{2g} - 1/3$.*

PROOF. If $\mathfrak{G}$ contains a subgroup of index 2, the statement is true, since $g/2 \geqq \sqrt[3]{2g}$ for $g \geqq 4$. Assume that $\mathfrak{G}$ does not have subgroups of index 2.

Suppose first that $\mathfrak{G}$ does not contain invariant involutions. If $\mathfrak{V}$ is a subgroup of $\mathfrak{G}$ of maximal order $v < g$, Theorem (2F) shows that $g/v < n(n+1)/2$. It follows from (5*) that $n \leqq n_1$, and since n_1 is the order of a subgroup $\mathfrak{N}(G_1) \neq \mathfrak{G}$, we have $n_1 \leqq v$. Thus $2g < v^2(v+1)$. One easily sees that this implies $v > \sqrt[3]{2g} - 1/3$.

The case in which $\mathfrak{G}$ contains invariant involutions can be treated in a manner similar to that used in the proof of (2D).

THEOREM (2H). *If $\mathfrak{G}$ is a group of even order g which contains m involutions and if $n = g/m$, then there exists a normal subgroup $\mathfrak{K} \neq \mathfrak{G}$ of $\mathfrak{G}$ such that $\mathfrak{G}/\mathfrak{K}$ is isomorphic to a subgroup of the symmetric group on u letters with $u = 2$ or $u < n(n+2)/2$. In particular, $(\mathfrak{G}:\mathfrak{K}) = 2$ or $(\mathfrak{G}:\mathfrak{K}) < [n(n+2)/2]!$ If $\mathfrak{G}$ contains at most one invariant involution, the number $n(n+2)/2$ can be replaced by $n(n+1)/2$.*

PROOF. If $\mathfrak{V}$ is the subgroup mentioned in (2F), there corresponds to $\mathfrak{V}$ a permutation representation of $\mathfrak{G}$ of degree u. We obtain (2H) by taking for $\mathfrak{K}$ the kernel of this representation.

COROLLARY (2I). *If $\mathfrak{G}$ is a simple group of even order $g > 2$ which contains m involutions and if $n = g/m$, then*

$$g < [n(n+1)/2]!$$

If J is an involution of $\mathfrak{G}$, then n in the inequality can be replaced by $n(J)$. There exist only a finite number of simple groups in which the normalizer of an involution is isomorphic to a given group.

PROOF. The first statement follows at once from (2H), since a simple group of even order $g > 2$ cannot contain an invariant involution. The second statement then follows from (5*), which implies $n \leqq n(J)$.

10. For a later application, we mention still another result which is obtained by the method used above.

THEOREM (2J). *If $\mathfrak{G}$ is a group of even order g which contains exactly m involutions, then the number k_1 of real classes of $\mathfrak{G}$ satisfies the inequality*

$$k_1 - 1 \geqq m(m+1)/g.$$

PROOF. In (4), ν_i can be replaced by $n_i - 1$. Then

$$m^2 \leqq m + rg - 2\textstyle\sum_{i=1}^{r} g/n_i + (k_1 - r - 1)g.$$

This, together with (5), yields

$$m^2 \leqq -m + (k_1 - 1)g.$$

III. Groups with more than one class of involutions

11. We now prove

LEMMA (3A). *If the two involutions X and Y of $\mathfrak{G}$ are not conjugate in $\mathfrak{G}$, there exists an involution J which commutes with X and Y.*

PROOF. Set $G = XY$. As we have seen in the proof of (2A), both X and Y transform G into G^{-1}. Then G is real, and X and Y are elements of the group $\mathfrak{N}^*(G)$ introduced in Section **6**. If $G = 1$, then $X = Y$. If G has order 2, then G is an involution which commutes with X and Y. Thus we may suppose that G has order greater than 2. Then $\mathfrak{N}^*(G)$ has order $2n(G)$. If $n(G)$ were odd, both $\{X\}$ and $\{Y\}$ would be 2-Sylow groups of $\mathfrak{N}^*(G)$. Then X and Y would be conjugate in $\mathfrak{N}^*(G)$ and hence in $\mathfrak{G}$, contrary to the hypothesis. Hence $n(G)$ is even. Let $\mathfrak{P}^*$ be a 2-Sylow group of $\mathfrak{N}^*(G)$ which contains X. Since $X \notin \mathfrak{N}(G)$, the intersection $\mathfrak{P} = \mathfrak{P}^* \cap \mathfrak{N}(G)$ must have index 2 in $\mathfrak{P}^*$, and $\mathfrak{P}$ is a 2-Sylow group of $\mathfrak{N}(G)$. The order of $\mathfrak{P}$ is at least 2, and since $\mathfrak{P}$ is normal in $\mathfrak{P}^*$ we can find a normal subgroup $\{J\}$ of order 2 of $\mathfrak{P}^*$ such that $\{J\} \subseteq \mathfrak{P}$. Then J is an involution which commutes with X and G and hence with $Y = XG$.

We now prove

THEOREM (3B). *Let $\mathfrak{G}$ be a group of order g which contains $r \geqq 2$ classes of involutions $\mathfrak{K}_1, \mathfrak{K}_2, \cdots, \mathfrak{K}_r$. For $G_i \in \mathfrak{K}_i$, let n_i denote the order of the normalizer $\mathfrak{N}(G_i)$ of G_i, and let ν_i denote the number of involutions in $\mathfrak{N}(G_i)$. If ν is the maximum of the ν_i, then*

$$g \leqq (\nu - 2)(\nu_1 - 1)/(n_2^{-1} + n_3^{-1} + \cdots + n_r^{-1}).$$

PROOF. Let J range over the $\nu_1 - 1$ involutions of $\mathfrak{N}(G_1)$ distinct from G_1, and for each J denote by $\mathfrak{A}(J)$ the set of involutions of $\mathfrak{N}(J)$ which do not commute with G_1. For a fixed J, $\mathfrak{A}(J)$ contains at most $\nu - 3$ elements, since G_1, J, and G_1J are distinct involutions in $\mathfrak{N}(J)$ which commute with G_1. It follows from (3A) that each involution not in $\mathfrak{K}_1$ and not in $\mathfrak{N}(G_1)$ must lie in one of the sets $\mathfrak{A}(J)$. If $\mathfrak{U}$ denotes the union of the classes $\mathfrak{K}_2, \mathfrak{K}_3, \cdots, \mathfrak{K}_r$, then at most $(\nu_1 - 1)(\nu - 3)$ elements of $\mathfrak{U}$ do not commute with G_1. Since at most $\nu_1 - 1$ elements of $\mathfrak{U}$ do commute with G_1, and since $\mathfrak{U}$ contains exactly $g(n_2^{-1} + \cdots + n_r^{-1})$ elements, we obtain

$$g(n_2^{-1} + \cdots + n_r^{-1}) \leqq (\nu - 2)(\nu_1 - 1).$$

This proves the theorem.

COROLLARY (3C). *If the notation is the same as in (3B), and if the notation is chosen such that $n_1 \leqq n_2 \leqq \cdots \leqq n_r$, then*

$$g < n_1 n_2 n_r; \qquad (r - 1)g < n_1 n_r \sqrt[r-1]{n_2 n_3 \cdots n_r} \leqq n_1 n_r^2.$$

Indeed, since $\nu_i \leqq n_i - 1$, we have

$$(\nu - 2)(\nu_1 - 1) < n_1 n_r.$$

On the other hand

$$n_2^{-1} + \cdots + n_r^{-1} \geqq n_2^{-1}$$

and

$$n_2^{-1} + \cdots + n_r^{-1} \geqq (r - 1) \sqrt[r-1]{(n_2 \cdots n_r)^{-1}} \geqq (r - 1)n_r^{-1}.$$

In particular, we have $n_r > \sqrt[3]{(r-1)g}$. This shows that if $\mathfrak{G}$ does not contain invariant involutions and if $r \geqq 2$, then the group $\mathfrak{B}$ in (2D) can be chosen as the normalizer of an involution. For $r \geqq 3$, we obtain an improvement of (2G).

12. Using the terminology introduced in the introduction, we state

THEOREM (3D). *If $\mathfrak{G}$ contains more than one class of involutions, then any two involutions of $\mathfrak{G}$ have distance at most* 3.

PROOF. If the two involutions X and Z belong to different classes, it follows from (3A) that $d(X, Z) \leqq 2$. Suppose then that X, Z belong to the same class $\mathfrak{K}_i$. It follows from (3A) that some element X_1 of $\mathfrak{K}_i$ must commute with an involution Y not in $\mathfrak{K}_i$. After replacing X_1 and Y by conjugates, we may assume X equals X_1. Since Z and Y belong to different classes, we have $d(Z, Y) \leqq 2$. On the other hand, $d(X, Y) = 1$. Hence $d(X, Z) \leqq 3$.

COROLLARY (3E). *If $\mathfrak{G}$ contains more than one class of involutions, then any two elements G_1 and G_2 with even $n(G_1)$, $n(G_2)$ have distance at most* 5.

Indeed, if $n(G_i)$ is even, there exists an involution X_i which commutes with G_i. Hence

$$d(G_1, X_1) \leqq 1, \qquad d(X_1, X_2) \leqq 3, \qquad d(X_2, G_2) \leqq 1.$$

It follows that $d(G_1, G_2) \leqq 5$.

REMARK. There exist groups with more than one class of involutions in which involutions of distance 3 occur. For instance, let $\mathfrak{G}$ be the symmetric group on p letters, where p is a prime and $p \geqq 5$. If G is a cycle of length p, there exists an involution X which transforms G into G^{-1}. Then $Y = XG$ also is an involution. If an element Z commutes with both X and Y, then Z would commute with G and hence Z would be a power of G. The only power of G which commutes with an involution is 1. Hence $Z = 1$ and this shows that $d(X, Y) > 2$.

A similar argument can be used to prove

(3F). *If $\mathfrak{G}$ is a group of even order which contains a real element G such that $n(H)$ is odd for every H different from* 1 *in $\mathfrak{N}(G)$, then $\mathfrak{G}$ contains involutions which have distance greater than* 2.

One can also show by examples that the number 5 in (3E) cannot be replaced by a smaller value.

IV. The set of real elements

13. We prove

LEMMA (4A). *If G is a real element of the group $\mathfrak{G}$ of even order and if $n(G)$ is odd, then there exists an involution J which transforms G into G^{-1}. All involutions which transform G into G^{-1} are conjugate in $\mathfrak{G}$, and the number of such involutions is equal to the index of $\mathfrak{N}(G) \cap \mathfrak{N}(J)$ in $\mathfrak{N}(G)$.*

PROOF. Since $n(G)$ is odd, G is not an involution. Then the group $\mathfrak{N}^*(G)$ has even order $2n(G)$ and therefore it contains an involution J. Since $n(G)$ is odd, J cannot transform G into G. Hence J transforms G into G^{-1}.

If X is any involution such that $X^{-1}GX = G^{-1}$, one sees as in the proof of (3A) that X is conjugate to J in $\mathfrak{N}^*(G)$. The number of elements in the class of J in $\mathfrak{N}^*(G)$ is equal to the index of $\mathfrak{N}^*(G) \cap \mathfrak{N}(J)$ in $\mathfrak{N}^*(G)$, and every element in this class is an involution which transforms G into G^{-1}. Since J does not belong to the subgroup $\mathfrak{N}(G)$ of index 2 of $\mathfrak{N}^*(G)$, it follows that $\mathfrak{N}(G) \cap \mathfrak{N}(J)$ has index 2 in $\mathfrak{N}^*(G) \cap \mathfrak{N}(J)$. Hence the index of $\mathfrak{N}(G) \cap \mathfrak{N}(J)$ in $\mathfrak{N}(G)$ is equal to the index of $\mathfrak{N}^*(G) \cap \mathfrak{N}(J)$ in $\mathfrak{N}^*(G)$. This completes the proof.

The following theorem is essentially a restatement of a result due to Burnside, [2], pp. 229, 230.

THEOREM (4B). *Let $\mathfrak{H}$ be a subgroup of $\mathfrak{G}$. If there exists an involution J in the normalizer of $\mathfrak{H}$, and if J commutes with no element of $\mathfrak{H}$ different from* 1, *then $\mathfrak{H}$ is abelian of odd order and J transforms every element of $\mathfrak{H}$ into its inverse.*

PROOF. Every element of $\mathfrak{H}$ can be written in the form $JH^{-1}JH$ for $H \in \mathfrak{H}$. Hence J transforms every element of $\mathfrak{H}$ into its inverse. This implies that $\mathfrak{H}$ cannot contain an involution. For H, $K \in \mathfrak{H}$,

$$KH = J(H^{-1}K^{-1})J = (JH^{-1}J)(JK^{-1}J) = HK,$$

and hence $\mathfrak{H}$ is abelian.

As an immediate consequence of (4B), we have

COROLLARY (4C). *Assume that $G \neq 1$ is an element of $\mathfrak{G}$ which is transformed into its inverse by the involution J. If $d(G, J) \geqq 3$, then $\mathfrak{N}(G)$ is abelian of odd order and J transforms each element of $\mathfrak{N}(G)$ into its inverse.*

We now prove

THEOREM (4D). *Assume that $d(G, J) \geqq 4$ in* (4C). *Then $\mathfrak{N}(G)$ is the normalizer of each of its elements different from* 1; *and $d(H, Z) = \infty$ for $H \in \mathfrak{N}(G)$, $Z \notin \mathfrak{N}(G)$, $H \neq 1$.*

PROOF. It follows from (4C) that $\mathfrak{N}(G)$ is abelian. If $H \in \mathfrak{N}(G)$, then $\mathfrak{N}(G) \subseteq \mathfrak{N}(H)$. For $H \neq 1$, we have $d(H, J) \geqq 3$ and hence (4C) can be applied to H instead of G: Since $\mathfrak{N}(H)$ is abelian and $G \in \mathfrak{N}(H)$, we have $\mathfrak{N}(H) \subseteq \mathfrak{N}(G)$ and hence $\mathfrak{N}(G) = \mathfrak{N}(H)$.

It is now clear that any element $H \neq 1$ of $\mathfrak{N}(G)$ has distance at most 1 from every element different from 1 of $\mathfrak{N}(G)$ and distance ∞ from every element not in $\mathfrak{N}(G)$.

COROLLARY (4E). *If a real element $G \neq 1$ has distance at least* 4 *from the set $\mathfrak{M}$ of involutions, then $d(G, \mathfrak{M}) = \infty$ and $\mathfrak{N}(G)$ is the normalizer of each $H \neq 1$ in $\mathfrak{N}(G)$.*

Indeed, (4A) shows that there exists an involution J such that $J^{-1}GJ = G^{-1}$. Then (4C) and (4D) apply. Since $n(G)$ is odd, all involutions lie outside $\mathfrak{N}(G)$.

14. We consider a subgroup $\mathfrak{H}$ of an arbitrary group $\mathfrak{G}$ of finite order g such that $\mathfrak{H}$ is the normalizer of each of its elements different from 1. Our results will apply to the subgroup $\mathfrak{N}(G)$ in (4D).

It is clear that $\mathfrak{H}$ will be abelian. If p is a prime dividing the order h of $\mathfrak{H}$, there exists an element P of order p in $\mathfrak{H}$. Let $\mathfrak{P}$ be a p-Sylow group of $\mathfrak{G}$ which contains P, and let $P_0 \neq 1$ be an element of the center of $\mathfrak{P}$. Then $P_0 \in \mathfrak{N}(P) = \mathfrak{H}$ and hence $\mathfrak{N}(P_0) = \mathfrak{H}$. Since $\mathfrak{P} \subseteqq \mathfrak{N}(P_0) = \mathfrak{H}$, it follows that p is prime to the index g/h of $\mathfrak{H}$.

Let $\mathfrak{N}$ denote the normalizer of $\mathfrak{H}$ in $\mathfrak{G}$. Since $\mathfrak{H}$ is a normal subgroup of $\mathfrak{N}$ and since h is relatively prime to $(\mathfrak{N}:\mathfrak{H})$, there exists a subgroup $\mathfrak{W}$ such that ([3], p. 125)

$$\mathfrak{N} = \mathfrak{H}\mathfrak{W}, \qquad \mathfrak{H} \cap \mathfrak{W} = \{1\}.$$

If $\mathfrak{W}$ has order w, then $\mathfrak{N}$ has order hw.

In $\mathfrak{N}$, the $h - 1$ elements $H \neq 1$ of $\mathfrak{H}$ have normalizers of order h. Hence they are distributed into $(h - 1)/w$ classes of conjugate elements each consisting of w elements. In particular, w divides $h - 1$. Actually, if p^a is the highest power of a prime p dividing h, then w divides $p^a - 1$. This is seen by considering a Sylow group of $\mathfrak{H}$.

If an element A of $\mathfrak{G}$ transforms an element $H \neq 1$ of $\mathfrak{H}$ into an element K of $\mathfrak{H}$, we have $A^{-1}\mathfrak{N}(H)A = \mathfrak{N}(K)$, that is, $A^{-1}\mathfrak{H}A = \mathfrak{H}$ and hence A lies in $\mathfrak{N}$.

No two distinct conjugates of $\mathfrak{H}$ can have an intersection different from 1, since each conjugate of $\mathfrak{H}$ is the normalizer of each of its elements different from 1. Now the arguments leading to Sylow's theorem show that the number of conjugates is congruent to 1 modulo h. If we denote this number by $1 + Nh$, where N is a rational integer, then $g/(hw) = 1 + Nh$ and hence $g = wh(1 + Nh)$.

We have proved

THEOREM (4F). *If $\mathfrak{G}$ is a group of finite order g and $\mathfrak{H}$ is a subgroup such that $\mathfrak{H}$ is the normalizer of each of its elements different from* 1, *then $\mathfrak{H}$ is abelian and its order h is relatively prime to its index g/h. We can set*

$$(9) \qquad g = hw(1 + Nh); \qquad h - 1 = wt,$$

where t, w, and N are rational integers, $t \geqq 0$, $w \geqq 1$, $N \geqq 0$. The normalizer $\mathfrak{N}$ of $\mathfrak{H}$ has order hw and there exists a subgroup $\mathfrak{W}$ of order w such that

$$(10) \qquad \mathfrak{N} = \mathfrak{H}\mathfrak{W}; \qquad \mathfrak{H} \cap \mathfrak{W} = \{1\}.$$

Each element of $\mathfrak{H}$ different from 1 *is conjugate in $\mathfrak{G}$ to exactly w elements of $\mathfrak{H}$ and any two of these w elements are conjugate in $\mathfrak{N}$.*

15. We now take for $\mathfrak{H}$ the group $\mathfrak{N}(G)$ in (4D). Since J maps each $H \in \mathfrak{H}$ on its inverse, we have $J \in \mathfrak{N}$. After replacing $\mathfrak{W}$ by a conjugate group in $\mathfrak{N}$, we may assume $J \in \mathfrak{W}$. Let H be a fixed element of $\mathfrak{H}$ different from 1. Since $\mathfrak{N}(H) = \mathfrak{H}$, only the elements of $\mathfrak{H}J$ will transform H into H^{-1}. On the other hand, for $W \in \mathfrak{W}$, the element $W^{-1}JW$ transforms each element of $\mathfrak{H}$ into its inverse. Hence we have $W^{-1}JW = H_0J$ with $H_0 \in \mathfrak{H}$. Since J, $W \in \mathfrak{W}$, it follows that $H_0 \in \mathfrak{W}$. Now (10) shows that $H_0 = 1$ and hence that $W^{-1}JW = J$. We now have

THEOREM (4G). *If $\mathfrak{G}$ is a group of even order g and G is a real element different from* 1 *which has distance at least* 4 (*and hence distance* ∞) *from the set of involutions, the results of* (4F) *apply to $\mathfrak{H} = \mathfrak{N}(G)$. If J is an involution which transforms G into G^{-1} and hence every element of $\mathfrak{H}$ into its inverse, we may choose $\mathfrak{W}$ in* (10) *such that $J \in \mathfrak{W}$ and $\mathfrak{W} \subseteqq \mathfrak{N}(J)$. The number w is even.*

16. Let $H \in \mathfrak{H}$, $H \neq 1$. Our results show that there exist exactly h involutions which transform H into H^{-1}. It then follows from (2A) and its proof that there exist exactly h ordered pairs (X, Y) of involutions with the product H; moreover, if (X, Y) is any such pair, then both X and Y transform H into H^{-1}. Then, by (4A), X and Y belong to the same class of $\mathfrak{G}$ as J does. Denote this class by $\mathfrak{K}_1$. We now see that there are exactly h ordered pairs of elements of $\mathfrak{K}_1$ with the product H.

From (0) we have

$$\mathrm{K}_1^2 = \textstyle\sum_{i=0}^{k-1} a_{11i}\mathrm{K}_i. \tag{11}$$

If $H \in \mathfrak{K}_\lambda$, then $a_{11\lambda}$ is equal to the number of ordered pairs of elements of $\mathfrak{K}_1$ with the product H. Hence $a_{11\lambda} = h$.

The number of elements in $\mathfrak{K}_1$ is g/n_1. It follows easily that $a_{110} = g/n_1$. Counting the number of group elements occurring on both sides of (11), we obtain

$$(g/n_1)^2 = g/n_1 + \textstyle\sum_{i=1}^{k-1} a_{11i}g/n_i. \tag{12}$$

For the class $\mathfrak{K}_\lambda$, we have $a_{11\lambda} = h$, $n_\lambda = h$, and thus the term in (12) for $i = \lambda$ is g. There are exactly $(h-1)/w = t$ classes $\mathfrak{K}_\lambda$ which contain elements of $\mathfrak{H}$ different from 1.

It may happen that there are several non-conjugate groups of the same type as $\mathfrak{H}$ whose elements are transformed into their inverses by the same involution J. Let us denote these groups by $\mathfrak{H}_i$ $(i = 1, 2, \cdots, s)$ and let t_i have the same significance for $\mathfrak{H}_i$ as t had for $\mathfrak{H}$. Then the elements of $\mathfrak{H}_i$ different from 1 will contribute t_i terms g to the sum in (12) and different $\mathfrak{H}_i$ must contribute different terms. Hence

$$g^2/n_1^2 \geqq g/n_1 + g\textstyle\sum_{i=1}^{s} t_i, \qquad g \geqq n_1 + n_1^2 \sum t_i.$$

We have shown

(4H). *Suppose that J is an involution of $\mathfrak{G}$ and that there exist elements $X_1, X_2, \cdots, X_s$ each of which is transformed into its inverse by J, each of which has distance at least* 4 *from J, and which are such that no element of the class of X_i commutes with X_j for $i \neq j$. If the elements different from* 1 *of $\mathfrak{H}_i = \mathfrak{N}(X_i)$ belong to t_i different classes in $\mathfrak{G}$, then*

$$g \geqq n(J) + n(J)^2 \textstyle\sum_{i=1}^{s} t_i. \tag{13}$$

17. Again let $\mathfrak{H}$ be the group mentioned in (4G), and consider the h sets $H\mathfrak{M}$ with $H \in \mathfrak{H}$. If two such sets $H_1\mathfrak{M}$ and $H_2\mathfrak{M}$ with $H_1, H_2 \in \mathfrak{H}$, $H_1 \neq H_2$, have an element D in common, there exist involutions J_1 and J_2 such that $D = H_1J_1 = H_2J_2$, $H_1^{-1}H_2 = J_1J_2$. Then, as we have seen in the proof of (2A), J_1 transforms $H_1^{-1}H_2$ into its inverse. Hence $J_1 \in \mathfrak{H}J$, $H_1J_1 \in \mathfrak{H}J$, and hence $H_1\mathfrak{M} \cap H_2\mathfrak{M} \subseteq \mathfrak{H}J$. Conversely, if H and H_0 are any two elements of $\mathfrak{H}$, then $J^{-1}H^{-1}H_0J = H_0^{-1}H$. It follows that $(H^{-1}H_0J)^2 = 1$. Since J does not lie in $\mathfrak{H}$, $H^{-1}H_0J \in \mathfrak{M}$. This shows that $\mathfrak{H}J$ is contained in each of the sets $H\mathfrak{M}$. Thus, $H_1\mathfrak{M} \cap H_2\mathfrak{M} = \mathfrak{H}J$.

If m again denotes the number of involutions in $\mathfrak{G}$, then each $H\mathfrak{M}$ contains the h elements of $\mathfrak{H}J$ and $m - h$ elements which do not appear in any of the other sets $H_1\mathfrak{M}$. The number of elements in the union of the sets $H\mathfrak{M}$ is therefore $h + h(m - h)$. No element of $\mathfrak{H}$ can appear in a set $H\mathfrak{M}$ since $\mathfrak{H}$ has odd order and cannot contain an involution. Since we have g elements in $\mathfrak{G}$, at most $g - h$ distinct elements can lie in the union of the sets $H\mathfrak{M}$. Hence

$$h + h(m - h) \leqq g - h.$$

This yields $mh - g \leqq h(h - 2)$. If we again set $m = g/n$, we obtain

$$g(h - n) \leqq h(h - 2)n.$$

(4I). *Let h be the order of the group $\mathfrak{H}$ in* (4G), *and let m be the number of involutions in $\mathfrak{G}$. If $h > g/m = n$, then*

$$g \leqq \frac{h(h - 2)n}{h - n}. \tag{14}$$

18. Set $n(J) = n_1$. Since w divides n_1 (cf. (4G)), we can set $n_1 = wz$, where z is a positive rational integer. On the other hand, n_1 divides g/h. Indeed, if this were not so, there would exist an element P in $\mathfrak{N}(J)$ of a prime order dividing h. Some conjugate P_1 of P then belongs to $\mathfrak{H}$ and hence $n(P_1) = h$. This implies that $n(P) = h$. However, since $J \in \mathfrak{N}(P)$, $n(P)$ must be even and we have a contradiction. Thus n_1 divides g/h. Since $n_1 = wz$, it follows from (9) that z divides $1 + Nh$. Set $1 + Nh = zx$, where x is a positive rational integer. Then

$$\begin{gathered} g = hwxz; \\ h - 1 = wt, \qquad 1 + Nh = xz, \qquad n_1 = wz. \end{gathered} \tag{15}$$

Suppose that $h > n_1$. It then follows from (5*) that $h > n$ and hence (14) holds. Since $n(h - n_1) \leqq n_1(h - n)$,

$$g \leqq \frac{h(h - 2)n_1}{h - n_1}. \tag{16}$$

Set $v = h - n_1 > 0$. We then have

$$xv = xh - xn_1 = xh - xwz = -w + h(x - wN).$$

It follows from (15) and (16) that $x \leqq (h - 2)/v$. Thus, we must have

$$x - wN = 1; \qquad xv = -w + h. \tag{17}$$

Since $wz = n_1 = h - v$, the equation (15) becomes

$$(18) \qquad g = hn_1(h - w)/(h - n_1) = h(h - v)(h - w)/v.$$

On the other hand, (13) shows that

$$n_1 + n_1^2 t \leqq g.$$

This in conjunction with (18) yields

$$(19) \qquad (1 + n_1 t)(h - n_1) \leqq h(h - w).$$

Multiply both members of (19) by w and recall that $wt = h - 1$. An easy computation yields

$$(20) \qquad h^2(n_1 - w) - h(n_1^2 + n_1 - w^2) + (w + n_1^2) \leqq 0.$$

If $w = n_1$, then (15) shows that $z = 1$, $x = 1 + Nh$, and since (17) implies $wN = hN$,. where $w \leqq h - 1$, we must have $N = 0$. Then $\mathfrak{H}$ is normal in $\mathfrak{G}$. If this case is excluded, then by (15) $n_1 > w$, $z > 1$. If we had $h \geqq (n_1^2 + n_1 - w^2)/(n_1 - w)$, the left hand side of (20) would be positive, which is impossible. Hence

$$h < (n_1^2 + n_1 - w^2)/(n_1 - w) = n_1 + w + n_1/(n_1 - w).$$

Now $n_1/(n_1 - w) = wz/(wz - w) = z/(z - 1) \leqq 2$. Thus $h \leqq n_1 + w + 1$. By (15), $h \equiv 1 \equiv 1 + n_1 \pmod{w}$, and since we assumed $h > n_1$, it follows that $h = 1 + n_1$ or $h = 1 + n_1 + w$. In the latter case, (19) becomes

$$(1 + n_1 t)(1 + w) \leqq h(1 + n_1) = (tw + 1)(1 + n_1),$$

and then $n_1 t + w \leqq wt + n_1$, $n_1(t - 1) \leqq w(t - 1)$. Since $n_1 > w$, we must have $t = 1$. Then $h - 1 = w$, and since $h = 1 + n_1 + w$, we obtain $n_1 = 0$, a contradiction. It follows that we must have $h = 1 + n_1$. This yields the result

THEOREM (4J). *Let $\mathfrak{G}$ be a group of even order g which contains a real element G different from* 1 *and with distance at least* 4 *from the set of involutions. Let J be any involution which transforms G into G^{-1}. If the group $\mathfrak{N}(G)$ is not normal in $\mathfrak{G}$, then its order h is at most $n(J) + 1$. The case $h = n(J) + 1$ occurs only if $g = h(h - 1)(h - w)$, where w is the order of the group $\mathfrak{W}$ mentioned in* (4G).

There exist infinitely many groups in which the case $h = n(J) + 1$ occurs. If $\mathfrak{G}$ is the group $LF(2, 2^a)$ of order $g = (2^a + 1)2^a(2^a - 1)$, there exists only one class of involutions, $r = 1$, $n = n_1 = 2^a$, and there exists a subgroup $\mathfrak{H}$ of the type here discussed with $h = 2^a + 1$. Here, $w = 2$, $t = (h - 1)/2 = 2^{a-1}$.

19. We conclude this section with a few simple remarks:

(4K). *If $\mathfrak{M}_0$ is a set consisting of m_0 involutions of $\mathfrak{G}$, any subgroup $\mathfrak{L}$ of order $l > g/(m_0 + 1)$ contains an element L_0 different from* 1 *which is transformed into its inverse by some element J of $\mathfrak{M}_0$.*

PROOF. If $\mathfrak{L}$ contains an element J of $\mathfrak{M}_0$, we may take $L_0 = J$ and we have $J^{-1}L_0J = L_0^{-1}$. Assume then that $\mathfrak{L}$ and $\mathfrak{M}_0$ are disjoint.

If two sets $L_1\mathfrak{M}_0$ and $L_2\mathfrak{M}_0$, with L_1, $L_2 \in \mathfrak{L}$, $L_1 \neq L_2$, are not disjoint, there exist involutions J_1, $J_2 \in \mathfrak{M}_0$ such that $L_1J_1 = L_2J_2$. Then $L_1^{-1}L_2 = J_1J_2$ and J_1 transforms the element $L_0 = L_1^{-1} L_2 \in \mathfrak{L}$ into its inverse.

If the l sets $L\mathfrak{M}_0$, $L \in \mathfrak{L}$, are pairwise disjoint, their union contains lm_0 distinct elements. Since no element of $\mathfrak{L}$ appears, we have $lm_0 \leqq g - l$ and hence $l \leqq g/(m_0 + 1)$.

As a special case, we note

(4L). *If $\mathfrak{G}$ contains m involutions, any subgroup $\mathfrak{L}$ of order $l > g/(m + 1)$ contains real elements different from* 1. *In particular, if $n = g/m$, any subgroup of order $l \geqq n$ contains real elements different from* 1.

The following example shows that this result cannot be improved substantially. If $\mathfrak{G} = LF(2, q)$ and q is a prime power with $q \equiv -1 \pmod 4$, the subgroups of order q do not contain real elements different from 1. On the other hand, $m = q(q - 1)/2$ and $g/(m + 1) < q + 1$.

As another consequence of (4K), we note that if the group $\mathfrak{G}$ in (4G) contains $r \geqq 2$ classes of involutions $\mathfrak{K}_1, \mathfrak{K}_2, \cdots, \mathfrak{K}_r$ and if $J \in \mathfrak{K}_1$, then

$$h \leqq (n_2^{-1} + n_3^{-1} + \cdots + n_r^{-1} + g^{-1})^{-1}.$$

Indeed, as we have seen above, no element of one of the classes $\mathfrak{K}_2, \mathfrak{K}_3, \cdots, \mathfrak{K}^r$ can transform an element of $\mathfrak{H}$ different from 1 into its inverse.

It is a consequence of (4G) that if subgroups $\mathfrak{H}$ of the type discussed there occur, then some of the Sylow groups of $\mathfrak{G}$ are abelian and consist entirely of real elements. We can obtain the same conclusion under slightly different assumptions.

(4M). *Let p be an odd prime. If $\mathfrak{G}$ contains real elements of an order divisible by p, and if every real element of order p has distance greater than* 2 *from the set of involutions of $\mathfrak{G}$, then the p-Sylow groups $\mathfrak{P}$ of $\mathfrak{G}$ are abelian and consist entirely of real elements. All the elements of $\mathfrak{P}$ different from* 1 *have the same normalizer, which is abelian and consists entirely of real elements.*

Proof. Let G be a real element of an order divisible by p. After replacing G by a suitable power, we may assume that G has order p. Then (4A) and (4C) show that there exist involutions J which transform G into G^{-1}, that $\mathfrak{N}(G)$ is abelian, and that J transforms every element of $\mathfrak{N}(G)$ into its inverse. Let $\mathfrak{P}$ be a p-Sylow subgroup of $\mathfrak{G}$ which contains G, and let G_0 be an element of order p in the center of $\mathfrak{P}$. Since $G_0 \in \mathfrak{N}(G)$, we can apply the above argument to G_0 instead of G. Since $\mathfrak{P} \subseteqq \mathfrak{N}(G_0)$, $\mathfrak{P}$ is abelian and consists entirely of real elements.

Now let P be an element of $\mathfrak{P}$ different from 1. A suitable power P^s of P has order p. The above argument shows that $\mathfrak{N}(P^s)$, and hence $\mathfrak{N}(P)$, is abelian and consists entirely of real elements. It now follows easily that all the elements of $\mathfrak{P}$ different from 1 have the same normalizer.

V. Results concerning the characters

20. Let $\mathfrak{G}$ be a group of even order g. Let $\chi_0, \chi_1, \cdots, \chi_{k-1}$ denote the ordinary irreducible characters of $\mathfrak{G}$, and let f_i denote the degree of χ_i. We take χ_0 to be the 1-character. It is well known that the number of real characters is equal to the number k_1 of real classes of conjugate elements. Let f be the minimal degree of a real character χ_i with $i > 0$. Since

$$\textstyle\sum_{i=0}^{k-1} f_i^2 = g,$$

it follows that

$$1 + (k_1 - 1)f^2 \leqq g.$$

Now (2J) shows that $m(m + 1)f^2 \leqq g(g - 1)$. This yields

(5A). *If $\mathfrak{G}$ is a group of even order g which contains m involutions, there exists a real character, not the* 1*-character, of a degree f such that*

$$f \leqq \sqrt{g(g - 1)/(m^2 + m)}.$$

In particular, if $n = g/m$, then $f < n$.

Thus if $n \leqq 2$, that is, if at least half of the elements of $\mathfrak{G}$ are involutions, $\mathfrak{G}$ has a real character of degree 1 which is not the 1-character. This implies that $\mathfrak{G}$ has a normal subgroup of index 2. One can also show that the elements in $\mathfrak{G}$ of odd order form a normal subgroup of $\mathfrak{G}$. Using the known groups of degree 2, one can obtain

(5B). *If the group $\mathfrak{G}$ of even order g contains at least $g/3$ involutions, then $\mathfrak{G}$ has a normal subgroup $\mathfrak{G}_0$ such that $\mathfrak{G}/\mathfrak{G}_0$ either is cyclic of order* 2 *or* 3 *or is the icosahedral group of order* 60.

If (5A) is combined with Jordan's and Blichfeldt's Theorems on linear groups of given degrees, results similar to (2H) can be obtained. However, our present knowledge in this matter does not enable us to improve the results given in II.

21. We denote by $\chi_{\rho i}$ the value of the character χ_ρ for the class $\mathfrak{K}_i$. It is well known that to every character χ_ρ of $\mathfrak{G}$ there corresponds a character ω_ρ of degree 1 of the center Λ of the group algebra Γ. The values of ω_ρ for the elements of the basis $\mathrm{K}_0, \cdots, \mathrm{K}_{k-1}$ of Λ are given by

$$\omega_\rho(\mathrm{K}_i) = \frac{g\chi_{\rho i}}{n_i f_\rho}.$$

It follows from (0) that

$$\omega_\rho(\mathrm{K}_i)\omega_\rho(\mathrm{K}_j) = \textstyle\sum_\mu a_{ij\mu}\omega_\rho(\mathrm{K}_\mu),$$

and hence

$$gn_i^{-1}n_j^{-1}\chi_{\rho i}\chi_{\rho j} = f_\rho \textstyle\sum_\mu a_{ij\mu}\chi_{\rho\mu}n_\mu^{-1}.$$

If we multiply both members of the last equation by $\bar{\chi}_{\rho\lambda}$ for a fixed value of λ, add over all ρ, and apply the orthogonality relations for group characters, we obtain the well known formulae

$$a_{ij\lambda} = gn_i^{-1}n_j^{-1}\textstyle\sum_\rho \chi_{\rho i}\chi_{\rho j}\bar{\chi}_{\rho\lambda}f_\rho^{-1}. \tag{21}$$

As above, we denote the classes containing involutions by $\mathfrak{K}_1, \mathfrak{K}_2, \cdots, \mathfrak{K}_r$. It follows from (1), (0), and (2) that

$$c_\lambda = \textstyle\sum_{i,j=1}^r a_{ij\lambda}. \tag{22}$$

If we take into account that $\chi_{\rho i}$ is real for $i = 1, 2, \cdots, r$, we obtain

$$c_\lambda = g\textstyle\sum_{i,j=1}^r n_i^{-1}n_j^{-1}\sum_\rho \chi_{\rho i}\chi_{\rho j}\chi_{\rho\lambda}f_\rho^{-1}. \tag{23}$$

We now show

(5C). *Suppose that G is a real element of the group $\mathfrak{G}$ of even order g for which $n(G)$ is odd and that J is an involution which transforms G into G^{-1}* (cf. 4A). *If p is a prime which divides $n(G)$ with the exact exponent ν but which does not divide $n(J)$, then $\mathfrak{G}$ possesses a p-block B of defect $d \leqq \nu$. We may choose B such that it contains characters of positive defect for* 2.

Proof. It follows from (4A) that all involutions transforming G into G^{-1} lie in one class, say in $\mathfrak{K}_1$. If G belongs say to $\mathfrak{K}_\lambda$, then (2A) and (4A) show that $c_\lambda = a_{11\lambda}$ and that c_λ is a divisor n_λ/s of n_λ, where s is the order of $\mathfrak{N}(G) \cap \mathfrak{N}(J)$. Then, for $i, j = 1$, (21) becomes

$$n_\lambda n_1^2 = gs\textstyle\sum_\rho \chi_{\rho 1}^2\chi_{\rho\lambda}f_\rho^{-1}.$$

Since p and n_1 are relatively prime, there must exist a value of ρ such that

$$gn_\lambda^{-1}\chi_{\rho 1}^2\chi_{\rho\lambda}f_\rho^{-1} = \chi_{\rho 1}^2\omega_\rho(\mathrm{K}_\lambda)$$

is not divisible by a prime ideal divisor $\mathfrak{p}$ of p in the field of characters. Then

$$\chi_{\rho 1} \not\equiv 0 \pmod{p}, \qquad \omega_\rho(\mathrm{K}_\lambda) \not\equiv 0 \pmod{\mathfrak{p}}. \tag{24}$$

The second condition implies that χ_ρ belongs to a p-block of defect $d \leqq \nu$. Indeed, if χ_ρ belongs to a p-block B of defect d, there exists a character χ_μ in B with $g/(p^df_\mu)$ prime to p. Now $\omega_\rho(\mathrm{K}_\lambda) \equiv \omega_\mu(\mathrm{K}_\lambda) \pmod{\mathfrak{p}}$. Since

$$\omega_\mu(\mathrm{K}_\lambda) = g\chi_{\mu\lambda}/(n_\lambda f_\mu)$$

is prime to $\mathfrak{p}$, n_λ must be divisible by p^d, that is, $\nu \geqq d$. The first condition (24) implies $\chi_{\rho 1} \neq 0$, and hence χ_ρ must be of positive defect for 2.

Corollary (5D). *If, in* (5C), *$n(G)$ is prime to p, then there exists a character of $\mathfrak{G}$ which is of defect* 0 *for p and of positive defect for* 2.

22. There is a second case in which we can prove that $\mathfrak{G}$ possesses characters of defect 0.

(5E). *Suppose that J is an involution and that for some odd prime p there exists a prime power group $\mathfrak{P}_0$ of order $p^c > 1$ such that no element of $\mathfrak{P}_0$ different from* 1 *is mapped on its inverse by any conjugate of J. If p divides $n(J)$ with the exact exponent ν, then there exists an irreducible character χ_ρ whose degree is divisible by $p^{c-\nu}$ and which is of positive defect for* 2. *In particular, if $\mathfrak{P}_0$ can be taken as a p-Sylow group of $\mathfrak{G}$ and if $\nu = 0$, then χ_ρ is of defect* 0 *for p.*

Proof. If J belongs to $\mathfrak{K}_1$, then the proof of (2A) shows that under our assumptions $a_{11\lambda} = 0$ for each class $\mathfrak{K}_\lambda$ with $\lambda > 0$ which contains elements of $\mathfrak{P}_0$. For $P \in \mathfrak{P}_0$, set

$$\psi(P) = \sum_\rho \chi_\rho(J)^2 \chi_\rho(P) f_\rho^{-1}. \tag{25}$$

It follows from (21) that $\psi(P) = 0$ for every element $P \neq 1$ in $\mathfrak{P}_0$. For $P = 1$, we see from the orthogonality relations that

$$\psi(1) = \sum_\rho \chi_\rho(J)^2 = n(J).$$

If φ denotes the character of the regular representation of $\mathfrak{P}_0$, it follows that

$$\psi = n(J)/p^c \varphi. \tag{26}$$

On the other hand, we can express the restriction of χ_ρ to $\mathfrak{P}_0$ in terms of the irreducible characters of $\mathfrak{P}_0$, in order to obtain an expression of $\psi(P)$ in terms of the irreducible characters of $\mathfrak{P}_0$. If the restriction of χ_ρ contains the 1-character of $\mathfrak{P}_0$ with the multiplicity b_ρ, then comparison of the multiplicity of this 1-character in (25) and (26) yields

$$\sum \chi_\rho(J)^2 b_\rho / f_\rho = n(J)/p^c.$$

Since the right hand side contains p with the exponent $c - \nu$ in the denominator, and since all $\chi_\rho(J)$ and b_ρ are rational integers, there must exist a value ρ such that $p^{c-\nu}$ divides f_ρ and $\chi_\rho(J) \neq 0$. This yields the statement.

An immediate consequence of (5E) is

(5F). *Let J be an involution and let p be an odd prime dividing g. If no element of order p is transformed into its inverse by J, and if p divides $n(J)$ with the exact exponent ν and g with the exact exponent a, then there exists an irreducible character whose degree is divisible by $p^{a-\nu}$ and which is of positive defect for* 2.

23. We conclude the paper with some remarks concerning the case that $\mathfrak{G}$ contains a subgroup $\mathfrak{H}$ which satisfies the assumptions of (4F). It is immaterial here whether the order g is even or odd, but we mention these remarks here since they can be applied in the case of (4G). If the notation is the same as in (4F), there exist t characters $\theta_1, \cdots, \theta_t$ of degree w of the group $\mathfrak{N}$. Then $\mathfrak{G}$ possesses t irreducible characters $\psi_1, \cdots, \psi_t$ all of the same degree z such that

$$\psi_j(H) = \gamma + \delta\theta_j(H)$$

for $H \in \mathfrak{H}$, $H \neq 1$. Here, γ and δ are independent of j and H, γ is a rational integer, and $\delta = \pm 1$. For elements G of $\mathfrak{G}$ which are not conjugate to such an element H, we have

$$\psi_1(G) = \psi_2(G) = \cdots = \psi_t(G).$$

If χ_j are the other characters, not of this "exceptional" kind, then $\chi_j(H)$ has a fixed rational integral value a_j for all $H \in \mathfrak{H}$, $H \neq 1$. The degree f_j of χ_j satisfies the congruence

$$f_j \equiv a_j \pmod{h},$$

while the degree z of the ψ_j satisfies

$$z \equiv \gamma + \delta w \qquad (\mathrm{mod}\ h).$$

These results are a special case of a more general result which was obtained originally as an application of a theorem on characters [1]. A direct simple proof using induced characters was given by M. Suzuki.

Using the orthogonality relations for group characters, one obtains the following additional relations:

$$(t - 1)\gamma^2 + (\gamma - \delta)^2 + \sum a_j^2 = w + 1, \qquad t\gamma z + \sum f_j a_j = \delta z.$$

Harvard University
University of Arizona

References

[1] R. Brauer, *A characterization of the characters of groups of finite order*, Ann. of Math., 57 (1953), pp. 357–377.

[2] W. Burnside, Theory of Groups of Finite Order, Cambridge, 1897.

[3] H. Zassenhaus, Lehrbuch der Gruppentheorie, Leipzig, 1937.