FINITE GROUPS WITH LARGE SUBGROUPS

BY
HELMUT BENDER[1]

1. Introduction

Considerations concerning the distribution of involutions in the cosets of a given subgroup are often useful in the study of groups of even order. The reason seems to be that if the index $|G:H|$ of a subgroup H of a (finite) group G is small compared to the number of involutions in G, not very many involutions can enjoy the privilege to sit in a coset of H without sharing it with any other involution. Those cosets however, which contain more than one involution are controlled by the normalizers of non-identity subgroups of H, because of the following observation:

Let $u \in G$ be an involution. Then an element $h \in H$ is inverted by u (i.e. $h^u = h^{-1}$) if and only if $h = vu$ with an involution $v \in Hu$.

In Section 2 we try to bring the above remarks in a more precise form, and the relations derived there will be illustrated at two examples in Sections 3 and 4.

2. An inequality

Let G be a group with a subgroup H such that $|J| > |G:H|$ where J denotes the set of involutions in G. Furthermore, define

J_n = *set of* $u \in J - H$ *such that* $|Hu \cap J| = n$,
b_n = *number of cosets* $Hg \neq H$ *such that* $|Hg \cap J| = n$,
c = *number of* $u \in J_1$ *such that* $C_H(u) \neq 1$,
$f = |J|/|G:H| - 1 > 0$.

Note that $|J_n| = nb_n$, and that J_n consists of those involutions outside H which invert exactly n elements of H. Clearly, H acts fixed-point-freely on the set of $u \in J_1$ satisfying $C_H(u) = 1$. Then the two equalities in the following lemma are obvious.

LEMMA. (1) $|J| = |J \cap H| + b_1 + 2b_2 + 3b_3 + \cdots$.
(2) $b_1 = c + m|H|$ *for some integer* $m \geq 0$.
(3) $b_1 < f^{-1}(|J \cap H| + b_2 + 2b_3 + 3b_4 + \cdots) - 1 - b_2 - b_3 - b_4 - \cdots$.

It remains to prove the inequality. Clearly, $|G:H| = 1 + \sum_{i\geq 0} b_i$. Hence

$$|J| - |G:H| = |J \cap H| - 1 - b_0 + b_2 + 2b_3 + 3b_4 + \cdots.$$

Received October 12, 1972.

[1] This research was partially done at the University of Illinois at Chicago Circle and was supported by a National Science Foundation grant.

Since $|J| - |G{:}H| = f|G:H|$, it follows that

$$b_1 = |G{:}H| - 1 - b_0 - \textstyle\sum_{i\geq 2} b_i$$
$$= f^{-1}(|J \cap H| - 1 - b_0 + b_2 + 2b_3 + 3b_4 + \cdots) - 1 - b_0 - \textstyle\sum_{i\geq 2} b_i.$$

As $b_0 \geq 0$, the inequality follows from this.

Remark. From some knowledge of normalizers of non-identity subgroups of H one can obtain a lower bound, say b, of b_0. Replacing b_0 in the above expression for b_1 by b, may then yield a more useful inequality.

3. The groups $L_2(7)$ and $L_2(9)$

To begin with an easy example for the application of the lemma, consider a group G of even order such that the centralizer of every involution is dihedral of order 8. We will see that G looks like $L_2(7)$ or $L_2(9)$.

Fix an elementary abelian subgroup V of order 4. Since V is contained in two distinct Sylow 2-subgroups (of order 8), $N_G(V)/V$ must be dihedral of order 6.

Fix a subgroup X of order 3 in $N_G(V)$. We refer to part (i) of the lemma as Lemma (i).

Case 1. $C_G(X) \nsubseteq N_G(V)$. Let $A = C_G(X)$ and $H = N_G(X)$. Then $H = A\langle t\rangle$ where t is an involution of $N_{N_G(V)}(X)$.

Since the centralizer of any involution is a 2-group, A has odd order, and $C_A(t) = 1$. The latter implies $x^t = x^{-1}$ for all $x \in A$. Hence A is abelian. Likewise, $C_G(x)$ is abelian and hence equal to A, for all elements $x \neq 1$ of A.

It follows that $H^g \cap A \neq 1$ implies $g \in N_G(A)$. Since every involution of $N_G(A)$ inverts A, H must contain all involutions of $N_G(A)$.

This implies $|H \cap H^u| \leq 2$ for all involutions u outside H.

Hence $b_n = 0$ for $n \geq 3$.

There are $a = |A|$ involutions in H, and each commutes with 4 involutions outside H. Hence $2b_2 = |J_2| = 4a$ and thus $b_2 = 2a$.

The number of involutions (they are all conjugate) equals the index of the centralizer of an involution. Hence $f = |J|/|G:H| - 1 = 2a/8 - 1 = (a-4)/4$.

Clearly, $a \geq 9$ and a divides b_1. Then Lemma 3 gives

$$0 \leq b_1 < \frac{4}{a-4}(a+2a) - 1 - 2a = 12 + 4\cdot 12/(a-4) - 1 - 2a$$
$$< 12 + 10 - 1 - 2a = 21 - 2a.$$

It follows that $a = 9$ and $b_1 = 0$. Now Lemma 1 yields

$$|G|/8 = |J| = |J \cap H| + 2b_2 = a + 4a = 5\cdot 9.$$

Hence $|G| = 9\cdot 8\cdot 5$; and since $|A| = 9$ divides $|G{:}N_G(A)| - 1$, it follows that $|N_G(A)| = 9\cdot 4$.

Case 2. $C_G(X) \subseteq N_G(V)$. Then $N_G(X) \subseteq N_G(V)$. Let $H = N_G(V)$. Let t be an involution outside H. Since t normalizes $H \cap H^t$, and since H contains the normalizer of every subgroup of order 3 and every subgroup $\neq 1$ contained in V, $H \cap H^t$ must be elementary abelian. Hence t inverts not more than two elements of H.

H has 6 involutions outside V, and each commutes with 2 involutions outside H. Hence $2b_2 = | J_2 | = 6 \cdot 2$ and thus $b_2 = 6$. Furthermore, $| J \cap H | = 9$ and $b_n = 0$ for $n \geq 3$. Since $| H | = 3 \cdot 8$, we have $f = | J |/|G : H| - 1 = 3 - 1 = 2$.

Now Lemma 3 yields $b_1 < \frac{1}{2}(9 + 6) - 1 - 6 < 1$. Hence $b_1 = 0$. Then Lemma 1 gives

$$| G |/8 = | J | = | J \cap H | + 2b_2 = 9 + 12 = 21.$$

Hence $| G | = 7 \cdot 3 \cdot 8$.

4. Janko's first simple group

Janko has studied a group G of even order satisfying the conditions (i) and (ii) below, and has shown that up to isomorphism there exists exactly one such group G.

(i) Involutions of G are conjugate

(ii) If $t \in G$ is an involution, then $C_G(t) = \langle t \rangle \oplus L$ where L is isomorphic to the simple group A_5 of order 60.

With help of our lemma we will determine the order of G. Another character-free proof of this result is contained in an unpublished paper of Thompson.

Fix a Sylow 2-subgroup Q of G and an involution $z \in Q$. Since Q has order 8, and involutions of Q are already conjugate in $N_G(Q)$, $N_G(Q)/Q$ must be a non-abelian group of order $3 \cdot 7$. We also need

4.1. *Let U be a subgroup in $C_G(z)$ of prime order $p \neq 2$. Then $C_G(U) = A\langle z \rangle$ where A has order p or 15. In particular, U is a Sylow p-subgroup of G.*

Proof. The proof of Janko's Lemma 3.1 shows that otherwise $C_G(U) = A\langle z \rangle$ with A elementary abelian of order 3^3, and $N_G(A) = AVX$ with V a four-group normalized by the subgroup X of order 3.

Since $C_G(V)$ is a Sylow 2-subgroup of G, X centralizes some involution and hence is conjugate to U. Hence $Y = C_A(X)X \subseteq B$ for some conjugate B of A. Then $Z = N_{N_G(A)}(Y) \subseteq N_G(B)$ because $B = C_G(Y)$.

Clearly, $C_A(V) = 1$ implies $| C_A(X) | = 3$. It follows that Z is non-abelian of order 3^3, and that A is the only abelian subgroup of order 3^3 in $N_G(A)$ and hence even in a Sylow 3-subgroup of G. However, $N_G(Z)$ has a normal Sylow 3-subgroup containing both A and B, a contradiction.

In the following, let $d = 3$ if the subgroup A in (4.1) (always) has order 15; in the other case, let $d = 1$.

Then (4.1) has the following consequence:

4.2. *A subgroup of order 3 is inverted by $6d$ involutions and centralized by $2d$-1 involutions.*

A subgroup of order 5 *centralizes d involutions.*

Next we prove:

4.3. *Let S be a subgroup of order* 7 *in $N_G(Q)$. If $N_G(S)$ has even order, then $C_G(S) = S$.*

Proof. Suppose false. Let $A = C_G(S)$. By (4.1), $a = |A|$ is not divisible by a prime ≤ 5. Hence $a \geq 49$, and $C_A(t) = 1$ for any involution t of $N_G(S)$. Then t inverts A, and A is abelian. Likewise, $C_G(x)$ is abelian, for every element $x \neq 1$ of A. Hence $C_G(x) = A$ for all those elements. Clearly, $N_{N_G(Q)}(S)$ has a subgroup of order 3.

We apply the lemma to $H = N_G(A) = AC_H(t)$. Since $C_H(t)$ contains a non-identity 3-element and is fixed-point-free on A, $C_H(t)$ is cyclic of order 6.

If u is an involution outside H, then $A \cap A^u = 1$, and hence $H \cap H^u$ is conjugate to a subgroup of $C_H(t)$.

H has a subgroups of order 6, and each is inverted by 6 involutions. Hence $|J_6| = 6a$.

H has a involutions, and each is inverted (i.e. centralized) by 30 involutions outside H. Hence $|J_2| + |J_6| = 30a$.

Likewise, since any subgroup of order 3 is inverted by $6d$ involutions (4.2), $|J_3| + |J_6| = 6da$. Let x be an element of order 3 in H, say $x \in N_G(Q)$. By (4.2), x is centralized by $2d$-2 involutions outside H; and since no such involution inverts a non-identity element of H, we get $c = 2(d - 1)a$. Since x centralizes an involution of Q, we cannot have $d = 1$. Thus $d = 3$.

It follows that $b_6 = a$, $b_3 = 4a$, $b_2 = 12a$, and $c = 4a$.

Now Lemma 3 yields (note that $|H| \geq 6\cdot 49 > 120 = |C_G(z)|$)

$$4a = c \leq b_1 \leq f^{-1}(a + 12a + 2\cdot 4a + 5a) - 12a - 4a - a.$$

Hence $21f < 26$. On the other hand,

$$f = |J|/|G:H| - 1 = 6a/120 - 1 \geq 49/20 - 1 = 29/20.$$

Thus $29 < 29\cdot 21/20 \leq 21f < 26$, a contradiction.

Next let $H = N_G(Q)$. Note that $|H| = 168 > |C_G(z)| = 120$, so that we are in a position to apply the lemma. In fact, $f = |J|/|G{:}H| - 1 = \frac{7}{5} - 1 = \frac{2}{5}$.

Let u be an involution outside H. Since Q is the centralizer of any four-group in H, $H \cap H^u$ has no subgroup of order 4. Hence the elements of H inverted by u form a subgroup of order 1, 2, 3, 6, or 7. This makes it easy to compute the numbers b_n, $n \geq 2$, and c.

H has 8 subgroups of order 7, and each is inverted by $7e$ involutions, with $e = 0$ or 1; see (4.3). Hence $|J_7| = 8\cdot 7e$.

H has $4\cdot 7$ subgroups of order 6, and each is inverted by 6 involutions. Hence $|J_6| = 4\cdot 7\cdot 6$.

H also has $4\cdot 7$ subgroups of order 3, and each is inverted by $6d$ involutions

(4.2). Hence $|J_3| + |J_6| = 4 \cdot 7 \cdot 6d$. Each subgroup X of order 3 is centralized by $2d - 1$ involutions (4.2). One of them lies in H, and $2e$ of them lie in J_7 because X normalizes 2 subgroups of order 7 in H. The remaining ones invert no non-identity element of H. Hence $c = 4 \cdot 7\,(2d - 2 - 2e)$.

Each of the 7 involutions of H commutes with 24 involutions outside H. Hence $|J_2| + |J_6| = 7 \cdot 24$, and thus $|J_2| = 0$.
We collect:

$$f = \tfrac{2}{5},$$

$$c = 8 \cdot 7\,(d - 1 - e) \quad \text{with} \quad e = 0 \quad \text{or} \quad 1,$$

$$b_1 = c + 7 \cdot 8 \cdot 3m \quad \text{with} \quad m \geq 0 \quad \text{an integer (see Lemma 2)},$$

$$b_3 = 8 \cdot 7\,(d - 1),$$

$$b_6 = 4 \cdot 7,$$

$$b_7 = 8e,$$

all other b_n equal 0, for $n \geq 1$.

Next we apply Lemma 3 to get information on m:

$$8 \cdot 7\,(d - 1 - e) + 7 \cdot 8 \cdot 3m$$
$$< \tfrac{5}{2}(7 + 2 \cdot 8 \cdot 7\,(d - 1) + 5 \cdot 4 \cdot 7 + 6 \cdot 8e) - 8 \cdot 7(d - 1) - 4 \cdot 7 - 8e.$$

This simplifies to

$$3m < \tfrac{5}{16} + 3d + \tfrac{25}{4} + \tfrac{15}{7}e - 5 + 1 + 1 - \tfrac{1}{2} - \tfrac{1}{7}e + e$$
$$< 3d + 3e + 3 + 1.$$

Hence

$$(4.4) \qquad m \leq d + e + 1 \leq 5.$$

From Lemma 1 we get

$$|J| = 7 + 8 \cdot 7\,(d - 1 - e) + 7 \cdot 8 \cdot 3m + 3 \cdot 8 \cdot 7\,(d - 1) + 6 \cdot 4 \cdot 7 + 7 \cdot 8e$$

which simplifies to

$$(4.5) \qquad |J| = 7(1 + 8(4d + 3m - 1)).$$

By (4.2), a subgroup of order 5 fixes exactly d involutions. Hence $|J| \equiv d \mod 5$. This together with (4.5) yields

$$(4.6) \qquad 5 \quad \text{divides} \quad 2d + 2m - 1.$$

Suppose $d = 1$. Then $m = 2$, by (4.4) and (4.6). Thus (4.5) yields $|G| = 8 \cdot 5 \cdot 3 \cdot 7 \cdot 73$. Fortunately, 73 is a prime. Let P be a subgroup of order 73. Then $|N_G(P) : P|$ divides $2 \cdot 3 \cdot 7$ since $C_P(x) = 1$ for all elements x of order

2 or 5 (or 3). Since obviously no divisor >1 of $8 \cdot 5 \cdot 3$ is $\equiv 1 \bmod 73$, we actually have $| G:N_G(P) | = 4 \cdot 5 \cdot 7x$ with x a divisor of 6. From $4 \cdot 5 \cdot 7 = 140 \equiv -6 \bmod 73$ we conclude that 73 divides $-6x - 1$.

This contradiction proves $d = 3$.

Next suppose $m = 0$. Then (4.5) yields $| G | = 8 \cdot 5 \cdot 3 \cdot 7 \cdot 89$. Let P be a subgroup of (prime) order 89. Since no divisor >1 of $8 \cdot 5 \cdot 3$ is $\equiv 1 \bmod 89$, and 88 is not divisible by 3 or 5, it follows that $| G:N_G(P) | = 4 \cdot 5 \cdot 3 \cdot 7x$ with $x = 1$ or 2. From $5 \cdot 3 \cdot 7 = 105 \equiv 16 \bmod 89$ we conclude that 89 divides $4 \cdot 16x - 1$, a contradiction.

Hence $m \neq 0$. Then (4.4) and (4.6) yield $m = 5$.

By (4.5), $| J | = 7(1 + 8(12 + 15 - 1)) = 7(1 + 208) = 7 \cdot 11 \cdot 19$.

Thus, the order of G is $8 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 19$.

Reference

Z. Janko, *A new finite simple group with abelian Sylow 2-subgroups and its characterization*, J. Algebra, vol. 3 (1966), pp. 147–186.

Universität
Kiel, West Germany