PACIFIC JOURNAL OF MATHEMATICS
Vol. 28, No. 2, 1969

FINITE GROUPS IN WHICH EVERY ELEMENT IS CONJUGATE TO ITS INVERSE

J. L. BERGGREN

Let $\mathfrak{S}$ denote the class of all finite groups all of whose irreducible characters over C (the complex numbers) are real. It is easy to verify, but important to observe, that this condition is equivalent to the condition that every element of the group is conjugate to its inverse (under an inner automorphism). Since $S_n \in \mathfrak{S}$, where S_n denotes the symmetric group on n letters, any finite group may be embedded in a group in $\mathfrak{S}$. The goal of § 1 will be to show that the two-Sylow subgroups of S_n also are in $\mathfrak{S}$, and, if A_n denotes the alternating group on n letters, that $A_n \in \mathfrak{S}$ if and only if $n \in \{1, 2, 5, 6, 10, 14\}$. The result on the two-Sylow subgroups of S_n will be used to show that any finite two-group is embeddable in a two-group in $\mathfrak{S}$. G. A. Miller has studied a class of groups related to those in $\mathfrak{S}$. The main theorem of § 2 gives a more intuitive characterization of the class of groups investigated by Miller, a consequence of which is a necessary and sufficient condition for a group in this class to be a member of $\mathfrak{S}$.

NOTATION. Throughout this paper we shall adhere to the notation of M. Hall [2], with these exceptions: $Fr(G)$ will denote the Frattini subgroup of the group G and GwH will denote the wreath product of G with H. The word "group" will denote a finite group. If $n, n_1, \cdots, n_k$ are positive integers then the symbol $\mathrm{n} = [n_1, \cdots, n_k]$ will mean $n = n_1 + \cdots + n_k$.

1. Burnside [1] observed that any nonidentity group in $\mathfrak{S}$ has even order. So, in investigating such groups one might start with those groups in $\mathfrak{S}$ that are two-groups. However, this section will show that, without additional hypotheses, there can be no general structure theorems for these.

THEOREM 1.1. *If $A = \langle a \rangle$ has order 2 and if $B \in \mathfrak{S}$ then $BwA \in \mathfrak{S}$.*

Proof. Since $(B, B^a) = 1$ and $B \in \mathfrak{S}$, elements of $B \times B^a$ are immediately conjugate to their inverses. It suffices, therefore, to consider elements in the coset $a(B \times B^a)$. These elements are of the form abc^a, where $b, c \in B$. But $abc^a = ac^ab = cab$ and $(cab)^c = abc$. Hence it suffices to consider elements of aB, say ab. Pick $x \in B$,

$b^x = b^{-1}$. Let $h = xx^a a$. Since $(a, xx^a) = 1 = (b, x^a)$, $(ab)^h = ab^{xa} = b^{-1}a = (ab)^{-1}$. Hence $BwA \in \mathfrak{S}$.

COROLLARY 1.1. *If T_n denotes a two-Sylow subgroup of S_n then $T_n \in \mathfrak{S}$.*

Proof. If $n = 2^m$ $(m = 1, 2, \cdots)$ then $T^n = (\cdots (CwC)wC)w \cdots)wC)$ is just the iterated wreath product of C m times, where C is the cyclic group of order 2, and the result follows from Theorem 1.1. But for arbitrary n, T_n is the direct product of groups of the above form. Since $A \times B \in \mathfrak{S}$ whenever A and B are in $\mathfrak{S}$, $T_n \in \mathfrak{S}$ for all n.

COROLLARY 1.2. *If G is any two-group then there exists a two-group $H \in \mathfrak{S}$ and a monomorphism $\tau : G \to H$.*

Proof. This follows from the Cayley Theorem and Corollary 1.1.

REMARK. Wreath-products are extremely useful in constructing counterexamples to conjectures about two-groups in $\mathfrak{S}$. For example: Let A and B be elementary abelian groups, of orders 2^m and 2^n respectively. Let $G = AwB$. Since any element of AwB may be written as the product of two involutions it is immediate that $G \in \mathfrak{S}$. But G has exponent 4 and nilpotence class at least n. So it is in general not possible to bound the class of $G \in \mathfrak{S}$ by bounding its exponent (except in the trivial case where the exponent is 2).

The only nilpotent groups in $\mathfrak{S}$ are two-groups. For $G = \prod_{i=1}^{n} H_i \in \mathfrak{S}$ if and only if $H_i \in \mathfrak{S}$ for $i = 1, \cdots, n$. It follows that, since any group in $\mathfrak{S}$ has even order, if G is any nilpotent group in $\mathfrak{S}$ then G is a two-group. Also, from Theorem 10.5.3 of [2], it follows that if G is super-solvable and if $G \in \mathfrak{S}$ then any two-Sylow subgroup of G is in $\mathfrak{S}$ (for if $G \in \mathfrak{S}$ then any homomorphic image of G is also in $\mathfrak{S}$).

Having shown that the two-Sylow subgroups of S_n are in $\mathfrak{S}$ for all n we shall now prove that $A_n \in \mathfrak{S}$ if and only if $n \in \{1, 2, 5, 6, 10, 14\}$. In particular we conclude that $\mathfrak{S}$ contains non-abelian simple groups.

The following terminology will be convenient in what follows. If $g \in A_n$ and $g = (u_1, \cdots, u_r) \cdots (v_1, \cdots, v_s)$ is an expression for g as a product of disjoint cycles then, setting $b = (u_2, u_r)(u_3, u_{r-1}) \cdots (v_2, v_s) \cdots$ yields $g^b = g^{-1}$. The above b will be called a *standard conjugator* of g.

THEOREM 1.2. *The alternating group $A_n \in \mathfrak{S}$ if and only if $n \in \{1, 2, 5, 6, 10, 14\}$.*

Proof. If $[n_1, \cdots, n_k]$ is a partition of n into distinct odd integers such that the number of $n_i \equiv 3(4)$ is odd then $A_n \notin \mathfrak{S}$. For, let g be any element of A_n corresponding to this partition. By Theorem 11.1.5 of [4], $[S_n: C_{S_n}(g)] > [A_n: C_{A_n}(g)]$. If $C_{S_n}(g) \nsubseteq A_n$ then $[S_n:C_{S_n}(g)] = [A_n: C_{S_n}(g) \cap A_n] = [A_n: C_{A_n}(g)]$, which is a contradiction. Thus, $C_{S_n}(g) \subseteqq A_n$. Since the number of $n_i \equiv 3(4)$ is odd the standard conjugator α of g is in $S_n - A_n$. If $g^\beta = g^{-1}$ for some $\beta \in A_n$ then $\alpha\beta \in C_{S_n}(g) \cap (S_n - A_n)$, which is a contradiction.

Next, notice that there exists a partition $[n_1, \cdots, n_k]$ of n into distinct odd integers such that the number of $n_i \equiv 3(4)$ is odd unless $n = 1, 2, 5, 6, 10, 14$. If $n = 4k$ then $[4k - 3, 3,]$ is such a partition. If $n = 4k + 3$ then $[4k + 3]$ is such a partition. If $n = 4k + 1$ then $n = [4k - 3, 3, 1]$ is such a partition provided $k > 1$ and, if $n = 4k + 2$, $k > 3$, then $[5, 1, 3, 4(k-1)-3]$ is such a partition. When $n = 1, 2, 5, 6, 10, 14$ every partition of n either contains an even integer, a repeated integer, or else the number of $n_i \equiv 3(4)$ is even.

Now if there exists an even integer or a repeated integer in a partition of n then any corresponding element $g \in S_n$ either is not in A_n or $[S_n: C_{S_n}(g)] = [A_n: C_{A_n}(g)]$, by Theorem 11.1.5 of [4]. In particular, g is conjugate to g^{-1} in A_n.

The remaining elements g of A_n correspond to partitions of n into distinct odd integers where the number of $n_i \equiv 3(4)$ is even. But this implies any standard conjugator of g is in A_n, so $g^\alpha = g^{-1}$ where $\alpha \in A_n$.

2. In [3] G. A. Miller examined the structure of those n-generator groups $M_n = \langle t_1, \cdots, t_n \rangle$ $(n > 1)$ such that $|t_i| > 2$ and $t_j^{-1}t_it_j = t_i^{-1}$, $1 \leqq i \neq j \leqq n$. We shall refer to M_n as the Miller group on n generators.

Let $M_n = \langle t_1, \cdots, t_n \rangle$ and $S = \{t_1, \cdots, t_n\}$. If $u, v \in S$ a short calculation shows that $|u| = 4$ and $u^2 = v^2$. Clearly, then, $|M_n^{(1)}| = 2$ and every element of M_n may be written uniquely apart from the order of the factors as $w \cdots z \cdot t_1^{2i}$, where w, $\cdots$, z and distinct elements of S and $i \in \{0, 1\}$. The main theorem of this section will show that M_n is built out of quaternion, dihedral, and cyclic groups. As a corollary we shall classify those n for which $M_n \in \mathfrak{S}$.

LEMMA 2.1. *Let* $g = s_1 \cdots s_m \cdot t_1^{2i} \in M_n$ *(where each* s_k *is a* t_j *and* $s_j = s_k$ *if and only if* $j = k$*). Then* $|g| = 4$ *if and only if* $m(m + 1) \not\equiv 0(4)$. *If, also,* $h = s'_1 \cdots s'_n \cdot t_1^{2k}$ *(with the same conditions on the* s'_i*) then* $(g, h) = t_1^{2\alpha}$, *where* $\alpha = mn - c(g, h)$ *and* $c(g, h) = |\{(i, k) \mid s_i = s'_k\}|$.

Proof. An easy calculation shows $g^2 = c^\beta$, where $\beta = m(m + 1)/2$ and $c = t_1^2$. As $|c| = 2$ the conclusion to the first part follows. Since all commutators are central and any commutator is equal to 1 or t_1^2

we have

$$\begin{aligned}(g, h) &= (s_1 \cdots s_m \cdot t_1^{2i},\ s_1' \cdots s_n' \cdot t_1^{2k}) \\ &= \prod_{\substack{1 \leqq i \leqq m \\ 1 \leqq j \leqq n}} (s_i, s_j') = t_1^{2\alpha} .\end{aligned}$$

THEOREM 2.1. *Let* $M_n = \langle t_1, \cdots, t_n \rangle$ *be the Miller group on* n *generators. Then there exist nonabelian groups of order* 8, $G_1, \cdots, G_k$ (*where* $k = k(n)$) *such that if* n *is even then*

$$M_n \cong (G_1 \times \cdots \times G_k)_A ,$$

whereas if $n \equiv 1(4)$

$$M_n \cong (G_1 \times \cdots \times G_k \times C_4)_A ,$$

and if $n \equiv 3(4)$

$$M_n \cong (G_1 \times \cdots \times G_k)_A \times C_2 ,$$

where $(\quad)_A$ *denotes the amalgamation of the square-generated subgroups of the factors and* C_r *is the cyclic group of order* r.

Proof: Define a new set of generators as follows:

$w_i = t_1 \cdots t_i$ $(i \geqq 1)$ and, for $i \geqq 3$, $u_i = t_i t_{i+1}$ and $v_i = w_{i-2} t_i$. It is clear that

$$\left.\begin{aligned} M_{4k} &= \langle t_1, t_2, u_3, u_5, \cdots, u_{4k-1}, v_4, v_6, \cdots, v_{4k} \rangle \\ M_{4k+1} &= \langle M_{4k}, w_{4k+1} \rangle \end{aligned}\right\} \ k > 0$$

and

$$\left.\begin{aligned} M_{4k+2} &= \langle M_{4k}, u_{4k+1}, v_{4k+1} \rangle \\ M_{4k+3} &= \langle M_{4k+2}, w_{4k+3} \rangle \end{aligned}\right\} \ \begin{aligned} &k \geqq 0, \text{ where we set } M_0 = \langle 1 \rangle \\ &\text{and } u_1 = t_1,\ v_1 = t_2. \end{aligned}$$

Now let $S_1 = \langle t_1, t_2 \rangle$, $S_3 = \langle u_3, v_4 \rangle, \cdots, S_{2k+1} = \langle u_{2k+1}, v_{2k} \rangle$. From Lemma 2.1. it follows that S_i is non-abelian of order 8 and that

$$\begin{aligned} M_{4k} &\cong (S_1^* \times \cdots \times S_{4k-1}^*)_A , && k > 0 \\ M_{4k+1} &\cong (S_1^* \times \cdots \times S_{4k-1}^* \times C_4)_A , && k > 0 \\ M_{4k+2} &\cong (S_1^* \times \cdots \times S_{4k+1}^*)_A \\ M_{4k+3} &\cong (S_1^* \times \cdots \times S_{4k+1}^*)_A \times C_2 \end{aligned}$$

where the S_1^* are disjoint copies of the S_i, $(\quad)_A$ denotes the amalgamation of the square-generated subgroups of the direct factors, and C_r is the cyclic subgroup of order r.

COROLLARY 2.1. *$M_n \in \mathfrak{S}$ if and only if $n \not\equiv 1(4)$.*

Proof. When $n \equiv 1(4)$ it follows from Theorem 2.1 that M_n has a central element of order 4; hence, in this case, $M_n \notin \mathfrak{S}$. If $n \not\equiv 1(4)$ it follows from Theorem 2.1 that M_n is the direct of product of either the identity group or C_2 with a factor group of a direct product of quaternion and dihedral groups. Since all of these groups are in $\mathfrak{S}$ it follows that $M_n \in \mathfrak{S}$.

It is possible, of course, to prove Corollary 2.1 directly without appealing to Theorem 2.1. However, since Theorem 2.1 is itself of some interest it seems better to prove things in the order they are done here.

The author wishes to thank C. Hobby for many valuable suggestions.

BIBLIOGRAPHY

1. W. Burnside, *The Theory of groups of finite order*, (2nd ed.) 1911, Dover, New York, 1955.
2. M. Hall, *The theory of groups*, MacMillan, New York, 1959.
3. G. A. Miller, *Second note on the groups generated by operators transforming each other into their inverses*, Quart. J. Math. **44** (1913), 142-146.
4. W. R. Scott, *Group theory*, Prentice-Hall, Englewood Cliffs, New Jersey, 1964.

Received October 25, 1967. This paper is part of the author's Ph. D. thesis. The author was supported by the Pre-Doctoral Traineeship Program of the National Aeronautics and Space Administration.