FINITE GROUPS IN WHICH ANY TWO PRIMARY SUBGROUPS OF THE SAME ORDER ARE CONJUGATE

Fletcher Gross

1. INTRODUCTION

Define a class $\mathscr{C}$ of finite groups as follows: the group G belongs to $\mathscr{C}$ provided that whenever H and K are subgroups of G of the same order, then H and K are conjugate in G. A. Machí [10] showed that if $G \in \mathscr{C}$ and some Sylow 2-subgroup of G is either an elementary abelian group of order 4 or a quaternion group of order 8, then A_4, the alternating group on 4 letters, is involved in G. The hypothesis $G \in \mathscr{C}$ seems so strong that it is natural to expect a stronger conclusion than Machí's result. One of the main results of the present paper is that if $G \in \mathscr{C}$, then $G/O_{2'}(G)$ is isomorphic to one of the following groups: a cyclic 2-group, A_5, $SL_2(5)$, $PSL_2(8)$, $P\Gamma L_2(32)$, A_4, $SL_2(3)$, or specific solvable groups of orders 56, 168, or 4,960. Thus the only simple nonabelian groups in $\mathscr{C}$ are A_5 and $PSL_2(8)$.

If p is a prime, the class $\mathscr{C}_p$ consists of the finite groups G with the property that whenever H and K are p-subgroups of the same order in G, then H and K are conjugate in G. Finally, let $\mathscr{D}$ consist of the groups that belong to $\mathscr{C}_p$ for every prime p. Clearly, $\mathscr{C} \subseteq \mathscr{D}$; but the reverse is not true. In Theorem 1, we list all the possibilities for $G/O_{2'}(G)$ if $G \in \mathscr{D}$. This immediately leads to the classification of groups belonging to $\mathscr{C}$.

2. NOTATION AND PRELIMINARY RESULTS

All groups considered in this paper are assumed to be finite. We use repeatedly the fact that the classes $\mathscr{C}$, $\mathscr{C}_p$, and $\mathscr{D}$ are closed under the operation of taking factor groups. J_1 denotes the simple group of order 175,560, discovered by Z. Janko [9]. If p is a prime and n is a positive integer, then the groups $R(p^n)$, $S(p^n)$, and $T(p^n)$ are defined as follows: Let V be the additive group of the field $GF(p^n)$, and let λ be a primitive $(p^n - 1)$th root of unity in $GF(p^n)$. Let A and B be the automorphisms of V defined by

$$vA = \lambda v \quad \text{and} \quad vB = v^p \quad \text{for } v \in V.$$

Then A and B generate a group $T(p^n)$ of order $n(p^n - 1)$. The semidirect product of V and the cyclic group generated by A is denoted by $R(p^n)$, while the semidirect product of V and $T(p^n)$ is denoted by $S(p^n)$. The orders of $R(p^n)$ and $S(p^n)$ are $p^n(p^n - 1)$ and $np^n(p^n - 1)$, respectively. All other notation is as in D. Gorenstein's book [5].

LEMMA 1. *Suppose* $G \in \mathscr{C}_p$ *and* P *is a Sylow* p-*subgroup of* G. *Then one of the following is true:*

Received February 14, 1972.
This research was supported in part by the National Science Foundation.

Michigan Math. J. (19) 1972.

(i) P *is a cyclic group;*

(ii) P *is an elementary abelian group;*

(iii) P *is a quaternion group of order* 8, *and* $p = 2$;

(iv) P *is a nonabelian group of order* p^3 *and exponent* p, *and* $p > 2$.

This was proved by R. Armstrong [1] under a weaker hypothesis. As will be seen, the last possibility cannot occur if $G \in \mathscr{D}$.

LEMMA 2. *Suppose that* $G \in \mathscr{C}_p$ *for an odd prime* p, *that* P *is a Sylow* p-*subgroup of* G, *and that* H *is a normal* p-*solvable subgroup of* G. *Assume* p *divides* $|H|$. *Then* P *is abelian, and either* $P \subseteq H$ *or* P *is cyclic.*

Proof. Under the hypothesis of the lemma, all subgroups of order p in G are contained in H and are conjugate in G. If P is not cyclic, the previous lemma implies that P has exponent p, from which it follows that $P \subseteq H$. Then $PO_{p'}(H)/O_{p'}(H)$ must be contained in $Z(O_{p'p}(H)/O_{p'}(H))$. Hence P is abelian.

LEMMA 3. *Suppose that* $G \in \mathscr{C}_p$, *and that* P, *a Sylow* p-*subgroup of* G, *is an elementary abelian group of order* $p^n \geq p^3$. *Let* $N = N_G(P)$ *and* $K = O_{p'}(N)$. *Assume that* N/K *is solvable (this must be the case if* $p = 2$, *by the theorem of W. Feit and J. Thompson* [4]). *Then one of the following is true:*

(i) $n = 3$ *and* N/K *is isomorphic to a subgroup of* $S(p^3)$; *if* $p = 2$, *then* N/K *is isomorphic either to* S(8) *or to* R(8);

(ii) $n = 5$, $p = 2$, *and* N/K *is isomorphic to* S(32).

Proof. Since P is abelian, a theorem of Burnside [5, Theorem 7.1.1] implies that two subgroups of P are conjugate in G if and only if they are conjugate in N. Hence $N \in \mathscr{C}_p$. Consequently, it is sufficient to prove the lemma in the special case $G = N$ and $K = 1$. Then, by the theorem of Schur and Zassenhaus, P has a complement H in G. Since G is solvable and $O_{p'}(G) = 1$, $C_G(P) = P$ [5, Theorem 6.3.2]. This implies that H is faithfully represented as a group of automorphisms of P. Since $G \in \mathscr{C}_p$, H transitively permutes the subgroups of order p in P. Similarly, H transitively permutes the subgroups of order p^2 in P. Now let L be the group of power automorphisms of P (in other words, let L consist of the automorphisms σ for which there is an integer m such that $x^\sigma = x^m$ for all $x \in P$). L is the center of Aut(P); therefore, considering H as a subgroup of Aut(P), we see that HL is a solvable subgroup of Aut(P). Clearly, HL transitively permutes the nonidentity elements of P. Since $n > 2$, Theorem 19.9 of [11] implies that either we may identify P with the additive group of $GF(p^n)$ in such a way that HL is a subgroup of $T(p^n)$, or else $p = 3$ and $n = 4$.

For the exceptional case, when HL is not a subgroup of $T(p^n)$, B. Huppert [7] shows that $|HL|$ is one of the numbers $2^7 \cdot 5$, $2^6 \cdot 5$, and $2^5 \cdot 5$. However, when $p = 3$ and $n = 4$, P contains exactly 130 distinct subgroups of order 9. Since H transitively permutes these subgroups, 130 must divide $|H|$, which is impossible.

Thus we may identify P with the additive group of $GF(p^n)$ in such a way that H is contained in $T(p^n)$. It then follows that G is a subgroup of $S(p^n)$. Since H transitively permutes the $(p^n - 1)/(p - 1)$ subgroups of order p in P, $|H|$ must be divisible by $(p^n - 1)/(p - 1)$. If $n = 3$ and $p = 2$, then $|H|$ must be divisible by 7. Since $|T(8)| = 21$, $|H|$ must be 7 or 21. It follows that $G = R(8)$ or S(8) when $n = 3$ and $p = 2$. The lemma is now proved for $n = 3$.

Assume $n > 3$. Then $|H|$ divides $|T(p^n)| = n(p^n - 1)$, and H transitively permutes the $(p^n - 1)(p^n - p)/(p^2 - 1)(p^2 - p)$ distinct subgroups of order p^2 in P.

It follows from this that $(p^n - 1)(p^n - p)$ divides $n(p^n - 1)(p^2 - 1)(p^2 - p)$. Hence $(p^{n-1} - 1)$ divides $n(p^2 - 1)(p - 1)$.

However, if $n \geq 6$, then $p^{n-1} - 1 > n(p^2 - 1)(p - 1)$. Thus $n = 4$ or $n = 5$. Suppose $n = 4$. Then $(p^3 - 1)$ divides $4(p^2 - 1)(p - 1)$. Therefore $(p^2 + p + 1)$ must divide $4(p^2 - 1)$. Since $(p^2 + p + 1, 4) = 1$, this implies that $(p^2 + p + 1)$ divides $(p^2 - 1)$, an impossibility.

Thus $n = 5$. Therefore $(p^4 - 1)$ divides $5(p^2 - 1)(p - 1)$. This implies that $(p^2 + 1)$ divides $5(p - 1)$. This can happen only if $p = 2$ or $p = 3$. In both of these cases, the fact that $(p^5 - 1)(p^5 - p)/(p^2 - 1)(p^2 - p)$ divides $|H|$, together with the fact that H is a subgroup of $T(p^5)$, implies that $H = T(p^5)$.

Hence $G = S(p^5)$, and either $p = 2$ or $p = 3$. Suppose $p = 3$. $T(3^5)$ contains exactly one element of order 2, and this element normalizes every subgroup of order 9 in P. Thus, if Q is a subgroup of order 9 in P, then $|H : N_H(Q)| \leq |H|/2$. Since the number of subgroups of order 9 in P is $|H|$ and H transitively permutes these subgroups, we have a contradiction. Therefore, $n = 5$ implies that $p = 2$ and $G = S(32)$.

3. THE MAIN RESULTS

THEOREM 1. *Suppose* $G \in \mathscr{D}$. *Then* $G/O_{2'}(G)$ *is isomorphic to one of the following:*

(i) *a cyclic* 2-*group*,

(ii) R(8),

(iii) S(8),

(iv) S(32),

(v) J_1,

(vi) $PSL_2(8)$,

(vii) $P\Gamma L_2(32)$,

(viii) $PSL_2(p)$,

(ix) $PSL_2(p^3)$,

(x) $SL_2(p)$,

(xi) $SL_2(p^3)$.

In (viii), (ix), (x), *and* (xi), p *is a prime and* $p \equiv \pm 3 \pmod 8$. *Conversely, each of the groups listed belongs to* $\mathscr{D}$.

Proof. We leave it to the reader to verify that the groups listed do belong to $\mathscr{D}$. Suppose $G \in \mathscr{D}$. Without loss of generality, we may assume that $O_{2'}(G) = 1$. Let Q be a Sylow 2-subgroup of G. If Q is cyclic, then G has a normal 2-complement [5, Theorem 7.6.1]. Since $O_{2'}(G) = 1$, it follows that $G = Q$.

We now assume that Q is not cyclic. Lemmas 1 and 3 then imply that Q is either a quaternion group of order 8 or an elementary abelian group of order 4, 8, or 32. Assume first that Q is abelian of order 2^n ($n = 2$, 3, or 5).

Case 1. G is solvable.

Since Q is abelian, Theorem 1.2.6 of [6] implies that G has 2-length 1. Since $O_{2'}(G) = 1$, the subgroup Q must be normal in G. Since $C_G(Q) = Q$ [5, Theorem

6.3.2], G must be isomorphic to a subgroup of the holomorph of Q. Since all involutions are conjugate in G and $|G/Q|$ is odd, we easily deduce that G is isomorphic to A_4 when $n = 2$ (A_4 is included in our list in (viii), since A_4 is isomorphic to $PSL_2(3)$). If $n = 3$ or $n = 5$, Lemma 3 implies that G is isomorphic to one of the groups R(8), S(8), or S(32).

Case 2. G is not solvable.

The main result of [13] implies that G has a normal subgroup H such that $|G/H|$ is odd and $H = A \times B_1 \times \cdots \times B_r$, where A is an abelian 2-group and $B_1, \cdots, B_r$ are simple groups chosen from the following list:

(a) J_1,

(b) $PSL_2(q)$, where q is a prime power ($q \geq 5$) and $q \equiv \pm 3 \pmod 8$,

(c) $PSL_2(2^m)$ ($m \geq 2$),

(d) a group of Ree type [14].

Now H' is normal in G, and $H' = B_1 \times \cdots \times B_r$. Since $G \in \mathscr{D}$, H' must contain all involutions in G. Hence A = 1. Since $B_1, \cdots, B_r$ are simple nonabelian groups, conjugation by elements of G permutes the factors. Thus, if $r > 1$ and t_i is an involution in B_i for i = 1, 2, then $t_1 t_2$ is an involution that is not conjugate to t_1. Hence r = 1, and therefore H is a simple group.

It follows that $C_G(H) \cap H = 1$. Since $|G/H|$ is odd, $|C_G(H)|$ must be odd. Therefore, $C_G(H) \subseteq O_{2'}(G) = 1$. Thus we may consider G as a subgroup of Aut(H) and identify H with the inner automorphism group.

If H is a group of Ree type, then a Sylow 3-subgroup of H is not cyclic and is not of exponent 3 [14]. Since this contradicts Lemma 1, H is not of Ree type.

If $H = J_1$, then Aut(H) = H [9], and therefore $G = J_1$. If $H = PSL_2(2^m)$, we need consider only m = 3 and m = 5, since $|Q| = 4$, 8, or 32, and since $PSL_2(4)$, being isomorphic to $PSL_2(5)$, is included in (b).

Suppose $H = PSL_2(8)$. Then Aut(H) = HF, where F is cyclic of order 3 and consists of the field automorphisms [12]. Thus G = H or G = HF. Since the subgroups of order 3 in HF are not all conjugate, $G \neq HF$. Hence $G = PSL_2(8)$.

Suppose now $H = PSL_2(32)$. Because $\mathrm{Aut}(H) = 5|H|$ (see [12]), the group G is either $PSL_2(32)$ or $\mathrm{Aut}(PSL_2(32))$. Now $|PSL_2(32)|$ is not divisible by 5, whereas Lemma 3 implies that $|N_G(Q)|$ is divisible by $2^5 \cdot 5 \cdot 31$. Hence $G \neq PSL_2(32)$. Therefore $G = \mathrm{Aut}(PSL_2(32)) = P\Gamma L_2(32)$.

Now assume that $H = PSL_2(q)$, where $q = p^s$ (p a prime) and $q \equiv \pm 3 \pmod 8$. Then s is odd and $p \equiv \pm 3 \pmod 8$. If s = 1, then $|\mathrm{Aut}(H)| = 2|H|$. Since $|G/H|$ is odd, it would follow that $G = PSL_2(p)$.

Suppose now $s > 1$. Let P be a Sylow p-subgroup of G. P cannot be cyclic, since $P \cap H$ is an elementary abelian group of order p^s. Lemma 1 implies that P has exponent p. Since H is normal in G and $G \in \mathscr{D}$, it follows that $P \subseteq H$. Now $N_H(P)$ is solvable (the subgroups of $PSL_2(q)$ are given in [3, page 285]) and G/H is solvable. Since $s \geq 3$, we can apply Lemma 3 to show that s = 3.

Therefore $|\mathrm{Aut}(H)| = 6|H|$, and hence $|G/H| = 1$ or 3. It follows that either G = H or G = HF, where F is cyclic of order 3 and consists of the field automorphisms [12]. However, 3 divides $|H|$, and therefore not all subgroups of order 3 in HF are conjugate. Hence $G = PSL_2(p^3)$.

We have now proved Theorem 1, provided Q is not a quaternion group of order 8. If Q is a quaternion group of order 8, then $|Z(G)| = 2$ [2]. It is easily verified that $O_{2'}(G/Z(G)) = 1$. Hence our previous work implies that $G/Z(G)$ is isomorphic either to $PSL_2(p)$ or to $PSL_2(p^3)$. From the theory of Schur multipliers [8, page 646], it follows that G is isomorphic to $SL_2(p)$ or $SL_2(p^3)$. Hence Theorem 1 is proved.

COROLLARY. *Suppose* $G \in \mathscr{D}$ *and* P *is a Sylow subgroup of* G. *Then one of the following is true:*

(i) P *is cyclic;*

(ii) P *is an elementary abelian group;*

(iii) P *is a quaternion group of order* 8.

Proof. If $P \cap O_{2'}(G) \neq 1$, then Lemma 2 implies that P is abelian. If $P \cap O_{2'}(G) = 1$, then P is isomorphic to a Sylow subgroup of $G/O_{2'}(G)$, and the result now follows from the theorem.

THEOREM 2. *Suppose* $G \in \mathscr{C}$. *Then* $G/O_{2'}(G)$ *is isomorphic to one of the following:*

(i) *a cyclic* 2-*group*,

(ii) R(8),

(iii) S(8),

(iv) S(32),

(v) $PSL_2(8)$,

(vi) $P\Gamma L_2(32)$,

(vii) A_4,

(viii) A_5,

(ix) $SL_2(3)$,

(x) $SL_2(5)$.

Conversely, the groups listed do belong to $\mathscr{C}$.

Proof. J_1 does not belong to $\mathscr{C}$, since J_1 has two conjugacy classes of groups of order 60 [9]. Now suppose q is a power of a prime $(q > 5)$, and $q \equiv \pm 3 \pmod 8$. Let $e = 1$ if $q \equiv 3 \pmod 8$ and $e = -1$ if $q \equiv -3 \pmod 8$. Then $PSL_2(q)$ contains a cyclic group of order $(q + e)/2$ and also a dihedral group of the same order. Hence $PSL_2(q)$ does not belong to $\mathscr{C}$. Since $PSL_2(q)$ is a factor group of $SL_2(q)$, we see that $SL_2(q) \notin \mathscr{C}$. Deleting J_1, $PSL_2(q)$, and $SL_2(q)$ for $q > 5$ from the list in Theorem 1, we arrive at Theorem 2 (note: A_4 is isomorphic to $PSL_2(3)$, and A_5 is isomorphic to $PSL_2(5)$). We leave it to the reader to verify that the remaining groups belong to $\mathscr{C}$.

4. RESULTS ON SOLVABLE GROUPS

The fact that $J_1 \in \mathscr{D}$ but $J_1 \notin \mathscr{C}$ shows that $\mathscr{D} \neq \mathscr{C}$. An example of a solvable group belonging to $\mathscr{D}$ but not to $\mathscr{C}$ is constructed as follows: Let A be the additive group of GF(25), and let B be the additive group of GF(49). Let λ be a primitive 24th root of unity in GF(25), and μ a primitive 48th root of unity in GF(49). Let V be the direct product of A and B, and let T be the automorphism of V defined by

$(u, v)T = (\lambda u, \mu v)$. Finally, let G be the semidirect product of V and T. Then G is solvable of order $2^4 \cdot 3 \cdot 5^2 \cdot 7^2$. It is easy to verify that $G \in \mathscr{D}$ ($G \in \mathscr{C}_2$, for example, since a Sylow 2-subgroup of G is cyclic). $G \notin \mathscr{C}$, however, since G has 2 conjugacy classes of subgroups of order 35.

THEOREM 3. *Suppose* G *is a solvable group belonging to* $\mathscr{D}$. *Assume that for all but at most one prime* p, *the Sylow* p-*subgroups of* G *are cyclic. Then* $G \in \mathscr{C}$.

Proof. We use induction on $|G|$. Suppose H and K are subgroups of the same order in G, and let M be a minimal normal subgroup of G. Then M is an elementary abelian p-group for some p.

Since $G \in \mathscr{C}_p$, we may assume (by replacing H by one of its conjugates, if necessary) that $H \cap K$ contains a Sylow p-subgroup of H and K. Then $H \cap M = K \cap M$. This implies that $|HM| = |KM|$.

Suppose $H \cap M = 1$. Since M must contain all subgroups of order p in G, p cannot divide $|H|$. By induction, HM/M and KM/M are conjugate in G/M. But H is a Hall p'-subgroup of HM, and K is a Hall p'-subgroup of KM. Thus H and K would be conjugate.

Now suppose $H \cap M \neq \{1\}$. If $H \cap M = M$, then $HM = H$ and $KM = K$. By induction, H/M and K/M would be conjugate, and this would imply that H and K are conjugate.

Finally, suppose $1 < |H \cap M| < |M|$. Since M contains all subgroups of order p in G and M cannot be cyclic (clearly, $|M| \geq p^2$), the corollary to Theorem 1 implies that M is a Sylow p-subgroup of G. Hence the Sylow q-subgroups of G for $q \neq p$ are cyclic. Let $N = N_G(H \cap M)$. Then H, K, and M are all contained in N. By the theorem of Schur and Zassenhaus, M has a complement L in N. By a theorem of Hall [5, Theorem 6.4.1], we may assume, by replacing H and K by conjugates under N, that $H \cap M = K \cap M$ and that L contains a Hall p'-subgroup A of H and a Hall p'-subgroup B of K. Now all the Sylow subgroups of L are cyclic. Hence $L \in \mathscr{D}$. By induction, we see that $L \in \mathscr{C}$. But

$$|A| = |H/H \cap M| = |HM/M| = |KM/M| = |B|.$$

Hence $A = B^x$ for some $x \in L$. Therefore $K^x = (B(H \cap M))^x = A(H \cap M) = H$.

Remark. Theorem 3 becomes false if we omit the hypothesis that G is solvable. J_1 satisfies the remainder of the hypothesis, but $J_1 \notin \mathscr{C}$.

COROLLARY. *If all the Sylow subgroups of the group* G *are cyclic, then* $G \in \mathscr{C}$.

Proof. Clearly, $G \in \mathscr{D}$. By [5, Theorem 7.6.2], G is solvable. The corollary now follows from the theorem.

If G is a solvable group belonging to $\mathscr{D}$, then the following statements are true: (i) the nilpotent length of G is at most 3; (ii) the derived length of G is at most 4; (iii) if a Sylow 2-subgroup of G is not a quaternion group, then the derived length of G is at most 3; (iv) G is a Sylow tower group.

These results are not difficult to prove, and they were obtained by Armstrong [1] under a similar but different hypothesis. Since Armstrong's ideas can be applied effectively here, I have omitted proofs of these statements. The upper bounds on the nilpotent length and derived length are best possible, as is shown by examples in [1].

REFERENCES

1. R. Armstrong, *Finite groups in which any two subgroups of the same order are isomorphic.* Proc. Cambridge Philos. Soc. 54 (1958), 18-27.

2. R. Brauer and M. Suzuki, *On finite groups of even order whose* 2-*Sylow group is a quaternion group.* Proc. Nat. Acad. Sci. U.S.A. 45 (1959), 1757-1759.

3. L. E. Dickson, *Linear groups with an exposition of the Galois field theory.* Teubner, Leipzig, 1901.

4. W. Feit and J. G. Thompson, *Solvability of groups of odd order.* Pacific J. Math. 13 (1963), 775-1029.

5. D. Gorenstein, *Finite groups.* Harper and Row, New York, 1968.

6. P. Hall and G. Higman, *The* p-*length of* p-*soluble groups and reduction theorems for Burnside's problem.* Proc. London Math. Soc. (3) 6 (1956), 1-42.

7. B. Huppert, *Zweifach transitive, auflösbare Permutationsgruppen.* Math. Z. 68 (1957), 126-150.

8. ———, *Endliche Gruppen. I.* Grundlehren, Band 134. Springer-Verlag, Berlin, 1967.

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

10. A. Machì, *On a class of finite groups.* (Italian summary) Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur. (8) 48 (1970), 147-151.

11. D. Passman, *Permutation groups.* Benjamin, New York, 1968.

12. R. Steinberg, *Automorphisms of finite linear groups.* Canad. J. Math. 12 (1960), 606-615.

13. J. H. Walter, *The characterization of finite groups with abelian Sylow* 2-*subgroups.* Ann. of Math. (2) 89 (1969), 405-514.

14. H. N. Ward, *On Ree's series of simple groups.* Trans. Amer. Math. Soc. 121 (1966), 62-89.

University of Utah
Salt Lake City, Utah 84112