CCN-GROUPS OF ORDER DIVISIBLE BY THREE PRIMES

HERBERT J. BERNSTEIN

1. **Introduction.** This paper continues the study of the nature of finite groups such that each cyclic subgroup of composite order is normal (CCN-groups) begun in [1], and is devoted to a proof of the following partial refinement of [1, Theorem 10.5, p. 306].

THEOREM 1.1. *Let G be a finite group of order divisible by at least three distinct primes. Then every cyclic subgroup of G of composite order is normal in G if and only if G is either*

(i) *isomorphic to A_5, the alternating group on five letters, or*

(ii) *Abelian, or*

(iii) *Hamiltonian, or*

(iv) *a split extension of an Abelian group A by a cyclic group $\{t\}$ of prime order p such that for all $x \in A$*

$$\text{(a) } (tx)^p = 1, \qquad \text{and} \qquad \text{(b) } txt^{-1} \in \{x\}.$$

The proof will use results from [1] and the following lemma.

LEMMA 1.2. *Let G be a finite group such that each cyclic subgroup of G of composite order is normal in G. Let G contain at least one element of composite order. Then the subgroup generated by the elements in G of composite order is of prime or trivial index in G.*

It is an immediate consequence of this lemma that the recursiveness of the characterization of CCN-groups given in Theorem 10.5 of [1] may be suppressed in all cases. The properties of CCN-groups of order divisible by at most two primes are still under investigation.

The difficulty with the remaining cases is that, for a CCN-group of order divisible by at most two primes, it is possible for the subgroup generated by the elements of composite order to be a p-group of nilpotence class two, or for the entire group to consist of elements of prime order yet not be A_5. In the first instance, simple conditions to restrict even the p-group to the class of CCN-groups are at present lacking, and the action of the remaining elements on this subgroup, while easily described, lacks the simplicity of case (iv) of Theorem 1.1, above. (See Theorem 10.5 of [1, p. 306].)

The degenerate case of a finite group without elements of com-

Presented to the Society, September 4, 1968; received by the editors September 24, 1968.

posite order has been handled in Theorem 8.1 of [**1**, p. 299], which is proven by appeal to powerful theorems from the literature. The author expects that similar tools will be required to obtain finer detail, since the structure of the Burnside groups of prime exponent would be needed for a final answer. (See Coxeter and Moser [**3**, pp. 80–82], for information on Burnside groups.)

Aside from their structure, CCN-groups are of interest because a version of Hajós' theorem holds for them. For further information on that topic, see in particular [**1**, pp. 289–290].

2. **Notation.** Let $\in$ denote the inclusion of an element in a set.

Denote by $\{x_\alpha\}$ the group generated by the items x_α enclosed.

For a finite group G, denote by $NP(G)$ the subgroup generated by elements of composite order.

Call a finite nontrivial group G a CCN-group if every cyclic subgroup of G of composite order is normal in G.

3. **Proof of Lemma 1.2.** The proof of Lemma 1.2 makes use of the techniques of Burnside [**2**, §248].

If $G=NP(G)$ we are done. Suppose $G\neq NP(G)$. Give $w\in G$, $w\notin NP(G)$. By the definition of $NP(G)$, w is of prime order p. If G is generated by w and $NP(G)$, $NP(G)$ being characteristic in G, the proof will be complete. On the other hand, for the remaining case we will obtain a contradiction.

Suppose there exists $v\in G$, $v\notin \{w, NP(G)\}$. v is of some prime order q. By hypothesis, there exists $x\in NP(G)$ of composite order. Since G is a CCN-group, we define automorphisms w^* and v^* on $\{x\}$ by

$$w^*(x) = wxw^{-1}, \qquad v^*(x) = vxv^{-1}.$$

As in the proof of Theorem 9.1 of [**1**, p. 300], it is easy to show w^* and v^* to be nontrivial. By Lemma 10.1 of [**1**, p. 304], $wvw^{-1}v^{-1}$ commutes with x, whence w^* commutes with v^*. If $p\neq q$, then w^*v^* is of order pq, which implies wv to be of composite order, i.e. $wv\in NP(G)$. This in turn implies $v\in \{w, NP(G)\}$, contrary to construction. Therefore $p=q$ and $\{w^*, v^*\}$ is of order p or of order p^2.

Suppose $\{w^*, v^*\}$ to be of order p. Then $v^*\in\{w^*\}$, i.e. there is an integer α such that vw^α commutes with x. By the construction of v, vw^α is of prime order. Now either $\{vw^\alpha\}$ has nontrivial intersection with $\{x\}$ or $vw^\alpha x$ has order a multiple of that of x. In the first case we would have, by the primeness of the order of vw^α, $vw^\alpha\in NP(G)$, and in the second case $vw^\alpha x\in NP(G)$, both contrary to the construction of v. Hence $\{w^*, v^*\}$ is of order p^2.

Let $\tau\in\{w^*, v^*\}$, $\tau\neq 1$. We know $\tau^p=1$. As in the proof of Theorem

9.8 of [1, p. 303], it is easy to show that

$$x\tau(x)\tau^2(x)\cdots\tau^{p-1}(x) = 1.$$

Now take

$$\tau_1 = v^*w^*,\ \tau_2 = v^*(w^*)^2,\ \cdots,\ \tau_p = v^*(w^*)^p = v^*,$$

for which we have

$$\begin{aligned} x\tau_1(x)\tau_1^2(x)\cdots\tau_1^{p-1}(x) &= 1,\\ x\tau_2(x)\tau_2^2(x)\cdots\tau_2^{p-1}(x) &= 1,\\ &\ \,\vdots\\ x\tau_p(x)\tau_p^2(x)\cdots\tau_p^{p-1}(x) &= 1, \end{aligned}$$

whence, by multiplying the left-hand sides together,

$$\begin{aligned} 1 &= x^p(\tau_1(x)\tau_2(x)\cdots\tau_p(x))\cdots(\tau_1^r(x)\tau_2^r(x)\cdots\tau_p^r(x))\cdots\\ &\quad\cdot(\tau_1^{p-1}(x)\tau_2^{p-1}(x)\cdots\tau_p^{p-1}(x))\\ &= x^pv^*(w^*(x)(w^*)^2(x)\cdots(w^*)^{p-1}(x)x)\cdots\\ &\quad\cdot(v^*)^r((w^*)^r(x)((w^*)^r)^2(x)\cdots((w^*)^r)^{p-1}(x)x)\cdots\\ &= x^p(v^*(1))^{p-1} = x^p. \end{aligned}$$

This contradicts the assumption that x was of composite order, which completes the proof.

4. **Proof of Theorem 1.1.** We prove sufficiency first. A_5 contains no subgroups of composite order; thus all such subgroups it contains are normal. Every subgroup of an Abelian or Hamiltonian group is normal; a fortiori every cyclic subgroup of composite order is normal. It remains to consider case (iv). Suppose G to be so defined. Let $x\in A$. Define $\tau(x)=txt^{-1}$. Then, by (a), $\tau(x)\tau^2(x)\cdots\tau^p(x)=1$, whence, by the commutativity of A and Lemma 9.5 of [1, p. 301], every element of G of composite order is an element of A. Again by the commutativity of A and by (b), every cyclic subgroup of A, a fortiori every cyclic subgroup of G of composite order, is normal in G. Thus conditions (i) through (iv) are sufficient for G to be a CCN-group.

We now prove necessity. Suppose G is a CCN-group of order divisible by three distinct primes.

Suppose G contains no elements of composite order. By Theorem 8.1 of [1, p. 299], either G is isomorphic to A_5 or is of order divisible by at most two primes, whence, by the hypothesis that G is of order divisible by at least three primes, G is isomorphic to A_5.

Now suppose G to contain at least one element of composite order. By Theorem 10.3 of [1, p. 305], $NP(G)$ is either Abelian, Hamiltonian, or a p-group of nilpotence class two. By Lemma 1.2 and the hypothesis on the order of G, $NP(G)$ is not a p-group.

If $G=NP(G)$ we are done. Assume $G\neq NP(G)$. By Lemma 1.2 and by Theorem 9.8 of [1, p. 303], G is a split extension of $NP(G)$ by a cyclic group $\{t\}$ of prime order p such that, among other conditions, $(tx)^p=1$, for all $x\in NP(G)$. By Lemma 10.2 of [1, p. 304], since $NP(G)$ is not a p-group, $txt^{-1}\in\{x\}$ for all $x\in NP(G)$. It only remains to show that $NP(G)$ is Abelian rather than Hamiltonian. But if $NP(G)$ were Hamiltonian, it would be of even order, which, by Theorem 10.4 of [1, p. 305], implies $NP(G)$ to be of even index in G. This, in turn, implies, by Theorem 9.2 of [1, p. 300], that $NP(G)$ was actually Abelian. This completes the proof.

References

1. H. J. Bernstein, *Extension of Hajós' factorization theorem to some non-Abelian groups*, Comm. Pure Appl. Math. **21** (1968), 289–311.

2. W. Burnside, *Theory of groups of finite order*, 2nd ed., Dover, New York, 1955.

3. H. S. M. Coxeter and W. O. Moser, *Generators and relations for discrete groups*, 2nd ed., Ergebnisse der Mathematik, Bd. 14, Springer-Verlag, New York, 1965.

Courant Institute of Mathematical Sciences, New York University