A CONDITION FOR A FINITE GROUP TO BE CYCLIC

J. H. E. COHN

Abstract. A finite group, with the property that for every prime power \( q = p^k \) there are at most \( p^{k+1} - 1 \) elements in the group whose \( q \)-th power is the identity, is a cyclic group.

It seems to be well known that a finite group, which need not be given to be abelian, must be cyclic if for every positive integer \( n \), the number of elements for which \( x^n \) is the identity does not exceed \( n \). The object of this note is to prove the stronger

**Theorem.** Let \( G \) be a finite group, with identity \( e \), such that for every prime power \( q = p^k \) there exist at most \( p^{k+1} - 1 \) elements satisfying \( x^q = e \). Then \( G \) is cyclic.

**Proof.** Suppose that \( p \nmid o(G) \), with say \( p^m \| o(G) \). Let \( H \) denote any Sylow \( p \)-subgroup. Then choosing \( q = p^{m-1} \) it follows that \( H \) is cyclic, since it has at least one element whose order does not divide \( q \).

Furthermore, \( H \) is the only Sylow \( p \)-subgroup, and so is a normal subgroup of \( G \). For in the contrary case, there would exist at least \( p + 1 \) distinct cyclic Sylow \( p \)-subgroups, no two of which could contain an element of order \( p^m \) in common. Thus they would contain together at least \( (p + 1)p^{m-1}(p-1) + p^{m-1} = p^{m+1} \) distinct elements, all of which would satisfy \( x^q = e \) with \( q = p^m \), contrary to hypothesis.

Thus \( G \) must be the direct product of its Sylow subgroups, each one of which is cyclic, and accordingly \( G \) must be cyclic.

**Corollary.** Every noncyclic finite group has for at least one prime power \( p^k \), at least \( p^{k-1}(p^2 - 1) \) elements of order \( p^k \) exactly.

**Proof.** Suppose on the contrary that for every prime power \( p^k \) there were less than \( p^{k-1}(p^2 - 1) \) elements of order \( p^k \). Now the number of such elements is divisible by \( p^{k-1}(p-1) \), for each one generates a cyclic subgroup with this number of generators. Thus there can be at most \( p^k(p-1) \) elements of order \( p^k \) for every prime power. But then there would be at most \( p^{k+1} - p + 1 \leq p^{k+1} - 1 \) elements satisfying \( x^q = e \) for every prime power \( q = p^k \), and the group would be cyclic by the theorem.

Department of Mathematics, Royal Holloway College, Englefield Green, Surrey, England

Received by the editors May 7, 1971.

AMS 1970 subject classifications. Primary 20A05; Secondary 20D20.

Key words and phrases. Finite group, cyclic group, order of element.